# Risk management for the prevention of serious engineering breakdowns and ensuring overall system safety

## 1. Scope of work

The current trend to support complex product development while supporting advanced engineering methods is towards the usage of comprehensive PLM systems as a company-wide information backbone. With such an approach, business processes are accelerated, and the design of new competitive products is supported, giving companies a framework that delivers transparency on product development throughout its entire life cycle. While this approach supports the integration of several engineering disciplines responsible for design content, it can be extended to integrate supporting disciplines that ensure the product's quality and customer acceptance.

The goal of an effective technical risk management system is to allow continuous system running and prevent serious engineering breakdowns, as well as to ensure the system safety and reliability. In order to achieve this goal, the technical risk management should be a living actor of the design process, linked to regulatory compliance needs to roll-out a product while meeting market and customer requirements. Integrating risk management to the design process enforcing it as real-time development driver ensures better design and project decisions, shortening time- to-market and reducing the risk of cost intensive product failures during the phases of usage and maintenance. As risk management is a process that accompanies the product during these later life-cycle phases it becomes also a driver of better new product development.

The sustained success of technical risk management is possible only through the efficient control of risks based on singular items or systems of a product. Different methods need to be applied for any instance of a product or product families, for this reason risk management needs to be used within the context of reusables assets, browsing through the product structure and considering all configured items. Therefore, the risk assessment and control methods need to become fully interoperable with configuration management within PLM as a fully integrated process, method, and application. As the basis for the method, which leverages the structured nature of PLM product representation, the items in the product structure can be associated with a tuple of failures, evaluations, and controls, enabling a systematic identification of risks based on the aggregation of the singular items and their associated risk tuples. The goal is the transparent presentation of all risk consequences, which then will be assessed qualitatively and quantitatively based on a specific product configuration. The impact of each change of an item and the associated risk assessment of the singular parts can be directly identified, being able to extrapolate the impact in the event that the items are reused in several product configurations.

With an appropriate model and method, the elimination of deficits (time delay, lower accuracy, etc.) within the assessment of interdependencies in risk consequences and the efficient control of technical risks becomes possible. The assessment and control of technical risks for any configuration needs to complete the closed loop of technical risk management within PLM that contains the process phases of identification, analysis, and assessment and control. In such a way, the overall gain of knowledge in the form of verification and validation of technical risk assessments can be realized. The impact of any design change can be investigated in the early phase of product development. The simulation of risk control measures should ensure the success of technical risk management. The developed solution (process, method, or application) should fulfil the requirements for product development of products based on international or national standards.

We consider the following research hypotheses:

1. The issue of interoperability of technical risk and configuration management is an uncertain issue.
2. The issue of interoperability of technical risk and configuration management is simultaneously a dynamic and multi-view issue.
3. A family of products discovers a core with shared technology. The developed solution (process, method, or application) should cover the product variety based on this core.
4. A family of products is defined as a deeply structured, dynamically configured system with an internal mechanism for the instantiation of a desired/dedicated product variant.

## 2. Objectives

In order to prevent serious engineering breakdowns and ensure the system's safety, a comprehensive model (formalism) for risk management integrating the impact of design changes should be proposed. A new rationale should for risk management modelling should be developed by defining reasonable approximations and expressing in useable formal form.

To make this formalism fully operational, several research issues arise, among others:

- What are the relevant characteristics of a configurable system-based product with regard to technical risk management? How can these characteristics be described in a formal way to propose appropriate methods in order to prevent serious engineering breakdowns and ensure the system's safety?
- How to integrate the "Dynamics" and "Multi-views" continuously and stepwise in the process of development and assessment of systems?
- Which constraints occur and how can those be mitigated and resolved to achieve a consensual or optimal systems convergence?
- Which software architecture is needed to achieve optimal data model and functional performance?
- How to evaluate the risk in order to prevent serious engineering breakdowns and ensure the system's safety.

## 3. Expected results

The conducted research activities on the integration of technical risk and configuration management within this project, which is a continuity of our research with Roche Diabetes Care GmbH (Germany), have to provide results with regard to processes, methods, and applications of technical risk management to prevent serious engineering breakdowns and ensure the system's safety. The implementation will be done in a development environment with the following capabilities:

- -Interactive modelling of risk for complex configurated products
- -Dynamic and multi-view modelling of technical risk and its assessment for the product family

- -Development of an integrated and distributed platform for technical risk assessment and control
- -Pilot usage of the proposed solution (process, method, or application) for technical risk management of an industrial product.