

FORMALSAFE - Formal Development for Safe Robotics

FORMALSAFE integrates and enhances basic technologies developed in various areas, such as *Formal Methods, Change Management, Semantic Documents*, to tackle evident challenges in supporting the development of safe and reliable technical systems.

Standards and regulations such as IEC 61508, or EN 50128 define safety requirements. Compliance to these norms and standards is certified by external evaluation bodies (e.g. TÜV in Germany). Such regulations do not only formulate requirements on the resulting system but also impose requirements on the *development process*. Developing highly safety-critical systems necessitates, for instance, the monitoring of how safety requirements have been addressed during the entire design- and implementation process (requirement tracing). These traces correlate documents in different phases of the development, giving rise to a notion of *consistency* of a development process.

Possible applications of FORMALSAFE range from maintaining e-documents to adaptation of Common Criteria evaluations to new software revisions. The envisioned techniques for change management cope with different degrees of formalisation. In all these cases, FORMALSAFE techniques help to ease and decrease the cost of the process of updating and evolving technical documents and systems.

FORMALSAFE provides:

- **comprehensive support for the development, adaptation and reuse of safe and dependable systems;**
- **heterogeneous structured document management and maintenance;**
- **a highly structured and highly flexible development process satisfying the requirements of certification;**
- **combinations of different logics and reasoning tools to support a sophisticated body of domain knowledge.**

Robotics

Robotics is a huge and growing market. However, applications in future key market areas such as service robotics, health care, or logistics require a high degree of *interaction with humans*, and are challenged by *safety* concerns. Key features of safety-critical systems are dependability and trustworthiness.



Robotics is an area where system development is characterised by rapid prototyping and the need for experiments. As opposed to software, which once finished (and verified) can be reproduced in unlimited number at negligible cost, hardware has a highly relevant production cost factor, the minimisation of which is an important economic goal. There is often a need to implement hardware changes in an existing product, when cheaper or better hardware components become available or the behaviour of a prototype is unsatisfactory. This will affect the entire design and development, leading to changes in the software that take the altered structure of the system into account. Initial assumptions for design decisions have to be revisited and possibly revised, and changes propagated through the entire development process.

Semantic Document Management

FORMALSAFE aims at a framework to embed, relate, and maintain the various types of documents occurring in a development. This comprises formal, semi-formal, and informal specifications, technical documents, hardware, software, and the corresponding

documentation. These documents vary in their degree of formalisation (and therefore in their degree of potential tool support), their underlying structuring, and also in the languages to describe them.

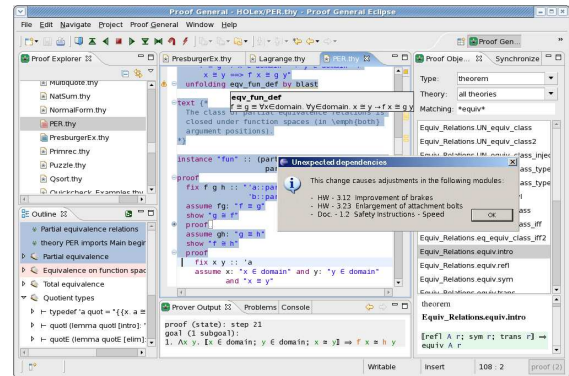
A *system-ontology* classifies documents according to their degree of formalisation, and the degree of tool support available. This enables one, for example, to pinpoint those paragraphs in an informal specification document that relate to a particular requirement formalised at a later stage of the development, and finally implemented by particular software functions or hardware components. The structuring of document parts can easily be formalised in terms of trees or graphs, allowing for the introduction of a notion of (weak) *consistency* by imposing constraints on permissible structures.

Management of Change

FORMSAFE supports the *evolutionary process* of constructing a development. This comprises the persistent update of individual documents as well as the evolution of the structuring relations between different document parts in the development processes. Imposing, for instance, a fixed (semantic) structure of document parts allows for comprehensive tool support when changing or updating existing parts.

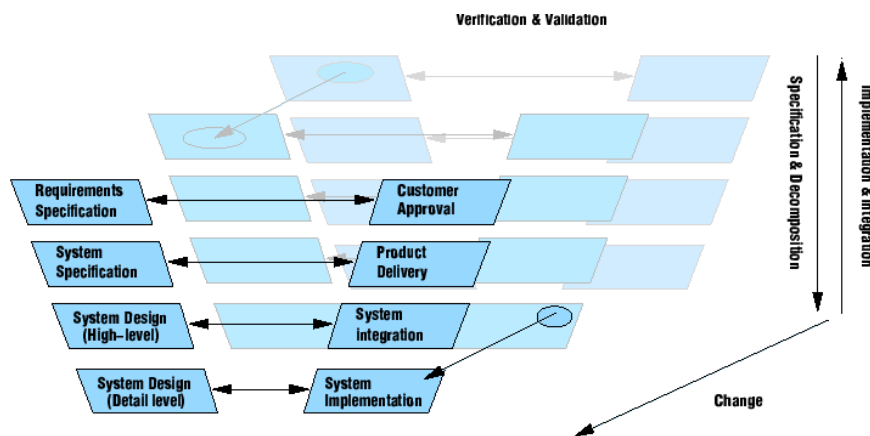
Changes in document parts can be propagated along the given relations to necessary changes in other dependent document parts. Depending on the degree of formalisation, the adaptation of these parts can be assisted by synthesis or reuse tech-

niques developed for formal methods. When changing, for instance, the informal requirements for a robot, there is a need for propagation of the changes to the related parts of the formal specifications, to parts of the resulting software, or even to necessary changes in the hardware. The higher the degree of formalisation, the more the system will be able to assist the user in performing the necessary changes.



Reuse of Developments

Reuse does not only encompass the adaptation of existing documents to changed needs, but also of the whole *development process*, by transferring the chronological evolution of the structuring relations between the various document parts to the changed situation.



CONTACT:

Prof. Dr. Bernd Krieg-Brückner

Deutsches Forschungszentrum für Künstliche Intelligenz
Safe and Secure Cognitive Systems
 Enrique-Schmidt-Straße 5, 28359 Bremen
 E-Mail: Bernd.Krieg-Brueckner@dfki.de

GEFÖRDERT VOM



Bundesministerium
 für Bildung
 und Forschung