

Entwicklung sicherheitskritischer Systeme – der Bereich der „Beckmesser der Informatik“

Der von apl. Prof. Dr. Bernhard Josko geleitete Forschungs- und Entwicklungs-Bereich „Sicherheitskritische Systeme“ (SC) ist spezialisiert auf die Entwicklung sicherheitsrelevanter Steuerungssysteme. Ein Beispiel dafür ist das Autopilotensystem eines Flugzeuges. Kleinste Systemfehler können hier katastrophale Folgen haben. SC entwickelt neue Methoden und Software-Werkzeuge, die es ermöglichen, solche elektronischen Steuerungssysteme schon im Entwurfsstadium auf alle denkbaren Fehler und Krisensituationen hin zu testen. Dabei spielen formale Methoden, präzise Semantiken und automatisierte Verfahren zur Verhaltensanalyse eine große Rolle. Mit dem Einsatz von derlei Techniken geht ein erheblicher Aufwand einher, der aber gerechtfertigt ist, wenn die Korrektheit des Ergebnisses sehr wichtig ist. Und wo ist es wichtiger, sich auf ein eingebettetes System hundertprozentig verlassen zu können, als wenn es um Menschenleben geht?

„Da schlägt die Stunde der Beckmesser der Informatik“, formuliert es mit einem Augenzwinkern PD Dr. Hungar, der im Bereich für die Technologieentwicklung zuständig ist. „Um gefährliche Fehler zu vermeiden, muss man sich an geordnete Vorgehensweisen halten und die Ergebnisse genau kontrollieren.“

Der Bereich kooperiert zumeist mit Anwendern aus dem Verkehrs-

bereich, also dem Automobil-, Luftfahrzeug- und Eisenbahnbau. Drei aktuelle Projekte werden in dieser Ausgabe jeweils kurz vorgestellt. Eine Anwendung der klassischen Verifikation finden wir in der BMW-Kooperation. Den Gesamtzusammenhang in der Entwicklung betrachtet das Projekt OpRail (Bahn). Dass neben der Elektronik auch der bedienende Mensch in die Analyse einbezogen werden muss, demonstriert SC im Luftfahrt-Projekt ISAAC.

Auch in Zukunft wird der Bereich wohl sein Schwergewicht in der Verkehrsdomäne haben. Ein wichtiger Baustein für die Weiterentwicklung ist die SafeTRANS-Initiative. SafeTRANS steht für „Safety in Transport Systems“. Hier kooperiert SC mit dem Forschungszentrum Sicherheitskritische Systeme der CvO-Universität und dem Deutschen Zentrum für Luft- und Raumfahrt in Braunschweig. Die SafeTRANS-Initiative plant u.a. die Beantragung eines Clusters an der CvO-Universität Oldenburg im Rahmen der Exzellenzinitiative der Bundesregierung.

Aber auch an eine Ausweitung der Anwendungsdomäne ist gedacht, selbst über den Bereich der sicherheitskritischen Systeme hinaus. Automatisierung und Nutzerfreundlichkeit einiger Verfahren haben ein Niveau erreicht, das eine Anwendung auch dann attraktiv macht, wenn Korrektheit nicht lebenswichtig ist. Über derartige Anwendungs-



Walter Hirche, Niedersächsischer Minister für Wirtschaft, Arbeit und Verkehr

Die zentrale marktwirtschaftliche Relevanz der Automobilbranche ist heute sprichwörtlich. Jedes Jahr werden weltweit 57 Millionen neue Fahrzeuge gebaut, mit denen ein Umsatz von 645 Milliarden Euro erzielt wird – das sind 15% des weltweiten Bruttosozialproduktes! Mit seinen Forschungen im Bereich der Erhöhung der Sicherheit und Zuverlässigkeit elektronischer Komponenten im Fahrzeug greift OFFIS für die Branche zentrale Fragestellungen auf – so dienen die Arbeiten ja insbesondere der Reduktion der Anzahl der Pannen und Rückrufe, oder der Absicherung extrem hoher Qualität für Teilsysteme, deren Ausfall hohe Risiken für Insassen bieten, die also sicherheitskritisch sind.

Dass OFFIS in diesem Bereich Spitzenstellung erreicht hat, wird durch die Vielfalt der Kooperationsbeziehungen und die Perspektiven zur Etablierung eines europäischen Centers of Excellence deutlich. Gerade für das Automobilland Niedersachsen ist die hierzu etablierte Kooperation im Rahmen der SafeTRANS-Initiative zur Erhöhung der Sicherheit von Transportsystemen mit dem DLR Institut für Verkehrsführung und Fahrzeugsteuerung in Braunschweig von strategischer Bedeutung. Mit dieser Ausgabe der datawork erhalten wir einen Einblick in die Ideenschmiede des Bereiches Sicherheitskritische Systeme – von Fragen der Absicherung des Codes in Steuergeräten bis hin zur Bewertung der Risiken von Bedienfehlern von Piloten wird eine breite Spannweite von Forschungsfeldern vorgestellt. Hierin sehe ich einen wertvollen Beitrag des OFFIS als Bindeglied für den Technologietransfer zwischen Wissenschaft und Wirtschaft.

szenarien wird in einer der nächsten Ausgaben der datawork zu lesen sein.

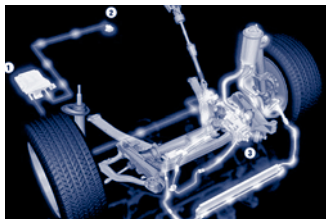
Bedienfehleranalyse im Luftfahrtbereich

Ein spezieller Fokus des EU-Projektes ISAAC liegt auf Autopilotensystemen und Fehlern, die bei ihrer Bedienung gemacht werden. Dafür müssen neuartige Techniken entwickelt werden. Neben dem System werden auch Bedienprozeduren, etwa Take-off und Landung, modelliert und dann in einem kognitiven Pilotenmodell verarbeitet. Das hier verwendete Pilotenmodell wurde bei einer Flugsimulatorstudie an der Lufthansa-Verkehrsfliegerstudie er-

stellt und fokussiert auf den kognitiven Prozess „gelernter Sorglosigkeit“. Bei der Bedienung von Autopiloten kann Sorglosigkeit entstehen, wenn sich bestimmte Bedienabläufe, z.B. Tastenabfolgen, als Routine einschleifen und die Piloten nach gewisser Zeit „verlernen“, dass es alternative Abläufe gibt und gewisse Vorsichtsmaßnahmen unterlassen. Unter Verwendung des Pilotenmodells wird in ISAAC automatisiert analysiert, welche Pilotenfehler durch „gelernte Sorglosigkeit“ entstehen können und welche Auswirkungen sie auf die Flugsicherheit ergeben. So kann menschliches Fehlverhalten bereits sehr früh im Entwicklungsprozess berücksichtigt und durch entsprechende Designänderungen vermieden werden.

BMW-Kooperation Verifikation

In einer Kooperation mit BMW hat SC eine bestehende Verifikationsumgebung an das Entwicklungswerkzeug ASCET-SD angeschlossen. Testfall war eine zentrale, sicherheitskritische Komponente in



einem Aktivlenkungssystem. Viele wichtige Eigenschaften konnten mit der formalen Verifikationsumgebung nachgewiesen werden, und so wurde nachhaltig das Vertrauen in die bereits im Einsatz befindliche Software begründet. Nach diesen positiven Testergebnissen konnte die Verifikation auch bei neueren, in der Entwicklung befindlichen Systemversionen erfolgreich einge-

setzt werden. So hat das Projekt die Grundlage für eine kommerzielle Nutzung der Verifikationstechnologie geschaffen.

OpRail – formale Methoden in der Bahn- systementwicklung

Der Bahnbetrieb bedarf präziser Regelungen, um die Gefahren unter Kontrolle zu halten. Da die Bahn historisch das erste der technischen Verkehrsmittel ist, hat sich dort eine eigene Kultur entwickelt. Zentrales Element ist die behördlich organisierte Zulassung der Systeme, sowohl der Infrastruktur (Weichen, Stellwerke, ...) wie auch des rollenden Materials. Eine Zulassung soll die Abwesenheit gravierender Sicherheitsmängel sicherstellen. Die entsprechenden Normen regeln insbesondere, welcherlei Methoden bei der Entwicklung benutzt werden können.

Nun berücksichtigen diese Normen nun in Ansätzen moderne Entwick-



lungsmethoden eingebetteter Systeme. Andererseits sind die Methoden und Werkzeuge der Informatik nicht im Hinblick auf die Erfordernisse der Bahnzulassung entwickelt worden. Dies ist das Spannungsfeld, in dem sich das vom BMBF geförderte OpRail bewegt. Vereinfachend formuliert, geht es folgender Frage nach: Inwieweit lässt sich eine UML-basierte Software-Entwicklung mit den normierten Erfordernissen der Zulassung vereinbaren? Im Fokus der Untersuchung stehen dabei



insbesondere formale Methoden, die mit ihrem Anspruch mathematischer Präzision inhaltlich das Kernproblem der Zulassung zu lösen versprechen.

Der beschriebene Weg führt von der Auswahl einer Teilsprache von UML über die Definition eines Prozesses mit klar beschriebenen Rollen der Werkzeuge und Methoden bis hin zur Anwendung auf ausgewählte Fallstudien. Nach mittlerweile 18 von insgesamt 30 Monaten Laufzeit hat die erste Erprobungsphase im Projekt begonnen. Es zeichnet sich ab, dass der Ansatz des Projektes fruchtbar ist und sowohl direkt nutzbare Ergebnisse erbringen wie auch weitere Forschungsfragen aufzeigen wird.

Kontakt: apl. Prof. Dr. Bernhard Josko

SpeAC-Projektabschluss

Ziel des Projektes „Spezifikation und Algorithmus/Architektur-Codesign für hochkomplexe Anwendungen der Automobil- und Kommunikationstechnik“, kurz SpeAC, war es, die Wirtschaftlichkeit beim Entwurf solcher Systeme zu steigern und dadurch die Möglichkeiten, welche sich aus der rasant voranschreitenden Miniaturisierung in der Mikroelektronik ergeben, nutzbar zu machen. Dafür untersuchte und bewertete OFFIS im Unterauftrag und in enger Zusammenarbeit mit den Vorentwicklungsabteilungen der Robert Bosch GmbH in Reutlingen und Leonberg neue Modellierungs- und Spezifikationsprachen (u.a. C/C++ basierte Systembeschreibungen, SystemC, UML, SDL und Matlab/Simulink). Es wurden neue Methoden und Werkzeuge untersucht, die versprechen die Lücke zwischen dem technologisch Machbaren und dem im Rahmen des Entwurfs Beherrschbaren zu schließen. OFFIS brachte hierbei seine Forschungsexpertise im Bereich der modernen Entwurfsmethoden ein, während Bosch die

zur praxisnahen Evaluation nötigen, industrierelevanten Beispiele und Rahmenbedingungen lieferte. Durch diesen Austausch zwischen industrieller Perspektive und praxisorientierter Forschung konnten besonders erfolgversprechende Ansätze, welche auf SystemC und Matlab/Simulink basieren, identifiziert und für den industriellen Einsatz in einem einheitlichen, durchgängigen und effizienten Entwurfsprozess vorbereitet werden. Resümierend erklärte Dr. Peter van Staa, Abteilungsleiter ‚Methods, Tools, Technologies‘ im Geschäftsbereich ‚Automotive Electronics‘ der Robert Bosch GmbH, gegenüber datawork: „Die Zusammenarbeit mit OFFIS im Projekt SpeAC war für uns ein wichtiger Baustein in unserem ständigen Bestreben unseren Entwurfsprozess noch effizienter und zugleich noch zuverlässiger zu gestalten. Dabei begeisterten uns Kompetenz und Engagement der OFFIS-Mitarbeiter. Wir freuen uns auf die Fortsetzung dieser erfolgreichen Zusammenarbeit im Rahmen weiterer Projekte“.



apl. Prof. Dr. Bernhard Josko

Wir gratulieren Herrn Dr. Bernhard Josko ganz herzlich zur Ernennung zum „Außerplanmäßigen Professor“ an der CVO-Universität Oldenburg. Mit dieser Ernennung wird ein hervorragender Wissenschaftler ausgezeichnet, der an der RWTH Aachen Informatik und Mathematik studierte und dort 1985 auch promovierte.

Seine Forschungsarbeiten zur Habilitation führte er zunächst noch

an der RWTH Aachen durch, wechselte dann aber 1988 auf eine Forschungsstelle im Fachbereich Informatik der Universität Oldenburg. Dort erhielt er 1993 mit einer Arbeit zur Spezifikation und Verifikation reaktiver Systeme die Venia Legendi für das Fach Informatik.

Seit 1994 ist er als leitender Mitarbeiter am OFFIS tätig, wo er maßgeblich am Aufbau des Themenfeldes „Eingebettete Systeme“ beteiligt war. Er leitete diesen FuE-Bereich bis zu seiner wachstumsbedingten Aufteilung in zwei FuE-Bereiche und wurde nach der Aufteilung zum Bereichsleiter für den FuE-Bereich „Sicherheitskritische Systeme“ ernannt.

1. IT Tag Oldenburg/Groningen

Ganz im Zeichen grenzüberschreitender Vernetzung und Kooperation stand der „1. IT Tag Oldenburg/Groningen“, den OFFIS gemeinsam mit den Wirtschaftsförderungen der Städte Oldenburg und Groningen veranstaltete. Über 40 Unternehmer

des „ICT-Clusters Groningen“ (<http://www.ictplatform.com>) reisten am 30.06.05 gemeinsam mit dem Bus nach Oldenburg, um sich über Inhalte und Forschungsprojekte des OFFIS berichten zu lassen.

Zusätzlich informierten drei im „IT-Quartier 101“ ansässige Firmen BTC, Chipvision und RedDot über die Aktivitäten des IT-Clusters in Oldenburg und vervollständigten das Bild der Groninger über die IT-Aktivitäten in Forschung und Wirtschaft in Oldenburg.

Den Nachmittag nutzten die Groninger Unternehmen um den anwesenden Oldenburgern über die Entwicklung der IT-Wirtschaft in

Groningen zu berichten. Die umfangreichen Marketingaktivitäten rund um den IT-Standort Groningen präsentierte der Vorsitzende des ICT-Clusters Jan Hut. Zusätzlich wurde das Projekt „LOFAR“ vorgestellt, welches zur Zeit rund um Groningen angelaufen ist. Dabei handelt es sich um eine neue Generation von Radioteleskop mit einem Radius von 150 km.

Natürlich sollte auch das Networking nicht zu kurz kommen. Nach einer kurzen Visite am „Statstrand“ und dem „Patio“ klang der Abend mit einem gemeinsamen Abendessen auf der Ausstellung „Future TechArt“ im Rahmen des „Jahrhundertschritt 05“ aus.



OB Schütz beim Abendempfang auf der Ausstellung „Future TechArt“

Leitfaden für Patienten-CDs

Im Rahmen der Versorgung von Patienten werden medizinische Bilder zunehmend über Datenträger (so genannte „Patienten-CDs“) zwischen den verschiedenen Versorgungseinrichtungen (z. B. Arzt und Krankenhaus) ausgetauscht. Diese positive Entwicklung schafft in der Praxis jedoch auch Probleme, denn neben nicht eindeutig geregelten Arbeitsabläufen auf Seiten des Datenempfängers (z. B. Import in ein Bildarchiv) werden von manchen Systemen auch fehlerhafte bzw. nicht standardkonforme Datenträger produziert, die beim Empfänger nicht immer zuverlässig gelesen werden können. Aufgrund der Vielzahl der Hersteller und medizinischen Institutionen ist eine zentrale Lösung notwendig, die einen problemlosen Austausch der Patienten-CDs garantiert.

Im Auftrag der Deutschen Röntgen-Gesellschaft (DRG) entwickelt OFFIS hierzu einen „Leitfaden für die Handhabung von Patienten-CDs“, der Arbeitsabläufe auf Seiten des Datenempfängers beschreibt sowie einen detaillierten Katalog mit technischen Anforderungen an „korrekte“ Patienten-CDs auf der Basis des DICOM-Standards umfasst. Zusätzlich wird OFFIS ein Prüfkonzept entwickeln, nach dem Hersteller zukünftig ihre Produkte zur Erzeugung von Patienten-CDs auf Konformität mit dem Anforderungskatalog und auf Interoperabilität mit gängigen Empfängersystemen prüfen lassen können.

Nach Erstellung des Leitfadens ist geplant, dass OFFIS im Auftrag der DRG die Prüfung der Produkte von Herstellern übernimmt. Die positiven Ergebnisse der Prüfungen sowie die ausführlichen Prüfberichte werden auf einer Webseite öffentlich bekannt gemacht.

Kontakt: Dr. Wilfried Thoben

Kooperationspartner BOSCH

Die Bosch-Gruppe ist ein international führender Hersteller von Kraftfahrzeug- und Industrietechnik, Gebrauchsgütern und Gebäudetechnik. Rund 242 000 Mitarbeiter erwirtschafteten im Geschäftsjahr 2004 einen Umsatz von 40 Milliarden Euro. Die Bosch-Gruppe wurde 2004 erstmals weltweit umsatzstärkster Automobilzulieferer. Im Jahr 2004 erzielte der Unternehmensbereich Kraftfahrzeugtechnik 25,3 Milliarden Euro Umsatz.

Im Technischen Zentrum Mikroelektronik in Reutlingen werden anwendungsspezifische integrierte Schaltkreise, Leistungshalbleiter, mikromechanische Sensoren und Steuergeräte in Hybridtechnik entwickelt und gefertigt. Beim Entwurf solcher Systeme spielt die Verfügbarkeit vollständiger, auf die Besonderheiten der Anwendungen optimal zugeschnittener, rechnergestützter Designumgebungen eine Schlüsselrolle für die Innovationsführerschaft bei Automobilsystemen mit der Zielsetzung des so genannten 3-S-Programms von Bosch, Fahr-

zeuge „sicher, sauber, sparsam“ zu machen.

In der Bosch Vorausentwicklung in Reutlingen werden in enger Zusammenarbeit mit dem Produktbereich Fahrerassistenzsysteme in Leonberg die hierfür nötigen Grundlagen geschaffen. Hierzu werden neue Methoden und Werkzeuge aus der Forschung und von kommerziellen Anbietern für den Entwurf solcher Systeme im industriellen Kontext erprobt und zu einem geschlossenen

Design-Flow für den produktiven Einsatz zusammengeführt. In diesem Kontext kooperiert Bosch mit OFFIS unter anderem in den Projekten SpeAC und ICODES mit dem Ziel, die Produktivität seiner Entwickler im Entwurf eingebetteter Hardware-/Software-Systeme zu steigern. Im Rahmen der genannten Projekte wurden und werden in enger Zusammenarbeit von Bosch und OFFIS neue Konzepte zur Spezifikation, zum Entwurf und zur Verifikation komplexer Systeme der Automobilelektronik entwickelt und anhand industrieller Applikationen erprobt. Dabei nimmt die Berücksichtigung zusätzlicher Entwurfsdomänen, etwa des Bereichs Software, sowie der Übergang zu einer abstrakteren Systemsicht einen zentralen Stellenwert ein. Aus der Kooperation zwischen Bosch und OFFIS resultieren innovative Lösungen, deren hohe Ausrichtung auf applikationsspezifische Problemstellungen einen effektiven Transfer in den industriellen Entwurfsablauf von Bosch ermöglicht.

Kontakt: Dr. Jens-E. Appell



Im Hörsaalzentrum der Universität Oldenburg präsentieren am 07.11.2005 acht niedersächsische Forschungsinstitute ihre Arbeitsschwerpunkte und geben fachübergreifende Impulse für neue Ideen. Minister Stratmann wird die Veranstaltung unter dem Motto „neugierig 05“ eröffnen. Weitere Informationen und Anmeldung über das OFFIS Sekretariat.



v. li. n. re.: Dirk Thole, Geschäftsführer EWE TEL und Beiratsmitglied im Centers of Competence, Prof. Dr. Hans-Jürgen Appelrath, Prof. Dr.-Ing. Wolfgang H. Nebel, Dr. Thomas Schüning, 2. Vorsitzender des Vorstands Centers of Competence e. V., Dieter Frikke, Vorsitzender Vorstand Centers of Competence e. V., Karl-Heinz Menke

OFFIS wird Mitglied im CoC

Der Centers of Competence e.V. (CoC) ist ein Bündnis aus Unternehmen im Nord-Westen von Deutschland, die zu definierten Themenfeldern (aktuell sind dies die Themen „Lasertechnologien“, „Beschaffung“ und „Gesundheit“) sehr eng zusammenarbeiten wollen.

Zu zahlreichen betrieblichen praxisorientierten Themen werden interne und externe Expertentreffen durchgeführt. Mit Wissensmärkten und Fachtagungen zur betrieblichen Gesundheit und der Lasertechnik gab es schon zahlreiche Events von beachtlicher Dimension und bedeutender nationaler Anerkennung. Die Unternehmen zu stärken und die Region zu fördern, ist der übergreifende Entwicklungsansatz des CoC.

OFFIS ist kürzlich offizielles Mitglied des CoC geworden und wird sich zu verschiedenen Themen einbringen. „Mit der starken IT-Kompetenz von OFFIS wird dem mehr produktionsorientierten Bündnis eine weitere wichtige innovative Komponente beigefügt“ betonte der Vorstandsvorsitzende des CoC, Dieter Frikke, bei der Unterzeichnung der Aufnahme von OFFIS. Die Mitgliedschaft unterstreicht den satzungsgemäßen Regionalauftrag des Instituts, der bereits seit Gründung sehr erfolgreich ausgeführt wird. Im Rahmen des „3. Wissensmarkt Gesundheit“ des CoC, der am 22.06.2005 in Bad Zwischenahn stattfand, hat OFFIS sich als neues Mitglied des CoC erstmals präsentiert.

Ammerländer Logistikverbund im Pflanzenbau

Das Ammerland ist für seine große Anzahl an Baumschulen weit über die Region hinaus bekannt – Ammerländer Pflanzen werden in die gesamte Bundesrepublik sowie ins benachbarte Ausland geliefert. Die Baumschulen sind kleine und mittelständische Unternehmen, die ihre Distributionslogistik selbst organisieren. Im Projekt AMMLOG, das durch die Stiftung Industrie-

forschung gefördert wird, baut OFFIS mit den beteiligten Ammerländer Baumschulen und regionalen Speditionen einen Logistikverbund auf, der neben der effizienten Abwicklung des eigentlichen Tagesgeschäftes eine hoch flexible, innovative und dynamische Logistik sicherstellt. Dies kann nur gelingen, wenn die Logistik in ganzheitlich und strategisch geplanten Prozes-

OFFIS wird ein Leistungszentrum für Forschungsinformation

Die Deutsche Forschungsgemeinschaft (DFG) richtet bei OFFIS ein Leistungszentrum für Forschungsinformation ein. Das Zentrum, das den Titel „Probado“ trägt, beschäftigt sich mit so genannten nicht-textuellen Dokumenten, die sich nicht mehr durch Texte beschreiben lassen, wie etwa Bilder, Animationen, Filme und dergleichen. Im Mittelpunkt steht dabei die Frage, wie wissenschaftliche Bibliotheken zukünftig mit solchen Dokumenten umgehen sollen.

OFFIS hat das Konzept für Probado gemeinsam mit den Universitäten Braunschweig und Bonn, der Technischen Informationsbibliothek Hannover und der Bayerischen Staatsbibliothek entwickelt. Innerhalb der nächsten fünf Jahre entstehen nun Werkzeuge und Systeme sowie Verfahren und Abläufe, die es wissenschaftlichen Bibliotheken erlauben, mit nicht-textuellen Dokumenten genau so selbstverständlich umzugehen wie heute mit Büchern und Zeitschriften. In der ersten Phase werden Musik, 3D-Computergrafiken und multimediale Lern-

materialien berücksichtigt, später sollen noch weitere Dokumententypen hinzukommen. OFFIS übernimmt die Koordination des Leistungszentrums und trägt die fachliche Verantwortung für den Bereich multimedialer Lernmaterialien.



Die DFG fördert mit der Einrichtung von Leistungszentren beispielgebende, neuartige Konzepte des wissenschaftlichen Informationsmanagements. Derzeit werden bundesweit 12 Leistungszentren gefördert. Mit „Probado“ konnte nun schon das zweite DFG-Leistungszentrum nach Oldenburg geholt werden. Bereits seit einem Jahr besteht in der Universität Oldenburg ein Zentrum zur Einführung eines integrierten Informationsmanagements.

Kontakt: Jochen Meyer

Impressum

datawork

Herausgeber

Kuratorium OFFIS e. V.,
Escherweg 2, 26121 Oldenburg
Tel. 0441 9722-0
Fax 0441 9722-102
E-Mail institut@offis.de
URL www.offis.de

Verantwortlich

Karl-Heinz Menke

Gestaltung

TEPE Marketingagentur,
Westerstede

datawork erscheint jährlich mit drei Ausgaben und wird kostenlos abgegeben.

Das Institut OFFIS wird vom Land Niedersachsen institutionell gefördert.



Stiftung
Industrieforschung