JASA Webセミナ
Safety の国際規格の動向 in 2022

機能安全関連規格

2022年9月28日

JASA 安全性向上委員会 委員
竹市　正彦

一般社団法人
組込みシステム技術協会
Japan Embedded Systems Technology Association

© Japan Embedded Systems Technology Association

内容

1. 講師紹介
2. 本セミナ対象規格の概要
   規格の背景、概要の紹介
3. 機能安全規格基礎規格の動向
   IEC61508の動向
4. 産業機械業界関連規格の動向
   IEC62061やISO13849関連
5. 自動車関連やその他規格の動向
   ISO26262, SOTIF, UL4600, ISO21434
6. まとめ

IEC 61508-1

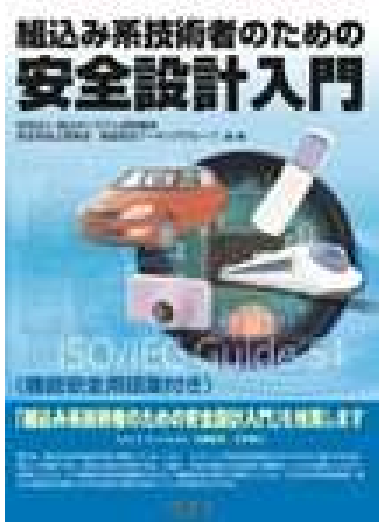
Edition 2.0 2010-04

第 2.0 版 2010 年 4 月

書籍紹介

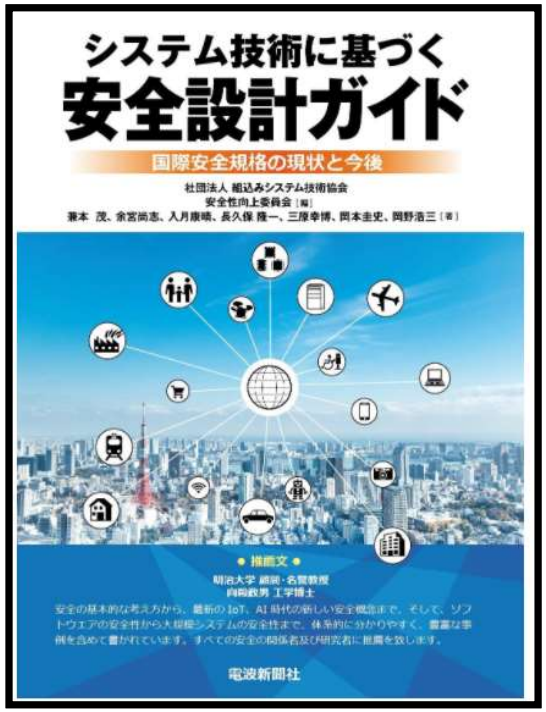
安全の基本的な考え方から、
最新のIoT、AI時代の新しい安全概念まで、
体系的に分かりやすく、豊富な事例を含めて書かれています。
すべての安全の関係者及び研究者に推薦を致します

安全の概念と安全設計の
基礎をしっかりと説明した
うえで、如何にコンピュータで
製品の安全性を確保する
かという機能安全の考え方を
紹介している。これからの
安全技術者，組込み技術者
の常識となる安全設計の
基本を紹介



組込みシステム技術協会／
安全性向上委員会（編）

税込み（¥2,200+税）



組込みシステム技術協会／
安全性向上委員会（編）

税込み（¥2,700+税）

一般社団法人
組込みシステム技術協会
Japan Embedded Systems Technology Association

1. 講師紹介

JASA 安全性向上委員会　委員

国際規格エキスパート

IEC　TC65（工業用プロセス計測制御），TC56（ディペンダビリティ），TC9（鉄道）

IEC 61508（機能安全基礎規格），IEC TR 63069（安全／セキュリティ規格），IEC 62278（鉄道向け機能安全規格），IEC PT 62452（鉄道向けサイバーセキュリティ規格策定プロジェクト），IEC 62853（オープン　システム　ディペンダビリティ）、IEC 規格 JIS化プロジェクト　等

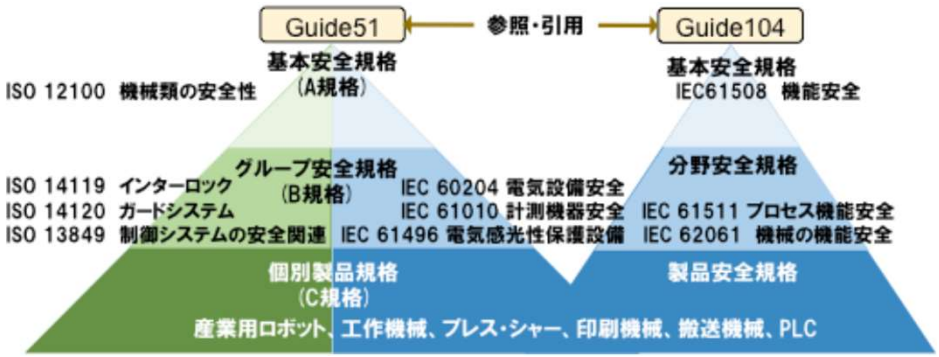
米国・欧州認証機関、日米　電子情報通信関連企業　R&D　ビジネス開発

2．本セミナ対象規格の概要

- 安全関連電子制御に不可欠な機能安全基礎規格 IEC61508および関連規格

IEC61508を基礎に様々な業界の技術基準策定
認証、法規制、PL訴訟の根拠

例えば、産業機械分野では
機能安全規格がさらに細かく体系化



出典：　厚生労働省　機能安全活用テキスト
https://www.mhlw.go.jp

機能安全関連規格

IEC61508以外の機能安全関連規格

ISO13849-1

Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design (ISO 13849-1:2015)

ISO19014 土木建築機械

Earth-moving machinery - Functional safety - Part 1: Methodology to determine safety-related parts of the control system and performance requirements (ISO 19014-1:2018)

ISO25119 農業機械

Tractors and machinery for agriculture and forestry – Safety-related parts of control systems – Part 1: General principles for design and development (ISO 25119-1:2018)

EN 15194

Cycles - Electrically power assisted cycles - EPAC Bicycles

UL 1998

STANDARD FOR SAFETY

Software in Programmable Components

UL 991

Standard for Tests for Safety-Related Controls Employing Solid-State Devices

ANSI/CAN/UL/ULC 2580:2021

JOINT CANADA-UNITED STATES NATIONAL STANDARD

STANDARD FOR SAFETY

Batteries for Use In Electric Vehicles

機能安全規格の概要

IEC 61508 Ed 2.0 2010-04　＞＞　Ed 3.0

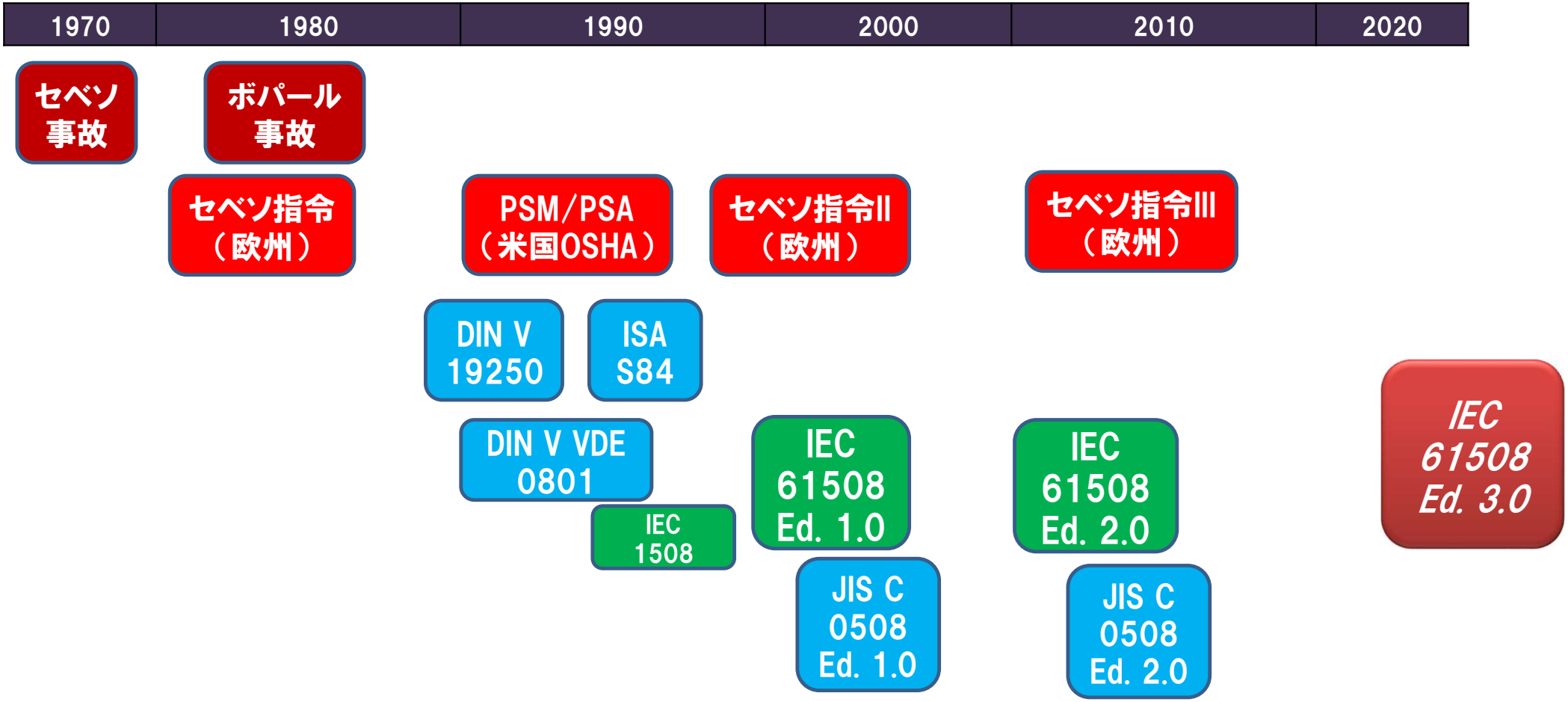
Functional safety of electrical/electronic/programmable electronic safety-related systems

電気・電子・プログラマブル電子安全関連系の機能安全

- 規格の構成

Part 1：一般要求事項安全ライフサイクル、機能安全管理・評価、システム・レベル要件	
Part 2:電気・電子・プログラマブル、電子安全関連系の要求事項	ハードウエア要件
Part 3:ソフトウェア要求事項	ソフトウエア要件
Part 4:用語の定義及び略語	
Part 5:安全度水準の決定方法の例	SIL決定方法の例
Part 6：IEC 61508・2及びIEC61508-3の適用の指針	安全分析手法等
Part 7:技法及び措置の概要	各種技術の説明

IEC61508経緯



一般社団法人 組込みシステム技術協会
Japan Embedded Systems Technology Association

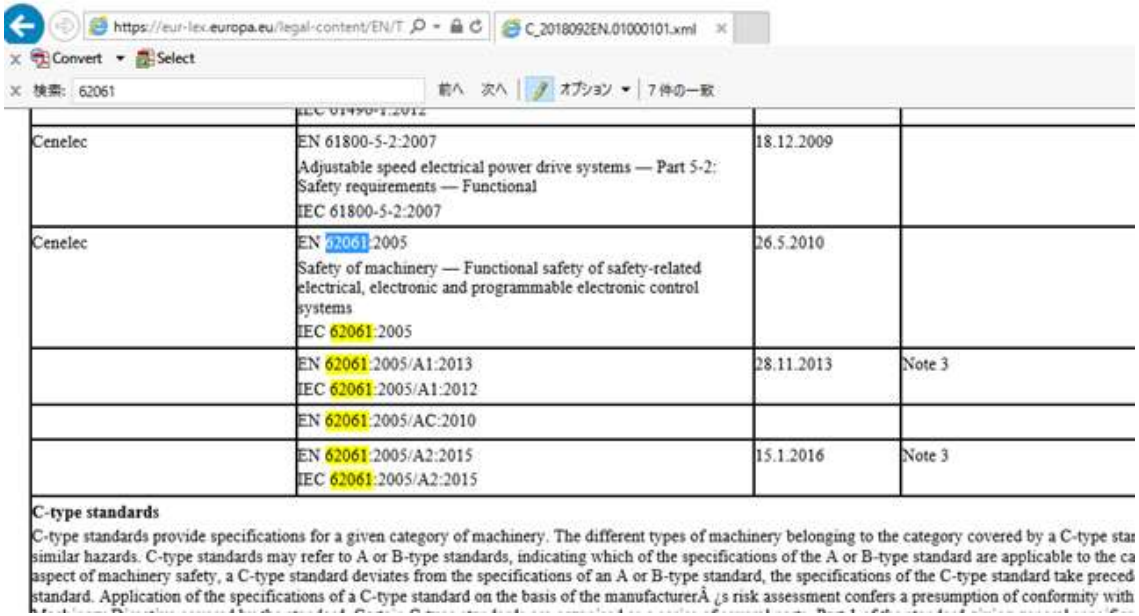
機能安全対応の法規化

- 法規化の動き

  国際機能安全規格（IEC61508）に基づく個別業界向け規格制定

  海外では法規化（欧州整合規格等）　ー＞　日本でも

  感電・火災・けが防止　ー＞　制御によるトラブル防止



Cenelec	EN 61800-5-2:2007 Adjustable speed electrical power drive systems — Part 5-2: Safety requirements — Functional IEC 61800-5-2:2007	18.12.2009	
Cenelec	EN 62061:2005 Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems IEC 62061:2005	26.5.2010	
	EN 62061:2005/A1:2013 IEC 62061:2005/A1:2012	28.11.2013	Note 3
	EN 62061:2005/AC:2010		
	EN 62061:2005/A2:2015 IEC 62061:2005/A2:2015	15.1.2016	Note 3

C-type standards

C-type standards provide specifications for a given category of machinery. The different types of machinery belonging to the category covered by a C-type sta similar hazards. C-type standards may refer to A or B-type standards, indicating which of the specifications of the A or B-type standard are applicable to the ca aspect of machinery safety, a C-type standard deviates from the specifications of an A or B-type standard, the specifications of the C-type standard take preced standard. Application of the specifications of a C-type standard on the basis of the manufacturerÂ ¿s risk assessment confers a presumption of conformity with

出典：https://eur-lex.europa.eu

機能安全対応の法規化

- 法規化の動き

  国際機能安全規格（IEC61508）に基づく個別業界向け規格制定

  海外では法規化（欧州整合規格等）　ー＞　日本でも

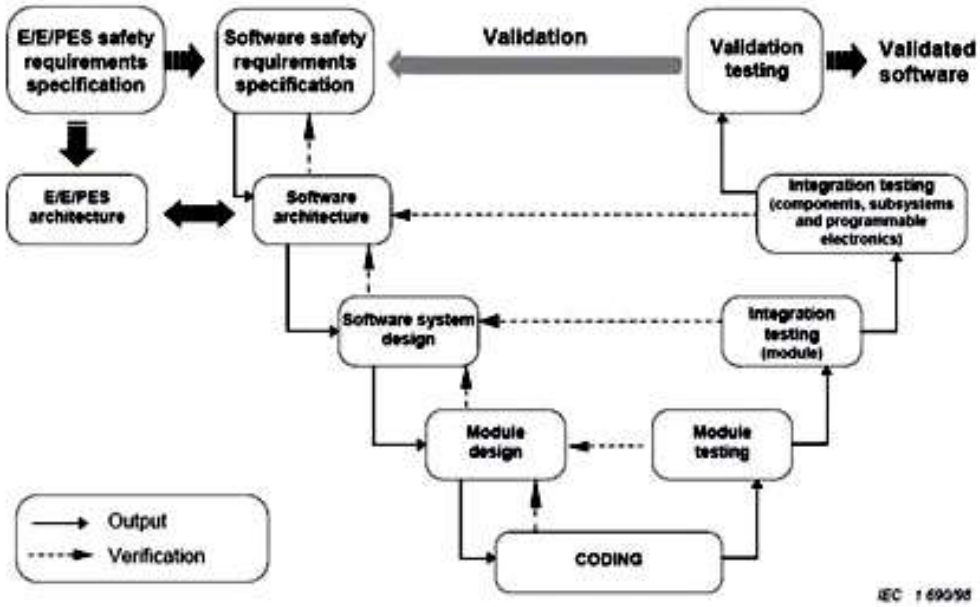
  感電・火災・けが防止　ー＞　制御によるトラブル防止

出典：https://www.mhlw.go.jp

機能安全の目的

本質的に品質管理ができている設計・開発・製造関連組織が取り組む

- ハードウエア偶発故障対応
  システム・レベル設計・分析ー＞ハードウエア（＋ソフトウエア）設計・分析
- システマティック故障対応
  システム・レベル設計・分析
  ー＞ソフトウエア安全設計・分析
  ライフサイクル全体詳細プロセス



- 最近の動向
  意図しない障害ー＞意図的な障害
  サイバーセキュリティ対応

出典:IEC規格

機能安全の目的

- ハードウエア偶発故障対応
  システム・レベル設計・分析ー＞
  ハードウエア（＋ソフトウエア）
  設計・分析

Circuit diagram:
Parts list:
Created by:
Review by:
Failure rate and distribution database: company specific (example)
Date of analysis:

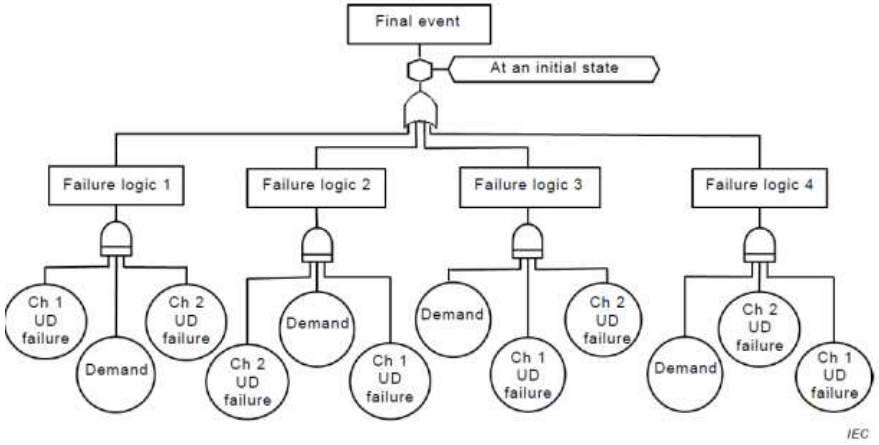
Name	Component	Function	Failure rate [FIT]	Failure mode	Failure
F50	Fuse	Short-circuit protection at the input	25	Fail to open	50 %
				Premature open	10 %
				Slow to open	40 %
D12	Suppressor diode	Over voltage protection (EMC)	7	Short	95 %
				Open circuit	5 %

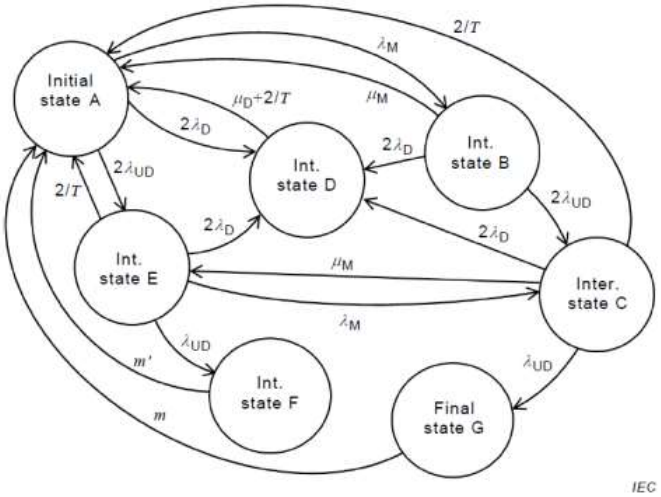
SIL	Target failure measures	
	Low demand mode of operation PFD_{avg} or risk reduction ratio φ/λ_M (SIL X)	High demand mode of/continuous operation PFH or hazardous/harmful event rate φ [1/h] (SIL Y)
4	$\geq 10^{-5}$ to $< 10^{-4}$ C (SIL 4)	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$ B (SIL 3)	$\geq 10^{-8}$ to $< 10^{-7}$ A (SIL 3)
2	$\geq 10^{-3}$ to $< 10^{-2}$ A (SIL 2)	$\geq 10^{-7}$ to $< 10^{-6}$ B (SIL 2)
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$ C (SIL 1)

出典：IEC規格

機能安全の目的

- ハードウエア偶発故障対応
  システム・レベル設計・分析ー＞ハードウエア（＋ソフトウエア）設計・分析



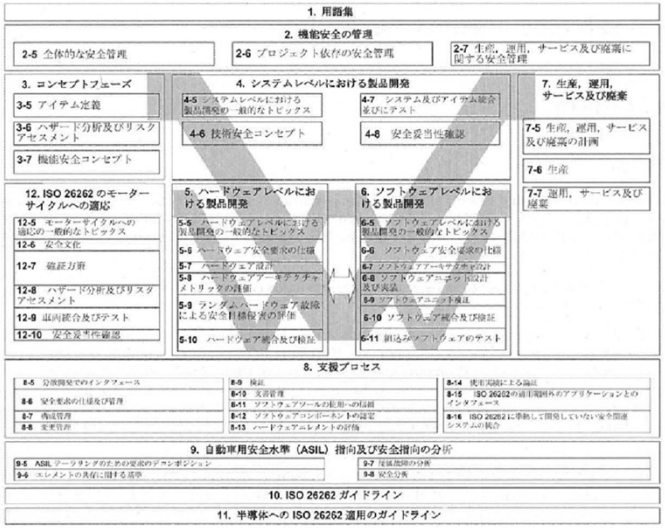


出典：IEC規格

準拠ポイント

1. 機能安全規格内容の理解
2. 品質管理規格に準拠した現状とのギャップの把握
   - 組織面　独立性　リソース力量
   - プロセス面
     受注・設計・開発・製造　内部規定
   - 技術面
     特に設計・開発　詳細技術情報管理
3. 対応戦略立案、予算確保
   組織のトップの理解
4. 実施
5. メンテナンス

専門家の支援



機能安全規格基礎規格の動向

■ IEC 61508 Ed 3.0

担当委員会 IEC TC65 SC65A MT61508

- IEC 61508

  状況:CD策定がほぼ終了。近々に関連TCに回覧。

  主な修正

  ー Part 1 Cyber Security 関連他

  ー Part 2 半導体関連、HW-SW連携、FSM関連他

  ー Part 3 HW-SW連携、Human Factor関連、Annex他

  ー Part 4 半導体関係、Tool関連、FSM関連他

  ー Part 5 System関連

  ー Part 6 解析方法修正

  ー Part 7 半導体関係

IEC 61508-1

Edition 2.0 2010-04

第 2.0 版 2010 年 4 月

IEC 61508関連

IEC TC65 SC65A MT61508関連

- IEC TS 61508-3-2 ED1

  Requirements and Guidance in the use of mathematical and logical techniques for establishing exact properties of software and its documentation

- IEC TS 61508-3-3 ED1

  Functional safety of electrical/electronic/programmable electronic safety-related systems - Part
  3-3: Requirements for object-oriented software in safety-related systems

- ISO/IEC TR 5469

  Artificial intelligence — Functional safety and AI systems

産業機械業界関連規格の動向

- IEC TS 63394 ED1

  Safety of machinery - Guidelines on functional safety of safety-related control system

- IEC 62061/AMD1 ED2

  Amendment 1 - Safety of machinery - Functional safety of safety-related control systems

- IEC TS 63074 ED1

  Safety of machinery - Security aspects related to functional safety of safety-related control systems

- ISO 13849-1

  Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design

産業機械業界関連規格の動向

- IEC TS 61496-4-2 ED2

  Safety of machinery – Electro-sensitive protective equipment – Part 4-2: Particular requirements for equipment using vision based protective devices (VBPD) – Additional requirements when using reference pattern techniques (VBPDPP)

- IEC TS 61496-4-3 ED2

  Part 4-3: Particular requirements for equipment using vision based protective devices (VBPD) – Additional requirements when using stereo vision techniques (VBPDST)

- IEC TS 61496-5 ED1

  Safety of machinery – Electro-sensitive protective equipment – Part 5: Particular requirements for radar-based protective Devices

- IEC 62046/AMD1 ED1

  Safety of machinery – Application of protective equipment to detect the presence of persons

自動車関連やその他規格の動向

- ISO26262:2018

  Road vehicles — Functional safety

- ISO21448:2022(SOTIF)

  Road vehicles — Safety of the intended functionality

- UL4600 : 2022

  Evaluation of Autonomous Products

- ISO21434 : 2021

  Road vehicles — Cybersecurity engineering

- ISO25119-1 : 2018 / Amd 1:2020

  Tractors and machinery for agriculture and forestry — Safety-related parts of control systems —

UL 4600:2020
安全規格　自律型製品の評価
Standard for Evaluation of Autonomous Products

詳細をみる

発行年月日：2020-04-01
邦訳版：有（英・日対訳版）

英語
-

邦訳
562ページ

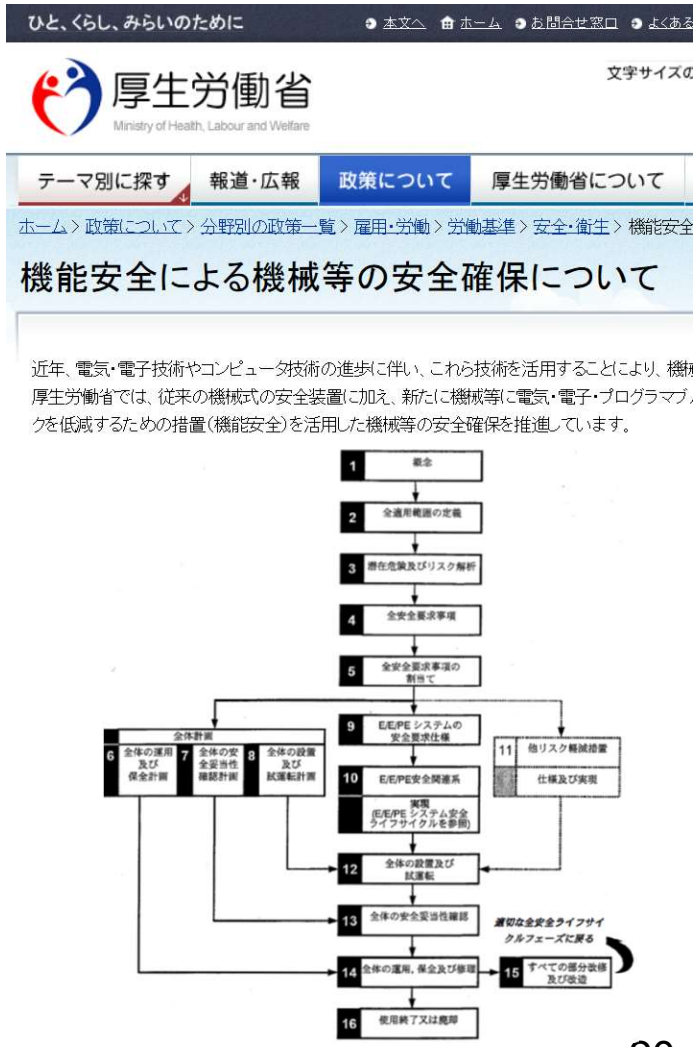
5．まとめ

対象規格の概要
　規格の背景、概要の紹介

機能安全規格基礎規格の動向
　IEC61508の動向

産業機械業界関連規格の動向
　IEC62061やISO13849関連

自動車関連やその他規格の動向
　ISO26262, SOTIF, UL4600, ISO21434



一般社団法人
組込みシステム技術協会
Japan Embedded Systems Technology Association