Specific Research Reports of the National Institute of Industrial Safety, NIIS-SRR-NO.27 (2002)
UDC 66.012-52; 681.536.5; 62-551.454

9. コンピュータを用いるプラント設備の安全制御設計手法と安全性評価

池田博康*, 齋藤　剛*, 杉本　旭**

9. Safety Control Design and Safety Evaluation for Computerized Plant System

by Hiroyasu IKEDA*, Tsuyoshi SAITO* and Noboru SUGIMOTO**

Abstract **:** With advancement of large-scaled plants, the use of a computer increases in the control, and there is a tendency that programmable equipment including a micro-processor is introduced into a hardware safety related system based on conventional electromagnetic relays. Because reliability of normal hard-wired system is low, and a fault diagnosis capability is uncertain and insufficient, it is a trend to replace the hard-wired with a flexible and functional software. However, as for such a programmable controller, indistinct characteristics remain in the use in safety security still, and, for example, potential systematic failures which can not be identified may appear and cause unsafe conditions.

A functional safety standard of programmable electronic safety systems is established and this standard divides instrumentation of an automatic control system into safety related part and control part. This standard requires expressing the safety integrity as unreliability. Therefore, general-purpose programmable controllers shall not be used as safety related parts when the characteristics of the controllers can not be analyzed and evaluated. The safety interlock system must be consisted with special consideration on safety in order to apply programmable equipment in a safety related parts.

This report proposes layered control systems with the functional controller and the safety interlock controller based on the concept of independent protection layers in case of adopting programmable equipment. And the role of each controller and safe performance required for safety integrity levels are examined. In addition, a safety function of process control is confirmed by a simple heat exchanger model. This model has three process controllers and one safety interlock system with a three channel programmable controller. Powerful self-checking functions and a diverse structure of the programmable controller can improve total safety integrity level of the heat exchange process.

Keywords**;** Process safety, Safety control, Safety interlock, Independent protection layer, Diversity, Redundancy

* 機械システム安全研究グループ　Mechanical and System Safety Research Group
** 北九州市立大学国際環境工学部環境機械システム工学科　The University of Kitakyusyu, Faculty of Environmental Engineering, Department of Mechanical Systems and Environmental Engineering

1. はじめに

プラント設備の大型化・高度化に伴い，その制御にコンピュータを利用することが多くなってきており，従来の電磁リレーを基本とするハードウェア安全関連システムにもコンピュータをはじめとするプログラマブル機器が導入される傾向にある。通常のハードワイヤシステムの信頼性が低く，故障等に対する診断能力が不確実で不十分であるため，フレキシブルで高機能のソフトウェアに代替することは自然な流れではある。しかし，このようなプログラマブルな制御器は安全性確保上，その利用には未だ不明な特性が残存しており，例えば，潜在的なシステマティック故障のように特定が困難な状況が起こり得る。

最近，電気・電子・プログラマブル電子安全関連系の機能安全規格が制定され，自動制御系の計装を安全関連部と制御（非安全関連）部に分けて，安全性を不信頼度によって表現することが求められている。したがって，汎用的な高機能プログラマブル機器が複雑であるが故に解析・評価ができない場合は，これをそのまま安全制御器として使用することはできない。プログラマブル機器を安全関連部に適用するためには，特別な安全上の配慮を施したシステムが構成されていなければならない。

本研究では，プログラマブル機器によるプロセス制御を設計するに当たり，独立防護階層の考え方に基づいて，機能的な制御器と安全制御器を階層的に組み合わせた制御システムを提案する。そして，各々の制御器の役割と要求される安全性能について検討を加える。また，簡単な熱交換器モデルによってプロセス制御の安全機能について検証を行う。

2. 安全計装システムと階層的防護

2.1 独立防護階層による安全機能

化学プラント分野では，安全化のためのリスク低減手法を体系的に整理する考え方として，独立防護階層（Independent protection layer：以下IPL）の概念が提唱されている[1)]。一般に，プラントが取り扱う物質自体の危険性やそれらの漏洩，爆発等が，プラント内外の人間や環境に与える影響は非常に大きい。そのため，プラントの運用時の安全対策のみならず，設計段階から廃棄に至るまでの全ライフサイクルにおいてリスクを総合的に低減する必要がある。IPLは，プラントプロセスの物理化学特性や機械設備要素，制御，オペレータの操作などに基づく種々のリスク低減方策を階層的に構築する。

Table 1 は，IPL各層の目的と内容を示したものであり，このような考え方は原子力プラントにおける深層防護と同様のものである。

Table 1　Contents of independent protection layers (IPL).
独立防護階層（IPL）の内容

階　層	名　　称	具　　体　　例
第１層	プロセス設計	プロセス設計における本質安全の領域。同じ目的のプロセスでも，温度や圧力をより下げられないか，危険物の滞留量を最小化できないか，といった検討を行う。
第２層	基本プロセス制御システム（BPCS）	分散形制御システム（DCS）など，通常運転時のプラント監視を主目的とするシステム。BPCS は，プロセス値が設定値から逸脱した際に警報を発し，オペレータの介入を要求する。
第３層	BPCS が発する警報と区別された「重要警報」	オペレータの介入のために必要な時間的余裕がある場合に適用される。
第４層	自動安全計装システム／緊急停止装置	計装による安全インターロックシステム（SIS）や緊急停止装置などにより，自動的にプラントを安全に停止させる。
第５層	物理的防御（安全弁）	圧力逃がし弁などの過圧防御システム。
第６層	物理的防御（防液堤）	液体の漏洩を局所化するための防液堤など。
第７層	プラント内緊急対応計画	事業所内の緊急時対応計画。
第８層	地域防災計画	地域住民や公共設備に対する緊急時対応計画。

IPLの特徴は，

① リスク評価に基づく安全システム設計を行う，
② リスク低減方策はその性質により分類される，
③ 危険事象の拡大に応じた防護の始動時間によって階層化される，

ことにあり，リスク低減方策の準備には優先順位[2]があることに注意を要する。すなわち，リスクの低減は，危険源自体を除去するか，リスク要因（危害の影響、発生頻度）を下げることによるが，前者は本質安全設計（第 1 層）によればリスクを生じないから後者より優先される。また，後者は，設計上の工夫，物理的手段，制御やインターロックによって実現するが，設計段階においては，通常，物理的手段（第 5，6 層）は制御（第 2 層），インターロック（第 4 層）に比べて自由度は制約を受ける。そこで，物理的手段を優先して設計する。なお，人間が介入あるいは関与する手段は最後に適用される。

IPLは**Table 1** で分類される方策を，対象の危険源が事象として発現・拡大していく過程において，それらが機能し始める時刻順で表現したものである。よって，より低層で危険事象の拡大を確実に防止することが望まれる。重要な点は，これらの防護層は各々独立に機能して，仮に低い層の方策が危険事象の阻止に失敗しても，より高い層の効果に全く影響を及ぼさないことが保証されることである。この独立性はリスク評価を簡便にするとともに，オペレータも独立層としてリスク低減に寄与すべきことを求めている。プラントの場合は，機能停止による経済的損失も勘案して総合的なリスク評価を行うため，オペレータの危険回避動作もシステムの一部と見なされるためである。

2.2 安全インターロックシステムの位置付け

IPLの第 2 層と第 4 層は共に制御器という範疇でまとめられ，外見上は同じものに見えることが多いが，その役割は全く異なるものである。第 2 層の制御器は運転制御器と呼ばれ，高機能な分散型制御システム（DCS）などが利用される。一方，第4層は安全制御器として，安全インターロックシステム（Safety interlock system：以下SIS）が構成される。これは，緊急時にプロセスを安全側に停止させる（緊急遮断：ESD）ものであり，**Fig. 1** に示すように，第 2 層の機能とは無関係にプロセスに作用する。

したがって，正常プロセス進行時は運転制御器のみが機能して通常動作を継続し，プロセス結果が制御器の制限を越えると，制御器あるいは別途制限器が警報を発してオペレータの回復操作を要求する。

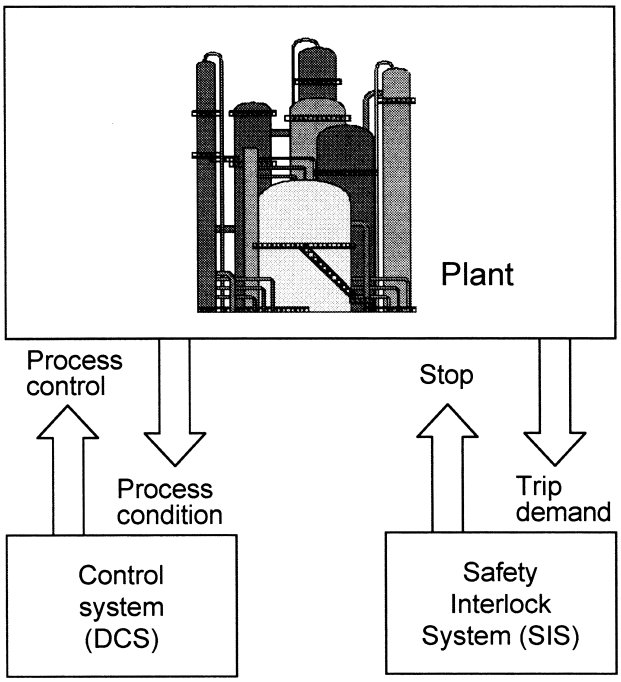

Fig. 1 Safety control system of plant.
プラント設備の安全制御システム

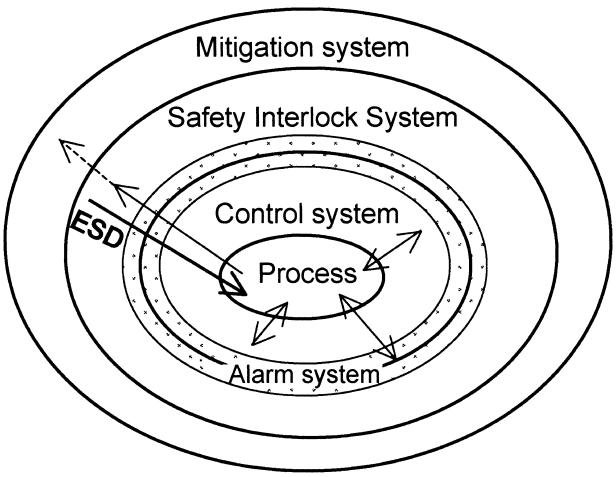

Fig. 2 Concept and relationship of layers of IPL.
IPLの概念と各階層間の関係

しかし，それでもプロセスが修正されずに緊急遮断のトリップレベルまで達すると，はじめてSISが他の全ての操作・制御に優先して機能する。すなわち，IPLに基づく安全計装システムでは，制御と安全の部分を明確に分けて，制御は安全が確保された条件下もしくは場の中に含まれるように構成されねばならない。**Fig. 2** にその概念を示すが，SISが制御器の機能も兼務することは可能であるが，その逆は許

されない構成である。それ故，SISはプラント設備や制御器の故障や異常に対して監視して対処するばかりでなく，自身の故障に対しても確実なインターロックを実行する能力，すなわち自己診断機能とフェールセーフ特性を持つことが必要条件となる。

2.3　安全計装へのプログラマブル機器の導入

電磁リレーは，リレー接点のロジックがそのままインターロックを実現できるため，安全計装用途に従来から広く利用されてきた。近年では，接点の強制解離機構を持ついわゆる安全リレーユニット[3]が普及して，フェールセーフ特性が向上した製品が入手可能となっている。しかし，このような簡単なリレー計装システムだけで大規模プラント設備に対応するのはもはや現実的でなく，また，誤トリップの可能性も小さくない上に配線異常等のシステム自己診断は難しい。

そのため，高機能化，高信頼化されたDCS等のプログラマブル機器を安全計装システムへ導入しようとすることは，自然な流れと言える。高信頼化ハードウェアがもたらす高い稼働率とプログラムによる機能設計の自由度の高さは，プログラマブル機器に強力な自己診断機能を与える。ただし，通常は制御用に特化した設計がなされるために，入出力信号の変化を前提としたリアルタイム性重視の診断が行われ，滅多に変化しない緊急遮断信号に対して故障を検出することは困難である。

一方，SISのような専用安全計装システムをプログラマブル機器で構成する場合，DCSのハードウェアとの大きな違いはないが，潜在危険故障を徹底して除去し，さらに緊急遮断信号を活性化してこの信号の頻繁な故障検出を可能とする[4]。故障の物理化学的現象が十分に把握できないプログラマブル機器は，古典的なフェールセーフ素子（例えば，巻き線抵抗器）のように故障モードを特定できないが，周期的な自己診断間隔を短くすることによって，診断の間に起こる故障による不安全事象の発生確率を小さくすることができる。なお，このような自己診断は，計装システムの入力から出力までカバーしなければならず，制御器の出力結果をフィードバックする安全ループが形成されねばならない。

プログラマブル機器が本質的に固有の安全の場を提供できず，故障特性が把握できない場合は，周期的診断による高信頼度維持がフェールセーフ化への唯一のアプローチとなる。そこで，改めてフェールセーフシステムの安全性について検討する。

3.　機能安全規格に基づく安全度水準

3.1　フェールセーフと不信頼度

近年，国際安全規格類の条文で「フェールセーフ」という言葉が姿を消しつつある。プログラマブル電子機器の安全関連系の機能安全規格JIS C 0508[5]（IEC61508）では，「故障時システムを安全状態に移行させること」と説明されており，「ハードワイヤシステムで，定義された欠陥群で安全状態に移行し，かつ，それらが検出される場合は，装置はフェールセーフに動作すると言われる。」と記述されている。ところが，一方では，システムが複雑で欠陥モードが定義できないこともあると認めて，その場合はフェールセーフが確認できないので概念の適用は不適切，とも説明されている。

他の規格類でも，このような理由から表現が消えていると推定されるが，この規格の本意は，安全性を求める場合にはフェールセーフ概念を除外するのではなく，本来フェールセーフを確立した上で高機能化を図るものと捉えることとする。つまり，対象機器のテスト（診断）を行って，その結果がフェールセーフ概念を満たすことと定義する。ISO/IEC Guide-51[6]によれば，危険性をリスクで表し，「安全」を受容可能なリスクと規定しているように，国際規格は絶対安全を要求してはいない。したがって，絶対的なフェールセーフ手法は実現できないが，よりフェールセーフに近い手法を適用して，故障時には許容リスクレベル以下を実現するものとする。

JIS規格C 0508は，安全性を不信頼度で評価することを要求している。そして，周期的なプルーフテスト（チェック）をすれば不信頼度を低く保てること，そのチェック時に異常がなければ信頼度は最高（すなわち 1）であることを初めて示した規格である。安全関連系が定められた期間，全ての定められた条件で要求される安全機能を果たす確からしさを安全度と定義して，安全度を不信頼度で示すことによって安全性の水準を決めている。これまで，安全性の高さと信頼性の高さが混同されることがあったが，この規格によって明確に安全度水準が定義された。

3.2　安全性の指標

前述の機能安全規格では，安全計装システムの安全性を対象システムの作動要求時に必ず正しく働くことが理想としている。つまり，SISの作動要求が正常時にあれば安全停止（遮断）が期待できるが，故障時にあった場合は停止できずに危険が拡大する

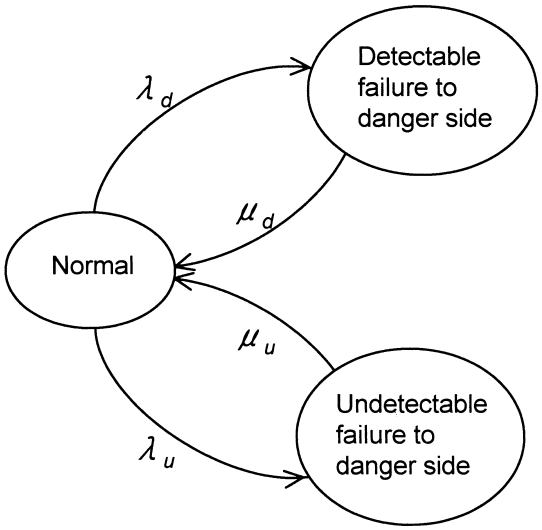

Fig. 3 Decrease of TFM by self-check.
自己診断によるTFMの低減モデル

恐れが生ずるわけであり，これを不信頼度として数字で表して安全度水準を求めることになる。

この不信頼度を全時間中の危険故障率TFMとして定義すると，潜在する危険故障をいかに漏れなく検出できるかが重要な問題となる。**Fig. 3** は自己診断によって潜在危険故障を低減する様子をマルコフモデルとして表したものだが，検出可能な危険故障状態は故障修復の間隔が小さいほど，また，潜在危険故障はプルーフテスト間隔が小さいほど不信頼度が小さくなることが分かる。この関係は次式で表される。

$$TFM=\lambda_d(MTTR)+\frac{1}{T}\int_0^T \lambda_u \cdot tdt \\ =\lambda_d(MTTR)+\lambda_u(\frac{T}{2}) \quad (1)$$

ここで，$MTTR$は平均修復時間，λ_dは検出可能な危険故障率，λ_uは潜在危険故障率であり，$\mu_d=1/MTTR$，$\mu_u=1/(T/2)$，また，Tはプルーフテスト間隔である。

いま，メンテナンスによって機能が完全に回復するものとすれば，TFMを改めて目標故障限度として潜在危険故障率とテスト間隔のみでシステムの安全度水準を定める指標とすることができる。機能安全の規格ではSISの動作要求頻度に応じて目安が示されており，1 回/年以下の頻度で，かつTの 2 倍より大きくない場合，**Table 2** の使用開始後の平均故障率，すなわち作動要求当たりの設計上の機能失敗平均確率で与えられる。作動要求が 1 回/年より大きい頻度で，かつTの 2 倍より大きい場合，**Table 3** で示すように連続運転中に生じる単位時間当たりの危険側故障率で与えられる。いずれも安全度水準SILは 1 ～ 4 まで設定され，SILが大きいほど要求される故障確率は小さくなる。例えば，高頻度要求モードでSIL 4（ここでは危険側故障率が 10^{-9}/h）のシステムの場合，この水準を維持しようとすると，少なくとも起動後 10 時間以内に試験を行って，安全機能が正しく動作することを確認（プルーフ試験）しなければならない。TFMを用いることによって，必要とする安全度水準のプルーフ試験間隔が定まることは，システムのメンテナンスの方法に応じて安全性が影響を受けることになる。

なお，本規格では，システムの要素にマイクロプロセッサのような故障モードやその挙動が把握できないものを用いる場合は，診断カバレッジ（検出可能な危険故障発生率と全危険故障発生確率の比）の値によってシステム構成が制約を受ける。例えば，診断カバレッジが 100 %ではない場合，多重の蓄積

Table 2 Safety integrity level of low demand mode of operation.
低頻度作動要求モードにおける安全度水準

SIL	低頻度作動要求モード
4	$10^{-5} \leqq TFM < 10^{-4}$
3	$10^{-4} \leqq TFM < 10^{-3}$
2	$10^{-3} \leqq TFM < 10^{-2}$
1	$10^{-2} \leqq TFM < 10^{-1}$

Table 3 Safety integrity level of high/continuous demand mode of operation.
高頻度作動要求/連続モードにおける安全度水準

SIL	高頻度作動要求／連続モード
4	$10^{-9} \leqq TFM < 10^{-8}$
3	$10^{-8} \leqq TFM < 10^{-7}$
2	$10^{-7} \leqq TFM < 10^{-6}$
1	$10^{-6} \leqq TFM < 10^{-5}$

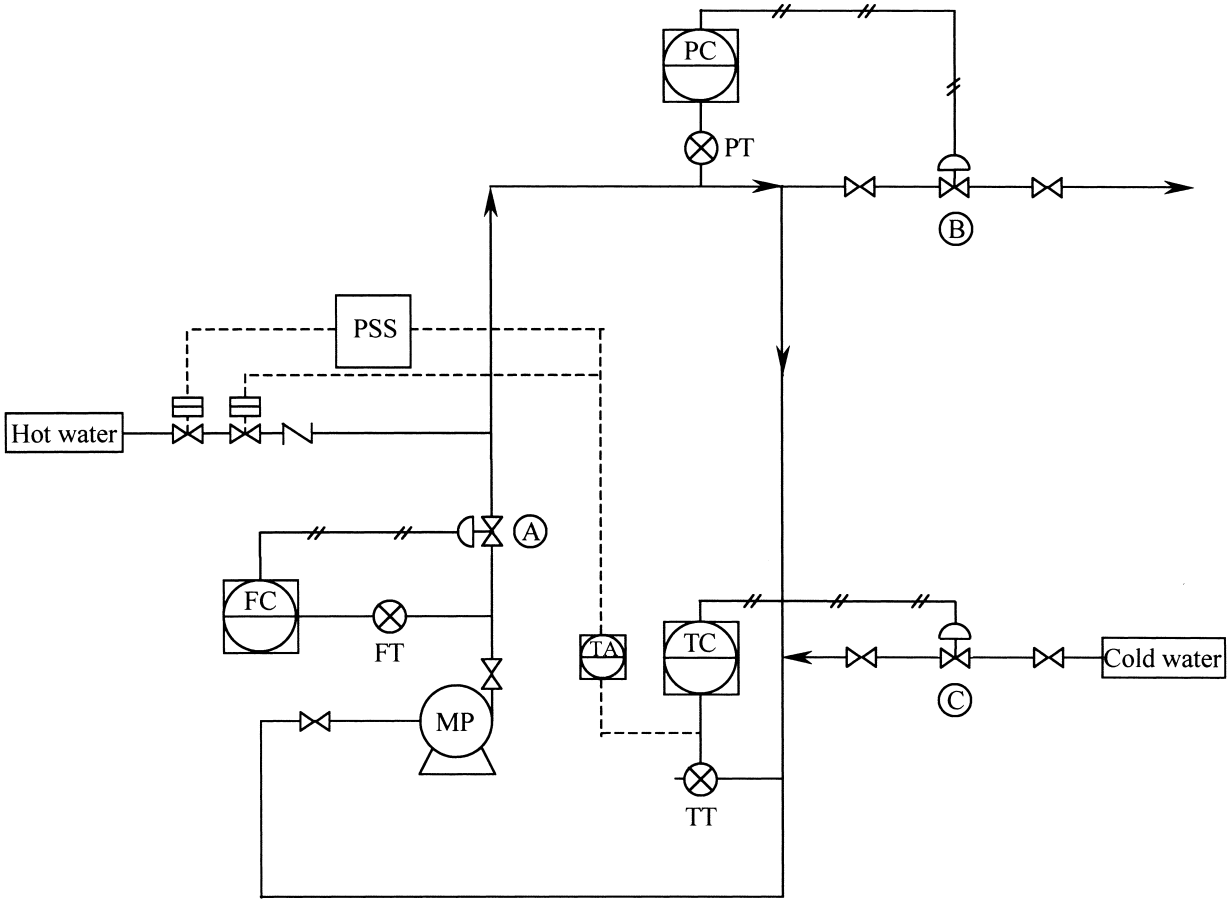

Fig. 4　Heat exchanger model with three controllers and one safety interlock system.
3制御器と1安全インターロックシステムを有する熱交換モデル

故障まで勘案する必要が生じて，より多重のシステム構成が要求されることになる。

4. 熱交換モデルによる安全性検証

4.1 熱交換モデルの概要

プログラマブル機器を導入したプラント設備の安全性を検証するため，本研究では，簡単な熱交換プロセス制御システムを準備した。基本的には，一定流量の定温水を供給するための設備として，ボイラにより沸かした温水に冷水を加えてポンプにより配水するものである（**Photo 1**）。

Fig. 4 は熱交換モデルの基本構成を示しており，温度制御器TCにより冷水流入量を冷水供給バルブCを介して調整し，流量制御器FCによりポンプMPから吐出される温水混合水の流量を流量調整バルブAを介して調整する。また，圧力制御器PCにより循環管路内の圧力を排水バルブBを介して調整すると共に配水量を調整する。温水は温度制御のないガスボイラにより供給され，水温センサTTの情報に応じて

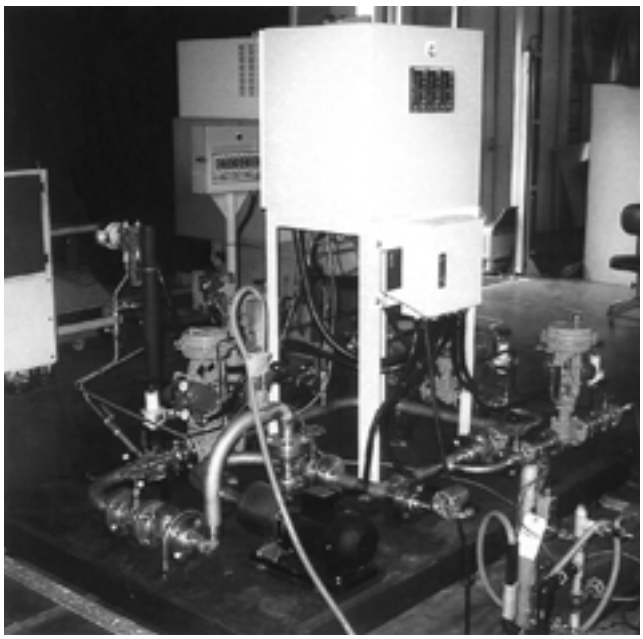

Photo 1　Exterior of heat exchanger model.
熱交換モデル外観

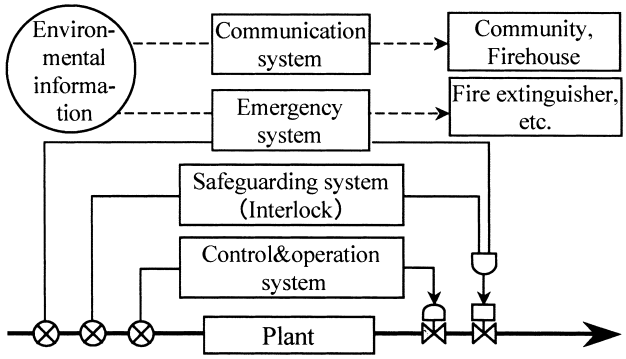

Fig. 5 Protection layers of heat exchanger model.
熱交換モデルの防護階層構成

Table 4 Parameters of PID controls for heat exchange process.
熱交換プロセスのためのPID制御パラメータ

制御仕様	温度制御系 TC	圧力制御系 PC	流量制御系 FC
比例帯 P (%)	700	150	799.9
積分時間 I (min)	0.5	0.5	0
微分時間 D (min)	0.1	0	0

供給/遮断が切り替えられるように安全制御器PSS（三重化ダイバシティ・プログラマブルコントローラ[7]）により電磁バルブが制御される。なお，バルブA，B，Cは全てパイロット式空気圧駆動型としている。

このPSSは**Table 1** の第 4 防護層となるように，3つの制御器とは独立して**Fig. 5** のような配置としている。PSSにより，熱交換プロセスにおいてリスクの大きな温水供給系の遮断を行わせると共に，ボイラ系においてもガス供給が遮断されて燃焼停止するというインターロックが組み込まれている。

ただし，第 5 層以降の防護方策（**Fig. 5** の破線に示す）については，制御システムとは無関係なので今回は形成していない。

3 つの制御器による通常のプロセス制御は，次の基本アルゴリズムによって実行される。

(1) 温度制御系

温度センサTTの出力情報に基づきPID（比例・積分・微分）制御を行い，バルブCの開度を調整する。TT出力が温度上限レベルを越えると，温水供給バルブを遮断すると共に警報を出力する。

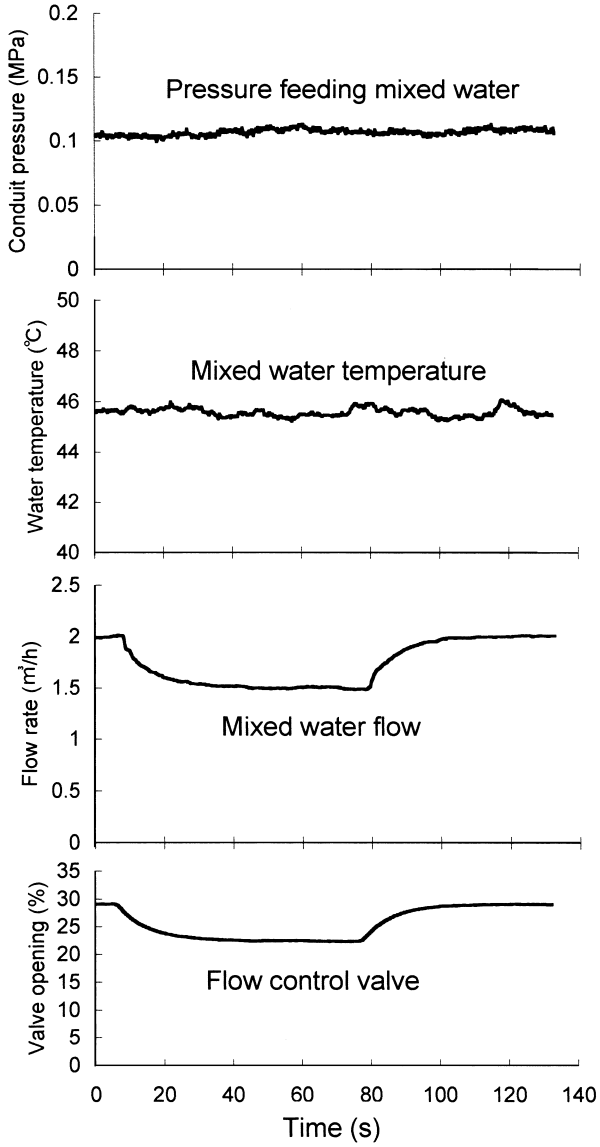

Fig. 6 Example of process control by three controllers.
3つの制御器によるプロセス制御結果例

(2) 流量制御系

流量センサFTの出力情報に基づきP制御を行い，バルブAの開度を調整する。ポンプによる混合水循環後に機能する。

(3) 圧力制御系

圧力センサPTの出力情報に基づきPI制御を行い，バルブBの開度を調整する。温水流入後に機能する。

各制御系の制御パラメータは，ボイラの温水供給能力（約 60℃，2 m^3/h max）と冷水供給能力（2 m^3/h max），及び配管サイズ（3/4 inch）を考慮した上で，試行錯誤の結果，**Table 4** に示す値を設定した。

Fig. 6 は，3 つの制御系を同時に機能させた場合のプロセス制御結果を記録したものであり，水温，流量，圧力の各々の定常制御状態から流量を変化させたときの各制御系の振る舞いを示している。バルブAを強制的に一部閉じるために，流量制御器FCの出力を手動で 6 %ほど下げた場合に，水温と圧力を定常値に維持したまま，実際の循環水路の混合水流量がFC出力に追従していることが分かる。

4.2　SISの構成と安全度水準

SISを構成する安全制御器PSSは，異種多重化PLC（プログラマブル・ロジックコントローラ）であり，異なるメーカのマイクロプロセッサを三重化することによって機能的に非対称故障特性を向上させているものである。この構造や機能の詳述は文献[8] に譲るが，マイクロプロセッサを利用することにより前述の診断カバレッジが低下することの補償として，3 out of 3 の冗長形態となっている。また，温水供給系は，温度制御器による通常遮断とSISによる緊急遮断の二重構成としている。

SISの機能を確認するため，プロセスの定常状態から冷水供給を停止させて混合水の温度を過上昇させた結果を**Fig. 7** に示す。バルブCを強制的に閉じるために，温度制御器TCの出力を徐々にゼロまで低下させた場合に，水温の上昇が始まり，設定済みの遮断温度 50℃を越えるとインターロックが機能し，非励磁型電磁バルブが遮断していることが分かる。このような機能は，温度制御器による正常プロセスから逸脱して警報が出力されたときにオペレータが回復操作をしない，あるいは失敗した場合に初めて発現する。したがって，インターロックが機能していない正常プロセス時に，いかにSISの安全性を証明するかが問題となる。

一般に，冗長構成のハードウェアに対する安全性評価では，次の項目が重要とされる[9]。

（a）故障検出のためにオンラインで行われる自己診断性能と時間間隔

（b）冗長構成に共通する故障（欠陥）を回避するためのダイバーシティ

（a）については，マイクロプロセッサを利用する場合，診断カバレッジを高くしようとすると個別要素に対するプルーフテスト間隔が長くなる恐れがある。つまり，時間のかかる厳重な診断中に，他の診断されない部分で多重の故障が蓄積される可能性が増すことになる。このような多重故障に対しては，**Fig. 3** のように簡単にモデル化できないため，プルーフテスト間隔を算出することは難しい。単一故障

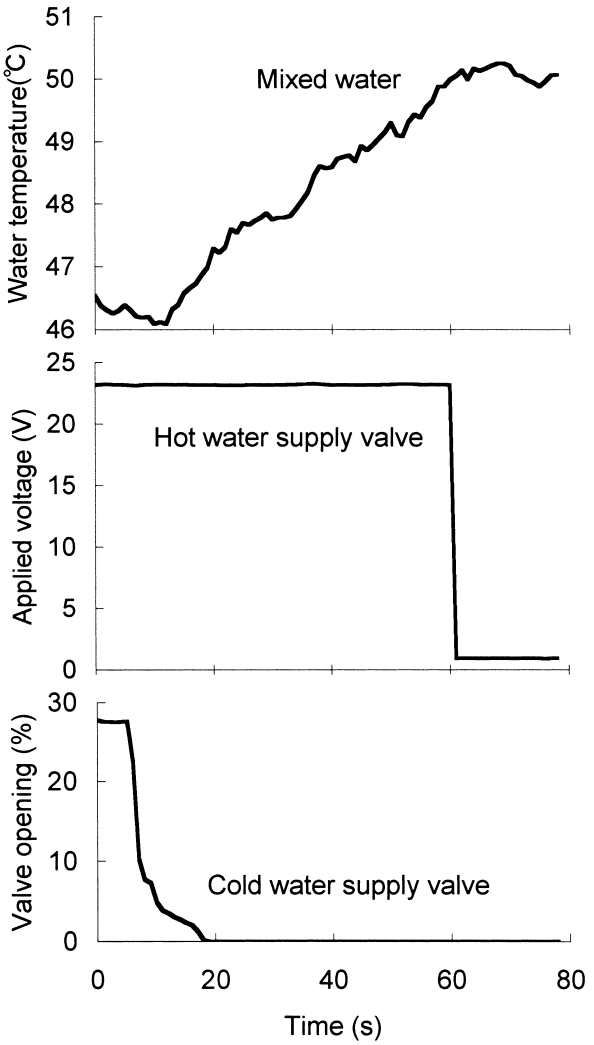

Fig. 7　Example of SIS process for shutdown of hot water supply.
温水供給系遮断のSISプロセス例

によって制御システムが危険側に誤らないという前提であれば，同時危険故障発生確率の 1/1000 の頻度でテストを行うことが規定されている例[10]がある。また，三重の故障に対するプルーフテスト間隔については，三重同時危険故障発生確率をP_{a2}，二重故障のプルーフテスト間隔をT_2とすると

$$T_2 \leq \frac{2}{P_{a2}} \qquad (2)$$

という算定式[10] が示されている。これによると，例えば，1 年間に約 1 回以上の頻度で二重故障の診断を行う必要のある場合，三重同時故障の発生に対する危険故障評価が要求されることになり，結局四重の冗長構成が必要とされる。

このような共通原因故障の存在による冗長問題を解決する手段が（b）の技法であり，冗長系全てが

同様な故障に対する振る舞いをする可能性を小さくすることが可能となる。今回利用した異種多重化PLCはこの手法の採用により，同時多重故障発生確率が 4×10^{-20}/h，潜在多重蓄積故障発生確率が 3.2×10^{-13}/hと算定されており[7]，要求されるプルーフテスト間隔は年単位となる。実際の自己診断は約30sほどで行われるため，安全度水準*SIL*は 4 以上を確保でき，十分な安全性が達成されていると判断できる。

ただし，SIS全体の*SIL*は，SISと接続されるサブシステム（今回は温度センサと温水供給バルブ）の平均故障率の和で定まるため，SIS全体の*SIL*はこれらのサブシステムの安全性によって左右される。*SIL*は故障率の 10 倍の順序で規定されているため，故障率の大小の組み合わせは大きな故障率，すなわち小さな*SIL*に支配されることになる。今回利用したセンサとバルブの具体的データがないため算定はできなかったが， 通常機械系のバルブの*SIL*は低く見積もられる。そのため，より高い*SIL*が要求されるシステムでは，SIS系におけるバルブの冗長構成とバルブのSISによる診断が不可欠となろう。

5. まとめ

プロセス制御の安全計装システムにプログラマブル機器を利用する場合，少なくとも従来のリレー等を用いたハードワイヤシステムと同等以上の安全性が確保されねばならない。高機能でフレキシブルなプログラマブル機器であっても，特別な安全への配慮が必要になる。

ここでは，インターロックを基本とする安全制御の役割をシステムの独立防護階層の考え方に基づいて明確にし，機能的な制御器と安全制御器を階層的に組み合わせた制御システムを提案した。プロセス制御システム全体の安全性は診断機能の安全性に大きく依存することになるため，SISを構成する安全制御器には異種多重化PLCを利用して，安全度水準の向上が図れる。今後は，SISの論理システム以外のサブシステムを含めた総合的安全性評価と診断手法について検討を進める必要がある。

参考文献

1）AIChE/CCPS，Guidelines for Safe Automation of Chemical Processes， AIChE, p. 14 （1993）.
2）AIChE/CCPS，Guidelines for Engineering Design for Process Safety， AIChE, pp. 6-7 （1993）.
3）安全技術応用研究会，日経メカニカル編，21 世紀の安全技術，日経BP社，pp.52-65（1999）.
4）三平律雄，“3 of 3” に基づいたフェールセーフ（安全）PLCの考え方と活用利点，計装，Vol. 40，No. 12 ，pp.63-68（1997）.
5）JIS C 0508, 電気・電子・プログラマブル電子安全関連系の機能安全（1999）.
6）ISO/IEC Guide51, Safety aspects -Guidelines for their inclusion in standards（1999）.
7）Guide to Machinery Safety 6th Edition, Pilz Automation Technology，pp.145-182（1999）.
8）池田博康，コンピュータを利用した安全制御技術の実態調査，産業安全研究所特別研究報告，NIIS-SRR-NO.19，pp.5-8（1999）.
9）安全技術応用研究会編，安全システム構築総覧，通算資料調査会，pp.530-534（2001）.
10）prEN 50159, Railway applications －Communication, signaling and processing systems（1998）.

（平成 14 年 9 月 30 日受理）