SCDL
Safety Concept Description Language

Concept project proposal for SCDL Next Gen.

Akira Takada
SCN-SG
Security SWG, SOTIF SWG, SCDL SA Draft team

March 21st, 2023

ASAM
Association for Standardization of
Automation and Measuring Systems

About myself: Akira Takada, DNV Business Assurance Japan

DNV

Functional safety Expert in Safety & Security dept.

- ISO 26262 training program coordinator, trainer, technical advisor and assessor of various E/E/PE systems in automotive industry
- Member of SCN-SG, SOTIF sub-working group, Security sub-working group

Experience

- FuSa development of chassis systems (steering systems, brake systems…), body electronic systems (lighting systems, airbags…)
- Development of company standard for FuSa
- Participation to Society of Automotive Engineers of Japan (JSAE) activities for ISO/TC22/SC3/WG16 and to Japan Automotive Manufacturers Association (JAMA) activities for drafting official interpretation of ISO 26262
- ISO 26262 training trainer, technical advisor and assessor
- EMC certification test project engineer

Previous positions

- Nissan Motors: Functional safety engineer
- TÜV Rheinland Japan: Functional safety engineer, EMC Project engineer

Agenda

1	ASAM SCDL 1.6.0
2	Three safety and security standards era
3	Motivations for SCDL evolution
4	Current situation of discussions regarding SCDL Next Gen.
5	Proposal for concept project

ASAM SCDL 1.6.0

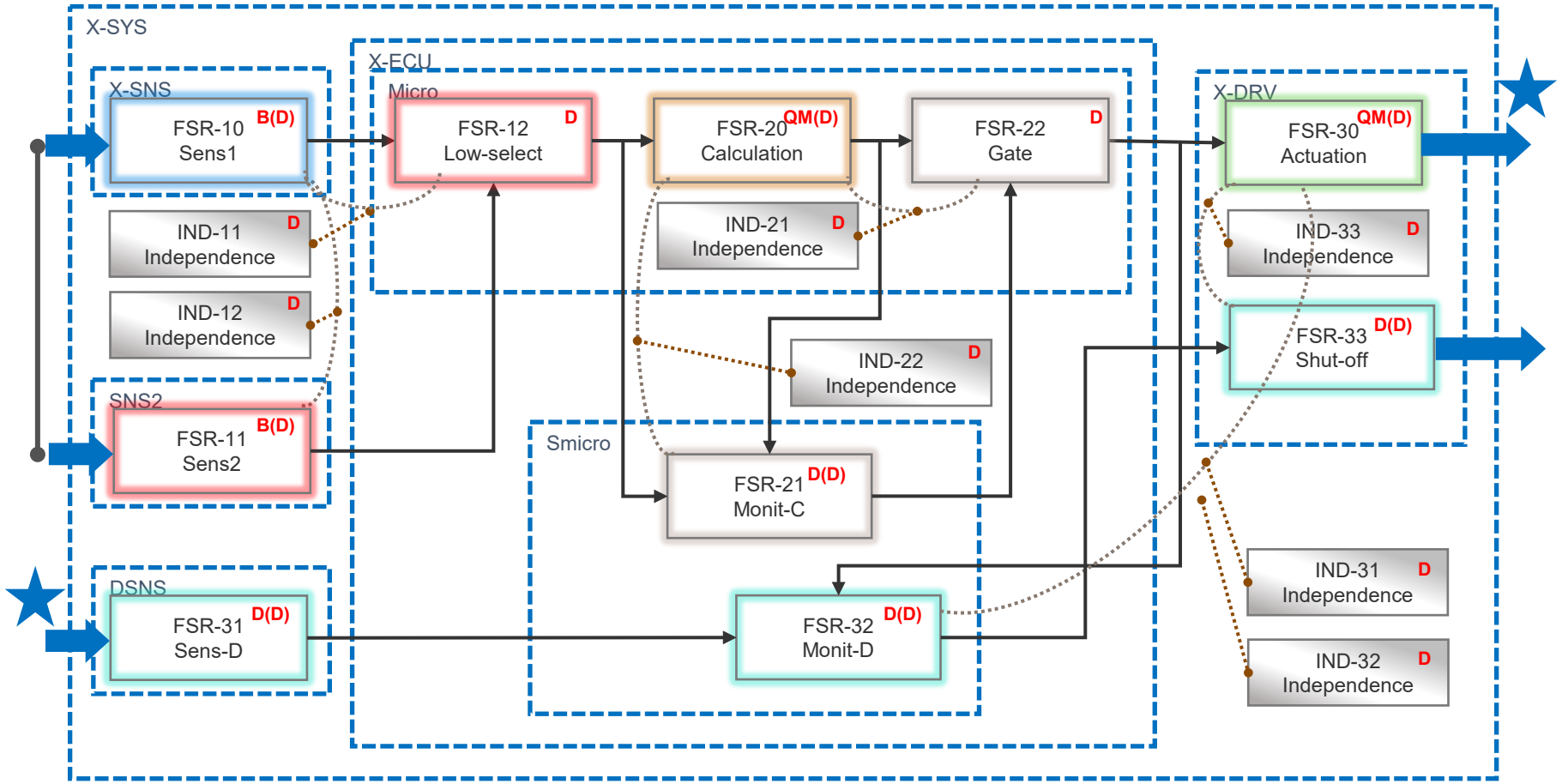
SCDL
Safety Concept
Description Language

- ASAM Standard SCDL 1.6.0 :2021, dedicated to notation of safety concept, which is a most important WP of ISO 26262, is published
- SCDL is well used in actual FuSa development field

ASAM

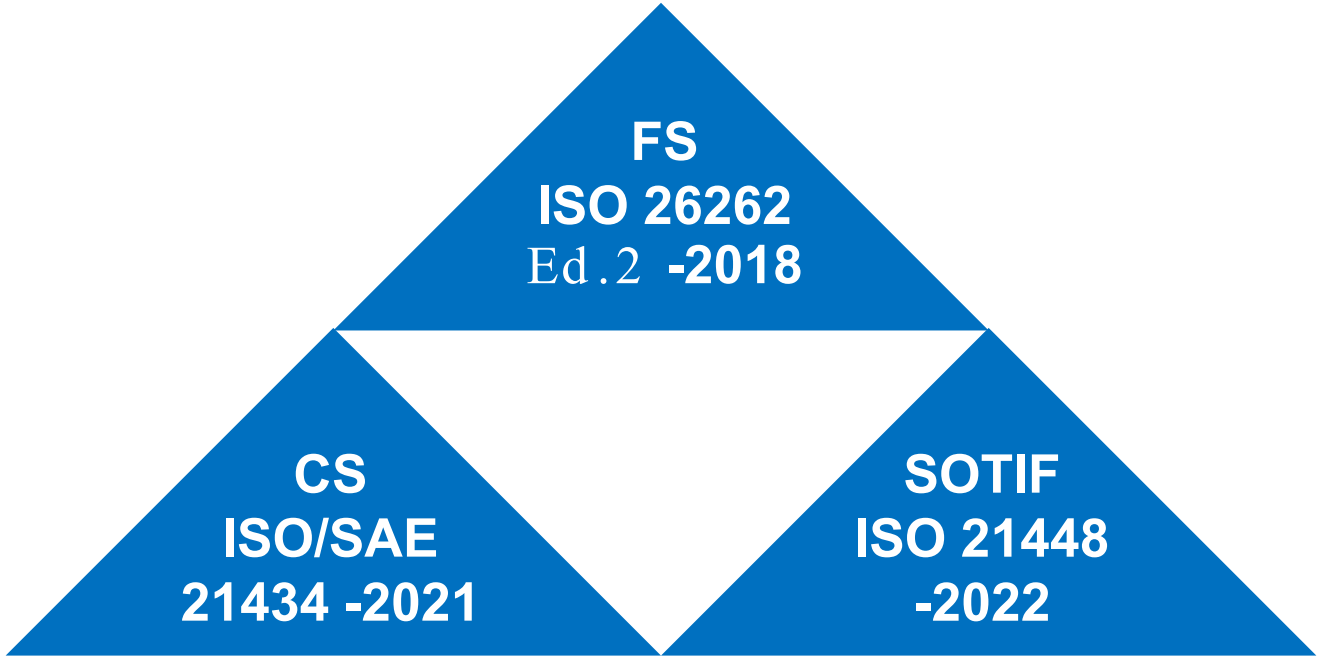
Example of FSC based on ASAM SCDL 1.6.0

Example of SCDL description of Functional Safety Concept in ISO 26262:



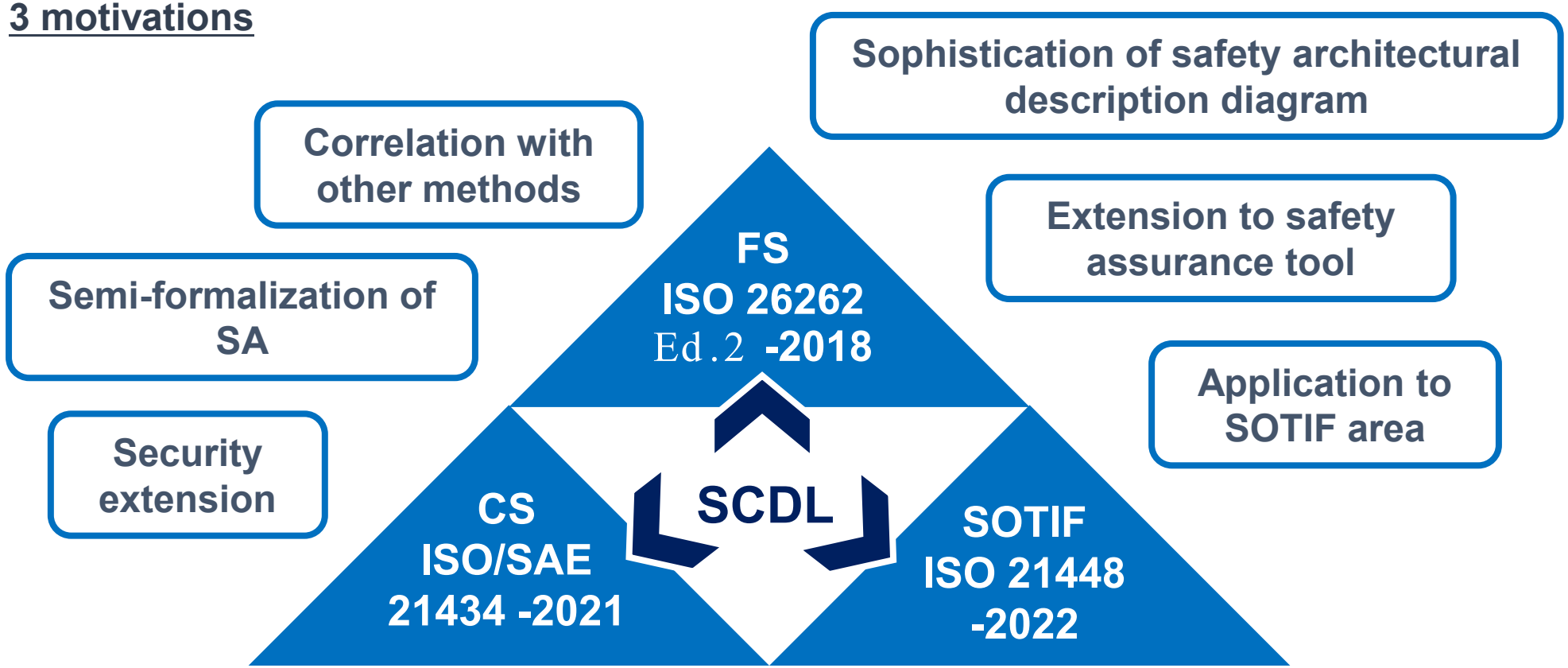
Three safety and security standards era has come

- 3 major safety related standards for automotive electrical control systems are existing since 2022
- Since all 3 standards are closely related each other, implementing all of them to control system development within efficient and effective correlation is necessary



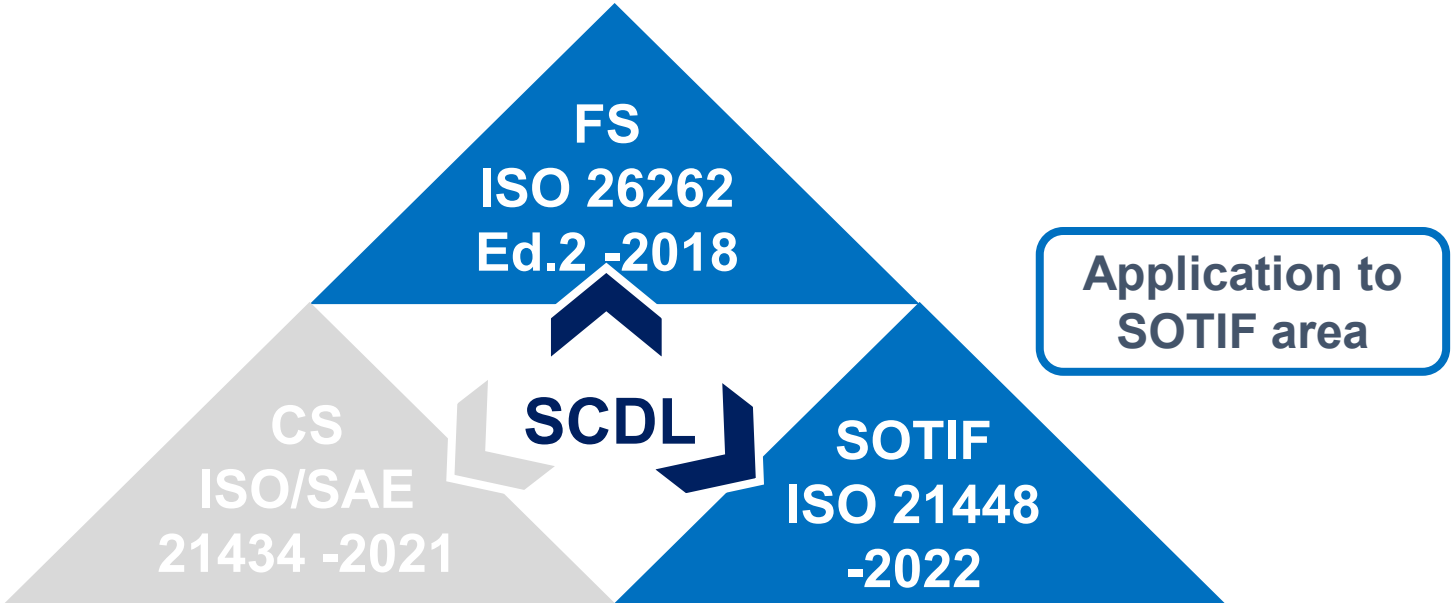
Discussions regarding evolution of SCDL to adapt to 3 standards era

- Necessity of SCDL extension considering 3 safety standards are started to point out
- Demands to increase SCDL practicality are also increasing
  - 3 motivations



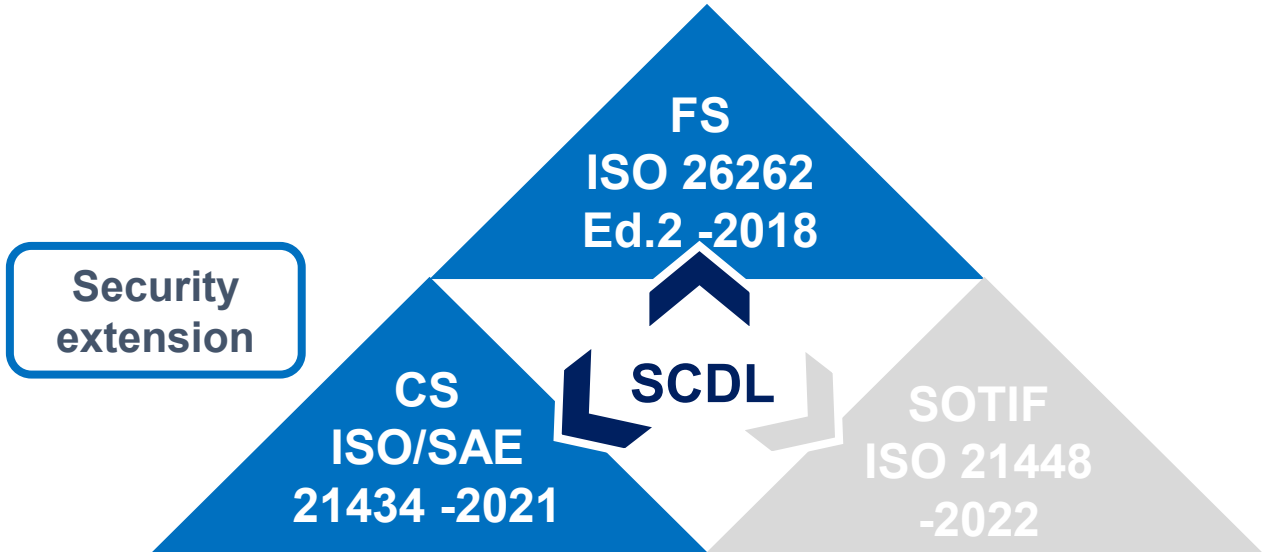
Motivation to evolve SCDL #1

- Expand SCDL application to SOTIF area
- The result of intended functionality (IF) development based on ISO 21448 is provided to item definition specified in ISO 26262. Utilization of SCDL to architectural description during SOTIF activity can support effective and efficient implementation of both standards to actual system development.



Motivation to evolve SCDL #2

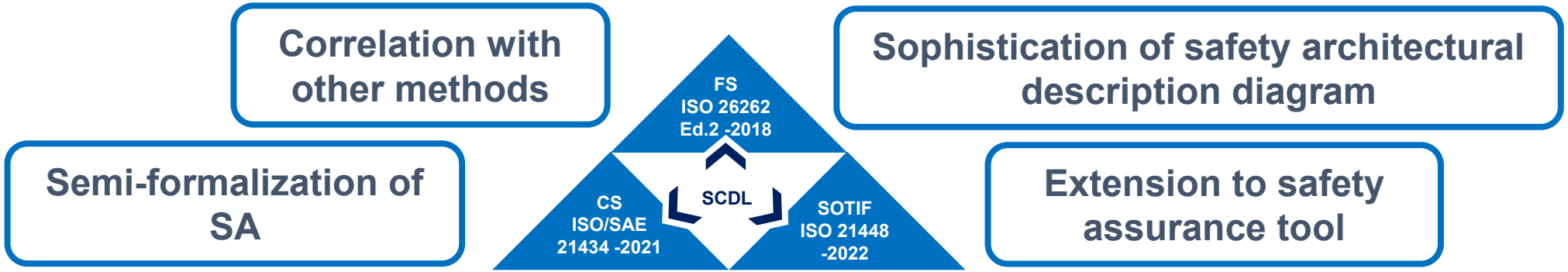
- Extension to CS area
- In ISO 21434, information, function, and physical assets which could be the target to threat shall be identified and their risks shall be analyzed and treated. It is already reported that application of SCDL to threat analysis from safety point of view is effective; but potentials for further extension of SCDL are pointed out in order to correlate both standards more effectively.



Motivation to evolve SCDL #3

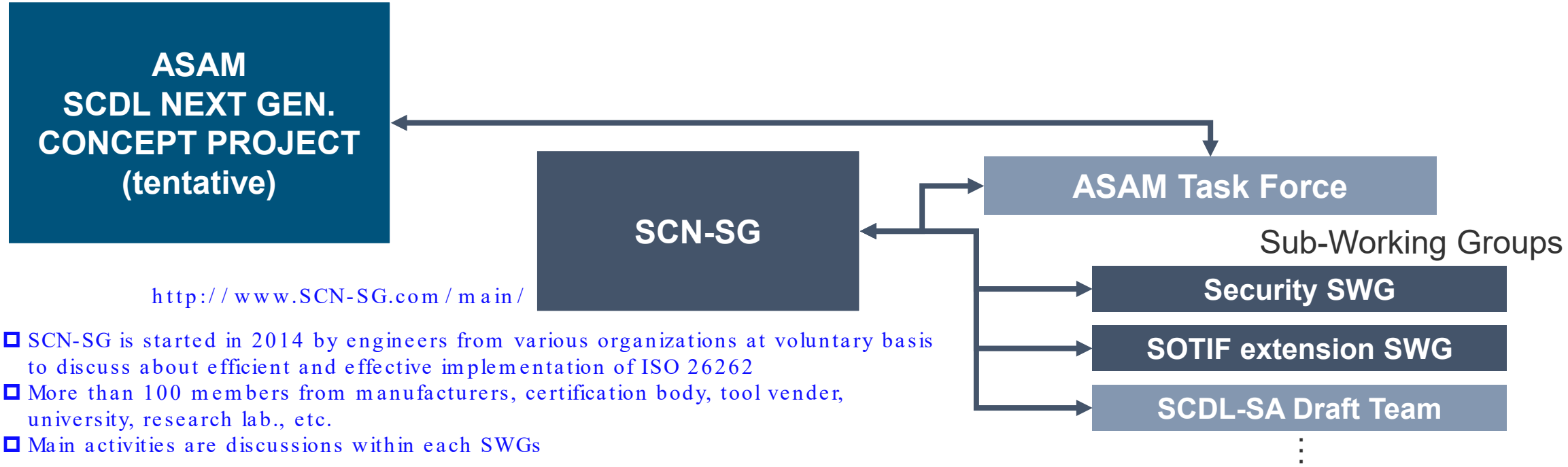
- Increase practicality of present SCDL
- Number of SRs of safety architecture through out TSC to HW/SW development phases could be up to few hundreds. In order to handle SRs/ELEs/Decomps/Coexs/SAs/DFAs adequately under this circumstance, further sophistication of SCDL is necessary.
- Since clear safety arguments are demanded in 3 standards era, the role as supporting tool to develop these safety arguments is getting more important

SR: Safety Requirement
ELE: Element
Decomp: Decomposition
Coex: Coexistence
SA: Safety Analysis
DFA: Dependent Failure Analysis



Current situation of discussions regarding SCDL NEXT GEN.

- Discussion for the SCDL next generation is started under voluntary organization SCN-SG, which is a group introduced basis of ASAM standard SCDL 1.6.0
- We would like to put together the concept for SCDL next generation based on result of SG discussions

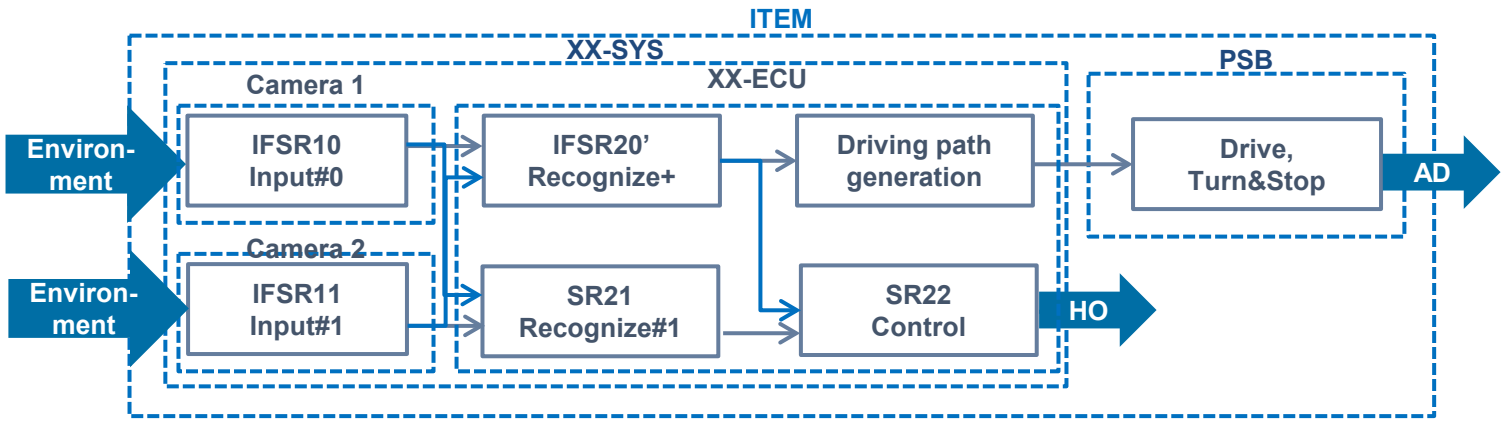


http://www.SCN-SG.com/main/

- SCN-SG is started in 2014 by engineers from various organizations at voluntary basis to discuss about efficient and effective implementation of ISO 26262
- More than 100 members from manufacturers, certification body, tool vender, university, research lab., etc.
- Main activities are discussions within each SWGs

Current situation of discussions regarding expansion of SCDL application to SOTIF area

- Case study of SCDL application to analysis of functional insufficiencies and consideration of measures to improve IFs is on going. Additionally, by using this output as item definition of FuSa, example of functional safety analysis and specification of safety mechanisms is also under discussion simultaneously.
- Within this case study, potentials for extending SCDL, such as expression of functional requirements regarding functional performance, process requirements regarding IF development, and expression of various kind of analyses, are under discussion.



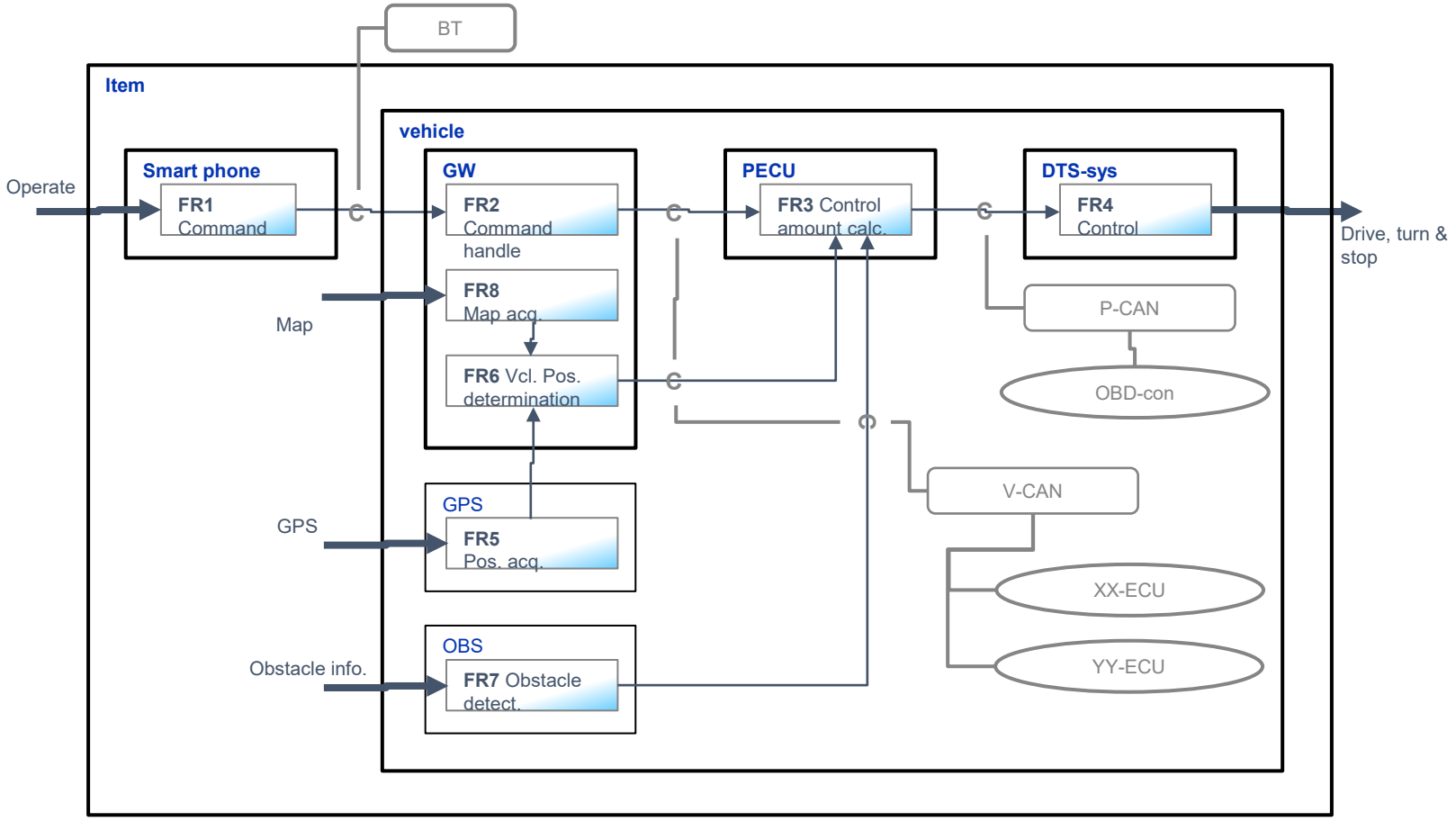
Current situation of discussions regarding SCDL extension to CS area

- It is already verified that SCDL is useful method for safety architectural description within the scope of providing precise expression of cyber attack object for threat analysis (Safe comp 2020*)
- Concerns regarding system architecture in CS discussion are not limited to SRs structure and result of their allocations to ELEs. For example, additional description method of information necessary for various analyses such as connections to external systems which could lead to vulnerability of the system, is already under discussion
- In addition, since many of CS mechanisms are objects of FuSa analysis and measures, verification of capability of present SCDL to handle these aspects is on going

*Safe comp 2020: 39th International Conference on Computer Safety, Reliability and Security
Threat analysis framework for safety architectures in SCDL by Kenji Taguchi (CAV)
:https://www.slideshare.net/KenjiTaguchi/2020-safecompsep18

Current situation of discussion of SCDL extension to CS area

- Example of description of connections to external systems which could lead to vulnerability of the system

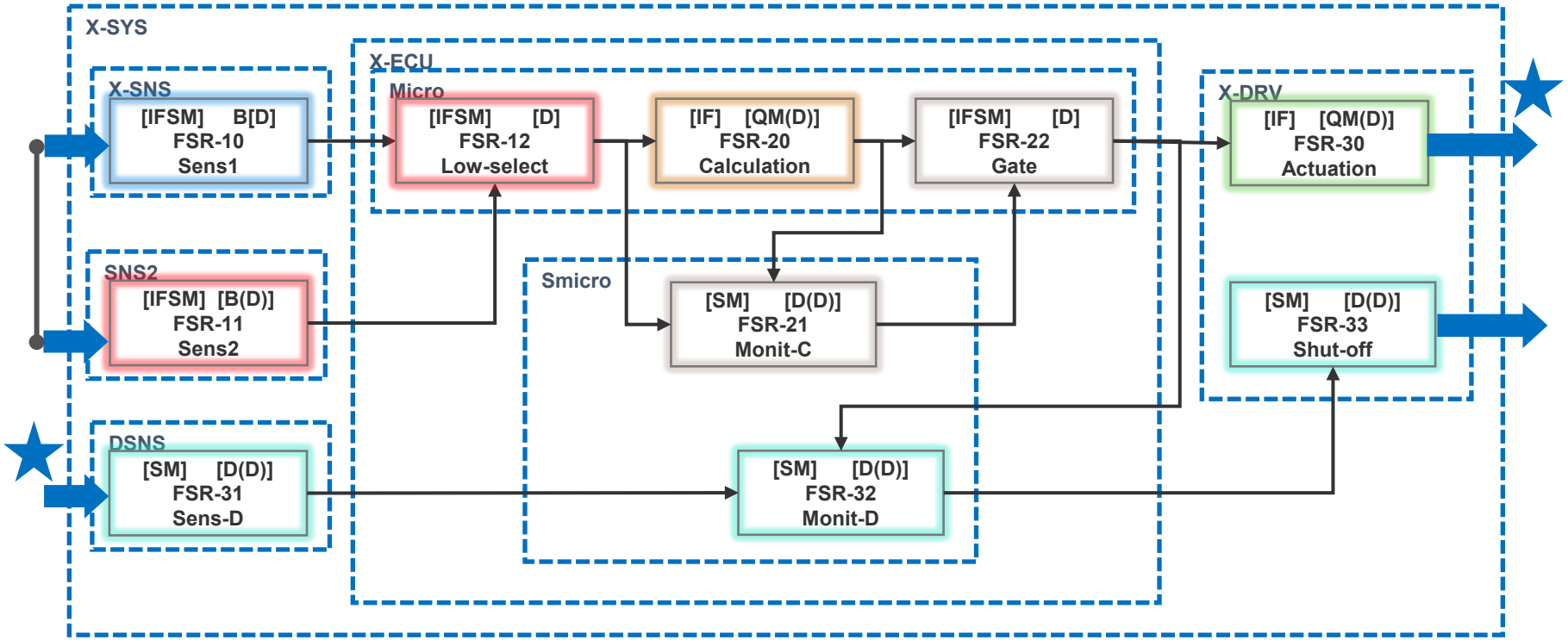


Current situation of discussions regarding increasing practicality of present SCDL

- Further sophistication of description method to manage large number of safety goals and SRs of large scale system and attempt to semi-formalize SAs to combine architecture and result of its SAs effectively are started
- In addition, since clear safety arguments are demanded in 3 standards era, the role as supporting tool to develop these safety arguments is getting more important. Further updates from this point of view are also under consideration.

Current situation of discussion of increasing practicality of present SCDL

Example of FSC



Proposal for concept project

- We would like to propose to start ASAM SCDL Next Generation Concept Project to discuss the concept for SCDL next gen. based on the present discussions within SCN-SG
- Candidates for project work packages are follows:

  WP1: Security extension

  WP2: SOTIF extension

  WP3: SCDL-SA

  …
- To have ideas from wider point of view, we would hope to have participants from various organizations around the world

Time schedule

Time schedule is shown in the table below:

When	Item	Task
Until 2023/4/End	Specification of the content of each WPs of Project Proposal	Preparation of Motivation, Use case, Technical Contents within each WPs
Week of 2023/5/29	Hold Proposal Workshop	Discuss and determine the content based on Project Proposal draft *ASAM members are welcome to join
2023/7(tentative)	TSC Meeting	Participation to the TSC meeting and explanation of the project by submitter
2023/8～2024/1	Concept Paper specification	Drafting SCDL Next Generation Concept Paper within each WPs
TBD (around 2024/3 to 4)	TSC Meeting	Participation to the TSC meeting and explanation of Concept Paper by Project Leader

We are looking forward to see you in the concept project!

Thank you for your attention