産業機器の機能安全

IoT・インフラ事業本部、ルネサスエレクトロニクス株式会社、中川 靖（プリンシパルスペシャリスト）
2022 年 3 月

概要

近年、産業機器分野ではシステムの安全性を確実に実現する手法として「機能安全」の考え方が広がっています。従来安全が重視されてきた自動車分野に加え、産業機器でも、機器の故障や事故の発生による工場稼動への影響や、人的被害による社会への影響、また経済的損失を防止するため、「機能安全」への重要性が増しています。人とロボットの協働作業による作業効率化が進む中、機械の安全性はますます重要視されています。このような、社会やユーザからの要請、商品競争力向上を目的として、新規に機能安全機器の対応を始めるセットメーカが増加しています。

本資料では、機能安全とは何か、なぜ求められているか、実際のシステムの構成、また開発における課題とそれを解決するルネサスの機能安全ソリューションを説明します。

機能安全とは

機能安全は、装置の誤動作、誤操作により装置が人に危害を及ぼす、あるいは財産や社会に損害を与えるといったリスクを“機能”によって許容限度以下に抑えることを目的としています。

具体的な説明として、ロボットなどのモータ制御装置において、危険な状況を回避するためにモータを停止させる場合を例に説明します。

図 1 は、モータを MCU で回転制御するシステムを機能安全対応した例です。機能安全の実現にむけ、最初に、装置に関係するリスクを分析し、その対策を検討します。これをリスクアセスメントと呼びますが、リスクアセスメントの結果から導かれる安全対策を、機能安全の装置（安全装置）として電子回路などで実現します。この時、機能安全が従来の安全装置と大きく異なる点は、IEC61508 などの国際規格で規格化され、安全装置としての仕様の妥当性が客観的かつ定量的な手法で実現されるように考慮されている点です。

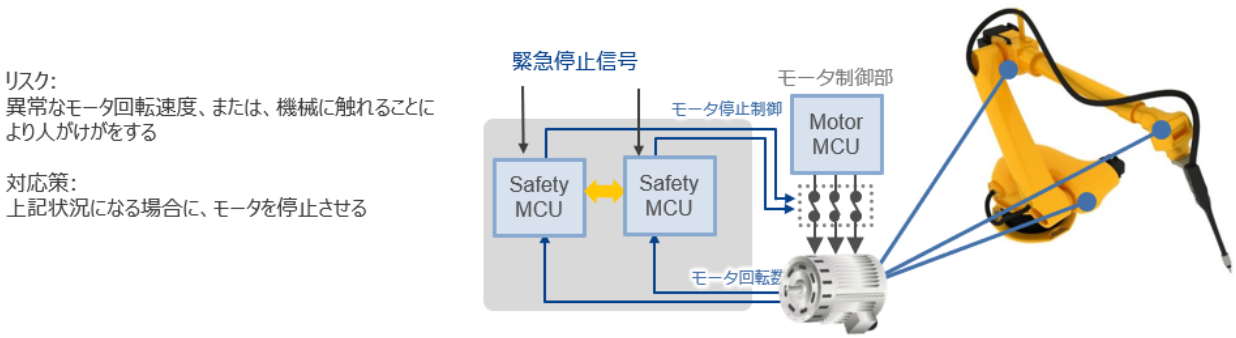


図 1:機能安全によるモータドライブ装置構成例

機能安全規格の要求事項としては、安全装置の故障による誤動作の影響を分析し、診断機能によって、故障しても安全な状態に導かれるような対策を講じ、ソフトウエア・ハードウエアの設計時におけるバグなどで誤動作をすることが無いよう、設計手法や設計プロセスを規定している点などが挙げられます。これにより、その安全仕様や安全装置としての動作の確実性（信頼度）が、より客観的に判断可能となります。また、このような FA システムにおいては、図 1 で示しているような二重化 MCU 構成をとることにより、一方の MCU 動作に故障などの動作不良が発生した場合でも、正常に動作する他方の MCU で確実に安全動作が行えるシステム構成も求められます。

産業分野における機能安全システムの具体例

実際のアプリケーションにおける機能安全システムの構成例として、FA システムで説明します。

図 2 は、機能安全対応のシステム構成例です。この FA システムは人の危険個所への立ち入りなどを検知する、セーフティセンサなどの入力機器、安全システム全体の制御を行うセーフティ PLC などで構成される制御機器、実際の機械を動かすドライブ機器、およびそれらを接続する network で構成されます。その内部構成としては、図 2 の下半分に示すように MCU2 個で構成される二重化 MCU の構造を持ちます。これは、安全機能のどこかに故障が発生しても正常に動作する側の MCU で危険回避のための動作を確実に実行させることができ、機器の安全動作を確実にするための機構として採用されています。

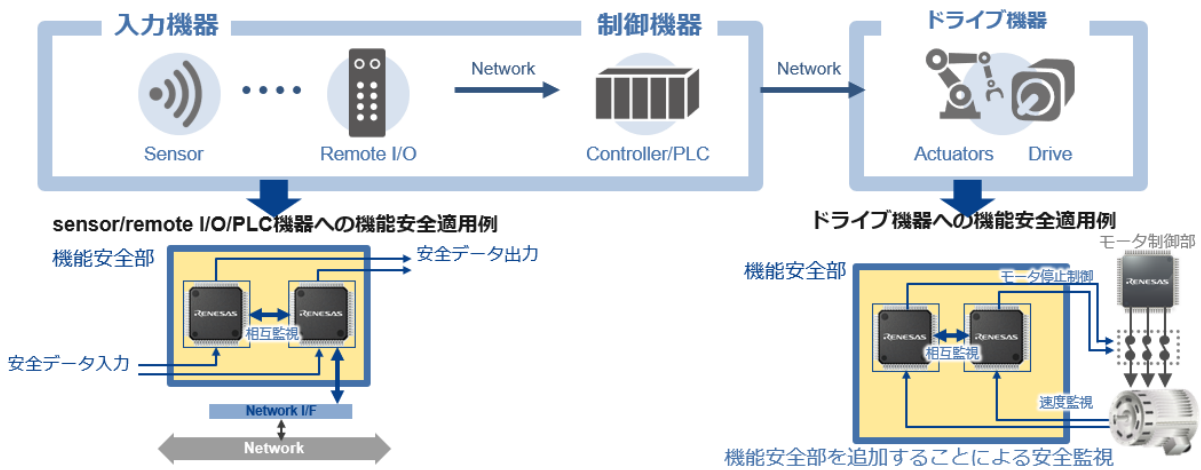
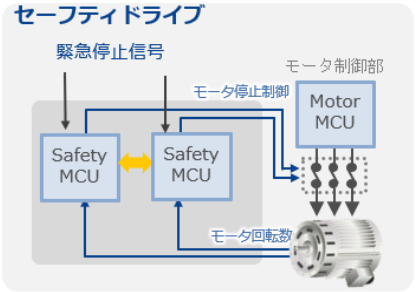


図 2: FA システム構成例

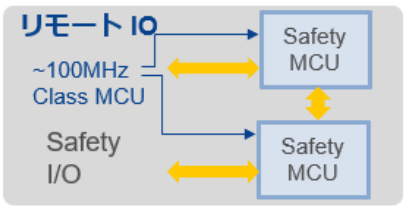
次に、この FA システムを構成する各機器である、セーフティドライブ機器、セーフティ IO 機器、および、セーフティネットワーク機器について説明します。

セーフティドライブ機器



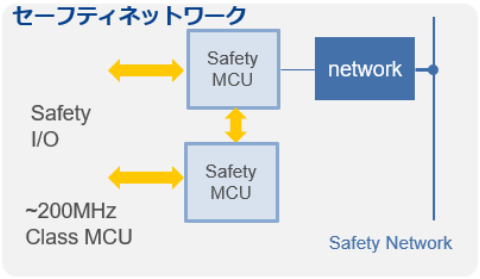
ドライブ機器の基本的な安全仕様は、モータが安全に制御されているかを監視することで実現されます。その構成は、冒頭の図 1 でも説明いたしましたが、一般にはモータを回転させる機構の外側にモータの安全動作を監視するための監視ユニットを追加する構成が取られます。この監視ユニットでモータ回転数と、緊急時など、装置を緊急停止させるための緊急停止信号を二重化された SafetyMCU で監視し、これらの状態が危険状態と判断される場合はモータ制御側にモータ停止信号を発生させる動作を行います。これら動作は二重化されているため、監視ユニット内で故障が発生した場合でも正常に動作するどちらかの SafetyMCU で安全動作に移行できるように考慮されています。なお、モータの監視方法と停止させる方法には FA システムの用途に合わせいくつかの種類があり、その仕様についてはモータドライブ機器の安全規格である IEC61800-5-2 に定義されています。

セーフティリモート IO 機器



セーフティセンサなどの入力信号に応じて緊急停止させる機器への信号出力など、信号を伝達するものです。こちらも内部構成は MCU が二重化されており、安全装置が故障した場合でも確実に安全動作が実行できるように構成されています。また、両 SafetyMCU で安全制御のためのプログラムを動作させることにより、同じ構成でセーフティ PLC（主にローエンドタイプ）も実現することができます。

セーフティセットワーク機器



産業用ネットワークでセーフティデータを通信できるようにしたものがセーフティネットワーク機器です。ここでも 2 個の SafetyMCU が使われており、セーフティ IO の処理に加え、セーフティネットワークの規格に沿って通信されるセーフティデータの処理が行われます。右側のネットワークのデバイスは”Black Channel”と呼ばれ、非安全扱いの部分になります。Black Channel とは、安全でないことを意味しますが、セーフティネットワークで規格化されたセーフティプロトコルは、この Black Channel を通して来たデータが正しく送られているかを確認する手段を有しており、これを 2 個の SafetyMCU で確認することで実現されます。

機能安全システム開発における課題

機能安全システムの開発は、仕様検討(導入＆コンセプトフェーズ)、詳細設計/評価(詳細設計、試作評価フェーズ)、第三者認証審査(メインインスペクション＆認証フェーズ)などの 3 つの開発認証フェーズに分かれて進められ、従来の開発プロセスには無い、技術要件やプロセスが求められます。

機能安全システムの開発の代表的な流れを図 3 に示します。上段の導入＆コンセプトフェーズ導入＆コンセプトフェーズでは、機能安全規格や MCU 仕様の理解など基礎的な知識習得ののち、安全分析と呼ばれる危険の分析を行い、危険を回避するための方法を決め、具体的な安全システムの仕様検討となるコンセプト検討設定します。また、必要なドキュメント

を作成し、認証機関のコンセプト審査を受けます。ここでの安全システム仕様はその次に続く詳細設計、試作評価フェーズ詳細設計、試作評価フェーズで実現可能な仕様になっている必要があります。認証機関の審査を通ると、中段の詳細設計、試作評価フェーズ詳細設計、試作評価フェーズに進み、コンセプトフェーズで定めた仕様に基づいた詳細なハードウエア・ソフトウエア設計評価を行います。これら一連の設計プロセスは、機能安全規格 IEC61508 が求める開発プロセスに従って進める必要があります。設計においては、機能安全規格の意味する内容を的確にとらえて開発を進める必要があり、また、そのハードウエアの故障分析とその診断手法の検討、ソフトウエアの不具合を回避するための適切な開発プロセスの実施が求められます。これらの作業には各設計プロセスでのドキュメント化、システムの故障率と診断率を基にした達成安全レベルの計算などが求められ、従来の開発プロセスには無い作業が必要になります。

詳細設計と評価が完了したのち、下段のメインインスペクション＆認証フェーズメインインスペクション＆認証フェーズにて、これまで設計評価した内容を認証機関に提出し、必要に応じて立ち合い試験なども経て、その内容が承認されれば認証となります。

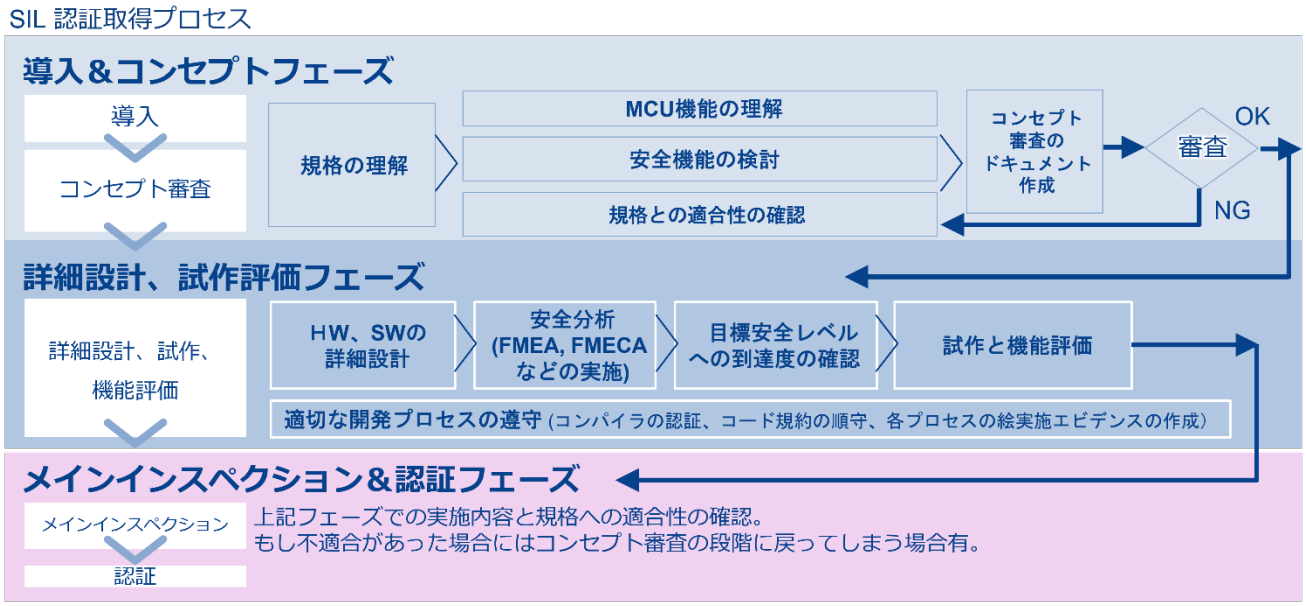


図 3 : 機能安全システムの開発プロセス

機能安全システム開発へのルネサスのご提案

これらシステムの機能安全規格認証取得のプロセスを進める上で、開発者が直面する技術的課題としては以下の事項が挙げられます。

1. 認証を取得する上での各種ドキュメントの記述方法、システムの安全分析（FMEA）、SIL レベル達成のための各種パラメータの計算方法
2. SafetyMCU 2 個で構成される二重化システム構成における MCU 自己診断、相互監視などの故障診断用ソフトウエアの実現
3. 二重化 SafetyMCU システムのハードウエア構成（相互監視の通信、入出力回路診断、電源診断の構成など）
4. アプリケーションに応じた機能安全機構の実現（モータシャットダウン機構、モータ回転数検知のためのエンコーダ、セーフティネットワークの実現など）

これら機能安全システム実現における課題に対し、ルネサスの機能安全ソリューションは、課題解決のための各種ソリューションをご提供しています。以下にこれら開発者の直面する課題に対応するソリューションをご紹介いたします。

ルネサスでは、機能安全システムの開発をサポートする図 4 に示す 1.~7.の各種ソリューションを用意しています。これらのソリューションが、課題をどのように解決するかを説明します。

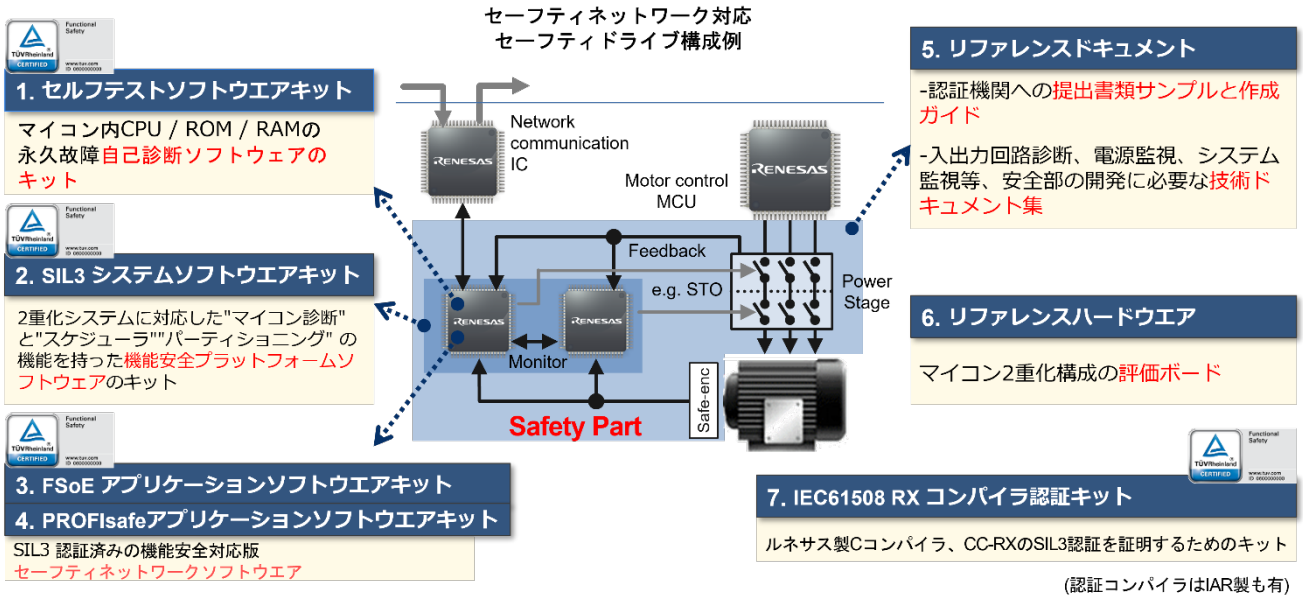


図 4: ルネサスの機能安全ソリューション

認証を取得する上での各種ドキュメントの記述方法：リファレンスドキュメント

機能安全システムを開発する上で最初に行う作業、仕様を検討する紺瀬プロフェーズでは、SRS,SC, SP,V&V など、必要なドキュメントを作成しますが、これらのドキュメントに記載する事項、記述方法は、認証取得の経験がない場合、手探りで進めざるを得ず、時間とコストに大きく影響します。5.のリファレンスドキュメントはコンセプトフェーズで必要なこれらのドキュメントを、モータドライブ装置のセーフティシステム実現を例に具体的に記述したものです。これをテンプレートとし、ユーザごとの仕様に合わせて変更していくことで、必要な情報が過不足なく記載できます。

二重化システムの診断 SW の実現：SIL3 システムソフトウエアキット、シセルフテストソフトウエアキット

機能安全システムでは、安全機能がハードウエアの故障によって正常に機能しない状態を回避するため、故障診断を行う必要があります。故障診断では、デバイス個々の故障検知に加え、動作中に放射線やノイズなどで発生するソフトエラーによる誤動作を検出し、異常時にはモータ停止などの安全動作に即座に移行させる必要があります。デバイス個々の故障診断は、各デバイスの故障モードの分析と、それを検出するための故障検出手法の検討と、その検出手法による故障検出率（診断率）の定義が必要です。また、ソフトエラーの検出にはプログラムの実行シーケンスを監視し、二重化 SafetyMCU を利用した相互比較による手法など、システム的な動作を利用して検出することも必要です。しかし、SafetyMCU のように複雑なデバイスの場合、故障検出の手法とその診断率の定義は、装置開発者にとって、かなりの作業負荷となります。さらに、プログラムシーケンスの監視や相互比較のための SafetyMCU 間通信の手法も、機能安全規格の要請に基づいて適切に行う必要があり、開発者の大きな負担となります。1.セルフテストソフトウェアキットは Safety、MCU の故障を検出する

ための自己診断プログラムを提供するもので、IEC61508 規格での SIL3 を実現する上で求められる診断率 90%を実現しています。2.の SIL3 システムソフトウエアキットは、二重化システムを実現する上で必要な相互監視やプログラムのシーケンス監視などのソフトウエアをあらかじめ組み込んだものです。主要な SafetyMCU 診断やプログラムシーケンス監視、二重化 SafetyMCU 間での相互監視に必要なソフトウエアを提供しており、IEC61508 の SIL3 認証を取得済みなので、開発者の方にそのままお使いいただけます。

これらのソリューションを活用することにより、開発者は、セーフティシステムに必要なアプリケーションプログラムをこのセルフテストソフトウェア、SIL3 システムソフトウエアキット、セルフテストソフトウエアキットで構築していくだけで、機能安全システムの開発が可能になり、面倒な SafetyMCU 診断や二重化 SafetyMCU の制御部分の開発から解放されます。

なお、これらのソフトウエアで使用するコンパイラは機能安全システム開発で使用しても問題ないことが証明されているものであることが求められます。ルネサスでは IEC61508SIL3 の認証を取得した 7.の CC-RX コンパイラを提供しております。IAR システムズからも SIL3 の認証を取得したコンパイラを提供しております。

二重化システムのハードウエアの実現：リファレンスドキュメントリファレンスハードウエア

二重化構成を実現するには、2 個の SafetyMCU 間で相互監視するのための通信手段、電源の分離や電源監視、入出力回路の診断など、特有のハードウエアが必要です。6.のリファレンスハードウエアは、二重化 SafetyMCU の電源回路を含む参考データを提供します。また、二重化構成を使用することによるメリットとして、互いの処理データを交換することにより、特殊な診断ハードウエアを使用することなく、動作が正常であることを確認できます。これら一連のハードウエア構成と診断の手法については、5.のリファレンスドキュメントに記載されています。

設計したハードウエア・ソフトウエアが、目標とする安全レベルに到達しているかの判断には、ハードウエアの故障率やその診断手法、診断率を定義し、信頼性理論に基づく複雑な計算式を用いて各種パラメータを計算し、安全レベルに応じた基準値を満たしているかを示す必要があります。これら認証用ドキュメントの記述サンプル、各種パラメータの計算手法についてもリファレンスドキュメントに詳しく記載されており、計算式は Excel 形式で提供されます。これらを活用することで、初めての開発者でも、故障率や診断率などのデータを表中に入力し、確実に進めることが出来ます。なお、SafetyMCU の周辺機能に関してはユースケースに応じて手法が異なるので、使用例に応じた診断手法がリファレンスドキュメントに記載されています。

アプリケーションに応じた安全機能の実現：リファレンスドキュメント FSoE アプリケーションソフトウエアキット、PROFIsafe アプリケーションソフトウエアキット

MCU 診断のソリューション以外にも、アプリケーションレベルで、セーフティドライブ機器、セーフティ IO 機器、セーフティネットワーク機器に有効なソリューションも提供しています。リファレンスドキュメントは、ドライブシステムのセーフティ規格である IEC61800-5-2 に対応するために必要なハードウエア構成、安全制御の手法、それらを安全コンセプトとして記述したものをサンプルドキュメントとして提供しています。この中ではドライブ向け機能安全の例をとって説明していますが、その構成は“セーフティ入力－セーフティ制御－セーフティ出力”といった一般的な機能安全機器の処理ブロックで構成されていおり、同じ構成を持つセーフティセンサ、セーフティリモート IO 機器の開発においても、参考にして頂けます。リファレンスドキュメントにはネットワークのセーフティ化についても記述されています。セーフティネットワークへのソフトウエアとしては、EtherCAT のセーフティ版である FSoE(Functional Safety over EtherCAT)にへの対応として 3.FSoE アプリケーションソフトウエアキットを提

供中です。さらに PROFINET のセーフティ版である PROFIsafe への対応として新たに 4.PROFIsafe アプリケーションソフトウエアキットのご提供を開始いたしました。

まとめ

これらルネサスの機能安全ソリューションは、図 5 に示すとおり、コンセプト段階における仕様検討、MCU 回りの機能安全にかかわる故障分析と診断プログラム、二重化構成と周辺診断、ネットワークなどのシステムレベル診断ソフトウエア、これらを認証機関に提出する際のドキュメント記載方法などを提供しており、機能安全システム開発の 6～7 割をサポートしています。これにより、開発者は機器固有部分の設計・開発を行うことで、安全システムを完成させることができます。

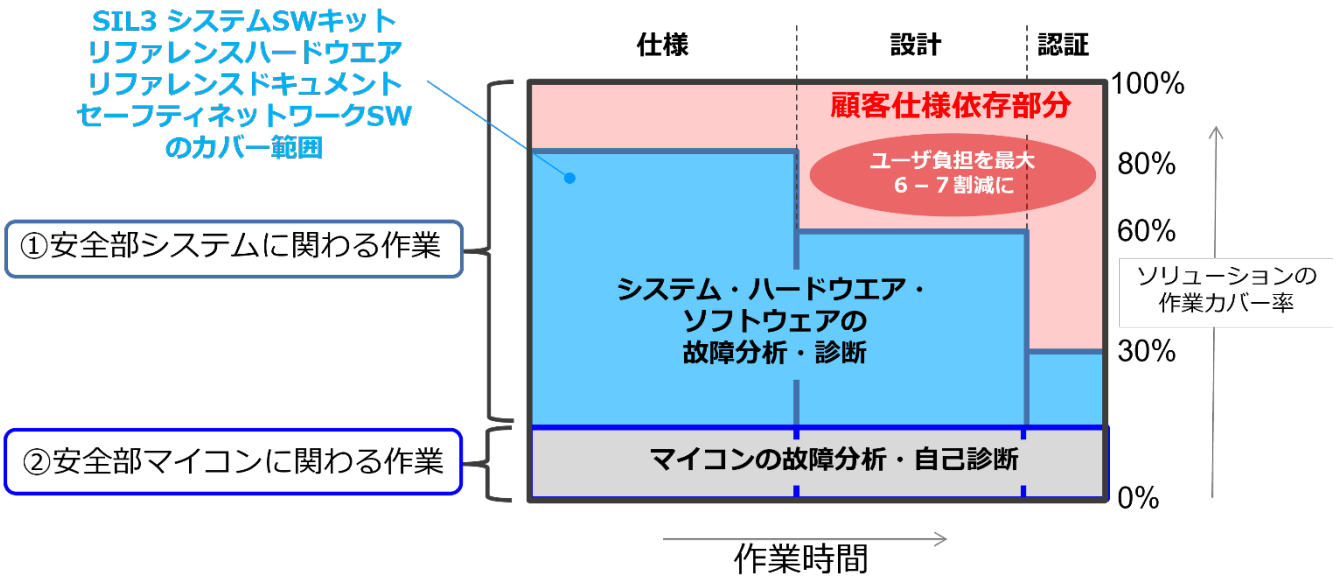


図 5 : ルネサス機能安全ソリューションのカバー範囲

ルネサスの機能安全ソリューションを活用することで、システム開発者は SafetyMCU 診断などのデバイス固有のソフトウエア開発や認証作業から解放され、システム開発にかける時間・コストを有効に活用することができます。ルネサスの機能安全ソリューションは、手探りで機能安全システムの開発を進めざるを得なかった開発認証作業に、確実な近道をご提供します。

参考資料

IEC の Functional Safety and IEC 61508

産業機器向け機能安全ソリューション

RX ファミリ （32-bit MCUs）

本社所在地

〒 135-0061 東京都江東区豊洲 3-2-24
（豊洲フォレシア）
https://www.renesas.com

お問合せ窓口

弊社の製品や技術、ドキュメントの最新情報、最寄りの営業お問合せ窓口に関する情報などは、弊社ウェブサイトをご覧ください。
http://www.renesas.com/contact/

Doc Number: R30WP0002JJ0100