

# Software-Qualität für Industrie 4.0

Änderungen, Herausforderungen und Forschungsansätze

Dr.-Ing. Henning Groenda, [groenda@fzi.de](mailto:groenda@fzi.de)

Dr.-Ing. Klaus Krogmann, [krogmann@fzi.de](mailto:krogmann@fzi.de)

Forschungsbereich Software Engineering


# Herausforderungen aus dem Fundus

- 20 Jahre+ Software-Lebenserwartung
- Personalwechsel
- Anforderungen
  - geänderte
  - (vergessene) alte
  - unvorhersehbare neue
- Hardwarewechsel
- Infrastruktur- und Technologiewechsel
  - Ausführungsplattform und API
  - Bibliotheken
  - Schnittstellen zu angebundenen Systemen
  - Neue Architekturkonzepte
- Änderung von Standards und konkurrierende Standards
- Wachsender Anteil von Software, ...


**News**   **Newsticker**   **7-Tage-News**   **Archiv**   **Foren**

Topthemen:   [Google I/O](#)   [Netzneutralität](#)   [NSA](#)   [TrueCrypt](#)   [Windows](#)

[heise online](#) > [News](#) > [2012](#) > [KW 39](#) > [Datenklau bei Softwareschmiede für kritische Infrastrukturen](#)

27.09.2012 19:48  [« Vorige | Nächste »](#)

## Datenklau bei Softwareschmiede für kritische Infrastrukturen

 vorlesen / [MP3-Download](#)

Der kanadische IT-Dienstleister und Netzausrüster [Telvent](#) hat seine Kunden informiert, dass Angreifer jüngst seine interne Firewall und andere Sicherheitssysteme überwunden hätten. Dabei seien Projektdateien für Software zur Überwachung und Steuerung industrieller Anlagen entwendet worden, [berichtet](#) der Security-Experte Brian Krebs.

Die abhanden gekommenen Daten beziehen sich auf die SCADA-Software [OASyS DNA](#), die es Energieversorgern erleichtern soll, ihre Infrastrukturen zu "intelligenten Stromnetzen" (Smart Grids) umzubauen. Um die Sicherheit des Steuerungsprogramms zu erhöhen, hatte Telvent erst Mitte September eine Partnerschaft mit der Security-Firma Industrial Defender [bekannt gegeben](#).

## Fernwartung: Sicherheitslücke bedroht Hightech-Heizungen

Von *Matthias Kremp*



Mikro-Blockheizkraftwerk Vaillant ecoPower 1.0: Update per Speicherkarte

Vaillant


**Hochmoderne Heizanlagen des deutschen Herstellers Vaillant haben ein Sicherheitsproblem - sie lassen sich übers Internet abschalten, womöglich beschädigen. Das notwendige Update kann nur von einem Techniker installiert werden. Bis der kommt, empfiehlt der Hersteller drastische Maßnahmen.**

<http://www.spiegel.de/netzwelt/gadgets/vaillant-sicherheitsluecke-bedroht-hightech-heizungen-a-894665.html>

14.08.2013 00:07

[« Vorige | Nächste »](#)

## Kritisches Sicherheitsupdate für 200.000 Industriesteuerungen

 [vorlesen](#) / [MP3-Download](#)

Der Schweizer Hersteller Saia-Burgess hat ein Firmware-Update für [seine Industriesteuerungen](#) veröffentlicht, das die von heise Security dokumentierte [Schwachstelle bei der Authentifizierung des Fernwartungszugangs](#) endlich beheben soll – **über ein halbes Jahr**, nachdem wir das Unternehmen über das Problem informiert haben. **Allerdings bleibt es auch nach Installation der abgesicherten Firmware-Version leichtsinnig, diese Systeme direkt über das Internet erreichbar zu machen.**

Industriesteuerung von Saia-Burgess erfreuen sich offenbar großer Beliebtheit: Sie schalten und warten in Rechenzentren, Wasserwerken, Gefängnissen und sogar Kirchen. Nach Herstellerangaben sollen über 200.000 dieser

<http://heise.de/-1934787>

# Industrie 4.0 ist...

... ein Probelauf der  
Verträglichkeit alter nicht für  
Vernetzung gedachter Software  
mit internetbasierter  
Vollvernetzung

... dauerhaft individuelleres  
Eingehen auf Kundenwünsche  
und Optimierung von Lieferketten

## **Herausforderungen durch Industrie 4.0**

- Stetig steigende Integration und Vernetzung
- Größe von verteilten Systemen
- Flexibilität als Wettbewerbsvorteil
- Sicherheit
- Performance
- Reaktionszeit - Wartbarkeit

# Industrie 4.0 ist...

... ein Probelauf der  
Verträglichkeit alter nicht für  
Vernetzung gedachter Software  
mit internetbasierter  
Vollvernetzung

... dauerhaft individuelleres  
Eingehen auf Kundenwünsche  
und Optimierung von Lieferketten

## Herausforderungen durch Industrie 4.0

- Stetig steigende Integration und Vernetzung
- **Software Engineering als Wettbewerbsvorteil**
- Große von verteilten Systemen
- Flexibilität als Wettbewerbsvorteil
- Sicherheit
- **Software Qualität als Wettbewerbsvorteil**
- Performance
- Reaktionszeit - Wartbarkeit

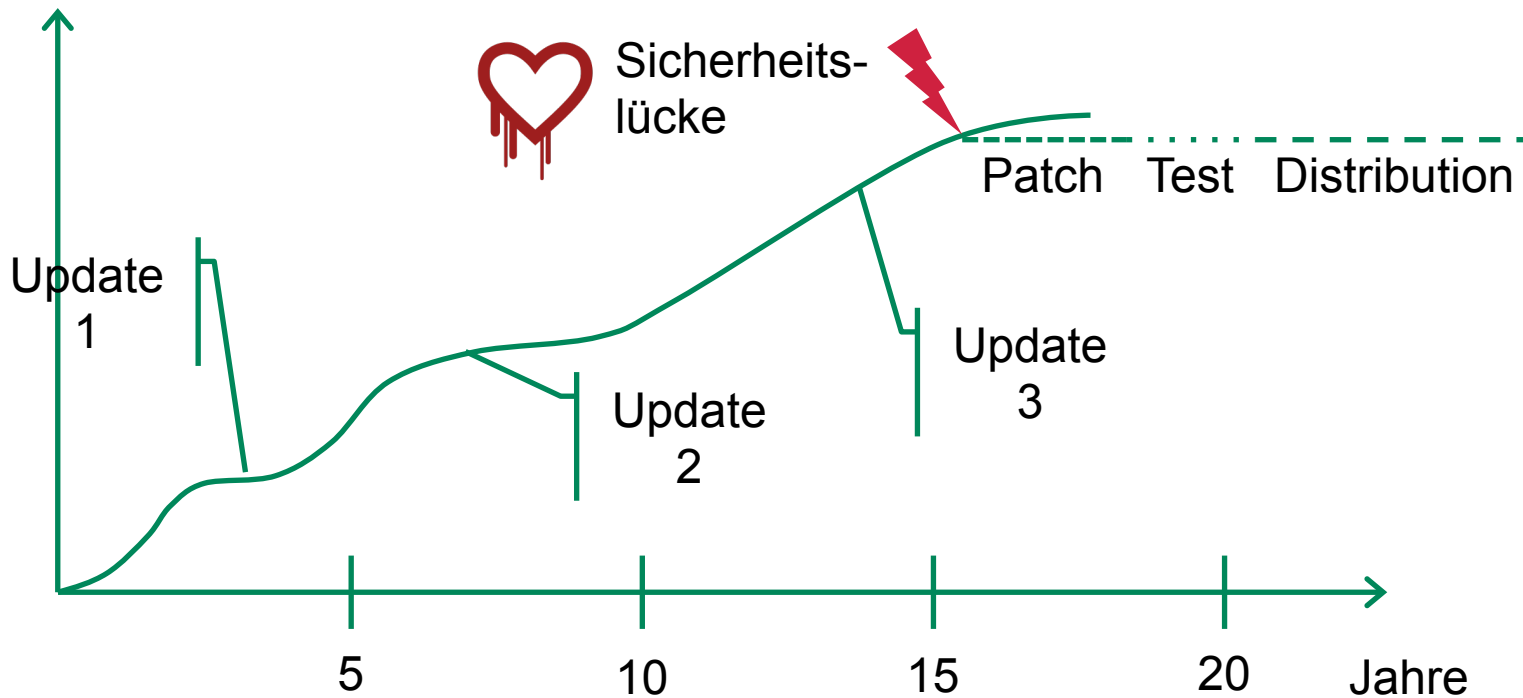
# Trends

- Virtualisierung und Dynamisierung
  - Unterstützung von Endkundenfeatures mit kurzer Time-to-Market
    - Neue Produktidee bis Auslieferung
    - Personalisierung
  - Dynamische Auswahl der Fertigungsstraße
    - Skalierung der Produktionsstraße (Einzelstück bis Massenfertigung)
    - Kürzere Rüstzeiten bei Änderungen
- Softwareintegration
  - Integriertes System vom Online-Shop über Produktion, Rechnungsstellung, ... bis zur Auslieferung
  - Kurzer Zyklus von Auftrag bis Auslieferung
  - Berücksichtigung später Änderungen nach Bestellung während Produktion
- ‚Big Data‘ / ‚Smart Data‘
  - Fehlerdatenanalyse/-vorhersage
  - Einbindung in Wartung
  - Vereinfachung von Abfragen und Formulierung von Analysefragen (Nutzer: Nicht-Datenanalyseexperte)



# Beispielherausforderung

Verbreitung



# Beispielherausforderung

- Patch? Triage von Wünschen, Fehlern und Meldungen aus Betrieb sowie extern
    - Über Vernetzung ausnutzbar
    - Zeitfenster bis zur Lösung
    - Umfang betroffener Geräte
  - Test?
    - Änderungen
      - Einhaltung existierender Entwurfsvorgaben und Anforderungen
    - Qualitätssicherung
      - Geeignete Testumgebung
  - Distribution?
    - Auslieferung
      - Service-Techniker
      - SmartCard
      - Downloadmöglichkeit
      - Direkte Netzwerkverbindung
    - Aktualisierung
      - Rechteverwaltung
      - Zertifikatsverwaltung
- Verbindung DevOps
- Verbindung ReqDevOps
- (Distributed, not owned) Ops

# Herausforderungen an Software-Qualität

- Sicherheit (Analysen, Nachweise)
  - Datenschutz, Schutz von Produkt-/Produktionsdaten, Resilienz
  - Intelligentes Verhalten
  - Architekturbasierte Sicherheitsnachweise
  - Betriebsübergreifende Analysen
    - Auch bei komplexen Zwischenbeziehungen
    - Auch bei Wechsel in der Liefer- / Produktionskette
    - Zusammenarbeit zwischen Konkurrenten ermöglichen
- QoS in heterogener Netz- und Softwareinfrastruktur
  - Cloud-basierte Vernetzung inkl. Hybrid-Cloud-Abwägungen
  - (Daten-) Verarbeitungsarchitektur (u.a. Voranalyse, Aggregation)
  - Bewertung der Zuverlässigkeit und Performance
  - Stabile Multiplattformunterstützung
  - Skalierbare und effiziente Architekturen zur Datenanalyse
- Benutzbarkeit
  - Leichtgewichtige Maschinen-/Produktionsstraßenkonfiguration
  - Abwägungen bezüglich größerer Alternativenauswahl
  - Sprachentwurf, Vereinheitlichung, Integration
  - Konfigurationsfehlererkennung bei Entwurf und Betrieb

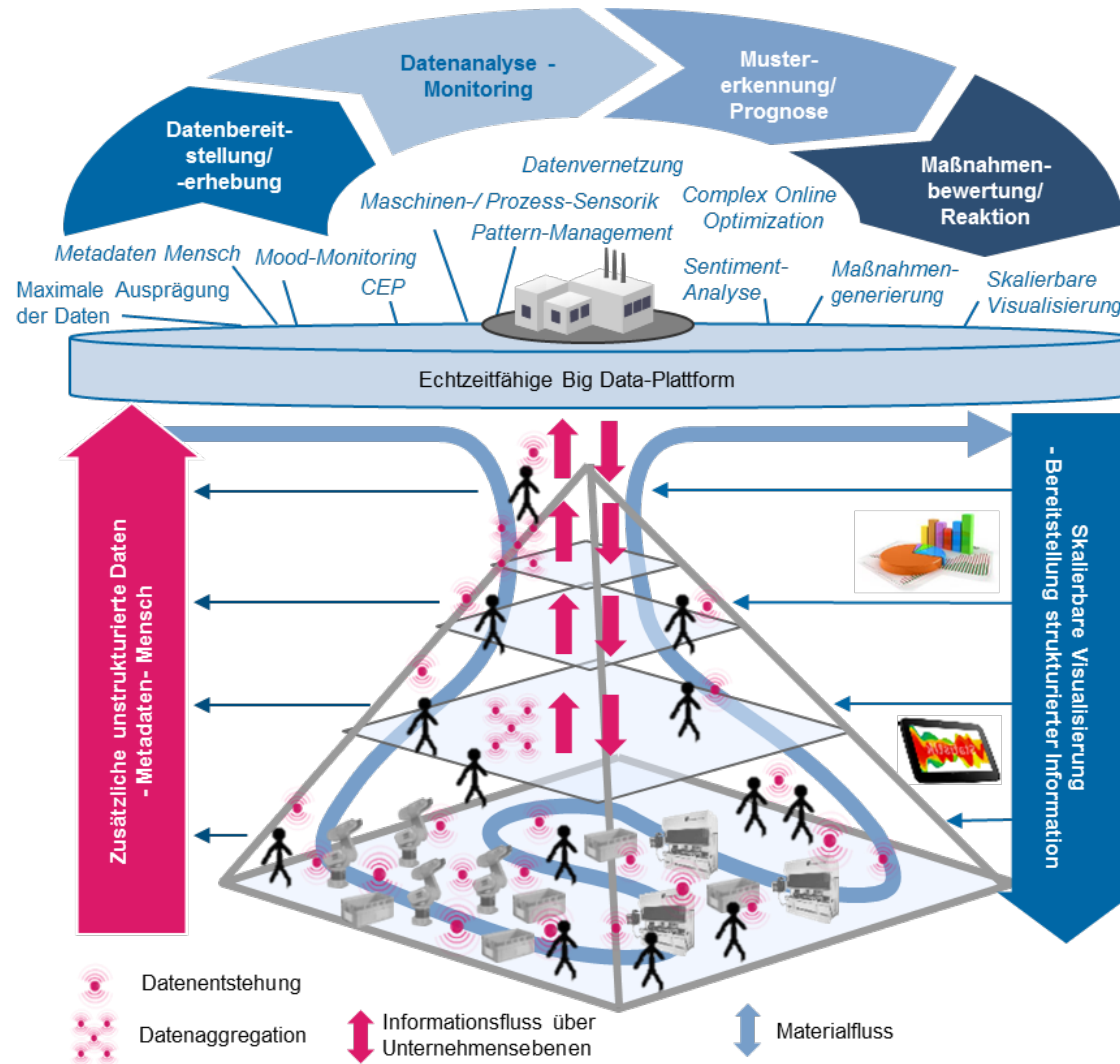
# Herausforderungen an Software-Qualität

- Softwarewartung
  - Langlebigkeit, Nachhaltigkeit bei stetigem Wechsel
  - Schnelle Erweiterbarkeit
  - Flexibilisierung der Gerätekomposition
  - Nachweise und (Re-)Zertifizierung
  - Hardwareunabhängigkeit
    - Bspw. Generative Techniken vs. Virtualisierungsschichten
- Prozessintegration (Produktions-, Logistik-, ...)
  - Optimierung, Ausrichtung an Menschen/Ressourcen/Unternehmenszielen
  - Analyse bestehender Prozesse auf Automatisierungspotential
  - Priorisierung von Teilschrittautomatisierung an Hand Effekt auf Produktivität
  - Verwaltung während des gesamten Lebenszyklus

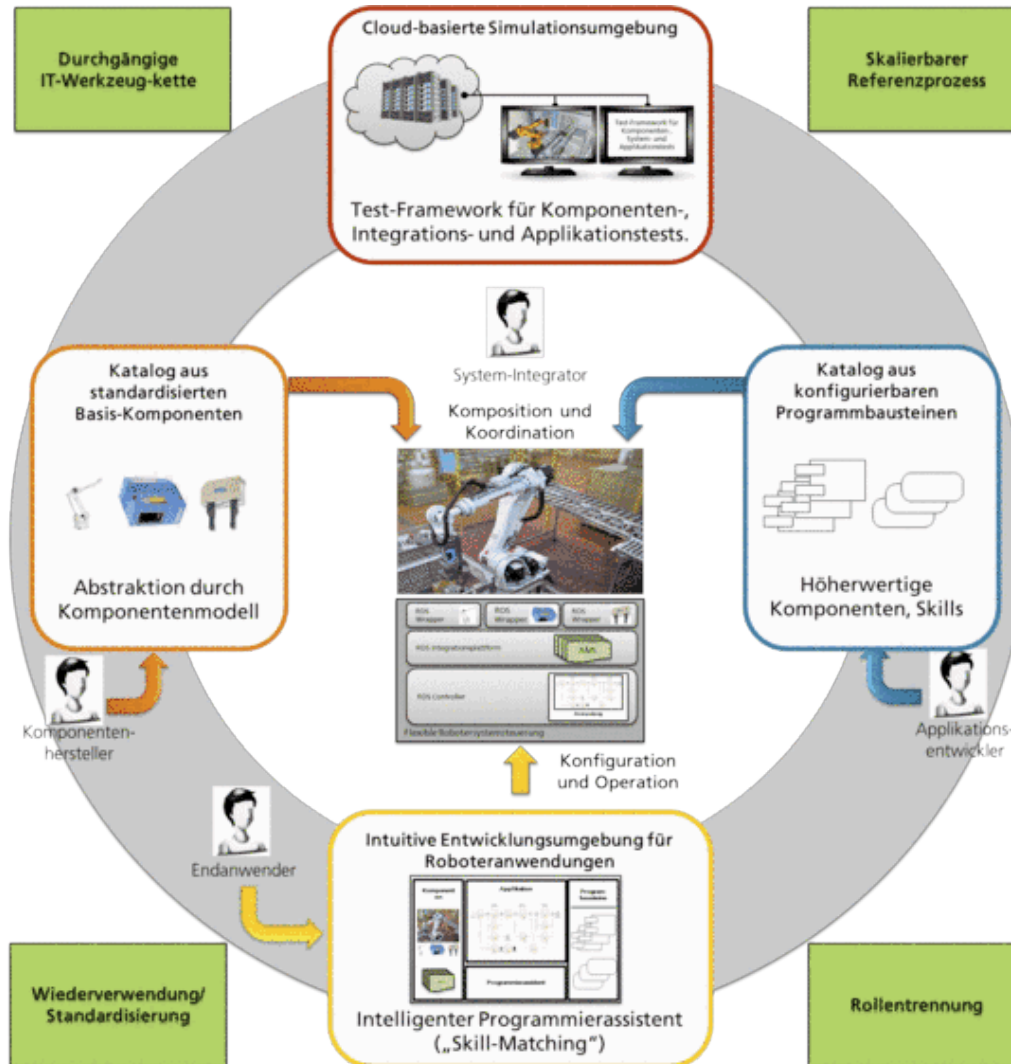
# Software Engineering Lösungsansätze

- **Angepasste Referenzsoftwarearchitekturen**
  - Für nicht vertrauenswürdige offene Umgebung (Paradigmenwechsel!)
  - Langfristige Aktualisierung in fremden Umgebungen
    - Automatische Aktualisierungen
    - Rechteverwaltung
  - Neue Datensicherheitsprimitive (Datendiode, Quorum-Firewall, ...)
- **Automatisierung im Softwareentwicklungsprozess**
  - Analyse
  - Bewertung und Nachweis
  - Auslieferung und Aktualisierung
- **Stärkere Verzahnung von**
  - Anforderungen (Req)
  - Entwicklung (Dev)
  - Betrieb (Ops)
- **Tendenz zu Continuous Delivery:**
  - Langzeitstabilität / -zuverlässigkeit: -
  - Anpassbarkeit: ++
  - Verfügbarkeit von Änderungen: +

# Aktuelle Forschung BigPro



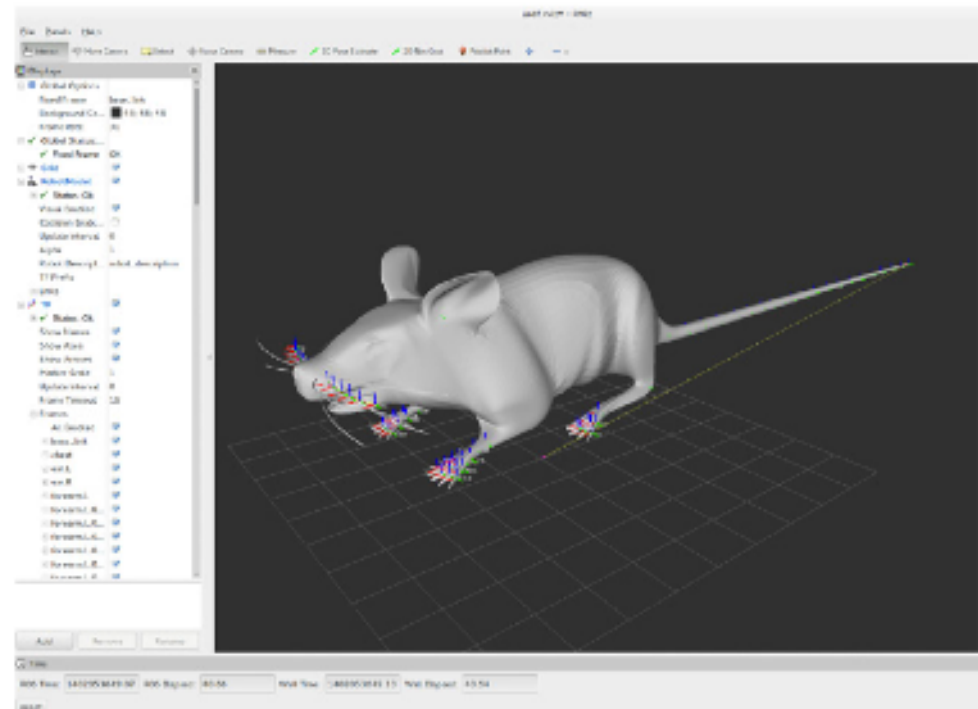
# Aktuelle Forschung ReApp



# Aktuelle Forschung Human Brain Project

- Human Brain Project – Neurorobotics (SP 10)

Ziel in diesem Sub-Projekt ist die Entwicklung einer möglichst realistischen Physik-/Robotersimulation mit Anbindung an verschiedene Gehirnsimulationen, die von den zahlreichen Neurowissenschaftlern für virtuelle Experimente mit Robotern oder auch simulierten Tieren genutzt werden kann.





## EMBOSYST: EMBEDDED OPERATING SYSTEM SECURITY THROUGH INTEGRITY, SYSTEM MANAGEMENT AND TRUST

Gemeinsam mit der Hyperstone GmbH und der WIBU-SYSTEMS AG befasst sich das FZI im BMBF-Projekt EmbOSYST mit der Erforschung und Entwicklung von Schutzmechanismen für den korrekten, vertraulichen und sicheren Betrieb eines eingebetteten Echtzeit-Betriebssystems in einer offenen Internetumgebung. Auf der Basis einer neuartigen Hardware-Architektur soll die Systemintegrität eines eingebetteten Systems über den gesamten Lebenszyklus garantiert werden.

### Projektbeschreibung



Ziel im Projekt EmbOSYST sind die Erforschung und Entwicklung von Schutzmechanismen für den korrekten, vertraulichen und sicheren Betrieb eines eingebetteten Echtzeit-Betriebssystems in einer offenen Internetumgebung. Auf der Basis einer neuartigen Hardware-Architektur soll die Systemintegrität eines eingebetteten Systems über den gesamten Lebenszyklus garantiert werden.

<http://www.fzi.de/de/forschung/projekt-details/embosyst/>

# Diskussion

- Trends
- Herausforderungen
- Forschungsansätze
- Wünsche aus der Industrie