

# Introduction to Intelligent Vehicles

## [ 14. Certification ]

Chung-Wei Lin

[cwlin@csie.ntu.edu.tw](mailto:cwlin@csie.ntu.edu.tw)

CSIE Department

National Taiwan University

Fall 2019

# Certification

## □ Certification

- "The procedure by which an authorized person or agency assesses and verifies characteristics of a system or product in accordance with established requirements, standards, or regulations." [Cofer '13]

## □ Motivations

- Provide a proof of quality
- Enhance customers' confidence
- Reduce companies' liability (?)
- Prove the fulfillment of governments' regulations

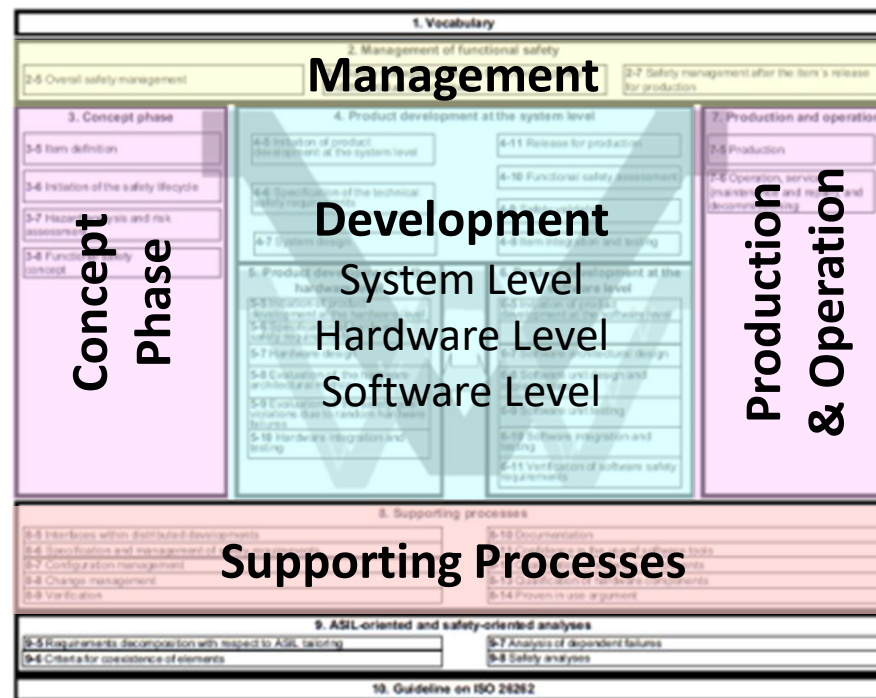


## □ Current status of automotive certification

- It has been well practiced in the domains of aviation and medical devices, but not so much for automotive systems

# ISO 26262

- ISO 26262 is recognized as the state-of-the-art standard for functional safety of automotive systems



# Automotive Safety Integrity Level (1/2)

## ❑ Severity Classifications (S)

- S0: no injuries
- S1: light to moderate injuries
- S2: severe to life-threatening (survival probable) injuries
- S3: life-threatening (survival uncertain) to fatal injuries

## ❑ Exposure Classifications (E)

- E0: incredibly unlikely
- E1: very low probability
  - Injury could happen only in rare operating conditions
- E2: low probability
- E3: medium probability
- E4: high probability
  - Injury could happen under most operating conditions

# Automotive Safety Integrity Level (2/2)

## □ Controllability Classifications (C)

- C0: Controllable in general
- C1: Simply controllable
- C2: Normally controllable (most drivers could act to prevent injury)
- C3: Difficult to control or uncontrollable

## □ ASIL Level D

- S3 + E4 + C3

## □ ASIL Level D → ASIL Level C → ASIL Level B → ASIL Level A

- In general, for each single reduction in any one classification, there is a single level reduction in the ASIL

## □ ASIL Level A → QM

- No safety relevance
- Only standard Quality Management processes required

# Examples

## ❑ Hardware level

- During hardware design, "simulation" is recommended for ASILs C and D
- Work products: verification plan, specification, and report

## ❑ Software level

- During software unit design and implementation, some software structures are NOT recommended for ASIL D
  - Dynamic objects and variables
  - Multiple uses of variable names
  - Implicit type conversions
  - Unconditional jumps
  - Recursions
- Work products: software unit design specification, software unit implementation, and software verification report

# Limitations and Short Summary

## ❑ Limitations

- The standard plans to but not yet consider connectivity and autonomy
- There is no enforcement from governments or strong push from customers
- Original Equipment Manufacturers (OEMs) do not have access to suppliers' confidential information
  - Any certification protocol?
- Process-based certification vs. product-based certification

## ❑ Summary

- ISO 26262 is recognized as the state-of-the-art standard for **functional safety** of automotive systems
- It can provide some guidelines for the legislation of law and regulation

# Certification Protocol: Motivation

- ❑ A potential conflict between certification issuers (e.g., OEM) and software suppliers (developers)
  - A certification process represents a systematic way to inspect the source codes
  - Some source codes of software suppliers (developers) are confidential
- ❑ Desired properties
  - Authenticity
    - Only authenticated results from compilers and analysis tools (verification, simulation, and/or testing) are considered by the certification issuers
  - Confidentiality
    - Sensitive source codes of the software suppliers and developers are not released to certification issuers



# Certification Protocol: Example

## ❑ Trusted third-party

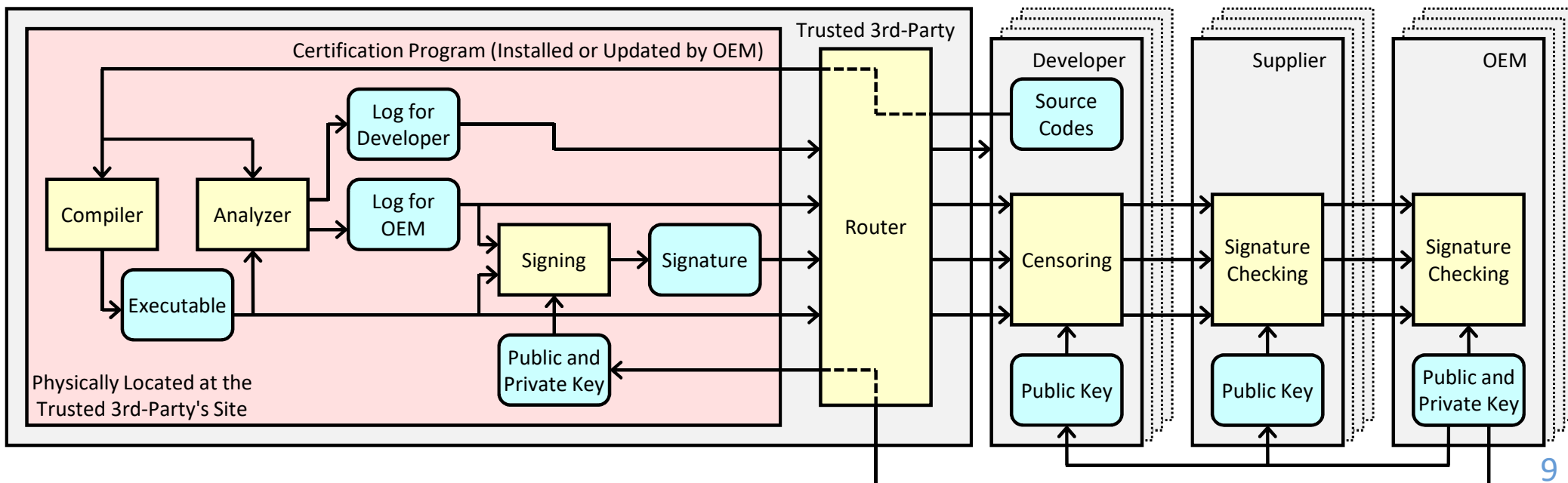
- Run a certification program which consists of a compiler and an analyzer
- Maintain a router which controls the input and the output

## ❑ Certification program

- All of the compiler, the analyzer, and the private key are updated by the OEM
- The updating process must be unidirectional to guarantee confidentiality

## ❑ Router

- Only the corresponding developer can be the receiver



# Q&A