

機械の安全・信頼性に関するかんどころ

機械製品に対する安全要求と設計方法

2011.2.28
(財)機械振興協会 技術研究所

機械製品の故障や事故で、使用者が危険な状態におかれるケースが目立っています。このような状況を改善するために、機械製品の安全設計が必須であり、安全な機械製品を造る要求条件とその設計方法の確立が望まれます。ここでは、機械製品に対する安全要求とその設計方法の一例を15回に分けて紹介していきます。

(第1回) 安全要求	—重大/致命的な危険に対する安全要求—
(第2回) 安全設計	—故障許容設計—
(第3回) 安全設計	—リスク最小化設計—
(第4回) 安全設計	—故障の伝播防止設計—
(第5回) 安全設計	—冗長系分離設計—
(第6回) 個別安全要求と設計	—構造—
(第7回) 個別安全要求と設計	—応力腐食割れ—
(第8回) 個別安全要求と設計	—圧力システム—
(第9回) 個別安全要求と設計	—シャープエッジ—
(第10回) 個別安全要求と設計	—材料要求と選別方法—
(第11回) 個別安全要求と設計	—電気システム—
(第12回) 個別安全要求と設計	—バッテリー—
(第13回) 個別安全要求と設計	—感電—
(第14回) 個別安全要求と設計	—接触温度—
(第15回) 個別安全要求と設計	—検証—

(第1回) 安全要求 —危険の制御—

(財)機械振興協会
技術研究所

機械製品における**安全要求**とは、以下に挙げる製品機能の非正常動作を制御、もしくは取除き、起こりえる**危険**を防止することです。

- ・機能の意図しない作動：作動してはいけないときに動作する。
- ・機能の喪失：作動しなければならないときに作動しない。

また、危険は「重要度」と「被害の大きさ」により、以下の2つに区分されます。

- ①**重大な危険**：使用者の損傷や装置にかなりの被害を与える状態です。
- ②**致命的な危険**：恒久的な損傷さらには人命損失や装置に重大な被害を与える状態です。

次ページ以降、「**重大な危険**」と「**致命的な危険**」に対する「**安全要求**」を解説していきます。

①重大な危険



②致命的な危険



(第1回) 安全要求 — 重大危険に対する安全要求 —

「重大な危険」に対しては、2つのパターン(①1つの故障、②1つの誤操作)により危険が生じない対策(1故障許容設計)をおこないます。そのために、以下の要求を満足させる必要があります。

要求1: 2個の独立した抑制機能(ここではインヒビットと呼びます)による制御を行う。(図1)

要求2: 上記インヒビットのモニタを必要に応じて行う。

要求3: 単一故障により危険が発生する場合には、その故障を除去する制御(制御の独立)を行う。(図2)

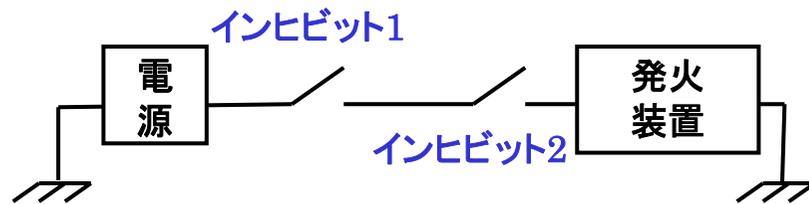
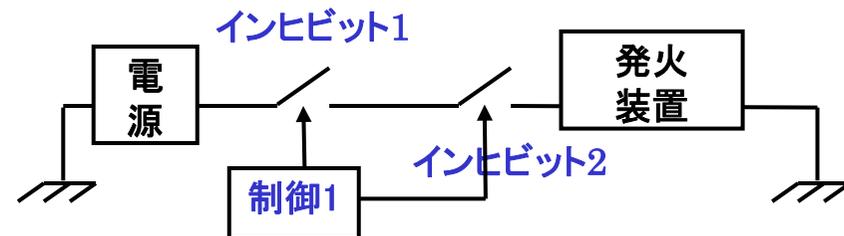
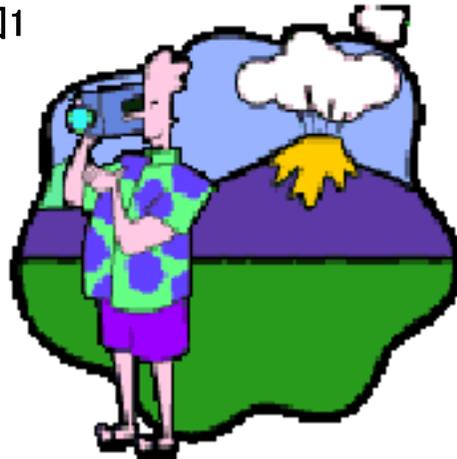


図1

ポイント: 重大な危険には
1故障許容設計!!



制御の
独立

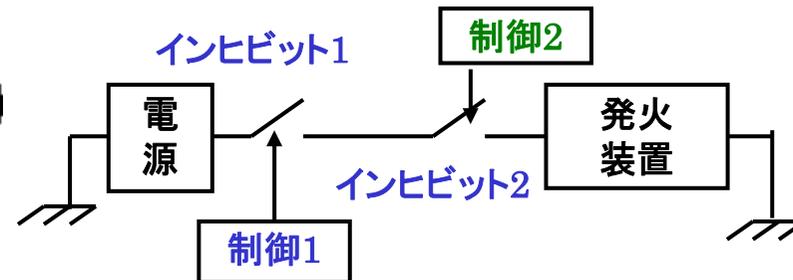


図2

(第1回) 安全要求 — 致命的な危険に対する安全要求 —

「致命的な危険」に対しては、3つのパターン(①2つの故障、②2つの誤操作、③1つの故障と1つの誤操作)により危険が生じない対策(2故障許容設計)を行います。そのために、以下の要求を満足させる必要があります。

- 要求1: 3個以上の独立したインヒビットによる制御を行う。(図3)
- 要求2: 3個のインヒビットのうち、一つは当該コンピュータに依らない。
- 要求3: 同一コンピュータ、同一製造者によるソフトウェアを使用しない。



ポイント: 致命的な危険には
2故障許容設計!!

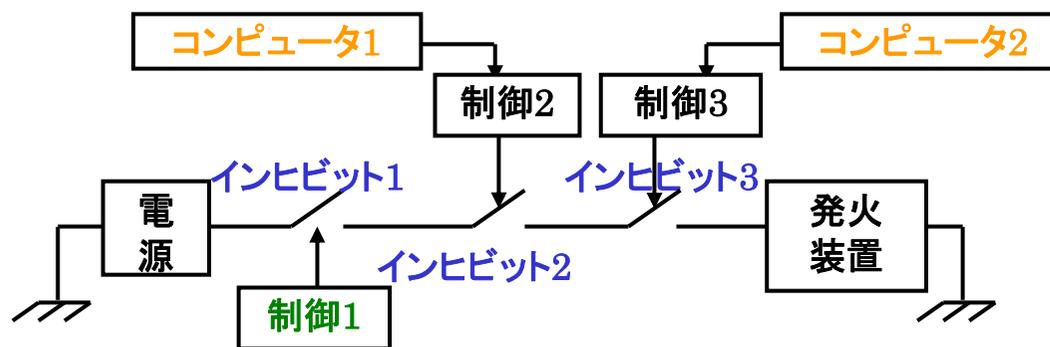


図3