電子/電気機器のリスク・アセスメントとリスク低減のガイド — CENELEC Guide 32 に基づく

株式会社 e・オータマ　佐藤智典

2023 年 11 月 28 日

目 次

1 概要

CENELEC Guide 32[1] では低電圧機器のリスク・アセスメントとリスク低減について述べられている。この文書は、ISO/IEC Guide 51[2] と同様、安全規格を策定する側を主な対象としているものの、その内容は電子/電気機器の製造業者にとっても有用と思われる。

本稿では、主に CENELEC Guide 32[1] に基づく形で、電子/電気機器のリスク・アセスメントとリスク低減について解説する。

なお、本稿は CENELEC Guide 32 に基づく記述を多く含むが、その内容を全てカバーしているわけではなく、またその文書に含まれない記載も含む。その文書の内容についてはその文書そのもの [1] を参照されたい。

1.1 安全な機器

一般に、どのような機器も怪我や火災などの好ましくない事象を生じないことが、すなわち安全であることが期待される。

だが、この種の話をする際には「安全」が何を意味するかを明確にすることが重要となる。例えば怪我や火災などの好ましくない事象を生じる可能性が全くないこと (絶対安全、ゼロ・リスク) のみを安全と呼べると考える人も居るかも知れないが、それは実際的な基準ではなく、また目標として好ましいものとも言い難い。†1

従って、この文脈で「安全」が何を意味するかの実際的な定義が、また機器が安全かどうかを判断するための実際的な基準が必要である。

CENELEC Guide 32 では、リスクがあることを前提とした、「受容できないリスクがないこと†2」のようなリスクに基づく「安全」の定義が用いられており、この考え方は他の分野を含めて広く受け入れられている。

この定義を用いれば、今度は「受容できないリスク」(あるいは「許容できないリスク」) が何を意味するかという疑問は生じるものの、機器が受容できないリスクを (あるいは許容できないリスクを) 生じないのであればその機器は安全であると判断できるようになる。

だが、「安全」という用語の使用は誤解を招くことがあるため、「安全」という用語の不用意な使用は避けることが望ましいだろう。

1.2 許容可能なリスク

CENELEC Guide 32 では「許容可能なリスク」は「社会の現在の価値観に基づいて特定の状況下で受け入れられるリスク」のように定義されている。

この定義でリスクが許容可能かどうかの判断は社会の価値観が基礎となること、それが時とともに変化するかも知れないこと、そしてそれが状況に依存することが示されているように、何を許容可能なリスクとして考えることができるかは様々な要因の影響を受け、一概に示すことはできない。†3†4

許容可能なリスクに関しては CENELEC Guide 32 の §9 (*Risk evaluation*) で述べられており、これについては本稿 §3.4で触れる。

†1 ゼロ・リスクを安全の基準とした場合、極論では、例えば安全性が非常に高い機器であっても、極めて稀な故障によって、あるいは異常な使い方をされることで危険を生じる可能性はあるかも知れないということで、おおよそいかなる機器も安全ではないということにもなるかも知れない。

†2 ここではその意味合いの違いには踏み込まないが、ISO/IEC Guide 51 (2014)[2] では「受容できないリスクがないこと (freedom from unacceptable risk)」は「許容できないリスクがないこと (freedom from risk which is not tolerable)」に変更されており、他の文書も順次この定義に切り替わると思われる。

†3 一般には、それが使用者の取り扱いに起因するものであったとしても、重大な事故を頻発する機器は受け入れ難いとみなされそうである。だが、電子/電気機器とは別の話ではあるが、自動車が関係する事故は極めて多い (2022 年の日本国内での自動車事故は 30 万件、死者 2600 人、重傷者 2 万 6 千人、軽症者 33 万人程度となっている) にも関わらず、多くの人が自動車を、あるいは自動車による危険に曝されている道路を日常的に利用しており、これはそのリスクを受容していると考えることができるだろう。一方、飛行機の移動距離当りの事故率は自動車よりも遥かに低いにも関わらず、飛行機の利用を不安に感じる人は少なくなく (これは特に飛行機が関係する事件や事故の後で顕著となる)、飛行機の利用に関するリスクの受容の水準を自動車に関するそれから演繹することはできそうにない。

†4 分野によってはリスクを受容可能かどうかの判断でベネフィットとのバランスが考慮される場合がある (例えば、かなりリスクが高い手術法の適用を、それを上回るベネフィットを期待でき、また患者側がそのリスクを理解して手術を希望する場合に許容するような)。だが、それが社会的なリスクの受容の判断への影響を介してリスク受容の判断に影響することはあるかも知れないものの、CENELEC Guide 32 が対象としている範囲では、リスク受容の判断の主要な要素としてベネフィットを直接用いること、例えば許容可能と言い難いリスクについて期待されるベネフィットがリスクを上回るということだけを理由としてそのリスクが受容可能であると主張するようなことは適切ではないだろう。

1.3 リスク・アセスメントとリスク低減の役割

リスク・アセスメントとリスク低減のプロセスの主な役割は、機器が受容/許容できないリスクを持たないかどうかを評価すること、そして必要であれば所望の水準に達するまでリスクを低減することとなる。

電子/電気機器の安全性の評価では安全規格も大きな役割を果たす。このような規格ではその種の機器の安全のために必要と判断された様々な事項が具体的な要求事項を含めて規定されており、そのような該当する安全規格に適合している製品は安全であるとみなされることがある。

だが、例えば次のような理由から、そのような規格を適用する場合であってもリスク・アセスメントの実施が必要となる、あるいは少なくともその実施が有用となるかも知れない:

- そのような規格がリスク・アセスメントの要求を含むことがある;
- 仕向け先の地域の法令などでリスク・アセスメントの実施を求められることがある;[†5]
- そのような規格がその機器に関係するリスク全てを適切にカバーしているとは限らない。

従って、その実施が必須とされているかどうかに関わらず、適切なリスク・アセスメントの実施は有用であり、製品の開発プロセスの一部としてリスク・アセスメントを実施する価値があると思われる。

2 主な用語

- 危害 (harm)

  人、財産、及び飼育動物に対する物理的な傷害や損害

- ハザード (hazard)

  危害の潜在的な原因

- 危険事象 (hazardous event)

  危害を引き起こし得る事象

- 危険状態 (hazardous situation)

  人、財産、及び飼育動物、あるいは環境が少なくとも 1 つのハザードに曝される環境

- インシデント (incident)

  過去の危険事象;

  発生して危害を引き起こしたインシデントはアクシデント (accident)、発生したが危害を引き起こさなかったインシデントはニアミス事象 (near miss occurrence) と呼ぶことができる

- 誤動作 (malfunction)

  以下のものを含む様々な理由に伴い電子/電気機器が意図された機能を実行しない状況:

  – 処理されている素材やワークピースの特性や寸法のばらつき
  – その 1 つ以上の構成部品や装備の故障
  – 外的な妨害 (例えば衝撃、振動、電磁干渉)
  – 設計上の誤りや欠陥 (例えばソフトウェアの誤り)
  – その電源の妨害
  – 周囲条件 (例えば温度変化に伴う結露)

- 保護方策 (protective measure)

  以下の者が実現する、適切なリスク低減の達成が意図された方策:

  – 設計者によって (本質的安全設計方策、安全防護、また補完的な保護方策、使用上の情報); また
  – 使用者によって (組織的なもの: 安全作業手続き、監督、訓練; 作業許可システム; 追加の安全防護の使用; 個人用保護具の使用)

- 意図する使用 (intended use)

  供給者が提供する使用のための情報に従った機器の使用

- 合理的に予見可能な誤使用 (reasonably foreseeable misuse)

  容易に予測できる人の挙動から生じるかも知れない、設計者が意図していない方法での機器の使用

[†5] 例えば EU 低電圧指令 2014/35/EU では規格を適用したかどうかに関わらずリスクの適切な分析と評価が求められる。また、機械類や医療機器については多くの場合にリスク・アセスメントの実施が求められる。

- 単一故障状態 (single fault condition)

  単一の保護 (強化保護を除く)、あるいは単一のコンポーネントやデバイスに障害がある状態[†6]

- リスク (risk)

  危害の発生の可能性と危害の厳しさの組み合わせ

- 残留リスク (residual risk)

  保護方策が講じられた後で残るリスク

- 許容可能なリスク (tolerable risk)

  社会の現在の価値観に基づいて特定の状況下で受け入れられるリスク

- リスク・アセスメント (risk assessment)

  リスク分析とリスクの評価から成る全般的なプロセス

- 安全 (safety)

  受容できないリスクがないこと

3　リスク・アセスメント

リスク・アセスメントのプロセスは実際的な範囲でのハザードの除去と保護方策の実施の反復性のプロセスで、以下のステップを含む (図 1):

(1) リスク分析

  (a) 機器の制限の決定 (§3.1)

  (b) ハザードの特定 (§3.2)

  (c) リスクの見積もり (§3.3)

(2) リスクの評価 (§3.4)

リスク分析はリスクの評価に必要な情報を与え、これは機器の安全性の判断を行なえるようにする。

リスク・アセスメントは判断に依存し、これは定性的な手法で、また可能な限り定量的な手法でサポートされる。定量的な手法は代替の保護手段を評価していずれが最も良い保護を与えるかを判断するために有用であり、危害の潜在的な厳しさや範囲が大きく、また資源やデータがそれを可能とする時に適切となり得る。だが、定量的な手法の適用は利用可能なデータによって制限され、多くの場合は定性的なリスク・アセスメントのみが可能となるだろう。

リスク・アセスメントは適用した手順と達成された結果を文書化できるような形で行ない、これはリスク低減が必要かどうかを決定する。

リスク・アセスメントで必要と判断された場合、これに引き続いて

(1) リスク低減 (§4)

(2) リスク低減方策を反映した状態でのリスクの見積もり (§3.3)、またリスクの評価 (§3.4)

を残留リスクが許容可能な水準に低下するまで繰り返す (図 1)。

この繰り返しの際、保護方策の適用によって新たなハザードが生じていないかどうかを確認することが重要である。[†7]新たなハザードが生じていれば特定されたハザードのリストにそれを追加し、そのハザードもリスクの見積もりとリスクの評価の対象とする。

3.1　機器の制限の決定

リスク・アセスメントの最初のステップ (通常、製品開発の初期段階に最初に実施され、必要に応じてやり直される) として、以下の事項を含む、機器の制限の決定を行なう:

(1) 使用上の制限、例えば:

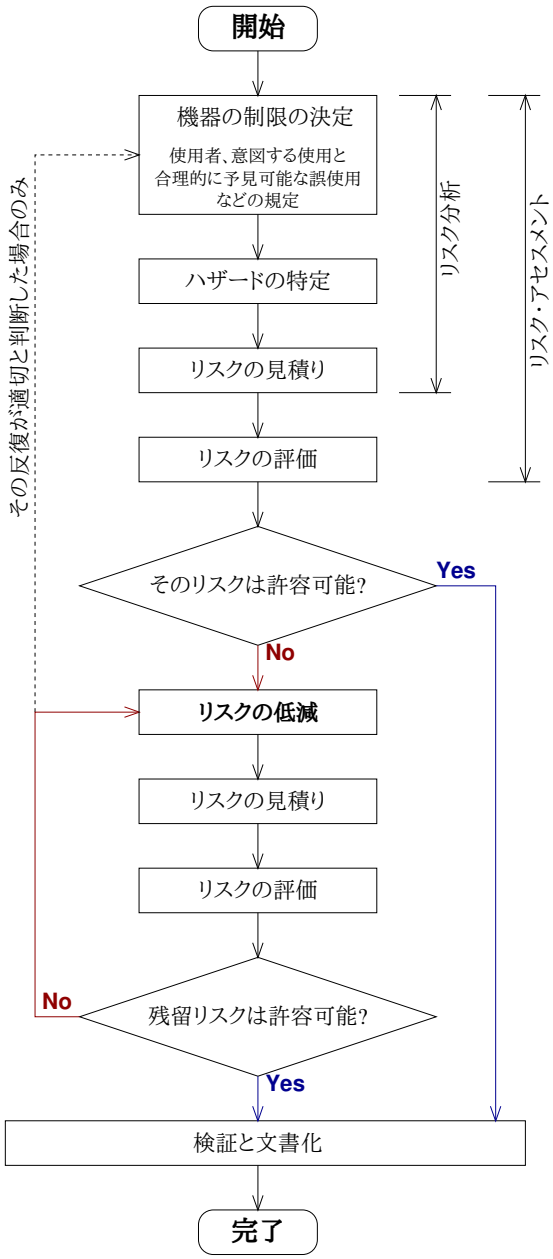
  (a) その機器の様々な動作モード、また使用者の様々な介入手続き (機器の誤動作の際に必要となる介入を含む) を考慮した、意図する使用と合理的に予見可能な誤使用;

  (b) 以下の事項も考慮した、使用者の予期される訓練、経験、力量の水準:

    - 例えば、一般の操作員、保守要員や技師、訓練生や実習生、一般公衆のような区分;
    - 規定できる範囲での、機器の用途 (例えば工業、非工業、また家庭のような)、また想定される使用者の性別、年齢、利き手、あるいは身体能力の制限 (例えば視覚や聴覚の障害、体格、体力) の範囲。

[†6] ここで言う「故障 (fault)」は一時的な誤動作なども含む。

[†7] 例えば可動ガードの追加によってガードによる挟み込みの危険を新たに生じるような。



リスク・アセスメントのプロセスは次のように行なわれる:

(1) 機器の制限の規定 — 機器の対象使用者、意図する使用と合理的に予見可能な誤使用などを特定する (§3.1)

(2) ハザードの特定 — 設計、生産、設置、保守、修理、廃棄などの機器のライフサイクルのそれぞれの段階でのハザードを特定する (§3.2)

(3) リスクの見積もり — 特定されたそれぞれのハザードによって引き起こされるリスクを推定する (§3.3)

(4) リスクの評価 — 特定されたハザードによって引き起こされるリスクを評価する (§3.4);
その評価がリスクが許容可能な水準にあることを示したならばそれ以上の作業は不要となる

(5) リスクの低減 — リスクが許容可能でない場合、リスク低減を実施する (§4);
その後、改めてリスクの見積もりと評価を行ない、残留リスクが許容可能な水準に低減されるまでこの作業を繰り返す

図 1: リスク・アセスメントとリスク低減の反復プロセス

(2) 空間的な制限、例えば:

(a) 動きの範囲

(b) その機器の設置と保守のための空間的な要求

(c) 人とのインタラクション、例えば「マン・マシン」インターフェース

(d) 「動力供給」インターフェース

(3) 時間的な制限、すなわち:

(a) 意図する使用と合理的に予見可能な誤使用を考慮した、その機器、及び/もしくはそのコンポーネント (例えばツールや摩耗部品) の「耐用寿命」

(b) 推奨保守周期

(4) 他の制限、例えば:

(a) 環境、例えば:

- 推奨最小/最大温度
- 屋内と屋外のいずれか
- 乾燥と湿潤の環境のいずれか
- 直射日光下で動作させられるか
- 塵埃や湿気への耐性、など

(b) 必要な清浄さ

機器の制限の決定の際、その機器のライフサイクルの関係する全段階を考慮する。

3.2 ハザードの特定

電子/電気機器のライフサイクルの全段階、すなわち

(1) 輸送;

(2) 組み立てと設置;

(3) 試験稼働;

(4) 使用;

(5) 安全に関係する範囲で、廃止措置、解体、及び処分[†8]

[†8] 多くの場合、適切なリサイクルやリカバリ、また有害な物質の適切な取り扱いが必要となる。

を考慮して、それが人、飼育動物、及び/もしくは財産のいずれに影響するかを区別し、その機器のライフサイクルの全ての段階で起こり得るハザード、危険状態、及び危険事象を体系的に特定する。

この特定の作業はハザード (原因) の想定から始めてそれによって引き起こされ得る危害 (結果) に向けてボトム・アップで行なう (例えば FMEA や ETA のような手法を用いて) ことも、その逆に危害 (結果) の想定から始めてその原因となり得るハザード (原因) に向けてトップ・ダウンで行なう (例えば FTA のような手法を用いて) こともできるであろうが、状況によってはその双方を用いるのが良いかも知れない (図 2)。

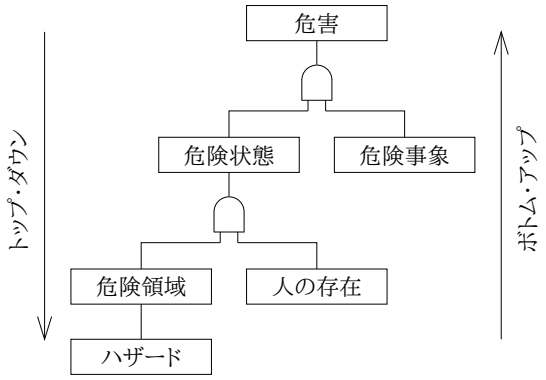


図 2: ハザード、危険状態、危険事象の特定 — ボトム・アップとトップ・ダウン

これらの特定のためには、その機器の動作、またそれと相互作用する人が実行する作業の特定が必要である。

作業に関しては以下の作業分類を含む様々な作業に関係する全てのハザード、危険状態、あるいは危険事象を特定する:

- 設定;
- 試験;
- プログラミング;
- 始動;
- 全ての動作モード;
- 機器からの生産物の取り出し;
- 通常停止;
- 緊急停止;
- 予期しない始動;
- 障害の特定 / トラブル解決 (オペレータの関与);

- 清掃と維持管理;
- 計画的な保守と修理;
- 計画外の保守と修理;
- 合理的に予見可能な誤使用;
- セキュリティ上の脅威 (通信、アクセス・チャネル)。

さらに、作業に直接関係しない、合理的に予見可能なその他のハザード、危険状態、あるいは危険事象 (例えば、地震、雷、雪荷重、騒音、機器の倒壊や崩壊) も特定する。

3.3 リスクの見積もり

ハザードの特定 (§3.2) の後、それぞれの危険状態について §3.3.2 で示すリスクの要素を決定することでリスクの見積もりを行なう。

3.3.1 リスクの見積もりで考慮すべき事項

3.3.1.1 機器の制限

リスクの見積もりでは、機器の制限 (§3.1)、特に意図した使用と合理的に予見可能な誤使用の考慮が必要となる。[†9]

3.3.1.2 故障状態

通常の状況に加え、単一故障状態の考慮が必要である。

2 つの独立した無関係な故障の同時発生は、そのような事象の可能性はそのリスクが通常は許容可能な水準となるほど低いため、通常は考慮の必要はないが、

- 最初の故障の結果である第 2 の故障、また同一の原因によって引き起こされる複数の故障 (共通原因故障) は単一故障状態に含める;
- 最初の故障が自動的に検知されない場合は 2 つの独立した無関係な故障による二重故障状態も考慮する。[†10][†11]

3.3.1.3 人や飼育動物の曝露

リスクの見積もりではハザードに曝される人、飼育動物、財産全てを考慮する。

3.3.1.4 曝露の種類、頻度、期間

検討対象のハザードへの曝露 (長期的な健康影響を含む) の推定ではその機器の運用と働き方の全ての形態の分析が必要である。特に、これは設定、ティーチング、工程の切り替えや修正、清掃、障害の特定、また保守に際してのアクセスの必要性に影響する。リスクの見積もりでは安全機能を停止させる必要がある状況 (例えば保守中に) も考慮する。

3.3.1.5 影響の累積や相乗効果

累積的な曝露の影響[†12]や相乗効果[†13]も考慮する。これらの影響を考慮してのリスクの見積もりは、それが実際的な限り、適切な認知されたデータに基づく。

3.3.1.6 ヒューマン・ファクタ

ヒューマン・ファクタはリスクに影響するかも知れず、リスクの評価で考慮しなければならない。[†14]

---

†9 一般に予見可能な誤使用は明白ではなく、同様の機能を持つものであっても機器によって異なるかも知れない (例えば、特定の機器の操作部の設計が誤使用を招く、など) ので、機器毎に慎重な検討が必要となるかも知れない。また、基本的には何が予見可能かは製造業者が判断すべきものとなり、明らかに異常な使い方などの予見可能でない誤使用の考慮は不要ではあるが、紛争の際にはそれが予見可能かどうかが論点となるかも知れない。

†10 例えばコンポーネントの故障への対応のために二重化を行なったとしても、そのいずれか一方の故障が自動的に検知/通知されない場合、その故障が点検で発見されるとしても点検が実施されるまで、そうでない場合は恒久的に一方が故障したままの状態となり、その状態でもう一方が故障すれば有害な影響 (例えばそれらが実現していた安全機能の喪失) が生じることになる。

†11 だが、該当する安全規格に適合した二重絶縁や強化絶縁の故障、またその規格で二重絶縁を横切って接続することが認められたコンポーネント (例えばクラス Y のコンデンサの短絡故障) の考慮は通常は不要であろう。また、カテゴリ 3 や 4 の安全関連部 (ISO 13849-1[5] による) では冗長化と監視が行なわれており、危険側故障の可能性は非常に低いことが期待できる。だが、カテゴリ 2 以下の安全関連部は冗長化されておらず、SIL 1 (IEC 61508[6]) では危険側失敗の頻度は 10^{-5} /h 未満に過ぎないので、機能安全規格に適合しているコンポーネントであっても危険側故障の可能性を無視できるとは限らない。

†12 例えば振動への長期間の曝露が健康被害 (例えば白蝋病) の原因となることが知られている。

†13 異なる曝露の影響は独立、または加算的と考えることが多いが、例えば単体では有意な健康影響が確認されない濃度の複数の化学物質に同時に曝露した時に有意な影響が現れる場合があることが知られている。

†14 §3.3.1.6〜§3.3.1.10 は CENELEC Guide 32 の §9.2 でリスク評価に関係するものとして述べられているものに基づく。

これは例えば以下の事項を含む:

- 誤動作の修正を含む、人の機器との相互作用;
- 人のあいだの相互作用;
- ストレスに関係する側面;
- エルゴノミクスの側面;
- 訓練、経験、また力量に依存する、人の能力。

人の能力に関しては以下の事項を考慮する:

- 必要なタスクの実行に必要な先天的な、また発達させられた能力;
- リスクの気付き;
- 意図的な、あるいは非意図的な逸脱なしに必要なタスクを実行する信頼のレベル;
- 所定の、また必要な安全作業プラクティスから逸脱する動機。[†15]

訓練、経験、また力量はリスクに影響するが、それらを本質的安全設計方策や安全防護などの保護方策の適用によるリスク低減の代わりになるものと考えてはならない。

3.3.1.7 保護方策の信頼性

リスクの見積もりではコンポーネントやシステムの信頼性も考慮する。

このため:

(1) 危害をもたらし得る状況 (例えばコンポーネントの故障、電源障害、環境パラメータ、電磁現象、電気的妨害、振動) を特定する;

(2) 適切な場合、代替の保護方策との比較のため、定量的方法、また使用による証明のプロセスを用いる;

(3) 適切な安全機能、コンポーネント、またデバイスの選択を可能とする情報を用意する。

安全機能に寄与するコンポーネントやシステムは、例えば信頼性、試験、環境条件への耐性に関して、特別な注意が必要となる。[†16]

複数の安全関連デバイスが安全機能に寄与する場合はそれらのデバイスの選択はその信頼性や性能の考慮に関して一貫していなければならず、例えばセンサ、PLC、及びアクチュエータは特定の安全機能を満足させるように正しく選択しなければならない。

設計段階で適用された保護方策は、スキルや訓練、作業組織、正しい行動、注意、個人用保護具の適用のような保護方策よりもかなり有効である。リスクの見積もりでは後者のような保護方策の比較的低い信頼性も考慮する。

3.3.1.8 保護方策の無効化や回避の可能性

リスクの見積もりでは保護方策の無効化や回避の可能性も考慮する。[†17]

この評価では例えば次のような保護方策の無効化や回避の動機も考慮する:

- 保護方策が生産を遅くし、あるいは他の任意の活動や使用者の好みに干渉する;[†18]
- 保護方策の使用が難しい;
- オペレータ以外の要員が関与する;[†19]
- 保護方策を使用者が承認しない、あるいはその機能のために適切なものとして受け入れない。

保護方策の無効化の可能性は保護方策の種類 (例えば可動ガード) とその設計の詳細の双方に依存する。[†20]

---

†15 例えば: 規定された方法での作業が非効率的に見え、そのような方法での作業が規定されている理由を理解していないことは、効率的かも知れないが危険な方法を用いる動機となることがある (例えば東海村 JCO 臨界事故)。また、安全のために所定の個人用保護具 (例えば耐熱手袋、レーザー保護めがね、耳栓など) の着用を規定している場合も、機器の側でその保護具を着用しての作業が適切に考慮されていない (例えば、耐熱手袋を着用しての操作が難しい、レーザー保護めがねを着用すると必要な情報の読み取りが難しい、など)、通常は危険状態が存在していないか危険性が明らかでない (例えばレーザー保護めがねの着用が規定されているが、レーザー光が不可視で裸眼でも眩しさなどを感じることがない) などの要因は保護具なしで作業を行なう動機となるかも知れない。

†16 一般に、この種のコンポーネントやシステムは信頼性などの規定を含む機能安全に関する要求の対象となる。

†17 例えば作業の邪魔だということで機械のカバーやガードを外す、可動ガードのインターロックを無効化してガードを開けた状態で動作させられるようにする、両手操作制御装置の一方を押したままとしてもう一方のスイッチのみで工程を始動させられるようにする、などの事例がしばしば見られる。[7]

†18 保護方策の無効化の動機を減らすため、その作業への悪影響を最小限とするように配慮することが望ましい。

†19 例えば保守に際して保護方策が無効化されることがある。

†20 無効化の可能性を下げるため、容易に無効化を行なえないように配慮することが望ましいだろう。例えば鉄片を貼り付けるだけで無効化できる単純な磁気スイッチや突出したアクチュエータをテープで固定するだけで無効化できるようなスイッチをインターロック用のスイッチとして用いるべきではない。また、片手で双方のスイッチを操作できないような配置や構造とし、また双方のスイッチをほぼ同時に押した時にのみ始動信号を出す

プログラマブル電子システムの使用は、もし安全関連ソフトウェアへのアクセスが適切に設計され、管理され、また監視されないならば無効化や回避のもう 1 つの可能性を与える。

リスクの見積もりでは、安全関連機能がその機器の他の機能から分離されているかどうかを識別し、アクセスが可能な範囲を特定することも必要となるだろう。これは診断や工程修正のために遠隔でのアクセスが必要な場合は特に重要である。

3.3.1.9　保護方策の維持の能力

リスクの見積もりでは保護方策が必要な水準の保護を与えるために必要な状態で維持されるかどうかも考慮する。

これに関しては、信頼性や耐久性 (§3.3.1.7)、無効化の困難さ (§3.3.1.8) などに加え、計画的な点検や保全の考慮も必要となるかも知れない。

3.3.1.10　使用上の情報

リスクの見積もりでは使用上の情報 (警告ラベルや対話的な作業指示なども含む) も考慮する。

使用指示書等での使用上の情報の提供は、

- 構成や表現は ISO/IEC 82079-1[†21] も参照すべき;
- 全ての動作モードを考慮しての、意図する使用の情報を提供する;
- 安全な使用と正しい使用を確かとするために必要な全ての指示を含める;
- 残留リスクについての情報と警告を含める;
- 機器の設計と説明から合理的に予見可能な使用を除外してはならず、特に合理的に予見可能な誤使用と安全関連のセキュリティ上の脅威を考慮して、機器のその情報で述べられたものと異なる方法での使用から起こり得るリスクも警告する;
- 輸送、組み立てと設置、試験稼働、使用 (設定、ティーチング、プログラミングや工程の切り替え、運用、清掃、障害調査、また保守)、そして必要であれば廃止措置、解体、及び処分を個別に、あるいは一括してカバーする。

3.3.2　リスクの要素

3.3.2.1　リスクの要素の組み合わせ

特定の状況や技術的プロセスに関連するリスクは以下の要素の組み合わせから導出される (図 3):

(1) 危害の厳しさ (§3.3.2.2);

(2) 以下のものの関数である、危害の発生の可能性 (§3.3.2.3):

  (a) 危険状態への曝露:

    i. ハザードへの曝露;

    ii. 危険事象の発生;

  (b) 危害を回避もしくは制限する技術的及び人の能力。

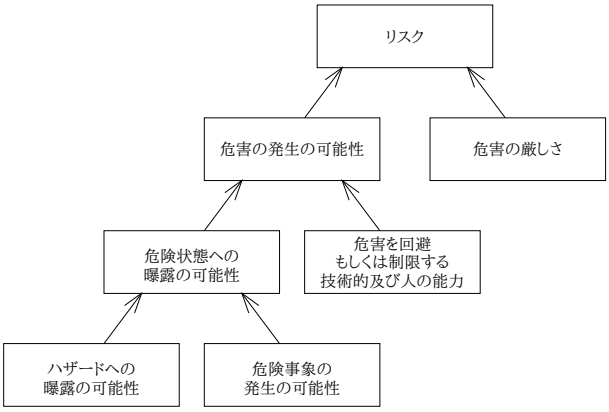


図 3: リスクの要素の組み合わせ

リスクの見積もりに用いる手法として、ISO TR 14121-2[4] では

- リスク・マトリックス法
- リスク・グラフ法
- 積算法 (numerical scoring)
- 定量的リスク推定法 (quantified risk estimation)

(一方のスイッチを押したままの状態としてもう一方のスイッチを操作しても始動信号は出ない) ようにすることで、片手での操作、また一方のスイッチを押したままとするような単純な方法での無効化の可能性を下げられる。

[†21] ISO/IEC 82079-1, *Preparation of information for use (instructions for use) of products — Part 1: Principles and general requirements*

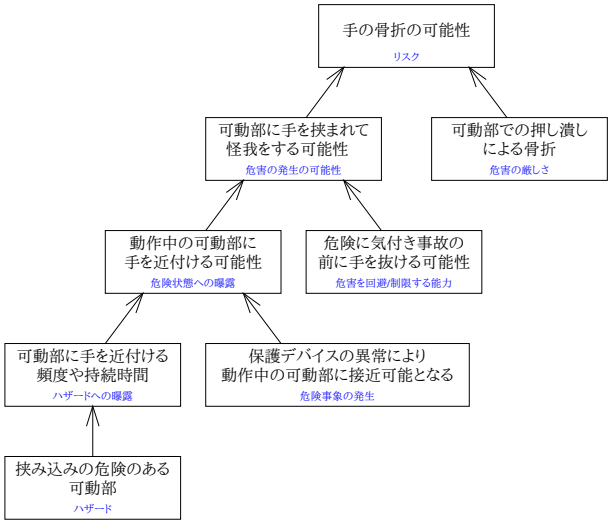


図 4: リスクの要素の組み合わせの例

- 複数の手法の組み合わせ (ハイブリッド法)

が示されている。

CENELEC Guide 32 では図 5で図示するようなリスク・グラフ法を用いる形で記載されているが、これは ISO TR 14121-2[4] で示されているものとは例えば次のような相違がある:

- 危害の厳しさが 2 段階 (S1〜S2) ではなく 3 段階 (S1〜S3) となっている;
- ハザードへの曝露の頻度や持続時間 (F1〜F2) と危険事象の発生の可能性 (O1〜O3) の代わりにそれらをまとめた危険状態への曝露の可能性 (F1〜F2) が用いられる;
- 危害の回避や低減の可能性 (A1〜A2) の代わりに危害を制限する能力 (P1〜P2) が用いられる;
- リスク・インデックスが 1〜6 ではなく 1〜5 となる。

3.3.2.2 危害の厳しさ

図 5 のパラメータ S は危害の厳しさを扱い、これは以下のものを考慮して推定できる:

(1) 危害の厳しさ:

(a) 軽微 (通常は短期間で回復可能か修理可能);

(b) 高度 (通常は長期間で回復可能か修理可能);

(c) 深刻 (通常は回復不能か修理不能)、あるいは死亡;

(2) 危害の範囲:

(a) 一人、その機器自身、あるいは隣接環境の財産;

(b) 複数人、あるいは広い環境の損害 (例えば建屋全体かそれ以上への影響)。

3.3.2.3 危害の発生の可能性

危害の発生の可能性は以下の要素を考慮して推定できる:[†22]

(1) 危険状態への曝露 (§3.3.2.3.1);

(2) 危害を回避もしくは制限する技術的及び人の能力 (§3.3.2.3.2)。

3.3.2.3.1 危険状態への曝露

図 5 のパラメータ F は人、飼育動物、あるいは財産の危険状態への曝露を扱い、これはハザードへの曝露、及び危険事象の発生の影響を含む。

(1) ハザードへの曝露:

人、あるいは飼育動物のハザードへの曝露には、例えば次のようなものが関係する:

(a) 危険領域へのアクセスの必要性 (例えば通常の運用のため (F2)、誤動作の修正のため (通常は F1)、保守や修理 (通常は F1));

(b) アクセスの性質 (例えば機器の手動操作 (F2)、あるいは自動操作 (通常は F1));

(c) 危険領域に留まる時間;

(d) アクセスを必要とする人の数;

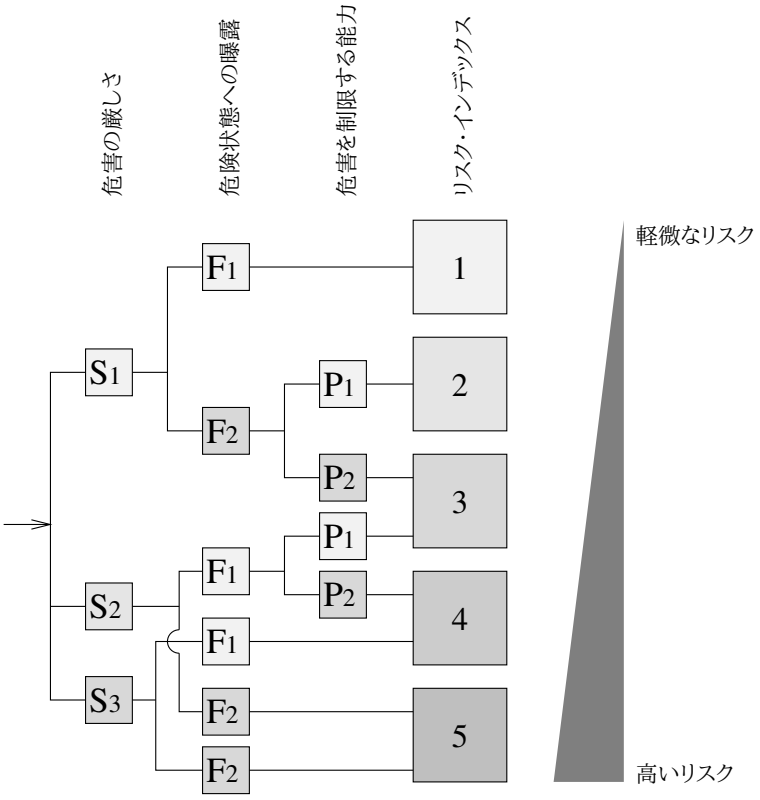
(e) アクセスの頻度;

(f) 既にある保護。

(2) 危険事象の発生:

危険事象の発生の可能性は、機器の分析から、また例えば次のような情報から導けるかも知れない:

†22 安全関連のコンポーネントの評価においては危険側故障の発生を危険事象の発生と、その安全関連のコンポーネントで保護されている危険領域への人のアクセスを危険状態への曝露と考えれば良いだろう。だが、機器の評価においてはこれらの区別はわかりにくいものとなるかも知れず、評価の開始に先立ってその機器に応じた形で明確化しておくことが望ましいかも知れない。



S_1: 軽微な危害 (短期間で回復可能)
S_2: 高度の危害 (長期間で回復可能)
S_3: 深刻な危害 (回復不能) か死亡

F_1: 稀、あるいはそれほど頻繁でない、かつ/もしくは曝露時間が短い
F_2: 頻繁、あるいは持続的、かつ/もしくは曝露時間が長い

P_1: 回避可能
P_2: 回避困難

図 5: リスクの見積もりのためのグラフ

(a) 信頼性やその他の統計データ;

(b) 健康上の被害やアクシデントの履歴;[†23]

(c) リスクの比較。

複数の人の負傷や死亡が予期されるならば発生の確率は F2 である。

3.3.2.3.2 危害を制限する能力

図 5 のパラメータ P は危害を回避もしくは制限する技術的及び人の能力を扱う。

危害の回避や制限には、例えば次のようなものが関係する:

(1) その機器を誰が操作するか:

- 熟練者;
- 非熟練者;
- 無人;

(2) その人が危害を回避し、あるいは制限する能力 (例えば反射、機敏さ、可能な離脱):

- 可能;
- 特定の状況では可能;
- 不可能;

(3) リスクの認知:

- 一般的な情報による;

[†23] この種の報告の多くは危険事象の発生ではなく危害の発生に関係するものとなるかも知れない。また、使用者などからのこの種の報告を受け取り、管理しているとしても、報告されるのは実際のアクシデントのごく一部のみとなることが、また報告の質もさまざまであることが予期されるので、この種の情報の利用に際してはその考慮が必要となりそうである。特に、過去にアクシデントがない、または少ないとしても、あるいはアクシデントが軽度のものであるとしても、それがリスクが低いことを示すものと仮定すべきではない。

- 直接的な観察による;
- 警告サインと表示デバイスを介して;

(4) 元となる実践的な経験と知識:

- その機器の;
- 類似の機器の;
- 経験なし;

(5) その危険状態がどの程度速やかに危害をもたらすか:

- 即座に;
- 早い;
- 遅い;

(6) 曝露された他の危害を受けやすい人の範囲、また危害を低減できる程度。

3.3.3 リスク・インデックス

リスク・インデックスはリスクのレベルを示し、以下のものに影響される (図 5):

(1) 危害の厳しさ (§3.3.2.2);

(2) 危害の発生の可能性 (§3.3.2.3):

(a) 危険状態への曝露 (§3.3.2.3.1);

(b) 危害を回避もしくは制限する技術的及び人の能力 (§3.3.2.3.2)。

3.4 リスクの評価

3.4.1 一般

リスクの見積もり (§3.3) の後、リスク低減 (§4) が必要か、それとも許容可能なリスクが達成されたかを判断するためにリスクの評価が行なわれる。

許容可能なリスクが達成されたか、それともそのリスクは許容可能でなくリスク低減 (§4) が必要かどうかの判断は、§3.4.2で述べる社会の価値観を考慮して、リスクの見積もり (§3.3) の結果 (§3.3.2〜§3.3.3 で述べたリスク・グラフ法ではリスク・インデックス (§3.3.3)) に基づいて行なう。[†24]

[†24] 通常、リスク・インデックスがいくつ以下であればそのリスクを許容可能とみなせるか (また、リスク・マトリックス法の場合もマトリックスのどのセルが許容可能なリスクに相当するか) をあらかじめ決めておく。

リスクの評価でリスクが許容可能でないと判断された場合、引き続いてリスク低減 (§4) を実施する。

リスクの評価に際して、認知された参照文書として基本安全規格やグループ安全規格を使用できる。

適切なリスク低減 (§4) の達成、またその適用が実際的であればリスクの比較 (§3.4.3) の好ましい結果とは、リスクが適切に低減されたという確信を与えるだろう。

3.4.2 社会の現在の価値観

リスクの非意図的な影響に対する社会の許容度は同一のリスクの意図的な影響に対するものよりも遥かに低い。社会はその構成員の一部、例えば子供や障害者に対して特別な保護を与える。関連する法律の厳しさや程度も社会の価値観を示す。科学的に裏付けられた議論や協定の内容も考慮されるが、個人的に、あるいは非公式に議論された見解はより低い重要性を持つ。

3.4.3 リスクの比較

リスクの評価のプロセスの一部として、機器に関係するリスクを以下の基準を満たす類似の機器と比較できる:

- その類似の機器が適切な国際規格に従っており安全である;
- 双方の製品の意図する使用、また設計や構成が同等である;
- ハザードとリスクの要素が同等である;
- 技術仕様が同等である;
- 使用条件が同等である。

但し、これはリスク・アセスメント・プロセスの適用を不要とするものではない。

4 リスク低減

4.1 一般

リスクの評価 (§3.4) でリスクが許容可能でないと判断された場合、そのリスクが許容可能となるようにリスクを低減することが必要となる。

この目標は、そのハザードを除去するか、リスクを決定する 2 つの要素、

(1) 検討中のハザードからの危害の厳しさ (§3.3.2.2)

(2) その危害の発生の可能性 (§3.3.2.3)

のそれぞれを別々に、あるいは同時に低減することで達成されるであろう。

このためのリスクの低減は下記の「3 ステップ・メソッド」を**その順序で**適用することで行ない (図 6)、これはハザードを除去するか残留リスクを効果的に低減し、その機器が安全かどうかという質問に答えられるようにするだろう:

(1) 本質的安全設計方策

例えば設計、危険性の低い素材や物質への置き換え、あるいはエルゴノミクス原則の適用により、ハザードを除去するかリスクを低減する。

(2) 安全防護と付加的な保護方策

その応用に対して適切な、意図する使用のためにリスクを適切に低減する技術的な保護方策 (デバイス) によってリスクを低減する。

(3) 使用上の情報

上記の手法を適用しても残留リスクが許容可能な水準まで低下しない、あるいは上記の手法の適用が実際的でない場合、存在するかも知れない任意の残留リスクの通知を含む、使用上の情報の提供を行なう。

これについては §4.2でもう少し詳しく触れる。

これらの 3 つのステップには明確な優先順位があり、例えば使用上の情報の提供を本質的安全設計方策や安全防護などの保護方策の適用の代替とみなしてはならない。

リスク低減のための方策の適用の後、残留リスクが許容可能かどうかの判断のため、リスクの見積もり (§3.3)、またリスクの評価 (§3.4) を改めて実施する。

特定のハザードに関連する残留リスクが許容可能かどうかの判断のためには以下の基準が有用かも知れない:

(1) 本質的安全設計方策の実施の全ての可能性が考慮されたか?

(2) もし技術的な保護方策の実施が必要であれば、該当する要求を含む水平安全規格かグループ安全規格、あるいは CENELEC や IEC か国際/欧州規格を策定するその他の標準化機関 (例えば CEN や ISO)[†25]からのその他の規格があるか?

もし適切な規格がないならば、その他の安全に関する出版物が有用かも知れない。

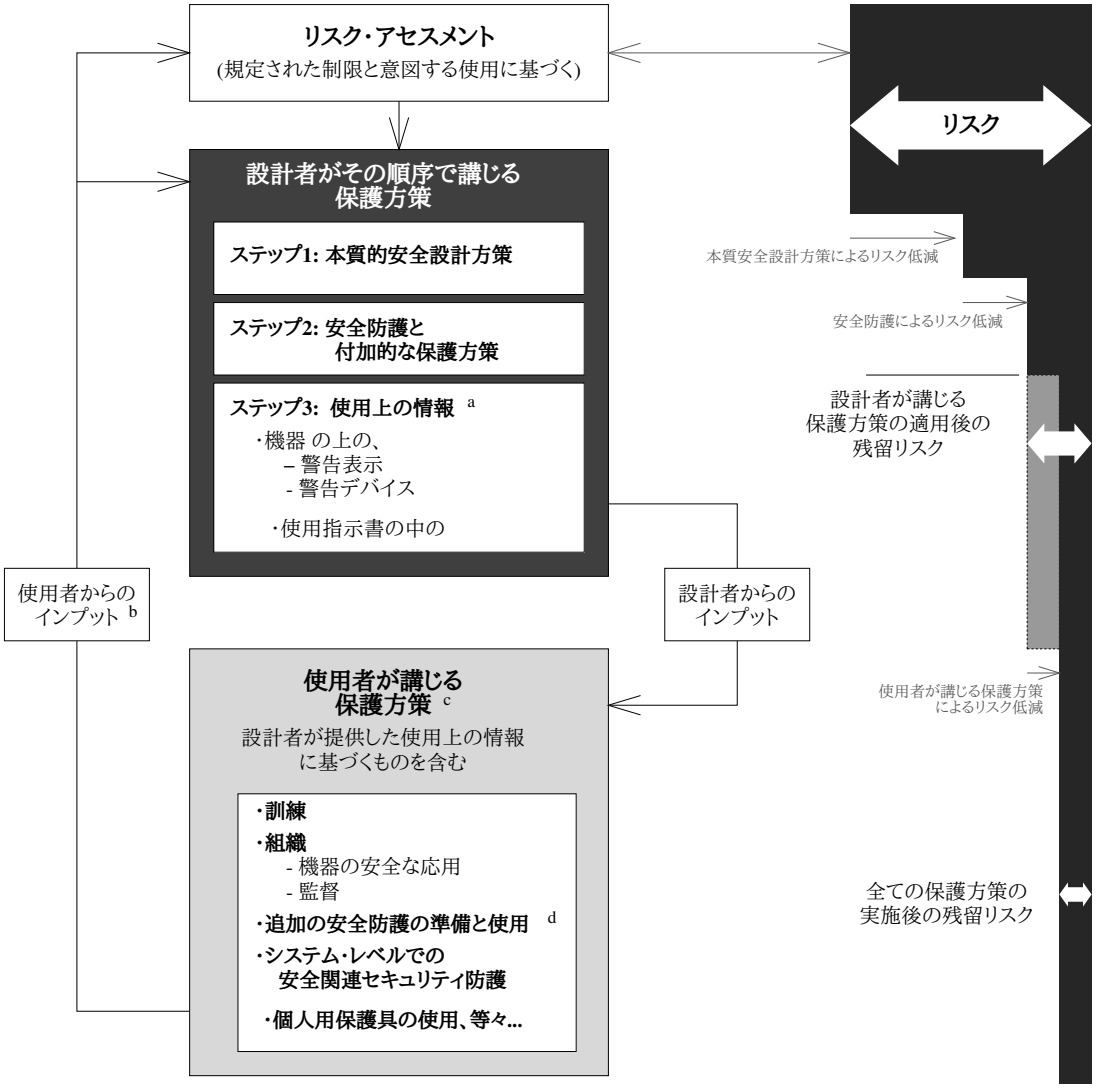
(3) 上記の規格で適切な要求がない場合、§3.2〜§4で述べた原則を適用して固有の要求事項を策定しなければならない。

図 1 で示したリスクの低減、そしてリスクの見積もりと評価の反復のプロセスはその機器について必要なリスク低減が達成されるまで繰り返して実施する。

リスク低減手続きの最後に、以下の事項を確認する:

- 全ての動作条件と全ての介入手続きが考慮されていること;
- 適用された方策が新たなハザードを生じないこと;
- 使用者が残留リスクについて充分に知らされること;
- 講じられた保護方策によって使用者の作業条件と機器のユーザビリティが損なわれないこと;
- 講じられた保護方策が互いに両立すること;
- 専門家向け/工業用に設計された機器の非専門家/非工業状況での使用から生じ得る結果が充分に考慮されていること。

†25 電子/電気機器に関する規格は、国際規格は主に IEC が、欧州規格は主に CENELEC が策定している。また、機械に関する規格は国際規格は主に ISO が、欧州規格は主に CEN が策定している。電子/電気機器に適用する規格 (通信関連を除く) は IEC や CENELEC が策定したものが中心となるが、そのような機器が ISO や CEN の規格で扱われているような機械的な側面を持つことも珍しくない。



(1) 適切な使用上の情報の提供はリスク低減への設計者の寄与の一部であるが、それらの保護方策は使用者が実施した時にのみ有効となる。

(2) 使用者からのインプットはその機器の意図する使用に関係する使用者団体と特定の使用者のいずれかから受け取った情報である。

(3) 使用者が講じる様々な保護方策のあいだに優先度はない。

(4) これらの保護方策は機器の意図する使用で示されていない特定のプロセスを、あるいは設計者がコントロールできない特定の設置条件を必要とする。

図 6: リスク低減プロセス

4.2 使用上の情報の提供によるリスクの低減

残留リスクに関する情報を含む、使用上の情報の適切な提供も、リスクの低減の手段として使用できる。

但し、一般に使用上の情報の効果はかなり限定的 (不確実) となるであろうこと、すなわち一般に大幅なリスク低減は難しいであろうことにも注意すべきである。[†26]

[†26] このような使用上の情報はその指示が遵守された場合にのみ意図されたリスクの低減を与えるであろう。このような指示はそれを遵守しようと務めている場合であってもある程度の確率 (かなりの個人差が予期される) で意図しない逸脱を生じることが予期され、場合によっては意図的 (個人的ではなく組織的なものかも知れない) かつ常習的な逸脱[†15] も生じるかも知れない。訓練や資格付与のような方策の効果もかなりの個人差が予期され、特に効果の監視やフォローアップが適切に行なわれない場合、効果はかなり限定的なものとなるかも知れず、また訓練からの時間などに応じて効果が低下するかも知れない。

この使用のための情報は以下のものを含むかも知れない:

(1) その機器の使用のための推奨される安全作業プラクティス要求を含む、機器の正しい操作、また必要な場合は行なってはならない操作;

(2) その機器を使用する人が満たすべき条件や、訓練プログラムの必要性;

(3) その機器のライフサイクルの様々な段階における残留リスクについて使用者に知らせる記述;

(4) 個人用保護具の必要性、また関連する訓練要求;

(5) 安全関連のセキュリティ保護に関する規定。

使用上の注意は、それが適切な場合は機器の上の警告表示として、また使用指示書への記載として提供できる。

それらの記載を含めて、機器の操作手順やその説明はその機器を使用する人やその機器に関連するハザードに曝され得る他の人の能力に見合ったものとする。

5 文書化

リスク・アセスメントの文書は、適用された手順を、また達成された結果を立証すること:

(1) アセスメントが行なわれた機器 (例えば仕様、制限、意図する使用):

- 行なわれた全ての関係する仮定 (例えば負荷、強度、安全率) の情報を含める;

(2) 特定されたハザード:

(a) 特定された危険状態;

(b) アセスメントで考慮された危険事象;

(3) そのリスク・アセスメントで基礎とした情報:

(a) 使用されたデータとその情報源 (例えば参照された規格やその他の文書、アクシデントの履歴、類似の機器に適用されたリスク低減から得られた経験);

(b) 使用されたデータに付随する不確かさ、またリスク・アセスメントへのその影響;

(4) 保護方策によって達成すべき目標;

(5) 特定されたハザードの除去やリスクの低減のために用いられた保護方策;

(6) その機器に関係する残留リスク;

(7) セキュリティの側面を含む、最終的なリスクの評価の結果。

6 低電圧機器に関係する安全側面

特定の機器で考慮すべきハザードはリスク・アセスメントの一部であるハザードの特定 (§3.2) の手続きの中で判断することになるだろうが、以下で述べる、CENELEC Guide 32 の Annex A で示されている安全側面のリストはその基礎として用いることができる。

6.1 電気的なハザードに対する保護

機能上の理由のために特別に許容される場合を除き、機器の接触可能な導電性の部分は危険な生きている部分であってはならない。その保護方策は機器の通常の使用のあいだにその絶縁が曝されそうな電気的、機械的、化学的、及び物理的ストレスを考慮しなければならない。特に、機器は以下のものから生じる電気的なハザードに対する適切な保護を与えなければならない:

(1) 漏洩電流;

(2) エネルギー供給;

(3) 蓄積された電荷;

(4) アーク;

(5) 感電;

(6) 火傷。

6.2 機械的なハザードに対する保護

機器によって、あるいは機器への予期される外的な力の作用によって引き起こされるハザード、また特に下記のようなものから生じる機械的なハザードに対する保護が必要となるかも知れない:

(1) 不安定性;

(2) 動作中の崩壊;

(3) 物体の落下や放出;

(4) 不適切な表面、エッジ、あるいは角;

(5) 可動部 — 特に部品の回転速度が変化するかも知れない場合;

(6) 振動;

(7) 部品の不適切な取り付け。

6.3 他のハザードに対する保護

6.3.1 爆発

爆発のハザードは機器自身によって、あるいは機器が生成するか使用する、もしくは機器が使用される場所に存在するかも知れないガス、液体、粉塵、蒸気、あるいはその他の物質によって引き起こされ得る。

潜在的爆発性雰囲気で使用される機器は爆発の防止 (防爆) に関する規則の対象にもなることがある。

6.3.2 電界、磁界、電磁界、その他の電離放射や非電離放射から生じるハザード

機器は機器が発生する電界、磁界、電磁界、その他の非電離放射線がその動作のために必要な範囲に制限されるように、また安全なレベルで動作するように設計され製造されること。

機器はいかなる電離放射線の放射もその動作のために必要な範囲に制限され、曝露された人への影響がないか危険でないレベルに低減されるように設計され製造されること。

6.3.3 電界、磁界、及び電磁妨害

機器はいかなるハザードの発生も防ぐように電気的、磁気的、及び電磁的な妨害に対する充分なイミュニティを持つように設計され構築されること。[†27]

また、ハザードを発生し得る他の機器への干渉を生じないように磁気的な、また電磁的な妨害のエミッションを制限するように設計されること。

6.3.4 光の放射

機器は危険な光の放射 (LED、レーザー、赤外線、紫外線の放射などを含む) への曝露を避けるように設計され構築されること。

6.3.5 火炎

機器の内部からの発火や火炎の拡がりのリスクが制限されることを確かとすること。規格は、温度制限デバイス、電流制限デバイス、漏洩電流検知デバイス、火炎の拡がりを低減する方法、また適切な素材の選択に関する規定を含むかも知れない。

6.3.6 温度

考慮が必要な 2 つの主な側面は:

- 接触可能な表面の温度;

  これは主に火傷の危険に関係する;

- 素材やコンポーネントへの温度の影響;

  これは主に素材やコンポーネントの性能や特性、また信頼性や耐久性に影響する (例えば電子部品の性能の悪化、機械部品の強度の低下、絶縁材の軟化や絶縁特性の劣化、寿命や故障率の悪化など)。

また、潜在的爆発性雰囲気で使用されるかも知れない、あるいは可燃性の物質が触れるかも知れない場合、温度の制限が爆発や発火の防止のために必要となることもある。

6.3.7 騒音

機器は騒音が可能な限り許容可能なレベルに制限されるように設計され構築されること。結果的なレベルが許容可能でない場合、製造業者の指示は外部の騒音抑制方策 (例えば遮音板やフード) の使用か個人用保護具 (例えばイヤーマフや耳栓) の使用を規定すること。

6.3.8 生物学的、及び化学的影響

以下のものから生じ得るハザードを防ぐための方策を規定すること:

[†27] 一般には電磁妨害に対するイミュニティは EMC (電磁両立性) で扱われるが、通常、EMC では安全への影響は考慮されない。また、EMC 試験は多くは通常の動作状態でのみ行なわれ、その試験では安全機能の劣化や喪失 (例えばガードを開いたり危険領域に人が侵入したりした時に正しく停止するか)、意図しない始動などの安全に関係する側面は評価されないことも多い。

(1) 病原体、腐敗菌、微生物、あるいは毒物などの微生物学的原因、例えば細菌、胞子、ウイルス、酵母、またカビの侵入や保有;

(2) 洗浄用や殺菌用の物質からのものを含む化学的原因、例えば潤滑油や洗浄液;

(3) 原材料、機器、あるいは他の原因から生じる異物、例えばアレルゲン、小動物、金属、また機器の構築で用いられている物質。

6.3.9 危険な物質 (例えばガス、液体、粉塵、ミスト、蒸気) の放出、生成、及び/もしくは使用

機器はそれが発生する危険な素材や物質の吸入、摂取、皮膚、眼、また粘膜への接触、また皮膚を通した貫入のリスクを避けられるように設計し構築すること。そのリスクを避けられない場合、使用者に適切な警告を与えること。

6.3.10 監視なしでの動作

様々な使用条件のもとでの監視なしでの機器の動作が予期される場合、その条件の選択と調整を安全かつ確実に行なえるように設計し構築すること。

6.3.11 電源への接続と停電

機器への電源の停電、及び/もしくは停電の後の復電が危険な状況を生じないこと。特に、機器が意図せずに始動せず、また機器の可動部の危険な形での落下や放出がないこと。

6.3.12 機器の組み合わせ

機器を他の機器と組み合わせて使用することが意図されている場合、それぞれの構成要素は危険を生じることなく組み立てられるように設計し指示書を提供すること。

6.3.13 内破

機器は負圧によって引き起こされる内破の原因に耐え、ガスやその他の物質を危険な形で放出しないこと。

6.3.14 衛生条件

機器は感染のリスクを生じないような形で清掃できること。

6.3.15 エルゴノミクス

機器は移動や取り扱いを安全に行なえることを含めてエルゴノミクス原則に従って設計され製造されること。

6.4 機能安全と信頼性

6.4.1 一般

機器は特に以下の事項から生じるハザードを防ぐように安全かつ信頼できるように設計し構築すること:

(1) 規格で示された電気的、磁気的、及び電磁的妨害を含め、予期される環境条件での使用に耐えられること;

(2) 合理的に予見可能な誤使用に耐えられること;

(3) 論理回路の誤り (一度に 1 つのみ発生する) がハザードを引き起こさないこと;

(4) 電源の停電や通常の変動がハザードを引き起こさないこと。

IEC 61508[6] 等の機能安全を扱う規格の適用範囲に入る機器、あるいは機器の構成要素は該当する規格に適合することが必要となるだろう。

6.4.2 機器の種類に関係するハザード

ある種の機器で考慮が必要かも知れない潜在的なハザードは以下のものを含む:

(1) 予期しない始動や停止;

(2) 停止しないことから生じるハザード。

6.4.3 システム障害

安全規格等は、システム障害の後の、あるいは電源の停電や変動のあいだやその後のハザードの防止に関連する規定を含むかも知れない。

6.5 システム関連セキュリティ

セキュリティ関連の以下の要求は IEC 62443[†28] から派生する。例えば USB, LAN, WLAN のようなインターフェースとその通信レイヤ (例えば TCP) の安全関連のセキュリティ・リスクが特定された場合、該当する規格などで、セキュリティを扱うための定性的なアプローチの決定、またそのリスク・インデックスを考慮しての以下のカテゴリのいずれかへの分類、またそのリスクに対する保護のための規定やガイドが示されるかも知れない:

(1) 偶発的な侵害に対する保護

(2) 少量の資源、一般的なスキル、また軽度の動機による、単純な手段を用いた意図的な侵害に対する保護

(3) 中程度の資源、対象の機器に関連する特定のスキル、また中程度の動機による、洗練された手段を用いた意図的な侵害に対する保護

(4) 広範な資源、対象の機器に関連する特定のスキル、また高度の動機による、洗練された手段を用いた意図的な侵害に対する保護

安全関連のセキュリティ・リスクに対する多くの保護方策は製品レベルではなくシステム・レベルでのみ管理できる。保護のための手段は以下のようなものを含むかも知れない:

(1) 個人識別と認証管理
(2) 使用の管理
(3) システム・インテグリティ
(4) 事象に対する迅速な対応
(5) 資源のアベイラビリティ

用いられるかも知れない方策の例は:

- システムとデータの無許可のアクセスからの保護のための認証とアクセス制御 (技術的、及び組織的手段を含むかも知れない);
- 無許可の操作の検知のための、伝送された、あるいはデバイスにローカルに保存されたデータのインテグリティの保護。

[†28] IEC 62443 series, *Security for industrial automation and control systems*

6.6 情報に関する要求

(1) 製造業者かサプライヤの名称、あるいはブランド名か商標が、機器に、あるいはそれが実際的でない場合はその包装に明確に印刷されること。適切な場合、製造の日付と場所を特定するためのマーキングも付けること。

(2) 機器に添付される情報は安全な設置 (組み立て)、保守、清掃、操作、及び保管のための指示も含むこと。

(3) 採用された全ての方策にも関わらずリスクが残留する場合、あるいは明らかでない潜在的なリスクがある場合、適切な警告を提供すること。

(4) それらを認知し遵守することが機器を意図された、また合理的に予見可能な用途で安全に使用できることを確かとするであろう基本的な特性は機器に、それが不可能な場合は添付される使用指示書に読みやすく消えないように表示すること。

(5) マーキングや使用指示書で提供された、機器の安全のために重要な情報は、意図された使用者が容易に理解できるものであること。

7 補足

7.1 リスクの見積もりの手法

CENELEC Guide 32 ではリスクの見積もりの手法として §3.3.2 で触れたようなリスク・グラフ法が示されているが、使用できる手法は他にもある。

またリスク・グラフ法を用いる場合も §3.3.2 で触れたものとは異なるリスク・グラフや入力パラメータを用いることもできる。例えば §3.3.2 をベースとして危害の程度 (S_n) や危害への曝露の頻度 (F_n) のレベル分けを細かくする (例えば 2 段階や 3 段階のレベル分けを 5 段階にする) ようなことも可能ではあるが、リスク・グラフが大きく複雑となるため、リスク・グラフ法は入力パラメータのレベル分けを細かくしたい場合にはあまり適さないかも知れない。

リスクの見積もりではしばしばリスク・マトリックス法も用いられ、これは多数のパラメータの使用には適さない (パラメータの数を増やすと 2 次元のマトリックスとして素直に表現できない) が、それ

ハザードの分類	ハザード	例	危険状態	危険事象	起こり得る危害や損害
感電やその他の電気的なハザード	漏洩電流	電線の接続	電線の劣化箇所での漏洩電流	電線の劣化箇所に触れる	人体を通した電流
	蓄積された電荷	モータの動作	静電気放電のスパーク	スパークが可燃性物質に飛ぶ	モータの焼損や人の火傷
火災のハザード	外部の着火源	機器への延焼	他の機器に接続された機器の着火	他の機器への延焼	他の機器の焼損や人の火傷
	内部の着火源	機器内での延焼	機器内のコンポーネントの過熱	コンポーネントの燃焼の開始	他の機器の焼損や人の火傷
機械的なハザード	不安定性	盤の組み立て	盤の不安定な組み立て	盤の落下	人の怪我や財産の損傷
	鋭いエッジ	機器の清掃	機器上の鋭いエッジの存在	機器の清掃中に鋭いエッジに触れる	手の切創
	振動	ドリルの使用	人が持ったドリルの強い振動	強い振動に伴いドリルを落とす	人の負傷
その他のハザード	騒音	真空掃除機の使用	真空掃除機が生じる騒音	騒音環境下に長期間居る小児	小児の耳鳴りや難聴
	危険な物質の使用	ガス絶縁スイッチギアの動作	ガス絶縁スイッチギアの絶縁材としての六フッ化硫黄 (SF_6) の使用	SF_6 の漏出	人に対する毒性
	電源への接続	ソケット・アウトレットの使用	誤った形状のソケット・アウトレットへのプラグの挿入	プラグの金属の接点に触れる	人体を通した電流
誤った動作から生じるハザード	ソフトウェアの論理的誤り	制御機器の動作	制御機器のソフトウェアの論理的誤り	論理的誤りを含む機能モジュールへのアクセス	機器の制御の誤り
電界、磁界、及び電磁界、その他の電離放射や非電離放射から生じるハザード	雷	機器の動作	機器の周囲の雷電磁インパルス	機器内でのサージ電圧の発生	機器の故障
エルゴノミクス	マン・マシン・インターフェース	データの読み取り	インターフェースに表示される曖昧な文字	データの読み間違い	誤ったデータの記録

表 1: ハザード、危険状態、危険事象の例

発生頻度		危害の程度				
		無傷	軽微	中程度	重大	致命的
		0	I	II	III	IV
5	頻発する	C	B3	A1	A2	A3
4	しばしば発生する	C	B2	B3	A1	A2
3	時々発生する	C	B1	B2	B3	A1
2	起こりそうにない	C	C	B1	B2	B3
1	まず起こり得ない	C	C	C	B1	B2
0	考えられない	C	C	C	C	C

表 2: R-Map — リスク・マトリックス

レベル	定性的な表現	人に対する危害	火災
IV	致命的	死亡	火災、建物焼損
III	重大	重傷、入院治療を要す	火災
II	中程度	通院加療	製品発火、製品焼損
I	軽微	軽傷	製品発煙
0	無傷	なし	なし

表 3: R-Map — 危害の程度 (厳しさ)

ぞれのパラメータを細かくレベル分けすることが可能である。

7.1.1 リスク・マトリックス法の例 — R-Map

R-Map[8][9][10] はリスクの見積もりにリスク・マトリックス法を用いており、危害の発生頻度 (表 4) と危害の厳しさ (表 3) に基づいて表 2 のような 6×5 のマトリックス上でリスクを表現し、大きく

- A 領域 — リスクを受け入れられない (intolerable)
- B 領域 — 実際的な範囲でリスクを低減すべき (ALARP; as low as reasonably practicable)
- C 領域 — リスクを受け入れられる (broadly acceptable)

の 3 つの領域に分類する。

図 5 と異なり、危害の回避の可能性はパラメータとして現れていないが、危害の発生頻度を

(1) 危険状態への曝露

(2) 危害を回避もしくは制限する技術的及び人の能力

レベル	定性的な表現	定量的な表現 (件/台 · 年)
5	頻発する	10^{-4}〜
4	しばしば発生する	10^{-5}〜10^{-4}
3	時々発生する	10^{-6}〜10^{-5}
2	起りそうに無い	10^{-7}〜10^{-6}
1	まず起り得ない	10^{-8}〜10^{-7}
0	考えられない	〜10^{-8}

表 4: R-Map — 危害の発生頻度 (家電品等)

の要素を考慮して見積もることで対応できる。[†29]

上では R-Map のリスクの見積もりの手法についてのみ触れたが、R-Map の体系にはリスク・アセスメントとリスク低減の他のステージで用いることのできる手法も含まれている。

R-Map、またリスク・アセスメント一般については様々な書籍が、またインターネット上で公開された情報 ([11] などの経済産業省が公表しているハンドブックや NITE からの様々な情報などを含む) がある。

[†29] また、実際の危害の発生頻度の適切なデータが利用可能な場合、そのデータをこれらの要素に分解することなく用いることもできるだろう。また、そのようなデータを利用できない場合も危害の発生頻度という 1 つの値のみを見積もれば済み、これはそれらの要素のそれぞれを決定するよりも簡単でわかりやすいように思われる。

8 参考資料

[1] CENELEC Guide 32 (2014), *Guidelines for Safety Related Risk Assessment and Risk Reduction for Low Voltage Equipment*
https://boss.cenelec.eu/media/Guides/CLC/32_cenelecguide32.pdf

[2] ISO/IEC Guide 51:2014, *Safety aspects — Guidelines for their inclusion in standards*

[3] ISO 12100, *Safety of machinery — General principles for design — Risk assessment and risk reduction*

[4] ISO TR 14121-2, *Safety of machinery — Risk assessment — Part 2: Practical guidance and examples of methods*

[5] ISO 13849-1, *Safety of machinery — Safety-related parts of control systems*

[6] IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems*

[7] 産業機械における安全防護物の無効化事由を踏まえた安全設計要件の考察, 岡部康平, 労働安全衛生研究」, Vol. 5, No.2, pp.63-72, (2012)

[8] R-Map 実践ガイダンス — 全ライフサイクルに対応した製品安全リスクマネジメント手法, 日科技連 R-Map 研究会, 2004, ISBN-13: 978-4817130464

[9] R-Map とリスクアセスメント (基本編、手法編 (1)、手法編 (2)), 日科技連 R- Map 実践研究会他, 2014

[10] R-Map と FTA を用いた消費生活用製品のリスクアセスメントについて, NITE 製品安全センター 製品安全技術課 事故リスク情報分析室 酒井健一, 2011,
https://www.nite.go.jp/data/000005682.pdf

[11] リスクアセスメント・ハンドブック, 経済産業省, 2010–2011,
https://www.meti.go.jp/product_safety/recall/risk_assessment.html

8.1 その他の関連資料

- 技術分野におけるリスクアセスメント, Mark G. Stewart, Robert E. Melchers, 酒井 信介, 小川 武史 訳, 2003, ISBN-13: 978-4627945715
- 技術者のための実践リスクマネジメント, 関根 和喜 他, 2008, ISBN-13: 978-4339024326
- 電子機器の「製品安全」技術入門, 井原 惇行 他, 1999, ISBN-13: 978-4526044229
- 知っておくべき家電製品事故 50 選 — 事故を知るとリスクが見えてくる, 中尾 政之, 宮村 利男, 2010, ISBN-13: 978-4526064975
- 機械・設備のリスクアセスメント — セーフティ・エンジニアがつなぐ、メーカとユーザのリスク情報, 向殿 政男 監修, 日本機械工業連合会, 2011, ISBN-13: 978-4542301856
- 機械・設備のリスク低減技術 — セーフティ・エンジニアの基礎知識, 向殿 政男 監修, 日本機械工業連合会, 2013, ISBN-13: 978-4542307018
- 安全の国際規格 (1): 安全設計の基本概念 — ISO/IEC Guide 51 (JIS Z 8051), ISO 12100 (JIS B 9700), 向殿 政男, 2007, ISBN-13: 978-4542404052
- 安全の国際規格 (2): 機械安全 — ISO 12100-2 (JIS B 9700-2), 向殿 政男, 宮崎 浩一, 2007, ISBN-13: 978-4542404069
- 安全の国際規格 (3): 制御システムの安全 — ISO 13849-1 (JIS B9705-1), IEC 60204-1 (JIS B9960-1), IEC 61508 (JIS C0508), 井上 洋一, 平尾 裕司, 蓬原 弘一, 川池 嚢, 2007, ISBN-13: 978-4542404076