

## 4. 安全

# 安全の定義 (ISO/IEC GUIDE51)

- 1) 害 (harm) : 直接的又は間接的な財物又は環境への損害の結果としての、健康又は財物に対する物理的外傷及び／又は損害
- 2) 危険 (hazard) : 潜在的な害源
  - 具体的な原因のことを指す
- 3) 危険な状況 : 人が危険にさらされる状況
- 4) 危険な事象 : 害を生じる危険な状況
- 5) リスク (risk) : 害の発生確率とその害の重度の組み合わせ

- 6)残留リスク : 防止措置を講じた後に残留するリスク
- 7)防止措置(protective measurement) : 少なくとも許容可能リスクを達成するために講じるリスク削減方策の組み合わせ
- 防止措置には、本質安全によるリスクの削減、保護機器、保護具、使用及び設置のための情報及び訓練を含む
- 8)許容可能リスク : 社会の現在の価値観に基づいて、所定の状況の中で受け入れられるリスク
- 例えば、 $10^{-6}$ ~ $10^{-8}$ 程度。これは自然災害によって死ぬ確率の程度で、自動車災害によって死ぬ確率よりも小さい
- 9)安全(safety) : 許容不能なリスクが無いこと

# 「安全」という用語の使用方法

安全(安全な)という用語は、時には機能(通常, 保護又は警告／警報など)を表わす用語の代わりに、又はそれと一緒に使用される。間違いではないが、記述形容詞としての安全という用語は、この場合好ましくない。この用語が有益で特別な情報を伝達しないで、保証付きの無リスクの保証として解釈されるからである。

× 安全帽, 安全靴    ○ 保護帽, 保護靴

# 絶対安全

- 絶対安全は存在しえない
- 多少のリスクは残る
- 従って製品, 工程又はサービスは相対的な安全でありうるにすぎない

# リスクを削減して安全にする方法

- リスクアセスメント
  - 予見できる誤使用や故障まで含めて発生しうる害を数え上げ, リスクを求める
- リスク削減
  - リスクが大きければ, なんらかのリスク削減対策をほどこす
- 安全になるまでこのプロセスを反復

# リスク削減方策

- 「リスク」＝「害の発生確率」  
×「その害の重度」
- もしも故障しなければ害が発生しないとしたならば、故障しないようにすればリスクは低減できる  
⇒ 信頼性

# 信頼性

- 故障しないものは存在しない！
- 故障は確率的に起る
- 故障にはいくつかのパターンがある

# 故障率の基本パターン

- 減少型
  - 時間とともに故障率が減少
  - 多くの電子部品は初期故障が多い
- 一定型
  - 時間に関わりなく故障率が一定
- 増加型
  - 時間とともに故障率が増加
  - 磨耗・老化等で寿命が来て集中的に故障する
  - 故障が集中する前の定期交換が有効

# 代表的な故障パターン

- 減少型・一定型・増加型が混在
  - はじめに初期故障期に故障が多発
  - その後故障の少ない偶発故障期
  - 最後に故障が頻発する磨耗故障期

# 信頼性を高めるには

- 信頼性の高い部品を使用
- 製造方法, 検査, 輸送などの信頼性を高める
- システムの多重化
  - 複数のシステムでバックアップすることによって, 一つが故障しても動作するようにする

# フェールセーフ (fail safe)

異常が発生したときに人に傷害を及ぼさないように設計されていること

情報分野でのフェールセーフとは、異常が発生してもプログラムの破壊やデータの紛失などが無いことを指し、意味が異なるので要注意

# フールプルーフ (foolproof)

人為的に不適切な行為や過失などが起こっても、要素またはシステムの信頼性・安全を保持するような設計または状態

# 障害物・ヒト検知の二つの方法

- 反射型センサ
- 透過型センサ

# 反射型センサ

- ヒトの有無を反射光で検出するセンサ
- ヒトがいるときに(危険時)反射光が戻る
- ヒトがいないときに(安全時)反射光は戻ってこない
- 故障すると信号が出ない  
= 危険側に故障
- 故障した際にはヒトがいてもそれを検出できずに事故に結びつく

# 透過型センサ

- 投光部と受光部の間にヒトがいると光が遮断されて検出されるセンサ
- ヒトがいるときに(危険時)光は遮断される
- ヒトがいないときに(安全時)光は受光される
- 故障すると信号が出ない  
= 安全側に故障
- 故障の時にも事故を防ぐことができる

# 踏切の障害物検出装置



フェールセーフを考慮  
して透過型センサを  
使っている

# 危険検出型安全と 安全確認型安全

- 危険検出型は、故障すると危険側になる
- 安全確認型は、故障すると危険信号が出るため、フェールセーフとなる

# ロボットの安全

# アイザックアシモフのロボット三原則 (I, Robot 1950)

1. ロボットは人間に危害を加えてはならない。また、その危険を看過することによって、人間に危害を及ぼしてはならない
2. ロボットは人間にあたえられた命令に服従しなければならない。ただし、あたえられた命令が、第一条に反する場合には、この限りではない
3. ロボットは前掲第一条及び第二条に反するおそれのないかぎり、自己を守らなければならない

# ロボットは危険

- 重いものを運ぶことができる
  - 大きな力で人間に怪我をさせる
- 高速に動作する
  - 大きな衝撃力で人間に怪我をさせる
- 汎用性が高い
  - 動きが予測不可能で人間に不意打ちを食らわせる

- ロボットが人間に衝突したときに、大型ロボットでは200Gもの衝撃力を与える
- 人間は通常100Gの衝撃力を受けると死亡事故の恐れがある！

# ロボットによる災害事例

- 3時の休み時間を利用してロボットの可動範囲内に入って実習を行っていたときに、戻ってきた担当者が可動範囲内に人間がいないことを確認せずに起動ボタンを押したためにロボットが動いて作業者が挟まれた
- ロボットが作業対象を落としたのに気づいた作業者が、スイッチを切らずにそれを取り除こうとしたために、ロボットに接触した

- 加工不良のためにすべての機械が止まっているのを発見した担当作業者が、コンベア上の不良ワークを取り除いたところ、突然ロボットが動作を始めた
- ティーチングボックスを用いたロボットの教示作業中に、溶接火花による電磁ノイズによって制御装置が暴走し、ロボットが高速で動作しはじめた

# ロボットで最も多い事故は、

ロボットの停止中に、人間がロボットの可動範囲内に進入しているとき、何らかの理由でアームが不意に作動したために、よけきれずに災害に至る

# なぜロボット（メカトロ機械）は危険なのか？

- ロボットは微小電力の電子機器によって制御され、大きな力を出す機械
- すなわち、微小な信号の乱れが大きなパワーの暴走につながる

# ロボットによる不意打ちのパターン を防ぐには

- トラブルを考慮した保護装置の必要性
- フェールセーフ、安全確認型

# ロボットの安全対策

- 隔離・停止の原則
- ロボットは人間から隔離する
  - ガード(柵・囲い)
- 隔離できないときにはロボットは停止する
  - 安全装置

# インターロック

- 条件が満足されなければ動作しないような構造
- 柵の扉を開けるところにインターロック構造にする

# 人間共存型ロボットの安全

- 人間と同じ空間で作業行うロボット（サービスロボット、パーソナルロボット、福祉ロボット）の場合には、「隔離・停止の原則」が適用できない！
- この場合の安全対策はどうする？

# 人間共存型ロボットの安全対策

- 近接センサによって接触前に検知
  - ⇒ フェールセーフにできない
- カセンサによる接触検知
  - ⇒ フェールセーフにできない
  - ⇒ 動きが速いと回避できる時間がない
- 柔軟構造
  - ⇒ 本当に柔らかいと安全なのか？
  - しなやかな鞭は使い方によっては大きな破壊力！

- 力制限機構によって、過大な力が発揮できないようにする
  - ⇒ 1自由度であれば効果的
  - ⇒ 多関節ロボットへの適用困難
- 結局現在はまだ良い方法が無い
- 唯一の方法はアクチュエータのパワーを制限すること