ASAM SCDL Security Extension

Ryo Kurachi – Nagoya University

30. Juni 2022

Note that this presentation includes current forecast based on the author's individual research.

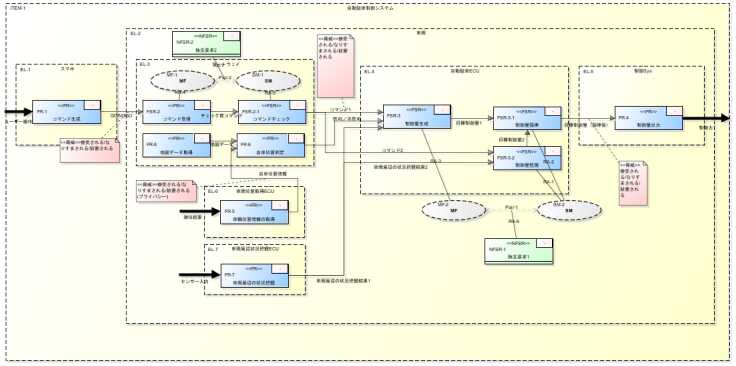
ASAM Association for Standardization of Automation and Measuring Systems

The activities of the Security Sub-Working in SCDL

[1] Kenji Taguchi, Ryo Kurachi, Kiyoshi Sasaki, Nobuhiko Nakamura, Kazuki Tomonaga, Shuhei Yamashita, “Threat Analysis Framework for Safety Architectures in SCDL”, The 39th International Conference on Computer Safety, Reliability and Security (SafeComp 2020), Sep 2020.

- Objective of this working
  - To study security domains of SCDL deliverables which gets from the functional safety domains.

- Current activities:
  - **<u>Activity1) Can SCDL be used for security activities (threat analysis) ?</u>**
    - Based on SAFECOMP 2020 paper[1], this paper focuses on to identify the issues of SCDL in security engineering.
    - This paper pointed out the SCDL **handling safety issues within the security domain**.
  - **<u>Activity 2) Define of the usecase for functional safety and security activity process</u>**
    - Started from FY 2022. This is collaborative project with ASAM.



SCDL from Safety domain

Input from safety domains

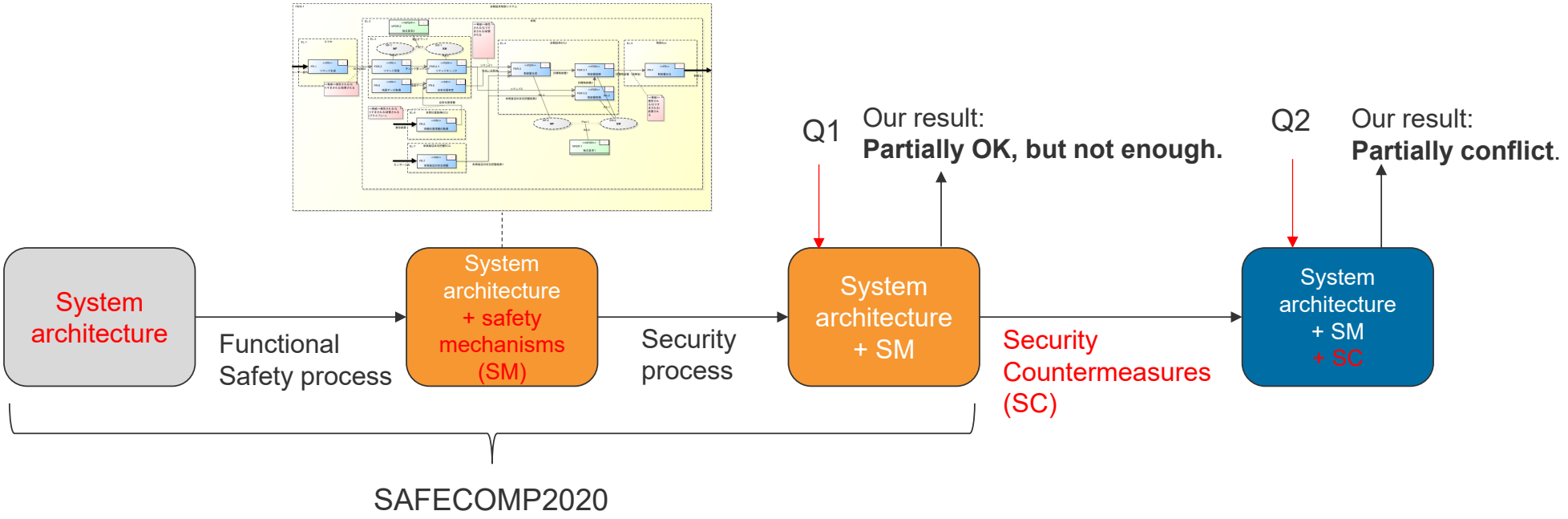
Security activities input the SCDL to identify the assets and threats.

Security domain

Handling safety issues within the security domain

From the system architecture point of view

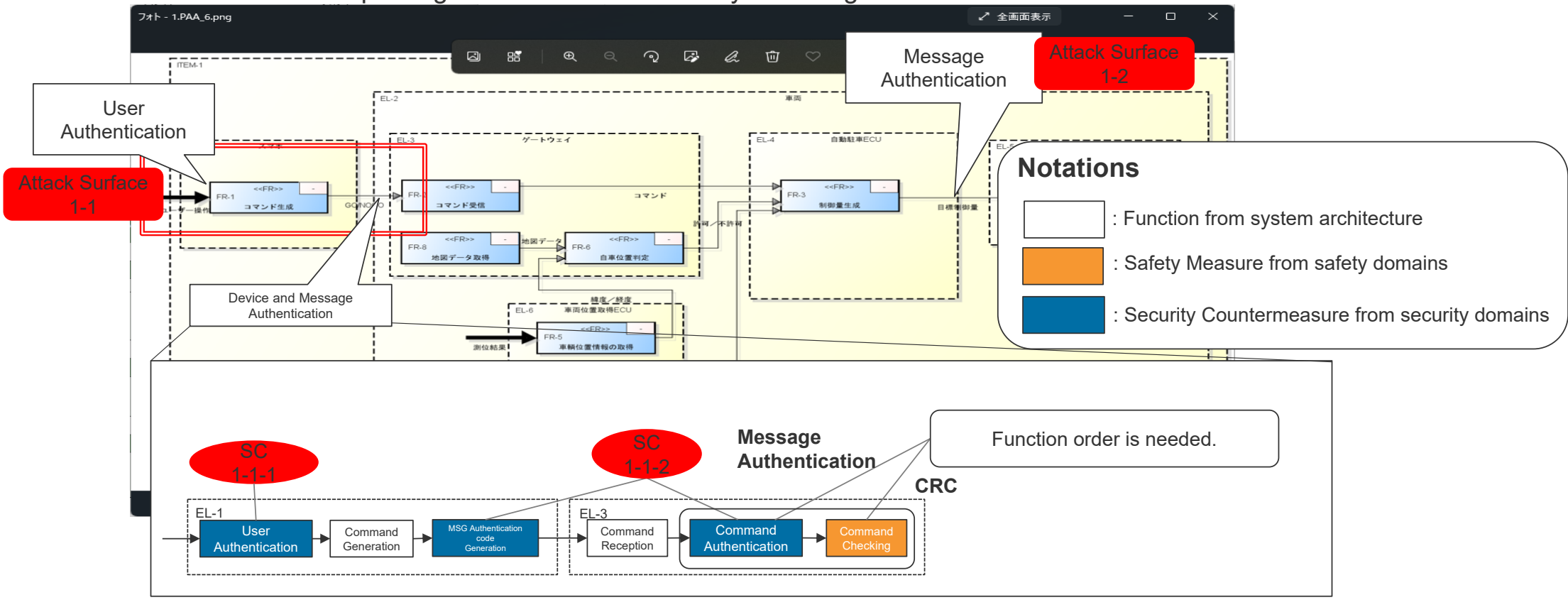
- **Q1. Does the safety mechanism (SM) become countermeasure to the threat?**
  - Our result for Q1 : Partially OK but not enough.
- **Q2. Do safety mechanisms (SM) and security countermeasures (SC) conflict?**
  - Our result for Q2 : Partially conflict.



Handling safety issues within the security domain

From the system architecture point of view

- Attack scenario 1-1. Spoofing of GO command by malicious user.
- Attack scenario 1-2. Spoofing of several commands by attaching unauthorized devices.

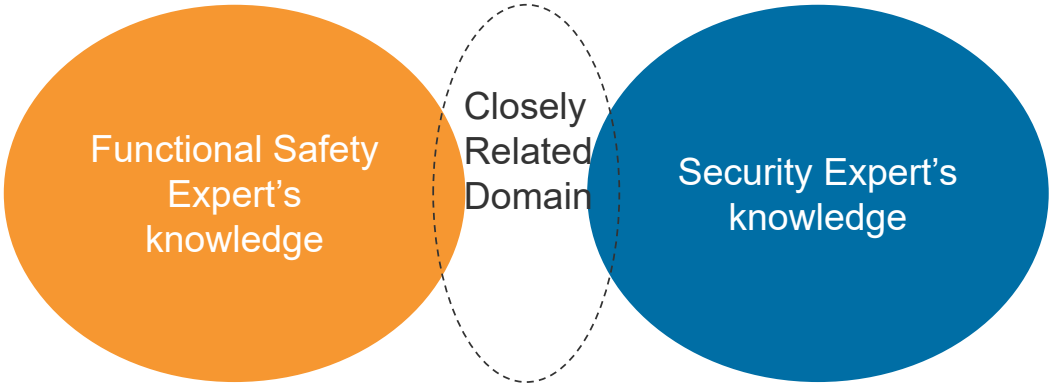


Handling safety issues within the security domain

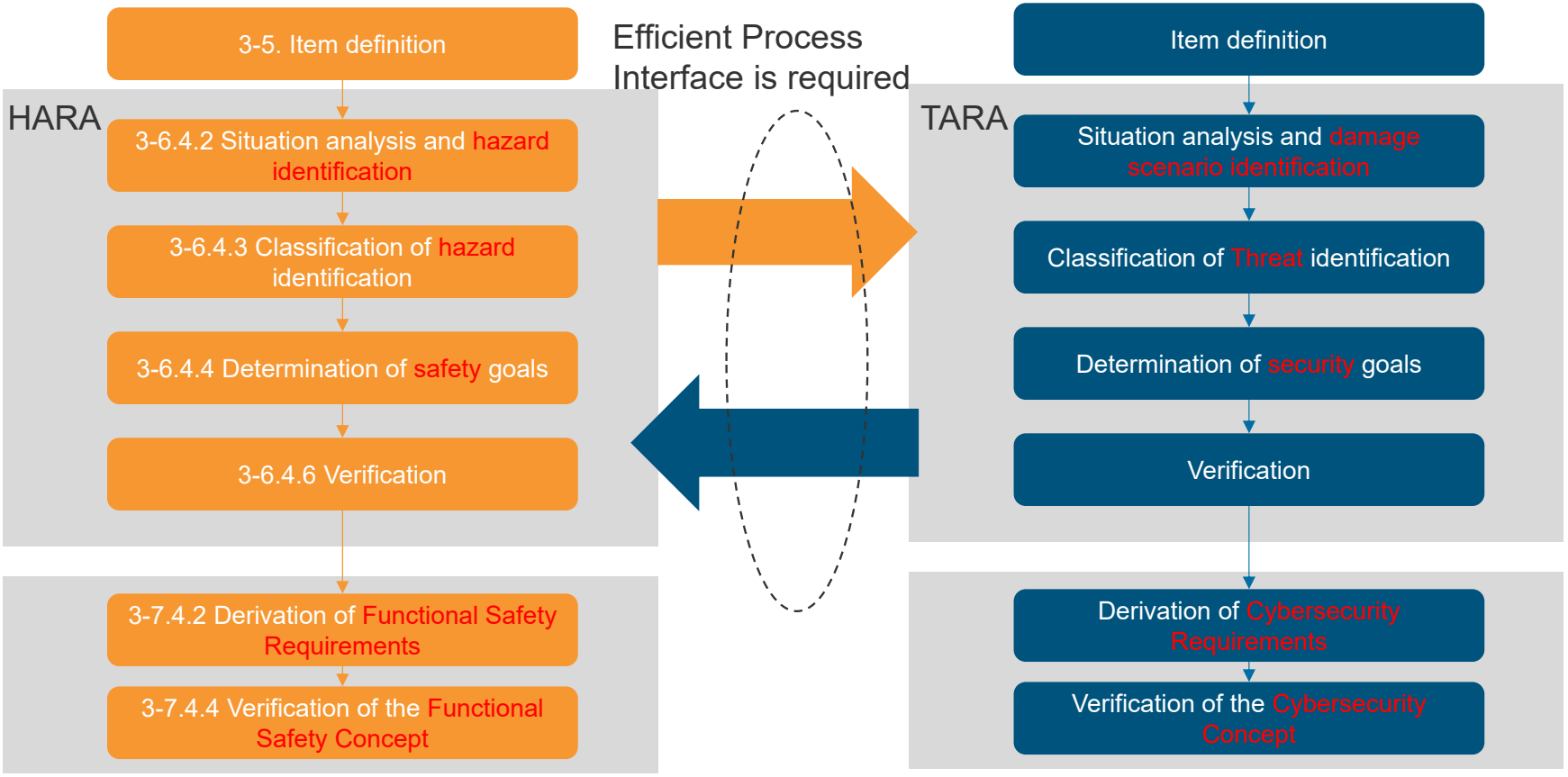
From the process domain point of view

- Safety Experts' knowledge required for HARA and Safety Concepts
- Security Experts' Knowledge required for TARA and Security Concepts
  -> Closely related domains, but the following differences:
  - Difference 1. Classical security rarely handles safety.
  - Difference 2. A single expert cannot handle both domains.

- What is needed:
  - Integration and combination of safety and security in the automotive industry
    -> How to integrate the safety and security domain process.



Safety and Security risk management workflows



Safety domain Process (from ISO26262)

Security domain Process (similar to ISO26262)

Requirement / Idea of Process Interfaces

- Requirements of the process interfaces.
  - For designing safe and secure products the safety and the security domain need to inform each other about their planned measures. Additionally, synergies between both domains make life easier
    -> We hope to define mandatory and beneficial process interfaces between both domains

- Our Idea of Process Interfaces.
  - Map to translate the safety and security deliverables.
    - SCDL becomes one of the process interfaces.

Safety deliverables	Security deliverables
Safety goal (*)	Security assets (**)
Violation of safety goal	One of the Security goals (**)
Hazard (*)	Damage scenario (**)
Safety measure (*)	Risk mitigation of damage scenario

(*) SCDL already can cover them.
(**) SCDL will be able to cover them.

Summary

- In order to design a safe and secure system a close cooperation of both domains is necessary.
- Currently, we discuss the idea of the process interfaces.

- We need to
  - Share information, especially concepts
  - Analyze this information with our own idea and methods
  - Align our concept and usecase
  - Deal with bidirectional translation between safety and security deliverables with SCDL and vice versa

- If you have some interests, please keep in touch with us !

scdlsec@scn-sg.com

Since we have just started, I apologize for the short introduction.