NISSAN MOTOR CORPORATION

2015 STPA Conference

A study on the fusion of STPA and Nissan's Systems Engineering

Nissan Motor Co., Ltd

Tetsunobu Morita, Takashi Nakazawa
Masaaki Uchida

Massachusetts Institute of Technology
John Thomas, Ph.D.

Summary

Nissan studied on the fusion of STPA and our layered RFLP process, and the results are

・ STPA has a strong affinity to layered RFLP* process

・ **STPA step1 is powerful to make “Requirements” substantial**

・ STPA step2 is powerful to check and close the design before delivering requirements to lower layer

*RFLP express

R: Requirements

F: Functional Architecture

L: Logical Architecture

P: Components/software and Implementation

Agenda

1. Background

2. **Introduction of Nissan’s systems engineering** (RFLP process)

3. Fusion of STPA and Nissan's RFLP process

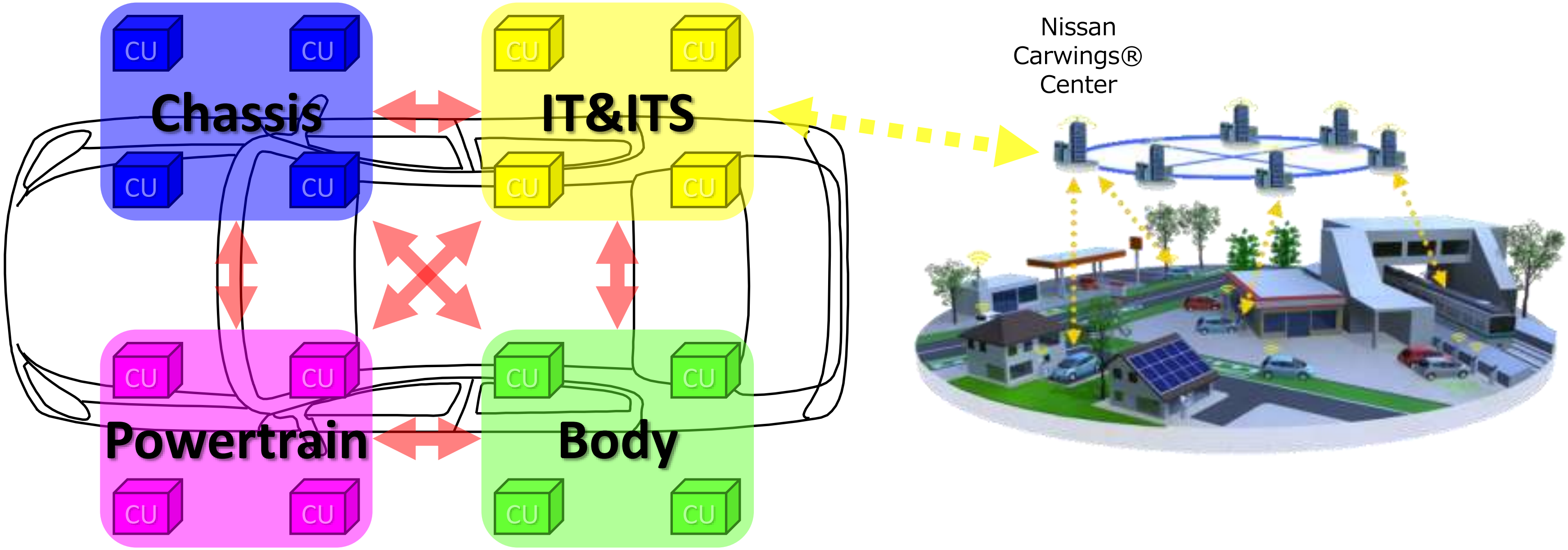
4. STPA trial result

5. Conclusion & future work

Background

✓ The vehicle system is growing more and more complex and constructed in wide-ranging fields.

--> Systems Engineering has been introduced to Nissan.

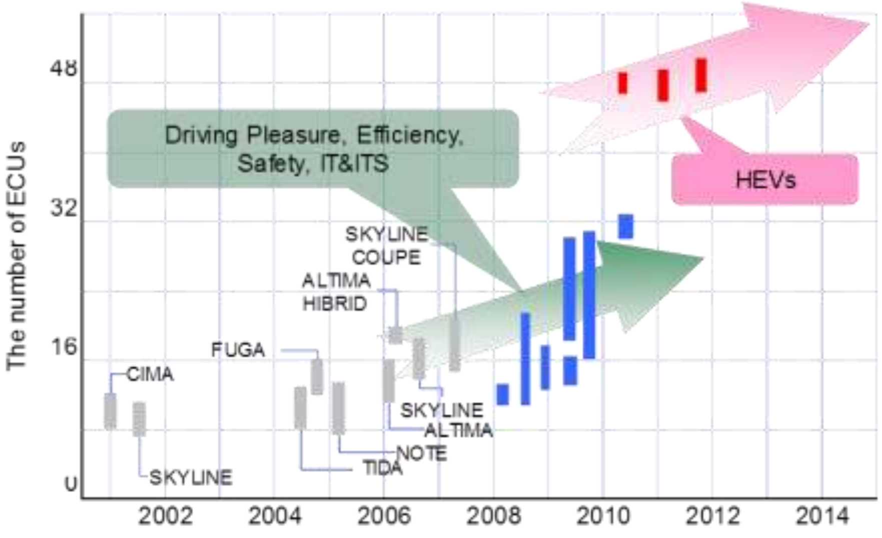


Background

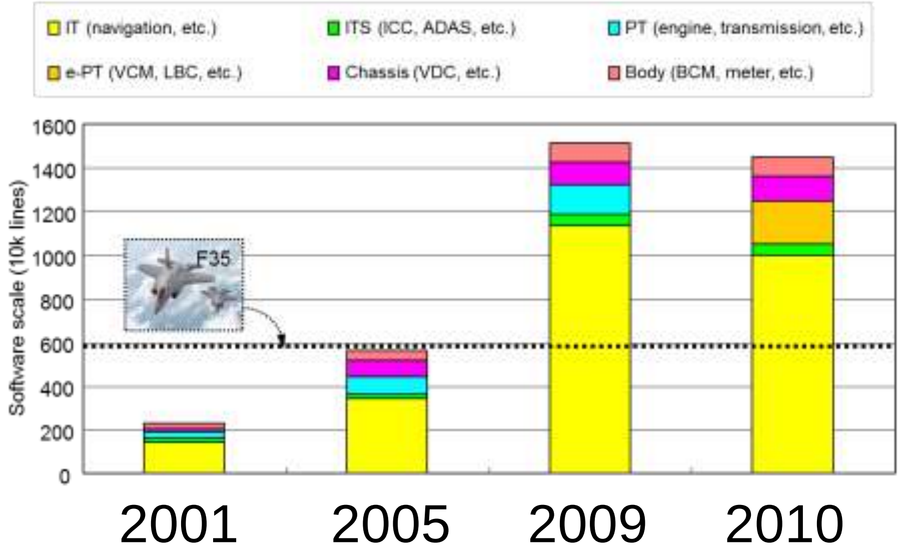
- ✓ The vehicle system is growing more and more large scale
- ✓ It is difficult to develop the software without dividing into appropriate size.

--> Systems Engineering has been introduced to Nissan.

Computer units
are increasing x5 / 10 years.



Software scale became
x10 / 10 years.



Agenda

1. Background

2. **Introduction of Nissan’s systems engineering** (RFLP process)

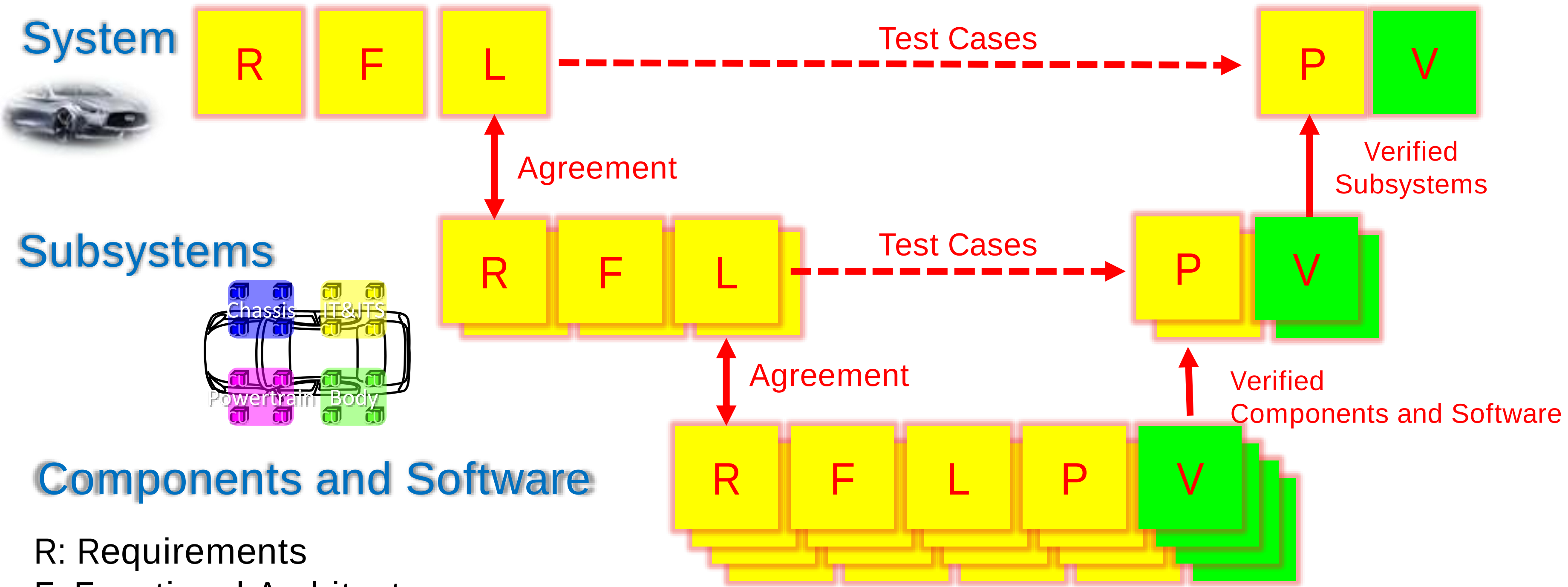
3. Fusion of STPA and Nissan's RFLP process

4. STPA trial result

5. Conclusion & future work

Nissan‘s Systems Engineering

- ✓ To develop complex and large vehicle system, we deploy systems engineering process, based on layered RFLP.
- ✓ We have to close system design before delivering requirements to lower layer systems.



System

R F L

Test Cases

P V

Agreement

Verified Subsystems

Subsystems

R F L

Test Cases

P V

Agreement

Verified Components and Software

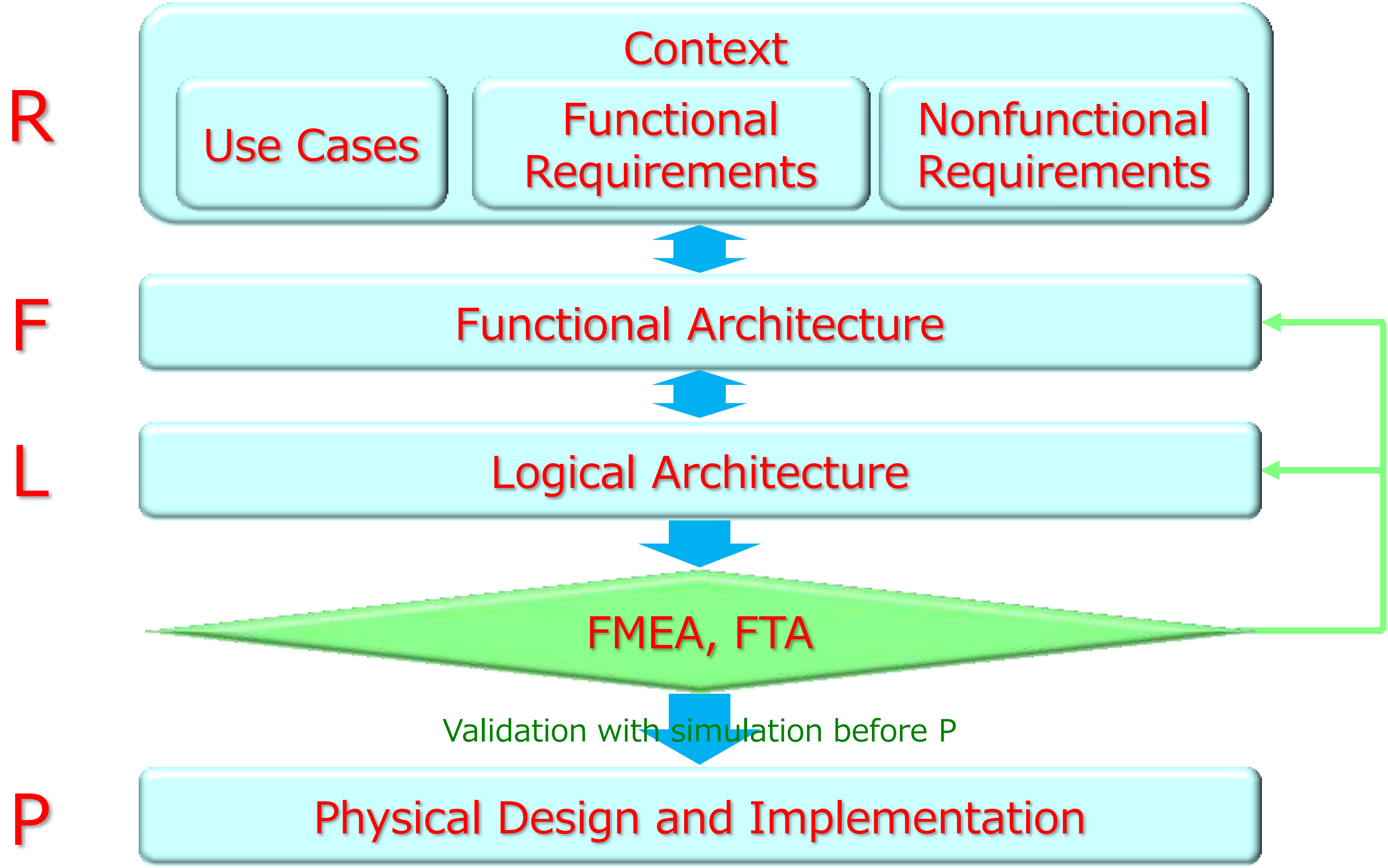
Components and Software

R F L P V

R: Requirements
F: Functional Architecture
L: Logical Architecture
P: components/software and Implementation

Current RFLP process in Nissan

- ✓ We implement FTA &FMEA after logical architecture



R
Context
Use Cases
Functional Requirements
Nonfunctional Requirements
F
Functional Architecture
L
Logical Architecture
FMEA, FTA
Validation with simulation before P
P
Physical Design and Implementation

Agenda

1. Background
2. **Introduction of Nissan's systems engineering** (RFLP process)
3. Fusion of STPA and Nissan's RFLP process
4. STPA trial result
5. Conclusion & future work

Approach to Innovation

For shifting from "Reliability Design" to "Safety Design", **we replace "FTA & FMEA" with "STPA"**

- **As "Requirements", "Safety Constraints" are needed** in addition to "Functional Requirements", "Nonfunctional Requirements" and "Use Case".

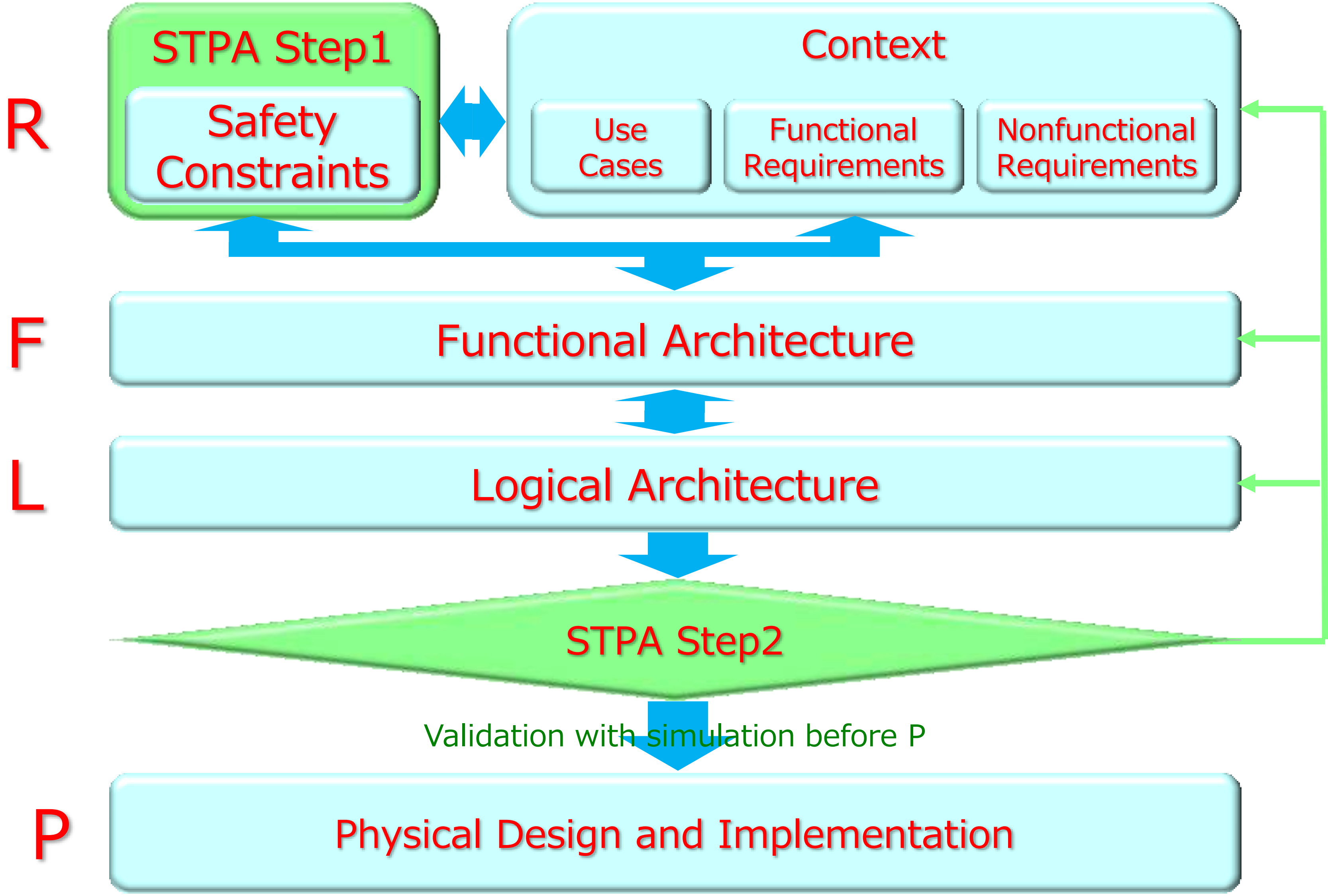
  --> Allocate "STPA step1" in "R"

- Before delivering requirements to lower layer, system design is needed to be closed

  --> **Allocate "STPA step2" after "L"**

New process under study

- ✓ For shifting from "Reliability Design" to "Safety Design", **we replace "FTA & FMEA" with "STPA"**



STPA Step1

Safety Constraints

Context

Use Cases

Functional Requirements

Nonfunctional Requirements

R

F

Functional Architecture

L

Logical Architecture

STPA Step2

Validation with simulation before P

P

Physical Design and Implementation

Agenda

1. Background

2. **Introduction of Nissan’s systems engineering** (RFLP process)

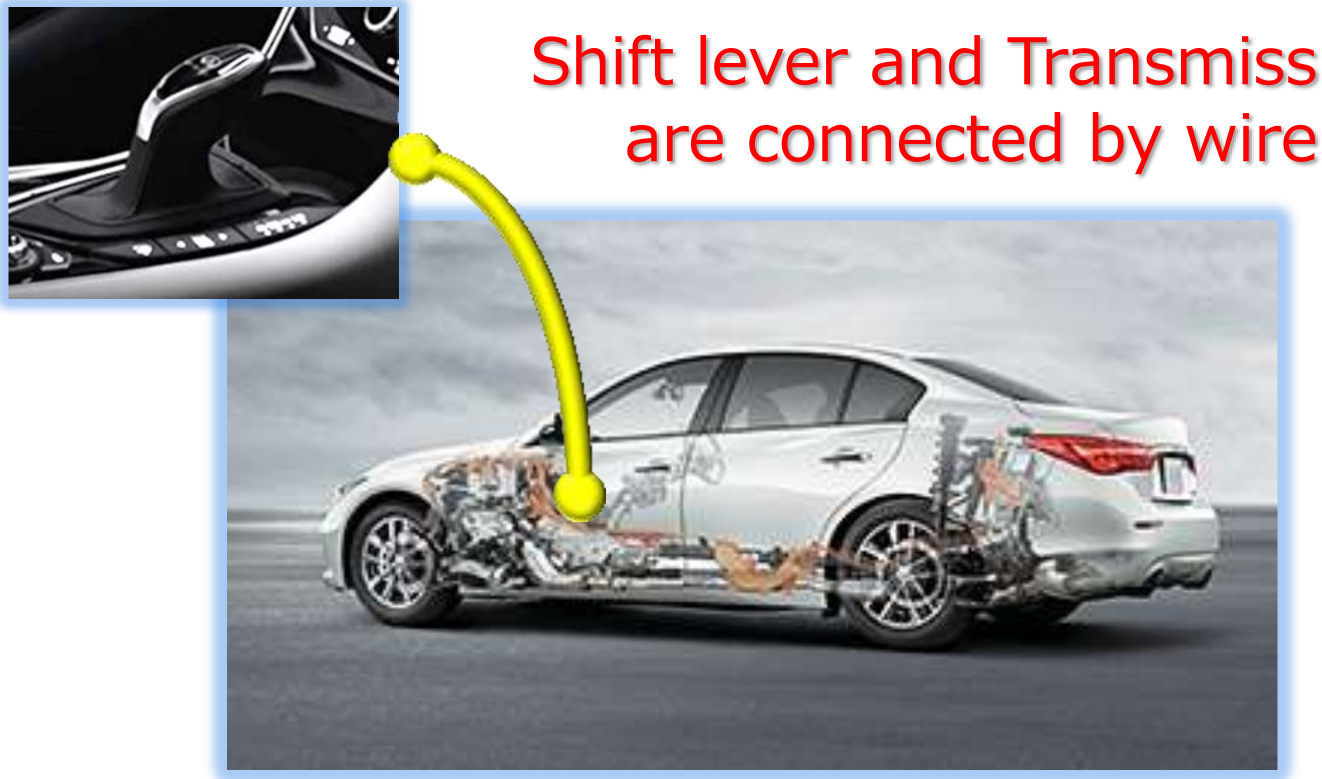
3. Fusion of STPA and Nissan's RFLP process

4. STPA trial result

5. Conclusion & future work

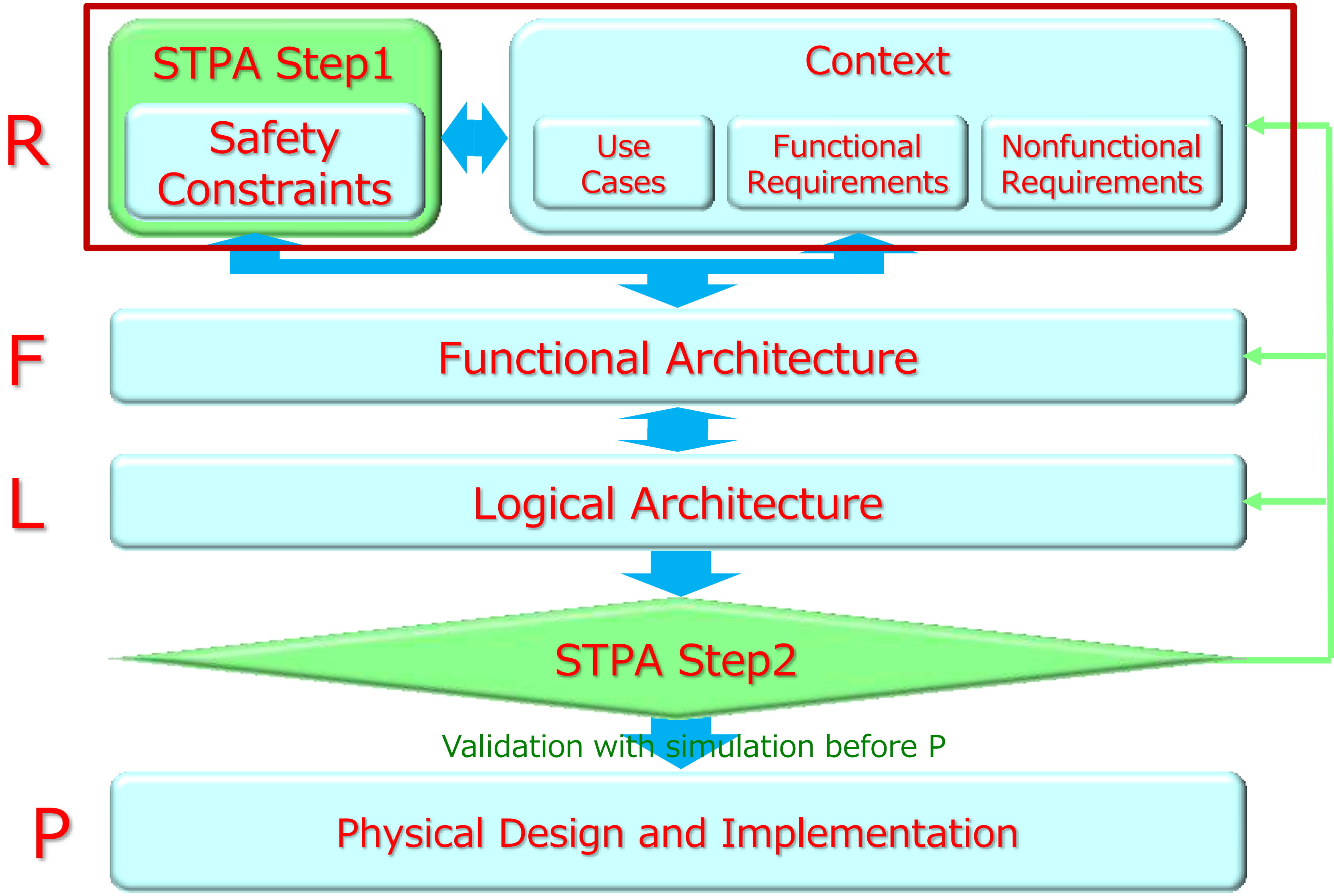
Trial system

As a trial of new process, we selected shift by wire system.



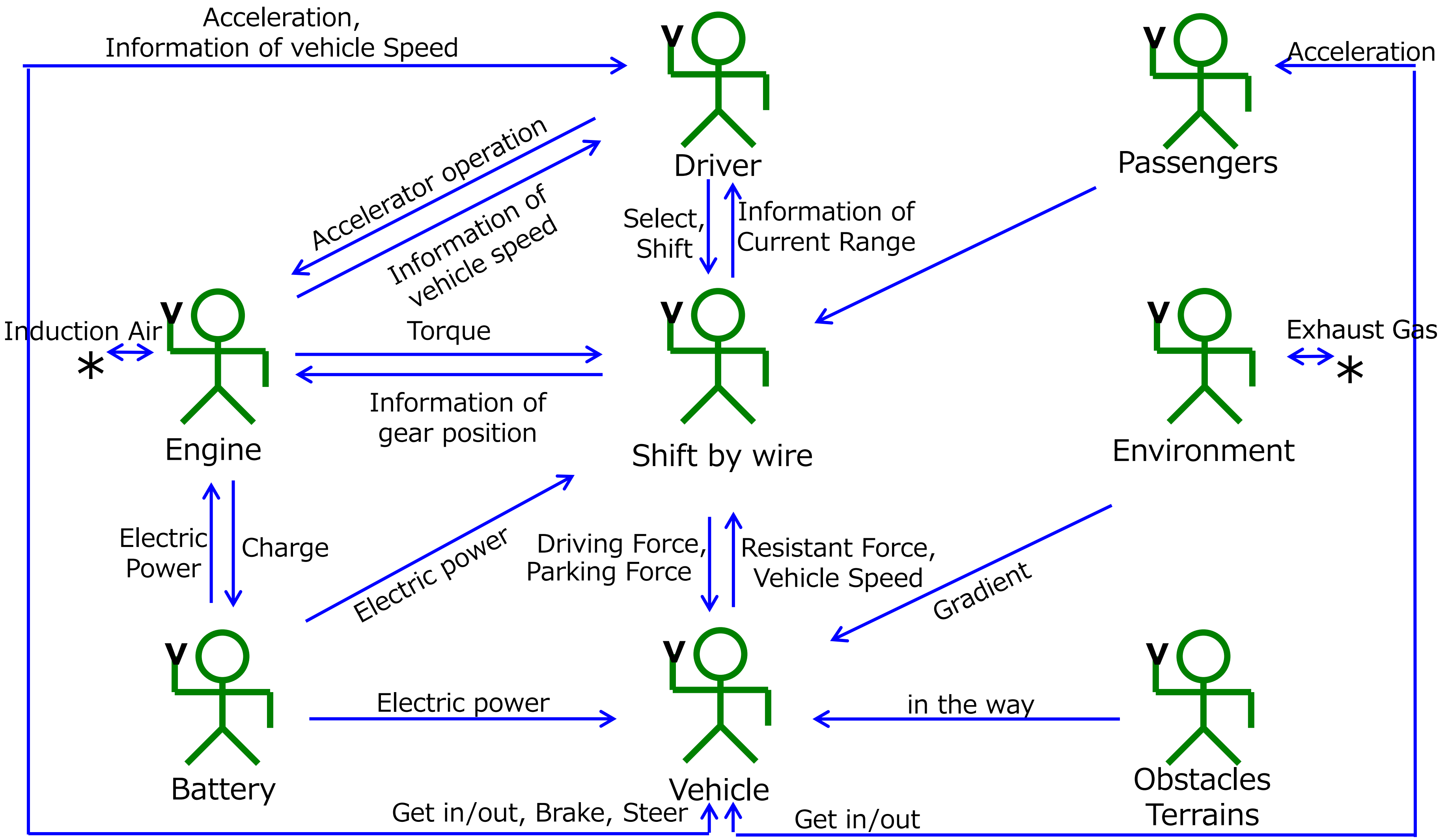
Shift lever and Transmission are connected by wire

Define requirements and implement STPA Step1



Requirements analysis in Nissan

- ✓ Interactions with scenarios between Shift by wire and stakeholder/external systems were identified



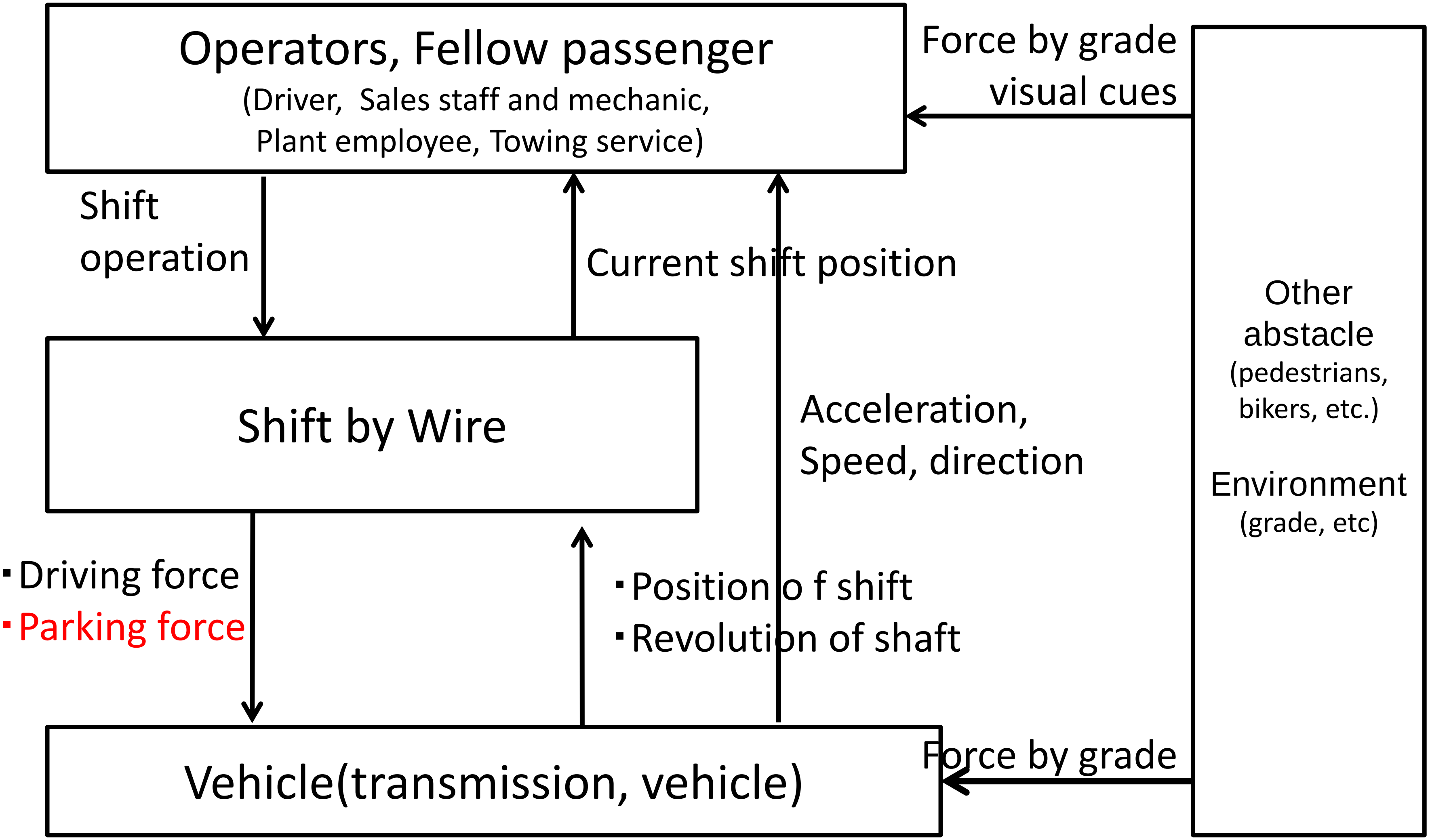
STPA : Identify Accident and Hazard

Accident	Description
A-1	Two or more vehicles collide
A-2	Vehicle collides with non-fixed obstacle
A-3	Vehicle crashes into terrain
A-4	Vehicle occupants injured without vehicle collision

Hazard	Description	Accident
H-1	Vehicle does not maintain safe distance from nearby vehicles	A-1
H-2	Vehicle does not maintain safe distance from terrain and other obstacles	A-2, A-3
H-3	Vehicle occupants exposed to harmful effects and/or health hazards	A-4

STPA : Construct Control structure

✓ Control structure was constructed easily from context diagram



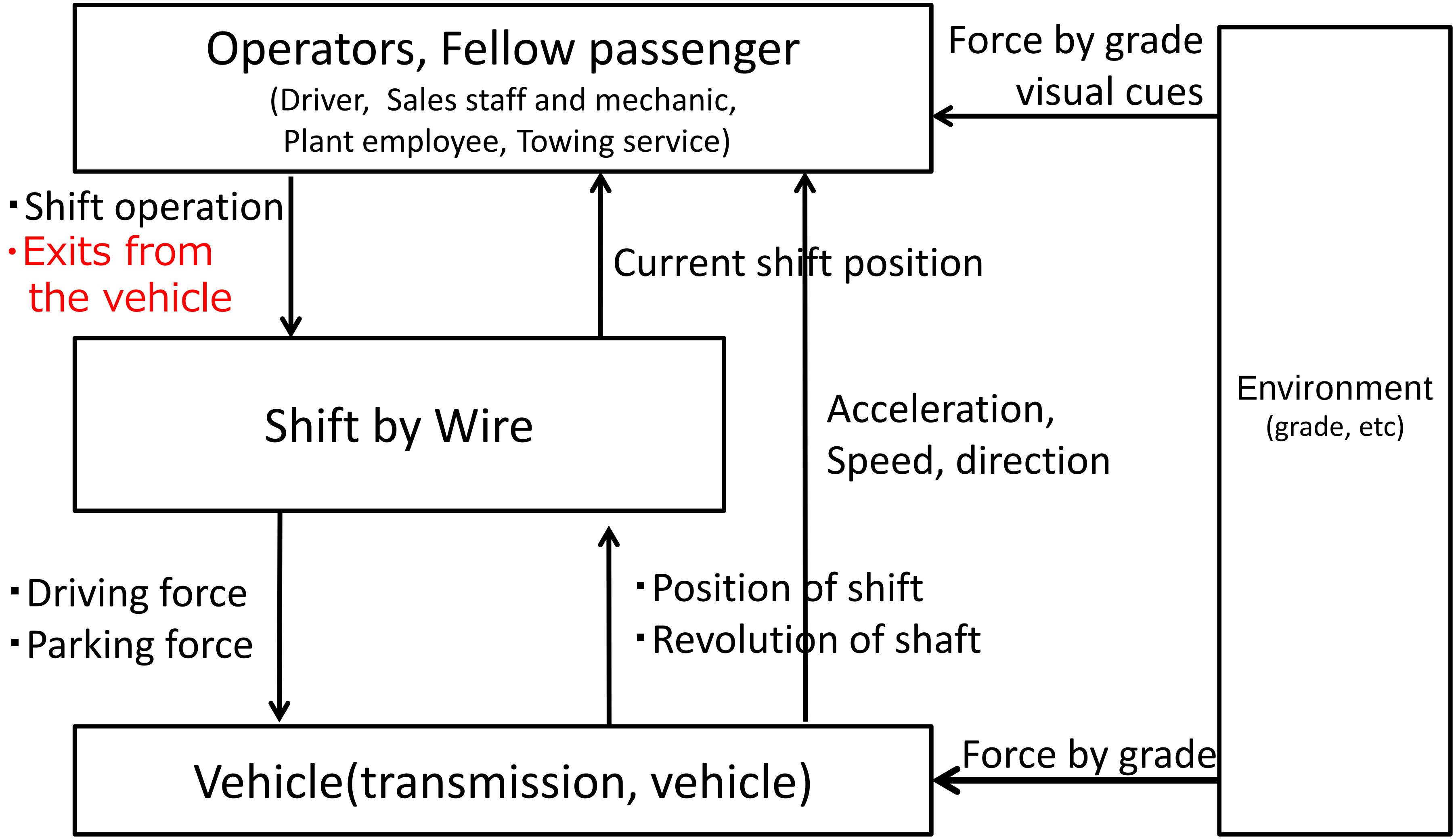
STPA Step1: Identify UCA and Safety Constraint

✓ Safety constrain was extracted as new requirement from step1

Control Action		Unsafe Control Actions	Safety Constraints
CA1 Provide parking force	Not providing causes hazard	UCA1: SBW doesn't provide parking force when driver leaves the vehicle	**SC1-1: SBW must provide parking force when driver leaves the vehicle**
	Providing causes hazard	UCA2: SBW provide parking force when vehicle is moving (>**km/h)	SC2-1: SBW must provide parking force when vehicle is moving (>**km/h)
	Too early, too late, wrong order	UCA3: SBW provide parking force too late	SC3-1: SBW must provide parking force soon (<**sec) after needed
	Stopped too soon, applied too long	UCA4: SBW stops to provide parking before diver get on the vehicle	SC4-1: SBW stops must provide parking by diver get on the vehicle

STPA Step1: Revise Control Structure

✓ Control structure was revised from safety constraint, therefore step1 was powerful to make "R" substantial.



Operators, Fellow passenger

(Driver, Sales staff and mechanic, Plant employee, Towing service)

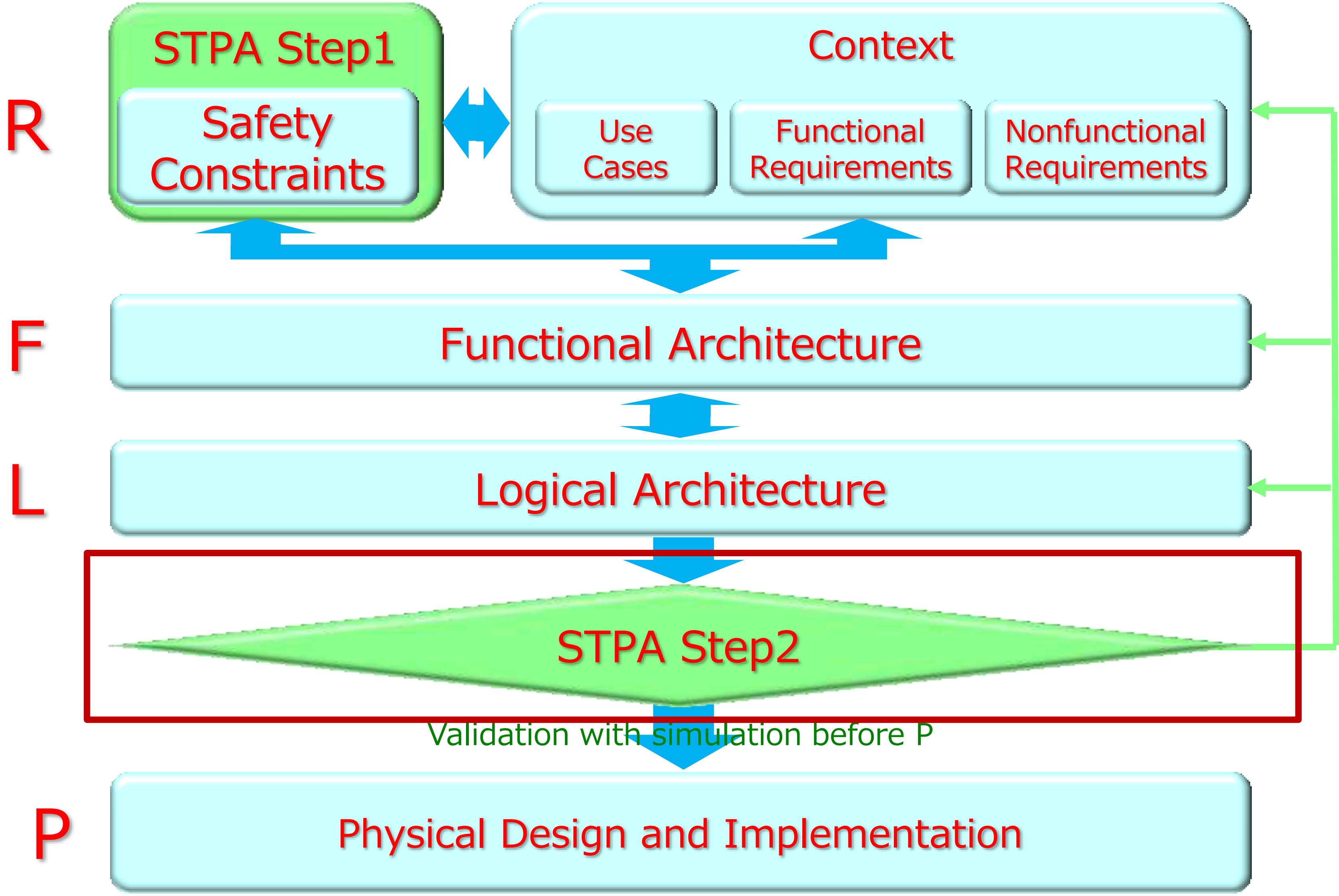
Shift by Wire

Vehicle(transmission, vehicle)

Environment

(grade, etc)

Design “F“ & “L“ in Nissan



R

STPA Step1

Safety Constraints

Context

Use Cases

Functional Requirements

Nonfunctional Requirements

F

Functional Architecture

L

Logical Architecture

STPA Step2

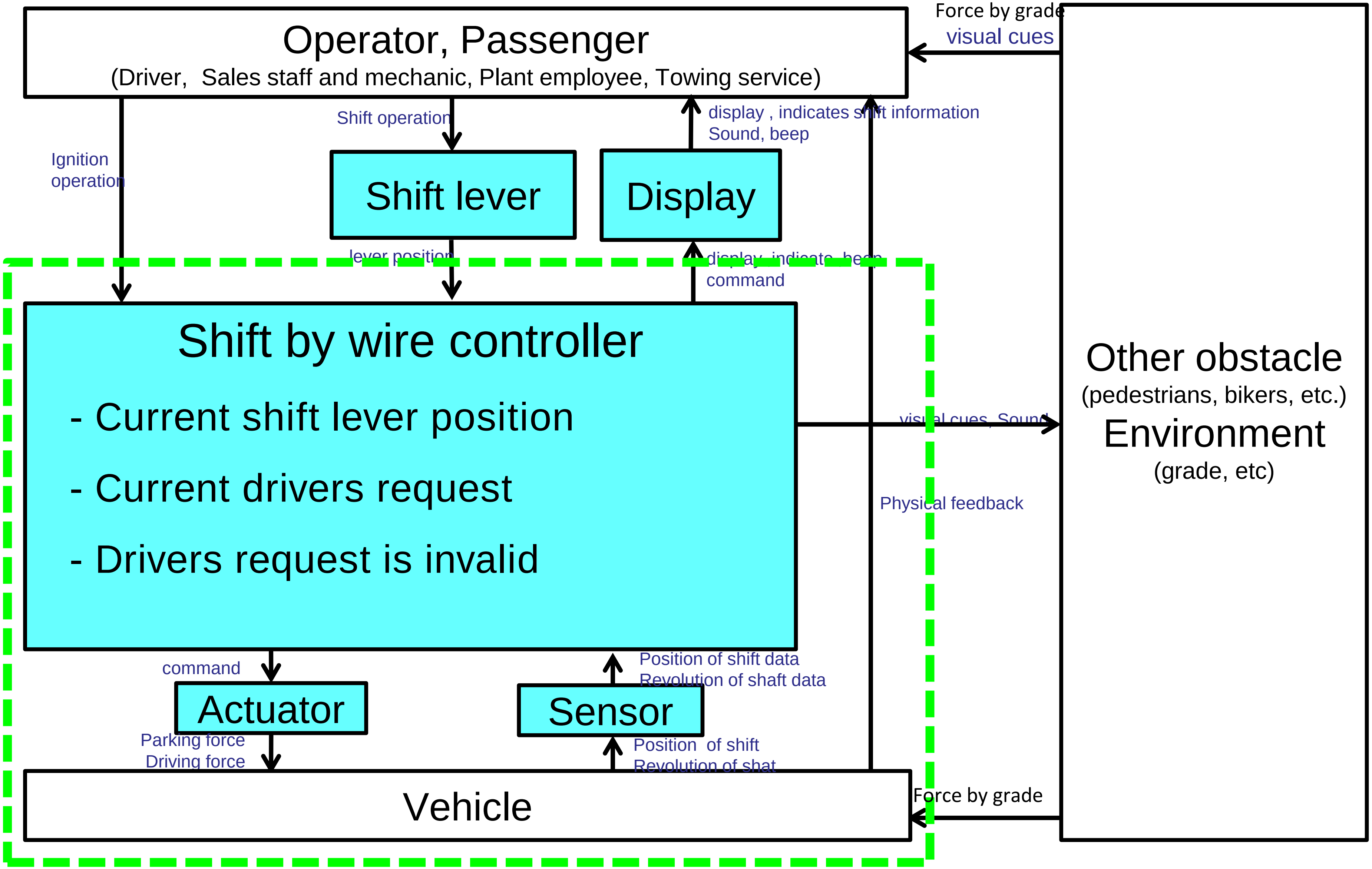
Validation with simulation before P

P

Physical Design and Implementation

STPA step2 : Identify Control Flow

✓ We identified Control flow from Control structure



Operator, Passenger

(Driver, Sales staff and mechanic, Plant employee, Towing service)

Force by grade

visual cues

Ignition operation

Shift operation

display , indicates shift information

Sound, beep

Shift lever

Display

lever position

display, indicate, beep command

Shift by wire controller

- Current shift lever position
- Current drivers request
- Drivers request is invalid

visual cues, Sound

Other obstacle

(pedestrians, bikers, etc.)

Environment

(grade, etc)

Physical feedback

command

Position of shift data

Revolution of shaft data

Actuator

Sensor

Parking force

Driving force

Position of shift

Revolution of shat

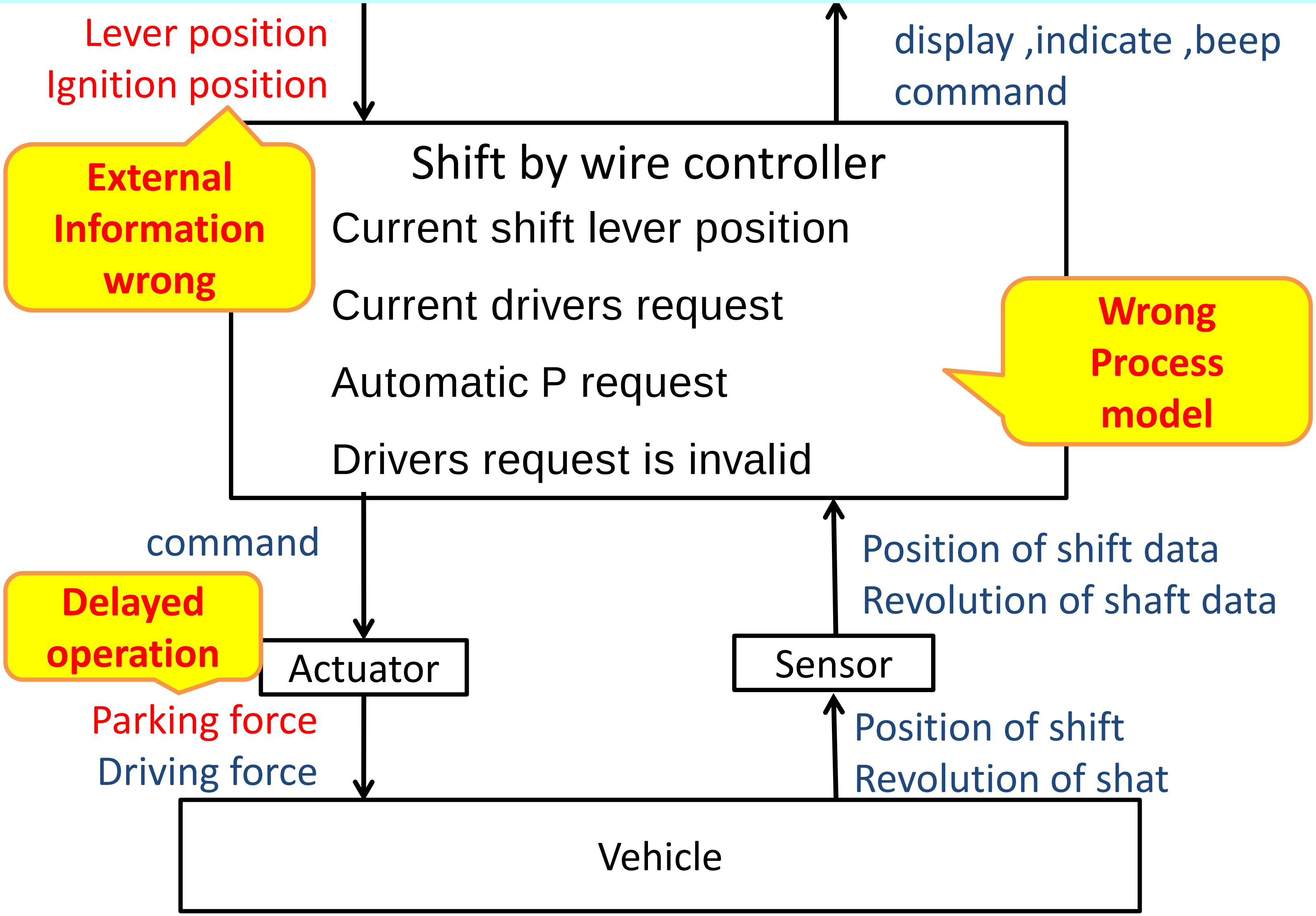
Vehicle

Force by grade

STPA step2 : Extract Causal Scenario

✓ Extracted causal scenario which violated the safety constraint

SC1-1 : SBW must provide parking force when driver leaves the vehicle



Lever position

Ignition position

display ,indicate ,beep

command

External Information wrong

Shift by wire controller

Current shift lever position

Current drivers request

Automatic P request

Drivers request is invalid

Wrong Process model

command

Position of shift data

Revolution of shaft data

Delayed operation

Actuator

Sensor

Parking force

Driving force

Position of shift

Revolution of shat

Vehicle

STPA Step2: Identify Causal Factor and Safety Req.

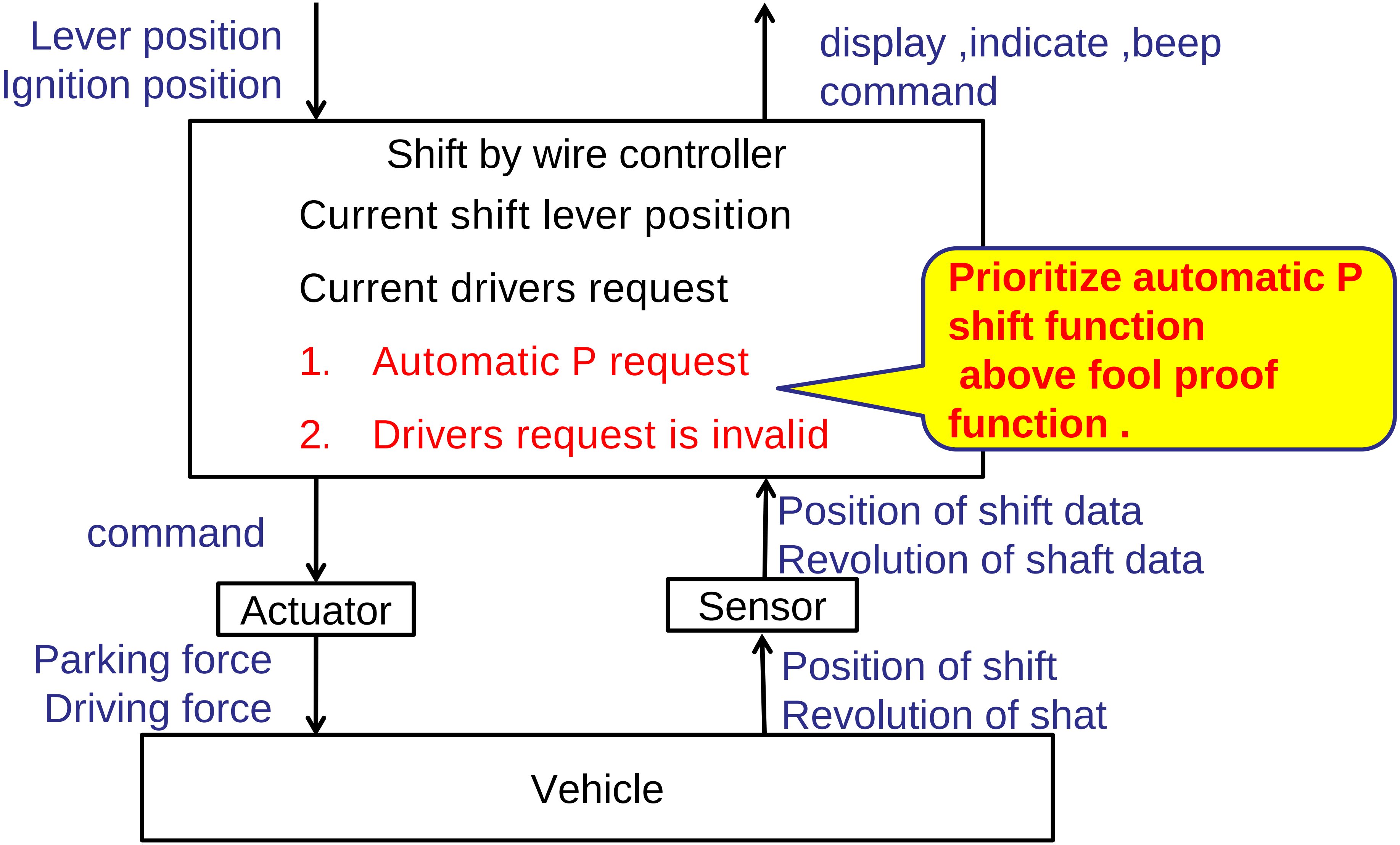
- ✓ We extracted additional safety requirements from causal factors which were failure and lack of design

SC1-1 : SBW must provide parking force when driver leaves the vehicle

Causal Scenario	Causal Factors	Safety Requirements
[External information wrong] SBW controller believes door not open, therefore shift by wire assume driver is in the vehicle.	**[Failure]** Door position switch is failed **[Failure]** CAN interface of door position is stacked	[Shift controller] detect (switch failure or CAN interface stacked) deliver warning message "Use parking brake" within ** sec
[Wrong process model] SBW controller reject driver's P shift request.	**[Lack of logical design]** automatic P shift function is invalid by fool proof function, in case if driver operate ignition off while vehicle speed is higher than **km/h	[Shift controller] Prioritize automatic P shift function above fool proof function .
[Delayed operation] Driver make P shift operation. But vehicle speed is increased by slope, parking gear is not engaged by ratcheting behavior	**[Lack of functional design]** Actuator operate too slow by low battery voltage.	[Shift controller] deliver warning message "Use parking brake" within ** sec

STPA step2 : Revise Control Flow

✓ Control flow was revised by new requirements, therefore step2 was powerful to check and close design



Lever position
Ignition position

display ,indicate ,beep
command

Shift by wire controller

Current shift lever position

Current drivers request

1. Automatic P request
2. Drivers request is invalid

Prioritize automatic P shift function above fool proof function .

command

Position of shift data
Revolution of shaft data

Actuator

Sensor

Parking force
Driving force

Position of shift
Revolution of shat

Vehicle

Agenda

1. Background

2. **Introduction of Nissan’s systems engineering** (RFLP process)

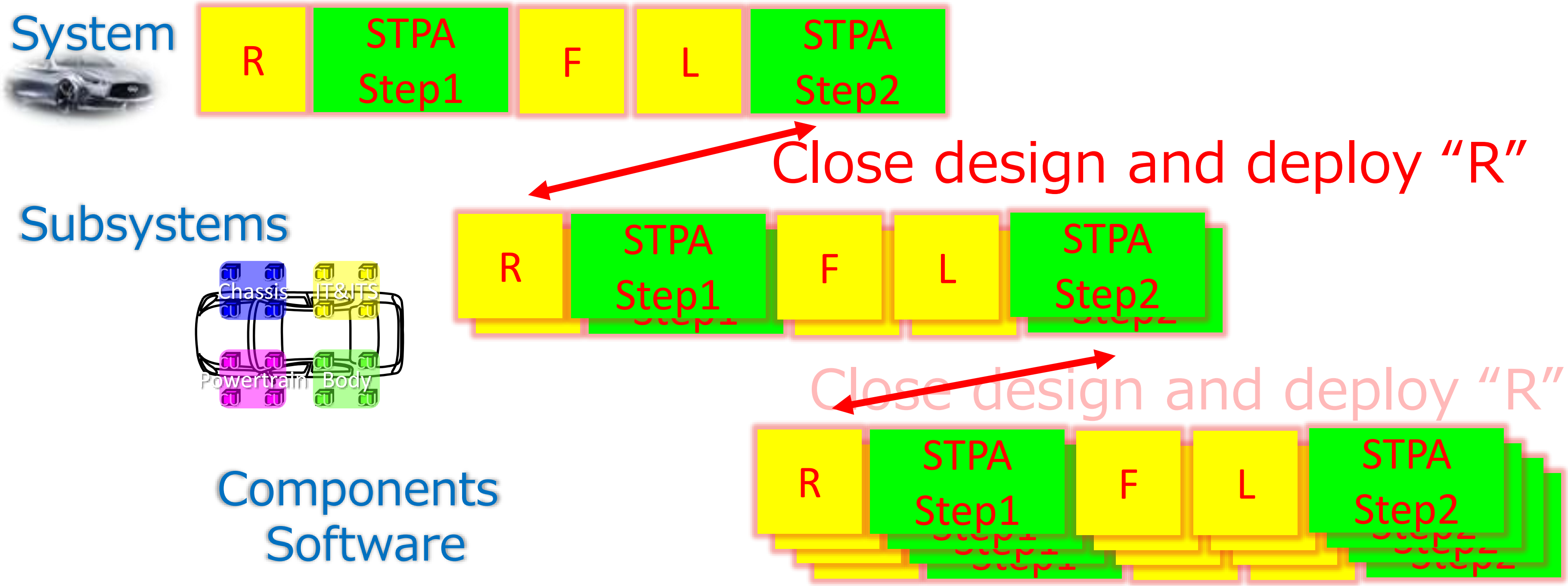
3. Fusion of STPA and Nissan's RFLP process

4. STPA trial result

5. Conclusion & future work

Conclusion

- ✓ STPA had a strong affinity to layered RFLP process and effectiveness for complex and large system
- ✓ We allocated STPA Step1 in “R” and step1 was powerful to make “R” substantial.
- ✓ We allocated STPA Step2 after “L” to check and close the design before deploying req. to lower layer systems



System

R | STPA Step1 | F | L | STPA Step2

Close design and deploy “R”

Subsystems

R | STPA Step1 | F | L | STPA Step2

Close design and deploy “R”

Components
Software

R | STPA Step1 | F | L | STPA Step2

Thank you

✓ For future work, we will study

-Advanced STPA and tools
-Human factors issues

✓ Technical information exchange is welcome.

Please contact to tetsunobu-morita@mail.nissan.co.jp

Appendix

Words definition

✓ The words are defined by Engineering a Safer World.

- Reliability
- Safety
- Accidents
- Hazards
- Unsafe Control Action
- Causal Scenario
- Causal Factor
- Safety Requirement