

# OPRAIL –

## Optimierung der Entwicklung bahntechnischer Systeme

Werner Damm, Hardi Hungar, Bernhard Josko  
Kuratorium OFFIS e.V.  
Escherweg 2  
26121 Oldenburg

### Kurzfassung

Zielsetzung des Projektes ist die Optimierung von CENELEC-konformen <sup>[1]</sup> Entwicklungsprozessen für bahntechnische Anwendungen. Hauptaugenmerk wird hier auf die für sicherheitskritische Anwendungen relevanten Sicherheitsstufen SIL 3 und SIL 4 <sup>[2]</sup> gelegt, welche den überwiegenden Anteil eisenbahntechnischer Systeme ausmachen. Hierbei sollen insbesondere die im Euro-Interlocking Konsortium <sup>[3]</sup> erarbeiteten Vorschläge mit berücksichtigt werden. An Hand ausgewählter industrieller Applikationen sollen zielgerichtet Optimierungen bezüglich Entwurfskosten und Entwurfszeit entlang folgender Grobziele betrachtet werden:

- Einsatz formaler und semi-formaler Methoden als Basis zur Implementierung modellbasierter Entwurfsprozesse
- Einsatz von Werkzeugen zur formalen Verifikation von Spezifikationen bahntechnischer Systeme
- Einsatz von Werkzeugen zur automatischen Generierung von Testfällen aus Spezifikationen
- Abschätzung des Laufzeitverhaltens von Software
- Erprobung und Bewertung der Methodik an Fallstudien
- Begleitende Begutachtung und Bestätigung der Normenkonformität der Prozesse und Methoden durch eine zugelassene Gutachterorganisation

Das Projekt ist Anfang des Jahres 2004 gestartet, so dass eine Vorstellung von Ergebnisse erst Mitte 2005 zu erwarten ist.



---

<sup>1</sup> Konformität zu den europäischen Normen für bahntechnische Anwendungen EN 50126, EN 50128, EN 50129 und EN 50159, die durch das europäische Komitee für elektrotechnische Normung (CENELEC, <http://www.cenelec.org>) entwickelt wurden.

<sup>2</sup> Die europäische Norm 50128 führt Techniken und Maßnahmen für 5 Software-Sicherheitsanforderungsstufen (Safty Integrity Level, SIL) auf, wobei 0 die niedrigste und 4 die höchste Stufe ist.

<sup>3</sup> Siehe [www.eurointerlocking.org](http://www.eurointerlocking.org)

# 1 Einleitung und Vorstellung des Themenkomplexes

## 1.1 Entwicklung bahntechnischer Systeme

Im Bereich der Bahntechnik gibt es eine lange Tradition, durch sorgfältig ausgewählte Methoden in der Entwicklung und eine gründliche Überprüfungspraxis bei der Zulassung einen hohen Stand der Systemzuverlässigkeit zu garantieren. Heutige Systeme enthalten in zunehmendem Umfang Software und komplexe elektronische Komponenten, womit erheblich leistungsfähigere und weniger personalintensive Systeme realisierbar werden. Mit der Verwendung der Digitaltechnik steigt die funktionale Komplexität Systeme enorm an, was einen erhöhten Aufwand nach sich zieht, um deren Zuverlässigkeit garantieren zu können.

Bekanntermaßen lassen sich selbst kleine Digitalkomponenten nicht erschöpfend für alle Eingaben und Systemzustände testen, weil die schiere Anzahl verschiedener Fälle den Zeitbedarf über jegliches realisierbares Maß hinaus ansteigen ließe. Es sind also andere, vom Ansatz her intelligenter und generellere Methoden gefragt, will man die Zuverlässigkeit nicht kompromittieren. Die resultierenden Aufwände in Entwicklung und Zulassung sind enorm, auf Seiten der Entwickler bahntechnischer Systeme herrscht ein großes Interesse an Verbesserungen des Entwicklungsprozesses. Aus Sicht der Forschung bietet sich zur Lösung die Verwendung „formaler Methoden“ an. Formale Methoden nutzen mathematisch-logische Verfahren, um über das Verhalten von Systemen wie Programmen, digitaler Hardware oder Digitalelektronik allgemein Aussagen zu gewinnen, wobei eben nicht jeder einzelne Fall separat betrachtet werden muss.

Hier liegt der Ansatzpunkt des Projektes OPRAIL: Die Integration von Werkzeugen und Verfahren, die auf formalen Methoden beruhen, in den industriellen Entwurfsprozess zur Sicherstellung der korrekten Funktion kritischer Komponenten und Systeme. Eine besondere Anforderung an den Transfer von Methoden, die aus der Forschung stammen, in den Bereich der Entwicklung von Bahnsystemen stellt die Formalisierung der Zuverlässigkeitsüberprüfung: Um für den Betrieb zugelassen zu werden, müssen die Systeme in einer den Normen entsprechenden Form entwickelt worden sein.

Die vom Europäischen Komitee für elektrotechnische Normung (CENELEC) etablierten europäischen Normen EN 50126 [<sup>4</sup>], EN 50128 [<sup>5</sup>], EN 50129 [<sup>6</sup>], EN 50159 [<sup>7</sup>] legen die verbindlichen Standards für die Entwicklungen von Systemen und Software von bahntechnischen Anwendungen, sowie für deren Sicherheitsanalyse fest. Diese Normen werden nachfolgend kurz als CENELEC-Normen bezeichnet. Sie definieren einheitliche Verfahren zur konsequenten Anwendung eines Managements für Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS [<sup>8</sup>]) für den gesamten Lebenszyklus bahntechnischer Systeme. Die Anforderungen steigen mit der Sicherheitsstufe (Safety Integrity Level, SIL) einer Anwendung: Anwendungen ohne Sicherheitsverantwortung wird die Sicherheitsstufe SIL 0, hochgradig sicherheitskritischer Software die höchste Sicherheitsstufe SIL 4, zugeordnet. Die

---

<sup>4</sup> Bahnanwendungen – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit; Deutsche Fassung EN 50126:1999.

<sup>5</sup> Bahnanwendungen – Software für Eisenbahnsteuerungs- und Überwachungssysteme; Deutsche Fassung EN 50128:2001.

<sup>6</sup> Bahnanwendungen – Sicherheitsrelevante elektronische Systeme für Signaltechnik; Deutsche Fassung prEN 50129:1999.

<sup>7</sup> Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme, Deutsche Fassung EN 50159:2001

<sup>8</sup> Reliability, Availability, Maintainability and Safety

Normen gehen auf Techniken und Maßnahmen zur Erreichung bestimmter Sicherheitsstufen ein und beschreiben den Zulassungsprozess für bahntechnische Anwendungen. Allerdings schreiben sie keinen konkreten Entwicklungs-Lebenszyklus vor, so dass sich einerseits der Vorteil größtmöglicher Prozessflexibilität, andererseits aber auch der Nachteil der fehlenden belastbaren Prozessgrundlage ergibt.

## 1.2 Ansatz des Projektes OPRAIL

Das Gesamtziel des OPRAIL-Projektes ist die Optimierung von CENELEC-konformen Entwicklungsprozessen für bahntechnische Systeme. Die Teilziele werden hier kurz skizziert und später näher erläutert:

- Erstellung eines modellbasierten Entwicklungsprozesses, der auf semi-formalen Methoden aufbaut und eine Integration formaler Methoden vorsieht. Insbesondere sollen hier die von Euro-Interlocking empfohlenen Methoden UML [<sup>9</sup>] und Statemate [<sup>10</sup>] betrachtet werden. UML ist eine sehr umfangreiche Sprache. In OPRAIL soll eine für sicherheitskritische bahntechnische Anwendungen adäquate Teilsprache identifiziert werden.
- Werkzeuge für die formale Verifikation, die automatische Testvektorgenerierung und die Abschätzung des Laufzeitverhaltens auf der Zielarchitektur werden entwickelt bzw. optimiert.
- Die Anwendbarkeit der entwickelten Prozesse und der eingesetzten Methoden und Werkzeuge wird anhand von Fallstudien evaluiert und die Konformität mit den CENELEC-Normen überprüft.
- Der Verlauf des Projektes wird in einschlägigen Fachmagazinen, auf Konferenzen und Gremien vorgestellt. Auch der Informationsaustausch mit Zertifizierungsstellen, Euro-Interlocking und dem Verband der Bahnindustrie in Deutschland e.V. [<sup>11</sup>] wird angestrebt.

Das Spektrum des Konsortiums reicht von der Forschung über Technologiespezialisten und Beraterfirmen bis hin zu Entwicklern von bahntechnischen Systemen. Durch die Einbeziehung des TÜV sind alle wesentlichen Kompetenzen zur Weiterentwicklung moderner, normkonformer Entwicklungsprozesse versammelt. Im einzelnen gehören dem Konsortium an:

- **Kuratorium OFFIS e.V.** (Koordinator). Der F&E-Bereich „Sicherheitskritische Systeme“ des Forschungsinstitutes arbeitet seit mehr als zehn Jahren an Methoden zur Optimierung der Entwurfsprozesse für eingebettete Systeme.
- **ALCATEL SEL AG.** Der beteiligte Unternehmensbereich „Transport Automation Systems“ der Alcatel SEL AG ist maßgeblich an der Entwicklung und dem Bau eigener Zugsteuerungs-Systeme, Stellwerks-Systeme und vielfältiger ergänzender Anlagen für die Deutsche Bundesbahn und ausländische Bahnverwaltungen im Nah- und Fernverkehr beteiligt.
- **Berner&Mattner Systemtechnik GmbH.** Ein Entwicklungs- und Beratungsunternehmen im Bereich technischer Software mit umfangreichen Erfahrungen im Bereich Automotive, Schienenverkehrstechnik sowie Aerospace & Defense zum Einsatz objektorientierter Prozesse und Methoden in Verbindung mit der UML.
- **DEUTA Werke GmbH.** Die Firma ist einer der führenden Anbietern von Komponenten und Systemen für die Ausrüstung von Schienenfahrzeugen.

---

<sup>9</sup> UML: Unified Modeling Language, siehe <http://www.omg.org/uml/>

<sup>10</sup> Siehe [www.ilogix.de](http://www.ilogix.de)

<sup>11</sup> Siehe <http://www.bahnindustrie.info>

- **OSC - Embedded Systems AG.** Die Firma vermarktet weltweit über ihren Kooperationspartner I-Logix Inc. Produkte zur Modellprüfung und Automatischen Testgenerierung für die Methoden StateMate und UML.
- **IfEV.** Das Institut für Eisenbahnwesen und Verkehrssicherung der TU Braunschweig bringt langjährige Erfahrungen im Bereich des Schienenverkehrs und der Anwendung formaler und semi-formaler Methoden ein.
- **TÜV.** Die Geschäftseinheit Rail der TÜV Automotive GmbH führt Prüfungen und Zertifizierungen sicherheitsrelevanter rechnergestützter Systeme, mit Schwerpunkt im Bahnbereich, durch.

## 1.3 Projektplan

### 1.3.1 Implementierung modellbasierter Entwurfsprozesse

Ausgehend von der aktuellen Situation werden die Anforderungen an einen Entwurfsprozess erfasst, die sich aus den Anforderungen der CENELEC-Normen für den Entwurf von sicherheitskritischen Systemen im Eisenbahnbereich ergeben. Als Grundlage für die Bewertung und Ableitung von Verbesserungsmaßnahmen werden etablierte Reifegradmodelle wie ISO/IEC 15504 (SPICE) [12] oder CMMI [13] eingesetzt. Aus den Analysen soll dann ein CENELEC-konformer Entwurfsprozess entwickelt sowie eine Methodik zum Einsatz formaler Methoden im Entwicklungsprozess erarbeitet werden.

Zentraler Bestandteil der Methodik ist der Einsatz von **Modellen** des Systems auf verschiedenen Entwurfsebenen. Eine Modellierung des Systems kann sowohl zur angemessenen Formulierung und Strukturierung der Anforderungen dienen wie auch die Grundlage für die Anwendung formaler Verifikations- und Validierungstechniken bilden.

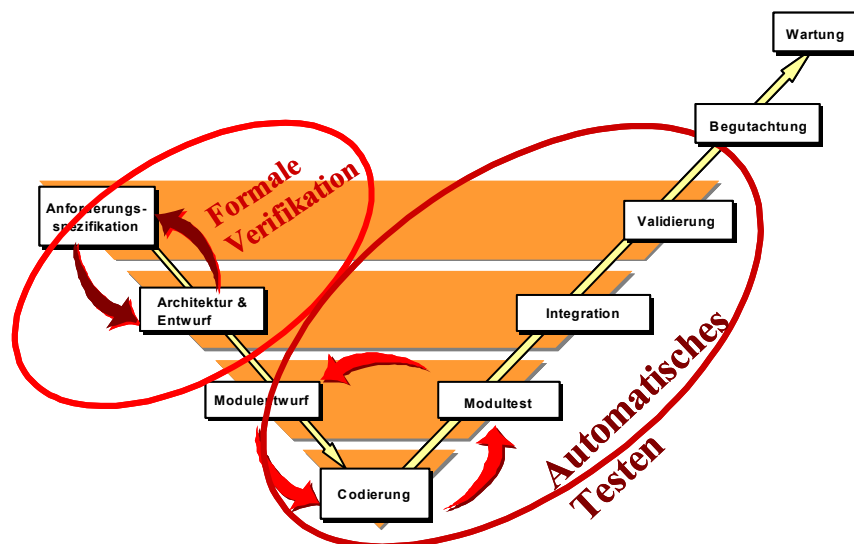


Abbildung 1 Entwicklungs-Lebenszyklus

<sup>12</sup> SPICE: Software Process Improvement Capability dEtermination. Siehe <http://www.sei.cmu.edu/iso-15504/>

<sup>13</sup> CMMI: Capability Maturity Model Integration. Siehe <http://www.sei.cmu.edu/cmmi/>

Die formale Verifikation erlaubt das Auffinden von Fehlern im System in frühen Phasen des Entwicklungsprozesses und verringert somit Entwurfszeit und -kosten. Die formalen Validierungstechniken ermöglichen automatisches Generieren von Testfällen. Somit kann die Funktionalität des implementierten Systems effizient gegen die Spezifikation geprüft werden.

Abbildung 1 zeigt einen in der CENELEC Norm EN 50128 empfohlenen Entwicklungs-Lebenszyklus, erweitert um die Anwendung formaler Methoden.

Unterschiedliche CASE-Tools werden bereits für den Ansatz der modellbasierten Entwicklung angeboten. In zunehmenden Maße erfährt auch die UML Beachtung in der Industrie. Die objektorientierte Beschreibungssprache UML beinhaltet ein reichhaltiges Repertoire an Beschreibungskonzepten und kann für die Softwareentwicklung unterschiedlichster Anwendungen eingesetzt werden. Für den Einsatz in sicherheitskritischen Anwendungen muss eine klare Einschränkung von Konzepten vorgenommen werden, um den Anforderungen für die Entwicklung sicherheitskritischer Systeme gerecht zu werden. Es wird daher auch Aufgabe des Projektes sein, eine geeignete Teilsprache zu identifizieren, die für die Entwicklung im Bahnbereich eingesetzt werden kann. Diese Teilsprache wird nachfolgend Safe-UML genannt.

### 1.3.2 Entwicklung prototypischer Werkzeuge für formale Methoden

Begleitend zur Entwurfsmethodik werden Werkzeuge zur Unterstützung der erforderlichen formalen Methoden bereitgestellt. Hier kann auf umfangreiche Vorarbeiten zurückgegriffen werden, die aber für den geplanten Anwendungsfall zu optimieren und signifikant zu erweitern sind. Die einzelnen Methoden werden im Folgenden vorgestellt

Zur Absicherung des korrekten funktionalen Verhaltens von Systemen sollen **formale Verifikationswerkzeuge** eingesetzt werden. Auf akademischer Seite sind hierfür zahlreiche Techniken entwickelt worden, die von automatischen über semi-automatische bis hin zu hochgradig interaktiven Verfahren reichen. Erfahrungen haben gezeigt, dass für den Einsatz im industriellen Umfeld vorrangig automatische Verfahren, so genannte Modellprüfverfahren (engl. Model Checking), geeignet sind. Innerhalb des Projektes sollen Modellprüfverfahren für Statemate und UML optimiert und weiter ausgebaut werden. Während für Statemate bereits auf ein kommerziell verfügbares Werkzeug zurückgegriffen werden kann, ist für UML nur ein erster Prototyp vorhanden, der für die Einsetzbarkeit im industriellen Umfeld noch wesentlich zu erweitern ist.

Für die Durchführung von Verifikationsaufgaben ist neben der Systemmodellierung in Statemate oder UML auch eine **formale Beschreibung der Eigenschaften**, die verifiziert werden sollen, erforderlich. Hierzu bieten sich zwei Formalismen an. Auf der einen Seite sollen durch Schablonen (property pattern) typische Verifikationsanfragen zur Verfügung gestellt werden. Diese stellen eine benutzerorientierte Sicht einer mathematischen Beschreibungssprache (Temporale Logik) dar. Hier sind im Kontext der bahntechnischen Anwendung relevante Schablonen zu identifizieren und werkzeugmäßig umzusetzen. Eine weitere Spezifikationsmethode bieten LSCs [<sup>14</sup>], eine Erweiterung der Sequenzdiagramme von UML. LSCs dienen zur Spezifikation der Interaktion zwischen einzelnen Komponenten.

Neben der eigentlichen Verifikationsaufgabe ist auch die Analyse der Verifikationsergebnisse entscheidend. Hierzu bieten die Modellprüfverfahren **Diagnosemöglichkeiten** an, in dem bei einer Widerlegung einer Beweisaufgaben Informationen in Form von einem Systemlauf, der ein Beispiel für die Widerlegung darstellt, angegeben werden. Diese Informationen sind für

---

<sup>14</sup> W. Damm and D. Harel. LSCs: Breathing Life into Message Sequence Charts. Formal Methods in System Design, 19(1):45 - 80, July 2001

den Benutzer in einer entsprechenden graphischen Darstellung oder in Form eines Simulationsskriptes aufzubereiten.

Um die Übereinstimmung eines entwickelten Systems mit einem (evtl. vorher validierten Modell) zu zeigen, sollen aus Systemmodellen auch **Testmuster** erzeugt werden. Hier sollen insbesondere die folgenden beiden Aspekte berücksichtigt werden:

- positive Testmuster zur Abdeckung des gewünschten Funktionsverhaltens
- negative Testmuster zur Überprüfung der Robustheit des Systems, d. h. Anlegen von Extremwerten, fehlerhafte Eingabesequenzen etc.

Beim Entwurf sicherheitskritischer Systeme spielen neben der Einhaltung funktionaler Aspekte einer Spezifikation die Erfüllung zeitlicher Bedingungen eine wesentliche Rolle. Um deren Einhaltung zu überprüfen zu können, sollen Methoden zur **automatischen Abschätzung der Laufzeiten** entwickelt werden. Als Besonderheit ist hier zu vermerken, dass insbesondere auch die Verteilung der einzelnen Softwaremodule (Tasks) auf einzelne Komponenten sowie die Verbindung zwischen diesen Modulen zu berücksichtigen ist.

### 1.3.3 Evaluierung und Bewertung des Ansatzes in Fallstudien

Die entwickelten Prozesse, Methoden und Werkzeuge werden in Fallstudien erprobt und bewertet. Hierbei werden auch Begrenzungen und Einschränkungen des Einsatzes formaler Methoden untersucht. Beide Bahntechnikentwickler ziehen hierfür Fallstudien aus der Entwicklungspraxis heran, so dass an realen Anwendungsbeispielen eine Bewertung der jeweiligen Ausprägungen des OPRAIL-Prozesses vorgenommen werden kann.

### 1.3.4 Einbindung von Gremien und Organen aus dem Eisenbahnbereich

Der in OPRAIL verfolgte Ansatz eines modellbasierten Entwicklungsprozesses unter Einbeziehung formaler Methoden ist bisher im Bereich der Bahnen nicht so stark verbreitet wie im Automobil- oder Luftfahrt-Sektor. Daher werden während der gesamten Projektlaufzeit aktuelle Ergebnisse bzgl. des entwickelten Entwurfsprozesses in einschlägigen Fachmagazinen veröffentlicht und auf Konferenzen präsentiert. Die Projektpartner pflegen Kontakte zu Institutionen und Fachgremien wie Euro-Interlocking [15], IRSE [16] oder AEIF [17] und werden diesen vom Projektverlauf berichten. Durch diese Aktivitäten wird nicht nur eine höhere Akzeptanz modellbasierter Softwareentwicklung im Eisenbahnbereich erwartet, sondern auch durch Diskussionen mit führenden Fachkräften fruchtbares Feedback für OPRAIL angeregt. Insbesondere ist geplant, nahe mit dem Eisenbahnbundesamt [18] und dem Verband der Bahnindustrie in Deutschland e.V. [19] zusammen zu arbeiten, um deren Anregungen aufzunehmen und potenzielle Probleme so früh wie möglich zu erkennen.

## 2 Projektstatus

Nach einer Laufzeit von einem halben Jahr hat das Projekt die im Antrag vorgezeichnete Planung überarbeitet, die wesentlichen Entscheidungen hinsichtlich der konkreten Ausgestaltung

---

<sup>15</sup> Siehe <http://www.euro-interlocking.org>

<sup>16</sup> IRSE: Institute of Railway Signal Engineers. Siehe <http://www.irse.org>

<sup>17</sup> AEIF: Europäische Vereinigung für Interoperabilität im Bereich der Bahn. Siehe <http://www.aeif.org/>

<sup>18</sup> Zertifizierungsstelle für bahntechnische Systeme in Deutschland. Siehe <http://www.eba.bund.de/>

<sup>19</sup> Interessensverband der Bahnindustrie. Siehe <http://www.bahnindustrie.info>

der Zusammenarbeit getroffen und die Bearbeitung der ersten technischen Arbeitspakete begonnen.

Als wesentliche Grundlage der Kooperation haben von einzelnen Partnern durchgeführte Schulungen die anderen in das jeweilige Spezialwissen eingeführt. Im einzelnen waren dies

- Berner&Mattner mit einer Einführung in die UML inklusive Werkzeugunterstützung für den UML-basierten Entwurf,
- TÜV Süd mit einer Vorstellung der für die Zulassung von Bahnanwendungen relevanten Normen sowie der Anforderungen an Entwurfsprozesse und –werkzeuge, welche aus den Normen resultieren, und
- OFFIS und OSC mit einer Einführung in die Grundlagen formaler Methoden sowie darauf basierender Techniken und Werkzeuge zur Validation, Verifikation und Testgenerierung.

Die Anwender DEUTA und ALCATEL komplementierten diese Schulungen durch eine detaillierte Darstellung der derzeitigen Entwicklungspraxis.

Auf technischer Seite sind geschehen:

- Die Anforderungen an einen Entwicklungsprozess, der innerhalb des Projektes exemplarisch realisiert und ausprobiert werden soll, sind zusammengestellt.
- Die Fallstudien, an denen die Methodik evaluiert werden soll, sind von den Bahntechnikentwicklern ALCATEL und DEUTA ausgewählt worden.
- Die Verfahren zum Modelchecken und zur Generierung von Testfällen in ihrer jetzigen Form sind einer Analyse im Hinblick auf die Anwendbarkeit im Bahntechnikbereich unterzogen worden.

### **3 Erfahrungen, Bewertungen und Ausblick**

Die einzigartige Konstellation der Kooperationspartner hat in der ersten Phase des Projektes für alle Beteiligten neue Perspektiven aufgezeigt.

Aus Sicht der Forschung herausfordernd sind die Aspekte, die sich aus der Zulassungsprüfung ergeben. Neben der rein technischen Beherrschung der formalen Analyse komplexer Systeme (welche bereits ein anspruchsvolles Problem darstellt) tritt die bisher wenig beachtete Notwendigkeit, die Vollständigkeit der Analyse nachweisbar zu machen.

Auf Seiten der Bahntechnikentwickler lässt die Möglichkeit, formale Methoden kennen zu lernen und deren Werkzeugunterstützung in der Praxis evaluieren zu können, einen Blick in die mögliche Zukunft der Entwicklungspraxis werfen.

Insgesamt sind Herausforderungen auf technischer – bestimmt durch die inhärente Komplexität der Systeme –, organisatorischer – die formalen Methoden müssen in einer den Entwicklern zugänglichen Form nutzbar gemacht werden – und formaler Ebene – die aus dem Zulassungsprozess resultierenden Anforderungen – identifiziert worden. Dies fand in der Formulierung einer Vision für das Projektergebnis eine Umsetzung: Ziel des Projektes soll es sein, die durch Anwendung formaler Methoden möglich gewordenen Analysen im praktischen Entwicklungsprozess vorteilhaft nutzbar zu machen.

Das bereits in der Anfangsphase schnell etablierte Klima der Zusammenarbeit zwischen den Partnern lässt eine erfolgreiche Fortführung des Projektes und das Erzielen eines greifbaren Ergebnisses im Sinne der Ziele der Forschungsoffensive „Software Engineering 2006“ erwarten.