

高機能安全装置の大規模生産システムへの適用と評価

清水 尚憲*1, 齋藤 剛*2, 濱島 京子*2, 池田 博康*3, 北條 理恵子*2

労働安全衛生規則第 150 条の 4 において、「産業用ロボット（定格出力 80W を超えるもの）に接触することにより危険が生ずるおそれがあるときは、柵又は囲い等を設けること」と規定されている。これは、産業用ロボットと作業者は、柵又は囲いにより空間分離をすることで安全を確保するというを示している。現在、産業用ロボットを含む統合生産システムでは、様々な危険源が存在し、その危険源に対するリスクを低減するために 2 つの原則に沿った次のリスク低減方策が採用されている。

- ① 危険領域の周囲に柵を設置することで作業者の安全を確保している（隔離の原則）。
- ② 作業者が柵の内側に侵入する場合に進入口に侵入検知センサやインターロック式ドアスイッチ等を設けて、柵の内側に作業者がいないことを条件に柵内の機械を稼働することを許可している（停止の原則）。

現在、複数の作業者が広大な領域で作業を行う大規模生産システムでは、人の資格と権限の未確認や作業者の作業位置が確認されないことによる災害が発生している。また今後、適切なリスクアセスメントの実施を条件として共存・協調作業を行うために安全柵を取り外して全方向からのアクセスを可能にする生産システムも提案されていることから、保護方策を適用した後に残る残留リスクに対する ICT 機器を利用したリスク低減方策の開発とともに事前の定性的なリスクアセスメント評価に対する有効性検証方法が求められている。そこで本研究では、まず、人・機械・環境の情報を Cyber Physical System (CPS) で共有することで安全制御を実現する場合の条件として、物理層・データ層・論理層の 3 つの基本要素から成る簡易的モデル化を検討し、安全の原理の展開を試みた。

次に、既存のリスク低減方策に加えて、ICT 機器を利用した新たなリスク低減方策として 3 ステップメソッドにおけるステップ 2 に ICT 機器を適用する方法として、市販されている Bluetooth Low Energy (BLE) タグの安全関連用途への適用を検証する一環として、PFH_D を低減する方法論とその実現可能性について検討を行った。その結果、二重化システムの構築やバッテリー充電時のリセットによる機能診断など、適切な安全設計が施すことができれば、安全制御関連システムが要求する危険側故障発生確率をクリアする可能性は高いことが確認された。

また、3 ステップメソッド適用後の残留リスクに対して ICT 機器を適用して人の注意力のみに依存しない支援的保護システムの提案を行った。さらに、実現場に導入した支援的保護システムと行動分析学の課題分析を組み合わせることにより、作業者とフォークリフトの接触災害によるリスクを可視化できることが確認された。

キーワード: 高機能安全装置, 支援的保護システム, リスクアセスメント, リスク低減方策, ヒューマンエラー, ICT 機器

1. はじめに

近年、生産現場では、非正規雇用者や短期労働者、外国人労働者の割合が増加する一方で、現場の安全を長年支えてきたベテラン作業者の割合が減少傾向にある。また、1 人作業の増加やコミュニケーション不足から、従来のように「人に頼る安全管理対策」には限界が来ている。特に、単体の機械を複合的に組み合わせた統合生産システム (Integrated Manufacturing System: IMS) を導入した生産現場では、危険点近接作業（作業者が機械の可動部を停止させずに可動部に近接した状態で行う運転確認、調整、加工、トラブル処理、保守・点検、修理、清掃、除去などの作業）において、経験の少ない作業による労働災害が依然として高い割合で発生している。また、近年は安全領域と危険領域を分離する作業形態から、人と機械の共存・協調型作業形態へと変化しており、

機械安全の原則である「停止と隔離」だけでは十分なリスク低減ができず、高い残留リスクが残存している。このように現状では、IMS を導入した生産現場では、いまだ人の注意力に大きく依存する安全管理体制により現場の安全のレベルが維持されている。今日、Connected Industries¹⁾や Industry4.0²⁾といった産業革命で求められている人と機械の共存・協調型作業形態においては、情報通信技術 (Information and Communication Technology: ICT) を利用した機器 (ICT 機器) の生産システムへの導入が進められている。このような生産システムを安全性と生産性を両立して運用するためには、保護装置と ICT 機器を組み合わせた安全管理を支援するシステムの構築が必要となるが、まだ十分検討されておらず、開発が急務である。

IMS において、通常作業中はガード内に作業者は侵入する必要がないため、作業者と機械は隔離をする形で安全を確保している。しかし、非常状態では、作業者は共存領域に侵入することになる。国際標準化機構が制定する国際規格 (International Organization for Standardization: ISO) 12100 では、このような非常作業においては、6.2.11.9 設定「(段取りなど), ティーチング, 工程の切り替え, 不具合 (障害) の発見, 清掃または保全」に規定されるように、各作業に対する制御

*1 労働安全衛生総合研究所 建設安全研究グループ。

*2 労働安全衛生総合研究所 機械安全研究グループ。

*3 労働安全衛生総合研究所 新技術安全研究グループ。

連絡先: 〒204-0024 東京都清瀬市梅園 1-4-6

労働安全衛生総合研究所 清水尚憲*1

E-mail: shimizu@s.jniosh.johas.go.jp

モードにおいては、以下の機能をすべて満たす特定の制御モードにより作業者の安全を確保しなければならない。

- ① 全ての他の制御モードを不作動にする。
- ② 機械の危険な要素の運転は、イネーブル装置、両手操作制御装置又はホールド・トゥ・ラン制御装置の操作を続けることにより許可する。
- ③ 機械の危険な要素の運転は、リスクが低減した状態においてだけ許可する（例えば、減速、低減した動力または力、段階的操作：例えば動作制限制御装置）。
- ④ 機械のセンサに対する故意又は無意識の行為で危険な機能が実行されることを防止する。この制御モードは、次の1つまたは複数の方策を組み合わせなければならない。

- ⑤ 可能な限り危険区域に接近することを制限する。
- ⑥ 非常停止制御器をオペレータのすぐ手の届く範囲に設置する。
- ⑦ 携行式制御ユニット（教示ペンダント）及び/又は局所用制御器（制御される要素を視認できる）。

一方、ISO12100「6.2.11.1 一般」では、制御システムの設計方針は、それらの安全関連性能が十分リスクを低減できるように選択しなければならないとしている。しかし、現在、非常作業において、上記に規定するような対策や適切な安全性能を持ったシステムがなく、人の注意力に依存しながら作業を行っているため、安全が確保できない作業環境が多く存在しているため、これらが原因となる危険事象での事故が発生している。

ICT 機器とは、情報通信技術（ICT）をもつ機器を指す情報技術（Information Technology: IT）よりも通信によるコミュニケーションの重要性を強調しているため、単なる情報処理にとどまらず、ネットワーク通信を利用した情報や知識の共有を重要視する機器である。この ICT 機器を用いた新たな安全管理システムを生産現場のリスク低減方策として使用することを考えた場合、以下に示す2通りの適用方法が考えられる（図 1-1 の①と②に対応する）。

- ① 安全防護（ガードまたは保護装置）の代替として使用する場合

リスクアセスメントに基づくリスク低減方策である安全防護物（ガード又は保護装置）と同等の安全度水準（Safety Integrity level: SIL）、要求パフォーマンスレベル（Required performance level: PLr）を満足する安全性と信頼性を持つ ICT 機器を3ステップメソッドのステップ2として適用する（安全防護物の代替として ICT 機器を使用する場合）場合が該当する。現在市販されている ICT 機器の多くは保護装置としての使用を目的としていないため、単体では保護装置としての安全の要件を満たすことは困難と考える。そのため、今後、保護装置との組み合わせで使用できる ICT 機器の開発や、複数の ICT 機器を組み合わせたシステムの認証制度の確立が求められる。

- ② 3ステップメソッドを適用した後の残留リスクに対して使用する場合

リスクアセスメントに基づき、3ステップメソッドである本質的安全設計方針、安全防護（保護装置、ガード）、付加保護方策により低減された残留リスクに対して、作業現場で行う適切な ICT 機器を組み合わせた支援的なリスク低減方策である。そのため、適用にあたっては、すでに実施されているリスク低減方策や安全管理対策な

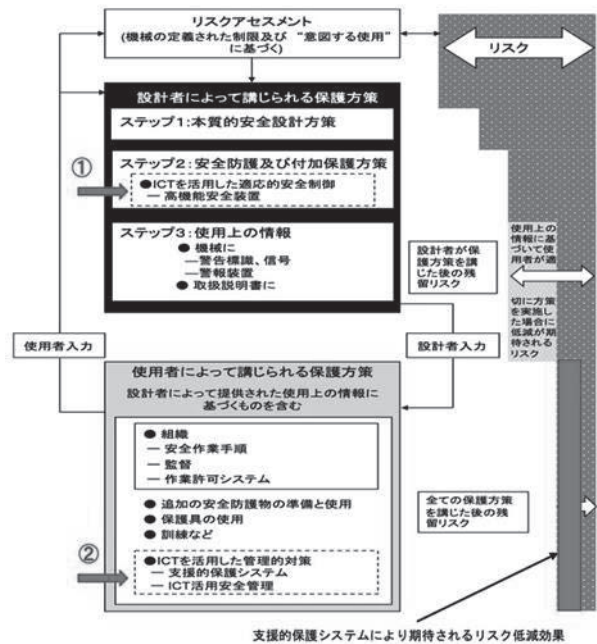


図 1-1 ICT 機器を活用したリスク低減方策の適用方法

どを代替として使用してはならない。また、設備の安全関連部に直接関与させずにはならず、作業者の実行の意志表示と行為に含まれるヒューマンエラーや意図的な不安全行動の発生確率を下げる事により、労働災害を防止することを目的に使用する。

本研究では、これらの検討を行うために以下の視点から検討を行った。

- ・協調安全を Connected Industries における次世代の機械安全の姿と位置付けるために物理層・データ層・論理層の3つの基本要素から成る簡易的モデル化を検討し、安全の原理の展開を試みる。
- ・Bluetooth Low Energy（BLE）タグの安全関連用途への適用を検証する一環として、 PFH_d を低減する方法論とその実現可能性について検討する。
- ・ICT 機器を支援的なリスク低減方策として活用するためのシステム試作と、実証実験によるリスク低減方策の妥当性検証を行う。

2. 協調安全の安全情報伝達に関する論理的考察

2.1. Cyber Physical System（CPS）の簡易モデル化と安全の原理

日本の次世代の産業の姿といわれる Connected Industriesでは、人・機械・環境の情報が Cyber Physical System³⁾（CPS）によって共有されることから、産業安全分野では、人を機械から隔離せずには協調安全が実現できると言われている。しかし、今まさに研究開発中の段階であるため、どのように情報を共有すれば協調安全とみなされるのか、などについての詳細はまだ明らかになってはいない。

ただし、協調安全を Connected Industries における次世代の機械安全の姿と位置付けるのであれば、その実現においては、ヒト・モノ・コトに関する情報をデジタル化することによって最適化や自律化に関する多様なサービスが生み出せるとされている CPS の中で他の技術分野と区別するためにも、安全制御に関する基本設計原則が CPS の中に落とし込まれている必要があろう。

そこで本章では「安全の原理」⁴⁾に着目する。CPS において安全情報がユネイトに伝達されるための条件を得るために、CPS を物理層・データ層・論理層の3つの基本要素から成るものとして簡易的にモデル化し、安全の原理の展開を試みる。

2.2 問題提起

2.2.1 現在の状況

Connected Industriesとは経済産業省が提唱する次世代の産業コンセプトである。極めて簡単にその概要を述べれば「Cyber Physical System (CPS) の中で展開される生産活動、モノづくりの姿」である。CPSの定義にはいくつかあるが電子情報技術産業協会 (JEITA) では、「実世界 (フィジカル空間) にある多様なデータをセンサーネットワーク等で収集し、サイバー空間で大規模データ処理技術等を駆使して分析/知識化を行い、そこで創出した情報/価値によって、産業の活性化や社会問題の解決を図っていくもの」としている。

このコンセプトに応じるようにして、産業安全分野でも CPS 中での新しい安全の実現に期待が高まっている。その一つに、機械が人から隔離されずに、人と共存し、共に作業をするための協調安全がある。これについて、一般社団法人セーフティグローバル推進機構 (IGSAP) の提唱する Safety2.0⁵⁾では「人・機械・環境の情報を共有すること」で上述の協調安全が実現できるとしている。しかし安全制御の基本設計原則に則ったCPSの構成が見えないため、何が・どうあれば、協調安全と認められるのか、議論そのものが難しい状況にある。

2.2.2 労働災害防止における問題

人と機械を隔離せずに済む協調安全の適用対象として考えられている機械は、現在のところ、主に次の2種類に大別できる。ひとつはロボット等の自動制御機械であり、他方は人間が運転操作をする車両系建設用機械及びこれに類似の機械である。

これら2種に適用される技術そのものを見ると、内容的に大きな違いはない場合も多い。しかし、事故が発生した場合に、両者に問われる「責任」には差異が生ずる。例えば、止まるはずの協働ロボットが止まらずに人に衝突してケガを迫わせた場合は、環境センシングや止まる仕組みの不具合が原因として追求されるだろう。一方、人が運転操作をする車両系建設用機械が止まらずに人に衝突した場合は、技術的原因はどうであれ、運転操作者の責任が最終的に問われるであろう。これは、前者の協調安全技術は保護装置として利用されているのに対して、後者は支援装置であり、その結果、責任の所在が異なると説明できる。しかし、これでユーザに対する説明責任は果たされるのであろうか。

また、CPS を活用した安全ではプログラムに潜在するバグなどの決定論的原因故障や労働者の個人に関する情報の管理に対して、運用段階でのリスク対応が必須となる。こうした事項も説明できなければならない。

後述するように労働災害は危険源が持つ有害なエネルギーが人間に到達して生じた危害を言う。現状では、このエネルギーの入出力制御が自動か手動かで、制御に係る責任は同一とは言いがたい。協調安全技術が本質的な安全を実現するものとして機械設計に最初から組み込まれるものなのであれば、その技術リスクは労働安全衛生規則第24条の13で努力義務とされている「機械に関する危険情報の通知」の対象となり得る。労働者をはじめとするユーザに、技術リスク及び安全に運用するための方法を説明するには、なんらかの枠組みを構築することが必要

と思われる。

2.2.3 安全の原理の必要性

技術の発展という観点では、CPSの中での安全制御システムは、従来の安全制御システムの概念や技術を発展させる形で構成されるものと考えられる。杉本らは「安全の原理」の中で、「安全は真に頼れるものでなければならず、安全の実現手段はその構造が公表されねばならない」とした。新しい技術を用いた安全制御システムであったとしても、そのシステムの根幹にある安全の概念は、これまでに十分に知られてきた安全の論理を踏まえていることが求められると考えられる。安全の論理を踏まえていれば、システムの構造が説明でき、その妥当性が理解される。

そこで、CPS を安全制御に用いる場合に何が要求されるのか、これまでに知られてきた安全の論理に照らして考察する。

2.3 安全 (確認) の原理

1999年に発行された安全工学の図書⁶⁾では、労働災害とは、有害なエネルギー (有害物質や位置のエネルギーも含む) が人間に到達して危害が及ぶことであると、有害なエネルギーが労働者に到達しない状態を安全な状態であるとしている。具体的には以下のように安全な状態を定めている。

【安全の状態とは】⁷⁾

- ① 危険源 (有害なエネルギー) がない状態、または、
- ② 危険源 (有害なエネルギー) があっても、人間が危害を受けることのないように対策がなされ、そのことが確認されている状態。

確認とエネルギー制御の視点から安全と労働災害防止対策を捉えているが、この思想はリスクの評価とその低減をベースとする現在の安全と全く矛盾しない。

上述の確認とエネルギーの関係は、「安全(確認)の原理」として、その論理構成が杉本らによって明らかにされている。以下にその概要を示す。

まず、安全を $S(t)$ 、危険を $H(t)$ とすると、式 2-1 が成立する。

$$\forall t, S(t) \wedge H(t) = 0 \quad (2-1)$$

安全な状態と危険な状態は同一の場所と時刻には発生し得ない。しかし、未来に向かって活動が行われるとき、将来起こる状況は事故か否かのいずれかであるにも関わらず、実際には、このいずれともわからない第3の状態、すなわち不安が存在する。この不安状態は、安全か危険かを予測する手段の不確実さから生ずる。そこで、この不安状態を $A(t)$ として、不安な状態も危険とみなすことにすれば、予測の不確実さを含む危険状態 $H_c(t)$ は式 2-2 のように表される。

$$H_c(t) = A(t) \vee H(t) \quad (2-2)$$

労働災害を防止するためには、本当は安全ではないのに、安全と予測することは許されない。これより、真の安全と予測される安全との間は、式 2-3 に表されるユネイトな論理関係になければならないとされる。これが安全 (確認) の原理である。

$$\overline{H(t)} \geq \overline{H_c(t)} \quad (2-3)$$

さらに、式(2-3)をもとに安全な状態のときのみ機械の

出力が許される論理構成は式(2-4)となる。これは安全作業の原理⁹⁾とされている。

$$\overline{H_c(t)} \geq U(t) \quad (2-4)$$

以上をまとめると、労働災害防止を目的とした機械の安全制御システムが満たすべき論理は式(2-5)となる。

$$\overline{H(t)} \geq \overline{H_c(t)} \geq U(t) \quad (2-5)$$

この論理式は、「エネルギーを持つ系（機械系）と人とが安全な共同作業を行う場合の構成条件として、安全を示す情報（安全情報）の生成から機械のエネルギー出力に至るまで、一貫してユネイトに伝達されねばならない⁹⁾」ことを示している。つまり、このユネイトな論理的関係がCPSでの安全情報伝達条件の基礎を与えるものである。

安全制御システムの実現方法として、以前は、確定論的な技術が使用されていたが、現在はコンピュータ制御技術による確率論的な技術が主流となっている。しかし、安全（確認）の原理の重要性は変わらず、安全情報の伝達は安全制御システム全体を通してユネイトな論理的関係にあらねばならない。すなわち、システムを構成する各要素の危険側故障の発生確率を許容値以下にするだけでなく、システム全体を安全情報伝達に関して危険側誤りが起こらない（その可能性を極力排した）構成とする必要があることを意味する。

2.4 CPSの簡易モデルを用いた考察

本研究では、協調安全が想定するCPSを、図2-1のように、物理層（エネルギーを扱う）・データ層（デジタルデータを扱う）・論理層（アルゴリズムを扱う）の3つの基本要素から成るものとして仮定する。

この簡易モデルでの協調安全の機能を次のように想定する：物理層（実空間）での人や機械などのモノの活動をセンシングデバイスを用いてデジタルデータ化し、データをデータ層に転写する。データ層には、実空間のデータが集積され、現実世界を映し出す仮想世界が構築される。論理層のアルゴリズムは、このデータを使って実空間での人や機械の動きを確認し、未来の安全を予測する。この結果に基づいて、機械や人の動作制御に関するデータが生成され、データ層から物理層にデータが伝えられることで人や機械が制御される。

前述した安全の原理の式(2-5)をこの簡易モデルに当てはめると、予想される安全 $(\overline{H_c})$ を3層が担うことになる。ここで、物理層、データ層、論理層で実行される処理をそれぞれ $P(t)$ 、 $D(t)$ 、 $L(t)$ で表すとすると、式(2-5)は式(2-6)のように書き表せる。

$$\overline{H(t)} \geq P(t) \geq D(t) \geq L(t) \geq U(t) \quad (2-6)$$

式(2-5)は、例えば、光電保護装置がダイレクトに動力源をシャットダウンするような場合に相当し、 $\overline{H_c(t)}$ には、安全状態の確認処理と安全制御系の操作出力の両方の意味が含まれているが、式(2-6)はこれらを明確に区別した表現と言える。ただし、実際には、アルゴリズムの判断結果はデータ層と物理層を経て最後に機械出力となるので、式(2-6)は式(2-7)のように表される。ここで、添字 i は物理層から論理層に向かう流れ、添字 o は論理層から物理層に向かう流れを示す。

$$\begin{aligned} \overline{H(t)} &\geq P_i(t) \geq D_i(t) \geq L(t) \\ &\geq D_o(t) \geq P_o(t) \geq U(t) \end{aligned} \quad (2-7)$$

図2-2は式(2-7)の模式図である。ここでの想定は、 $\overline{H(t)}$ が現実（真の安全）であり、 $P_i(t)$ が物理層でのセンサのデータ出力式(2-3)の安全確認信号 $\overline{H_c(t)}$ に相当)とし、 $U(t)$ がアクチュエータ出力で $P_o(t)$ は安全制御系がアクチュエータを操作する出力式(2-4)の $\overline{H_c(t)}$ に相当)である。

以下に、式より導かれる安全制御の構成条件を示す。

(1) 各層間でのデータ伝送において危険側の誤りが生じてはならない。

真の安全状態は物理層のみに存在するため、転写時に誤りが生じれば、以降の処理には危険側誤りが起こりうる。この誤りには例えば、物理層でIoTを用いてセンシングしたデータをデータ層に転写する際に生ずるデータの欠損や書き換えなどがある。この危険側誤りについては、産業サイバーセキュリティ研究会にて、フィジカル・サイバー間を正確に転写する機能の信頼性確保が必要であるとして、検討が進められている¹⁰⁾。

(2) 論理層でのアルゴリズムは安全の判断に関して危険側に誤ることは許容されない。

想定されるアルゴリズムには、対象空間の地図作成や、人や機械などオブジェクトの識別、状態および定位の推定、移動速度と方向の推定、衝突予測などが挙げられる。これらの推定の結果、実空間にいる労働者に危険を及ぼすおそれが生じてはならない。

(3) 各層は自らの正常性を確認できること。

各層が、実行する「安全確認および安全制御のための機能」および「機能を実行するハードウェアやソフトウェア」に故障などの異常が生じていないことを確認し、この確認が次の層に伝達されていくことを意味する。ここでの異常には、偶発故障と決定論的原因故障だけでなく、人の不正行為による機能不全も含まれる。データ層や論理層に権限のない者が容易に侵入できる状態である場合、アルゴリズムが危険側に誤るようなデータの書換えやソフトウェアの変更が行われる恐れがあり、この正常性確認の条件を満たしているとは言い難い。

(4) 層内および層間で時刻同期がとれていること。

式(2-7)のユネイトな論理関係を実現するためには、時刻 t の同期が取れていなければならない。予測される安全 $\overline{H_c(t)}$ には有効寿命が存在する¹¹⁾。安全は未来のある時刻に対して確認され、安全であると予測されているその時刻までエネルギー出力が許可されるためである。

層内および各層間での時刻が一致していなければ、予測の有効期間が保証されず、誤った時刻にエネルギー出力がなされるなどの危険が起こりうる。

2.5 協調安全を確立するために必要な検討事項

協調安全は、人・機械・環境の情報をCyber Physical System (CPS)で共有することで安全制御を実現しようとするものである。本章では、安全の原理に照らし合わせて、CPSでの安全情報伝達に係る条件抽出を試みた。まず、CPSを物理層・データ層・論理層の3つの基本要素で構成されるシステムとして簡易的かつ抽象的にモデル化し、各要素に論理変数を割り当てた上で安全情報がユネイトに伝達されるための条件を考察した。

この結果、伝達の条件として、①各層間でのデータ伝送には危険側の誤りが生じてはならないこと、②論理層でのアルゴリズムは安全の判断に関して危険側の誤りが生じてはならないこと、③各層は自らの正常性を確認できなければならないこと、④層内および層間で時刻同期がとれていることを得た。

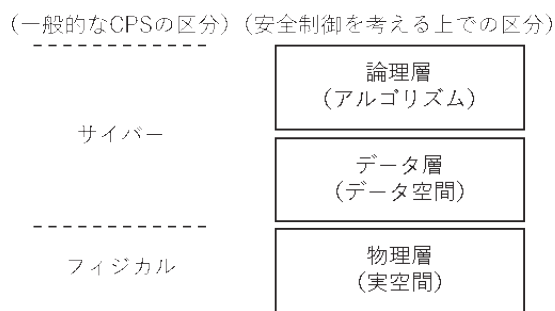


図 2-1 協調安全で想定される実世界と仮想空間の簡易モデル

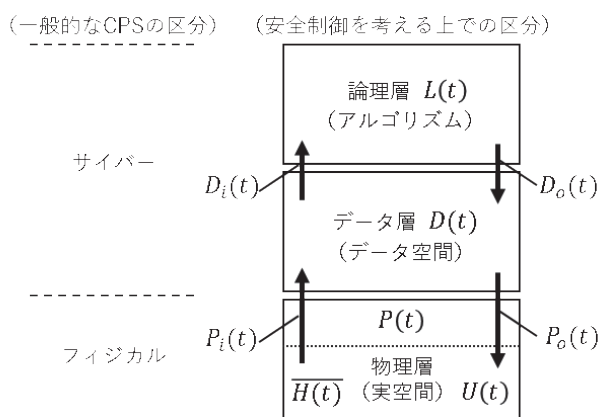


図 2-2 簡略化されたモデル時計算式との論理的関係

さらに CPS での安全では、安全情報伝達の条件にセキュリティとプライバシー保護を加えるべきことを示した。協調安全には、人の行動をコントロールする一面があり、データとアルゴリズムが人や機械の動きを決めることから、情報をもつエネルギー制御以外の側面も踏まなければならない。

今後は、CPS モデルを詳細化して検討を重ねると共に、各論理変数の内容を検討していく予定である。

3. Bluetooth を用いたスマートタグの安全関連用途への適用可能性の検討

3.1 Bluetooth タグの利用現状と安全性

近年、著しいデジタル無線通信技術の進展と普及に伴い、携帯又は身体に装着が可能な小型の IoT デバイスにより、所持品の位置特定や移動履歴の記録、あるいは、心拍数や血圧といった健康状態のモニタリングといったアプリケーションでの利用が広く浸透してきている¹¹⁾。これらのデバイスは一般にスマートタグと総称され、中でも、パーソナルコンピュータやカーナビゲーション装置、モバイル端末など他の電子機器との近距離無線通信方式に Bluetooth Low Energy¹²⁾ を用いたスマートタグ (以下、BLE タグと記す) は、省電力での作動が可能で、かつ、比較的省コストで実装できるなどの利点から安価で市販され普及が進んでおり、一部で、機械設備を使用する事業場での作業者の安全管理への応用も試み始められている。例えば、機械の操作、又は、設定・点検・トラ

ブル処理など非正常作業を実行する際に、特定の資格や権限をもつ作業者のみが作業を実施するように管理する方策として、これまでは、機械の起動や動作モード切替えを行う鍵を管理することや、危険区域に侵入する作業者が出入口で札を掲示することが主に行われてきた¹³⁾。これに代わり、清水らは、BLE タグを用いて作業者の危険区域内での位置情報や特定の出入口での入退情報を取得し、危険な機械への動力供給や動作機能の作動許可を制御・管理・記録するシステムを提案し、その有用性を報告している¹⁴⁾。

しかし、BLE タグを一部に使って実行される制御機能が、機械設備全体のリスク低減に大きく関与する安全機能であり、機能の失敗や故障がリスクの増加に直ちにつながる場合、BLE タグを含む制御システムには、実行する機能が担うリスク低減効果に応じてより低い危険側故障発生確率 (：単位時間当たりの危険側故障発生の平均確率、Probability of dangerous failure per hour. 以下、 PFH_D と記す) の達成が要求される^{15, 16, 17)}。しかし、Bluetooth を用いた通信機器に関する先行研究では、通信の速度や品質の向上・達成に関する報告^{18, 19, 20)} はあるものの、安全関連用途を想定した危険側故障に関する研究は調査の範囲では見当たらない。BLE タグの危険側故障により誤った資格権限情報に基づいて機械の危険な動作の実行が許可されれば、動力可動部の予期せぬ起動といったリスクに作業者が曝されることになる。

そこで、本章では、BLE タグの安全関連用途への適用を検証する一環として、 PFH_D を低減する方法論とその実現可能性について考察する。具体的には、まず、BLE タグを適用する安全関連用途として「作業者個人を識別し、所有する資格と権限に基づいて機械の作動を許可する」ことを想定し、その上で、 PFH_D を低減する手法として BLE タグを二重化構成とする設計の採用を掲げる。ただし、構成要素の二重化においては共通原因故障に対する方策の導入が不可欠であり、中でも、機器が使用される環境の温度、湿度、電磁妨害といった環境要因で発生する障害が PFH_D に大きく影響することを示す。この予備的検討に基づき、市販されている 3 種の BLE タグを対象に、機能安全規格にある要求レベルを参考にして試験基準を定め、電磁妨害に対するイミュニティ試験及び温湿度サイクル試験を実施する。得られた結果から、二重化した BLE タグで達成可能な安全性能を推定し、現状の機械設備で実装されている一般的な安全機能の一部に BLE タグを適用できる可能性について考察する。

3.2 安全関連用途に適用する BLE タグの条件

3.2.1 想定する安全関連用途

BLE タグが応用可能な安全関連用途には種々のものが考えられるが、本研究では「非正常作業において作業者個人を識別、保有する資格と権限を照合し、その条件に基づいて機械の特定の危険な動作・機能の実行を許可する」方策に用いることを想定する。

従来、このような用途は、起動や動作モード切替えをキー付きスイッチで行うように機械システムを構成した上でキーを管理する手順及び組織体制を確立するといった管理的方策で対処されるのが一般的であった。このとき、仮に権限のない作業者がキーを操作したとしても、それが機械システム全体のリスク低減に直接影響しない場合 (例えば、機械可動部が作業者に衝突するなどのリスクが別途講じた保護装置によって適切に低減されており、誤ったキー操作だけでは危険事象に至らない場合) では、上述のキー及びキー付きスイッチは安全関連とは見做されない。しかし、キー操作によって保護装置が無

効化され、危険区域内に人が進入した状況であるにもかかわらず、工具の設定や保守点検などの目的から機械が運転可能な状態になる場合には、キー管理に基づく運転許可の誤りが動力可動部の予期せぬ起動といったリスクの増加に直接影響するため、安全関連として必要な条件を満たさなければならない。

本章では、BLE タグを応用する用途が上記のような安全関連であることを前提に議論を進める。作業者個人の識別を、従来のキー管理に代えて BLE タグを用いた方策とすることで、システムの一部停止が機能的に可能になるメリットがある。

一方、BLE タグを用いて個人を識別する機能は、Bluetooth 通信にかかわる半導体チップに組み込まれた“デバイス ID”に基づいて実行されると想定する。現実の BLE タグのアプリケーションとしては、個人の識別情報に付加してタグを身に着けた者の現在位置や地表からの高度、あるいは、心拍数や呼吸回数などのバイタル情報などを伝送するのが一般的ではあるが、議論を容易にする目的から、本章では、BLE タグのデバイス ID が正しく伝送されれば、取得した ID から作業者の識別は実行できるものと仮定する。作業者の資格や権限を判定すること、ならびに、これらに応じて許可される機械の動作にかかわる動力制御などは、上位のコントローラで処理されるとする。よって、ここで問題となる BLE タグの危険側故障とは、「デバイス ID が何らかの理由で変化又は異なるデータとして外部に出力されてしまい、所有する作業者を誤認識する」とことと定義できる。BLE タグが一時的に機能障害に陥ることや動作停止することを含めてデバイス ID が伝送されないことは故障ではあるが、危険側故障とは見なされない。

3.2.2 BLE タグの動作原理と基本構造

BLE タグは分類としてはいわゆるアクティブ RFID (Radio Frequency Identification) タグに含まれるが、スマートフォンの BLE 対応と Apple 社開発の iBeacon に採用されて急速に普及している。

無線機器は通常親機と子機に分かれるが、図 3-1 に示すように BLE では親機をセントラル、子機をペリフェラルと呼び、ペリフェラル機器は接続待ちの間、定期的なアドバタイズを発信している。このアドバタイズにはペリフェラル機器の名前や属性データを含めて発信することができる。一方、セントラル機器はスキャンすることによってアドバタイズを受信することにより、周囲に存在するペリフェラル機器を知ることができ、見つけたペリフェラル機器の中から 1 対 1 の通信接続をしたい相手を選び、接続要求を送信できる。ペリフェラル機器がアドバタイズ発信後に接続要求を待っており、このタイミングで接続要求を受信すると 1 対 1 の接続通信に切り替える。

この 1 対 1 の接続通信を GATT(Generic ATTribute Profile) 通信と呼び、ペリフェラル機器がセントラル機器に公開して共有するデータ構造 (キャラクタリスティック) を介してデータのやりとりが行われる。これらのキャラクタリスティックには UUID(Universally Unique Identifier) という 16 バイトの一意番号が付けられ、セントラル機器は UUID を指定してキャラクタリスティックのデータ内容にアクセスする。

タグタイプのペリフェラル機器のハードウェア構成は、コアモジュールと呼ばれるシリコンモノリシック集積回路内に、RAM 搭載の専用チップ (例えば Nordic 製 nRF52832 など) を混成集積する形が多い。このとき、GATT 通信を含む通信のレイヤーに対応するソフトウェアにファームウェアが書き込まれ、上記固有の ID も

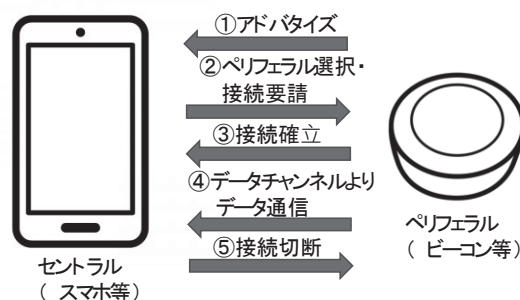


図 3-1 BLE 機器構成と通信方法

書き込まれる。ユーザはアプリケーションレイヤーでプロフィールを規定して書き込むことができるが、デバイス特有の ID はメーカーが SIG (Special Interest Group) 認証取得時に書き込んで変更することはできない。

3.2.3 BLE タグの PFH_D 低減方策

現在、産業機械分野で安全関連系の設計基準と一般原則を規定する規格には JIS B 9705-1 と JIS B 9961^{注1)} の 2 つがある。JIS B 9705-1 は機械の安全機能を実行する制御システムを設計する際の技術区分や一般原則を定めた規格として欧州で 1990 年代から使用されてきた EN 954-1 から発展した規格、一方、JIS B 9961 は発電所や化学プラント等に対する機能安全技術の一般要求事項を定めた IEC 61508 を基に、そのフレームワークを機械の電気・電子制御システムに適用した規格で、システムの計画から廃棄までの全ライフサイクルを対象に人・組織・技術の総合的なマネジメントを要求している点に特徴がある。両規格とも機械の安全関連系に対する要求事項を扱いながら、制定の経緯の違いから、例えば、信頼性評価の方法や危険側故障回避のために採用される技法に対する価値付けなど細部が異なるが、安全関連系の設計原則として重視されている事項には共通する点がある。

その一つが、対象とする制御機能が機械設備全体のリスク低減に寄与し、その故障がリスクの増加に直ちにつながる場合、当該制御機能は「安全機能」と同定され、この機能の実行に関連する制御システム部分 (以下、安全関連系と記す) には意図したリスク低減効果に応じた PFH_D の低減を要求している点である。JIS B 9705-1 と JIS B 9961 の安全機能に対して適用される PFH_D の基準を表 3-1 に示す。JIS B 9705-1 ではこの基準を Performance Level (PL) と呼び PL a~PL e の 5 段階に、また、JIS B 9961 では Safety Integrity Level (SIL) と呼び SIL 1~SIL 3 の 3 段階にそれぞれ区分している。

表 3-1 安全機能に適用される PFH_D の区分

JIS B 9705-1 Performance Level (PL)	単位時間当たりの危険側故障発生率の平均確率 PFH _D	JIS B 9961 Safety Integrity Level (SIL)	
PL e	10 ⁻⁸ 以上 10 ⁻⁷ 未満	SIL 3	
PL d	10 ⁻⁷ 以上 10 ⁻⁶ 未満	SIL 2	
PL c	10 ⁻⁶ 以上 3.0×10 ⁻⁶ 未満	SIL 1	
PL b	3.0×10 ⁻⁶ 以上 10 ⁻⁵ 未満		
PL a	10 ⁻⁵ 以上 10 ⁻⁴ 未満	該当なし	

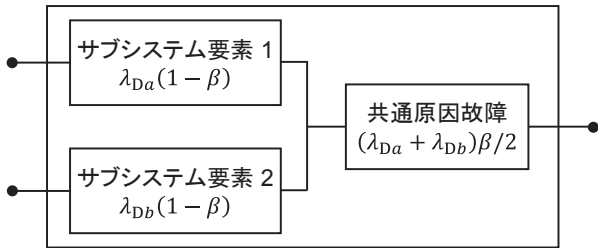


図 3-2 構成要素が二重化されたサブシステムの論理的信頼性モデル (JIS B 9961 図 3-8 に著者加筆)

陰側故障率 λ_D が各々 λ_{Da} 、 λ_{Db} で表される要素を二重化したアーキテクチャにおいてこのサブシステム全体^{注2)}の信頼性を論理的に表現したモデルを図 3-2 に示す。ただし、このサブシステムが作動要求頻度が年 1 回を超える高頻度作動要求モードで運用されるとする。この場合、JIS B 9961 の単純化手法に従えば、 PFH_D は次式で推定される。

$$PFH_D = (1 - \beta)^2 \lambda_{Da} \lambda_{Db} T + (\lambda_{Da} + \lambda_{Db}) \beta / 2 \quad (3-1)$$

ここで、 β は要素の全故障に対して 1 つの事象に起因して冗長化された系統が同時に故障する共通原因故障が占める割合 (以下、共通原因故障係数という。)、 T はシステムのすべての故障、障害、劣化を検出し必要があれば修復を施す診断テストの実施間隔 (以下、ブルーテスト間隔という。)である。サブシステム要素 1, 2 が同じ設計で、 $\lambda_{Da} = \lambda_{Db} = \lambda_D$ である場合、式 3-1) は次式となる。

$$PFH_D = (1 - \beta)^2 \lambda_D^2 T + \lambda_D \beta \quad (3-2)$$

現在のところ、産業機械分野では、制御機能が安全機能と位置付けられる場合、それを実行する安全関連系には少なくとも PL c 又は SIL 1 以上のレベルが要求されるのが一般的である。

また、低い PFH_D を達成するシステム構成 (ハードウェアアーキテクチャ)の考え方にも共通する点が見られ、両規格とも、構成要素の冗長化、ならびに、要素の故障を検出する定期的な診断テストの導入によって PFH_D が低減できるとしている。例として、単位時間当たりの危

表 3-2 共通原因故障係数 β の簡易推定で評価する側面 (JIS B 9705-1 表 F.1 と JIS B 9961 表 F.1 に著者加筆)

評価の側面	JIS B 9705-1 が掲げる項目	JIS B 9961 が掲げる項目
分離又は隔離	<ul style="list-style-type: none"> 信号経路間の物理的な分離、例えば、 <ul style="list-style-type: none"> 配線及び配管での分離 動的試験によるケーブルの短絡及び断線の検出 各チャンネルの信号経路の個別シールド プリント基板上での回路間の十分なクリアランス及び沿面距離 	<ul style="list-style-type: none"> 各チャンネルの信号ケーブルは、すべての場所で他のチャンネルから分離して配線されているか又は十分にシールドされているか。 情報のエンコーディング/デコーディングが使われる場合、信号伝送誤りの検出が十分に行われるか。 安全関連系の信号ケーブル及び電源ケーブルは、すべての場所で分離されているか又は十分にシールドされているか。 サブシステム要素が共通原因故障を生じることがある場合、それらは局所的なエンクロージャに収納した物理的に別個のデバイスとして用いられるか。
多様性及び冗長性	<ul style="list-style-type: none"> 異なる技術的方式、設計又は物理的原理の使用、例えば、 <ul style="list-style-type: none"> 第 1 チャンネルは電子又はプログラマブル電子方式、第 2 チャンネルは電気機械式のハードワイヤ方式 安全機能の各チャンネルは異なる信号によって始動 (例えば、位置、圧力、温度) デジタル及びアナログによる測定 (例えば、距離、圧力又は温度) 異なる製造業者によるコンポーネント 	<ul style="list-style-type: none"> サブシステムは、異なる電気技術方式のチャンネルを用いているか。例えば、一方をプログラム式デバイス、他方を電磁リレーにするなど。 サブシステムは、異なる原理を用いる要素を使用しているか。例えば、ガードドアにおける検出器として機械式のものや磁気式のものを用いるなど。 サブシステムは、機能の作動及び故障モードが異なる要素を使用しているか。 サブシステム要素は、間隔 1 分以下の自己診断機能をもつか。
設計、適用又は経験	<ul style="list-style-type: none"> 過電圧、過圧力、過電流、過熱などに対する保護 使用のコンポーネントは“十分吟味されている” 	<ul style="list-style-type: none"> 診断テストに用いられるものを除き、サブシステムのチャンネル間のクロス接続は防止されているか。
査定及び分析	<ul style="list-style-type: none"> 制御システムの安全関連部の各部分に対して、FMEA が実施されており、その結果は、設計段階において共通原因故障を回避するために考慮されている。 	<ul style="list-style-type: none"> 共通原因故障を見つけるために FMEA の結果を調べたか。共通原因故障の原因を計画的に除去したか。
設計者の適格性 (能力)	<ul style="list-style-type: none"> 共通原因故障の原因及び結果を理解できるような設計者の訓練 	<ul style="list-style-type: none"> サブシステム設計者は、共通原因故障の原因及び結果を理解しているか
環境要因	<ul style="list-style-type: none"> 電気/電子システムに対して、適切な規格 (例えば、JIS C 61326-3-1) に従った共通原因故障に対する汚染及び電磁妨害の防止。 流体システム：圧力媒体のろ過、ほこりの侵入の防止、圧縮空気の水抜き、例えば、圧力媒体の純度に関してはコンポーネント製造業者の要求事項に従う。 温度、湿度、衝撃、振動のような全ての環境関連 (例えば、関連の規格で規定される) の影響に対して耐性の要求事項を考慮する。 	<ul style="list-style-type: none"> サブシステムは JIS C 61326-3-1 で指定した限界までの (限度値を含む) 電磁妨害からの過酷な影響に耐えるか。 サブシステム要素は、外部の環境制御なしに常に試験時に適用した温度、湿度、腐食、ほこり、振動などの範囲内で作動するか。

表 3-3 イミュニティ試験及び温湿度サイクル試験の項目、主な仕様及び性能判定基準

試験項目	方法及び手順	試験レベル	性能判定基準
放射イミュニティ試験	JIS C 61000-4-3	強度:最大 20 V/m, 周波数:80 MHz~1.0 GHz, 水平及び垂直偏波, 80% AM 変調正弦波 (1 kHz)	DS(安全用途での使用が意図された機能を維持しているかについての判定基準)
		強度:最大 10 V/m, 周波数:1.4 GHz~2.0 GHz, 水平及び垂直偏波, 80% AM 変調正弦波 (1 kHz)	
		強度:最大 3 V/m, 周波数:2.0 GHz~3.0 GHz, 水平及び垂直偏波, 80% AM 変調正弦波 (1 kHz)	
静電気放電試験	JIS C 61000-4-2(卓上装置に対する直接印加)	接触放電:±8.0 kV, 印加箇所:露出導電部, 放電回数:各箇所 10 回	DS
電源周波数磁界試験	JIS C 61000-4-8(浸漬法)	強度:30 A/m, 周波数:50 Hz 及び 60 Hz	DS
温湿度サイクル試験	JIS C 60068-2-38	低温サブサイクルを含む 24 時間サイクルを 5 回, 低温サブサイクルを含まない 24 時間サイクルを 5 回(計 10 回) 試験開始前に, 標準予備乾燥状態に 24 時間放置	DS

本章では,安全関連用途で利用する BLE タグの PFH_D を低減する設計方策として図 3-2 に示す二重化構成の採用を提案する.ただし,式 3-1),式 3-2) では, β の値と λ_D の値のオーダの違い(β が 0.1~0.005 をとるのに対し, λ_D は例えば I/O が 256 点の汎用 PLC で 10^{-6} ~ 10^{-7} [1/h] とされる²¹⁾) から,多くの場合,右辺第二項が支配的となることが知られている²²⁾.すなわち,二重化構成の採用によって PFH_D の低減が図れるか否かは,共通原因故障係数 β に大きく左右されることになる.

なお, JIS B 9705-1 と JIS B 9961 では,さらに PFH_D の低減が必要な場合,多重化された要素が互いに処理結果や出力を自動的に監視し合う自己診断機能の導入が求められるが,このような機能が組み込まれた BLE コアは現時点では一般に普及してはいない.このため,本章では,図 3-2 に示す自己診断機能のない単純な二重系を前提に議論を進めることとする.

3.2.4 共通原因故障係数の簡易推定

電気・電子・プログラマブル電子安全関連系のハードウェアの共通原因故障の影響を定量的に評価する包括的な手順については, JIS C 0508-6²³⁾ の附属書 D に詳細に述べられており,中でも β 係数法が広く知られている.これは,設計製造段階で導入される共通原因故障を低減させる方策をいくつかのカテゴリごとに分類して列挙し,それぞれの方策に特定のスコアを定め,実際に導入された方策に応じたスコアの合計値から β を 0.5~10% の幅で推定する手法である.これに基づき,機械の制御システムへの適用を考慮して, JIS B 9705-1 と JIS B 9961 では β の推定により簡易化されたアプローチを採用している. β を推定する際に評価する項目として JIS B 9705-1 と JIS B 9961 が掲げる項目を表 3-2 に示す.両規格で評価される項目は概ね同一であり,大別すると次の 3 つの側面にまとめられる.

- ① 採用したアーキテクチャ,配線の配置・仕様,使用する要素や部品の選定など設計・製造に関わる側面.
- ② 故障解析の実施など設計の正当性及びそれに携わる設計者の技量や適格性に関わる側面.
- ③ 機器が使用される環境の温度,湿度,電磁妨害とい

た環境要因に起因して生じる故障の排除及び防止方策に関わる側面.

上記のうち,①は技術的工夫によって,②は開発人員環境の整備によって対処されることになる.これらに対し,③については BLE コアの基本回路設計に依存する事項であり,一般的に入手可能な規格化されたデバイスの耐環境性能が十分なものでないのであれば,解消することは極めて困難である.

なお,Bluetooth で相互通信する機器のうち,親機にあたる受信機については,環境要因の影響が許容できるレベル以下となるように設置場所や運用方法を特別に配慮するなど,デバイス以外のアプローチで環境要因に起因する故障を回避・抑制することも考えられる.しかし,子機にあたる BLE タグについては,それを身体に装着又は携帯した作業者が活動・滞在する工場内の様々な場所(例えば,製造工程上発生する高温多湿区域や低温区域,稼動している大型電動駆動機や溶接加工機の周辺)の環境条件に曝されることを前提とする必要がある.

この点に関し,Bluetooth を用いた通信機器を扱った先行研究では,通信の速度や品質の向上・達成に関する報告はあるものの,安全用途を想定した危険側故障に関する研究,中でも使用環境要因に起因する故障について報告しているものは,調査した範囲では見当たらなかった.そこで,本章では,使用される環境の温度,湿度,電磁妨害といった環境要因で発生する BLE タグの障害について,機能安全規格にある要求レベルを参考にして試験基準を定め,電磁妨害に対するイミュニティ試験及び温湿度サイクル試験を行って危険側故障発生の実態を見ることとした.

3.3 BLE タグの耐環境性能試験

3.3.1 試験項目と性能判定基準

本節で市販の BLE タグに対して実施したイミュニティ試験及び温湿度サイクル試験の項目,主な仕様及び性能判定基準を表 3-3 に示す.

イミュニティ試験については,特に指定のない一般工業環境において SIL 1~3 の安全関連系での使用を意図した装置に対するイミュニティ要求事項を定めた JIS C 61326-3-1²⁴⁾ に基づいて設定した.この規格は,交流 1.0

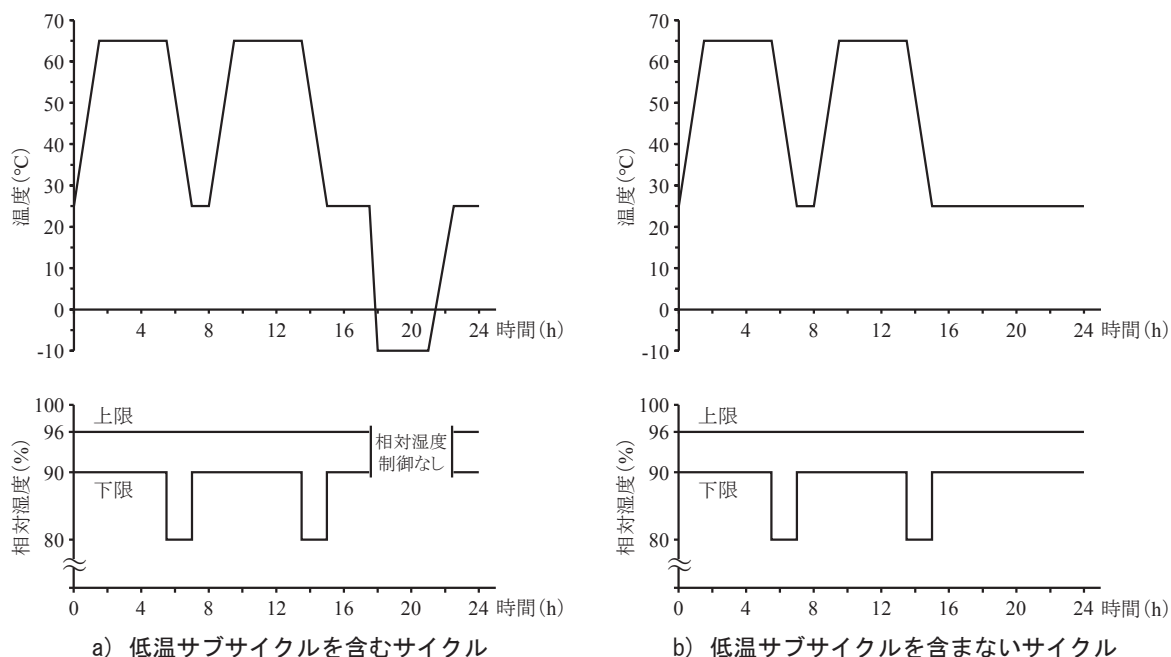


図 3-3 設定した 24 時間温湿度サイクル

kV 以下又は直流 1.5 kV 以下の電源又は電池で動作する装置全般の電磁両立性（EMC：Electromagnetic compatibility）に関する一般要求事項を扱う JIS C 61326-1²⁵⁾ の内容に加え、安全機能の遂行を意図した制御システム及び電気・電子装置のための要求事項を規定したものである。電磁現象が引き起こす危険側故障を回避するための対応策として JIS C 61326-1 よりも厳しい試験レベルが指定されており、結果として、作動要求時の失敗確率などのハードウェアの安全度の定量化に当たって電磁現象の影響を考慮する必要があるがこの規格への適合をもたなくなることが箇条 4 に記されている。

ただし、安全性を考慮して、放射無線周波電磁界試験（以下、放射イミュニティ試験という。）について、規格では最高 6.0 GHz（電界強度 3.0 V/m）までの電磁界印加が要求されているが、本研究では、国立研究開発法人情報通信研究機構の主導で実施されている多種無線通信実験プロジェクト（Flexible Factory Project）の一環として 2019 年に行われた稼働中の工場での電磁ノイズ測定で、「溶接工程、プレス工程、鋳造工程、金属加工工程、組み立て工程等において、大型の製造機器があっても、1.0 GHz を超える周波数帯でノイズは観測されていない」と報告されていること²⁶⁾を参考にして、表 3-3 に示すように試験範囲をマージンを取って 3.0 GHz までとした。



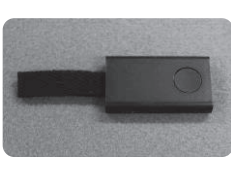
さらに、静電気放電試験について、JIS C 61326-3-1 では ±6.0 kV の接触放電と ±8.0 kV の気中放電の印加が規定されているが、本試験で実施したところ試料 B 及び V について 8.0 kV では気中放電を発生させることができず、このため、電圧を ±8.0 kV とした接触放電に代えることとした。また、放電回数について、JIS C 61326-3-1 では「SIL3 の用途で用いることを意図した装置の場合、放電回数は基本規格で規定する回数の 3 倍にする」との注記があるが、本研究では BLE タグが SIL 3 (PL e) が求められるほどの安全機能に利用されることは推奨しないため、基本規格である JIS C 61000-4-2²⁷⁾に従い、各印加箇所それぞれ 10 回と設定した。

一方、温湿度サイクル試験については、高温高湿及び

低温の条件で電気・電子部品の劣化を評価する温湿度組み合わせ(サイクル)試験を規定した JIS C 60068-2-38²⁸⁾ に基づいて試験方法を決定した。この規格の試験は、周囲温度の変化による呼吸作用及び浸入した水分の氷結作用の影響を検証することを目的としたもので、他の規格が規定する試験と、①規定時間内での温度変化の回数が多いこと、②温度変化の速度が速いこと、③0°C以下の低温条件を含んでいることなどの点で異なっている。本研究では、BLE タグを作業者が携帯/装着して工場内の様々な場所を移動することを想定しており、この想定に上述の特徴が合致することから選択した。この規格では、低温サブサイクルを含む 24 時間サイクル 5 回と低温サブサイクルを含まない 24 時間サイクル 5 回を組み合わせ、計 10 回のサイクル実行が要求されている。これに従い、本研究では許容範囲内で最も温度変化が急な条件となる図 3-3 a), b) に示すサイクルを設定し試験を行った。

また、性能判定基準“DS(Defined State)”は、機能安全の分野で安全用途の機能だけに適用する目的で定義された基準であり、EUT(Equipment under test)が電磁現象に曝された場合、その影響を受けずに機能し続けるか、又は、定義した状態に移行することが要求される。安全関連用途において、定義した状態とは、一般に、EUT 及び関連する被制御系が安全な状態を達成するか又は維持することを意味し、第 3.1 節で述べたように「BLE タグのデバイス ID が変化せず、かつ、異なるデータとして外部に出力されない」状態となる。BLE タグの動作停止や一時的な機能障害の結果としてデバイス ID が伝送されない状態はこれに含まれ、その後正常に復帰する限り、許容される。

表 3-4 被試験機器 (EUT) としての BLE タグの主な仕様

	試料 A	試料 B	試料 C
外 観			
製品名	MEDiTAG	Polar OH1	Qrio Smart Tag
製造元	ホンデン(株)	ポラール・エレクトロ・ジャパン(株)	Qrio(株)
寸 法	39 × 25 × 10 mm	φ 30 × 9.5 mm	46 × 26 × 8.5 mm
質 量	8.0 g	8.5 g	10.0 g (電池含む)
通信方式	Bluetooth 4.0 Low energy	Bluetooth 4.0 Low energy	Bluetooth 4.0 Low energy
電 源	Li-ion 二次電池	Li-ion 二次電池	CR 系一次電池 (CR2032)
連続作動時間	約 16 時間	約 12 時間	—
主な用途	オフィスや工場において、装着者の位置や高度、あるいは心拍数などのバイタル情報を専用受信機(親機)を介してクラウドサーバに送信する。	ランニングや水泳など運動中、装着者の心拍数を光学式センサーで計測、スマートフォンのアプリケーションソフトに送信する。	鍵や財布などに取り付け、スマートフォンからの操作でブザーを鳴らし、存在位置を知らせる。逆に、ボタン操作でスマートフォンを鳴らせることも可能。
参照先	https://www.hosiden.co.jp/meditag/	https://www.polar.com/ja/products/accessories/oh1-optical-heart-rate-sensor	https://qrio.me/smarttag/

3.3.2 被試験機器 (EUT)

本節では、入手可能な市販 Bluetooth デバイスから表 3-4 に示す 3 種を EUT として選定し、それぞれ 3 台を対象にイミュニティ試験及び温湿度サイクル試験を行った。いずれも安全関連用途での利用を目的とはしておらず、また、通信方式は Blue-tooth 4.0 Low energy である。ただし、試料 A は専用の受信装置を親機とし、試料

B 及び C は一般のスマートフォンを親機としている点が異なっている。また、試料 A 及び B は Li-ion 二次電池を内蔵した充電式であるが、試料 C は CR 系一次電池駆動である。

3.3 試験の方法及び結果

3.3.1 放射イミュニティ試験

放射イミュニティ試験は、各試料について、一度に 3

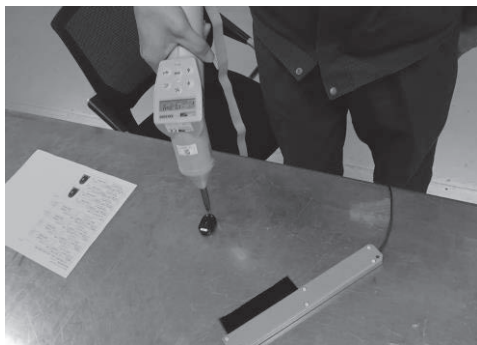


図 3-5 試料 A の静電気放電試験の様子

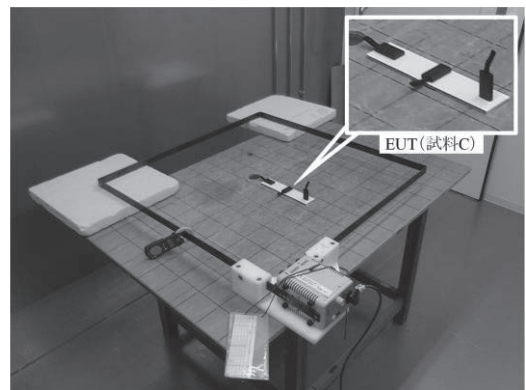


図 3-6 試料 C の電源周波数磁界試験の様子

表 3-6 各試料の接触放電箇所


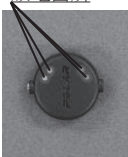
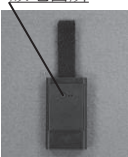
試料 A	試料 B	試料 C
放電箇所 	放電箇所 	放電箇所 
1cm ↔	1cm ↔	1cm ↔
充電用電極 (2 点)	充電用電極, データ伝送用電極 (4 点)	電池カバー固定ビス (1 点)



図 3-7 温湿度サイクル試験の様子

台ずつ、表 3-3 に示した強度及び周波数範囲の電界を水平・垂直偏波の両方で 1% の周波数ステップで順次放射していく方法で行った。放射イミュニティ試験の基本規格 JIS C 61000-4-3²⁹⁾ に従い、搬送波信号は、実際の妨害を模擬するとされる 1 kHz の正弦波による 80% 振幅変調とした。また、3 台の EUT は、電波暗室内の木製テーブル上に、事前に校正した均一領域内で、電磁界発生アンテナに対して正面、側面、上面が対峙する向きに配置した。例として、試料 A の試験の様子を図 3-4 に示す。一度の実施ごとに EUT の向きを変え、試験を 3 回行うことで、1 台につき、正面、側面及び上面の 3 方向から放射電界を受けるようにした。

危険側故障発生の確認は、表 3-5 に示す計 42 回の強度、周波数のタイミングで、一時的に電界放射を中断し、各 EUT が発信するデバイス ID を読み取ることで行った。また、試験環境として、試料 A については、東京都立産業技術研究センター多摩テクノプラザの電波ノイズ試験室 (20℃, 48%RH)、試料 B 及び C については労働安全衛生総合研究所の 3m 法電波暗室 (22℃, 52%RH) にて試験を行った。また、イミュニティ試験装置(電界発生器)として、試料 A では Amplifier Research 社製 1000W1000C 及び 240S1G3A を、試料 B 及び C には Rohde & Schwarz 社製 SMB100A/02 を用いた。

試験の結果、すべての試料 3 台とも、表 3-5 に示したタイミングで危険側故障は発生せず、デバイス ID 変化は確認されなかった。それぞれ機能的にも正常に作動し、異常は一切なかった。

3.3.2 静電気放電試験

放射イミュニティ試験を経た各試料 3 台について、JIS C 61000-4-2 の卓上形機器に対する試験環境設定(試験セットアップ)に准じ、シールドルーム内にて表 3-3 に示した電圧で接触放電試験を行った。例として、試料 A の試験の様子を図 3-4 に示す。放電の印加箇所は、表 3-6 に示すように、各試料の露出金属部(背面にある充電用電極又は電池カバー固定ビス)とし、各箇所にて +8.0 kV と -8.0 kV を 10 回ずつ印加した(なお、表 3-6 において、試料 A の中央部は緑色光学脈波センサの投受光部である)。試験環境として、試料 A については、東京都立産業技術研究センター多摩テクノプラザのシールドルーム (20℃, 36%RH)、試料 B 及び C については労働安全衛生総合研究所のシールドルーム (25℃, 28%RH) にて試験を行った。また、静電気放電発生器として、試料 A では EMC Partner 社製 ESD3000 を、試料 B 及び C には(株)ノイズ研究所製 ESS-B3011 を用いた。

試験の結果、試料 A については、-8.0 kV 印加時に 2 台で、+8.0 kV 印加時に 3 台とも、一時的な作動不能が起き、緑色光学脈波センサが消灯した。しかし、デバイス ID が変化することはなく、いずれもリセットを兼ねた再充電操作で直ちに正常復帰した。また、試料 B 及び C については、3 台とも特段の異常は見られず、デバイス ID 変化は確認されなかった。

3.3.3 電力周波数磁界試験

各試料について、JIS C 61000-4-8³⁰⁾ の卓上形機器に対する試験環境設定(試験セットアップ)に准じ、一度に 3 台ずつ、表 3-3 に示した強度及び周波数の連続磁界内に 1 分間さらす浸漬法で電力周波数磁界試験を行った。例として、試料 C の試験の様子を図 3-6 に示す。放射イミュニティ試験と同様、一度の実施ごとに EUT の向きを変え、試験を 3 回行うことで、1 台につき 3 方向から磁界にさらされるようにした。すべての試料について、

誘導コイルには 1 m×1 m の正方形の標準誘導コイル (EMC Partner 社製 MF-1000) を用いた。また、試験環境は、試料 A については、東京都立産業技術研究センター多摩テクノプラザのシールドルーム (20℃, 36%RH)、試料 B 及び C については日本品質保証機構安全電磁センターのシールドルーム M-1 (24℃, 44%RH) にて行った。

試験の結果、すべての試料 3 台とも、デバイス ID 変化は確認されず、機能的にも正常に作動を継続した。

3.3.4 温湿度サイクル試験

以上のイミュニティ試験を経て、すべての試料 3 台に対し、JIS C 60068-2-38 に基づく温湿度サイクル試験を労働安全衛生総合研究所の温湿度試験器(楠本化成(株)ETAC 事業部製 TH403HA)を用いて行った。試験の様子を図 3-7 に示す。規格では「スイッチを切った状態で温湿度サイクルを行うこと」とされているが、本試験では、実際の使用状況をより再現することを意図し、試料 A 及び B については毎サイクル開始前に十分充電し、槽内で可能な限り連続作動させた状態で、また、試料 C については電池交換はせずに作動を継続させたまま、サイクルを実施した。危険側故障の発生は、試験開始時と終了時にデバイス ID を読み取ることで確認した。なお、実際の使用状況を再現することに加え、充電用電極部を保護することからも、試験中、試料 A には製品付属のゴム製リストバンドを、試料 B には付属の樹脂製専用カバーを装着した。

図 3-3 a), b) に示す温湿度サイクルを各々 5 回ずつ実施した結果、すべての試料 3 台とも、特段の異常は一切見られず、デバイス ID 変化は確認されなかった。

3.3.5 イミュニティ試験及び温湿度サイクル試験の考察

以上のように、イミュニティ試験及び温湿度サイクル試験の結果、すべての試料において危険側故障として定義したデバイス ID 変化は確認されなかった。

なお、BLE 自体は Wi-Fi と共通の 2.4GHz 帯を使用するため、混信により電波干渉によるデータ情報誤りは起こりえる。しかし、ファームウェアとして書き込まれた固有のデバイス ID が書き換わるためには、ペリフェラル機器であるタグ側へ強力なパワー(電力)が注入されてオーバーライトされる可能性しか考えにくい。

一般的に、電子デバイスの外部から強力な電磁界が放射されてそのエネルギーがデバイス内部回路に影響を与えるためには、電源ケーブル等の有線による電磁誘導かアンテナ等の導体部からの電波受信が想定される。しかし、BLE タグはバッテリー駆動のため電源ケーブルは存在せず、アンテナはプリント基板上に高利得で無指向性のチップアンテナ (3×5mm 程度が多い) が搭載されるため、過大な入力を受けにくく、また、通常内部チップの損傷を防ぐ目的で電圧リミッタ回路が内蔵される。さらには、モジュールは金属筐体で覆われているため、アンテナ以外の回路パターン上はシールドされており、プリント基板上のパターンによる電磁誘導も起こりにくい。これらの理由により、イミュニティ試験に対する耐性を示したと考えられる。

温湿度サイクルに対する耐性に関しては、汎用的なチップの動作温度範囲が -40~85℃ とかなり広いため、高温の影響は小さかったと思われる。防湿性能については、結露状態暴露も含まれていたが、影響を受けた資料はなかった。さらに長期間の暴露が続けば、BLE タグのシールド構造や製品品質の差異が生じると推察される。

一方、BLE タグの安全制御関連システムへの適用可能性については、今回のコミュニティ及び温湿度環境試験の結果が良好だったとは言え、タグのIDが書き換わる危険側故障の発生確率にかかわる要素の一部の評価であるため、単純にこの発生確率が低減したとは言えません。そのため、図3-2で示した二重化システムの構築やバッテリー充電時のリセットによる機能診断など、適切な安全設計が施すことができれば、安全制御関連システムが要求する危険側故障発生確率をクリアする可能性は高いと考えられる。

4. ICT 機器を適用した支援的保護システムに関する研究

4.1 ICT 機器を用いた製造現場における支援的保護システム

図4-1にISO12100に規定されているリスク低減方策の適用順位を示す。ここで示されているステップ1からステップ3までのリスク低減方策である3ステップメソッドとは、機械の設計段階で実施するリスク低減方策で、以下の3つの方策となる。

① ステップ1 (本質的安全設計方策)
ガードまたは保護装置を使用しないで機械の設計または運転特性を変更することによる保護方策で危険源の除去または危険源に近づく必然性をなくすことでリスク低減を行う。

② ステップ2 (安全防護及び付加保護方策)
ガードまたは保護装置及び付加保護方策による保護方で隔離と停止の原則に基づいたリスク低減を行う。

③ ステップ3 (使用上の情報)
ステップ1と2の方策を実施しても低減されなかったリスクに対して、使用上の情報(残留リスク情報)を提供することによりリスク低減を行う。リスク低減方策として支援的保護システムを適用する場合、事前にリスクアセスメントを行い、3ステップメソッドにてリスクを低減しておくことが前提となる。その上で残るリスクに対してICT機器を適用するため、万が一、適用したICT機器が故障した場合には、採用されている保護装置等により当該機械を停止させたり、危険区域に侵入することができなくなるような階層インタロックを構成することが必要となる。

図4-2は災害に至るプロセスと災害発生を抑制するための検討事項の優先順位を示したものである。危険源と人が同じ空間に同時刻に存在することで、危険状態が発生し、その危険状態に対する保護方策が不適切であると危険事象が発生する。そしてその危険事象の発生に対して、回避に失敗すると災害が発生する。そこで、それぞれのタイミングで次の事象の発生を抑制するための検討を行うが、それには優先順位があり、上位の検討事項がより確実に災害防止の効果が高い(それぞれの検討事項の数値はリスク低減方策を検討する際の優先順位を示す)。

4.2 ICT 機器を活用した支援的保護システムの実証実験

筆者らが開発し、国際的にも評価を得ているICT機器を活用した支援的保護システム³¹⁾を対象に、システムの改善・妥当性及び有効性検証を目的とし、フォークリフトと人が共存する製造業においてシステムを使用した実証実験を行った。

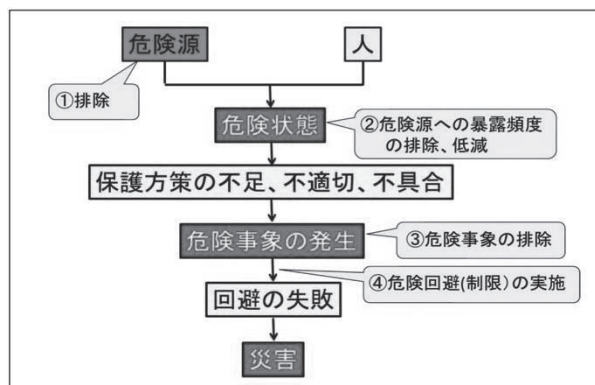


図4-1 危険源から危害に至るプロセス

現場に、人と機械の位置情報を検知するシステム(支援的保護システム)を導入し、得られた情報をもとに行動分析学的手法の一つである「行動タスク分析」を行った。この手法は以前から行動分析学の領域ですでに活用されているものであるが、一場面での行動の分析と問題行動の解決に使用されているものであった。本研究では、新規に行動タスク分析に作業者及び機械の動線、作業空間及び、作業時間の要因を取り入れることで、作業に対する動的な分析が可能となり、目まぐるしく変化する作業の変化に伴うリスクの経時的な同定(リスクポイントの検出)と評価の実現可能性が示唆された。さらにこの研究成果は、今後の協調安全管理システムに必要と思われる、「動的リスクアセスメント」の手法確立への糸口となることが確認された。

4.2.1 背景

現在、製造における生産システムは変化を遂げている現場に、人と機械の位置情報を検知するシステム(支援的保護システム)を導入し、得られた情報をもとに行動分析学的手法の一つである「行動タスク分析」を行った。この手法は以前から行動分析学の領域ですでに活用されているものであるが、一場面での行動の分析と問題行動の解決に使用されているものであった。本研究では、新規に行動タスク分析に作業者及び機械の動線、作業空間及び、作業時間の要因を取り入れることで、作業に対する動的な分析が可能となり、目まぐるしく変化する作業の変化に伴うリスクの経時的な同定(リスクポイントの検出)と評価の実現可能性が示唆された。さらにこの研究成果は、今後の協調安全管理システムに必要と思われる、「動的リスクアセスメント」の手法確立への糸口となることが確認された。

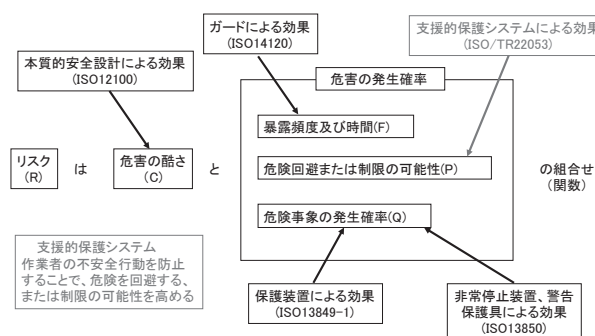


図4-2 リスク要素とリスク低減方策の関係

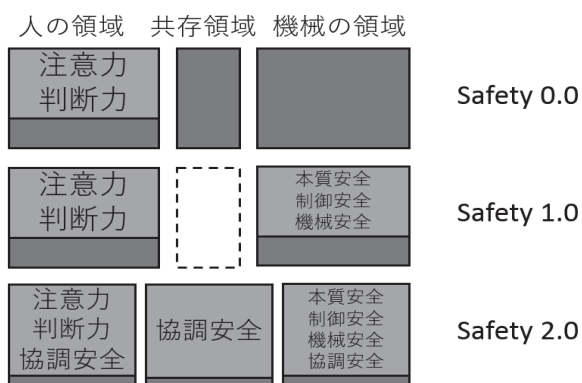


図 4-3 協調安全を構築するための Safety2.0の概念

すべての情報は中央システムで収集および管理されつつある。日本では、新しい社会スタイルとして Society5.0 が提案され、新たな生産システムとして Connected Industries が提唱されている。加えて、格差のないよりよい社会創造への国際的な活動として、持続可能な開発目標「Sustainable Development Goals (以下 SDGs と称す)」が、推進されている。いずれのシステムも、機械や環境との人間中心 (Human - Centered) の概念を強調している。そのため、安全管理システムの考え方も、従来の機械の「停止と隔離」における安全から、新たなものへの変化が求められている。

新しい労働安全管理支援システムの概念は、Safety2.0 として日本から発信されている (図 4-3)。それは、機械と人が共存・協調して働く形態を考慮したシステムである。

本研究は、人と機械が同空間で同時間に作業する某企業の現場において、接触事故を削減するため、行動分析学の問題行動の改善・解決のための一手法である「行動課題分析」を用いた。現場でのリスクは、複数の作業者とフォークリフト (以下、FL と称す) の接触事故である。作業状態をビデオ録画して課題分析することで不安全行動の削減、リスクが発生しやすい場所の特定 (リスクポイント) 及び作業の最適化を目的とした。

4.2.2 行動モニタリングシステム

本実験で使用の行動モニタリングシステムは、複数のカメラやセンサー同士を連携させることで屋外使用を可能にするシステムである。このシステムにより、異常検知及び通知、予知予測に繋がる解析のための作業者と重機

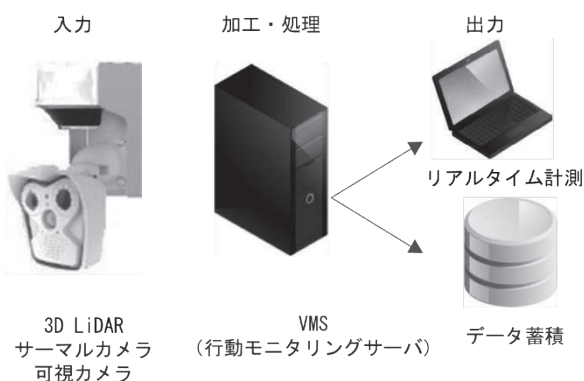


図 4-4 行動モニタリングシステム

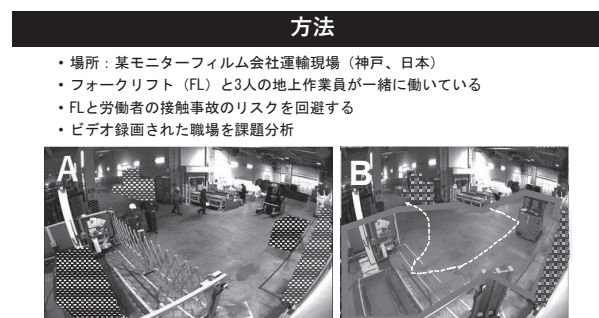


図 4-5 実験を行った作業現場

の位置・大きさ・温度データ等の取得が可能となった。主な仕様及び機能は以下となる (図 4-4)。

- ① 入力機器: 行動モニタリングシステムは入力機器として、可視カメラ、Mobotix 社製サーマルカメラ (ドイツ) 及び 3D-LiDAR を組み合わせて使用した。
- ② データの統合・解析・出力: 各機器のデータは、Video Management Software (VMS) を介して統合・解析を行い、結果を出力する。提供する情報は、動画とそれにタグ付けされた行動分析データとなる。
- ③ 作業員及び重機の位置を正確に捉えるための技術: 行動モニタリングシステムは、センサー動画データを保存・蓄積・管理する VMS を活用したセンサーフュージョンを用いた。この技術により、屋外環境であっても正確な行動分析データ取得を実現する。以上が行動モニタリングシステムの仕様となる。

4.2.3 実験方法

実験は、モニターフィルムを製造する会社内の輸送現場で実施した。

図 4-5 に示すように、FL と複数の地上作業員が同一場所にて作業している。FL 及びそのオペレーターの動線は、白い破線となる。

作業内容は、ワーク (製品) がエレベータから運ばれ、FL で包装機に運ばれ、包装されてから現場外に運び出される。そしてワークに ID シールを貼る、ラップフィルムを止める等の移送以外の作業の必要があるため、FL のオペレーター以外にも、地上で作業をサポートする複数の作業員が存している。

4.2.4 結果と考察

はじめに、1人、2人、または3人の作業員の作業状況をビデオ録画で分析した (図 4-6)。

本作業現場では、通常勤務では3人作業、夜間は1人作業となる。

図 4-6A は、作業時間あたりの FL との作業員の接触時間、図 4-6B は、包装機への接近時間を示している。どちらも2人または3人での作業のリスクが高くなる傾向がみられた。

単独 (1人) 作業では、接触災害のリスクはほとんどない。すなわち、一人作業においては、FL のオペレーターが一人ですべての地上作業も行うため、動いている FL と接触する機会がないため、事故は発生しない。図 4-6C は、作業物がエレベータに接触した回数を示す。ここでは、3人で作業する場合、リスクが高くなっていることが明らかになった。図 4-6D は作業量を示す。1人作業の負担は大きいといえるが、本実験で標的としたリスクは、FL と作業員との接触災害であるため、そのリスクが

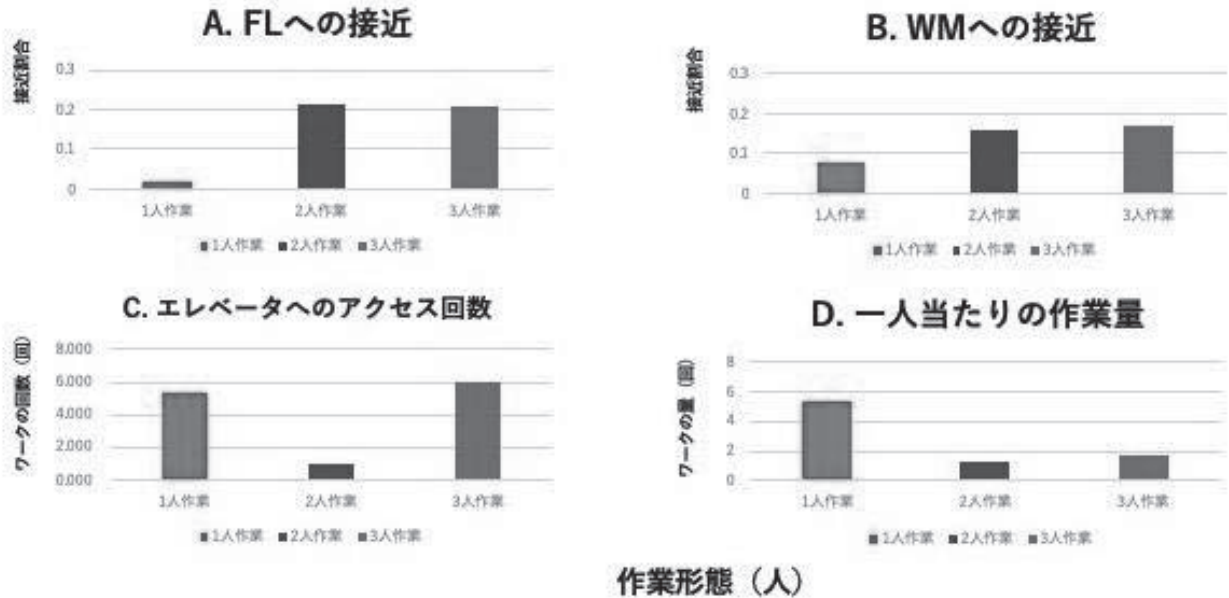


図 4-6 作業人数における作業負担の解析

高いことが示された 3 人の作業の状況を課題分析した (図 4-7)．FL と作業員の接触事故が発生しやすい場所を同定するために、作業現場を、デスク (図 4-7 中の赤い部分)、共通 (図 4-7 中の緑)、ラッピング (図 4-7 中の黄色)、および清掃作業 (図 4-6 中の紫) の 4 エリアに分割した。

図 4-8 は、当該作業現場における 3 人作業の職場の課題分析図を示す。この図には、時間と場所の要素が含まれている。図中のピンクの矢印は作業者 1、すなわち FL のオペレーターの動線を示している。同様に、緑と青の矢印は、2 番目と 3 番目の労働者の動きを示す。

黒い矢印は製品の動線を示す。色付きの四角形の部分は、分割された各エリアを示しており、それぞれの色は図 4-4 のエリアと対応している。すなわち、赤い四角はデスク領域、緑は共通領域、黄色はラッピング領域を示す。ピンクの矢印は FL の動きを表しており、緑と青の矢印すなわち残りの 2 名の作業者が交差する点が FL との接触事故が発生しやすい場所 (リスクポイント) となる。リスクポイントは、図 4-8 中では、紫の円で示されている。課題分析によると、リスクポイントは、共通エ



図 4-7 課題分析に用いた作業現場のエリア分割

リアからラッピングエリアの境界に存在することが明らかになった。

次に、勤務時間中に製品が現場に配達された個数により、交差の回数がどう変化するかを分析した (図 4-9)．図中の赤い丸の大きさの違いは、交差点の数を示しており、大きくなるにつれて接触災害のリスクが大きくなることを示している。図の左上の課題分析は、作業時間中に製品が 3 個運ばれてきた場合である。これを見ると、リスクはそれほど大きくないことが明確となった。また、製品が 4 個、または 5 個であってもリスクは大きくないことが示された。しかしながら、6 つの製品が運ばれてきた場合には、リスクポイントが大きくなり、接触災害のリスクが大きく変化することが明らかとなった。その結果、3 人作業下で比較的 safely に作業するためには、勤務時間内の製品の処理は 6 個以下に抑えることが望ましいことが示唆された。

4.2.5 実験結果から得られた結果と今後の検討事項

人の位置情報を検知するために ICT 機器を活用した支援的保護システムと行動分析学の課題分析を組み合わせることにより、

- 1) 現場の、人と FL の接触災害のリスクを可視化することが可能となった。
- 2) これらのリスクについて、労働者の数と作業の内容別に比較検討され、対策の優先順位が明確となった。
- 3) 3 人の作業者の最適な作業量 (作業数) を定量的に決定することができた。

これまで、当該現場での接触事故の防止は、作業者の注意力に依存していたが、本実験で開発した ICT 機器を活用した支援的保護システムと産業行動分析学 (BBS: Behavior based safety)³²⁾ の組み合わせは、有効であるといえる。さらに、課題分析の手法を情報通信技術 (ICT) デバイスを使用し、新しい作業分析システムの構築が今後待たれる。

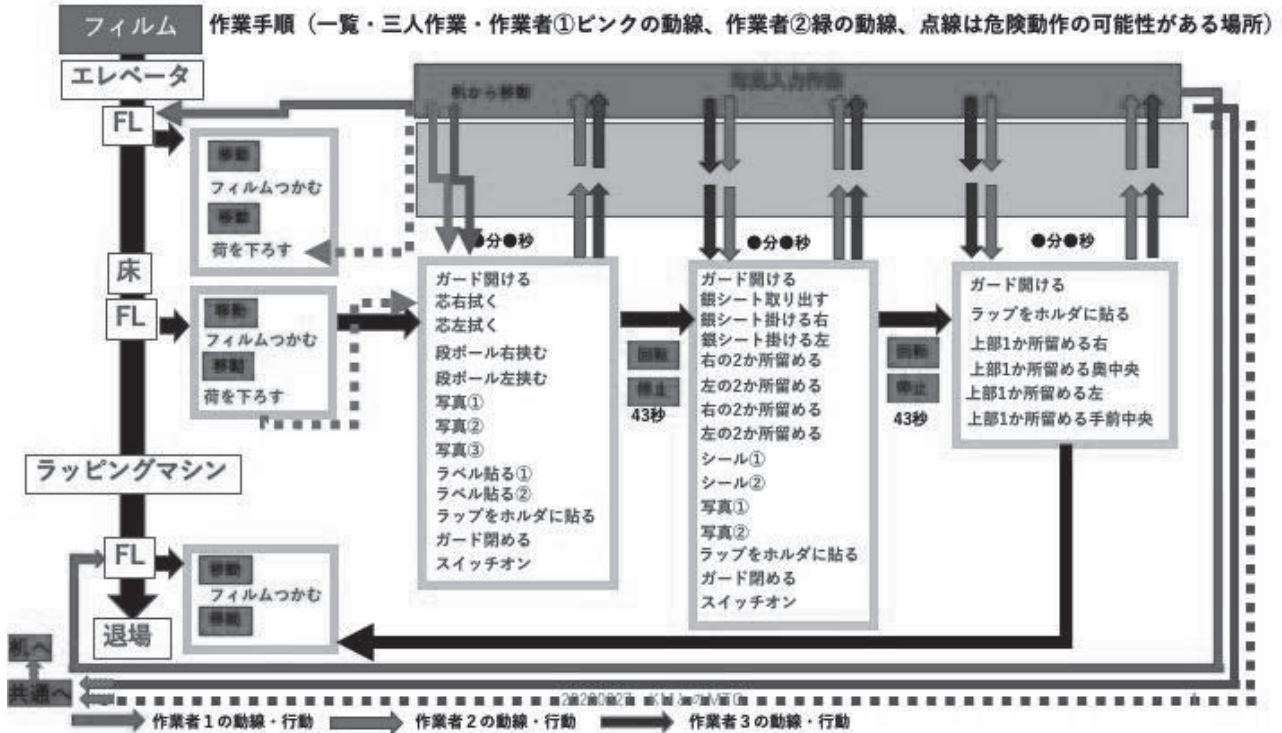


図 4-8 3人作業における課題分析図



図 4-9 製品数とリスクポイントの関係

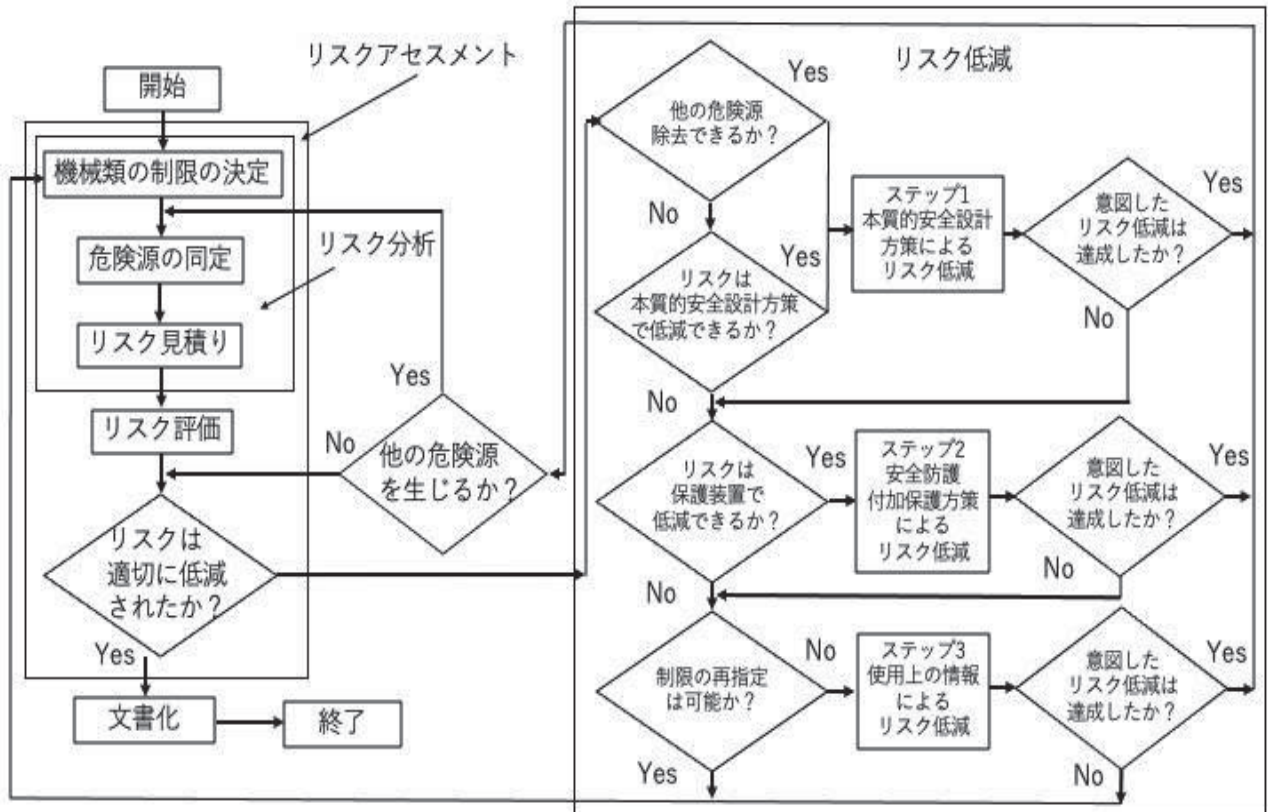


図 4-10 ISO12100 に基づくリスク低減プロセス

4.3 リスクアセスメントの考え方と問題点

4-3-1 国際安全規格に基づくリスクアセスメントの考え方

現在、Society5.0 や Connected Industries 等の新しい生産システムが推進されている。これらのシステム下では、人・モノ（機械）・環境が一体となって作業を行う共存・協調の作業形態が求められる。このような作業現場の安全を管理する必要があると思われるが、その体制はまだ十分に整っていない。そこで、我々は新たな生産システムに適合可能な安全管理支援システムの一手法として「ダイナミックリスクアセスメント」を提案する。この手法により、人と機械、環境が互いに情報を共有・交換し、作業現場における安全を統合的に維持・増進することが可能となる。

機械を安全にするためには、機械の危険源を分析・評価して、リスクを低減させることが必要となる。そのためリスクアセスメントとリスク低減の手順が ISO12100:2010 機械類の安全性-設計のための一般原則-リスクアセスメント及びリスク低減 に定められている。機械の安全化は図 4-10 に示すように、次に示す5つの手順で実現される。

① 手順 1：機械類の制限の決定

「機械類の制限の決定」とは、リスクアセスメントを実施する際に考慮すべき前提条件を決めることである。使用上の制限とは、以下の内容を考慮する必要がある。

- a. 全てのライフサイクル段階に対する必要事項
- b. 機械の意図する使用方法と、合理的に予見可能な誤使用と誤動作
- c. 使用者の性別、年齢、身体能力の限界などによる制限
- d. 予想される使用者の訓練、経験、能力、資格など
- e. 空間上の制限、時間上の制限など

② 手順 2：危険源の同定

「危険源の同定」とは、機械に付随するすべての危険源、危険状態及び危険事象を洗い出すこと。危険源の種類の一例は以下に示す。

- a. 機械的危険源
- b. 電気的危険源
- c. 熱的危険源
- d. 騒音による危険源
- e. 振動による危険源
- f. 材料及び物質による危険源
- g. 人間工学原則の無視による危険源
- h. 機械が使用される環境に関する危険源

③ 手順 3：リスク見積り

「リスクの見積り」とは、機械の危険な状態及び危険事象を確認した後、リスク要素を決定し、「危害の酷さ」と「危害の発生確率」からリスクの大きさを推定することである。なお、見積りに際しては、考えられる最悪値評価を行う事が原則となる。

④ 手順 4：リスク評価

「リスク評価」とは、リスクの見積りを行った後にそのリスクの評価を行い、リスク低減が必要か否かを決定することである。

⑤ 手順 5：リスク低減

「リスク低減」とは、以下に示す3つのステップによる方で許容可能なリスク低減を達成する必要がある。

- a. ステップ 1: 本質的安全設計方策
- b. ステップ 2: 安全防護及び付加保護方策
- c. ステップ 3: 使用上の情報

なお、上記一連のプロセスで検討された内容は文書化

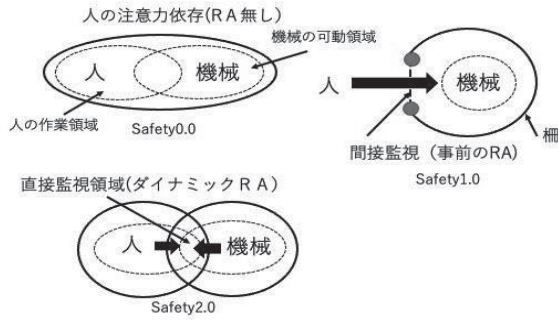


図 4-11 3つの安全確保の考え方

して、機械の安全設計の根拠を示すものとして保管しておく必要がある。

4.3.2 既存のリスクアセスメントの問題点

既存のリスクアセスメントでは、洗いだされた危険源及び危険状態に対して、考えられる最大のリスクを考えて、そのリスクが許容不可能であれば、許容可能なレベルになるまで、リスク低減を行うことが求められている。しかし現実には、最大のリスクとなる時間は全ての時間ではなく、一部の時間に限定されている。

もし全ての時間帯に対して、最悪値評価を行った結果からリスク低減措置を行えば、許容可能なリスクレベルにある時間帯に対しても、最大のリスクを想定した低減措置が実施されることになる。具体的には、機械を停止しなくても良い時間帯で機械が停止されることになり、生産性は損なわれることになる。この状態は、作業者が機械を止めないようにして、保護装置を無効化したり、取り外したりする意図的な不安全行動を誘発する可能性が考えられる。

図 4-11 は人とモノ（機械）の関係において、人の注意力に依存した安全を Safety0.0、人と機械を隔離する安全または、人と機械が近づいたことで機械を停止させる安全を Safety1.0、情報の共有による協調型作業の安全を Safety2.0 とする考え方を示したものである。

図 4-12 は、時間軸上で変化するリスクに対応したリスクアセスメントの概念図である。対象となる危険源に対するリスクは、人とモノと環境条件の変化により大きく変化している。そのため時間軸上で変化する人と機械と環境条件をリアルタイムに計測して、許容不可能なリスクレベルになることが予測される前に危害発生を防ぐことで安全性と生産性を両立できると考える。

5. おわりに

本研究では、大規模生産システムを対象としたリスク低減方策として、ICT 機器を活用するためにまず、人・機械・環境の情報を Cyber Physical System (CPS) で共有することで安全制御を実現する場合の条件として、物理層・データ層・論理層の3つの基本要素から成る簡易的モデル化を検討し、安全の原理の展開を試みた。

次に、既存のリスク低減方策に加えて、ICT 機器を利用した新たなリスク低減方策として3ステップメソッドにおけるステップ2に ICT 機器を適用する方法として、市販されている Bluetooth Low Energy (BLE) タグの安全関連用途への適用を検証する一環として、PFH_D を低減する方法論とその実現可能性について検討を行った。その結果、二重化システムの構築やバッテリー充電時のリセットによる機能診断など、適切な安全設計が施すこ

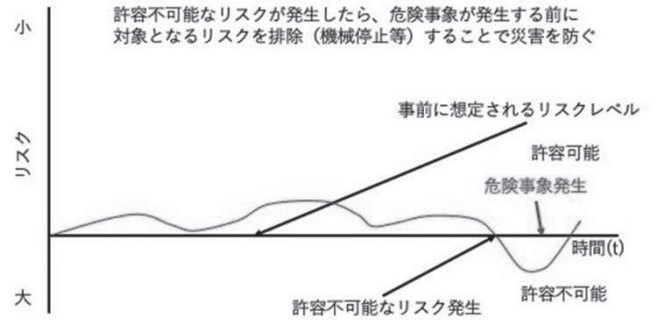


図 4-12 ダイナミックリスクアセスメントの提案

とができれば、安全制御関連システムが要求する危険側故障発生確率をクリアする可能性は高いことが確認された。

また、3ステップメソッド適用後の残留リスクに対して ICT 機器を適用して人の注意力のみに依存しない支援的保護システムの提案を行った。さらに、実現場に導入した支援的保護システムと行動分析学の課題分析を組み合わせるにより、作業者とフォークリフトの接触災害によるリスクを可視化できることが確認された。

ユーザーが現場で実施する安全管理の支援的対策として ICT 機器を活用する支援的保護システムを検討する場合は、現場で実施している教育・訓練や安全管理体制については人の注意力に大きく依存したリスク低減方策である場合が多いため、今一度3ステップメソッドに従ってリスク低減方策を再検討するとともに、人の注意力や判断力に大きく依存したリスクを洗いだし、そのリスク低減の確定性を向上させるための検討が必要である。

参考文献

- 1) 経済産業省, "Connected Industries," https://www.meti.go.jp/policy/mono_info_service/connected_industries/index.html (2020年4月22日確認)。
- 2) 総務省,情報通信白書平成30年版, <https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/html/nd135210.html>
- 3) 一般社団法人電子情報技術産業協会, "CPS とは," <https://www.jeita.or.jp/cps/about/> (2020年4月22日確認)。
- 4) 杉本旭, 蓬原弘一, "安全の原理," 日本機械学会論文集 C 編, 56 巻, 530 号, pp. 2601-2609, 1990. <https://doi.org/10.1299/kikaic.56.2601> (2020年4月22日確認)。
- 5) 一般社団法人セーフティグローバル推進機構, "協調安全, Safety2.0 とは," <https://institute-gsafety.com/safety2/> (2020年4月22日確認)。
- 6) (社)実践教育訓練研究協会編, "安全に対する基本的な考え方, 安全基礎工学入門 労働災害の原因と対応技術," pp.13-17,工業調査会, 東京, 1999.
- 7) 池田博康, 齋藤剛, 杉本旭, "人間と共存するロボットの本質安全化-国際安全規格に基づく危険源除去のプロセス," システム制御情報学会論文誌, Vol.13, No.12, pp.575-584, 2000. https://doi.org/10.5687/isclie.13.12_575 (2020年4月22日確認)。
- 8) 杉本旭, 梅崎重夫, 池田博康, 桑川壮一, 深谷潔, "安全制御システムの基本構成-安全制御の原理とフェールセーフシステムの構成方法-, "産業安全研究所研究報告 NIIS-RR-95, pp.9-22, 1996. <https://www.jniosh.johas.go.jp/publication/doc/rr/RR-95-2.pdf> (2020年4月22日確認)

- 9) 経済産業省産業 サイバーセキュリティ研究会, “第2層: フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース,” 2019年8月2日開催資料, https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/dainiso/001.html (2020年4月22日確認).
- 10) 梅崎重夫, 濱島京子, 清水尚憲, “機械安全で使用する安全情報と労働安全衛生マネジメントシステムで使用する危険回避情報の基本特性の比較,” 安全問題研究論文集, Vol.4 (2009年11月), pp.17-22, 2009.
- 11) 例えば, 株式会社 WHERE: “EXBeacon プラットフォーム”, <https://where123.jp/> (2021年7月1日確認).
- 12) Bluetooth SIG, Inc.: “Bluetooth Radio Versions”, <https://www.bluetooth.com/learn-about-bluetooth/radio-versions/> (2021年7月1日確認).
- 13) ANSI/ASSP Z244.1-2016 (R2020) “The Control of Hazardous Energy Lockout, Tagout and Alternative Methods”.
- 14) 清水尚憲, 他: 機械安全-支援的保護システム(Supportive Protective system, SPS)-統合生産システム(IMS)における SPS のリスク低減効果, 日本機械学会論文集, 84巻, 860号, pp1~15, 2018年4月20日
- 15) JIS B 9705-1:2019 機械類の安全性 - 制御システムの安全関連部 - 第1部: 設計のための一般原則 (対応国際規格: ISO 13849-1:2015 Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design).
- 16) JIS B 9961:2008+Amd.1:2015 機械類の安全性 - 安全関連の電気・電子・プログラマブル電子制御システムの機能安全 (対応国際規格: IEC 62061:2005 + Amd.1:2012 + Amd.2:2015 Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems).
- 17) 厚生労働省: “機能安全による機械等に係る安全確保に関する技術上の指針”, 平成28年厚生労働省告示第353号 (2016).
- 18) M. B. Aimonetto, F. Fiori, “Investigation on the Susceptibility of BLE Receivers to Power Switching Noise”, IEEE Trans. on Electromagnetic Compatibility, Vol. 60, No. 5, pp.1529-1538 (2018).
- 19) C. Klünder, J. L. ter Haseborg, “Effects of High-Power and Transient Disturbances on Wireless Communication Systems Operating inside the 2.4 GHz ISM band”, Proc. IEEE Int. Symp. on Electromagnetic Compatibility, pp.359-363 (2010).
- 20) Inside the 2.4 GHz ISM Band 中矢猛, 杉浦彰彦: “周波数ホッピングを用いた近距離無線通信方式の他局間干渉低減法の影響評価”, 情報処理学会論文誌, Vol. 44, No. 12, pp.2912-2924 (2003)
- 21) 戸枝毅, “制御システムにおける共通原因故障の影響と対策”, 日本機械学会産業・化学機械と安全部門研究発表講演会 2011 講演論文集 (2011), pp.17-18.
- 22) 梅崎重夫, 清水尚憲, 齋藤剛, “厚生労働科学研究費「プレス作業を対象とした安全技術の高度化に関する研究」平成17年度総括・分担研究報告書”(2006), p.31.
- 23) JIS C 0508-6:2012 電気・電子・プログラマブル電子安全関連系の機能安全 - 第6部: 第2部及び第3部の適用指針 (対応国際規格: IEC 61508-6:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3)
- 24) JIS C 61326-3-1:2020 計測用, 制御用及び試験室用の電気装置-電磁両立性要求事項- 第3-1部: 安全関連システム及び安全関連機能 (機能安全) の遂行を意図した装置に対する イミュニティ要求事項-一般工業用途 (対応国際規格: IEC 61326-3-1:2017 Electrical equipment for measurement, control and laboratory use - EMC requirements - Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) - General industrial applications)
- 25) JIS C 61326-1:2017 計測用, 制御用及び試験室用の電気装置 - 電磁両立性要求事項 - 第1部: 一般要求事項 (対応国際規格: IEC 61326-1:2012 Electrical equipment for measurement, control and laboratory use - EMC requirements - Part 1: General requirements)
- 26) 国立研究開発法人情報通信研究機構ワイヤレスネットワーク総合研究センター, “製造現場における無線通信トラブル対策事例集”, p.13, <https://www2.nict.go.jp/wireless/ffpj.html> (2021年7月1日確認)
- 27) JIS C 61000-4-2:2012 電磁両立性 - 第4-2部: 試験及び測定技術 - 静電気放電イミュニティ試験 (対応国際規格: IEC 61000-4-2:2008, Electromagnetic compatibility (EMC) - Part 4-2: Testing and measurement techniques - Electrostatic discharge immunity test)
- 28) JIS C 60068-2-38:2013 環境試験方法 - 電気・電子 - 第2-38部: 温湿度組合せ(サイクル)試験方法(試験記号: Z/AD) (対応国際規格: IEC 60068-2-38:2009, Environmental testing - Part 2-38: Tests - Test Z/AD: Composite temperature /humidity cyclic test)
- 29) JIS C 61000-4-3:2012 電磁両立性 - 第4-3部: 試験及び測定技術 - 放射無線周波電磁界イミュニティ試験 (対応国際規格: IEC 61000-4-3:2010, Electromagnetic compatibility (EMC) - Part 4-3: Testing and measurement techniques - Radiated, radio-frequency, electromagnetic field immunity test)
- 30) JIS C 61000-4-8:2016 電磁両立性 - 第4-8部: 試験及び測定技術 - 電源周波数磁界イミュニティ試験 (対応国際規格: IEC 61000-4-8:2009, Electromagnetic compatibility (EMC) - Part 4-8: Testing and measurement techniques - Power frequency magnetic field immunity test)
- 31) ISO/TR22053:2021, Safety of machinery-Safeguarding supportive system
- 32) 産業安全行動分析学研究会ホームページ, <https://sites.google.com/view/sangyokodo/>