



JASA Webセミナー Security の国際規格の動向 in 2022

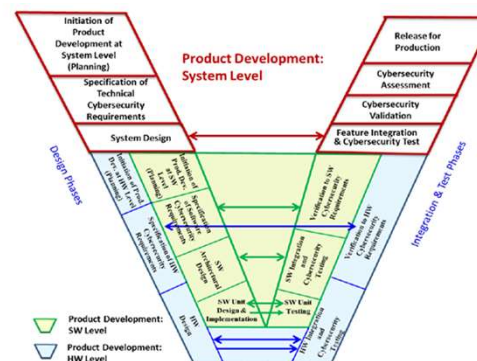
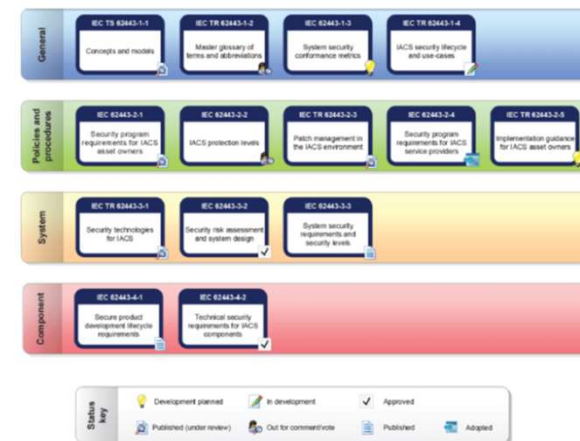
機能安全関連規格

2022年9月28日
JASA 安全性向上委員会 委員
竹市 正彦

内容



1. 講師紹介
2. 本セミナー対象規格の概要
機能安全規格とサイバーセキュリティ規格
3. サイバーセキュリティ規格の概要
IEC62443等の概要
4. IEC62443規格の動向
5. 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

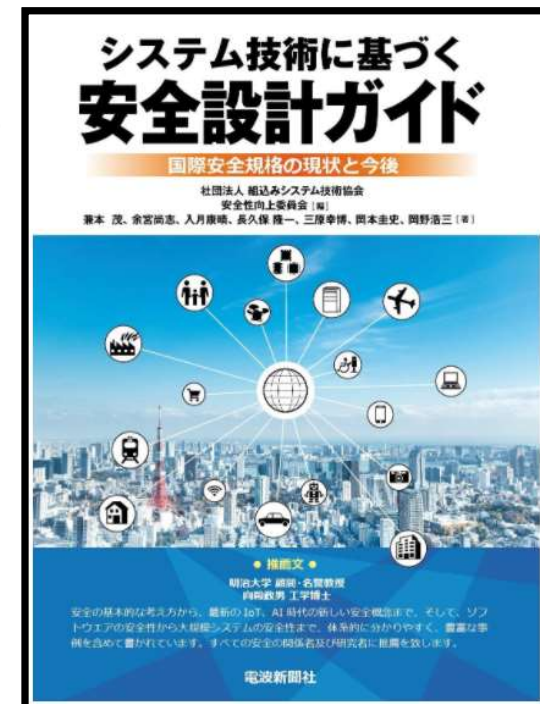
安全の概念と安全設計の基礎をしっかりと説明したうえで、如何にコンピュータで製品の安全性を確保するかという機能安全の考え方を紹介している。これからの安全技術者、組込み技術者の常識となる安全設計の基本を紹介



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）

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



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）

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. 本セミナー対象規格の概要



IEC 62443

Security for industrial automation and control systems

IEC TR 63069

Edition 1.0 2019-05

Industrial-process measurement, control and automation – Framework for functional safety and security

IEC 61508-1

Edition 2.0 2010-04

第2.0版 2010年4月

ISO/SAE FDIS 21434

Road vehicles — Cybersecurity engineering

SAE J3061

Cybersecurity Guidebook for Cyber-Physical Vehicle Systems

TECHNICAL SPECIFICATION

CLC/TS 50701

Railway applications - Cybersecurity

ISO 26262-1

Second edition
2018-12

第2版
2018年12月

機能安全規格とサイバーセキュリティ規格



1. 用語集

2. 機能安全の管理

2-5 全体的な安全管理

2-6 プロジェクト依存の安全管理

2-7 生産、運用、サービス及び廃棄に関する安全管理

3. コンセプトフェーズ

3-5 アイテム定義

3-6 ハザード分析及びリスクアセスメント

3-7 機能安全コンセプト

4. システムレベルにおける製品開発

4-5 システムレベルにおける製品開発の一般的なトピックス

4-7 システム及びアイテム統合並びにテスト

4-6 技術安全コンセプト

4-8 安全妥当性確認

7. 生産、運用、サービス及び廃棄

7-5 生産、運用、サービス及び廃棄の計画

7-6 生産

7-7 運用、サービス及び廃棄

12. ISO 26262 のモーターサイクルへの適用

12-5 モーターサイクルへの適用の一般的なトピックス

12-6 安全文化

12-7 検証方策

12-8 ハザード分析及びリスクアセスメント

12-9 車両統合及びテスト

12-10 安全妥当性確認

5. ハードウェアレベルにおける製品開発

5-5 ハードウェアレベルにおける製品開発の一般的なトピックス

5-6 ハードウェア安全要求の仕様

5-7 ハードウェア設計

5-8 ハードウェアアーキテクチャメトリックスの計画

5-9 ランダムハードウェア故障による安全目標侵害の評価

5-10 ハードウェア統合及び検証

6. ソフトウェアレベルにおける製品開発

6-5 ソフトウェアレベルにおける製品開発の一般的なトピックス

6-6 ソフトウェア安全要求の仕様

6-7 ソフトウェアアーキテクチャ設計及び実装

6-8 ソフトウェアコンポーネント設計及び実装

6-9 ソフトウェアユニット検証

6-10 ソフトウェア統合及び検証

6-11 組込みソフトウェアのテスト

8. 支援プロセス

8-5 分散開発でのインタフェース

8-9 検証

8-6 安全要求の仕様及び管理

8-10 文書管理

8-7 構成管理

8-11 ソフトウェアツールの利用への保証

8-8 変更管理

8-12 ソフトウェアコンポーネントの認定

8-13 ハードウェアエレメントの評価

8-14 使用開始による検証

8-15 ISO 26262の適用範囲外のアプリケーションとのインタフェース

8-16 ISO 26262に準拠して開発していない安全関連システムの統合

9. 自動車用安全水準 (ASIL) 指向及び安全指向の分析

9-5 ASIL テーティングのための要求のデコンポジション

9-7 信頼性の分析

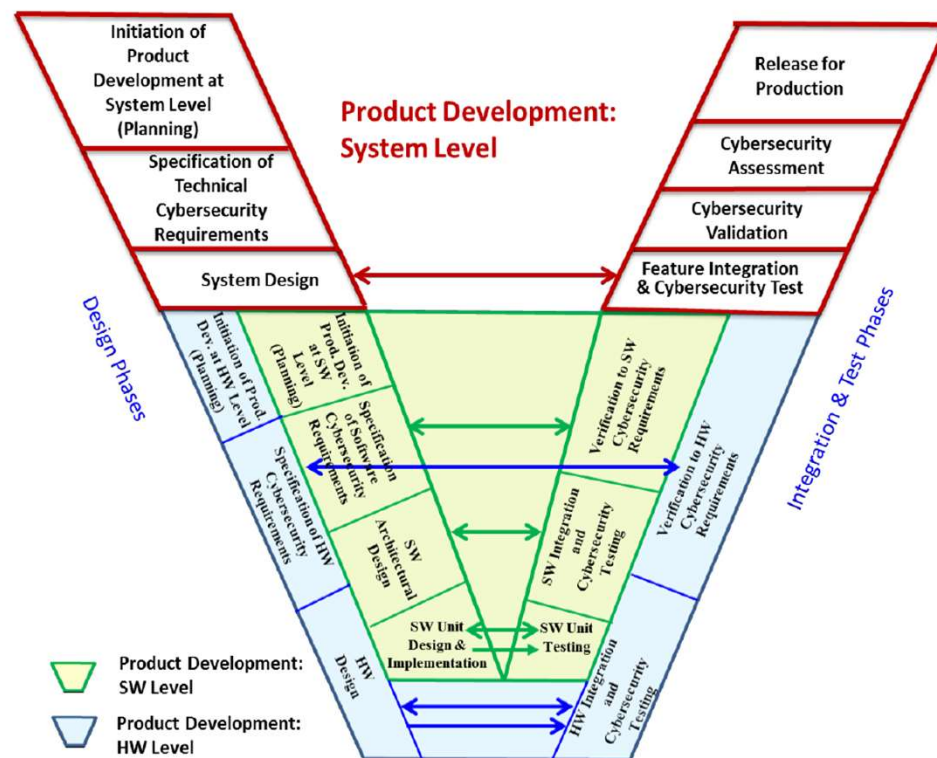
9-6 エレメントの共有に関する基盤

9-8 安全分析

10. ISO 26262 ガイドライン

11. 半導体への ISO 26262 適用のガイドライン

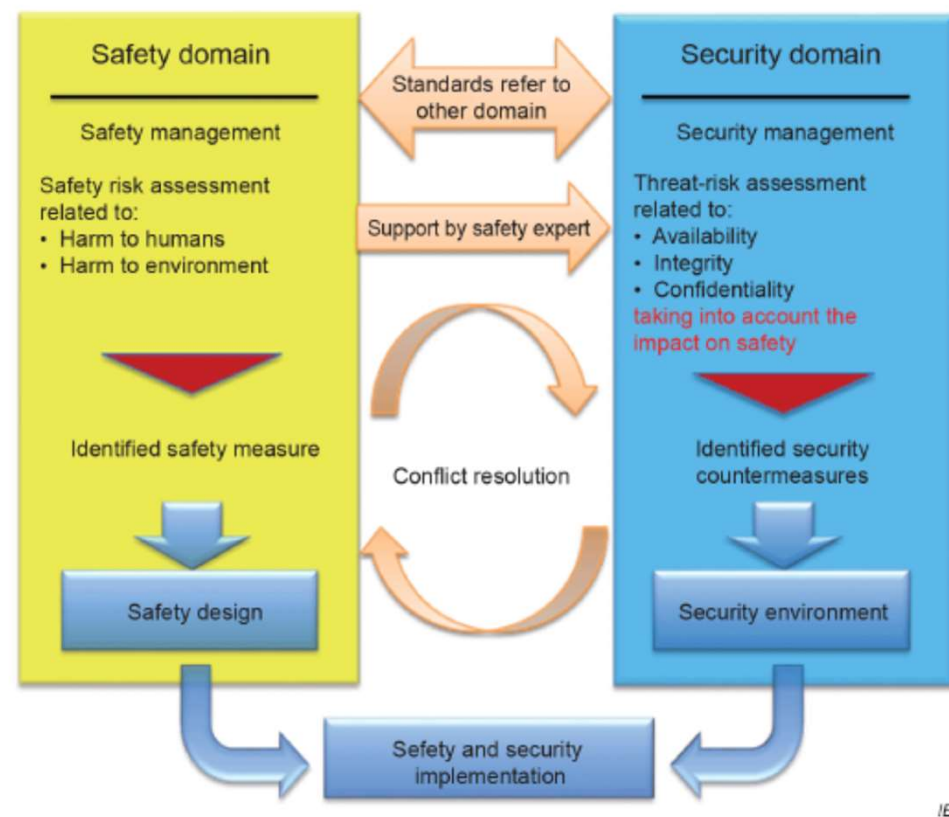
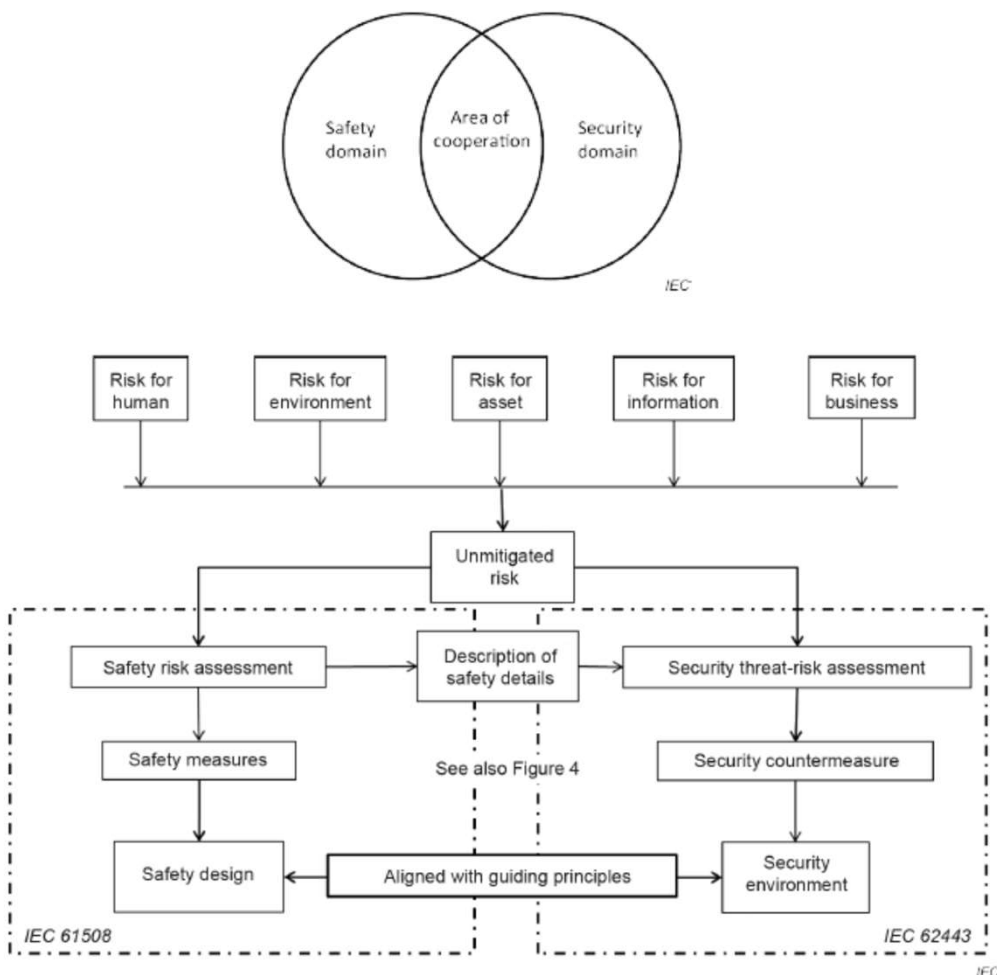
ISO26262



SAE J3061

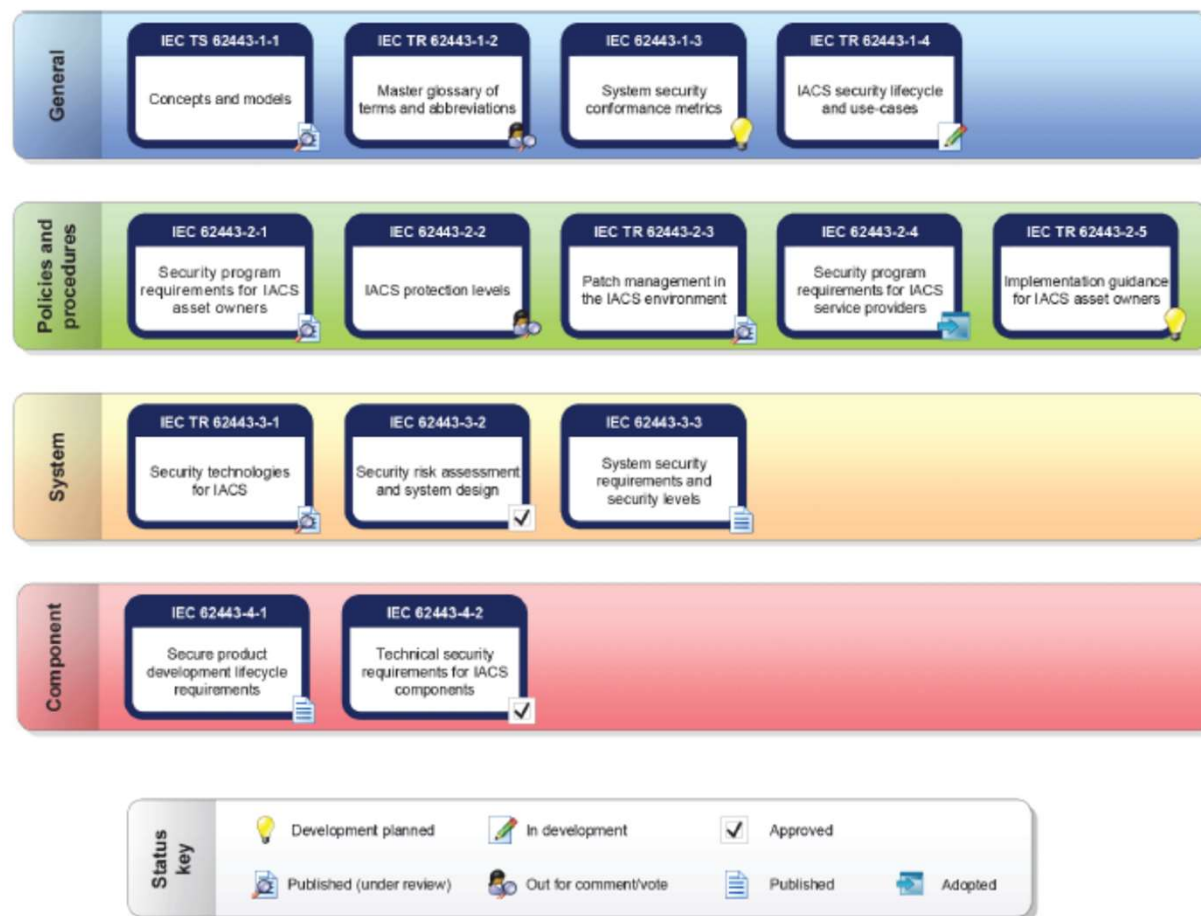
出典： ISO, SAE規格

機能安全、サイバーセキュリティ



出典: IEC TR 63069

3. IEC62443規格要件の概要



IEC

対象

Par 1: 全般

Part 2: アセットオーナー

Part 3: システムインテグレータ

Part 4: サプライヤー

規格要件の概要



Security levels

IEC 62443-4-2 [7] defines SLs in terms of four different levels (1, 2, 3 and 4), each with an increasing level of security. SL 0 is implicitly defined as no security requirements or security protection necessary.

- **SL 1:** Protection against casual or coincidental violation
- **SL 2:** Protection against intentional violation using simple means with low resources generic skills and low motivation
- **SL 3:** Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation
- **SL 4:** Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation

SR System Requirement

RE Requirement Enhancement

CR Component Requirement

FR Foundational Requirement

SAR Software Application Requirement

EDR Embedded Device Requirement

HDR Host Device Requirement

NDR Network Device Requirement

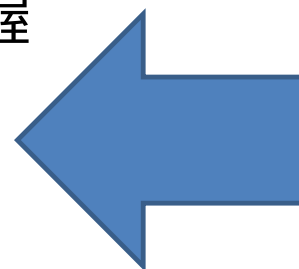
Table B.1 – Mapping of CRs and REs to FR SL levels 1-4

SRs and REs	SL 1	SL 2	SL 3	SL 4
FR 1 – Identification and authentication control (IAC)				
CR 1.1 – Human user identification and authentication	✓	✓	✓	✓
RE (1) Unique identification and authentication:		✓	✓	✓
RE (2) Multifactor authentication for all interfaces			✓	✓
CR 1.2 – Software process and device identification and authentication		✓	✓	✓
RE (1) Unique identification and authentication			✓	✓
CR 1.3 – Account management	✓	✓	✓	✓
CR 1.4 – Identifier management	✓	✓	✓	✓

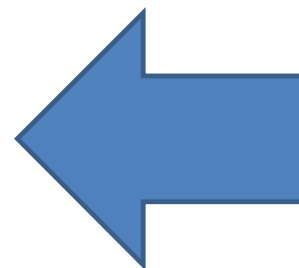
準拠ポイント



1. 機能安全・サイバーセキュリティ規格内容の理解
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



機能安全規格
準拠済みであれば有利



専門家の支援

4. IEC62443規格の動向



■ 水平規格（Horizontal Standard） 化の議論

- JAG 25, JAG26の設置
 - Questionnaire to ask about comments on the Terms of Reference (TOR) of the joint advisory group TC 65/JAG 25. This TC 65/JAG 25 is between IEC TC 65 and ISO/IEC/JTC 1/SC 27
 - Questionnaire regarding the creation of the joint advisory group TC 65/JAG 26 and to open this JAG 26 to liaison representatives as part of the assignment by the SMB of Horizontal security function for OT to TC 65.

■ 規格更新

- IEC TS 62443-1-5 ED1
Security for industrial automation and control systems – Part 1-5: Scheme for IEC 62443 cyber security profiles



■ 規格の更新

- IEC 62443-2-1 ED2
Security for industrial automation and control systems - Part 2-1: Security program requirements for IACS asset owners
- IEC 62443-2-2 ED1
Security for industrial automation and control systems – Part 2-2: IACS Security Protection
- IEC 62443-2-4 ED2
Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers
- IEC TS 62443-6-1 ED1
Security evaluation methodology for IEC 62443 – Part 2-4: Security program requirements for IACS service providers
- IEC TS 62443-6-2 ED1
Security evaluation methodology for IEC 62443 - Part 4-2: Technical security requirements for IACS components

規格の動向



■ IEC TC9 AHG20

Electrical equipment and systems for railways

Study ACSEC Guide 120 in view of implications on the work of TC 9

■ IEC TC9 PT63425

Railway applications - Cybersecurity

NIS Directive



CLC/TS 50701:2021
Railway application - Cybersecurity



Security
CLC/TS 50701 > IEC
IEC 62443 horizontal standard?

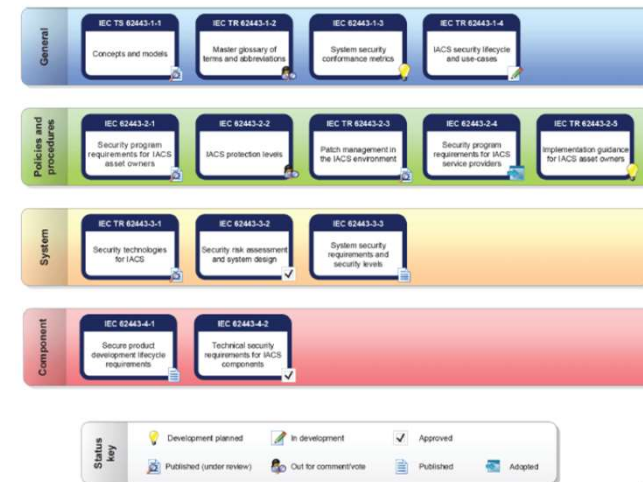
vs.

Safety (Functional Safety)
EN 5012x – IEC 62278

5. まとめ



- 本セミナー対象規格の概要
機能安全規格とサイバーセキュリティ規格
- サイバーセキュリティ規格の概要
IEC62443等の概要
- IEC62443規格の動向



IEC