Ensuring Quality Requirements for Critical Systems in Agile Development

Dr. Christof Ebert, Vector

REConf, Munich, 13. March 2019

V1.0 | 2019-03-13

Agenda

1. Welcome
2. Motivation
3. Ensuring Consistency in Agile Development
4. Conclusions and Outlook

VECTOR

Prepare for the Future: ACES makes Digital Winners

Industry Trends

- **A**utonomy

- **C**onnectivity

- **E**cology

- **S**ervices

Impacts on Business

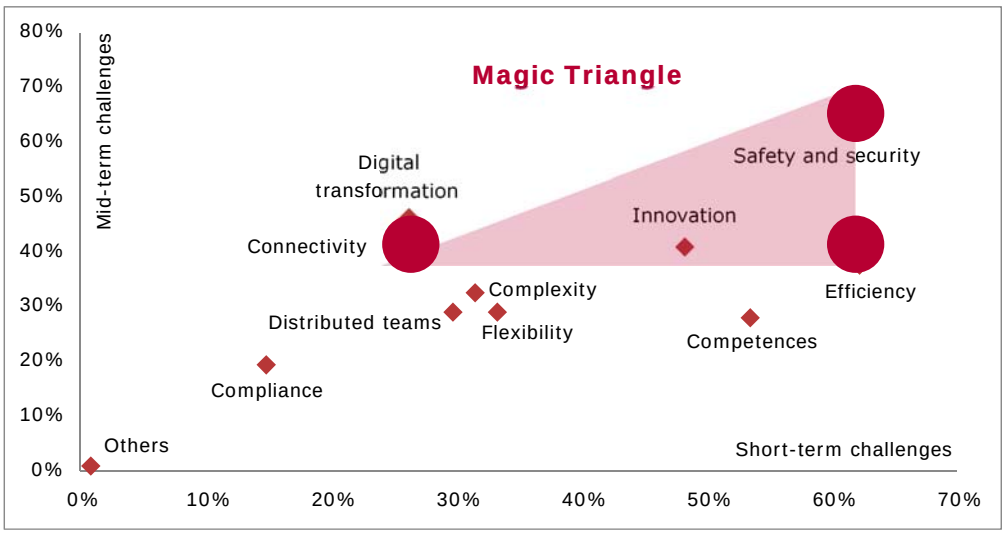
- Services are the real products
- Fluid business models
- “Smartphone-like” adaptive and flexible delivery
- Lean valuation
- Growing liability risks

Impacts on Engineering

- Convergence IT and E/E
- Service-oriented architectures
- Agile innovation
- Continuous development, delivery and deployment
- Need for service and convergence competences

VECTOR

Vector Client Survey: Security and Safety are Major Challenges



Vector Client Survey 2018.
Details: www.vector.com/trends.
Horizontal axis shows short-term challenges; vertical axis shows mid-term challenges.
Sum > 200% due to 5 answers per question.
Strong validity with >4% response rate of 2000 recipients from different industries worldwide.

Safety and Cybersecurity have arrived as major challenges – now and in future.
Solution: Agile innovation

Overview: Agile Safety and Cybersecurity

Challenge
Frequent and late changes in safety-related product development are often hindered because they take too much effort to release with right quality level.

Example: Fast reaction to cybersecurity attacks with safety impact

Vision
Safe and secure product release within few hours with formal approval process and documentation

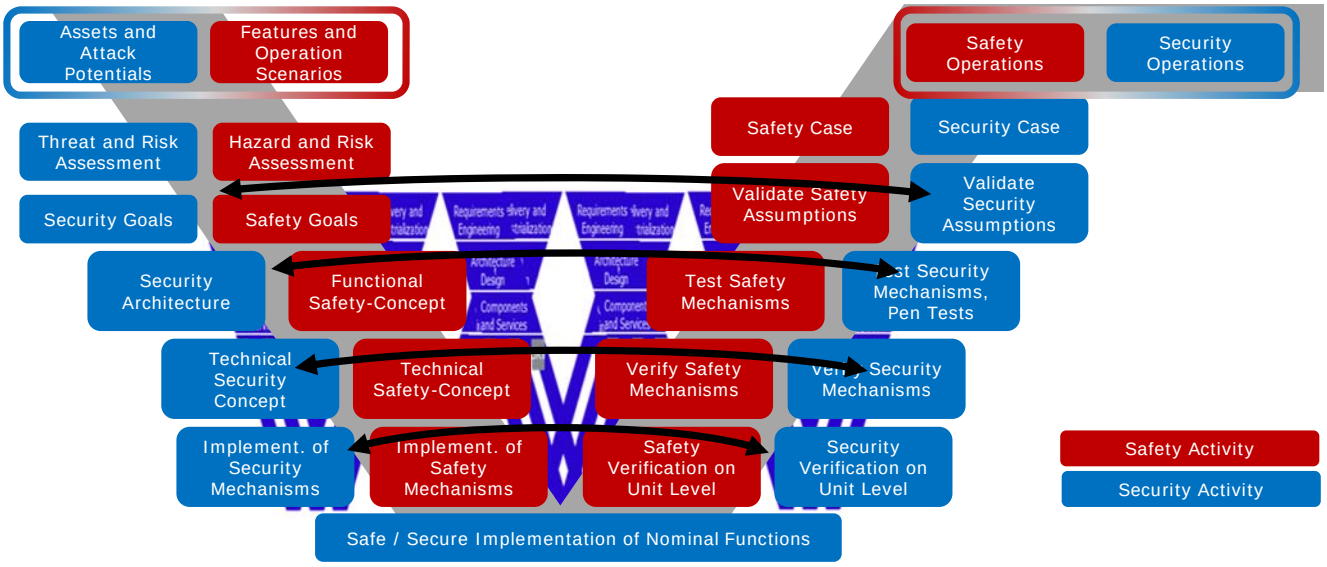
Solution
Agile process for critical systems engineering: **Method, Organization, Tooling**

With the growth of IoT and convergence of IT and embedded systems this approach applies to practically all industries

Agenda

VECTOR

Method: Quality Requirements in Agile Lifecycle



- Safety and cybersecurity must be integrated to the development process
- For efficient and fast ramp-up, connect security with existing safety governance

VECTOR

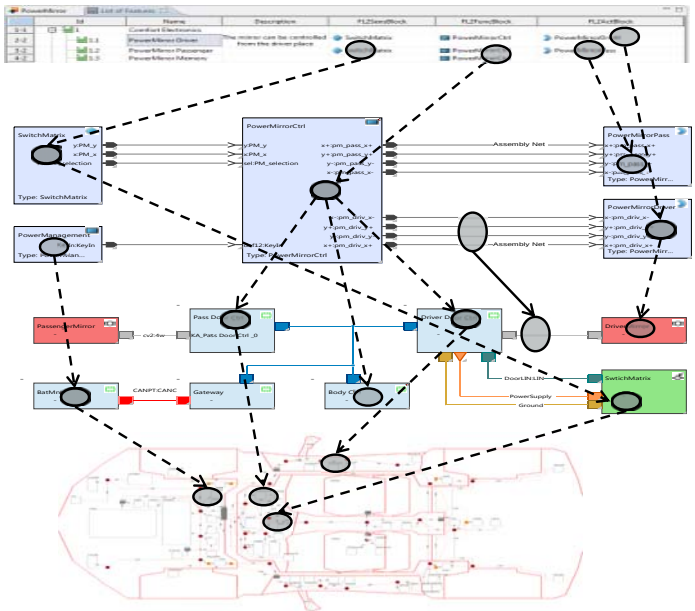
Method: Model-Based Dependency Analysis (1/2)

System Requirements

Logical System Architecture

Component Architecture

Simulation Implementation



System FTA/FMEA, TORE

Component FTA/FMEA, traceability

Robustness, TDD, code analysis, CD

Traceability from changes based on hierarchic modelling and update of analysis and tests

VECTOR

Method: Model-Based Dependency Analysis (2/2)

Target:

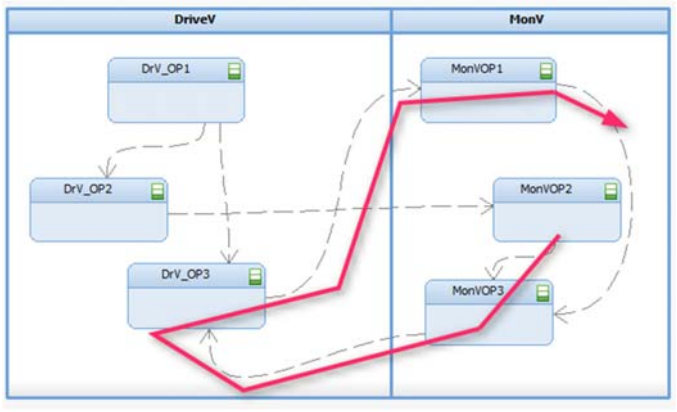
“Continuous” consistency of quality requirements, even in agile development

Case study: Functional safety

Challenge: Perceived small change negatively impacts safety

Approach:

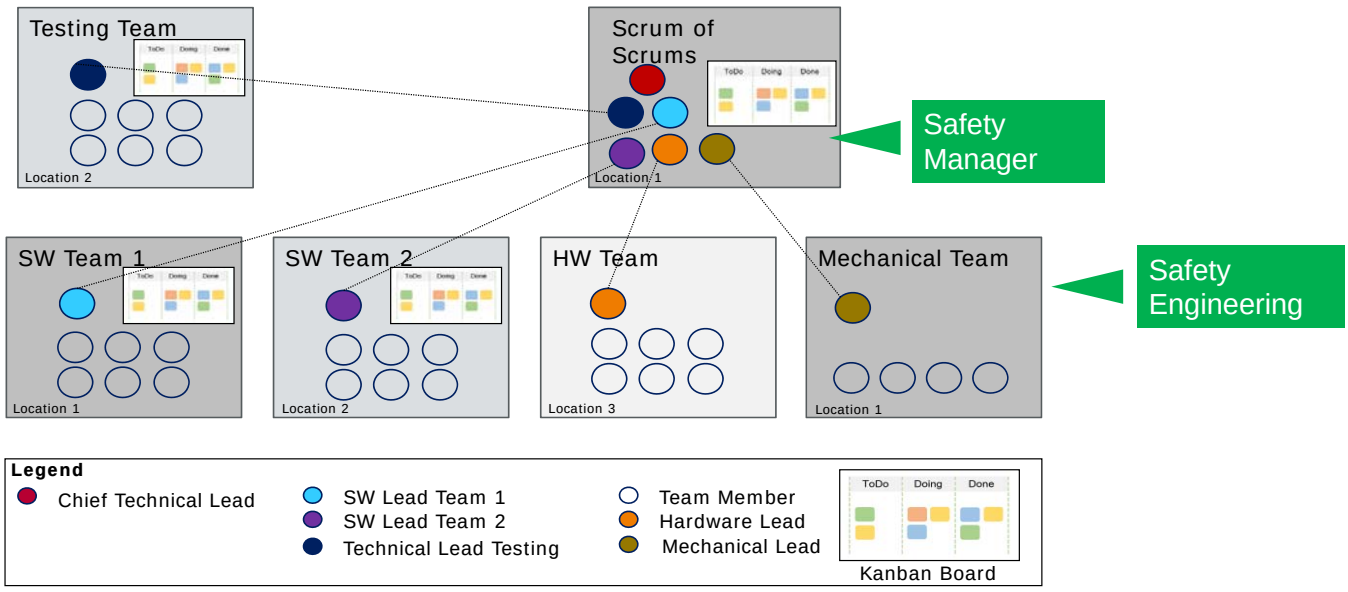
- Activity Diagram (SysML) helps to investigate impact of changes
- Based on this “effect chain analysis” the related tasks for safety analysis update can be identified (e.g. are safety related operations affected by change)



Automatic roundtrip engineering is still a “white elephant” – but methods and tools evolve

VECTOR

Organization: Agile Scaling for Critical Systems



Agile teams must exhibit necessary competences to ensure quality requirements

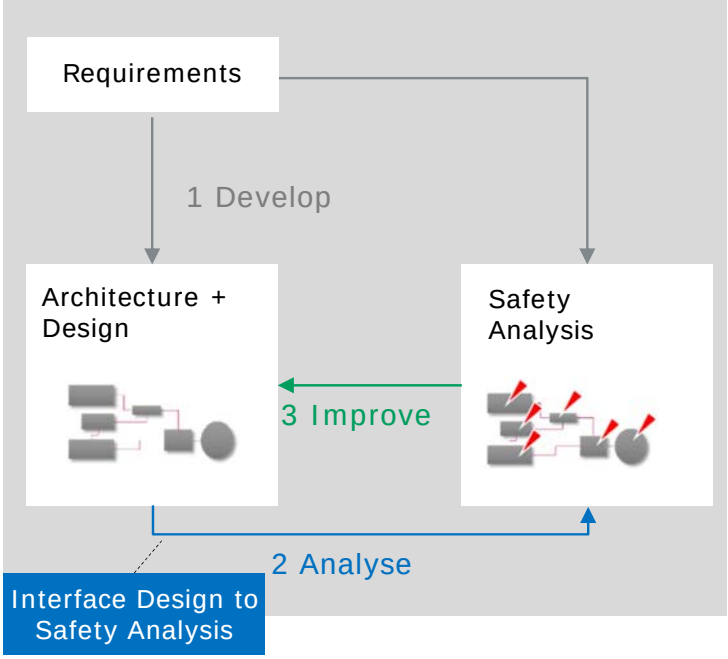
VECTOR

Tools: PLM and Dependency Management

Why are tools important?

Safety Analysis **depends** on

- Respective scope, i.e. System-, SW-, HW-Design
- Specific safety requirements
- Dependencies from cybersecurity threat analysis
- This means lots of effort with each single software change



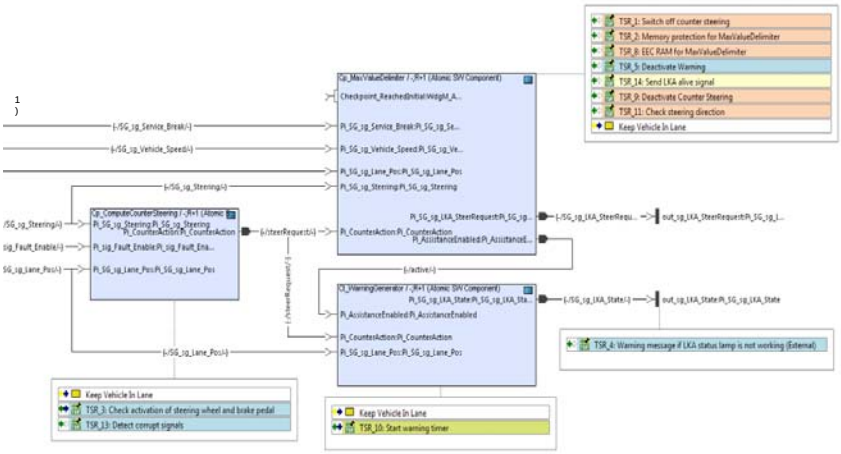
Changes have complex dependencies and interactions across work products.

Tooling is mandatory for efficient and consistent change handling.

VECTOR

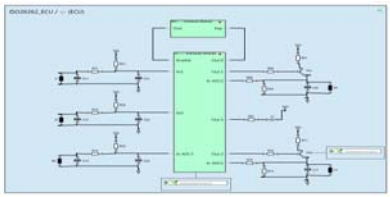
Tools: SW and HW Consistency with PREEvision

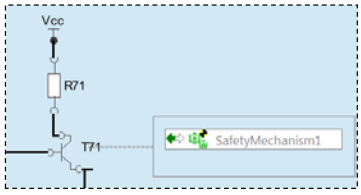
- **SW and HW safety design are modeled and kept consistent from Logical and systems level to the device level**



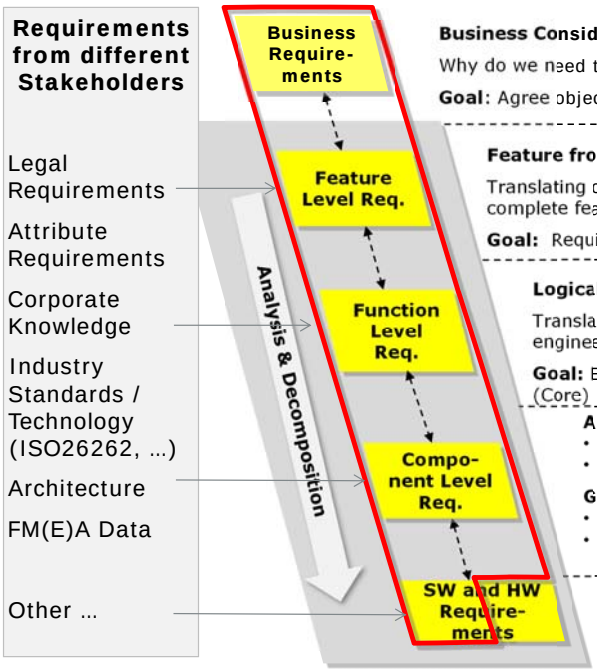
- **SW safety design**, technical safety requirements (TSR), faults and safety mechanisms (SM) can be detailed down to ports, interfaces and data elements
- AUTOSAR Import / Export of SW Architecture

- **HW elements** can be modeled and associated with technical safety requirements, faults and safety mechanisms
- Powerful library concept for faults and safety mechanisms





Case Study Ford: Consistency in Systems Engineering



Business Considerations

Why do we need the feature? What plans do we have with that feature

Goal: Agree objectives between business stakeholders (e.g. marketing, x-Carline Planning)

WHY?

Feature from a customer perspective

Translating customer wants and market needs to stable, consistent and complete feature requirements

Goal: Requirements agreed between all stakeholders

WHAT?

Logical functions necessary to implement the features

Translating customer requirements to **implementation independent** engineering requirements.

Goal: Enable efficient reuse of specifications across ECUs and car lines (Core)

HOW? Logical Solution (i.e., reusable Part)

Allocated logical functions (platform / ECU)

- Technical interfaces of components are determined
- Component behavior is enhanced/refined by technical requirements

Goal:

- Consistency of x-ECU interfaces enable interoperability
- Efficient data exchange with supplier

HOW? Detailed Technical Solution (i.e., Carline Specific Adaptions)

Depending Business Model

- Relate SW specification details to external impacts, e.g. SW, HW and Systems suppliers

Agenda

Conclusion: Safety/Security are Possible in Agile Development

Integration of safety and cybersecurity in agile projects is possible and has benefits…

…if the following conditions are fulfilled

- **Methods**
  - **Consistency across work products** from HARA/TARA to safety/security goals and requirements to design, implementation, (regression) test and safety/security case documentation
- **Organization**
  - **Quality responsibility is with each agile team** (e.g., safety manager, safety engineer).
  - **Agile team has necessary safety and security competences**.
- **Tools**
  - **Sufficient tool based traceability** (requirements, architecture, tests, change sets..) is established.
  - **Specific tooling supports interfaces to design tools** (e.g. HARA and TARA with System, SW, HW).

Safety and cybersecurity engineering must be part of each agile team.
Systematic integration ensures efficient and robust development in agile context

Agile in Practice

Vector Forum 2019

Agile Scaling - Scaled Agile

27. June 2019 in Stuttgart

- With Bosch, Daimler, Festo, Knorr-Bremse, ZF, Vector and other agile leaders
- Practical experiences across industries
- Enhance your competences
- Grow your networks

Details and free registration…
www.vector.com/forum

Thank you for your attention.
For more information please contact us.

Passion. Partner. Value.

Vector Consulting Services

@VectorVCS
www.vector.com/consulting
consulting-info@vector.com
Phone: +49-711-80670-0