The Study of TSN Profiling for Safety and Reliability on Automotive Network

Japan Automotive Software Platform and Architecture

Ethernet & IP @ Automotive Technology Day

25 September 2019

Takumi Nomura (Honda)

Katsuyuki Akizuki (NEC Communication Systems)

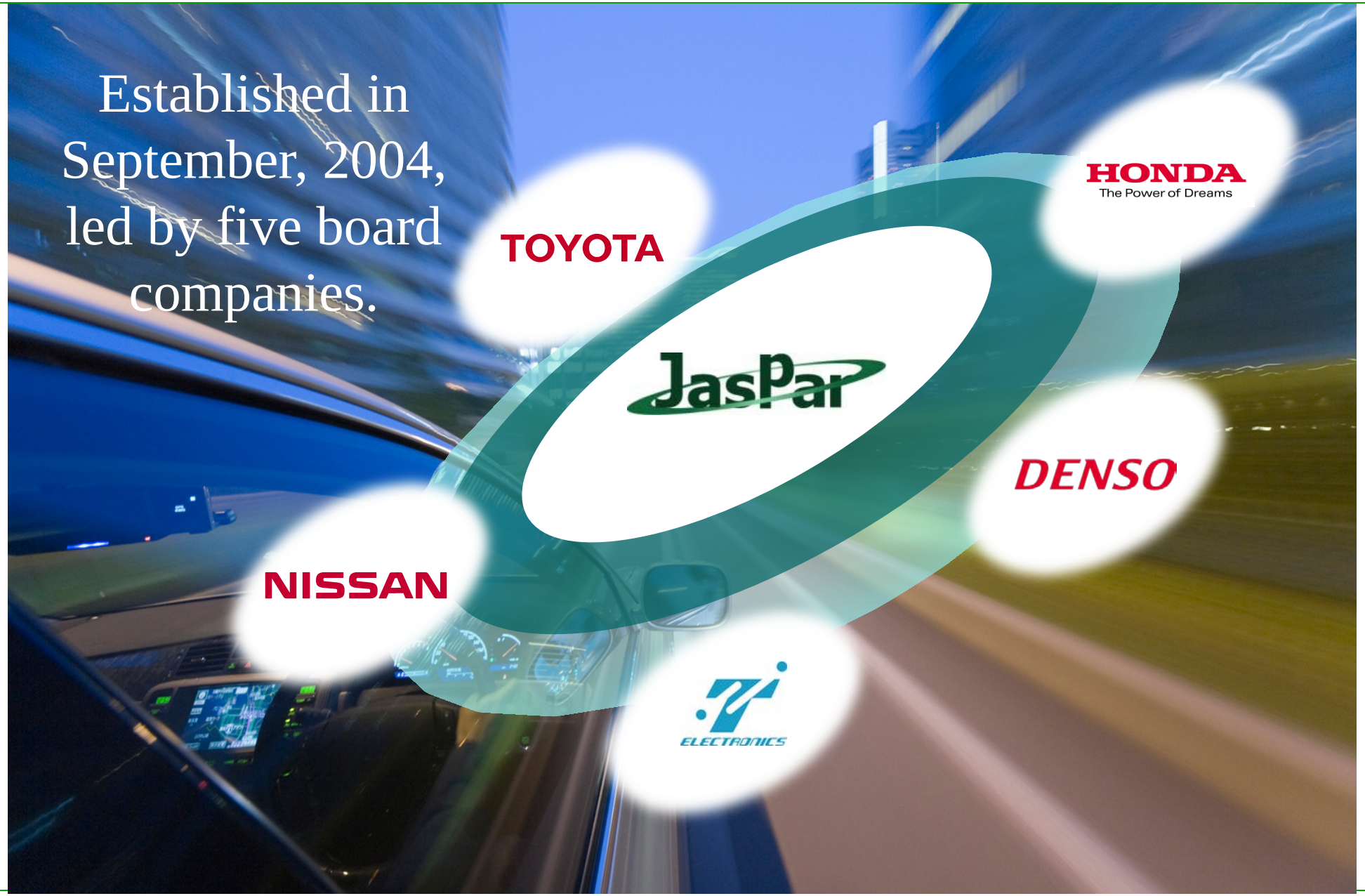
Ken Ueda (NEC Communication Systems)

Ryohei Kawabuchi (Mazda)

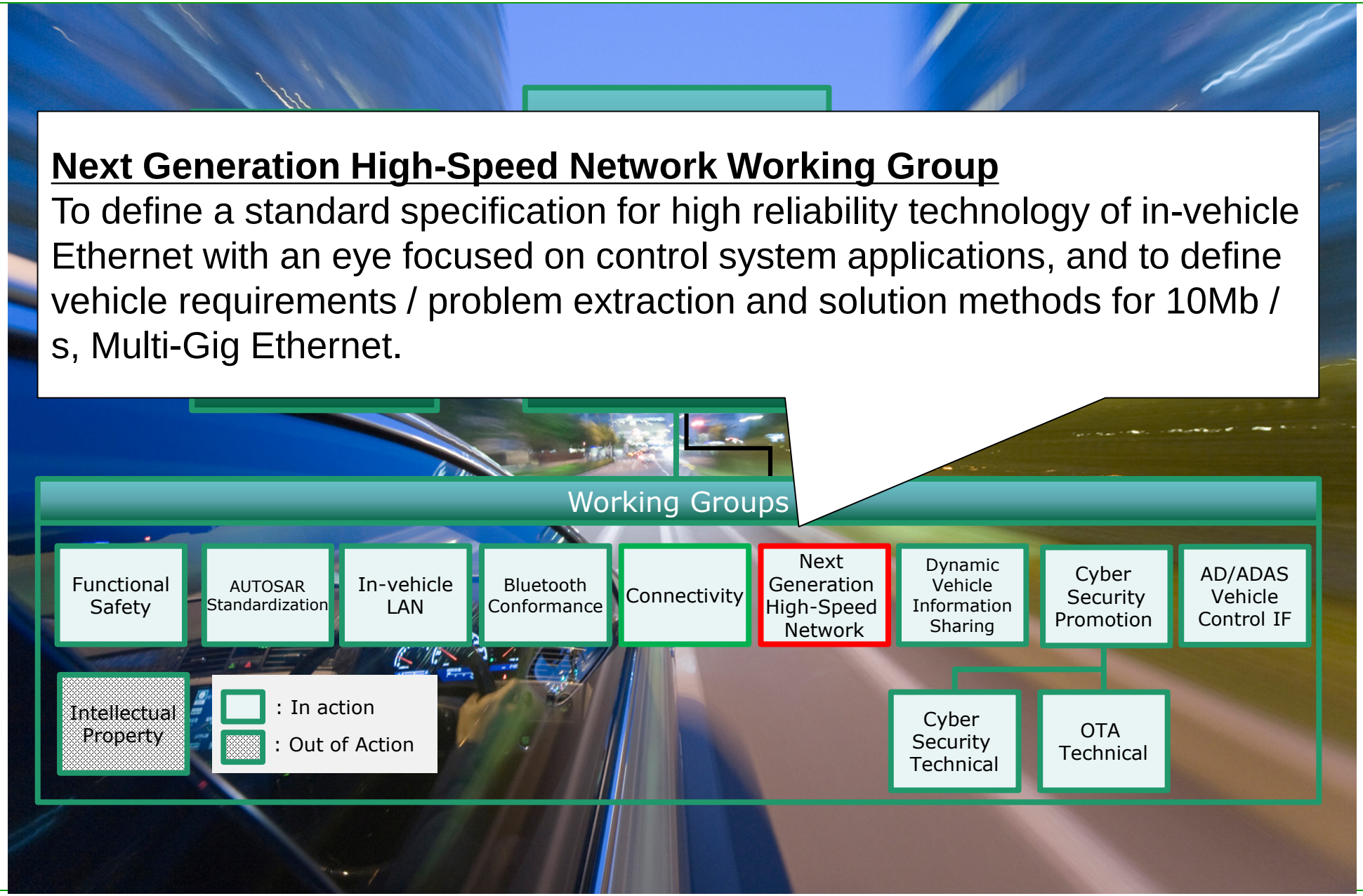
Yoshifumi Hotta (Mitsubishi Electric)

Company: JASPAR (Toyota, Nissan, Honda, Mazda)

1. Introduction
2. Background
3. Objective
4. Case Study
   - Use case
   - Workflow
   - Requirement
   - Profiling
   - Circuit scale estimation
5. Next Activities
6. Conclusion


Established in September, 2004, led by five board companies.
TOYOTA
HONDA
The Power of Dreams
JasPar
DENSO
NISSAN
ELECTRONICS

Introduction: Next Generation High-Speed Network Working Group



■ TSN is the most promising candidate to realize the next generation automotive network.

■ Automotive profile is indispensable to select TSN features and quantities for on-board system.

■ In Jaspar, we discussed **Fault Tolerant** and Real Time features which are required for the automotive network.

■ In this presentation, our **TSN profiling case study** related to Fault Tolerant behavior is shown as an example.

- Provide use case study examples to create the Automotive Profile.
  - ✓ Create use cases
  - ✓ Extract Requirements
  - ✓ Profiling
- Elaborate profiling effectiveness from device circuit scale reduction viewpoint.
- Consider how TSN fault tolerant features contribute to functional safety.
  - ✓ How TSN features improve the diagnostic coverage?
  - ✓ Additional study is required…

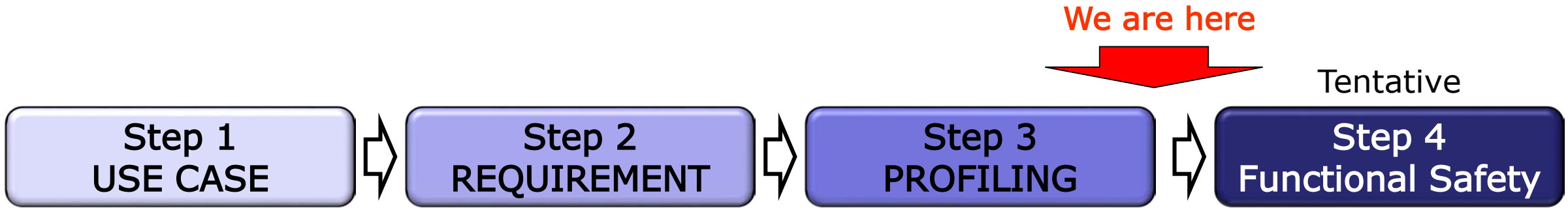
4-Step Flow

■ Step1
Define the simple ADAS use case.

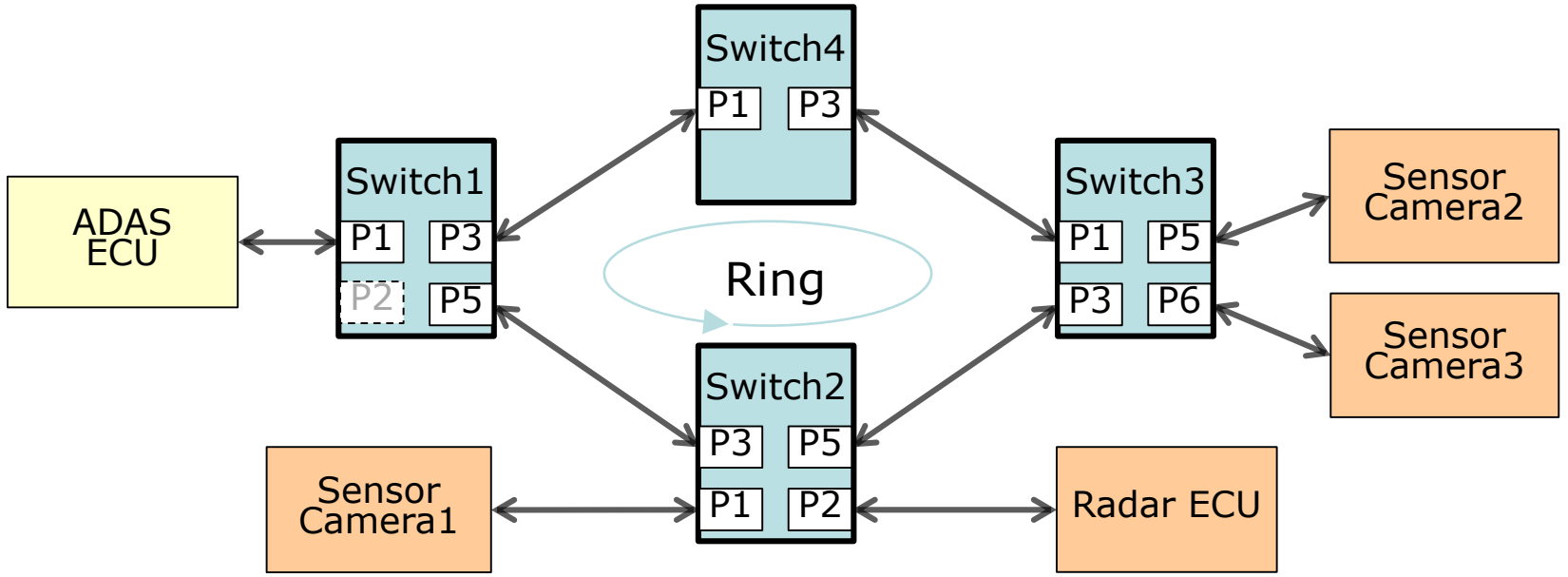
■ Step2
Derive the safety requirements for the use case.

■ Step3
Investigate how TSN features are applied to realize the requirements.

■ Step4 (Tentative)
Investigate how selected TSN features affect functional safety.



- An ADAS system as an example, which requires TSN.
- Expected network topology is a Ring composed by 4 switches since the minimum physical redundancy is required to apply fault tolerant features of TSN.
- Multiple data streams, such as sensor and control data are listed.



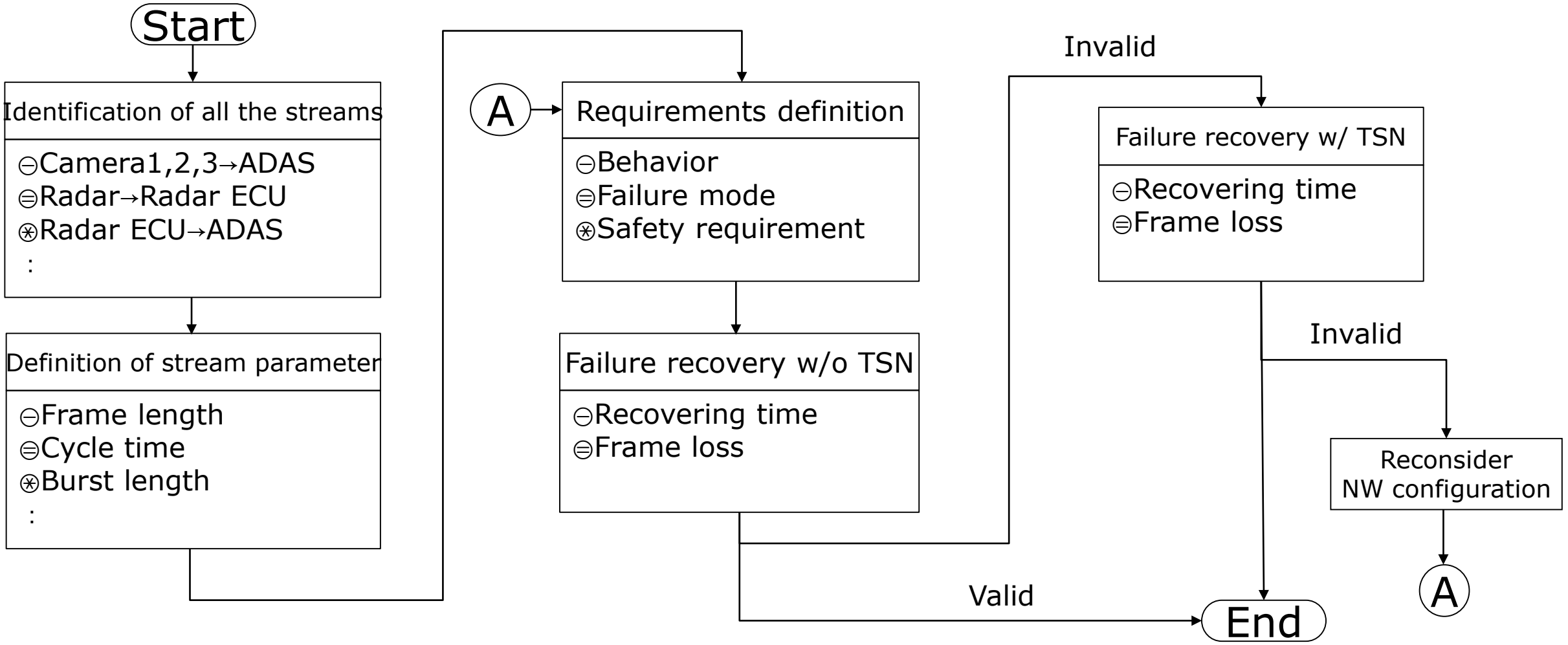
Use Case: ADAS

Stream Number	Stream Classification	Priority	Allowable delay time (ms)	Maximum delay time (ms)	Within allowable delay time?	Maximum delay time minus allowable delay time (ms)
1	Image data	1	13.34	16.51	NO	3.18
2	Image data	1	13.34	16.51	NO	3.17
3	Control	1	26.67	11.27	YES	-15.40
4	Control	1	26.68	11.27	YES	-15.40
5	Image data	1	13.34	16.52	NO	3.18
6	Image data	1	13.34	16.51	NO	3.18
7	Control	1	26.68	11.28	YES	-15.40
8	Control	1	26.68	11.28	YES	-15.40
9	Image data	1	13.34	16.52	NO	3.18
10	Image data	1	13.34	16.52	NO	3.18
11	Control	1	26.68	11.28	YES	-15.40
12	Control	1	26.68	11.28	YES	-15.40
13	Radar	1	13.34	0.46	YES	-12.87
14	Control	1	13.34	0.12	YES	-13.22
15	Radar	1	40.01	16.63	YES	-23.38
16	Radar	1	40.01	16.64	YES	-23.38
17	Control	1	40.01	16.61	YES	-23.40
18	Control	1	40.01	16.61	YES	-23.40
19	Image data	1	26.67	6.17	YES	-20.50
19_2	Vehicle control	1	8.01	0.01	YES	-7.99
20	Setting	1	NA(non-RT)	NA(non-RT)	NA(non-RT)	NA(non-RT)
21	Setting	1	NA(non-RT)	NA(non-RT)	NA(non-RT)	NA(non-RT)
22	Setting	1	NA(non-RT)	NA(non-RT)	NA(non-RT)	NA(non-RT)
23	Setting	1	NA(non-RT)	NA(non-RT)	NA(non-RT)	NA(non-RT)
24	Setting	1	NA(non-RT)	NA(non-RT)	NA(non-RT)	NA(non-RT)
25	Setting	1	NA(non-RT)	NA(non-RT)	NA(non-RT)	NA(non-RT)
26	Setting	1	NA(non-RT)	NA(non-RT)	NA(non-RT)	NA(non-RT)
27	Setting	1	NA(non-RT)	NA(non-RT)	NA(non-RT)	NA(non-RT)
28	Setting	1	NA(non-RT)	NA(non-RT)	NA(non-RT)	NA(non-RT)
29	NM	1	2.67	0.01	YES	-2.66
30	Status	1	8.01	0.01	YES	-7.99

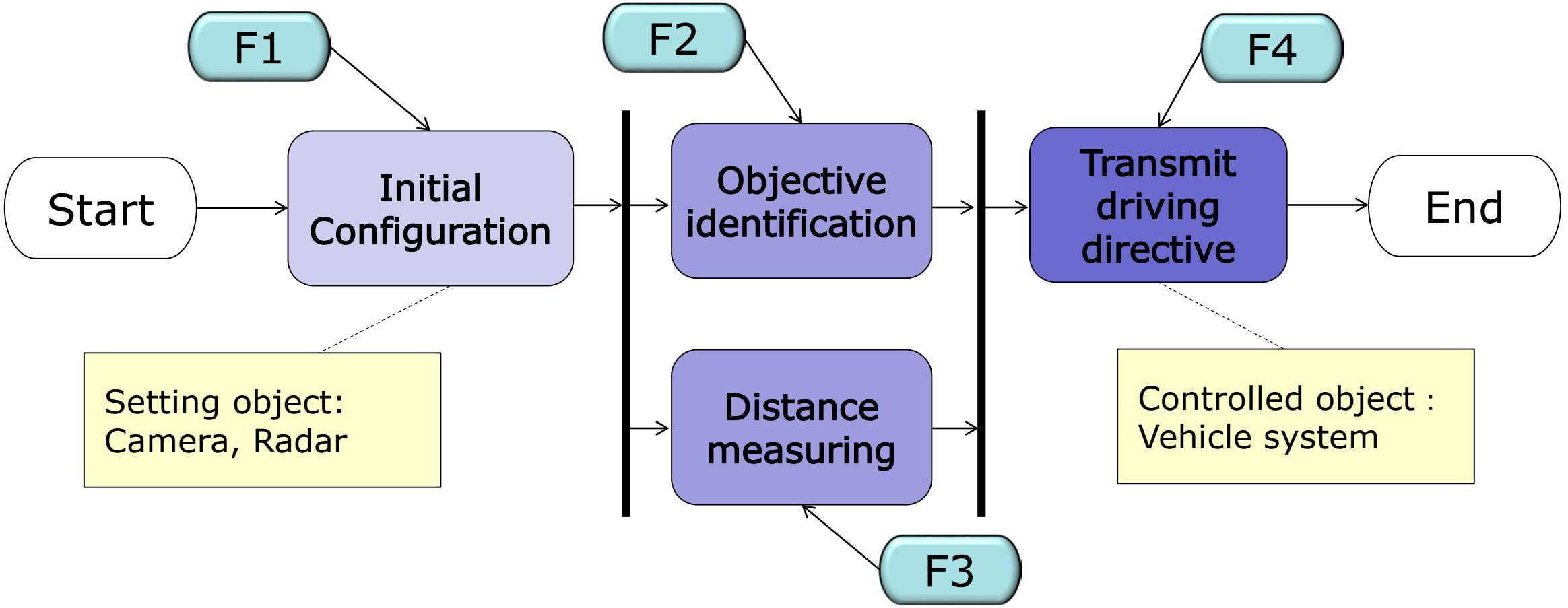
*) NA : Not Applicable

Stream List

■ Find the required function for fail-operation under the route failure



Step2: Definition of the Failure Mode



F1 : Failure of the initial configuration for camera and radar

F2 : Failure of the objective identification

F3 : Failure of the distance measuring from object

F4 : Failure of the driving directive transmission

Ex: F2 Failure of the objective identification

■ Failure mode

Harness disconnection on path 1,2 and 3

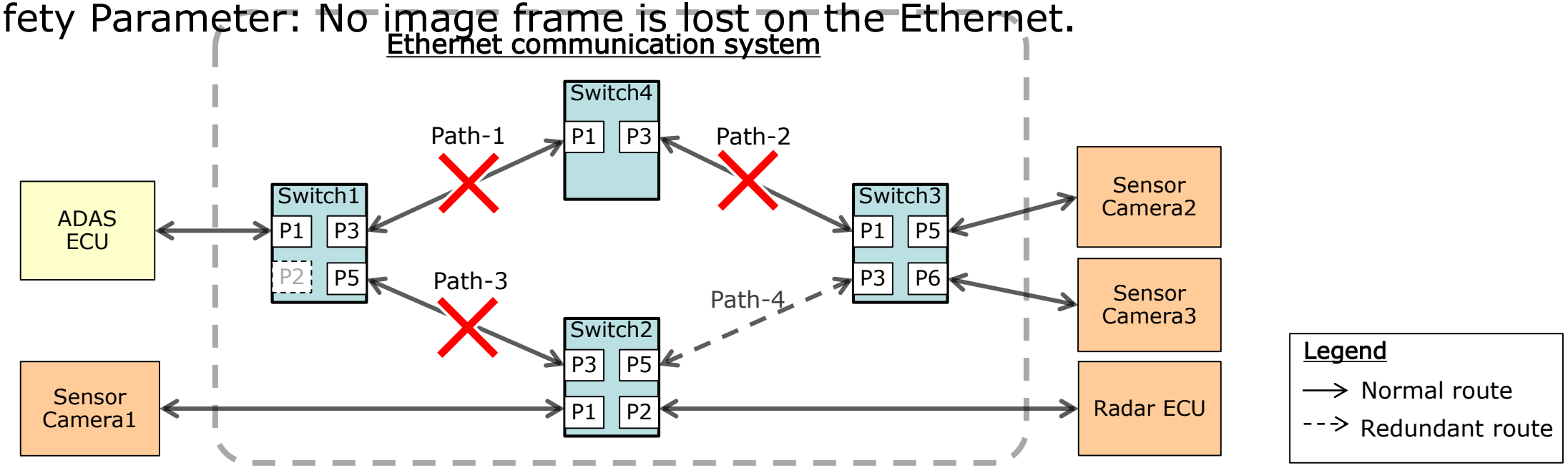
■ Safety Requirement to ADAS

ADAS ECU can continue objective identification based on camera information.

■ Safety Requirement for Ethernet communication system

Safety Condition: Picture information reaches ADAS ECU.

Safety Parameter: No image frame is lost on the Ethernet.

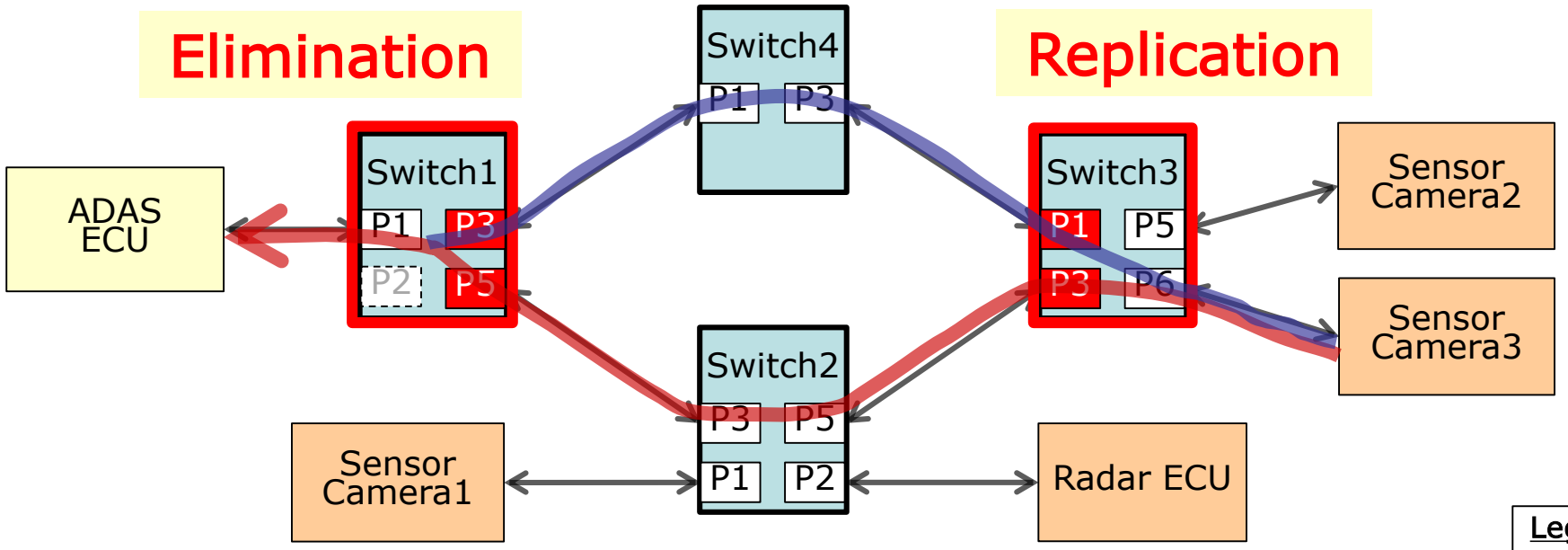


Summary of the Requirement Analysis

Safety requirement to communication system	Behavior		
	Initial Configuration	Objective identification	Distance measuring
[Requirement 1] Safety condition	Setting of camera and radar shall be completed.	Object image data from camera shall reach ADAS ECU.	Object distance data from radar shall reach ADAS ECU.
[Requirement 2] Safety parameter	Safety condition shall be within 1000msec after initial setting start. This requirement should be satisfied regardless of the generation timing of the cause phenomenon.	No image data shall be lost on the Ethernet.	No distance data shall be lost on the Ethernet.

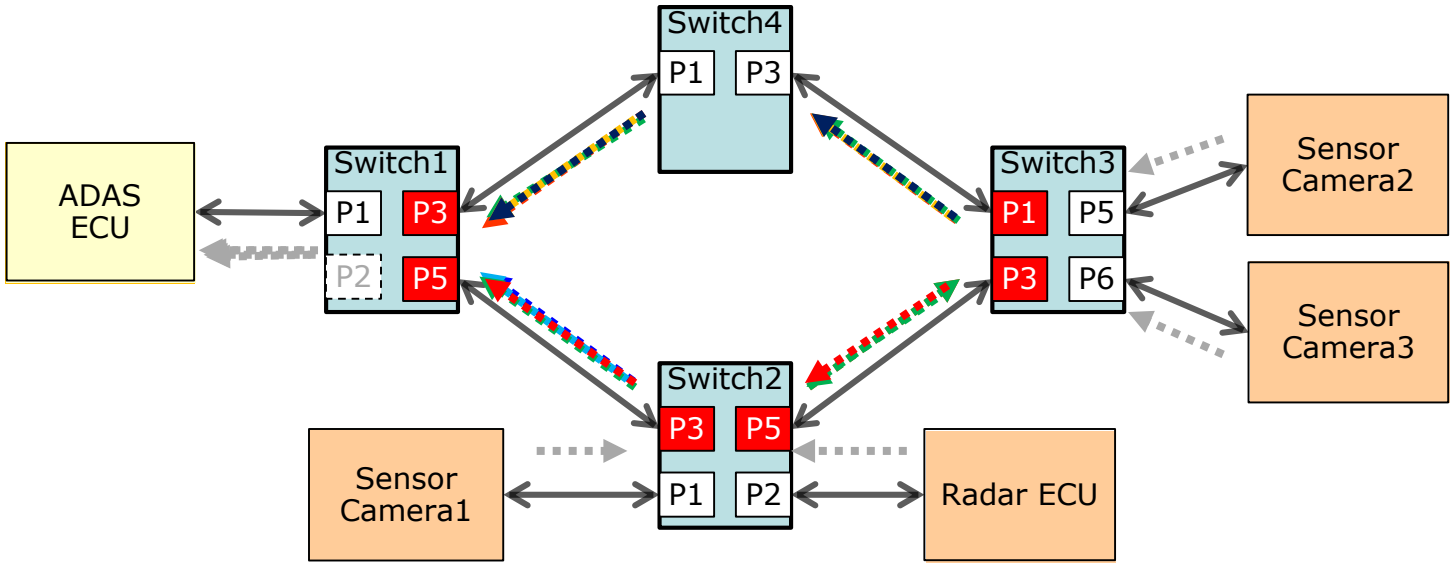
- IEEE 802.1CB “Frame Replication and Elimination for Reliability” duplicates frames and transmits them via multiple routes.
- Even though frame loss occurs on one route because of failure, another frame can arrive at the destination node via another route.
- Thus we chose **IEEE 802.1CB** that **satisfies the requirements**.

- IEEE 802.1CB is composed of Frame Replication and Elimination function.
- Following picture shows 802.1CB functional allocation to switches and ports, in case of protecting image data flow between Sensor Camera 3 and ADAS ECU.



Functional allocation, in case of Camera3 image data flow

- Distance/image data flow from Radar ECU, Sensor Camera2 and 1 need to be protected as well
- Thus IEEE 802.1CB functions need to be allocated to 3 switches, 6ports as following:



System configuration

Legend

Px Port with 802.1CB function

■ Result of the profiling is shown in the matrix below.
Columns indicate nodes and ports. Rows indicate the functions of IEEE 802.1CB.

■ Necessary functions are plotted for each port.

For stream identification, only the Null Stream Identification is applied since DA and VLAN-ID are enough to identify the stream.

Main Functions		Sw1			Sw2				Sw3				Sw4	
		P1	P3	P5	P1	P2	P3	P5	P1	P3	P5	P6	P1	P3
Stream identification	Null Stream identification (6.4)	O	I	I	I	I	O	I/O	O	I/O	I	I	O	I
	Source MAC and VLAN Stream identification (6.5)	–	–	–	–	–	–	–	–	–	–	–	–	–
	Active Destination MAC and VLAN Stream identification (6.6)	–	–	–	–	–	–	–	–	–	–	–	–	–
	IP Stream identification (6.7)	–	–	–	–	–	–	–	–	–	–	–	–	–
FRER	Sequencing (7.4)	–	I	I	–	–	O	O	O	O	–	–	–	–
	Stream splitting (7.7)	–	–	–	–	–	O	O	O	O	–	–	–	–
	Individual recovery (7.5)	–	I	I	–	–	–	–	–	–	–	–	–	–
	Sequence encode/decode (7.6)	–	I	I	–	–	O	O	O	O	–	–	–	–

* “I” : Input, “O” : Output, “-” : Not implemented

Estimation of the Circuit Scale 1/2

- In Full-set;
  - Both Replication and Elimination are implemented.
  - All types of Stream identification are supported.

- In Sub-set;
  - Either one of Replication or Elimination will be implemented.
  - Only Null Stream identification will be supported.

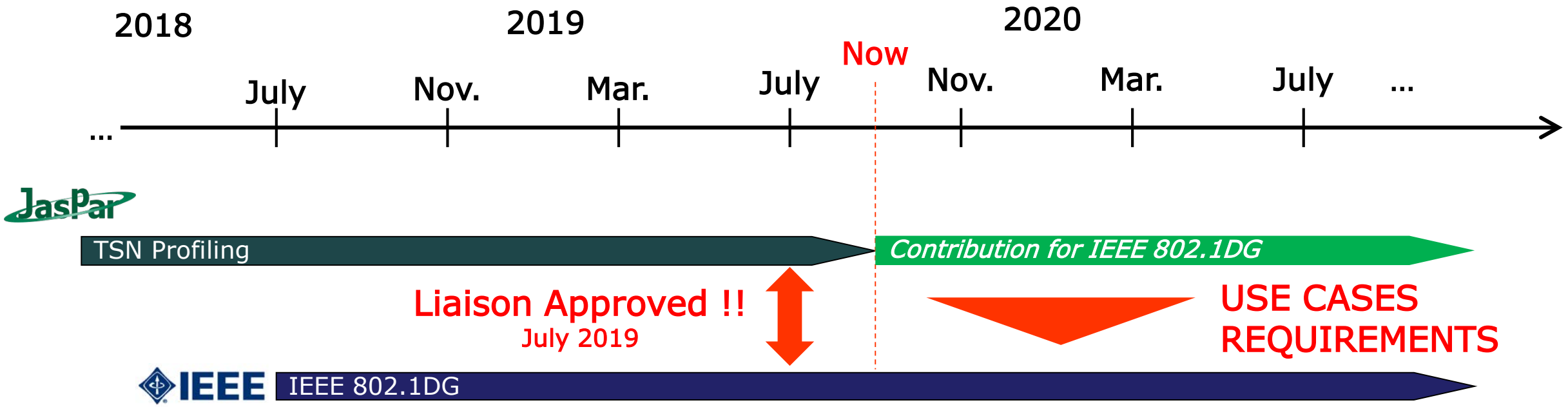
- Other conditions
  - Recovery functions from failure state are not considered
  - No wiring length difference between redundant paths
  - No time delay difference between redundant paths
  - Redundant route is 2 way
  - Both Full-set and Sub-set have the same implementation for Stream entries, Counters and Error detection functions.

Estimation of the Circuit Scale 2/2

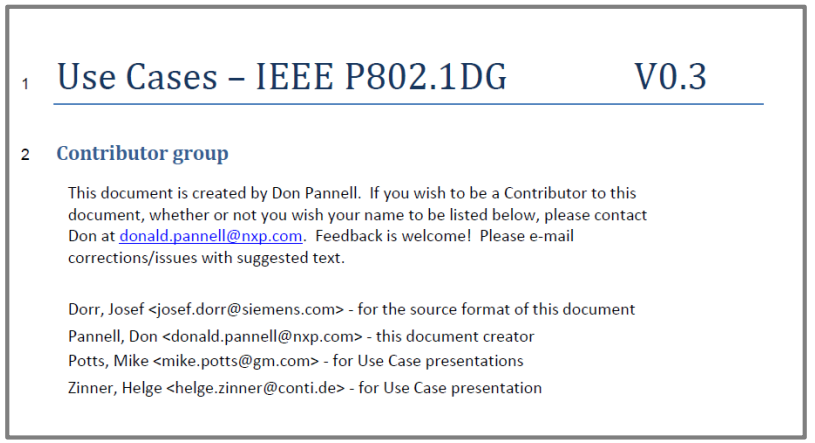
Function	Terms	Full-set	Sub-set (for Replication)	Sub-set (for Elimination)
Stream identification	Identification function & Stream identity table	All - Null Stream identification - Source MAC and VLAN Stream identification - Active Destination MAC and VLAN Stream identification - IP Stream identification	- Null Stream identification	- Null Stream identification
	Header modification (Destination MAC address, VLAN, priority)	Implemented	Not Implemented	Not Implemented
	Stream identification counters	- Operational per-port per-Stream - Operational per-Stream Stream	- Operational per-Stream Stream	- Operational per-Stream Stream
FRER	Sequencing	- Sequence generation and recovery - latent error detection	- Sequence generation - latent error detection	- Sequence recovery - latent error detection
	Stream splitting	Implemented	Implemented	Not Implemented
	Individual recovery	Implemented	Not Implemented	Implemented
	Sequence encode/decode	Replication and Elimination	Replication	Elimination
	Entry table	Replication and Elimination	Replication	Elimination
	Stream split table	Implemented	Implemented	Not Implemented
	Auto configuration	Implemented	Not Implemented	Not Implemented
	FRER counters	- Operational per-port per-Stream - Operational per-Stream Stream	- Operational per-Stream Stream	- Operational per-Stream Stream
Estimation the circuit scale		100%	29%	28%

- Compared to the Full-set, the circuit scale of Sub-set (for Replication) is reduced to **29%** and Sub-set (for Elimination) is reduced to **28%**.

Next Activity 1 : Contribution to IEEE 802.1DG



P802.1DG Automotive Use Cases & Requirements [1]



1 Use Cases – IEEE P802.1DG V0.3

2 **Contributor group**

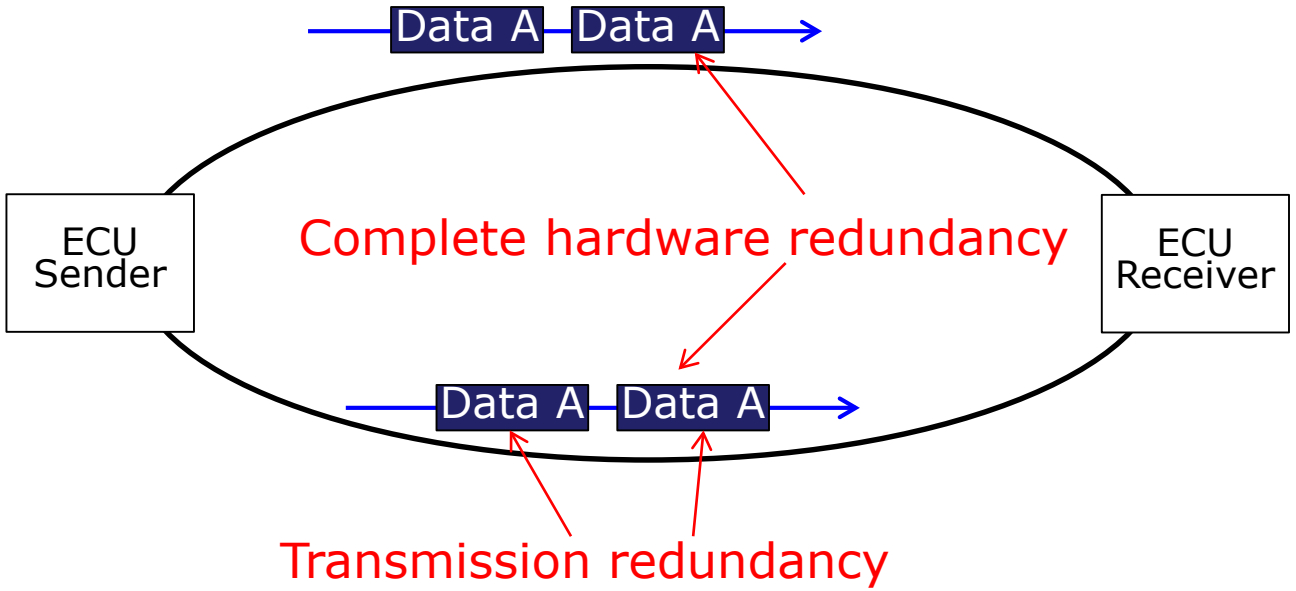
This document is created by Don Pannell. If you wish to be a Contributor to this document, whether or not you wish your name to be listed below, please contact Don at donald.pannell@nxp.com. Feedback is welcome! Please e-mail corrections/issues with suggested text.

Dorr, Josef <josef.dorr@siemens.com> - for the source format of this document
Pannell, Don <donald.pannell@nxp.com> - this document creator
Potts, Mike <mike.potts@gm.com> - for Use Case presentations
Zinner, Helge <helge.zinner@conti.de> - for Use Case presentation

[1] http://www.ieee802.org/1/files/public/docs2019/dg-pannell-automotive-use-cases-0719-v03.pdf

■ Extracts from ISO26262:2018 Part5 Annex D TableD.6 Communication Bus

Safety mechanism/measure	Typical diagnostic coverage considered achievable	Note
Complete hardware redundancy	High	Common mode failures can reduce diagnostic coverage
Transmission redundancy	Medium	Depends on type of redundancy. Effective only against transient faults



IEEE 802.1CB may be able to achieve **High/Medium diagnostic coverage**.

Conclusion

- ADAS system was used as an example
- Case study of profiling TSN was implemented from the Safety and Reliability perspective.
- Proposed profile can reduce the circuit scale by 70% (Cost Effective!)
- Significant effect may be brought by profiling based on the use case and requirement of automotive.
- From now on, our investigation of profiling will move to IEEE 802.1DG.
- First of all, start from USE CASE proposal.
- IEEE 802.1CB is also carried out as a key technology of functional safety – we will collaborate with Functional Safety Working Group for further investigation.

Thank you for your attention.