Dokumentation des 5ten GI/ASQF/IRC Schloß-Steinhöfel-Seminars zum Thema „Zukunft gestalten“, 10. April 2008

editiert von Jan deMeer, smartspacelab.eu GmbH, GI-Regionalgruppe Berlin

Das „Schloß-Steinhöfel-Seminar“ wird gemeinsam gestaltet von der Gesellschaft für Informatik (GI) – Regionalgruppen Berlin u. Brandenburg, dem Arbeitskreis für Software-Qualität u. Fortbildung e.V. (ASQF) Potsdam, der ZAB - enterprise europe network Berlin-Brandenburg und der Industrie u. Handelskammer (IHK) Frankfurt(Oder).

Es bietet in Ergänzung zu den GI/ASQF-Fachgruppen ein Expertenforum an, an welchem die fachliche Expertise aus der Region Berlin und Brandenburg, gepaart mit dem Know-how und der Erfahrung der unterstützenden Fachvereinigungen und -gruppen, sich zu neuen Synergien zusammenfindet.

Das „Schloß-Seminar“ findet in idyllischer Umgebung mitten im Land Brandenburg, in der Nähe von Fürstenwalde, aber gut erreichbar von Berlin aus, statt. (Anfahrt: http://www.schloss-steinhoefel.de/start.htm)

In der von Lenne gestalteten Umgebung gedeihen kreative Gespräche, die den Technologietransfer inspirieren und Synergien für die Region freisetzen sollen.

Ihr Ansprechpartner:

Frau Kerstin Seidel,

Tel +49 331 231810 -19(tel), -10(fax)

mailto:kerstin.seidel@asqf.org

fachliche Leitung:

Stephan Goericke (ASQF e.V. Potsdam),

Prof. Uwe Meinberg (GI RG Brandenburg),

Alexandra Pohl (IRC Potsdam),

Frank Kutschke IHK Frankfurt(Oder)

Jan deMeer, Jeronimo Dzaack (GI RG Berlin).

Inhaltsverzeichnis:

1. *Das Tagesprogramm*

9:00 Registration und erster Kaffee

9:30 Begrüßung der Teilnehmer und Eröffnung des Seminars:

Stephan Goericke, iSQI GmbH

Vorstellung des Seminarprogramms:

Jan deMeer (Moderator), GI/ASQF Sprecher, smartspacelab.eu GmbH

9:45 – 11:15 BIT-Workshop: Business Intelligence Technologien:

Thema: Lateral zur Implementierung und Produktion komplexer Anwendungen und einhergehend mit der Leistungssteigerung formaler Engineering –Methodik müssen in den Technologieunternehmen ebenso innovative BI-Techniken zur Steuerung des Herstellungsprozesses (V-Modell) vorangebracht werden. Die geforderte Nachweisbarkeit von Eigenschaften muß geeignet dokumentiert und verwaltet werden. Industrielle Auftraggeber haben i.d.R. eigenen Vorstellungen über die Nachweisbarkeit von Sicherheitsanforderungen.

1. wibas IT Maturity Services Darmstadt: Der Weg zur professionellen IT

Autor: Dipl.-Wirtsch.-Inf. Mareike Solbach

Profil: Mareike Solbach ist Senior Executive Consultant der wibas IT Maturity Services GmbH. Sie ist eine erfahrene Software Projektleiterin, leitet seit vielen Jahren CMMI Assessments und unterstützt Verbesserungsprojekte vieler internationaler Unternehmen. Sie denkt sich sehr gut und schnell in die Praxisprobleme Anderer hinein und steckt diese mit ihrer Begeisterung für Verbesserungen an. Sie ist Mitautorin des Anfang Oktober 2007 im Springer Verlag erschienenen Buches "Der Weg zur professionellen IT", in dem Erfahrungen im praktischen Veränderungsmanagement zur Umsetzung von CMMI/ITIL zusammengetragen sind.

2. ASQF e.V./iSQI GmbH: Personalzertifizierung als Königsweg zu hoher Softwarequalität

Autoren: Jana Noack, Silvia Huhse

Referentenprofil: Silvia Huhse ist seit Anfang 2006 beim ASQF e.V. und der iSQI GmbH beschäftigt. Seit Anfang 2007 leitet Sie beim iSQI die Bereiche Internationale Zertifizierungen und ist beim ASQF zuständig für die Mitglieder-Kommunikation.

3. DomData Sp. z o.o., Poznan: IT-Systeme für den Mittelstand – Modellierung von Geschäftsprozessen

Autoren: Dipl.-Phys. Dieter Krawczynski

Referentenprofil: Dieter Krawczynski ist Physiker und arbeitet als Berater mit den Schwerpunkten Organisation, IT und Qualitätsmanagement. Er ist Kooperationspartner des polnischen IT-Systemhauses DomData aus Posen, das europaweit agiert. In seinem Vortrag stellt er das Unternehmen DomData vor und informiert über Produkte, Dienstleistungen, Projektbeteiligungen und Kooperationsmöglichkeiten.

11:15 – 11:30 Kaffeepause

11:30 – 13:00 MCA-Workshop: Sicherheitstechnologien für Mission-Critical Application:

Thema: Mit MCA sind komplexe Anwendungen, u.a. Verkehrssysteme in der Luft, auf der Schiene und auf der Straße, aber auch Logistiksysteme etc. gemeint. Die Sicherheit dieser anwendungsbezogenen Systeme ist einerseits von den verfügbaren IT-Technologien abhängig, aber in viel größerem Maße von dem Zusammenwirken der eingebauten Komponenten in einem System von Systemen, z.B. Airbus, ICE, TGV, Fahrzeugen, Kontroll- und Leitsysteme etc. [s.a. SECTEC Sicherheit(-stechnologien) f. Bürger, Unternehmen u. Staat]

1. Otto-von-Guericke-Universität Magdeburg, Institut für Technische und Betriebliche Informationssysteme, Arbeitsgruppe Multimedia and Security: COMO B3 – IT Security Automotive

Autoren: Dipl.-Inf. Tobias Hoppe, Prof. Jana Dittmann

Profil: Tobias Hoppe, Arbeitsgruppe Multimedia and Security der Otto von Guericke Universität Magdeburg, forscht schwerpunktmäßig an Themen der IT-Sicherheit. Neben Evaluierungen zu modernen IT-Angriffen auf Desktop-PC-Systeme und geeigneten Gegenmaßnahmen untersucht er seit 2007 auch Aspekte der IT-Sicherheit für automotive Systeme im Teilbereich B3 (IT-Security Automotive) des Projekts COMO (COmpetence in MObility) der Universität Magdeburg.

2. Ifak – Institut f. Automation u. Kommunikation e.V. Magdeburg: Testfallgenerierung aus modellbasierten Systemspezifikationen

Autoren: Dipl.-Ing. Jan Krause, Dipl.-Ing. Franziska Wolf, Dipl.-Ing. Andreas Herrmann

Referentenprofil: Jan Krause ist Diplom-Wirtschaftsingenieur für Automatisierungstechnik und Controlling und arbeitet als wissenschaftlicher Mitarbeiter im Bereich Verkehrstelematik am ifak. Der Schwerpunkt seiner Arbeiten sind die Entwicklung und Anwendung von Methoden und Werkzeugen zur Spezifizierung und Evaluierung von IT-Systemen insbesondere aus dem Bereich des Verkehrsmanagements.

3. Dpm Identsysteme GmbH Cottbus: System- und Planungsgrundlagen für Auto-Id-Systeme

Autoren: Dipl.-Ing. Andreas Wenzel

Referentenprofil: Andreas Wenzel ist geschäftsführender Gesellschafter der dpm Identsysteme GmbH und Inhaber der CDSIdent e.K. Er ist in der Auto-Id-Branche seit 1990 in der Hardware-Entwicklung von RFId-Geräten beschäftigt.

4. Ifak e.V. Anforderungen der Informationssicherheit in den Bereichen der industriellen Automation u. Verkehrstelematik

Autoren: Dipl.-Ing. Franziska Wolf, Dipl.-Ing. Heiko Adamczyk
Referentenprofil: Franziska Wolf ist Wissenschaftliche Mitarbeiterin im Institut für Automation und Kommunikation ifak e.V. im Bereich Verkehrstelematik mit dem Schwerpunkt Fahrzeug- und Infrastruktursysteme.

13:00 – 14:00 Mittagspause

14:00 – 15:30 EKS-Workshop: Software Qualität - Engineering -Methodik für komplexe Systeme:

Thema: Zur Qualitätsbeurteilung komplexer Systeme werden Methoden und Werkzeuge für ein sog. *Predictable System Engineering(PSE)* benötigt, andernfalls sind die hohen Sicherheits- bzw. Qualtiätsstandards aus den Anwendungsbereichen nicht erfüllbar. Das Engineering komplexer Systeme muß daher berechenbare (nachweisbare) Eigenschaften erzeugen. Dies kann weitgehend nur mit Hilfe einer Formalierung der Methoden und Techniken für *Requirement Capturing, Model Checking/Translation, Test Case Derivation, Safety Assessment*, Generierung von Metriken und Zertifizierungen, geschehen.

1. PhiloTech GmbH Cottbus: Validation komplexer Systeme auf Grundlage des Software-Entwicklungsstandards RTCA DO-178B

Autoren: Dipl.-Ing. Katja Winder

Referentenprofil: Katja Winder ist Diplom-Informatikerin und arbeitet als Beraterin im Bereich Qualitätssicherung. Der Schwerpunkt ihres Vortrags wird die Validation und Verifikation von Software nach dem im zivilen Luftfahrtbereich eingesetzten Software-Entwicklungsstandards RTCA-DO-178B sein.

2. smartspacelab.eu GmbH: Security & Safety Verification & Validation in der Standardisierung

Autoren: Jan deMeer, smartspacelab.eu GmbH, Hans v. Sommerfeld, Rhode& Schwarz GmbH

Referentenprofil: Jan deMeer ist Angehöriger des Normenausschusses DIN NIA27 „IT Security“. Er beschäftigt sich dort mit Methoden der Kryptographie und Sicherheitsarchitekturen. Im Jahre 2007 hat er sich mit anderen Wissenschaftlern, an der Gründung eines deutsch-kanadischen Unternehmens, aus der Brandenburgisch Technischen Universität (BTU) heraus, beteiligt. Das Unternehmen transformiert wissenschaftliche Methoden, Techniken und Architekturkonzepte zur sicheren und zuverlässigen Kommunikation in komplexen Systemen.

3. Fraunhofer-Gesellschaft, Institut FOKUS: Modellgestütztes Testen komplexer Systeme,

Autoren: Prof. Ina Schieferdecker, Dipl.-Ing. Axel Rennoch, Dipl.-Ing. Andreas Hoffmann

Referentenprofil:

Andreas Hoffmann ist Angehöriger des FhG-Kompetenzzentrums „Modelling and Testing for System and Service Solutions“ (MOTION) und Mitglied in Europäischen Standardisierungs-organisationen ETSI TISPAN, OMG und ITU. Dort ist er u.a. in die Standardisierungsvorhaben IMS, ITU-ODL, eODL, SDL involviert. In der OMG-Gruppe leitet er Vorhaben zur Standardisierung von Deployment und Konfigurations Management von komponenten-basierten Verteilen Systeme.

15:30 – 15:45 Kaffeepause

15:45 – 17:15 Middleware-Workshop:

1. TFH FB Informatik Berlin: Informationsintegration in heterogen verteilten Datenbanken

Autoren: Prof. Petra Sauer, Dipl.-Ing.(FH) Marc-Florian Wendland

Referentenprofil: Prof. Petra Sauer ist Professorin für Informatik, auf dem Gebiet Datenbanken, an der Technischen Fachhochschule Berlin. Ihr Forschungsfokus liegt vor allem auf dem Datenbankentwurf, sowie den X-Technologien.

2. T-Systems Berlin: MAMS – Service-Generierung für Nichtexperten:

Autoren: Dipl.-Ing. Horst Stein, Dipl.-Ing. Bettina Lehmann

Referentenprofil: Bettina Lehmann und Horst Stein arbeiten im Auftrag der Deutschen Telekom Laboratories an der Bereitstellung netzwerkzentrierter Services. Das Zusammenspiel zwischen Telko-Services und Web2.0 Ansätzen soll künftig nicht nur für Entwickler, sondern auch für IT-Anwender aus dem geschäftlichen Umfeld möglich sein. Einsatzmöglichkeiten und Ansätze zur Service Erstellung und zum Betriebs aus dem Forschungsprojekt MAMS werden dargestellt.

Ab 18:00 Apres-Workshop „Spätschoppen“:

Abendessen mit ernsten und nicht-so-ernsten Kamingesprächen.

(Bitte beachten Sie, daß nach 18:00 Uhr alle Ausgaben auf eigene Rechnung gehen.)

Aus organisatorischen Gründen wird um Anmeldung zum Apres-WS gebeten!

Vielen Dank für Ihr Verständnis!

2. *Zusammenfassung Seminarergebnisse:*

Unter dem Motto „Zukunft gestalten“ hat das „Schloß-Steinhöfel-Seminar“ zum 5. mal am 10. April 2008 in jenem Brandenburger Schloß, das dem Seminar seinen Namen geliehen hat, stattgefunden. Das Schloß-Seminar ist ein gemeinsames Produkt der Gesellschaft für Informatik (GI) – Regionalgruppen Berlin u. Brandenburg, des Arbeitskreises für Software-Qualität u. Fortbildung e.V. (ASQF) Potsdam, der ZAB - *enterprise europe network* Berlin-Brandenburg und der Industrie u. Handelskammer (IHK) Frankfurt(Oder).

Das Konzept des Schloß-Seminars ist es, den technologischen Akteuren, vorzugsweise in der Region Berlin-Brandenburg, aber nicht darauf beschränkt, wie auch jene Teilnehmer aus der angrenzenden polnischen Region und aus den anderen Landesteilen der Republik zeigen, ein Forum zu geben, auf welchem sie Ideen und Konzepte austauschen, aber auch neue Projektideen finden können.

Desweiteren kann und soll der Kontakt zwischen Unternehmen, Forschungseinrichtungen, Universitäten, Standardisierungsgremien, forschungspolitischen Foren und Fach- und Fördereinrichtungen des Bundes und der Region hergestellt werden.

Im Ergebnis möchte das Schloßseminar eine Stimme haben, die die regionalen, wirtschaftlichen und technologischen Entwicklungsbedürfnisse bündelt und artikuliert.

So wurde in den Workshops des diesjährigen Schloßseminars 2008 der qualitative Zusammenhang zwischen dem Bedürfnis nach permanenter Veränderungen der betrieblichen Organisationsstrukturen, dem persönlichen Qualitäts-Management und von Sicherheits- und Zuverlässigkeitsaspekten bei der (Software) Produktentwicklung für komplexe, industrielle System diskutiert.

Beispiele für komplexe industrielle Systeme sind Kommunikationssysteme im Airbus, die Leit- und Steuertechnik bei der Bahn, im automotiven Bereich *car-to-car-* zwischen fahrenden Autos und Bus- Kommunikationssysteme innerhalb eines Autos.

Solcherart komplexer Systeme sind, im Hinblick auf Zuverlässigkeit und Sicherheit, schwierig einzuschätzende Systeme. Noch schwieriger ist es, Testmittel und Verfahren auszuwählen, womit, gemessen an den hohen Sicherheitsstandards der Industrie, aussagekräftige Tests von den zuliefernden Unternehmen durchgeführt werden können. An dieser Stelle sieht das Schloßseminar enormen Forschungsbedarf, der, zusammen mit der Industrie und KMUs, erörtert und vertieft werden und an die lokalen Forschungseinrichtungen addressiert werden muß.

Die Gemeinschaft des Schloßseminars 2008 hat diese Fragestellung aus unterschiedlichen Blickrichtungen in 4 Workshops diskutiert:

1. Veränderungsmanagement der sog. business intelligence im BIT Worshop;

2. Abhängigkeit von Sicherheit und Zuverlässigkeit in industriellen Systemen der Automation und Verkehrstelematik im MCA Workshop;

3. Verifikations- und Validationsfähigkeiten formaler Test- und Engineeringmethoden für industrielle Systeme im EKS Workshop;

4. technischen Möglichkeiten der Informationsintegration und Dienstegenerieurung auf geeigneten Plattformen im middleware Workshop.

3. Ergebnisse BIT-Workshop „Business Intelligence Technologies“

3.1. *Mareike Solbach, wibas IT Maturity Services Darmstadt: „Der Weg zur professionellen IT“*

Aus dem SW Business-Institut der CMU stammt das Zitat „ … And Then a Miracle Happens“, wenn in einem Unternehmen das Projekt-team erklärt, daß alles über die Inbetriebnahme eines neuen Systems im Großen Handbuch geschrieben steht; wobei die Inbetriebnahme aus der Ankündigung des Handbuchs besteht.

Der eigentliche Vorgang der Inbetriebnahme wird dabei völlig ignoriert, woraus sich wiederum Widerstand von jenen ergibt, die das inbetriebgenommene System verwenden sollen.

Unter diesen Voraussetzungen ist ein Straucheln des Unternehmens vorprogrammiert. Entweder gibt das Unternehmen auf, oder versucht eine andere Lösung zu finden.

Veränderungen erfordern konkrete Maßnahmen in der gesamten Organisation, nicht nur eine Erstellung und Verkündung. So wie auf dem Bild dargestellt geht es sicherlich nicht, denn Verbesserung bedeutet Veränderung und erfordert eine Entwicklung der Organisation.

Veränderungen sollen mit dem Ziel eingeführt werden, die Unternehmensleistung zu erhöhen, bedingen aber damit eine Entwicklung der Unternehmensorganisation.

Bei der Organisationsentwicklung werden neue Arbeitsweisen etabliert, was wiederum die Unternehmenskultur wesentlich beeinflußt.

Verbesserungen in einem Unternehmen durchzuführen ist ein Projekt, dessen Ergebnisse in eine kontinuierliche Verbesserung münden müssen. Während revolutionäre Verbesserungen ein altes Leistungsniveau durch ein neues ersetzen, bleiben bei einem kontinuierlichen Verbesserungskonzept das alte Leistungsniveau vorläufig bestehen, bzw, wird gehalten und wird nur langsam verbessert.

Notwendigkeit und Dringlichkeit der Prozeßverbesserung müssen vermittelt werden, damit die Organisation bereit ist mitzuwirken. Zu diesem Zweck sollte ein sog. „Verbesserungsprojekt“ aus den Mitarbeitern der betroffenen Organisationseinheit gebildet werden. Diese ausgewählte Gruppe verschafft sich zuerst Lösungen für ihre eigenen Projekte, bzw. Bereiche, ohne diese zu verlassen. Wenn sich diese Lösungen bewährt haben, dann werden sie zu Pilotprojekten weitergetragen und schließlich zu allen Projekten der Organisation oder des Unternehmens.

Dieses Vorgehen ist erfolgreich, weil Veränderungen schrittweise von typischen Gruppen adoptiert werden, die jeweils auf die Vorgängergruppe als Fürsprecher hört.

Es sorge getragen werden, damit jedes Projekt mit seinem Projektleiter konkrete Maßnahmen zur Verbesserung plant und auch durchführt, z.B. im monatlichen Rhythmus. Die Qualitätsprüfung prüft die Umsetzung in jedem Folgemonat.

Mit qualifizierten Projektleitern wird das ein Erfolg, solange Ressourcen zur Verbesserung den Projekten zur Verfügung gestellt wird. Die Ressourcen werden zur Überwindung von Umsetzungsschwellen benötigt. Mit Ressourcen ist folgendes gemeint:

- Zeit, um neue Arbeitsweisen zu erlernen, bzw. umzusetzen;
- Coaching, um Multiplikationswirkungen zu erreichen;
- Zielabsprachen mit den Mitarbeitern, um die Veränderungen zu verankern;
- Werkzeuge, die zur Unterstützung der Arbeitsabläufe benötigt werden.

Umfangreiche Prozeßbeschreibungen sind zu verweiden, schon deswegen weil sie niemand lesen wird. Weniger ist also mehr!

Eine Verbesserung und Veränderung umfaßt folgende einmalige Maßnahmen zur Umsetzung und Regeltätigkeiten zur Aufrechterhaltung:

- Um eine dauerhafte Wartung zu etablieren, müssen geeignete Arbeitsweisen und Werkzeuge entwickelt werden;
- Um eine nachhaltige Ausbildung zu gewährleisten, müssen Ausbidlungskonzepte geschaffen und durchgeführt werden;
- Organisationsstrukturen sind kritisch zu betrachten und ggf. zu verändern;
- Kommunikations-strukturen und –verhalten müssen analysiert werden;
- Der Nutzen all dieser Maßnahmen muß dauerhaft meßbar sein.

Im Verbesserungsprozeß muß auf Genauigkeit bei der Erhebung der Anforderungen geachtet werden. Allein die Einführung neuer Verbesserungsmodelle, wie z.B. „Capability Maturity Model Integration (CMMI) ist kein vernünftiges Ziel.

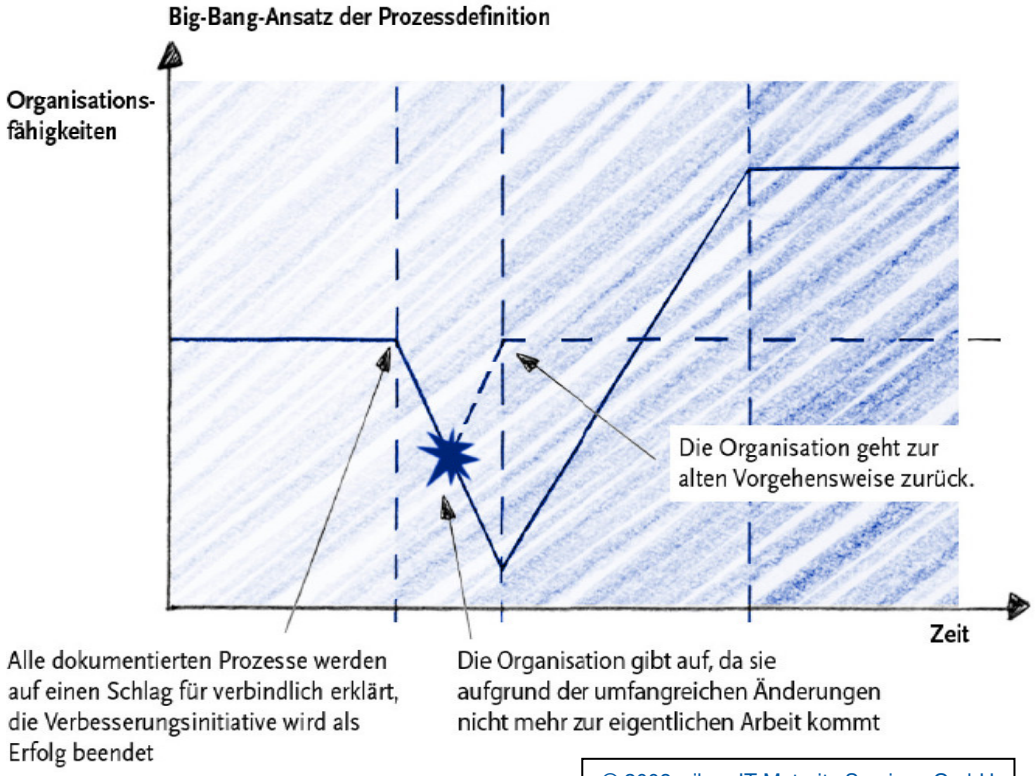
Bei der Erhebung der Anforderungen sind die folgenden Gesichtspunkte zu berücksichtigen:

- Benutzerfreundlichkeit der Prozeßbeschreibungen
- Geschäfts- und Verbesserungsziele

- Rahmenbedingungen bei der Verbesserung

- Referenzmodelle für die Verbesserung

Ein häufiger Fehler im Verbesserungsprozeß sind Maßnahmen, die viel zu große Veränderungen auf einen Schlag für verbindlich erklären. Damit kann die Verbesserungsinitiative nicht erfolgreich fortgesetzt werden. Die Gruppen der Organisation geben auf, da sie aufgrund umfangreicher Veränderungsmaßnahmen nicht mehr zur eigentlichen Arbeit kommen:



Aus diesen Gründen muß die Veränderung in kleine Schritte umgesetzt werden, damit die Projekte eine Chance haben, die Verbesserungen zu begreifen und umzusetzen. Es müssen kleine, abgegrenzte Päckchen, die der Organisation echten Nutzen bringen, gebildet werden. Eine Priorisierung der Päckchen ist äußerst hilfreich. Zum Schnüren eines Päckchens gehören zuerst die Geschäftsziele, aber auch die Angaben von Stärken und Schwächen, eine Risikoliste und Anreize zur Erhöhung der Veränderungsbereitschaft.

Eine monatiliche Taktung der Verbesserung sichert die konsequente Umsetzung, fokussiert das Verbesserungsvorhaben und ermöglicht die Einarbeitung von *feedback*.

Der Verbesserungsprozeß kann folgendermaßen beschrieben werden:

1. Geschäfts- und Verbesserungsziele nennen
2. initiale Standortbestimmung durchführen, indem ein Verbesserungs- backlog eingerichtet und die Paketprioritäten festgelegt werden;
3. daraus ergeben sich die in einem Monat umsetzbaren Verbesserungen, die in täglichen und monatlichen Meetings begleitend, erreicht werden sollen;

4. die sich aus den Meetings ergebenden Änderungswünsche und ggf. beobachtete Fehler werden zurückgeführt in eine erneute Standortbestimmung. Der Verbesserungsprozeß ist zyklisch und fährt mit Schritt 2 fort.

5. Die erfolgreiche Abbruchbedingung des Verbesserungsprozesses tritt ein, sobald die Organisationsgruppen die Verbesserungen loben, bzw. für geeignet deklarieren.

In einem erfolgreichen Verbesserungsprozeß muß das Management, die Organisation, das Audit- und das Verbesserungs-Team eng zusammenarbeiten, indem sie gemeinsam Lösungen erarbeiten, sich gegenseitig „coachen“, den Verbesserungsprozeß verfolgen und steuern. Die drei Hierarchien des Verbesserungsprozesses: Management – Organisation – Audit-team haben im Prozeß die entsprechenden Aufgaben: Führung (fordern, begutachten, unterstützen) – Lebendigkeit (verbessern, verändern) – Kontrolle (Umsetzung beobachten) anzunehmen und konstruktiv auszuführen.

Die Mitgestaltung und Verantwortung des Management ist der größte Einflußfaktor bzgl. der Ressourcen Zeit und Kosten und stellt somit ein k.o.-Kriterium für die Verbesserung dar.

Das Audit- team hilft, daß die Organisation vorankommt und zeigt an, wie schnell, oder langsam. Es bewertet die Prozesse, z.B. rot: nicht erfüllt, gelb: teilweise erfüllt, grün: voll erfüllt, weiß: nicht betroffen und wichtet die Abweichungen. Dem Gewicht der Abweichung (y-Achse) wird die Dauer der Abweichung (x-Achse) gegenübergestellt.

Der Seniormanager muß die Veränderung führen, indem er geeignete Grundsätze etabliert, die Prozesse mit den Projekten „durchspricht“ und mit dem mittleren Management Stausbesprechungen durchführt.

Das mittlere Management ist für die Umsetzung der Verbesserung in seinem Bereich verantwortlich und gestaltet die geplanten Verbesserungen aktiv mit.

Die Führung, Betrieb und die Projekte einer Organisation sind über die Rechte und Pflichten, den Statusbeschreibungen, Kennzahlen, Ressourcen, Zielvorgaben und Aus- und Weiterbildungsmaßnahmen im Verbesserungsprozeß eng miteinander verquickt.

Die Führung muß die Arbeitsanweisen nachhaltig und selbstverständlich machen, indem Kontakt zu den betroffenen Personen aufgenommen wrid; ein neues Bewußtsein für die Notwendigkeit der Veränderung geschaffen wird; die Veränderungen verstanden und positiv wahrgenommen; die Veränderungen installiert und ggf. angepaßt werden können; die Veränderungen institutionalisiert werden. Nur so wird fehlendes Bewußtsein, Verwirrung, negative Wahrnehmung, Unverständnis für Veränderungen, Abbruch der Umsetzungsmaßnahmen vermieden.

Die Vorgehensweisen des Unternehmens sind innerhalb des Senior-Management-Verbesserungszyklus zu verankern. Der Senior-Manager gibt die Richtlinien und Grundsätze aus und spricht gleichzeitig mit dem Verbesserungsteam und den betroffenen Projekten und dem Unternehmensbetrieb die Grundsätze durch.

Das Verbesserungsteam übernimmt die Richtlinien und Grundsätze vom Management und transferiert sie in Prozeßbeschreibungen und geeignetem Unterstützungsmaterial. Das Team erhält von der Umsetzung der Prozeßbeschreibungen in den Projekten und Betrieb technisches *feedback*, das es wiederum in strategischen *feedback* umsetzen und mit dem Management durchsprechen muß. Das Audit-team beobachtet alle 3 Handlungsebenen.

Das CMMI- Verbesserungs- Referenzmodell ist eine systematische Aufbereitung des Selbstverständlichen und dient der Verpflichtung, Orientierung und objektiven Überprüfung. Indem man sich auf ein Referenzmodell stützt, kann man beim Start, Fortschritt und Zielerreichung eine objektive Überprüfung erreichen; bewährte Praktiken nutzen; ausufernde Diskussionen über Selbstverständliches einschränken; beteiligte Personen und Organisationen verpflichten; etc. Natürlich darf das Refernzmodell nicht zum Ziel werden, es ist nur ein Werkzeug!

Mit dem CMMI-Werkzeug wird spezifiziert WAS getan werden muß. Das WIE findet seinen Niederschlag in der Prozeßbeschreibung (SE/PM books) und in der Arbeit im Projekt.

Die CMMI-Prozesse sind in 4 Themenblöcke aufgeteilt: Projektmanagement, Entwicklung, Unterstützung und Verbesserung.

wibas IT Maturity Services is official SEI Partner of the Software Engineering Institute of the Carnegie Mellon University

for SCAMPI appraisals and CMMI training. For inquiries, call:

wibas IT Maturity Services GmbH

Yvonne Fischer

Customer Relations Manager

Otto-Hesse-Str. 19 B

64293 Darmstadt

Germany

Tel: 0049 – 6151 – 50 33 49 – 21

Fax: 0049 – 6151 – 50 33 49 – 33

yfischer@wibas.de

Malte Foegen

Dipl. Wirtsch.-Inform.

Partner

e-mail: mfoegen@wibas.de

Claudia Raak

Dipl. Wirtsch.-Ing.

Partner

e-mail: claudia.raak@wibas.de

Mareike Solbach

Dipl. Wirtsch.-Inform.

Senior Executive Consultant

e-mail: mareike.solbach@wibas.de

3.2. *Silvia Huhse, ASQF e.V./iSQI GmbH: Personalzertifizierung als Königsweg zu hoher Softwarequalität*

Software ist allgegenwärtig!

Softwaresysteme sind ein essentieller Bestandteil unseres täglichen Lebens, wie z.B. Bargeld am Automaten abheben, mit dem Mobiltelefon anrufen, im Internet „shoppen“, die Fensterscheibe herunterlassen etc.

- Ein durchschnittliches Mobiltelefon enthält 2 Millionen Zeilen Software-Code; 2010 wird es 10 mal so viele haben!
- General Motors Corp. rechnet damit, dass ihre Fahrzeuge in 10 Jahren 100 Millionen Code-Zeilen haben werden!

Genauso allgegenwärtig sind Softwarefehler:

- NASA Mars Climate Orbiter, Incident Date: 9/23rd/1999, Price Tag: $125 million:

Ursache des Navigationsfehlers: Während die NASA Impulse in der international gebräuchlichen Einheut Newton x Sekunde berechnete, wurde die Navigationssoftware des MCO vom Hersteller in Pfund x Sekunde ausgelegt, also um den Faktor 4,45 größer. Als weitere Ursachen des Verlusts wurden mangelnde Erfahrung, Überlastung und schlechte Zusammenarbeit der Bodenmannschaften angeführt. Eingespielte Teams hätten den Einheitenfehler auch während des Flugs entdecken können und so den Verlust verhindert.

- General Motors, Michigan, Incident Date: 1985, Price Tag: n.n.

Alle schwarzen Autos verließen die Montagehalle ohne Windschutzscheibe; die für das Einsetzen vorhandenen Roboter erkannten die Farbe Schwarz nicht!

IT-Experten sind sich einig, daß solche Fehler zu oft passieren, unabhängig von Land oder Unternehmensgröße; genauso wie in kommerziellen oder non-profit-Organisationen, in Verwaltungen; ohne Rücksicht auf Status und Reputation.

Die Kosten für Unternehmen und Gesellschaft - in Anbetracht von Aktienanteilen, Steuermitteln, Subventions- und Investment-Zahlungen - gehen in die Milliarden. Mit verstärkter Anonymisierung durch die Anwendung von IT werden die Probleme eher größer als kleiner.

Häufige Fehlerquellen für gescheiterte Projekte sind:

- Unrealistische Zielsetzung bei Software-Projekten
- Falsche Annahmen über benötigte Ressourcen
- Unzureichend definierte Systemanforderungen
- Ungenügende Dokumentation des Projektstatus
- Keinerlei Risiko-Abwägung
- Mangelnde Kommunikation zwischen Kunden, Entwicklern, Nutzern
- Benutzen von nicht ausgereifter Technologie
- Unvermögen das Projekt in seiner Komplexität zu erfassen & zu managen
- Interessengruppen-geleitete Priorisierung
- Kommerzielle Zwänge.

Mit folgender Diagnose:

- Fehler in Software-Entwicklungs-Projekten sind meist menschlich!

Und möglicher Therapie:

- Das „Pullover-Stricken-Prinzip“ – je eher die Fehlerbehebung / Fehlervermeidung ansetzt, desto geringer der Arbeitsaufwand.

Mit der Konsequenz, die „strickende Person“, d.h. den Software-Entwickler zu schulen, um die erforderliche Qualität von Anfang an gewährleisten zu können. Im Schulungsumfang müssen Projektmanagement, Risikomanagement, Qualitätsmanagement enthalten sein.

Aus dieser Beobachtung ergeben sich folgende gute Gründe für eine standardisierte, lebenslange, begleitende Weiterbildung:

- Professionalisierung
- Sicherung eines Basiswissens
- Anerkannte und bewährte Ausbildung für Berufsbilder der Praxis
- Nationale und internationale Vergleichbarkeit von Berufsqualifikationen
- Hersteller- und produktunabhängige Standardisierung
- Globale Zusammenarbeit und Kommunikation über Landesgrenzen und Sprachbarrieren hinweg.

Ohne Standardisierung geht es nicht, sie wird gebraucht, weil

- Es multinationale Beteiligungen an IT-Projekten gibt,
- variierende, landesspezifische Erstausbildung unvermeidlich ist,
- es überall Wildwuchs an Zertifikaten gibt.
- meist fokus auf Wissensabfrage gelegt wird,
- Praxis-bezogene Kompetenzen fehlen.

Aktivität in der Standardisierung und weltweite Koordinierung garantieren und sichern

- Gleichbleibende Qualität
- Verläßliche Orientierung
- Hohe Transparenz
- Akzeptanz und Gültigkeit
- Internationale Wettbewerbsfähigkeit

Das Fazit heißt: Umdenken und lebenslanges Lernen, d.h. Personalzertifizierung ist der Königsweg zu hoher Softwarequalität, wenn:

- lebenslanges Lernen als Verknüpfung von neu erlerntem theoretischen Wissen und praktischer Erfahrung in den Köpfen der Menschen als MUSS verankert ist;
- der Fachkräftemangel durch Weiterqualifizierung statt nur durch Neu-Anlernen oder -Anwerben junger Kräfte angegangen wird;
- lebenslanges Lernen nach Qualitätsaspekten in der beruflichen Weiterbildung systematisiert und standardisiert wird;

- Internationale Konsensbildung erfolgt.

Und zum Schluß noch ein Zitat von Klaus Kobjol, Gewinner des European Quality Awards 1998: „Der einzige Mensch, der sich über Veränderungen freut, ist ein Baby in nassen Windeln“.

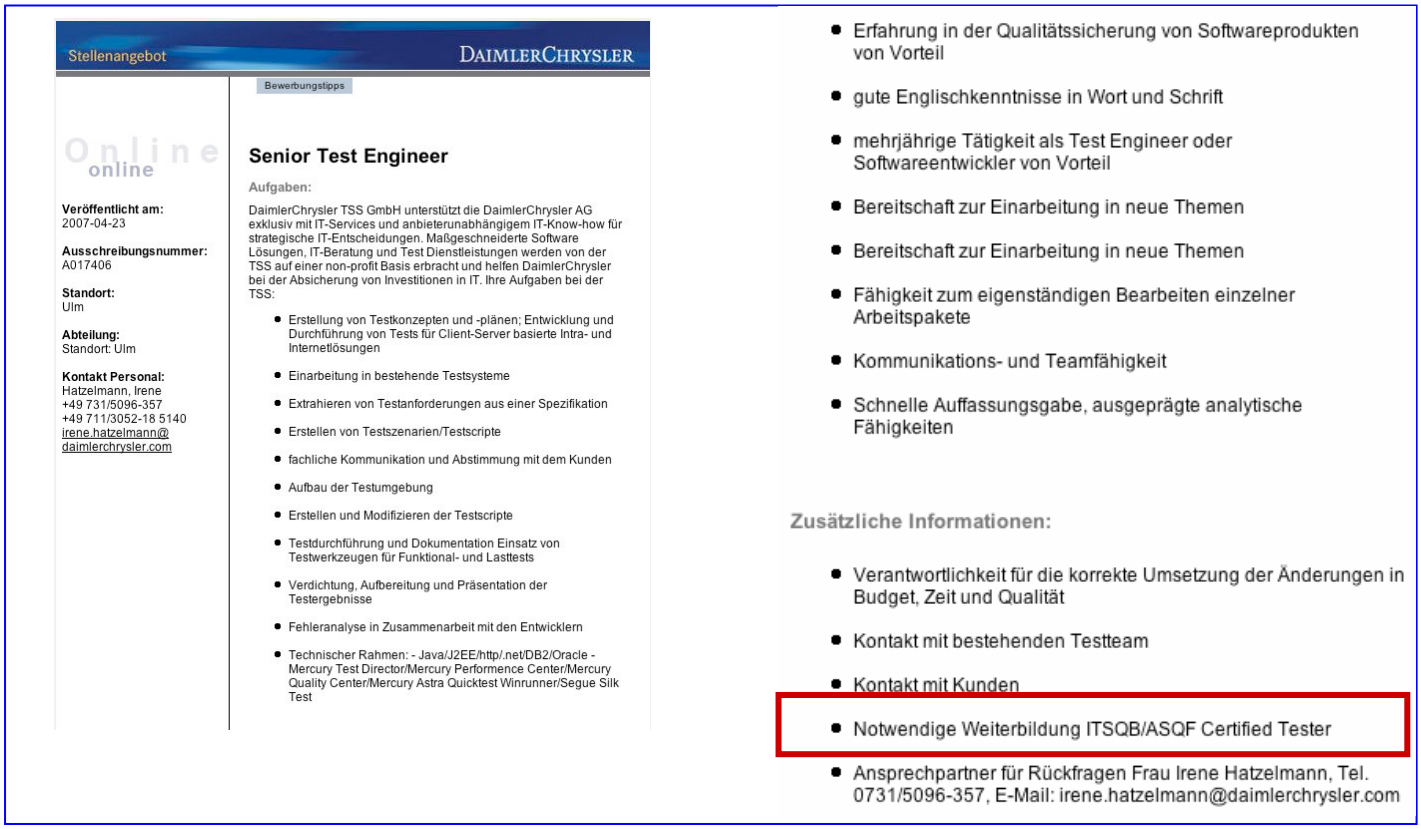
Das internationale Software Quality Institute (iSQI) unterhält Kooperationen mit folgenden internationalen Institutionen:

- ISO/IEC JTC1 SC7 Working Groups (ISO15504, ISO12207, ISO15288, …)
- ISO (International Organization for Standardization)
- EQN (European Quality Network)
- EOQ-SG (European Organization for Quality - Software Group)
- EURUSS (Know-How Transfer for Certified EU Project Managers in Russia)
- EuroSPI (European Software Process Improvement Initiative)
- GESA e.V. (German European Security Association)
- iNTACS (International Assessor Certification Scheme)
- iNTCCM (International Certified Configuration Manager)
- ISTQB (International Software Testing Qualifications Board)
- USTQB (Ukraine) und LSTQB (Lettland)
- SeSamBB (Security and Safety made in Berlin-Brandenburg. e.V.)
- IKT-DIALOG Brandenburg - Leitung der AG Aus- und Weiterbildung
- E-Health-Forum Berlin Brandenburg - Leitung der AG Aus- und Weiterbildung

Das internationale Software Quality Institute (iSQI) verfügt über folgende Zertifzierungsprogramme:

- QAMP® - Quality Assurance Management Professional
- ISTQB® Certified Tester Foundation Level
- ISTQB® Certified Tester Advanced Level
- iSQI® Certified Professional for Software Architecture
- iSQI® Certified Professional for Project Management
- iNTACS™ Provisional Assessor (ISO/IEC 15504)
- iNTACS™ Competent Assessor (ISO/IEC 15504)
- (Provisional und Competent jeweils auch für AutomotiveSPICE®)
- IREB® Certified Professional for Requirements Engineering
- iNTCCM® Certified Professional for Configuration Management
- EU Certified Innovation Manager
- TTCN-3-Certificate®
- iSQI® Certified Professional for IT Security Management
- ISSECO® Certified Professional for Secure Software Engineering.

Beispiel ISTQB Certified Tester:



Stellenangebot — DaimlerChrysler

Bewerbungstipps

Online
online

Veröffentlicht am:
2007-04-23

Ausschreibungsnummer:
A017406

Standort:
Ulm

Abteilung:
Standort: Ulm

Kontakt Personal:
Hatzelmann, Irene
+49 731/5096-357
+49 711/3052-18 5140
irene.hatzelmann@daimlerchrysler.com

Senior Test Engineer

Aufgaben:

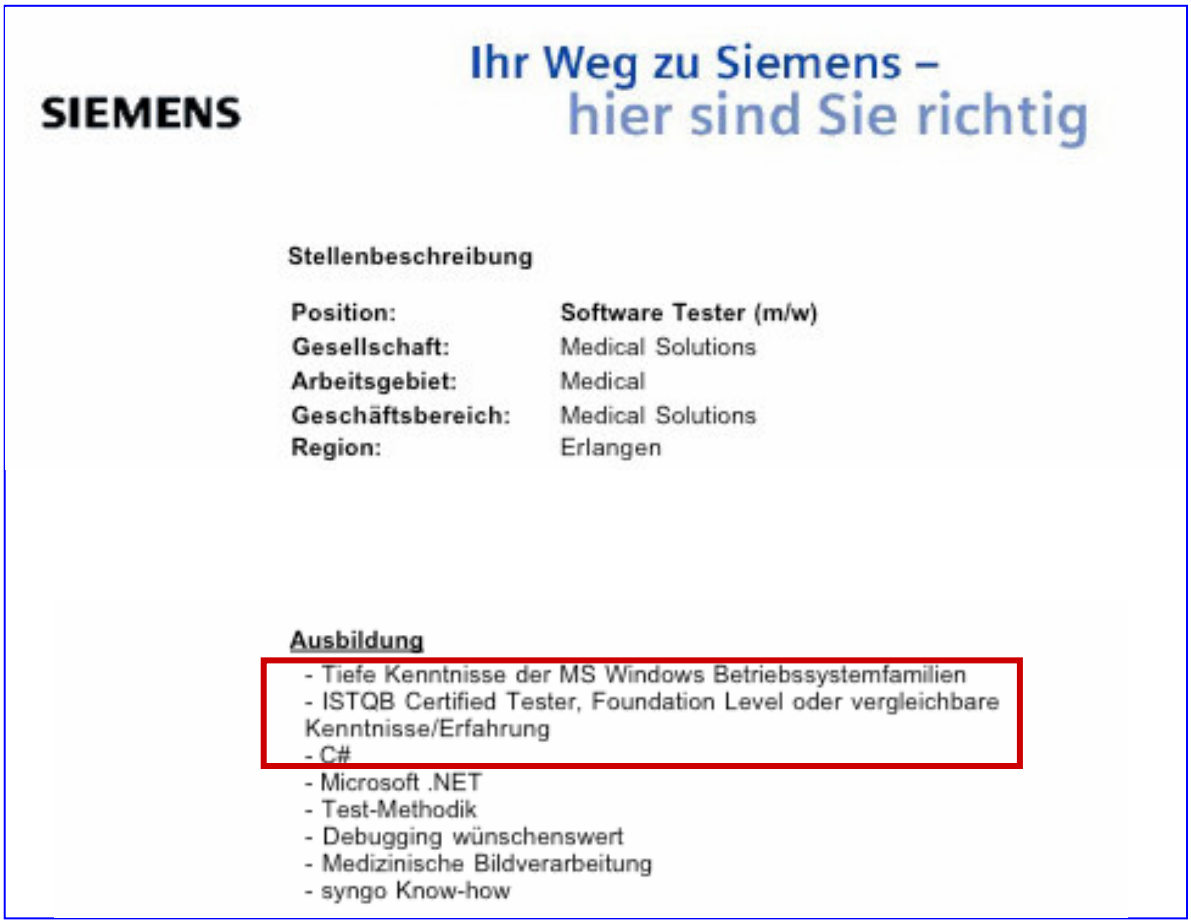
DaimlerChrysler TSS GmbH unterstützt die DaimlerChrysler AG exklusiv mit IT-Services und anbieterunabhängigem IT-Know-how für strategische IT-Entscheidungen. Maßgeschneiderte Software Lösungen, IT-Beratung und Test Dienstleistungen werden von der TSS auf einer non-profit Basis erbracht und helfen DaimlerChrysler bei der Absicherung von Investitionen in IT. Ihre Aufgaben bei der TSS:

- Erstellung von Testkonzepten und -plänen; Entwicklung und Durchführung von Tests für Client-Server basierte Intra- und Internetlösungen
- Einarbeitung in bestehende Testsysteme
- Extrahieren von Testanforderungen aus einer Spezifikation
- Erstellen von Testszenarien/Testscripte
- fachliche Kommunikation und Abstimmung mit dem Kunden
- Aufbau der Testumgebung
- Erstellen und Modifizieren der Testscripte
- Testdurchführung und Dokumentation Einsatz von Testwerkzeugen für Funktional- und Lasttests
- Verdichtung, Aufbereitung und Präsentation der Testergebnisse
- Fehleranalyse in Zusammenarbeit mit den Entwicklern
- Technischer Rahmen: - Java/J2EE/http/.net/DB2/Oracle - Mercury Test Director/Mercury Performence Center/Mercury Quality Center/Mercury Astra Quicktest Winrunner/Segue Silk Test

- Erfahrung in der Qualitätssicherung von Softwareprodukten von Vorteil
- gute Englischkenntnisse in Wort und Schrift
- mehrjährige Tätigkeit als Test Engineer oder Softwareentwickler von Vorteil
- Bereitschaft zur Einarbeitung in neue Themen
- Bereitschaft zur Einarbeitung in neue Themen
- Fähigkeit zum eigenständigen Bearbeiten einzelner Arbeitspakete
- Kommunikations- und Teamfähigkeit
- Schnelle Auffassungsgabe, ausgeprägte analytische Fähigkeiten

Zusätzliche Informationen:

- Verantwortlichkeit für die korrekte Umsetzung der Änderungen in Budget, Zeit und Qualität
- Kontakt mit bestehenden Testteam
- Kontakt mit Kunden
- Notwendige Weiterbildung ITSQB/ASQF Certified Tester
- Ansprechpartner für Rückfragen Frau Irene Hatzelmann, Tel. 0731/5096-357, E-Mail: irene.hatzelmann@daimlerchrysler.com



SIEMENS

Ihr Weg zu Siemens –
hier sind Sie richtig

Stellenbeschreibung

Position:	**Software Tester (m/w)**
Gesellschaft:	Medical Solutions
Arbeitsgebiet:	Medical
Geschäftsbereich:	Medical Solutions
Region:	Erlangen

Ausbildung

- Tiefe Kenntnisse der MS Windows Betriebssystemfamilien
- ISTQB Certified Tester, Foundation Level oder vergleichbare Kenntnisse/Erfahrung
- C#
- Microsoft .NET
- Test-Methodik
- Debugging wünschenswert
- Medizinische Bildverarbeitung
- syngo Know-how

3.3. *Dieter Krawczynski, DomData Sp. z o.o., Poznan: IT-Systeme für den Mittelstand – Modellierung von Geschäftsprozessen*

Die Firma DomData sp. zo. o aus Poznan (www.domdata.com) wurde im Jahre 1994 durch die Firma WohnData aus Hamburg, einem damals führenden Hersteller wohnungswirtschaftlicher Software auf dem deutschsprachigem Markt , als polnisches Tochterunternehmen gegründet.

Nach der Fusionierung der Wohndata mit einem größeren deutschen Softwarehaus und sich mehrfach veränderten Unternehmensstrukturen ist die DomData seit 1998 ein polnisches Unternehmen mit dem Stammhaus in Poznan und Vertriebstöchtern in Deutschland und der Schweiz. Zur Zeit sind ca. 250 Mitarbeiter beschäftigt.

Die DomData versteht sich als europäisches IT-Systemhaus. Das zeigt sich in den Kundenstrukturen und u.a. auch darin, daß die Mehrheit der SW-Produkte in deutsch, polnisch und englisch angeboten wird.

Basis für die Projektarbeit in verschiedenen europäischen Staaten und in den USA sind neben den guten Informatikkenntnissen auch die sprachliche Kompetenz der Techniker und Berater. Dementsprechend müssen sich Bewerber einer Sprachprüfung durch die unternehmenseigene Übersetzungsabteilung unterziehen.

Die deutsche und die polnische Wohnungswirtschaft sind nach wie vor wichtige Geschäftsfelder des Unternehmens.

Die DomData vertreibt auf dem polnischen Markt eine eigene Immobilien- Verwaltungssoftware, die inzwischen von mehr als 150 Kunden eingesetzt wird, wobei der größte Kunde die Stadt Breslau mit 58000 Wohnobjekten ist.

Inzwischen sind auch eine Reihe von Produktentwicklungen an den Schnittstellen zu Energie- und Wärmeversorgern sowie zu Banken und Versicherungen entstanden, die die wohnungswirtschaftlichen Kernprozesse unterstützen.

Ausgehend von den Forderungen der Wohnungs- und Immobilienwirtschaft sind Ende der 90-iger Jahre, Produkte für das betriebswirtschaftliche Controlling (Inforum-Produktfamilie) und zur Unterstützung von Organisationsprozessen und Qualitätsmanagementsystemen (Management Planet, DomData Intranet Plattform, Worknet) entwickelt wurden.

Diese Produktfamilien werden im polnischem Markt über eigenständige Internetplattformen (www.inforum.pl bzw. http://www.mp3-bpm.com) vertrieben.

Diese Produkte sind außerordentlich flexibel, durch den Kunden gut konfigurierbar und damit branchenunabhängig einsetzbar.

Neuere wohnungswirtschaftlich Anforderungen wie das Betriebskostenbenchmarking und der Energieausweis führten zum Aufbau eines Internetportals (siehe www.bekobench.de).

Die hier gewonnen Erfahrungen fließen gegenwärtig in das multinationale EU-Projekt save4home@works ein. Neben der Vermarktung eigener Produkte und der Durchführung entsprechender Einführungsprojekte haben verschiedene Formen der Auftragsprogrammierung einen ständig wachsenden Anteil am Geschäftsergebnis.

Wichtiger Auftragnehmer aus Deutschland ist Siemens. Neben einer Reihe von Einzelprojekten wurde u.a. ein Projektleitstand entwickelt.

Durch die Zusammenarbeit mit einem großen Stamm freiberuflicher Übersetzer kann ein breites Sprachen- und Fachspektrum abgedeckt werden.

Im polnischen Markt arbeitet man sehr intensiv mit einer Reihe von Banken zusammen. Hier wurden die SEPA-Anforderungen frühzeitig aufgegriffen und entsprechende Produktentwicklungen realisiert. Eine vielfältige Zusammenarbeit besteht auch zur Volkswagen Polska AG und deren Lieferanten.

Die Übersetzungsabteilung der DomData unterstützt die Lokalisierung der eigenen Produkte in fremden Märkten führt aber auch die Polonisierung ausländischer Software durch.

Durch die Zusammenarbeit mit einem großen Stamm freiberuflicher Übersetzter kann ein breites Sprachen- und Fachspektrum abgedeckt werden.

Neben technischen Dokumentationen werden auch Übersetzungen zu politischen, ökonomischen und juristischen Themen realisiert.

Die DomData ist zertifizierter Übersetzer der polnischen Regierung für die Dokumente der Europäischen Union.

Kontakt: Berlin – Brandenburg

DomData GmbH

Bergstraße 26

D-15230 Frankfurt (Oder)
Tel. +49 (335) 6800649

Fax +49 (335) 6840049
email: Dieter.Krawczynski@domdata.com

4. Ergebnisse MCA-Workshop „Mission-Critical Applications“

4.1. Tobias Hoppe, Otto-von-Guericke-Universität Magdeburg, Institut für Technische und Betriebliche Informationssysteme, Arbeitsgruppe Multimedia and Security: COMO B3 – IT Security Automotive

Einleitung / Motivation:

In modernen Automobilen finden sich bereits komplexe IT-Infrastrukturen aus eingebetteten IT-Systemen (Steuergeräten), Sensoren und Aktoren. Die Vernetzung dieser Systeme wird zunehmend komplexer, sowohl innerhalb des Fahrzeugs (z.B. aus Gründen der Kabelreduktion), aber zukünftig auch zunehmend nach außen, wie z.B. zu anderen Fahrzeugen oder Infrastrukturen (Car-to-Car / Car-to-Infrastructure).

Angesichts dieser Entwicklung werden daher auch für das Automobil zunehmend umfassende Maßnahmen hinsichtlich der IT-Sicherheit erforderlich, um absichtliche Angriffe auf diese IT-Strukturen durch verschiedenste Personengruppen mit individuellen Interessen möglichst zu erschweren.

Die Sicherheit von Automobilen stellt zumindest im Sinne des englischen Begriffs „Safety“ (zur Einschränkung von Personenschäden) einen klassischen Schwerpunkt in der Entwicklung von Automobilen dar. Hierbei werden jedoch hauptsächlich *unbeabsichtigte* Funktionsstörungen oder Ausfälle von Komponenten betrachtet und versucht, die Schwere ihrer Auswirkungen zu minimieren.

Zum Schutz vor gezielt *beabsichtigten* Angriffen auf automotive IT werden jedoch andere Schutzmechanismen benötigt. Die Beachtung der IT-Sicherheit (im Sinne von engl. Security) ist gerade im automotiven Bereich zunehmend erforderlich, denn im Gegensatz zum Heim-PC können sich Verletzungen der IT-Security hier auch direkt auf die Safety (also Leib und Leben der Insassen und im Umfeld befindlichen Personen) auswirken.

Das Verbundprojekt COMO, das Teilprojekt B3 und ausgewählte Forschungsschwerpunkte:

An der Otto-von-Guericke-Universität Magdeburg wird unter dem Titel COMO: COmpetence in MObility im Rahmen eines Forschungsschwerpunkts zu Automotive-Themen interdisziplinäre Forschung auf diesem Gebiet betrieben. Der Teilbereich B3 befasst sich dabei insbesondere mit Fragen der IT-Sicherheit mit Bezug auf unterschiedliche Anwendungen im IT-System Automobil. Die geplanten Arbeitspunkte sehen zunächst eine *Bedrohungsanalyse und die Erarbeitung pauschalisierter Richtlinien* und Designpattern vor.

Zusätzlich werden auf verschiedene Anwendungen bezogene *Beispielszenarien* entworfen und bearbeitet: Einerseits wird ein *multimodales biometrisches Authentifizierungssystem* betrachtet, welches biometrische Authentifizierungen am Beispiel von Gesichts- und Sprechererkennungen unter den wechselnden Bedingungen im automobilen Umfeld vornehmen soll.

Bezüglich des *sicheren Datenmanagements im Automobil* werden im Rahmen einer Domänenanalyse (am konkreten Anwendungsbeispiel des adaptiven Fahrwerks) Konzepte und ihr Potential untersucht, um automotives Datenmanagement zu verbessern.

Während dies zukünftig vielseitiges Verbesserungspotential bei der Entwicklung automotiver Systeme verspricht, erfolgt die Betrachtung der Datenhaltung und -bereitstellung hier insbesondere auch mit Blick auf Anforderungen der IT-Sicherheit.

Eine weitere Teilaktivität ist die Entwicklung von Designpattern für sichere automotive Kommunikation, insbesondere mit Fokus auf die zunehmend diskutierte, berührungslose *Car-to-Car- Kommunikation*.

Diese Szenarien dienen als exemplarische Anwendungsfälle, um die entwickelten *Pauschalisierungen und Designempfehlungen zu evaluieren* und verifizieren und so abschließend eine *Restrisikoabschätzung* vornehmen zu können.

Die B3-Laborausstattung und praktische Einblicke in bisherige Versuche:

In diesem Beitrag wurden einige praktische Einblicke in die verschiedenen Themengebiete gegeben, die gegenwärtig in Projektbereich B3 bearbeitet werden. Praktische Einblicke in Beispiele der aktuellen Forschung wurden mit einem Einblick in die für praktische Versuche zur Verfügung stehende Laborausstattung eingeleitet.

Hierzu steht dem Projektbereich automotive Technik aus aktuellen Modellreihen verschiedener, internationaler Automobilhersteller zur Verfügung (Baujahre 2004-2007). Hier stehen in jeweils wesentliche Steuergeräte und Bedienelemente eines realen Fahrzeugs (größtenteils über die originalen Kabelbäume verbunden), in einem Pultaufbau zur Verfügung. Verschiedene Schnittstellen zu Diagnose- und Systembussen sowie entsprechende Softwarelösungen (Diagnose und Analyse/Entwicklungsumgebungen) bieten vielfältige Möglichkeiten zu praktischen Experimenten und Auswertungen.

Als praktische Einblicke in die aktuell behandelten Themen wurden vier Beispiele kurz vorgestellt.

Beispiel1: Ansatz biometrische Authentifizierung über adaptive dynamische Fusion biometrischer Merkmale[1]:

Kurz vorgestellt wurde ein Modell zur dynamischen, adaptiven multimodalen Authentifizierung im Automobil. Dieses bezieht über verschiedene biometrische und nichtbiometrische Sensoren Eingabedaten von Mensch und Umwelt, wertet diese aus und kann über eine Fusion einzelner uni-modaler Ähnlichkeitswerte unter Einbeziehung der aktuellen Umgebungseinflüsse zwischen Akzeptanz und Abweisungen entscheiden. Als Einsatzzweck hierzu ist eine Vielzahl von Anwendungsszenarien denkbar.

Beispiel 2: Modellierung für sicheres automotives Datenmanagement[2]:

Das gezeigt Modell wurde konzipiert, um schon während der Spezifikation einzelne Daten (z.B. Kilometerstand) anhand ihrer spezifischen Eigenschaften und Anforderungen (letztere aus Sicht der Security , Safety, des Komforts und der Datenmanagements) einzuordnen und (auch unter Einbeziehung typischer Abhängigkeiten) daraus Designrichtlinien und Anforderungen für das Gesamtsystem und seine Komponenten ableiten zu können.

Beispiel 3: Angriff auf Warnblinker und Ansatz zur Erkennung durch IDS-Techniken[3]:

Bei diesem in einer Videosequenz gezeigten informationstechnischen Angriff auf die im Versuchsaufbau vorliegende Fahrzeugtechnik wurde vorbereitend ein Einbruch in den Fahrzeuginnenraum eines gesicherten Fahrzeugs simuliert. Das daraufhin einsetzende Alarmsignal über die Warnblinkanlage wurde im Zuge des gezeigten Angriffs durch Einspielen zusätzlicher Nachrichten in die fahrzeuginterne Kommunikation im Resultat erfolgreich unterdrückt werden. Gleichzeitig wurde anhand dieses Beispielangriffs eine erste prototypische

Implementierung einer IDS-Komponente für den automotiven Einsatz demonstriert, die die Aktivität dieses Angriffs erkennt und signalisiert.

[1] Aus: Andrey Makrushin, Jana Dittmann, Stefan Kiltz, Tobias Hoppe: Exemplarische Mensch-Maschine-Interaktionsszenarien und deren Komfort-, Safety- und Security-Implikationen am Beispiel von Gesicht und Sprache; In: Alkassar, Siekmann (Hrsg.): Sicherheit 2008; "Sicherheit - Schutz und Zuverlässigkeit"; Beiträge der 4. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), 2.-4. April 2008 in Saarbrücken; pp. 315 - 327, ISBN 978-3-88579-222-2, 2008

[2] Aus: Sandro Schulze, Stefan Kiltz, Tobias Hoppe, Jana Dittmann: Modelling Data Requirements for a Secure Data Management in Automotive Systems. In: Tagungsband des Workshops "Modellbasierte Entwicklung von eingebetteten Fahrzeugfunktionen" auf der Modellierung 2008, März 2008

[3] Erscheint in: Tobias Hoppe, Stefan Kiltz, Jana Dittmann: IDS als zukünftige Ergänzung automotiver IT-Sicherheit, DACH Security 2008, Technische Universität Berlin, 24. und 25. Juni 2008

Beispiel 4: Angriff auf Airbag-Systeme: Verbergen von Diebstahl-Delikten und Risiken[4]:

Dieser ebenfalls als Videosequenz aufbereitete praktische Angriffsversuch demonstrierte, wie ein Angreifer den Diebstahl von Airbagsystemen (hier anhand des zusätzlichen Entfernens des Airbag-Steuergeräts demonstriert) verbergen kann. Durch bösartige Interaktion mit der fahrzeuginternen Kommunikation wird einerseits das Erlöschen der Warnleuchte in der Instrumentenkombination erzwungen. Andererseits wird durch Nachbilden des Diagnoseprotokolls erreicht, dass sich auch während einer elektronischen Fahrzeugiagnose in der Werkstatt das (entfernte!) Airbagsteuergerät meldet und vorgibt fehlerfrei zu sein.

Motivation von Schutzkonzepten:

Motiviert durch diese Beispiele wird deutlich, dass zukünftig ganzheitliche Ansätze für IT-Sicherheit im Automobil notwendig werden, insbesondere angesichts des zunehmend diskutierten Einsatzes von Car-to-Car und Car-to-Infrastructure Kommunikationstechnologien. Langfristig gilt es, adäquate Schutzziele zur Absicherung automotiver IT-Netzwerke zu identifizieren. Mit Blick auf absichtliche Angriffe sind dies beispielsweise die Integrität der einzelnen Steuergeräte gegen Manipulationen an sowohl der Soft- als auch der Hardware. Auch der gesamte Verbund ist hinsichtlich der untereinander abgewickelten Kommunikation zu schützen, wobei unter anderem die Authentizität Verfügbarkeit und Integrität von Nachrichten gegen unautorisierte Eingriffe zu bewahren ist sowie teilweise auch die Vertraulichkeit von Nachrichteninhalten relevant sein kann.

Beispiele für aktuell diskutierte Ansätze:

Zur Berücksichtigung derartiger Fragen automotiver IT-Sicherheit wurden einige aktuell diskutierte Ansätze kurz vorgestellt. Neben dem bereits im eigenen Beispiel demonstrierten IDS-Ansatz wurden zusätzlich zwei Beispiele aus der aktuellen Forschung erwähnt:

Ein System, das von der Bundesdruckerei entwickelt wurde, verwendet eine Public-Key-Infrastruktur (PKI) über GSM-Verbindungen zur Zertifizierung von Harware-Komponenten über digitale Zertifikate [BZ08]. Bei Fahrzeugstart wird von jeder Komponente ein Hash-Wert abgefragt und ihre Unversehrtheit durch Verwendung einer PKI über entsprechende Zertifikate verifiziert. Im Fall, dass das Fahrzeug als gestohlen gemeldet wird, kann es zudem gesperrt werden. Um zu vermeiden, dass der gegenwärtige Fahrzeugführer (i.d.R. der Dieb) in Gefahr kommt, wird dazu die maximale Reichweite und Geschwindigkeit auf minimale Werte von bis zu 50 km bei 10 km/h reduziert.

Als Grundstein für langfristige Lösungen wird zudem der Nutzen von Trusted-Computing Technologie als Etablierung einer sicheren Hardware-Plattform für den Einsatz im automobilen Umfeld erforscht [WWW07]. Hierzu muss einerseits den speziellen Anforderungen auf diesem Einsatzgebiet als auch dem individuellen Bedrohungspotenzial Rechnung getragen werden, die sich zum Teil stark vom klassischen Bereich der Desktop-IT unterscheiden.

Zusammenfassung und Ausblick:

Zusammenfassend lässt sich feststellen, dass IT-Sicherheit in ihrem Einsatz im Automobil zukünftig eine zunehmende Bedeutung zukommen wird. In diesem Beitrag wurden einzelne Forschungsaktivitäten aus dem Projektbereich B3: IT Security Automotive des Projektes COMO (COmpetence in MObility) vorgestellt, die sich mit verschiedenen Aspekten der Sicherheit in automotiven Systemen auseinandersetzen. Beginnend mit Einblicken in Forschung zu sicherem automotiven Datenmanagement

[4] Aus: Tobias Hoppe, Jana Dittmann: Vortäuschen von Komponentenfunktionalität im Automobil: Safety- und Komfort-Implikationen durch Security-Verletzungen am Beispiel des Airbags; In: Alkassar, Siekmann (Hrsg.): Sicherheit 2008; "Sicherheit - Schutz und Zuverlässigkeit"; Beiträge der 4. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), 2.-4. April 2008 in Saarbrücken; pp. 341 - 353, ISBN 978-3-88579-222-2, 2008

und Einsatz von Biometrie im Automobil wurden zudem einige exemplarische Angriffe auf aktuelle automotive IT vorgestellt. Hieran wurde gezeigt, dass derartige Angriffe auch heute schon realistisch sind

und oft auch schon ohne Zugang zu firmeninternen Spezifikationen realistisch sind. Durch die Testergebnisse werden gleichzeitig ganzheitliche Ansätze zur Berücksichtigung der IT-Sicherheit in zukünftigen automotiven Entwicklungen motiviert, um letztendlich auch Safety-kritische Folgen als Resultat von Angriffen auf die IT-Security einzuschränken.

Referenzen:

[WWW07] A.Weimerskirch, M.Wolf, T.Wollinger: "State of the Art: Embedding Security in Vehicles", In EURASIP Journal on Embedded Systems (EURASIP JES), Special Issue: Embedded Systems for Intelligent Vehicles, 2007

[BZ08] Detlef Borchers, Peter-Michael Ziegler: Mit PKI gegen den Autoklau, Heise Newsticker 5.3.2008, http://www.heise.de/newsticker/meldung/104593

4.2. *Jan Krause, Ifak – Institut f. Automation u. Kommunikation e.V. Magdeburg*
Testfallgenerierung aus modellbasierten Systemspezifikationen

In der Entwicklung von Verkehrsmanagement- und Verkehrsinformationssystemen werden immer mehr Methoden und Werkzeuge des modernen Software Engineerings verwendet. So wird z. B. innerhalb des Forschungsprojekts Dmotion, in welchem ein baulastträger-übergreifendes Verkehrsmanagementsystem realisiert werden soll, ein speziell auf den Verkehrsbereich abgestimmtes Vorgehensmodell auf Grundlage des Rational Unified Process (RUP) entwickelt. Zur Systemspezifikation wird dabei innerhalb von Dmotion ausschließlich die Unified Modeling Language (UML) eingesetzt. Neben der Erfassung und Verwaltung der Systemanforderungen wird aber auch das geforderte Verhalten der verschiedenen Systemkomponenten mit Hilfe der UML, z. B. durch UML-Zustandsmaschinen, beschrieben.

Daneben werden innerhalb von Dmotion auch Methoden und Werkzeuge zur Validierung der Systemeigenschaften entwickelt. Auf Grundlage der vorliegenden UML-Systemspezifikation sollen so Systemeigenschaften verifiziert und weitere Arbeitsschritte zur Qualitätssicherung automatisiert durchgeführt werden können.

Ausgangspunkt einer Systementwicklung ist eine umfassende Anforderungsanalyse, deren Ziel eine detaillierte Spezifikation des zu erstellenden Systems ist. Diese Spezifikation ist gleichzeitig Grundlage der Implementierung als auch der Validierung des IT-Systems.

Grundsätzlich werden dabei keine Vorgaben gemacht, in welcher Form die Spezifikation des Systems, die sich aus der Anforderungsanalyse ergibt, zu beschreiben ist. In der Praxis werden die einzelnen Anforderungen im Regelfall mit Hilfe der natürlichen Sprache ausgedrückt und in Textdokumenten (z. B. Lasten- und Pflichtenheft) festgehalten. Nachteilig an dieser Art der Spezifizierung des Systems ist deren Interpretationsfähigkeit. Verschiedene Interpretationen der Spezifikation erschweren die Kommunikation unter den Entwicklungspartnern und erleichtern das Auftreten von Fehlern bei der Implementierung des Systems.

Aus diesem Grund ist es vorteilhaft, eine vorliegende dokumentenbasierte Spezifikation formal durch ein Modell zu beschreiben. Als Modellierungssprache eignet sich für diesen Zweck die UML/SysML sehr gut. Mit Hilfe der unterschiedlichen Diagrammtypen der UML kann sowohl das Design wie auch das geforderte Verhalten des Systems modelliert werden. Ausgehend von diesem erstellten Modell der Spezifikation des Systems sind mehrere notwendige Aktivitäten zur Realisierung und Validierung des Systems zumindest teilweise automatisierbar bzw. leichter durchzuführen. Abbildung 1 zeigt die grundlegenden Schritte zur Erstellung und Validierung eines Systems auf Grundlage eines UML-Modells.

Inhalt dieser Arbeit ist die kurze Vorstellung einer Methode zur automatischen Generierung einer Testsuite aus der Spezifizierung des geforderten Verhaltens des Systems. Voraussetzung für diese Methode ist die Beschreibung des geforderten System-Verhaltens mit einer UML-Zustandsmaschine. Die Durchführung eines Konformitätstests auf Grundlage der generierten Testsuite bringt Ergebnisse, die eine Aussage darüber treffen, ob das implementierte System sich konform gegenüber seinen spezifizierten Anforderungen verhält.

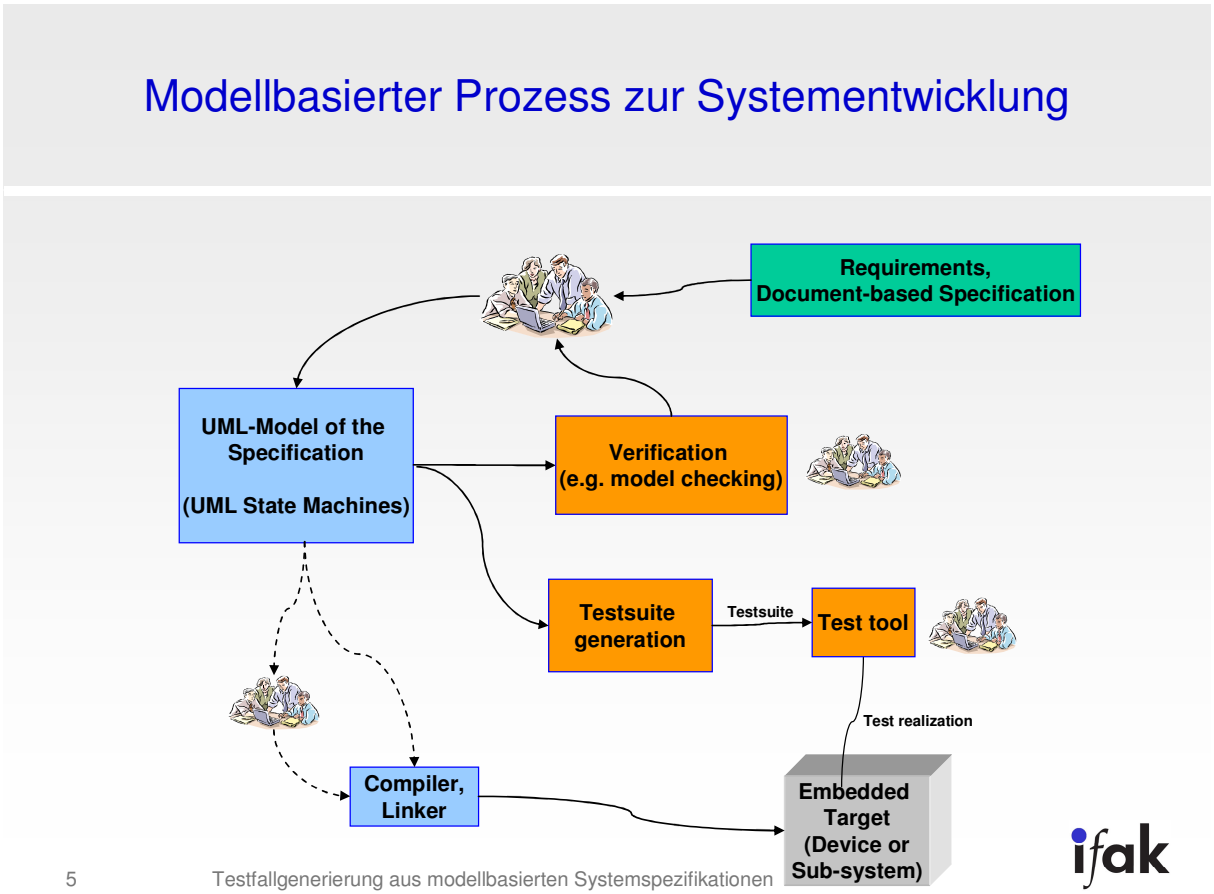


Abbildung 1 Modellbasierter Prozess zur Systementwicklung

Abbildung 2 zeigt die innerhalb von Dmotion entwickelte Methodik zur automatischen Ableitung von Testfällen aus modellbasierten Systemspezifikationen. Ausgehend von der Modellierung des gewünschten Systemverhaltens mit (kommunizierenden) UML Zustandsmaschinen können mit dieser entwickelten Methode automatisch Testfälle abgeleitet werden. Dabei decken die generierten Testfälle alle alternativen Pfade der Spezifikation ab und erreichen damit eine höhere Testabdeckung als die in der Praxis oft verwendeten Kriterien „alle (Knoten-) Zustände“ und/bzw. „alle Transitionen“.

Zur Generierung der Testfälle werden bekannte Methoden der Petri-Netz Theorie verwendet. Dazu ist die Abbildung der Verhaltensmodellierung auf ein Petri-Netz nötig. Um einen UML-Zustandsautomaten möglichst komplett abbilden zu können, wurde ein neuer Petri-Netz-Dialekt (Extended Safe Place/Transition Net – ESPTN) innerhalb von Dmotion entwickelt. Zur Testsuitegenerierung wird das komplette Präfix der Entfaltung des entstandenen ESPTN berechnet. In dem kompletten Präfix der Entfaltung können dann alle möglichen alternativen Prozesse des ESPTN und damit auch der zugrunde liegenden Verhaltensspezifikation identifiziert werden. Neben dieser Eigenschaft, welche zur Testfallgenerierung verwendet wird (je Prozess → ein Testfall) eignet sich das komplette Präfix der Entfaltung eines Petri-Netzes auch zur formalen Verifikation des Netzes (u. a. Model Checking) und damit auch der Verhaltensspezifikation (siehe auch Abbildung 1).

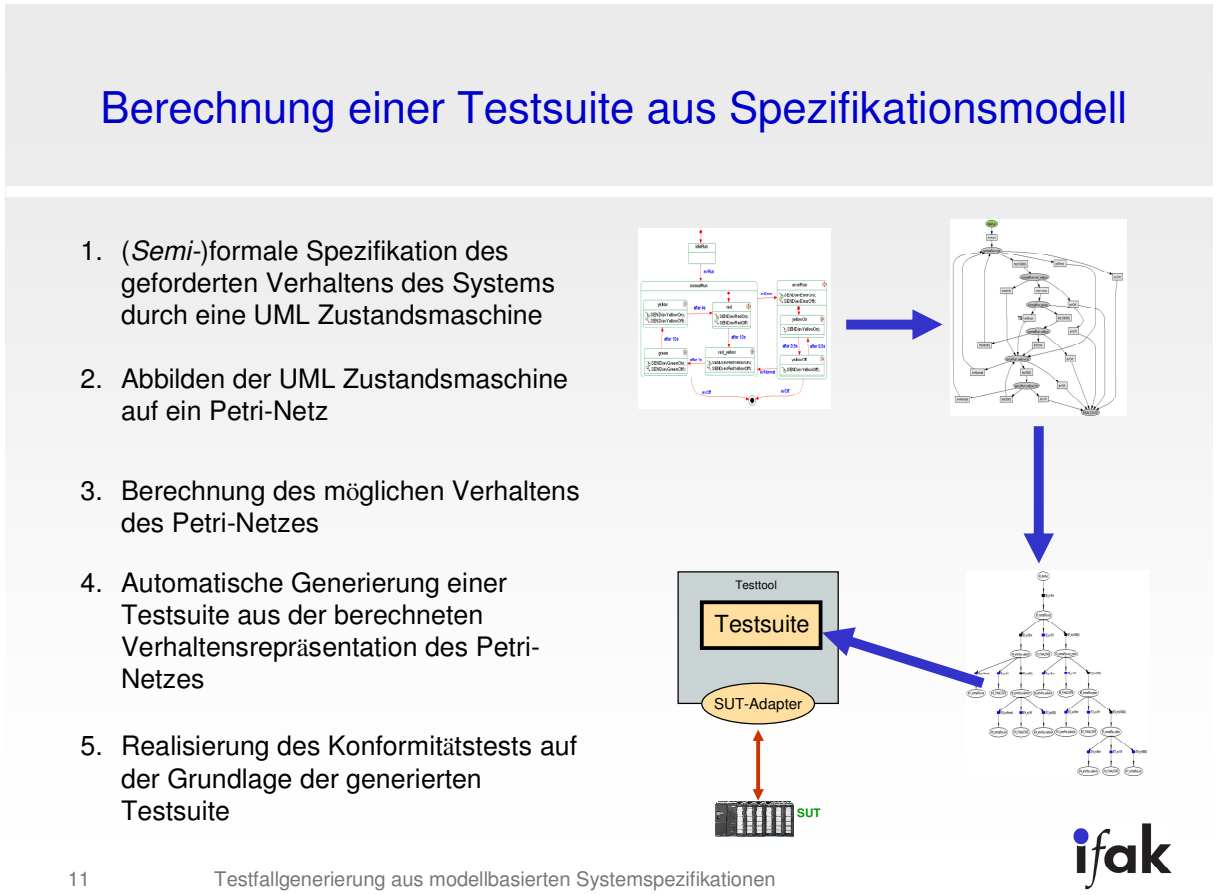


Abbildung 2 Methode zur automatischen Generierung einer Testsuite

Die entwickelte Methode zur automatischen Testfallgenerierung wird anhand einer Komponente des innerhalb von Dmotion realisierten Verkehrsmanagementsystems exemplarisch angewendet und evaluiert. Weitere Arbeiten werden sich mit der weiteren Formalisierung und der Adaption bekannter Methoden zur formalen Verifikation beschäftigen.

Autoren:

Dipl.-Wirtsch.-Ing. Jan Krause,
Wissenschaftliche Mitarbeiter Bereich Verkehrsmanagement
Verkehrstelematik - Institut für Automation und Kommunikation (ifak) Magdeburg

Dipl.-Ing. Franziska Wolf,
Wissenschaftliche Mitarbeiterin Bereich Fahrzeug- und Infrastruktursysteme
Verkehrstelematik - Institut für Automation und Kommunikation (ifak) Magdeburg

Dipl.-Ing. Andreas Herrmann
Bereichsleiter Verkehrstelematik
Verkehrstelematik - Institut für Automation und Kommunikation (ifak) Magdeburg

4.3. *Andreas Wenzel, Dpm Identsysteme GmbH Cottbus: System- und Planungsgrundlagen für Auto-Id-Systeme*

Was sind Automatische Identifikation (Auto-ID-) Systeme?

Auto-ID-Systeme kombinieren Barcode- mit RFID- Systemen, Magnet- und Chipkarten mit biometrischen Sicherungskonzepten.

Wozu System- und Planungsgrundlagen?

Beispiel einer typischen Anfrage:

- Wir wollen Auslieferungen erfassen.
- Wir haben 250 Fahrzeuge.
- Die Fahrzeuge fahren 7 Filialen an.
- Eine Access-Datenbank ist vorhanden.

Hierfür wollen wir ein Angebot haben!

mögliche Reaktionen könnten sein:

<u>eine weitere Reaktion</u>

Angebot 0815:

Preis je nach Konfiguration
ca. 200 – 875 T€

Wenn es nationale oder globale Anwendungsstandards für die Branchen

- Automobilindustrie
- Discounter
- Tierkennzeichnung
- Geldtransporte
- Pharmaprodukte u.s.w.

gibt, dann sind die Datenträger i.d.R. vorgeschrieben.

Ein großer Anwenderkreis nutzt dennoch, speziell für innerbetriebliche Abläufe, firmenspezifische Datenträger!

Zur Verwendung eines bestimmten Datenträgers sind folgende Fragen zu beantworten:

Sind Sicherheitskriterien zu erfüllen?

- Zurtittskontrolle
- Personendaten
- Geldtransfer

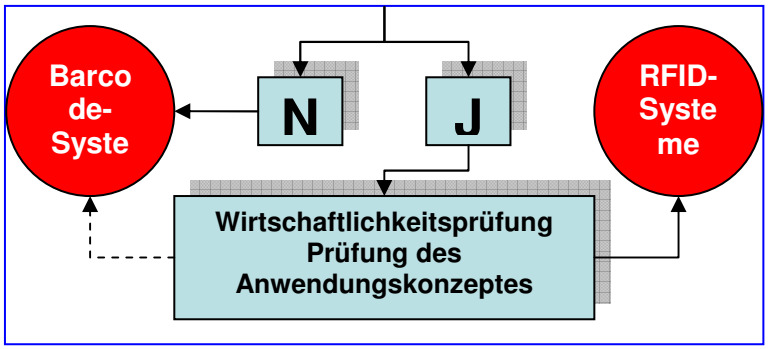
Werden langfristig Erfassungen wiederholt?

- Mehrwegtransportbehälter
- Anlagegüter

Besteht eine Nachweispflicht?

- Wartung von Anlagen
- Serviceleistungen

Müssen Daten ohne Systemhintergrund verfügbar sein?



Die Konkurrenz von Barcode- und RFID-Datenträger ist gegenwärtig nicht maßgebend. Beide Datenträger ergänzen sich im jeweiligen Anwendungsgebiet.

Vergleichendes Kostenrechnungsbeispiel für Auswahl eines Datenträger:

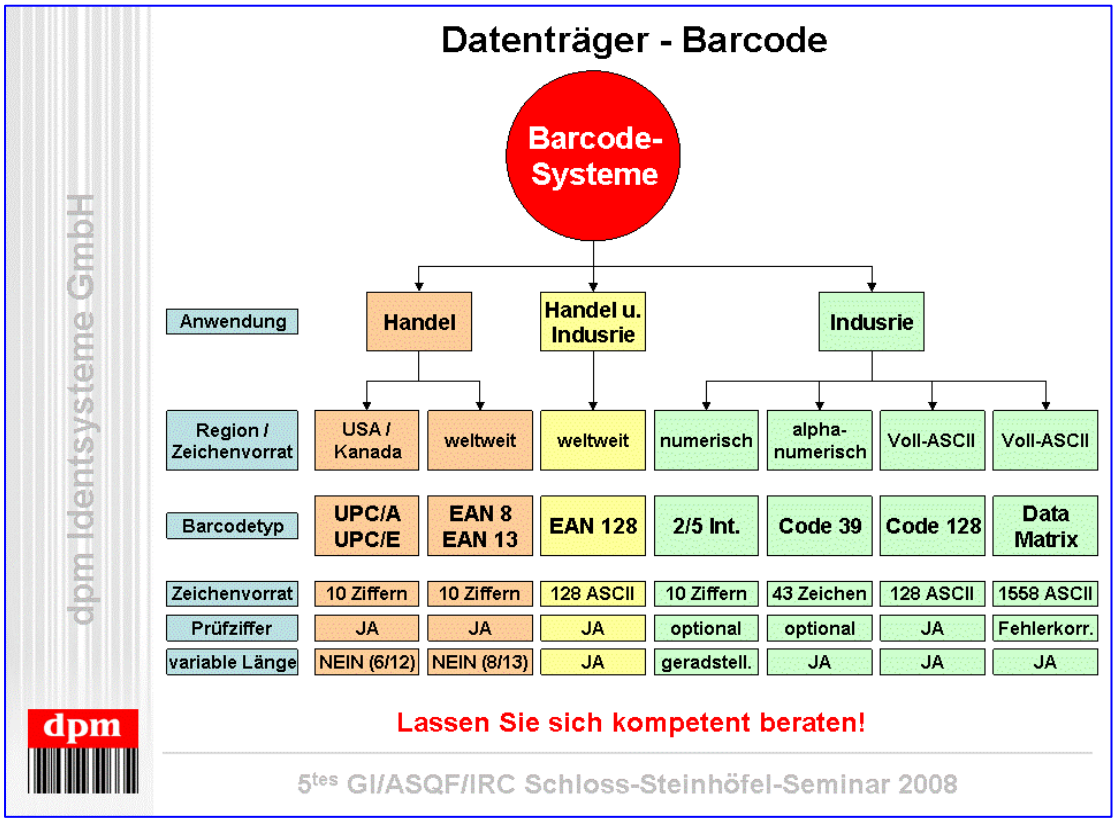
1. Etikettierkosten (5 Jahre):

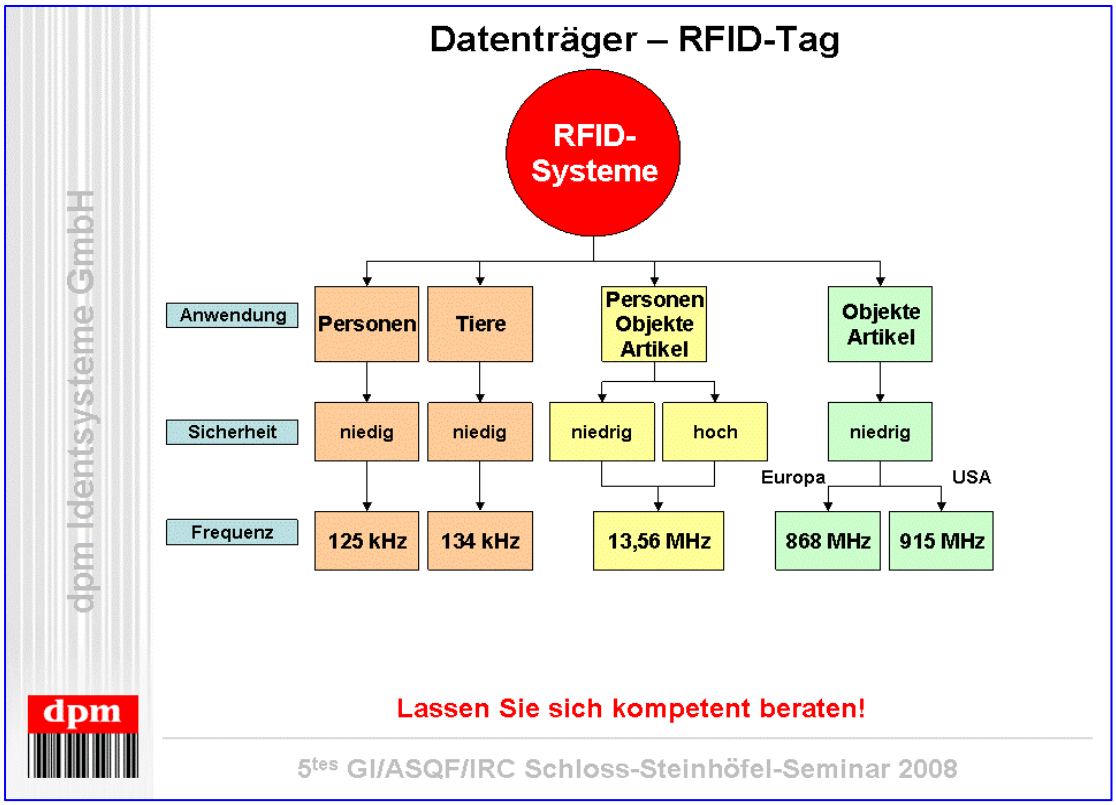
- Papieretikett ca. 100x50 mm bedruckt
- 100.000 Etiketten pro Jahr
- Thermo-/Transferdrucker
- incl. Installation/Service
- Kosten pro Jahr: ca. 4.400,- € * 5 Jahre = 22.000€

2. RFID-Kosten:

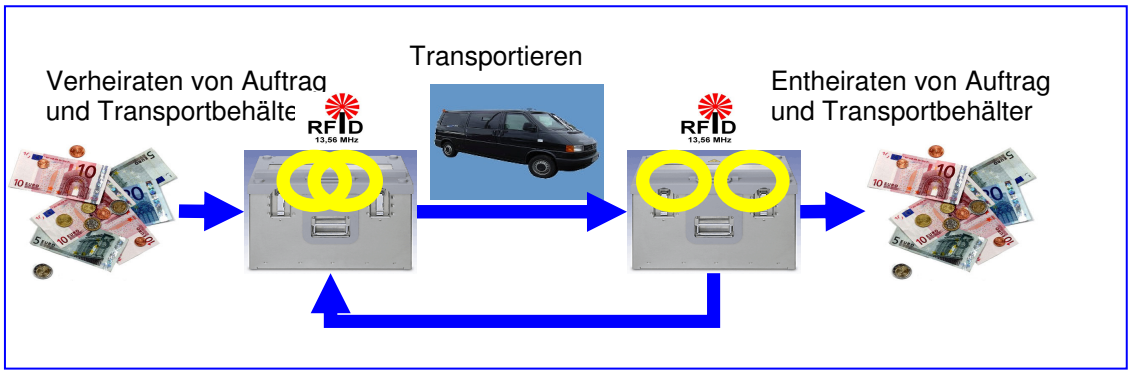
- 1.000 Tag‘s a 3,- €
- incl. Anbringung (1.000,- €)
- einmalige Kosten : ca. 4.000,- €

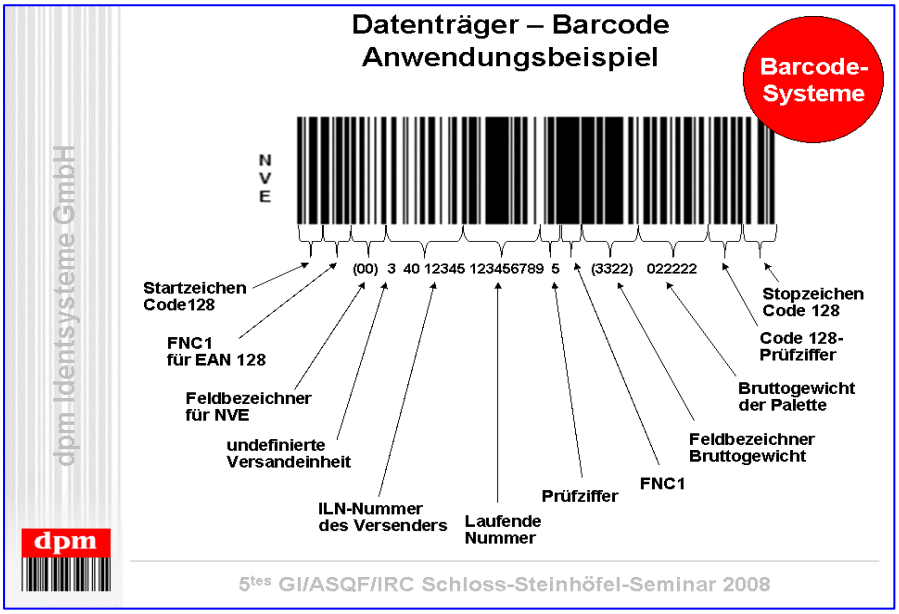
In 5 Jahren ergibt sich, bei Verwendung von RFID, anstelle von Etiketten, eine Kostenersparnis von 18.000€!

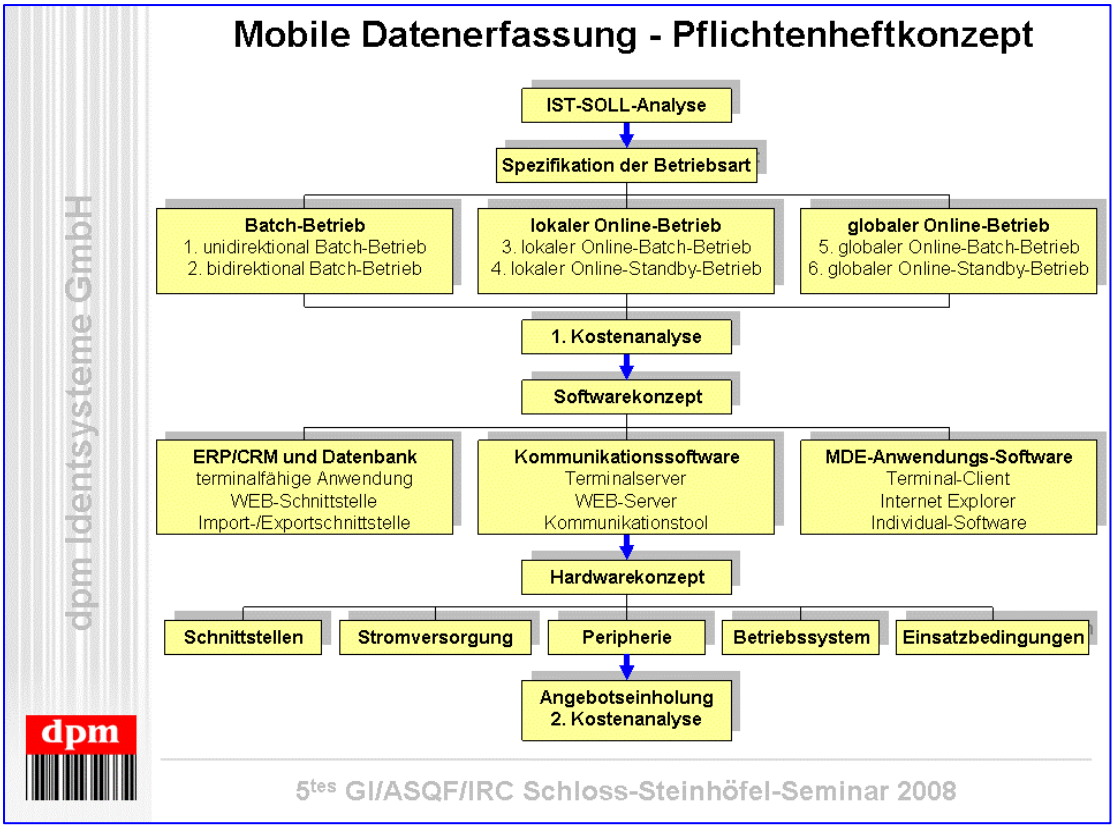

Datenträger - Barcode
Barcode-Systeme
Anwendung
Handel
Handel u. Indusrie
Indusrie
Region / Zeichenvorrat
USA / Kanada
weltweit
weltweit
numerisch
alpha-numerisch
Voll-ASCII
Voll-ASCII
Barcodetyp
UPC/A UPC/E
EAN 8 EAN 13
EAN 128
2/5 Int.
Code 39
Code 128
Data Matrix
Zeichenvorrat
10 Ziffern
10 Ziffern
128 ASCII
10 Ziffern
43 Zeichen
128 ASCII
1558 ASCII
Prüfziffer
JA
JA
JA
optional
optional
JA
Fehlerkorr.
variable Länge
NEIN (6/12)
NEIN (8/13)
JA
geradstell.
JA
JA
JA
dpm Identsysteme GmbH
dpm
Lassen Sie sich kompetent beraten!
5tes GI/ASQF/IRC Schloss-Steinhöfel-Seminar 2008


Datenträger – RFID-Tag
RFID-Systeme
Anwendung
Personen
Tiere
Personen Objekte Artikel
Objekte Artikel
Sicherheit
niedig
niedig
niedrig
hoch
niedrig
Europa
USA
Frequenz
125 kHz
134 kHz
13,56 MHz
868 MHz
915 MHz
dpm Identsysteme GmbH
dpm
Lassen Sie sich kompetent beraten!
5tes GI/ASQF/IRC Schloss-Steinhöfel-Seminar 2008

Verwendung von RFID-tags:







Ist-Analyse:

1. Prüfung vorhandener ERP/CRM-Software:

- Welche Daten kann ich mit vorhandenen Systemen
- (ERP/CRM) darstellen und auswerten?
    - ERP (Enterprise Resource Planning) – Planung der Unternehmensressourcen
    - CRM (*Customer Relationship Management*) - die Dokumentation und Verwaltung von Kundenbeziehungen

2. Prüfung vorhandener Datenbanksysteme:

- Welche Datenbanken stehen zur Verfügung?

3. Prüfung bestehender Schnittstellen:

- Sind Import-/Exportschnittstellen vorhanden?
- Ist eine WEB-Anbindung möglich?
- Sind terminalfähige Anwendungen (Terminalserver) vorhanden?

Soll-Analyse:

1. ERP/CRM- Analyse:

- Welche Daten sind für die Betriebsabläufe notwendig?
- Welche Daten können zur Verbesserung der Betriebsablaufe dienen?
- Welche Daten benötigt mein Kunde oder Lieferant zukünftig, bzw. welche Daten biete ich als Dienstleistung an?
- Ist das vorhandene ERP-System geeignet?

2. Datenbankanalyse:

- Sind die vorhandenen Dantenbankressourcen ausreichend?

3. Schnittstellen- Analyse:

- Müssen Schnittstellen geschaffen werden?

4. Zeit- und Ortanalyse:

- Zu welchem Zeitpunkt sind an welchem Ort welche Daten erforderlich?
    - ENTSCHEIDUNG FÜR EINE BETRIEBSART!

4.4. *Franziska Wolf, Ifak – Institut f. Automation u. Kommunikation e.V. Magdeburg: Anforderungen an die Informationssicherheit in den Bereichen der industriellen Automation und der Verkehrstelematik*

Der Einzug der Standard -IT-Technologien in die industrielle Automation ist in vollem Gange. Durchgängigkeit, Flexibilität und günstige Kosten sind dabei die offensichtlichen Vorteile. Mit diesen Möglichkeiten lassen sich neue Anwendungsfelder erschließen. Aber wo Licht ist, ist bekanntlich auch Schatten.

Allein durch das Aufschmelzen der harten Hierachieebenen, durch die Nutzung von Ethernet als durchgängige Kommunikationstechnologie und insbesondere weitverteilte industrielle Anwendungen, die drahtlose Kommunikationstechniken und private/ öffentliche Weitverkehrsnetze nutzen, werden zunehmend Anforderungen an die Informationssicherheit (IT-Security) gestellt. Erste Standards im industriellen Umfeld sind gerade verabschiedet (z. B. IEC 62443-3). Darüber hinaus stehen mit der VDI/VDE Richtlinie 2182 Blatt 1 auch Guidelines bzw. Best Practises zur Verfügung, die Hersteller, Integratoren/Maschinebauer und Anwender bei der Entwicklung und dem Betrieb sicherer (securer) Automatisierungslösungen unterstützen.

Technologien der modernen Verkehrswelt, ob in Automobilen oder im Verkehrsmanagement werden ebenfalls mehr und mehr von Methoden der Informationstechnologien beeinflusst. Anwendungen werden bestimmt von Vernetzung und verteilter Informationsbearbeitung. Techniken der Car-to-Infrastructure und Car-to-Car Kommunikation können so in Zukunft eine übergreifende und adaptive Verkehrsführung mit mehr Komfort und Sicherheit für die Verkehrsteilnehmer ermöglichen.

Dabei ist die Entwicklung in der Verkehrstechnik derzeit vergleichbar mit der in der Automatisierung vor einigen Jahren. Unterschiedliche Systemarchitekturen sind entstanden, welche automatisierte Verarbeitungen immer größerer Datenmengen ermöglichen.

Die breitere Anwendung oftmals auch modular verteilter Systeme ermöglicht nicht nur eine größere Nutzungsvielfalt für Anbieter und Nutzer, sondern zeigt auch eine verstärkte Bedrohung der Systeme. Bekannte Gefährdungen nebst ausführlichen Beschreibungen können in den Grundschutzkatalogen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) nachgeschlagen werden. Bedrohungen können im Zusammenhang mit den Faktor Mensch hervorgerufen werden, wie er etwa bei unauthorisierten Zugriffen auf Systeme vorliegt, bei welchen bewusst nach Lücken im System gesucht wird. Dies kann aus reiner Neugier, zur gezielten Spionage oder Sabotage geschehen, je nach der Art des angegriffenen Systems und dem

Hintergrund des Angreifers. Allerdings können Bedrohungen auch ohne den Faktor Mensch durch unvohergesehener Vorfälle, wie etwa höherer Gewalt (wie Blitzeinschläge, Personalausfall) oder technischen Versagen (Ausfall der Stromversorgung oder defekte Datenträger) entstehen.

Bedrohungen, wie vorsätzliche Angriffe und unbeabsichtigte Gefährdungen können negative Auswirkungen auf Schutzziele von Systemen haben. Schutzziele sind beispielsweise Verfügbarkeit, Integrität, Vertraulichkeit, Authentifizierung, Zugriffskontrolle, Nichtbestreitbarkeit und Aufzeichenbarkeit. Dabei wird von der konkreten Anwendung bestimmt, welche der Schutzziele zutreffend sind und wie die Priorisierung der Schutzziele erfolgt.

Heutige Automatisierungssysteme sind gekennzeichnet durch Office-Architekturen innerhalb der Fabrik- und Zellebene. Hier sind typischerweise Manufactoring Execution Systeme (MES) und Enterprise Ressource Planning (ERP) Systeme zu finden. Die darunter liegende Schicht innerhalb der in

Abbildung 3 Schematischer Aufbau industrieller Automatisierungssysteme dargestellten typischen Automatisierungspyramide ist die Steuerungsebene.

In ihr sind die Steuerungen (z.B. Speicherprogrammierbare Steuerung - SPS) zu finden. Die Komunikationssysteme der beiden oberen Ebenen basieren heutzutage weitestgehend auf der Ethernet Technologie. Als Kommunikationssysteme der untersten Ebene, der Feldebene, sind heute klassische Feldbussysteme (z. B. PROFIBUS) fest etabliert.

Aus Sicht der Informationssicherheit ist die Feldebene durch den Einsatz dieser Feldbussysteme weitestgehend imun gegen bekannte IT-Security Angriffe. Das liegt im allgemeinen daran, dass die Kommunikationsysteme der Feldebene auf keiner Standard IT-Technolgie beruhen. Bekannte Bedrohungen der IT „laufen“ daher nicht auf Geräte der Feldebene (Sensorik, Aktorik). Natürlich besteht aufgrund der unterschiedlichen Kommunikationssysteme der Feld- und Steuerungsebene auch eine Art „harte Systemgrenze“. Die Durchgängigkeit ist damit nicht gegeben und genannten Gefährungen besitzen wenig nenneswertes Risikopotential.

Durch die eingangs erwähnten Trends, beispielsweise Entwicklungen zur Dezentralisierung von Automatsierungsfunktionen, werden derzeit Feldbussysteme entwickelt, die ebenfalls auf der Basis von Ethernet arbeiten. Mit diesen neuen Ethernet-basierten Feldbussen ist nun der letzte Schritt zu einer vollständigen, vertikalen Integration von IT-Technologien bis hinunter zur Feldebende gelungen. Diese Connectivity und damit der Wegfall bisheriger harter Systemgrenzen führt letztenendes zu einer zunhemenden Bedrohung der Feldbussysteme.

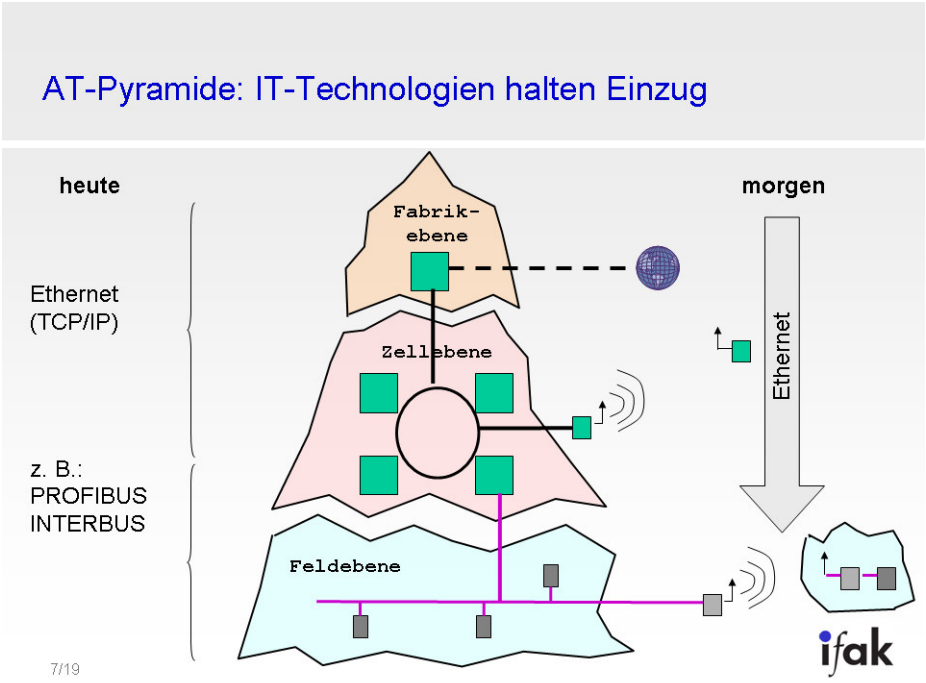


Abbildung 3 Schematischer Aufbau industrieller Automatisierungssysteme

Im Bereich der Verkehrstelematik, hier am Beispiel der sich schnell entwickelnden Systeme der Car-to-Car Kommunikation erläutert, stellt sich die Entwicklung ähnlich dar. Wie in Abbildung 4 dargestellt, kann eine Systemgrenze zwischen den Bussystemen innerhalb des Fahrzeuges und den Kommunikationsstrukturen von Fahrzeugen zu Infrastruktureinrichtungen gezogen werden.

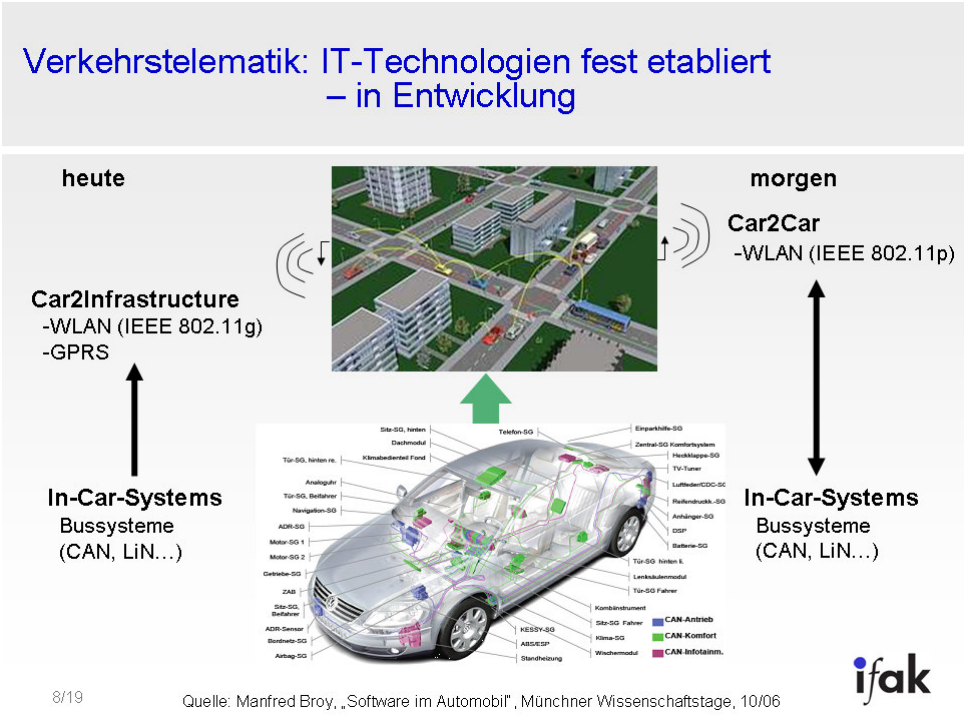


Abbildung 4 Kommunikationsstruktur in der Car to Car Kommunikation

Die Architektur innerhalb des Fahrzeuges sind weitgehend standardisiert und kann als geschlossenes System bezeichnet werden, da es bisher nicht ohne weiteres möglich ist, von außen auf die Bussysteme des Fahrzeuges zuzugreifen. Dieses geschlossene System, ähnlich der Feldebene der industriellen Automation, öffnet sich durch gegenwärtige Entwicklungen zusehens.

Bei der Car-to-Infrastructure-Kommunikation etwa werden Informationen, wie Geschwindigkeit, Position oder Abbiegevorgänge, mittels Sensoren ermittelt, über Bussysteme weitergeleitet und über WLAN oder GPRS an Verkehrszentralen gesendete. Diese Daten können in Informationsdiensten des öffentlichen Personennahverkehrs (ÖPNV) genutzt und Passagiere bereitgestellt werden. Da die Kommunikation in eine Richtung, von den Bussystemen hin zu den Infrastruktureinrichtungen durchgeführt wird, sind derzeit die Möglichkeiten von gezielten Angriffen auf die fahzeugseitigen Systeme mittels kabelloser Schnittstellen noch eingeschränkt.

Doch auch für diese Systemen werden Strategien entwickelt, welche ähnlich der industriellen Automation zukünftig interaktive, drahtlose und die Systemgrenzen übergreifende Kommunikationsmechanismen realisieren sollen. Die Car-to-Car Kommunkation nutzt dabei fahrzeugeigene Daten für dynamische Fahrzeitanalysen oder adaptives Verkehrsmanagement.

Verkehrsinformationen können unabhängig von vorhandenen Infrastrukturen direkt von Fahrzeug zu Fahrzeug übertragen werden.

Die Informationswege werden dabei in beide Richtungen durchgeführt, wodurch das bis dahin praktisch geschlossene System durch bidirektionale drahtlose Kommunikationwege geöffnet

wird. Daher entstehen für verkehrstelematische Systeme ähnliche Bedrohungen, wie das bei der industriellen Automation und letztendlich der Standard IT der Fall ist.

Die zu bennenden Schutzziele sind dabei bei der industriellen Automation und der Verkehrstelematik auf Grund von Einsatzfeldern, -orten und Technologien unterschiedlich. Während bei der Automation insbesondere die Verfügbarkeit im Vordergrund steht, muss bei der Verkehrstelematik ein besonderer Schwerpunkt auf die Integrität der Daten gesetzt werden. Die Prioritäten der Schutzziele beider Technologien sind in Abbildung 5 aufgeführt.

Abbildung 5 Schutzziele in Automatisierung und Car2X Systemen

Im Bereich der industriellen Automatisierungstechnik konnten in den letzten Jahren verschiedene Strategien der IT-Security entwickelt werden. Zum einen konnten die eher abstrakt gehaltenen Schutzempfehlungen und Vorgehensweisen des BSI-Grundschutzes für die Umsetzung der IT-Security Anforderungen adaptiert werden.

Darüberhinaus sind fehlende Aspekte zu berücksichtigen. Unter anderem ist die Anwendung von Gefahren-/Risikoanalysen zur Ermittlung geeignetter und damit wirtschaftlicher Lösungen zu prüfen. Praktikable Vorgehensweisen, die Anforderungen der industriellen Automation berücksichtigen, werden weitestgehend in der Gremienarbeit erarbeitet. Ziel ist die Definition notwendiger Richtlinien und Normenwerke zur Beachtung von Anforderungen an die Informationssicherheit industrieller Automatsierungslösungen und zur Gewährleistung von Interoperabilität.

Eine ähnliche Entwicklung ist auch für die IT-Security der verkehrstelematischen Systme denkbar und zweckhaft. In zukünftigen Arbeiten können auch hier die Strategien des Grundschutzes adaptiert und den verkehrstelematischen Ansprüchen angepasst werden. Das Car to Car Communication Consortium (C2CCC) stellt ein solches erstes Gremium dar, in welchem auch die Standardisierung von IT-Security ein wichtiges Arbeitsgebiet ist.

Es ist zu hoffen, dass die Chance genutzt wird Strategien und grundlegende Methoden sicheren Systemdesigns in der generellen Entwicklung dieser neuen, erst entstehenden Arbeitsgebieten zu festigen. Nur so können in Zukunft maßgeschneiderte Kommunikationssysteme entstehen, in denen Sicherheit und Funktionalität, Safety und Security keine Widersprüche, sondern sich gegenseitig stützende Konzepte darstellen.

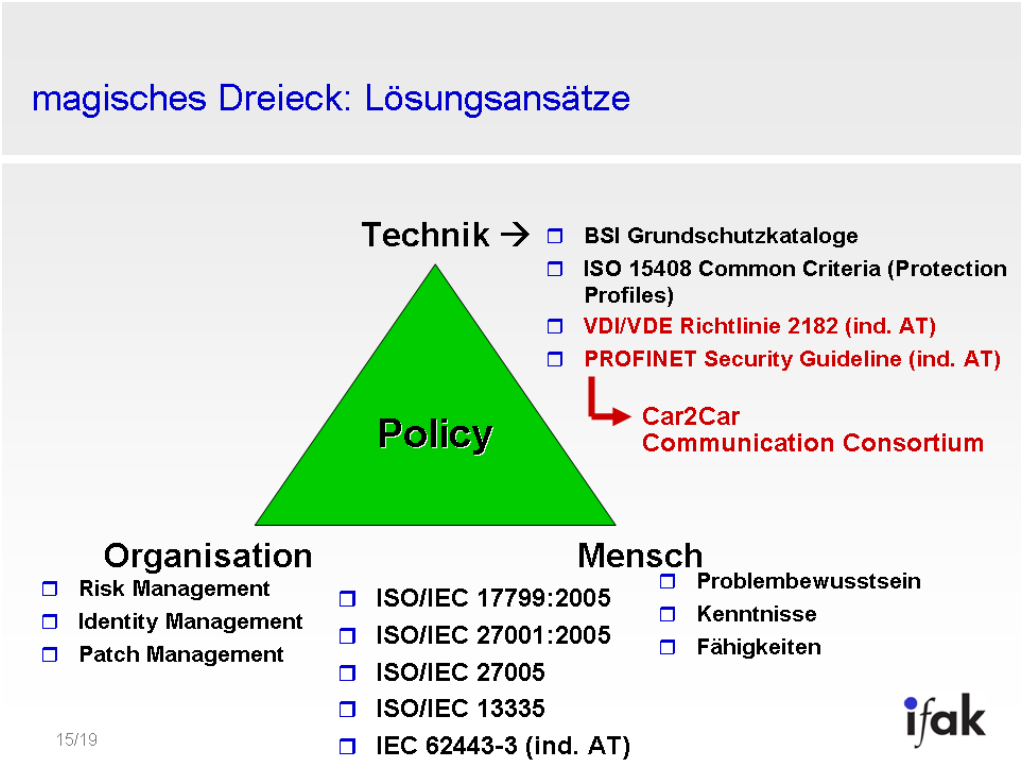


Abbildung 6 Synergien von Maßnahmen der IT-Security für ind. Automation und Verkehrstelematik

Dipl.-Ing. Franziska Wolf,
Fahrzeug- und Infrastruktursysteme
Verkehrstelematik

Institut für Automation und Kommunikation e.V. Magdeburg

Dipl.-Ing. Heiko Adamczyk,
Leiter Sichere industrielle Kommunikation

Institut für Automation und Kommunikation e.V. Magdeburg

ifak - Institut f. Automation und
Kommunikation e.V. Magdeburg
Werner-Heisenberg-Str. 1
39106 Magdeburg
Tel.: +49 391 990140
Fax: +49 391 9901590

5. Ergebnisse EKS-Workshop „Engineering Komplexer Systeme“

5.1. Katja Winder, PhiloTech GmbH Cottbus: Validation komplexer Systeme auf Grundlage des Software-Entwicklungsstandards RTCA DO-178B

Abbildung A380 Erstflug am 27. April 2005

Qualitätssicherung im Luftfahrtbereich:

Die steigende Komplexität von Systemen und die zunehmenden Qualitätsanforderungen an diese erfordern:

- Standardisierte Entwicklungsmethoden
- Effiziente Verifikationsmethoden

Wichtige Verifikationsziele im Luftfahrtbereich:

- Vollständige und korrekte Funktionalität
- Betriebssicherheit
- Robustheit
- Anwenderfreundlichkeit
- Wartbarkeit

RTCA DO-178B Standard für die Software-Entwicklung im Bereich Luftfahrt:

- Kategorisierung in Sicherheitslevel (DAL A - E) und Partitionierung
- Dokumentation aller Entwicklungsschritte
- Sicherheitslevel legt Testtiefe fest
- Unabhängigkeit im Verifikationsprozess
- Rückverfolgbarkeit aller Verifikationsergebnisse
- Häufig eingebettet in ein System aus kundenspezifischen Standards, z.B. Airbus Directive 100 (ABD 0100)

Einordnung der Software anhand der Fehlerfolgen:

- Bei Funktionsausfall
- Im Fehlerfall

Partitionierung in einzelne Teile unter Berücksichtigung von:

- Gemeinsamer Hardware
- Datenfluß
- Kontrollfluß

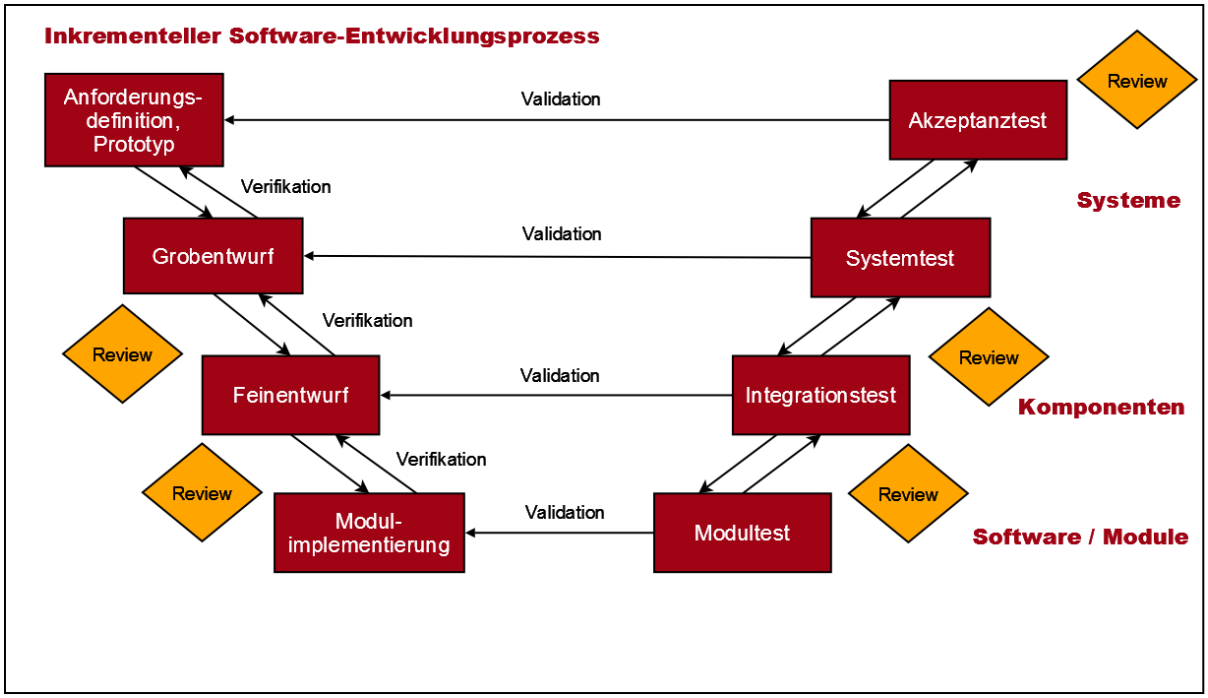
Statische Analysen und Reviews

- Design-Review
- Code-Review
- Test-Review
- Kontrollflussanalyse
- Datenflussanalyse

Testen

- Modultests
- Software/Software-Integrationstests
- Hardware/Software-Integrationstests
- Systemtests

Software-Verifikation im V-Modell:



Schwerpunkte beim Test nach DO-178B:

1. Immer basierend auf der Spezifikation der Software
    - Blackbox-Testen hat immer Vorrang
    - Whitebox-Testen dient der Vervollständigung
2. Strukturierte Testfallentwicklung
    - Testfälle für normale Eingabewerte
    - Robustness Tests
    - Stress-/ Lasttests
    - Überdeckungsmaß abhängig vom Sicherheitslevel
    - Statement Coverage, Decision Coverage und Modified Condition/Decision Coverage
3. Rückverfolgbarkeit der Testergebnisse zu den Anforderungen
4. Unabhängigkeit der Tester und Reviewers
5. Strukturelle Überdeckungskriterien:
    - **Statement Coverage**: Es soll sichergestellt sein, daß jedes statement im Quellkode mindestens einmal ausgeführt worden sein!
    - **Decision Coverage**: Jeder Einstiegs- und Ausstiegspunkt, jedes Entscheidungs-Statement, jede Ein-/Ausgabe eines Programms muß mindestens einmal vom Tester involviert worden sein.
    - **Modified Condition/Decision Coverage (MC/DC)**:

Jedes bedingte Statement eines Programms muß alle möglichen Entscheidungen mindestens einmal durchlaufen haben. Für jede Bedingung in einem solchen Statement muß gezeigt werden, daß die Entscheidung nicht beeinflußt werden kann.

Dies kann gezeigt werden, indem die Eingangsbedingung variiert wird und gleichzeitig alle anderen Bedingungen festgehalten werden.

Zusammenfassung:

Wichtige Faktoren für die Entwicklung qualitativ hochwertiger Software:

- Definierter Software-Entwicklungsprozesses
- Kontinuierliche Prozeßverbesserung
- Nutzung aktueller und bewährter Technologien.

Gutes Testen ...

- ... kann viel zur Qualität der Software beitragen
- ... sollte immer Teil einer den gesamten Entwicklungsprozess umfassenden Qualitätssicherungsstrategie sein.

DO-178B als Entwicklungsstandard

- Garantiert lückenlose Dokumentation
- Fördert fehlerarme Applikationen
- Garantiert keine Fehlerfreiheit.

Philo*tech* – an enterprise with prospects

Philotech GmbH

Founded: 1987

Business: Engineering company

Headquarter: **München**

Eschenstrasse 2, D-82024 Taufkirchen

Locations: Hamburg, Bremen, Cottbus, Manching, Freiburg etc.

Subsidiary in Madrid

Employees: ~ 300

Philotech HAMBURG	**Philotech BREMEN**	**Philotech COTTBUS**
Bebelstraße 44	Hinterm Sielhof 4/5	Karl-Liebknechtstr. 127
D-21614 Buxtehude	D-28277 Bremen	03046 Cottbus
T.: +49 (0) 4161 50 20 - 0	+49 (0) 421-878 459 - 0	+49 (0) 355-355484 0

F.: +49 (0) 4161 50 20 - 20 +49 (0) 421-878 459 - 9 +49 (0) 355-355484 10

E-Mail: info@philotech.net
Home Page: www.philotech.net

5.2. *Jan deMeer, smartspacelab.eu GmbH: Security & Safety Verification & Validation in der Standardisierung*

Der Arbeitskreis DIN NIA27 (ISO/IEC JTC1/SC27) bearbeitet die folgenden 4 Themen für die Normung:

1. Benennung der grundsätzlichen Anforderungen an Sicherheitsdienste in IT-Systemen
2. Spezifizierung von Sicherheits-Richtlinien und Standards für das Sicherheitsmanagement
3. Spezifikation von Kriterien für die Evaluierung und Zertifizieurung von IT-Sicherheit.
4. Entwicklung von IT-Sicherheitstechniken und –Mechanismen, z.B. Kryptographie.

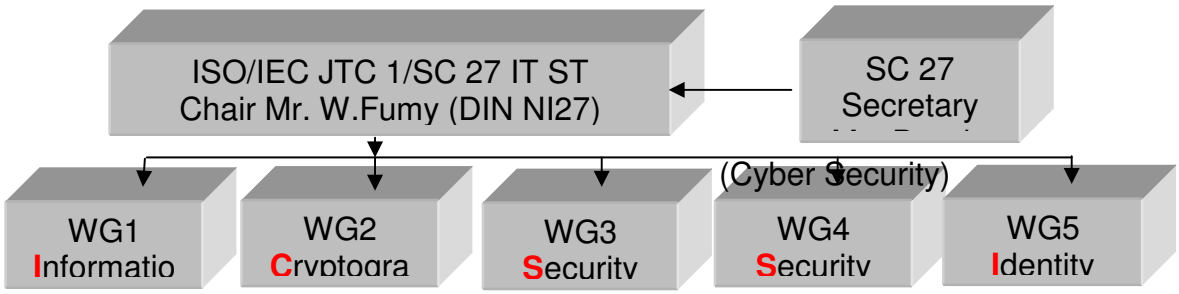


Abbildung: Struktur der IT-Security Normung im DIN

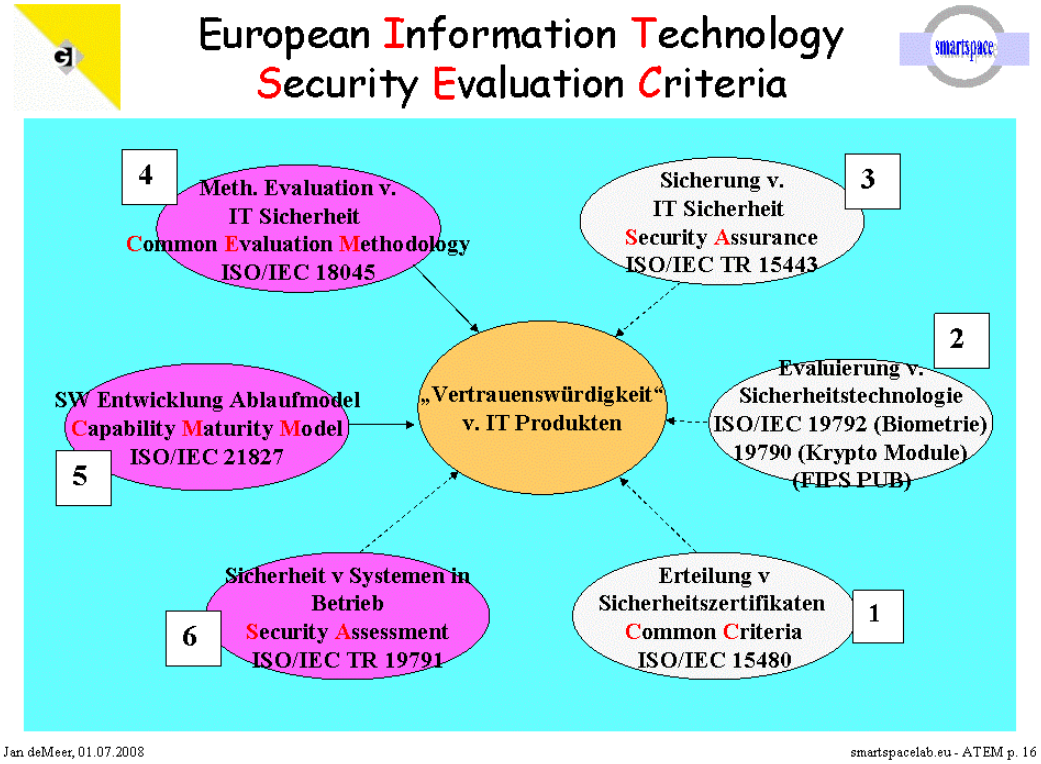


Abbildung: Sicherheitsevaluierungskriterien

Um Vertrauenswürdigkeit für (Software-) Produkte für Endabnehmer als auch für Komponenten, die in komplexe Systemen eingebaut werden müssen, benötigt man je nach Anforderung, die ganze oder teilweise Erfüllung der folgenden 6 Normen und Standards (s. Abbildung Sicherheitsevaluierungskriterien).

1. Erfüllung der sog. ***Common Criteria*** für die Erteilung von Sicherheitszertifikaten
2. Prüfung von biometrischen und kryptographischen Anforderungen, entsprechend des sog. FIPS Kriterienkatalogs
3. Nachweis von Maßnahmen zur Sicherung von IT Sicherheit (**Security Assurance**)
4. Nachweis der Anwendung der Common Evaluation Methodology, d.h. methodisches Testen und Evaluierung der IT Sicherheit
5. Für die Software Entwicklung der Nachweis, daß ein Capability Maturity Model oder Vorgehensmodell verwendet worden ist.
6. der Nachweis der Sicherheit eingebauter Systeme im Betrieb, z.B. Airbus, Bahnsignalisierung, etc. (**Security Assessment**)

Aus diesen Rahmenbedingungen ergeben sich für unterschiedliche Anwendungsbereiche unterschiedliche Vorgehensweisen:

Airborne Verification & Validation:

- Safety Regulatory Requirements ESA RR4

  (Safety Regulation Commission Document 4 - ATM2000+):

  - Verification is the proof, „confirmation by examination of evidence“, of a product, process or service fulfills a set of requirements
  - Validation is the proof, „confirmation by examination and provision of evidence“, of intended use, i.e. behaviour is fulfilled by an object or service

Railway-borne Verification & Validation:

- ISO/IEC 62278, DIN EN 50126

  (ISO/IEC 62279, DIN EN 50128):

  - Verification is the proof, „activity of determination“, of a correct development step/engineering phase, i.e. a set of requirement is captured by a transformation of an object (system component)
  - Validation is the proof, activity of demonstration“, of comparing two sets of requirements of two different objects being related (inclusion, equality, etc.)

Application Security Semantics:

- Airborne: RTCA DO 178B, MIL-STD-498, …
- Railway: DIN EN 50126 (RAMS), DIN EN 50128, …
- Automotive: …

Systems Engineering Semantics:

- Specification: UML
- Modelling & Verification: Hybrid Automota, TLA, Z, UPPAAL
- Testing & Validation: TTCN-3, LDRA-Method
- Platforms & Tools: LDRA-, TestingTech®- Workbenches

Quality Management Semantics:

- CQM DIN EN ISO 9000ff
- V-Model® XT
- ISO/IEC SC27 IT Security Techniques

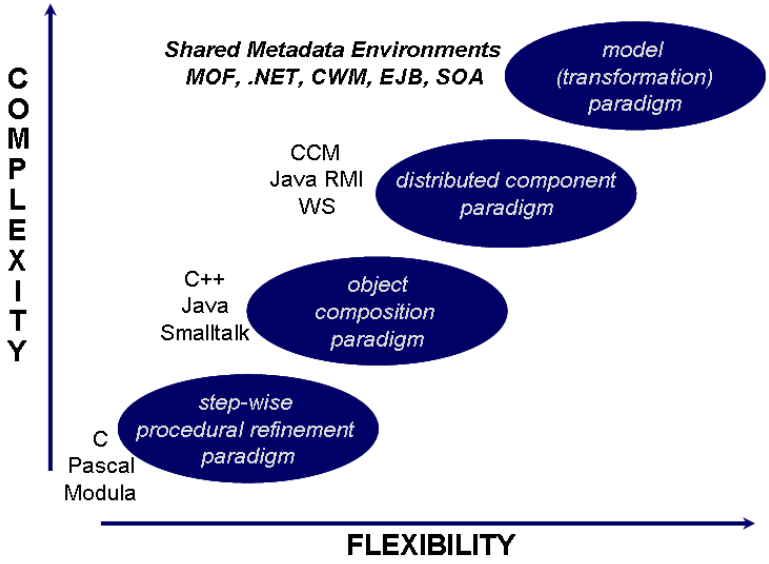
Practice Semantics:

- ESACS – Enhanced Safety Assessment of Complex Systems
- EICOSE - European Institute for Complex Safety-critical System Engineering
- AVACS - Automatic Verification and Analysis of Complex Systems
- smartspace® - smart man-vicinity communication in embedded systems
- etc.

5.3. Andreas Hoffmann, Axel Rennoch, Ina Schieferdecker, FhG-Institut FOKUS Berlin: Modellgestütztes Testen komplexer Systeme

Introduction

The paradigms for system development have significantly changed over time starting from step-wise procedural refinement paradigm to the model (transformation) paradigm as depicted in the figure below. The goal for modern test development is to adopt the modelling paradigm also for testing.



Due to the increasing complexity, concurrency and dynamics of today's software systems, software quality becomes a key factor for the success of a software product. Software quality has many different aspects such as functionality, performance and scalability of the software product but also availability, reliability, maintainability, etc.

Testing is the mean to obtain an objective quality metrics about a system in its target environment. In addition, it is the central mean to relate the system's requirements and specification to the real implemented and running system. The main objectives of testing can be summarised as follows:

- To gain confidence in the quality of the developed system and to show how well it works,
- To identify faults (defects) which cause the malfunctioning as early as possible, and
- To assess the risks of software defects remaining in the software system after its deployment.

Exhaustive testing of complex software systems is impractical due to the size of the input space. Thus, many approaches have been developed in the last decades:

- Coverage-based testing relies on coverage criteria for control and data flow graphs. It defines sub-domains where only a representative of each sub-domain is chosen in order to cover the system space.
- Fault-based testing uses a fault model and generates tests to check for these system faults only.
- Statistical testing uses probability distributions to capture usage patterns of the system under test.

- Evolutionary testing uses an optimization criteria and a genetic algorithm to mutate an initial test input set for optimal test results.

Goals and Concepts of Model-based Testing

In the recent years new approaches using models for the test development process have been developed:

- Model-based testing is a system-model-based approach where test data and test procedures are derived from a system model describing selected structural and (non-) functional aspects of a system under test (SUT).
- Model-driven testing uses test models to guide the test process and to derive test cases from iteratively refined test models. It can be understood as the application of MDA (Model Driven Architecture defined by the Object Management Group) to test development.

The goal for using models for testing is to support:

- Automation for test design, test specification, test execution, test synthesis,
- Better integration of the test process into the overall system development process,
- Reusing information from system models (if available).

The reuse of information from system models allows for deriving:

- The test matter, in particular the test behavior, system input and expected output, evaluation of output and the overall test,
- The architecture of the test system, i.e. the interface between the test system and the SUT, the execution method of test system, and the internal architecture of test system.

Selected Techniques for Test Modelling

TTCN-3 (Testing and Test Control Notation) is a standardised notation developed by a large group of international test experts for implementation-independent test models. It also supports and controls automated local, remote and distributed test execution. It is suitable for many kinds of testing such as

- System and integration testing,
- Conformance and interoperability testing,
- Scalability / load, performance, robustness and regression testing.

TTCN-3 is applicable for black-box testing for reactive and distributed systems in many domains such as

- Telecom systems (ISDN, ATM, Parlay)
- Mobile (telecom) systems (GSM, GPRS, UMTS, TETRA, WiMAX)
- Internet (IPv6, SIP, IMS, SIGTRAN)
- Middleware platforms (CORBA, CCM, EJB, Web Services, OSCI)
- Embedded systems (automotive, avionics, space, SmartCards)
- Programming interfaces (Java, XML)

TTCN-3 is also used for standardised test suites such as Autosar, WiMAX, SIP, IPv6, etc.

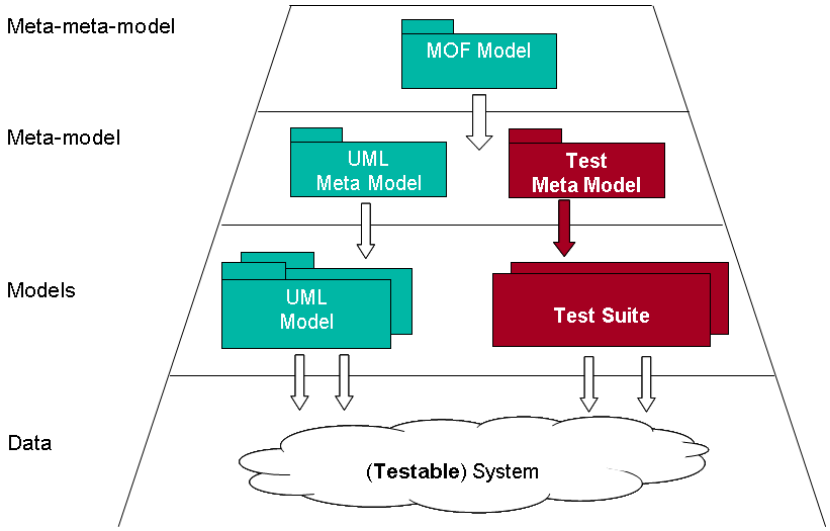
The UML2 Test Profile has been defined by a large group of international test experts at the Object Management Group. It extends the Unified Modeling Language (UML2) with dedicated test concepts. The goals of the test profile are:

- To allow black-box testing (i.e. at UML interfaces) of computational models in UML,
- To enable the test definition and test generation based on structural (static) and behavioral (dynamic) aspects of UML models, and

- Specification of test purposes and test cases in an implementation independent manner.

Model-Driven Architecture

Model Driven Architecture (MDA) is the new OMG architecture for system development. MDA defines an approach to separate system functionality specification from specification of implementation of that functionality on a specific platform. It is mainly based on base technologies such as MOF, UML, OCL, CWM and QVT. The MDA approach defines a stepwise refinement of models from platform-independent level down to platform-specific models. The transformation between models is based on meta-models and realised by model transformers. The figure below shows the different modelling levels for system and test modelling according to the MDA approach.



The aim of the MDA approach (with dedicated extensions for testing) is to apply modelling methods and tools to integrate system and test development as well as to develop system engineering tools running in a common environment that ensure consistent artefacts for the system and test (anti-) system.

The major benefits of MDA are:
- Language-, vendor- and middleware neutral,
- Scalability, robustness, security, implemented in the best possible manner,
- Reduced costs from beginning to end,
- Increased re-usability through model repositories,
- Reduced development time for new applications,
- Smooth integration across middleware platform boundaries.
- Rapid inclusion of emerging technologies into existing systems

Conclusion

- What you should NOT expect from Model-based Testing
  - Exhaustive testing: “Generated test case are enough, nothing else is required”
  - Complete automation: “Push only one button to finish test”

- Efficiency of test modelling

  - You can express “meaning” of test case
  - You can reuse the test
  - You can execute the test

- Efficiency of test derivation
  - You can get appropriate test system architecture for SUT
  - You can do testing before the details of SUT have been developed
  - You can execute basic features of SUT automatically

- Early integration of testing into the development process is essential

- TTCN-3 is a standardised test technology that supports
  - Platform-independent testing of systems in several industrial domains
  - Automated test execution
  - Tools are ready for use, e.g. www.testingtech.de (free evaluation copy downloadable)
- The UML2 Test Profile introduces dedicated test concepts into the UML2 language (family).

Contacts

Test Solutions @ FOKUS
Andreas Hoffmann
Tel.: +49 – (0)30-3463-7392, Fax: -8392
Email: andreas.hoffmann@fokus.fraunhofer.de
Web: http://www.fokus.fraunhofer.de/motion/

Prof. Ina Schieferdecker
Tel.: +49 – (0)30-3463-7241, Fax: -8241
Email: ina.schieferdecker@fokus.fraunhofer.de

6. Ergebnisse middleware-Workshop

6.1. Prof. Petra Sauer, TFH FB Informatik Berlin: Informationsintegration in heterogen verteilten Datenbanken im BAER-Projekt

Abstract:

Die heutige Zeit ist mehr denn je den Anforderungen ausgesetzt, Massendaten zu persistieren. Diese Daten liegen zumeist in unterschiedlichsten Datenmodellen und Datenquellen vor. So wird vor allem das relationale und das XML- Datenmodell für die Datenhaltung bzw. als Austauschformat verwendet. Besteht nun der Bedarf Daten aus heterogenen Datenmodellen oder Datenquellen zu integrieren, sind zahlreiche Probleme zu lösen. An diesem Punkt setzen so genannte Integrationssysteme an, die von der eigentlichen Datenverteilung abstrahieren. Die in dieser Arbeit besprochene Integrationsschicht eXIIL[5] verwendet zur Steuerung der transparenten Informationsintegration eine austauschbare XML-Konfigurationsdatei.

Einführung:

In der Forschung haben sich in den letzten Jahren diverse Verfahren etabliert, die darauf abzielen differente Datenquellen kohärent zu integrieren. Abhängig von der Art der Integration und der verwendeten Architektur des Integrationssystems resultieren verschiedene Integrationsszenarien.

Am Beispiel des Datenhaltungskonzepts im interdisziplinären, EFRE-geförderten Forschungsprojekt BAER der TFH Berlin werden projektbezogen relevante Integrationsszenarien vorgestellt. Heterogene Datenbestände aus heterogenen Datenmodellen sind hier integriert zu verarbeiten. Inhaltlich betrifft dies Datenbestände der Tier- und Pflanzenarten, Daten der Infrastruktur eines Zoologischen Gartens einschließlich der verschiedenen Gebäude- und Gehegearten, Daten der Futtermittelbestellung und –bewirtschaftung, Messdatenreihen von Boden-, Wasser- und Luftuntersuchungen sowie verschiedene externe Datenbestände wie Tierstammbäume, Daten des Artenschutzprogrammes etc. Die verwendeten Quelldatenmodelle sind relationale, XML-Datenbanken sowie Excel-, Word-, CSV-Dateien etc. Als Zieldatenmodell wird das objektrelationale Modell eingesetzt. Zur Integration wird das in diesem Beitrag besprochene Integrationssystem eXIIL verwendet.

Informationsintegration mit der objektorientierten Integrationsschicht eXIIL:

eXIIL verwendet zur Steuerung der Anfrageabarbeitung für die Datenintegration heterogener Datenquellen eine XML-Konfigurationsdatei und wird über eine API angesprochen. Die Datenebene wird von der Anwendungslogik entkoppelt, in dem eine weitere Schicht in Form eines objektorientierten globalen Schemas der Systemarchitektur hinzufügt wird. Die Integrationsschicht ist als konsequente Weiterentwicklung der 3-Schichten-Architektur monolithischer Datenbanken zu verstehen.

eXIIL ist durch die externe XML-Konfiguration in der Lage, Datenbasen verschiedener Datenmodelle konsistent anzufragen und zu integrieren. Als kanonisches Datenmodell verwendet die Integrationsschicht eine Instanz des XQuery 1.0/XPath 2.0-Datenmodells

(XDM). Abschließende oder vorbereitende Integrationen werden über XSLT oder XQuery definiert.

Da eXIIL keine regelbasierte, Datenquellen übergreifende Anfrageplanung bzw. –optimierung unterstützt, trägt der Entwickler die Verantwortung die für die Anwendung benötigten Globalen

[5] eXIIL steht für eXchangeable InformationIntegration Layer.

Anfragen, durch Selektion passender lokaler Datenquellen zu realisieren. [LN06] sprechen in diesem Fall von canned queries. Dieses Verfahren erleichtert die Einbeziehung von eXIIL in den bestehenden Kontext einer Anwendung, da die Entwickler keine Kenntnis über den Strukturen oder die Anzahl der beteiligten Datenquellen benötigen. Die in der eXIIL-Konfiguration definierten Anfragen stellen gewissermaßen die Schnittstelle zwischen dem Datenbank- und dem Anwendungsentwickler dar.

Der große Vorteil der abstrahierenden Schicht liegt darin, das globale Datenunabhängigkeit geschaffen wird. Ähnlich wie das externe Schema in einer relationalen Datenbank von der konzeptuellen Ebene abstrahiert, entsteht durch die Inklusion eines Globalen Schemas (4. Schicht) Verteilungstransparenz. Zwischen der Anwendung und den beteiligten Datenbasen entsteht eine lose Kopplung. Bei einer etwaigen Redistribution der Datenbasen ist lediglich das XML-Konfigurationsskript auszutauschen. Die Anwendungslogik des anfragenden Softwaresystems bedarf keiner Reimplementierung oder Rekompilierung.

Zusammenfassung:

Informationsintegration ist ein komplexer Prozess. Die Autoren haben mit der eXIIL-Integrationsschicht gezeigt, dass höchst heterogene Datenquellen kohärent im Sinne verschiedener Anwendungsszenarien integriert werden können. Weitere Arbeiten widmen sich der Hinzunahme strukturierter Anfragen an das Integrationssystem, durch die weitere Flexibilität bezüglich der konkret von einer Anwendung benötigten Daten geboten wird.

Literaturverzeichnis:

[LN06] Leser, Ulf.; Naumann, Felix: Informationsintegration. Dpunkt-Verlag, 3-89864-400-6, Heidelberg, 2007.

Referenten:

Prof. Dr. Petra Sauer ist Professorin für Informatik, insbesondere Datenbanken, an der Technischen Fachhochschule Berlin. Sie leitet das Teilvorhaben Datenhaltung im Forschungsprojekt BAER. Ihr Forschungsfokus liegt vor allem auf dem Datenbankentwurf sowie den X-Technologien.

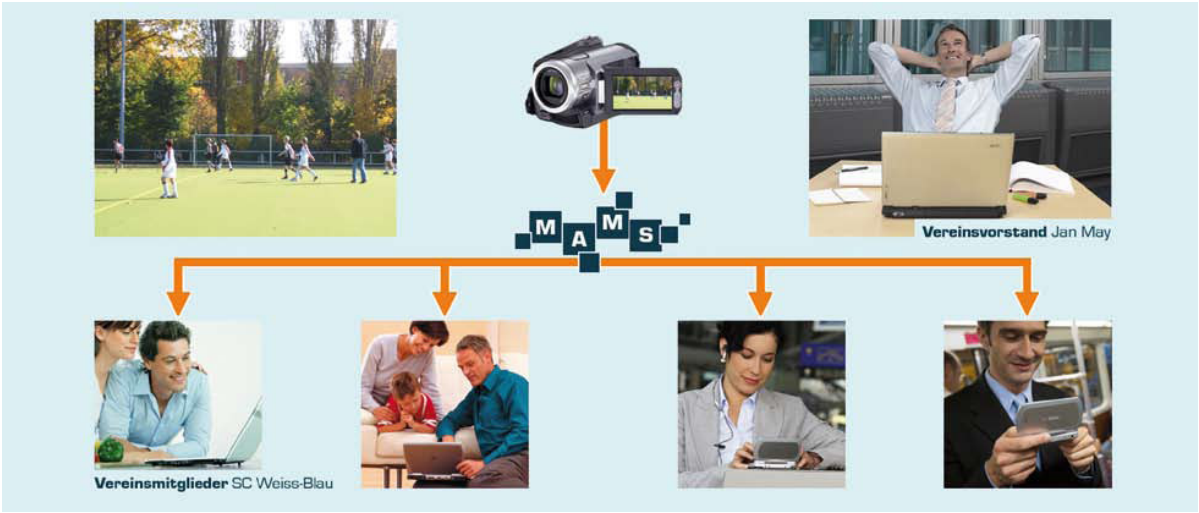
Dipl.-Inform. (FH) Marc-Florian Wendland ist derzeit Student im Masterstudiengang Informatik an der Technischen Fachhochschule Berlin und war Mitarbeiter im Forschungsprojekt BAER. Derzeit ist er Hilfswissenschaftler im Fraunhofer-Institut FOKUS. Sein Interessengebiet umfaßt die X-Technologien sowie Informationsintegration.

6.2. Dr. Horst Stein, Deutsche Telekom Laboratories: MAMS – Individuelle Dienste für Jedermann

Im Rahmen des vom BMBF-geförderten Projektes wird ein Multi-Access Modular-Services Framework (MAMS) entwickelt, welches es Nutzern ohne Programmierkenntnisse ermöglicht, eigene IKT-Dienste zu erstellen und zu betreiben.

Vision:
Unternehmen nutzen zunehmend Informations- und Kommunikationstechnologien (IKT), um interne Geschäftsprozesse zu unterstützen, ihre Wertschöpfungsketten zu erweitern oder neue Marktanteile zu gewinnen. Damit werden aber auch die eingesetzten IKT immer komplexer. Insbesondere kleine und mittlere Unternehmen (KMU) wollen neue Ertragsquellen erschließen ohne immer wieder zusätzliche Kosten in IKT Services zu investieren oder eigene IKT Kompetenzen aufbauen zu müssen.

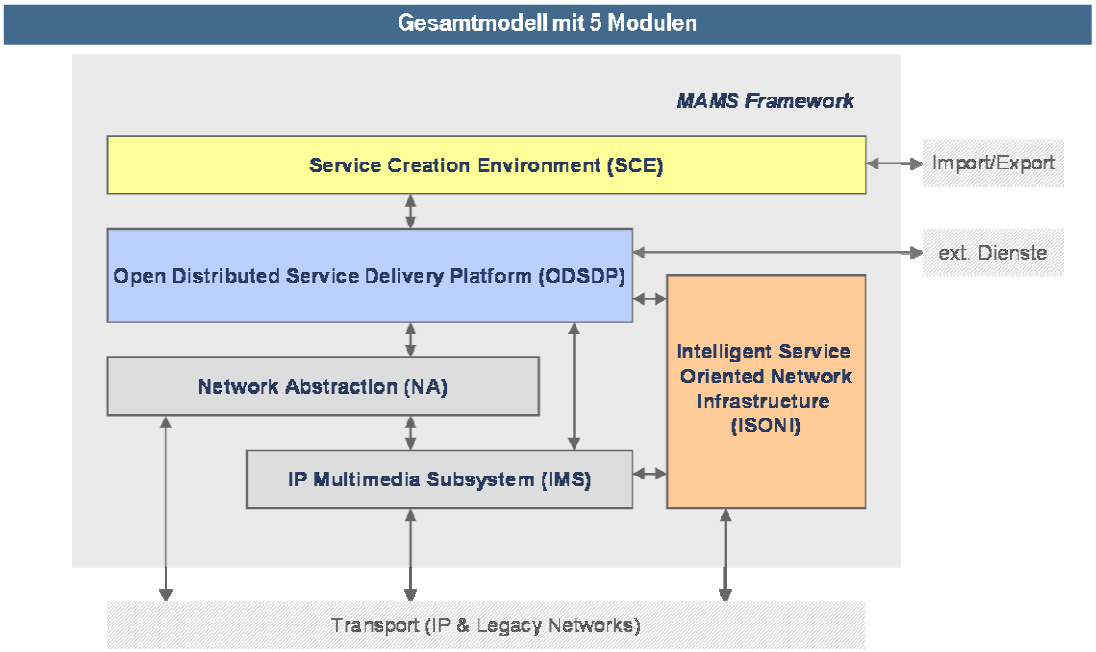
Das Multi-Access Modular-Services Framework (MAMS) ist ein Entwicklungs- und Produktionssystem für IKT Dienste, das auf Basis vorkonfigurierter IKT Basisdienste und telematischer Infrastrukturen Benutzern ohne Programmierkenntnisse die Entwicklung, Zusammenstellung und Aktivierung von eigenen Diensten ermöglicht.



Als innovativer Schwerpunkt des BMBF-geförderten Projektes wird ein Framework mit einer grafischen Benutzeroberfläche und entsprechenden Entwicklungswerkzeugen bereitgestellt. Es erlaubt auch Nutzern ohne spezielle Fachkenntnisse der Informations- und Kommunikationstechnik, Kommunikations- bzw. Multimediadienste zu entwickeln und für ihre Kunden zu betreiben.

Wichtiges Forschungsziel ist das koordinierte Zusammenspiel und das Management der einzelnen Dienste.

Aufbau der Plattform:
Die Service Creation Workbench (SCW) stellt den Kunden von MAMS eine Entwicklungs-Umgebung bereit, in der mit graphischen Werkzeugen individuelle Dienste erstellt werden können. Ein Dienst kann dabei aus vorgefertigten Basisdiensten in einer intuitiv bedienbaren Oberfläche zusammengefügt und konfiguriert werden.



Die Open Distributed Service Delivery Platform (ODSDP) ist die Ausführungsumgebung für die im oben beschriebenen SCW erzeugten Dienste. Sie steuert die Umsetzung der Dienstlogik und die Ausführung der Basisdienste mit den angegebenen Konfigurationen.

Als Basisdienste werden einfache oder komplexe Telekommunikations- oder Multimediadienste (z.B. Streaming Service, Konferenzdienste, Messaging Service) bereitgestellt.
IP Multimedia Subsystem (IMS) und Intelligent Service Oriented Network Infrastructure (ISONI) stellen Kontroll- und Managementfunktionen für den Transport der Daten dar. Sie ermöglichen die Ausführung von Diensten unabhängig von Technologien und Protokollen der darunter liegenden Kommunikationsnetze (z.B. Mobilfunknetze, Festnetz). Die ISONI ist eine Dienstplattform, die auf verteilten, rekonfigurier- und programmierbaren Servern basiert.

Anwendungsschwerpunkt Gesundheit
Im Gesundheitsbereich, in Rehabilitation und Nachsorge, besteht eine wesentliche Medizinische Einrichtungen wie Reha-Kliniken, Krankenhäuser und ärztliche Praxen verbessern ihre bisherigen Versorgungsangebote künftig mit neuartigen IKT-gestützten Prozessen. Diese Prozesse eröffnen einen neuen Informations- und Kommunikationsraum für eine effektive und nachhaltige Sekundärprävention, die in der Regel in der Reha-Klinik beginnt.