# Safety Argument based on GSN for Automotive Control Systems

Yutaka Matsubara
Nagoya University
yutaka@ertl.jp
02.26.2014

# Agenda

1. Safety argument in ISO26262
2. Requirements related to safety argument
3. Goal Structuring Notation(GSN)
4. Examples of GSN
5. Discussion
6. Conclusion

# Safety argument in ISO 26262

Product argument

- A safety argument that argues safety based directly on **the features of the item implemented**.

Process argument

- A safety argument that argues safety based on **the features of the development and assessment process**.

We focused on product argument for safety of an Electric Power Steering(EPS) control system.

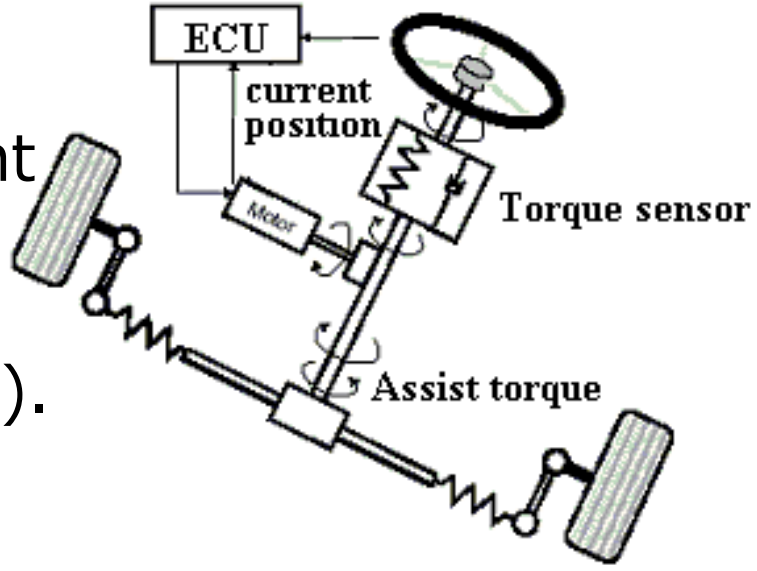
# EPS control system

## Main functions

- EPS uses an electric motor to assist the driver of a vehicle.
- Sensors detect the position and torque of the steering column, and an ECU applies assistive torque via the motor.
    - This allows varying amounts of assistance to be applied depending on driving conditions.

## Our activities

- Hazard analysis and risk assessment
- Specifying safety goals, functional safety requirements(FSRs), and technical safety requirements(TSRs).
- Verification and Validation of FSRs and TSRs



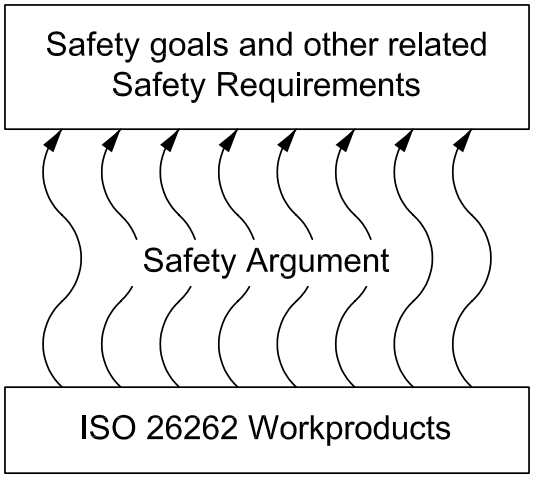

http://www.ni.com/white-paper/4204/en/

Notice: This diagram is not related to real products.

# Requirements related to safety argument

## Safety Case

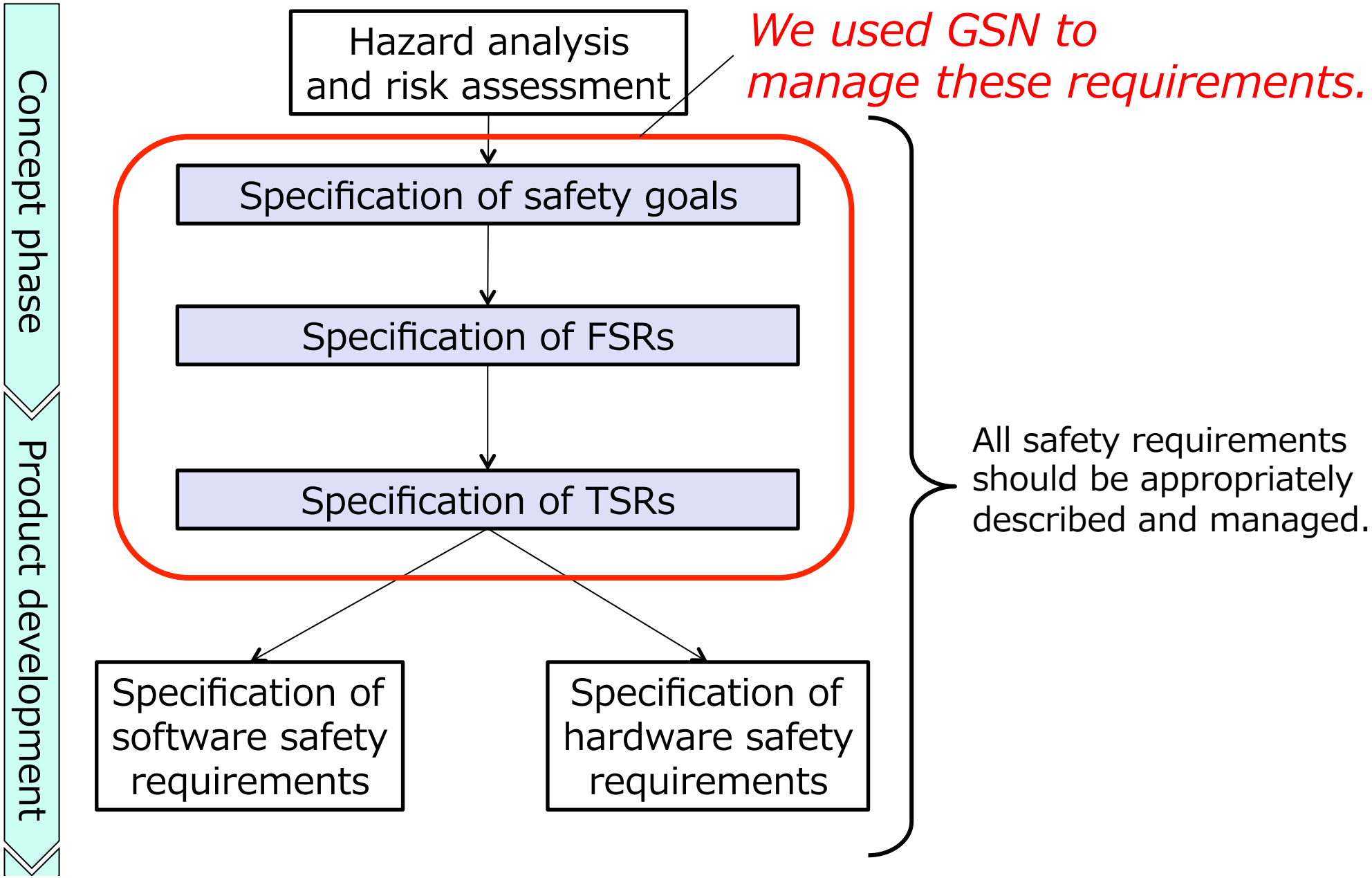
- The purpose of a safety case is to provide a clear, comprehensive and defensible argument, supported by evidence to guarantee safety of an item.
- A safety case for ASIL (A), B, C or D should be generated as a work product during the safety lifecycle (part.2-6.4.6).




## Management of Safety Requirements

- Objectives are to ensure
  - the correct specification of safety requirements with respect to their attributes and characteristics, and
  - consistent management of safety requirements during the safety lifecycle.
- To achieve the above objectives, requirements of management of safety requirements are listed in part. 8 sec. 6.

# Structure of safety requirement



# Management of safety requirements

To comply with the followings, appropriate notation and management techniques are required.

a) Hierarchical structure

- The safety requirements must be structured in several successive levels.

b) Organizational structure

- The safety requirements of each level are grouped together, which usually corresponds to the architecture.

c) Completeness

- The safety requirements at one level fully implement all of the safety requirements of the previous level.

*ISO 26262:part 8 ,clause 6.4.4.3*

# Management of safety requirements(cont.)

## d) External consistency

- Multiple safety requirements must not contradict each other.

## e) No duplication

- The contents of the safety requirements are not repeated in any other safety requirements at a different level of the hierarchical structure.

## f) Maintainability

- The set of requirements can be easily modified or extended, e.g., by the introduction of new versions of requirements or by adding/removing requirements from the set of requirements.

**How can we achieve the above requirements?**

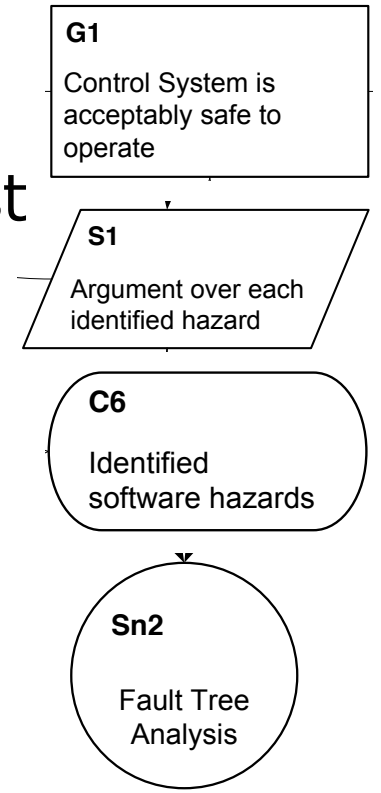
# Goal Structuring Notation(GSN)

## What's GSN

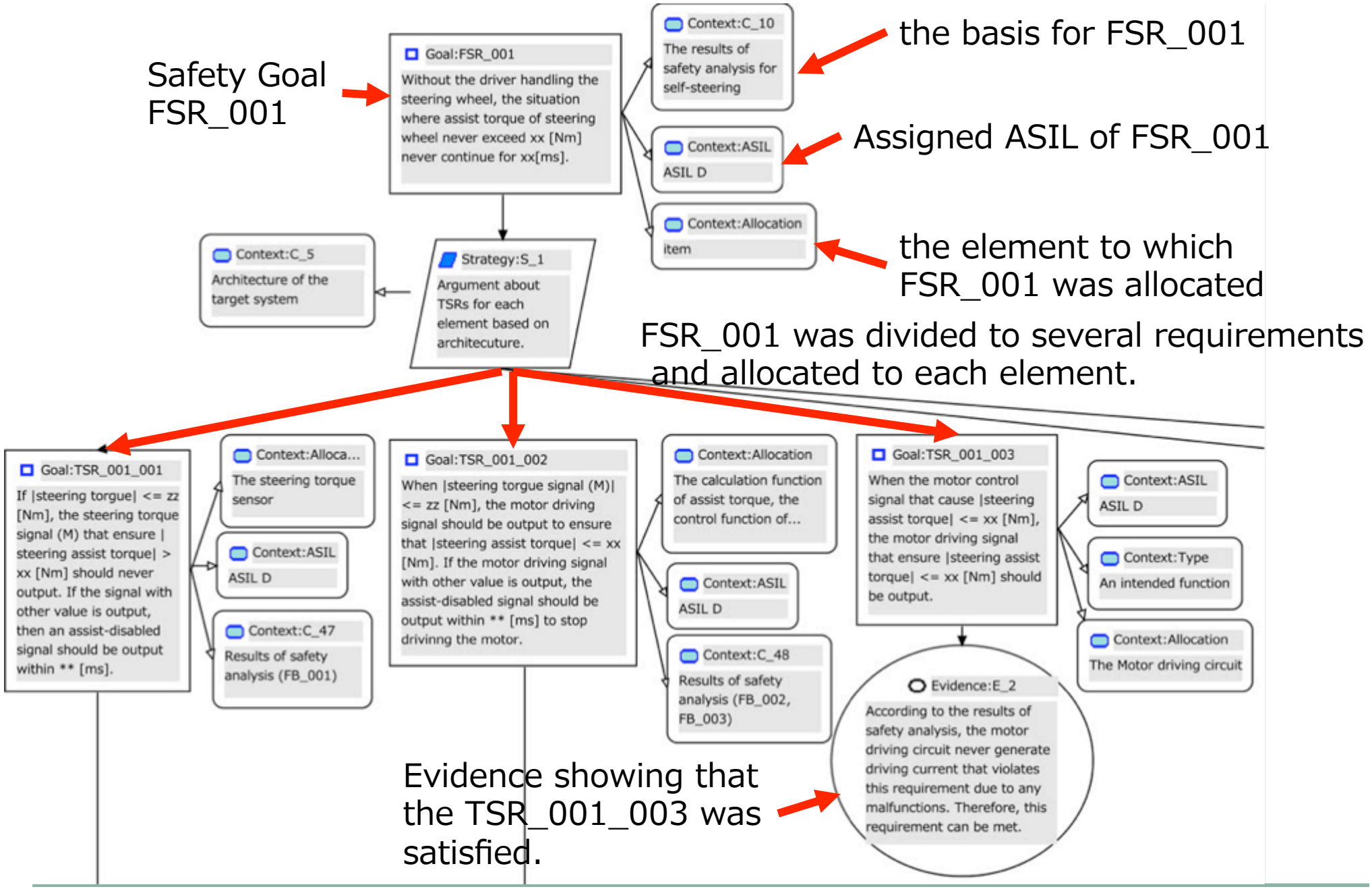
- GSN is a graphical argument notation.
- It can be used to document explicitly the elements and structure of an argument and the argument's relationship to evidence.

## Main notations

- Goal(Requirement): the claims of the argument, or the safety objectives that must be addressed to assure safety.
- Strategy(Argument): how the evidence indicates compliance with the requirements.
- Context: identifying the basis for the argument presented.
- Solution(evidence): evidence to guarantee that a goal could be satisfied.



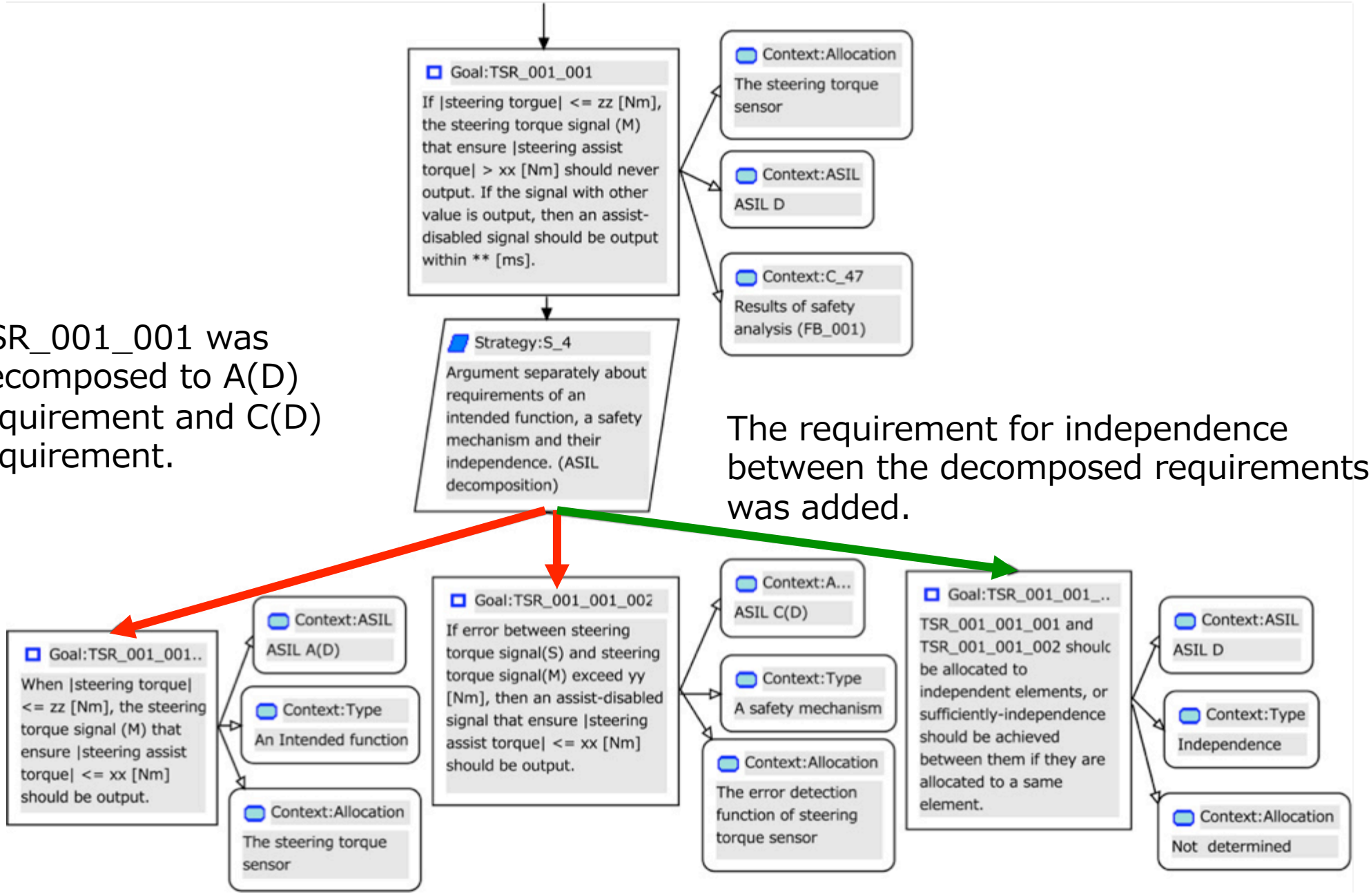
# Example of GSN: Organizational structure



# Example of GSN: ASIL decomposition

TSR_001_001 was decomposed to A(D) requirement and C(D) requirement.

The requirement for independence between the decomposed requirements was added.



# Good points of GSN compared to natural languages

- The relationships between a goal and sub-goals could be clearly described by *argument* elements. → **Req. b)**
- The completeness of the safety requirements specifications becomes obvious. → **Req. c)**
- Duplication and contradiction of safety requirements specifications could be avoided by reviewing the relationships between the specifications. → **Req. d),e)**
- A hierarchical structure is easily achieved by a *system* element. → **Req. a)**

**GSN was one of appropriate techniques for describing a safety case and management of safety requirements.**

# Weak points

- The semantics of the *context* elements should be restricted because the elements can be used with various meanings. → **Req. f)**
- Tool cooperation should be improved to ensure traceability.
  - For example, the GSN description tool should work with the traceability management tools, hazard analysis tools, system architectures, and so on.
- For ASIL C or D requirements, other semi-formal or formal methods may be needed because contents of each element of GSN are described in natural languages.

# Requirements for notation of safety requirements

## Notation methods

ISO 26262-8:2011, Table.1

| Methods | | ASIL | | | |
|---|---|---|---|---|---|
| | | A | B | C | D |
| 1a | Informal notations for requirements specification | ++ | ++ | + | + |
| 1b | Semi-formal notations for requirements specification | + | + | ++ | ++ |
| 1c | Formal notations for requirements specification | + | + | + | + |

*highly recommended*

## Practical situation in Japan

- The safety requirements have been described in natural languages in many cases.

Informal notation

To develop items with ASIL C or D, semi-formal notations should be used instead of natural languages.

# Semi-formal notation methods

Definition of “Semi-formal” notation

- Descriptive techniques where the syntax is completely defined but where the semantics definition can be incomplete.

Examples

- System Analysis and Design Techniques (SADT)
- Unified Modeling Language (UML)
  - Widely used in practical situation

These methods are suitable for design of item and software, but not suitable for description of requirements.

→ **A method that is suitable for description of safety requirements is required.**

# Conclusion

- We presented a case study of a safety argument description for the EPS control system by GSN.
- We compared the capacities of natural languages and GSN for describing the safety case and management of safety requirements specifications.
- Based on the case study, we confirmed that GSN was an appropriate technique for these purposes.
- However, some future works were found to spread GSN in practical situations.

*Thank you for your attention. Any question?*

# References


1. ISO: ISO 26262:2011 Functional safety - road vehicles. ISO, (2011)
2. Goal Structuring Notation Working Group: GSN Community Standard Version 1. http://www.goalstructuringnotation.info/, (2011)
3. B. Palin, D. Ward, I. Habli and R. Rivett: ISO 26262 safety cases: compliance and assurance. In: IET Intl. System Safety Conf., (2011)
4. Y. Matsuno: D-Case Ediotor: http://www.il.is.s.u-tokyo.ac.jp/deos/dcase/