Combined application of agile practices and functional safety in automotive software development

Steffen Kuhn, Elektrobit / ZVEI
Agile Automotive
October 8, 2020
ISO 26262 is the relevant automotive functional safety standard

It defines four automotive safety integrity levels (ASIL A – D, D = highest)

Functional safety results in

• Additional development tasks (e.g. error detection mechanisms)
• Additional process requirements depending on the ASIL

Functional safety drivers in automotive:
• Highly automated driving
• Electrification...

Functional safety protects human lives from machines
When agile and safety shall be combined, two worlds collide

Agile development

Automotive safety

Left: Photo by fauxels from Pexels, Right: Photo by Taras Makarenko from Pexels

© Elektrobit (EB) 2020
Misconceptions regarding agile and safety

<table>
<thead>
<tr>
<th>Agile = No processes</th>
<th>Safety = Sequential process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agile = No documentation</td>
<td>Safety does not allow agile</td>
</tr>
</tbody>
</table>
**Results from ZVEI WG “Agile Software development”**

**Kernthesen (2017)**

1. Assessoren beziehen wenig eigene Erfahrungen mit agile Vorgehensweisen
   ➞ Frühzeitige Einbindung, projektrelevante Assessments

2. Cross-funktionale Teams
   ➞ Verantwortlichkeiten müssen geregt sein, Projektteam muss nötige Kompetenzen und Befugnisse besitzen

3. Frühzeitiges Feedback
   ➞ Nicht nur bzgl. implementierter Funktionalität, auch für Sicherheitsfunktionen
   ➞ Auch bzgl. Dokumenten (schnelle schrittweise Rückspracheförderung)

4. Sprintplanung
   ➞ Zusätzlich gesamthafte Meilensteinplanung für das Projekt notwendig

5. Überlappende Phasen, kurze Iterationen
   ➞ Kein Widerspruch zur ISO 26262

6. Inkrementelle Reviews
   ➞ Ersetzen keine vollständigen Reviews

7. Automatisierte Testdurchführung
   ➞ Geeignete Werkzeuge nötig

8. Umgang mit Varianten
   ➞ Keine spezifische Fragestellung agiler Softwareentwicklung

**Introduction to Agile & Safety (2020)**
Agile, ASPICE and Functional Safety complement each other

How to solve complex problems in small iterations

What to do in automotive software projects (as basic argumentation for “QM” level)

What to do for safety levels ASIL A-D

Agile (e.g. Scrum)

ASPICE

Functional Safety
### Scrum

#### Workflow
- **Sprint Planning I**
- **Sprint Planning II**
- **Daily Scrum Meeting**
- **Sprint Review**
- **Retrospective**
- **Backlog Refinement**
  - Tag backlog items as safety-relevant
  - Consider additional effort depending on ASIL

#### Roles
- **Product Owner (PO)**
  - Responsible for functional safety
  - Defines safety-related backlog items
- **Scrum Master (SM)**
  - Ensures adherence to the company-specific process
- **Development Team (DT)**
  - Develops safety-related solutions¹
  - Adheres to safety process requirements (e.g. coding and testing guidelines)
- **Manager**
  - Must ensure sufficient safety expertise
- **Safety Manager (SaM)**
  - Ensures achievement of functional safety

#### Artifacts
- **Product Backlog, Sprint Backlog, Task Board**
  - Additional backlog items for safety mechanisms and safety artifacts (e.g. safety plan)

- **Sprint result**
  - Must achieve the defined level of functional safety

- **Definition of Done (DoD)**
  - Differs according to sample phase/release/maturity level and ASIL.
  - May be used as verification plan

---

1: Safety mechanisms, redundant architecture

© Elektrobit (EB) 2020
**Product Owner**
- Creates safety-related product backlog items (e.g. development of a safety mechanism), supported by the Safety Manager
- Requests achievement of functional safety

**Scrum Master**
- Ensures adherence to the company-specific process and additional process requirements (=> Definition of Done)
- Informs the Safety Manager and Product Owner about the achievement of functional safety

**Development Team**
- Considers higher effort for ISO 26262 compliance in estimations
- Derives software safety requirements
- Implements and tests software safety requirements
- Performs safety analyses
- Considers definitions and activities from the safety plan in all development activities, e.g.:
  - Programming guidelines
  - Use of adequate tools (tool confidence)
  - Minimum test coverage according to ASIL

**Safety Manager**
- Ensures that the team adheres to the safety plan and organizational rules
- Supports the Product Owner in the creation of safety-related backlog items
- Collaborates with the Development Team regarding all safety topics

---

1: Product Owner is responsible for the product including its ISO26262 requirements
2: Either Scrum Master or other Scrum team members must have knowledge regarding ISO26262 requirements
3: “Highlander principle”: There is always just one responsible for the backlog, which is the Product Owner
A suitable model for the safety manager role shall be chosen

Small team/complexity

- PO
- SM
- DT

Larger team/complexity

- PO
- SM
- SaM
- DT

Full time Safety Manager within Scrum Team

Multiple teams

- PO
- SM
- DT

- PO
- SM
- DT

- One Safety Manager for multiple teams
- Multiple members per team with safety expertise (PO, SM or DT member)

Part time Safety Manager (combined with Product Owner, Scrum Master or Development Team member role)

PO: Product Owner, SM: Scrum Master, DT: Development Team, SaM: Safety Manager, ST: Scrum Team. Note: The Safety Manager does not have to be organizationally independent from the team!
Further recommended agile practices

**Refactoring**
- Lower degree of complexity
- Easier maintenance/testability
- Simpler expandability

**Pair programming**
- Early prevention of error development
- Observer as a safety net and guide
- Can replace reviews/inspections during development

**Continuous integration**
- Early error detection and quicker location
- Improves transparency and communication
- Higher development efficiency
Key take-aways

1) Agile methods like Scrum can be combined with functional safety.

2) It is beneficial to use agile methods like Scrum in complex safety-related developments.

3) In safety-related development, agile teams must consider additional activities and process requirements.

4) The role of the safety manager can be integrated into agile teams.

5) The agile practices refactoring, pair programming and continuous integration are recommended for use in safety-related development.
Contact us!

Steffen Kuhn, Elektrobit Consulting
steffen.kuhn@elektrobit.com