# WG 2: ASIL: HOW TO ALLOCATE, HOW TO MIX, WHAT TO CONSIDER

## SESSION 4: HOW-TO'S WORK GROUPS

24TH MARCH 2021
RICCARDO VINCELLI
DIRECTOR, FUNCTIONAL SAFETY COMPETENCE CENTER,
AUTOMOTIVE TECHNOLOGY DEVELOPMENT DEP.
RENESAS ELECTRONICS CORPORATION

# RICCARDO VINCELLI

Working as Director of the Functional Safety Competence Center

- >20 years at Renesas
- Responsible for independent technical assessment of Renesas products (MCU, SoC, ASICs, SW) targeting world wide market

Involved in

- Safety activities since 2005 for the development of Renesas components based on IEC60730, IEC61508 and ISO26262
- Standardization activities of IEC61508, ISO26262 (and ISO PAS 19451), UL4600 as well as SAE Safety Groups

**PAS**: Publicly Available Specification

# TARGET OF THE DISCUSSION

- Presentation covers a basic argument triggering however challenging points
- Many engineers are today familiar with the concept of ASIL and may expect this presentation for beginners
- However still too many engineers do fall in some basic traps
- Topics we will be covering today
  - Is the intended functionality always assigned an ASIL?
  - Is a safety related requirement always assigned an ASIL?
  - Does the reason an ASIL is assigned has an influence on the development/capabilities of an element?
  - Is the ASIL alone sufficient to identify the capabilities of an element?
  - What are the implications when dealing with SEooC?
  - Can I mix different ASILs?

# STEPS TO FOLLOW WHEN DEVELOPING AN ITEM

*Airbag deployed in case of a crash to protect the driver*

Can fall into ISO21448 (SOTIF) scope

Start with defining the intended functionality

*A fault may cause the airbag to deploy also in absence of a crash*

Perform hazard analysis and risk assessment (HARA) to judge effect of faults

*Hazard is present all the time and can have a very sever impact with no controllability from the driver*

Severity

Controllability


Probability of Exposure

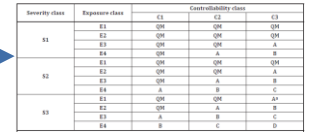
ISO26262 scope

*Avoid airbag being deployed due to a fault*

Safety Goal needed?

Yes

*ASIL D*

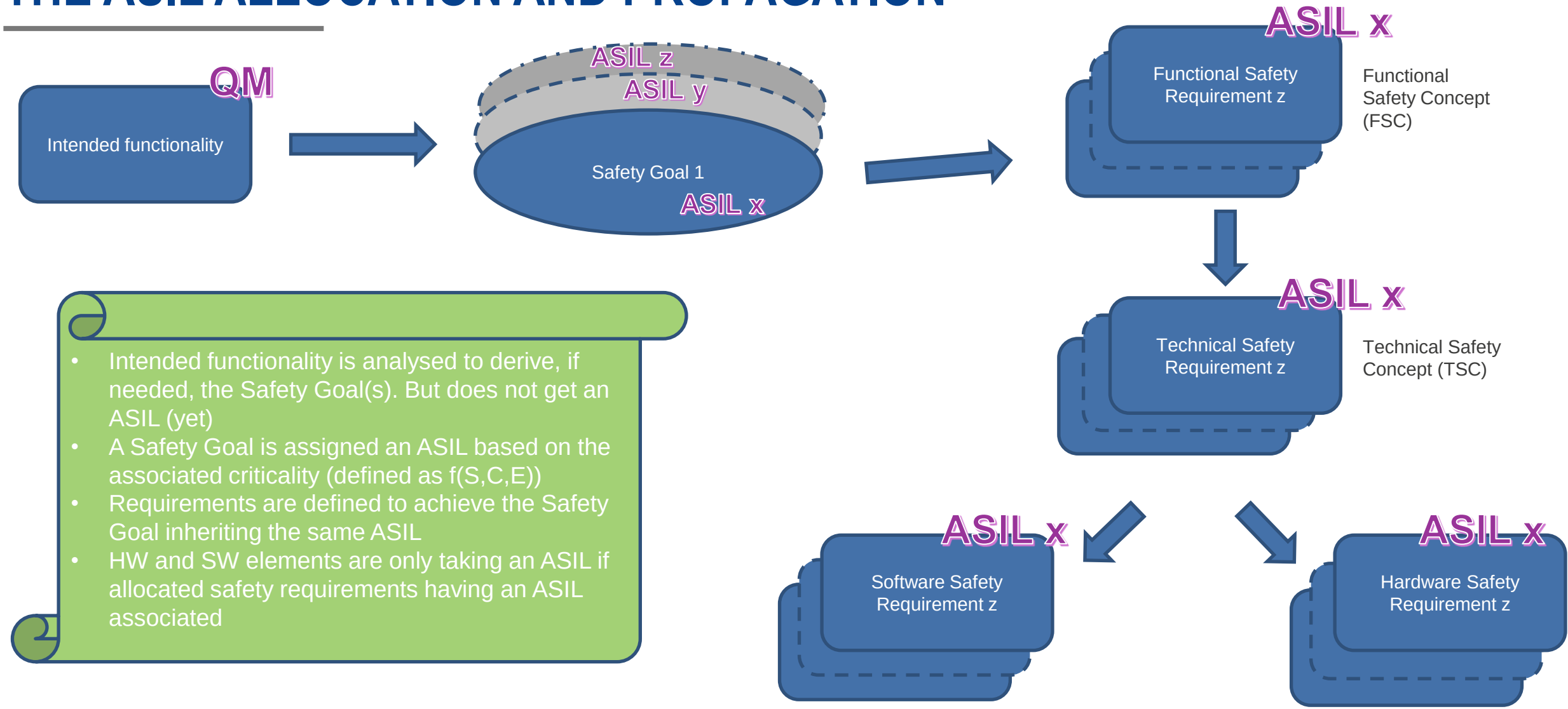


QM or no ASIL

QMS scope

- Out of scope of ISO26262 does not necessarily mean “non-safety related”! It may be safety related but having a so low risk not to require compliance to ISO26262

# THE ASIL ALLOCATION AND PROPAGATION




- Intended functionality is analysed to derive, if needed, the Safety Goal(s). But does not get an ASIL (yet)
- A Safety Goal is assigned an ASIL based on the associated criticality (defined as f(S,C,E))
- Requirements are defined to achieve the Safety Goal inheriting the same ASIL
- HW and SW elements are only taking an ASIL if allocated safety requirements having an ASIL associated

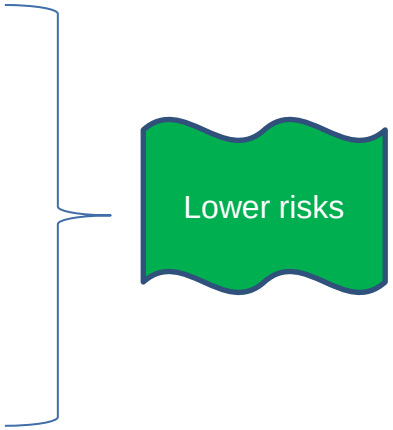
# AND IN CASE OF SEooC?

- Safety Element out of Context are elements developed without targeting a specific item
- Quite useful option when targeting elements that may end up in a large number of final items
- The main difference from a full development is that a number of inputs are replaced with assumptions that must be confirmed or addressed before the final production
- The development for an SEooC can start at different points of the full lifecycle
  - SEooC System
    - At least at TSC level
  - SEooC HW component
    - At least at HW requirements level but with some basic TSC considerations to link to expected SW and external elements that may be required
  - SEooC SW component
    - At least at SW requirements level – in many cases SW is developed at least in the context of the associated SEooC HW safety concept

- For SEooC the ASIL is assigned based on assumptions

# CAN THE ASIL CHANGE DURING THE PROPAGATION?

- The ASIL is allowed to change only in 3 specific conditions:
  1. Co-existence with requirements having an higher ASIL
     - This is when the requirement is allocated to an (SW or HW) element that is also allocated requirements derived from a stricter SG **and** the analysis shows that a possible (random HW or systematic) fault may interfere with such requirements
     - In this case the highest ASIL must be considered
     - Described in ISO26262-9, 6
  2. Requirement decomposition with respect to ASIL tailoring (“ASIL decomposition”)
     - Criticality can be relaxed as dealing with MPF
     - Described in ISO26262-9, 5
  3. Safety mechanisms to prevent Dual Point Failures
     - Criticality can be relaxed as dealing with MPF
     - Described in ISO26262-4, 6.4.2.5


- In all other situations the ASIL has to remain the same as the ASIL of the Safety Goal it is derived from

# AND IN CASE OF SEooC?

- In an SEooC development also the ASIL may either be assumed or derived using some assumed inputs
- The actual required ASIL may differ from the one considered during the SEooC development
  - Item requires same ASIL as the one considered
    - A confirmation about the suitability is still needed (remember: ASIL A, B and C can be derived from different combinations of severity/exposure/controllability that, in turn, may also lead to quite different requirements!)
  - Item requires a higher ASIL than the one considered
    - There may be some critical gaps that may not allow the usage of the SEooC element without some re-work
  - Item requires a lower ASIL than the one considered
    - The SEooC element may be considered as “overdesigned” for what is needed and then usable. However a full analysis shall always be performed to really judge all implications
    - Note: ASIL decomposition can be an option to consider in this case

- The capabilities of the elements available or to be developed will influence the functional safety concept

# WHAT IS THE REAL MEANING OF ASSIGNING AN ASIL?

- ISO26262 specifies rules to follow, unless tailored out with a justification, based on the ASIL assigned
  - ASIL-independent requirements
  - Requirements recommended or highly recommended based on the ASIL
  - Methods recommended or highly recommended based on the ASIL
  - Quantitative targets (SPFM/LFM/PMHF/EEC) suggested for ASILs B to D
- Still the ASIL alone does not give sufficient information about the criticality associated
  - Same ASIL, with only exception of ASIL D, can be linked to different severity/exposure and controllability classes
- It does provide however an indication about the rigour expected or efforts (to be) spent in reducing the risk of violating the safety goal (or top level requirement in case of SEooC) due to systematic and/or random HW faults
  - This is strongly context dependent (back to the label!)
  - Two elements may have same functionality and same ASIL, but one assumed to have all requirements as potential SPF and one having only few or no requirements as potential SPF (remember ASIL decomposition!). This can lead to quite different products!
  - In the worst case an element targeting lower ASIL could be even more “robust” than one with higher ASIL…

**SPFM**: Single Point Fault Metrics, **LFM**: Latent Fault Metrics, **PMHF**: Probabilistic Metric for HW random Faults, **EEC**: Evaluation of Each Cause of safety goal violation

# WHAT IS THE IMPLICATION OF THE ASIL?

- Whenever an ASIL is assigned this requires 2 main considerations

1. Suitability in term of systematic faults

   a) Reduce to an acceptable level, during development, the systematic faults that can violate the SG

      - Achieved taking into consideration the expected usage (and some foreseeable unexpected one) in the test strategy

   b) Apply sufficient mitigations during field operation for remaining risks

      - This may include some run-time protections as per ISO26262-6, 7 but also diversity, including ASIL decomposition

2. Suitability in term of random HW faults

   a) Reduce to an acceptable level, during development, the risk that random HW faults, that can violate the SG (linked to PMHF/EEC), may occur during the lifetime

   b) Apply sufficient mitigations during field operation for remaining risks (SPFM/LFM)

      - Understanding about the implications of all faults is needed (directly able to violate the SG – linked to SPFM, or indirectly – linked to LFM)

Point to reflect: is it easier to control systematic or random HW faults?

**SPFM**: Single Point Fault Metrics, **LFM**: Latent Fault Metrics, **PMHF**: Probabilistic Metric for HW random Faults, **EEC**: Evaluation of Each Cause of safety goal violation

# AND IN CASE OF SEooC? – 1/2

- Biggest challenge of SEooC is that they are developed based on assumptions
- This may also include assumption about the ASIL
- The reason an ASIL is assigned is not always sufficiently justified and documented
  - Part of the safety concept of a particular application where the typical ASIL is assigned
  - Assigned due to co-existence
  - Assigned due to “golden plating”
  - Considerations about future reusability
  - …
- This means that it is not always possible to effectively apply all considerations
- Often a “worst case” approach is considered
  - In particular …

# AND IN CASE OF SEooC? – 2/2

1. Suitability in term of systematic faults
   a) Reduce to an acceptable level, during development, the systematic faults that can violate the SG
      - Effectiveness strongly depends on the assumptions defined
   b) Apply sufficient mitigations during field operation for remaining risks
      - Indications can be recommended in the product (Safety Application Note) SAN
2. Suitability in term of random HW faults
   a) Reduce to an acceptable level, during development, the risk that random HW faults, that can violate the SG (linked to PMHF/EEC), may occur during the lifetime
      - Conservative approach may be taken (unless valid reason all faults are considered as potential SPF)
   b) Apply sufficient mitigations during field operation for remaining risks (SPFM/LFM)
      - Similar to 2. a). Also here potentially not all faults may really be able to affect the actual SG in the final item

# CAN THE ASIL BE ASSIGNED IF NOT NEEDED BY THE SG?

- Several requirements/elements involved in safety related applications may not have an ASIL assigned at start
- An ASIL may need to be assigned, to requirements not derived from an SG, in only 1 condition:
  1. Co-existence with requirements having an ASIL attribute
     - Already mentioned before and described in ISO26262-9, 6
     - This is when the requirement is allocated to an (SW or HW) element that is also allocated requirements derived from a Safety Goal **and** the analysis shows that a possible (random HW or systematic) fault may interfere with such requirements
     - In this case the highest ASIL must be considered
     - This is also the reason why the whole of the intended functionality may be assigned an ASIL in many cases
- In all other situations there is no need to assign an ASIL or “golden plate” the rigour of compliance

# WHAT IS THE IMPLICATION IF ASIL IS DUE TO CO-EXISTENCE?

- Whenever an ASIL is assigned this requires 2 main considerations

1. Suitability in term of systematic faults

   a) Reduce to an acceptable level, during development, the systematic faults that can violate the SG

      - Achieved taking into consideration how the interferences may happen into the testing strategy

   b) Apply sufficient mitigations during field operation for remaining risks

      - Potentially not needed considering the ASIL was assigned to address this

2. Suitability in term of random HW faults

   a) Reduce to an acceptable level, during development, the risk that random HW faults, that can violate the SG (linked to PMHF/EEC), may occur during the lifetime

   b) Apply sufficient mitigations during field operation for remaining risks (SPFM/LFM)

      - Understanding about the implications of the interferences is needed (directly able to violate the SG – linked to SPFM, or indirectly – linked to LFM)

Depending on the reason the ASIL is assigned the points to consider can change

**SPFM**: Single Point Fault Metrics, **LFM**: Latent Fault Metrics, **PMHF**: Probabilistic Metric for HW random Faults, **EEC**: Evaluation of Each Cause of safety goal violation

# AND IN CASE OF SEooC?

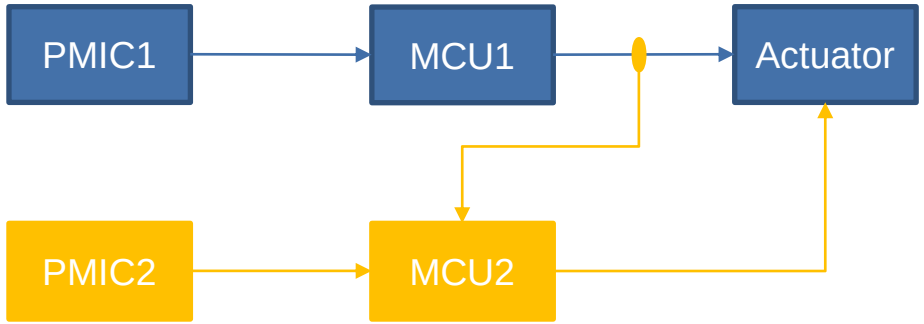
1. Suitability in term of systematic faults
   a) Reduce to an acceptable level, during development, the systematic faults that can violate the SG
      - Unless it is made clear that the ASIL is assigned due to co-existence and details are described, it would need to be handled as if derived from the SG!
   b) Apply sufficient mitigations during field operation for remaining risks
      - Potentially not needed considering the ASIL was assigned to address this. But again this background needs to be made visible
2. Suitability in term of random HW faults
   a) Reduce to an acceptable level, during development, the risk that random HW faults, that can violate the SG (linked to PMHF/EEC), may occur during the lifetime
      - Conservative approach may need to be taken if the background about the interface is not described. Potentially too much
   b) Apply sufficient mitigations during field operation for remaining risks (SPFM/LFM)
      - Similar to 2. a). Also here potentially not all faults may really be able to propagate to the co-existing ASIL domains and details must be available to judge

The assumptions related to co-existence are important when developing SEooC to best optimize the scope

# FUNDAMENTAL PROBLEM: THE WORLD HAS NO ASIL!

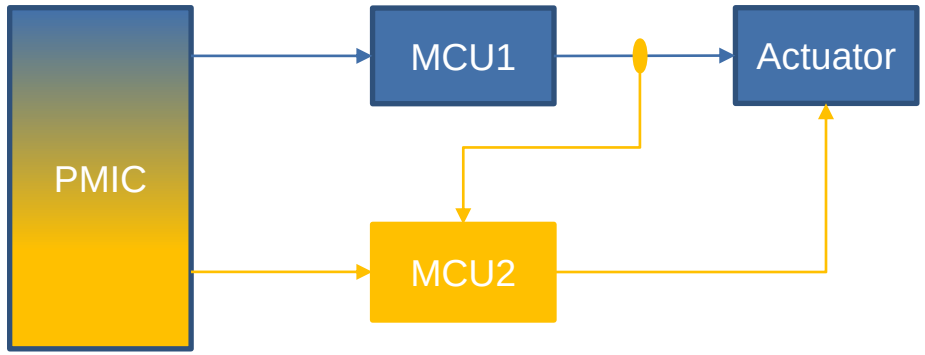

- No matter the robustness of the processing elements, the safeness of the system relies on the capability to sense the environment and observability of the actuator behaviour (and communications between all the elements)
  - This also requires considerations about “other technologies”
- SPFM of the processing element only quantify their risk of introducing undetected faults in the chain
  - Without special care this will be just a GIGO (Garbage In – Garbage Out)
- The supplier of the processing element can, based on agreements:
  - Just inform the capability of the element to be used by the system integrator to create a safe system
  - Define at least one use case to make the system safe (e.g. usage of an extra input for consistency checks)
- Important: the safeness of the system is not the result of an “ASIL composition”. Each element can contribute to the safeness of the other elements
- Similar situation when elements with a different ASIL capabilities are combined

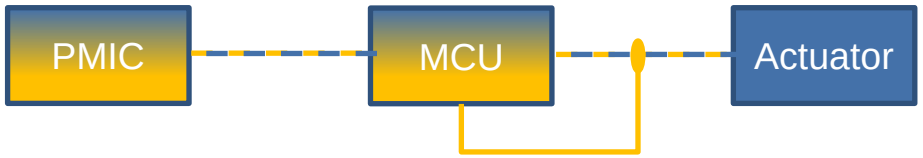
# WALKING THROUGH EXAMPLE 1




- Situation often used in Industrial applications (based on IEC61508) with an Equipment Under Control (EUC) and a Control System (CS)
- If targeting a fail-silent system, hypothetically the capability of the EUC are not relevant, only the one of the CS
- In reality protection from the CS is not 100%, hence the impact must be considered

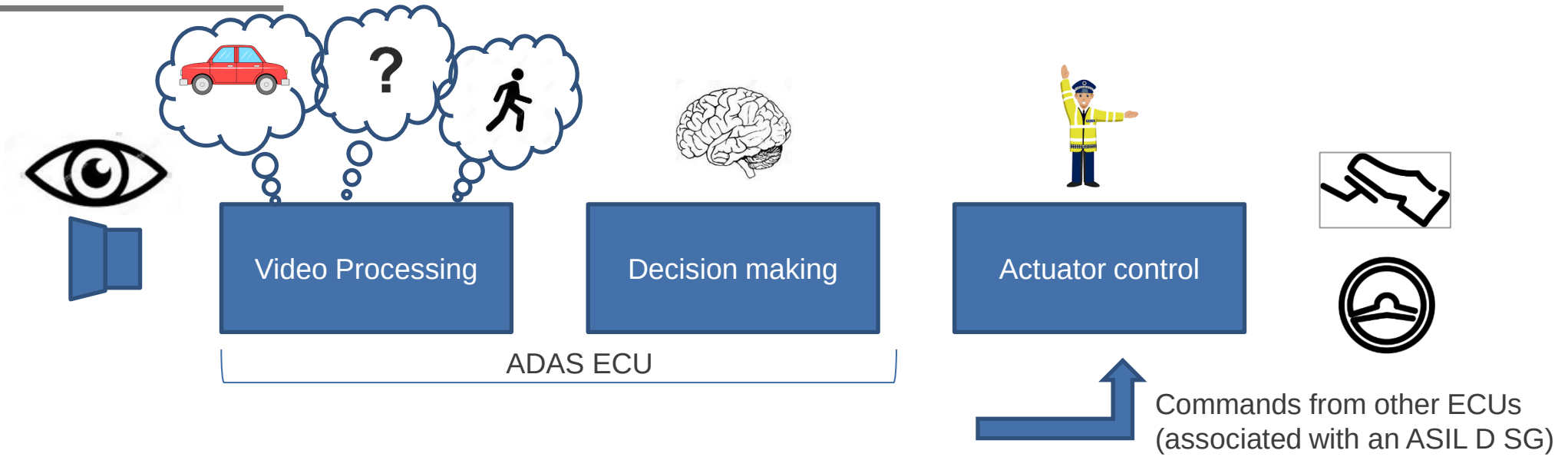
- Situation more complex as the PMIC is now a CCF between EUC and CS as well as having co-existent requirements
- PMIC can be partitioned and designed to allow ASIL + QM or fully assigned an ASIL



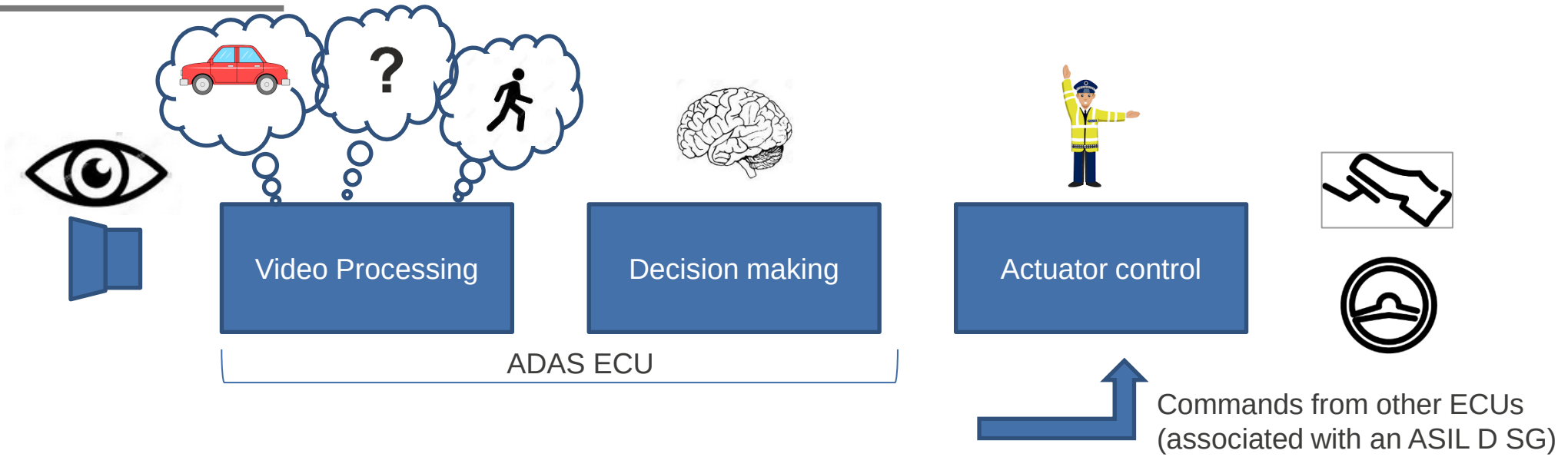

- Similar as the 2nd case but with the considerations extended to the MCU and connections

# WALKING THROUGH EXAMPLE 2: EMERGENCY BRAKING




- This chain is related to intended function. Hence at first no ASIL is assigned at all
- This processing chain is used to perform hazard analysis and define SGs getting an ASIL (let's assume ASIL D for AEB)
- Requirements derived from the SGs are then allocated to elements of the processing chain and/or to new one added on top
  - This may force requirements with an ASIL back to one or more elements of the chain
  - The functional safety concept strongly depends on the capabilities possible and, in this case, also by SOTIF
- In this case decision making and actuator control may be considered with an ASIL D
- The video processing and, especially, the camera unit may not be available with ASIL D requiring validation measures for usage

# WALKING THROUGH EXAMPLE 3: LANE DEPARTURE ASSIST.




- Similar considerations as the AEB example
- In this case actuator control may be considered with an ASIL D
- The video processing and decision making may be taking an ASIL B (unless requirements from higher ASILs are co-existing)
- The camera unit can also have an ASIL B capabilities but still requiring validation measures as providing non-trustable inputs
- The actuator control may have the job to validate the commands from the decision making mitigating possible “out of range” commands

Renesas.com