セーフティグローバル推進機構 規程

IGSAP Rules

IGSAP S01：2023

Safety 2.0 適合審査登録制度
Safety 2.0 構築・運用のための一般要求事項：第 2 版

Safety 2.0 compliance registration program
General requirements for the development and establishment of
Safety 2.0 system in collaborative safety: Edition 2

2023 年 4 月 1 日

一般社団法人
セーフティグローバル推進機構
The Institute of Global Safety Promotion

制定：Safety 2.0 適合基準として 2018 年 2 月 26 日
改正：Safety 2.0 に関する一般要求事項 2019 年 10 月 29 日
改正：Safety 2.0 構築・運用のための一般要求事項：第 2 版　2023 年 4 月 1 日

目次

Safety 2.0 適合審査登録制度

Safety 2.0 構築・運用のための一般要求事項：第 2 版

Safety 2.0 compliance registration program
General requirements for the development and establishment of
Safety 2.0 system in collaborative safety: Edition 2

序文

本規格は、一般社団法人セーフティグローバル推進機構(IGSAP)が推進する協調安全の方策である Safety 2.0 を構築し、運用するために必要となる事項を規定したものである。

労働環境における安全を確保するため、機械類の利用に伴う様々なリスクを低減する方策が追求され、発展が図られてきた。各種の機械を使用する人が注意をして安全に使いこなすことが求められるステージである Safety 0.0 から、機械の運用者の注意のみに依存せず、機械自体で受け入れ可能なリスクのレベルまで低減するステージである Safety 1.0 が、製造業を中心に普及している。このステージでは、①本質安全の原則、②隔離の原則、③停止の原則、のもとにリスク低減を図るものである。しかしながら、Safety 1.0 においては、人と機械が共存環境で作業を実施することを前提としておらず、隔離、停止による作業効率の低下の可能性がある。他方、情報通信技術（ICT）や AI 技術を活用し、人と機械、さらには周辺の環境との間で、安全に係る各種の情報を相互に共有し、協調することにより、リスクを一層低下させる協調安全の考え方が発展してきた。Safety 2.0 はこの協調安全を実現するための方策であり、これにより、人と機械、及び機械相互の連携を図ることにより、危険事象の発生確率を低減し、さらに安全性を確保した上での効率性の向上を可能にすることが期待されている。ひいては、要員、及びその他関係する人における安心感と働き甲斐を高め、ウェルビーイングの向上に資するものである。

IGSAPでは、2019 年度より本スキームによる適合審査事業を実施しているが、これまでの Safety 2.0 の適合審査結果を踏まえ、規定内容をより明確化する目的で改訂を行った。本文書は、実施する様々な安全方策において Safety 2.0 を構築・適用する際の参照に用いることが可能である。また、併せて IGSAP がスキームオーナーとして実施する Safety 2.0 適合審査のための規格としても用いられる。

1. 適用範囲

本規則は、人と機械とが共存する環境に対し、協調安全における安全方策である Safety 2.0 を適用する場合の一般要求事項について規定する。Safety 2.0 の導入は、システムやコンポーネントを構築する供給者と当該システムを運用する運用者の連携によって安全に関するリスクの低減を図ることを前提としており、この 一般要求事項は、供給者と運用者の双方に対して適用する。

2. 引用規格

次に掲げる規格は，この規格に引用されることによって，この規格の規定の一部を構成する。これらの引用規格は，最新版の規格を適用する。

ISO/IEC Guide 51：Safety aspects−Guidelines for their inclusion in standards

IEC Guide 116：Guidelines for safety risk assessment and risk reduction for low voltage equipment

ISO12100：Safety of machinery − general principles for design − Risk assessment and risk reduction

ISO9001：Quality management systems - Requirements

ISO45001：Occupational health and safety management systems - requirements with guidance for use

3. 用語及び定義

この基準で用いる主な用語及び定義は、次による。

3.1. 協調安全

人と機械と環境とが情報を共有し、協調することによりリスクを低減する安全確保の考え方。

3.2. Safety 2.0

人と機械と環境との情報共有により、危険事象の発生を検知または予測するとともに、自律的に安全側に誘導または制御することにより、災害のリスクを低減するための方策である。これには運用ルールなどのマネジメント並びに要員の教育及び訓練等の運用体制を含む。

3.3. 機械

Safety 2.0 システムが直接的又は間接的に関係するコンポーネント、装置及びその集合。

3.4. 環境

人と機械とが共存するサイトの物理的環境（例：温度、湿度、照度、塵埃、騒音）。広義には、当該サイトの適正な機能を維持するためのマネジメント環境、規制等の付帯的条件や社会的環境も含む。

3.5. 人

当該サイトにおいて、主として業務に従事する人をいうが、それ以外の関係者も含む。

3.6. Safety 2.0 システム

Safety 2.0 の安全方策が、ハードウェア、ソフトウェアにより構築され運用されるシステム。

3.7. コンポーネント

Safety 2.0 システムを構成するハードウェアやソフトウェア。

3.8. サイト

Safety 2.0 システムを包含し、一定の作業、運用プロセスを含む特定領域をいう。

3.9. リスク及び関連用語

この規格の別項で規定のない限り、ISO/IEC Guide 51 の 3 項（用語及び定義）に規定するリスク及び関連用語の定義を適用する。

3.10. 要員

Safety 2.0 の運用に直接的又は間接的に関与する人員であって、その運用組織において規定された教育訓練を受けて固有の知見や経験を有する人員。

3.11. マネジメントシステム

Safety 2.0 の運用に際して意図した機能を適正かつ持続的に運転・稼働させるために必要な管理の仕組み。

3.12. 供給段階

Safety 2.0 を構成する基幹コンポーネント及びその組合せで構成されるシステムを設計し、インテグレーションを行う段階。

3.13. 運用段階

特定されたサイトにおいて、Safety 2.0 を構成する基幹コンポーネント及びその組合せで構成されたシステムが稼働する段階。

3.14. 安全方策

リスク低減のための保護方策に加え、安全・安心・ウェルビーイングの向上を意図した方策。

4. Safety 2.0 の基本原則

Safety 2.0 が達成すべき目標は、これを採用する現場で生産性や効率を犠牲にすることなく、安全上のリスクを低減し、人・要員に安心感を提供することである。これを実現する Safety 2.0 システムの開発、構築、運用にあたっては、“The state of the art”の原則の基に、下記基本事項のすべてを満たさなければならない。

a) 人と機械と環境とがリスク情報を共有し、活用することで、リスクが低減されること

b) 人と機械と環境とが有する能力を活用することで、効果的な安全方策を実現すること

c) Safety 2.0 システムの供給段階から運用段階まで包括的にリスク低減を実施すること

注記 “The state of the art”の原則とは最新の情報や技術の動向を把握したうえで適切に活用し、常に安全の水準の向上を目指す原則。

5. Safety 2.0 のリスク低減方策

5.1. リスク低減目標

Safety 2.0 システムの導入により実現される残留リスクのレベルは、許容可能なレベル以下でなければならないが、広く受け入れ可能なリスクレベルの実現に向け、その一層の低減化を図ることが望ましい。

5.2. リスク低減プロセス

人に危害を及ぼすおそれのある危険源を特定し、リスクの分析、評価を行い、受入れ可能なレベルにまで低減する手順については、Safety 2.0 システムにおいても、ISO/IEC Guide51 及び関係規格で規定されているリスクアセスメントやスリーステップメソッドに従うことを原則とする。ステップ2、及びステップ 3 においては、Safety 2.0 による保護方策として、安全側への誘導情報の発信、危険回避情報の発信、人の動作の制限、AI を活用した危険予知の保護方策等を講じることにより、更なるリスク低減を図ることが可能である。また、当該サイトで Safety 2.0 システムの構築や運用において生じる新たなリスクについて、人、システム、環境の観点から以下のリスクを特定し、低減策を講じる必要がある。

- 人の心理、挙動、適性に起因するリスク
- Safety 2.0 システムの機能、動作、制御に起因するリスク
- 現場の物理的環境、又は現場作業や運転ルールに起因するリスク

図1は、Safety 2.0 によるリスク低減方策について包括的に図示したものである。

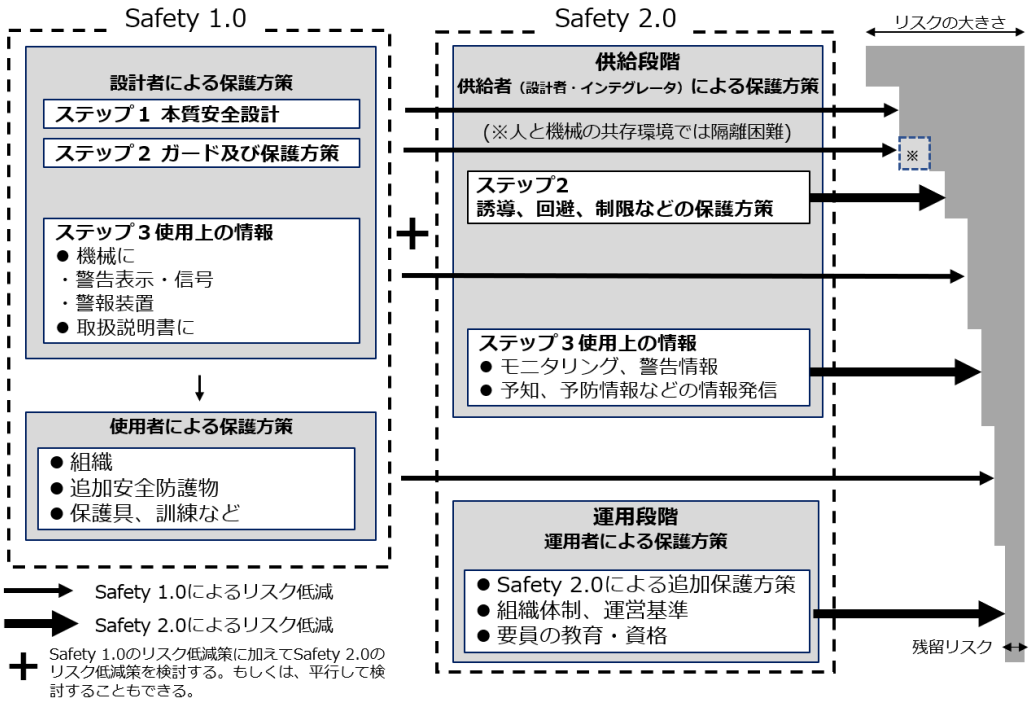

図1　リスク低減のプロセス

6.　Safety 2.0 適用の要求事項

6.1.　安全性の目標

Safety 2.0 の安全性に関する目標を設定し、実効性を確認する仕組みをもたなければならない。

6.2.　情報共有

人と機械と環境とが、相互に交換しリスク低減に有効となる情報と内容及びその利用方法を明確にしなければならない。注記 Safety 2.0 では、人と機械と環境が相互に有する情報を活用し、不安全状態を回避することから、この活用情報の対象と内容が Safety 2.0 構築の基礎となる。

6.3.　安全制御システムの安全性

安全制御システムに要求される安全性は、リスクの大きさに応じて設定しなければならない。

6.4.　付帯的要件

人と機械と環境とが有すべき付帯的要素に対する必要条件を明確にしなければならない。
注記 Safety 2.0 では、人と機械と環境とが情報を共有し安全制御等の安全防護システムに活用することのみならず、人の能力やマネジメントなどの付帯的要素を活用することにより、包括的に危険事象の発生確率を低減することを包含している。リスクアセスメントに際してもこれらの要素を反映することができる。
例えば、

- （人の場合）要員としての経験や保有資格、スキル、教育による誤操作や誤使用による危険事象の発生確率の低減
- （機械の場合）危険事象発生又は予測情報の発信による人・要員の注意力の喚起
- （環境の場合）作業ルールの整備による誤操作や誤使用による危険事象の発生機会の低減

7.　Safety 2.0 のリスク管理に関する要求事項

7.1.　Safety 2.0 によるリスク低減の妥当性の確認

Safety 2.0 適用前、適用後のリスクアセスメントの結果を比較し、Safety 2.0 のリスク低減策の妥当性を確認しなければならない。

7.2. 供給段階(システムの設計、構築段階)で設定するリスク低減方策

供給段階で設定する Safety 2.0 による保護方策等について、以下を明確にするとともに、リスクアセスメントに反映し、実効性の評価を行わなければならない。また、運用者に対して適切に伝達しなければならない。

a) Safety 2.0 による保護方策を実施するシステムの構成とコンポーネントの特定
b) 相互に有する情報を利用し、防止しようとする危険事象、及び低減できるリスクの大きさとその内容
c) 供給者が意図したシステムやコンポーネントの使用方法に関する情報
d) システムの設置及び廃棄の方法
e) 残留リスクの内容及び残留リスクへの対処方法
f) システム運用に必要となる Safety 2.0 システムの機能、運転手順、保守手順及び点検手順の情報
g) システム運用に必要となる Safety 2.0 システムに関する管理、教育及び訓練の情報

7.3. 運用段階で設定するリスク低減方策

運用段階で実施する Safety 2.0 による保護方策等について以下を明確にするとともに、運用段階におけるリスクアセスメントに反映し、実効性に関して評価を行わなければならない。

a) Safety 2.0 による保護方策の構成とその内容
b) a)の保護方策により防止可能な危険事象及び低減されるリスクの大きさとその内容
c) 7.2 f)及び g)に加えて管理・運用上必要な、Safety 2.0 システムに関する運用、保守、点検の手順
d) 組織管理体制及び当該システムの運用体制
e) 当該システムに関与する個々の要員が保有する力量

7.4. マネジメントシステム

Safety 2.0 による機能の持続性を確保し、継続的改善を推進するため、技術開発・設計、インテグレーション、稼働・運用、に関するマネジメントシステムとして、以下を確立し、実施しなければならない。また Safety 2.0 の実効性を確保するためには、これらの取組みに関して、システム供給者であるシステム開発者、システムインテグレータと運用事業者の連携が不可欠であり、両者の間でマネジメント面での連携を図らなければならない。

a) Safety 2.0 システム開発時点の責任分担の決定
   Safety 2.0 システムの安全性・生産性に対する目標をシステム運用者が決定し、その目標の達成のためシステム供給者と運用者は、協議のうえその責任分担を合意すること。
b) 安全を担保するための情報伝達の確実な実施
   供給者は、使用上の情報、残留リスク情報を運用者に提供すること。 運用者は、現場の管理者及び要員にその情報を周知すること。
c) 継続的改善
   Safety 2.0 システムの安全性の目標に対する実現状況を継続的に評価し、必要により改善策を実施すること。
d) 変更管理手順
   Safety 2.0 システムの機能や運用に影響するマネジメントシステムの変更管理の手順を確立すること。変更管理の対象例として、運用ルールの変更、要員の変更、コンポーネントの仕様変更や交換がある。
e) 異常時の措置手順の確立
   事故の発生の有無にかかわらず Safety 2.0 システムにおいて機能の正常性が確認されなくなった場合、その

情報を関係責任者に報告するとともに、是正措置を決定し関係要員に周知すること。また、再発防止を確実にする手順を規定すること。

f) 上記以外のマネジメント項目については、可能な限りISO9001、ISO45001などのマネジメントシステム規格の該当項目を参照の上、ルール化すること。

8. Safety 2.0 システム及びコンポーネントに対する要求事項

Safety 2.0を構成し、その機能に寄与するシステム及びコンポーネントを供給するにあたっては、安全確認型であるほか、以下の要求事項を満たさなければならない。適合できない場合はそれが妥当である理由を明確にするとともに、必要な場合は代替策を有しなければならない。

a) 意図する安全に関する機能及び技術的要件を明確にするとともに以下を運用者に確実に伝達すること。
   1) 使用条件に対する信頼性、耐久性を考慮した、システム、コンポーネントの交換時期・点検時期
   2) コンポーネントを供給し、システムインテグレータ或いは運用者にそのシステム構築を委託する場合は、コンポーネントが意図するSafety 2.0の機能を実現する適切な設置条件及び運用方法
   3) Safety 2.0 システムのリスクアセスメントや、コンポーネントの故障モード分析による、危険な事象に至る故障の情報

b) 想定される内的及び外的要因により安全に関する機能が損なわれない構造となっていること。または、危険側故障率が許容可能なレベルとなっていること、もしくは合理的な代替策を有すること。
   注記 合理的な代替策としては以下をあげることができる
   安全に関する機能が正常に動作している状態を適切に表示、または確認する手段を設ける。
   例えば
   - センサー、カメラ等の情報取得装置、及びディスプレイ等の情報表示装置を装備したシステムは、塵埃や明るさ等の周囲の環境変化により性能面での影響を受けない対策
   - 通信機能をもつコンポーネントは、通信状態を示す表示手段

c) 内蔵されるソフトウェアは、リスクアセスメントにより安全性が評価されていること。

d) 内蔵されるソフトウェアは、リスクアセスメントによりセキュリティ面での評価が行われていること。

e) 供給者はシステム及びコンポーネントが接続するネットワーク環境のセキュリティ要件を提示すること。

f) システムの設置環境に応じ、その機能維持のための配線や接続等、適切な保護方策を講じること

解説：Safety 2.0 の基本的考え方

本解説は規格の一部ではなく、Informative Annex として規格要求事項の理解促進のための基礎情報として提供するものである。

1. ICT の特性を活用した Safety 2.0 への展開

ICT 特性を活用して様々な産業セクターへの適用が可能となる。Safety 2.0 構築に共通的に適用可能な ICT 特性の事例を図 1 に示す。

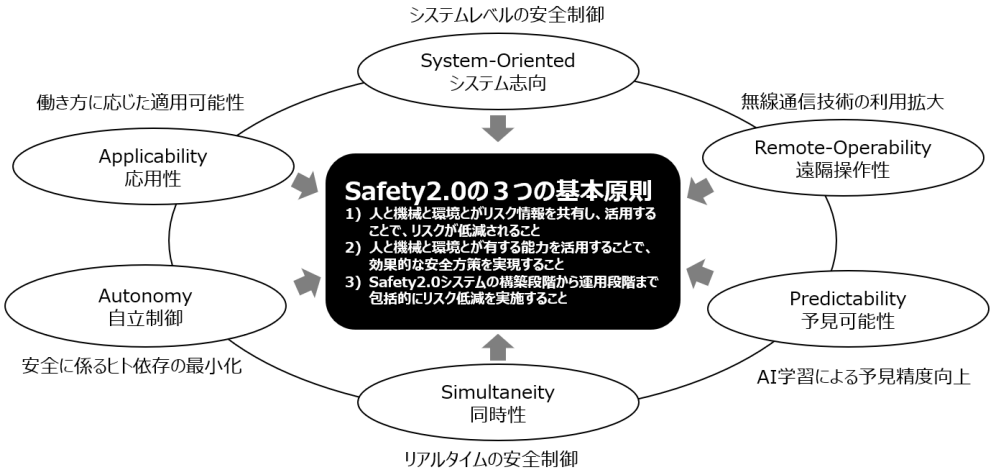

図1　Safety 2.0 構築に共通的に適用可能な ICT 特性の事例

2. 情報連携と安全制御

Safety 2.0 の意図するところは、リスク関連情報を共有し、不安全状態を回避すべく、未然に人の行動や機械の動きを停止或いは制御することであり、情報の対象と内容が Safety 2.0 構築の基礎となっている。 リスク情報及び安全制御指示情報の連携事例を図2に示す。

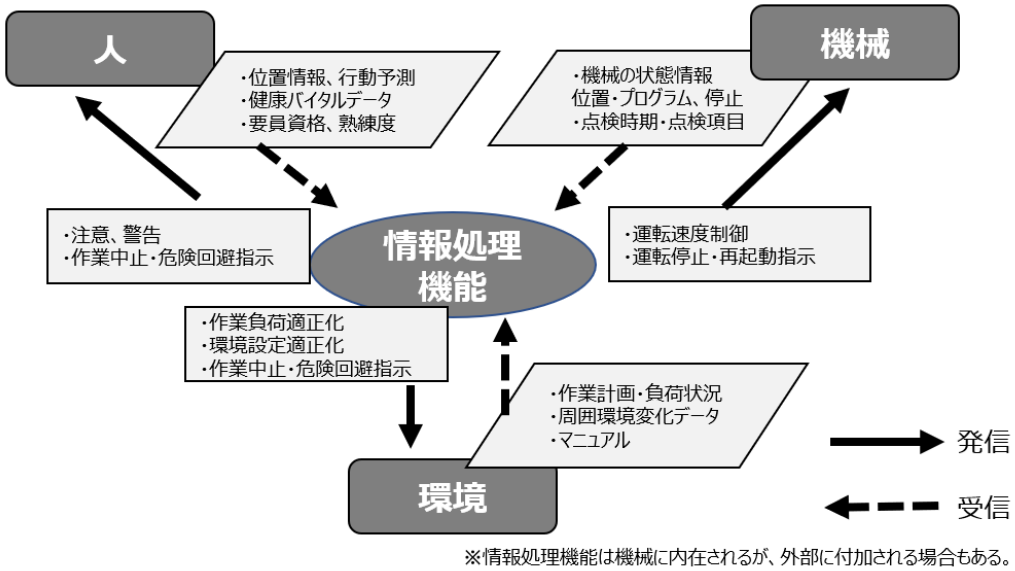

図2 リスク情報及び安全制御指示情報の連携事例

3. 受入れ可能なリスクレベルの決定

リスクの大きさは、合理的に実行可能な限りできるだけ小さくすることが必要であるが、現状、許容領域であっても、Safety 2.0 の採用により、広く一般が受容する領域を目指し、さらなるリスクの低減が求められる。図 3 は ALARP（As Low As Reasonably Practicable）モデルと呼ばれる受け入れ可能なリスクレベルの決定の考え方を示したものである。

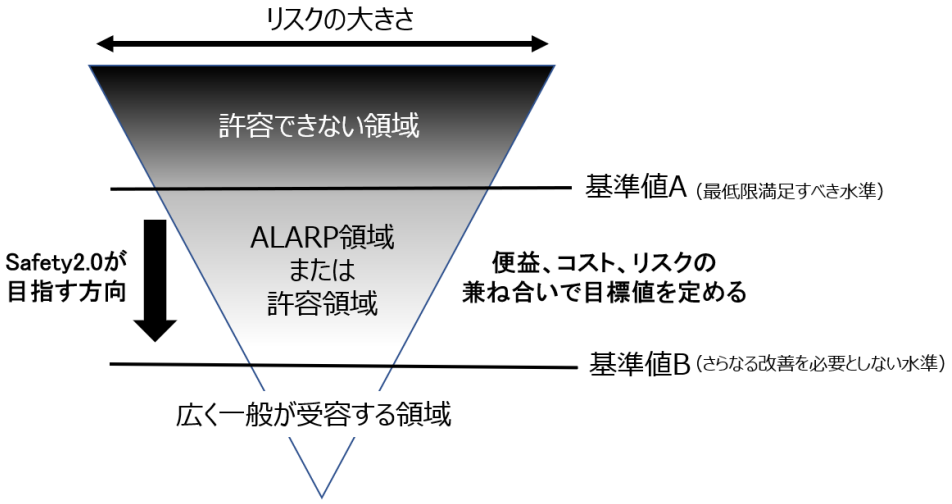

図3 ALARP モデルの考え方

4. Safety 2.0 のマネジメントシステム

Safety 2.0 を現場で運用するためには、採用した技術が現場で持続性をもって適正に機能するためのマネジメントシステムが不可欠である。これには ISO45001 や ISO9001 の該当項目に従う Safety 2.0 技術マネジメントを行うことにより達成可能となる。その関係図を図 4 に示す。

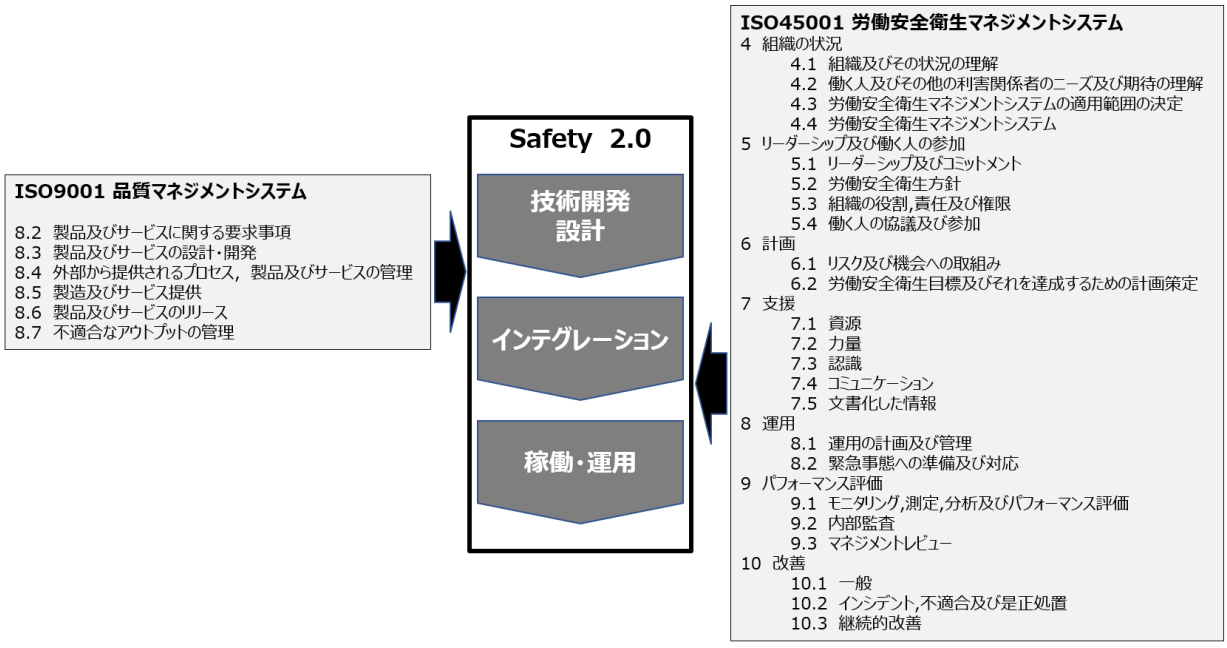

図 4 マネジメントシステム規格のSafety 2.0 への適用