Modellbasiertes Sicherheits- und Compliance-Management

Prof. Dr. Jan Jürjens

Fraunhofer-Attract-Gruppe „Apex“

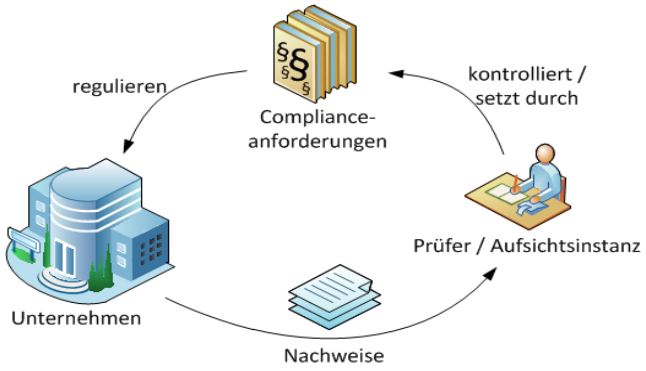
Fraunhofer-Institut für Software- und Systemtechnik ISST, Dortmund

Fraunhofer ISST

http://www.isst.fraunhofer.de/de/geschaeftsfelder/it-compliance-fuer-die-industrie.html

http://jan.jurjens.de

Steigende Bedeutung von Regulierungen



Beispiele:

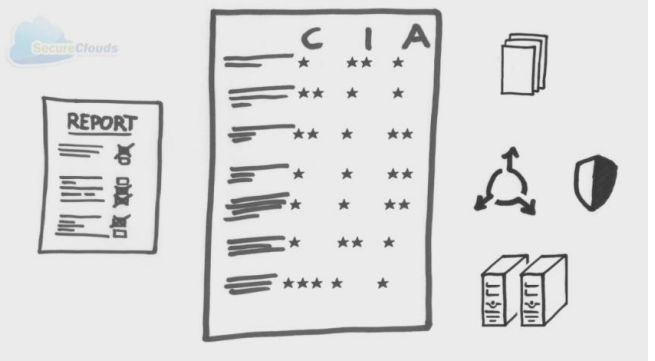
- **Versicherungen**: Solvency II (bis 2016), MARisk VA
- **Banken**: Basel III (bis 2018), MARisk BA
- **Gesundheit**: Medizinproduktegesetz (MPG)
- **Pharma**, **Lebensmittel**: Arzneimittelmarktneuordnungsgesetz (AMNOG), Good Manufacturing Practices (GMP, US Food & Drugs Admin. (FDA))

Branchenunabhängig:

- Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (**KontraG**); US: **Sarbanes-Oxley**
- **Bundesdatenschutzgesetz** (BDSG)
- IT-Sicherheit (**BSI-Grundschutz**)

90 % Unternehmen: **min. 3 Compliance-Programme** erfüllen (IDC 2007).

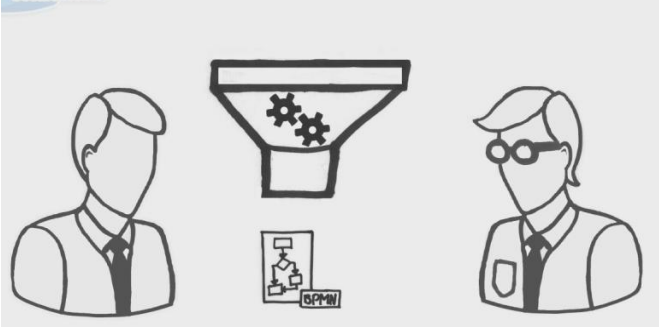
Herausforderung Compliance



- **Steigende Anzahl** / **Verzahnung** zu prüfender Vorgaben (ggf.: bedingen einander / stehen im Widerspruch).
- Audit **regelmäßig wiederholen** => änderungsbasierte Analyse
- Erforderliche Daten schwer manuell erfassbar => **Erfassung** der Daten **automatisieren**.
- **Prüfung** einzelner Eigenschaften bereits so **komplex** / umfangreich, dass manuell nicht durchführbar => Werkzeuge benötigt.
- **Aggregation** verschiedener Vorgaben bei komplexen IT-Systemen.
- **Verteilung** von Unternehmen über verschiedene Standorte
- **Anbindung** von Lieferanten bzw. Partnern
- Nutzung von **Cloud-Computing** o.ä.

O.g. Herausforderungen können zusammen auftreten / sich potenzieren.

Werkzeuge für Compliance-Management



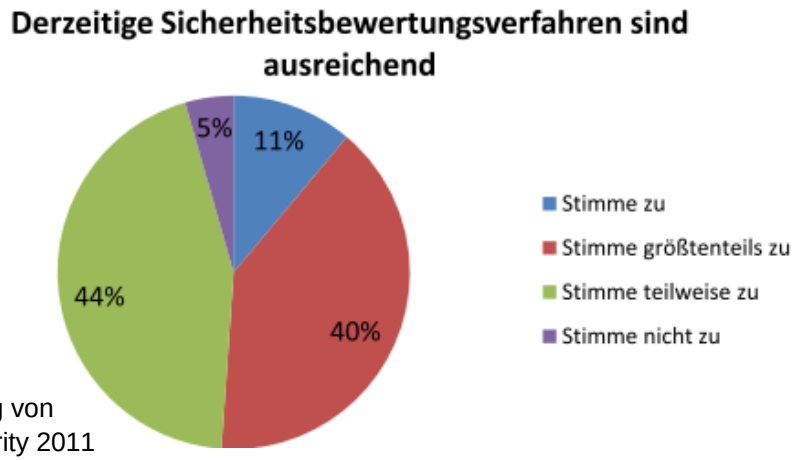
Manueller Nachweis aufwendig und kostenintensiv.

⇒ Großer Bedarf an **Compliance-Werkzeugen** (1,3 Mrd.$ / Forrester 2011).

Werkzeuge: bislang i.W. manuelle Dokumentation von Compliance-Prozess.

Schwachpunkte:

- **Integration** mit IT-Infrastrukturen der Unternehmen für Geschäfts- und Produktionsprozesse (=> Daten z.B. für Nachverfolgbarkeit von Transaktionen / Produktbestandteilen).
- **Überwachung** von Compliancevorgaben an IT (z.B. Sicherheit dieser Daten; Schutz personenbezogener Daten (BDSG)).
- Integration effektiver **Kontrollsysteme** (Risiken / Missbrauch verhindern).
- Derzeitige **Risiko-Bewertungsmethoden** nicht ausreichend.[1]



[1] S. Taubenberger, J. Jürjens: Durchführung von IT-Risikobewertungen und die Nutzung von Sicherheitsanforderungen in der Praxis. Studie, Fraunhofer ISST 2011 und DACH security 2011

Fraunhofer ISST

Mission Statement: Werkzeuggestütztes Compliance-Management

Ziele:

- Bessere **Überprüfbarkeit** / Nachvollziehbarkeit für Compliance-Nachweis.
- **Kostenersparnis** durch Werkzeugunterstützung und Integration mit Aktivitäten im Bereich Qualitätssicherung und Risikomanagement.

Idee:

- Entwicklung automatischer Werkzeuge: **Management und Analyse** von **Compliance-Anforderungen** auf Basis von vorhandenen Artefakten:
  - Textdokumente, Software-/Geschäftsprozess-Modelle, Log-Daten...
- **Expertensystem für Compliance**
- Insbesondere auch Anwendung auf Einsatz von **Clouds**[1] (secureclouds.de).
- Berücksichtigung **ökonomischer Aspekte** (seconomicsproject.eu)

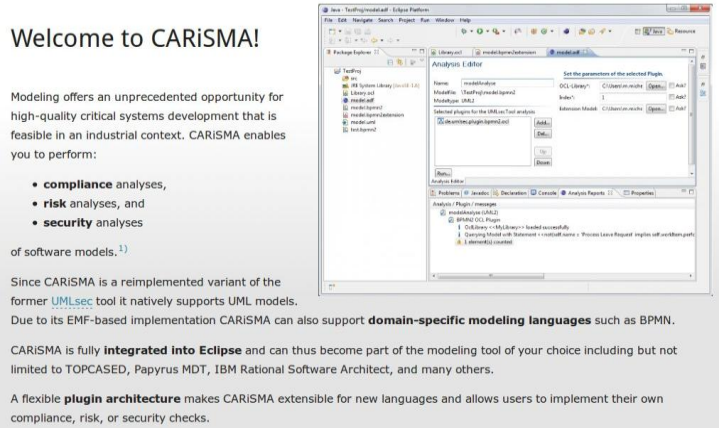
Compliance-Report

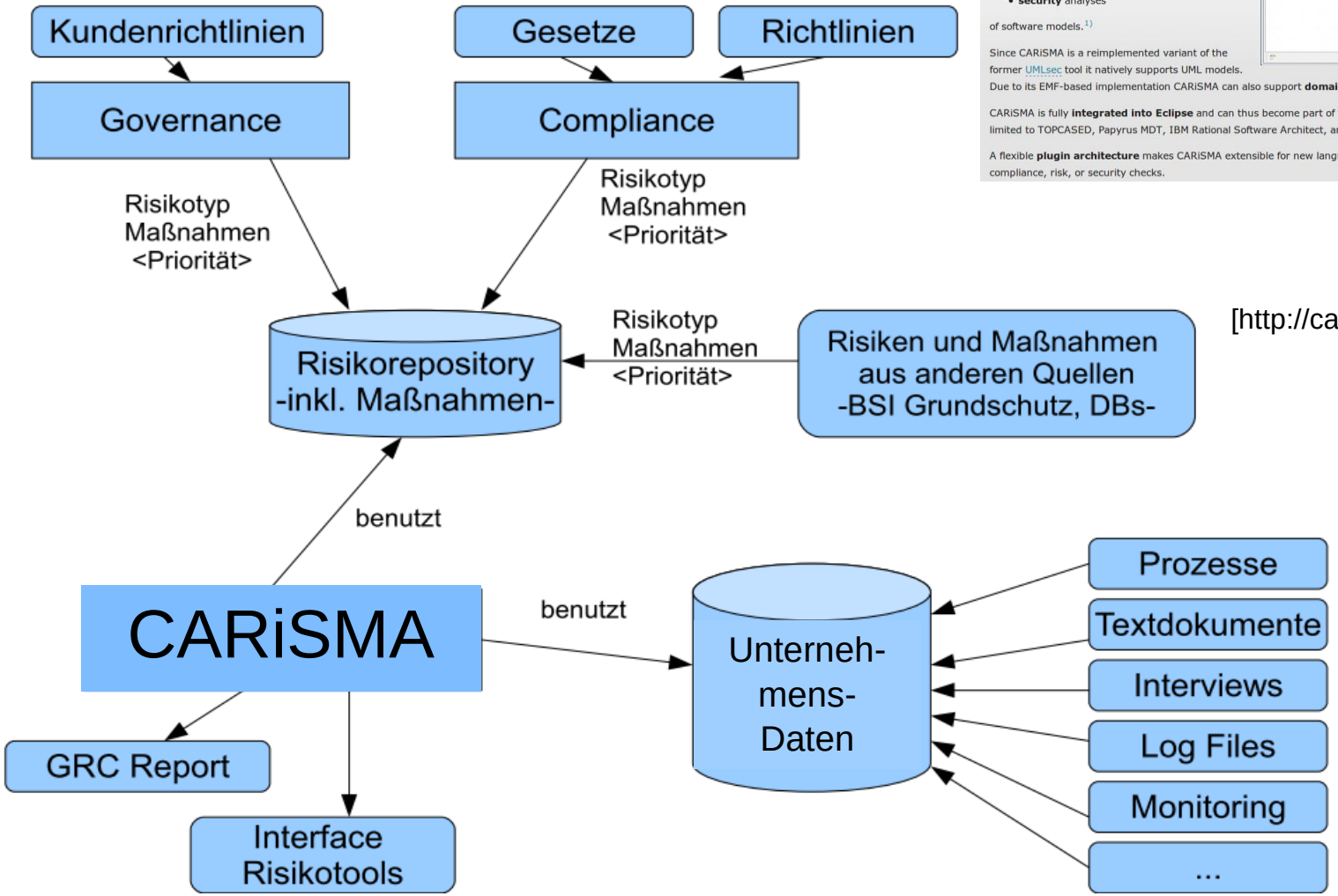
Compliant: NEIN
Verstöße:
- MaRISK VA 7.2: Einhaltung von BSI G3.1 nicht erfüllt
Maßnahmen:
- BSI Maßnahmen-katalog M 2.62

[1] S. Wenzel, C. Wessel, T. Humberg, J. Jürjens, Securing Processes for Outsourcing into the Cloud, 2nd Int. Conf. on Cloud Computing and Services Science (Closer 2012)

Fraunhofer ISST

Werkzeugunterstützung: Workflow





[http://carisma.umlsec.de]

Fraunhofer ISST

Vorgehen (1): Von Compliance zur IT

Jürjens et al., Journal on Software and System Modeling 10(3): 369-394 (2011)

MaRisk VA

7.2 (2) Materiell bedeutsame Einzelentscheidungen und Anweisungen von Führungsebenen unterhalb der Geschäftsleitung, die gegen die innerbetrieblichen Leitlinien verstoßen, sind schriftlich zu begründen, zu dokumentieren und der Geschäftsleitung zur Kenntnis vorzulegen.

Anforderungen an GP-Modelle ableiten

Werden angewendet auf

Werkzeug-Repository: formalisierte Compliance-Anforderungen

Dann: Begründung für Unterschrift dokumentieren

d:Unterschrift

Wenn: Ausnahme von innerbetrieblicher Leitlinie

d:Aushändigung

Unterschrift durch Sachbearbeiter

Unterschrift durch Unterschrifts-berechtigten

Dokumentation über Begründung für eigene Unterschrift schreiben

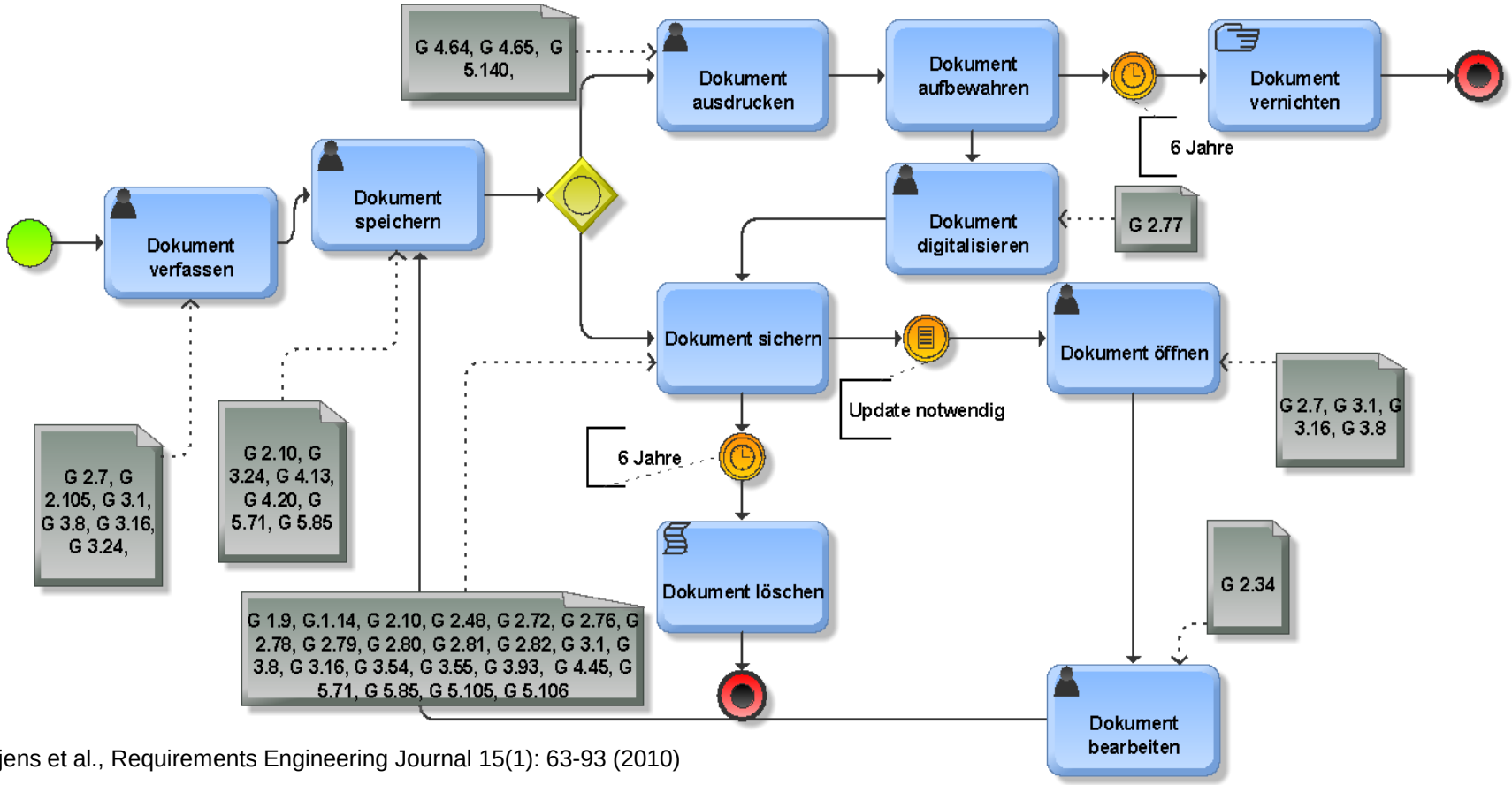
Rechtsgültiger Vertrag liegt vor

Aushändigung des Vertrags

Fraunhofer ISST

Vorgehen (2): Berücksichtigung von Standards

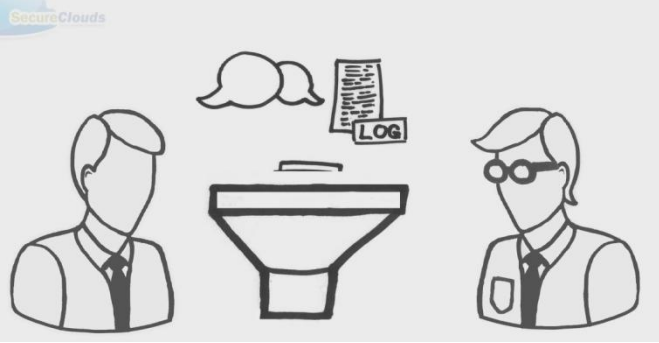
Automatische Annotation von GP-Modellen mit Risiken anhand BSI-Grundschutzkatalog:



Jürjens et al., Requirements Engineering Journal 15(1): 63-93 (2010)

Fraunhofer ISST

Vorgehen (3): Modell-basierte Compliance-Analyse



- **Strukturanalyse** eines Geschäftsprozesses auf Basis von Compliance-Mustern
- Beispiel: Für jedes Auftreten eines Vertragsabschlusses wird 4-Augen-Prinzip überprüft.

```
formula four\_eyes\_principle ( a1 : activity , a2 : activity ) :=
forall [ p:person | ( !(execute(p, a1)) \/ !(execute(p, a2)) ) ];
```

Jürjens et al., Int. Journal on Intelligent Systems 25(8): 813-840 (2010)

Fraunhofer ISST

Ausgabe/Ergebnis

Relevante Pattern je Aktivität

- Numerische **Bewertung der Relevanz**

Aktivität

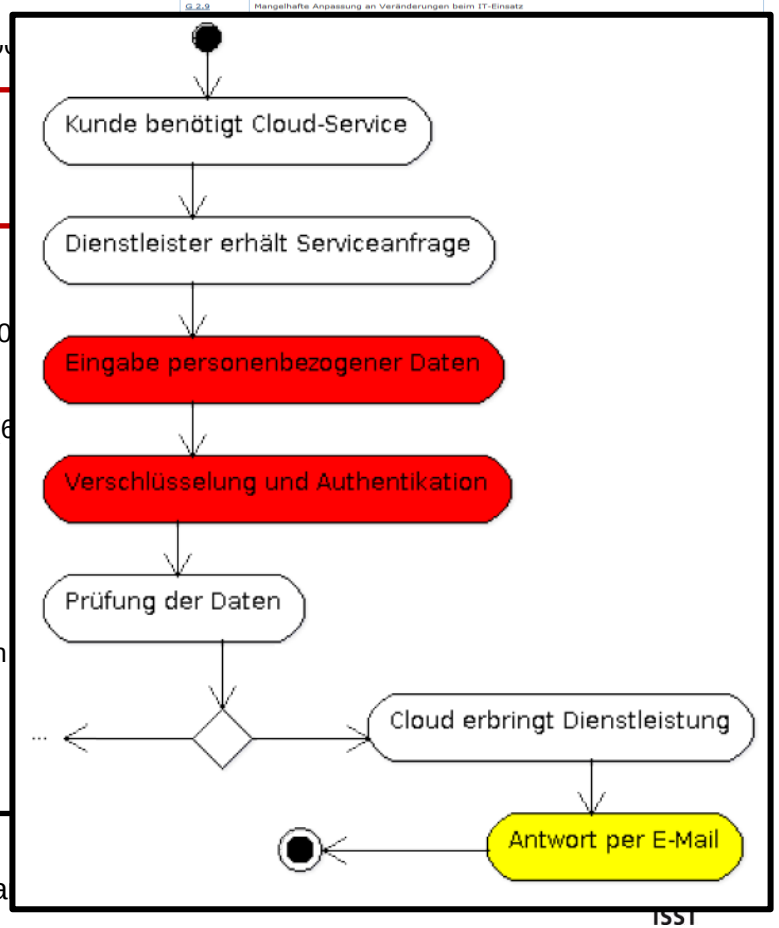
[Kunde benötigt Cloud-Service (233)]
4 Relevante Worte: [Information(200.0), Meldung(200.0), Nachricht(200.0), Internet(10
22 relevante Pattern:
B_5.10 : Internet Information Server (300.
G_2.96 : Veraltete oder falsche Informatio einem Webangebot (200.0)
G_3.13 : Weitergabe falscher oder inte
G_3.44 : Sorgl sigkeit im Umgang mit
…

Identifizierte Ausdrücke

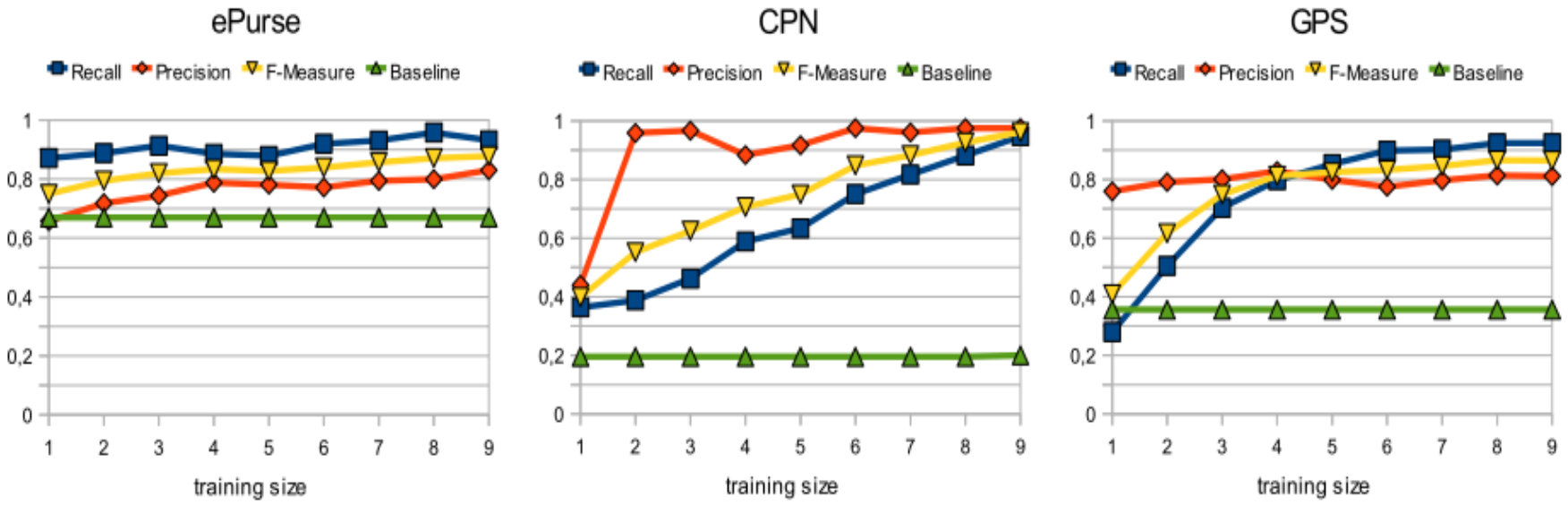
[Dienstleister erhält iceanfrage (600)]
7 Relevante Worte: [D ister(500.0), E-Mail(500.0), Information(100.0), Internet(10
16 relevante Patter
G_1.19 : Ausfall er Zulieferers (600.0)
G_2.84 : Unzulä gelungen mit einem externen Dienstleister (6
…

Gefundene Pattern

[Kunde gibt Daten ein (667)]
19 Relevante Worte: [Daten(500.0), Datei(200.0), Information(200.0), Meldung(200.0),
59 relevante Pattern:
M_2.205 : Übertragung und Abruf personenbezogener Daten (700.0)
M_4.64 : Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von
B_1.15 : Löschen und Vernichten von Daten (600.0)
G_2.61 : Unberechtigte Sammlung personenbezogener Daten (600.0)
G_4.13 : Verlust gespeicherter Daten (600.0)
…



Textbasiertes Risiko-Mining: Experimentelle Resultate



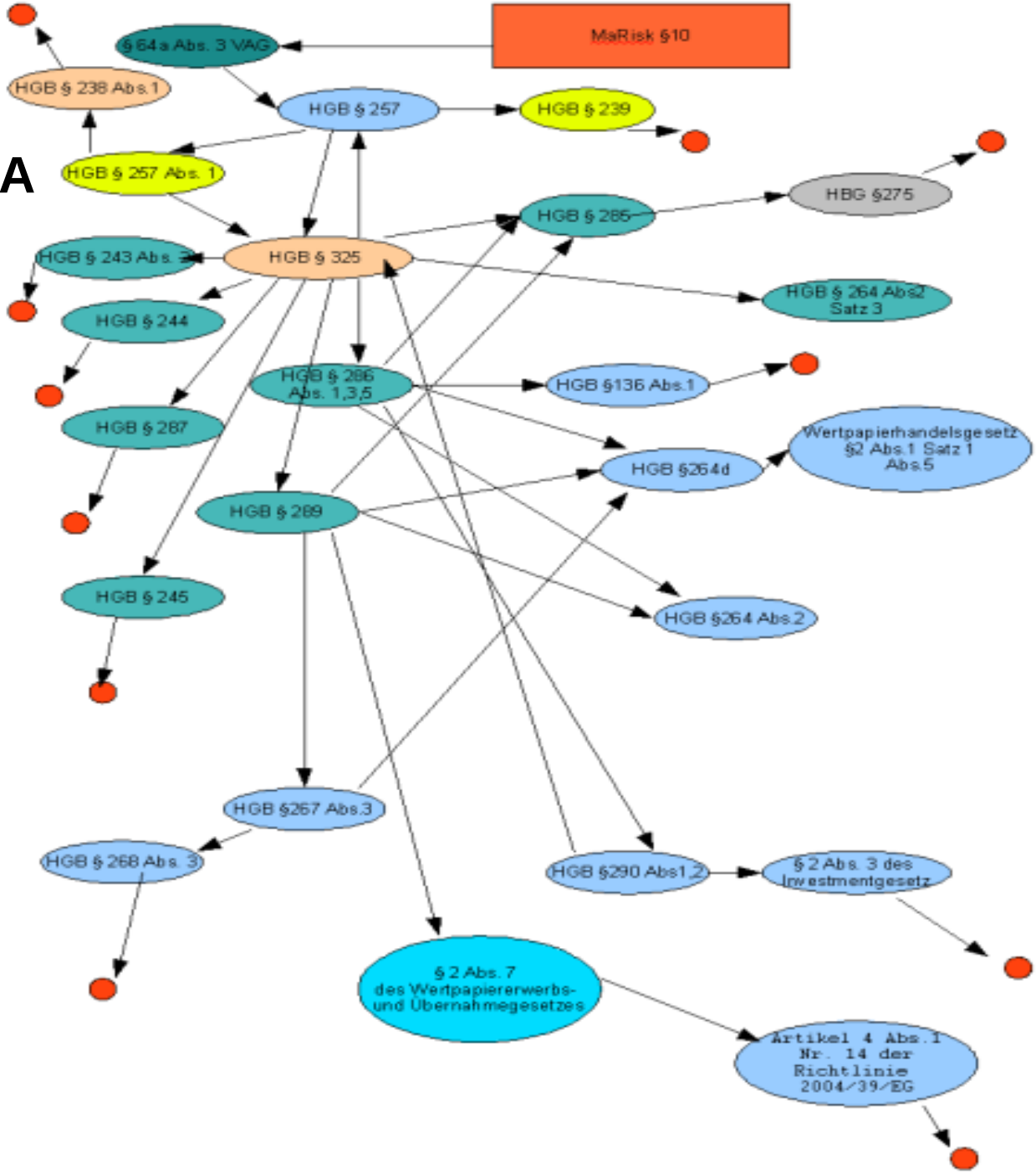
- Industrielle Anforderungsdokumente
  - Common Electronic Purse Specifications (ePurse)
  - Customer Premises Network specification (CPN)
  - Global Platform Specification (GPS)
- Metriken für Information Retrieval:
  - Recall: Trefferquote
  - Precision: Genauigkeit
  - F-Measure: Kombination P&R
  - Baseline: Alle Anforderungen als security relevant klassifiziert

K. Schneider, E. Knauss, S. Houmb, S. Islam, J. Jürjens: Enhancing Security Requirements Engineering by Organisational Learning. In: Requirements Engineering Journal (REJ)

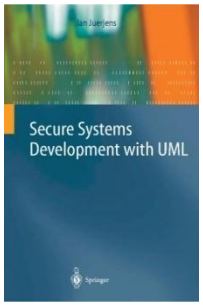
Fraunhofer ISST

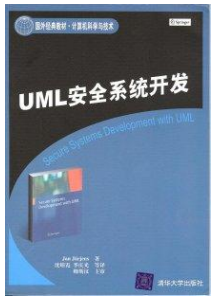
Beispielergebnis: Abbildung MA-Risk VA auf Sicherheits-anforderungen

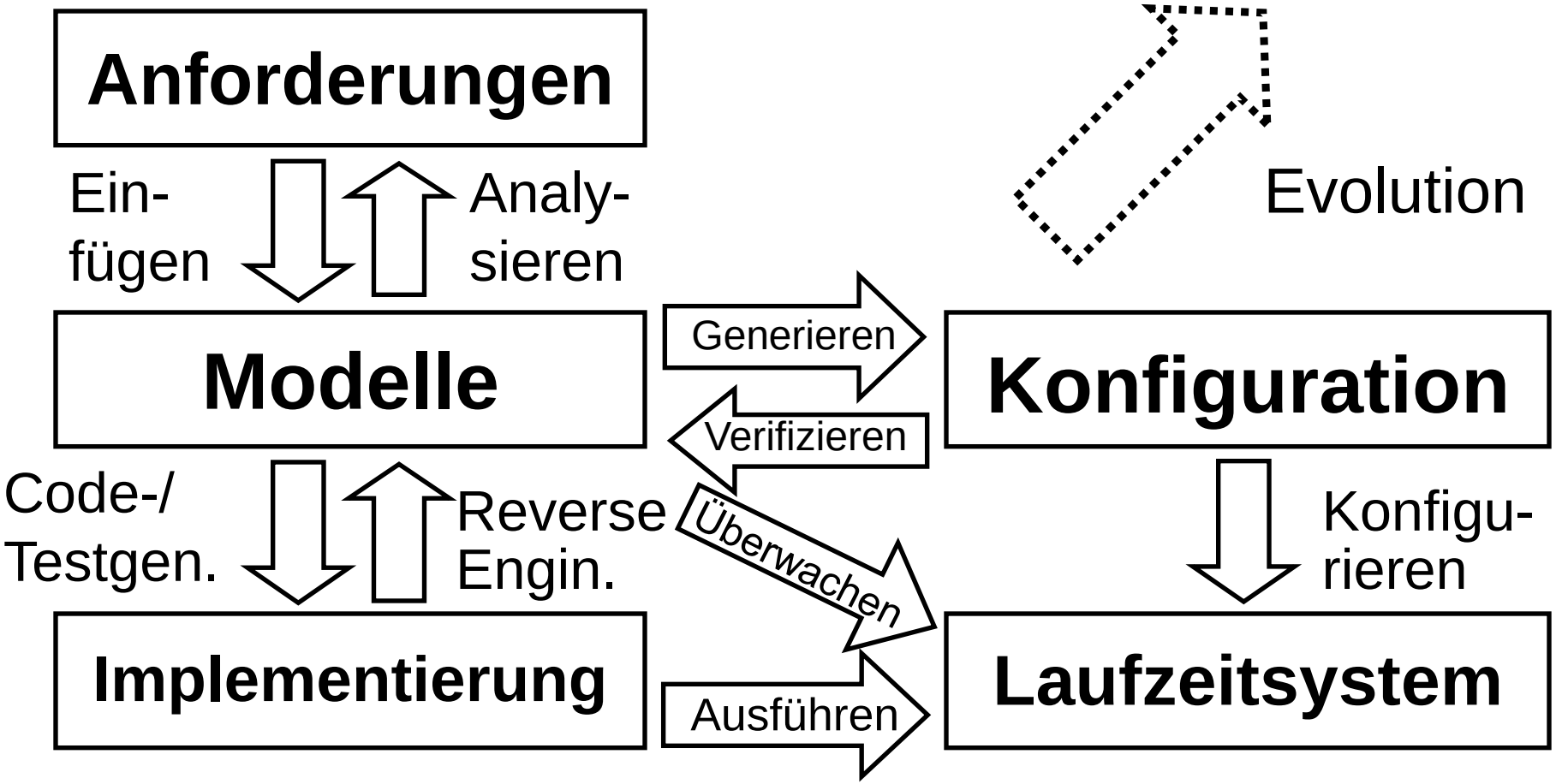
- Framework zur Abbildung von **regulatorischer Compliance** auf **Security Policies**
- Berücksichtigung von **Cross-References** ausgehend von MA-Risk VA



Wissenschaftliche Grundlage: Modellbasiertes Compliancemanagement



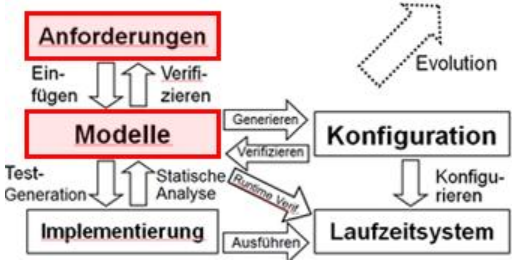




[Jan Jürjens: Secure systems development with UML. Springer 2005. Chines. Übers. 2009]

Fraunhofer ISST

Modellbasiertes Compliancemanagement: Automatische Modellanalyse



Beispiel: Überprüfung von Softwareservice auf Complianceeinhaltung.

Formalisierung der Modellausführung. Gegeben: Statechart-Transition $t=(source,msg,cond[msg],action[msg],target)$ und erhaltene Nachricht m.

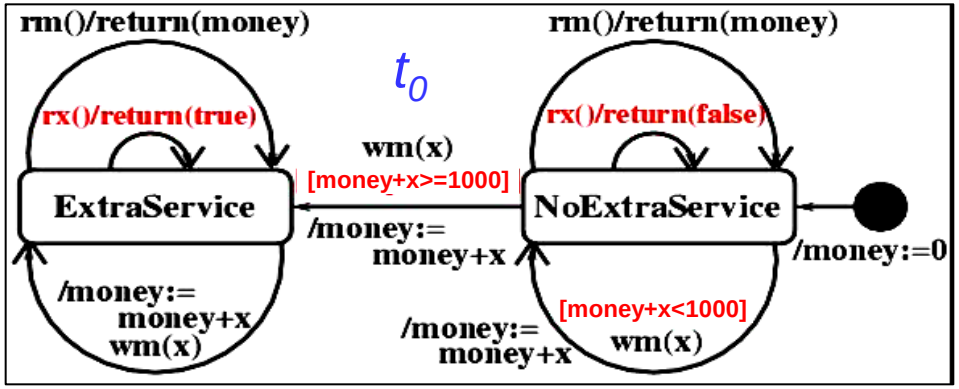
Formalisierung der Ausführung der Transition:

$$Exec(t,m) = [state_{current}=source \wedge m=msg \wedge cond[m]=true \Rightarrow action[m] \wedge state_{current.t(m)}=target\ ].$$

(wobei $state_{current}$ aktueller Zustand; $state_{current.t(m)}$ Zustand nach Ausführung von t mit Nachricht m).

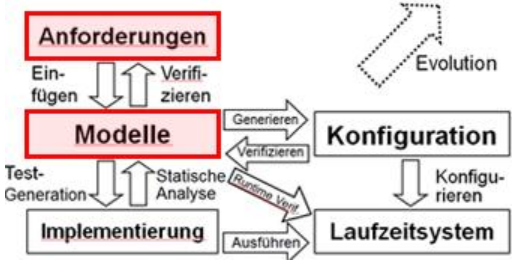
Beispiel: Transition t_0:

$$Exec(t_0,m)= [\ state_{current}=NoExtraService \wedge m=wm(x) \wedge money_{current}+x>=1000 \Rightarrow money_{current.t_0(m)}=money_{current}+x \wedge state_{current.t_0(m)}=ExtraService\ ].$$



Fraunhofer ISST

Modellbasiertes Compliancemanagement: Automatische Analyse der Compliance



Beispiel „sicherer Informationsfluss“:

Kein Informationsfluss von vertraulichem zu öffentlichem Wert.

Analyse: Wenn zwei Systemzustände $state_{current}$, $state'_{current}$ sich nur in den Werten der vertraulichen Attribute unterscheiden, darf ihr öffentlich beobachtbares Verhalten sich nicht unterscheiden:

$$state_{current} \approx_{pub} state'_{current} \Rightarrow state_{current.t(m)} \approx_{pub} state'_{current.t(m)}$$

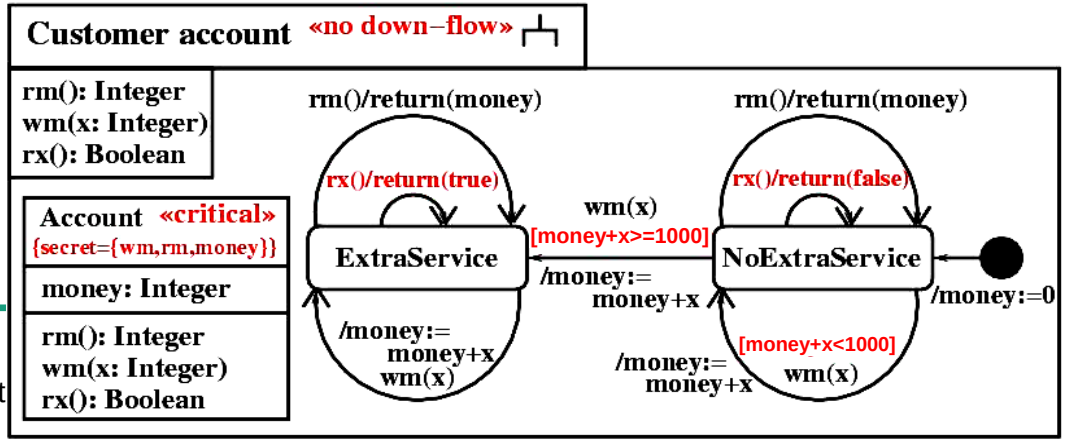
(wobei $state_{current} \approx_{pub} state'_{current}$ falls $state_{current}$ und $state'_{current}$ sich in ihrem öffentlich beobachtbaren Verhalten nicht unterscheiden).

Beispiel: Unsicher, weil vertrauliches Attribut *money* den Rückgabe-Wert der öffentlichen Methode *rx()* beeinflusst.

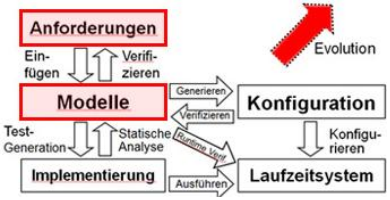
$ExtraService \approx_{pub} NoExtraService$

aber nicht:

$ExtraService.rx() \approx_{pub} NoExtraService.rx()$



Evolution vs. Design- / Architekturprinzipien



Betrachte Designtechniken und Architekturprinzipien, die Management von Evolution unterstützen.

Frage: Unter welchen Voraussetzungen bewahren sie Anforderungen ?

Designtechnik: **Verfeinerung von Spezifikationen.** Unterstützt Evolution zwischen Verfeinerungen einer abstrakten Spezifikation.

Architekturprinzipien: **Modularisierung** unterstützt Evolution, indem Auswirkungen auf Systemteile beschränkt bleiben.
Verschiedene Dimensionen:

[Ochoa, Jürjens, Warzecha: A Sound Decision Procedure for the Compositionality of Secrecy. ESSoS'12]

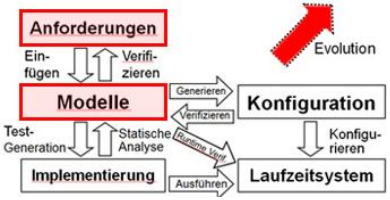
- Schichtung von **Architekturebenen**
- **Komponenten**-orientierte Architekturen
- **Dienst**-orientierte Architekturen
- **Aspekt**-orientierte Architekturen

Jeweils Resultate zu Bedingungen für Bewahrung von Anforderungen.

Im Folgenden am Beispiel von Sicherheitsanforderungen.

Fraunhofer ISST

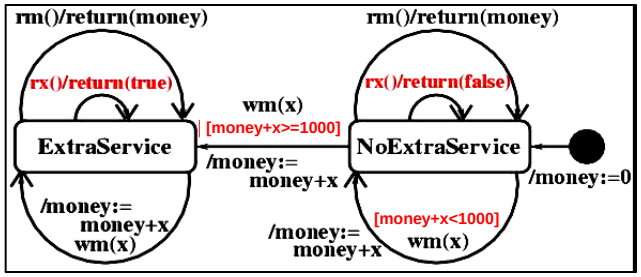
Designtechnik: Verfeinerung



Bei verhaltensbewahrender Verfeinerung würde man Bewahrung von Verhaltens-Anforderungen erwarten.

„**Verfeinerungsparadox**“: Im Allgemeinen jedoch nicht der Fall [Roscoe‘96].

Beispiel: Im obigen Beispiel sind die Transitionen *rx()/return(true)* (bzw. *false*) Verfeinerung der „sicheren“ Transition *rx()/return(random_bool)*.



Beobachtung: Problematisch: Vermischung von Nichtdeterminismus zur Unterspezifikation bzw. als Sicherheits-mechanismus. Unser Spezifikationsansatz trennt beide Aspekte.

Resultat: Verfeinerung bewahrt wichtige Verhaltens-Anforderungen.

Nachweis: mittels formaler Semantik.

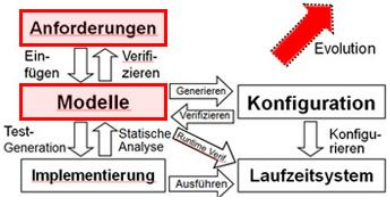
Definition Q refines P ($P \rightsquigarrow Q$) if for each $\vec{s} \in \mathbf{Stream}_{I_P}$ have $[\![P]\!](\vec{s}) \supseteq [\![Q]\!](\vec{s})$.

Theorem If P preserves secrecy of m and $P \rightsquigarrow Q$ then Q preserves secrecy of m.

Obiges Beispiel: mit unserem Ansatz **keine** Verfeinerung.

Fraunhofer ISST

Architekturprinzip: Modularisierung

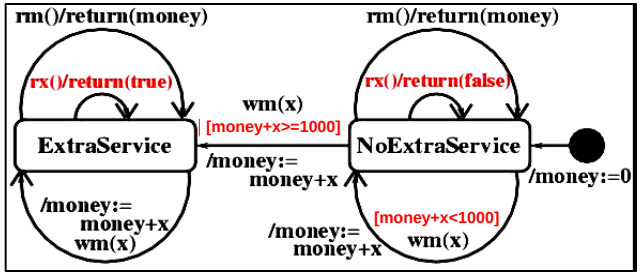


Problem: Verhaltens-Anforderungen i.A. nicht kompositional.

Obiges Beispiel: Zustände *ExtraService* und *NoExtraService* jeweils „sicher“ (nur ein Rückgabewert von *rx*), aber Komposition in Statechart nicht.

Frage: Unter welcher Bedingung bewahrt Komposition Anforderungen ?

Lösungsansatz: Anforderung als „Rely-guarantee“-Bedingung definieren.

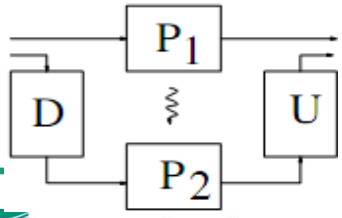


Resultat: Für so definierte Anforderungen Bedingungen für Kompositionalität.

Nachweis: mittels formaler Semantik.

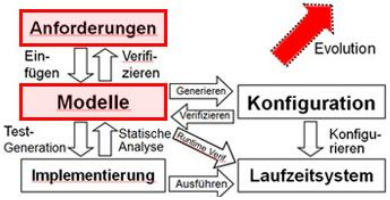
Theorem 5. *Let P_1, P_2, D and U be processes with $I_{P_1} = I_D$, $O_D = I_{P_2}$, $O_{P_2} = I_U$ and $O_U = O_{P_1}$ and such that D has a left inverse D' and U a right inverse U'. Let $m \in (\mathbf{Secret} \cup \mathbf{Keys}) \setminus \bigcup_{Q \in \{D', U'\}} (S_Q \cup K_Q)$.*
If P_1 preserves the secrecy of m and $P_1 \overset{(D,U)}{\rightsquigarrow} P_2$ then P_2 preserves the secrecy of m.

Obiges Beispiel: Rely-guarantee Formalisierung zeigt, dass sichere Komposition nicht möglich.



Fraunhofer ISST

Evolution auf Design-Ebene: Differenz-basierte Verifikation



Differenz-basierte Verifikation – Idee:

- Erstmalige Verifikation: Registrieren, welche **Modellelemente** bei Verifikation gegebener Eigenschaft **referenziert**.
- Im verifizierten Modell **gespeichert**, inkl. Teil-Resultate („proof-carrying models“).
- Mit Heuristiken **Bedingungen an Änderungen** definiert, die Verifikationsergebnis bewahren.
- **Evolutions-Differenz** zwischen altem und neuem Modell berechnen (z.B. mit SiDiff [Kelter]).
- Nur die **Modell-Teile re-verifizieren**, die
  1) sich **geändert** haben und
  2) in der Verifikation **referenziert** wurden und
  3) deren Änderung die Bedingungen **nicht erfüllt**.

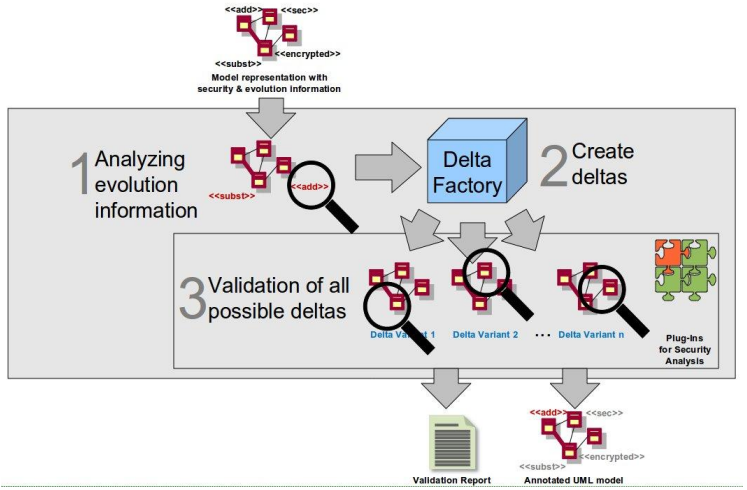
Erheblicher **Performanzgewinn** gegenüber einfacher Re-Verifikation.

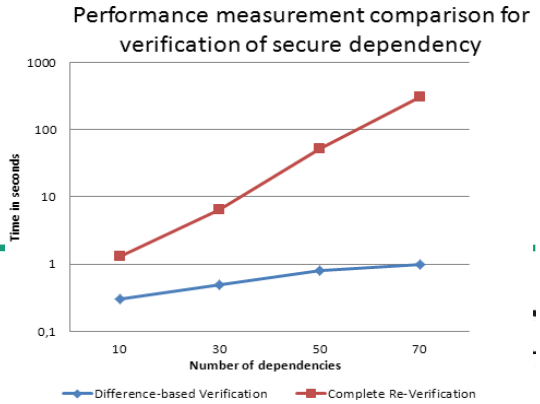
Theorem 1 *Assume that the program p' evolved from the program p where p and p' are related as in the following cases*

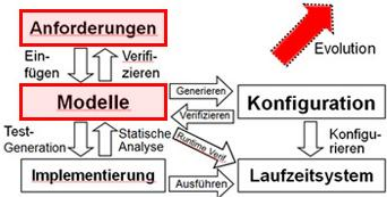
$p =$ *either* p' *or* p''**:** *This implies* $p \succcurlyeq p'$ *and* $p \succcurlyeq p''$.

$p =$ *if* $E = E'$ *then* p' *else* p''**:** *For any expression* $X \in \mathbf{Exp}$ *such that* p *preserves the secrecy of* X*:*
p' *preserves the secrecy of* X *assuming* $E = E'$ *and*
p'' *preserves the secrecy of* X *assuming* $E \neq E'$.

...



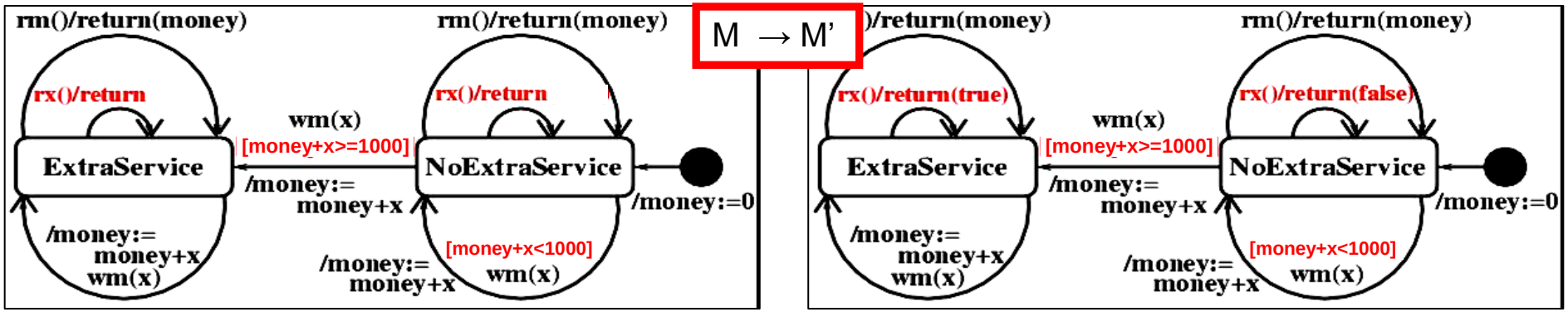




Evolutions-basierte Verifikation: Beispiel

Beispiel: Heuristik zu sicherem Informationsfluss bei Evolution M → M‘: Nur Systemzustände *s*, *s‘* betrachten, für die:

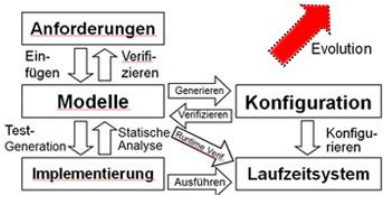
- $s \approx_{pub} s'$ in M‘ aber nicht in M, oder
- $s.t(m) \approx_{pub} s'.t(m)$ in M aber nicht in M‘.



Beispiel: $wm(0).rx() \approx_{pub} wm(1000).rx()$ in M aber nicht in M‘. Impliziert, dass M‘ **nicht sicheren Informationsfluss erfüllt** (vertrauliche Argumente *0* und *1000* unterscheidbar).

Fraunhofer ISST

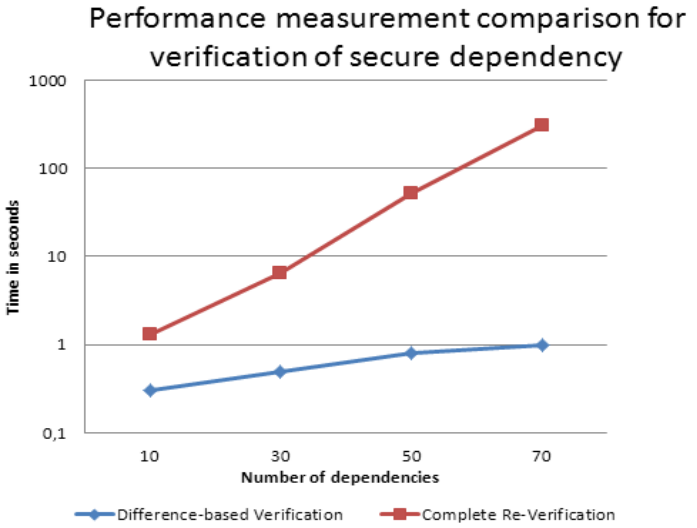
Technische Validierung



- **Korrektheit**: mittels formaler Semantik
- **Vollständigkeit**: jede Modell-Transformation darstellbar als Folge von Löschen, Ändern und Hinzufügen von Modell-Elementen

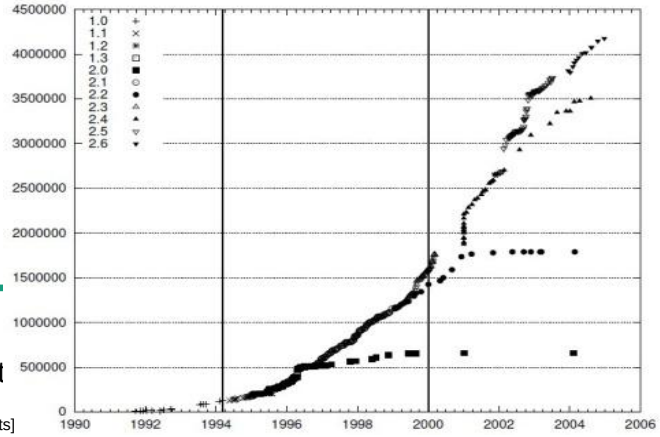
Performanzgewinn am **größten**, wenn **Differenz << Software.** Beispiel-Resultat:

- Evolutions-basierte Verifikation: Laufzeit **linear** in Softwaregröße (bei gleichbleibender Differenzgröße)
- Komplette Re-Verifikation: Laufzeit **exponentiell** in Softwaregröße



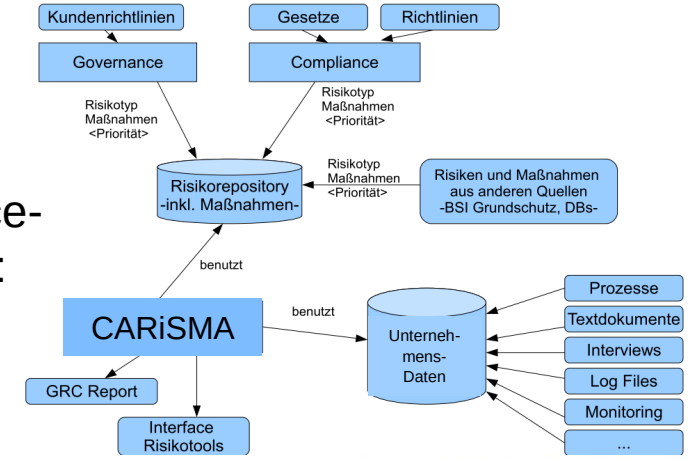
Ist erfüllt:

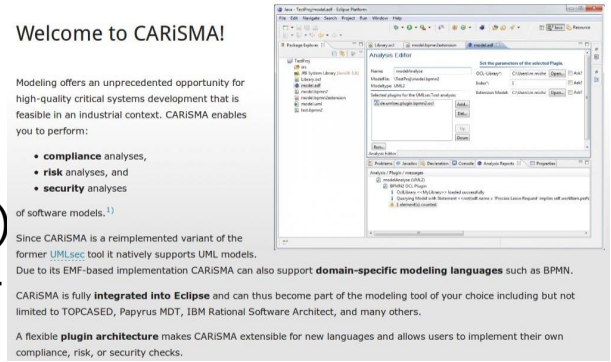
- bei **Wartung stabiler Software-Versionen**
- bei **änderungsbegleitender QS** (z.B. nightly builds)



[Robles et al.: Evolution and Growth in Large Libre Software Projects]

Einige technologische Assets





Werkzeug CARiSMA: Sicherheits-, Risiko- / Compliance-analysen auf Geschäftsprozess-/Software-Modellen:

- **BPMN-/UML-Modellanalyse**
- Anbindung von **Process-Mining**
- Differenzberechnung nach **Modelländerungen**
- **Re-Verifikation** auf Sicherheit nach Modelländerungen

Ontologie zur systematischen Herleitung, Formalisierung, Verwaltung von Sicherheits/Compliance-Anforderungen

Taxonomie für Sicherheitsstandards (z.B. BSI Grundschutz)

Modell für **Cloud-Umgebungen** über Extraktion sicherheits-relevanter Daten über Cloud-Interfaces.

Werkzeugunterstützung zur Erfassung von **Quelltexten** (z.B. Gesetzestexte, BSI-Grundschutzkataloge), deren Verarbeitung und automatisierte Erkennung und Erfassung der Querbeziehungen.

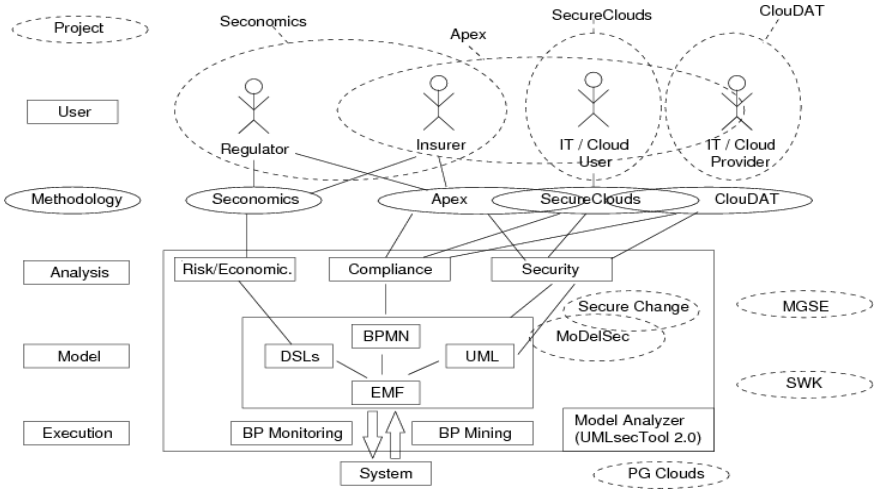
- „**RiskFinder**“: Findet Sicherheits-/Compliance-Risiken in Prozessbeschreibungen.
- Werkzeug zur **textbasierten** Analyse von **Compliance**-Anforderungen.

Analysewerkzeug für **Rentabilität** von Sicherheitsmaßnahmen (in Entwicklung).

Analysewerkzeug für **Clouds** auf Sicherheitsanforderungen (in Entwicklung).

Fraunhofer ISST

Spin-Off-Projekte



SecureClouds (BMBF): Analyse von Geschäftsprozessen auf Sicherheit und Compliance bei Auslagerung in Cloud:

- **Ontologie** für **Sicherheits-** und **Compliance-Anforderungen**
- Analysewerkzeug „**RiskFinder**“.

SECONOMICS (EU): Werkzeuge für modellbasierte Analyse von IT-Sicherheitsrisiken und ökonomische Bewertung der **Rentabilität von Sicherheitsmaßnahmen**, insbesondere in **cyber-physikalischen Systemen**.

FhG-interne Studie: Untersuchung der Anwendbarkeit eines **Informations-sicherheitsrisikomanagements** nach ISO 2700x in der Fraunhofer Gesellschaft

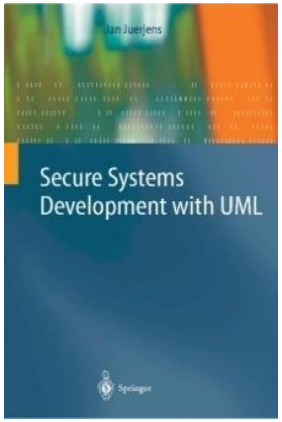
ClouDAT: Werkzeugunterstützung für **Cloud-Zertifizierung** auf Sicherheits-anforderungen gemäß Standards (z.B. ISO 27002, BSI-Grundschutzhandbuch).

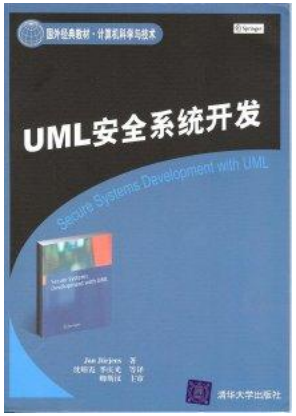
Secure Change (EU, via TUDo): **Rezertifizierung** von Software auf Sicherheitsanforderungen nach **Änderungen** der **Software**

SecVolution (DFG, via TUDo): Rezertifizierung von Software auf Sicherheitsanforderungen nach **Änderungen** der **Systemumgebung**

Fraunhofer ISST

Veröffentlichungen





Impakt:

- „10 years most influential paper“ f. UML’02-Veröffentlichung
- Mehr als 3000 Zitierungen, h-index 29

Einige aktuelle Veröffentlichungen (ab 2011):

Vorträge zu **Sicherheit** und **Compliance** (z.B. in **Clouds**) auf: iqnite 2012, Anw. Informationstechnik und Telekommunikation (AKIT) 2012, CloudConf 2011, CloudDays 2011, Object-Oriented Programming (OOP 2011), iqnite 2011

Compliance-Management:

- S. Islam, H. Mouratidis, J. Jürjens. A Framework to Support Alignment of Secure Software Engineering with Legal Regulations. Journal of Software and Systems Modeling (SoSyM) 2011

Sichere Software Migration in die Cloud:

- S. Wenzel, T. Humberg, C. Wessel, D. Poggenpohl, T. Ruhroth, J. Jürjens. Ontology-Based Analysis of Compliance and Regulatory Requirements of Business Processes. In: 3rd Int. Conference on Cloud Computing and Services Science (Closer 2013)
- S. Wenzel, C. Wessel, T. Humberg, J. Jürjens. Securing Processes for Outsourcing into the Cloud. In 2nd Int. Conf. on Cloud Computing and Services Science 2012.

Text-basiertes Risk-Mining:

- K. Schneider, E. Knauss, S. Houmb, S. Islam, J. Jürjens. Enhancing Security Requirements Engineering by Organisational Learning. Requirements Engineering Journal (REJ), 2012.

ModellbasiertesSicherheits-Testen:

- E. Fourneret, M. Ochoa, F. Bouquet, J. Botella, J. Jürjens, P. Yousefi. Model-Based Security Verification and Testing for Smart-cards. In ARES 2011

Werkzeugunterstützung:

- M. Ochoa, J. Jürjens, J. Cuellar. Non-interference on UML State-charts. In 50th Int. Conference on Objects, Models, Components, Patterns (TOOLS Europe 2012)
- M. Ochoa, J. Jürjens, D. Warzecha. A Sound Decision Procedure for the Compositionality of Secrecy. In 4th Int. Symp. on Engin. Secure Software and Systems 2012

Rezertifizierung bei Softwareevolution:

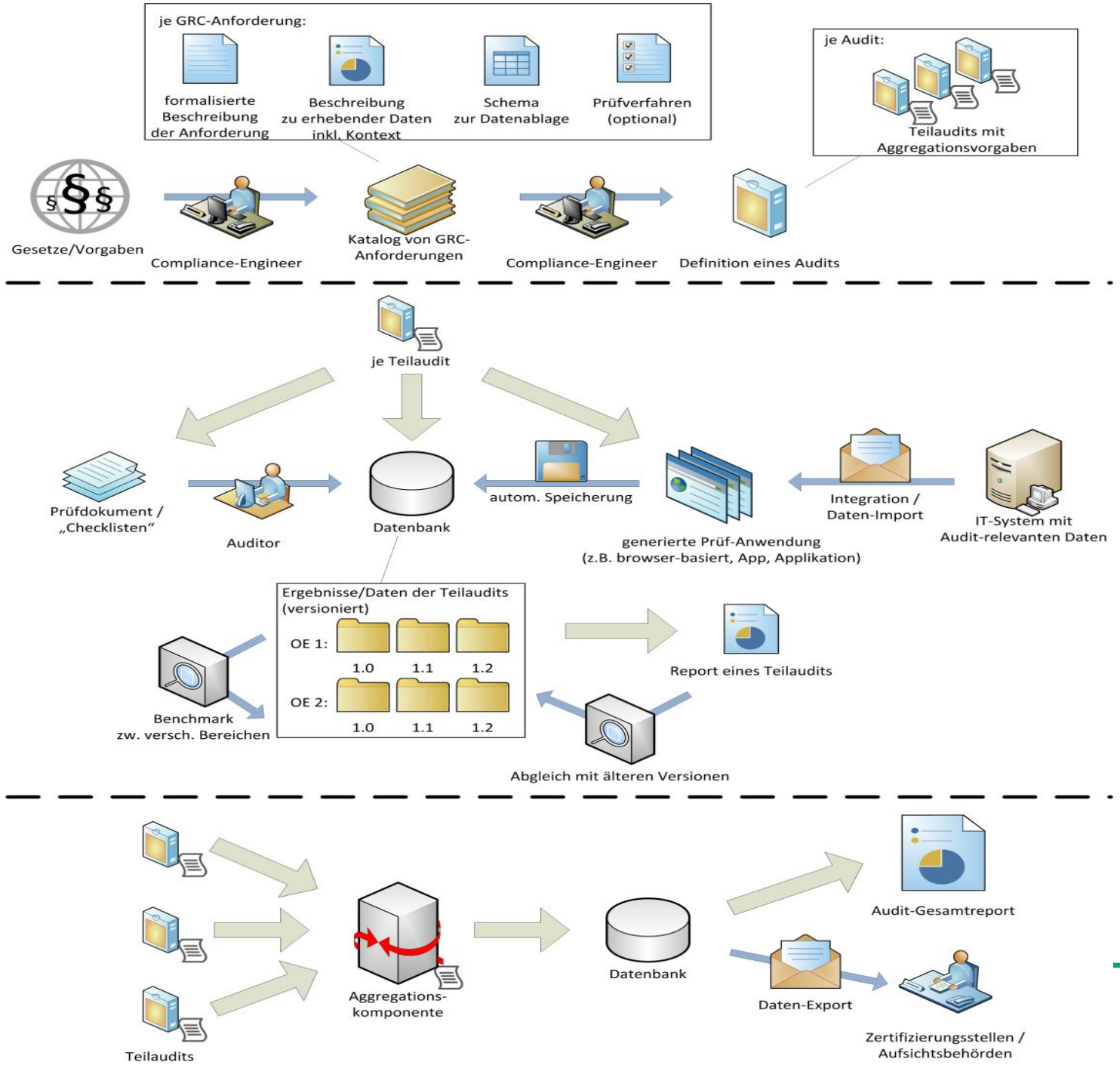
- A. Bauer, J. Jürjens, Yijun Yu. Runtime Security Traceability for Evolving Systems. The Computer Journal, Oxford Univ. Press, vol. 54, no. 1, 2011, pp. 58–87.
- J. Jürjens, K. Schneider. On modelling non-functional requirements evolution with UML (invited contribution). In Festschrift for Martin Glinz 2012
- T. Ruhroth, J. Jürjens. Supporting Security Assurance in the Context of Evolution: Modular Modeling and Analysis with UMLsec. In 16th IEEE Intern. Symposium on High Assurance Systems Engineering (HASE 2012), IEEE, 2012
- F. Massacci, F. Bouquet, E. Fourneret, J. Jürjens, M.S. Lund, S. Madelenat, J.T. Mühlberg, F. Paci, S. Paul, B. Solhaug, S. Wenzel, F. Piessens. Orchestrating Security and System Engineering for Evolving Systems (Invited paper). In 4th European Conference ServiceWave 2011, LNCS vol 6994, Springer 2011, pp. 134–143

Studien zu IT-Sicherheits-Risikobewertung in der Praxis:

- S. Taubenberger, J. Jürjens, Y. Yu, B. Nuseibeh. Resolving Vulnerability Identification Errors using Security Requirements on Business Process Models. J. Inform. Management & Computer Security, 2013
- S. Taubenberger, J. Jürjens. Studie zu IT-Risikobewertungen in der Praxis. In D-A-CH Security 2011.
- S. Taubenberger, J. Jürjens, B. Nuseibeh, Yijun Yu. Problem Analysis of Traditional IT-Security Risk Assessment Methods – An Experience Report from the Insurance and Auditing Domain. In 26th IFIP International Information Security Conference (IFIP SEC 2011), Lucerne, 7-9 June 2011
- J. Jürjens, K. Schneider: The SecReq approach: From Security Requirements to Secure Design, Software Engineering 2014

Fraunhofer ISST

Aktuelle Arbeiten: Integrierte Compliance Management Plattform (ICMP)



Fraunhofer ISST

Zusammenfassung

Problem: Compliance zunehmend komplexe Herausforderung.

Lösung: **Automatische Werkzeuge** für **Compliance-Management** und **-Analyse** auf Basis von relevanten Artefakten (z.B. Textdokumente, Software-/Geschäftsprozess-Modelle, Log-Daten).

Erfolgreicher Piloteinsatz in verschiedenen Projekten.

Aktuelle Arbeiten:

- Sicherheit/Compliance vs Software/Systemevolution
- Automatische Werkzeuge für ökonomische Bewertung v. Investitionen in Compliance / Sicherheit (Seconomics).
- Werkzeuge für Cloud-Zertifizierung (ClouDAT)
- Integrierte Compliance Management Plattform (ICMP)

Compliance-Report

Compliant: NEIN
Verstöße:
- MaRISK VA 7.2: Einhaltung von BSI G3.1 nicht erfüllt
Maßnahmen:
- BSI Maßnahmen-katalog M 2.62

Fraunhofer ISST