SCDLのセキュリティサブワーキングの取り組み

名古屋大学 大学院情報学研究科
附属組込みシステム研究センター
倉地　亮

自己紹介

- 倉地　亮 (くらち　りょう)
  - 博士(情報科学)
  - 所属: 名古屋大学大学院 情報学研究科
    附属組込みシステム研究センター 特任准教授

- 現所属にて何をしているのか？
  - リアルタイムネットワークのスケジューリング解析手法
  - 車載制御システムの設計技術
  - 〃　　のセキュリティ強化技術

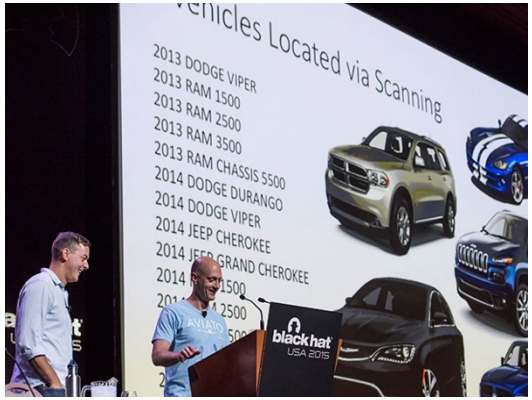
- 学外での活動
  - 自動車技術会 サイバーセキュリティ講座委員会 委員長
  - 自動車技術会 教育会議 委員
  - SCDL セキュリティサブワーキング 座長
  - J-Auto-ISAC 学術会員
  - 電子情報通信学会 情報セキュリティ研究会(ISEC) 専門委員
  - SIP 自動走行システムの社会的影響に関する検討委員会 委員
  - モビリティイノベーション連絡会議 個人会員
  - Trusted Computing Group (TCG) Invited Expert
  - AUTOSAR WP-SEC, FT-ST member など

アジェンダ

- 1. セキュリティサブワーキングの活動紹介
  - 研究背景
  - 活動概要
  - 現状の成果物
- 2. セーフティとサイバーセキュリティのエンジニアリングの課題
  - 課題1. 前提となる専門性/知識の違い
  - 課題2. セーフティとセキュリティの開発プロセスの統合/連携
- 3. 現在の議論
  - 議論1. 機能安全とサイバーセキュリティの連携プロセス
  - 議論2. Concept Phaseで取り扱うべき抽象度(粒度)

背景. 自動車のサイバーセキュリティ強化が要求

- 研究者らにより自動車のセキュリティ上の脅威が指摘
- 実際に販売される車両にもセキュリティ強化技術が適用されつつある
- 現在では一部車両の型式認証にサイバーセキュリティ強化が必須



https://spectrum.ieee.org/jeep-hacking-101

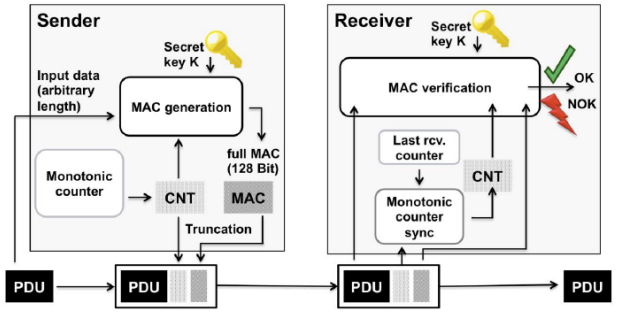
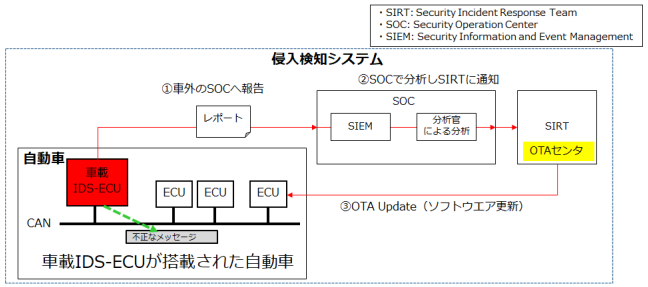
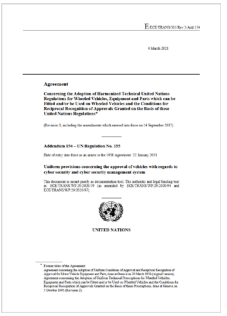


Figure 1: Message Authentication and Freshness Verification

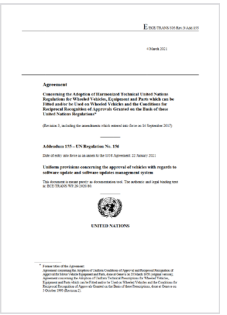
適用されつつある技術の例1. メッセージ認証
AUTOSAR version R21-11 Requirements on
Module Secure Onboard Communication



適用されつつある技術の例2. 侵入検知システム



国際基準　UN-R155
（サイバーセキュリティ）



国際基準　UN-R156
（ソフトウェアアップデート）

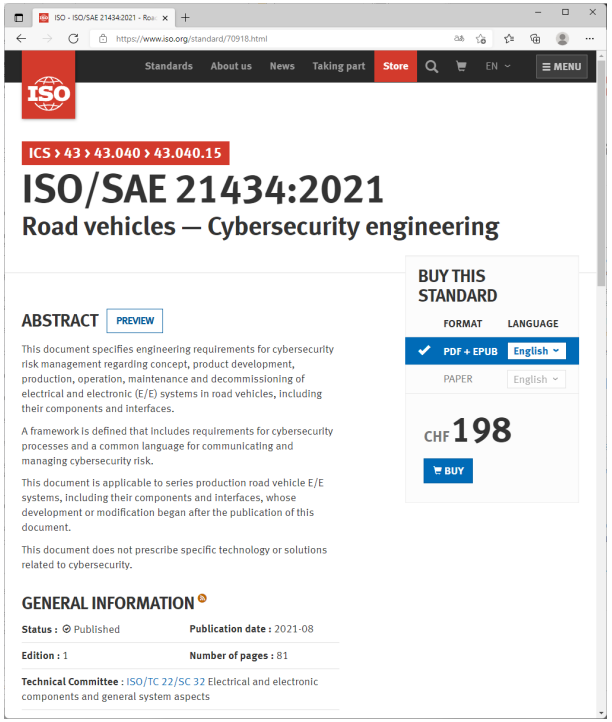
脅威事例
（2010～）

セキュリティ強化
(2019～)

国際基準と法制度化
（2022～）

背景. 自動車のサイバーセキュリティ強化が要求

- 2016年1月にSAEからCybersecurity Guidebook for Cyber-Physical vehicle Systems (J3061)が発行
- 2021年8月にISO/SAE 21434正式発行
- 2021年7月 Automotive SPICE for Cybersecurityが発行



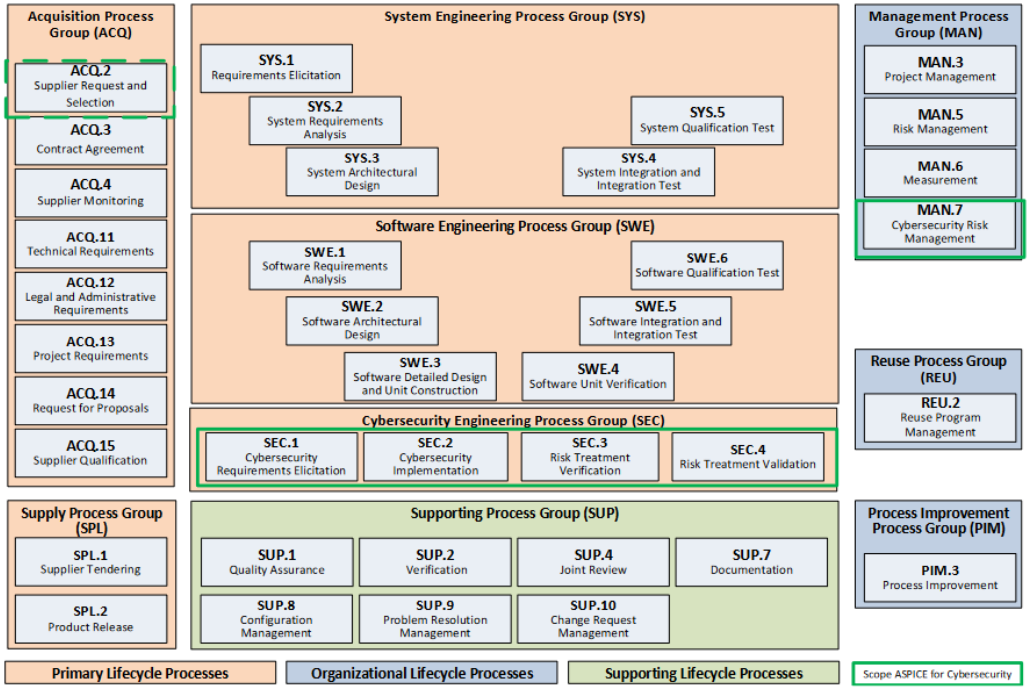


Figure 2 — Automotive SPICE and Automotive SPICE for Cybersecurity Process Reference Model – Overview

https://www.iso.org/standard/70918.html

https://vdachina.com.cn/upload/default/20210316/4b7fa0169a65d1812962b169f2464969.pdf

脅威をどのように扱うか論証していくことが重要になっている

1. セキュリティサブワーキングの活動紹介

背景

- 機能安全でのSCDLの活用は進められている
- 一方で，「サイバーセキュリティでSCDLは活用できるか？」という課題が存在

機能安全の専門家

サイバーセキュリティの専門家

うまく連携するにはどうしたら良いか（＝SCDLが役に立たないか）

1. セキュリティサブワーキングの活動紹介

活動目的

- SCDLの成果物をサイバーセキュリティ適用について検討を進めている

活動概要

- 昨年度の成果であるSAFECOMP2020の論文を基に，セキュリティエンジニアリングにおけるSCDLの課題点を洗い出すため，脅威分析を実施中
- 現状でも色々な課題が出てきており，SCDLを活用しセーフティとセキュリティの違いや課題点について整理中

活動体制

- 月1回のWeb会議で実施(次回 12/21(水) 13:00～)

1. セキュリティサブワーキングの活動紹介

■ 参加者(2021年9月10日時点): 38人(昨年，今年度共に増加傾向)

(一財)日本自動車研究所	伊藤　寛
	福田　和良
(株)アトリエ	水口　大知
(株)今仙電機製作所	山内　保尚
DNV GLビジネス・アシュアランス・ジャパン(株)	小澤　弘正
おおた開発効率化プロジェクト	小笠原　豊和
おがたコンサルティング	緒方　健
オムロン(株)	廣部　直樹
ガイオ・テクノロジー(株)	田中　伸明
(株)アドヴィックス	河野　文昭
(株)構造計画研究所	太田　洋二郎
	市村 健太朗
	東道　徹也
(株)三菱総合研究所	石黒　正揮
産業技術総合研究所	三科　雄介
	寶木　和夫
スズキ(株)	村松　稔久
住友電気工業(株)	左近　透
名古屋大学	倉地　亮
日本大学	松野　裕
ベクター・ジャパン(株)	中村　伸彦
マレリ(株)	佐々木　喜好
三菱電機(株)	友永　一生
仙台高等専門学校	岡本　圭史
DNV GLビジネス・アシュアランス・ジャパン(株)	高田　聖
	山下　修平
	平野　薫
	松並　勝
(株)チェンジビジョン	岩永　寿来
ガイオ・テクノロジー(株)	猪狩　秀夫
	岡田 利一
	小野 嘉翔
	三宮　雅人
	肥田野 文之
	大西 建児
	光山　栄太
	荻野(Web担当)
(株)シーエーブイテクノロジーズ	田口　研治

2. セーフティとサイバーセキュリティのエンジニアリングの課題

課題1. 前提となる専門性/知識/アプローチの違い

- 機能安全：安全工学
- サイバーセキュリティ： 情報セキュリティ，暗号数学，暗号実装

➡ **機能安全とサイバーセキュリティの専門家の連携方法が必要**

課題2. セーフティとセキュリティの開発プロセスの統合/連携

- 開発プロセスの連携についても議論が存在
- ただし，従来の議論は理想的な人員や体制，開発期間に応じた理想的なモデル

➡ **現実的なモデルを検討する必要あり**

以降では，上記課題2点についてそれぞれ概説する

2. セーフティとサイバーセキュリティのエンジニアリングの課題

- 課題1. 前提となる専門性/知識/アプローチの違い
- 1. 機能安全
  - 機能的な工夫（安全を確保する機能）により極力安全を確保
  - 信頼性が重視

  ➡ 安全性を確保するための機能を実装
- 2. 情報セキュリティ
  - 情報の機密性，完全性および可用性の維持
  - さらに真正性，責任追跡性，否認防止，信頼性などの特性の維持を含める
  - 機密性(Confidentiality)

    ― アクセスに認可された者だけが情報にアクセスできること
  - 完全性(Integrity)

    ― 情報及び処理方法が正確であること及び完全であること
  - 可用性(Availability)

    ― 認可された利用者が，必要なときに情報及び関連する資産にアクセスできること

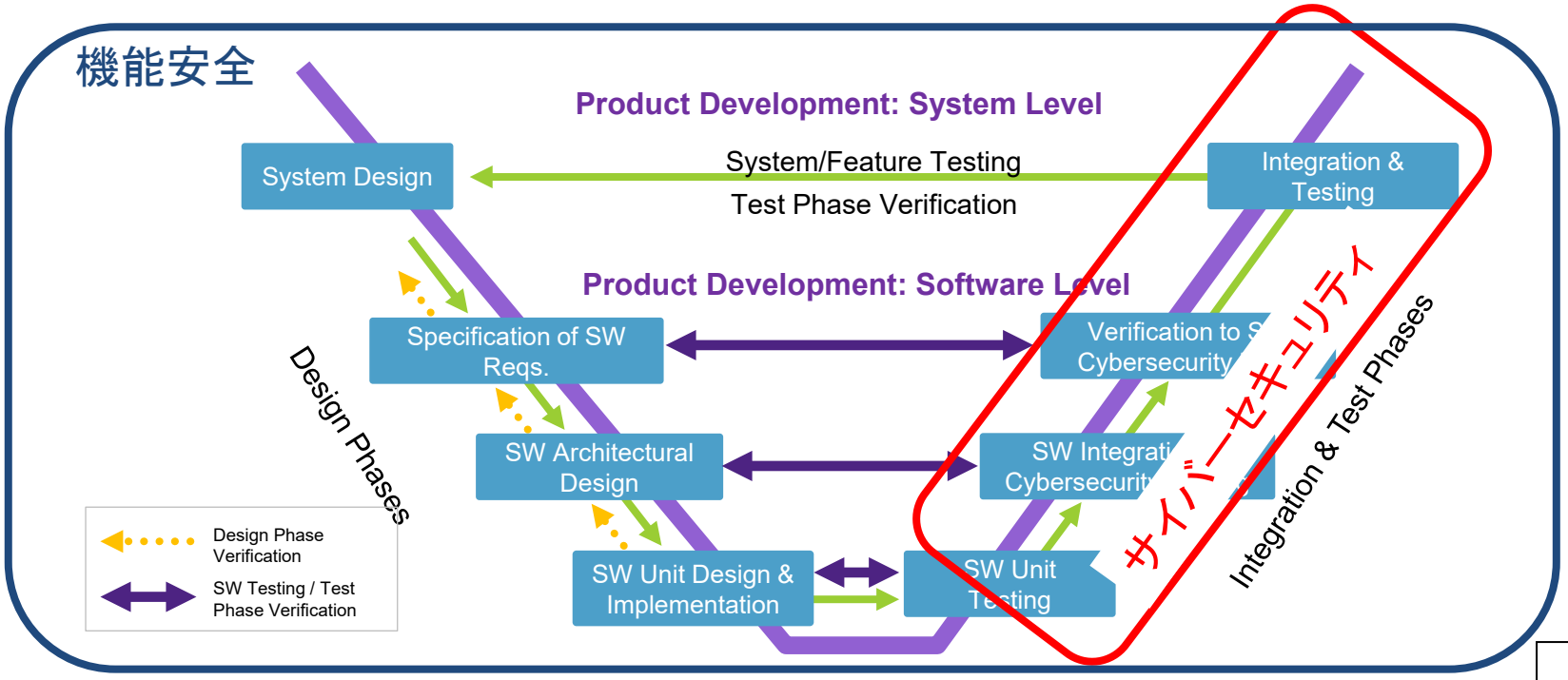
  ➡ システムの弱い点(≒脆弱性)を保護する機能を実装

2つの異なる分野の専門家が開発時にすり合わせる必要性あり

2. セーフティとサイバーセキュリティのエンジニアリングの課題

課題1. 前提となる専門性/知識/アプローチの違い

- **機能安全の文化: 保証ケースを重視**
  - ― 上流から保証ケースを決定したい
- **サイバーセキュリティの文化: ベストプラクティスの文化**
  - ― 動作検証/テストにより脆弱性がないことを保証したい
  - ― Security by design(近年，上流設計から考慮することも重要視されている)



2. セーフティとサイバーセキュリティのエンジニアリングの課題

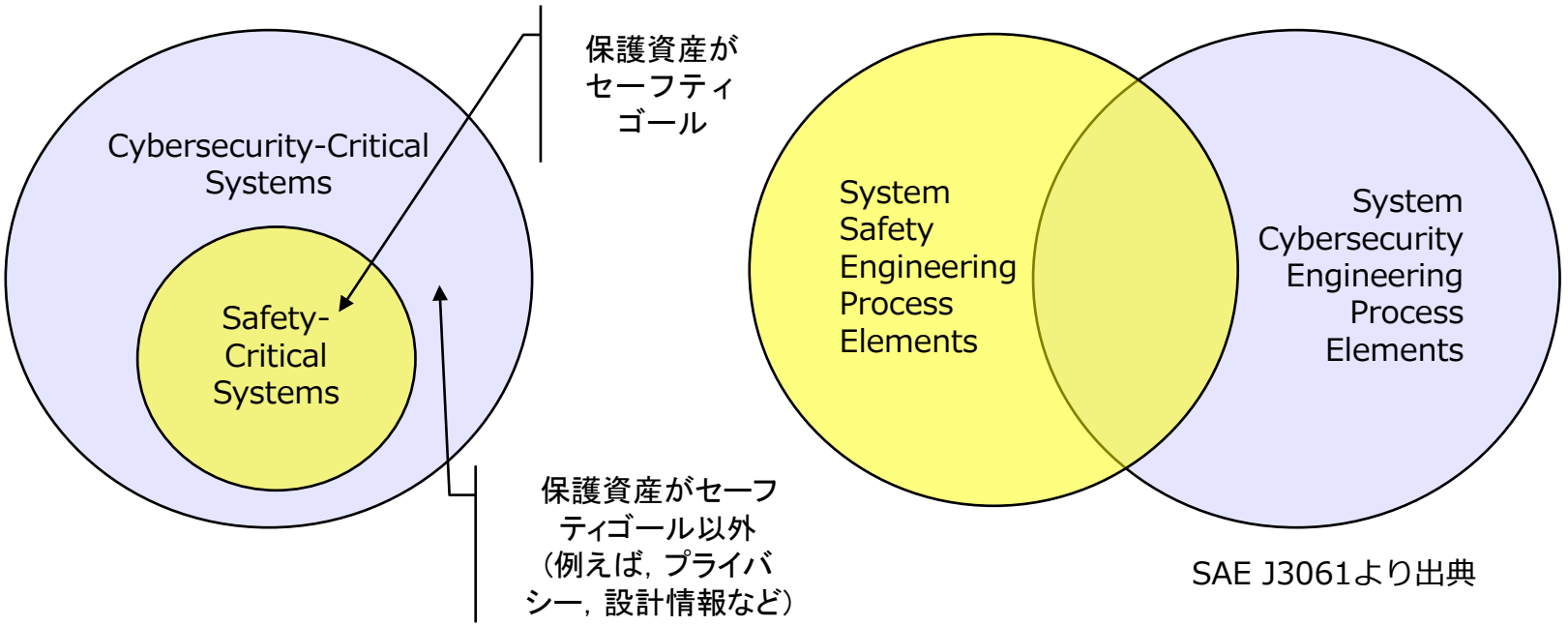
- 専門性の違い/考え方のギャップをどのように埋めるか？
  - ➡ “知識/経験が重要”
  - ➡ お互いを知ることが大切．そして，擦り合わせも必要
- 機能安全とサイバーセキュリティの重要度は対等

セキュリティSWGでは機能安全の専門家が脅威分析を実施

2. セーフティとサイバーセキュリティのエンジニアリングの課題

課題2. セーフティとセキュリティの開発プロセスの統合/連携

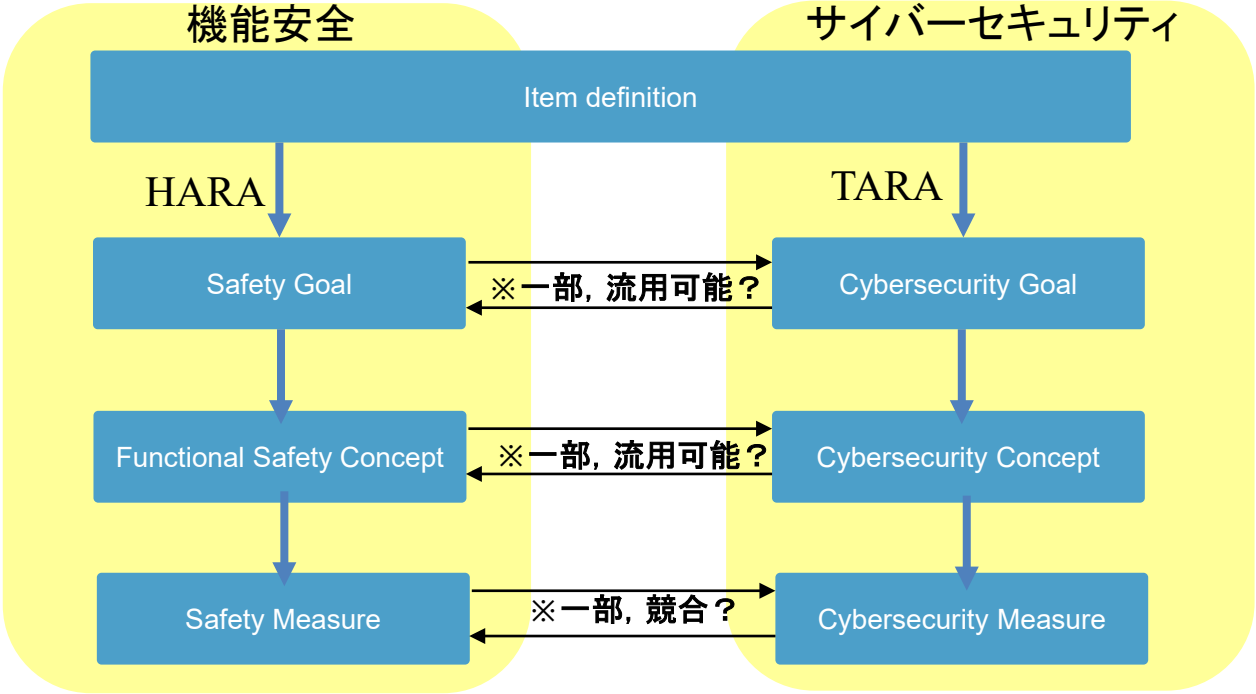
- セーフティクリティカルシステムはサイバーセキュリティクリティカルシステムとして扱われる
- 一方，エンジニアリングプロセスは，両者をうまくテーラリングすることが必要



2つの異なる分野の専門家が開発時にすり合わせる必要性あり

2. セーフティとサイバーセキュリティのエンジニアリングの課題

- 課題2. セーフティとセキュリティの開発プロセスの統合/連携
- 1. 機能安全(ISO26262)
  - Hazard Analysis and Risk Assessment (HARA) を実施
    - ―Safety Goals, Functional Safety Concept が導出
- 2.サイバーセキュリティ(ISO/SAE 21434)
  - Threat Analysis and Risk Assessment (TARA) を実施
    - ―Cybersecurity Goals, Cybersecurity Concept が導出



2. セーフティとサイバーセキュリティのエンジニアリングの課題

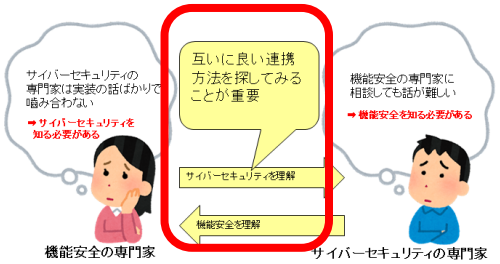
■ 開発プロセスの統合/連携をどのように進めるか？

➡ 前提の違いを理解する

	Safety	Financial	Operational	Privacy
機能安全	◎ （詳細化）	△ （範囲外）	△ （範囲外）	× （対象範囲外）
サイバーセキュリティ	△ （詳細化は困難）	○ （対象範囲）	○ （対象範囲）	○ （対象範囲）

➡ 成果物の相互活用が重要

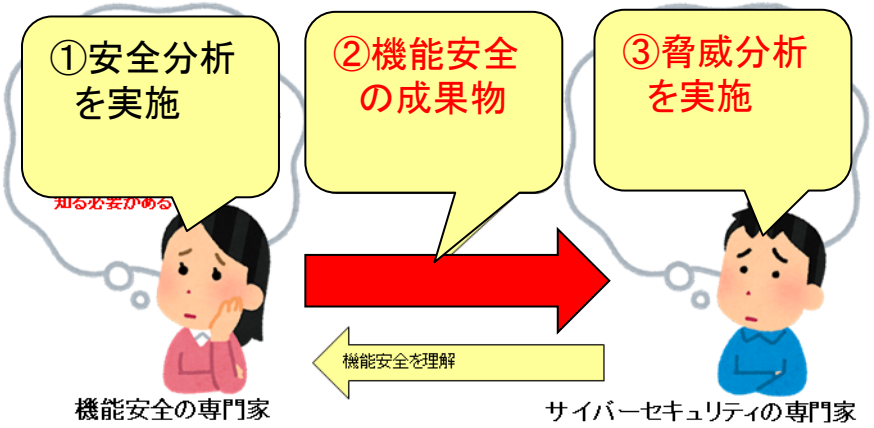
機能安全プロセスの成果物をサイバーセキュリティでも利用してみる
（逆の場合も同様）

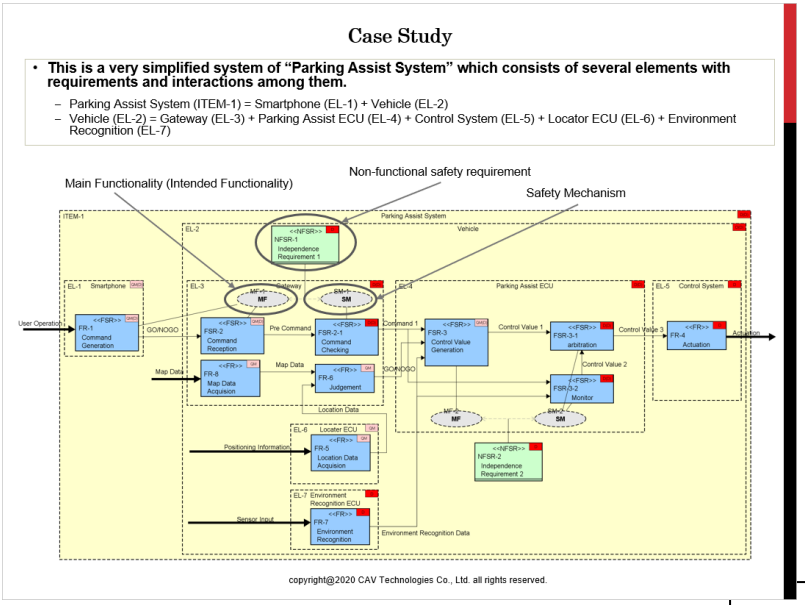


SCDLがコミュニケーションツールになるのではないかと仮説

セキュリティSWGにおける過去の成果

- 事例1. 機能安全の成果物を利用し脅威分析を実施
  - ➡ 評価対象システムとして“(安全機構が入った)スマホでパーク“を使用
  - ➡ 安全機構はセキュリティ強化策として有効か？
- 結論
  - 安全機構が役に立つ場合もあるが，セキュリティ強化策がないと不十分
    - ― 攻撃者がなりすまし/多重故障を引き起こし安全ゴールを侵害可能
- 取り組み
  - セキュリティ強化策の導出
  - 安全分析へのフィードバック





現在の議論

- 議論1. 機能安全とサイバーセキュリティの連携プロセス
  - 安全機構（セキュリティ強化策）への影響や干渉がないか？
- 議論2. Concept Phaseで取り扱うべき抽象度(粒度)
  - SCDLの記法も拡張が必要か？

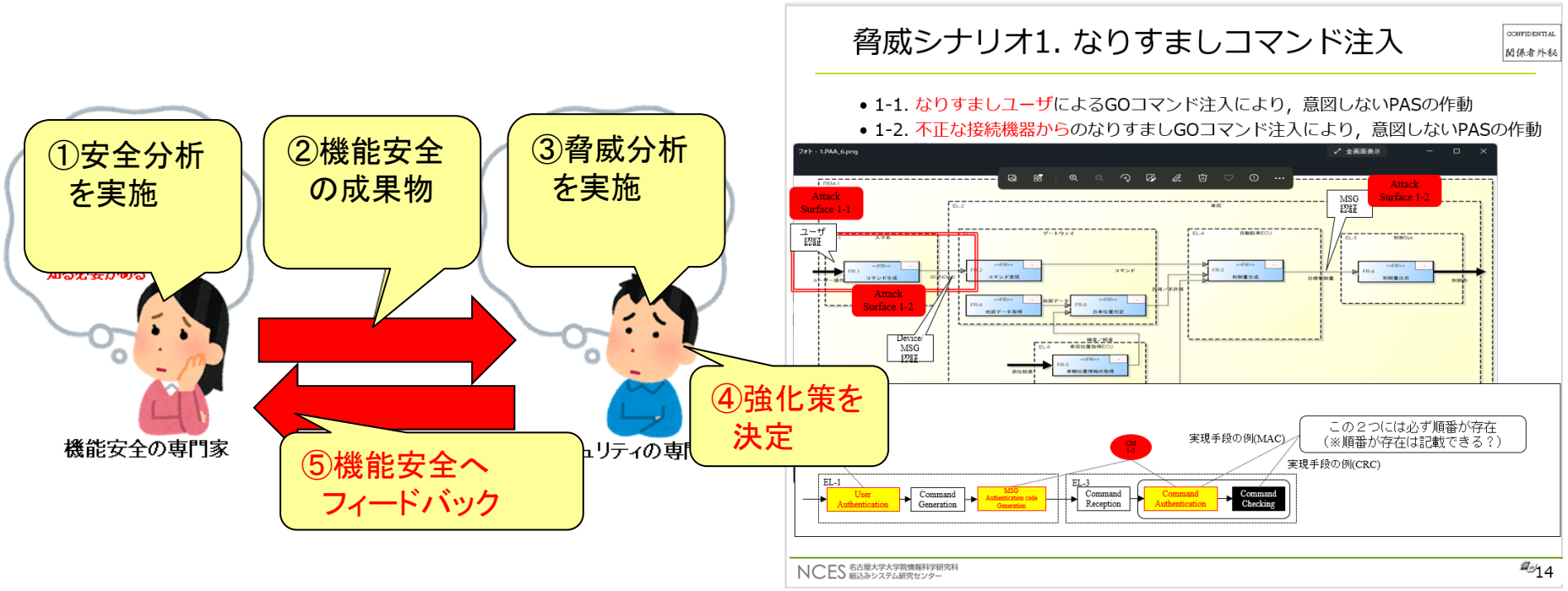
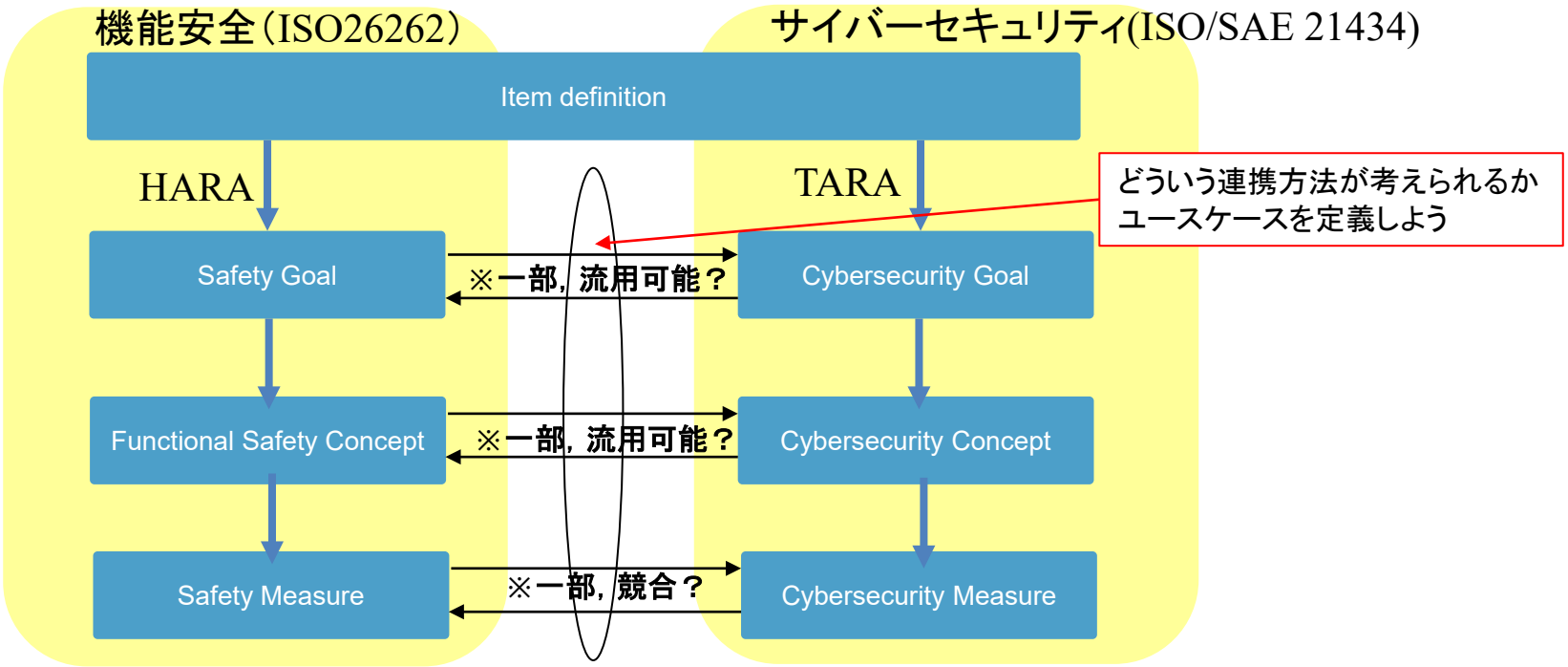


図1. 強化策を導入した場合の事例

セキュリティ要求が安全要求に影響を与える可能性がある

議論1. 機能安全とサイバーセキュリティの連携プロセス

- 機能安全（ISO26262）側から提供される成果物
  - セーフティゴール，機能安全コンセプト，セーフティメジャー
- サイバーセキュリティ(ISO/SAE 21434）側から提供される成果物
  - サイバーセキュリティゴール，サイバーセキュリティコンセプト，サイバーセキュリティメジャ



HARA: Hazard Analysis and Risk assessment
TARA: Threat Analysis and Risk assessment

議論2. Concept Phaseで取り扱うべき抽象度(粒度)

- 抽象的に議論したい機能安全 vs 具体的に議論したいサイバーセキュリティ
  - 落としどころが必要ではないか？
  - 適切な抽象度を議論中
    - ― 脅威や強化策の抽象度を議論

表1. Concept Phaseで取り扱うべき抽象度(粒度)

分類	システムの抽象度	機能安全のConcept Phase	サイバーセキュリティのConcept Phase
論理的	サービス，機能	○	○
	システム/サブシステム	○	○
具体的	デバイス/ECU	×	△(※1)
	コンポーネント	×	△(※1)
	インタフェース	×	△(※1)
	プロトコル	×	△(※1)

高い(抽象的)
抽象度
低い(具体的)

どういう抽象度で取り込むか？

・脆弱性
・攻撃方法
・強化技術

多層防御
➡ Defense in depth

脅威分析(＝セキュリティの性質)

脆弱性(＝機器に)

(※1) 脆弱性やCountermeasureと関連

3. 最後に

- セキュリティSWGでは，SCDLのサイバーセキュリティでの活用法を検討
- 脅威分析事例を通じて，安全分析と比較し違いの明確化を議論中

➡ **自動車のサイバーセキュリティにおけるベストプラクティスを目指す**

- 皆様へのお願い事項
  - 是非，セキュリティに興味がある方はセキュリティSWGにもご参加下さい．
  - たまに顔を出す程度のオブザーバ参加も歓迎いたします

本内容に関するお問い合わせはどうぞお気軽に．

scdlsec@scn-sg.com