1/ Break silos,
2/ Ensure full traceability,
3/ Modularity
4/ Automate reporting

Eurospi 2015
INTRODUCTION

How KTM AG company addresses ISO26262 functional safety challenges internally and with its partners?

Four key resolutions to success:
- 1st - breaking the silos between safety and other departments/suppliers,
- 2nd - ensuring traceability between development items to cover the norms,
- 3rd - accessing the modularity and reusability organisation to make the most of legacy knowledge,
- 4th - automating the reporting to ensure engineers focus on design (not on document generation).

KTM targets an environment embracing Model Based Engineering and a repository of crosswise (work fields) design items.

With a strong focus on system engineering, KTM’s ambition is not to provide an ideal environment but to introduce one solving its current issues for its present maturity.

The environment described in this presentation is implemented and operational on a major KTM project as a proof of concept for future KTM projects.
KTM FUNCTIONAL SAFETY ENVIRONMENT

Context

Eurospi 2015
Intelligent Transport Systems (ITS) have significant potential to enhance traffic safety. The potential for developments for motorcycle is great; several ITS technologies in-vehicle system to be introduced and adapted to motorcycles:

- advanced driver assistance system,
- intelligent speed adaptation,
- driver monitoring system,
- collision warning and avoidance system,
- lane keeping and lane-change warning system,
- visibility enhancing system,
- seat belt/helmet reminder system.

Complexity dramatically increases with connectivity, safety features, etc. How to fulfill the OEM role and duties in such conditions? Which environment for this challenge? Which requirements for this challenge?
KTM FUNCTIONAL SAFETY ENVIRONMENT

KTM Requirements

Eurospi 2015
KTM REQUIREMENTS

Req1 - Central repository for traceability, workflows, configuration and change management

- We want a central repository of design to ensure “full” traceability over the product lifecycle. We also want this repository to provide workflows, configuration and change management capacities to support all the lifecycle processes requested by Automotive SPICE [11] process reference model or similar.

Rationale: Our engineers and functional safety managers are losing too much time checking consistency between the different sources of information (usually hosted in different tools). This prevents from having traceability. Risk management requires traceability between risks, requirements and design.
KTM REQUIREMENTS

» Req2 - Model Based Engineering

– We want to introduce the Model Based System Engineering and the safety analysis by the models in a fluent and integrated manner. The goal is to execute the safety analysis activity based on described and updated model by the architects (not based on more or less equivalent side architectures because of tools constraints).

Rationale: contribute to break silos in a manner which avoids unproductive and error prone processes due to multiple interface tools exchanging information. Safety teams are always running after the current baseline. Safety analysis and requirements shall be available for all and integrated in the architecture baseline.
KTM REQUIREMENTS

» Req3 - Joint Activities Management
  – We want to cover the functional safety management scope in the same environment R&D and other departments operate in. This includes Model Based Engineering but also project management, specifications, planning, etc. As for Model Based Engineering, we want the stakeholders to share the same working content.

Rationale: to break the silos between functional safety and R&D (and any other department).
KTM REQUIREMENTS

 Req4 - Automatic Reporting

- We want an automatic documentation generation to avoid errors and maximize productivity; the underlying content shall still be validated and reviewed; but the formatting and the generation of the documentation shall be executed automatically based on iterative patterned representation of structured data.

**Rationale:** our engineers would focus more on their core objective (safety, design, etc.) instead of the formatting of documents or the consistency of its content. Another argument is that ISO26262 required safety case is basically a good report. What if the safety case was automatically generated out of a consistent database (with reviews)?
 Req5 - Modularity and Reuse

- We want to access the modularity knowledge and skills.
- We want to populate our new projects with existing and validated items (functions, products, requirements, risks, etc.).
- We want to be able to “branch” design items (copy an item in another project and make it evolve independently from the original instance).
- We want to create platforms of products reusable on various bikes for modularity.

Rationale: we do not reuse enough legacy developments which is the core knowledge of the company. Doing so could save significant time, money and risks.
KTM FUNCTIONAL SAFETY ENVIRONMENT

ISO26262 coverage of the KTM environment

Eurospi 2015
ISO26262 COVERAGE OF KTM ENVIRONMENT

KTM understanding of major ISO26262 artefacts and activities:

- KTM aims at getting the largest coverage possible for these identified artefacts and activities. The KTM environment keeps this objective as a requirement.

- For a better readiness of what is covered by the KTM development process, every ISO26262 chapter and its coverage status are listed.

- Please refer to the paper for a complete and detailed coverage listing.

Most of the system and concept phase is covered because, as an OEM, KTM does not have hardware / software developments. Though, KTM expects a low effort to ensure this environment complies with the hardware / software requirements (part 5 / 6 of the ISO26262).
KTM FUNCTIONAL SAFETY ENVIRONMENT

KTM solution to its problem

Eurospi 2015
KTM SOLUTION TO ITS PROBLEM

**Tools**

- Matlab Simulink
  - For the simulation
  - For the hosting of the models (functional, safety and physical)

- Hip-Hops plugin for Matlab Simulink
  - Plugin developed by The Dependable Systems Research Group at the University of Hull
  - Implementation of safety description in models
  - Dependability analysis (flow propagation) to produce FTA and FMEA based on the models.

- Cognition Cockpit
  - For the hosting of engineering and management items (requirements, design, actions, tests, risks, etc.)
  - Central repository of development in a “PLM manner”

3 tools to cover most of KTM needs. With Matlab Simulink + Hip-Hops, we offer a workspace for various fields to work together, avoiding subjective interpretations. With Cockpit, we manage our data, make analysis and produce automatic documentation.
KTM FUNCTIONAL SAFETY ENVIRONMENT

KTM solution to its problem
→ Matlab Simulink & Hip-Hops

Eurospi 2015
Matlab Simulink - Intended use

- Used for physical simulation of some performance systems during the last years,
- Identified as a winner for our functional architecture needs as well,
- With HiP-HOPS plugin (generates functional safety analysis work products based on models) and Matlab Simulink, E/E systems could be entirely modelled under Matlab Simulink (physical, functional & safety),
- Investigate the architecture modularity topic: Simulink offers the use of libraries hosting reusable components. These components can embed different information such as safety.

Matlab Simulink – coverage of KTM requirements

<table>
<thead>
<tr>
<th>Req1</th>
<th>Central Repository</th>
<th>+</th>
</tr>
</thead>
<tbody>
<tr>
<td>Req2</td>
<td>Model Based Engineering</td>
<td>x</td>
</tr>
<tr>
<td>Req3</td>
<td>Joint Activities Management</td>
<td>x</td>
</tr>
<tr>
<td>Req4</td>
<td>Automatic Reporting</td>
<td>+</td>
</tr>
<tr>
<td>Req5</td>
<td>Modularity &amp; Reuse</td>
<td>x</td>
</tr>
</tbody>
</table>

Legend:
- x : fullfil the need
- +: contribute to the fulfilment of the need

The Simulink environment is made of 2 worlds. A world dedicated to the intended project and a library world for modularity. The project world intends to pick some modular components out of the library world. Safety content is integrated to models.
KTM FUNCTIONAL
SAFETY ENVIRONMENT

KTM solution to its problem
→ Cognition Cockpit

Eurospi 2015
Cognition Cockpit - Description

– Cognition Cockpit is well-known as a requirement management tool, especially in MD
– According to KTM, this solution has much more to offer than this basic feature. It is also a repository with a unified data model which can host any KTM required items during a dev:
  • Requirements Management: Requirements, Tests,
  • Design Management: Features, Products, Interfaces, Flows, etc.
  • Project Management: Meetings, Actions, Change request, Stakeholders,
  • Risks management: Risks, Failures, Mitigations
– All these items can be traced, follow a defined lifecycle, be managed in configuration, be part of a change request, be documented, etc.
– Once configured, the tool can support the state of the art processes such as SPICE
– It covers a chapter of the Design for Six Sigma, *measure product capabilities* (design parameters – CTQs), triggering Matlab Simulink simulation to update the design values and propagate the change to the top and thus measure the current product capability,
– The environment is open and very flexible. With existing features and some modifications, KTM has set up an ISO26262 environment. A connector with Matlab Simulink also offers the retrieval of any architecture items (blocks, flows, content, etc.).

*An ambitious, lightweight and flexible tool to gather them all.*
KTM SOLUTION TO ITS PROBLEM

Cognition Cockpit - Intended use

- Web-based solution identified as the one to fulfil the single repository of items feature
- The management of items is fully covered (traceability, configuration, change, documentation). The documentation is automatic and flexible. Therefore, KTM delivers documentation always consistent with the design.
- The Matlab Simulink Cognition cockpit connector allows retrieving the entire architecture (design & safety) in the repository.
- Each Matlab Simulink artefact is represented as a Cockpit object which has specific attributes, workflows and relationships.
- The relationships described under Matlab Simulink are retrieved likewise to Cockpit (a flow between two functions, a function allocation to a product, vehicle functions part of an item, a failure to a function, etc.).
- The change management is considered as well since each new synchronization with Matlab Simulink generates an impact analysis under Cockpit, highlighting outdated elements for example.

Complete management of objects, automatic documentation and interfaces with Matlab Simulink
KTM FUNCTIONAL SAFETY ENVIRONMENT

KTM SOLUTION TO ITS PROBLEM

Cognition Cockpit - Intended use
- Design artefacts from Matlab are then modelled under Cockpit as so:

Thanks to the architecture of KTM models, we can describe various items under Matlab Simulink which can later be reused in Cockpit for design management & documentation.
KTM SOLUTION TO ITS PROBLEM

Cognition Cockpit - Intended use

- KTM uses for ASIL purpose, Cockpit ability to create static and dynamic attributes
- Static ASIL objective for Hazards/Failure Modes/Failures artefacts

(*) Dynamic because it computes the value of the ASIL based on the maximum ASIL found on its linked artefacts. Allocation of ASIL takes place at Failures level. Other artefacts like Function dynamically provides an ASIL equal to the maximum ASIL found on its linked Failures.

We have a propagation of ASIL allocation based on the single allocation done at Failures level. The allocation analysis is executed once and data model automatically computes the maximum ASIL within an item, whichever level it is, giving an idea of the criticality of the artefact. A similar approach used for FIT rate is described in appendix.
All the artefacts, linked together is a solid foundation to fulfill ISO26262 in an elegant and fluent manner: Every decision can be documented. Every change is traced and can be justified. Every meeting has its minutes available. The change history of any artefact and its links can be reconstructed within a click. Documents represent the real content!
KTM SOLUTION TO ITS PROBLEM

» Cognition Cockpit - Intended use
  – Besides the design artefacts, Cockpit provides various supporting artefacts for development:
    • Processes,
    • Milestones,
    • Meetings,
    • Actions,
    • Users,
    • Change requests – As a parallel world, you can virtually impact the referential to validate changes or revert,
    • Documents – basically data mapping to a visual representation tabular or graphic,
    • Lifecycle

» Cognition Cockpit – coverage of KTM requirements

<table>
<thead>
<tr>
<th>Req1</th>
<th>Central Repository</th>
<th>x</th>
</tr>
</thead>
<tbody>
<tr>
<td>Req2</td>
<td>Model Based Engineering</td>
<td></td>
</tr>
<tr>
<td>Req3</td>
<td>Joint Activities Management</td>
<td>x</td>
</tr>
<tr>
<td>Req4</td>
<td>Automatic Reporting</td>
<td>x</td>
</tr>
<tr>
<td>Req5</td>
<td>Modularity &amp; Reuse</td>
<td>+</td>
</tr>
</tbody>
</table>

Legend:
• x : fullfil the need
• +: contribute to the fulfilment of the need

Cockpit fullfills 3 KTM requirements and innovate in the 1st one: Central repository with unique features as far as we have investigated the market
KTM FUNCTIONAL SAFETY ENVIRONMENT

Conclusion

Eurospi 2015
CONCLUSION

» Already large, since unquantified, benefits
  – Saving time by automatically importing architectures, document it and export it
  – Reuse of various steps of the dev. shows evidence of productivity and quality improvement.
  – Use of safety analysis dependability within a shared development model also proves collaboration improvement and consistent documentation.

» Still two worlds
  – Segregation between two environments which, according to KTM experience, also raises useless error prone processes and remaining silos of data. Investigation in progress to improve this environment and tries to make it even more integrated but the lack of flexible solutions embracing the whole process is remarkable on the market.

» Next steps
  – Generate more document from Cockpit data
  – Integrate the physical behaviour within the current models (Functional + Safety) and make use of the “product capability” feature of Cockpit ➔ See Appendix

“No matter how long the journey appears to be, the important thing is to go in the right direction”, Matthieu Ricard.
KTM FUNCTIONAL SAFETY ENVIRONMENT

Appendix

Eurospi 2015
The vehicle shall have a braking distance of **less than 50 meters** @ 90Km/h on dry a road ➔ **65.3 meters**

**Vehicle Level**

**Matlab Simulink**

- The vehicle shall have a braking distance of **less than 50 meters** @ 90Km/h on dry a road ➔ **65.3 meters**
- The vehicle shall have a friction indice of **at least 0.8** on dry roads
- The vehicle shall start wheel braking within **less than 300ms** following the rider request
- The vehicle shall have a braking torque of **at least 2000Nm**

**Excel File**

**Cockpit Formula**

- The braking system shall weight **less than 900Kg**
- The braking system shall be composed of **2** braking assemblies (one per wheel)
- The braking system shall weight **less than 21Kg**
- The braking system shall mechanically react within **less than 300ms** following the rider request
- The vehicle shall have a braking distance of **less than 50 meters** @ 90Km/h on dry a road ➔ **65.3 meters**

**Component level**

- The braking disk unitary shall weight **less than 10.5Kg**
- The braking disks shall provide each a surface of **1m²**
- The braking disks shall provide each a surface of **1m²**

**Cognition Cockpit & Simulink** to provide this great feature
Cockpit offers to monitor the system performances during the development phase through models hosted under Cockpit (Simulink, Excel, internal). Within a click we can check the concatenated performance compliance and confidence from the top.
APPENDIX

Application of performances management through FIT rates allocation and management

- FIT rate allocation is considered by KTM as a complex activity on large systems. A function can be part of 2 or more hazards at the same time. It is complex to find an optimum.

1. Excel bi-directional connector provided with Cockpit: hazards FIT objective, the minimal cut-sets and initial function objectives are exported out of Cockpit into an Excel template for FIT rate optimized allocation.

2. Excel solver is launched and computes an optimal FIT rate allocation for each function considering the objective (to have a maximum overall FIT rate, to make sure we constraint the less our suppliers) and constraints (to remain under the hazards ISO26262 FIT rate objective for a given ASIL).

3. Excel file is uploaded and optimal data are retrieved to Cockpit. The FIT rate of each function is updated.

4. FIT rate target are allocated to functions. Cockpit handle now the management of overall FIT rate compliancy through Minimal Cut Sets traceability. A new release of a product specification would then contain the new FIT rate requirements in line with the overall hazard objective.

KTM has implemented performances management through Cockpit + Excel for FIT rate.

KTM has not yet implemented the performances management through Cockpit + Simulink but has elected a project for the Proof of Concept starting next month.