Safety versus agility - being flexible and getting safety

DETANGLE's objective is aligning the engineering of safety-critical systems with agile methods by monitoring the ability to flexibly handle safety requirements during later iterations as well without an extensive up-front design which is hard to adapt afterwards. DETANGLE offers the appropriate dashboards and views to show safety compliance to certification authorities based on engineering data and evidence.

Generally, software projects aim at developing maintainable and comprehensible systems to be able to add functionality later and fix errors fast. Additionally, engineering safety-critical systems has to guarantee a high level of correctness and and a very low proneness to errors of safety requirements and unintentional side-effects in between. Developing software for safety-critical systems normally proceeds along the V-Model by completing each of its phases in a subsequent order. For instance, the design needs to know all safety-related requirements and their potential risk analysis beforehand to guarantee the safety properties of the system. The implementation and validation phases have to provide a high-level of evidence that each safety requirement and property has been implemented correctly.

In contrast, developing software in an agile way implies a much more granular iteration process with clarifying requirements just for the next iteration only. It provides flexibility for project managers and engineers since not all requirements have to be fully specified at an early stage and the design has not to be completed, thus excluding any major changes later.

Engineers and managers would prefer to design a well-structured safety-critical ystem AND benefit from the advantages of the agile approach like more flexibility with respect to changes. Nevertheless, there has to be built-in certification support of a mixed approach to guarantee safety-critical properties when using agile approaches.

Applying the DETANGLE method and analysis allows achieving more than traceability of safety requirements from specification down to code level. DETANGLE creates a new level of safety transparency of the design and implementation by analyzing code changes continuously across the repository to combine and augment it with data from Requirements-Engineering and Bug-Tracking systems.

Managers and engineers are able to monitor the comprehensibility and error-proneness of the code behind safety requirements. The DETANGLE Requirements Maintainability Index measures the modularity of safety requirements, their implementation cohesion and separation degree from each other in code. Engineers and managers know at any point of time which parts of the code can easily be adapted to safety requirements later. By using the DETANGLE Feature Effort Estimation Index they also get an estimation about the effort needed to improve the changeability of less flexible code modules. In general, DETANGLE provides data-driven evidence to be used for certification purposes about the safety compliance of the software of a safety-critical system.