

# 安全に関連する機械等(SIL含む)の認証の考え方と 審査項目

2015年2月24日

技術支援部 石田豊

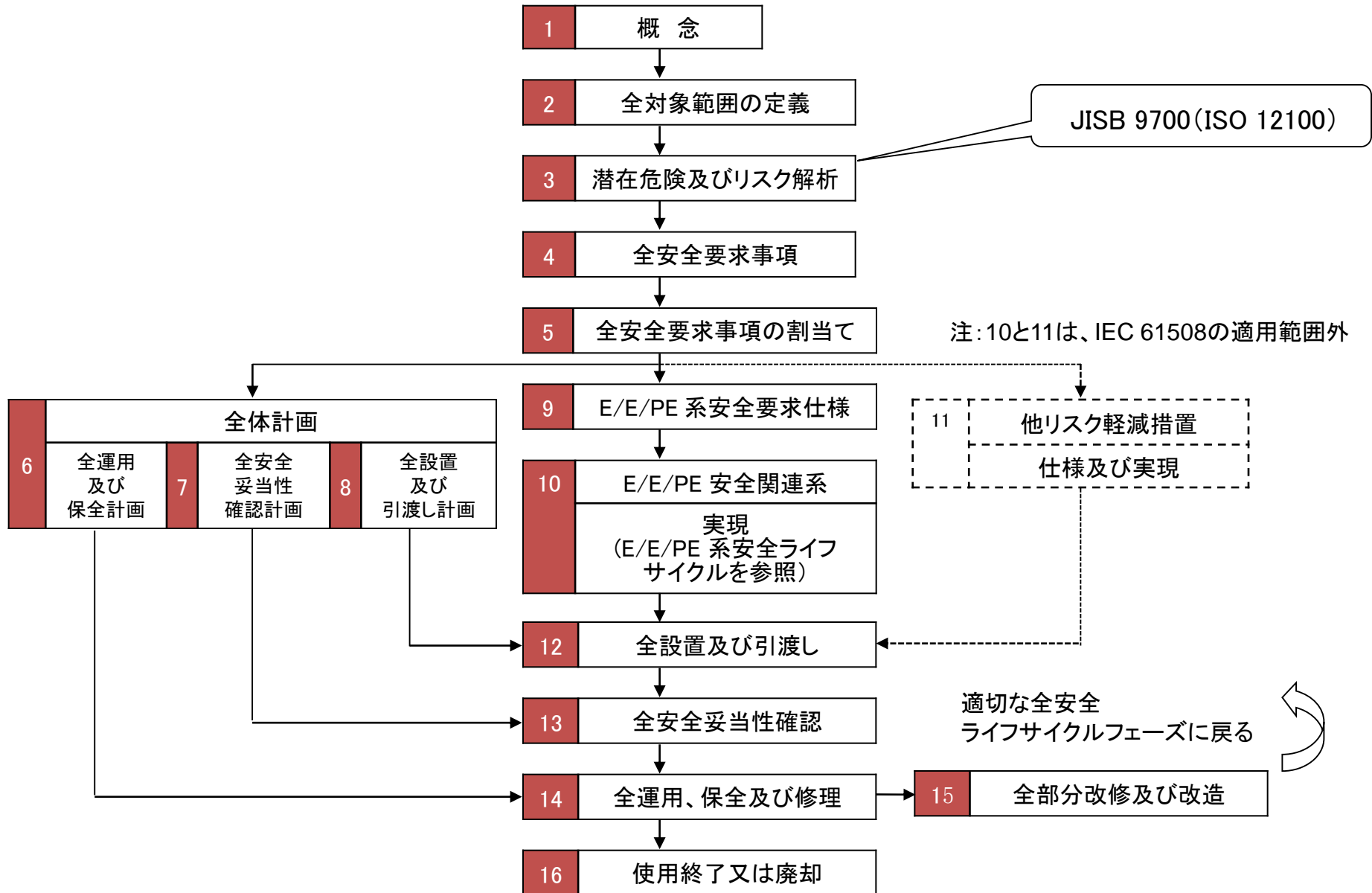


公益社団法人

**産業安全技術協会**

Technology Institution of Industrial Safety

## 全安全ライフサイクル (JIS C0508-1:2012 図2より)



### 安全状態 (safe state)

「安全が達成されているEUCの状態」 JIS C0508-4の3.1.13項

EUCが、どのような入力に対しどのような出力をしている時が安全状態なのかを決める。

この安全状態に如何に失敗なく到達するか？を問うもの。

EUCの安全状態はユーザが、また、EUCサブシステム(例センサ)の安全状態はその製造者が決める。

### ランダムハードウェア故障 (random hardware failure)

「時間に関して無秩序に発生し、ハードウェアの多様な劣化メカニズムから生じる故障」 JIS C0508-4の3.6.5項

ハードウェアはランダムに故障が発生すると想定したうえで検出できない危険側故障がどれくらいの割合で発生するかを机上で計算する。一般にFMEDA(Failure Modes, Effects and Diagnostic Analysis)という手法を使う。IEC 61508-2では、FMEA。

### 決定論的原因故障 (systematic failure)

「決定論的原因故障の事例」 JIS C0508-4の3.6.6項の注記3

- 安全要求仕様(中のヒューマンエラー)
- ハードウェアの設計, 製造, 設置及び運転(中のヒューマンエラー)
- ソフトウェアの設計, 実施, その他(中のヒューマンエラー)

以上は「設計の部分改修、製造過程、運転手順、文書化又はその他の関係する要因の修正によってだけ除くことができる」と定義されており、マネジメントで故障を回避。

### H/W

決定論的原因故障

+

ランダムハードウェア故障

TOE; Target of Evaluation

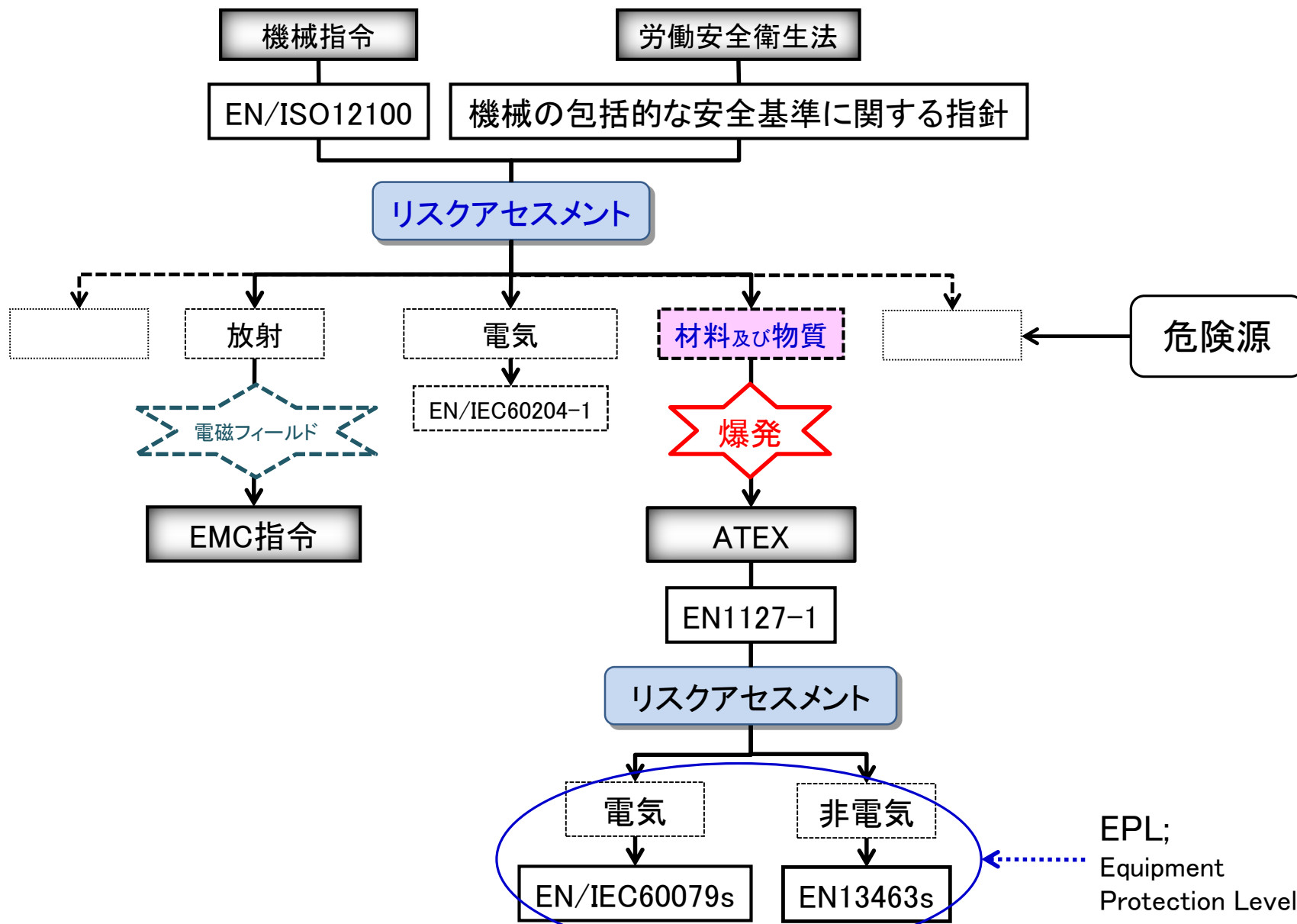
FMEA (FMEDA)

### S/W

決定論的原因故障

TOE; Target of Evaluation

TOE Ref.	Target of Evaluation (TOE)	Purpose of TOE	IEC 61508 Clauses & Tables	Comments	Assessors comments from document review and audit
1	Functional Safety Management System		1/6.2.1 to 6.2.18		
2	Functional Safety Policy		1/6.2.2, Figs 2,3,4, Table 1, and 1/6.2.1 as framework.		
3	Organisation and Responsibilities		1/6.2.3, Figs 2,3,4, and 1/Table 1, See Note under 6.2.1		
4	Identification of relevant lifecycle phases		1/6.2.1, Figs 2,3,4, and 1/Table 1		
5	Documentation structure and content policy		1/6.2.4, 1/5		
6	Techniques and Measures conformance plan		1/6.2.12.a, (see parts 2, 3 and 6)		
7	Corrective action procedure		1/6.2.5, 1/6.2.10, 1/7.4, 1/7.8, 1/7.14, 1/7.16, 1/7.18, 1/8.0 Parts 2 and 3, Figs 2,3,4 and 1/Table 1 as framework.		
8	Competence assessment process		1/6.2.13, 6.2.14.a-k, 6.2.15 Figs 2,3,4 and 1/Table 1 as framework.		
9	Procedure for handling of hazardous incidents.		1/6.2.5.f, 6.2.6		
10	Procedure for O&M performance analysis		1/6.2.12.c, Figs 2,3,4 and 1/Table 1 as framework.		
11	Functional safety audit process		1/6.2.7,		
12	Modification process for Safety related systems		1/6.2.8.a, 1/6.2.8.b, Figs 2,3,4 and 1/Table 1 as framework. 1/7.16.2.2		
13	Procedures for maintaining information on hazards with respect to Safety-Related Systems		1/6.2.9		
14	Configuration management procedures		1/6.2.10, Figs 2,3,4 and 1/Table 1 as framework.		
15	Procedures for provision of training and information for the emergency services		1/6.2.11		
16	Functional Safety Management System - Formal Reviews		1/6.2.16		
17	Supplier Assessment Process		1/6.2.17		
18	Functional Safety Assessment		1/6.2.12.b, 1/8.1, 1/8.2, 1/Table 4, 1/Table 5, 3/8, 3/Table A10		



### IEC 60079-33: 2012 Explosive atmospheres – Part 33: Equipment protection by special protection 's' 爆発性雰囲気 – 第33部 特殊防爆構造”s”による装置の防護

#### - INTRODUCTION - より

この規格は、基本的な安全要求事項が今ある規格によりカバーしていない場合どのようにして本質的安全要求事項に合致することができるのかをデモンストレートし、**革新を受け入れ、未知ものを取り扱うフレームワークを規定**することを意図している。

#### 2 引用規格

IEC 60079(全パート), 爆発性雰囲気

IEC 60079-0, 爆発性雰囲気 – 第0部: 機器 – 一般要求事項

IEC 60079-29-1, 爆発性雰囲気 – 第29-1部: ガス検知器 – 可燃性ガスに対する検知器の特性の要求事項

IEC 60079-29-2, 爆発性雰囲気 – 第29-2部: ガス検知器 – 可燃性ガス及び酸素に対するガス検知器の選択、設置、使用及び点検

IEC 61508(全パート), 電気/電子/プログラマブル電子の安全関連系の機能安全

IEC 61511(全パート), 機能安全 – プロセス産業分野に対する安全計装システム

IEC 62061, 機械類の安全 – 安全関連電気、電子及びプログラマブル電子制御システムの機能安全

ISO 13849-1:2009, 機械類の安全 – 制御システムの安全関連部分 – 第1部: 設計の一般原理

ISO 13849-2, 機械類の安全 – 制御システムの安全関連部分 – 第2部: 検証

## 8 アセスメントおよび試験仕様の準備

### 8.1 一般事項

爆発保護の完全性に影響を与える、すべての適切なIEC 60079シリーズの要求事項が適用されること。

### 8.2 アセスメントおよび試験仕様

アセスメントおよび試験仕様は、製造者により準備され～



## 1 適用範囲

製品、プロセス及びサービスの認証機関に対する能力、一貫性のある運営及び公平性に関する要求事項について規定する。この規格に基づき運用する認証機関は～

## 2 引用規格

JIS Q 17000 適合性評価－用語及び一般原則 注記 対応国際規格

JIS Q 17020 適合性評価－検査を実施する各種機関の運営に関する要求事項

JIS Q 17021 適合性評価－マネジメントシステムの審査及び認証を行う機関に対する要求事項

JIS Q 17025 試験所及び校正機関の能力に関する一般要求事項

## 3 用語及び定義

### 4 一般要求事項

4.1 法的及び契約上の事項

4.2 公平性のマネジメント

4.3 債務及び財務

4.4 非差別的条件

4.5 機密保持

4.6 情報の公開

## 5 組織運営機構に関する要求事項

### 5.1 組織構造及びトップマネジメント

### 5.2 公平性確保のメカニズム

## 6 資源に関する要求事項

### 6.1 認証機関の要員

### 6.2 評価のための資源

## 7 プロセス要求事項

### 7.1 一般

### 7.2 申請

### 7.3 申請のレビュー

### 7.4 評価

### 7.5 評価結果のレビュー

### 7.6 認証の決定

### 7.7 認証文書

### 7.8 認証された製品の登録簿

### 7.9 サーベイランス

### 7.10 認証に影響を与える変更

### 7.11 認証の終了, 範囲の縮小, 一時停止又は取消し

### 7.12 記録

### 7.13 苦情及び異議申立て

## 8 マネジメントシステム要求事項

### 8.1 マネジメントシステムに関する選択肢

選択肢A→ISO 9001認証未取得

選択肢B→ISO 9001認証取得

### 8.2 マネジメントシステム文書(選択肢 A)

#### 8.3 文書管理(選択肢 A)

#### 8.5 マネジメントレビュー(選択肢 A)

#### 8.6 内部監査(選択肢 A)

#### 8.7 是正処置(選択肢 A)

#### 8.8 予防処置(選択肢 A)