自動車業界の未来を支える！
最新サイバーセキュリティと機能安全
サステナビリティ セミナー

When you need
to be sure

自動運転及びAIから見える !!
半導体の機能安全開発

C&P Connectivity
SGS Japan Inc.

23/05/2025

SGS

Speaker

松尾　健彦　AFSE SC-AFSE CACSE IFSE

Function Safety C&P Connectivity

SGS Japan Inc.

takehiko.matsuo@sgs.com

2024 - **Semiconductor Steering Committee Director SGS Japan**

2020 - **Functional safety technical team leader for Semiconductor SGS Japan**

2016 - **Functional Safety Project Engineer at SGS Japan**

Support about **50 semiconductor** manufacturers and **more than 100 semiconductor projects.**

Experience in supporting MCU, SoC, and SBC such as AD/ADAS including Lidar, Millimeter waves and Camera. Also support projects related to industrial chips complying with IEC 61508.

2011 - 2016 **Functional Safety manager and expert for ISO26262 at Semiconductor supplier**

Experienced in functional safety development in semiconductors including SEooC, and has a wide range of know-how such as IC, IP level requirements and safety mechanism derivation, FMEA, FMEDA, DFA implementation, failure injection, etc.

2008 - 2016 **Development at Semiconductor supplier**

Semiconductor engineer and developed Mixed-signal IC for vehicles

Product development for applications requiring functional safety such as electric power steering, braking system, autonomous driving system and so on.

Agenda

- 自動運転およびAI時代を見据えた半導体機能安全 最新動向
  - 技術トレンドとビジネスモデルの変化
  - AIを含むISO26262 3rd Edition動向
- 自動運転およびAIを踏まえた半導体における機能安全開発のポイント
  - 現実的な安全要求の想定
  - 複雑化するアーキテクチャを踏まえた分析と検証

© SGS Société Générale de Surveillance SA. (2025)

Agenda

- **自動運転およびAI時代を見据えた半導体機能安全 最新動向**
  - 技術トレンドとビジネスモデルの変化
  - AIを含むISO26262 3rd Edition動向
- 自動運転およびAIを踏まえた半導体における機能安全開発のポイント
  - 現実的な安全要求の想定
  - 複雑化するアーキテクチャを踏まえた分析と検証

© SGS Société Générale de Surveillance SA. (2025)

自動運転時代の到来により車載システムが進化！

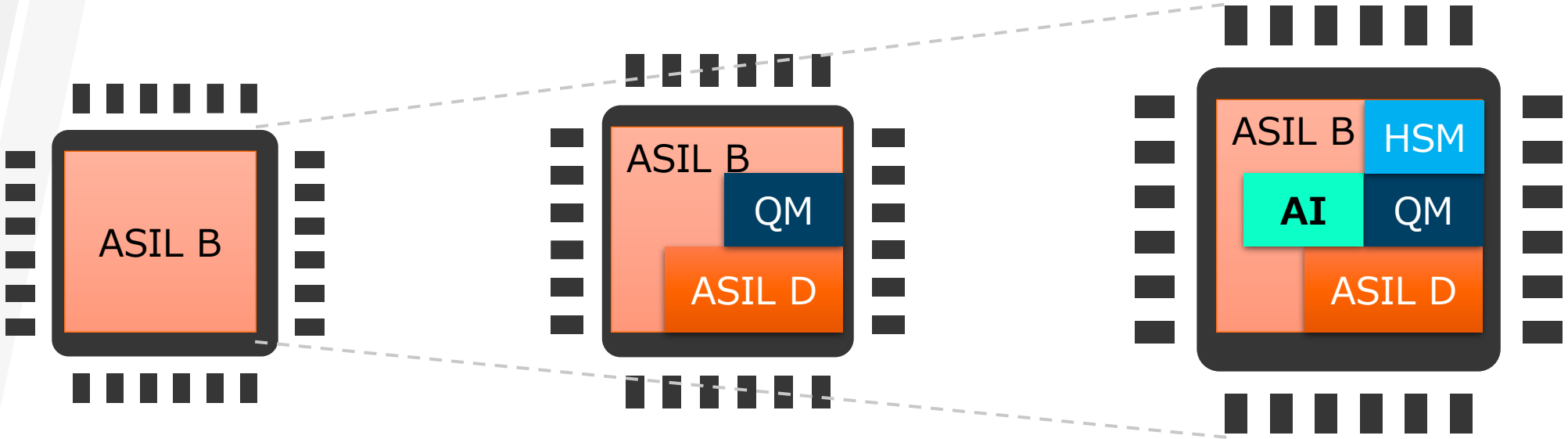
© SGS Société Générale de Surveillance SA. (2025)

車載システムの進化を実現する半導体機能安全トレンド

- シンプルな構成
- 単一のASILレベル
- 自社開発
- 安全要求が明確

- ASIL共存
- QM IPの統合
- SWとの協調
- 安全論証が高度化

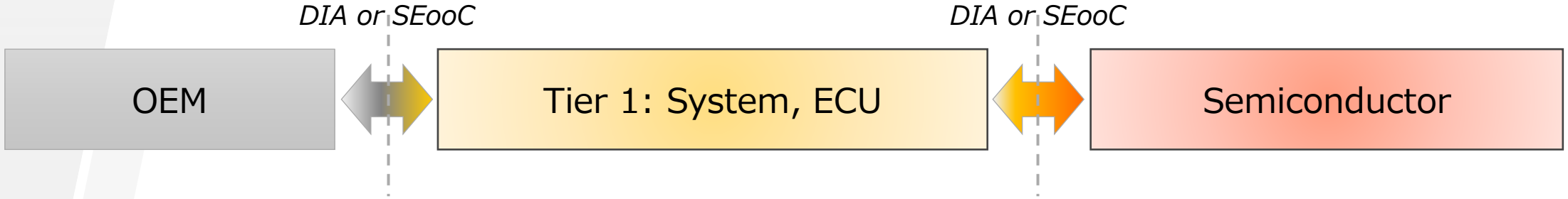
- セキュリティとの融合
- AI IPの安全論証
- Chip let 統合
- パフォーマンスのジレンマ



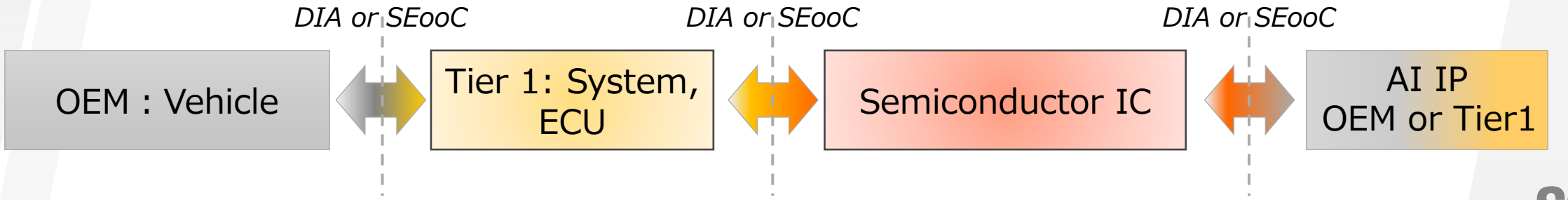
© SGS Société Générale de Surveillance SA. (2025)

半導体機能安全開発のビジネスモデルも変化

- 一般的な車載開発および機能安全対応
  - 階層間がある程度はっきりしており、サプライチェーン全体で機能安全対応

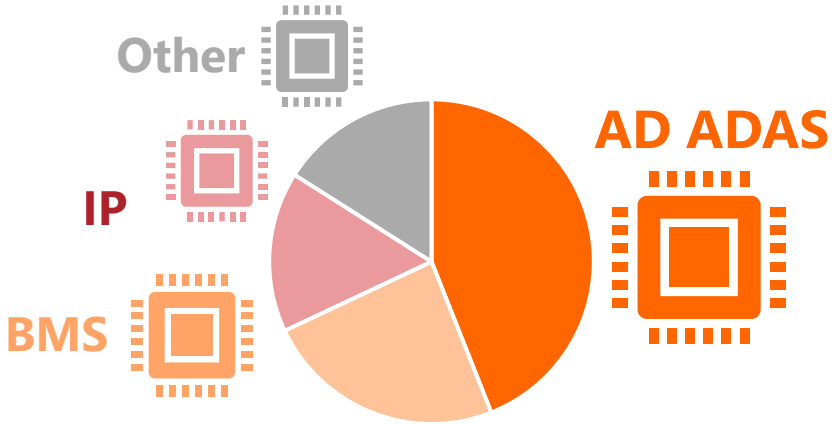


- 半導体機能安全開発のビジネスモデルも変化
  - コアとなるエレメント(自動運転AI IPやSoCなど)を自社開発するグローバルメーカが増加



© SGS Société Générale de Surveillance SA. (2025)

自動運転向け半導体製品認証も加速



- 機能安全プロセス認証 -> 製品認証を目指す半導体メーカがグローバルで拡大
- 特に自動運転関連は上位メーカから認証要求が増加
  - Camera SoC
  - Lidar SoC
  - Fusion SoC
  - Communication IC
  - AI IP
  - System Based PMIC


SGS TÜV SAAR

CERTIFICATE NO.: [redacted] PAGE 1/1

LICENCE HOLDER

[redacted]

Project-No/-ID: V1UL

LICENSED TEST MARK

Report No.: [redacted]

Tested according to: ISO 26262-5: 2018 (Clause 8 and 9)

Certified Product(s): [redacted]

Technical Data/Parameter: The above-mentioned product has been approved based on the safety assessment of a reference configuration (see certification report for details).
The architectural metrics SPFM (Single Point Fault Metric), LFM (Latent Fault Metric) and PMHF (Probabilistic Metric for random Hardware Failures) are in conformance with **ASIL B** target values.

Specific Requirements: The certificate is for type approval and based on a detailed functional safety assessment. Any changes to the design, materials, components or processing may require repetition of some of the assessment steps in order to retain type approval. The certificate report is an integral part of this certificate. All requirements and specifications of the current valid revision of this report shall be met.

Certification Body for Functional Safety SGS-TÜV Saar GmbH

[redacted]

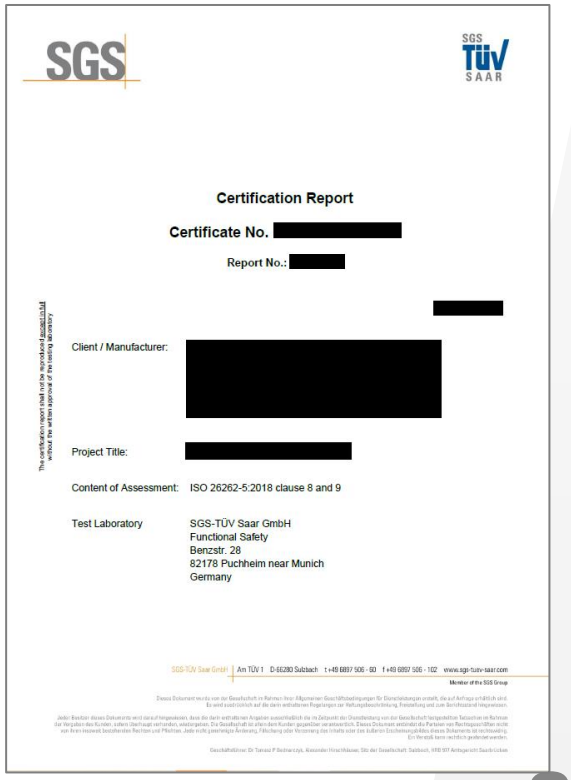
Liu Min

The validation status is documented via SGS Certification Database.

The test mark regulation is an integral part of this certificate.

SGS-TÜV Saar GmbH, Im Stadtwald / Germany

CERTIFICATE


SGS TÜV SAAR

Certification Report

Certificate No. [redacted]

Report No.: [redacted]

[redacted]

Client / Manufacturer: [redacted]

Project Title: [redacted]

Content of Assessment: ISO 26262-5:2018 clause 8 and 9

Test Laboratory: SGS-TÜV Saar GmbH
Functional Safety
Benzstr. 28
82178 Puchheim near Munich
Germany

SGS-TÜV Saar GmbH | Am TÜV 1 | D-66280 Sulzbach | t +49 6897 506 - 60 | f +49 6897 506 - 102 | www.sgs-tuev-saar.com

Member of the SGS Group

© SGS Société Générale de Surveillance SA. (2025)

ISO26262 3rd Edition 動向

- ISO26262 3rd Editionの議論がいよいよ本格化
- 来年 2026年にコミッションドラフト(CD)、DISおよび2027年に正式リリースで進行中
- ISOのいくつかの委員会で**AI**を含む、以下のトピックスが検討されており、3rd Editionに含めることを検討

＜ISO委員会のトピックス＞

- ISO/TR 9968 - Application to generic rechargeable energy storage systems for new energy vehicle
- **ISO/TR 9839 - Application of predictive maintenance to hardware with ISO 26262-5**
- **ISO/PAS 8926 - Functional safety - Use of pre-existing software architectural elements**
- **ISO/CD PAS 8800 - Safety and artificial intelligence**

© SGS Société Générale de Surveillance SA. (2025)

ISO/CD PAS 8800　安全性と人工知能 (AI規格)

- AIの用途と関連する安全要求が広範囲に及ぶこと、および最先端技術が急速に進化していることから、AIシステムの使用に関連する残存リスクを許容できるレベルまで低減するためのプロセスまたは製品特性に関する詳細な要件を提供することは不可能
- ISO26262およびISO21448で定義されている既存のアプローチを調整または拡張し、AIに対する安全性のフレームワークを定義 (AIエレメントの安全性に関するプロジェクト固有の論証をサポートすることにフォーカス)

› ISO/CD PAS 8800から参照されている規格類

ISO 21448:2022, Road vehicles — Safety of the intended functionality

ISO 26262:2018, Road vehicles — Functional safety

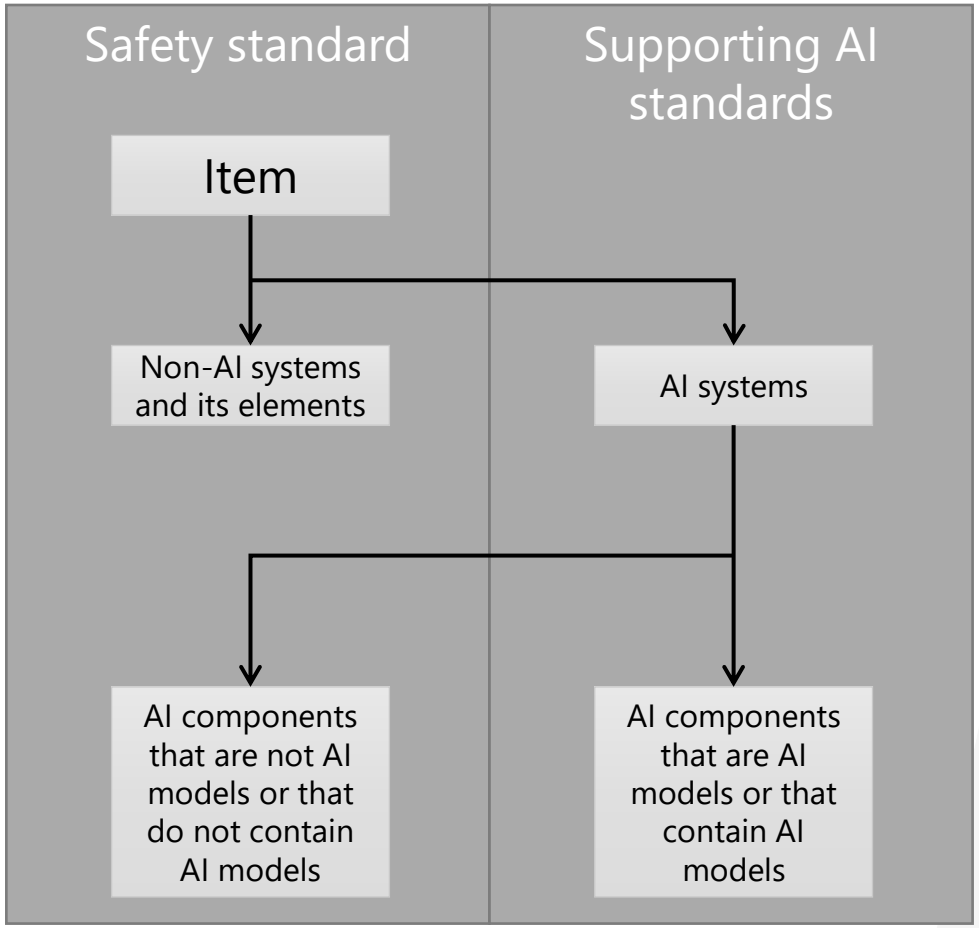
ISO/IEC 22989:2022, Information technology — Artificial intelligence

ISO/IEC TR 5469:2024, Artificial intelligence – Funcitonal safety and AI systems

© SGS Société Générale de Surveillance SA. (2025)

ISO26262との関連性

- PAS 8800は、AIシステムの安全性を対処するため、ISO 26262シリーズと組み合わせて適用することを目的としている
- AIモデルではない、またはAIモデルを含まないAIコンポーネントの場合、ISO26262シリーズを単独で適用可能
- AIモデルである、またはAI モデルを含むAIコンポーネントの場合、ISO26262シリーズをカスタマイズして、PAS 8800と組み合わせて適用可能



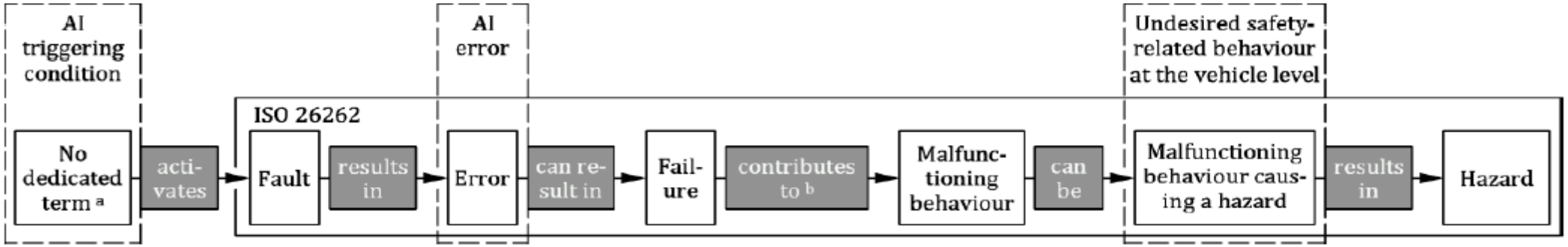


Figure 6-11 – Mapping of the cause-and-effect chain of ISO 26262 to the terms of this document

© SGS Société Générale de Surveillance SA. (2025)

AIシステム、コンポーネントの位置付け

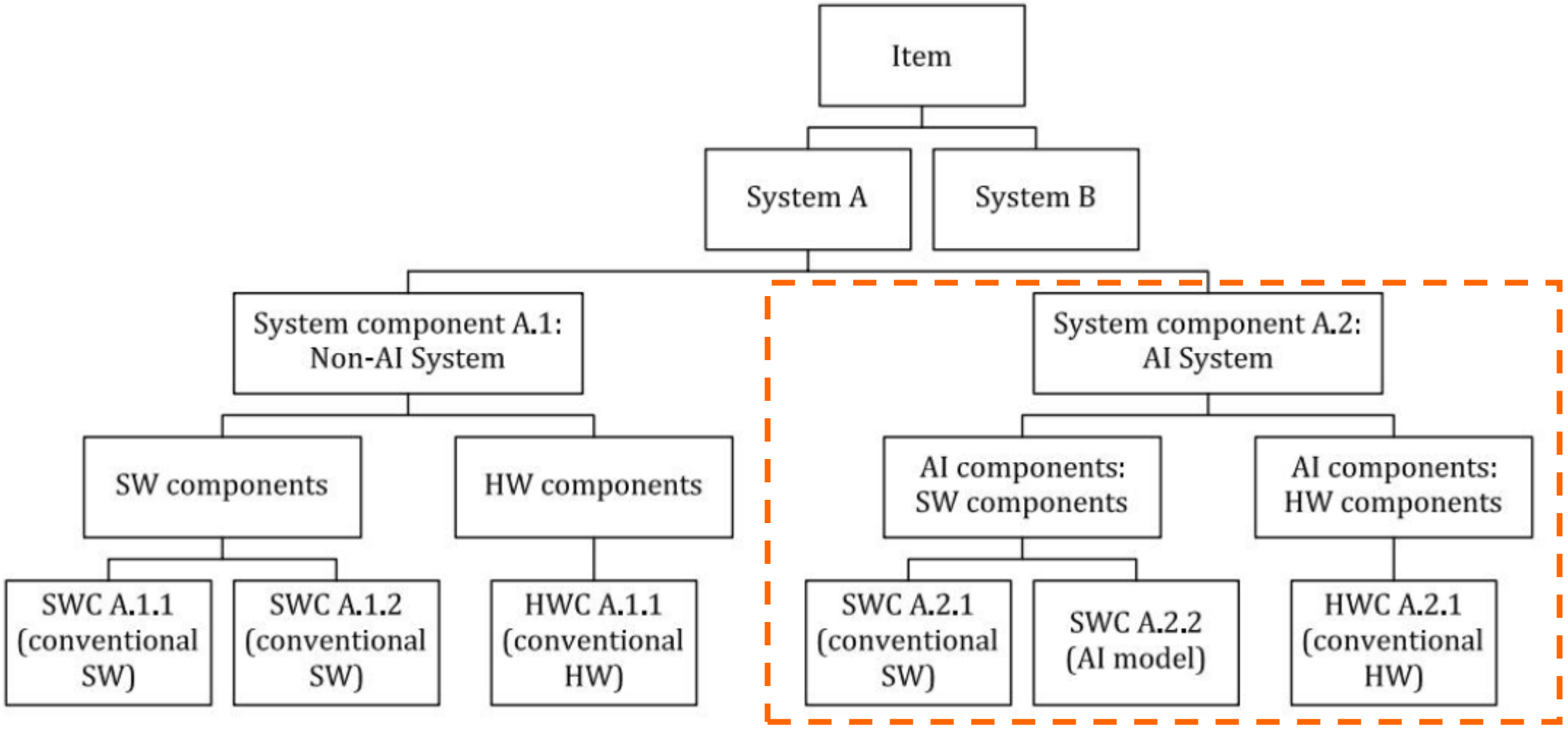


Figure 6–5 — Example of a hierarchical decomposition of an item into its elements down to the component level - decomposition tree view

 © SGS Société Générale de Surveillance SA. (2025)

ISO26262との関連性

PAS 8800の考慮が必要

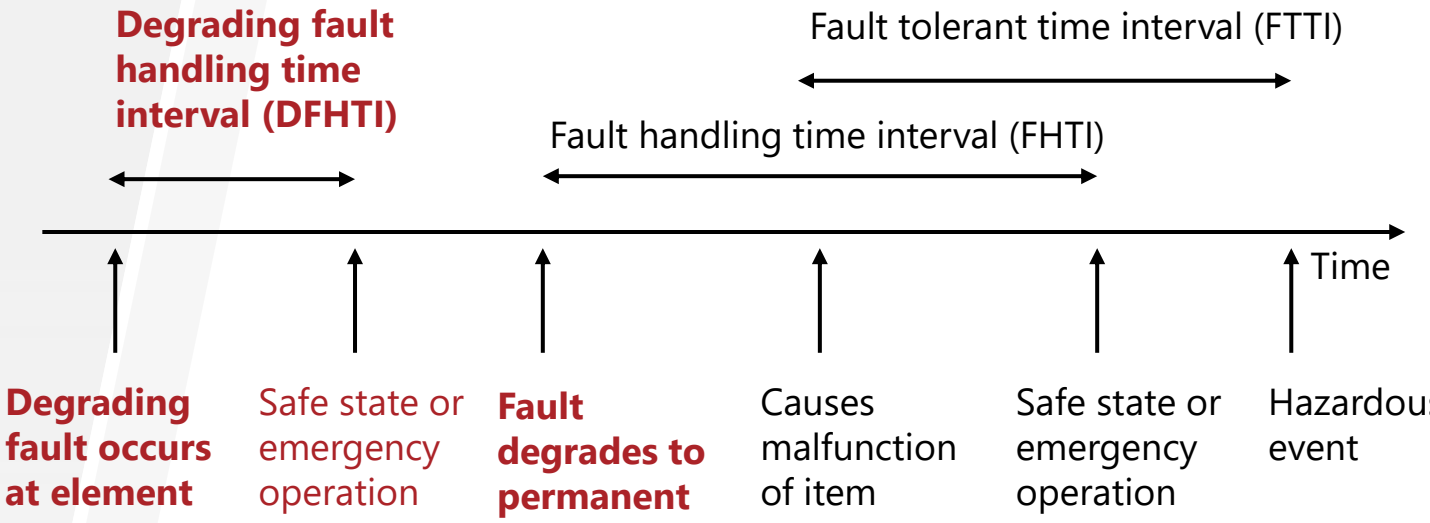
PAS 8800 Annex Cに
ISO26262 Part4、Part6に
対するGAPが定義

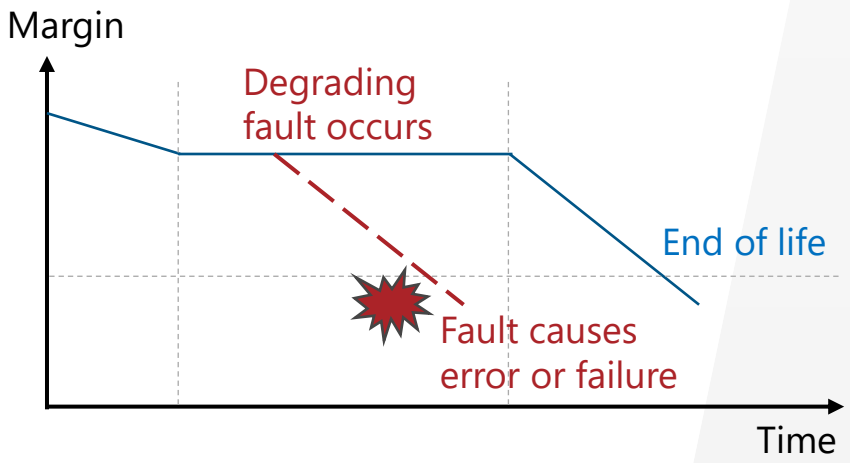
ISO 26262:2018	AIシステムを含むアイテム	AIシステム：HWとSWコンポーネントで構成	AIコンポーネント: 従来のHWコンポーネント (CPU、GPU、FPGAなど、AIモデルを実装するために特別に設計されていないHW)	AIコンポーネント: ソフトウェアコンポーネントによって実装されたAIモデル
Part 2 Safety management	AIの安全管理はアイテムの安全管理の一部	AIの安全管理にも対応できるように適用	直接適用可能	AIの安全管理にも対応できるように適用
Part 3 Item, HARA, SG, FSC	AIシステムに割り当てられた安全要求	-	-	-
Part 4 TSC	AIシステムに割り当てられた安全要求の導出元	適用可能 (但し、テーラリングが必要)	HW安全要求はAIシステムに割り当てられた技術安全要求から導出	SW安全要求はAIシステムに割り当てられた技術安全要求から導出
Part 5 Hardware	AIエレメントに割り当てられたHW安全要求の導出元	適用可能 (但し、テーラリングが必要)	適用可能	HSIのリファイン
Part 6 Software	AIエレメントに割り当てられたSW安全要求の導出元	適用可能 (但し、テーラリングが必要)	HSIのリファイン	適用可能 (但し、テーラリングが必要)

© SGS Société Générale de Surveillance SA. (2025)

ISO/TR 9839　予防保全 (Predictive maintenance)

- ハードウェアエレメントの劣化フォールトと予防保全技術を検討するためのアプローチを提供
  - 半導体における故障メカニズム：TDDB, HCI, NBTI, EM, etc
- 故障率(BFR)に劣化フォールトも含めることを言及しているが、データブック(IEC61709やSN29500など)による算出は難しいため、劣化フォールトを考慮したSPFM, LFM, PMHFの計算に課題有





参考：　2つのリング発振器　(1つは通常状態で実行され、もう1つはストレス状態で実行される)の比較を使用した劣化検出メカニズムが事例として言及

© SGS Société Générale de Surveillance SA. (2025)

ISO/PAS 8926 SWコンポーネント認定

- SWコンポーネントの「複雑度」と「起源、保管、所有権に関する情報」に応じてクラスを分類し、認定手法を選定

Complexity	Provenance		
	P1	P2	P3
C1	Class Ⅰ	Class Ⅰ a	Class Ⅱ
C2	Class Ⅱ b	Class Ⅱ	Class Ⅱ
C3	Class Ⅱ	Class Ⅱ	NR c

C1:決定された複雑さの尺度がいずれも高い複雑さを示さない場合

C2:決定された複雑さの尺度が高い複雑さを示すが、許容できると評価される場合、特定された複雑さによる体系的な障害のリスクが、対象のソフトウェアアーキテクチャ設計で十分に低いか、または高いが管理可能である場合

C3: 上記以外

※ 複雑度はAnnex Bに従って決定

P1: ソフトウェア開発プロセスが適切な国内または国際規格(ISO/IEC/IEEE 12207など)または異なる機能安全規格(IEC61508、RTCA DO-178C[7]など)に基づいているという証拠がある場合

P2: P1を完全に主張することはできないが、ソフトウェア開発プロセスのギャップが許容できると評価される場合

P3: 上記以外

- **Class Ⅰ**： ソフトウェアコンポーネントの認定をISO26262 Part8-12に従って対応
- **Class Ⅱ**： SWアーキテクチャ分析、SSR割り当て、安全分析、検証など追加の活動が必要
- **C3+P3**： 機能安全として推奨されない

© SGS Société Générale de Surveillance SA. (2025)

Agenda

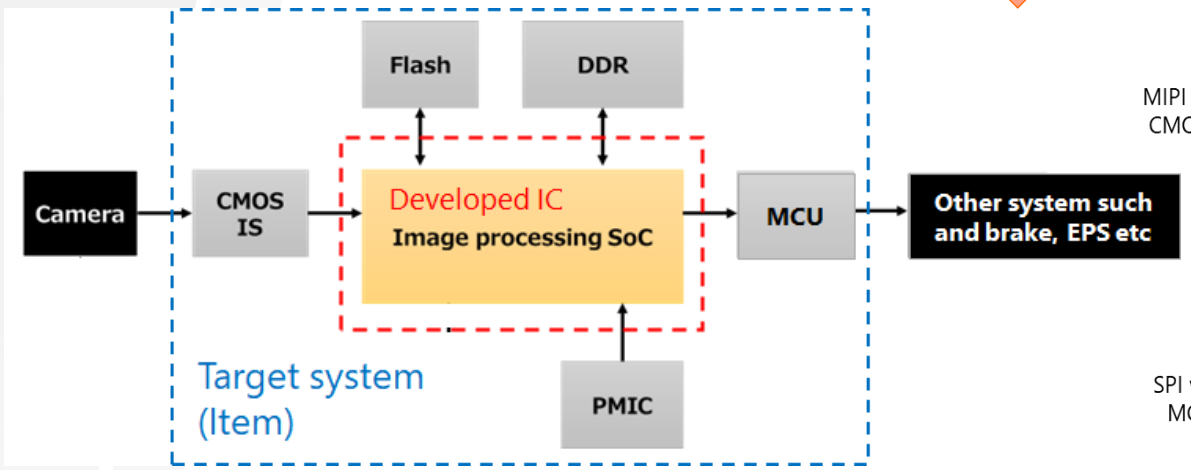
- 自動運転およびAI時代を見据えた半導体機能安全 最新動向
  - 技術トレンドとビジネスモデルの変化
  - AIを含むISO26262 3rd Edition動向
- **自動運転およびAIを踏まえた半導体における機能安全開発のポイント**
  - 現実的な安全要求の想定
  - 複雑化するアーキテクチャを踏まえた分析と検証

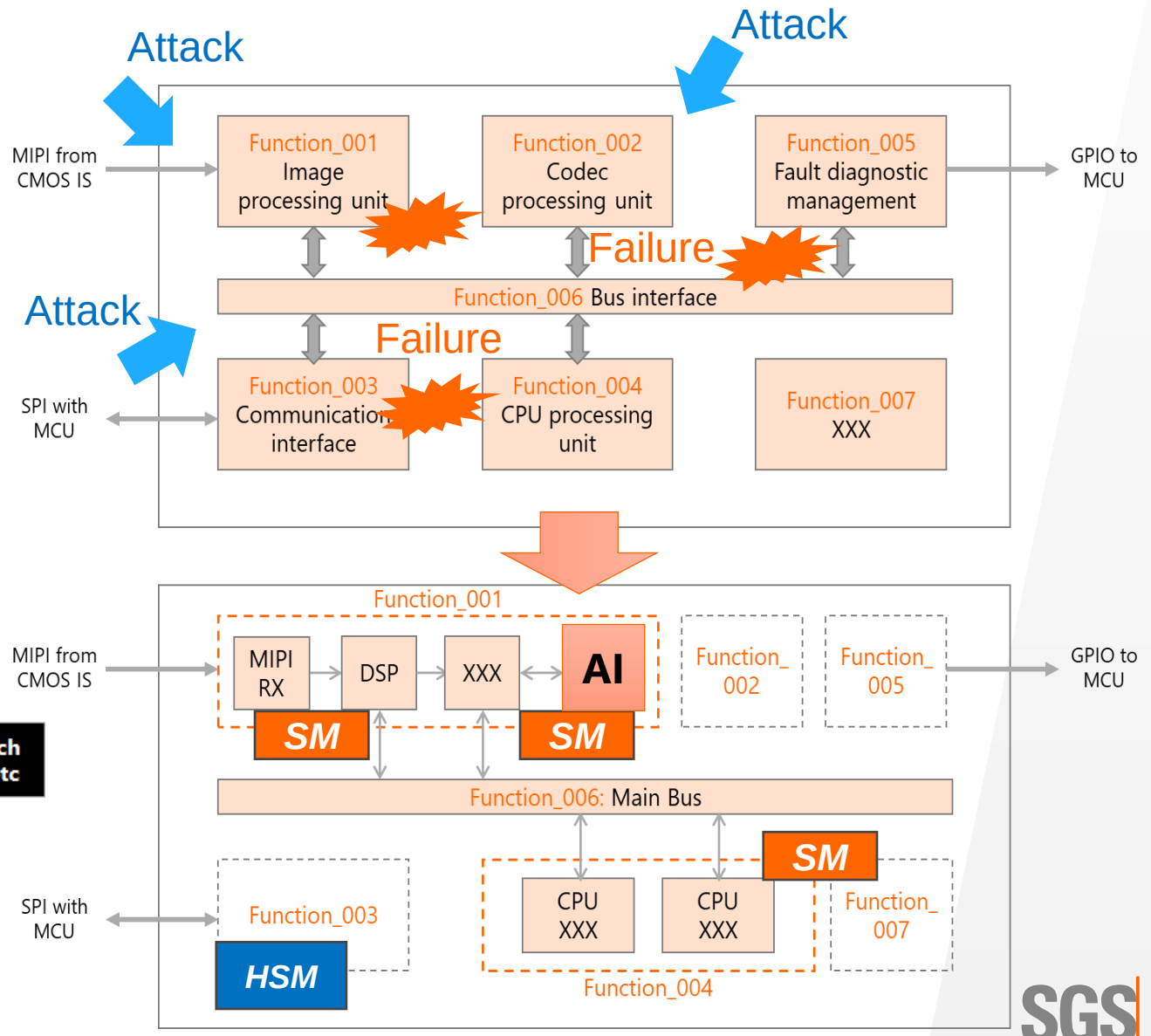
© SGS Société Générale de Surveillance SA. (2025)

現実的な要求の想定

- ターゲットシステムを踏まえた上で、System -> Sub system -> IP level のように階層を定義し、Step by Step で要求をリファイン !!

AD/ADAS事例





 © SGS Société Générale de Surveillance SA. (2025)

Safety and Security 要求想定事例

Functional Safety

- Hazard: Unintended camera image data anomaly
- SG: Prevent the unintended camera image data anomaly
- FSR: Shall detect the unintended camera image data failure and report to the external system within 10ms.
- TSR: SOC shall detect the data processing error (Application CPU) and report to the external MCU within 5ms.
- HSR: Shall implement the WDT for detecting the CPU overflow failure.

Cybersecurity

- Threat: The control parameters used for image processing are tampered
- SG: Prevent tampering with control parameters from external attacks
- CSR: Shall verify the integrity of control parameters read from external memory using a digital signature
- TCSR: SoC shall store the encryption key for digital signatures in a partitioned memory area.
- HCSR: Shall Implement a memory protection unit to protect cryptographic key

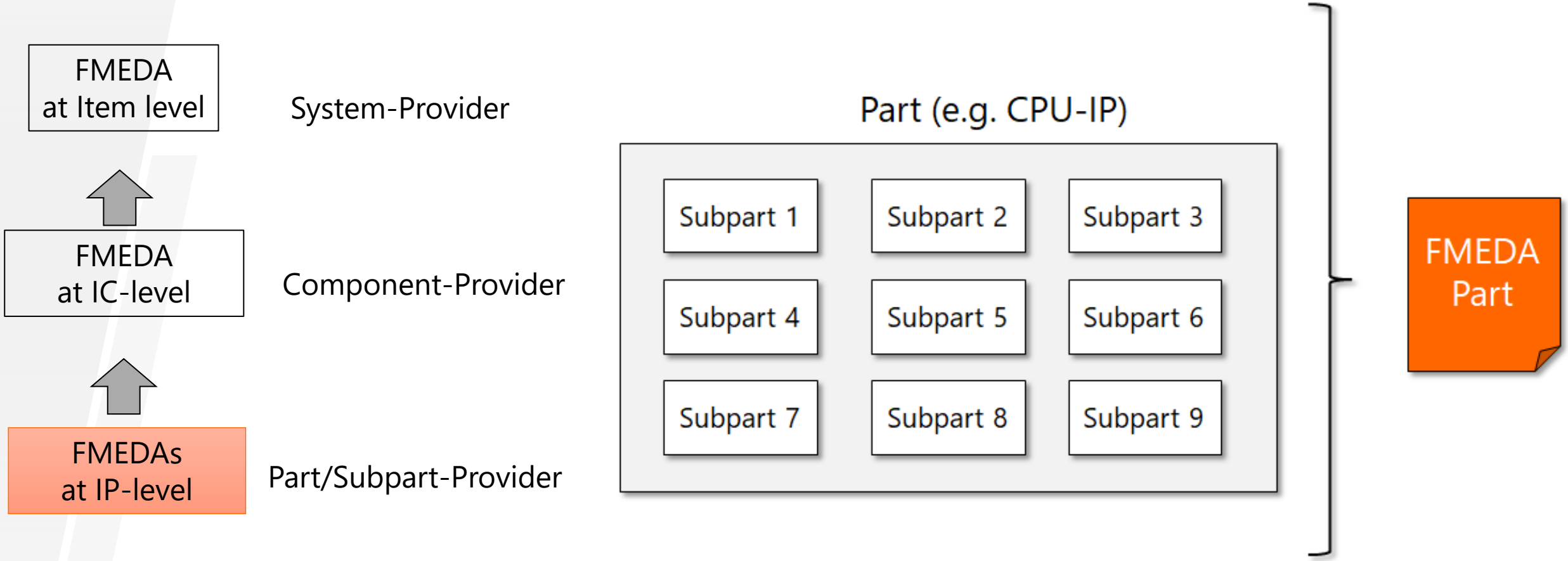
© SGS Société Générale de Surveillance SA. (2025)

開発初期段階から安全分析により検証するケースも増加

Structure analysis			Failure analysis				Safety violation			Risk analysis					
Component level	Part level	Sub-part level	Failure effect	Severity S	Failure mode	Failure cause	Violation of safety goals (Yes or No)	Safety goal ID or Safety requirement ID	Classification of SPF and LF	Current Prevention Control of Failure Cause	Occurrence O	Current Detection Control of Failure Cause	Detection D	RPN	DFMEA AP
ISP	Bus interface	AXI Bus interface	Can't output the recognition data.	9	Can't communicate the data between internal IPs.	Requested transaction not delivered	YES	SG_0001	SPF	Use case: Experienced steering system Process: Adopting experienced 16nm Design: Change only environmental conditions	3	Global simulation: PVT Sim and additional heat Sim	2	54	L
			Output the unintended recognition data.	9	Communicate the data at unintended timing.	Transaction delivered without a request	YES	SG_0001	SPF		3	**Safety mechanism** **Timeout detection Parity check**	2	54	L
			Output the recognition data at unintended timing.	7	Communicate the data at unintended timing.	Transaction delivered with incorrect timing	YES	SG_0001	SPF		3		2	42	L
			Output the unintended recognition data.	9	Communicate as unintended data.	Transaction delivered with incorrect data	YES	SG_0001	SPF		3		2	54	L
	Image processing unit	AI IP	Can't output the recognition data.	9	Can't execute the pixel data processing.	Given instruction flow(s) not executed.	YES	SG_0002	SPF	Use case: Experienced steering system Process: Adopting experienced 16nm Design: Change only environmental conditions	3	Global simulation: PVT Sim and additional heat Sim	2	54	L
			Output the unintended recognition data.	9	Execute as unintended pixel data processing.	Un-intended instruction(s) flow executed.	YES	SG_0002	SPF		3		2	54	L
			Output the recognition data at unintended timing.	7	Execute the pixel data processing at unintended timing.	Incorrect instruction flow timing	YES	SG_0002	SPF		3	**Safety mechanism** **SWBIST**	2	42	L
			Output the unintended recognition data.	9	Execute as unintended pixel data processing.	Incorrect instruction flow result	YES	SG_0002	SPF		3		2	54	L

© SGS Société Générale de Surveillance SA. (2025)

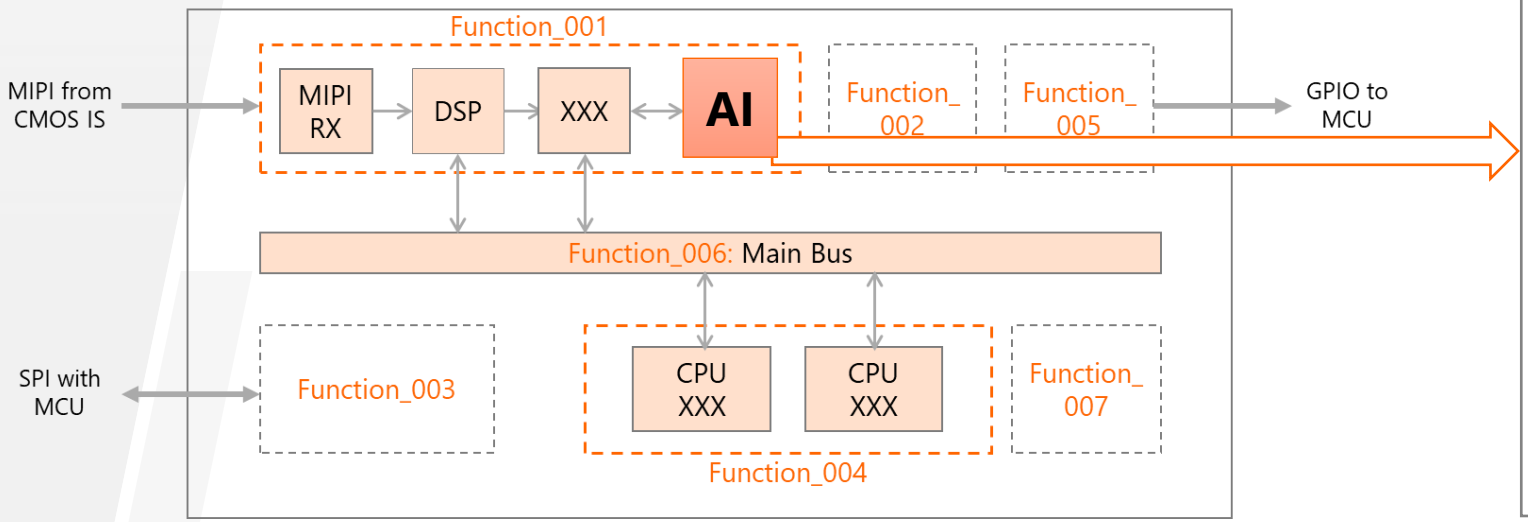
複雑化するアーキテクチャおよび回路構成こそ段階的にFMEDAを統合



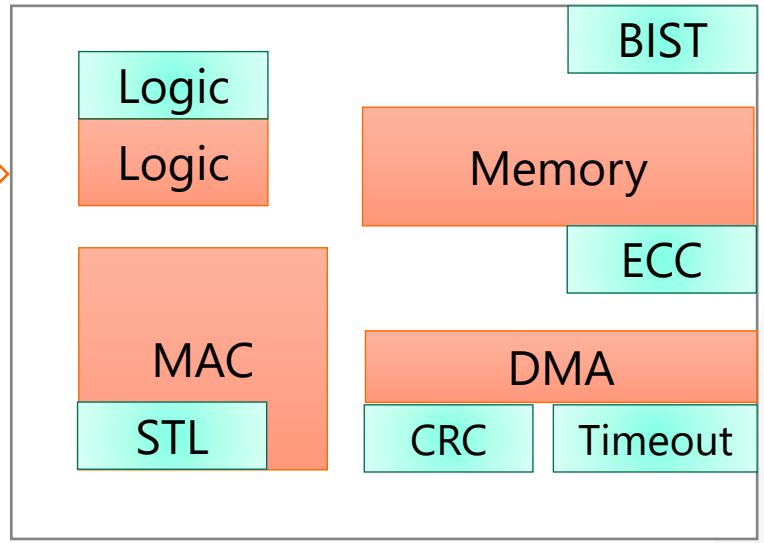
© SGS Société Générale de Surveillance SA. (2025)

IPの詳細分析から階層的にICトップへ統合

AD/ADAS SoC architecture



AI IP architecture example



Sub-IP	Sub-IP Failure Mode	IP Failure effect	Safety mechanism for SPF	Failure rate (FIT)	Failure mode distribution	Failure rate for each failure mode (FIT)	Diagnostic coverage and failure rate for single point fault			Safety mechanism for LF	Diagnostic coverage and failure rate for latent fault		
							Diagnostic coverage (%)	λSPF λRF (FIT)	λIF,DPF (FIT)		Diagnostic coverage (%)	λIF, DPF, latent (FIT)	λIF,DPF,detected (FIT)
MAC	Given instruction flow(s) not executed	NPU cannot perform recognition processing	STL	2	0.5	1	70	0.3	0.7	STL	100	0	0.7
	Incorrect instruction flow result	NPU output incorrect recognition result	STL		0.5	1	70	0.3	0.7	STL	100	0	0.7
Logic	Logic function not delivered when needed	NPU cannot perform recognition processing	Duplication	3	0.5	1.5	99	0.015	1.485	BIST	60	0.594	0.891
	Logic function provides incorrect output	NPU output incorrect recognition result	Duplication		0.5	1.5	99	0.015	1.485	BIST	60	0.594	0.891
Memory	Content of memory is corrupt	NPU output incorrect recognition result	ECC	4	1	4	99	0.04	3.96	ECC	100	0	3.96
DMA	No requested data transfer	NPU cannot perform recognition processing	Timeout	2	0.5	1	90	0.1	0.9	Timeout	100	0	0.9
	Incorrect output	NPU output incorrect recognition result	CRC		0.5	1	99	0.01	0.99	CRC	100	0	0.99

© SGS Société Générale de Surveillance SA. (2025)

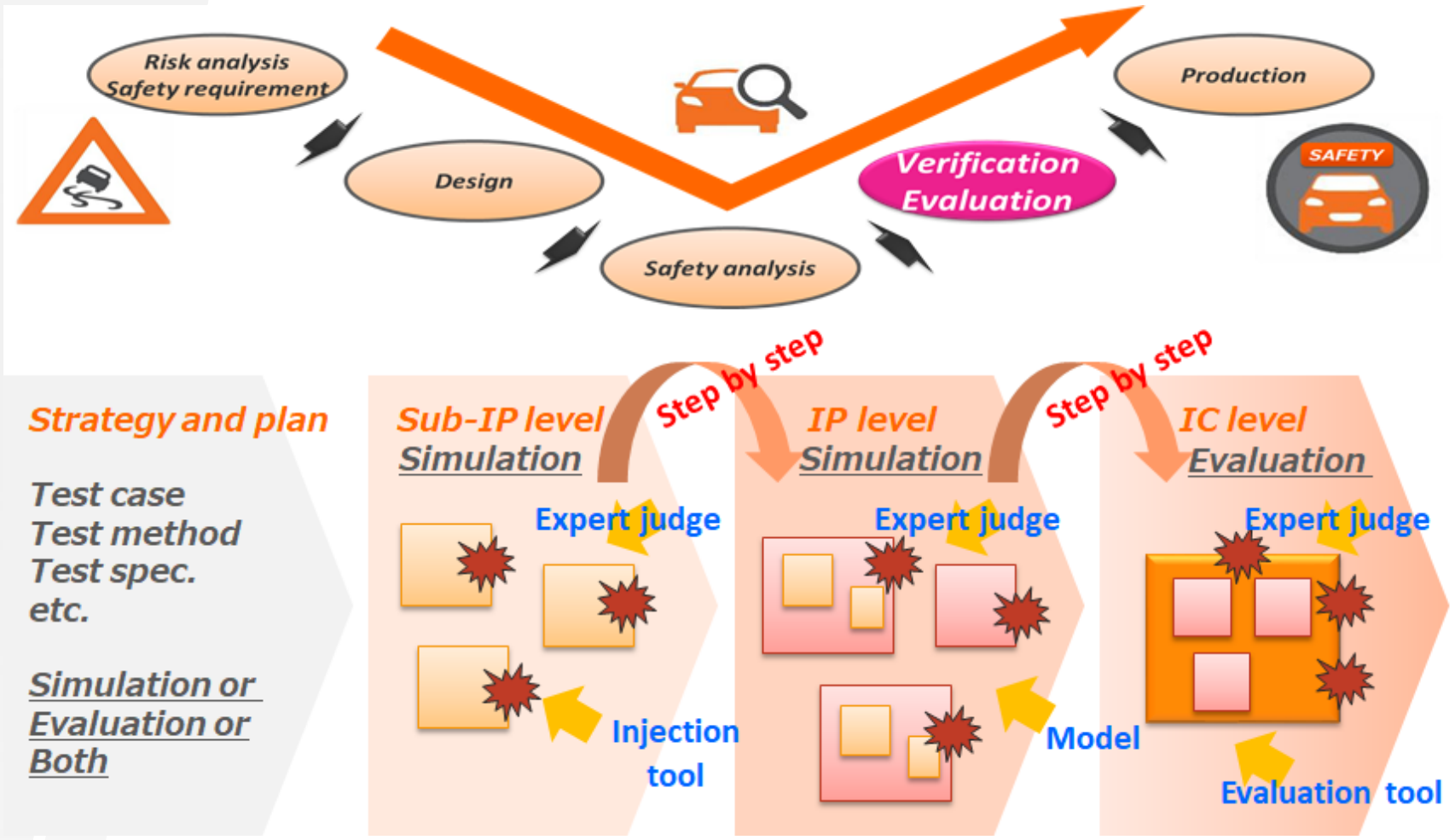
安全機構の論証と検証の重要性

戦略を明確化して、
一貫性がある論証が重要

Safety Mechanism	Fault detection target	Fault detection measures	Fault control measures	Measures to maintain a safe state	Measures to prevent latent fault	DC (%)	Argument	FHTI MPDTI
STL	MAC	The SoC's safety CPU periodically performs software diagnostics on the MAC accelerator and compares it with the expected value.	Safety CPU report failure information to EMU in safety island	EMU notify to the external MCU via GPIO	Not applicable	70%	Refer to ISO 26262-5:2018, D.2.3.1 Perform fault injection simulation and finally calculate DC from the result	5ms
Logic duplication	Control Logic	Not applicable	The control logic in the NPU is redundant, so it continues to operate even if each logic fails.	Not applicable	Logic BIST is performed on the control logic at boot time, and if a fault occurs, the EMU notifies the external MCU via GPIO.	99%	Refer to ISO 26262-5:2018, D.2.3.6 Representative fault injection XXX	NA
ECC	SRAM	SECDED ECC detect SRAM incorrect value (1 bit correct, 2 bit detect) for NPU Memory	Safety CPU report failure information to EMU in safety island	EMU notify to the external MCU via GPIO	Not applicable	99%	Refer to ISO 26262-11:2018, Table 33, 5.1.13.1 XXX	1ms
Timeout	DMAC	Timeout detect overflow failure for NPU DMA	Safety CPU report failure information to EMU in safety island	EMU notify to the external MCU via GPIO	Not applicable	90%	Refer to ISO 26262-5:2018, D.2.5.8 XXX	1ms

© SGS Société Générale de Surveillance SA. (2025)

効率的な検証と課題

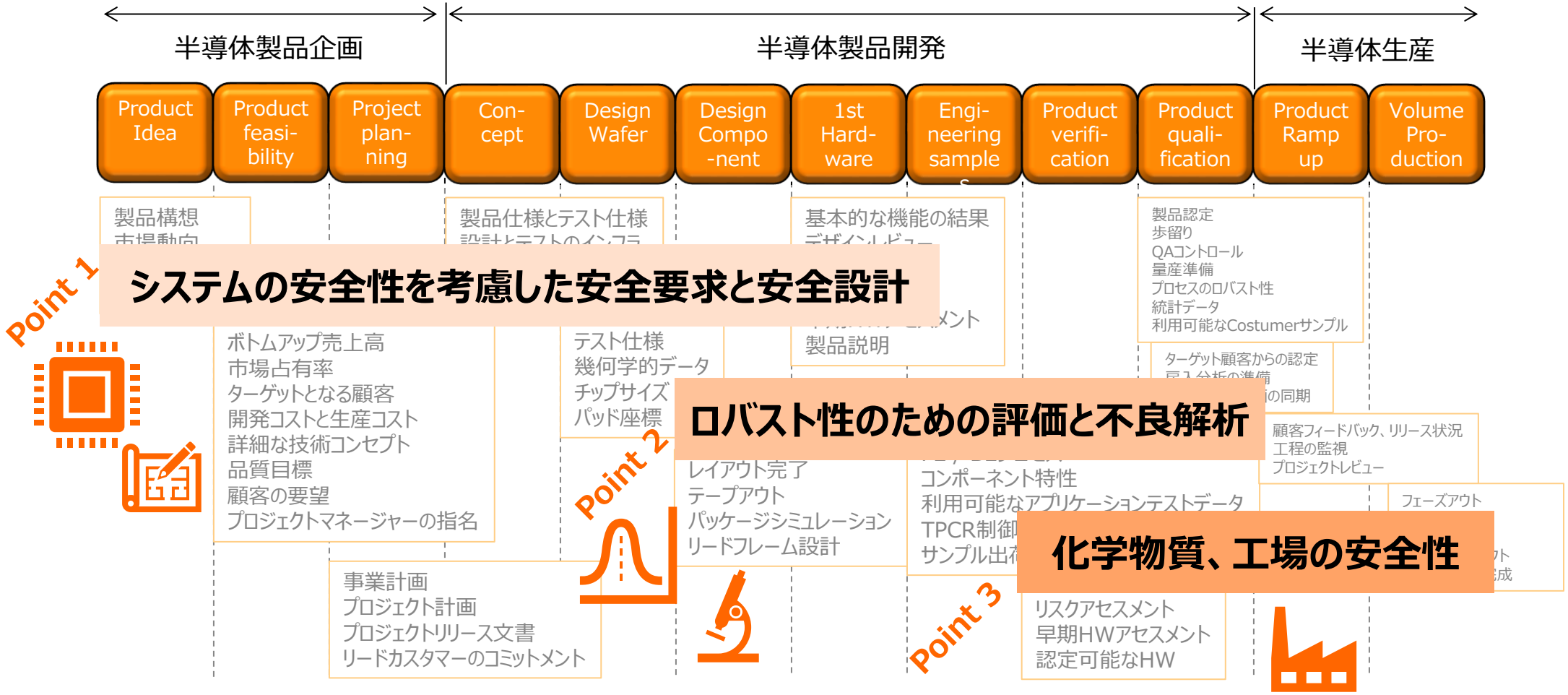


- Hierarchy
- Verification scheme
- Scenarios and patterns
- Observation points
- Fault model (transient)
- Injection point
- RTL or Gate
- Manual or automatic

© SGS Société Générale de Surveillance SA. (2025)

人々の”安心”・”安全”を支えるSGS半導体サービス

その一方で、複雑化するシステムにとって、半導体に対する”安全性”の確保も益々重要になってきています。



© SGS Société Générale de Surveillance SA. (2025)

人々の”安心”・”安全”を支えるSGS半導体サービス

安全仕様・設計からロバスト評価、不良解析、化学物質管理、工場の安全性など、お客様の半導体開発、生産の安全性をトータルソリューションでサポート致します。

サイバーセキュリティ

- サイバーセキュリティ教育・プロセス認証・製品認証
- 脅威分析・セキュリティコンセプト支援
  - お客様のターゲットシステムに対する脅威分析、セキュリティコンセプトの最適化をサポート
- サイバーセキュリティテスト
  - SGS Brightsightによる業界最高水準のテスト

機能安全

- 半導体機能安全教育・プロセス認証・製品認証
- 機能安全開発プロセス・検証プロセス最適化
  - 業界相場観を踏まえた最適なプロセス構築支援
- 機能安全仕様・設計検証サポート
  - 企画段階の製品コンセプトから安全設計、安全検証をトータルサポート

信頼性試験・故障解析

- 半導体信頼性試験
  - SGS Globalネットワークを活用した最適な信頼性試験サポート(JEDECやAEC Q100など業界標準の試験を実施可能)
- 半導体故障解析
  - X線、SAT、SEMなど幅広い解析サポート

EMC評価

- EMCフロントローディング
  - 低ノイズ基板設計サポート(各種I/Fのフィルタ設計、GND強化、基板パターンなど)
- EMC評価
  - CISPR25など業界標準、自動車メーカ規格に対応
  - 車載電波暗室を使用した大型機器の試験可能

工場向けサービス

- 代行検査サービス
  - ベンダー評価、第三者検査、工程確認などお客様の負担を軽減し、業務を最適化
- 高度人材派遣・紹介
  - 工場建設や管理など最適な人材確保を支援
- 配管の非破壊検査

化学物質管理

- 製品含有化学分析
  - PFASや各国RoHS・欧州REACH等、幅広い物質分析を支援
- 法規制調査・適合支援
  - 法規制インパクト調査・含有可能性評価サービス
- 化学物質管理体制構築・セミナー・教育支援

製品安全

- 半導体製造装置安全評価、試験
  - SEMI規格（S2,S6,S8,S14,S22,S30など）や各国の安全規格への適合性を評価・試験・サポート
- 製品認証、申請代行
  - 半導体製造装置、産業機械などの各国の認証のための試験、申請代行などトータルサポート

© SGS Société Générale de Surveillance SA. (2025)

今後も引き続き、宜しくお願い致します。

SOTIF

機能安全

半導体

ASPICE

サイバーセキュリティ

開発経験及び市場相場観に基づく現実的なサポート

業界No.1の技術力

複雑化する業界に対してお客様ごとに最適なプロセスを構築

トレーニングからプロセス構築、認証まで
One stopサービス

海外動向も踏まえたプロジェクトサポート

SGS

© SGS Société Générale de Surveillance SA. (2025)