In safety-critical applications, special measures are required to avoid software errors in crucial control systems. Where extremely high safety requirements must be met, the use of formal methods is recommended. And, in future, their use in such application fields will actually be necessary , the "classical" development of safety-critical systems being too error-prone. These ever-increasing requirements result in high costs. Thus, an adequate tool support based on formal notations together with an appropriate development method must be designed. The integrated project, ESPRESS, which is funded by the German Federal Ministry for Education, Science, Research and Technology (BMBF) and coordinated by Daimler-Benz Research, is intended to fill this gap.

Goals

The ESPRESS project seeks to broadly improve productivity in the development of complex safety-critical embedded systems and to enhance system reliability itself. The main concern here is to provide a uniform, methodical, tool-supported software platform. The suitability and practical orientation of such a platform will be ensured by constant evaluation and the stepwise improvement of components, concepts and the corresponding tools. This will be achieved by conducting industrial case studies with practical relevance, that is based on real applications of the project partners in the areas of electronic automobile and traffic systems.

Overall Methodology

The methodology envisaged for the development of safety-critical embedded systems may be outlined as follows (see figure). The essentials are 1) an explicit separation of functional and safety requirements, 2) the combination of graphical (Statecharts) and formal (Z) techniques for specification,
3) (semi-)automated verification and code generation and 4) the execution of systematic tests. The development process consists of three phases:

1. Abstract requirements specification

2. Concrete design and refinement

3. Program and test generation

The successful application of formal techniques calls for the explicit formalization of background knowledge about the application domain - knowledge that is generally only available in the experts' heads. But it is only with such knowledge, taking real-time and distribution aspects into account, that the relevant physical and technical constraints can be given adequate consideration in safety requirements.

Such safety requirements and the correctness of the development steps performed are checked using available verification techniques. System validation is done by systematic testing, where the determination of test cases and test execution and evaluation are highly automated. The application of formal specification techniques in the early development phases is utilized to automate subsequent development steps and to avoid errors or identify them at an early stage, such that they can be eliminated at reasonable cost.

Extensive prototypical tool support is provided to ensure the efficient application of the overall methodology. Using commercially available tools, the overall tool environment offers a uniform and sophisticated framework supporting all phases of development.c

ESPRESS

Ingenieurmäßige Entwicklung sicherheitsrelevanter eingebetteter Systeme

Engineering of Safety-Critical Embedded Systems

http://www.first.gmd.de/~esp ress

DAIMLERBENZ
doerr@DBresearch-berlin.de

lienert@fli.sh.bosch.de BOSCH

ISST
aborusan@isst.fhg.de

GMD
sergio@first.gmd.de

TU berlin
wg@cs.tu-berlin.de

Für sicherheitsrelevante Anwendungen werden in kritischen Regelwerken besondere Maßnahmen zur Vermeidung von Software-Fehlern gefordert. Für höchste Sicherheitsanforderungen wird der Einsatz formaler Methoden empfohlen. In Zukunft wird ihr Einsatz in solchen Anwendungsfeldern sogar unerläßlich sein, da die "klassische" Entwicklung sicherheitsrelevanter Systeme zu fehleranfällig ist. Diese steigenden Anforderungen erfordern einen hohen Aufwand. Daher müssen eine angemessene Werkzeugunterstützung auf Basis formaler Techniken und eine geeignete methodische Vorgehensweise entwickelt werden. Das Verbund-Projekt ESPRESS, das durch das BMBF gefördert und von der Daimler-Benz-Forschung koordiniert wird, soll diese Lücke füllen.

Ziele

Das Vorhaben ESPRESS zielt auf eine breite Verbesserung der Produktivität bei der Entwicklung komplexer sicherheitsrelevanter eingebetteter Systeme und auf eine Steigerung der Verläßlichkeit der Systeme selbst. Das Hauptanliegen besteht darin, eine durchgängige methodische und werkzeugunterstützte Software-Technologie bereitzustellen. Die Angemessenheit und Praxisorientierung dieser Software-Technologie werden durch die begleitende Erprobung und schrittweise Verbesserung ihrer Bestandteile, Konzepte und zugehörigen Werkzeuge sichergestellt, und zwar anhand praxisrelevanter industrieller Fallstudien, die aus realen Anwendungsfällen der Projektpartner in den Bereichen Kraftfahrzeug- und Verkehrselektronik stammen.

Gesamtmethodik

Die angestrebte Methodik zur Entwicklung sicherheitsrelevanter eingebetteter Systeme wird folgendermaßen umrissen (siehe Abbildung): Schwerpunkte sind 1) die explizite Trennung von funktionalen und Sicherheitsanforderungen, 2) die Kombination graphischer (Statecharts) und formaler Techniken (Z) in der Spezifikation, 3) die (halb-)automatische Verifikation und Code-Generierung sowie 4) die Durchführung systematischer Tests. Die Entwicklung wird in drei Phasen aufgeteilt:

1. Abstrakte Anforderungsspezifikation,

2. Konkreter Entwurf und Verfeinerung,

3. Generierung von Programmen und Tests.

Der erfolgreiche Einsatz von formalen Techniken erfordert die explizite Formalisierung von Hintergrundwissen über das Anwendungsgebiet, das in der Regel nur in den Köpfen der Experten vorhanden ist. Nur mit solchem Wissen, unter Einbeziehung von Realzeit- und Verteiltheitsaspekten, können in Sicherheitsanforderungen die relevanten physikalisch-technischen Randbedingungen ausreichend berücksichtigt werden.

Mit vorhandenen Verifikationstechniken werden Sicherheitsanforderungen und die Korrektheit durchgeführter Entwicklungsschritte nachgewiesen. Die Validierung der Systeme erfolgt durch systematisches Testen, wobei die Testfallermittlung, -durchführung und -auswertung automatisiert durchgeführt werden. Die Verwendung von formalen Spezifika-tionstechniken schon in frühen Entwicklungsphasen wird dazu genutzt, die weitere Entwicklung zu automatisieren, sowie Fehler zu vermeiden oder frühzeitig aufzudecken, so daß sie kostengünstig behoben werden können.

Zur effizienten Anwendung der gesamten Methodik wird eine umfangreiche prototypische Werkzeugunterstützung bereitgestellt, die einen einheitlichen und komfortablen Rahmen zur Entwicklung auf der Basis kommerzieller Werkzeuge liefert.