ResilTech

Technologies for Resilience

ISO26262 at work: car maker and supplier working side by side for safety

Automotive SPIN Italia

9° Automotive Software Workshop

1/12/2011

Milan, Italy

ResilTech
Technologies for Resilience

Roadmap

- **Our company**
- **Introduction**
- **Main 26262 aspects impacting OEM and supplier relationship**
- **Use cases from project experience**
- **Conclusion**

ResilTech
Technologies for Resilience

RESILTECH

*Tech*niques and *Tech*nologies for *Resil*ience

- **Company**
  - SRL born in late 2007
  - Founded by
    - university researchers expert in resilient computing and
    - specialists in the industrial field of Verification and Validation (V&V) of critical systems
- **Mission**

  «To provide **engineering consulting and design services** to companies and public bodies mainly for, but not limited to, the field of **resilient systems and infrastructures**»

- **Research**
  - Strong relations with both universities and research institutes
  - Activities on FP7 projects
  - Artemis

SEVENTH FRAMEWORK PROGRAMME

ISTITUTO DI SCIENZA E TECNOLOGIE DELL'INFORMAZIONE "A. FAEDO"

ISTI-CNR (Pisa-italy)

STUDIORUM FLORENTINA UNIVERSITAS

Università degli Studi di Firenze (Florence-Italy)

- **Automotive Working groups**
  - ISO SC3/WG16 for ISO26262 ("Road vehicles - Functional safety")
  - AUTOSAR Phase III (development member)
    - WP 1.3 – Safety

AUTOSAR
AUTOMOTIVE OPEN SYSTEM ARCHITECTURE

ResilTech

Introduction 1/2

- **ISO 26262 – Road vehicles – Functional safety, Part 1 to Part 9**
  - Date of publication: November 15, 2011.

Were all vehicles engineered so far “unsafe”?

- **Answer is “No” but…**
  - in many cases valid technical solutions already present but not integrated in a well defined safety lifecycle;
  - as a consequence risk of having different “safety concepts” at different level of the supply chain, for instance:
    - “safe state” of a subsystem not completely in line with vehicle level safety architecture

ResilTech
Technologies for Resilience

Introduction 2/2

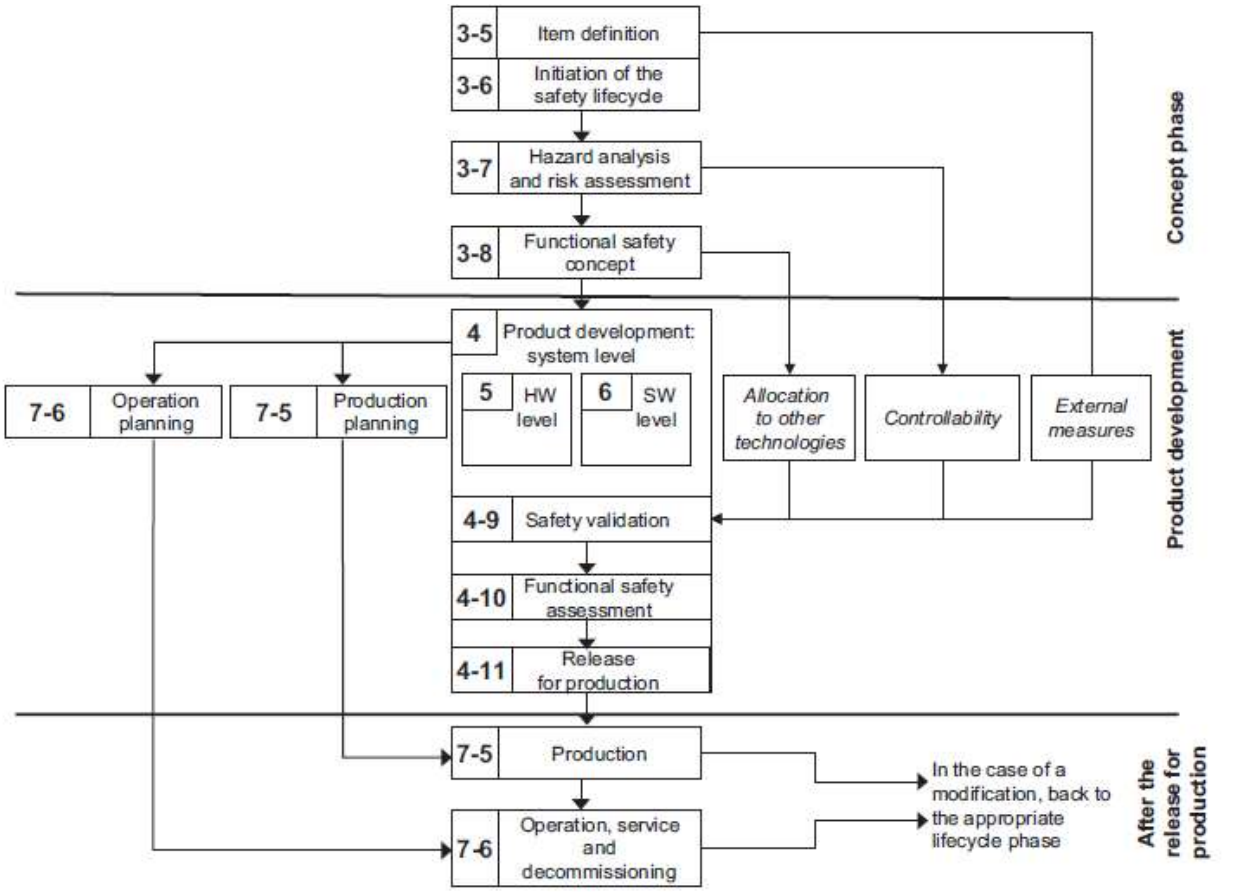
- **Good steps forward can be made by adopting a common, standard approach that links together in a safety project all the stakeholder, from OEM to component providers;**
- **thus enabling the implementation of a consistent development lifecycle starting from the vehicle level Hazard Analysis and ending with its validation (again at vehicle level).**

As many other things in life this is not coming for free…

ResilTech
Technologies for Resilience

ISO26262 and distributed development 1/2

- **ISO2626 safety lifecycle is seen as whole, unique flow from safety top level requirements to vehicle decommissioning.**
- **Requiren**
- **Anyway t** **d do not suggest a** **es,**
  - even th **nsibility**
- **This is nc** **ical" consequ** **stem attribute**



ISO26262 and distributed development $_{2/2}$

- **With respect to the pre-26262 customer-supplier relantioship sharing of new safety activities and resposabilities generally implies more interaction in relation to:**
  - the definition of high level safety requirements
  - exchange of deliverabiles and sharing of information/evidence
    - possible disclore of company confidential information
  - increase probability of design change request from lower levels of the development chain
    - E.g. SW analysis on detailed HW/SW level shows that identified Safety Mechanisms are not as effective as expected triggering a change in the original safety concept

Challenge: ***adapt to these new needs <u>efficiently</u>***

Use cases

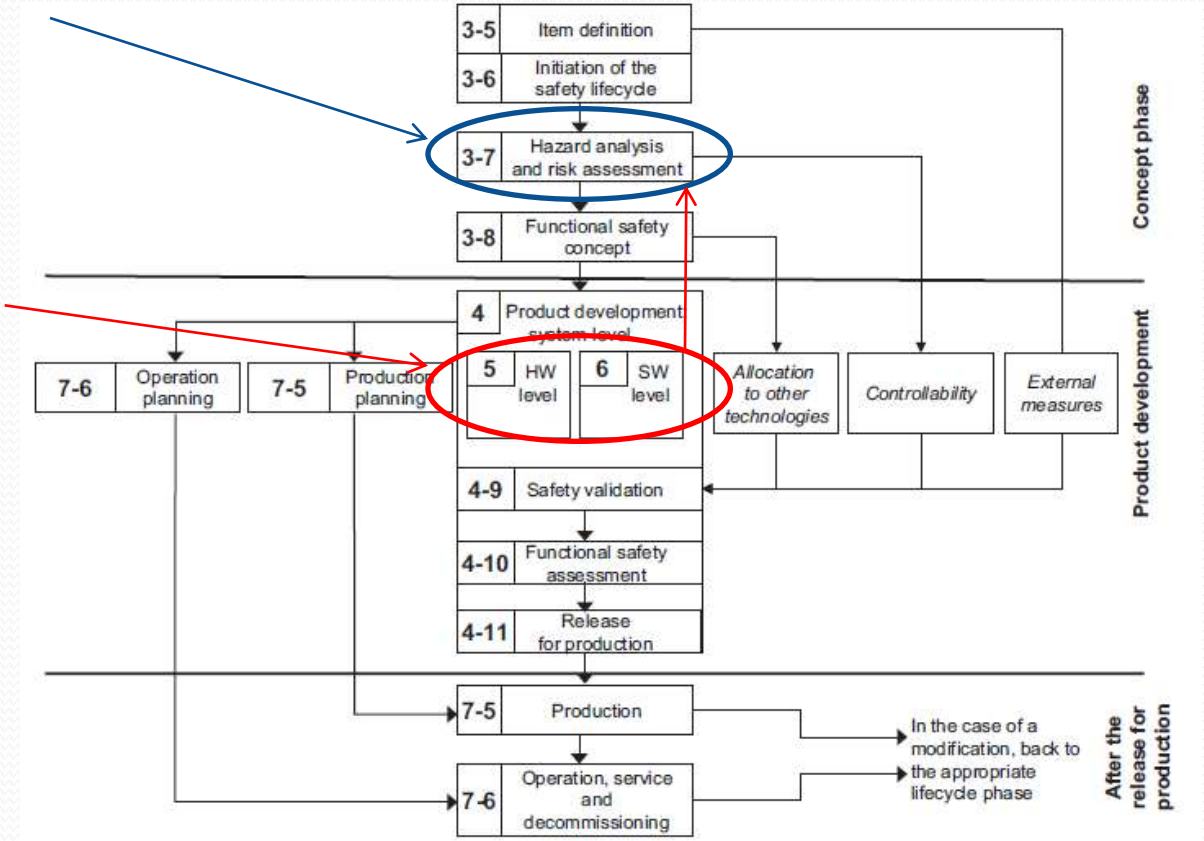
- **Let's see how the distributed development paradigma applies to the following topics**
  - Hazard log
  - Definition of "top" level safety requirements
  - HW metrics

Case of the Hazard log 1/2

- **Hazard log is a living document managing the hazards during the project lifecycle**
  - Not explicitely mentioned as ISO2626 Work Product but manteinance of the hazards through the change management process is clearly identified
- **Activities related to “hazard management” are generally intended to be OEM responsability.**
- **Anyway review/update of the hazard status is expected at different stages of the development.**
- ***This implies that suppliers are involved!***

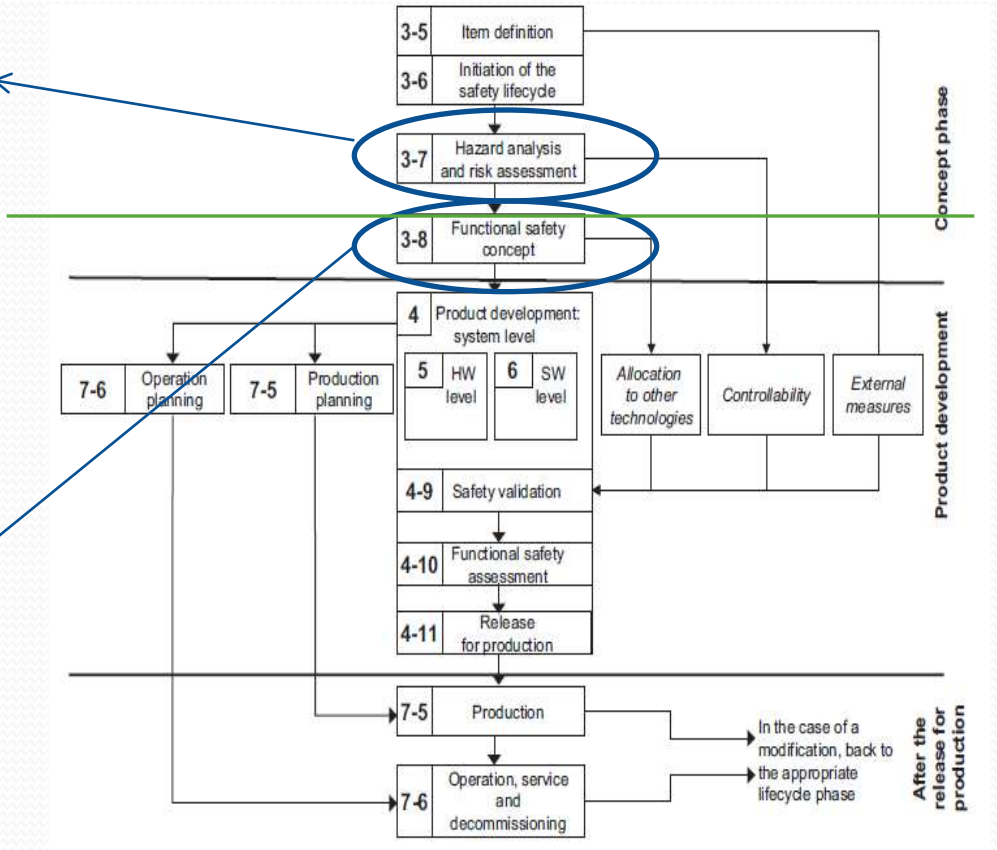
Case of the Hazard log 2/2

- Start with Hazard Identification
- Suppplier involved in the Hazard Analysis but mainly to provide technical information
- “New hazards” potentially identified during HW or SW development
- Feedback on Hazard Analysis



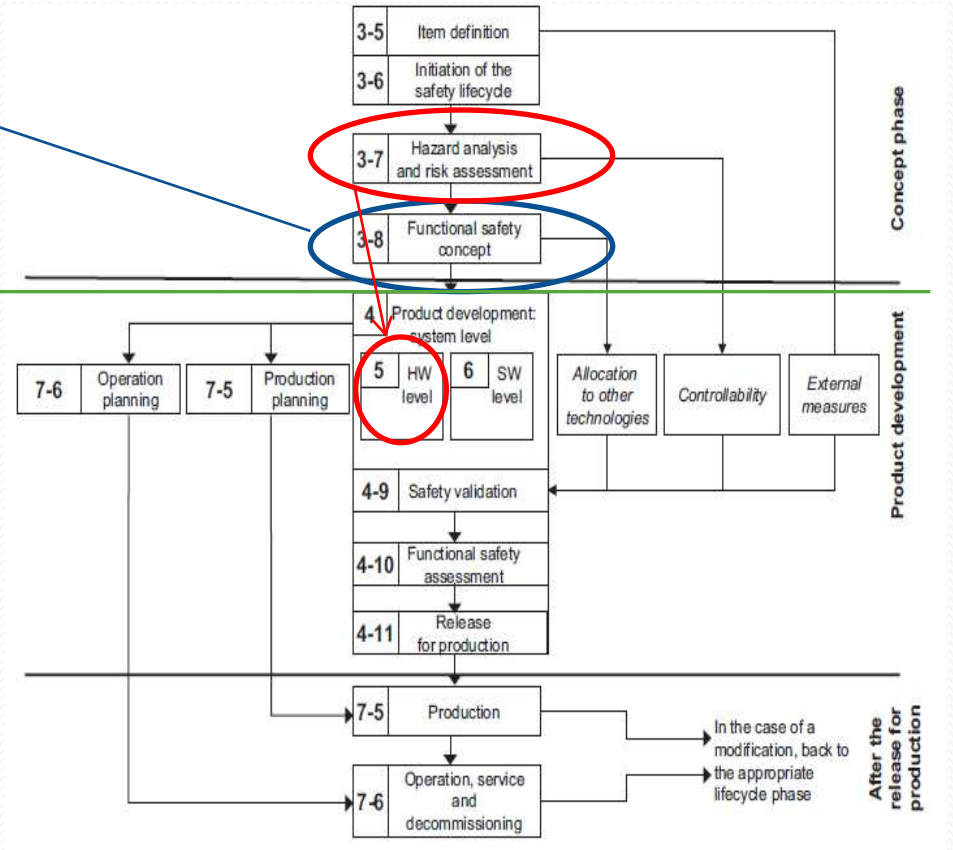
Case of supplier "top level" safety requirements *1/3*

- **OEM can specify as the highest level of safety requirements the *safety goals.***
- **Probably a good split of responsabilities in terms of safety lifecycle.**
- **But this cound not be a suitable level of information in RFQ phase.**
- **Indeed depending on the safety concept feasible architectures and related costs can vary significantly.**



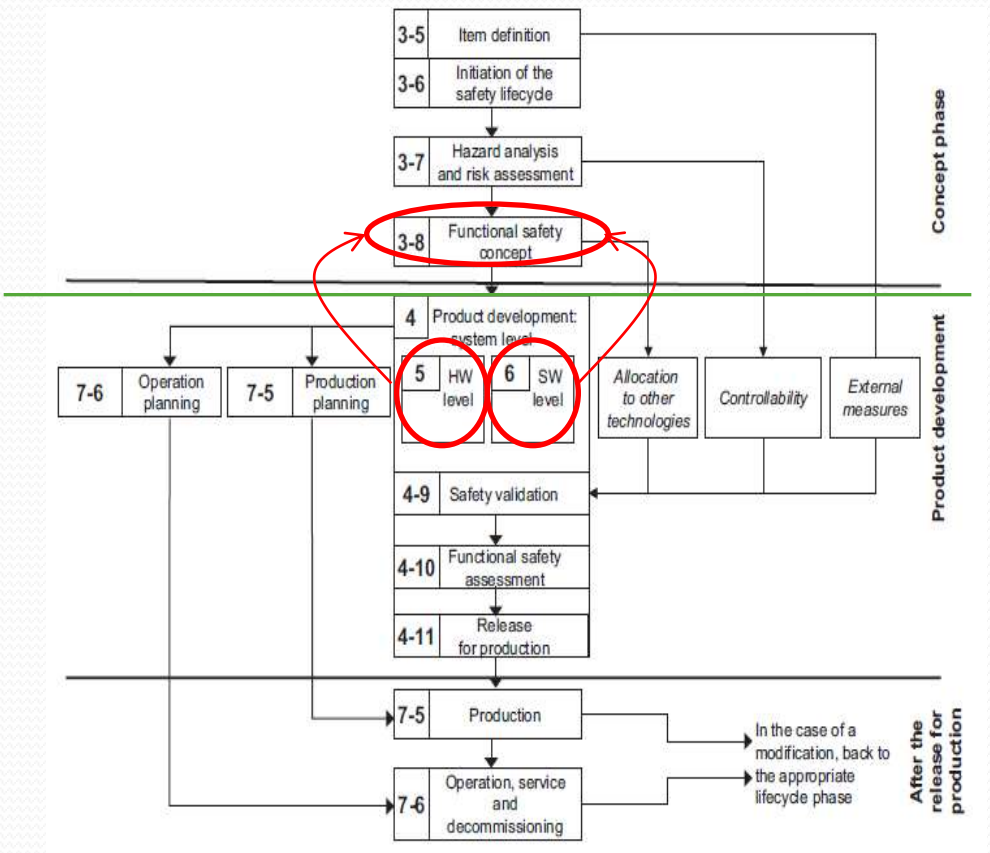
Case of supplier "top level" safety requirements *2/3*

- **Another possibility is then for the OEM to "suggest" requirements for the functional safety concept.**
- **The concept describes already top level architecture features for safety including safety mechanism principles, safe states.**
- **Interaction with supplier is still important in this phase.**
- **In this case can the OEM "hide" information about the safety goals?**
  - As an example take care that for evaluation of the HW metrics safety goals are the primary observation points to evalute the impact of the random HW faults.



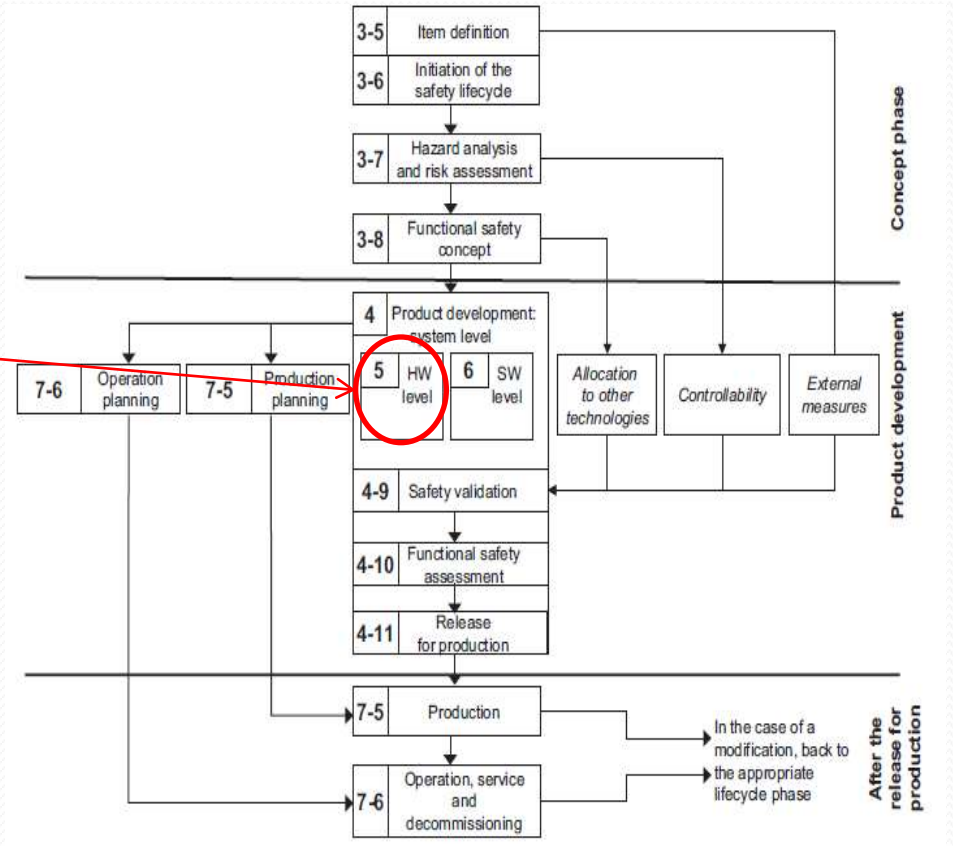
Case of supplier "top level" safety requirements *3/3*

- **In relation to the request changes across the OEM-supplier border please note that Safety Analysis at both HW and SW level can show that selected safety concept is not effective with respect to the failure mode of the "final" architecture**



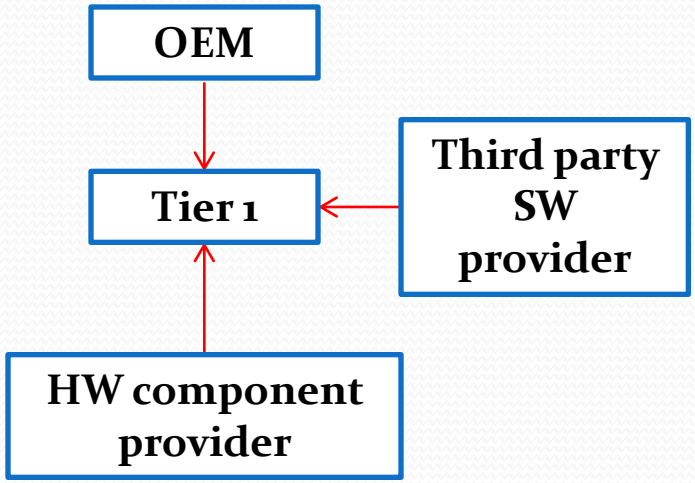
One activity involving all parties: HW metrics 1/2

- Let's consider the case of the evaluation of the HW metrics: a mean to evaluate the "robusteness" of the architecture against random HW faults.
- This is an activity part of the Safety Analysis whose resposability is typically assigned to the Tier1 (HW) supplier.
- Let's see how this is actually involving more parties.



One activity involving all parties: HW metrics 2/2

- Tier 1 (the responsible for HW development) is in charge of evaluting these parameters, but
- evalutation is done against thresholds defined at system level: OEM is in the natural position to define these thresholds.
- Complex HW components as microtrollers contributes with a white-box approach to the definition of these parameters: information/interaction from component providers is fundamental.
- Specific diagnostic SW or even application SW (e.g. End-to-End protection) can contribute to the calculation of these parameters (providing “coverage” over HW faults) then (if present) third party SW providers are directly invoved.



Conclusion

- **Choosing compliance with ISO26262 will support the implementation of a well defined “integrated” lifecycle for all the project stakeholders.**
- **New activities are expected but moreover new interactions between the different stakeholders.**
- **This implies to rethink some of the interfaces different players in the project to implement *efficiently* the safety lifecycle on a relal project.**

ResilTech
Technologies for Resilience

Thanks for your attention!

francesco.rossi@resiltech.com