

“MELSEC iQ-Rシリーズ”安全シーケンサ

内越正弘*

"MELSEC iQ-R Series" Safety Programmable Logic Controller

Masahiro Uchikoshi

要旨

近年、FA(Factory Automation)システムに対して一般制御と安全制御を統合した省スペース・省配線・省コスト化の要求がある。従来の安全シーケンサは安全専用システムであり、一般制御とは別にシステムを構築する必要があった。そこで、“一般制御と安全制御の統合”をコンセプトとした“MELSEC iQ-Rシリーズ”安全シーケンサを開発した。

(1) 製品の特長

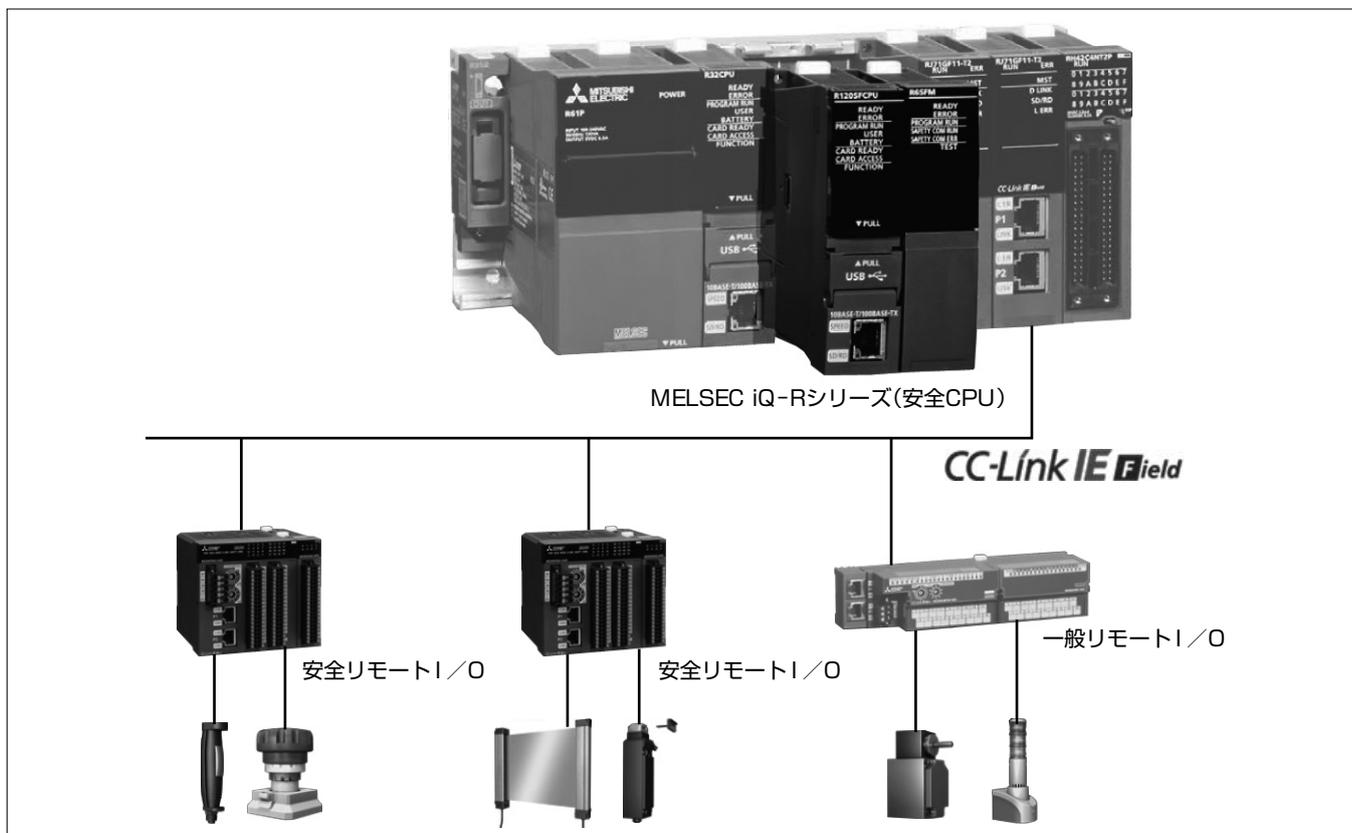
MELSEC iQ-Rシリーズ安全シーケンサでは、一般制御と安全制御を統合して、同一ベースユニット上や同一ネットワーク上で一般制御と安全制御のユニットを混在させ、1つのシステムで一般制御と安全制御を実現する。これによって、MELSEC iQ-Rシリーズで安全ソリューションを容易に構築することができる。また、一般制御

と安全制御を統合することで、e-F@ctoryによる安全ソリューションと情報システムの連携が容易になり、安全の見える化に寄与する。

(2) 製品コンセプト実現のための技術

一般制御と安全制御の演算処理を同時に実行して、一般制御の演算処理に影響されずに安全制御を実行する。さらに、一般制御部の故障等による安全制御部への不正書き込みを検出する。

また、同一ベースユニット上に一般制御と安全制御のユニットを装着可能にして、安全制御が継続できないような異常や故障が発生した時には、安全ユニットで異常や故障を検出して安全ユニットだけをシャットダウンさせて安全状態へ移行する。



“MELSEC iQ-Rシリーズ”安全シーケンサ

三菱シーケンサMELSEC iQ-Rシリーズに、安全制御を実現する“安全CPU”と“CC-Link IEフィールドネットワーク ブロックタイプ安全リモートI/O(Input/Output)ユニット”を新たにラインアップに加えた。これらのユニットは、世界有数の第三者認証機関であるTÜV Rheinlandから国際安全規格ISO(International Organization for Standardization) 13849-1 PLeカテゴリ4及び機能安全規格IEC(International Electrotechnical Commission) 61508 SIL(Safety Integrity Level) 3の認証を受けている。

1. ま え が き

安全シーケンサとは、国際安全規格の適合認証を取得したシーケンサで、労働災害を防止するための安全システムである。安全入力に応じて安全出力をOFFにする安全制御を行う。安全入力とは、国際安全規格に適合した安全機器(非常停止スイッチ・セーフティライトカーテンなど)からの入力信号を示す。安全出力とは、危険源(モータ、ロボットなど)への動力を確実に遮断するための出力信号を示す。

安全シーケンサの起動時や稼働中には、国際安全規格で要求される高いレベルの自己診断を実施する。安全シーケンサ自体に故障が発生した場合は、自己診断によって故障を検出して安全出力を強制的にOFFする。これによって、故障による安全機能の不動作にならないことが、一般シーケンサとの一番の相違点である。

従来、三菱電機のシーケンサでは“MELSEC QSシリーズ”安全シーケンサがあったが、安全制御専用システムであるため一般制御とは別にシステムを構成する必要があり、FAシステムに対する省スペース・省配線・省コスト化の要求に応えられなかった。そこで、MELSEC iQ-Rシリーズでは、“一般制御と安全制御の統合”をコンセプトとした安全シーケンサを開発した。

本稿では、製品の特長と一般制御と安全制御の統合のための技術について述べる。

2. 安全規格

機械安全では対象機械のリスクアセスメントを実施してリスクを定量化するため、リスクの受傷度合い、遭遇可能性及び回避可能性によって分類する安全カテゴリがよく使われている(図1)。安全カテゴリの値が高くなると安全機器に対する要求も厳しくなり、安全カテゴリ3では単一故障で安全機能を損なわないこと、安全カテゴリ4では単一故障は安全機能実行時又はその前に検出されることが要求事項である。したがって、部品の二重化や徹底的な自己診

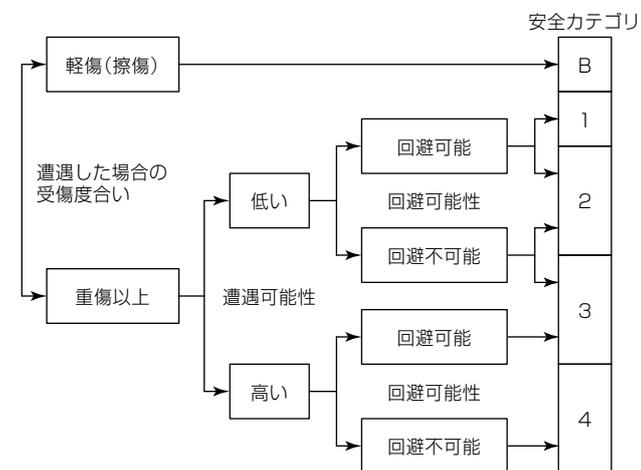


図1. 安全カテゴリによるリスクの定量化(ISO13849-1)

断が必要となる⁽¹⁾。

MELSEC iQ-Rシリーズ安全シーケンサでは、ISO13849-1 PLe カテゴリ 4 及びIEC61508 SIL3の適合認証を得ている。

3. 製品の特長

MELSEC iQ-Rシリーズ安全シーケンサの主な特長について、次の3つの観点から示す。

3.1 同一ベースユニット上での一般ユニットと安全ユニットの混在

従来、一般制御と安全制御は別のシステム構成とする必要があって2つのシステムになるため、システム購入コストやシステム立ち上げコストが割高であった。また、2つのシステムを収納する必要があるため、制御盤が大きくなっていった。

MELSEC iQ-Rシリーズの安全CPUでは、一般制御用プログラムと安全制御用プログラムを実行できる。これによって、1つのCPUで一般制御と安全制御を統合させて使用できる。

また、一般ユニット(CPU, I/O, アナログ, 位置決め/カウンタユニット), 安全ユニット(安全CPU), 一般/安全共用ユニット(電源, ネットワークユニット)を同一ベースユニット上に装着できる(図2)。これによって、一般制御と安全制御を1つのシステムで構成でき、省スペース・省配線・省コスト化が可能となる。

3.2 一般制御と安全制御のネットワーク統合

従来は、一般制御用ネットワーク(一般通信)と安全制御用ネットワーク(安全通信)は別々に敷設する必要があった(図3(a))。このため、ネットワークケーブルの本数が増え、配線スペースの増加やケーブル敷設工数の増加を招いていた。

MELSEC iQ-Rシリーズ安全シーケンサでは、CC-Link

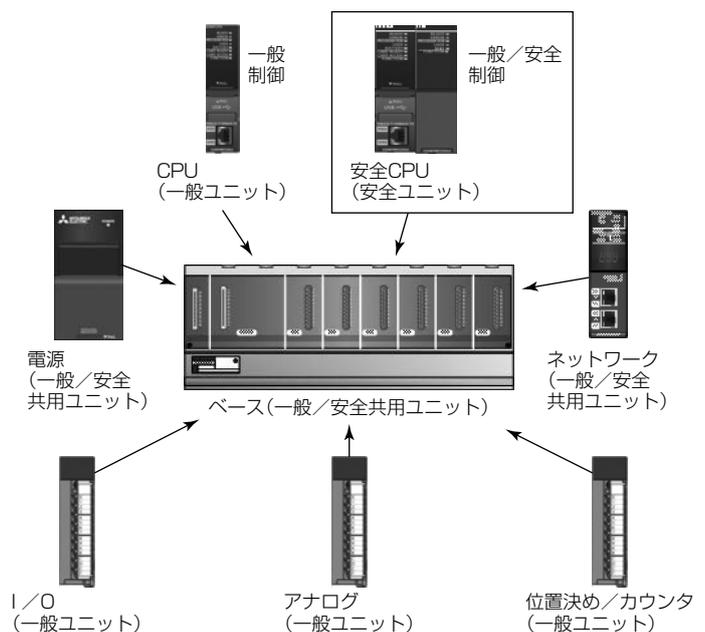


図2. 同一ベースユニット上での一般ユニットと安全ユニットの混在

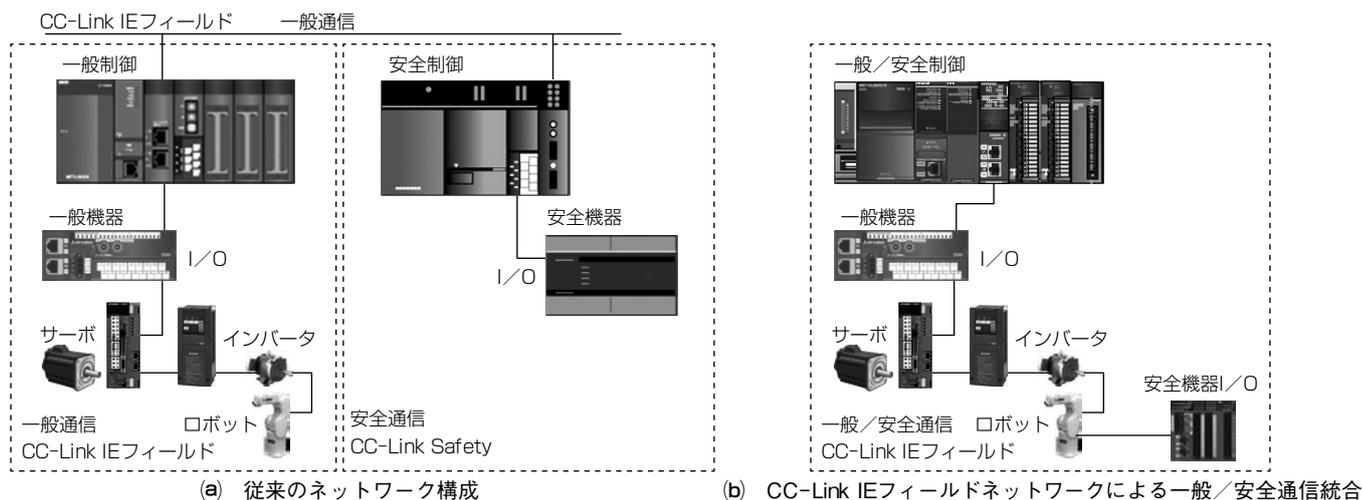


図3. 一般通信と安全通信のネットワーク統合

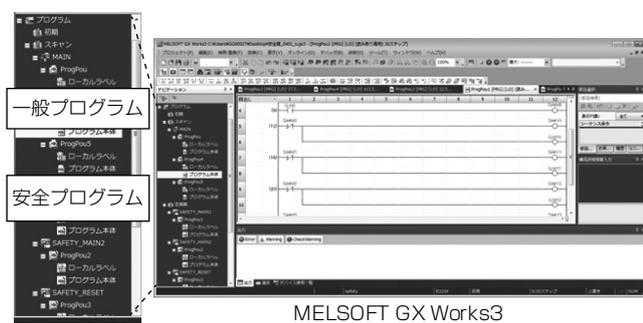


図4. 開発環境の統合

IEフィールドネットワークで一般通信と安全通信を混在させて使用でき(図3(b)), 敷設するネットワークはCC-Link IEフィールドネットワーク1本にできる。これによって, 配線スペースの削減, ケーブル本数の削減, ケーブル敷設工数削減が可能となり, ネットワーク構築時の省スペース・省配線・省コスト化が可能となる。

3.3 開発環境の統合

従来のエンジニアリングソフトウェアは, 一般制御用に“MELSOFT GX Works2”を使用して, 安全制御用に“MELSOFT GX Developer”を使用していた。

MELSEC iQ-Rシリーズ安全シーケンサでは, エンジニアリングソフトウェア“MELSOFT GX Works3”を使って, 一般制御のプログラミングだけではなく安全制御のプログラミングや各種設定操作も一元的に行うことができる(図4)。従来のように2つのエンジニアリングソフトウェアの操作を覚えなければならない煩わしさを軽減できる。

4. 一般制御と安全制御統合のための技術

一般制御と安全制御を統合するための3つの主な技術について述べる。

4.1 一般制御と安全制御の実行

一般制御と安全制御を統合するためには, 安全CPUで一般プログラムと安全プログラムの両方を実行する必要がある。

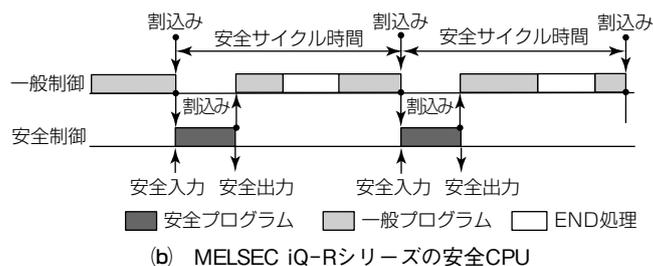
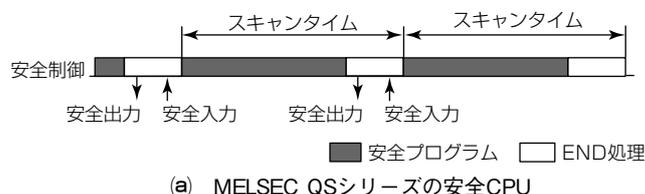


図5. 一般制御と安全制御の実行

従来は, 安全プログラムの演算を実行して, END処理内で安全入力/出力処理を実行していた(図5(a))。

しかし, この処理に一般プログラムの演算を加えるとスキャンタイムが延びるため, 安全入力/出力の応答性能を確保できない。このため, MELSEC iQ-Rシリーズの安全CPUでは, 安全プログラムの演算や安全入力/出力処理を一定周期(安全サイクル時間)の割り込み処理で実行する(図5(b))。

これによって, 一般プログラムを実行するスキャンタイムに影響されずに安全プログラムを実行でき, 安全入力/出力の応答性能を確保できる。

この技術に加えて, MELSEC iQ-Rシリーズのシステムバス性能の向上, CPUの演算処理性能の向上, CC-Link Safetyより高速なCC-Link IEフィールドの採用によって, 従来製品MELSEC QSシリーズと比較すると, 安全応答時間(最悪値)が1/3以下に性能向上した(表1)。

4.2 一般制御から安全制御への不正書き込み検出

一般制御と安全制御を統合するため, 安全CPUで一般プログラムと安全プログラムの両方を実行すると, 一般制

表 1. 安全応答時間(最悪値)の比較

項目	(単位: ms)						
	安全リモートI/O接続台数(台)						
	2	8	16	32	42	64	120
MELSEC iQ-Rシリーズ (CC-Link IEフィールド)	26	28	30	34	36	45	68
MELSEC QSシリーズ (CC-Link Safety)	103	103	104	126	127	-	-

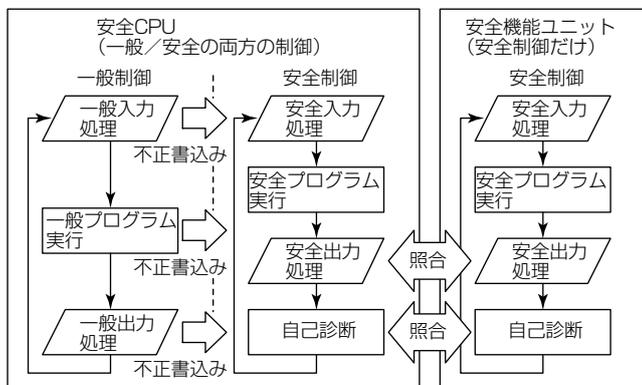


図 6. 一般制御からの不正書き込み検出

御部の故障やメモリのビット化け(ソフトウェア)等で安全制御部への不正書き込みが発生する可能性があります, これを検出する必要があります。

このため, MELSEC iQ-Rシリーズの安全CPUでは, 一般制御と安全制御を両方実行する安全CPUと, 安全制御だけを実行する安全機能ユニットの2つのユニットで安全プログラムと自己診断を実行して, プログラム実行結果から得られる安全出力値と自己診断結果を照合する(図6)。これによって, 安全CPUでの一般制御部からの不正書き込みを検出できる。

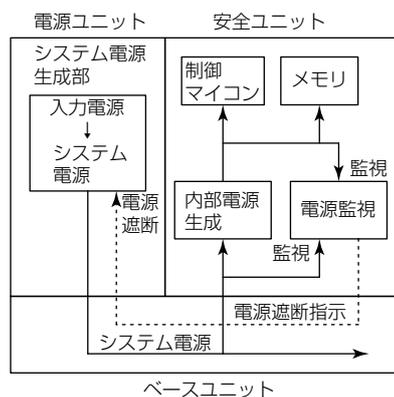
4.3 安全ユニットのシャットダウン

国際安全規格では, 安全制御を実行する回路の電源に安全制御を継続できない異常や故障が発生した場合, シャットダウンさせて安全状態へ移行させるなどの手法が必要である。

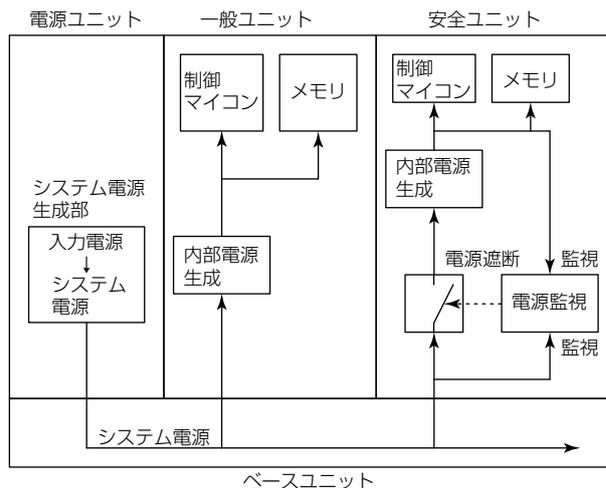
従来のMELSEC QSシリーズの安全シーケンサでは, 安全CPUで内部電源とシステム電源を監視して, 電圧異常時に安全電源ユニットでシステム電源を遮断することでシャットダウンさせる方法を取っていた(図7(a))。

MELSEC iQ-Rシリーズ安全シーケンサでは, 同一ベースユニット上に一般ユニットと安全ユニットが装着され, 電源ユニットからシステム電源が供給される。安全制御を実行する回路の電源に安全制御を継続できない異常や故障が発生した場合, 安全ユニットをシャットダウンさせて安全状態へ移行する必要がある。さらに, 電源ユニットから供給されるシステム電源から安全制御を実行する回路の電源を生成するため, 電源ユニットの異常や故障発生時も安全状態へ移行する必要がある。

また, 安全ユニットである安全CPUをシャットダウンさせると, 安全CPU内の一般制御を継続させることがで



(a) MELSEC QSシリーズ安全シーケンサ



(b) MELSEC iQ-Rシリーズ安全シーケンサ

図 7. 安全ユニットの電源遮断

きない。このため, 安全状態へ移行後も情報系処理などの一般制御を継続するシステムでは, 一般CPUと安全CPUのマルチCPU構成として, 安全CPUのシャットダウン後も一般CPUは動作を継続する必要がある。

したがって, 安全ユニットで内部電源とシステム電源を監視して, 異常や故障が発生した時には, 安全ユニット内部でシステム電源を遮断してシャットダウンさせる(図7(b))。これによって, 安全ユニット以外への電源供給が維持され, 一般ユニットは制御を継続できる。また, 一般ユニットと安全ユニットで電源ユニットを共用できる。

5. む す び

一般制御と安全制御を統合させたMELSEC iQ-Rシリーズ安全シーケンサについて, 製品の特長と一般制御と安全制御の統合のための技術について述べた。

規格と法制度の整備によって安全シーケンサに対する要望は日増しに増えており, 機能・性能・サポートなど多くの要望に応えるため製品力強化を進めていく。

参 考 文 献

- (1) 神余浩夫, ほか:安全シーケンサ“MELSEC Safety”, 三菱電機技報, 81, No.4, 277~280 (2007)