セーフティ・リファレンス・マニュアル

Allen-Bradley

GuardLogix 5580およびCompact GuardLogix 5380 コントローラ システム

Cat. No. 1756-L81ES、1756-L82ES、1756-L83ES、1756-L84ES、1756-L8SP、1756-L81ESK、1756-L82ESK、1756-L83ESK、1756-L84ESK、1756-L8SPK、5069-L306ERMS2、5069-L306ERS2、5069-L310ERMS2、5069-L310ERS2、5069-L320ERMS2、5069-L320ERS2、5069-L320ERS2K、5069-L320ERMS2K、5069-L330ERMS2、5069-L330ERS2、5069-L330ERS2K、5069-L330ERMS2K、5069-L340ERMS2、5069-L340ERS2、5069-L350ERMS2、5069-L350ERS2、5069-L350ERS2K、5069-L350ERMS2K、5069-L380ERMS2、5069-L380ERS2、5069-L3100ERMS2、5069-L3100ERS2

お客様へのご注意

本装置の設置、構成および操作については、本書および参考資料に記載された資料に目を通してから、本製品の設置、構成、操作、メンテナンスを行なってください。ユーザは適用されるすべての条例、法律、規格要件に加えて、設置、配線指示に熟知している必要があります。

設置、調整、供用開始、使用、組立て、分解、メンテナンスを含めた作業は、適切な実施基準に従って適切な訓練を受けた作業員しか実施しないでください。

本装置を製造メーカの指定した方法以外で使用した場合、装置の保護機能が低下する可能性があります。

この機器の使用によって何らかの損害が生じても当社は一切責任を負いません。

本書で使用した図表やプログラム例は内容を理解しやすくするためのものであり、その結果としての動作を保証するものではありません。個々の用途については数値や条件が変わることが多いため、当社では図表やプログラム例に基づいて実際に使用した場合の結果については責任を負いません。

本書に記載されている情報、回路、機器、装置、ソフトウェアの利用に関して特許上の問題が生じても、当社は一切責任を負いません。製品改良のため、仕様などを予告なく変更することがあります。

Rockwell Automation, Inc. の書面による許可なく本書の全部または一部を複製することは禁じられています。

本書を通じて、特定の状況下で起こりうる人体または装置の損傷に対する警告および注意を示します。

	警告：危険な環境で爆発が発生し、それにより人員の傷害や死亡、財産の損傷、あるいは経済的損失につながる可能性のある操作または状況に関する情報を示します。
	注意：人員の傷害や死亡、財産の損害、あるいは経済的損失につながる可能性のある操作または状況に関する情報を示します。危険を示し、危険を防止し、結果を認識する助けとなるよう注意を促します。
重要	本書内の「重要」は、製品を正しく使用および理解するために特に重要な事項を示します。

ラベルは特定の注意を促すために、装置の外部もしくは内部にも貼ってあります。

	感電の危険：危険な電圧が生じる恐れがあることを警告するために、ドライブやモータなどの装置または装置の内部にラベルを貼っています。
	やけどの危険：表面が危険な温度に達する恐れがあることを警告するために、ドライブやモータなどの装置または装置の内部にラベルを貼っています。
	アーク閃光の危険：モータ・コントロール・センタなどの装置上、または装置内にあるラベルは、アーク閃光などが発生する可能性があることを警告します。アーク閃光は重傷または死亡にいたる恐れがあります。適切な保護具 (PPE) を装着してください。作業の安全と保護具 (PPE) に必要な規制要件を順守してください。

はじめに

変更内容 7
用語 7
参考資料 8

第 1 章

安全度水準 (SIL) の概念

SIL 認可 11
プルーフテスト 12
GuardLogix アーキテクチャ 13
コントローラの仕様 15
システム応答時間 15
　安全タスクの応答時間 15
　安全タスク時間と安全タスクウォッチドッグ 16
デバイスに故障が発生した場合の連絡先情報 16

第 2 章

GuardLogix コントローラシステム

GuardLogix 5580 コントローラのハードウェア 17
　プライマリコントローラ 18
　安全パートナ 18
　シャーシ 18
　電源 18
Compact GuardLogix 5380 コントローラのハードウェア 19
　電源 20
ネットワーク通信 20
　EtherNet/IP ネットワーク 20
　DeviceNet Safety ネットワーク 23
プログラミングの概要 24

第 3 章

GuardLogix 制御システム用の安全 I/O

安全 I/O デバイスの標準的な安全機能 25
　診断 25
　ステータスデータ 26
　ステータスインジケータ 26
　オンディレイまたはオフディレイ機能 26
応答時間 26
安全 I/O デバイスの安全に関する注意事項 27
　所有者 27
　安全 I/O の構成署名 27
　安全 I/O デバイスの交換 28

第 4 章

CIP Safety および安全ネットワーク番号

固有のノード参照 31
安全ネットワーク番号 (SNN) 31
ルーティング可能な CIP Safety システム 32
SNN の割付けに関する注意事項 32
安全デバイスへの SNN の割付方法 34

SNN フォーマット 35
タイムベースの SSNN フォーマットと割付け 35
手動の SNN フォーマットと割付け 36
初期状態のデバイスの SNN 37

第 5 章

安全タグ、安全タスク、安全プログラムの特性

標準と安全の違い 39
安全タスク 40
安全タスクの制限 40
安全タスク実行の詳細 41
SIL 2 および SIL 3 安全アプリケーションの違い 42
高速 I/O モジュール 43
ヒューマン・マシン・インターフェイスの使用 44
注意事項 44
安全関連のシステムへのアクセス 45
安全プログラム 46
安全ルーチン 46
安全タグ 47
安全ルーチンの標準タグ (タグマッピング) 48

第 6 章

安全アプリケーションの開発

安全概念の前提条件 49
アプリケーション開発とテストの基本 50
ライフライフサイクルの立ち上げ 52
安全機能の仕様 53
プロジェクトの作成 54
アプリケーションプログラムのテスト 54
安全署名の生成 54
プロジェクトの検証 55
プロジェクトの確認 56
安全評価 57
コントローラのロック 57
安全アプリケーションプログラムのダウンロード 58
安全アプリケーションプログラムのアップロード 59
メモリカードからのプロジェクトの保存とロード 59
データの強制 59
デバイスの禁止 60
オンライン編集 60
安全アプリケーションの編集 61
オフライン編集の実行 61
オンライン編集の実行 62
修正の影響テスト 62

第 7 章

ステータスのモニタおよびフォルトの処理

ステータスインジケータ 65
システムステータスのモニタ 65
CONNECTION_STATUS データ 65
入力と出力の診断 66
I/O デバイスのコネクションステータス 67

トリップシステムに対するオフ状態 67
システム値の取得 (GSV) 命令およびシステム値の設定 (SSV) 命令 67
安全フォルト 68
回復不能なコントローラフォルト 68
安全アプリケーションでの回復不能な安全フォルト 68
安全アプリケーションでの回復不能な安全フォルト 69
フォルトの表示 70
フォルトコード 70
安全パートナフォルト 70

付録 A

安全命令

安全命令 71

付録 B

安全アドオン命令の作成と使用

アドオン命令テストプロジェクトの作成 77
安全アドオン命令の作成 77
命令署名の生成 77
安全命令署名 77
SIL 2 または SIL 3 のアドオン命令認証テスト 78
安全アドオン命令の検証 78
署名履歴エントリの作成 78
安全アドオン命令のエクスポートとインポート 78
安全アドオン命令署名の確認 79
アプリケーションプログラムのテスト 79
プロジェクト検証 79
安全評価 79

付録 C

応答時間

コネクション応答時間制限 81
要求パケット間隔 (RPI) の指定 82
Maximum Observed Network Delay の表示 82
システム応答時間 83
Logix システムの応答時間 83
単純な入力ロジック出力チェーン 83
プロデューサ / コンシューマ安全タグを使用するロジックチェーン 84
Logix 応答時間コンポーネントに影響する要因 85
Guard I/O 入力モジュールの遅延時間設定の構成 86
入力および出力安全コネクション応答時間制限の構成または表示 86
安全タスク時間およびウォッチドッグの構成 88
プロデューサタグ / コンシューマタグのデータへのアクセス 88

GuardLogix 安全アプリケーションのチェックリスト

付録 D
GuardLogix コントローラシステムのチェックリスト 92
安全入力のチェックリスト 93
安全出力のチェックリスト 94
安全アプリケーションプログラム開発のチェックリスト 95

GuardLogix システムの安全データ

付録 E
耐用年数..... 97
安全データ 97
製品故障率 98

Studio 5000 Logix Designer アプリケーション バージョン 31 以降の安全アプリケーション命令

付録 F
トリップシステムに対するオフ状態..... 99
コネクション・ステータス・データを使用した
プログラムによるフォルトの起動 99

用語集 105

索引 111

項目	参照ページ
用語	7
参考資料	8

このマニュアルはGuardLogix® 5580およびCompact GuardLogix 5380コントローラシステムについて説明しています。これらのシステムは、型式認証を受けており、11ページの「SIL認可」に詳しく説明したように安全アプリケーションでの使用を認可されています。

このマニュアルは、Studio 5000 Logix Designer®アプリケーションを使用するGuardLogix 5580またはCompact GuardLogix 5380コントローラベースの安全システムを開発、動作、保守を行なうためのものです。GuardLogix 5580またはCompact GuardLogix 5380コントローラベースの安全システムの操作を行なう前に、このマニュアルに記載された安全概念と要件を読み、理解し、適用される標準(IEC 61508、IEC 62061、IEC 61511、ISO 13849-1など)に馴染んでください。

変更内容

本書には、以下の表に示す新しい情報と更新情報が記載されています。

項目	参照ページ
「はじめに」の文章を更新	7
安全パートナの文章を更新	18
Compact GuardLogix 5380コントローラのハードウェアセクションに「重要」のステートメントを追加	19
安全概念の前提条件のセクションを更新	49
表9のタイトルを更新	74
製品故障率のセクションを更新	98

用語

ここでは、このマニュアルで使用する用語を定義します。

このマニュアルでは、「GuardLogixコントローラ」または「GuardLogixシステム」という用語は、特に断りのない限りGuardLogix 5580コントローラとCompact GuardLogix 5380コントローラの両方に適用されます。

また、「SIL 2」はSIL 2、SIL CL2、およびPLdを表し、「SIL 3」はSIL 3、SIL CL3、およびPLeを表します。

一般的な略語とその他の定義は、105ページの「用語集」を参照してください。

参考資料

以下の資料には、ロックウェル・オートメーションが提供する関連製品の使用時に役立つ情報が記載されています。

マニュアル名	説明
ControlLogix 5580 and GuardLogix 5580 Controllers User Manual (Pub. No. 1756-UM543)	Studio 5000 Logix Designerプロジェクトで ControlLogix® 5580コントローラと GuardLogix 5580コントローラを取付け、構成、プログラミングおよび使用する方法に関する説明
CompactLogix 5380 and Compact GuardLogix 5380 User Manual (CompactLogix 5380 および Compact GuardLogix 5380 コントローラ ユーザーズマニュアル) (Pub. No. 5069-UM001)	CompactLogix™ 5380コントローラと Compact GuardLogix 5380を取付け、構成、プログラミングおよび使用する方法に関する説明
1756 ControlLogix and GuardLogix Controllers Technical Data (Pub. No. 1756-TD001)	ControlLogixおよびGuardLogixコントローラの製品仕様と認可のリスト
CompactLogix 5380 Controllers Specifications (Pub. No. 5069-TD002)	CompactLogix 5380コントローラおよびCompact GuardLogix 5380コントローラの製品仕様と認可のリスト
ControlLogix Chassis and Power Supply Installation Instructions (ControlLogixシャーシおよび電源インストレーションインストラクション) (Pub. No. 1756-IN005)	さまざまなControlLogixシャーシおよび電源の取付け方法の説明
CompactLogix 5380 Controllers Installation Instructions (Pub. No. 5069-IN014)	CompactLogix 5380コントローラの取付け方法の説明
Replacement Guidelines: Logix5000 Controllers Reference Manual (Pub. No. 1756-RM100)	これらのコントローラの次の交換方法に関するガイドライン: • ControlLogix 5560 または 5570 コントローラを ControlLogix 5580 コントローラに交換 • CompactLogix 5370 L3 コントローラを ControlLogix 5380 コントローラに交換
GuardLogix Safety Application Instruction Set Reference Manual (Pub. No. 1756-RM095)	GuardLogix安全アプリケーション命令セットに関する説明
GuardLogix 5580 Controllers Installation Instructions (Pub. No. 1756-IN048)	GuardLogix 5580コントローラの取付け方法の説明
Kinetix 5700 Safe Monitor Functions Safety Reference Manual (Pub. No. 2198-RM001)	Logix5000™コントローラおよびKinetix® 5700サーボドライブでの統合停止機能と安全モニタ機能に関する説明
Compact 5000 Safety Sinking Input Module Installation Instructions (Pub. No. 5069-IN020)	5069-IB8Sモジュールの取付け方法に関する説明
Compact 5000 Configurable Safety Output Module Installation Instructions (Pub. No. 5069-IN021)	5069-OBV8Sモジュールの取付け方法に関する説明
Compact 5000 Digital and Safety I/O Modules User Manual (Logix5000制御システムの5000シリーズのデジタルI/Oモジュール ユーザーズマニュアル)(Pub. No. 5000-UM004)	一部のモジュールを安全アプリケーションで使用する方法を含む、Compact 5000™デジタルモジュールおよび安全I/Oモジュールの使用方法に関する説明
Guard I/O DeviceNet Safety Modules User Manual (Guard I/O DeviceNet Safety モジュール ユーザーズマニュアル) (Pub. No. 1791DS-UM001)	Guard I/O™ DeviceNet Safetyモジュールの使用方法に関する説明
Guard I/O EtherNet/IP Safety Modules User Manual (Guard I/O EtherNet/IP 安全モジュール ユーザーズマニュアル) (Pub. No. 1791ES-UM001)	Guard I/O EtherNet/IPセーフティモジュールの使用方法に関する説明
POINT Guard I/O Safety Modules User Manual (Pub. No. 1734-UM013)	POINT Guard I/O™モジュールの取付けおよび使用方法に関する説明
Kinetix 5500 Servo Drives User Manual (Kinetix 5500サーボドライブ ユーザーズマニュアル) (Pub. No. 2198-UM001)	Kinetix 5500サーボドライブの取付けおよび使用方法に関する説明
Kinetix 5700 Servo Drives User Manual (Kinetix 5700サーボドライブ ユーザーズマニュアル) (Pub. No. 2198-UM002)	Kinetix 5700サーボドライブの取付けおよび使用方法に関する説明
PowerFlex 527 Adjustable Frequency AC Drive User Manual (PowerFlex 527 可変周波数 AC ドライブ ユーザーマニュアル)(Pub. No. 520-UM002)	PowerFlex® 527ドライブの取付けおよび使用方法に関する説明
Logix5000 Controllers General Instructions Reference Manual (Logix5000コントローラ汎用インストラクション・セット・リファレンス・マニュアル) (Pub. No. 1756-RM003)	汎用命令、モーション命令、およびプロセス命令を含むLogix5000命令セットに関する説明
Logix5000 Controllers Common Procedures Programming Manual (Pub. No. 1756-PM001)	プロジェクトファイルの管理、タグの整理、ルーチンのプログラムおよびテスト、フォルト処理を含むLogix5000コントローラのプログラムに関する説明
Logix5000 Controllers Add-On Instructions Programming Manual (Pub. No. 1756-PM010)	Logixアプリケーションでの標準および安全アドオン命令の作成と使用方法に関する説明
DeviceNet Modules in Logix5000 Control Systems User Manual (Pub. No. DNET-UM004)	Logix5000制御システムでの1756-DNBモジュールの使用方法に関する説明
EtherNet/IP Modules in Logix5000 Control Systems User Manual (EtherNet/IPネットワーク構成 ユーザーズマニュアル)(Pub. No. ENET-UM001)	Logix5000制御システムでの1756-ENBTモジュールの使用方法に関する説明
ControlNet Modules in Logix5000 Control Systems User Manual (Pub. No. CNET-UM001)	Logix5000制御システムでの1756-CNBモジュールの使用方法に関する説明
Logix5000 Controllers Execution Time and Memory Use Reference Manual (Pub. No. 1756-RM087)	命令の実行時間とメモリ使用量の推定方法に関する説明

マニュアル名	説明
Logix5000 Import Export Reference Manual (Pub. No. 1756-RM084)	Studio 5000 Logix Designer Import/Exportユーティリティの使用方法に関する説明
Industrial Automation Wiring and Grounding Guidelines (配線と接地のガイドライン) (Pub. No. 1770-4.1)	ロックウェル・オートメーションの産業用システムを取付けるための一般的なガイドラインを提供する。
製品の認可に関するWebサイト: http://www.rockwellautomation.com/global/certification/overview.page	適合宣言書、認可、およびその他証明の詳細を記載している。

これらの資料は、http://www.rockwellautomation.com/global/literature-library/overview.page で閲覧またはダウンロードできます。

印刷されたマニュアルを購入するには、当社または代理店までご連絡ください。

Notes:

安全度水準(SIL)の概念

項目	参照ページ
SIL 認可	11
プルーフテスト	12
GuardLogix アーキテクチャ	13
コントローラの仕様	15
システム応答時間	15
デバイスに故障が発生した場合の連絡先情報	16

SIL認可

ここでは、コントローラのSIL認可と安全遂行レベルについて説明します。

コントローラシステム	IEC 61508 以下の水準までの安全アプリケーションでの使用のために型式認証を受け認可されています。	IEC 62061 以下の水準までを含む安全アプリケーションでの使用に適しています。	ISO 13849-1 以下の水準までを含む安全アプリケーションでの使用に適しています。
GuardLogix 5580 コントローラシステム	SIL 2(2) SIL 3(3)	SIL CL2(2) SIL CL3(3)	安全遂行レベル PLd (カテゴリ 3)(2) 安全遂行レベル PLe (カテゴリ 4)(3)
Compact GuardLogix 5380 SIL 2 コントローラシステム(1)	SIL 2	SIL CL2	安全遂行レベル PLd (カテゴリ 3)

(1) 例えば、5069-L3*xxxx*S2 のように末尾に「2」のある Compact GuardLogix 5380 コントローラカタログ番号は、SIL 2 までの安全アプリケーション用です。
(2) 安全パートナなしで使用されるプライマリコントローラ。
(3) 安全パートナと共に使用されるプライマリコントローラ。

重要 このマニュアルでは、これ以降、以下に注意してください。

- SIL 2 は SIL 2、SIL CL2、および PLd を表す
- SIL 3 は SIL 3、SIL CL3、および PLe を表す

TÜV Rheinlandは、電源が投入されていない状態を安全状態と見なす安全関連アプリケーションにGuardLogix 5580およびCompact GuardLogix 5380コントローラシステムを使用することを認めています。

このマニュアル内に記載されているI/Oの例のすべては、標準的な機械安全と非常シャットダウン(ESD)システムのために安全状態としてオフにすることに基づいています。

重要　システムユーザは以下の作業に対して責任を負います。

- GuardLogix システムに接続されるすべてのセンサ、アクチュエータのセットアップ、SIL の評価、および妥当性確認
- プロジェクト管理および機能テスト
- パスワードの取扱いを含む、安全システムへのアクセス制御
- このセーフティ・リファレンス・マニュアルおよび以下のマニュアルに従ったアプリケーションとデバイス構成のプログラミング
  - ControlLogix 5580 and GuardLogix 5580 Controllers User Manual (Pub. No. 1756-UM543)
  - CompactLogix 5380 および Compact GuardLogix 5380 コントローラユーザーズマニュアル (Pub. No. 5069-UM001)

機能安全を適用するときは、トレーニングを受けて経験がある、資格と権限が与えられた人にアクセスが制限されています。

GuardLogix 5580およびCompact GuardLogix 5380コントローラのプログラムを作成するには、Studio 5000 Logix Designerアプリケーションを使用します。安全機能には、標準タスクではなく安全タスクのみを使用します。

プルーフテスト

IEC 61508は、システムで使用する装置の各種プルーフテストを実行することを必要とします。プルーフテストは、ユーザが定義した間隔で実施されます。例えば、プルーフテストは、1年ごと、15年ごと、または適切なタイムフレームにすることができます。

GuardLogix 5580およびCompact GuardLogix 5380コントローラの耐用年数は20年で、プルーフテストは必要ありません。安全I/Oデバイス、センサ、アクチュエータなどのシステムの他のコンポーネントは、プルーフテスト間隔が短い可能性があります。

重要　アプリケーションによって耐用年数のタイムフレームが決まります。

GuardLogix アーキテクチャ

このセクションでは、以下を含むSIL 3システムおよびSIL 2システムについて説明します。

- 安全機能全体
- 安全機能全体におけるGuardLogix部分
- 外部機能を動作しながら他のデバイス(HMIなど)を接続する方法

図1 - SIL 3システムの例

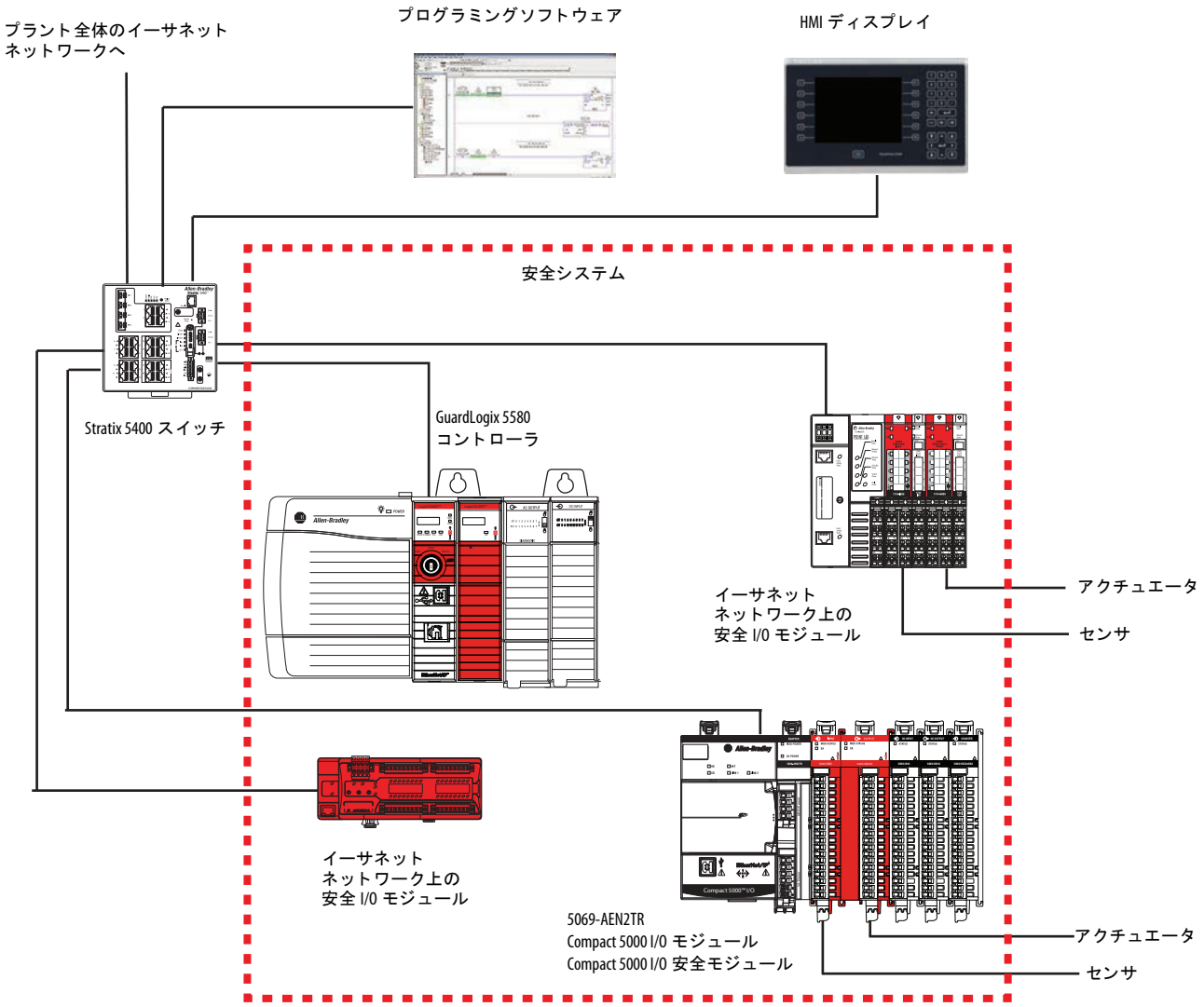
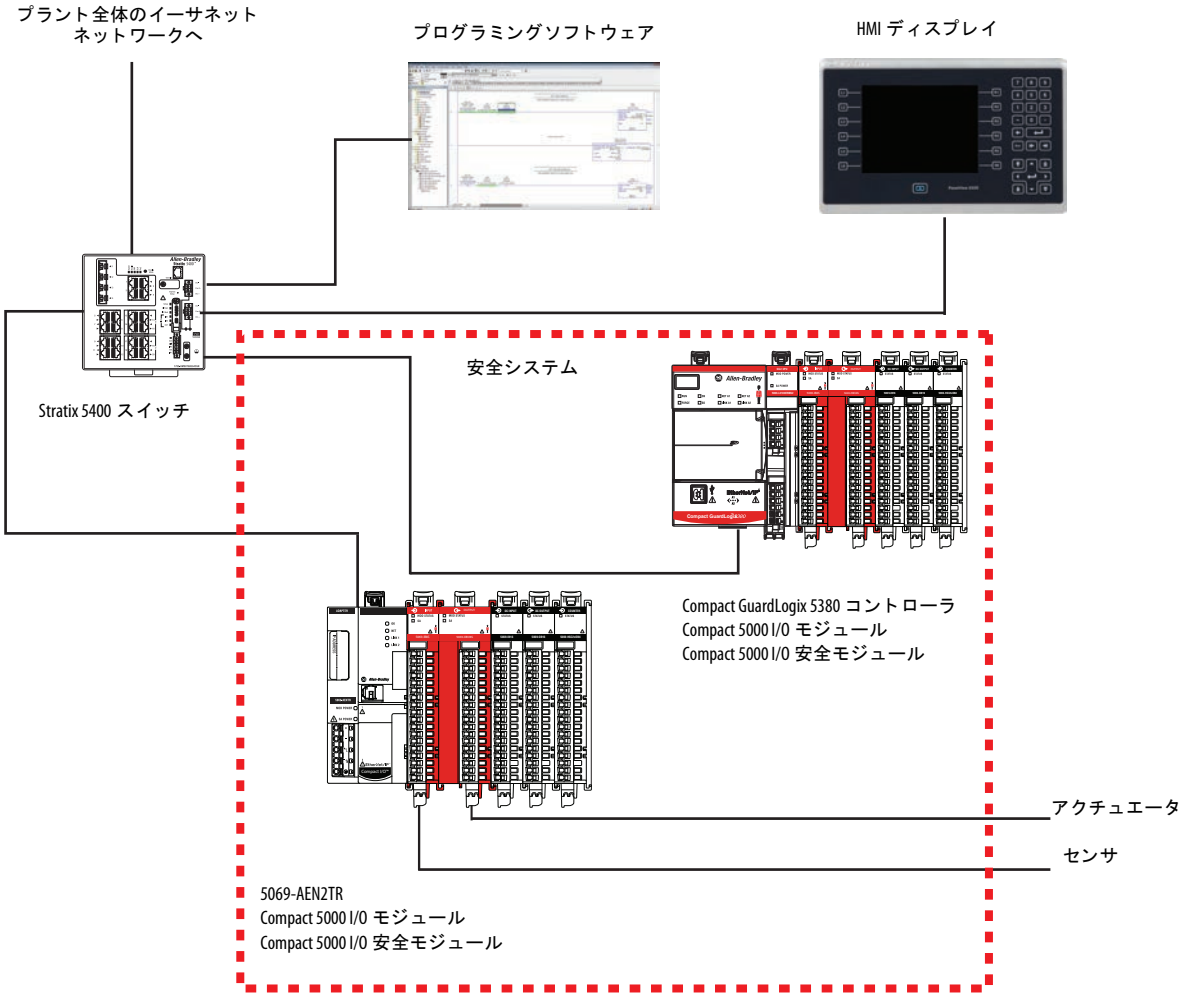


図2 - SIL 2システムの例



コントローラの仕様

以下の資料には、製品の使用と機関の認可がリストされています。

- ControlLogix Controllers Technical Data (Pub. No. 1756-TD001)
- CompactLogix 5380 Controllers Specifications Technical Data (Pub. No. 5069-TD002)

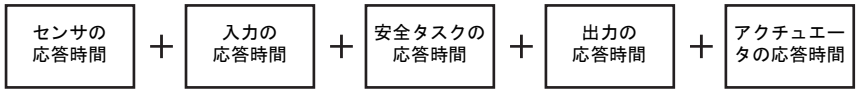
機関の認可は、製品のラベルにも印されています。

適合宣言、認可、および他の承認については、以下のWebサイトを参照してください。
http://www.rockwellautomation.com/global/certification/overview.page

システム応答時間

システム応答時間は、システムへの入力としての安全関連イベント、またはシステム内のフォルトが、システムを安全状態にするまでの最悪の場合の時間です。

この最悪の場合の定義には、非同期の通信の影響、およびシステム内での複数の潜在フォルトが含まれます。実際の応答時間は、これよりも短い場合があります。



各応答時間は、I/Oデバイスのタイプやプログラムで使用される命令などの要因によって異なります。

重要　応答時間の計算の詳細は、81 ページの付録 Cを参照してください。

安全タスクの応答時間

安全タスクの応答時間は、コントローラに送られる任意の入力変更から、処理された出力が出力プロデューサによって設定されるまでの最悪の場合の遅延です。次の式は、安全タスクの応答時間を決定するために使用します。

安全タスクの応答時間 = (安全タスク時間 + 安全タスクウォッチドッグ) x 1.01

マルチプライヤはクロックの変動の可能性のためです。

安全タスク時間と安全タスクウォッチドッグ

安全タスク時間は、安全タスクを実行する間隔のことです。

安全タスクウォッチドッグ時間は、安全タスク処理の最大許容時間です。安全タスク処理時間が安全タスクウォッチドッグ時間を超えると、コントローラで回復不能な安全フォルトが発生し、自動的に安全状態(オフ)に切り換わります。

安全タスクウォッチドッグ時間は、安全タスク時間以下で定義しなければなりません。

安全タスクウォッチドッグ時間は、Studio 5000 Logix Designer アプリケーションのタスクプロパティのウィンドウで設定します。この値はコントローラモードに関係なくオンラインで変更できますが、コントローラが安全ロックされている場合、または安全署名が作成されている場合には変更できません。

デバイスに故障が発生した場合の連絡先情報

安全デバイスで故障が発生した場合は、最寄の当社事業所または当社代理店までご連絡のうえ、以下の手続きを行なってください

- 該当のカタログ番号を正しく記録し、履歴に故障が記録されるようにして、当社にデバイスを返送します。
- 必要に応じて、故障の原因の究明のための故障分析を要求します。

第 2 章

GuardLogix コントローラシステム

項目	参照ページ
GuardLogix 5580 コントローラの ハードウェア	17
Compact GuardLogix 5380 コントローラの ハードウェア	19
ネットワーク通信	20
プログラミングの 概要	24

安全認可情報については、
http://www.rockwellautomation.com/global/certification/safety.pageをご覧ください。フィルタを使用してご使用の製品を検索してください。

GuardLogix 5580およびCompact GuardLogix 5380コントローラの取付け情報については、8ページの「参考資料」を参照してください。

GuardLogix 5580 コントローラの ハードウェア

GuardLogixコントローラは、SIL 2アプリケーションで単独で使用できるプライマリコントローラ(ControlLogix 558*x*S)、およびSIL 3対応のコントローラを作成するために追加される安全パートナ(ControlLogix 558SP)で構成されます。

プライマリコントローラと安全パートナは、両方とも電源投入時とランタイム時にコントローラ内のすべての安全関連コンポーネントの機能診断テストを実行します。

- 安全パートナなしで使用されるプライマリコントローラはSIL 2までです。
- 安全パートナを追加して使用されるプライマリコントローラはSIL 3までです。

コントローラ	Cat. No.
GuardLogix 5580 コントローラ	1756-L81ES、1756-L82ES、1756-L83ES、1756-L84ES、1756-L8SP、1756-L81ESK、1756-L82ESK、1756-L83ESK、1756-L84ESK、1756-L8SPK

認可されたGuardLogixコントローラと安全I/Oのシリーズおよびファームウェアバージョンの最新リストは、
http://www.rockwellautomation.com/global/certification/safety.pageのSafety Certificatesを参照してください。

ファームウェアリビジョンは、ロックウェル・オートメーションの製品互換性およびダウンロードセンター(PCDC)のサポートWebサイトからダウンロードできます。
http://www.rockwellautomation.com/global/support/pcdc.page

GuardLogix SIL 2またはSIL 3システムに使用しないSIL 2またはSIL 3システムシャーシのスロットには、低電圧指令とEMC指令で認可された他のControlLogix (1756)モジュールを取付けることができます。

コントローラとI/Oモジュールの認可を確認するには、以下のWebサイトを参照してください。
http://www.rockwellautomation.com/global/certification/overview.page

プライマリコントローラ

プライマリコントローラは、標準および安全制御機能を実行し、GuardLogix制御システムの安全関連機能のために安全パートナと通信するプロセッサです。プライマリコントローラは、中央プロセッサ、I/Oインターフェイス、およびメモリで構成されます。

安全パートナ

SIL 3要件を満たすには、ControlLogix 558SP安全パートナをプライマリコントローラのすぐ右側のスロットに取付ける必要があります。安全パートナは、システムの安全関連機能の1oo2アーキテクチャを提供するコプロセッサです。1oo2システムは機能が低下した状態では実行されません。2 つのプロセッサが食い違う場合、または相互に通信できない場合、メジャーな回復不能なコントローラフォルトの発生という結果をもたらします。この状況への対応方法については、ロックウェル・オートメーションのナレッジベースの記事63983を参照してください。

SIL 2の要件では、安全パートナを取付けないでください。

プライマリコントローラはセーフティパートナを構成します。ユーザプログラムをプライマリコントローラに一度だけダウンロードすることが必要です。プライマリコントローラは、安全パートナの動作モードを制御します。

シャーシ

シャーシは、モジュールと1756 GuardLogixシステムの間を物理的に接続します。故障があれば、システムの1つまたは複数のアクティブコンポーネントによって故障として検出されます。したがって、シャーシは安全の検討には無関係です。

電源

ControlLogix電源のSIL 2またはSIL 3動作には、追加の構成や配線は必要ありません。故障があれば、GuardLogixシステムの1つまたは複数のアクティブコンポーネントによって故障として検出されます。したがって、電源は安全の検討には無関係です。

Compact GuardLogix 5380 コントローラのハードウェア

Compact GuardLogix 5380コントローラは、Compact GuardLogix制御システムで安全関連の標準の機能および安全制御機能を実行するSIL 2対応のコントローラです。

コントローラ	Cat. No.
Compact GuardLogix 5380 コントローラ	5069-L306ERMS2、5069-L306ERS2、5069-L310ERMS2、5069-L310ERS2、5069L320ERMS2、5069L320ERS2、5069-L320ERS2K、5069-L320ERMS2K、5069-L330ERMS2、5069-L330ERS2、5069L330ERS2K、5069-L330ERMS2K、5069-L340ERMS2、5069-L340ERS2、5069-L350ERMS2、5069-L350ERS2、5069L350ERS2K、5069-L350ERMS2K、5069-L380ERMS2、5069-L380ERS2、5069-L3100ERMS2、5069-L3100ERS2

重要　この装置は、屋内使用向けに「開放型」装置として出荷されています。特定の環境条件に適合し、帯電部への接触による人体への危険を防ぐように適切に設計されたエンクロージャ内に取付ける必要があります。

このエンクロージャは適切な難燃性を持ち、火炎の広がりを防ぐか最小限に抑えるもので、非金属製の場合は火炎伝播率が5VAであるか、用途に対して承認されたものである必要があります。また、何らかのツールを使用しなければエンクロージャの内部にアクセスできないような構造が必要です。

特定の製品安全認可に準拠するために必要な特定のエンクロージャ型式の定格については、『Compact GuardLogix 5380 SIL 2 Controllers Installation Instructions』(Pub.No. 5069-IN014)を参照してください。

認可されたGuardLogixコントローラと安全I/Oのシリーズおよびファームウェアバージョンの最新リストは、http://www.rockwellautomation.com/global/certification/safety.page の Safety Certificatesを参照してください。

ファームウェアリビジョンは、ロックウェル・オートメーションの製品互換性およびダウンロードセンター(PCDC)のサポートWebサイトからダウンロードできます。
http://www.rockwellautomation.com/global/support/pcdc.page

システムバスの拡張スロットには、電源の手順に従って、低電圧指令とEMC指令で認可されたCompact 5000 I/O拡張モジュールを取付けることができます。

コントローラとI/Oモジュールの認可を確認するには、以下のWebサイトを参照してください。
http://www.rockwellautomation.com/global/certification/overview.page

電源

機能安全アプリケーションでは、モジュール電力(MP)とセンサ/アクチュエータ(SA)電力の両方に安全特別低電圧/保護特別低電圧の電源が必要です。

電源を選択する際は、以下を考慮してください。

- Compact GuardLogix 5380コントローラのMP電力には、DC24VのSELV/PELV電源を使用する必要があります。
- ローカルのDC24V安全I/Oのすべてで SELV/PELV 電源を使用する必要があります。
- Compact GuardLogix 5380コントローラのSA電力コネクタを使用している場合は、DC24VのSELV/PELV電源が必要です。
- Compact GuardLogix 5380シャーシでローカルのAC120/240V I/Oを使用している場合、そのAC120/240V I/OのSA電力は、Cat. No. 5069-FPDのモジュールに接続している必要があります。
- SELV/PELV 電源を使用していない標準 I/O を使用する場合、そのI/O 電力は、Cat.No. 5069-FPDのモジュールに接続している必要があります。

重要　**CompactLogixまたはCompact GuardLogixコントローラがあるときの、5069 プラットフォームへの電源投入方法については、『CompactLogix 5380 および Compact GuardLogix 5380 コントローラ ユーザーズマニュアル』(Pub. No. 5069-UM001)を参照してください。**

ネットワーク通信

このセクションでは、ネットワーク通信の構成の例を示します。

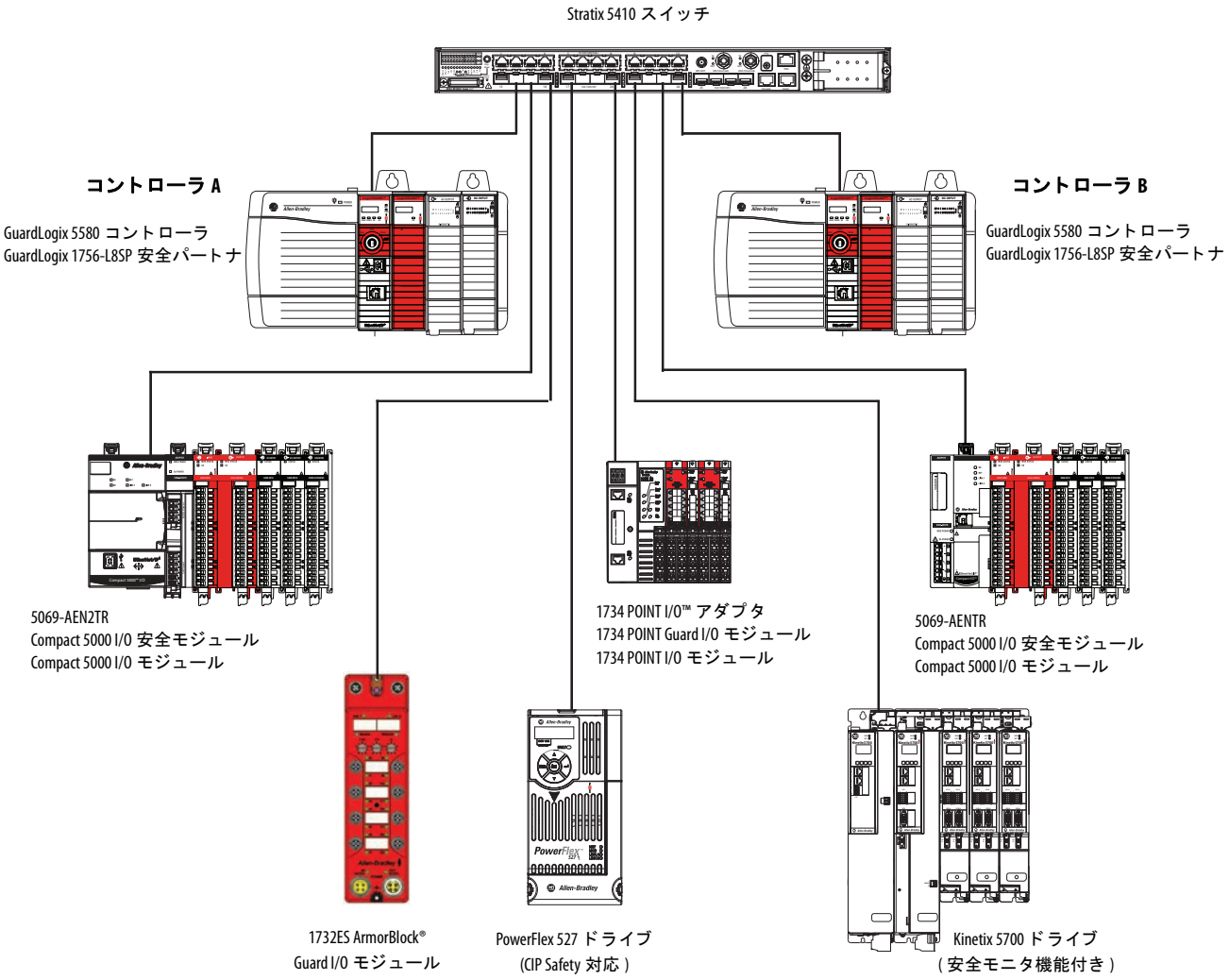
EtherNet/IPネットワーク

GuardLogix 5580 コントローラは、オンボード Ethernet ポートを介してEtherNet/IPネットワークに直接接続し、ネットワーク速度10/100/1000MBpsをサポートしています。別のEthernet通信モジュールは必要ありませんが、ローカルシャーシで使用することもできます。

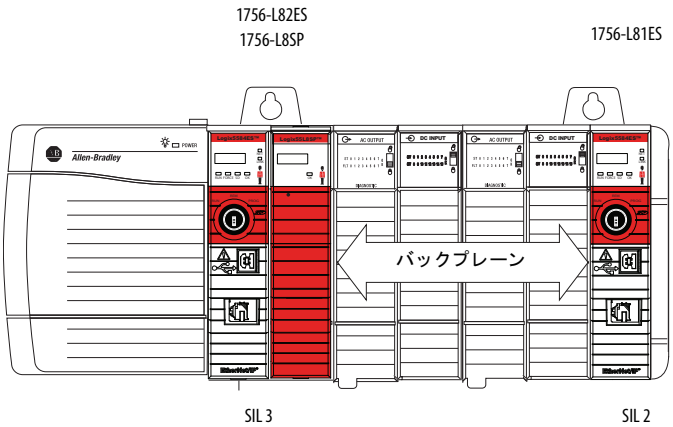
GuardLogix 5580システムで使用可能なその他の通信インターフェイスモジュールについては、当社または当社代理店にお問い合わせください。

GuardLogixコントローラ間のピア・ツー・ピアの安全通信は、EtherNet/IPネットワークを使用して行なうことができます。GuardLogixコントローラは、オンボード・イーサネット・ポートまたはEtherNet/IPブリッジを介して、EtherNet/IPネットワーク上の安全I/Oデバイスを制御したり安全データを交換したりすることができます。

図3 - EtherNet/IPネットワークを介したGuardLogix 5580ピア・ツー・ピア通信

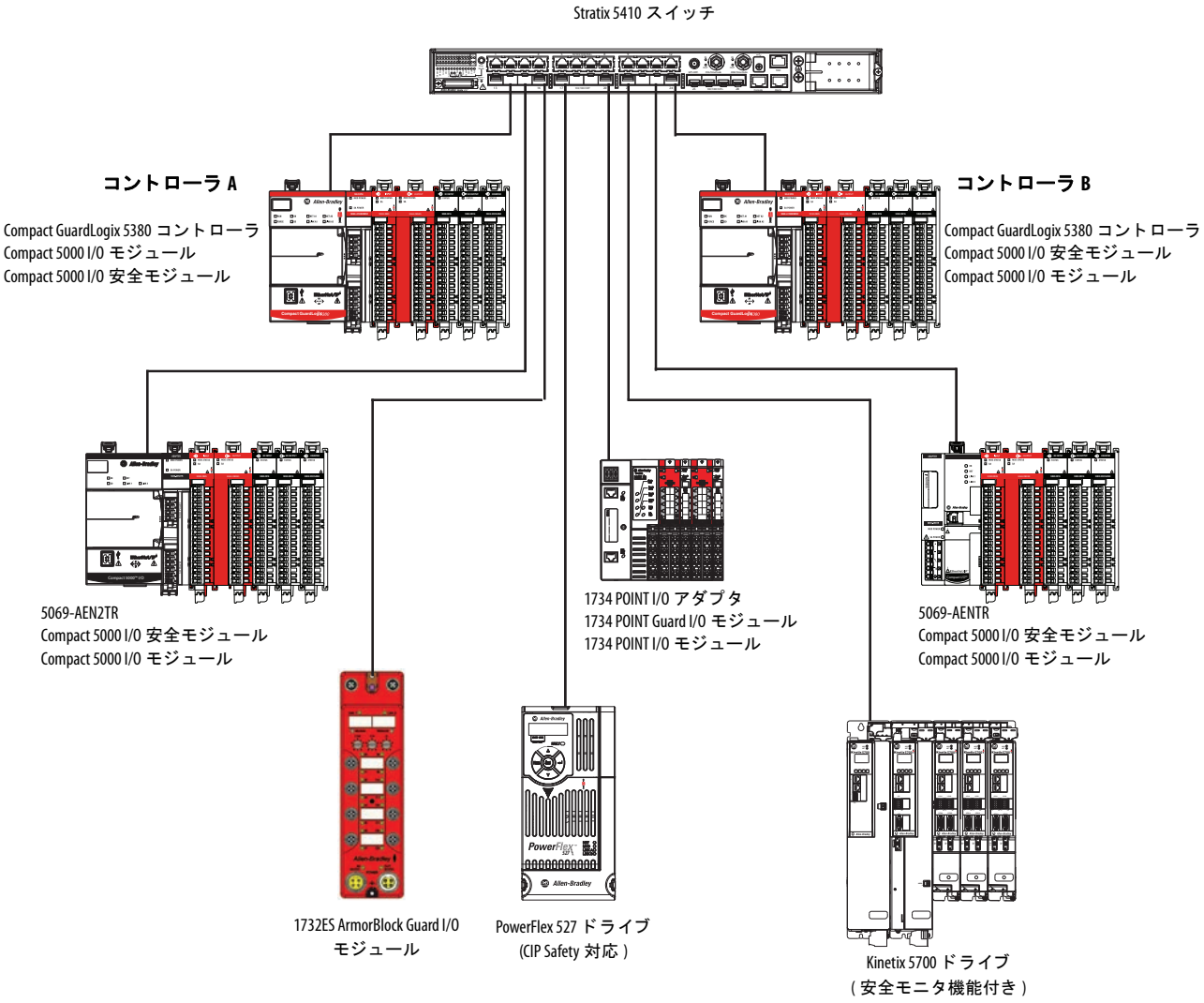


ヒント　同じシャーシ内の2つのGuardLogix 5580コントローラ間のピア・ツー・ピア安全通信は、バックプレーンを介しても確立できます。



Compact GuardLogix 5380コントローラは、オンボード・イーサネット・ポートを介してEtherNet/IPネットワークに直接接続します。また、ネットワーク速度10/100/1000 Mbpsもサポートしています。ローカルイーサネット通信モジュールは使用されません。

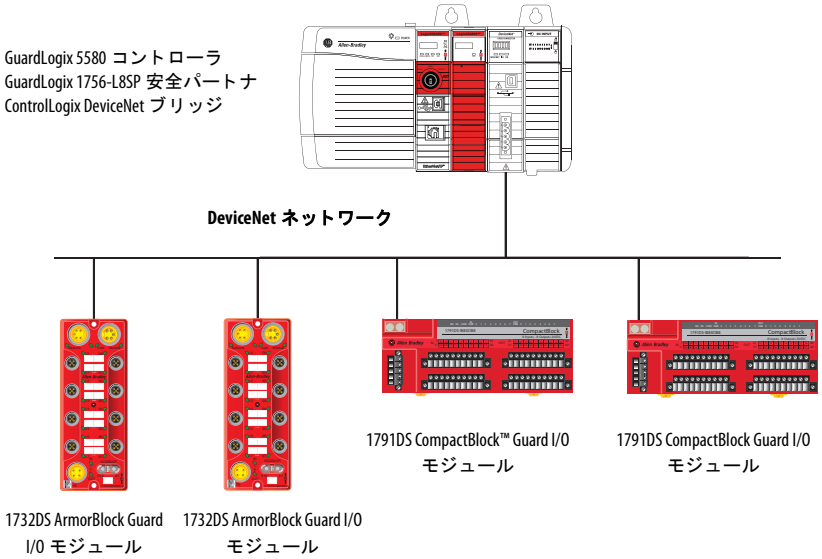
図4 - EtherNet/IPネットワークを介したCompact GuardLogix 5380ピア・ツー・ピア通信



DeviceNet Safety ネットワーク

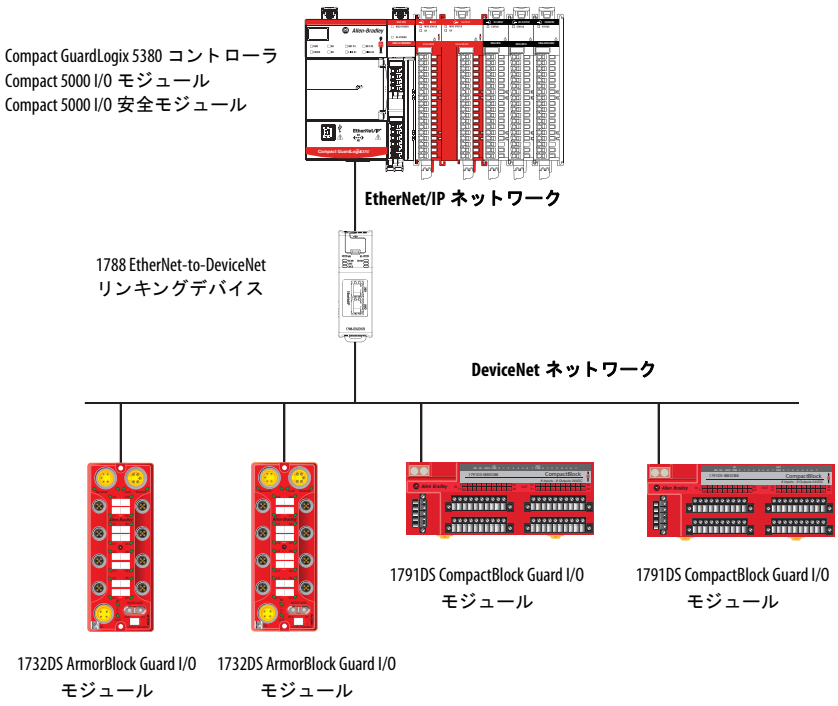
DeviceNetブリッジを使用すると、GuardLogixコントローラがDeviceNetネットワーク上の安全I/Oモジュールと安全データを制御および交換できます。

図5 - DeviceNetブリッジを介したGuardLogix 5580通信



Compact GuardLogix 5380 コントローラは、DeviceNet リンキングデバイスの1788-EN2DNR EtherNet/IPによってDeviceNetネットワーク上の安全デバイスと通信できます。

図6 - DeviceNetネットワークでのCompact GuardLogix 5380コントローラ



プログラミングの概要

GuardLogix セーフティコントローラをプログラムするには、Studio 5000 Logix Designer アプリケーションを使用します。

Studio 5000 Logix Designer アプリケーションを使用して、I/O デバイスおよびコントローラの位置、所有権、構成を定義し、プログラムロジックを作成、テスト、デバッグします。GuardLogix 安全タスクでは、ラダーロジックのみがサポートされます。

安全プロジェクトに使用可能なロジック命令セットについては、71 ページの付録 A を参照してください。

重要	**GuardLogix コントローラがランモードまたはプログラミングモードになっていて、アプリケーションプログラムがユーザによって検証されていない場合、ユーザが安全条件の保守の責任を負います。**

第3章

GuardLogix制御システム用の安全I/O

項目	参照ページ
安全 I/O デバイスの 標準的な安全機能	25
応答時間	26
安全 I/O デバイスの安全に関する注意事項	27

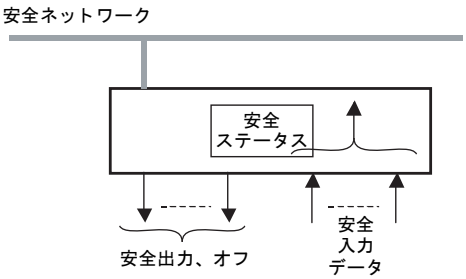
安全I/OデバイスでGuardLogix安全システムを使用する前に、それらの製品の製品マニュアルに記載された安全情報をすべて読み、理解し、遵守する必要があります。

安全I/Oデバイスは、センサやアクチュエータなどの安全入出力デバイスに接続できます。GuardLogixコントローラは、デバイスをモニタし、制御します。安全データについては、CIP Safetyプロトコルを使用した安全接続によってI/O通信が行なわれ、安全ロジックは、GuardLogixコントローラ内で処理されます。

安全I/Oデバイスの標準的な安全機能

以下は、安全I/Oデバイスの安全状態として扱われます。

- 安全出力：オフ
- コントローラへの安全入力データ：オフ



安全I/Oデバイスは、安全出力がオフになる安全状態でアプリケーションに使用してください。

診断

安全I/Oデバイスは、電源投入時、および動作中は定期的に自己診断を実行します。診断エラーが検出されると、(コントローラへの)安全入力データおよびローカルの安全出力が、安全状態(オフ)に設定されます。

ステータスデータ

安全I/Oデバイスは、安全入力および出力データのほかに、デバイスとI/O回路の状態をモニタするためにステータスデータをサポートしています。特定の製品の機能については、ご使用のデバイスの製品マニュアルを参照してください。

ステータスインジケータ

安全I/Oデバイスには、ステータスインジケータがあります。ステータスインジケータの動作については、該当のデバイスの製品マニュアルを参照してください。

オンディレイまたはオフディレイ機能

一部の安全I/Oデバイスには、入力信号のオンディレイとオフディレイ機能をサポートしているものがあります。一部のアプリケーションでは、システム応答時間の計算時にオフディレイまたはオンディレイ、あるいはそれらの両方を含む必要があります。

例えば、オン/オフディレイフィルタは、入力ロジックレベルに影響するノイズをフィルタアウトするために役立ちます。

システムの応答時間については、81ページの付録Cを参照してください。

応答時間

入力の応答時間は、信号が入力端子で変わってから、安全データがGuardLogixコントローラに送信されるまでの時間です。

出力の応答時間は、安全データがGuardLogixコントローラから受信されてから、出力端子の状態が変わるまでの時間です。

入力および出力の応答時間を決定する方法については、該当のCIP Safety I/Oデバイスの製品マニュアルを参照してください。

システムの応答時間の計算方法については、81ページの付録Cを参照してください。

安全I/0デバイスの安全に関する注意事項

安全ネットワークに取付ける前に、必要に応じてすべてのデバイスをノードアドレスまたはIPアドレスと、通信速度で作動する必要があります。

所有者

1つのGuardLogixシステム内では1つのGuardLogixコントローラが各安全I/Oデバイスを所有します。シャーシまたはネットワーク上で、複数のGuardLogixコントローラと安全I/Oデバイスを必要に応じて制限なしで使用できます。I/Oデバイスを所有するコントローラは、そのデバイスに対して定義した構成データを格納します。この構成は、システム内のデバイスの動作方法を制御します。

制御の観点からは、1つのコントローラが安全出力デバイスを制御します。さらに1つのコントローラが各安全入力デバイスを所有します。安全入力データは複数のGuardLogixコントローラで共有(消費)できます。

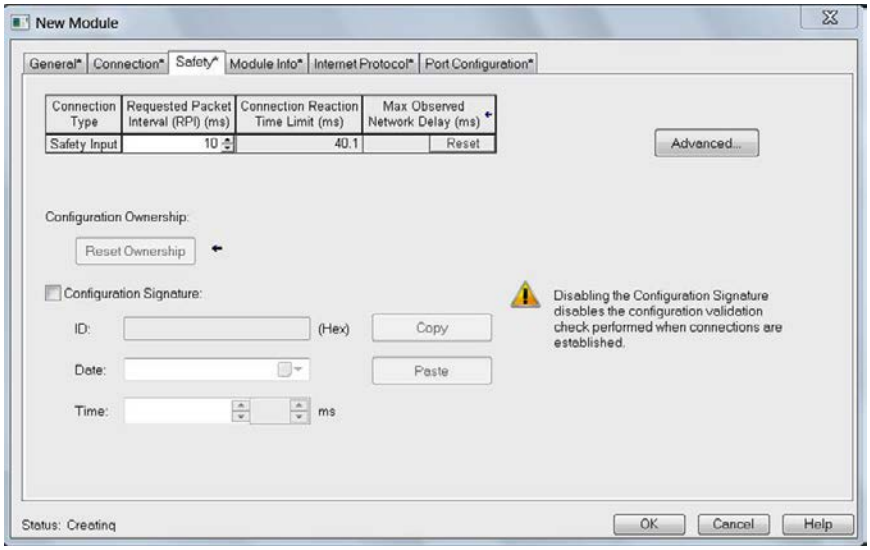
安全I/0の構成署名

重要　**安全I/0構成署名は、個々の安全モジュールに適用されます。これは、コントローラの安全部分のすべてに適用されるコントローラ安全署名と異なります。**

構成署名は、安全I/Oデバイスの構成から計算されます。構成署名は、安全アプリケーションによってデバイスが予想どおりに構成されていることを確認するために使用します。GuardLogixコントローラを使用しているときは、この署名をモニタする必要はありません。GuardLogixコントローラは、自動的に署名をモニタします。構成署名が予期せずに変更された場合、コントローラとI/Oモジュール間の安全接続は中断されるため、I/Oモジュールは安全状態に入ります。

サードパーティモジュールを使用し、構成署名なしで安全I/Oに接続する場合、その安全I/Oデバイスに有効な構成があることを確認する必要があります。

重要　ロックウェル・オートメーション安全I/Oモジュールは、通常、デフォルトで構成署名を使用し、システムは構成署名なしでは実行できません。



安全I/Oデバイスの交換

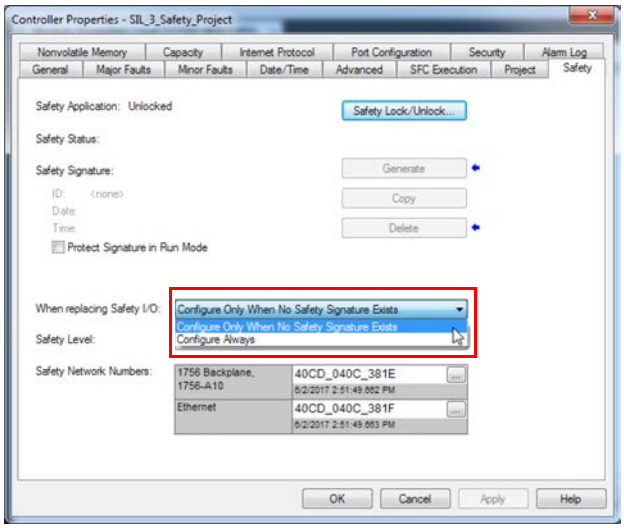
安全デバイスの交換には、交換用のデバイスが適切に構成され、その動作が確認される必要があります。

注意：デバイスの交換または機能テスト中のシステムの安全は、影響されるデバイスのいかなる部分にも依存してはなりません。

Studio 5000 Logix Designerアプリケーションの Controller Propertiesダイアログボックスにある Safety タブでは、I/Oデバイス交換に関する2つのオプションを使用できます。

- Configure Only When No Safety Signature Exists (安全署名が存在しないときのみ構成)
- Configure Always (常に構成)

図7 - 安全I/Oの交換オプション



Configure Only When No Safety Signature Exists

この設定では、安全タスクに安全署名がなく、交換用のデバイスが初期状態で安全ネットワーク番号がない場合に、安全デバイスを構成することを指定します。

コントローラに安全署名がある場合は、以下の条件のすべてが真であれば、GuardLogixコントローラで交換用の安全I/Oデバイスが自動的に構成されます。

- デバイスに適切な安全ネットワーク番号が設定されています。
- デバイスの電子キーイングが適切です。
- ノードまたはIPアドレスが適切です。

コントローラの安全署名がある場合に適切な安全ネットワーク番号(SNN)を設定するには、適切なSNNをダウンロードするために手動の操作が必要になります。Studio 5000 Logix Designerアプリケーションで GuardLogixまたはCompactGuardLogix コントローラにオンラインアクセスし、Module Propertiesダイアログ、Generalタブを開き、Safety Network Numberの横の"..."ボタンをクリックします。Setボタンを使用して、モジュールに手動でSNNを書込みます。この手動の操作を終了すると、残りの構成は自動的にダウンロードされます。

詳細は、コントローラの以下のユーザーズマニュアルで安全I/Oデバイスの交換手順を参照してください。

- ControlLogix 5580 and GuardLogix 5580 Controllers User Manual (Pub. No. 1756-UM543)
- CompactLogix 5380 および Compact GuardLogix 5380 コントローラユーザーズマニュアル (Pub. No. 5069-UM001)

Configure Always

交換用の安全I/Oデバイスが初期状態の場合、GuardLogixコントローラでは、そのデバイスの構成が試みられます。(安全ネットワーク番号が交換用安全デバイスに存在せず、ノード番号とI/Oデバイスのキーイングがコントローラの構成と一致する場合。)

注意：デバイスの交換と機能テスト中に、ルーティング可能な安全制御システム全体が SIL 2 または SIL 3 の動作の保持に依存していないときのみ、Configure Always 機能を有効にしてください。32 ページの「ルーティング可能な CIP Safety システム」を参照してください。

安全制御システムの一部にSIL 2またはSILの維持がかかっている場合は、コントローラのConfigure Always機能が無効になっていることを確認してください。

デバイスの交換時に正しい安全機能が保持されるようにするためのプロセスの実装は、ユーザの責任で行なってください。

注意：Configure Always 機能が有効な場合に初期状態のデバイスを安全ネットワークに配置するには、ユーザーズマニュアルのデバイス交換手順に従ってください。

- ControlLogix 5580 and GuardLogix 5580 Controllers User Manual (Pub. No. 1756-UM543)
- CompactLogix 5380 および Compact GuardLogix 5380 コントローラ ユーザーズマニュアル (Pub. No. 5069-UM001)

第4章

CIP Safetyおよび安全ネットワーク番号

項目	参照ページ
固有のノード参照	31
安全ネットワーク番号 (SNN)	31
ルーティング可能な CIP Safety システム	32
SNN の割付けに関する注意事項	32
安全デバイスへの SNN の割付方法	34
SNN フォーマット	35
初期状態のデバイスの SNN	37

固有のノード参照

CIP Safety制御システムは、通信ネットワークによって相互に接続されたCIP Safetyデバイスで構成されます。これらのネットワークは、SIL 2またはSIL 3認可を受けていないデバイス(スイッチ、ブリッジ、アダプタなど)で構成される場合があります。そのため、CIP Safetyデバイスは本質的にネットワーク送信エラーからの保護を必要とします。

CIP Safetyプロトコルは、エンドノードからエンドノードへの安全プロトコルです。この構成を使用すると、認可されていないブリッジ、スイッチ、ルータを介してCIP Safetyデバイス間でCIP Safetyメッセージをルーティングできます。

CIP Safetyプロトコルの主要な要素は、固有のノード参照(固有ノードIDまたはUNIDとも呼ばれる)の概念です。各CIP Safetyデバイスでは、各CIP Safety対応ポートにUNID値が割付けられている必要があります。

重要 相互に通信できるすべてのデバイスの範囲内で、すべてのUNIDが一意であることを確認することはユーザの責任です。

安全ネットワーク番号(SNN)

制御システムとの通信は、ブリッジコンポーネントまたはルーティングコンポーネントと相互接続されているサブネットを介して行われれます。サブネットの例:

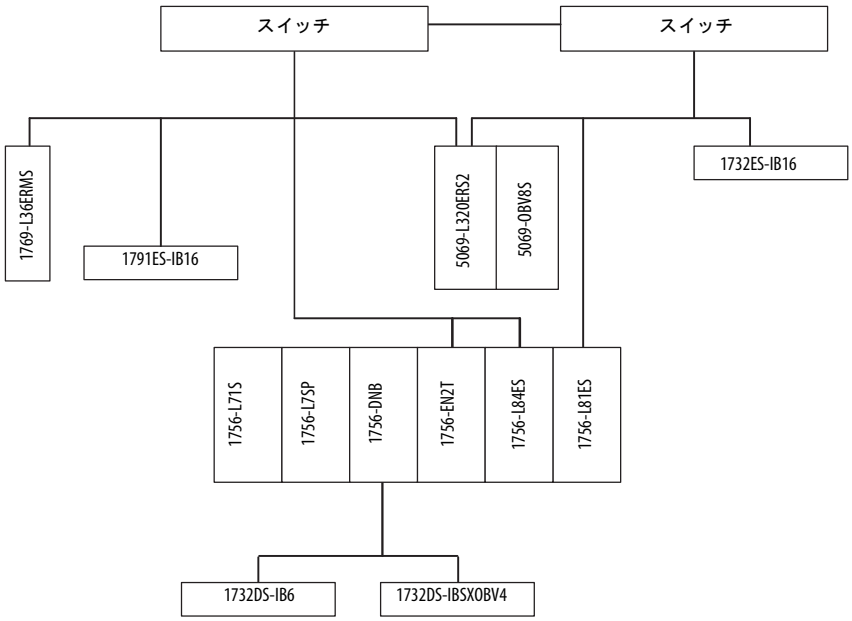
- シャーシのバックプレーン
- I/Oモジュールバンク
- LAN内のEthernetサブネット

各CIP SafetyデバイスのUNIDを直接作成する(大型のシステムではエラーを起こしやすい)代わりに、固有の安全ネットワーク番号(SNN)画'各サブネットに割付けられ、SNN + ノードアドレスからUNIDが作成されます。

ルーティング可能な CIP Safety システム

図8に示したシステムの例は、大型のプラント全体のイーサネットバックボーンを通して別のCIP Safetyシステムと相互接続されていません。そのため、図8は、ルーティング可能なCIP Safetyシステムの範囲を示しています。

図8 - 安全システムの例



この例の説明:

- バックプレーンポートでは、SNN　がバックプレーンに割付けられており、ノードアドレスはデバイスのスロット番号です。
- Ethernet ポートでは、SNN が EtherNet/IP ネットワークに割付けられており、ノードアドレスはデバイスの IP アドレスです。
- 5069-L320ERS2は、デュアルIPモードであり、2つの別々のEtherNet/IPネットワークに接続されています。両ネットワーク間でのパケットの間違ったルーティングを防ぐため、それらのネットワークはSNN 値を共有してはなりません。

SNNの割付けに関する注意事項

コントローラプロジェクトの作成時、Studio 5000 Logix Designerアプリケーションでは、CIP Safetyデバイスを含む新しいサブネットが見つかるたびに、自動的にSNN値が生成されます。

- コントローラ上の各CIP Safety対応ポートにSNNが割付けられます。
- ブリッジデバイスまたはアダプタデバイスが　I/O　ツリー内にある場合、子CIP Safetyデバイスを追加すると、そのブリッジまたはアダプタによって作成されたサブネットにSNN が割付けられます。

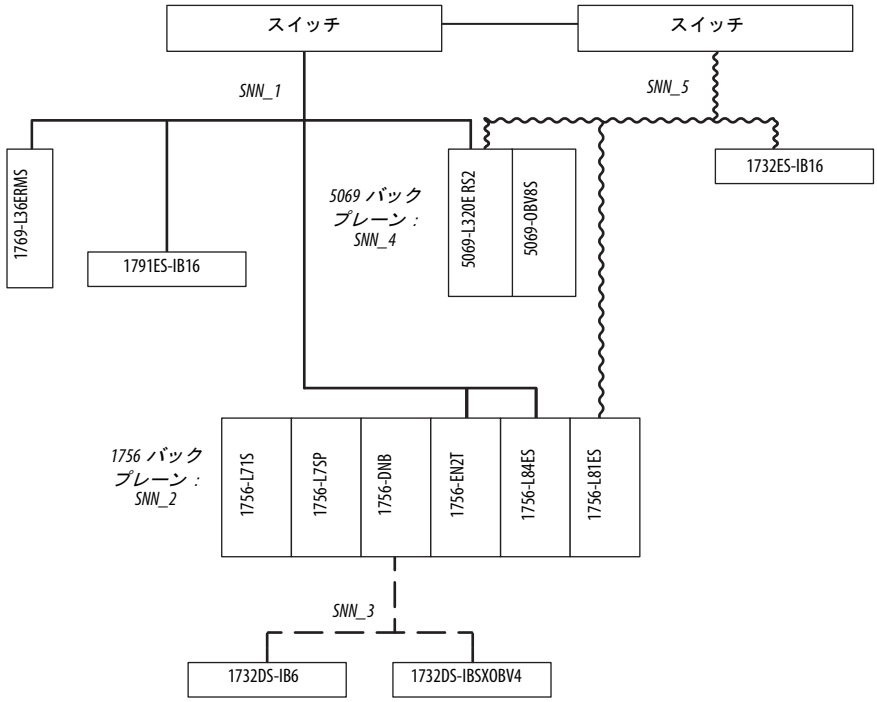
CIP Safetyシステム全体が1つのコントローラプロジェクトで構成される場合、自動的に生成されたこれらのSNN値で十分です。

同じ安全I/Oと対話したり同じ安全I/Oにアクセスする必要のある複数のコントローラがある場合、CIP Safetyシステム設計者は、別々のプロジェクトファイル間でSNN 値を調整する必要があります。Studio 5000 Logix Designerアプリケーションは、この調整を可能にするために、SNN割付けへのコピー/貼り付けアクセスを提供します。

また、ルーティング可能なシステム全体(全プラントのシステム)を綿密に計画することを選択し、各サブネットにSNNを手動で割付けることもできます。Studio 5000 Logix Designerアプリケーションでは、この設計方法を可能にするために、手動入力によってSNN値を割付けることができます。

図9は、SNNをサブネットに割付ける例を示しています。

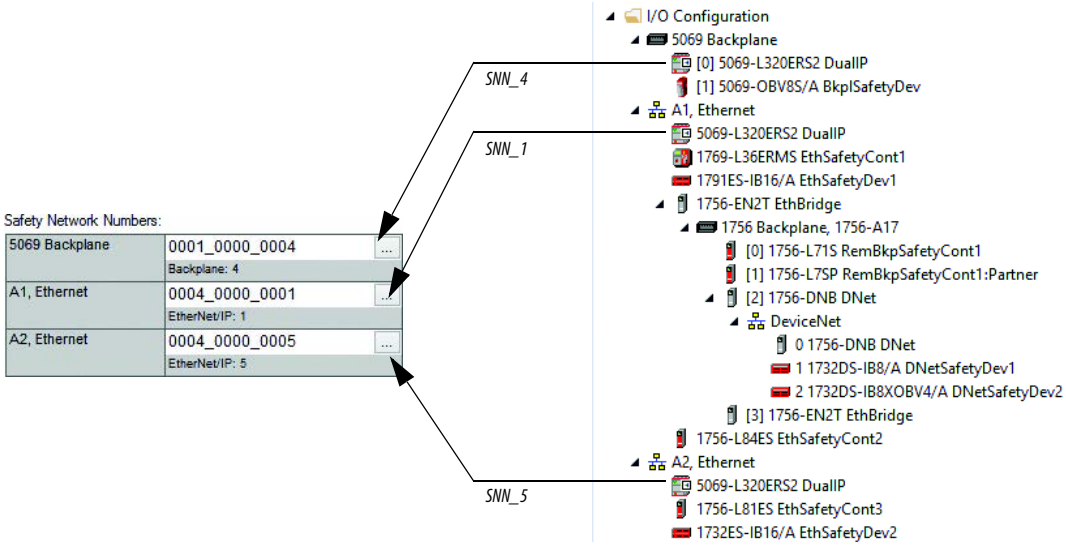
図9 - SNN割付けの例



サブネット	タイプ	ライン	SNN 割付け
SNN_1	EtherNet/IP	———	1769-L36ERMSイーサネットポート、1791ES-IB16、5069-L320ERS2イーサネットポートA1 (図10はこのポートへのSNN 0004_0000_0001の割付けを示す)、1756-EN2T、および1756-L84ESイーサネットポート
SNN_2	バックプレーン	なし	1756-L71S、1756-L84ESバックプレーンポート、および1756-L81ESバックプレーンポート
SNN_3	DeviceNet	– —— –	1732DS-IB6、1732DS-IBSX OBV4
SNN_4	バックプレーン	なし	5069-L320ERS2バックプレーン(図10はこのポートへのSNN 0001_0000_0004の割付けを示す)、および5069-OBV8S
SNN_5	EtherNet/IP	～～～	5069-L320ERS2 Ethernetポート A2 (図10はこのポートへのSNN 0004_0000_0005の割付けを示す)、1732ES-IB16、および1756-L81ESイーサネットポート

34ページの図10は、前述の例のCompact GuardLogix 5380 (Cat. No. 5069-L320ERS2)コントローラオーガナイザI/Oツリーとの関連を示しています。

図10 - コントローラオーガナザ



I/Oツリー内の各CIP Safetyデバイスの構成プロファイルには、デバイスへのCIP Safetyコネクションの確立時にコントローラで使用するSNN値のパラメータが含まれます。このパラメータでは、プロジェクトで認識されているSNNにょって既に確立されているSNN値が自動的に採用されます。

- GuardLogix コントローラ直属の子である安全デバイス (セーフティコントローラを含む) では、安全モジュールへの接続に使用されるポートのコントローラと一致するSNN が採用されます。
  - バックプレーンポートの直下にある安全デバイスでは、GuardLogix コントローラのバックプレーンポートの SNN が採用されます。
  - Ethernet ポートの直下にある安全デバイスでは、GuardLogix コントローラの Ethernet ポートが SNN を採用されます。
- リモートサブネット上の安全デバイス(セーフティコントローラを含む)では、そのサブネットに既に割付けられているSNN値が採用されるか、そのサブネット上の最初のCIP Safetyデバイスに対して新しいSNN が生成されます。

各コントローラSNNを、サブネットで既に確立しているSNNに割付けることをお奨めします。これにより、Studio 5000 Logix Designer アプリケーションは、プロジェクトに追加された各安全I/Oモジュールおよびセーフティコントローラに正しいSNNを割付けることができます。

安全デバイスへのSNNの割付方法

ほとんどのCIP Safety I/Oモジュール(工場出荷時の状態)は、そのモジュールを所有するコントローラによって割付けられたSNNを受け入れます。Studio 5000 Logix Designerアプリケーションでそのモジュールの接続に対して自動的に採用されるSNN値は、コントローラが最初にモジュールに接続する際に受け入れられます。

重要　CIP Safety I/Oモジュールは、割付けたUNID (SNN + ノード)を維持するため、別の値を使ってモジュールを再使用する前には、リセットが必要になります。

I/Oツリー内の別のセーフティコントローラのように、一部のデバイスは、プログラミングワークステーションからSNN構成を受け取ります。それらのデバイスでは、Studio 5000 Logix Designer アプリケーションで正しい

SNNが自動的に割付けられなかった場合、デバイスにプログラムによって組み込まれたものと同じSNNを使用するように、手動で接続を構成する必要があります。

SNNフォーマット

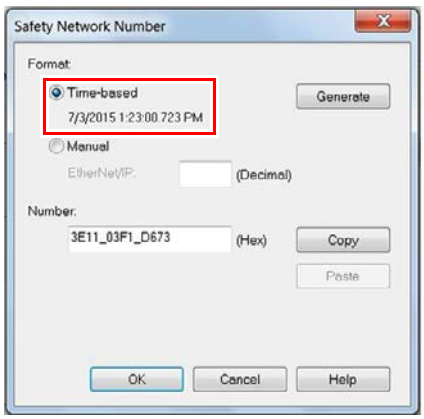
システムで使用するSNNは、6バイトの16進数です。SNNは、タイムベースまたは手動の2つの形式で設定および表示できます。

- タイムベース
- 手動

タイムベースのSSNNフォーマットと割付け

タイムベースのフォーマットを選択すると、SNNは現地の日付と時刻を示します。

図11 - SNNフォーマット



GuardLogixセーフティコントローラプロジェクトを作成する場合、またはIPモード(Compact GuardLogix 5380のみ)またはコントローラのタイプを変更してEtherNet/IPを追加する場合、タイムベースのSNNの割付けは、自動的に行われます。ソフトウェアによって生成されるタイムベースのSNNは、プロジェクト作成によって生成された場合もIPモードの変更によって生成された場合も、そのプロジェクト内で一意です。コントローラボートの下に直接作成されたデバイスは、デフォルトで、コントローラ上のそのポートと同じSNNを持ちます。

重要	アプリケーションのネットワークダイアグラム(図9など)がある場合、コントローラのSNNを編集して、それがネットワークダイアグラムと一致するようにする必要があります。コントローラオーガナイザでI/O構成にデバイスを追加する前にSNNを編集することをお奨めします。

アダプタ(コントローラ自体ではなく)の下のポートに追加された新しい CIP Safety I/Oデバイスも同様なルールに従います。

- ボートの下に　SNN　を使用するデバイスが他にない場合は、タイムベースのSNNが自動的に割付けられます。
- その他の場合は、アドレス順序で　SNN　を持つ最初のデバイスと同じSNNがデバイスに割付けられます。

手動のSNNフォーマットと割付け

手動フォーマットを選択すると、SNNはネットワークタイプを表し、1～9999の10進数値である必要があります。

図12 - SNNフォーマット

SNNの手動操作は、以下の状況で必要です。

- すべてのプロジェクトで、同じサブネット上の各セーフティコントローラボートに同じSNNがあることを確認する場合。
- 安全プロジェクトをコピーする場合。

注意：安全プロジェクトが別のハードウェアまたは別の物理的な場所で使用する別のプロジェクトにコピーされて、新しいプロジェクトが同じルーティング可能な安全システム内にある場合、各 SNN は 2 番目のシステムで変更する必要があります。SNN 値を反復することはできません。

SNN の変更方法については、以下のユーザーズマニュアルを参照してください。

- ControlLogix 5580 and GuardLogix 5580 Controllers User Manual (Pub. No. 1756-UM543)
- CompactLogix 5380 および Compact GuardLogix 5380 コントローラ ユーザーズマニュアル (Pub. No. 5069-UM001)

重要　SNNを手動で割付けるときは、システムを拡張する際にSNNと固有のノード参照の組合せが重複していないことを確認してください。

プロジェクトに重複するSNNと固有のノード参照の組合せが含まれる場合は、警告が表示されます。プロジェクトを確認することはできますが、重複する組合せは解決することをお奨めします。

ただし、同じSNNとノードアドレスを持ち、プロジェクトには含まれない安全デバイスが、ルーティング可能な安全ネットワーク上にある場合があります。その場合、それらのデバイスはStudio 5000 Logix Designerアプリケーションでは認識されないため、警告が表示されないことがあります。

重複する固有ノード参照がある場合、システムユーザーは、危険な状態にならないことを証明する必要があります。

初期状態のデバイスのSNN

初期状態のCIP Safety I/OデバイスにはSNNはありません。SNNは、デバイスを所有するGuardLogixコントローラによって構成がデバイスに送信されると設定されます。

重要　構成されたGuardLogixシステム(SNNはGuardLogixコントローラにある)にCIP Safety I/Oデバイスを追加するには、CIP Safetyネットワークに追加する前に、交換用CIP Safety I/Oデバイスに正しいSNNを割付けてください。

詳細は、コントローラの以下のユーザーズマニュアルで安全I/Oデバイスの交換手順を参照してください。

- ControlLogix 5580 and GuardLogix 5580 Controllers User Manual (Pub. No. 1756-UM543)
- CompactLogix 5380 および Compact GuardLogix 5380 コントローラユーザーズマニュアル (Pub. No. 5069-UM001)

Notes:

第5章

安全タグ、安全タスク、安全プログラムの特性

項目	参照ページ
標準と安全の違い	39
安全タスク	40
SIL 2 および SIL 3 安全アプリケーションの違い	42
ヒューマン・マシン・インターフェイスの使用	44
安全プログラム	46
安全ルーチン	46
安全タグ	47

標準と安全の違い

これはLogixコントローラであるため、標準(非安全関連)と安全関連の両方のコンポーネントをGuardLogix制御システムで使用できます。

標準オートメーション制御は、GuardLogixプロジェクト内の標準タスクから実行できます。GuardLogix 5580コントローラとCompact GuardLogix 5380コントローラは、他のコントローラと同じ機能を備えています。標準コントローラとの差は、これらのコントローラではSIL 2またはSIL 3対応の安全タスクも提供されていることです。

ただし、アプリケーションの標準関連部分と安全関連部分の間には、論理的および視覚的な区別が必要です。Studio 5000 Logix Designerアプリケーションでは、安全タスク、安全プログラム、安全ルーチン、安全タグ、および安全I/Oデバイスを使用して区別します。

- GuardLogix 5580コントローラでは、安全タスクによってSIL 2とSIL 3の両方の水準の安全制御がサポートされます。11ページの「SIL認可」を参照してください。
- Compact GuardLogix 5380コントローラでは、安全タスクによってSIL 2の水準の安全制御がサポートされます。11ページの「SIL認可」を参照してください。

安全タスク

重要　安全タスクで使用できるのは、71ページの付録Aにリストされた命令のみです。

GuardLogixプロジェクトを作成すると、1つの安全タスクが自動的に作成されます。安全タスクには以下の追加特性があります。

- GuardLogixコントローラは、安全タスクをサポートする唯一のコントローラです。
- 安全タスクは削除できません。
- GuardLogixコントローラは1つの安全タスクをサポートします。
- 安全タスクでは、複数の安全ルーチンで構成された複数の安全プログラムを使用できます。
- 安全タスク内から標準ルーチンを実行することはできません。

安全タスクは周期的タスクであり、ユーザがその期間と優先順を構成する必要があります。安全タスクは、標準タスクと同じルール(どのユーザタスクよりも優先されるモーションタスクによる中断を含む)に従って、中断することができます。

優先順位の高い(小さい数値)安全タスクを構成することで、実行時の変動を低減できます。それにより、安全タスクウォッチドッグを低く設定することができるため、安全システムの応答時間が短縮されます。

重要　マップされた安全タグが多数ある場合や、安全プロデューサ/コンシュマタグのデータが多量の場合、コントローラの安全タスクのスキャン時に変動が発生する場合があります。

安全タスクの制限

安全タスク時間と安全タスクウォッチドッグの両方を指定します。安全タスク時間は、安全タスクの連続した実行の間隔です。安全タスクウォッチドッグは安全タスクのスケジュール実行の開始から完了までにかかる最大時間です。

安全タスクウォッチドッグについては、81ページの付録Cを参照してください。

安全タスク期間は最大500msecに制限され、オンラインでは修正できません。再度トリガされる前に完了するだけの十分な時間が安全タスクにあることを確認してください。ウォッチドッグの期限が切れる前に安全タスクが完了しない場合、GuardLogixコントローラで回復不能な安全フォルトである安全タクス・ウォッチドッグ・タイムアウトが発生します。

詳細は、65ページの第7章を参照してください。

安全タスク実行の詳細

安全タスクは、以下の点を除いて標準周期的タスクと同じように実行します。

- 安全入力タグと安全コンシューマタグは、安全タスクの実行開始時にのみ更新されます。このプロセスは、I/O RPIは安全タスク時間よりも短くても、安全入力タグのデータが更新されるのは、安全タスクの実行の開始時のみであることを意味します。安全タスクの開始後に到着する安全入力およびコンシューマパケットは、安全タスクが時間実行されるまでバッファに格納されます。
- 時間は安全タスクの実行開始時に凍結されます。　その結果として、安全タスクの実行中には、TONやTOFなどのタイマ関連命令は更新されません。これらの値は、1つのタスク実行から別のタスク実行までの正確な時間を保持しますが、安全タスクの実行中に累積時間は変わりません。

注意：この動作は、標準の Logix タクス実行と異なります。

- 安全タグにマップされた標準タグの場合、安全タスクの開始時に標準タグ値が安全タグにコピーされます。
  - 標準タグは、引き続き自由に変更できます。

重要	**マップしたタグを追加すると、スキャン時間が長引くことがあります。**

  - ユーザコードは、安全タスク内で安全タグを変更できますが、標準タグにはその変更は反映されません。
- 安全出力タグ値は、ユーザの安全アプリケーションコードによって安全タスクスキャン中に変更できます。最終値は安全タスクスキャンの終了時に安全モジュールに送信されます。同様に、安全タスクによって生成された値は、安全タスクスキャンの終了時にコンシューマセーフティコントローラに送信されます。

重要	安全ロック解除状態で安全署名がないときは、コントローラは安全タスクと通信コマンドから安全メモリへの同時書込みアクセスを禁止します。その結果、通信が更新を完了するまで安全タスクをオフのまま保持できます。更新に必要な時間は、タグサイズによって異なります。したがって、安全コネクションタイムアウトおよび安全ウォッチドッグタイムアウトが発生することがあります(例えば、安全タスクレートが1msecに設定されている場合にオンライン編集を行なうと、安全ウォッチドッグタイムアウトが発生することがあります)。 通信の更新のための延期時間を補正するために、安全ウォッチドッグ時間を延長する必要があります。 編集によっては、安全タスクが動作を完了するために十分な時間がない場合があり、ウォッチドッグタイムアウトが発生します。 コントローラが安全ロックされているか、または安全署名が存在するときには、この注意で説明した状況は発生しません。

SIL 2およびSIL 3安全アプリケーションの違い

リスクアセスメントは、安全機能にSIL 2またはSIL 3のどちらが必要かを判定します。例えば、複数の安全機能を備えた機械があるとします。その機械の最大リスクにSIL 2しか必要でない場合、SIL 2対応のコントローラを使用できます。また、別のマシンは複数の安全機能を備えていますが、少なくとも1つのリスクでSIL 3が必要です。その場合、SIL 3対応のコントローラが必要になります。

このマニュアルで説明したように、SIL 2の GuardLogix 5580コントローラにはプライマリコントローラのみが必要で、SIL 3 GuardLogix 5580コントローラにはプライマリコントローラと安全パートナの両方が必要です。

重要	SIL 2アプリケーションにおいて55°C (131°F) 以上で使用する場合、コントローラの隣にあるスロットに6.2W以上のモジュールを取付けないでください。

SIL 2ソリューションかSIL 3ソリューションのどちらを使用しているかにかかわらず、どちらの安全度水準にも安全署名が必要です。詳細は、54 ページの「安全署名の生成」を参照してください。

重要	安全タスクには、多数の安全機能が含まれる場合があります。特定の機能がSIL 3であるためには、デバイスのチェーン全体と、センサからアクチュエータへのプログラミングもSIL 3である必要があります。SIL 3を必要とする安全機能にSIL 2の入力信号を使用しないように注意してください。

高速I/Oモジュール

安全度水準間の違いは、SIL 2にはシングルチャネルI/Oデバイスで対応できますが、通常SIL 3にはデュアルチャネルI/Oデバイスが必要です。

安全アーキテクチャの観点からは、シングルチャネルを使用することは、ハードウェア・フォルト・トレランス(HFT)がゼロであることを意味します。HFTがゼロの場合、プロセス安全時間内にフォルトを検出して、安全機能を安全状態にする必要があるというガイドラインがあります。診断テストレートが要求レートの100倍の場合、例外が適用されます。安全I/Oモジュールをシングルチャネルの SIL 2アプリケーションで使用する場合は、以下を考慮する必要があります。

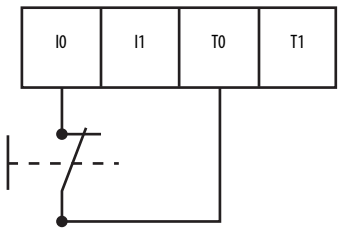
- 入力チャネルまたは出力チャネルで安全パルステストを構成する必要があります。
- プロセス安全時間が600 msec（通常の安全I/Oパルステスト間隔)よりも大きいか、要求レートが1秒当たり1要求より小さい(例えば1時間に1つ)必要があります。

CompactBlock Guard I/O (1791シリーズ)、ArmorBlock Guard I/O (1732シリーズ)、POINT Guard I/O (1734シリーズ)、およびCompact 5000 I/O Safety (5069シリーズ)の安全入力モジュールは、シングルチャネルSIL 2 (前述の注意事項を参照)およびデュアルチャネルSIL 3の安全入力回路をサポートしています。これらのモジュールは、SIL 2およびSIL 3動作の定格を持っているため、同じモジュール上にSIL 2回路とSIL 3回路の両方を混在させることができます。

図13は、SIL 2安全回路をGuard I/O安全入力モジュールに配線する方法を示しています。

重要　テストソースは、パルステスト用に構成する必要があります。

図13 - 入力配線の例



2つのSIL 2安全回路がある場合、2番目の安全回路は図14のように追加することができます。

図14 - ペアの入力配線例

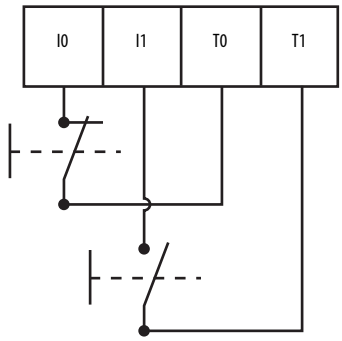
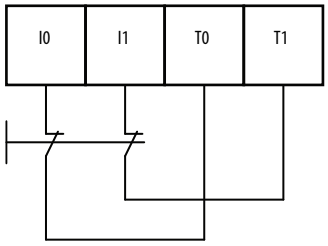


図15に、標準的なSIL 3配線図を示します。

図15 - SIL 3配線



重要	これらの配線図は、配線構成の例です。I/Oデバイスとシステム構成により、他の配線構成も使用できます。

重要	通常、オンボード・パルス・テストの出力(T0～Tx)は、機械的な接点のあるフィールドデバイスで使用されます。電子出力のある(安全入力に給電する)安全デバイスを使用する場合、このデバイスには適切な安全定格が必要です。

ヒューマン・マシン・インターフェイスの使用

HMIデバイスをSIL認可のGuardLogixシステムで使用する場合、以下の注意事項やガイドラインに従ってください。

注意事項

HMIデバイスに関する注意事項に従い、特定の技術を使用する必要があります。以下に注意事項を示しますが、これに限定されるわけではありません。

- アクセス制限および安全保護
- 仕様、テスト、検証
- データとアクセスの制限
- データとパラメータの制限

HMIデバイスを標準的なSILループに適合させる方法については、13ページの「GuardLogix アーキテクチャ」を参照してください。

HMIとコントローラ内のアプリケーションソフトウェアには安全な技術を使用してください。

安全関連のシステムへのアクセス

HMI関連機能は、データの読取りと書込みという2つの主要なアクティビティで構成されます。

安全関連システムのパラメータの読取り

読取りは安全システムの動作に影響を及ぼさないため、データの読取りには制限はありません。ただし、読取りの回数、頻度、データのサイズによっては、コントローラの性能に影響を及ぼすことがあります。安全関連の誤ったトリップを防止するために、適切な通信手段を使用してコントローラの通信プロセスへの影響を抑えるようにしてください。読取り速度を最高速度に設定しないでください。

SIL 定格システムのパラメータの変更

外部(安全ループの外側にある)デバイス(HMIなど)によって安全関連ループのパラメータを変更する場合は、以下のような制限があります。

- 認可され特別な訓練を受けた人（オペレータ）のみが、HMI を使用して安全関連システムのパラメータを変更できます。
- HMI を使用して安全関連システムを変更するオペレータは、その変更が安全ループに与える影響に対して責任を負います。
- 変更する変数を明確に文書化する必要があります。
- HMI を使用して安全関連の変更を行なうには、わかりやすく明確なオペレータ手順を使用する必要があります。
- 安全関連システムで変更が受入れられるのは、以下の一連のイベントが発生する場合に限定されます。
  a. 新しいパラメータ値は、異なる 2 つのタグに 2 回送信する必要があります。つまり、1 つのコマンドで両方の値を書込んではなりません。
  b. HMI からパラメータを受け取る 2 つの標準タグは、2 つの安全タグにマップされる必要があります。
  c. コントローラで実行する安全関連コードでは、両方の安全タグが同値であり、かつ範囲内にあることを確認する必要があります(境界チェック)。
  d. 新しい変数はどちらも、HMI デバイスに読返されて表示される必要があります (HMI 画面は、標準タグからマップされたタグ値を受け取る安全タグを読取る必要があります)。
  e. 訓練を受けたオペレータが、両方の変数が同値であり、かつ値が適切であることを視覚的に確認する必要があります。
  f. 訓練を受けたオペレータが、安全ロジックにコマンドを送信するHMI画面で値が適切であることを手動で確認する必要があります。これにより、新しい値を安全機能で使用できるようになります。

いずれの場合も、変更を受入れて安全ループに適用する前に、オペレータが変更の妥当性を確認する必要があります。

- 安全評価手順の一環として、すべての変更をテストします。
- 以下を含めて、HMI　から行なわれたすべての安全関連の変更を適切に文書化します。
  - 認証
  - 影響の分析
  - 実行
  - テスト情報
  - リビジョン情報
- 安全関連システムへのプロセス安全の変更は、IEC 61511 の要件に従う必要があります。
- 安全関連システムへの機械安全の変更は、IEC 62061 の要件に従う必要があります。
- 開発者は、その他のアプリケーションソフトウェア開発において安全な同じ開発技術と手順に従う必要があります。これには、オペレータインターフェイスと、プログラムの他の部分へのアクセスの妥当性確認とテストが含まれます。コントローラ・アプリケーション・ソフトウェアでは、HMIからアクセスできるテーブルを作成し、必要なデータポイントにしかアクセスできないようにアクセスを制限します。
- システムの妥当性確認とテストが完了したら、コントローラプログラムと同様に、HMI ソフトウェアを保護および保守し、SIL に準拠させます。

安全プログラム

安全プログラムは、安全タスクでのみスケジュールできることを除き、標準プログラムのすべての属性を持っています。安全プログラムは、プログラム範囲の安全タグを定義することもできます。安全プログラムは、スケジュール型または非スケジュール型にできます。

安全プログラムは安全コンポーネントのみを含めることができます。安全プログラム内のルーチンは、すべて安全ルーチンです。安全プログラムには、標準ルーチンまたは標準タグを含めることはできません。

安全ルーチン

安全ルーチンには、標準ルーチンと同じ属性がありますが、安全プログラムのみに存在できること、標準タグの読み書きができないこと、およびラダーロジックのみで実行できることが相違点です。各安全プログラムで1つの安全ルーチンをメインルーチンとして指定する必要があります。その安全プログラムで別の安全ルーチンをフォルトルーチンとして指定できます。安全認可された命令のみが、安全ルーチンに使用されます。

安全命令のリストは、71ページの付録Aを参照してください。

安全タグ

GuardLogix制御システムは、同じプロジェクトで標準タグと安全タグの両方の使用をサポートしています。ただし、プログラミングソフトウェアは、標準タグと安全タグを操作上区別します。

安全タグには標準タグの属性すべてがあり、さらに構成されたSIL (SIL 2またはSIL 3)のデータの整合性を提供するためのメカニズムが追加されています。

安全タグは、以下で構成することができます。

- すべてのプリミティブなデータタイプ(例えば、BOOL、SINT、INT、DINT、LINT、REALなど)
- 安全アプリケーション命令に使用する事前定義型
- ユーザ定義のデータタイプ、または前の　2　つのタイプで構成される配列

Studio 5000 Logix Designerアプリケーションは、安全プログラムで無効なタグが直接作成されることを防止します 誤ったタグをインポートしても、確認できません。

重要　**標準タグと安全タグ間のエイリアスは、安全アプリケーションでは禁止されています。**

安全タグに分類されるタグは、コントローラ用またはプログラム用のいずれかです。コントローラ用の安全タグは、標準ロジック、安全ロジック、他の通信デバイスのいずれかで読取ることができますが、書込みは安全ロジックまたは他のGuardLogixセーフティコントローラでしか実行できません。プログラム用の安全タグは、ローカル安全ルーチンからしかアクセスできません。これらのルーチンは、安全プログラム内に存在します。

安全I/Oおよびプロデューサまたはコンシューマ安全データに関連するタグは、コントローラ用の安全タグでなければなりません。

重要　**安全入力タグと安全コンシューマタグは、任意の標準ルーチンで読取ることができますが、更新レートは、安全タスクの実行に基づいています。これらのタグは、安全タスク実行の開始時に更新されます。これは標準のタグの動作と異なります。**

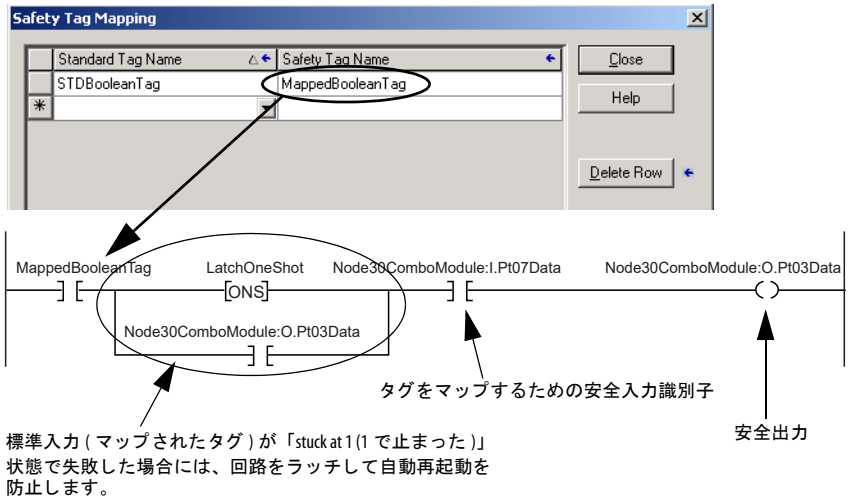
安全ルーチンの標準タグ(タグマッピング)

コントローラ用の標準タグを安全タグにマップして、標準動作と安全動作を同期させるメカニズムを提供することができます。

注意：安全ルーチンに標準データを使用しているときは、データが適切な方法で使用されていることを確認するための信頼できる手段を提供する責任があります。安全タグで標準データを使用しても、安全データにはなりません。標準タグデータで安全出力を直接制御してはなりません。

この例では、標準データを安全データで識別するための方法を示しています。

図16 - 標準データを安全データで識別



第6章

安全アプリケーションの開発

項目	参照ページ
安全概念の前提条件	49
アプリケーション開発とテストの基本	50
ライフライフサイクルの立ち上げ	52
安全アプリケーションプログラムのダウンロード	58
安全アプリケーションプログラムのアップロード	59
メモリカードからのプロジェクトの保存とロード	59
データの強制	59
デバイスの禁止	60
オンライン編集	60
安全アプリケーションの編集	61

安全概念の前提条件

安全概念は、以下の条件を前提としています。

- アプリケーションの作成、操作、保守の責任者は、安全システムの特別なトレーニングを受け、経験があり、十分な資格を有していること
- ロジックを正しく適用して、プログラミングエラーを検出できること。仕様、プログラミングルール、命名規則に厳密に準拠することによって、プログラミングエラーを検出できること
- アプリケーションの厳密な分析を行ない、障害を検出するために可能な手段をすべて講じていること
- 安全署名を手動でチェックして、アプリケーションのダウンロードをすべて確認すること
- 安全関連システムを起動する前に、システム全体の完全な機能テストを実行すること このテストには以下が含まれます。
  - 個々のデバイスの制限を超えて(境界テスト)、アドオンプロファイルで実行される I/O 構成を含む、実装された安全機能の全般的な機能を検証する。
  - ソフトウェアの正しいバージョンが使用されていることを確認する。

表1 - 安全実行に対するコントローラモードの影響

コントローラモード	コントローラの動作
プログラム	• 安全入力コネクションと安全出力コネクションが確立し、維持されている。 – 安全入力タグが安全入力値を反映して更新されている。 • 安全タスクロジックがスキャンされていません。
テスト	• 安全入力コネクションと安全出力コネクションが確立し、維持されている。 – 安全入力タグが安全入力値を反映して更新されている。 • 安全タスクロジックはスキャンされています。
ラン	• 安全入力コネクションと安全出力コネクションが確立し、維持されている。 – 安全入力タグが安全入力値を反映して更新されている。 – コントローラは、「ラン」安全出力パケットを送信する。 • 安全タスクロジックはスキャンされています。 • すべての安全タスク・プロセス・ロジック、相互比較ロジック出力。ロジック出力は安全出力に書込まれます。

表2 - 安全アプリケーションのステータス

安全タスクのステータス	安全規格への準拠(1)	コントローラの動作
ロックを解除した状態 署名なし	開発のためのみ	• 安全I/0の強制がある場合がある。 • 安全I/0の強制を変更できる。 • 安全オンライン編集が可能です。 • 安全メモリは隔離されているが保護されていない(読取り/書込み)。
ロックした状態 署名なし	開発のためのみ	• 安全I/0強制はできない(ロックするには安全I/0の強制を削除する必要がある)。 • 安全タスクのオンライン編集はできない。 • 安全メモリは保護される(読取りのみ)。
ロックを解除した状態 署名あり	SIL 3/PLe/ カテゴリ 4 制御の信頼性	• 安全I/0の強制を使用できない。(署名を生成するには、安全I/0の強制を削除する必要がある。) • 安全タスクのオンライン編集はできない。 • 安全メモリは保護される(読取りのみ)。 • 安全署名を使用すると、再度ダウンロードせずに、回復不能な安全フォルから回復できる。 • 安全署名は保護されておらず、コントローラにアクセスできるユーザなら誰でも削除できる。
ロックした状態 署名あり	SIL 3/PLe/ カテゴリ 4 制御の信頼性	• 安全I/0の強制を使用できない。 • 安全タスクのオンライン編集はできない。 • 安全メモリは保護される(読取りのみ)。 • 安全署名を使用すると、再度ダウンロードせずに、回復不能な安全フォルから回復できる。 • 安全署名は保護される。ユーザが安全署名を削除するには、ロック解除用のパスワードを入力してコントローラをロック解除する必要がある。

(1)　このレベルを達成するには、このセーフティ・リファレンス・マニュアルで定義された安全要件に従う必要があります。

アプリケーション開発とテストの基本

目的のSIL 2またはSIL 3システムのアプリケーションプログラムについては、安全アプリケーションのトレーニングを受けて経験のあるシステムインテグレータまたはユーザが開発してください。開発者は、以下の適正な設計基準に従う必要があります。

- フローチャート、タイミングチャート、シーケンスチャートなどの機能仕様を使用します。
- 安全タスクロジックのレビューを実行します。
- アプリケーションの妥当性確認を実行します。

Studio 5000環境とは、IEC 61508-3の条項7.4.4でオフラインツールとして認可されたツールスイートのことです。安全アプリケーションの開発に際しては、次のことを考慮してください。

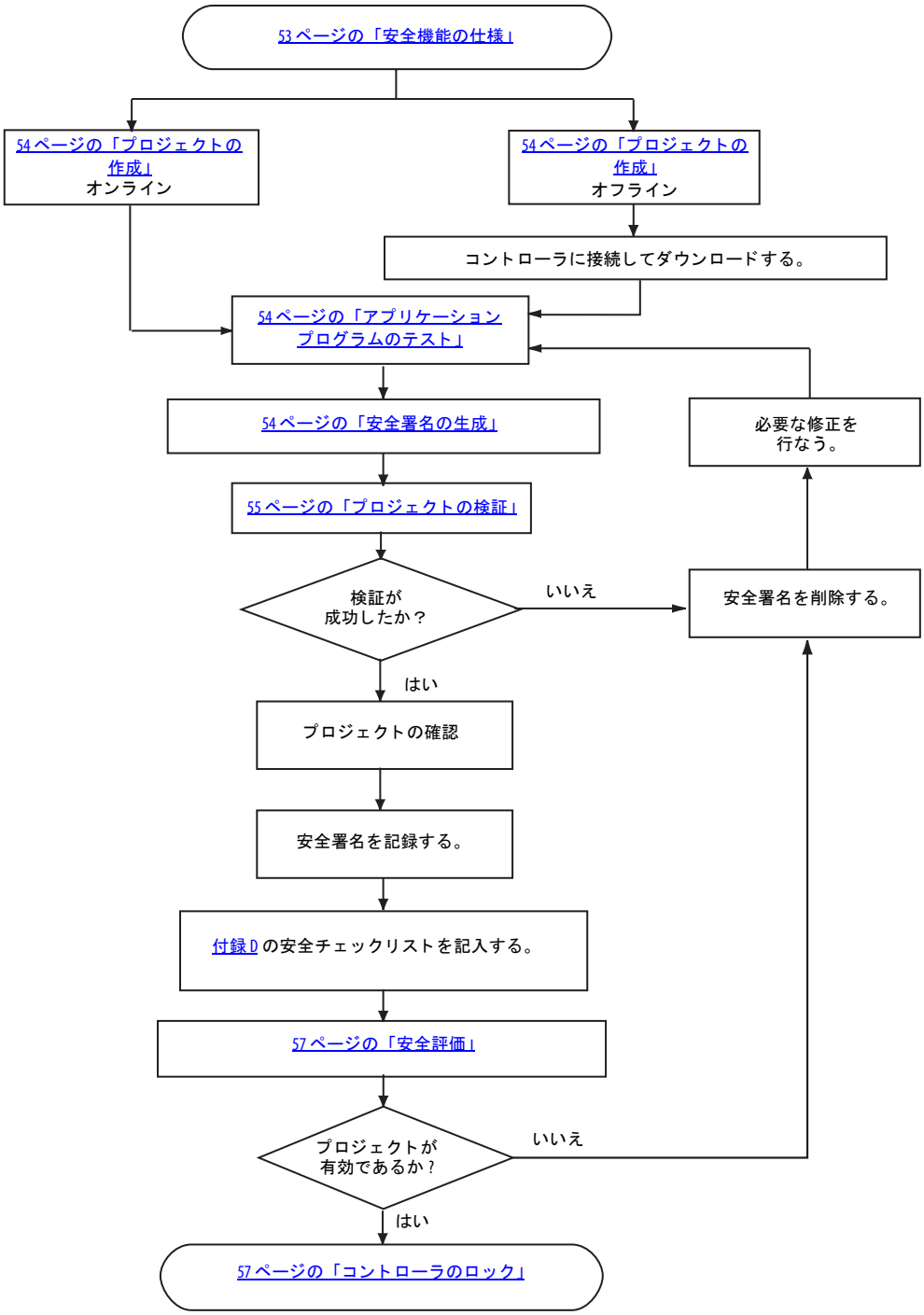
重要

- Studio 5000 Logix Designer アプリケーションは、IEC 61508-3 Edition 2の条項 7.4.4 で認可されており、GuardLogix ベースのアプリケーションのコーディングライフサイクルで、またモジュールテスト、統合テスト、および検証テストのライフサイクル段階での支援として使用できます。その結果、それらのライフサイクル段階での使用の追加の理由は必要ありません。ただし、他のツールを単独で、または Studio 5000 Logix Designer アプリケーションと共にしようした場合、他のツールのついての追加の理由が必要になる場合があります。すべてのライフサイクル段階で使用されるその他のオフラインツールが、ソフトウェア開発活動の一貫した部分として選択されていることを確認するのはユーザの責任です。
- Studio 5000 Logix Designer アプリケーションの信頼性の負担と、製品のマニュアルで指定された以外の方法で Studio 5000 Logix Designer アプリケーションを使用したときに実行可能なソフトウェアに影響する可能性のある潜在的な障害メカニズムを判断するための評価を実施することはユーザの責任です。
- Studio 5000 Logix Designer アプリケーションに入力され、コントローラにダウンロードされるプログラミング情報および構成情報のすべてがご使用のアプリケーションの要件を満たしていることを確認する必要があります。詳細は、56 ページの「プロジェクトの確認」を参照してください。
- 安全度水準の要件に従い、ソフトウェアまたは設計表現はアプリケーションの特性と一致する必要があります。
- 安全度水準の要件に従い、ソフトウェアまたは設計表現は、Studio 5000 Logix Designer アプリケーションと GuardLogix コントローラでサポートされる機能と互換である必要があります。希望のソフトウェアと設計表現が Studio 5000 Logix Designerアプリケーションと GuardLogixコントローラでサポートされていることを確認することはユーザの責任です。
  例 : 設計がフローチャートフォーマットで表現されている場合、その設計をラダーダイアグラムに変換する必要があります。
- GuardLogix コントローラへのコンパイルとダウンロードのために、Studio 5000 Logix Designer アプリケーションにインポートするロジックを自動的に生成するためにサードパーティ製のツールまたは内部で開発したツールを使用する場合、開発サイクルでそのツールを選択する時点で、適合性の評価が必要になります。

ライフライフサイクルの立ち上げ

以下のフローチャートに、GuardLogixシステムの立上げに必要な手順を示します。これらの項目の説明については、リンク先をご覧ください。

図17 - システムの立上げ



安全機能の仕様

安全機能の仕様を作成する必要があります。この仕様を使用して、プログラムロジックがアプリケーションの機能制御および安全制御の要件に正しく完全に対応していることを確認します。アプリケーションによっては、異なるフォーマットで仕様を示す場合があります。ただし、仕様には以下を含む詳細な説明が必要です(該当する場合)。

- 動作のシーケンス
- フローチャートとタイミングチャート
- シーケンスチャート
- プログラムの説明
- プログラムのプリントアウト
- ステップ条件および制御対象のアクチュエータの書面による説明(以下を含む)
  - 入力の定義
  - 出力の定義
  - I/O 配線図と参考資料
  - 動作理論
- ステップ条件および制御対象のアクチュエータのマトリックスまたは表(シーケンスチャートとタイミングチャートを含む)
- 限界条件(動作モードや非常停止など)の定義

仕様のI/O部分には、フィールド回路の解析(センサとアクチュエータのタイプ)を含める必要があります。

- センサ(デジタルまたはアナログ)
  - 標準動作での信号(デジタルセンサの待機電流の原理、センサがオフのときには信号がないことを意味する)
  - IL レベルに必要な冗長性の決定
  - 不一致のモニタと視覚化(診断ロジックを含む)
- アクチュエータ
  - 標準動作での位置と起動(通常はオン)
  - スイッチオフまたは電源異常時の安全対応 / 位置決め
  - 不一致のモニタと視覚化(診断ロジックを含む)

プロジェクトの作成

アプリケーションのプログラミングで使用するロジックと命令は、以下の要件を満たす必要があります。

- 理解しやすい
- 追跡しやすい
- 変更しやすい
- テストしやすい

すべてのロジックに対してレビューとテストを行なってください。安全関連のロジックと標準ロジックは分けてください。

プログラムのラベル付け

以下のラベルを使用してアプリケーションプログラムを明確に識別します。

- 名称
- Date (日付)
- Revision (リビジョン)
- その他のユーザ識別子

アプリケーションプログラムのテスト

この手順は、プロジェクト検証テストに備えてアプリケーションを正しく実行するために必要となる項目で構成されます。これには、ランモードとプログラムモード、オンラインまたはオフラインの編集、アップロードとダウンロード、非公式テストなどが含まれます。

安全署名の生成

注意：コントローラが SIL 2 または SIL 3 の定格で動作するには、安全署名が必要です。安全署名なしでの実行は、開発時にのみ許されます。

重要	**安全署名を生成するには、Professional、Full、Lite Edition のいずれかの Studio 5000 Logix Designer アプリケーションのエディション、または別個の 9324-RLDGLXE GuardLogix エディタが存在する必要があります。**

安全署名は、コントローラの安全部分全体に適用され、ロジック、データ、構成を含む各プロジェクトを一意に識別します。安全署名は、ID (識別番号)、日付と時刻で構成されています。

以下の条件がすべて満たされているときは、安全署名を生成することができます。

- Studio 5000 Logix Designerアプリケーションがコントローラでオンラインであること
- コントローラがプログラムモードであること
- コントローラが安全ロックされていること
- コントローラに安全強制またはペンディング中のオンライン安全編集が存在しないこと
- 安全タスクステータスがOKであること

アプリケーション・プログラム・テストが完了したら、安全署名を生成する必要があります。生成後に、プログラミングソフトウェアによって、安全署名が自動的にアップロードされます。

重要	**安全アプリケーションの検証時、安全アプリケーションが変更されていない場合でも、再ダウンロードが必要になることがあります(標準アプリケーションの編集など)。** **正しい安全アプリケーションがダウンロードされたことを確認するには、最初に作成した安全署名を手動で記録し、各ダウンロードの後で安全署名をチェックし、それがオリジナルと一致することを確認します。**

安全署名を削除できるのは、GuardLogixコントローラの安全ロックが解除されていて、オンラインの場合にキースイッチがREMまたはPROG位置にあるときだけです。Protect Signature in Run modeがチェックされているときは、コントローラはランモードで安全署名を削除できません。

安全署名がある場合、ファームウェアを更新することはできません。

安全署名が存在するときには、安全タスク内で以下の操作は許可されません。

- オンラインまたはオフラインのプログラミング、または安全コンポーネントの編集
- 安全I/Oの強制
- 安全コンポーネントのデータ操作　(　ルーチンロジックまたは別のGuardLogixコントローラによる場合は除く)

プロジェクトの検証

アプリケーションプログラムが仕様を順守しているかを確認するには、アプリケーションを対象とする一連の適切なテストケースを作成する必要があります。この一連のテストケースは、テスト仕様としてファイルして保管する必要があります。

一連のテストを含めて、アプリケーションロジックで使用されている計算(式)の妥当性を証明する必要があります。このときに、同等の範囲テストを使用できます。これらは、定義された値の範囲、制限値、または無効な値の範囲でのテストです。必要なテストケースの数は、使用する計算式によって決まり、臨界値のペアを含む必要があります。

ソース(フィールドデバイス)のアクティブシミュレーションも行なう必要があります。シミュレーションは、システム内のセンサとアクチュエータが正しく配線されていることを確認する唯一の方法です。センサとアクチュエータを手動で操作して、プログラムされた機能の動作を確認します。

また、配線エラーとネットワーク通信障害に対する応答を確認するテストも行なう必要があります。

プロジェクトの検証には、フォルトルーチン、入力/出力チャネルのテストが含まれており、これにより安全システムが正しく動作することを確認します。

GuardLogixコントローラのプロジェクト検証テストを実行するには、アプリケーションのすべてのテストを実施する必要があります。各安全機能に関連するそれぞれのセンサとアクチュエータを切換える必要があります。シャットダウン機能は通常動作では使用しない機能であるため、シャットダウン機能はすべてテストしてください。

また、プロジェクト検証テストは、テストを実施する特定のアプリケーションに対してのみ有効です。安全アプリケーションを別のインストールに移動した場合は、新しいセンサ、アクチュエータ、配線、ネットワーク、および制御システムの物理機器の状況に合わせて、安全アプリケーションのスタートアップおよびプロジェクト検証を実行する必要があります。

プロジェクトの確認

プロジェクトを印刷または表示し、アップロードされた安全I/Oおよびコントローラの構成、安全データ、安全タスク・プログラム・ロジックを比較して、安全アプリケーションプログラムに正しい安全コンポーネントがダウンロード、テスト、保持されていることを確認する必要があります。

また、命令署名によって封印された安全アドオン命令がアプリケーションプログラムに含まれている場合は、アドオン命令を封印したとき記録した値と、命令署名、日付と時刻、安全命令署名を比較する必要があります。

SIL 3アプリケーションで安全アドオン命令を作成および使用する方法については、75ページの付録Bを参照してください。

以下の手順は、プロジェクトを確認する1つの方法を説明しています。

1. オンラインで、コントローラがプログラムモードにある状態で、プロジェクトを保存します。
2. Upload Tag Values プロンプトに対して、Yes と答えます。
3. Studio 5000 Logix Designer アプリケーションがオフラインの状態で、Offlineprojectname.ACD などの新しい名前を付けてプロジェクトを保存します (この場合、projectname はプロジェクトの名前です)。このファイルが新しいテスト済みのマスタ・プロジェクト・ファイルになります。
4. プロジェクトを閉じます。

5. オリジナルプロジェクトのアーカイブファイルをカレントディレクトリから移動します。このファイルを削除するか、アーカイブ可能な場所に格納できます。Studio 5000 Logix Designer アプリケーションはこのディレクトリで projectname.ACD ファイルを見つけると、コントローラプロジェクトに関連付けますが、実際のアップロードは実行されないため、この手順が必要になります。
6. コントローラがプログラムモードにある状態で、プロジェクトをコントローラからアップロードします。
7. アップロードしたプロジェクトを Onlineprojectname.ACD として保存します (この場合、projectname はプロジェクトの名前です)。
8. Upload Tag Values プロンプトに対して、Yes と答えます。
9. Studio 5000 Logix Designer Program Compare ユーティリティを使用して、以下を比較します。
   - GuardLogix コントローラと CIP Safety I/O デバイスのすべてのプロパティ
   - 安全タスク、安全プログラム、安全ルーチンのすべてのプロパティ
   - 安全ルーチンのすべてのロジック
10. すべてのコントローラと I/O 構成がアプリケーション仕様の要件を満たしていることを確認します。

安全評価

システムが動作を認可されるためには、独立した第三者機関によって安全システムを検証する必要がある可能性があります。IEC 61508 SIL 2 または SIL 3 では、独立した第三者機関による認可が必要な可能性があります。

コントローラのロック

GuardLogix コントローラを安全ロックして修正されないように保護することをお奨めします。ただし、コントローラの安全ロックは、SIL 2 または SIL 3 の要件ではありません。安全ロック機能は、安全タスク、安全プログラム、安全ルーチン、安全タグ、安全アドオン命令、安全 I/O、および安全署名などの安全コンポーネントにのみ適用されます。ただし、安全ロックだけでは SIL 2 または SIL 3 の要件を満たしません。

コントローラが安全ロック状態にある間は、どの安全面も修正することはできません。コントローラが安全ロックされているときは、安全タスクで以下の操作は許可されません。

- ファームウェアを更新します。
- オンラインまたはオフラインプログラミングまたは編集
- 安全 I/O の強制
- 安全コンポーネントのデータ操作
  (ルーチンロジックまたは別の GuardLogix コントローラによる場合は除く)

- 安全アドオン命令の作成または編集
- 安全署名の生成または削除

重要　安全署名が存在し、コントローラが安全ロックされている場合、一致する安全署名のあるプロジェクトのみ、コントローラにダウンロードできます。

コントローラのデフォルト状態では、コントローラの安全ロックは解除されています。オンラインまたはオフラインであるか、およびプログラムのオリジナルソースを持っているかどうかに関係なく、安全アプリケーションを安全ロック状態にすることができます。ただし、安全強制またはペンディング中の安全編集があってはなりません。キースイッチがRUN位置にあるときは、安全ロックまたは安全ロック解除のステータスは変更できません。

保護レイヤを追加するには、コントローラを安全ロックまたはロック解除するのに異なるパスワードを使用できます。パスワードはオプションです。

安全ロック機能の詳細は、コントローラのユーザーズマニュアルを参照してください。

- ControlLogix 5580 and GuardLogix 5580 Controllers User Manual (Pub. No. 1756-UM543)
- CompactLogix 5380 および Compact GuardLogix 5380 コントローラユーザーズマニュアル (Pub. No. 5069-UM001)

安全アプリケーションプログラムのダウンロード

安全署名が存在する場合を除き、ダウンロード時にはアプリケーションのテストが必要です。

重要　正しい安全アプリケーションがダウンロードされたこと、またはメモリカードから復元されたことを確認するには、その安全署名が安全ドキュメントのオリジナルの署名と一致することを手動でチェックする必要があります。

安全ロックされたGuardLogixコントローラへのダウンロードは、オフラインプロジェクトの安全署名とファームウェアリビジョンが、ターゲットのGuardLogixコントローラとすべて一致し、コントローラの安全タスクステータスがOKの場合にのみ許可されます。

重要　安全署名が一致せず、コントローラが安全ロックされている場合、ダウンロードするためにはコントローラのロックを解除する必要があります。この場合、コントローラへのダウンロードによって安全署名は削除されます。したがって、アプリケーションの妥当性を再度確認する必要があります。

安全アプリケーションプログラムのアップロード

GuardLogixコントローラに安全署名が含まれる場合、その安全署名はプロジェクトのオンライン保存時にアップロードされます。その結果、すべてのオフライン安全タグ値は、署名の生成と同時に保存されるスナップショット値にアップロードされます。この場合、タグ値をアップロードするオプションは、標準タグ値のみに影響します。

メモリカードからのプロジェクトの保存とロード

GuardLogixおよびCompact GuardLogixコントローラは、メモリカードを使用したファームウェアの更新、ユーザプログラムの保存と取得をサポートします。GuardLogixシステムでは、プライマリコントローラのみがメモリカードを使用します。

安全プロジェクトをメモリカードに保存する場合、ロードモードつまりロード後のコントローラのモードとしてリモートプログラムを選択することをお奨めします。実際の機械の運転前に、機械を作動させるためオペレータの介入が必要です。

メモリカードからのロードを実行できるのは、以下の場合のみです。

- メモリカードに保存したプロジェクトで指定されたコントローラタイプが、実際のコントローラタイプと一致する場合
- メモリカード上のプロジェクトのメジャーリビジョンとマイナーリビジョンが、コントローラと一致する場合

重要　**リビジョンの不一致によって防止されるのは、ユーザ定義のロードのみです。コントローラで開始されたロードは、メモリカードの内容によってコントローラ上のファームウェアを上書きします。**

- コントローラがランモードでない場合

安全ロックされたコントローラへのプロジェクトのロードは、メモリカードに保存されたプロジェクトの安全署名が、コントローラ上のプロジェクトと一致する場合にのみ許可されます。安全署名が一致しない、またはコントローラが安全署名なしで安全ロックされている場合は、まずコントローラのロックを解除してから、不揮発性メモリを介してコントローラの更新を試みてください。

重要　**コントローラのロックを解除してメモリカードからのロードを開始した場合、ロードが完了すると、安全ロックステータス、パスワード、および安全署名は、メモリカードに保存されていた値に設定されます。**

データの強制

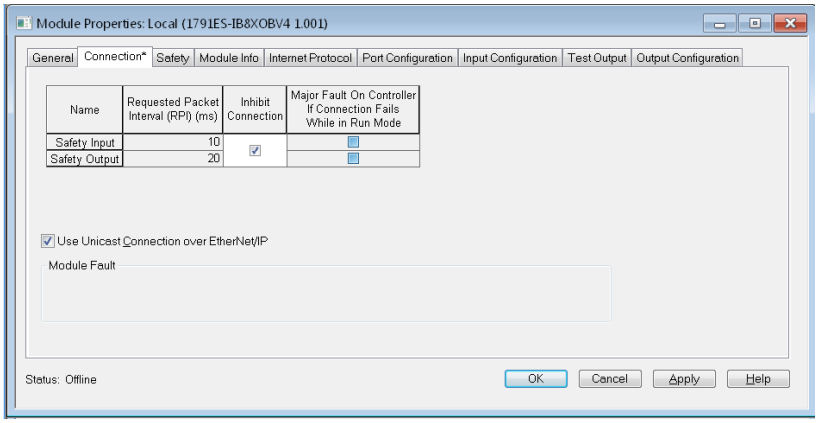
プロジェクトが安全ロック解除され、安全署名が存在しないときは、I/Oに含まれているすべてのデータ、CONNECTION_STATUS を含むプロデューサまたはコンシューマ安全タグを強制することができます。ただし、安全プロジェクトを安全ロックするか、または安全署名を生成する前に、すべての安全タグの強制を無効にするだけでなく削除する必要があります。プロジェクトが安全ロックされているか、または安全署名が存在するときは、安全タグを強制することはできません。

ヒント　**標準タグの場合は、安全ロックまたは安全ロック解除状態に関わらず、強制をインストールまたは削除することができます。**

デバイスの禁止

アプリケーションプログラムが安全ロックされているか、または安全署名が存在する場合、安全I/Oデバイスおよびプロデューサコントローラを禁止または禁止解除することはできません。以下の手順に従って、特定の安全I/Oデバイスを禁止してください。

1. Studio 5000 Logix Designer アプリケーションでデバイスを右クリックし、Properties を選択します。
2. Module Properties ダイアログボックスで、Connection タブをクリックします。
3. Inhibit Connection をチェックしてから Apply をクリックします。



デバイスは、このチェックボックスがオンになっているときに常に禁止されます。通信デバイスが禁止されると、すべての下流のデバイスも禁止されます。

オンライン編集

標準ロジックのオンライン編集は、安全状態の影響を受けません。

ヒント　標準ルーチンのオンライン編集は、安全ロックまたは安全ロック解除状態の影響を受けません。

注意：オンラインの変更（ロジック、データ、または構成に対する変更）を実行すると、それがアプリケーションの実行中である場合は、システムの安全機能に影響する可能性があります。オンラインの変更は、どうしても必要な場合にのみ行なってください。変更が正しく行われなかった場合、アプリケーションが停止することがあります。したがって、オンラインの変更を実行する前に、更新中に代替の安全対策を使用する必要があります。

安全ロジックのオンライン編集はコントローラが安全ロック解除の状態で安全署名がない場合にのみ実行できます。安全ロジックをオンラインで編集する場合は、次のガイドラインに従ってください。

- コントローラが安全編集でロックされている場合、編集をアセンブルまたはキャンセルするには、コントローラをロック解除する必要があります。
- 安全ルーチンでは、ペンディング中の編集がある場合はコントローラをロックできませんが、テスト編集がある場合はロックできます。

- 既存の安全命令の命令構成パラメータを変更する場合は、変更を有効にするには、コントローラをプログラムモードに移行してからランモードに戻す必要があります。

オンライン中は標準または安全アドオン命令の編集はできません。

安全アプリケーションの編集

Studio 5000 Logix Designerアプリケーションで安全アプリケーションプログラムを変更するには、以下の規定に従ってください。

- 認定され特別なトレーニングを受けた担当者だけが、プログラムを編集することができます。これらの担当者は、コントローラのキースイッチやソフトウェアパスワード保護などの利用可能なすべての管理方法を使用する必要があります。
- 認可され特別なトレーニングを受けた担当者がプログラム編集を行なうときは、変更処理中の安全を確保する中心的な役割を担います。さらにこれらの担当者は、安全アプリケーションの動作も維持する必要があります。
- オンライン編集時には、システムの安全を維持するために代替の保護手段を使用する必要があります。
- プログラム編集では、以下の情報を文書化しておく必要があります。
  - 認証
  - 影響の分析
  - 実行
  - テスト情報
  - リビジョン情報
- 標準ルーチン内でのみオンライン編集を行なった場合は、通常動作に戻る前にこれらの編集の妥当性を検証する必要はありません。
- 標準ルーチンへの変更が、タイミングとタグマッピングに関して安全アプリケーションで受入れ可能であることを確認する必要があります。
- 以降で説明するように、オフラインまたはオンライン時に、プログラムのロジック部分を編集することができます。

オフライン編集の実行

標準プログラムの要素にのみオフライン編集を行ない、ダウンロード後に安全署名が一致する場合は、動作を再開することができます。

オフライン編集が安全プログラムに影響を与える場合は、動作を再開する前に影響の分析で指定される通りにアプリケーションの該当するすべての要素の妥当性を再検証する必要があります。

63ページの図18は、オフライン編集のプロセスを示しています。

オンライン編集の実行

オンライン編集が安全プログラムに影響を与える場合は、動作を再開する前に影響の分析で指定された指示に従ってアプリケーションの該当するすべての要素の妥当性を再検証する必要があります。63ページの図18は、オンライン編集のプロセスを示しています。

ヒント　オンライン編集は、セットポイント変更、ロジックの追加、削除、修正などの簡単なプログラム修正に限定してください。

GuardLogixコントローラの安全ロックおよび安全署名機能は、オンライン編集に影響します。

詳細は、57ページの「コントローラのロック」の54ページの「安全署名の生成」を参照してください。

オンライン中のLogix Designerアプリケーションでのラダーロジックの編集方法については、『Logix5000コントローラ クイックスタート』(Pub. No. 1756-QS001)を参照してください。

修正の影響テスト

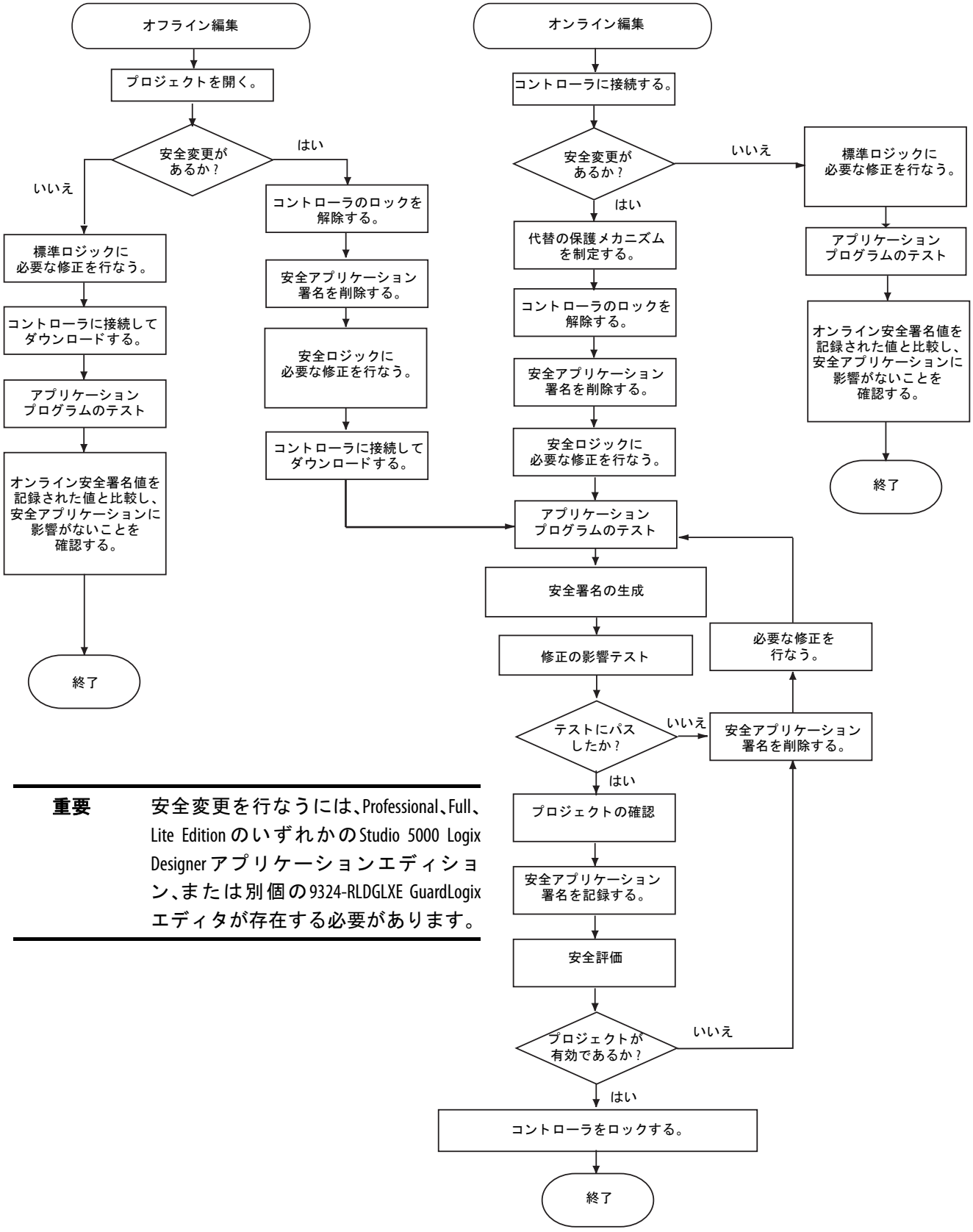
検証済みソフトウェアの修正、機能拡張、改良を行なう場合は、機能安全システムへの影響に関する計画と分析が必要です。影響の分析で示されるとおりに、ソフトウェアの安全ライフサイクルの該当するすべての段階を実行する必要があります。

少なくとも影響を受けるすべてのソフトウェアの

- 機能テストを実施してください。
- ソフトウェア仕様への修正はすべて文書化してください。
- テスト結果も文書化してください。

詳細は、IEC 61508-3のセクション7.8(Software Modification)を参照してください。

図18 - オンライン編集とオフライン編集のプロセス



重要　安全変更を行なうには、Professional、Full、Lite Edition のいずれかの Studio 5000 Logix Designer アプリケーションエディション、または別個の 9324-RLDGLXE GuardLogix エディタが存在する必要があります。

Notes:

ステータスのモニタおよびフォルトの処理

項目	参照ページ
ステータスインジケータ	65
システムステータスのモニタ	65
安全フォルト	68
安全パートナフォルト	70

GuardLogixアーキテクチャには、システム内のフォルトを検出して応答するための多くの方法があります。フォルトを処理する最初のステップは、アプリケーションのチェックリストを完了したか確認することです(91 ページの付録Dを参照)。

ステータスインジケータ

ステータスインジケータの動作の詳細は、コントローラのユーザーマニュアルを参照してください。

- ControlLogix 5580 and GuardLogix 5580 Controllers User Manual (Pub. No. 1756-UM543)
- CompactLogix 5380 および Compact GuardLogix 5380 コントローラユーザーズマニュアル(Pub. No. 5069-UM001)

重要 **ステータスインジケータは、安全機能のインジケータとしては信頼できません。立上げまたはトラブルシューティング時の一般的な診断にのみ使用してください。動作ステータスを判断するのに、ステータスインジケータを使用しないでください。**

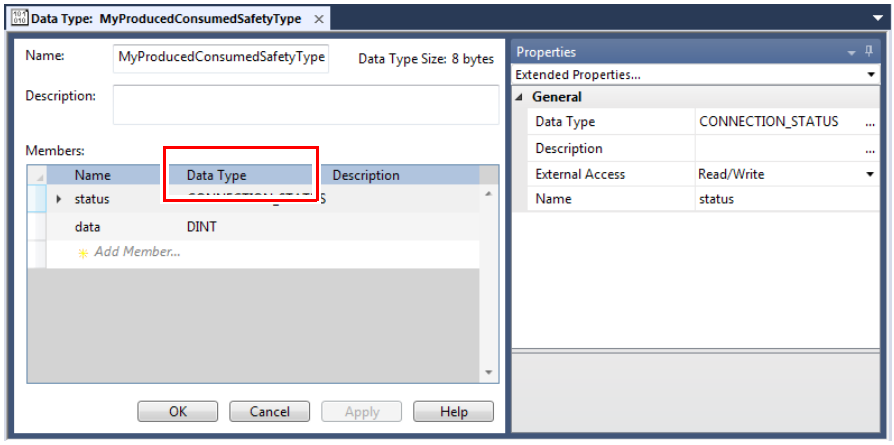
システムステータスのモニタ

安全タグのコネクションステータスを確認できます。また、各種のデバイスオブジェクトを取り出すことで現在の動作ステータスを判別できます。ユーザは、シャットダウンシーケンスを開始するのに最適なデータを判別する責任があります。

CONNECTION_STATUSデータ

安全入力データとプロデューサ/コンシューマ安全タグに関連付けられたタグ構造体の最初のメンバーには、コネクションステータスが含まれています。このメンバーは、CONNECTION_STATUS という定義済みのデータタイプです。

図 19 - Data Type ダイアログボックス



CONNECTION_STATUS データタイプの先頭2ビットには、デバイスの RunMode および ConnectionFaulted ステータスビットが含まれます 表3 に、RunMode と ConnectionFaulted の状態の組合せについて説明します。

表 3 - 安全コネクションのステータス

RunMode のステータス	ConnectionFaulted のステータス	安全コネクションの動作
1 = ラン	0 = 有効	データは生成デバイスでアクティブに制御されている。プロデューサデバイスはランモードです。
0 = アイドル	0 = 有効	コネクションはアクティブで、プロデューサデバイスはアイドル状態です。安全データは安全状態にリセットされる。
0 = アイドル	1 = フォルト発生	安全コネクションにフォルトが発生する。プロデューサデバイスの状態は不明です。安全データは安全状態にリセットされる。
1	1	誤った状態です。

注意：安全 I/O コネクションとプロデューサ / コンシューマ接続の構成によって、コネクションが失われてシステムが安全状態に移行した場合に自動的にコントローラをフォルトにすることはできません。したがって、システムが SIL 3 を保持していることを確認するために、デバイスのフォルトを検出する必要がある場合、安全 I/O の CONNECTION_STATUS ビットをモニタして、プログラムロジックによりフォルトを開始する必要があります。

入力と出力の診断

Guard I/O モジュールはパルステストとモニタ機能を備えています。モジュールが故障を検出すると、原因の入力または出力をモジュールの安全状態に設定して、コントローラに故障を報告します。故障は入力または出力のステータスを介して表示され、故障を修理した後に構成可能な時間保持されます。

重要　ユーザは、これらの I/O エラーをラッチして、システムが正しく再起動するかどうかを確認するアプリケーションロジックを提供することに対して責任があります。

I/Oデバイスのコネクションステータス

CIP Safetyプロトコルを使用すると、I/O データの受信者はそのデータのステータスを決定できます。

- コントローラは入力コネクションエラーを検出すると、すべての入力データを安全状態に設定し、関連する入力ステータスをフォルトに設定します。
- 出力デバイスは出力コネクションエラーを検出すると、出力をオフにします。
- 通常、セーフティコントローラにも出力デバイスからの入力コネクションがあります。セーフティコントローラは、これらの入力コネクションのステータスを決定しますが、入力コネクションステータスは、出力をオフにする主要なメカニズムではありません。

重要　**ユーザは、これらのI/Oエラーをラッチして、システムが正しく再起動するかどうかを確認するアプリケーションロジック対して責任があります。**

トリップシステムに対するオフ状態

GuardLogixコントローラは、トリップシステムに対するオフ状態の一部です。つまり、0が安全状態です。一部の安全デバイスでフォルトが検出されると、すべてのデバイス入力/出力は安全状態に設定されます。特定の入力チャネルに関連付けられたフォルトが検出された場合、そのチャネルが安全状態に設定されます。例えば、チャネル0に固有のパルス・テスト・フォルトが検出されると、チャネル0の入力データは安全状態に設定されます。チャネルに固有ではない、デバイスの一般的なフォルトの場合、統合されたステータスビットがフォルトステータスを表示し、すべてのデバイスデータは安全状態に設定されます。

GuardLogix安全アプリケーション命令の使用方法については、99ページの付録Fおよび『GuardLogix Safety Application Instructions Safety Set Reference Manual』(Pub. No. 1756-RM095)を参照してください。

システム値の取得(GSV)命令およびシステム値の設定(SSV)命令

GSV命令とSSV命令によって、デバイスオブジェクトに保存されたコントローラのシステムデータを取得(GSV)および設定(SSV)されます。GSV/SSV命令を入力すると、プログラミングソフトウェアによって命令ごとに有効なオブジェクトクラス、オブジェクト名、属性名が表示されます。安全コンポーネントでGSV命令とSSV命令を使用するには、制限があります。

重要	安全タスクは、標準属性でGSVまたはSSV操作を実行できません。 標準タスクが書込める安全オブジェクトの属性は、診断目的のみです。これらの属性は、安全タスクの実行には影響を与えません。

GSV命令とSSV命令を使用してアクセスできる安全属性の詳細は、コントローラのユーザーズマニュアルを参照してください。

- ControlLogix 5580 and GuardLogix 5580 Controllers User Manual (Pub. No. 1756-UM543)
- CompactLogix 5380 および Compact GuardLogix 5380 コントローラユーザーズマニュアル (Pub.No. 5069-UM001)

GSV命令とSSV命令の使用については、『Logix5000 コントローラ汎用インストラクション・セット・リファレンス・マニュアル』(Pub. No. 1756-RM003) を参照してください。

安全フォルト

GuardLogix 5580およびCompact GuardLogix 5380 システムのフォルトには以下があります。

- 回復可能なコントローラフォルト
- 回復不能なコントローラフォルト
- 安全アプリケーションでの回復不能な安全フォルト
- 安全アプリケーションでの回復可能な安全フォルト

回復不能なコントローラフォルト

これらのフォルトは、コントローラの内部診断でフォルトが検出されたときに発生します。回復不能なコントローラフォルトが発生すると標準タスクと安全タスクの実行が停止され、出力コネクションも停止されます。安全I/Oデバイスは、安全状態に移行することで出力データの喪失に対応します。リカバリするには、アプリケーションプログラムの再度ダウンロードすることが必要です。

安全アプリケーションでの回復不能な安全フォルト

安全アプリケーションで回復不能な安全フォルトが発生したときは、安全ロジックと安全プロトコルが終了します。安全タスクウォッチドッグと制御パートナシップのフォルトはこのカテゴリに分類されます。

安全タスクで回復不能な安全フォルトが発生すると、標準の回復可能なメジャーフォルトもログに記録され、コントローラ・フォルト・ハンドラがある場合は、それが実行されます。コントローラ・フォルト・ハンドラがこのフォルトを処理する場合、安全タスクはフォルト状態のままでも、引き続き標準タスクが実行されます。

注意：安全フォルトを無効にしてもフォルトはクリアされません。安全フォルトを無効にする場合、システムの動作が安全に保持されることを証明する責任はお客様側にあります。

安全フォルトを無効にした後も安全動作が保持されるという証明を承認機関に提供する必要があります。

安全署名がある場合、フォルトをクリアして安全タスクを有効にして実行できます。安全署名がない場合、アプリケーション全体を再度ダウンロードするまで安全タスクは実行できません。

安全アプリケーションでの回復不能な安全フォルト

安全プログラムで回復可能なフォルトが発生すると、安全プログラムのプログラム・フォルト・ハンドラ(存在する場合)がフォルトを処理するかどうかにより、安全タスクの実行が停止される場合があります。

回復可能なフォルトがプログラムでクリアされるときは、安全タスクの実行は中断せずに継続されます。

安全アプリケーションの回復可能なフォルトがプログラムでクリアされないときは、タイプ14、コード2の回復可能な安全フォルトが発生します。安全プログラムの実行が停止し、安全プロトコルコネクションが一度閉じてから再度開き、再度初期化されます。安全出力は安全状態になり、安全コンシューマタグのプロデューサがコンシューマも安全状態にするよう命令します。

回復不能な安全フォルトが処理されない場合、標準の回復可能なメジャーフォルトも記録され、コントローラ・フォルト・ハンドラがある場合は、それが実行されます。コントローラ・フォルト・ハンドラがこのフォルトを処理する場合、安全タスクはフォルト状態のままでも、引き続き標準タスクが実行されます。

回復可能なフォルトの発生は、アプリケーションコードが無効なデータ値または条件から保護されていないことを意味します。これらのフォルトを実行時に処理するかわりに、アプリケーションを修正してそれらを排除することを検討してください。

注意：安全フォルトを無効にしてもフォルトはクリアされません。安全フォルトを無効にする場合、システムの動作が安全に保持されることを証明する責任はお客様側にあります。

安全フォルトを無効にした後も安全動作が保持されるという証明を承認機関に提供する必要があります。

フォルトの表示

Controller Properties ダイアログボックスの Major Faults タブの Recent Faults ダイアログボックスには、2 つのサブタブ (標準フォルト用と安全フォルト用) があります。

コントローラのステータス画面にもフォルトコードが簡単なステータスメッセージと共に表示されます。ステータスインジケータの詳細は、以下を参照してください。

- ControlLogix 5580 and GuardLogix 5580 Controllers User Manual (Pub. No. 1756-UM543)
- CompactLogix 5380 および Compact GuardLogix 5380 コントローラユーザーズマニュアル (Pub.No. 5069-UM001)

フォルトコード

表4 に、GuardLogix 5580 および Compact GuardLogix 5380 コントローラに固有のフォルトコードを示します。タイプとコードは、Controller Properties ダイアログボックスの Major Faults タブに表示されるタイプとコード、PROGRAM オブジェクト、MAJORFAULTRECORD (または MINORFAULTRECORD) 属性に対応します。

表 4 - メジャー安全フォルト (タイプ 14)

コード	原因	ステータス	処置
01	タスクウォッチドッグが経過した。ユーザタスクが指定時間内に完了しなかった。プログラムエラーによって無限ループが発生したか、プログラムが複雑すぎて指定どおりに素早く実行できない、または優先度の高いタスクやバックグラウンドタスクがあるためにこのタスクが完了できない。	回復不能	フォルトをクリアする。 安全署名があるときは、安全メモリを再初期化すると安全タスクが実行を開始する。 安全署名がないときは、安全タスクを実行できるようにプログラムを再度ダウンロードする必要がある。 アプリケーションで許容される場合は、ウォッチドッグ時間を増やす。
02	安全タスクのルーチンにエラーがある。	回復可能	ユーザプログラムのロジックのエラーを訂正する。
07	安全タスクが動作不能。 このフォルトは、安全ロジックが無効か、存在しない場合に発生する。	回復不能	フォルトをクリアする。 安全署名があるときは、安全メモリを安全署名で再初期化すると、安全タスクが実行を開始する。 安全署名がないときは、安全タスクを実行できるようにプログラムを再度ダウンロードする必要がある。

『Logix5000 Controllers Major and Minor Faults Programming Manual』 (Pub. No. 1756-PM014) では、Logix コントローラに共通するフォルトコードについて説明しています。

安全パートナフォルト

安全パートナは、OK ステータスインジケータを備えています。

SIL 構成が SIL 2 に設定されており、安全パートナが安全プライマリの隣のスロットに取付けると、次の動作が発生します。

- 安全パートナで OK ステータスインジケータが赤色に点滅します。
- コントローラがタイプ 14、コード 12 のマイナーフォルトを記録し、コントローラが SIL 2 用に構成され、安全パートナが存在することを示します。
- Studio 5000 Logix Designer アプリケーションが、SIL 2 アプリケーションのダウンロードを拒否します。

安全命令

注意：これらの安全命令は、SIL 2 または SIL 3 アプリケーションでの安全タスクで使用できる唯一の命令です。

認可された命令の最新情報については、以下の安全認証とリビジョンリリースのリストを参照してください。
http://www.rockwellautomation.com/global/certification/safety.page

安全命令

以下の表に、SIL 2 またはSIL 3アプリケーションでの使用のために認可されている安全アプリケーション命令をリストします。

表 5 - 一般的な安全アプリケーション命令

ニーモニック	名称	説明
CROUT	構成可能な冗長出力	冗長出力を制御およびモニタする。
DCA	デュアルチャネル入力 – アナログ (整数バージョン)	2 つのアナログ値の偏差と許容差範囲をモニタする。
DCAF	デュアルチャネル入力 – アナログ (浮動小数点バージョン)	
DCS	デュアルチャネル入力 – 停止	非常停止、セーフティ・ライト・カーテン、ゲートスイッチなどの停止機能を提供することを主な目的としたデュアル入力安全デバイスをモニタする。
DCST	デュアルチャネル入力 – テスト機能付き停止	非常停止、セーフティ・ライト・カーテン、ゲートスイッチなどの停止機能を提供することを主な目的としたデュアル入力安全デバイスをモニタする。 停止デバイスの機能テスト起動機能が追加されている。
DCSTL	デュアルチャネル入力 – テストおよびロック機能付き停止	非常停止、セーフティ・ライト・カーテン、ゲートスイッチなどの停止機能を提供することを主な目的としたデュアル入力安全デバイスをモニタする。 停止デバイスの機能テスト起動機能が追加されている。安全デバイスからのフィードバック信号をモニタし、安全デバイスにロック要求を指令することができる。
DCSTM	デュアルチャネル入力 – テストおよびミュート機能付き停止	非常停止、セーフティ・ライト・カーテン、ゲートスイッチなどの停止機能を提供することを主な目的としたデュアル入力安全デバイスをモニタする。 停止デバイスの機能テストの起動機能、および安全デバイスのミュート機能が追加されている。
DCM	デュアルチャネル入力 – モニタ	デュアル入力安全デバイスをモニタする。
DCSRT	デュアルチャネル入力 – 始動	機械を安全に起動することが主な機能である、イネーブルペンダントなどのデュアル入力安全デバイスをオンする。
SMAT	セーフティマット	セーフティマットに人が乗っていないかどうかを示す。
THRSe	両手制御ランステーション – 拡張	右手用の押しボタンからの 1 つと左手用の押しボタンからの 1 つの 2 つのさまざまな安全入力をモニタして、1 つの出力を制御する。両手制御ランステーションをバイパスするために、構成可能なチャネル間のディスクレパンシ時間と拡張機能が搭載されている。
TSAM	2 センサ非対称ミューティング	非対称に配置された 2 つのミューティングセンサを使って、自動的にライトカーテンの保護機能を一時的に無効にする。
TSSM	センサ対称ミューティング	対称に配置された 2 つのミューティングセンサを使って、自動的にライトカーテンの保護機能を一時的に無効にする。
FSBM	4 センサ双方向ミューティング	ライトカーテンの感知フィールドの前後に連続的に配置された 4 つのセンサを使用して、ライトカーテンの保護機能を一時的に自動的に無効にする。

表 6 - 金属加工安全アプリケーション命令

ニーモニック	名称	説明
CBCM	クラッチブレーキ連続モード	連続動作が必要なときにプレスアプリケーションに使用する。
CBIM	クラッチ・ブレーキ・インチ・モード	プレスのセットアップなどの、わずかなスライド調節が必要なプレスアプリケーションに使用する。
CBSSM	クラッチ・ブレーキ・シングル・ストローク・モード	シングルサイクルのプレスアプリケーションに使用する。
CPM	クランクシャフト位置モニタ	プレスのスライド位置を決定するために使用する。
CSM	カムシャフトモニタ	カムシャフトの始動、停止、および実行動作のモーションをモニタする。
EPMS	8 ポジション・モード・セレクタ	8 つの安全入力をモニタして、アクティブ入力に対応する 8 つの出力の 1 つを制御する。
AVC	補助バルブの制御	メインバルブと共に使用される補助バルブを制御する。
MVC	メインバルブの制御	メインバルブを制御およびモニタする。
MMVC	保守動作中の手動バルブ制御	保守作業中にバルブを手動で駆動するために使用する。

RSLogix 5000® の命令については、99 ページの付録 F を参照してください。

表 7 - RSLogix 5000 安全アプリケーション命令の説明

ニーモニック	名称	説明
ENPEN	イネーブルペンダント	2 つの安全入力をモニタして、1 つの出力を制御する。入力の不一致によるタイムアウト値は 3sec。
ESTOP	非常停止 (E-Stop)	2 つの安全入力をモニタして、1 つの出力を制御する。入力の不一致によるタイムアウト値は 500msec。
RIN	冗長入力	2 つの安全入力をモニタして、1 つの出力を制御する。入力の不一致によるタイムアウト値は 500msec。
ROUT	冗長出力	1 つの入力の状態をモニタして、2 つの出力を制御およびモニタする。
DIN	多様入力	2 つの多様安全入力をモニタして 1 つの出力を制御する。入力の不一致によるタイムアウト値は 500msec。
FPMS	5 ポジション・モード・セレクタ	5 つの安全入力をモニタして、アクティブ入力に対応する 5 つの出力の 1 つを制御する。
THRS	両手制御ランステーション	右手用の押しボタンからの 1 つと左手用の押しボタンからの 1 つの 2 つのさまざまな安全入力をモニタして、1 つの出力を制御する。
LC	ライトカーテン	ライトカーテンからの 2 つの安全入力をモニタし、1 つの出力を制御する。

安全タスク内のルーチンでは、以下のラダーダイアグラム安全命令を使用できます。

表 8 - ラダーダイアグラム安全命令

タイプ	ニーモニック	名称	説明
配列 (ファイル)	COP (1)	コピー	タグ間でバイナリデータをコピーする (型変換はなし)。
	FAL(2)	ファイル算術論理演算命令	配列に格納されたデータのコピー、演算、論理、関数演算を実行する。
	FLL	ファイルフィル	Source (ソース) 値を変更せずに配列の要素にソース値を埋め込む。
	FSC	ファイル検索と比較	配列の値を要素単位で比較する。
	SIZE	要素サイズ	配列の次元サイズを検索する。
ビット	XIC	A 接点命令	ラング状態を 1 にセットまたは 0 にリセットするために、データビットを調べる。
	XIO	B 接点命令	ラング状態を 1 にセットまたは 0 にリセットするために、データビットを調べる。
	OTE	出力	ビットを制御する (ラング状態に応じてセット演算とクリア演算の両方を実行する)。
	OTL	ラッチ出力	ビットを 1 にセットする (保持)。
	OTU	アンラッチ出力	ビットを 0 にリセットする (保持)。
	ONS	ワンショット	イベントを 1 回発生させる。
	OSR	立上り時ワンショット	ラング状態が False(0) から True(1) にセットされる (立上り) たびに、1 スキャンの間だけ出力ビットをセットする。
	OSF	立下り時ワンショット	ラング状態が True(1) から False(0) にリセットされる (立下り) たびに、1 スキャンの間だけ出力ビットをセットする。

表 8 - ラダーダイアグラム安全命令 (続き)

タイプ	ニーモニック	名称	説明
タイマ	TON	オン・ディレイ・タイマ	タイマが有効な時間を計測
	TOF	オフ・ディレイ・タイマ	タイマが無効な時間を計測
	RTO	保持型タイマ	時間を累積する。
	CTU	アップカウンタ	カウントアップする。
	CTD	ダウンカウンタ	カウントダウンする。
	RES	リセット	タイマまたはカウンタを 0 にリセットする。
比較	CMP(2)	比較	式で指定した算術演算の比較を実行する。
	EQU	イコール	2 つの値が等しいかをテストする。
	GEQ	グレータ・ザン・オア・イコール	一方の値がもう一方の値以上の値であるかをテストする。
	GRT	グレータザン	一方の値がもう一方の値を超える値であるかをテストする。
	LEQ	レス・ザン・オア・イコール	一方の値がもう一方の値以下の値であるかをテストする。
	LES	レスザン	一方の値がもう一方の値未満の値であるかをテストする。
	MEQ	マスク付き比較	ソースをマスクを介して値を比較して、等しいかをテストする。
	NEQ	ノットイコール	2 つの値が等しくないかをテストする。
	LIM	リミットテスト	値が指定範囲内であるかをテストする。
移動	CLR	クリア	値をクリアする。
	MOV	移動	値をコピーする。
	MVM	マスク付き移動	整数の特定部分をコピーする。
	SWPB	スワップバイト	値のバイトを再配列する。
論理	AND	ビット単位の論理積	ビット単位の論理積演算 (AND) 操作を実行する。
	NOT	ビット単位の論理否定	ビット単位の論理否定演算 (NOT) 操作を実行する。
	OR	ビット単位の論理和	ビット単位の論理和演算 (OR) 操作を実行する。
	XOR	ビット単位の排他的論理和	ビット単位の排他的論理和演算 (XOR) 操作を実行する。
プログラム制御	JMP	ジャンプ	ロジックのスキャンが同じルーチン内のラベル付き位置にジャンプする。
	LBL	ラベル	JMP 命令のターゲット位置を識別する。
	JSR	サブルーチンジャンプ	別のルーチンにジャンプする。
	RET	リターン	サブルーチンの結果を返す。
	SBR	サブルーチン	JSR 命令によってサブルーチンに渡されるデータを受入れる。
	TND	テンポラリエンド	ルーチン実行を中断するテンポラリエンドをマークする。
	MCR	マスタ・コントロール・リセット	ロジックの 1 つのセクション内のすべてのラングが False(0) 状態で実行されることを強制する。
	AFI	常時 False 命令	ラングを False(0) に強制する (実行するラング状態)。
	NOP	動作なし	ロジックにプレイスホルダを挿入する。
	EVENT(3)	イベントタスクのトリガ	イベントタスク実行のトリガをかける。
算術 / 演算	ADD	加算	2 つの値を加算する。
	CPT (2)	演算	式で定義された算術演算を実行する。
	SUB	減算	1 つ目の値から 2 つ目の値を減算する。
	MUL	乗算	2 つの値を掛ける。
	DIV	除算	1 つ目の値を 2 つ目の値で割る。
	MOD	剰余	1 つ目の値を 2 つ目の値で割った後の剰余を求める。
	SQR	平方根	値の平方根を計算する。
	NEG	符号変更	値の符号を反対にする。
	ABS	絶対値	値の絶対値を求める。
I/O	GSV(4)	システム値の取得	コントローラのステータス情報を取得する。
	SSV(4)	システム値の設定	コントローラのステータス情報を設定する。

(1) 安全ルーチンで COP 命令を使用する場合、Length (長さ) オペランドは定数であり、ソースと宛先の長さが同じであることを確認する必要があります。
(2) SIN、COS、TAN などの高度なオペランドは、安全ルーチンではサポートされません。
(3) イベント命令は標準タスクのスキャンのトリガをかける。
(4) GSV 命令と SSV 命令を使用する際の特別な考慮事項については、『ControlLogix 5580 and GuardLogix 5580 Controllers User Manual』(Pub. No. 1756-UM543)、または『CompactLogix 5380 および Compact GuardLogix 5380 コントローラ ユーザーズマニュアル』(Pub. No. 5069-UM001) を参照してください。

表 9 - ドライブ安全命令(1)

ニーモニック	名称	説明
SS1	安全停止 1	安全停止 1 命令は、指定の速度ランプに従って、速度 0 への軸の減速をモニタし、その出力 (01) を制御して安全トルクオフ (STO) を開始する。
SS2	安全停止 2	安全停止 2 命令は、設定された範囲内でのモータ減速を開始およびモニタし、モータが動作停止になることを確認する。停止すると、SS2 は引き続きモータの動作停止をモニタする。
SOS	安全動作停止	安全動作停止命令は、モータまたは軸の速度または位置をモニタし、静止状態の速度または位置からの偏差が定義された値を超えていないことを確認する。
SLS	安全制限速度	安全制限速度命令は、軸の速度をモニタし、命令のアクティブ制限入力値を超える場合は、SLS 制限出力を設定する。
SLP	安全制限位置	安全制限位置命令は、モータまたは軸の位置をモニタして、位置が定義された制限値から外れていないことを確認する。
SDI	安全方向	安全方向命令は、モータまたは軸の位置をモニタし、意図しない方向への、定義した量よりも大きい移動を検出する。
SBC	安全ブレーキ制御	安全ブレーキ制御 (SBC) 命令: • ブレーキを作動させる安全出力を制御する。 • ブレーキとトルクオフ要求出力の間のタイミングを設定する。 • ブレーキフィードバックと I/O ステータスをモニタする。
SFX	安全フィードバックスケーリング	安全フィードバックインターフェイス命令は、モータの速度と位置のフィードバックをドライブモジュールからユーザスケーリング単位に変換する。絶対参照位置も定義する。

(1)　モーション安全命令は、GuardLogix 5580 コントローラ、Compact GuardLogix 5380、および Kinetix 5700 ERS4 ドライブを Studio 5000 Logix Designer アプリケーション (バージョン 31 以降) と共に使用する場合に利用できます。

重要　Kinetix 5500 ドライブ、Kinetix 5700 サーボドライブ、または PowerFlex 527 ドライブでモーション直接コマンドを使用する場合は、安全アプリケーションでのこの機能の使用法について、ドライブのユーザーマニュアルを参照してください。

- Kinetix 5500 Servo Drives User Manual (Kinetix 5500 サーボドライブユーザーズマニュアル) (Pub. No. 2198-UM001)
- Kinetix 5700 Servo Drives User Manual (Kinetix 5700 サーボドライブユーザーズマニュアル) (Pub. No. 2198-UM002)
- PowerFlex 527 可変周波数 AC ドライブ ユーザーズマニュアル (Pub. No. 520-UM002)

詳細は、以下の資料を参照してください。

表 10 - 参考資料

マニュアル名	説明
GuardLogix Safety Application Instructions Safety Set Reference Manual (Pub. No. 1756-RM095)	安全アプリケーション命令を詳細に説明する。
Logix5000 Controllers General Instructions Reference Manual (Logix5000 コントローラ汎用インストラクション・セット・リファレンス・マニュアル) (Pub. No. 1756-RM003)	汎用命令、モーション命令、およびプロセス命令を含む Logix5000 命令セットに関する説明。

安全アドオン命令の作成と使用

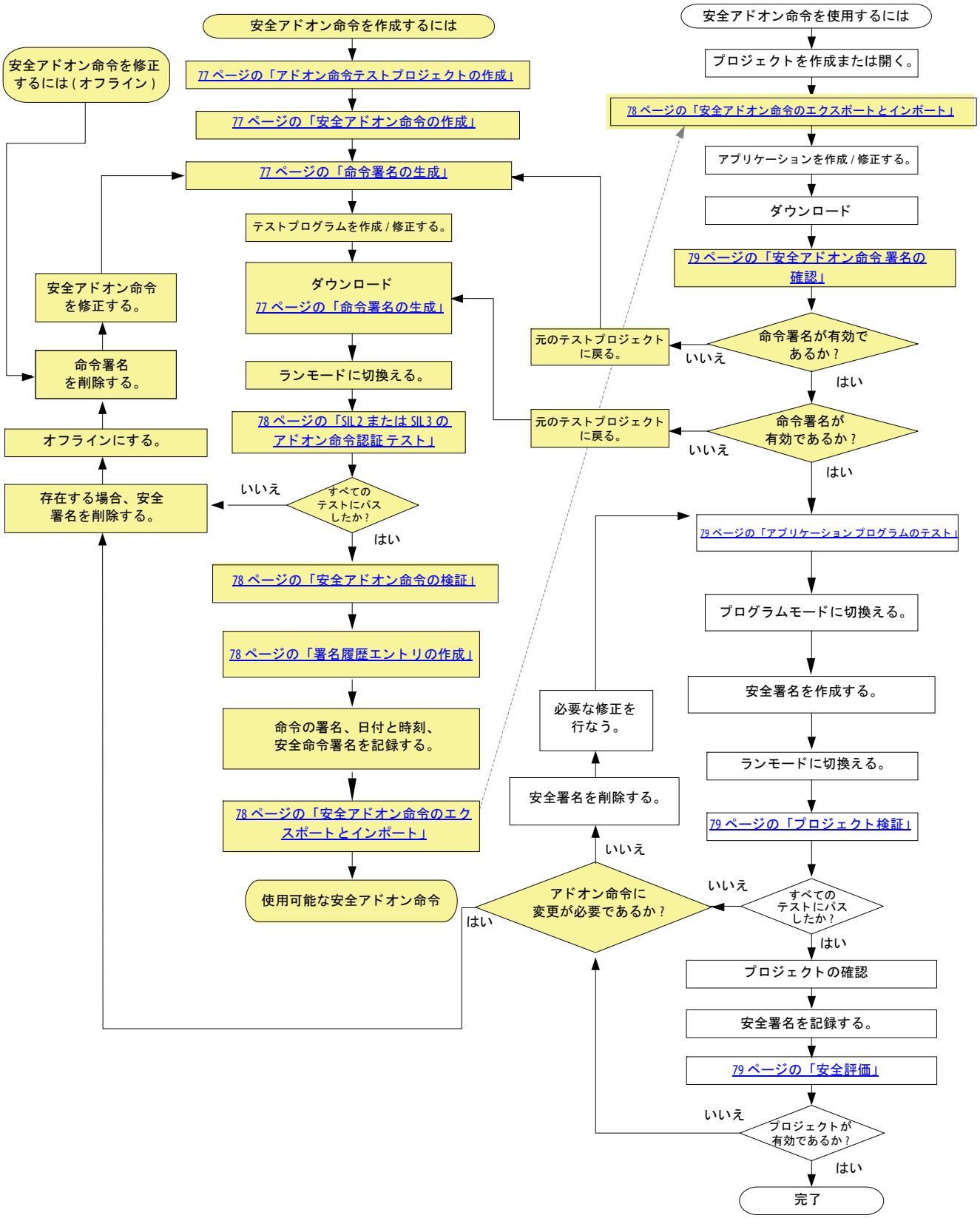
項目	参照ページ
アドオン命令テストプロジェクトの作成	77
安全アドオン命令の作成	77
命令署名の生成	77
安全命令署名	77
SIL 2 または SIL 3 の アドオン命令認証 テスト	78
安全アドオン命令の検証	78
署名履歴エントリの作成	78
安全アドオン命令のエクスポートとインポート	78
安全アドオン命令 署名の確認	79
アプリケーション プログラムのテスト	79
プロジェクト検証	79
安全評価	79

Studio 5000 Logix Designerアプリケーションでは、安全アドオン命令を作成できます。安全アドオン命令を使用して、よく使用する安全ロジックを1つの命令にカプセル化し、モジュールにして再利用しやすくすることができます。

安全アドオン命令は、整合性の高いアドオン命令の命令署名を使用してSIL 3を含む安全関連の機能でSIL 3安全命令署名も使用します。-

76ページの図20に、安全アドオン命令を作成して、それを安全アプリケーションプログラムで使用するために必要な手順を示します。色つきの項目は、アドオン命令に固有の手順です。これらの項目の説明については、リンク先をご覧ください。

図20 - 安全アドオン命令の作成と使用のフローチャート



アドオン命令テストプロジェクトの作成

安全アドオン命令の作成とテストには、固有のテストプロジェクトを作成する必要があります。このプロジェクトは、予期しない影響を最低限に抑えるため個別の専用プロジェクトにしてください。

54ページの「プロジェクトの作成」に記載されたプロジェクトガイドラインに従ってください。

安全アドオン命令の作成

アドオン命令の作成方法については、『Logix5000 Controllers Add-On Instruction Programming Manual』(Pub. No. 1756-PM010)を参照してください。

命令署名の生成

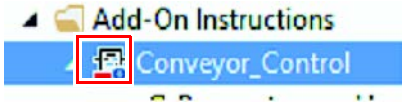
命令署名を使用して、命令が修正されたかどうかを素早く判断できます。各アドオン命令で、それぞれ個別の署名を使用できます。命令署名は、アドオン命令が安全関連の機能で使用されるときに必要で、規制産業で必要になる場合があります。アプリケーションに高いレベルの整合性が必要な場合に命令署名を使用します。

命令署名は、その時点でのアドオン命令の内容を示すID番号とタイムスタンプで構成されます。

生成されると、命令署名はアドオン命令を封印し、署名が適切な場所にある間は命令の編集を防止します。防止される編集には、ラングコメント、タグの説明、作成済みのあらゆる命令の文書化が含まれます。命令が封印されると、以下の操作のみ実行できます。

- 命令署名のコピー
- 署名履歴エントリの作成またはコピー
- アドオン命令のインスタンス作成
- 命令のダウンロード
- 命令署名の削除
- レポートのプリント

命令署名が生成されると、Studio 5000 Logix Designerアプリケーションはシールアイコンと共に命令の定義を表示します。



重要　Studio 5000 Logix Designerアプリケーションのソース保護機能によってアドオン命令を保護する場合、命令署名を生成する前にソース保護を有効にします。

安全命令署名

封印された安全アドオン命令を初めてダウンロードすると、安全命令署名が自動的に生成されます。安全命令署名は、安全アドオン命令の実行特性を示すID番号です。

SIL 2またはSIL 3のアドオン命令認証テスト

安全アドオン命令テストは、意図しない影響を最低限に抑えられていることを確認するために、別の専用のアプリケーションで実行する必要があります。適切に設計されたテスト計画に従い、安全アドオン命令のユニットテストを実行する必要があります。このテストでは、全入力パラメータの有効および無効な範囲を含むロジックにより、すべての可能な実行パスを実施します。

安全アドオン命令の検証

命令が使用を認可されるためには、独立した第三者機関によって安全アドオン命令を検証する必要がある可能性があります。機能安全認可の取得には、独立した第三者機関による検証が必要な場合があります。

署名履歴エントリの作成

署名履歴は、将来参照するための記録になります。署名履歴エントリは、命令署名、ユーザ名、タイムスタンプ値、ユーザ定義の説明で構成されます。最大6つの履歴エントリを保存できます。署名履歴エントリは、オフラインで作成してください。

ヒント　**Studio 5000 Logix Designerアプリケーションの署名リストレポートは、命令署名、タイムスタンプ、安全命令署名をプリントします。レポートをプリントするには、コントローラオーガナイザでAdd-On Instructionを右クリックしてから、Print → Signature Listingを順番に選択します。**

安全アドオン命令のエクスポートとインポート

安全アドオン命令をエクスポートする場合、すべての参照されたアドオン命令とユーザ定義のタイプを同じエクスポートファイルに含めるオプションを選択します。参照されたアドオン命令を含めることで、署名の保存が容易になります。

アドオン命令をインポートするときは、以下のガイドラインに従ってください。

- 安全アドオン命令を標準コントローラプロジェクトにインポートすることはできません。
- 安全ロックされた安全プロジェクトまたは安全署名のあるセーフティコントローラのプロジェクトに、安全アドオン命令をインポートすることはできません。
- 安全アドオン命令をオンラインでインポートすることはできません。
- 命令署名を含むアドオン命令を、参照されるアドオン命令またはユーザ定義データタイプが使用できないプロジェクトにインポートする場合、必要に応じて署名を削除します。

詳細は、『Import/Export Project Components Programming Manual』(Pub. No. 1756-PM019)を参照してください。

安全アドオン命令署名の確認

インポートされた安全アドオン命令を含むアプリケーションプロジェクトをダウンロードした後、命令署名値、日付およびタイムスタンプ、安全命令署名値は、安全アドオン命令をエクスポートする前に記録された元の値と比較する必要があります。値が一致すれば、安全アドオン命令は有効であり、アプリケーションの検証に進むことができます。

アプリケーションプログラムのテスト

この手順は、ランモードとプログラムモードの任意の組合せ、オンラインまたはオフラインのプログラム編集、アップロードとダウンロード、およびアプリケーションを正しく実行させるために必要な非公式テストから構成されます。

プロジェクト検証

安全システムを含むアプリケーションのエンジニアリングテストを実行します。

詳細は、55ページの「プロジェクトの検証」を参照してください。

安全評価

システムが動作を認可されるためには、独立した第三者機関によって安全システムを検証する必要がある可能性があります。機能安全認可の取得には、独立した第三者機関による検証が必要な場合があります。

安全評価の詳細は、『Machinery SafeBook 5』を参照してください。

Notes:

応答時間

項目	参照ページ
コネクション応答 時間制限	81
システム応答時間	83
Logix システムの応答時間	83
Logix 応答時間 コンポーネントに影響する要因	85

コネクション応答時間制限

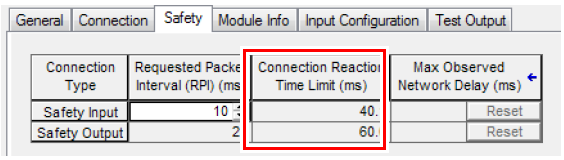
コネクション応答時間制限は、対応するコネクションの安全パケットの最大寿命です。コンシューマデバイスに使用されるデータの寿命がコネクション応答時間制限を超えると、コネクションフォルトが発生します。次の式は、コネクション応答時間制限を決定します。

入力コネクション応答時間制限 =
入力RPI x [タイムアウトマルチプライヤ + ネットワーク遅延マルチプライヤ]

出力コネクション応答時間制限 =
安全タスク時間 x [タイムアウトマルチプライヤ + ネットワーク遅延マルチプライヤ - 1]

コネクション応答時間制限は、Module Properties ダイアログボックスの Safety タブに表示されます。

図21 - コネクション応答時間制限



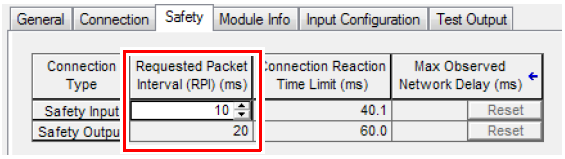
要求パケット間隔(RPI)の指定

RPIは、コネクションを介してデータが更新された時に期間を指定します。例えば、入力モジュールは、割付けたRPIでデータを生成します。

安全入力コネクションでは、Module Propertiesダイアログボックスの Safetyタブで RPIを設定できます。RPIは、1msec単位で入力されます。

コネクション応答時間制限は、RPIがStudio 5000 Logix Designerアプリケーションで変更されるとすぐに調整されます。

図22 - 要求パケット間隔)



安全出力コネクションの場合、RPIは安全タスク時間で固定です。対応するコネクション応答時間制限が適切でないときは、Safety Task Propertiesダイアログで安全タスク期間を調整できます。

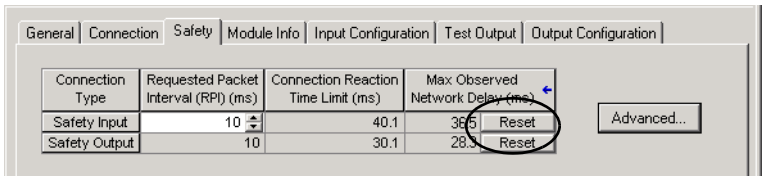
安全タスク時間については、15ページの「システム応答時間」を参照してください。

標準的なアプリケーションでは、通常は、4 x RPIの入力コネクションのデフォルトのコネクション応答時間制限、および3 x RPIの出力コネクションのデフォルトのコネクション応答時間制限で充分です。複雑な要件の場合は、86ページで説明するようにAdvancedボタンを使用してConnection Reaction Time Limit (コネクション応答時間制限)パラメータを変更します。

Maximum Observed Network Delayの表示

Maximum Observed Network Delay (最大監視ネットワーク遅延) は、Module Propertiesダイアログボックスの Safetyタブに表示されます。オンライン時に、Resetをクリックして Maximum Observed Network Delayをリセットします。

図23 - Maximum Observed Network Delayのリセット

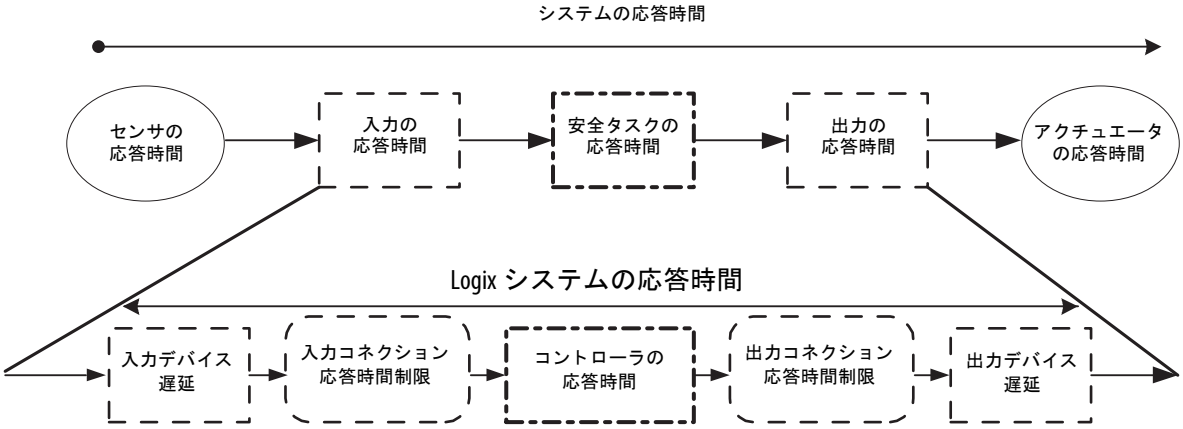


システム応答時間

任意の制御チェーンのシステムの応答時間(詳細は15ページの「システム応答時間」を参照)を求めるには、安全チェーン内のすべてのコンポーネントの応答時間を合計する必要があります。

システムの応答時間 = センサの応答時間 + Logix システムの応答時間 + アクチュエータの応答時間

図24 - システムの応答時間



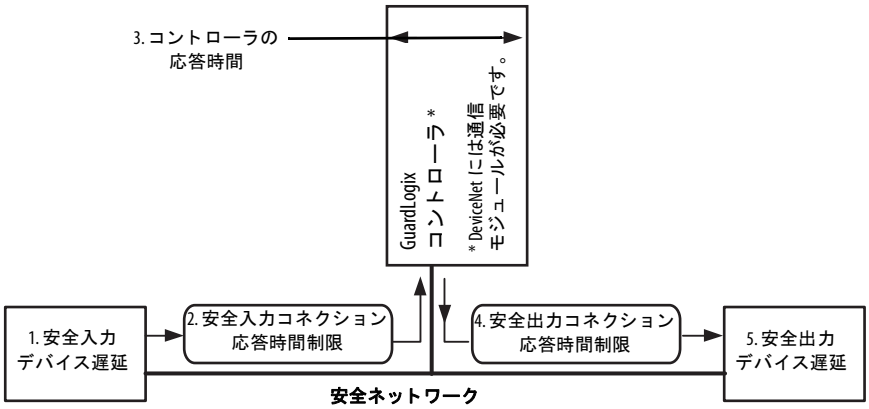
Logixシステムの応答時間

以降のセクションでは、単純な入力ロジック出力チェーンと、ログチェーンでプロデューサ/コンシューマ安全タグを使用するより複雑なアプリケーションのLogixシステム応答時間の計算方法を説明します。

単純な入力ロジック出力チェーン

ここでは、単純な入力-ロジック-出力に対するLogix システムの応答時間について説明します。

図25 - 単純な入力-ロジック-出力に対するLogixシステム応答時間(最悪の場合)



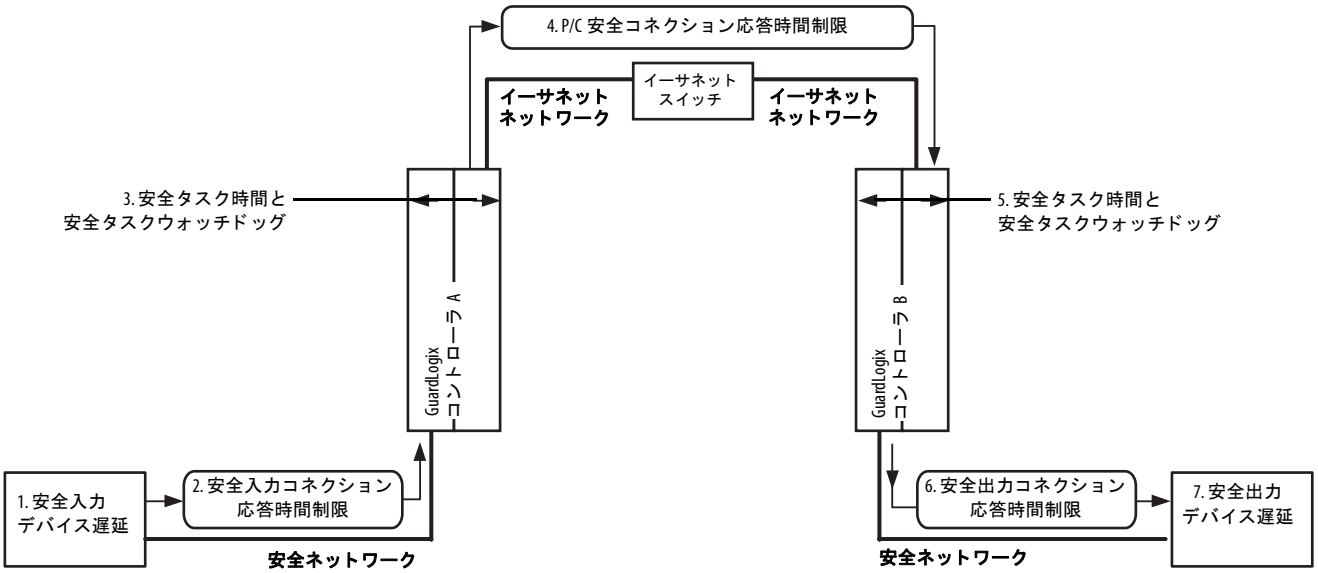
単純な入力-ロジック-出力チェーンに対するLogixシステムの応答時間は、以下の5つのコンポーネントで構成されます。

1. 安全入力デバイスの応答時間 + 入力遅延時間 (該当する場合)
2. 安全入力コネクション応答時間制限
   (Studio 5000 Logix Designer アプリケーションの Module Properties ダイアログボックスから読取られ、安全入力デバイスコネクションの RPI の倍数になります。)
3. コントローラの応答時間 (15 ページの「安全タスクの応答時間」を参照)
4. 安全出力コネクション応答時間制限
   (Logix Designer アプリケーションの Module Properties ダイアログボックスから読取られ、安全タスク時間の倍数になります。)
5. 安全出力デバイスの応答時間

プロデューサ/コンシューマ安全タグを使用するロジックチェーン

このセクションでは、単純な入力コントローラAロジック コントローラB出力に対するLogix システムの応答時間について説明します。

図26 - 入力コントローラAロジック コントローラBロジック-出力チェーンのLogix システム応答時間



入力-コントローラAロジック-コントローラ Bロジック-出力チェーンに対するLogixシステムの応答時間は、以下の7つのコンポーネントで構成されます。

1. 安全入力デバイスの応答時間 + 入力遅延時間 (該当する場合)
2. 安全入力コネクション応答時間制限
3. コントローラ A の安全タスク時間 + 安全タスクウォッチドッグ時間

4. プロデューサ / コンシューマ安全応答時間制限
   (コンシューマ・タグ・コネクションの Safety タブから読取られます。)
5. コントローラ B の安全タスク時間 + 安全タスクウォッチドッグ時間
6. 安全出力コネクション応答時間制限
7. 安全出力デバイスの応答時間

Logix応答時間コンポーネントに影響する要因

前のセクションで説明したLogixの応答時間コンポーネントに影響する可能性のある要因は多数あります。

表 11 - Logix システム応答時間に影響を与える要因

応答時間コンポーネント	影響を与える要因
入力デバイス遅延	入力デバイスの応答時間
	各入力チャネルのオン - オフおよびオフ - オンの遅延設定 (該当する場合)
安全入力コネクション応答時間制限	以下の入力デバイスの設定 : • 要求パケット間隔(RPI) • タイムアウトマルチプライヤ • ネットワーク遅延マルチプライヤ
	ネットワーク通信トラフィックの量(1)
	システムの EMC 環境 (1)
安全タスク時間と安全タスクウォッチドッグ	安全タスク時間
	安全タスクウォッチドッグの設定
	安全タスクの命令の数と実行時間(2)
	安全タスク実行に優先する最優先的なタスク (2)
プロデューサ / コンシューマ安全コネクション応答時間制限	以下のコンシューマタグの設定 : • 要求パケット間隔(RPI) • タイムアウトマルチプライヤ • ネットワーク遅延マルチプライヤ
	ネットワーク通信トラフィックの量 (1)
	システムの EMC 環境 (1)
出力コネクション応答時間制限	安全タスク時間
	以下の出力デバイスの設定 : • タイムアウトマルチプライヤ • ネットワーク遅延マルチプライヤ
	ネットワーク通信トラフィックの量 (1)
	システムの EMC 環境 (1)
出力モジュールの遅延	出力モジュールの応答時間

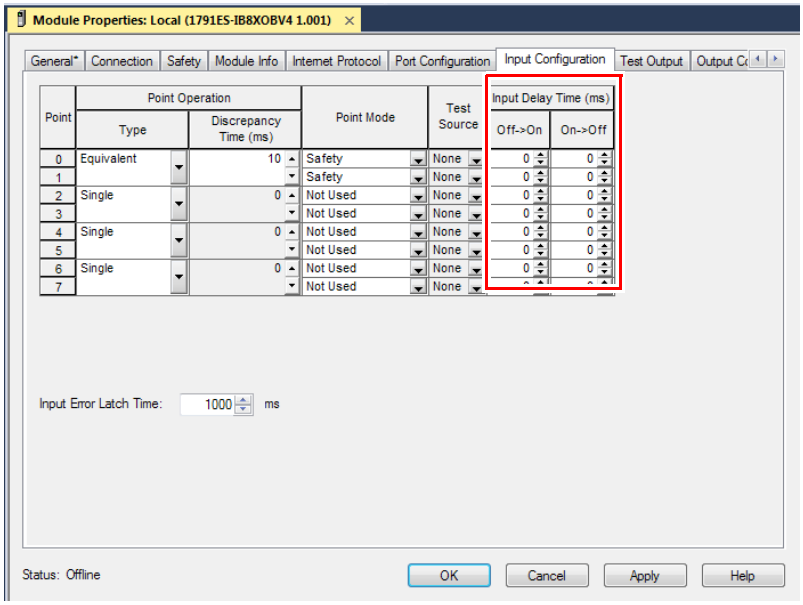
(1) ネットワークトラフィックと EMC は、タイムアウトマルチプライヤとネットワーク遅延マルチプライヤに使用できる値の下限値を作成します。
(2) 安全タスクおよびコントローラ内のその他の優先的タスクに含まれる命令は、安全タスク時間と安全タスクウォッチドッグで使用できる値の下限値を作成します。

以降のセクションでは、これらの多くの要素のデータや設定にアクセスする方法について説明します。

Guard I/O 入力モジュールの遅延時間設定の構成

以下の手順に従って、Studio 5000 Logix Designerアプリケーションで入力モジュールの遅延時間を構成してください。

1. 構成ツリーで Guard I/O モジュールを右クリックし、Properties を選択します。
2. Input Configuration タブをクリックします。
3. アプリケーションの要件に応じて入力遅延時間を調整します。



入力および出力安全コネクション応答時間制限の構成または表示

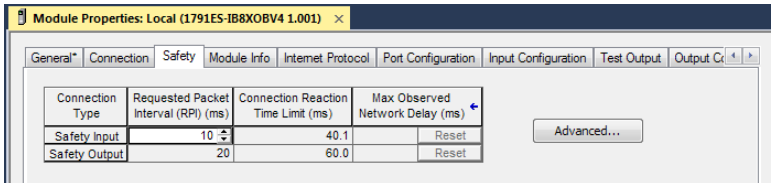
次の3つの値は、コネクション応答時間制限(CRTL)を定義します。

値	説明
要求パケット間隔 (RPI)	入力と出力のパケットが配線 (ネットワーク) 上に配置される頻度です。
タイムアウトマルチプライヤ	タイムアウトまでの再試行回数です。
ネットワーク遅延マルチプライヤ	ネットワーク上の既知の遅延を考慮する。このような遅延が発生した場合に、このパラメータを使用してタイムアウトを回避できる。

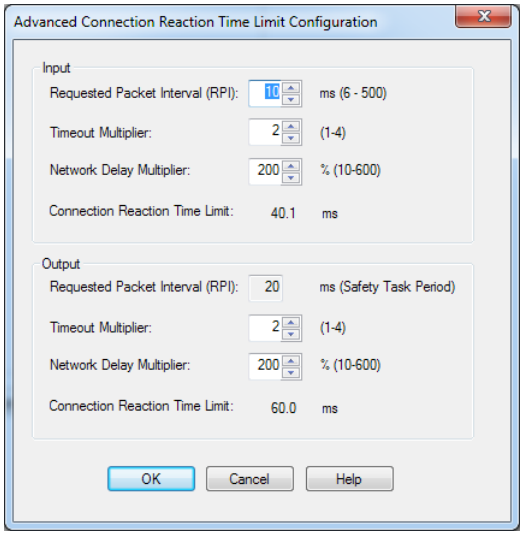
これらの値を調整すると、コネクション応答時間制限を調整できます。CRTL以内に有効なパケットが受信されないと、安全コネクションはタイムアウトになり、入力データと出力データは安全状態になります。

以下の手順に従って、これらの設定を確認または構成してください。

1. 構成ツリーで安全I/Oデバイスを右クリックし、Propertiesを選択します。
2. Safety タブをクリックします。



3. Advanced をクリックして、Advanced Connection Reaction Time Limit ダイアログボックスを開きます。



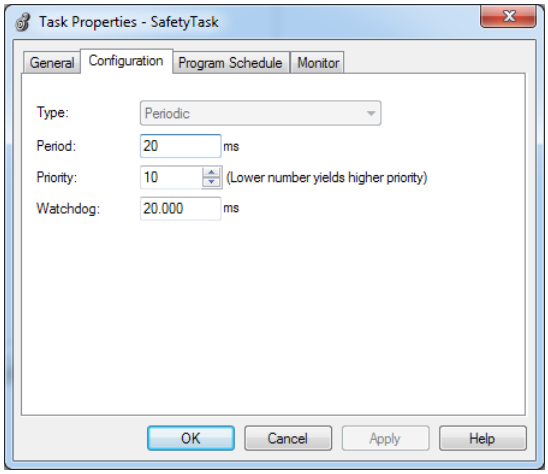
重要　タイムアウトマルチプライヤとネットワーク遅延マルチプライヤは、ネットワークの信頼性と性能のばらつきに対する耐性を提供する。

これらのパラメータの値を下げると誤作動の可能性が高くなるため、その際には注意して行なってください。

安全タスク時間およびウォッチドッグの構成

安全タスクは、周期的/時限タスクです。Logix Designerプロジェクトで、Task Properties - Safety Taskダイアログボックスからタスク時間、タスクプライオリティと、およびウォッチドッグ時間を選択します。

安全タスク時間とウォッチドッグ時間の設定にアクセスするには、Safety Taskを右クリックし、Propertiesを選択します。

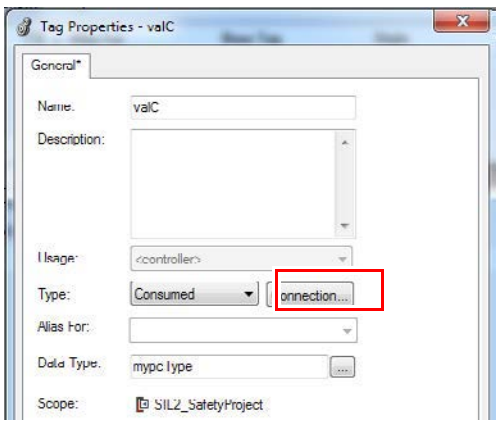


安全タスクウォッチドッグがプライオリティの高いタスクによってタスク割込みが発生しているかどうかをモニタするため、安全タスクのプライオリティは安全には関連しません。

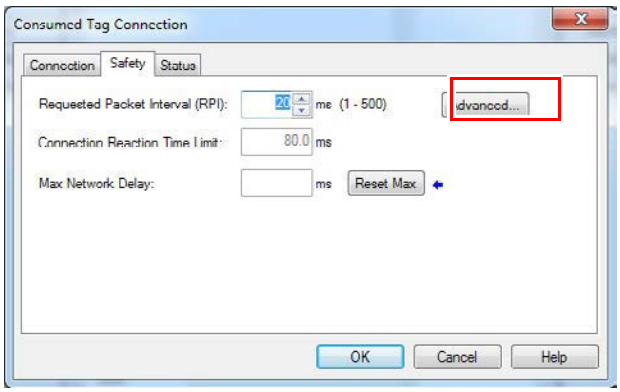
プロデューサタグ/コンシューマタグのデータへのアクセス

以下の手順に従って、安全タグのコネクションデータを確認または構成してください。

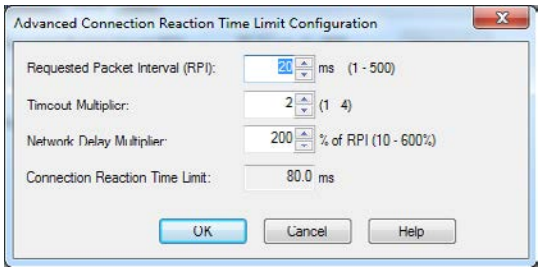
1. 構成ツリーで Controller Tags を右クリックし、Edit tags を選択します。
2. タグエディタでタグの名前を右クリックし、Edit Properties を選択します。
3. Connection をクリックします。



4. Safety タブで Advanced をクリックします。



5. 現在の設定は、Advanced ダイアログボックスで表示または編集できます。



詳細は、次の資料を参照してください。

- ControlLogix 5580 and GuardLogix 5580 Controllers User Manual (Pub. No. 1756-UM543)
- CompactLogix 5380 および Compact GuardLogix 5380 コントローラ ユーザーズマニュアル(Pub. No. 5069-UM001)

Notes:

GuardLogix安全アプリケーションのチェックリスト

項目	参照ページ
GuardLogix コントローラシステムのチェックリスト	92
安全入力のチェックリスト	93
安全出力のチェックリスト	94
安全アプリケーションプログラム開発のチェックリスト	95

この付録のチェックリストは、GuardLogix安全アプリケーションの計画、プログラム、および開始のために必要です。これらは、計画のガイドとして使用することができ、また、検証テスト中に使用できます。計画ガイドとして使用しているときは、チェックリストは計画の記録として保存できます。

以降のページのチェックリストは安全に関する注意事項の例であり、検証項目の完全なリストを意図しているわけではありません。特定の安全アプリケーションには、追加の安全要件がある可能性があります。そのために、チェックリストにはスペースを取ってあります。

ヒント　**チェックリストは、後で使用する必要があるときのために、コピーしてお使いください。**

GuardLogix コントローラシステムのチェックリスト

GuardLogix システムのチェックリスト				
会社名				
住所				
安全機能の定義				
番号	**システム要件**	**チェック**		**コメント**
		はい	**いいえ**	
1	以下の Web サイトにリストされた、SIL 認可されたコンポーネントのみを対応するファームウェアリリースで使用していますか？ http://www.rockwellautomation.com/global/certification/safety.page	☐	☐	
2	安全機能ごとに、システムの安全応答時間を計算しましたか？	☐	☐	
3	システムの応答時間に、ユーザ定義の安全タスク・プログラム・ウォッチドッグ (ソフトウェアウォッチドッグ) 時間と安全タスクレート / 期間の両方を含みましたか？	☐	☐	
4	システム応答時間がプロセスの安全時間に対して適切に対応していますか？	☐	☐	
5	各安全機能の確率 (作動要求時機能失敗確率 /PFH) 値が計算されていますか？	☐	☐	
6	すべての適切なプロジェクト検証テストを実行しましたか？	☐	☐	
7	システムがどのようにフォルトを処理できるかを決定しましたか？	☐	☐	
8	安全システム内のネットワークごとに固有の SNN がありますか？	☐	☐	
9	各安全デバイスを正しい SNN で構成しましたか？	☐	☐	
10	安全署名を生成しましたか？	☐	☐	
11	将来の比較のために安全署名をアップロードおよび記録しましたか？	☐	☐	
12	ダウンロードの後、コントローラの安全署名が、記録された安全署名と一致することを確認しましたか？	☐	☐	
13	オンライン編集の際に、システムの安全度を保持するための別の手段がありますか？	☐	☐	
14	93 ページと 94 ページに記載された SIL 入力と出力の使用に関するチェックリストを考慮しましたか？	☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

安全入力のチェックリスト

プログラミングまたはスタートアップ時には、システム内の安全入力をすべて1つずつ記入するために個別のチェックリストを使用してください。これは、要件が完全で明確に実装されたことを確認する唯一の方法です。このチェックリストは、アプリケーションプログラムへの外部配線の接続用の資料として使用することもできます。

GuardLogix システムの入力チェックリスト

会社名

住所

安全機能の定義

SIL 入力チャネル

番号	入力デバイスの要件	チェック		コメント
		はい	いいえ	
1	適合可能な安全規格を満たすために、インストレーションインストラクション (取付け手順書) と注意事項に従いましたか ?	☐	☐	
2	システムとデバイスでプロジェクト検証テストを実行しましたか ?	☐	☐	
3	制御、診断、アラームの機能をアプリケーションロジックで順番に実行しましたか ?	☐	☐	
4	各デバイスの構成をアップロードして、構成ツールで送信された構成と比較しましたか ?	☐	☐	
5	デバイスの配線は目標基準と必要な安全基準に準拠していますか ?	☐	☐	
6	センサが入力の電気的な仕様に対応していることを確認しましたか ?	☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

安全出力のチェックリスト

プログラミングまたはスタートアップ時には、システム内の安全出力をすべて1つずつ記入するために、個別の要件チェックリストを使用してください。これは、要件が完全で明確に実装されたことを確認する唯一の方法です。このチェックリストは、アプリケーションプログラムへの外部配線の接続用の資料として使用することもできます。

GuardLogix システムの出力チェックリスト				
会社名				
住所				
安全機能の定義				
SIL 出力チャネル				
番号	**出力デバイスの要件**	**チェック**		**コメント**
		はい	**いいえ**	
1	適合可能な安全規格を満たすために、インストレーションインストラクション (取付け手順書) と注意事項に従いましたか ?	☐	☐	
2	デバイスでプロジェクト検証テストを実行しましたか ?	☐	☐	
3	各デバイスの構成をアップロードして、構成ツールで送信された構成と比較しましたか ?	☐	☐	
4	テスト出力を安全出力として使用しないことを確認しましたか ?	☐	☐	
5	デバイスの配線は目標基準と必要な安全基準に準拠していますか ?	☐	☐	
6	アクチュエータが出力の電気的な仕様に対応していることを確認しましたか ?	☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

安全アプリケーションプログラム開発のチェックリスト

以下のチェックリストを使用して、安全アプリケーションプログラムの作成および修正時に安全を確実に保持してください。

GuardLogix アプリケーションプログラム開発のチェックリスト

会社名	
住所	
プロジェクト定義	

番号	アプリケーションプログラムの要件	チェック		コメント
		はい	いいえ	
1	バージョン 31 以降の(1)Studio 5000 Logix Designer アプリケーション、(2)GuardLogix システム・プログラミング・ツールを使用していますか？	☐	☐	
2	安全アプリケーションプログラムの作成中に 49 ページの第 6 章のガイドラインに従いましたか？	☐	☐	
3	安全アプリケーションプログラムには、ラダーダイアグラムだけが含まれていますか？	☐	☐	
4	安全アプリケーションのプログラミングに適合するように、安全アプリケーションプログラムは 71 ページの付録 A に記載された命令のみを含んでいますか？	☐	☐	
5	安全アプリケーションプログラムは、安全タグと標準タグを明確に区別していますか？	☐	☐	
6	安全ルーチンには安全タグのみを使用していますか？	☐	☐	
7	安全ルーチンが標準タグを読み書きしていないことを確認しましたか？	☐	☐	
8	安全タグが標準タグにエイリアスされて (または逆) いないことを確認しましたか？	☐	☐	
9	各安全出力タグが適切に構成され、物理的な出力チャネルに接続されていますか？	☐	☐	
10	すべてのマップされたタグが安全アプリケーションロジックで条件付けられていることを確認しましたか？	☐	☐	
11	フォルトルーチンがモニタするプロセスパラメータを定義しましたか？	☐	☐	
12	すべての安全アドオン命令を命令署名によって封印し、安全命令署名を記録しましたか ?1 回限り使用するアドオン命令ではオプション。必要なアドオン命令は、異なるアプリケーションで再使用されます。	☐	☐	
13	独立した安全レビューアが、必要に応じてプログラムをレビューしましたか？	☐	☐	
14	レビューを文書化し、署名しましたか？	☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

(1) Studio 5000 Logix Designer アプリケーションのバージョン 31 以降は、GuardLogix 5580 および Compact GuardLogix 5380 コントローラをサポートしています。

(2) 最新のソフトウェアとファームウェアを入手するには、ロックウェル・オートメーションの製品互換性およびダウンロードセンター (PCDC) のサポート Web サイトを参照してください。http://www.rockwellautomation.com/global/support/pcdc.page

Notes:

GuardLogixシステムの安全データ

項目	参照ページ
耐用年数	97
安全データ	97
製品故障率	98

以下の例は、GuardLogix 1oo1 SIL 2システムまたは1oo2 SIL 3システムの安全機能の要求当たりの危険側不動作確率(PFD)値および単位時間当たりの危険故障確率(PFH)値を示しています。

安全I/OモジュールのPFD値とPFH値を含む安全データについては、該当するデバイスのマニュアルを参照してください。詳細は、8ページの「参考資料」を参照してください。

耐用年数

GuardLogixコントローラの耐用年数は20年です。

安全データ

PFD値とPFH値を含むI/Oデバイスの安全データについては、それらの製品のマニュアルを参照してください。

ロックウェル・オートメーションの機械安全製品のデータは、ライブラリファイルの形式で入手可能になり、Safety Integrity Software Tool for the Evaluation of Machine Applications (SISTEMA:機械設計評価用の安全統合ソフトウェアツール)で使用できます。

ライブラリファイルは、以下のWebサイトからダウンロードできます。
http://www.marketing.rockwellautomation.com/safety-solutions/ en/MachineSafety/ToolsAndDownloads/sistema_download

製品故障率

以下の表のデータは、20年以下のミッション時間に適用されます。

表 12 - 安全パラメータ

項目	GuardLogix 5580 コントローラと安全パートナ[2][3]	GuardLogix 5580 コントローラ[2][3]	Compact GuardLogix 5380 コントローラ[3]
安全機能アーキテクチャ(HFT)[1]	1	0	0
パーツなし / 影響なしの検出済み故障レート (λ_{NPED}) [時間]	2.80E-06	2.58E-06	4.04E-06
安全故障レート (λ_S) [故障件数 / 時間]	7.24E-07	6.61E-07	7.33E-07
危険故障レート (λ_D) [故障件数 / 時間]	7.10E-07	6.61E-07	7.33E-07
検出済み危険故障レート (λ_{DD}) [故障件数 / 時間]	7.10E-07	6.54E-07	7.26E-07
未検出の危険故障レート (λ_{DU}) [故障件数 / 時間]	7.38E-11	6.40E-09	7.23E-09
自動診断テスト間隔 (T_D) [時間]	—	<SRT	<SRT
耐用年数 [年]	20	20	20
決定論的能力 (SC)	3	3	3

(1) ここに指定されている HFT (ハードウェア・フォルト・トレランスは、内部 HFT です。
(2) これらの値は、製品を信頼性ブロックダイアグラム (RBD) で現す場合に使用する製品故障レートです。
(3) これらの製品故障レートは、最大周囲温度 60°C (140°F)、最大高度 2000m (6561.7 フィート) で有効です。Pub. No. 1756-TD001 と 1756-IN048 を参照してください。

表 13 - 安全計算

項目	GuardLogix 5580 コントローラと安全パートナ	GuardLogix 5580 コントローラ	Compact GuardLogix 5380 コントローラ
PFD_{ave} (ミッションタイム20年)	6.46E-06	5.61E-04	6.33E-04
PFH	7.38E-11	6.40E-09	7.23E-09
STR	4.23E-06	3.90E-06	5.50E-06
$MTTF_d$ [年]	160.82	172.74	155.66

安全計算の仮定:

- コンポーネントの故障レートは、製品の寿命を通して一定している。
- 検出されたすべての故障 (安全および危険) は、安全状態 (平均修理時間=0) となる。
- ミッション時間の例は10～20年。指定された耐用年数(20年)以内。プルーフテストの必要なし。

$$PFD_{ave} = (\lambda_{DU} + \lambda_{DD}) t_{CE}$$

$$STR = \lambda_S + \lambda_{DD} + \lambda_{NPED}$$

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$MTTF = \frac{1}{\lambda_D}$$

$$PFH = \lambda_{DU}$$

Studio 5000 Logix Designerアプリケーション バージョン31以降の 安全アプリケーション命令

項目	参照ページ
トリップシステムに対するオフ状態	99
コネクション・ステータス・データを使用したプログラムによるフォルトの起動	99

重要 この付録で詳しく説明した命令ではなく、一般的な安全アプリケーション命令(71ページの表5)を使用することをお奨めします。

トリップシステムに対するオフ状態

CIP Safetyコネクションフォルト状態が検出された場合、特定のコネクションに関連する安全入力値のすべてが安全状態に設定されます。Diverse Inputのペアを使用する場合、その入力の1つで値1を使用して安全機能を起動します。これには、(入力値が0のままでも)入力フォルトの発生時に安全機能が実行されるように、フォルト状態を評価する安全ロジックが必要になります。

コネクション・ステータス・データを使用したプログラムによるフォルトの起動

以下の図は、I/Oエラーのラッチとリセットに必要なアプリケーションロジックの例を示しています。これらの例は、入力専用モジュールに必要なロジックと、入力と出力の組合せモジュールを示しています。例では、Combined Status (組合せステータス) と呼ばれるI/Oモジュールの機能を使用しています。この機能は、1つのブーリアン変数内の全入力チャネルのステータスを表します。別のブーリアン変数は、全出力チャネルのステータスを表します。この方法によって、必要なI/O条件付けロジックの量が減少し、影響を受けたモジュールのすべての入出力チャネルのシャットダウンをロジックに強制します。

100ページの「入力フォルトのラッチとリセットのフローチャート」を使用して、さまざまなアプリケーション状況でロジックのどのラングが必要かを判断してください。101ページの「ラダーダイアグラムの例1」は、フォルト条件が存在する間、実際の入力タグ変数を上書きするロジックを示しています。入力エラーがラッチされている間、トラブルシューティングのために実際の入力状態が必要な場合は、102ページの「ラダーダイアグラムの例2」に示されたロジックを使用してください。このロジックは、アプリケーションロジックで使用される入力を示す内部タグを使用します。入力エラーがラッチされている間は、内部タグが安全状態に設定されます。入力エラーがラッチされていない間は、実際の入力値が内部タグにコピーされます。

103 ページの「出力フォルトのラッチとリセットのフローチャート」を使用して、103 ページの「ラダーダイアグラムの例 3」にあるアプリケーションロジックのどのラングが必要かを判断してください。

図27 - 入力フォルトのラッチとリセットのフローチャート

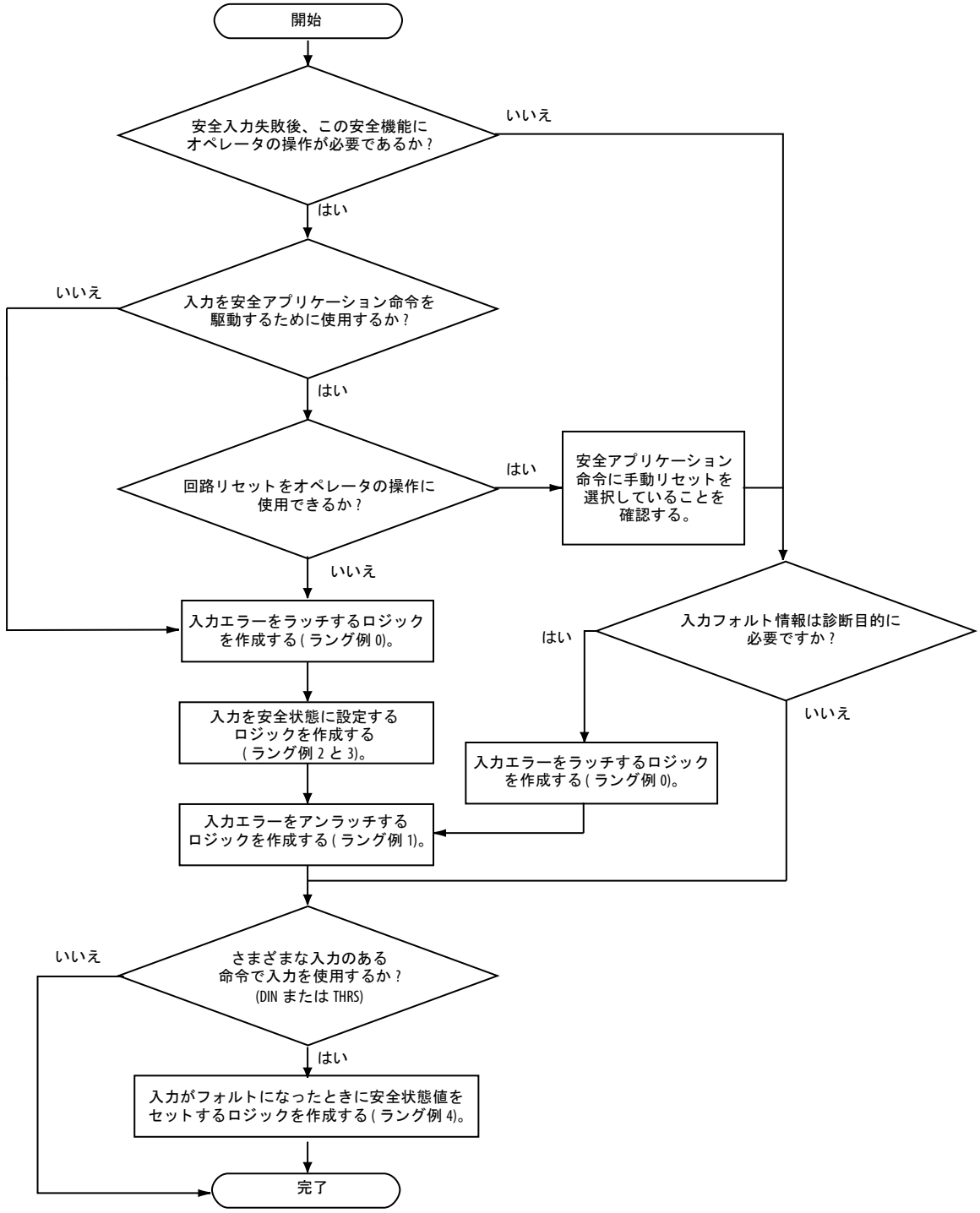


図28 - ラダーダイアグラムの例1

図29 - ラダーダイアグラムの例2

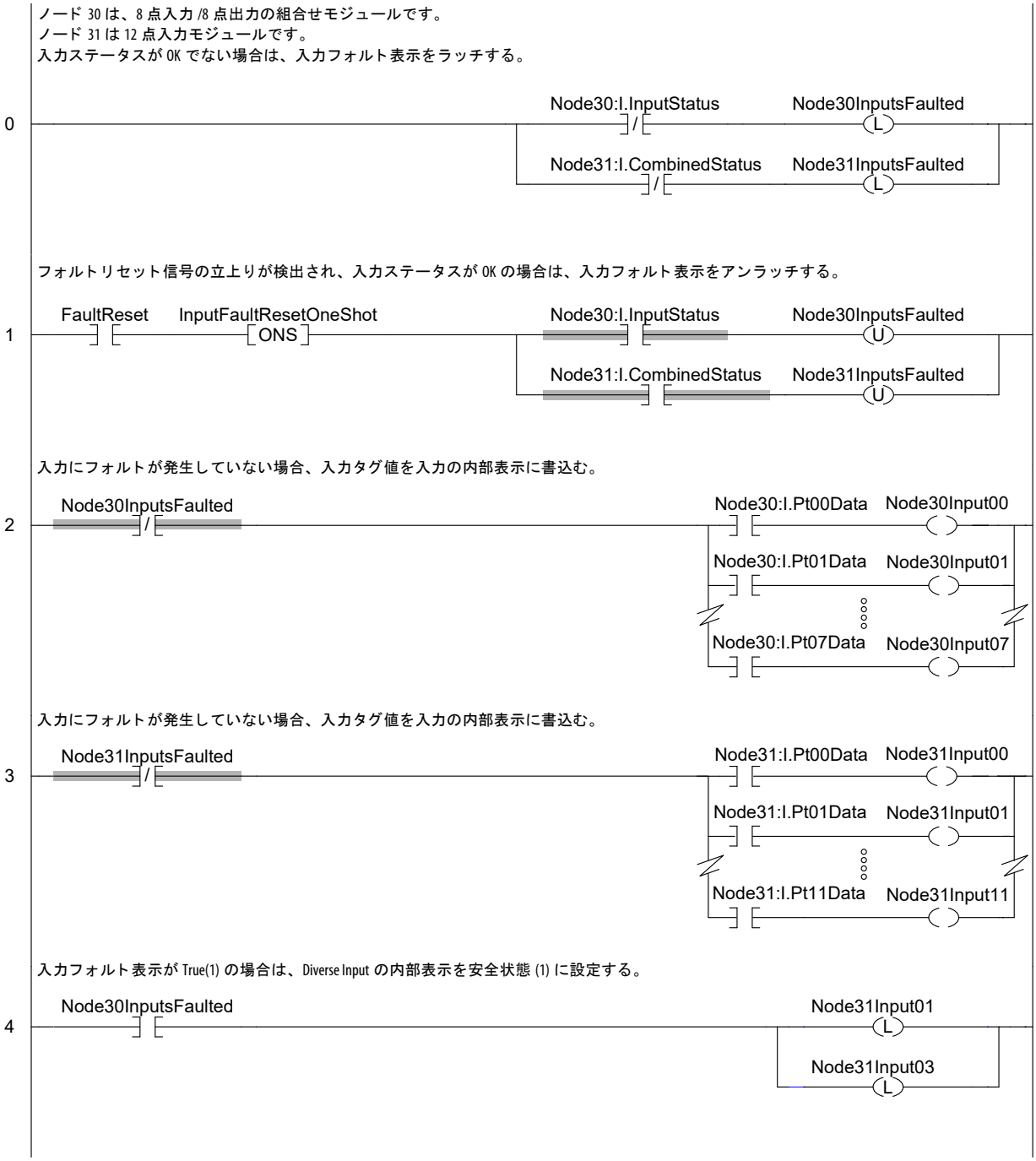


図30 - 出力フォルトのラッチとリセットのフローチャート

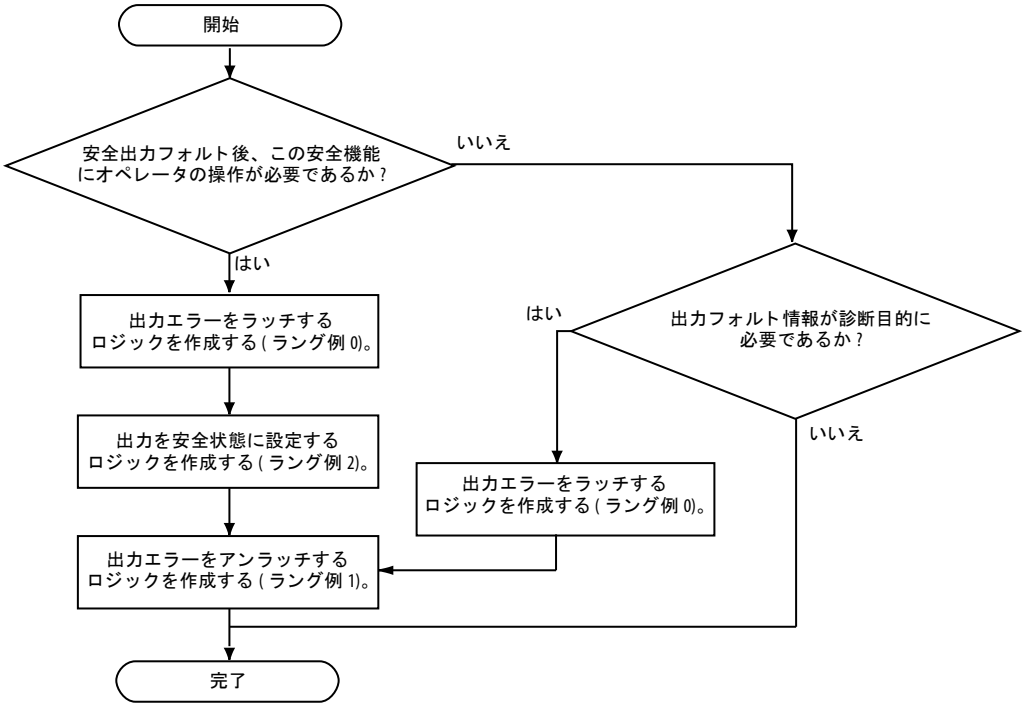
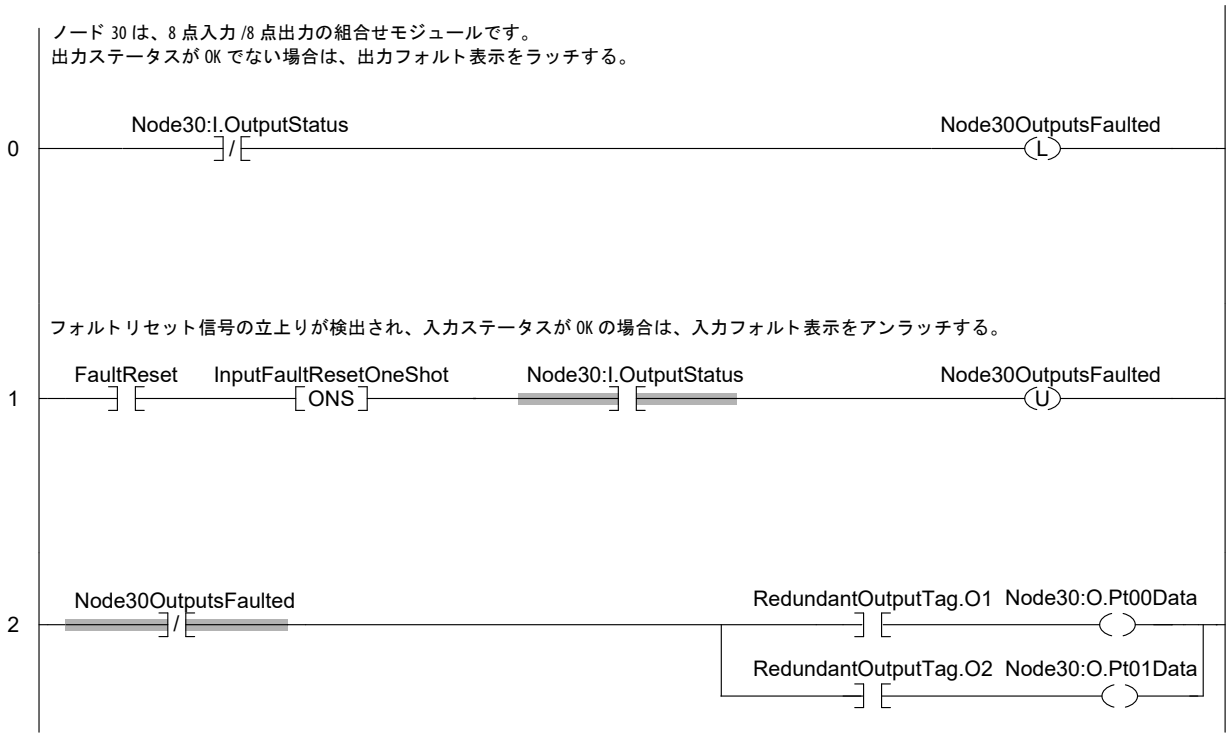


図31 - ラダーダイアグラムの例3



Notes:

このマニュアルでは、以下の用語と略語を使用します。ここに記載されていない用語の定義については、『Allen-Bradley Industrial Automation Glossary』(Pub. No. AG-7.1)を参照してください。

1oo1 (one-out-of-one) プログラマブル電子コントローラアーキテクチャを示します。1oo1 はシングル・チャネル・システムです。

1oo2 (one-out-of-two) プログラマブル電子コントローラアーキテクチャを示します。1oo2はデュアル・チャネル・システムです。

CIP (産業用共通プロトコル) Logix5000ベースの自動化システムで使用される産業用通信プロトコル。EtherNet/IP、ControlNet、DeviceNet通信ネットワークで使用します。

CIP Safety (産業用共通プロトコル – 安全認可) 編集の受入れ SIL 2またはSIL 3定格のCIPバージョン。

European Norm (EN 規格) (EN) 公式の欧州規格

MT (ミッション時間) デバイスが、交換が必要になる前に、PFD、PFH、およびλ定格を維持する時間。

SIL 付与限界 (SILCL) アーキテクチャの制約と系統的な安全整合性に関連して、SRECSサブシステムに対して主張できる最大SIL定格。(IEC 62061から)

アドオン命令 Logix命令セットにアドオンを作成する命令。定義されると、アドオン命令は他のLogix命令のように使用でき、さまざまなプロジェクトにわたって使用できます。アドオン命令はパラメータ、ローカルタグ、ロジックルーチン、オプションのスキャン・モード・ルーチンで構成されます。

安全 I/O 安全I/Oは、データの整合性を保証するSIL 2またはSIL 3認可されたメカニズム機能があることを除き、標準I/Oのほぼすべての属性を備えています。

安全アドオン命令 安全アプリケーションの命令を使用できるアドオン命令。安全アドオン命令は、整合性の高いアドオン命令の命令署名を使用するだけでなく、安全関連機能で使用するSIL 2またはSIL 3安全命令署名の機能も備えています。

安全アプリケーションの命令 安全関連機能を提供する安全命令。安全ルーチンで使用するSIL 2またはSIL 3認可を受けています。

安全 / 故障比率 (SFF) 安全故障の合計に危険検出済み故障を加算し、すべての故障の総計で除算した値。

安全コンポーネント 安全関連項目としてマークされたすべてのオブジェクト、タスク、プログラム、ルーチン、タグ、またはモジュール

安全署名 安全システムのロジックと構成を固有に示す、ファームウェアが計算した値。コントローラへのダウンロード中に、安全アプリケーションプログラムの整合性を確認するために使用します。

安全タグ 安全タグは、GuardLogixコントローラが関連付けられたデータの整合性を保護するためにSIL 2またはSIL 3認可されたメカニズムを提供することを除き、標準タグのすべての属性を備えています。プログラム範囲またはコントローラ範囲で使用することができます。

安全タスク 安全タスクは、GuardLogixコントローラのみで有効であり、安全プログラムだけをスケジュールできることを除いて、標準タスクのすべての属性を備えています。1台のGuardLogixコントローラには、1つの安全タスクしか存在できません。安全タスクは、周期的/時限タスクでなければなりません。

安全タスクウォッチドッグ 安全タスク実行の開始から完了までの許容可能最大時間。安全タスクウォッチドッグを超過すると、回復不能な安全フォルトがトリガされます。

安全タスク時間 安全タスクが実行される時間。

安全タスクの応答時間 安全タスク時間＋安全タスクウォッチドッグの合計。　この時間は、GuardLogixコントローラに提出された任意の入力が、出力として処理されてプロデューサ接続で利用可能になるまでの最悪の場合の遅延です。

安全遂行レベル (PL) コントロールシステムの安全関連パーツが予測可能な条件下で安全機能を実行する能力を指定するために、EN ISO 13849-1で使用されるディスクリートレベル。

安全度水準 (SIL) 安全機能によって提供される、またはリスク低減のターゲットレベルを指定するためのリスク低減の相対レベル。

安全命令署名 安全命令署名は、安全アドオン命令の実行特性を示すID番号です。署名は、安全アドオン命令のコントローラへのダウンロード中に整合性を確認するために使用します。

安全入力 安全入力にマッピングされたプロデューサ安全タグとコンシューマ安全タグの組合せと、安全モジュールからの入力。

安全ネットワーク番号 (SNN) 安全システム内の全ネットワークにおいて、あるネットワークを固有に識別する番号。各安全ネットワークまたはシステム内の安全サブネットに固有の番号を割付けるのは、ユーザの責任です。安全ネットワーク番号は、固有ノード識別子(Unique Node Identifier (UNID))の一部となります。

安全パートナ デュアル・プロセッサ・コントローラでプライマリコントローラと共に動作して、SIL 3システムで安全関連機能を実行するプロセッサ。

安全プログラム 安全プログラムは、安全タスクでのみスケジュールできることを除き、標準プログラムのすべての属性を備えています。安全プログラムは、ゼロ個以上の安全ルーチンで構成されます。標準ルーチンまたは標準タグを含めることはできません。

安全プロトコル データを高い整合性を持って転送するように設計され、認可されたネットワーク通信方法。

安全ルーチン 安全ルーチンは、安全プログラムでのみ有効であり、安全アプリケーションに適した1つまたは複数の命令で構成される点を除き、標準ルーチンのすべての属性を備えます(安全ルーチンのロジックで使用可能な安全アプリケーション命令および標準的なLogix命令については、71ページの付録Aを参照)。

オンライン コントローラのプログラムをモニタ/修正している状況です。

オーバーラップ タスクが前のトリガからまだ実行中に、そのタスク(周期またはイベント)がトリガされること

回復不能な安全フォルト セーフティコントローラによって提供されたフォルト処理メカニズムで正しく処理されても、すべての安全タスク処理を終了させ、外部ユーザ操作として安全タスクを再起動する必要があるフォルトです。

回復不能なコントローラフォルト すべての処理を強制終了させ、コントローラ電源を切断後に再投入することが必要なフォルト。ユーザプログラムは保存されず、ダウンロードする必要があります。

回復可能なフォルト コントローラに備えられたフォルト処理メカニズムを実行して正しく処理されると、ユーザロジックの実行を強制終了させないフォルトです。

決定論的能力 (SC) 決定論的安全度水準が指定の安全度水準(SIL)を満たしているという信頼度。(IEC 61508-4から)

検出される障害 診断テスト、プルーフテスト、オペレータの介入、または通常の動作で検出される障害。

構成署名 デバイスの構成を識別する固有の番号。構成署名は、ID番号、日付、時刻で構成されます。

作動要求当たりの設計上の機能失敗平均確率 (PFD) 作動要求当たりの設計上の機能失敗平均確率。

自己診断率 (DC) 検出される危険故障レートと危険故障レートの比率。

システム値の取得 (GSV) 特定のコントローラステータス情報を取得して、宛先タグに格納するユーザアプリケーション命令。

システム値の設定 (SSV) コントローラシステムのデータを設定するユーザーアプリケーション命令

周期的タスク オペレーティングシステムが周期的に繰り返しトリガするタスク。時間が期限切れになると、常にこのタスクがトリガされ、そのプログラムが実行されます。タスク内のプログラムにより設定されたデータと出力は、タスクが次に実行されるまで、または別のタスクに操作されるまでその値を保持します。周期タスクは、常に連続タスクを中断します。

システム応答時間 システムへの入力としての安全関連イベント、またはシステム内のフォルトが、システムを安全状態にするまでの最悪の場合の時間。システムの応答時間には、センサとアクチュエータの応答時間、入力および出力の応答時間(ネットワークコネクション遅延を含む)、およびコントローラの反応時間が含まれます。

シンボルを使用するアドレス指定 タグ名のASCII解釈を行なうアドレス指定方法です。

タイムアウトマルチプライヤ この値は、コネクションエラーが宣言される前に失われる可能性があるメッセージ数を決めます。ネットワーク遅延 マルチプライヤも参照してください。

タスク プログラムを実行するためのスケジュールメカニズム。タスクには、特定の基準に基づいて実行される1つまたは複数のプログラムセットのスケジュールと優先度の情報が存在します。タスクがトリガ(起動)されると、すべてのプログラムがタスクに割付けられ(スケジュールされ)、コントローラオーガナイザに表示される順序で実行されます。

単位時間当たりの危険故障確率 (PFH) 動作システムでの単位時間当たりの危険故障確率(失敗確率)

単位時間当たりの危険故障確率 (失敗確率) (PFH) 動作システムでの単位時間当たりの危険故障確率(失敗確率)。

テスト編集 オンライン編集が受入れられると、コントローラメモリ内には2つのバージョンのユーザロジックが存在します。Studio 5000 Logix Designer アプリケーションのTest Editsコマンドを使用すると、新しく編集されたバージョンのユーザロジックがコントローラで実行されます。オリジナルの未編集のバージョンのユーザロジックは、まだコントローラメモリ内にありますが、実行はされません。未テスト編集を参照してください。

ネットワーク遅延 マルチプライヤ この値は、通信ネットワークでのメッセージの転送時間を表します。タイムアウトマルチプライヤも参照してください。

パーソナルコンピュータ (PC) Studio 5000環境を使用してLogixベースのシステムとインターフェイスをとり、制御するために使用するコンピュータ

ハードウェア・フォルト・トレランス HFT は、*n* で、*n*+1 のフォルトにより安全機能が失われる可能性があります。HFTが1の場合、安全機能が失われるまでに2つのフォルトが必要です。

パートナシップ パートナシップを確立するには、プライマリコントローラと安全パートナの両方がSIL 3に存在し、ハードウェアとファームウェアに互換性がある必要があります。

標準 安全関連項目ではないプロジェクト内のすべてのオブジェクト、タスク、タグ、プログラム、またはコンポーネント(つまり、標準コントローラとは、通常ControlLogix またはCompactLogix コントローラを意味する)。

標準コントローラ このマニュアルでは、標準コントローラとは、通常ControlLogixコントローラまたはCompactLogixコントローラを意味します。

標準コンポーネント 安全関連項目としてマークされないすべてのオブジェクト、タスク、プログラムなどです。

プライマリコントローラ 標準コントローラ機能を実行し、安全パートナと通信を行なって安全関連機能を実行するデュアル・プロセッサ・コントローラのプロセッサ

編集のアセンブル 編集のアセンブルは、コントローラプログラムにオンライン編集による変更を行なうときに、編集をテスト、未テスト、キャンセルすることが必要なくなったため、この変更を永続的に適用する場合に行ないます。

編集の受入れ オンライン編集の変更を受入れ、ダウンロードする操作。ペンディング中の編集も参照してください。

編集のキャンセル アンアセンブルされたオンライン編集の変更をすべて拒否して削除する操作

ペンディング中の編集 Studio 5000 Logix Designerアプリケーションでルーチンが変更されたが、編集の受入れによってコントローラへの通信がまだ行なわれていない変更です。

未検出の障害 診断テスト、プルーフテスト、オペレータの介入、または通常の動作で検出されない障害。

未テスト編集 オンライン編集が受入れられると、コントローラメモリ内には2つのバージョンのユーザロジックが存在します。Studio 5000 Logix DesignerアプリケーションのUntest Editsコマンドを使用すると、元の未編集のバージョンのユーザロジックがコントローラで実行されます。新しく編集されたバージョンのユーザロジックは、まだコントローラメモリ内にありますが、実行はされません。テスト編集を参照してください。

命令署名 命令署名は、その時点でのアドオン命令の定義内容を示すID番号と日付/タイムスタンプで構成されます。

有効なコネクション 開いていて有効で、エラーのない安全コネクション

要求パケット間隔 (RPI) 元のアプリケーションがターゲットアプリケーションからのデータの送信を必要とする頻度。

ラムダ (λ) 故障率の指定。

ルーチン ラダーダイアグラムなどの1つのプログラミング言語によるロジック命令のセット。ルーチンには、コントローラプロジェクトの実行コードがあります。プログラムごとに1つのメインルーチンがあります。オプションルーチンを指定することもできます。

Notes:

A

AOI「アドオン命令」を参照

C

CIP Safety 31
ルーティング可能な
システム 32
CIP Safetyプロトコル
定義 106
Compact GuardLogix
コントローラ 19
電源 20
CONNECTION_STATUS
データ 65

D

DeviceNet
Safetyネットワーク 23

E

EtherNet/IPネットワーク 20
European Norm (EN規格)
定義 105

G

Guard I/O
入力モジュール
遅延時間設定 86
GuardLogix
安全アプリケーション
チェックリスト 91
安全パートナ 18
コントローラ 17
コントローラシステム
チェックリスト 92
システムの安全データ 97
シャーシ 18
制御システム安全I/O 25
電源 18
プライマリコントローラ 18
GuardLogixコントローラ
システム 17

I

I/Oデバイス
コネクションステータス 67

L

Logix
SIL 3認可コンポーネント 17, 19
応答時間の要因 85
システムの応答時間 83
計算 84

M

Major Faultsタブ 70
Minor Faultsタブ 70

S

Safetyタブ
コネクションデータ 81
SIL
概念 11
SIL 2
安全アプリケーション 42
システムの例 14
SIL 3
安全アプリケーション 42
システムの例 13
認可 11
SIL定格システム
パラメータの変更 45
SIL認可 11
SNN 31
初期状態のデバイス 37
フォーマット 35
手動 36
タイムベース 35
割付け
注意事項 32
例 33
Studio 5000 Logix Designer
アプリケーション
安全アプリケーション命令 99

U

UNID 31

あ

アクセス
安全関連システム 45
アップロード
安全アプリケーション
プログラム 59
アドオン命令
安全
確認 79
作成 77
安全検証 78
安全命令署名 77
エクスポートとインポート 78
テストプロジェクトの作成 77
認証テスト
SIL 2またはSIL 3 78
フローチャート 76
命令署名 77
アプリケーション
開発 50
テスト 50

アプリケーションプログラム
テスト 54, 79
変更 61
アプリケーションプログラムの変更 61
安全
アドオン命令
作成と使用 75
フローチャート 76
計算 98
入力
チェックリスト 93
評価 57
フォルト 68
安全I/O
安全機能 25
構成署名 27
デバイスの交換 28
モジュール 43
GuardLogix制御システム 25
安全アドオン命令
エクスポートとインポート 78
作成 77
署名の確認 79
安全アプリケーション 27
SIL 2 42
プログラムのアップロード 59
プログラムのダウンロード 58
命令 71
安全アプリケーションの命令
定義 105
安全アプリケーション命令
Studio 5000 Logix Designer アプリケーション 99
安全概念
前提条件 49
安全関連システム
アクセス 45
パラメータの読取り 45
安全機能
安全I/O 25
仕様 53
安全検証
アドオン命令 78
安全コネクション応答時間制限(CRTL)
入力と出力 86
安全出力
チェックリスト 94
安全状態 11, 25
安全署名
削除 55
制限付き動作 55
生成 54
定義 105
安全遂行レベル 11
定義 106
安全タグ 47
定義 106
安全タスク
ウォッチドッグ 16
変更 16
ウォッチドッグ時間 88
ウォッチドッグタイムアウト 40
応答時間 15, 106
概要 40
時間 16
実行 41
制限 40
定義 106
プライオリティ 88
安全タスクウォッチドッグ
設定 16
定義 106
安全タスク時間 82
定義 106
安全データ 97
安全度水準
概念 11
安全度水準(SIL) 3認可
TÜV Rheinland 11
安全認可 17
安全ネットワーク番号 31
初期状態のデバイス 37
定義 106
安全パートナ 17
GuardLogix 18
定義 106
安全パートナフォルト 70
安全評価 79
安全プログラム 46
定義 106
安全命令署名 77
定義 106
安全ルーチン 46
定義 107
安全ロック
コントローラ 57
制限付き動作 57
デフォルト 58
パスワード 58

い

インジケータ
ステータス 26, 65
インターフェイス
HMIの使用とアプリケーション 44

インポート
安全アドオン命令 78

う

ウォッチドッグ
安全タスク 16
時間 88
ウォッチドッグタイムアウト
安全タスク 40

え

エクスポート
安全アドオン命令 78

お

オーバーラップ
定義 107
応答時間 81
Logixシステム 83
安全タスク 15
計算、システム 83
システム 15, 107
出力 26
入力 26
応答時間制限
CIP Safey I/O 81
オフディレイ
機能 26
オフライン編集 61
プロセス 63
オンディレイ
機能 26
オンライン
定義 107
オンライン編集 60, 62
プロセス 63

か

概念
安全度水準(SIL) 11
開発
アプリケーション 50
回復可能な安全フォルト 69
回復可能なフォルト 107
クリア 69
回復不能な安全フォルト 68, 107
安全タスクの再開 69
回復不能なコントローラ フォルト 68, 107
概要
プログラミング 24
拡張
スロット 19
モジュール 19
確認
安全アドオン命令署名 79
プロジェクト 56
監視ネットワーク遅延 82

き

機械安全システム 11
機関の認可 15
機能
オフディレイ 26
オンディレイ 26
機能安全 12
強制
データ 59
禁止 60
デバイス 60

く

クリア
フォルト 69

け

検証
プロジェクト 55, 79

こ

構成署名 27
故障分析 16
コネクション応答時間制限 81
コネクションステータス 66
I/Oデバイス 67
コネクション・ステータス・データ
フォルトの起動 99
固有のノード参照 31
コンシューマタグ
データ 88
コントローラ
Compact GuardLogix 19
GuardLogix 17
ロック 57

さ

削除
安全署名 55
作成
アドオン命令
テストプロジェクト 77
安全アドオン命令 75, 77
署名履歴 78
プロジェクト 54
作動要求当たりの設計上の機能失敗平均確率(PFD)
定義 107

し

時間
応答 81
識別
標準データ 48
自己診断率
定義 107
システム
GuardLogixコントローラ 17
応答時間 15
トリップに対するオフ状態 67
システムステータス
モニタ 65
システム値の取得(GSV)
定義 107
命令 67
システムの応答時間
計算 83
システム変数の設定(SSV)
命令 67
シャーシ
GuardLogix 18
周期的タスク
定義 107
修正の影響
テスト 62
出力
安全コネクション
応答時間制限(CRTL) 86
応答時間 26
診断 66
出力フォルトのラッチとリセット
フローチャート 103
手動
SNNフォーマットと割付け 36
仕様
安全機能 53
使用
安全アドオン命令 75
初期状態のデバイス
SNN 37
署名 27
署名履歴 78
所有者 27
診断 25
入力と出力 66

す

ステータス
コネクション
I/Oデバイス 67
ステータスインジケータ 26, 65
ステータスデータ 26

せ

セーフティコントローラ 39
制御および情報プロトコル
定義 105
制限付き動作
安全署名 55
安全ロック 57
生成
安全署名 54
命令署名 77
製品故障率 98

そ

ソフトウェア
アプリケーション
プログラムの変更 61

た

タイムアウトマルチプライヤ 85
定義 108
タイムベース
SNNフォーマットと割付け 35
耐用年数 97
ダウンロード
安全アプリケーション
プログラム 58
タグ
「安全タグ」も参照
タブ
Major Faults 70
単位時間当たりの危険故障確率(PFH)
定義 108

ち

チェックリスト
GuardLogix安全
アプリケーション 91
GuardLogixコントローラ
システム 92
安全出力 94
安全入力 93
プログラム開発 95
遅延時間設定
Guard I/O入力モジュール 86
注意事項
SNN割付け 32

つ

通信
ネットワーク 20

て

データ
CONNECTION_STATUS 65
GuardLogixシステムの安全 97
安全 97
強制 59
プロデューサタグと
コンシューマタグ 88
テスト
アプリケーション 50
アプリケーション
プログラム 54, 79
修正のインパクト 62
テストプロジェクト
作成
アドオン命令 77
デバイス 60
安全I/O、交換 28
デフォルト
安全ロック 58
電源
Compact GuardLogix 20
Compact GuardLogix 5380システム 20
GuardLogix 18
GuardLogix 5580システム 18

と

トリップシステムに対する
オフ状態 67, 99

に

入力
安全コネクション
応答時間制限(CRTL) 86
応答時間 26
診断 66
入力フォルトのラッチとリセット
フローチャート 100
入力モジュール
Guard I/O
遅延時間設定 86
入力ロジック出力チェーン 83
認可 15
認証テスト
アドオン命令
SIL 2またはSIL 3 78

ね

ネットワーク
DeviceNet Safety 23
EtherNet/IP 20
通信 20
ネットワーク遅延
監視 82
ネットワーク番号
安全 31

の

ノード参照
固有 31

は

パートナシップ
定義 108
パスワード
安全ロック 58
パラメータの変更
SIL定格システム 45
パラメータの読取り
安全関連システム 45

ひ

非常シャットダウンシステム 11
ヒューマン・マシン・
インターフェイス
使用とアプリケーション 44
評価
安全 57, 79
表示
フォルト 70
標準コントローラ 39
標準データ
識別 48

ふ

ファームウェアリビジョン 17
フォルト
安全 68
安全パートナ 70
回復可能 107
回復可能な安全 69
回復不能な安全 68
回復不能なコントローラ 68
クリア 69
表示 70
フォルトコード
ステータス画面 70
メジャー安全フォルト 70
フォルトの起動
コネクション・ステータス・
データ 99
プライマリコントローラ 17
GuardLogix 18
定義 108
プルーフテスト 12

フローチャート
出力フォルトのラッチとリセット 103
入力フォルトのラッチとリセット 100
プログラミングの概要 24
プログラム
オフライン編集 61
オンライン編集 62
チェックリスト 95
ライフサイクルの編集 63
ラベル 54
プロジェクト
確認 56
検証 55, 79
作成 54
プロデューサタグ
データ 88
分析
故障 16

へ

編集
オフライン 61
オンライン 60, 62
プロセス 63

ほ

保存
プロジェクト、メモリカードから 59

ま

マッピング
タグ 48

め

命令
安全アプリケーション 71
システム値の取得(GSV) 67
システム変数の設定(SSV) 67
命令署名 77
定義 109
メジャー安全フォルト 70
メモリカード
プロジェクトの保存 59
プロジェクトのロード 59

も

モジュール
安全I/O 43
モニタ
システムステータス 65

よ

要求パケット間隔
安全I/O 82
要求パケット間隔(RPI)
定義 109
用語 7
用語集 105

ら

ライフサイクル
立ち上げ 52
ライフサイクルの立ち上げ 52
ラダーダイアグラム
安全命令 72
例 101, 102, 103
ラベル
プログラム 54

る

ルーティング可能
CIP Safetyシステム 32

れ

例
ラダーダイアグラム 101, 102, 103

ろ

ロード
プロジェクト、メモリカードから 59
ロジックチェーン
プロデューサ/コンシューマ安全タグ 84
ロック
コントローラ 57

当社のサポートサービス

サポート情報については、以下のリソースをご利用ください。

テクニカル・サポート・センター	ナレッジベース記事、ハウツービデオ、FAQ、チャット、ユーザフォーラム、製品更新のお知らせ。	https://rockwellautomation.custhelp.com/
最寄りのテクニカルサポート窓口の電話番号	お住まいの地域の電話番号を検索していただけます。	http://www.rockwellautomation.com/global/support/get-support-now.page
直接ダイヤルコード	製品別の直接ダイヤルコードが記載されています。このコードを使用すると、テクニカル・サポート・エンジニアと直接通話できます。	http://www.rockwellautomation.com/global/support/direct-dial.page
文書ライブラリ	インストレーションインストラクション、マニュアル、カタログ、テクニカルデータ。	http://www.rockwellautomation.com/global/literature-library/overview.page
製品互換性およびダウンロードセンター (PCDC)	製品がどのように連携しているかの特定に役立つ情報、特長および機能の確認、対応するファームウェアを検索できます。	http://www.rockwellautomation.com/global/support/pcdc.page

マニュアルに関するご意見やご要望

お客様のコメントはより良いマニュアル作りに役立ちます。本書の内容の改善についてご意見がある場合は、http://literature.rockwellautomation.com/idc/groups/literature/documents/du/ra-du002_-en-e.pdf の「How We Are Doing?」に記入のうえお送りください。

ロックウェル・オートメーションでは、以下の Web サイトで最新の製品環境情報を公開しています。
http://www.rockwellautomation.com/rockwellautomation/about-us/sustainability-ethics/product-environmental-compliance.page

Allen-Bradley、ArmorBlock、Compact 5000、CompactBlock、CompactLogix、ControlLogix、Guard I/O™、GuardLogix、Kinetix、Logix5000、POINT Guard I/O™、POINT I/O™、PowerFlex、Rockwell Automation、Rockwell Software、RSLogix 5000、Stratix、Studio 5000、および Studio 5000 Logix Designer は、Rockwell Automation, Inc. の商標です。
CIP Safety は、ODVA, Inc. の商標です。
Rockwell Automation に属さない商標は、それぞれの企業に所有されています。

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

ロックウェル オートメーション ジャパン株式会社
本社営業部 〒104-0033 東京都中央区新川1-3-17 Tel (03) 3206-2786 Fax (03) 3206-2796
関西支店 〒532-0003 大阪市淀川区宮原4-1-14 Tel (06) 6397-1020 Fax (06) 6397-1090
中部支店 〒460-0003 名古屋市中区錦1-6-5 Tel (052) 222-7060 Fax (052) 222-7065

Publication 1756-RM012B-JA-P - April 2018

Copyright © 2018 Rockwell Automation, Inc. All rights reserved. Printed in the U.S.A.