危険から始まる安全工学(HBSE)に基づく安全設計　[No.1]

製品安全は、メーカーの安全設計、及びユーザーの安全な使用によって達成されることは、言うまでもありません。 特に機械設備については、危険源の同定と保護対策、残留リスクを含めたリスクアセスメントは、その基本的な考え方について、国際規格 ISO-12100:2010 (Safety of machinery - general principles for design - Risk assessment and risk reduction) で規定され、リスクアセスメントに基づくリスク低減プロセスを確実に実施することにより、機械設備使用者、及び機械設備製造者においても下記のような効果があるとされています。

●製品安全への直接的効果

1. 危険源を顕在化することによって、保護方策が適用できる。
2. リスク対策の優先順位を決めて、その対応がリスク対応方針に従って可能になる。
3. リスクの大きさを知って合理的な対策が実施できる。
4. リスクが明確になり、使用者（ユーザー）に則した対策が実施できる。
5. 機械安全の基本的な考え方が明確になり、第三者の理解が容易になる。
6. 国際的な機械安全と整合性が図れる。

●企業経営への間接的効果

1. 安全な機械設備を提供することにより企業イメージの向上が期待できる。
2. 安全性の差別化によって競争力の向上する。
3. 製造物責任予防として対応することによってリスククベースの経営的判断が出来る。

機械安全に関するリスクアセスメント手法においてリスクを低減するための3ステップメソッドは、
その基本的な方法ですが、危険源の同定や危害のひどさ、危険事象の発生確率は、実効性のある手法で行われているか、と言う問いに対しては、疑問の残ることが実際で現行の国際規格のISO 12100:2010の規格要求をベースにした実効的な機械の安全性向上のためのリスクアセスメントが望まれています。

機械の重要な危険性を漏れなく洗い出すこと、危険事象の発生確率を適切に行うことは、機械に関連する危険性・有害性を洗い出し、危険源から危害に至るプロセスを明確にして製品設計に反映させることによって実質的な安全対策（保護方策）を行うことが可能となります。

本題の危険から始まる安全工学は、危険源の同定や危害のひどさを漏れなく行うための手法としてその有効性が期待されて、これを**ハザードベース・セーフティー・エンジニアリング（HBSE: Hazard-Based Safety Engineering）**と呼んでいます。元祖は、ヒューレット・パッカード（HP）社で開発されてその後、国際規格 **IEC 62368-1**（Audio/video, information and communication technology equipment – Part 1: Safety requirementsの考え方のベースとなっています。

AV・ITコミュニケーション機器を対象とした**IEC 62368-1第1版が2010年に発行**され、この規格は ITコミュニケーション機器用の規格 **IEC 60950-1** とAV機器用の規格 **IEC 60065**の内容を一部包含していまが、安全に対するアプローチはHBSEを基本としたもので、その内容は従来と大きく異なっています。

HBSEは、メーカーが製品研究・開発を行うにあたって最も基本的なニーズに応えるものであり、
安全規格による安全基準要求に単なる適合化する以上の実質的な安全対策手法として有効活用が出来るとされています。

■HBSEの基本的な考え方

ハザードベース、即ち、危険から始まる安全の基本原理は、「傷害（危害）は、ある人体に、十分な大きさ、かつ時間のエネルギーが加えられた時のみ発生する」と言う考え方で概念は、下図で示されます。

●スリーブロック・エネルギー伝達モデル

＜着眼点＞

・どのような形態のエネルギーが機械装置から出てくるか、または蓄えられているか？

・そのようなエネルギー源は、製品稼働時、他の形態のエネルギーに変換されるか？

傷害(危害)の種類やエネルギーを人体から外へ移す（人が危険箇所へ接近）、または、人体に移す（危険箇所が人に暴露）などの伝達の方向に関係なく、機械装置が危害を及ぼすのは、エネルギーの伝達時に限られます。危険なエネルギーの伝達が起こる時には、そのエネルギー源と人体を結ぶ伝達のメカニズムが必ず存在しています。つまり、危険なエネルギー源と人体が正しく絶縁されていたら、傷害が起こる可能性を減少させることができます。この考え方が下図の「傷害に至らない」モデルです。

●安全エネルギーモデル　＊「傷害に至らない」

エネルギーの大きさと継続時間の限界値を、人体に傷害を生じないで耐えられる最高のレベルに設定します。エネルギの大きさとそれにかかる時間が人体の耐えられる度合を超えない限り、被害はないことになります。例えば、室温と同じ水は、危険なエネルギー源ではなく、指がその水に触れても人体に伝達されるエネルギは許容可能なレベルにあります。

●危険エネルギー減衰モデル　＊「傷害に至らない」

危険エネルギー源が大きさ、継続時間の条件において存在する場合、そのエネルギーを適切に減衰させるものをその危険エネルギー源と人体の間に入れて対策することでたとえ接触しても、人体が接するエネルギーは安全なレベルとなります。この減衰器はエネルギーを遮断し、危険エネルギー源を取り除くことで、傷害の発生を完全になくすることができます。

例えば、沸騰したお湯は、危険エネルギー源ですが、耐熱グローブをつけると、それが指に触れても、人体に伝達されるエネルギーは許容可能なレベルになります。

重要危険源の多くは「危険なエネルギーがある箇所から発生している点」に着目してリスクアセスメントにおいて危険エネルギーを追跡することによって、発生する可能性のある危害の保護対策を行う。
このことは、先に述べた危険から始まる安全工学(HBSE)と同様な考え方に基づいています。

■エネルギー追跡法(UHIM)　＊UHIM: Utility oriented Hazard Identification Method

エネルギー源から危険源（原因）に至るプロセスを分析して重要危険源を特定（同定）する手法です。

危険源（原因）から危険源（結果）に至るプロセスを分析するユーティリティ追跡法は、エネルギの伝達メカニズムを把握して同定するひとつのツールとして活用できます。
（但し、位置エネルギーや機械の不具合により発生する危険源を見つける事が困難なことがある。）

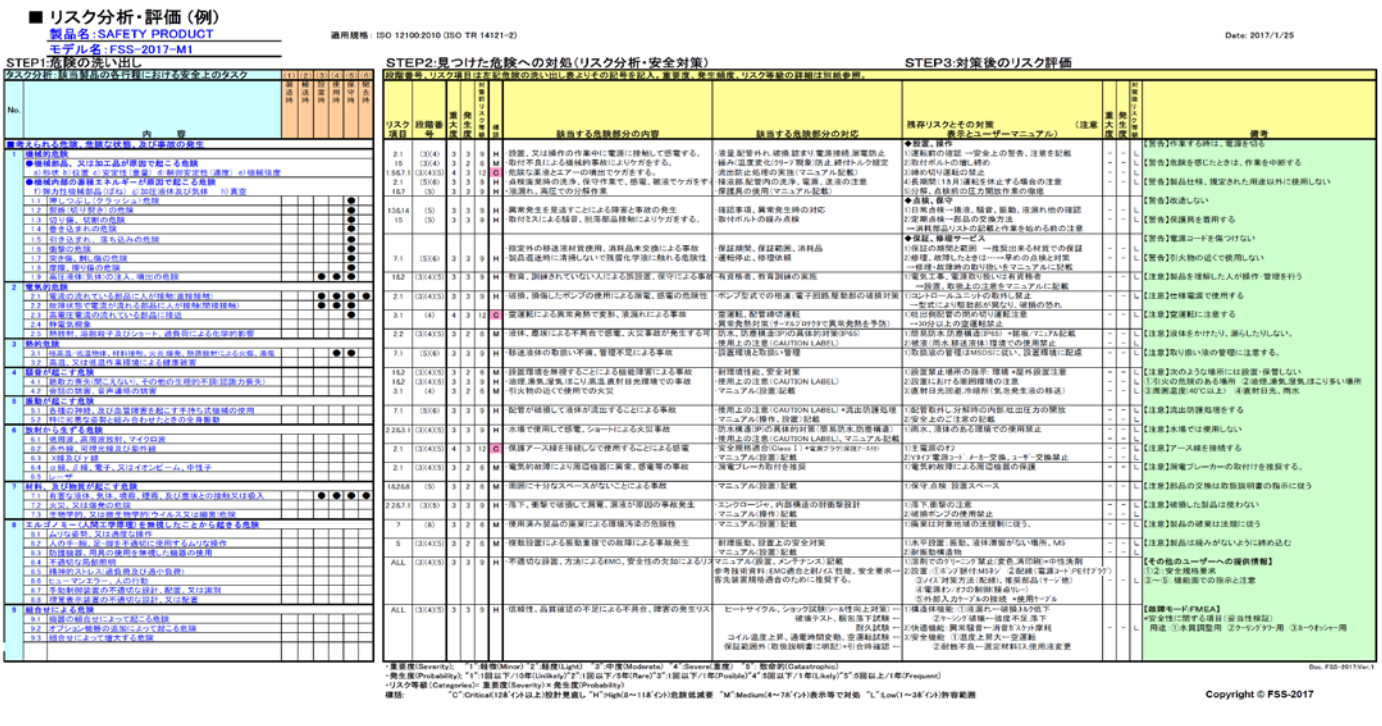
●エネルギ伝達による分類

エネルギー源(Ⅰ次)(E-Ⅰ) → **Ⅱ次エネルギー(E-Ⅱ)** → **Ⅲ次エネルギー(E-Ⅲ)**

- **エネルギー源(Ⅰ次)(E-Ⅰ)**
  - ･電気エネルギー
  - ･空圧エネルギー
  - ･蒸気エネルギー
- **Ⅱ次エネルギー(E-Ⅱ)**
  - ・力学 (運動・位置)エネルギー
  - ・電気エネルギー
  - ・熱エネルギー
  - ・放射、光エネルギー
  - ・化学エネルギー
- **Ⅲ次エネルギー(E-Ⅲ)**
  - ・音エネルギー
  - ・振動エネルギー
  - ・蓄積エネルギー

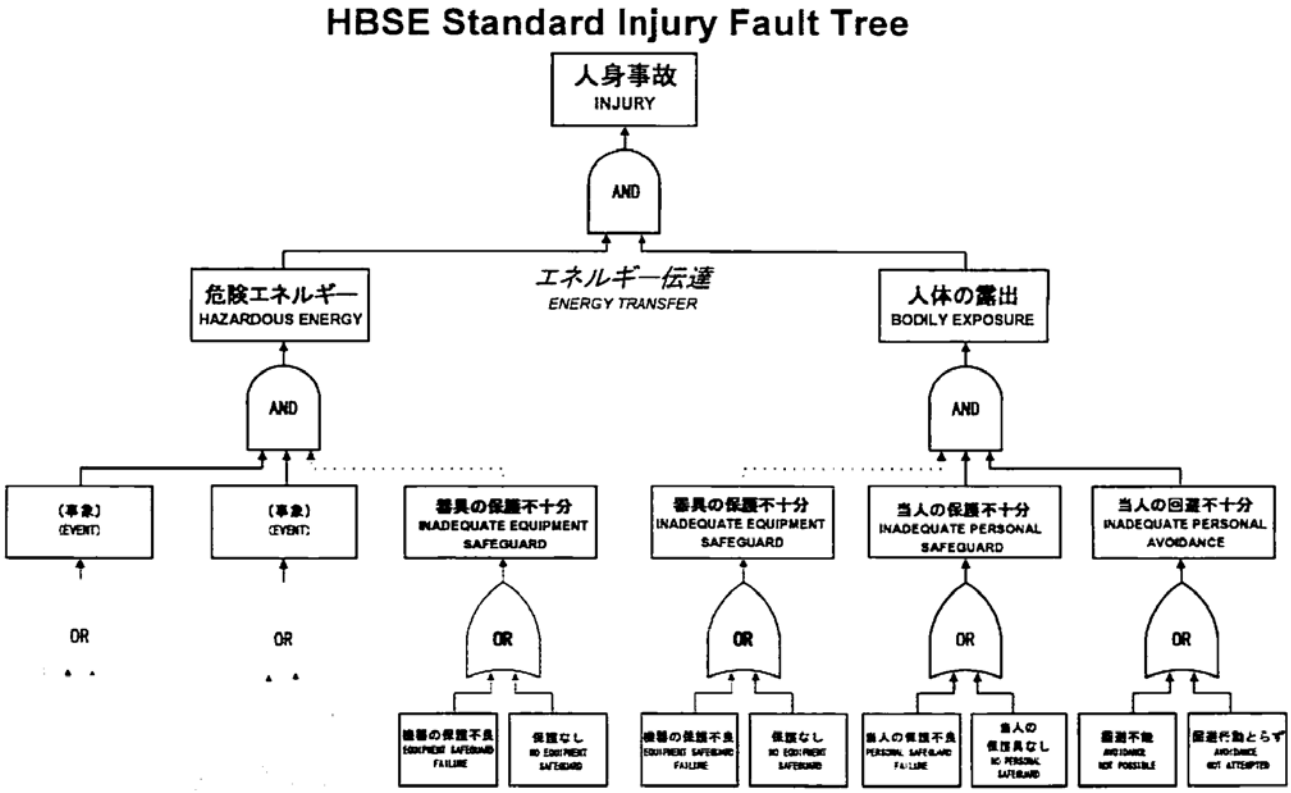
●ISO12100：2010で示される危険源（原因） ＊リスクアセスメントシートの例

※下記URL参照
http://fujisafety.jp/files/case/JS4-No4.pdf

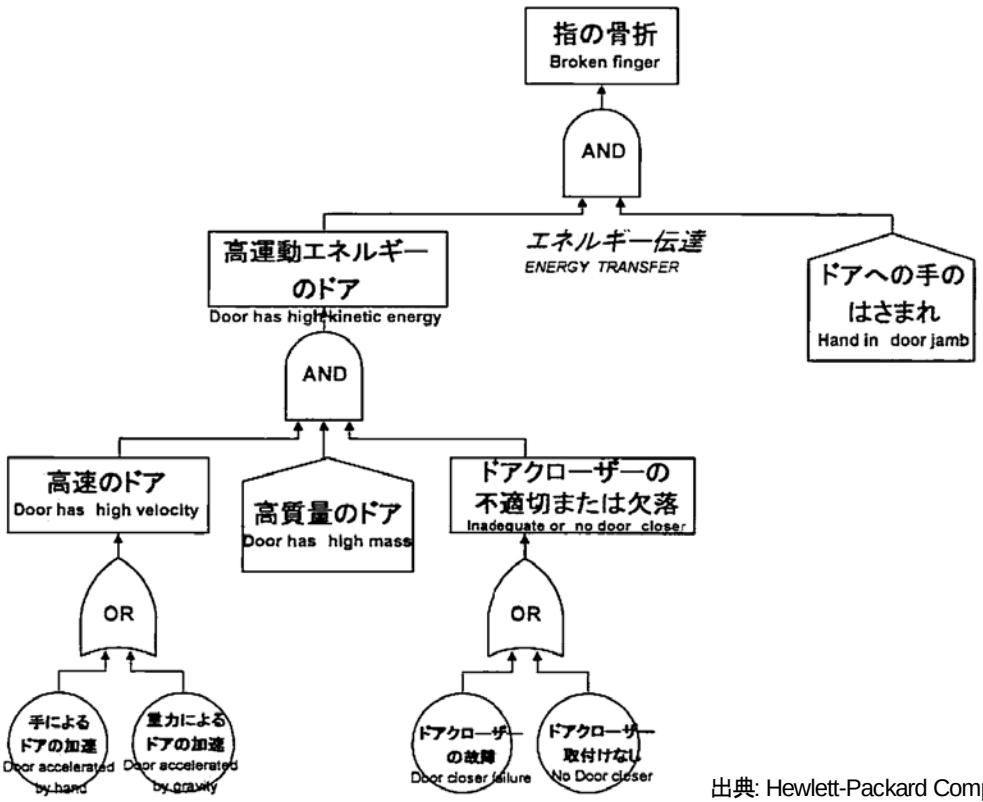

■ リスク分析・評価（例）
製品名：SAFETY PRODUCT
モデル名：FSS-2017-M1
適用規格：ISO 12100:2010 (ISO TR 14121-2)
Date: 2017/1/25
STEP1:危険の洗い出し
STEP2:見つけた危険への対処(リスク分析・安全対策)
STEP3:対策後のリスク評価
タスク分析：該当製品の各行程における安全上のタスク
危険箇所等、リスク項目は左記危険の洗い出し表よりその記号を記入。重要度、発生頻度、リスク等級の詳細は別紙参照。
Copyright © FSS-2017

■危険エネルギーのフォルトツリー解析（FTA）

危険エネルギーによるハザードは、その伝達プロセスにおいて正常状態と異常状態が考えられます。
設計段階のリスクアセスメント（分析）では両者の状態を考慮して安全設計を行うことが要求されますが、特に異常状態（不具合）については、フォルトツリー解析（FTA: Fault Tree Analysis)故障モード解析 (**FMEA**: Failure Mode and Effects Analysis) などが有効とされています。



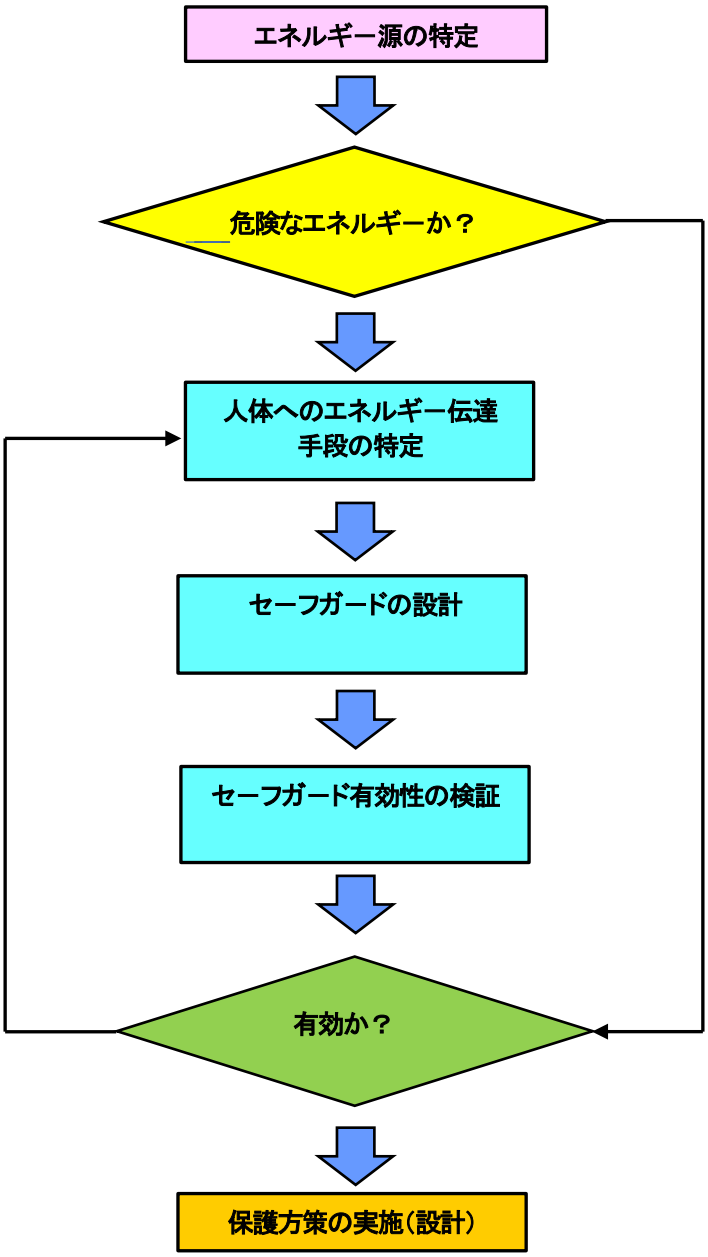
Example



出典: Hewlett-Packard Company(1990/1998)

■HBSEのプロセス

HBSEの具体的な対応プロセスは、「エネルギー源の特定」から始まります。
一般的なエネルギー源には、その経験から特定できるものもありますが、大きな機械設備システム、及び、最近のIoT技術を活用した機械設備は、前述のエネルギー追跡法(UHIMの手法を使うことによって漏れのない危険源の同定が期待されます。



＜着眼点＞

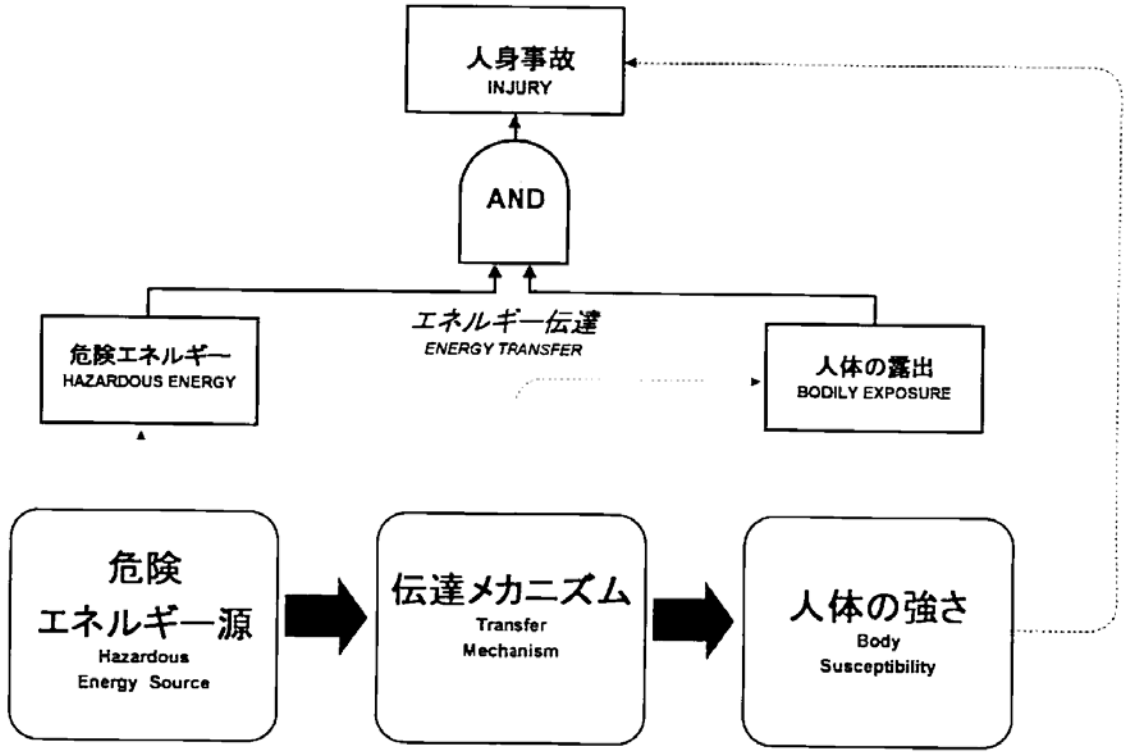
1. どのようなエネルギー源があるのか？
   最初に設計した時の危険エネルギーの形態、大きさは？

2. 機械装置を使用する時、危険エネルギーはどのように伝達され、
   どのような二次、三次の違うエネルギー形態となっているのか？

3. 不具合発生したの場合の危険エネルギーの状態はどのようになっているか？

4. 潜在的エネルギーの生成とその形態は何か？

下図のように設計段階でのリスク分析でエネルギー源を特定して、対象の危険エネルギー源の種類、大きさ、発生頻度がどのような傷害（危害）をもたらすのか、セーフガード（保護方策）の安全設計の前に先ず、危険エネルギーの伝達メカニズムを含めて把握して対策することが重要です。



出典: Hewlett-Packard Company(1990/1998)

以上、機械設備のリスクアセスメントを行って、そのリスク低減のための保護方策を実施するためには危険エネルギー源を特定してそのエネルギー形態を把握して、伝達メカニズムのリスク分析を系統的・科学的に行うことが最も重要となります。

リスクアセスメントは、ハザード・ベース(HBSE)の考え方を基にして、その手段としてエネルギー追跡法(UHIM)を使って、危害のひどさ、発生確率を危険状態が危険事象に至る過程を適切に把握してメーカー及び、ユーザーを含めたトータルリスクアセスメントによって安全な機械設備にすることが重要です。

特に現在、課題となっていることに下記が有りますが、今後、国際規格のあり方を含めて実効性のあるリスクアセスメントによる保護方策の実施が求められています。

1. 重大な危険源を見落とすことがない同定方法
2. 危害のひどさを具体的に判断できる方法
3. 危害の発生確率をいい加減に見積もらない方法