安全性と使いやすさを両立させたセーフティコントローラの開発

清水 隆義[*1]　大杉 典史[*1]　高向 靖仁[*1]　増田 英介[*1]　阪下 友子[*1]
土肥 正男[*1]　錦 朋範[*1]

Development of safety controller that achieves high level of safety and usability

Takayoshi Shimizu[*1], Norifumi Ohsugi[*1],Yasuhito Takamuki[*1], Eisuke Masuda[*1],
Tomoko Sakashita[*1], Masao Dohi[*1] and Tomonori Nishiki[*1]

Abstract - To establish safe environments becomes more and more vital in the various working environment for not only industrial machine applications such as industrial robots and machine tools but also elevators and industrial furnace applications. With the evolution of technology and the growing interest in safety, the required safety performance for machines are much advanced and complicated than ever. Therefore the specialized knowledge and a lot of expenses are necessary to achieve the safe machines and applications. That is one of disincentives for growth of the safe environments. Reflecting such situations we report the next generation safety controller with the highest safety performance and the prominent usability which the person without specialized knowledge can establish safety-related control systems with.

Keywords: Safety, Usability, Functinal safety, Safety of machnary and Safety controller

1.　はじめに

近年、図 1 に示すように、工場のみならず、広く一般に利用される機械や一般家庭における機器においても「事故」や「安全」をキーワードとした新聞報道が増えている。例えば、装置の操作を誤ったり、また、幼児が巻き込まれるような悲惨な事故が増加しており、機械への安全性配慮不足だけでなく、複雑化、高性能化にともなう操作ミスや、熟練作業者の減少にともなうヒューマンエラーの増大も事故発生の大きな要因のひとつとして上げられる。日本国内においても、2001 年に厚生労働省労働基準局より通達された「機械の包括的な安全基準に関する指針」、2004 年に機械安全の基本である国際安全規格 ISO12100 に整合した JIS B9700「機械類の安全性－設計のための基本概念」の発行に加え、2006 年 4 月 1 日に「改正労働安全基準法」が施行されるなど、よりいっそう安全性に配慮した機械類や設備の構築が必要となってきた。このような状況において、「危険ゼロ」の実現や「安全なヒューマンインタフェース」による本質的安全の確保がますます重要視されている。[1-4]

そこでわれわれは、誰もが簡単に最高レベルの安全制御システムを構築することを可能とし、「危険ゼロ」と「安全なヒューマンインタフェース」とを実現した、安全性とユーザビリティに優れたセーフティコントローラ

図 1　安全制御システムの導入が求められる産業分野
Fig.1 The safety-related control system is required in a lot of industries.

*1: IDEC 株式会社
*1: IDEC Corporation

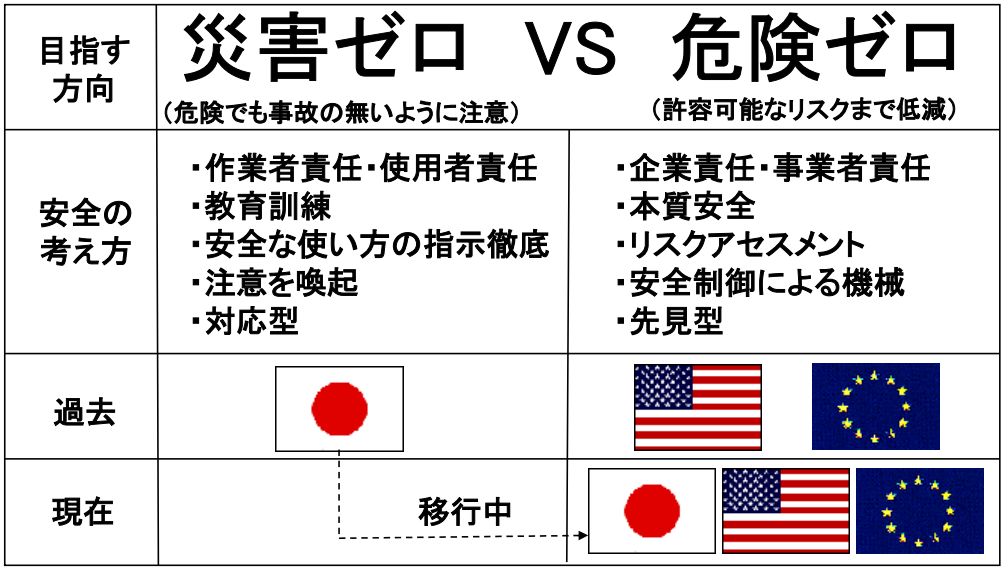


図２　製造業が目指すべき安全の考え方
Fig.2 Attitude to establish safe environments in manufacturing.

の開発を行ったので報告する。

2.　目指すべき安全とその必要性

2.1　災害ゼロから危険ゼロへ

日本と欧米における製造現場での安全構築の考え方の根本的な違いを図 2 に要約して示す。

従来の日本の場合、工場や FA 環境における安全構築の方法は、現場作業者への安全教育や指示徹底に基づく「作業者責任」であり、災害ゼロを目標として運営されてきた。どこの企業でも「災害ゼロ○×日」と掲示されており、もちろんこのような活動は事故減少に有効な手法である。しかしながら、国際的に一般的な安全に関する考え方は、より根本的に重要なこととして、作業者が働く環境に対して経営者が「危険ゼロ」環境を実現することである。そのため、企業責任において事業者側がリスクアセスメントを行い、本質的に安全な機械や環境を「経営責任」として構築することを基本としており、「災害ゼロ」と「危険ゼロ」の考え方は根本的に異なっている。

2.2　国際社会が求める安全

「危険ゼロ」とは、リスクを許容可能なレベルまで低減することを意味している。ここで重要となってくるのがリスクアセスメントと同時に国際安全規格の 3 階層構造であり、図 3 にその内容を示す。様々な安全技術は IEC や ISO 国際安全規格の階層化構造に則って適用される必要がある。産業分野において使用される様々な機械装置システムは、個別機械規格としての C 規格（最下層）に位置している。その上位に、制御技術分野に関するグループ規格としての B 規格があり、インタロック規格、非常停止規格、制御安全規格、機能安全規格等があり、安全構築のための技術が詳細に述べられている。さらにその上位に基本規格の A 規格として、機械類の安全設計のための一般原則である ISO12100 やリスクアセスメント規格の ISO14121 があり、3 段階の階層化構成となっている。このようにグローバルに通用する安全の考え方の骨格は既に構築されており、今後の安全技術はこの体系の中で進化を続けることとなる。これら A,B,C 規格は相互に関連付けられており、安全性を構築するための機能やヒューマンインタフェースに関わる規格が非常に多い。これらの規格を熟知した上でリスクアセスメントをまず行い、そして機械の本質安全設計を重視して行うことが求められている。

日本国内における改正労働安全基準法においても、リスクアセスメントを努力義務としながら、さらに「危険性又は有害性等の調査等に関する指針」が通達されるなど、事実上作業現場におけるリスクアセスメントは必須となっている。[5]

リスクアセスメントとは、使用する機械設備の危険源を見つけ出し、その危険源によるリスクを見積り、評価し、リスクが許容可能となるまで低減を図る作業であり、機械の設計段階および現場での運用時や改修時に実施しなければならない。リスク低減方法は、3 ステップメソッドと呼ばれており、本質的安全設計方法、安全防護および付加保護法策、使用上の情報の順で行う。

このような国際的な要求に基づき、われわれは機械安全を実現するために必要とされる様々な安全機器の提案、報告を行い、開発を進めてきた。[6-14]

2.3　安全制御システムへの要求事項

様々なシステムでそれに適合したリスクアセスメントを行い、リスク低減方策を行ううえで、その方策に安全制御システムが含まれる場合は、機械類に使用される制御システムの安全関連部設計のための一般原則である ISO13849 や、電気・電子・プログラマブル電子安全関連系の機能安全について規定した IEC61508 といった国際

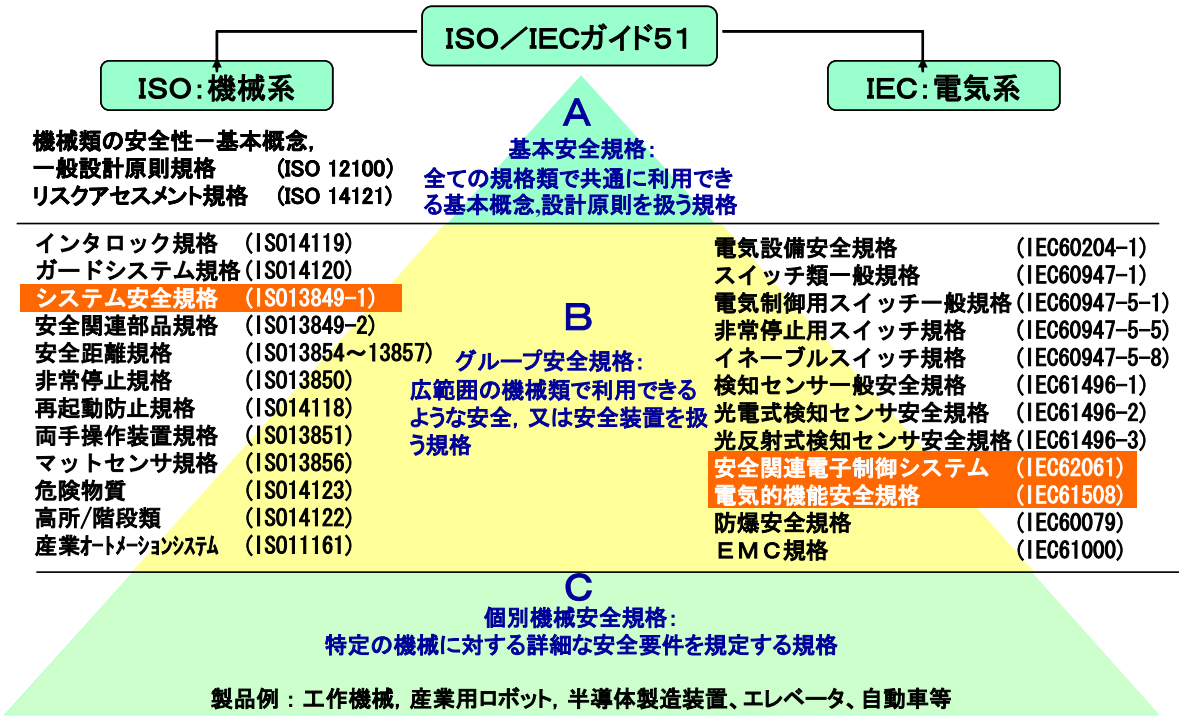


図３　国際安全規格の階層化構成
Fig.3 Hierarchical Diagram for International Safety Standards.

安全規格に適合した設計手法を用いることで、安全性能を満たすことができる。[15-18]

ISO13849 では、安全制御システムにおける安全機能の故障の確率を最小化するために、通常考慮される「品質向上」だけでなく、「定期的な故障のチェック」、「故障に対する安全機能の維持」および「故障検出時の適切な制御」等、予め故障を認めたうえで安全を確保する考え方が規定されている。この規格では「安全機能を維持する能力」を B、１、２、３、４の「カテゴリ」と呼ばれる性能に分類し、信頼性を示す「MTTFd（平均危険側故障時間）」や「DC（診断範囲）」、「CCF（共通原因故障への対策）」の要素までも取り入れたパフォーマンスレベル（PL）と呼ばれる a～e までの 5 段階の安全性能レベルについて規定している。

IEC61508 は、ISO13849 で規定される「安全機能を維持する能力」や「信頼性」といったハードウェアに求められる安全性能に加え、ソフトウェアを含む複雑な電気・電子回路の安全性能について規定した国際安全規格である。従来の規格では、安全関連部へのソフトウェアの使用は認められず、ハードウェアによる構成のみが認められていた。IEC61508 は、近年のマイクロプロセッサ技術の進歩と IT 技術の浸透、ならびに制御の複雑化などの理由により、マイクロプロセッサやソフトウェアを用いて安全制御システムを構築したいという要求を受け、発行された規格である。ハードウェアとソフトウェアに加え、製品の安全ライフサイクルを含めた安全インテグリティレベル（SIL）と呼ばれる 1～4 までの 4 段階の安全性能レベルについて規定されている。産業機器に求められる安全性能の最高レベルは SIL3 までであり、SIL4 はプラントや原子力発電所など、事故が起きた際の周囲への影響度が大きい場合に適用される。

ISO13849 や IEC61508 は様々な産業分野に影響を与える規格であり、例えば IEC61508 に関して言えば、この規格をもとにして、機械類に使用される電気・電子・プログラマブル電子安全関連制御機器について規定した IEC62061 やプロセス工業部門の安全計装システムについて規定した IEC61511 などが作成され、運用されている。[19][20]

3.　セーフティコントローラによる安全の実現

このように、日本における安全要求の高まりと、国際社会が求める安全から、誰もが簡単に最高レベルの安全制御システムを構築することを可能とした FS1A 形セーフティコントローラ（以下セーフティコントローラ）の開発をおこなった。

3.1　セーフティコントローラの特長

一般的に安全制御システムを構築するには、

(A)安全リレーや安全リレーモジュール

(B)安全プログラマブルコントローラ（以下安全 PLC）や安全ネットワーク

を用いる方法がある。

(A)は接点の乖離性能を保証した安全リレーや、その安全リレーやトランジスタなどの電子部品を用いてモジュール化した安全リレーモジュールにより、ハードワイヤリングでシステムを構築する方法である。少点数の制

御においては、周辺機器と配線のみでシステム構築が可能であるため、簡単に安全制御システムを構築することが出来るが、点数の多い制御や複雑な制御においては、機器や配線が多くなるため、システムの構築が難しくなる。(B)は専用のプログラミングツールを用いた安全 PLC や、安全性能が保証された安全ネットワークを用いてシステムを構築する方法である。ソフトウェアによる柔軟性やネットワークによる拡張性に安全性能を加えた優れたシステムである。しかし、ハードウェアの安全性能の確認に加えて、安全ネットワークに関する知識の習得、専用ソフトウェアの学習や作成したプログラムの安全性の立証やその管理など、ソフトウェアに対する安全性能の確認も必要となるため、システム構築に多くの時間と費用が必要となる。そこで、(A)と(B)の利点を活かした安全制御システムを構築する方法として

(C)セーフティコントローラ

を用いる方法を新たに提案し、簡単で扱いやすい安全制御の方法を実現した。図 4 は(A)(B)(C)のそれぞれの機器が最も有効である範囲を、X 軸を安全入出力の点数、Y 軸を制御の複雑さとし、記載したものである。(A)は少点数で簡単なシステムに有効であり、(B)は多点数で複雑なシステムに有効な方法である。それらに対して新たに提案する(C)は(A)の簡単さと(B)の柔軟性を併せ持つため、広い範囲で有効な方法である。また、制御安全規格である ISO13849 と機能安全規格 IEC61508 シリーズの産業機器分野における最高レベルの安全性能であるパフォーマンスレベル e および安全インテグリティレベル 3 をセーフティコントローラ単体で満たしているため、簡単に最高レベルの安全制御システムの構築を可能としている。

3.2 セーフティコントローラにより実現された安全インタフェース

セーフティコントローラは安全入力として使用可能な入力を 14 点、安全出力として使用可能な出力を 4 点有し、多数の安全機器の制御を可能としている。安全入力や安全出力の回路は、接続された安全機器の故障や内部回路の異常、配線の誤りなどの検出が可能となっており、これは各回路が独立したチェック信号を有することで実現されている。このため、万一配線を誤った場合でも、その誤りを検出、危険源を停止させることで安全を確保することができる。また、安全入力と安全出力が接続されるコネクタ部には、配線作業が容易に行えるよう脱着可能なツーピースコネクタを使用しているが、コネクタを挿し間違えることが無いように、入力用と出力用とで異なる極数を使用し、かつ、キーイングを有したものを使用した。

また、内部のロジックと呼ばれる動作処理は、セーフティコントローラに搭載されたスイッチを使用して、安全かつ簡単に設定することが可能となっている。ロジックの概要を図 5 に示す。セーフティコントローラは安全制御システムに最適なロジックを複数有しており、ユーザーはその中からそれぞれの設備にあったロジックを選択、設定することで簡単に安全制御システムを構築することが可能である。このロジックの設定は、①スイッチの保護カバーを開ける。②搭載されたスイッチを用いて設定したいロジックを選択する。③選択したロジックの番号が LED に表示されていることを確認する。④エンターボタンを押して設定を承認する。⑤保護カバーを閉じてロックする。という手順で安全かつ簡単、確実に設定することが可能となっている。

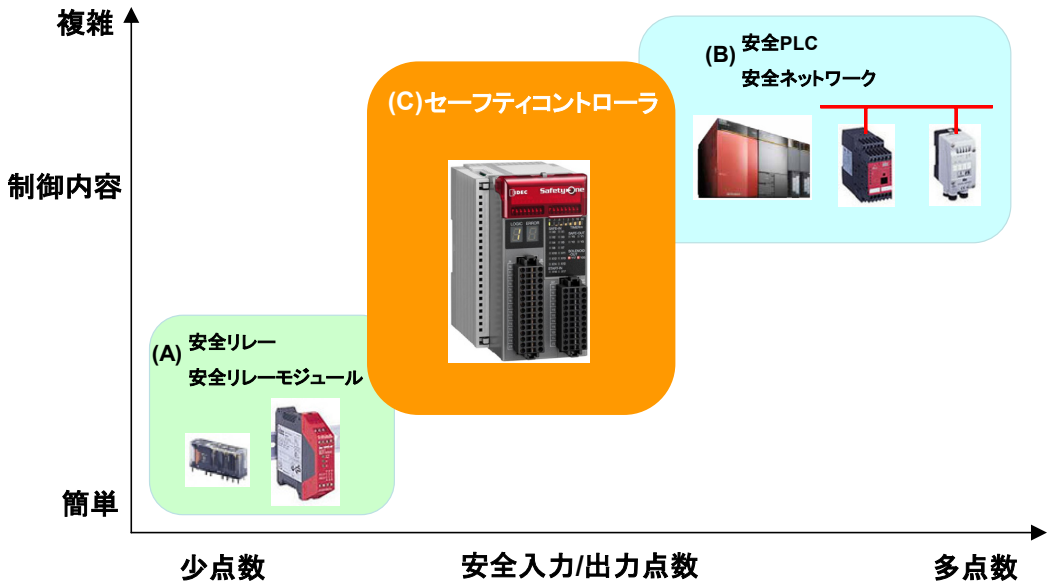


図 4　安全制御機器の動向
Fig.4 Trend of Safety-related Control Components.

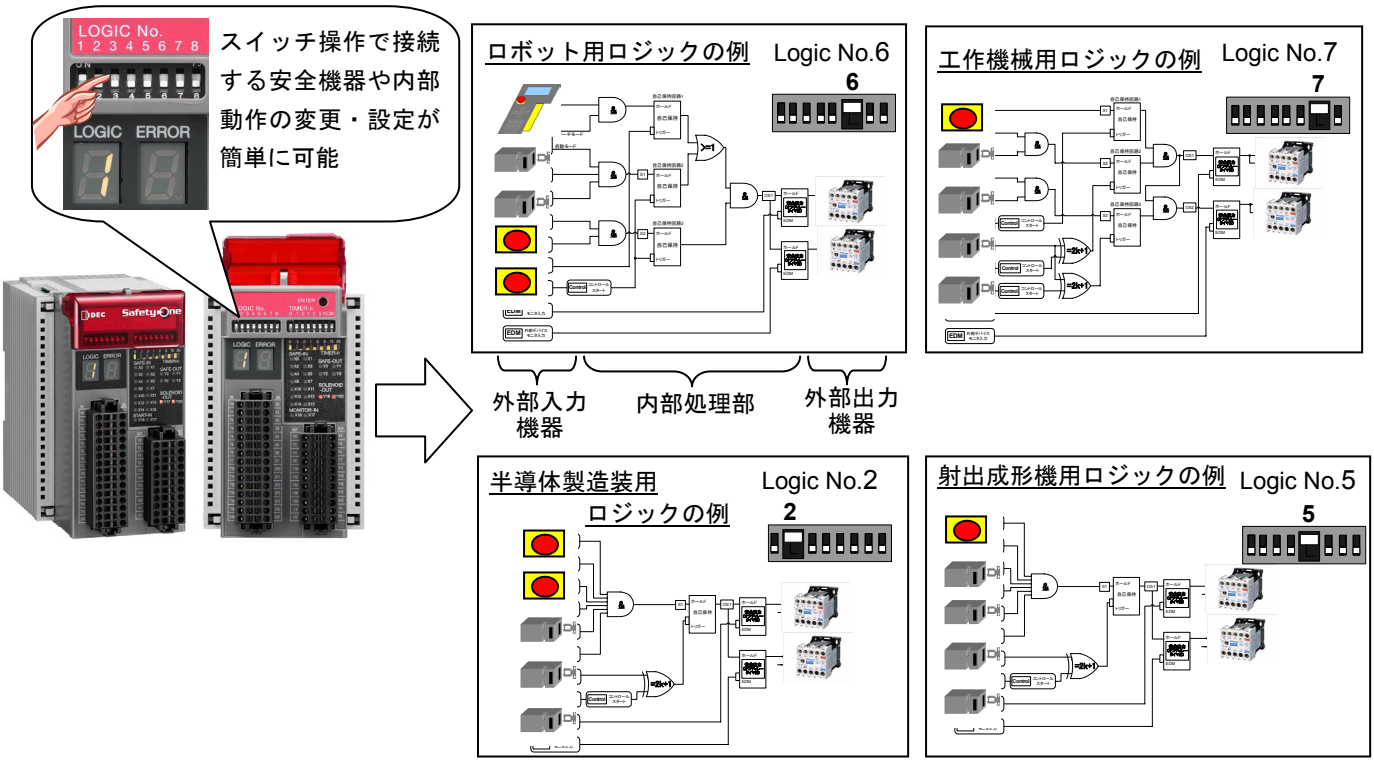


図５　セーフティコントローラのロジック
Fig.5 The LOGICs of Safety Controller.

さらに、モニタ出力や LED 表示によりユーザーは接続された機器やセーフティコントローラの動作や異常の状態が把握できるため、システムのメンテナンスを容易に行うことができる。

4.　安全制御機器とそのユーザビリティ

このような特長をもつ(C)セーフティコントローラを用いて安全制御システムを構築した場合と、(A)安全リレーモジュールや(B)安全 PLC を用いて安全制御システムを構築した場合とでは、ユーザビリティの観点からどのような違いがあるか比較を行った。

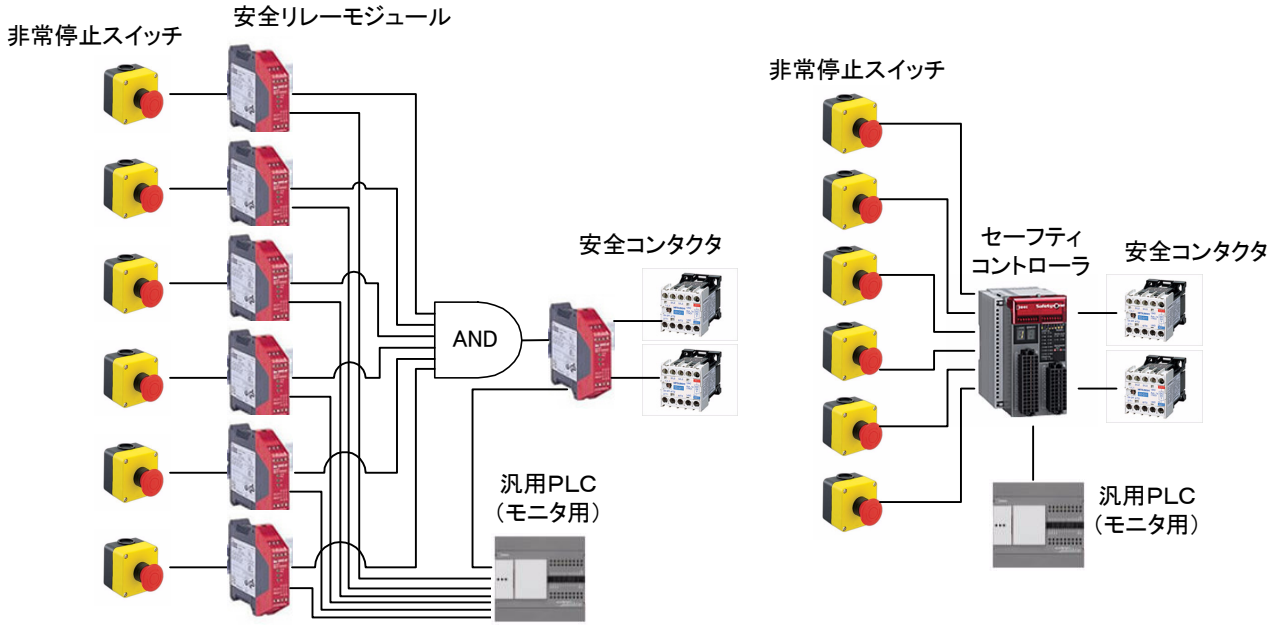
4.1　安全制御システムの構築に必要な作業とその難易度

表 1 に(A)(B)(C)それぞれの安全機器を用いて安全制御システムの構築を行う際の作業と難易度ついて 4 段階に分類したものを記す。すなわち、システム構築時に必要でありかつ多大な時間や費用が求められる場合を「▲必要（困難）」、必要でありかつ内容に見合った時間や費用が求められる場合を「△必要」、必要であるが比較的容易に行える場合を「○必要（簡単）」、必要としない場合を「◎不要」とした。

表１　安全制御システムの構築に必要な作業とその難易度
Table 1 Difficulty Level for Configuration of Safety-related System.

項目	(A)安全リレーモジュール	(B)安全 PLC	(C)セーフティコントローラ
1. リスクアセスメントの実施	△	△	△
2. 安全仕様書の作成	△	△	△
3. 安全システムの知識やノウハウの習得	△	△	△
4. 安全回路の設計	▲	○	○
5. 配線	▲	○	○
6. 専用ソフトウェアの知識の習得	◎	▲	◎
7. ソフトウェアの設計	◎	▲	◎
8. 安全性能の検証	△	△	○
9. 妥当性確認用の文書作成	△	△	○
10. 妥当性確認	▲	▲	○
11. ソフトウェアの管理	◎	△	◎

▲必要（困難）、△必要、○：必要（簡単）、◎：不要

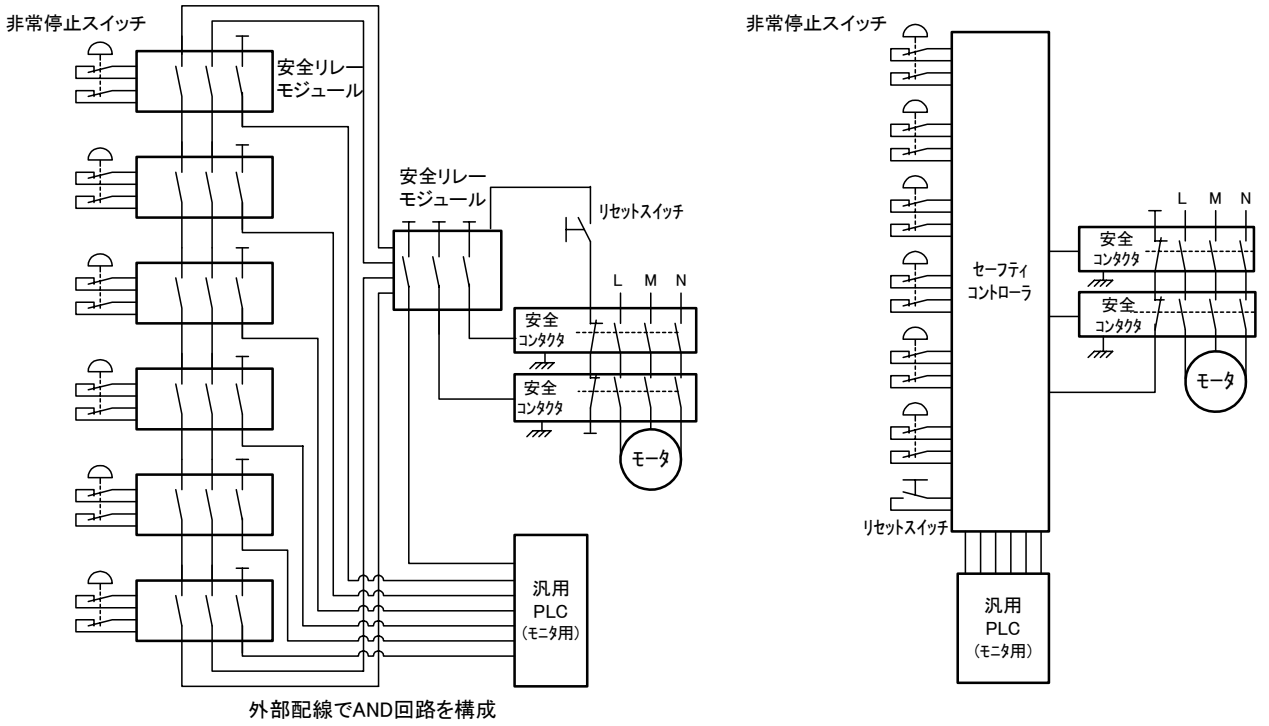


(a)　安全リレーモジュール(A)を用いた場合　　(b)　セーフティコントローラ(C)を用いた場合

図 6　安全制御システムの構成比較
Fig.6 Configuration Comparison of Safety-related Control System.

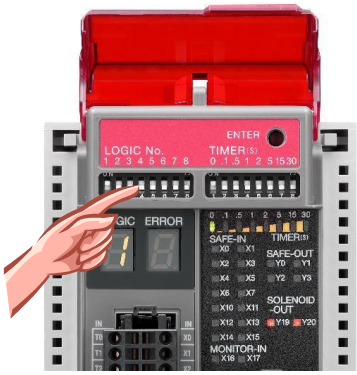
安全制御システムを構築する際にはじめに行う「1.リスクアセスメントの実施」や安全性能の実現方法を規定した「2.安全仕様書の作成」、「3.安全制御システムの知識やノウハウの習得」については、いずれの安全機器も製造者がそのシステムに合わせて情報を入手したり、文書を作成する必要があるため「必要」と評価した。

図 6 に安全リレーモジュール(A)を用いた場合と、セーフティコントローラ(C)を用いた場合の安全制御システムの構成比較例を示す。ここでは 6 台の非常停止スイッチを用いる安全制御システムを想定し、さらに各々のスイッチの状態を汎用 PLC でモニタする構成とした。図 6 (a)に示すように安全リレーモジュール(A)を用いる場合、安全性能を確保するために、複数の安全リレーモジュールが必要となり、システム構成が複雑なものとなる。一

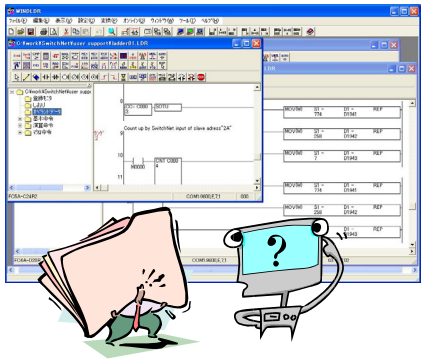


(a) 安全リレーモジュール(A)を用いた場合　　(b) セーフティコントローラ(C)を用いた場合

図 7　安全制御システムの回路配線比較
Fig.7 Wiring Comparison of Safety-related Control System.



(a)セーフティコントローラの設定部



(b)安全 PLC の設定には専用ソフトウェアが必要

図８　設定方法の違い
Fig.8 Comparison of Configuration Method between Safety Controller and Safety PLC.

方、図 6 (b)に示すようにセーフティコントローラ(C)を用いた場合、ソフトウェア処理でロジックが組まれているため、単体で簡単にシステムが構成できる。図 7 (a)(b)に、図 6 (a)(b)のそれぞれの安全制御システムに対応する配線図を示す。安全リレーモジュール(A)を用いた場合、安全リレーモジュール間や PLC への接続により、配線数が多くなる。このため表 1 の「4.安全回路の設計」や「5.配線」の項目を、「必要（困難）」と評価した。一方、セーフティコントローラ(C)を用いた場合は、安全リレーモジュール間や PLC への接続に必要な配線の大部分が、内部のソフトウェア処理で実施されるため「必要（簡単）」と評価した。

安全 PLC(B)を用いてシステムを構築する場合、図 8 (b)に示すように専用ソフトウェアを用いて、内部動作のプログラミングを行う必要がある。プログラミングを行うためには、安全回路の実現方法やプログラムデバックの方法など、ソフトウェアの使用方法を習熟する必要があるため、表 1 の「6.専用ソフトウェアの知識の習得」や「7.ソフトウェアの設計」の項目を「必要（困難）」と評価した。また、作成したプログラムの PLC への書き込み作業やプログラムの管理も必要となるため、「11.ソフトウェアの管理」に対する評価を「必要」としている。セーフティコントローラ(C)の場合、図 8 (a)に示すようにセーフティコントローラ上部に設置されたスイッチを用いて簡単に行うことができるため、ソフトウェアを使用しない安全リレーモジュール(A)と同様に、評価は「不要」とした。

システム設計完了後の「8.安全性能の検証」や「9.妥当性確認」、「10.妥当性確認用の文書作成」では、第三者認証機関における確認済みのロジックを有するセーフティコントローラ(C)の評価を、「必要（簡単）」とした。

4.2　安全制御機器におけるユーザビリティの比較

表 1 に基づいて、それぞれの安全機器を用いて安全制御システムを構築した場合のユーザビリティについて、分析・比較を行った結果を図 9 に示す。ここではユーザビリティを示す要素として「安全性の検証」「省配線」「設計のしやすさ」「メンテナンス性」「柔軟性」の 5 つの項目で分析を行った。安全回路やソフトウェアの検証の容易性を示す「安全性の検証」では、第三者認証機関による認証済みのロジックが使用できるセーフティコン

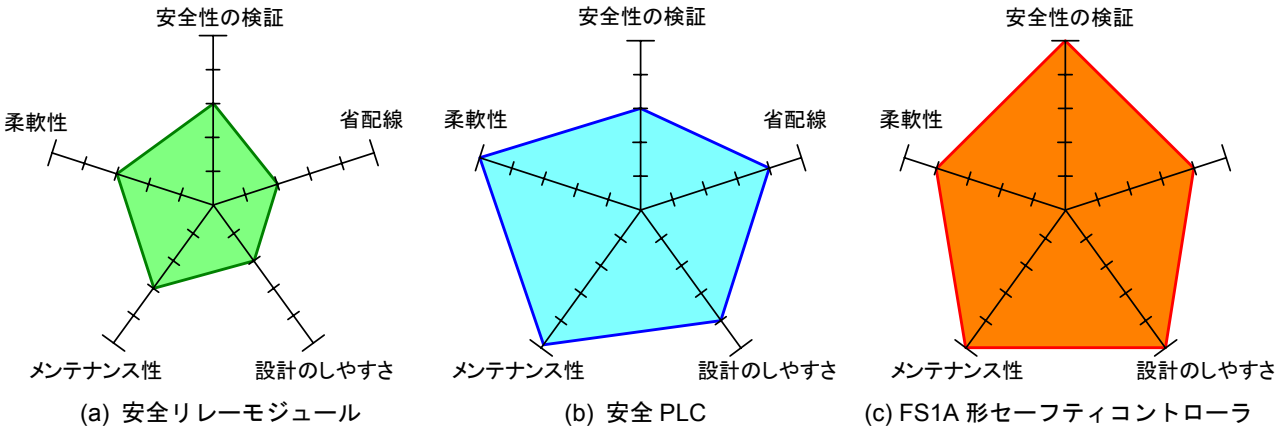


図９　安全機器におけるユーザビリティの比較
Fig.5 Usability Comparison of Safety-related Control Components.

トローラ(C)が最も容易に安全性の検証が行える機器であると評価した。配線作業の容易性を示す「省配線」では、複雑な安全回路の配線を行う必要がない安全 PLC(B)とセーフティコントローラ(C)の評価が高い。安全回路設計の容易性を示す「設計のしやすさ」では、複雑な安全回路の設計や、プログラミングが不要なことからセーフティコントローラ(C)の評価が最も高い。システム構築後のメンテナンスの容易性を示す「メンテナンス性」については、プログラミングが可能な安全 PLC(B)と、モニタ出力や状態表示用の LED を有するセーフティコントローラ(C)の評価が高い。最後に、様々なシステムへの柔軟な対応の容易性である「柔軟性」については、プログラミングや拡張性に優れた安全 PLC(B)が最も評価が高く、次にロジックの切り替えがスイッチで簡単にできるセーフティコントローラ(C)の評価が高くなった。

「安全性の検証」「省配線」「設計のしやすさ」「メンテナンス性」の 4 つの項目での高い評価から、今回開発を行ったセーフティコントローラは、最高レベルの安全性能とユーザビリティを併せ持つ優れた制御機器であると考える。

5. 今後の展開

セーフティコントローラは安全制御システムの構築を行う際、安全の確保とユーザビリティの向上を図る上で優れた機器である。「安全なものをつくる」と同時に「安全にものをつくる」ためにも、ロジックの追加や入出力の拡張、ネットワークへの対応など、更なるユーザビリティの向上を目指し、製品開発を進める所存である。

参考文献

[1] ISO 12100-1, -2:2003, Safety of machinery -- Basic concepts, general principles for design -- Part 1: Basic terminology, methodology, Part 2: Technical principles.

[2] JIS B 9700-1:2004, 機械類の安全性－設計のための基本概念，一般原則－第 1 部：基本用語，方法論

[3] ISO 14121-1:2007, Safety of machinery -- Risk assessment -- Part 1: Principles

[4] 平成 17 年 11 月 2 日「労働安全衛生法の一部を改正する法律」（平成 17 年法律第 108 号）

[5] 平成 18 年 3 月 10 日「危険性又は有害性等の調査等に関する指針」（危険性又は有害性等の調査等に関する指針公示第 1 号）

[6] 福井他: 機械安全における 3 ポジションイネーブルスイッチの人間工学的必要性;ヒューマンインターフェイスシンポジウム 2007, p.759-764 (2007).

[7] 松本他: 非常停止スイッチの人間工学的な観点から見た操作性; ヒューマンインターフェイスシンポジウム2007, p.765- 770 (2007).

[8] 清水他: 機械安全に必要な安全機器のネットワーク化によるユーザビリティの向上; ヒューマンインターフェイスシンポジウム 2004, p.755-758 (2004)

[9] 柿崎他: IDEC におけるグローバルに進化する「ものづくり安全」ヒューマンインターフェース研究開発; ヒューマンインターフェース学会誌 Vol.9 No.3 2007, p.67-72 (2007)

[10] 岡田他: ロボット制御セル生産システムのリスクアセスメントと最適な安全方策; ヒューマンインターフェイスシンポジウム 2006, p.433-438 (2004).

[11] 米島他: グローバルスタンダードを目指したロボットティーチング用ペンダント形操作表示器の開発; 第 26 回 日本ロボット学会学術講演会(2008).

[12] 米澤: ものづくり分野におけるヒューマンインタフェース研究の取り組み; ヒューマンインタフェース学会誌 Vol.10, No.2, p.147-148(2008).

[13] T. Fukui, et al.: DEVELOPMENT OF SAFETY TECHNOLOGY TO ENSURE SAFETY OF TWO OR MORE OPERATORS IN HAZARDOUS AREAS BY PREVENTING ERRONEOUS RESETTING; International Conference - Safety of Industrial Automated Systems(SIAS 2007).

[14] T. Fujita, et al.: Robot Control Cell Production System of Senju (thousand-handed) Kannon Model that Demonstrated Optimality to the Multi-product Production in Varying Volumes for Eight Years; IEEE Conference on Automation Science and Engineering 2008 (IEEE CASE 2008).

[15] ISO 13849-1:2006, Safety of machinery -- Safety-related parts of control systems -- Part 1: General principles for design.

[16] IEC 61508-1:1998, Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements

[17] IEC 61508-2 :2000, Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems

[18] IEC 61508-3 :1998, Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements

[19] IEC 62061 :2005, Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems

[20] IEC 61511-1 :2003, Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and software requirements