ISO26262 and liability: discussion on Open Source solutions

Francesco Rossi, Resiltech Srl,
francesco.rossi@resiltech.com
Paolo Gai, Evidence Srl,
pj@evidence.eu.com

ResilTech
Technologies for Resilience

EVIDENCE®
EMBEDDING TECHNOLOGY

The Safety "Impact" 1/2

- As seen in the previous presentation, the Toyota UA paves the way for a big discussion about the "safety impact" of modern electronic control system in our cars and particularly about the crucial role of the SW.
- Often "safety" is perceived in a very abstract way until some accident occurs and human lives have been already exposed to danger,
- …or until a big economic loss is present.
- Anyway without being too much idealist we need to face the reality of the "cost" of safety

ResilTech
Technologies for Resilience

EVIDENCE®
EMBEDDING TECHNOLOGY

The Safety "Impact" 2/2

- Since few years in order to mitigate hazards the state-of-the-art points to the adoption of activities and techniques specified by the ISO26262:2011.
- Nevertheless within the industry its full application is still not completed with one of the main reason being the often underestimated impact on project cost and specially for the part related to SW development and verification.
- In conjunction with an aggressive time to market it could happen that small/medium Tier1/Tier2 are in such conditions that "prevent" them from being fully compliant with the standard requirements.

ResilTech
Technologies for Resilience

EVIDENCE®
EMBEDDING TECHNOLOGY

Not conforming: which risks?

- Technical standards as the ISO26262 are not laws.
- And generally there is no law explicitly pointing to a technical standards.
- Anyway technical standards are used by lawyers to interpret laws.
- In Europe the General Product Safety Directive 2001/95/EC is present
  - Here it is mentioned the responsibility of the developer to comply with the State-of-the-Art development principles.
- It is possible to justify state-of-the-art compliance without implementing the ISO26262?
- Or it is sufficient?

ResilTech
Technologies for Resilience

EVIDENCE®
EMBEDDING TECHNOLOGY

OEM and Tier1 relations

- Generally the OEM is the product owner and, as such, is the first responsible for a the consequences of a product failure.
- Anyway clear links is present to bind the OEM and Tier1
- Anyway a DIA (Development Interface Agreement) in place represents a legal binding toward possible Tier1 responsibilities.
- There the provider (e.g. Tier1) asserts his will to fulfil the ISO26262 requirements (with a possible tailoring),
- but some duties are “left” to the Tier1
  - Important to get evidence (e.g. test results) even if not shared with customer/OEM
  - Important to properly perform a complete safety analysis
  - Important to similarly “control” Tier2/other providers

ResilTech
Technologies for Resilience

EVIDENCE®
EMBEDDING TECHNOLOGY

Possible solutions?

- In order to reduce cost or rather to focus the project resources on specific activities (e.g. V&V, Safety Analysis) is the adoption of a common platform which could collect “contributions” coming from different companies.

ResilTech
Technologies for Resilience

EVIDENCE®
EMBEDDING TECHNOLOGY

Open source as a common platform?

- Open Source SW a possible solution?

- The following two main aspects need to be carefully considered
  1. What is the SW development process?
  2. What is the level of SW reliability?
     Which evidence can be provided?
  3. Who is taking responsibility for SW misbehaviour
     responsible for a system failure?

- At least two main approaches, presented in the following slides, can be recognized in the market.

ResilTech
Technologies for Resilience

EVIDENCE®
EMBEDDING TECHNOLOGY

Open-source and ISO26262

http://www.comasso.org

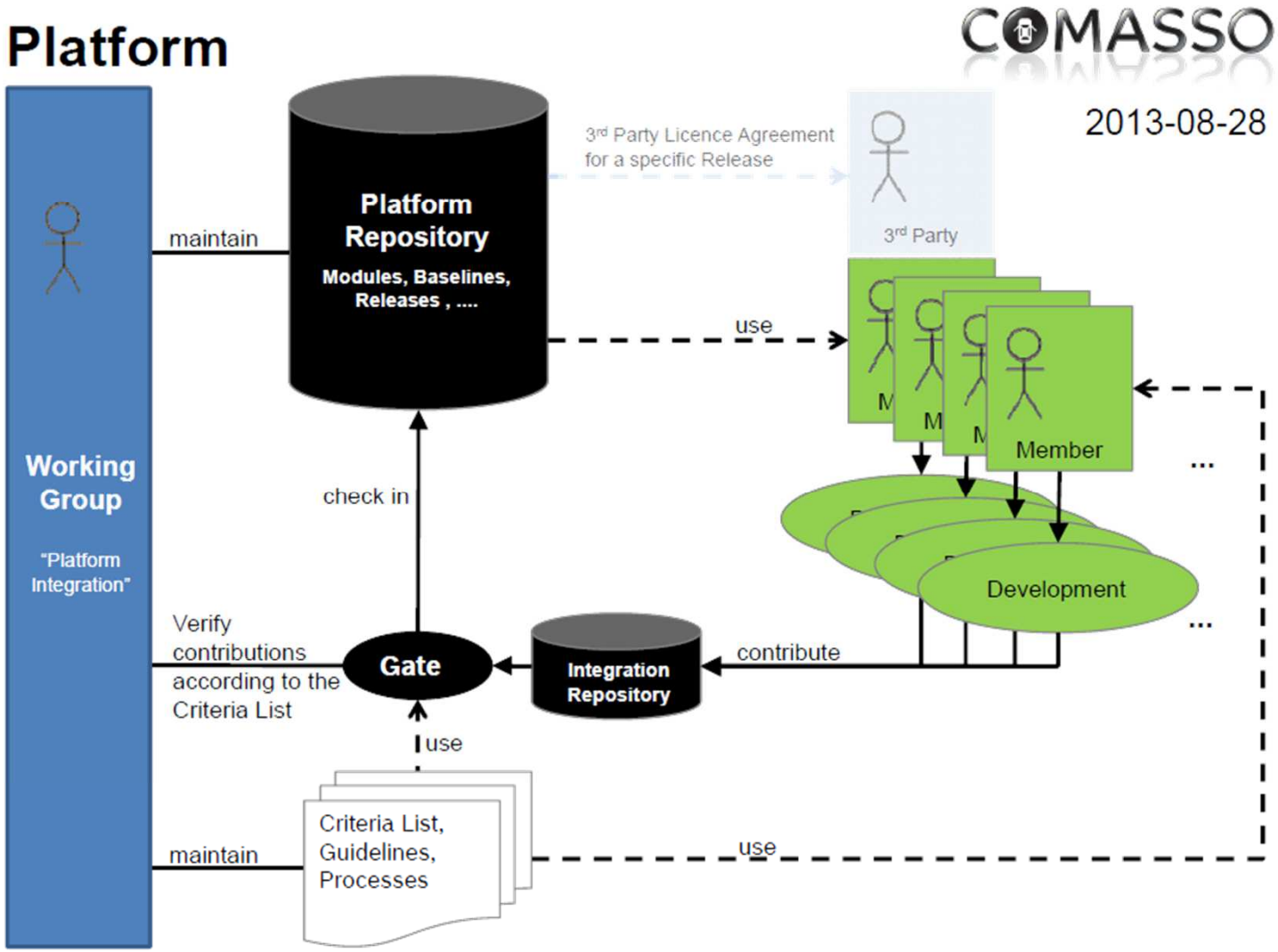
- Born from the need to have a “reference” AUTOSAR implementation
- Bosch and ETAS behind it initially
- Creating a common environment, protected by a consortium
- Simil- “Open source” for consortium members
- Limited possibility for derivative software

→ In this case, SW qualification could be part of the duties of the consortium in addition to the development model proposed by the COMASSO Association

ResilTech
Technologies for Resilience

EVIDENCE®
EMBEDDING TECHNOLOGY

The COMASSO Build system

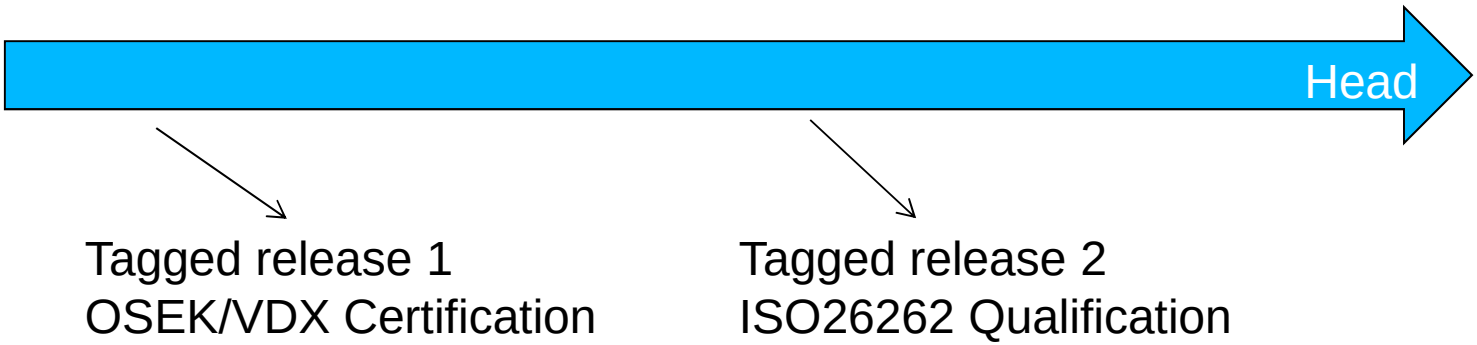


Open-source with tagged releases

Another option is a pure open-source model,
where customers makes a derivative to be tested and integrated

ERIKA ENTERPRISE

http://erika.tuxfamily.org



ResilTech
Technologies for Resilience

EVIDENCE®
EMBEDDING TECHNOLOGY

Open points for discussion

What are the possibility to cooperate among various Tier1 to collaborate on the development of platforms for providing qualified ISO26262 projects?

What is the role, if any, of silicon vendors in a common platform?

Which is the preferred approach on the platform development?

Does they really match the market requirements?

ResilTech
Technologies for Resilience

EVIDENCE®
EMBEDDING TECHNOLOGY

Thank you for listening !

Questions ?

ResilTech
Technologies for Resilience

EVIDENCE®
EMBEDDING TECHNOLOGY