セミフォーマル記述としてのSCDLの体験 An Experience of SCDL as semiformal notation

ミュンヘンワークショップ向け課題

Material for ASAM workshop in Munich

5th September 2018

Problem for the WS

Question:

How and what do you describe SR Specification and SC for the given system and SA?

SR : Safety Requirement
SC : Safety Concept
SA : Safety Analysis

Exercise:

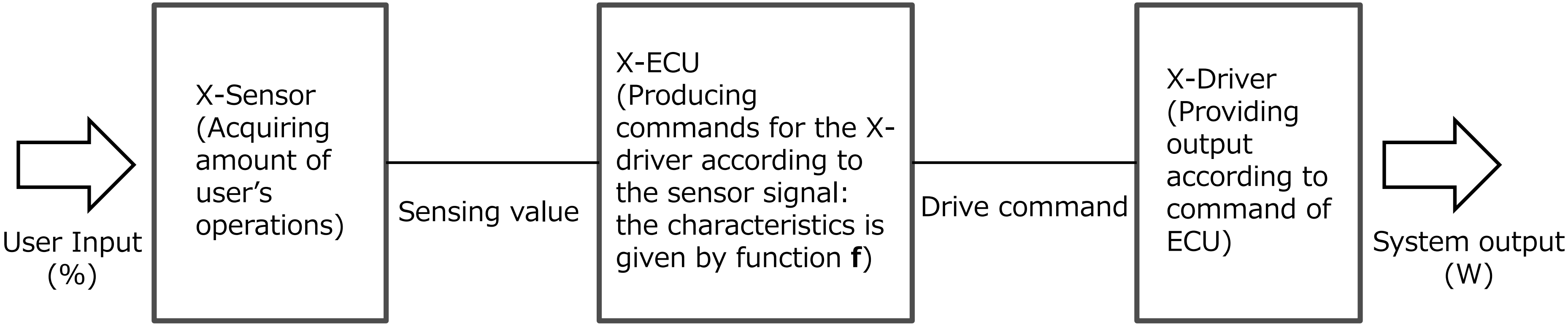
Please present them by using your most familiar methods or languages which can be recognized as semi-formal.

Item Definition

Item Definition including PAA and FC :

- Functionality of System-X: Providing output based on user's input.
- System's structure : consists of three components :
  - Input device : X-Sensor
  - Controller : X-ECU (electronic control unit)
  - Output device : X-Driver

SR : Safety Requirement
SC : Safety Concept
PAA : Preliminary Architectural Assumptions
FC : Functional Concept
ECU : Electronic Control Unit


User Input (%)
X-Sensor (Acquiring amount of user's operations)
Sensing value
X-ECU (Producing commands for the X-driver according to the sensor signal: the characteristics is given by function **f**)
Drive command
X-Driver (Providing output according to command of ECU)
System output (W)

Structure of item (X-system)

X-ECU Characteristic

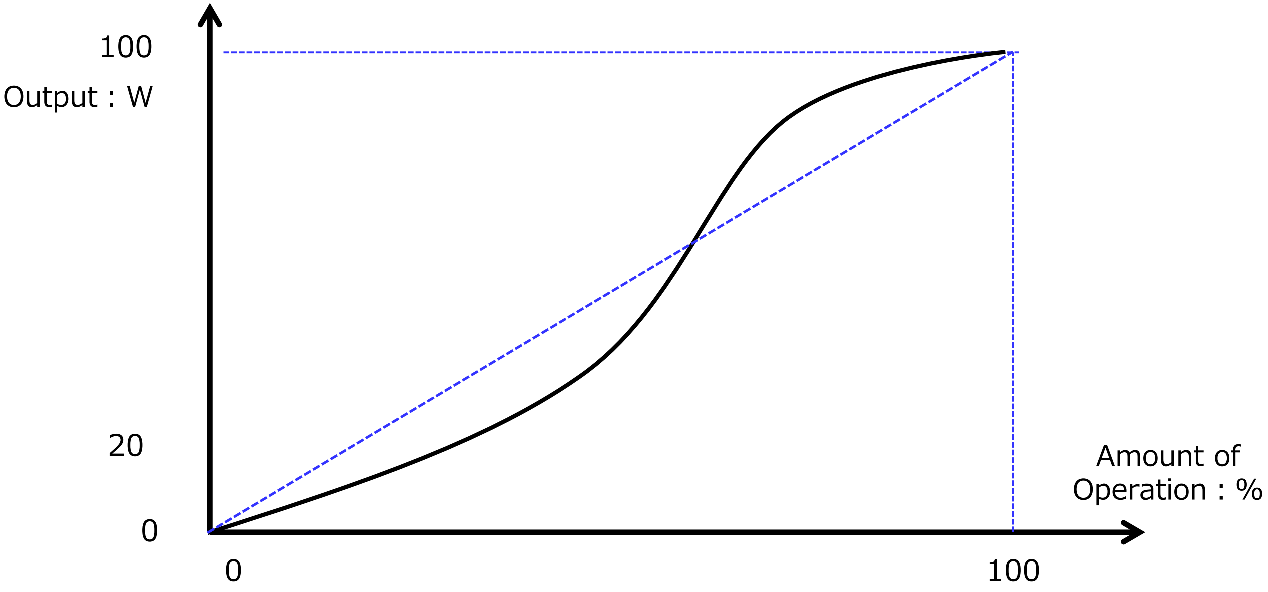
- Output Characteristic:
  - ECU has output characteristic by function **f** as a tuning attribute for improving operability.

ECU : Electronic Control Unit

  - **f** has following characteristics as a monotonically increasing function.

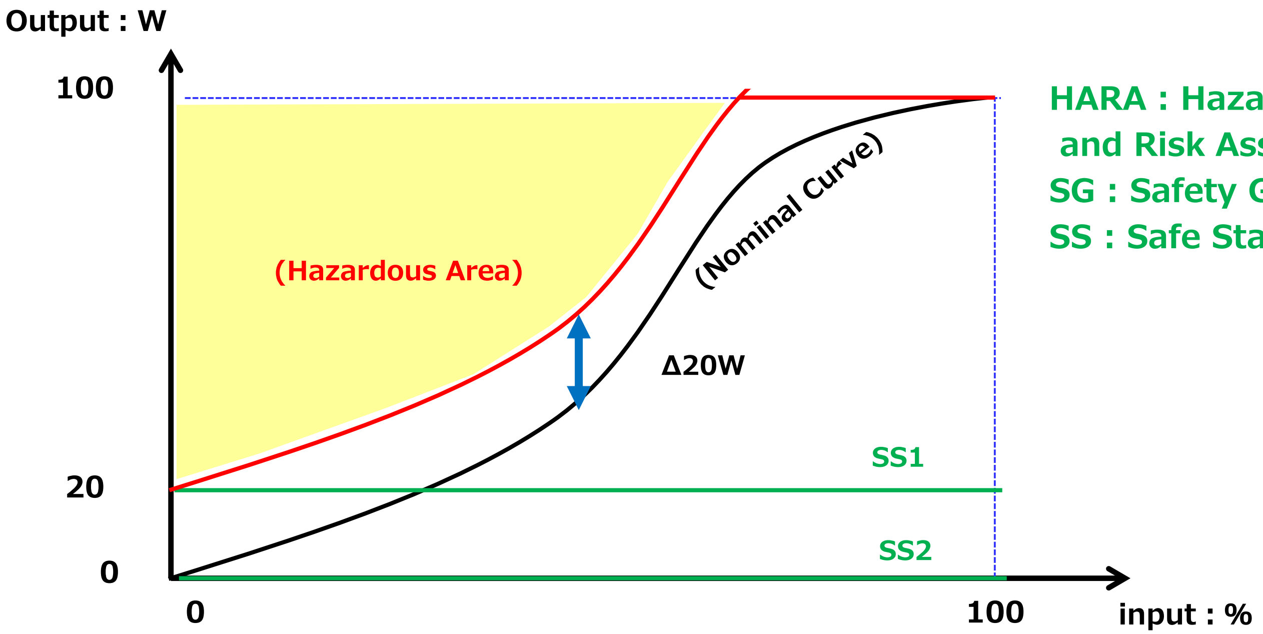
output = f(input) ≒ a x input

f(0) = 0, f(100) = 100



Results of HARA

- Identified hazard : Exceeding the nominal value of system output by +Δ20W.
- Premise : Following SG and ASIL are obtained by HARA regarding the hazard.
- Safety Goal :
  - During operation of the system, output should not exceed the nominal curve by +Δ20W.
  - SS1 : Fixed output in 20W
  - SS2 : Shut off power supply for X-driver (Fixed output in 0W)
  - ASIL-D



HARA : Hazard Analysis and Risk Assessment
SG : Safety Goal
SS : Safe State

Initial SA and SM

- Premise : SMs are defined in following table based on the item definition, SG and other related information.

System components	Functionalities of components	Malfunction which potentially violates SG	Safety Mechanism
Input sensor	Acquiring user's input	Erroneous acquisition of user's input : too high compared with user's intention.	Dual channels + select low (SM-10).
ECU	Driving the output module according to the user's operation.	Erroneous calculation : exceeding nominal values by +Δ20W.	Command value monitoring by additional monitoring processor + controlling function which transitions to SS1 when erroneous value is detected (SM-20).
Output module	Providing output according to command from the ECU	Erroneous output : exceeding nominal values by +Δ20W.	Output monitoring by additional sensor + shut off relay which transitions to SS2 when erroneous output is detected (SM-30).

SA : Safety Analysis

SM : Safety Mechanism

SG : Safety Goal

SS : Safe State

ECU : Electronic Control Unit

Solution

Solution for the Task with SCDL

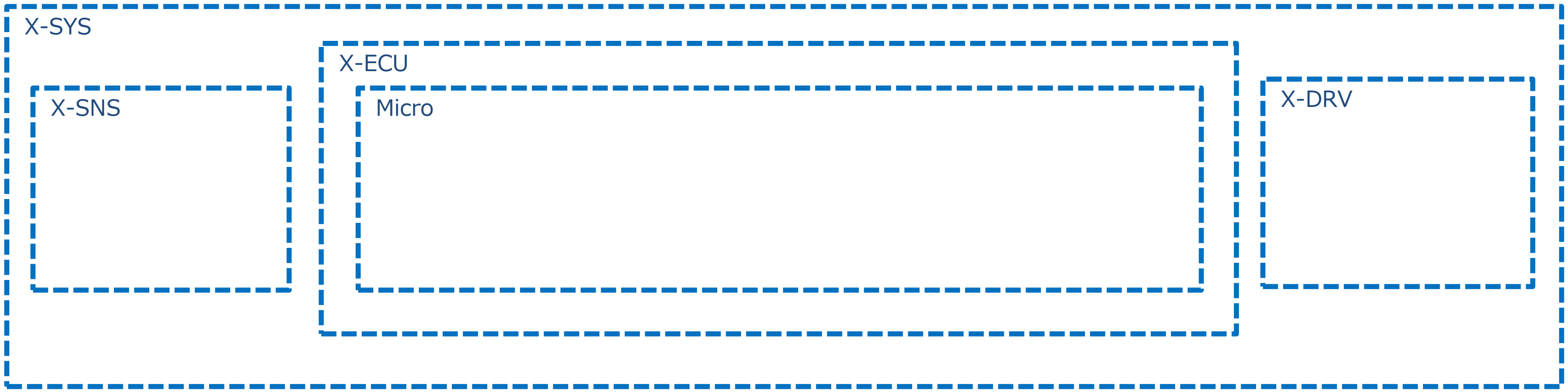
Notice:
The answer is only one example for the question: approaches, processes and every steps we took as well.
It’s including suggestion for effective SCDL usages.

Plot:
- Item definition is done in SCDL.
- Safety analysis is also done in SRVA manner.
- SR derivation and decomposition are performed for each SM.
- All SMs are merged into one architecture which is resulting FSC for the system.
- Related SR Table and Element Table are also finalized.

SR : Safety Requirement
SRVA : SR Violation Analysis
SM : Safety Mechanism
FSC : Functional Safety Concept

Item Definition (in SCDL)

Element Architecture of the Item



Item Definition (Element table)

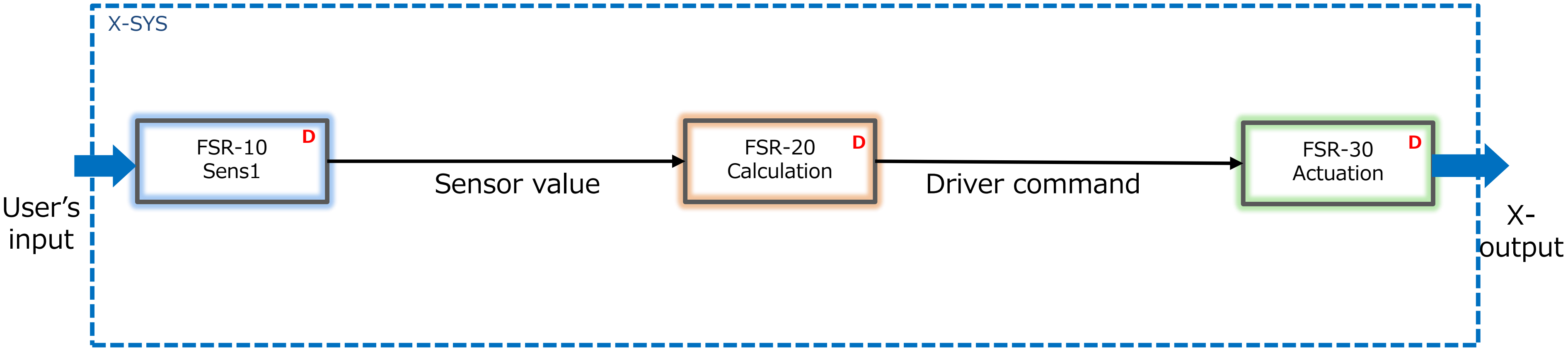
Element Specifications

ID	Short Name	Details / Spec.	ASIL
ITEM-00	X-system	Automotive on-board system which provides X function	D
EL-10	X-SNS	Input device for X-system which acquire user’s operation	TBD
EL-20	X-ECU	ECU for X-system	TBD
EL-21	Micro	Main micro controller implemented in X-ECU	TBD
EL-30	X-DRV	Output device for X-system	TBD

TBD : To Be Determined

Item Definition (in SCDL)

SR Structure for the Item



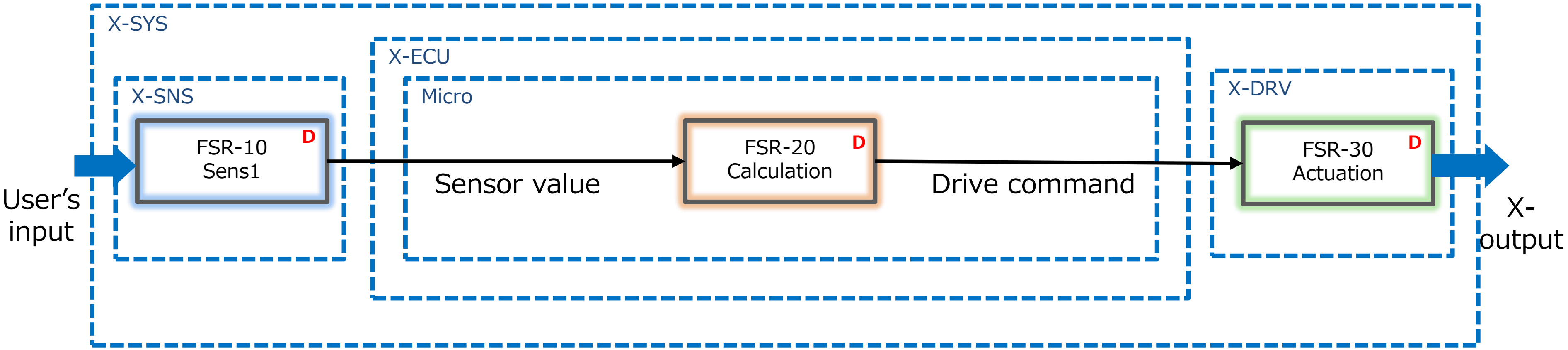
Item Definition (SR table)

Safety Requirement (for Intended Functionality)

SR ID / short name	SR in Natural Language	ASIL	input	output	allocation
FSR-10 / sensing	Acquire driver's input	D	User's input	Sensor value	X-sens
FSR-20 / calculation	Calculate amount of output	D	Sensor value	Drive command	X-ECU
FSR-30 / actuation	Drive actuator	D	Drive command	X-output	X-driver

Item Definition (in SCDL)

Functional Concept of the Item



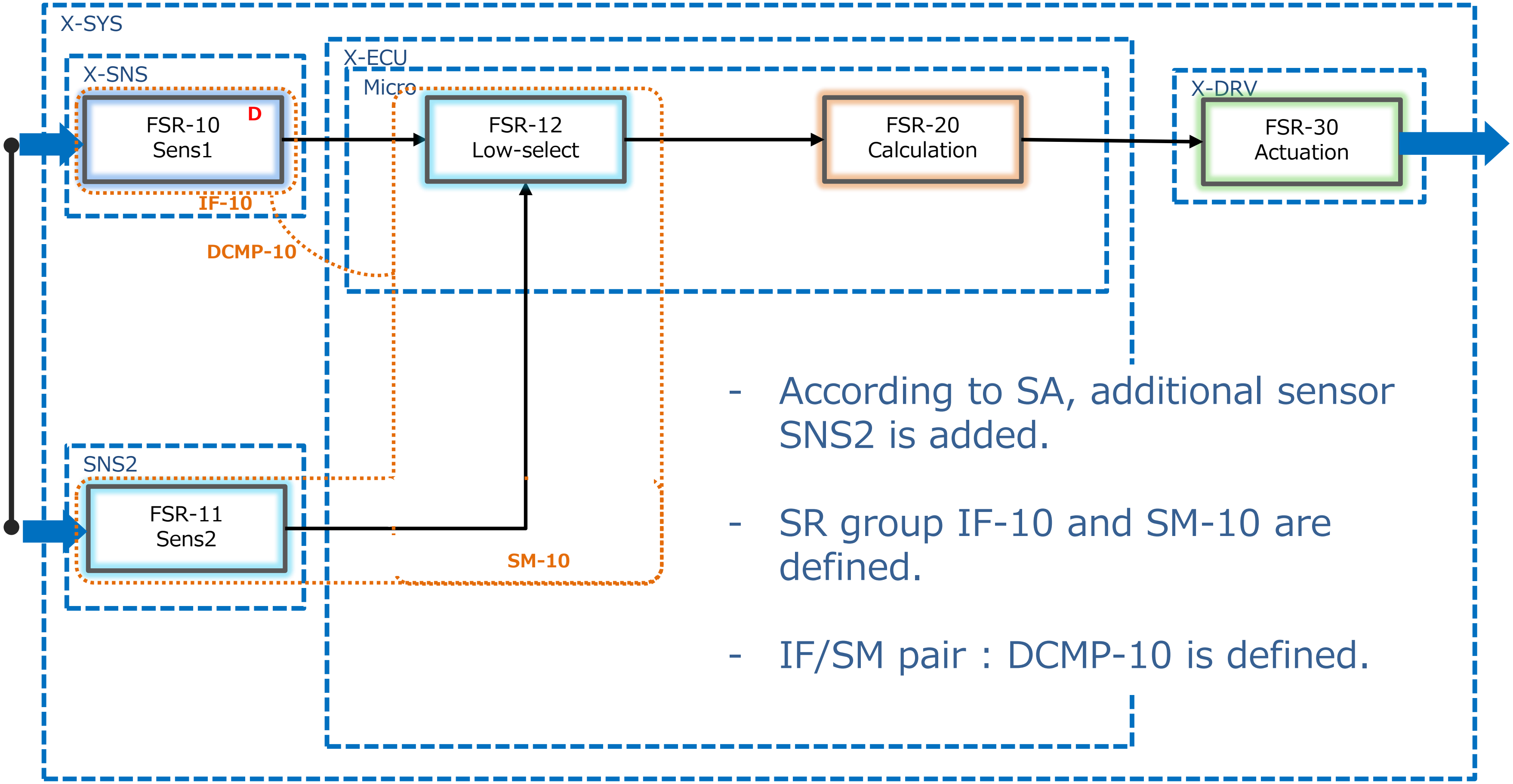
Safety Analysis (Item level)

SRVA on the Intended Functionality of X-system

SR	SR in NL	Possible SRV mode regarding intended functionality which has potential to lead SGV.	Safety measures / Safety mechanisms **(ID)**
FSR-10 / sensing	Acquire driver's operation	Erroneous sensing : too high	Dual channel solution for sensor architecture **(SM-10)**
FSR-20 / calculation	Calculate amount of output	Erroneous calculation : exceeding by +Δ20W.	Online monitoring of calculated value by sub-micro: if erroneous result is detected the value is substituted by fixed one **(SM-20)**
FSR-30 / actuation	Drive actuator	Erroneous output by +Δ20W.	Output monitoring by additional sensor : in case of erroneous output power supply for X-driver is shut off **(SM-30)**

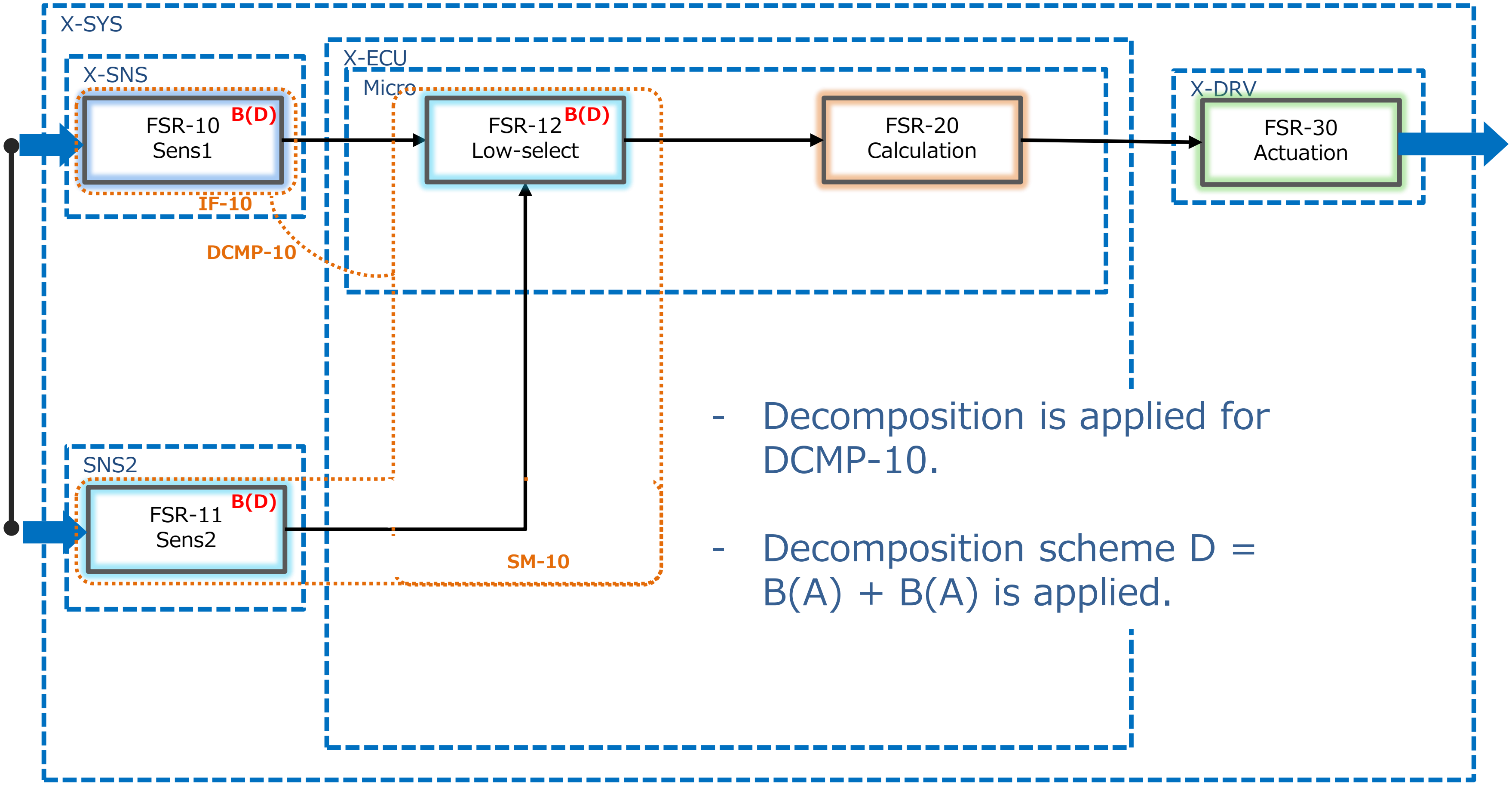
SM-10

Consideration on SM-10



- According to SA, additional sensor SNS2 is added.
- SR group IF-10 and SM-10 are defined.
- IF/SM pair : DCMP-10 is defined.

Consideration on SM-10



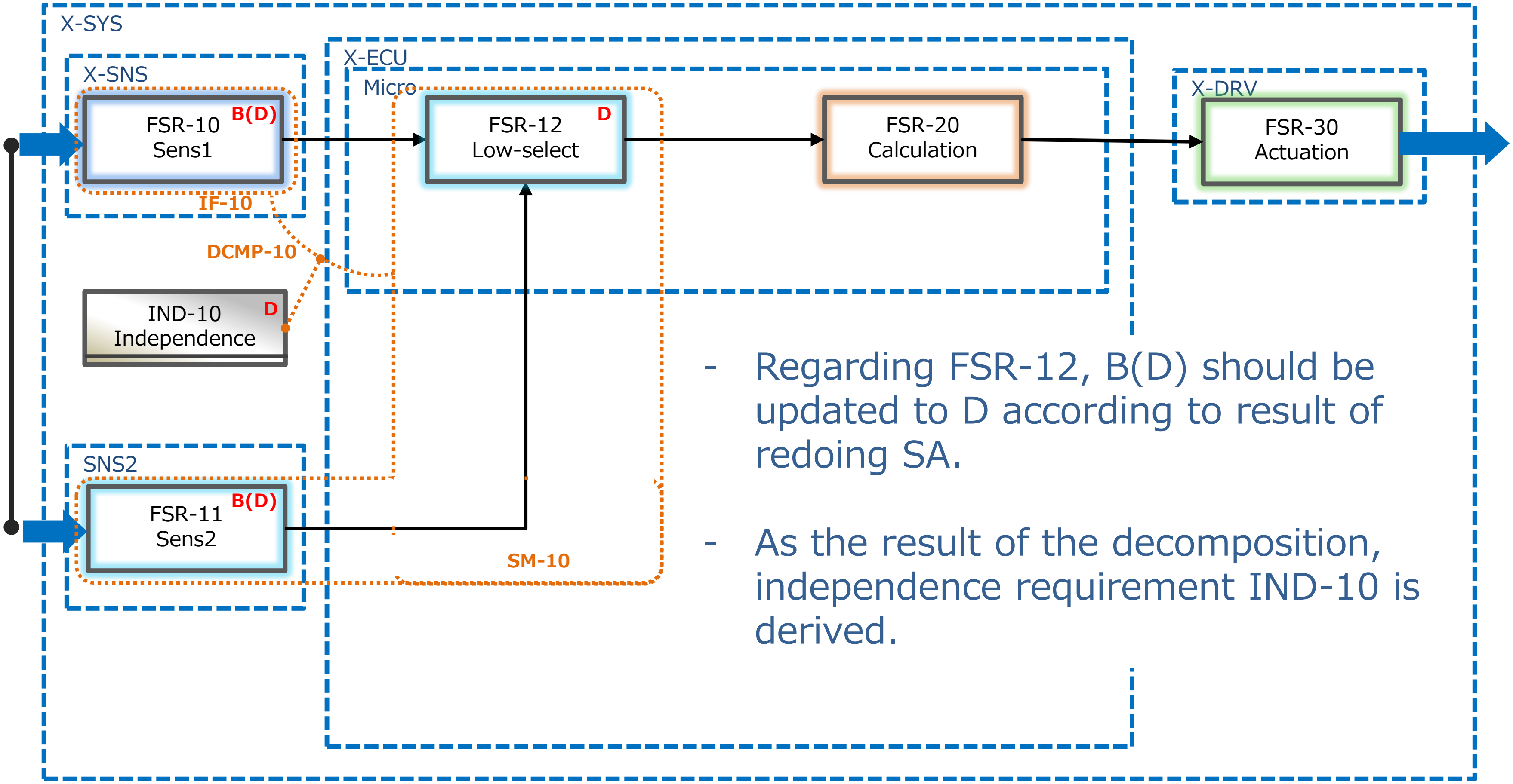
- Decomposition is applied for DCMP-10.
- Decomposition scheme D = B(A) + B(A) is applied.

Decomposition Scheme [Part 9-5]

One of the following decomposition schemes shall be chosen in accordance with the ASIL before decomposition

ASIL Before Decomposition	ASIL After Decomposition
ASIL D	ASIL C(D) + ASIL A(D)
	ASIL B(D) + ASIL B(D)
	ASIL D(D) + QM(D)
ASIL C	ASIL B(C) + ASIL A(C)
	ASIL C(C) + QM(C)
ASIL B	ASIL A(B) + ASIL A(B)
	ASIL B(B) + QM(B)
ASIL A	ASIL A(A) + QM(A)

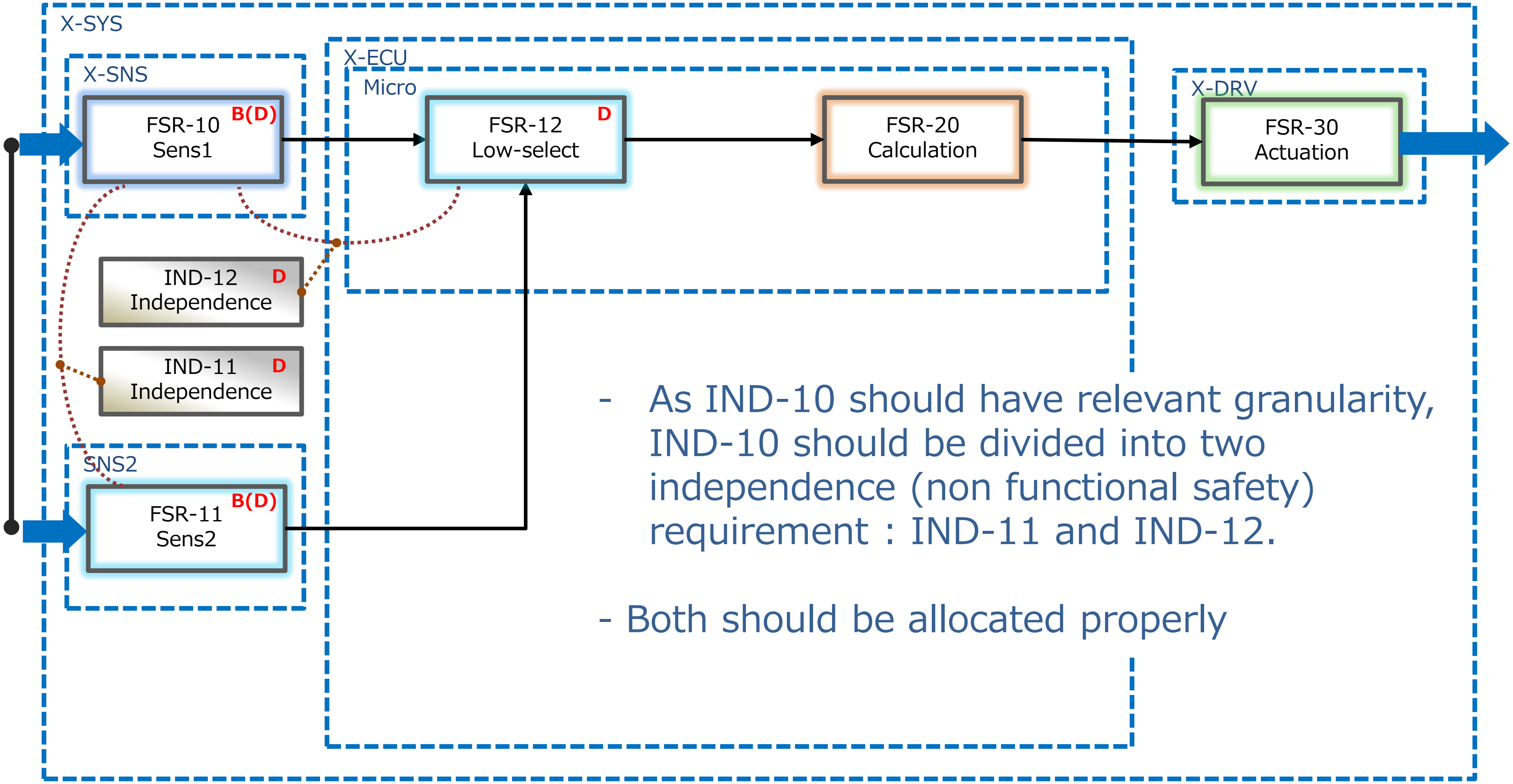
Consideration on SM-10



- Regarding FSR-12, B(D) should be updated to D according to result of redoing SA.

- As the result of the decomposition, independence requirement IND-10 is derived.

Consideration on SM-10

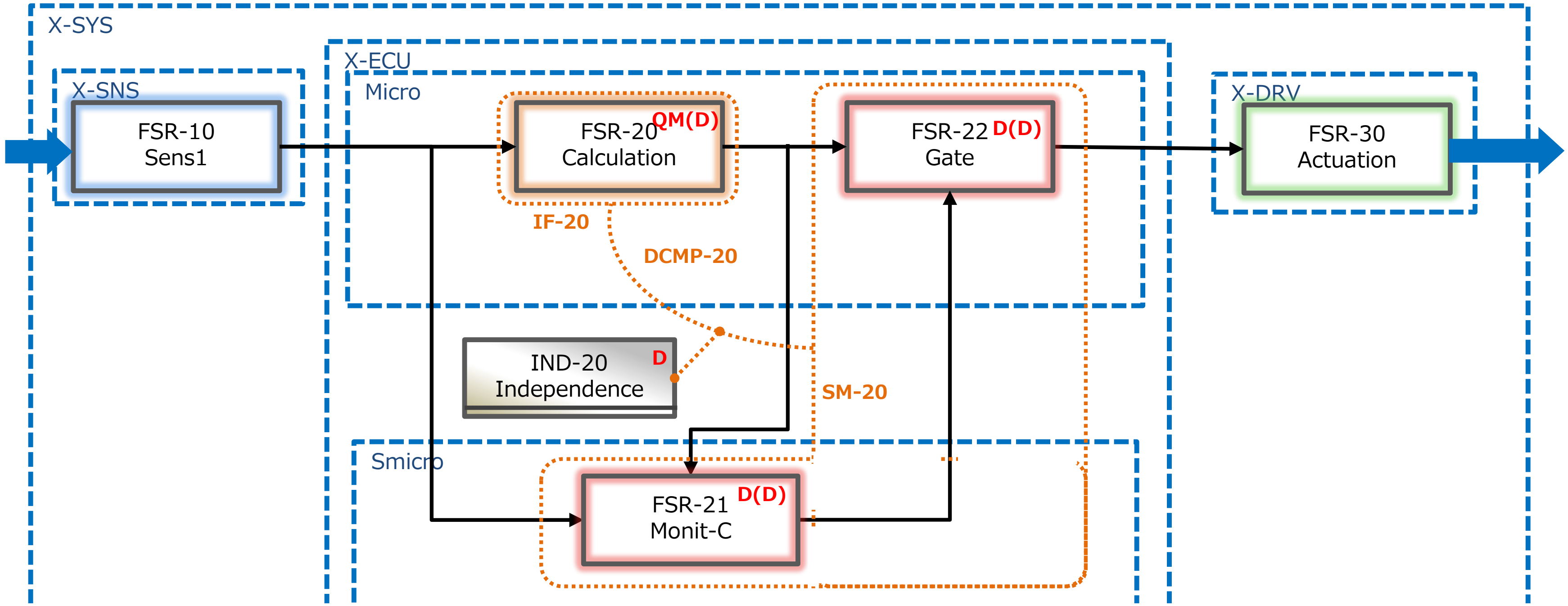


- As IND-10 should have relevant granularity, IND-10 should be divided into two independence (non functional safety) requirement : IND-11 and IND-12.

- Both should be allocated properly

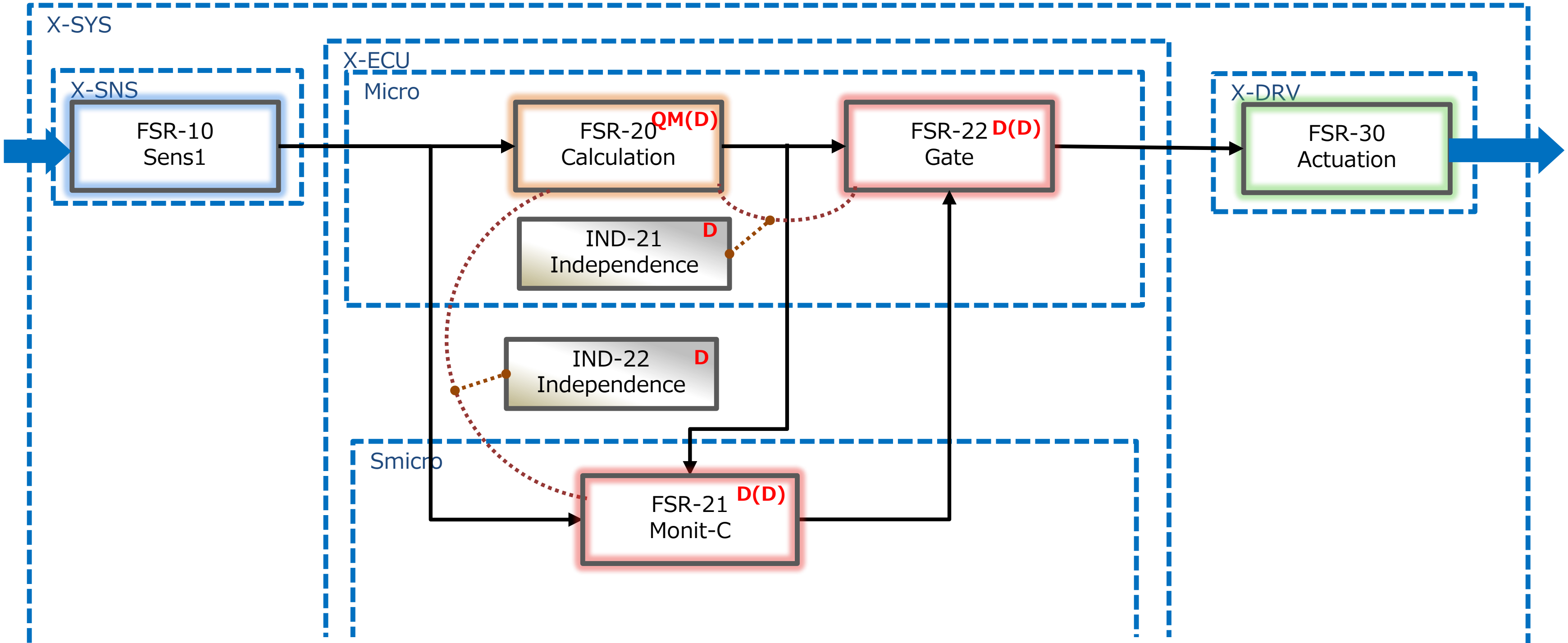
SM-20

Consideration on SM-20



- According to SA, additional monitoring micro : Smicro is added.
- SR group IF-20 and SM-20 are defined. IF/SM pair : DCMP-20 is defined.
- Decomposition is applied for this DCMP-20.
- Decomposition scheme D = QM(D) + D(D) is applied.
- As the result of the decomposition, independence requirement IND-20 is derived.

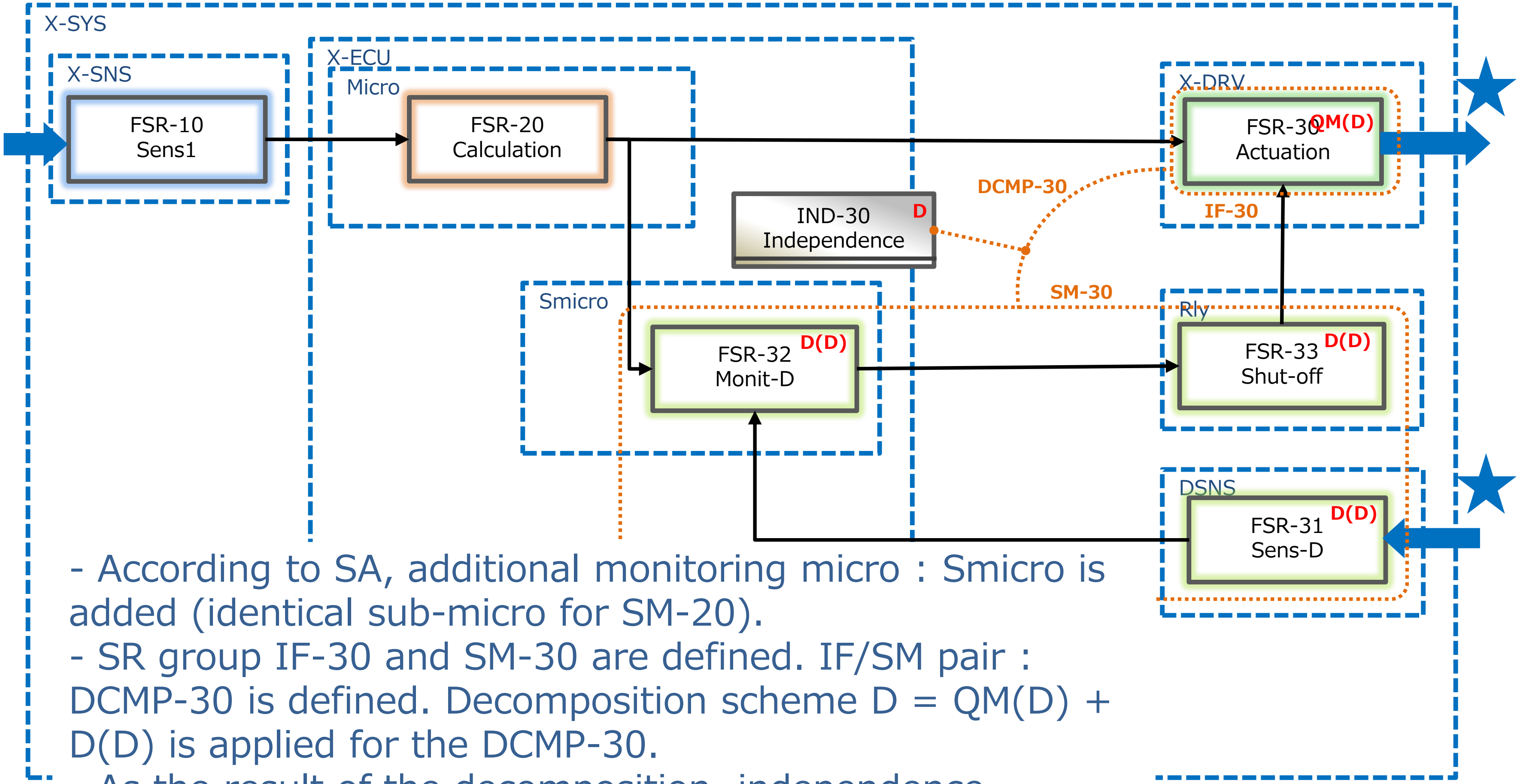
Consideration on SM-20



- As IND-20 should have relevant granularity, IND-20 should be divided into two independence requirement : IND-21, IND-22
- They should be allocated properly

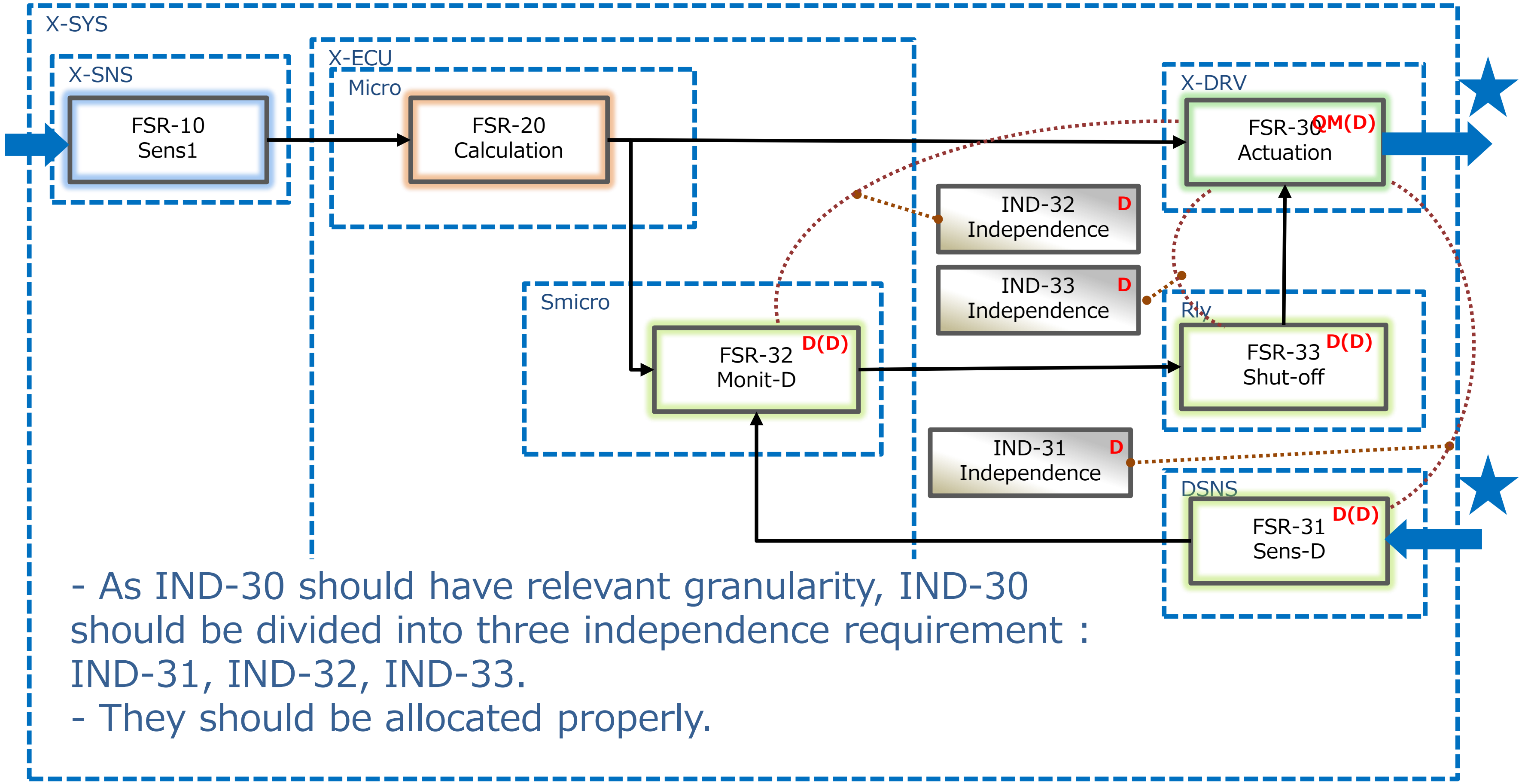
SM-30

Consideration on SM-30



- According to SA, additional monitoring micro : Smicro is added (identical sub-micro for SM-20).
- SR group IF-30 and SM-30 are defined. IF/SM pair : DCMP-30 is defined. Decomposition scheme D = QM(D) + D(D) is applied for the DCMP-30.
- As the result of the decomposition, independence requirement IND-30 is derived.

Consideration on SM-30

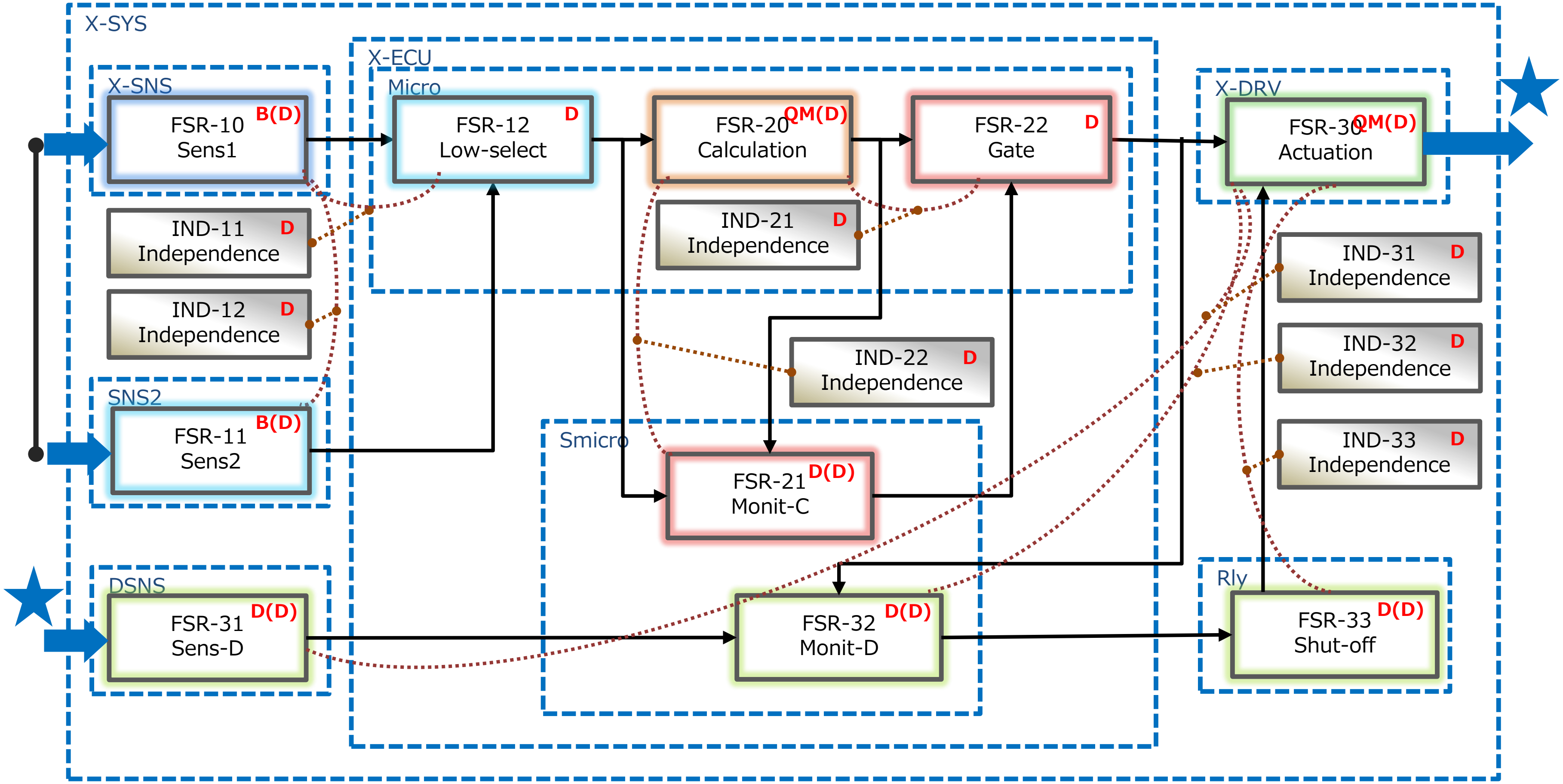


- As IND-30 should have relevant granularity, IND-30 should be divided into three independence requirement : IND-31, IND-32, IND-33.
- They should be allocated properly.

Merging

Merging three SMs into one architecture

In the last process of SC building, all considered SMs should be put into one architecture. Some arbitrations or other trims may be considered.



Element table (Updated)

Element Specifications

ID	Short name	Details / Spec.	ASIL (tentative)
ITEM-00	X-system	Automotive on-board system which provides X function	D
EL-10	X-SNS	Input device for X-system which acquire user's operation	B(D)
EL-11	S-SNS	Redundant sensor for X-SNS	B(D)
EL-20	X-ECU	ECU for X-system	D
EL-21	Micro	Main micro controller implemented in X-ECU	D
EL-22	S-Micro	Sub micro controller for monitoring mechanisms	D(D)
EL-30	X-DRV	Output device for X-system	QM(D)
EL-31	D-SNS	Monitoring sensor for X-DRV output	D(D)
EL-32	RLY	Shutoff relay for power supply of X-DRV	D(D)

SR Table (Updated)

Safety Requirement Specifications

SR ID / short name	SR in Natural Language	ASIL	input	output	allocation
FSR-10 / Sens1	Acquire driver’s input	B(D)	User’s input	Sensor value1	X-SNS
FSR-11 / Sens2	Acquire driver’s input	B(D)	User’s input	Sensor value2	SNS2
FSR-12 / Low-select	Select lower input	D	Sensor value1, Sensor value2	Sensor value (selected)	Micro
FSR-20 / Calculation	Calculate amount of output	QM(D)	Sensor value (selected)	Drive command	X-ECU
FSR-21 / Gate	Gate drive command according to gating information	D	Drive command Gating	Drive command (gated)	Micro
FSR-22 / Monit-C	Monitor Calculation	D(D)	Sensor value (selected)	Gating	S-Micro
FSR-30 / Actuation	Drive actuator	QM(D)	Drive command (gated)	X-output	X-driver
FSR-31 / Sens-D	Acquire X-output	D(D)	X-output	Sensor-D value	D-SNS
FSR-32 / Monit-D	Check relevance of X-output	D(D)	Drive command (gated), Sensor-D value	Shut- off info	S-Micro
FSR-33 / Shut off	Shut off X-drive power	D(D)	Shut-off info	Shut-off	RLY

Expected Next Steps

- DFA should be performed triggered by each independence requirement.

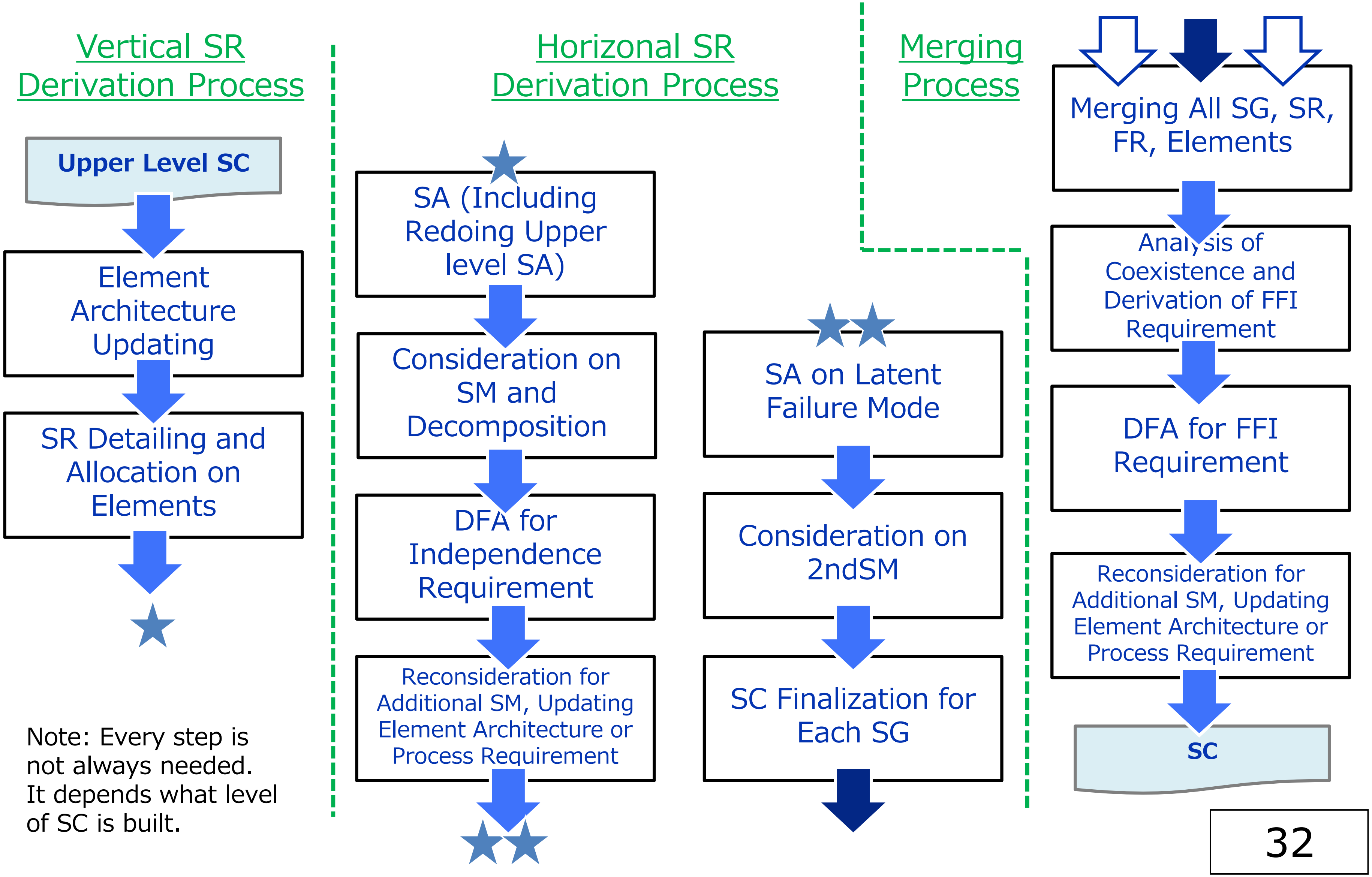
- Each SR should be detailed and additional SR may be derived. (e.g. TSRs will be obtained from FSRs).

- SRVA should be applied again for next detailed level SRs.

- And so on.

(See SC Building Process Reference Model on the next slide)

SC Building Process Reference Model



Vertical SR Derivation Process

Upper Level SC

Element Architecture Updating

SR Detailing and Allocation on Elements

★

Horizonal SR Derivation Process

★

SA (Including Redoing Upper level SA)

Consideration on SM and Decomposition

DFA for Independence Requirement

Reconsideration for Additional SM, Updating Element Architecture or Process Requirement

★★

★★

SA on Latent Failure Mode

Consideration on 2ndSM

SC Finalization for Each SG

Merging Process

Merging All SG, SR, FR, Elements

Analysis of Coexistence and Derivation of FFI Requirement

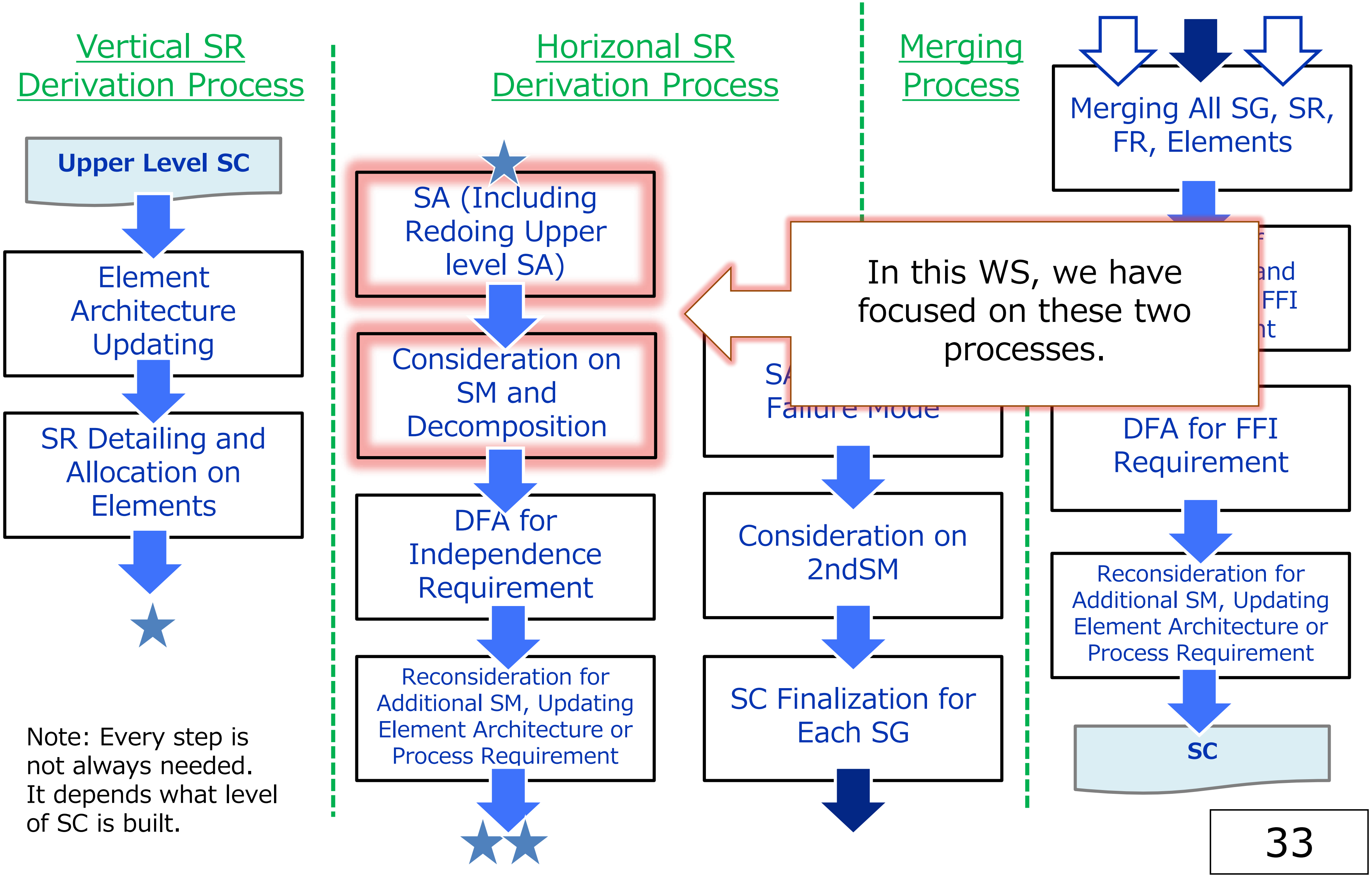
DFA for FFI Requirement

Reconsideration for Additional SM, Updating Element Architecture or Process Requirement

SC

Note: Every step is not always needed. It depends what level of SC is built.

SC Building Process Reference Model


Vertical SR Derivation Process
Upper Level SC
Element Architecture Updating
SR Detailing and Allocation on Elements
Horizonal SR Derivation Process
SA (Including Redoing Upper level SA)
Consideration on SM and Decomposition
DFA for Independence Requirement
Reconsideration for Additional SM, Updating Element Architecture or Process Requirement
SA
Failure Mode
Consideration on 2ndSM
SC Finalization for Each SG
Merging Process
Merging All SG, SR, FR, Elements
and
FFI
nt
DFA for FFI Requirement
Reconsideration for Additional SM, Updating Element Architecture or Process Requirement
SC

In this WS, we have focused on these two processes.

Note: Every step is not always needed. It depends what level of SC is built.

Q & A
Discussion