新たなセンサシステム規格の開発状況（IEC 62998）

2017年3月9日

国立研究開発法人 産業技術総合研究所
ロボットイノベーション研究センター
角 保志

IEC 62998 とは

SAFETY OF MACHINERY –
Safety-related sensors used for protection of person

- 安全センサのための新しいジェネリックな規格
  - 人や危険物体を検出し、機械を安全な状態にすることで、人を保護
  - 公共の場所での使用も視野
- IEC/TC44/WG14で、技術仕様書（TS）として開発中

本日の内容

- IEC 62998 の概要
- 安全関連センサ（SRS）と
  安全関連センサシステム（SRSS）
- SRS/SRSS の設計・開発
- SRS/SRSS のユーザインタフェース
- SRS/SRSS のインテグレーションと実装
- SRS/SRSS の運転、メンテナンス、改修
  検証と妥当性確認
  使用上の情報

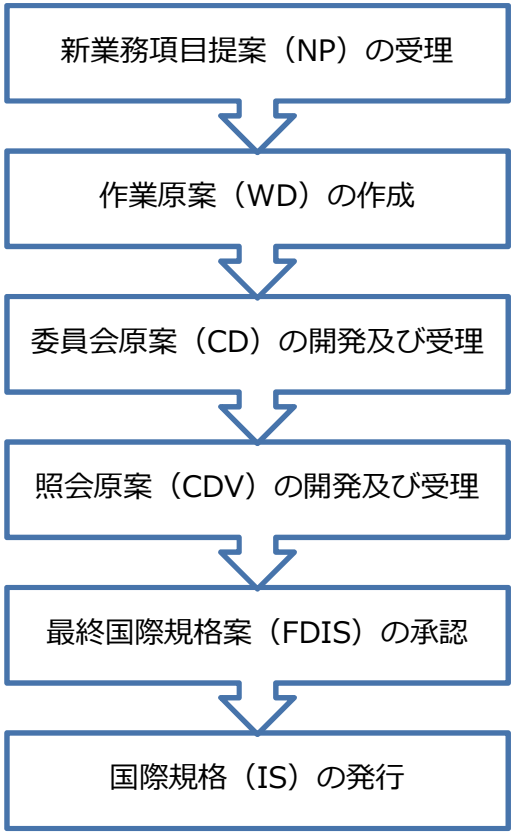
IEC CD 62998

IEC 62998 の概要

IEC 62998の開発状況

2014/12　ドイツから提案 (NP)
2015/10　作業原案 (WD)
　　TC44/WG14 第1回会議 (Düsseldorf)
2016/1　　TC44/WG14 第2回会議 (London)
　　/4　　TC44/WG14 第3回会議 (Milano)
　　/9　　TC44/WG14 第4回会議 (京都)
　　/12　TC44/WG14 第5回会議 (Waldkirch)
2017/1　委員会原案（CD）

　　/5　　TC44/WG14 第6回会議 (Sankt Augustin)
　　/6　　TC44/WG14 第7回会議 (Helsinki)
　　/6　照会原案（CDV）
2018/1　　TC44/WG14 第8回会議 (場所未定)
　　/4　最終案
　　/10　技術仕様書（TS）として発行



国際規格開発の手順 （通常の場合）

IEC CD 62998 のスコープ

- 安全関連センサ（SRS）およびセンサシステム（SRSS）の、開発とインテグレーションに関する要求事項を規定
- 既存のセンサ規格では対応しきれない（もしくは、該当するセンサ規格が無い）場合に適用
- SRS/SRSSパフォーマンスクラスを定義
  - PL, SILcl, SIL等に対応
- 屋内・屋外の環境
  - 公共の場所での人の保護。例： 農業、駅

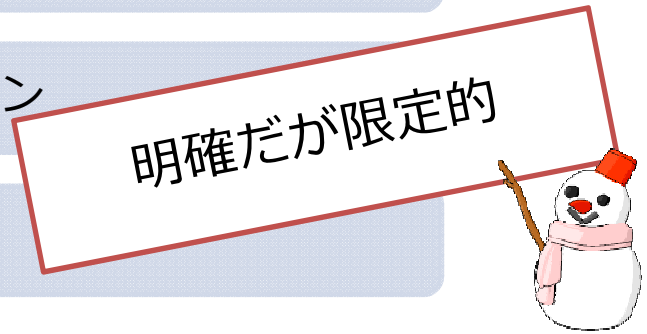
既存センサ規格の例
- IEC 61496シリーズ（安全ライトカーテン等）
- IEC 60947-5-2（近接スイッチ）

IEC 61496シリーズ とは

- 電気的検知保護設備の技術的な要求事項を規定
- 屋内（工場）での使用を想定

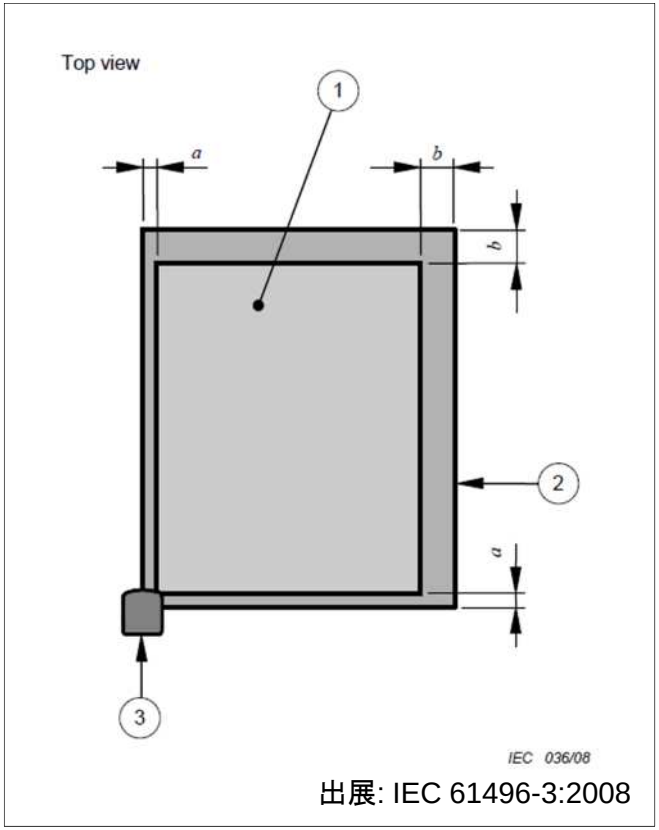
電気的検知保護装置（ESPE, Electro-Sensitive Protective Equipment）：
機械の危険な部分の周辺に設定した進入禁止区域に人が進入したら、これを検出して機械に停止信号を生成する保護装置

IEC 61496-1	• 一般
IEC 61496-2	• 安全ライトカーテン
IEC 61496-3	• 安全レーザースキャナ
IEC/TS 61496-4-2	• カメラ＋背景パターン
IEC/TS 61496-4-3	• ステレオビジョン



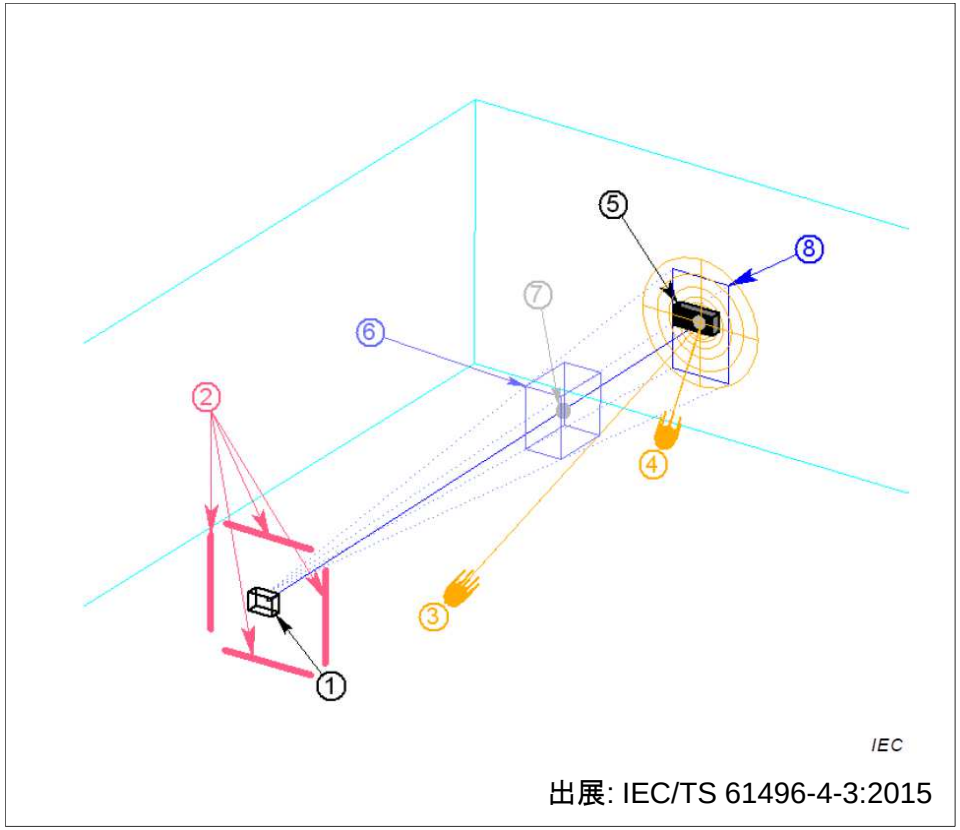
IEC 61496の要求事項の例

IEC 61496-3（レーザースキャナ）の検出区域



出展: IEC 61496-3:2008

IEC/TS 61496-4-3（ステレオビジョン）の光干渉試験設定

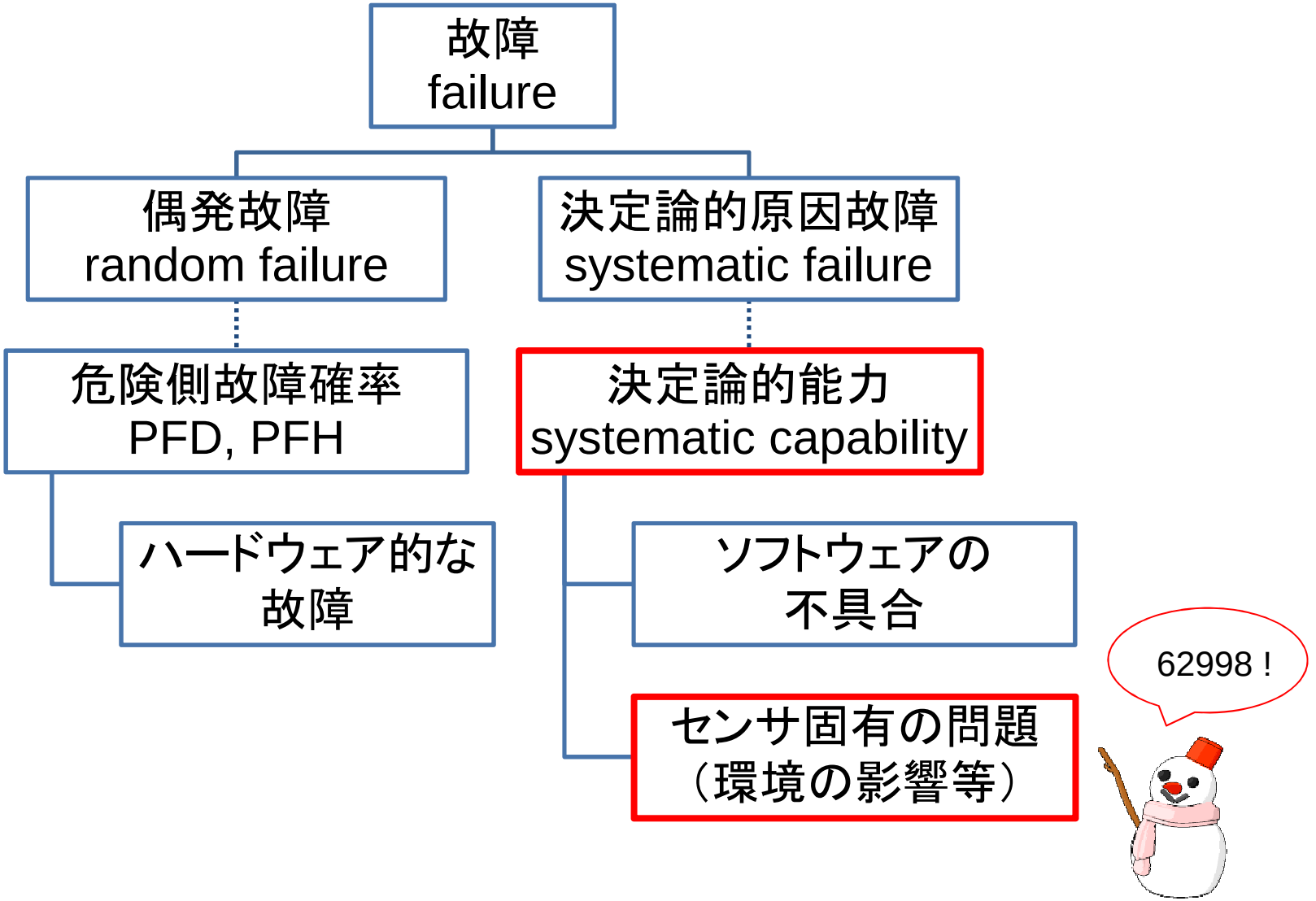


出展: IEC/TS 61496-4-3:2015

IEC CD 62998 のイントロダクション

- 読者: SRS/SRSSのサプライヤ
  - SRS/SRSSの製造者
  - SRSSのインテグレータ
- 技術：
  - 新しいセンサ技術（レーダー、超音波）
  - 新しいセンサ機能（物体認識、物体位置計測）
  - センサの組み合わせ（フュージョン）
- 内容：
  - 既存の機能安全規格とセンサ規格のギャップの解消
  - SRS/SRSS の決定論的能力 (systematic capability)

安全関連センサと Systematic Capability



IEC CD 62998の引用規格

- IEC 60068 (all parts), Environmental testing
- IEC 60721 (all parts), Classification of environmental conditions
- IEC 61508 (all parts), Functional safety of electrical/electronic/programmable electronic safety-related systems
- IEC 62061, Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems
- ISO 13849 (all parts), Safety of machinery – Safety-related parts of control systems
- ISO/IEC 17025, Conformity assessment - General requirements for the competence of testing and calibration laboratories

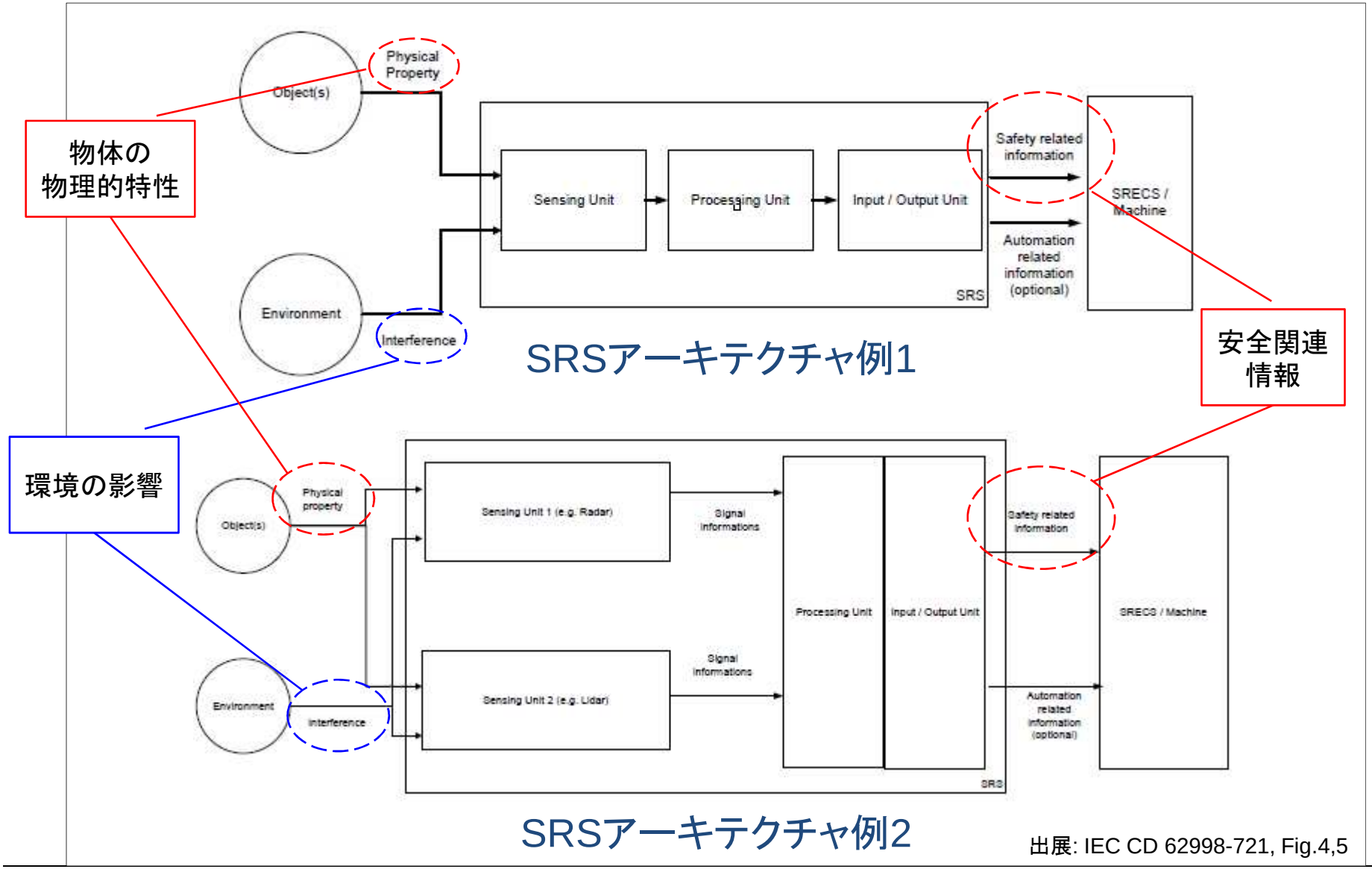
IEC CD 62998の構成

IEC CD 62998

安全関連センサ（SRS）と安全関連センサシステム（SRSS）

安全関連センサのアーキテクチャ

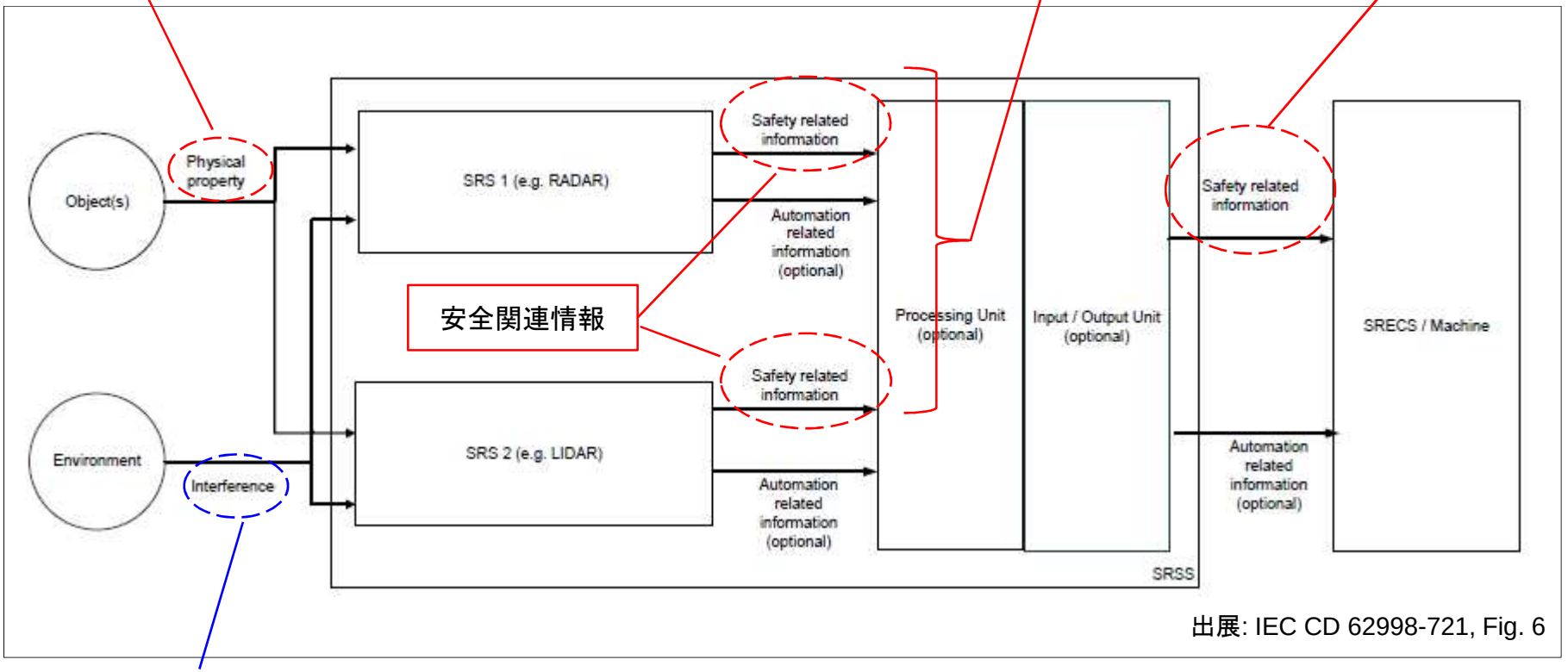
SRS: Safety Related Sensor



出展: IEC CD 62998-721, Fig.4,5

安全関連センサシステムのアーキテクチャ

SRSS: Safety Related Sensor System



SRSSアーキテクチャ例

SRS/SRSSパフォーマンスクラス

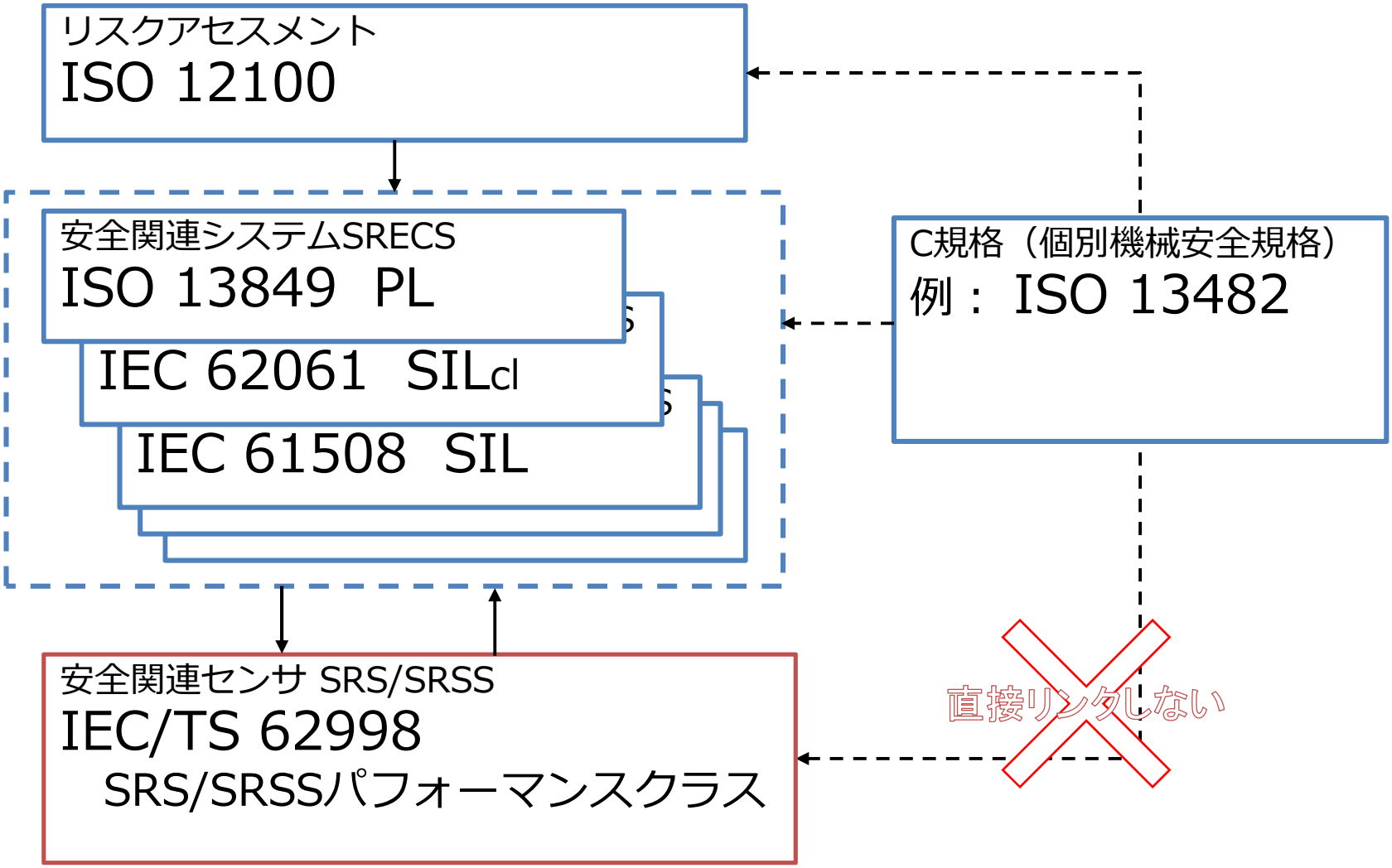
- リスク分析で特定
- 安全性能レベル（PL, SIL_{cl}, SIL等）に対応
  - IEC 61496の「Type」とはリンクしない
- サプライヤが「使用上の情報」に記載

  記載例：Sensor Subsystem SIL 2 in accordance to IEC 62061. SRS performance class D in accordance to IEC 62998 used for examination of systematic capabilities.

表1: 安全性能レベルとSRS/SRSSパフォーマンスクラスの対応

SRS/SRSS パフォーマンスクラス	A	B	C	D	E	F
ISO 13849	PL_a	PL_b	PL_c	PL_d	PL_e	
IEC 62061			SIL_{cl} 1	SIL_{cl} 2	SIL_{cl} 3	
IEC 61508			SIL1	SIL2	SIL3	SIL4
… …						

IEC/TS 62998の位置づけ

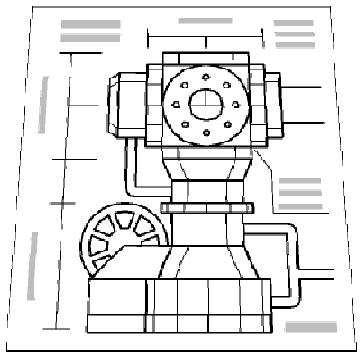


IEC CD 62998

SRS/SRSSの設計・開発

SRS/SRSS設計・開発の要求事項

最低限以下をカバーして設計・開発



- 意図した使用を決定
- SRS/SRSS機能を定義
- 安全要求の文書化
- ハード・ソフトの安全関連設計
- 設計分析・シミュレーション
  - 検出区域
  - 検出能力（detection capability）と
    ディペンダビリティ (dependability)

「SRS/SRSS機能」の要求事項

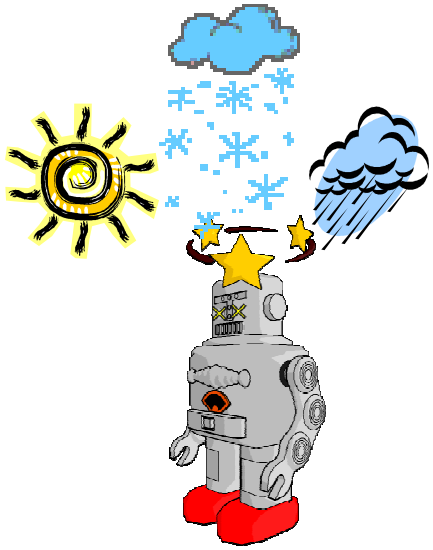
サプライヤが定義

- 何を検出するのか
  - 対象となる「物体」と、その物理特性
- どこで使用するのか
  - アプリケーションの環境条件と使用上の制限
- 何を出力するのか
  - 適切な出力信号
- 機能の分類
  - 安全関連機能
  - 危険物体（検出）機能
  - 人検出機能
  - オートメーション関連機能

SRS/SRSSの検出能力の要求事項

以下を考慮して分析＆試験

- 物体のクラスと物理特性
  - 安全関連物体：人
    - 子ども含む
  - 安全関連物体：潜在的な危険物体
  - オートメーション物体
    - 検知漏れが危険側故障にならない物体
- 使用上の制限
- SRS/SRSSパフォーマンスクラス
- 環境の影響



「環境の影響」についての要求事項

サプライヤが規定

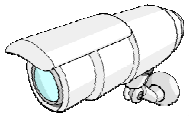
- 環境条件とその範囲（制限）を規定
  - 危険側故障の条件
  - 正常運転の条件
- 既存の環境条件に関する規格を参照
  - 例：ISO 15003（農業）、EN 50125-1（鉄道）、IEC 60721-3-5（環境条件分類：車載）
- 考慮する環境条件：

a. 屋内か屋外か
b. 静止か移動か
c. 温度、湿度
d. 降水（雨、あられ・雹、雪）と風
e. 圧力（大気圧、水圧など）
f. 太陽放射と温度放射
g. 結露と着氷
h. 霧、塵、砂、煙霧
i. 震動と衝撃
j. 動物相と植物相（カビなど）
k. 化学的影響
l. 電気電磁気的影響
m. 機械的負荷
n. 音

環境の影響の適用例（附属書F.2）

SRS/SRSSのアプリケーション

- 静止カメラ
- 工場の入口をモニタ
- 屋外、保護あり



分析

環境の影響

- 温度と湿度
- 霧
- 結露と着氷
- 太陽放射（間接）
- ほこりと砂
- 振動と衝撃
- 電気電磁的影響

関連規格

- IEC 60721-3-0（環境条件：通則）
- IEC 60721-3-3（環境条件：屋内固定）

適用結果（表.F2 環境の影響と分類の例）

環境の影響	IEC 60721-3-3によるクラス	制限
温度	3K6	-25~+55℃
温度変化率	3K6	0.5 K/min
相対湿度	3K6	100%
結露	3K6	Possible
太陽放射		700 W/m^2
振動	3M1	振幅0.3 mm 加速度1mm/s^2
衝撃	3M1	40 m/s^2

IEC 60721-3-3
3K6： ビルの入口、ガレージ、家畜小屋、丸太小屋、屋根裏、電話ボックス、工場及び製造プラント用の建屋、無人装置の設置場所、電気通信用の無人の建屋、耐凍結性の製品を対象とした通常の倉庫、農場の建屋など
3M1： 振動および衝撃の少ない場所

環境の影響による危険側故障

サプライヤが分析（表3の上限を超えないこと）

- 環境の影響と検出能力の関係を分析
  - シミュレーション
  - 試験
- 検出能力を喪失させる環境条件の限界を決定

表3：環境の影響による検出能力の喪失の上限
（高頻度作動要求モード）

SRS/SRSS パフォーマンスクラス	1年あたり危険側故障 最大累積時間
A	1 h
B	5 min
C	1 min
D	5 sec
E	0.5 sec
F	反応時間

IEC CD 62998

SRS/SRSSの
ユーザインタフェース

SRS/SRSSの
ユーザインタフェースの要求事項

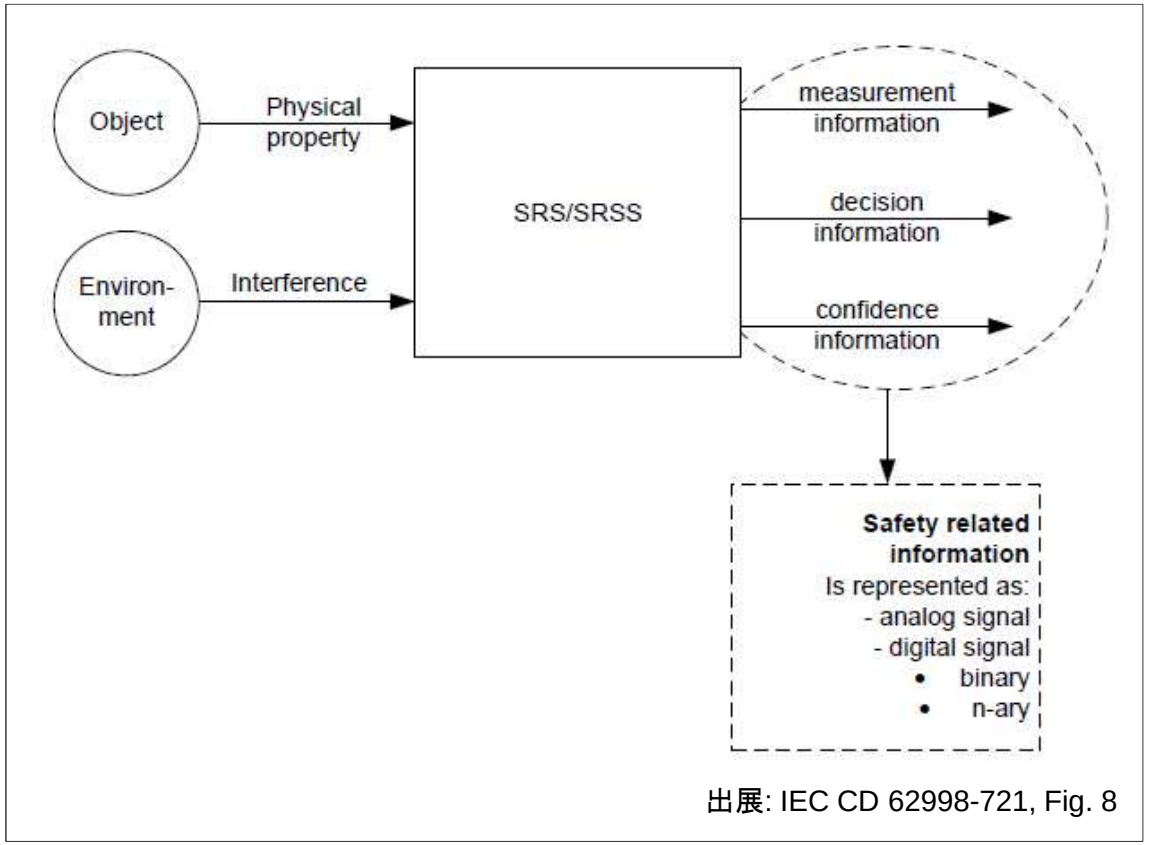
サプライヤが規定

- 取り付け方 mounting
- 出力（安全関連情報）
- ライフサイクルを通じての
  リスク低減方策
  - 例：メンテナンス試験

SRS/SRSSの安全関連情報の要求事項

サプライヤが定義

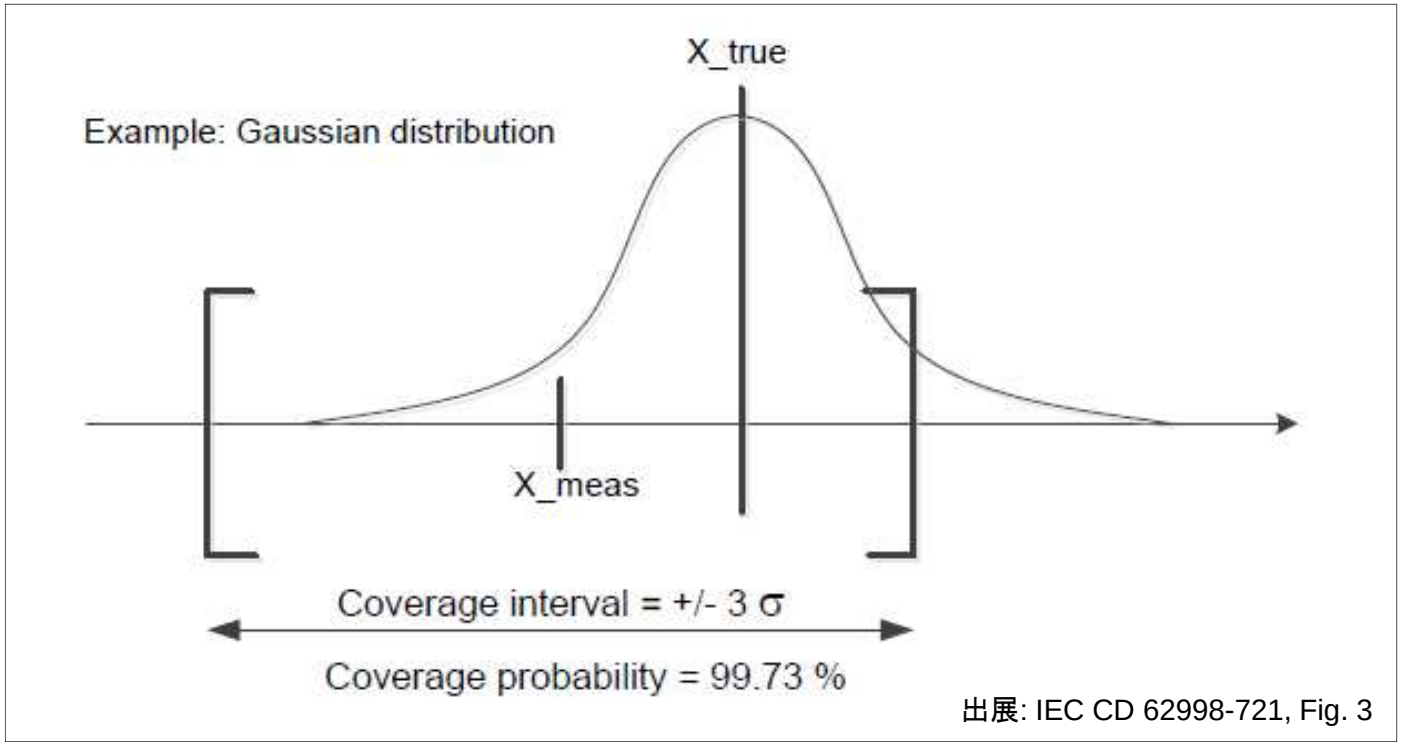
- 計測情報
  - 計測値
- 判定情報
  - 存在判定
- 信頼性情報
  - 計測の不確かさ
  - 判定の不確かさ



出展: IEC CD 62998-721, Fig. 8

信頼性情報について

- 安全関連情報の「不確かさ」を表現
  - 包含確率 coverage probability
  - 包含区間 coverage interval



出展: IEC CD 62998-721, Fig. 3

参考文献
- 「計測における不確かさの表現のガイド」 (Guide to the Expression of Uncertainty in Measurement; GUM)
- 「不確かさの入門ガイド」, NITE, http://www.nite.go.jp/data/000050641.pdf
- 「不確かさ評価入門」, AIST, https://unit.aist.go.jp/mcml/rg-mi/uncertainty/docs2/IntroductionToUncertainty.pdf

SRS/SRSSの信頼性情報

- 信頼性情報の最小値（SRS/SRSSパフォーマンスクラス別）

Table 4 – Minimum required coverage probability/ decision probability at high demand rate

SRS/SRSS performance class	A	B	C	D	E	F
assumed high demand rate	1/24h	1/h	1/h	4/h	4/h	4/h
Coverage probability if measurement information is provided	>1-2,4 * 10^{-3}	>1-1 * 10^{-5}	>1-3 * 10^{-6}	>1-2,5* 10^{-7}	>1-2,5* 10^{-8}	>1-2,5* 10^{-9}
Decision probability if decision information is provided	>1-2,4 * 10^{-3}	>1-1 * 10^{-5}	>1-3 * 10^{-6}	>1-2,5* 10^{-7}	>1-2,5* 10^{-8}	>1-2,5* 10^{-9}

$$\text{coverage probability or decision probability} > 1 - \frac{\text{(upper limit PFH corresponding to SRS/SRSS class)} \cdot}{\text{application specific demand rate per h}}.$$

Formula 1 – Calculation of coverage probability and/or decision probability for application specific demand rate

出展: IEC CD 62998-721

IEC CD 62998

SRS/SRSSの
インテグレーションと実装

SRS/SRSSの
インテグレーションと実装の要求事項

製造者が定義、サプライヤが情報提供

- SRS/SRSSの、SRECSへのインテグレーション
- 複数SRSをインテグレーションしてSRSSを構築 ＝ フュージョン
- SRS/SRSSの実装
- SRS/SRSSのキャリブレーション

（それぞれ、該当する場合）

フュージョンの例（附属書I）

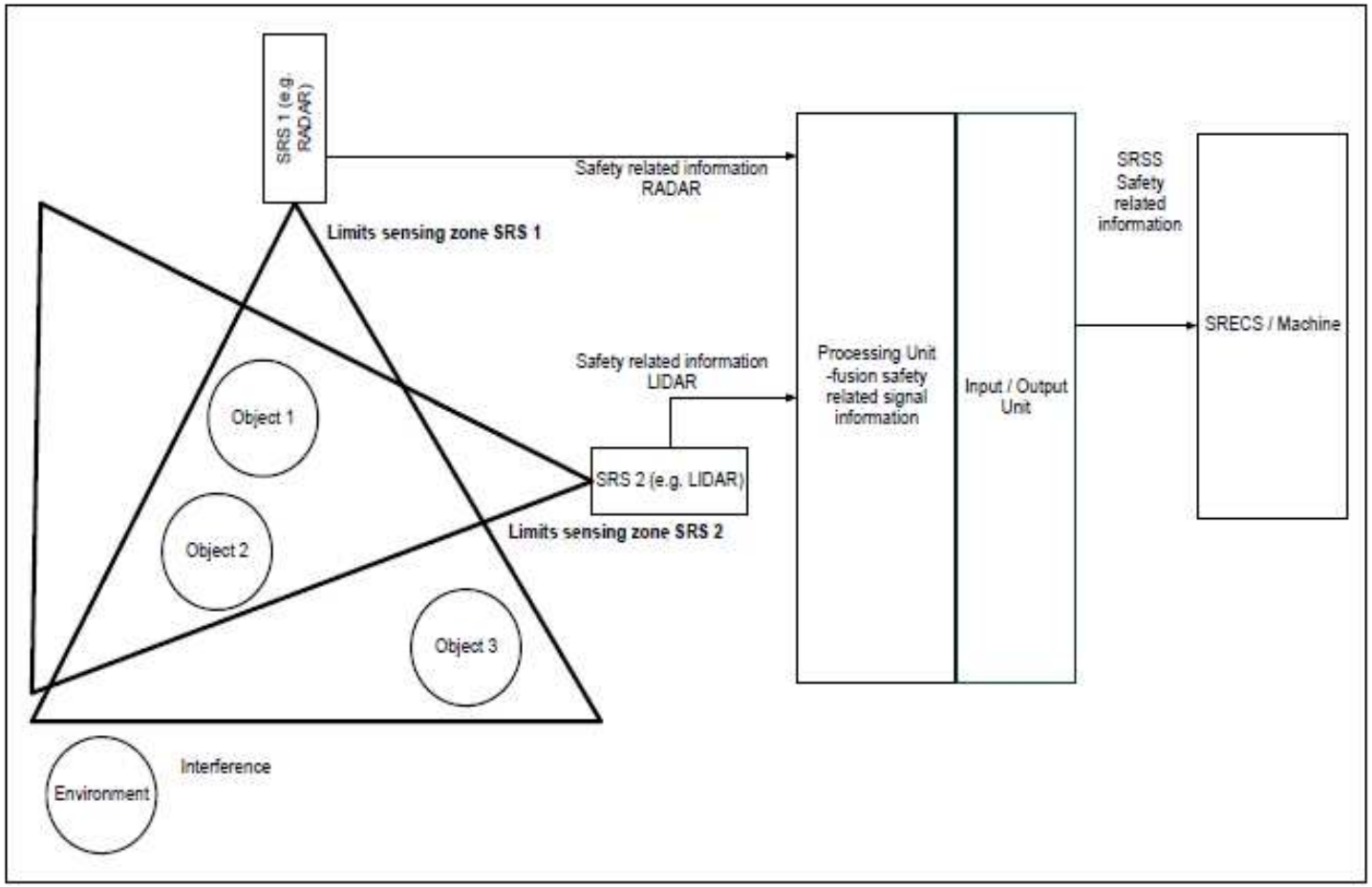


Figure I.3 – Example fusion of 2 SRS into an SRSS with combined sensing zones

出展: IEC CD 62998-721

フュージョンに関する要求事項

SRSSインテグレータが規定

- SRSSの意図した利用の決定
- SRS機能を考慮したSRSS機能の定義
- 安全要求の文書化
- 安全関連ハード・ソフトの設計要求
  - SRSSのパフォーマンスクラスが、もとのSRSのパフォーマンスクラスより向上している場合
- SRSSの使用上の制限の定義
  - もとのSRSが、使用上の制限内で使われていることを確認
  - SRSSの使用上の制限が、もとのSRSより向上していることを確認
  - ユーザへの情報提供

フュージョン後の使用上の制限に関する要求事項

SRSSインテグレータが定義

- 検出能力
- 検出区域
- 環境の影響
- 出力（安全関連情報）
- SRS/SRSSパフォーマンスクラス
- 反応時間

フュージョン後の最大SRSSパフォーマンスクラス

表5

SRS 2 パフォーマンスクラス ＼ SRS 1 パフォーマンスクラス	A	B	C	D	E	F
A	B	B	C	D	E	F
B	B	C	C	D	E	F
C	C	C	D	D	E	F
C	D	D	D	E	E	F
E	E	E	E	E	F	F
F	F	F	F	F	F	F

- 3個以上のフュージョンも可能
- 表5によるフュージョンは1回のみ
- フュージョン後のクラスは要検証

IEC CD 62998

SRS/SRSSの

- 運転、メンテナンス、改修
- 検証と妥当性確認
- 使用上の情報

SRS/SRSSの運転、メンテナンス、改修の要求事項

製造者が定義、サプライヤが情報提供

- 運転（operation）
- メンテナンス（maintenance）
- 改修（modification）

を通じて、安全関連機能を実現

SRS/SRSSの検証と妥当性確認

製造者が定義、サプライヤが情報提供

- SRS/SRSSの決定論的能力を保証
- 検証と妥当性確認（分析、試験）

SRS/SRSSの使用上の情報

実装、使用、メンテのための適切な情報を提供

提供すべき使用上の情報の概要（数字はIEC CD 62998の節番号）

4.2	The supplier shall state the Level of safety performance (PI, SIL or SIL CL) and the referenced standard in customer documentation.
5.2	The SRSS function shall be defined by the supplier in accordance to general description of Table 3.
5.6	Specification of safety related zones.
5.7	Specification of automation zones if applicable.
5.8.2.1	The supplier shall define limits of the physical properties within which the SRS/SRSS function is performed.
5.8.2.1 **5.8.2.4**	The supplier shall specify the physical properties used for person detection and the limits within which the person detection function is performed.
5.8.2.1 **5.8.2.3**	The supplier shall specify the property of length, area and volume used for person detection and the limits within which the person detection function is performed.
5.8.2.1 **5.8.2.4**	The supplier shall specify the property of reflection used for person detection and the limits within which the person detection function is performed.
5.8.2.1 **5.8.2.5**	The supplier shall specify the property of velocity assumed for person detection and the limits within which the person detection function is performed.
5.8.2.6	The supplier shall specify the physical properties used for hazardous object detection and limits of the physical properties within which the hazardous object function is performed.
5.8.2.7	The supplier shall specify objects used to perform automation functions.
5.8.3.1	The supplier shall specify the environmental influences relevant for the dependability of the detection capability of the SRSS.
5.8.3.2	The supplier shall specify for all relevant environmental influences the limits for failure to danger condition.
5.8.3.2	The supplier shall specify for all relevant environmental influences the limits for normal operation condition.
5.8.3.3	The supplier shall provide relevant information to the user on the results of analysis of the influence of relevant environmental conditions on the loss of detection capability and consequences if the limits are not achieved in the application.
5.8.3.3	The supplier shall provide additional information for use if one of the additional approaches of Annex G are used.
5.9.2	The supplier shall provide information on restriction in mounting position of a sensing unit/SRS/SRSS.
5.9.2	The supplier shall provide information location of detection zone(s) relative to mounting surfaces or reference point at the sensing units/SRS/SRSS.
5.9.2	The supplier shall provide information on location and limitations in mounting of sensing unit/SRS/SRSS.
5.9.2	The supplier shall provide information on the detection capability in an SRS/SRSS as a result of mounting.

5.9.2	The supplier shall provide information on the location and geometry of SRS/SRSS detection zone(s).
5.9.2	The supplier shall provide information on measures to prevent or monitor changes in mounting resulting in failure to danger.
5.9.3.1	The supplier of the SRS/SRSS shall define the safety related information provided by the output unit.
5.9.3.1	The fault reaction function and the fault response time of the fault reaction function shall be specified and provided within the information for use for SRS/SRSS performance class C to F.
5.9.3.2	The supplier shall specify the measurement information if applicable.
5.9.3.2	The supplier shall specify the decision information if applicable.
5.9.3.2	The supplier shall specify confidence information for the safety related information.
5.9.3.3	The supplier shall specify the response time.
6.1	The supplier shall give information for integration and installation within the information for use.
6.2.1	The SRSS Integrator shall provide information for use of the SRSS and each fused SRS.
6.2.2	The SRSS Integrator shall define the limits of use of the SRSS.
6.2.2	The SRSS integrator shall define and document if the fusion of two or more SRS into an SRSS results in an improvement, in a reduction or in equal characteristic as defined for each SRS by the manufacturer.
6.2.3	The SRSS integrator shall specify the SRSS detection capability resulting after fusion.
6.2.4	The SRSS integrator shall specify the sensing zone(s) resulting after fusion.
6.2.5	The SRSS integrator shall specify environmental conditions in type and limits resulting after fusion for no failure to danger.
6.2.5	The SRSS integrator shall specify environmental conditions in type and limits resulting after fusion for normal operation condition.
6.2.6	The SRSS integrator shall specify logic functions performed in a processing unit on SRSS level and shall specify the safety related information provided by the SRSS.
6.2.7	The SRSS integrator shall specify the sensor performance resulting after fusion.
6.2.8	The SRSS integrator shall specify the response time resulting after fusion.
6.3.1	The supplier of an SRS/SRSS shall define whether a calibration procedure is or is not required in the application to achieve the stated detection capability.
6.3.2	The supplier shall describe the procedure of calibration by the user.
6.3.3	The supplier shall provide information on how the results of calibration procedure shall be documented at user side.
7	The supplier of an SRS/SRSS shall give appropriate information for operation, maintenance and installation.
8.5.1	The supplier shall describe test and test set up for verification respective validation to be performed at user side within information of use.

まとめ

- IEC 62998は、
  - 多方面に影響する可能性.
  - 引き続き動向を注視していく必要あり.

- 今後の予定

2017/6	照会原案（CDV）
2018/4	最終案（FDIS）
/10	技術仕様書（TS）

ご注意

本資料は、

- IEC CD 62998（2017年1月）をもとに作成しました。
- 2018年発行予定の IEC TS 62998 とは、内容が一致しない可能性があります。

ご静聴ありがとうございました