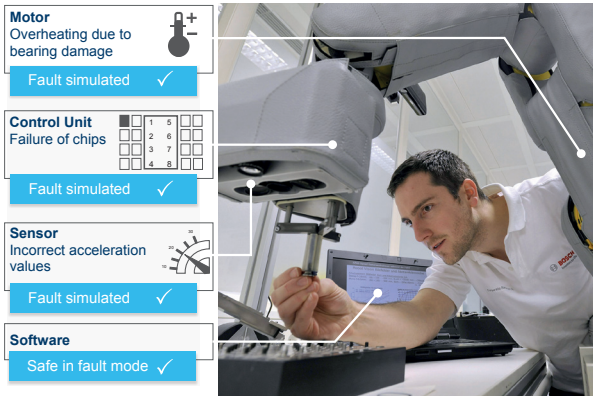
Goals and Scope of EffektiV

The EffektiV project explores and develops novel methods and tools for efficient fault effect simulation of intelligent motion control systems in industrial automation.



Following this path EffektiV aims at:

Early Verification of Correct and Safe Functionality of Heterogeneous Systems by Virtual Stress Test

The EffektiV benefits are:

- » **Safety** Operational Safety against faults that could not be provoked in hardware
- » **Flexibility** Fast adaptation of system tests to custom specific variants for Industry 4.0 applications
- » **Efficiency** Avoidance of expensive iterations due to issues during final hardware system test

Domains Addressed in EffektiV

Software Domain

Mechanical/ Physical Domain

Electrical/ Electronic Domain

Partner

BOSCH

SIEMENS

Universität Bremen

EBERHARD KARLS UNIVERSITÄT TÜBINGEN

infineon

FZI

UNIVERSITÄT PADERBORN
Die Unternehmer der Informationsgesellschaft

Subcontractors

Fraunhofer IIS

OFFIS
INSTITUTE FOR INFORMATION TECHNOLOGY

TUM

Support is provided by:

edacentrum

DLR Projektträger

EffektiV

Efficient Fault Simulation with Virtual Prototypes for Qualification of Intelligent Motion-Control-Systems in Industry Automation

a public funded research project

Runtime: 10/2013 - 09/2016

Abstract

The EffektiV project explores and develops novel methods and tools for efficient fault effect simulation of intelligent motion control systems in industrial automation. The goal is to analyze fault effects by using virtual prototypes in early design phases. The project focuses on the development of cross-domain fault models and the application of a virtual model for efficient, fast but yet accurate, fault effect simulation at higher levels of abstraction. Thereby the control software can be made safe against diverse faults by extensive stress tests. Even a comprehensive observation of all relevant fault scenarios becomes possible at an early stage. This avoids iterations with expensive design changes, reduced functionality or even putting the product success and competitiveness at risk. Furthermore, the methods, which are developed in the project, allow the simplification and acceleration of the FMEDA process.

Contact

Dr. Jan-Hendrik Oetjens
(Project Coordination)
Robert Bosch GmbH
phone +49 7121 35 4684
jan-hendrik.oetjens@de.bosch.com

Dr. Andreas Vörg
(Project Management)
edacentrum GmbH
phone +49 511 762-19686
voerg@edacentrum.de

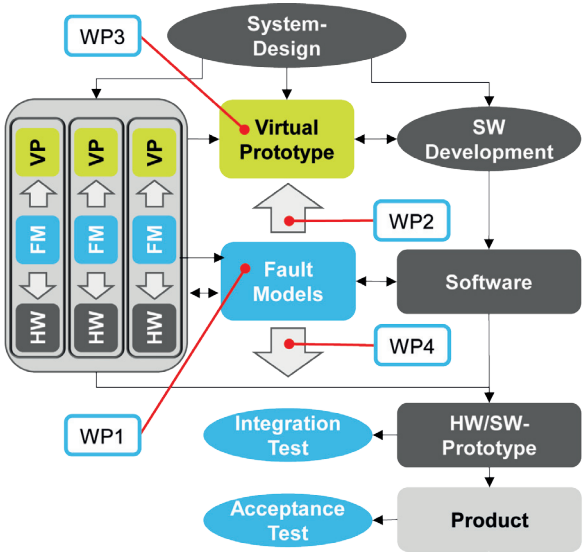
SPONSORED BY THE
Federal Ministry of Education and Research

The EffektiV project (project label 01IS13022) is supported within the Research Programme ICT 2020 by the Federal Ministry of Education and Research (BMBF).

Structure

The EffektiV project is divided in the following workpackages:

» WP1: Fault Modeling
» WP2: Fault Simulation Environment
» WP3: Fault Scenarios and Stress Test
» WP4: Connection to Development Process



Based on a top-down approach from the system level, hardware components (left) and software (right) are developed in parallel. The application of fault effect simulation is not only performed by the supplier of the system components (left), but also by the integrator using the virtual prototype (VP) of the system (middle). In work package WP1, requirements are defined for fault tolerant systems and fault models. Furthermore fault modeling and related libraries are developed. In work package WP2, the simulation of fault effects in virtual prototypes of the system components and the total system are developed. Besides the injection of faults, also the creation of efficient fault simulation environments is subject of the research. Based on the general methodology for fault injection, in work package WP3, a strategy for the definition, analysis and refinement of fault scenarios with tight connection to the requirements engineering is worked out. The objective is to have an efficient verification strategy in place. Work package WP4 is focused on the concrete application of the developed methods and on libraries for the creation of stress tests.

Certified Safety for Industry 4.0 by Efficient Fault Effect Simulation

In the context of the Industry 4.0 initiative, production plants become highly complex intelligent systems, which combine a variety of electronic, electrical, and mechanical components that need to interact smoothly during their operation. Novel cross-domain fault models and efficient qualification techniques are required for the evaluation of functional safety aspects in early design phases.

Highly critical issues in the development of future production plants are imposed by motion control systems, which manage the fast and most accurate positioning and motion control of conveyor belts and robot arms, for instance. As of today, the final tests of those systems are mainly based on physical prototypes to ensure the correct and safe operation of the system.

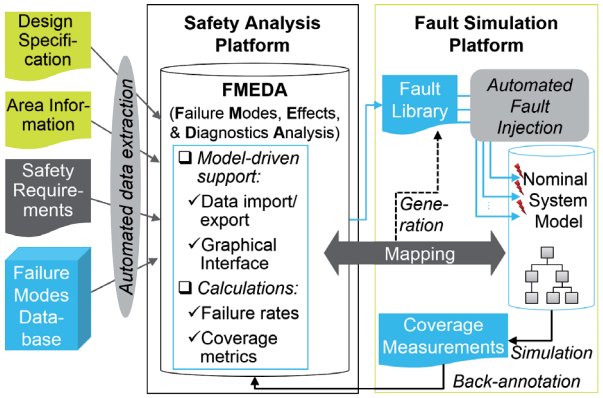
But what happens, if for instance single chips in a robot's control unit fail, if a motor due to a bearing damage overheats or a sensor delivers faulty data? Is it possible to develop and test the control software of these systems in a way that in case of faults in one or more components the total system always remains in a safe state? Is it guaranteed that humans near to these machines are not harmed and expensive parts like motors or robot arms are not destroyed?

In conventional system development, physical prototypes and extensive system tests are needed. However, those prototypes are available only in later phases of the design process. Additionally, due to physical constraints, several specific errors can hardly or not at all be injected or provoked during a physical prototype based test. To overcome those constraints, EffektiV promotes the use of fault effect simulation based on virtual prototypes, which provide hardware simulation models of electrical and electronic components replacing their physical counterparts for safety qualifications in early design phases.

Fault effect simulation will allow for safeguarding the reaction of complex systems for future production as well as for automotive and safety engineering against such faults that could hardly or not at all run through in real hardware tests yet. Thereby the safety of the systems is increased in spite of their fast growing complexity. Additionally, the efficient development of safe, reliable and robust products for instance complying with the standards IEC 61508 and ISO 26262 is essentially supported. EffektiV observes all relevant components along the value chain. Thereby, based on the EffektiV methodology, it will be possible to gain early and comprehensive insights into the system behavior in fault situations and to integrate the findings in product development. EffektiV will allow for an increase of the innovation pace and thereby an additional competitive advantage in the area of safety-sensitive systems.

EffektiV and FMEDA

In the EffektiV project problematic divergences between the two main safety evaluation aspects: probabilistic analysis and fault simulation are addressed. In fact, both of them are considered to certify systems deployed in safety-critical domains with respect to robustness properties. Therefore, a systematic data exchange between safety analysis and fault simulation is convenient.



Through model-driven development techniques, we formalize Failure Modes, Effects, and Diagnostics Analysis (FMEDA) and establish a link to fault injection and simulation. Thereby, the traditional FMEDA process is simplified and accelerated. Manual data entering is replaced by an automated extraction of the conventional inputs such as the design specification, area information, application-dependent safety requirements, and failure modes database. A graphical user interface is used within the safety analysis platform to enhance data handling and visualization. Furthermore, plausibility checks are implemented to help safety analysts to assess the consistency of FMEDA calculations (failure rates and diagnostic coverage metrics). Matching algorithms are used to map specific artefacts of the FMEDA data model to appropriate system model elements. Subsequently, a library of concrete faults to be injected is generated. During simulation runs, corresponding diagnostic coverage values are measured. These are back-annotated into the FMEDA model in order to detect potential deficiencies of the safety measures and accordingly refine them. The EffektiV solution offers a considerable speed-up of the safety assessment cycle, reduces cumbersome and error-prone tasks, and improves the quality of evaluation outcomes.