◆一般論文◆

# “MELSEC iQ-Rシリーズ”のIEC61508 SIL2対応二重化シーケンサ

百目木栄悦*

*"MELSEC iQ-R Series" IEC61508 SIL2-compliant Redundant Programmable Logic Controller*

*Eietsu Domeki*

**要　旨**

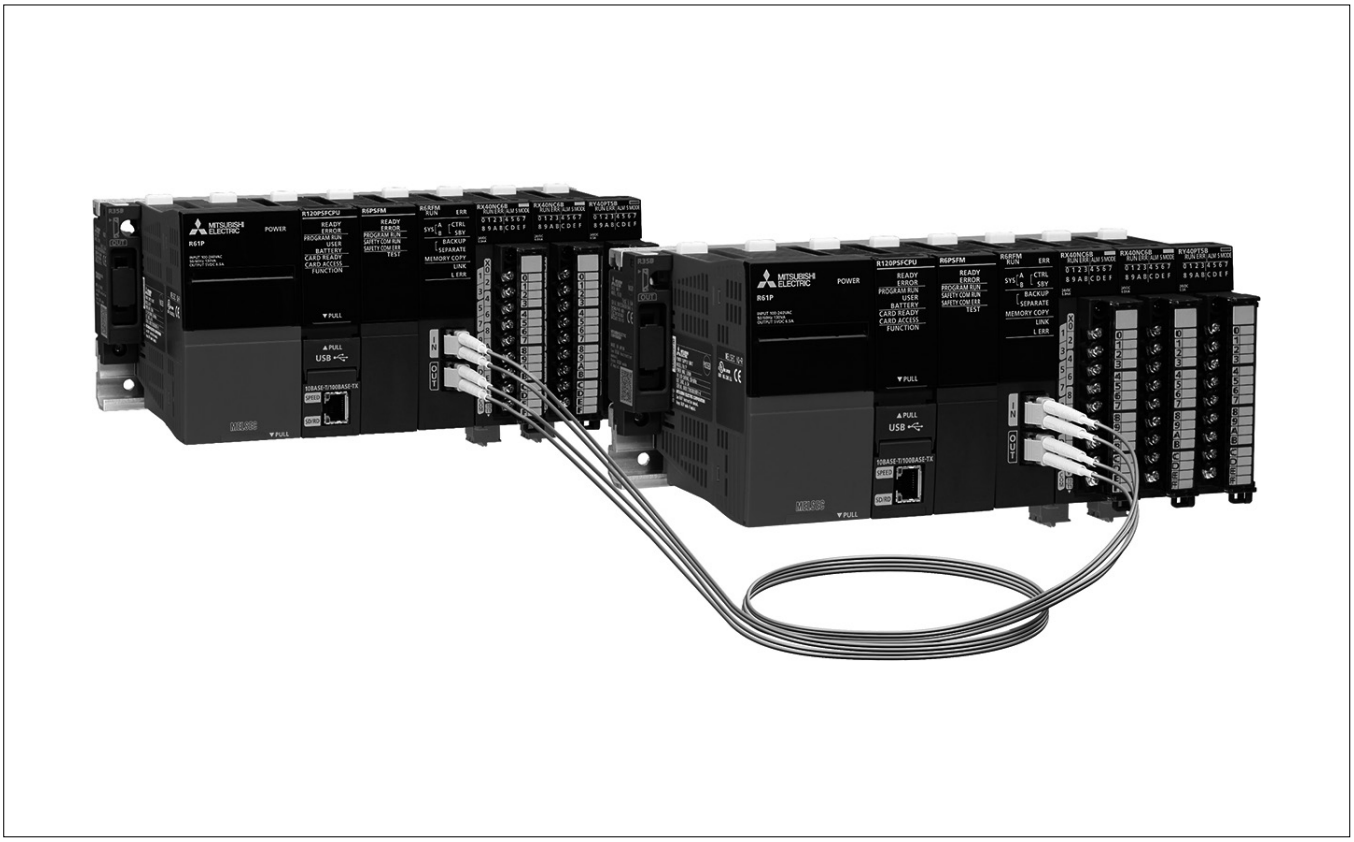
近年，社会インフラの水処理や地下鉄の空調システムなどの公共案件の市場規模が新興国を中心に拡大している。これら公共案件は可用性向上のために二重化したシステムが必須である。さらに最近の発注仕様では，構築するシステムに使用するコンポーネントの信頼性の指標として，国際安全規格IEC61508 SIL2適合が要求されてきている。

この要求に対応するため，今回三菱シーケンサ“MELSEC iQ-Rシリーズ”にIEC61508 SIL2に適合した二重化シーケンサを新たに追加した。この製品の特長は次のとおりである。

⑴ 二重化システム構成をとることで，片系に異常が発生しても，もう一方の系で安全制御を継続可能にした。これによって高い稼働率と安全性の両立を実現した。

⑵ “MELSEC iQ-Rシリーズ”安全シーケンサのコンセプトを踏襲し，一つのシステムでプロセス制御と安全制御を実現した。これによって二重化安全制御システムを容易に構築することができる。

⑶ 安全入出力として，診断機能付きI/O(Input/Output)ユニットを使用する構成とした。IEC61508 SIL2適合のシステムを構築する際は，診断機能付きI/Oユニットを２台組み合わせて使用する。SIL2適合が要求されないシステムでは診断機能付きI/Oユニット１台での使用も可能であり，これによって補用品の機種共通化を可能にした。



**“MELSEC iQ-Rシリーズ”のIEC61508 SIL2対応二重化シーケンサ**

三菱シーケンサMELSEC iQ-Rシリーズに，二重化システム構成を構築するユニットとして“SIL2プロセスCPU(Central Processing Unit)セット”を新たにラインアップに加えた。SIL2プロセスCPUセット，及び入出力を行う“診断機能付きI/Oユニット”は，第三者認証機関であるTÜV Rheinlandから機能安全規格IEC(International Electrotechnical Commission) 61508 SIL(Safety Integrity Level)2の認証を受けている。

*名古屋製作所

## 1. まえがき

近年，社会インフラの水処理や地下鉄の空調システムなどの公共案件の市場規模が新興国を中心に拡大している。これら公共案件のシステムは停止した場合の影響が大きく，止められないため，可用性向上のために二重化したシステムが必須となっている。さらに最近の公共案件の発注仕様では，システムに使用するコンポーネントにも高信頼な製品が求められ，その信頼性の指標として国際安全規格IEC61508 SIL2適合が要求されている。

このような状況に対して，三菱電機はMELSEC iQ-Rシリーズ[1]にIEC61508 SIL2対応二重化シーケンサ(以下“SIL2対応二重化シーケンサ”という。)を新たに追加した。この製品によって，IEC61508 SIL2に適合したシーケンサを使用したプロセス制御と安全制御によってユニットを集約してTCO(Total Cost of Ownership)削減を図るとともに，これらを二重化したシステム構成とすることで可用性を向上させている。

本稿では，SIL2対応二重化シーケンサの製品特長，及び開発時の課題とその解決のために適用した技術について述べる。

## 2. 製品の特長

SIL2対応二重化シーケンサの主な特長は，次のとおりである。

(1) 二重化システムによって，片系に障害が発生した場合でも系を切り替えて制御を継続することが可能である。

(2) 一システム内で，プロセス制御と安全制御を実行することが可能である。

(3) 標準的なユニットを組み合わせて，IEC61508 SIL2に適合したシステムの構成が可能である。

### 2.1 SIL2対応二重化シーケンサのシステム構成

SIL2対応二重化シーケンサのシステム構成例を**図1**に示す。CPU及びネットワークは二重化しており，制御系と待機系として動作する。I/Oはリモート局に装着する。

SIL2対応二重化シーケンサは，二重化したCPUの一方が制御系，もう一方が待機系として動作する。制御系が動作している間，待機系は制御を行わず，制御系の演算結果を毎スキャン制御系から受信して，待機系の内部メモリに反映している。

制御系側で障害を検出した場合，CPU及びネットワークは系切替えを行い，新たに制御系となった系のCPU及びネットワークが内部メモリのデータを用いて処理を再開することで制御を継続する。系切替えを行う要因としては，制御系の電源OFFや停止エラー発生時，ネットワークケーブル断線による通信不可などの障害がある。

### 2.2 一般制御と安全制御の統合

SIL2対応二重化シーケンサでのプロセス制御と安全制御については，MELSEC iQ-Rシリーズの安全CPUの特長を引き継いでいる[2]。安全CPUでは，一般プログラムと安全プログラムを統合して1台のシーケンサで実行可能である。SIL2対応二重化シーケンサも同様に，プロセス制御命令を実行可能な一般プログラムと，安全入出力を制御する安全プログラムを1台のシーケンサで実行可能である。

プログラミングについてもエンジニアリングソフトウェア“GX Works3”を使用して，プロセス制御拡張機能を含む一般プログラムと安全プログラムの編集，及び各種設定操作を一元的に行える。

二重化システムのトラッキングは一般制御と安全制御両方の全エリアを対象としており，安全制御で使用する安全ラベル／デバイスのデータも毎スキャン待機系の内部メモ

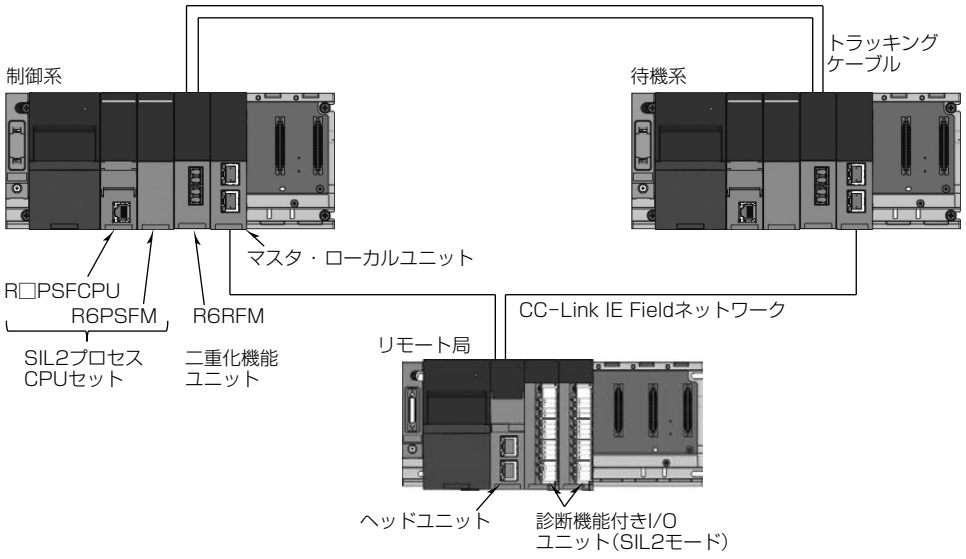



**図1．SIL2対応二重化シーケンサのシステム構成例**

リに反映されている。そのため，系切替えを行った後，新制御系で安全プログラムを実行できる。

さらに，一般制御用ネットワークと安全制御用ネットワークも安全CPUと同様混在することが可能である。このネットワークについてもSIL2二重化対応にし，一般入出力と安全入出力が混在したシステムで，系切替え後に新制御系で一般制御と安全制御を継続して実行することを可能にした。

安全制御では，CPUとI/Oユニットとの間で確立した安全通信を通じて入出力を行う。ここで安全通信とは，CPUとI/Oユニット間の通信が，ノイズなどの要因による破損や遅れなどのデータの欠損が発生せず正常に継続していることを保証するため，コネクションを確立して常に通信状態を診断する機能を備えたネットワーク通信プロトコルによる通信である。

二重化システムで系切替えが発生したとき，一度この安全通信は切断するが，入出力を一定時間ホールドし，このホールド時間中にすみやかに新制御系から再接続して安全制御を再開する。

### 2.3　複数台のユニットを組み合わせた安全入出力

安全入出力処理は，入力断線検出機能や，出力短絡検出機能などの診断機能を強化した診断機能付きI/Oユニットに搭載している。診断機能付きI/Oユニットは２台組み合わせて安全入出力機能を提供する。２台構成で互いに入出力信号や制御処理結果を照合することで故障検出を強化し，IEC61508 SIL2に適合している。

診断機能付きI/Oユニットは１台でも診断機能を利用可能であり，安全制御に用いない一般入出力としても使用できるため，補用品を一般のユニットと共用できる。

SIL2対応二重化シーケンサで使用するユニットの一覧を**表１**に示す。

これらの機能によって，**図１**で示すようなシステム構成を構築することが可能である。

**表１．SIL2対応二重化シーケンサで使用するユニット**

| ユニット | 形名 | 説明 |
|---|---|---|
| SIL2プロセスCPUセット | R08PSFCPU-SET | SIL2プロセスCPUユニット（R□PSFCPU）とSIL2機能ユニット（R6PSFM）のセット品 |
| | R16PSFCPU-SET | |
| | R32PSFCPU-SET | |
| | R120PSFCPU-SET | |
| 診断機能付き入力ユニット | RX40NC6B | ２台で安全入力に使用 |
| 診断機能付き出力ユニット | RY40PT5B | ２台で安全出力に使用 |
| 二重化機能ユニット | R6RFM | 制御系と待機系を接続する |
| CC-Link IE Field マスタ・ローカルユニット | RJ71GF11-T2 | ネットワークユニット（SIL2二重化対応） |
| CC-Link IE Field ヘッドユニット | RJ72GF15-T2 | |

（電源，ベース，一般入出力等はMELSEC iQ-Rシリーズユニットを使用）

## 3.　実現のための技術

### 3.1　安全ラベル／デバイスのトラッキング通信

二重化システムのプロセス制御では，制御系が，シーケンサのプログラム実行周期であるスキャン処理が完了するごとに，内部データからトラッキングデータを生成して待機系に送信する。待機系は受信したトラッキングデータを自身の内部メモリに反映する。この処理をトラッキング通信処理という。

制御系と待機系は，毎スキャンのEND処理でトラッキング通信を行う。これによって，常に制御系と待機系の内部データを一致させ，系切替え発生時に待機系が新制御系として処理を継続できるようにしている。

安全制御についても同様に，制御系で実行した安全制御で更新された安全ラベル／デバイスのデータを毎スキャン待機系に送信し，待機系の内部メモリに反映しておくことで，系切替え後の処理継続に対応する。ただし，安全制御にかかわる安全ラベル／デバイスは，通信路及び各ユニット内に異常がなく，待機系に正しく反映されたことを保証する必要がある。

この課題に対して，安全ラベル／デバイスのトラッキングデータの生成時にCRC（Cyclic Redundancy Check）値を付与し，待機系に反映した後に再度算出したCRC値と照合することで，正しく反映されたことを確認し，その結果を制御系に応答する処理フローを搭載した。

安全ラベル／デバイスを含むトラッキング通信処理フローの全体を**図２**に示す。

安全トラッキングのデータが破損した場合や，安全ラベル／デバイスが待機系に正しく反映できなかった場合は，系切替え不可とする。系切替え可かどうかは毎スキャン確認しており，また安全ラベル／デバイスは毎スキャン，変更の有無によらずデータ全体を送信し続ける。そのため，次回のトラッキングデータ送信で待機系にデータが正しく反映できたことが確認できれば，系切替え可となる。

これらの処理によって，一般制御と安全制御で使用する内部メモリを制御系と待機系で毎スキャン一致させることで，系切替えによって制御を継続可能にしている。

### 3.2　安全通信の系切替え対応

まずSIL2対応二重化シーケンサの安全通信について述べ，その後に系切替え時の安全通信の動作について述べる。

#### 3.2.1　SIL2対応二重化シーケンサの安全通信

SIL2対応二重化シーケンサでは，制御系のCPUと，安全入出力を行うI/Oだけが安全通信の接続を確立しており，待機系は安全通信接続を行っていない。安全通信の接続を**図３**に示す。

ネットワーク（CC-Link IE Field）は一般通信と安全通

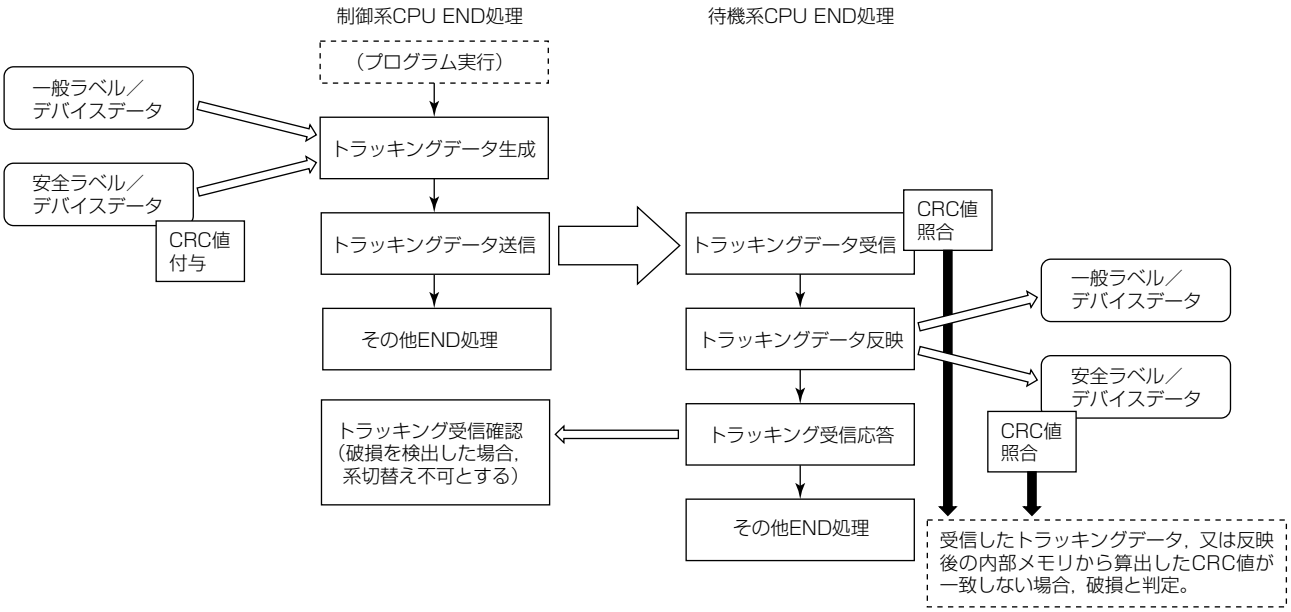



**図2．トラッキング通信処理フロー**

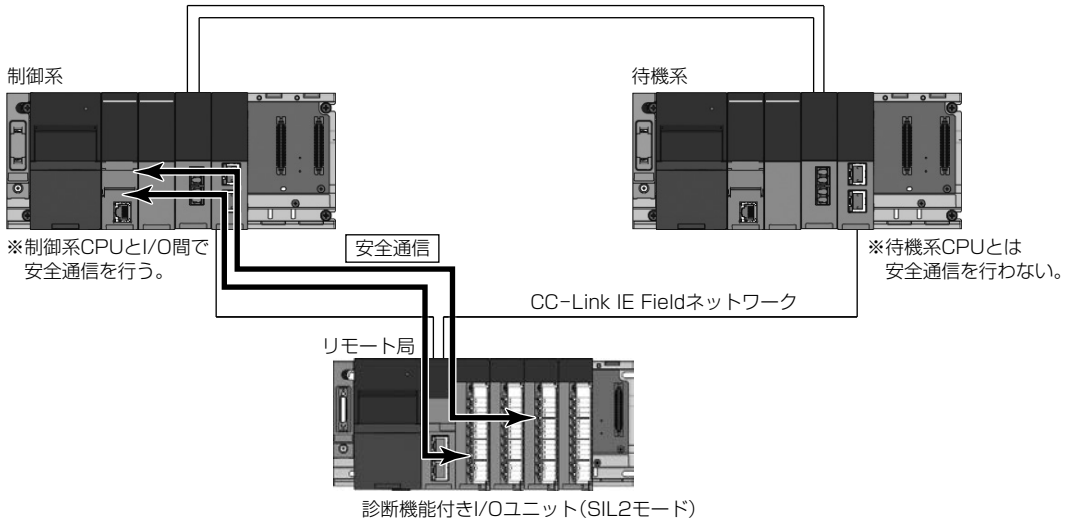



**図3．安全通信の接続**

信が混在可能であり，安全通信のパケットは常にネットワーク上に流れており，診断を実施している。安全通信のパケットが，ノイズやネットワークの再構築等の要因によって設定した時間以上中断されると，CPUとI/Oとで通信タイムアウトを検出する。また，安全通信のパケットが意図しない順番で到着した場合や，破損を検出した場合にはエラーを検出する。通信タイムアウトやエラーを検出した場合は安全通信を切断し，安全入出力は安全状態であるOFFとする。

### 3. 2. 2　系切替え時の安全通信の動作

**3. 1節**で述べたように，制御系で演算した結果の安全ラベル／デバイスのデータは，毎スキャン待機系へ送信されている。系切替えが発生した場合，安全ラベル／デバイスを引き継ぐだけでなく，安全通信を新制御系から接続し直して，制御を継続する必要がある。

系切替え時の安全通信の処理の動きを**図4**に示す。

**図4**にあるように，系切替え時は旧制御系との安全通信を一度切断する。このとき，本来の安全通信の動作では安全通信が切断された場合は安全状態となるため，安全入出力はOFFとなる。しかし，系切替え時に入出力がOFFになることは認められない。

この問題に対して今回の開発では，系切替え時の安全通信切断から，あらかじめパラメータで設定した時間が経過するまで安全入出力をホールド状態にし，その時間内に安全通信を再接続する動作にした。

新制御系が安全通信を再接続した後は，安全制御を継続できる。再接続しないまま設定した時間が経過すると，安全入出力はOFFになる。

この動作によって，二重化システムでの安全通信の系切替え対応を実現した。

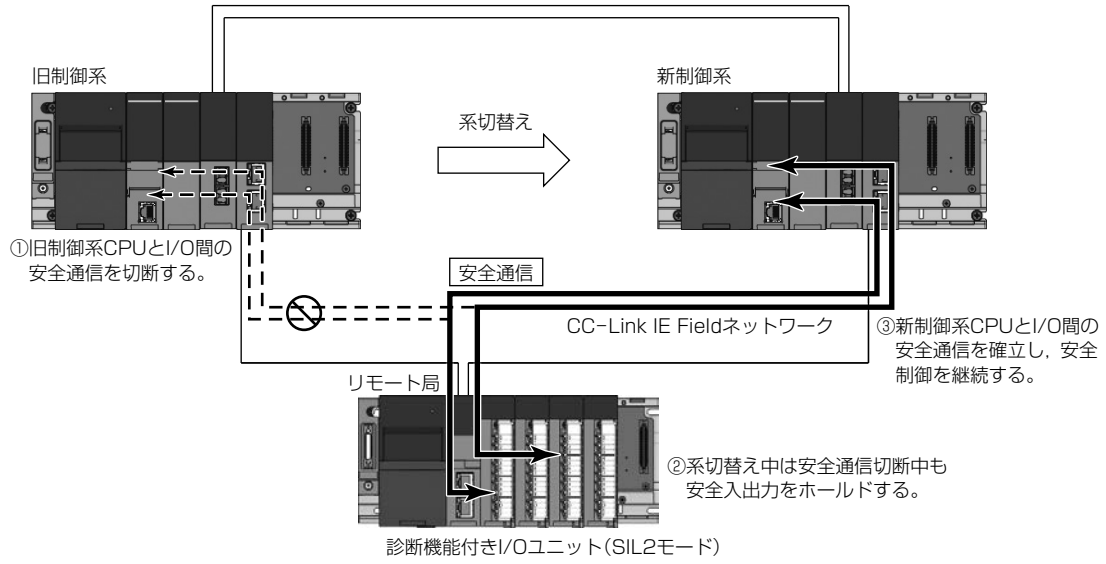



**図４．系切替え時の安全通信の再接続**

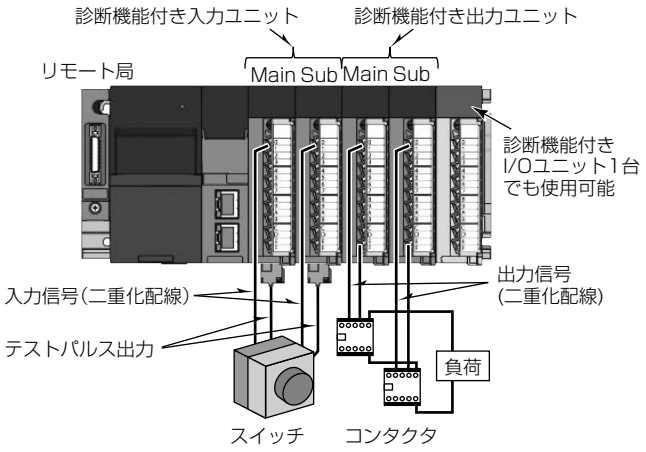



**図５．診断機能付きI/Oユニットの配線例**

### 3.3　複数ユニット組合せによる安全入出力

SIL2対応二重化シーケンサでは，１台で一般入出力に使用できる診断機能付きI/Oユニットを，２台組み合わせて安全入出力を構成する形とした。

安全入出力を行うためには，診断機能付きI/Oユニット２台を隣接したスロットに並べて装着し，それぞれSIL2モードのMain，Subに設定する。配線は入力信号，出力信号とも二重化配線を行い，入出力時に診断機能付きI/Oユニット同士で信号を照合する。また，制御処理もMain，Sub両方で実行し，その結果を互いに照合する。照合不一致の場合は安全入出力をOFFにする。

この仕様によって，診断機能付き入力ユニット，及び診断機能付き出力ユニットを，IEC61508 SIL2適合のシステム構築時は２台，一般入出力では１台構成で使用することで，補用品の機種を削減できる。SIL2対応時の，診断機能付きI/Oユニットの配線例を**図５**に示す。

## 4. む　す　び

社会インフラ分野(公共案件)をターゲットとして，信頼性の指標として要求が増えている国際安全規格IEC61508 SIL2適合の“MELSEC iQ-Rシリーズ”二重化シーケンサの特長と開発時に適用した技術について述べた。

今後は，IEC61508 SIL2に適合したアナログ入力，アナログ出力，及び温度入力ユニットについて製品ラインアップを拡大し，ASEANを中心とした社会インフラ分野での要求対応力の強化を進める。

## 参　考　文　献

(1) 志水義信，ほか：三菱シーケンサ“MELSEC iQ-Rシリーズ”，三菱電機技報，**89**，No.4，211～214 (2015)
(2) 内越正弘：“MELSEC iQ-Rシリーズ”安全シーケンサ，三菱電機技報，**90**，No.4，215～218 (2016)