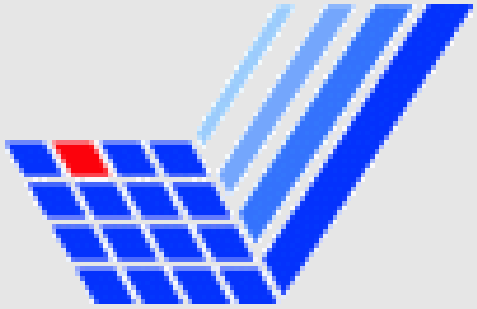
Test & Diagnose

Thomas Romanek

thomas.romanek@udo.edu

PG AutoLab
Seminarwochenende 21.-23. Oktober 2007



Überblick

- Einführung
- Tests zur Qualitätssicherung
  - V-Modell
  - Spezielle Verfahren in Automotive
- Das Diagnosesystem
  - Überwachung
  - Diagnosesystem
  - Kommunikationsstandards
- Zusammenfassung & Einordnung in die PG
  - CANoe 6.1
- **Fragen**

Einführung

! Versagen von sicherheitskritischen Funktionen
→ Schwere Unfälle
→ Hohe Anforderungen an Sicherheit und Zuverlässigkeit

- Testen
  - Qualitätssicherung
    - ➔ Spezifikations- und Implementierungsfehler nachweisen
  - Auch: Frühzeitiges Erkennen von Fehlern ⇒ Kostenersparnis
- Diagnose
  - Überwachung sicherheitsrelevanter Systeme
  - Fehlersuche in Werkstätten

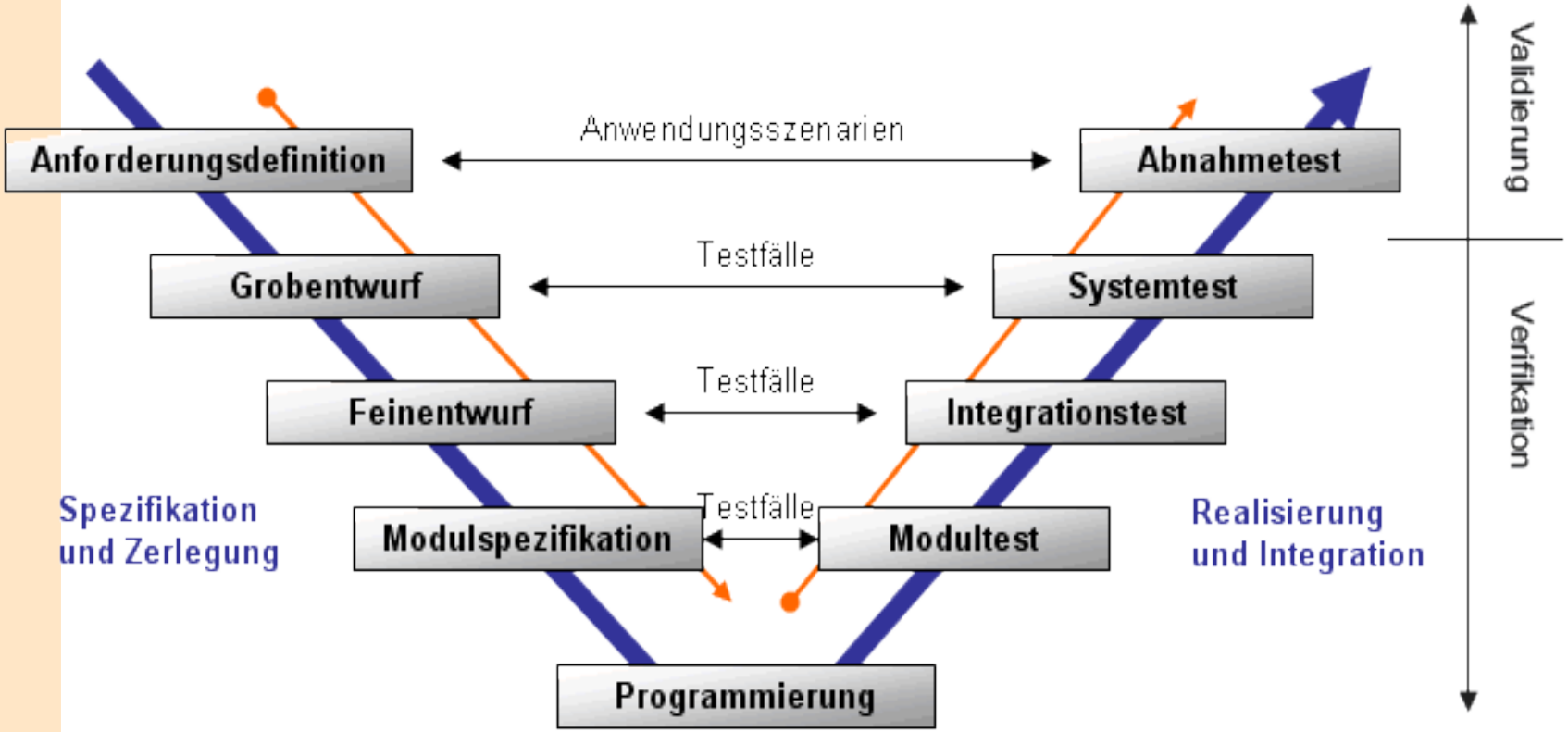
Tests zur Qualitätssicherung

Erinnerung:
- Qualitätssicherung
- Kostenersparnis

Tests zur Qualitätssicherung

- Zum frühestmöglichen Zeitpunkt auf allen Systemebenen
- Keine Fehler gefunden ≠ keine Fehler vorhanden
  - Statische Tests
    - z.B. Reviews
  - Dynamische Tests
- Maßgeblich: V-Modell

Tests: Allgemeines V-Modell



Quelle: http://www.jprofil.de/Dokumentation/SoftwareEngineering/Vorgehensmodelle/images/vModell-02.gif

Tests: Spez. Verfahren in Automotive 1/5

- Zusätzliche Testschritte um Entwicklungsablauf zu verkürzen
  - Frühzeitig Spezifikationsfehler ausschließen
  - Tests, die erst in einem späteren Stadium möglich wären, vorziehen
    - Model in the loop
    - Rapid Prototyping
    - Software in the loop
    - Hardware in the loop

Tests: Spez. Verfahren in Automotive 2/5

- Model in the loop
  - Frühzeitiges Erkennen von Spezifikationsfehlern
  - Simulation von
    - Software-Funktionen
    - Umgebungskomponenten
  - → Verifiziertes Modell schon in der Spezifikationsphase
- Rapid Prototyping
- Software in the loop
- Hardware in the loop

Tests: Spez. Verfahren in Automotive 3/5

- Model in the loop

- Rapid Prototyping
  - Simulation mittels Modell
  - Aber: Schnittstelle zum realen Fahrzeug
    - Umgebung wird nicht simuliert
    - ➔ Einsatz dynamischer Prüfmethoden
      - ➔ Sonst erst nach Integrationsschritt der Software mit der Hardware

- Software in the loop
- Hardware in the loop

Tests: Spez. Verfahren in Automotive 4/5

- Modell in the loop
- Rapid Prototyping

- Software in the loop
  - Realisierte Software-Komponenten in simulierter Umgebung ausführen
  - Keine Abhängigkeit von Zielhardware
  - → Frühzeitig dynamische Software-Tests durchführen

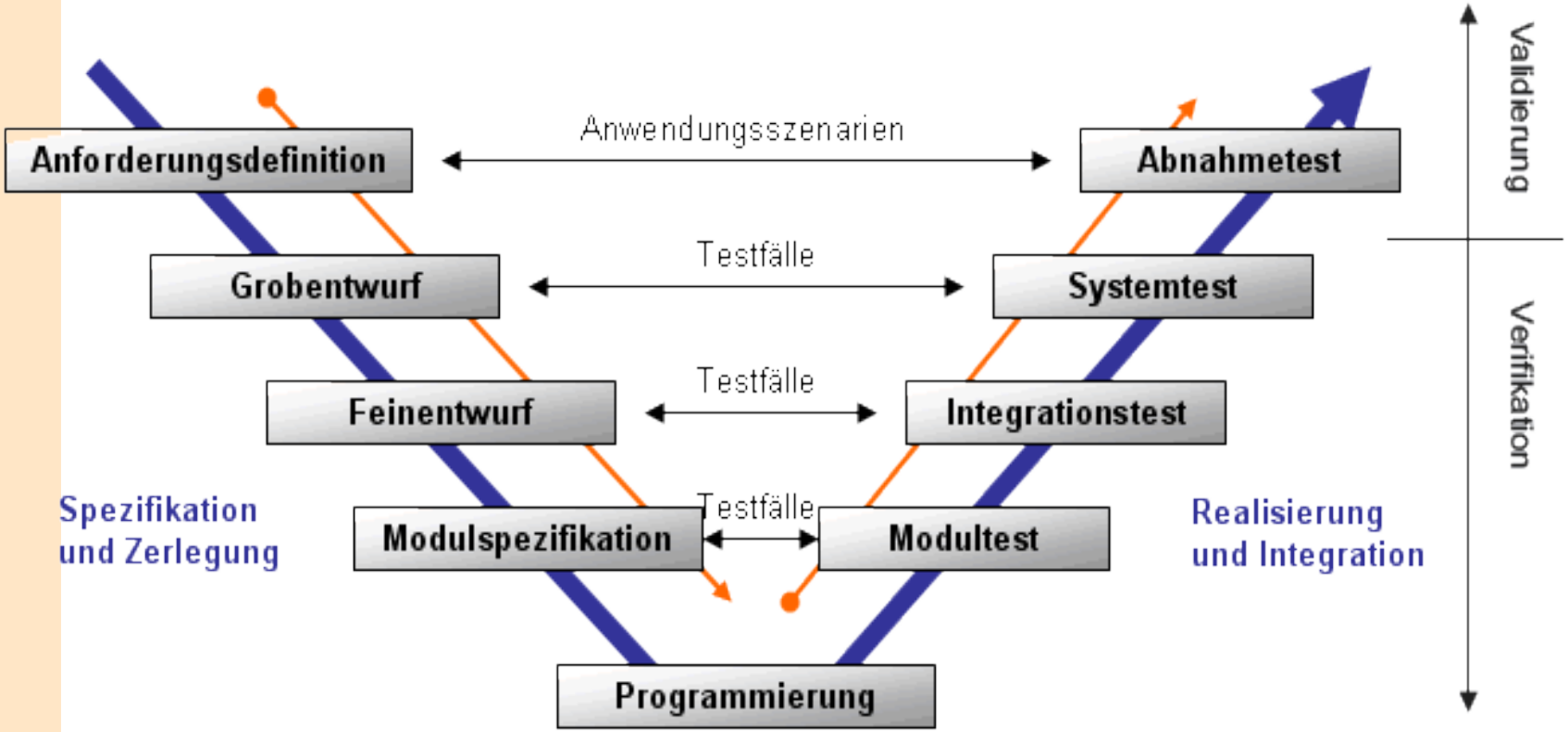
- Hardware in the loop

Tests: Spez. Verfahren in Automotive 5/5

- Modell in the loop
- Rapid Prototyping
- Software in the loop

- Hardware in the loop
  - Hard- und Software eines Steuergeräts stehen zur Verfügung
  - Testen von Regelungsfunktionen: Steuergerät als Komponente im Regelkreis
  - Nicht nur auf Regelungsfunktionen beschränkt
    - Viele Prüfschritte ins Labor verlagert
    - Laborfahrzeuge und Prüfstände

Tests: Allgemeines V-Modell



Quelle: http://www.jprofil.de/Dokumentation/SoftwareEngineering/Vorgehensmodelle/images/vModell-02.gif

Test: V-Modell-Testschritte 1/2

- Komponentest
  - Komponente gegen ihre Spezifikation testen
  - Verschiedene statische Tests
  - Dynamische Methoden durch Einsatz von SiL
- Integrationstest
- Systemtest
- Akzeptanztest

Test: V-Modell-Testschritte 1/2

- Komponentest
- Integrationstest
  - Voneinander abhängige Komponenten eines Systems im Zusammenspiel miteinander testen
  - ... der Software:
    - Statische Tests gegenüber Implementierungsrichtlinien
  - ... des Systems:
    - Möglichst frühzeitige Durchführung durch Nachbildung fehlender Komponenten (HiL)
- Systemtest
- Akzeptanztest

Test: V-Modell-Testschritte 2/2

- Komponententest
- Integrationstest

- Systemtest
  - Möglicherweise Fehler in der Modellbildung
  - → Systemtest im Fahrversuch
    - → Risiken durch Vernachlässigung in der Modellbildung nicht mehr vorhanden

- Akzeptanztest

Test: V-Modell-Testschritte 2/2

- Komponententest
- Integrationstest
- Systemtest

- Akzeptanztest
  - System gegen die Benutzeranforderungen testen
  - In ihrer realen Systemumgebung
  - Aus der Benutzerperspektive

Das Diagnosesystem

Erinnerung:

- Überwachung sicherheitsrelevanter Systeme
- Fehlersuche in Werkstätten

Diagnose: Überwachung 1/3

- Sicherheitsrelevantes System nicht mehr funktionsfähig
  - ➔ Potentielle Gefahr
- ➔ Fehler und mögliche Folgen frühzeitig erkennen und behandeln

Diagnose: Überwachung 2/3

Fehlererkennungsverfahren:
Prüfung, ob zwischen mindestens zwei Werten, die zwischen diesen Werten bestehenden Zusammenhänge erfüllt sind

- Referenzwertüberprüfung
- Überprüfung anhand redundanter Werte
- Beobachtung von Kommunikationsverbindungen
- Beobachtung von physikalischen Eigenschaften
- Beobachtung der Programmausführung
- Modellbasierte Fehlererkennung

Diagnose: Überwachung 3/3

Fehlerbehandlung:
Festlegung, wie auf Fehlersymptome reagiert wird

- Verwendung redundanter Werte
- Abschaltung von Subsystemen oder des Gesamtsystems
- Verharren im Fehlerzustand oder Strategiewechsel
- Fehlerspeicherung
- Fehlerbeseitigung

Diagnose: Diagnosefunktionen

- Diagnosesystem Grundumfang eines Seriensteuergeräts
  - Realisiert die Überwachung

  - Onboard-Diagnosefunktionen
    - Im Steuergerät selbst ausgeführt
    - z.B. Ein- und Ausgänge des Steuergeräts überprüfen
    - Eintrag im Fehlerspeicher

  - Offboard-Diagnosefunktionen
    - Steuergerät wird an einen Diagnosetester angeschlossen

Diagnose: Spezielle Diagnosefunktionen

- Sollwertgeber- & Sensordiagnosefunktion
  - Messung von Steuergeräteeingangssignalen und steuergeräteinternen Größen
  - Können an Diagnosetester übertragen werden
- Aktuatordiagnosefunktion
  - Über Diagnosetester gezielt einzelne Aktuatoren des Steuergeräts aktivieren
  - Nur unter festgelegten Bedingungen

Diagnose: Fehlerspeichermanager

- Speicherung von durch Onboard-Diagnosefunktion erkannten Fehlersymptomen
- Im EEPROM abgelegt
- Meist als eigenständige Software-Komponente realisiert
- Speicherung:
  - Fehlercode (engl. Diagnostic Trouble Code, DTC)
  - Zusätzliche Informationen durch gesetzliche Vorgaben
- Mögliche Löschung der Fehler nach Beseitigung

Diagnose: Offboard-Kommunikation

- Für die Kommunikation zwischen Steuergerät und Diagnosetester: Standards
- Am weitesten verbreitet: Keyword 2000 Protokoll
  - Zunächst mit K-Line und später mit CAN-Bussystemen realisiert
- Nachfolger: Unified Diagnostic Services (UDS)
  - Zu KWP 2000 nah verwandtes Protokoll
  - Neue Bussysteme wie LIN oder FlexRay sollen leichter integriert werden können

Diagnose: KWP2000

- Gesamte Kommunikation geht vom Testgerät aus
- Verwendung von Diagnosesitzungen
  - Bedingungen zur Öffnung einer Sitzung vom Fahrzeughersteller festgelegt. Üblich:
    - Fahrzeug in einem bestimmten Zustand
    - Diagnosetester muss sich beim Steuergerät mit Hilfe eines Schlüsselaustausches (Seed and Key) anmelden
  - Time-Out-Mechanismus
- Steuergeräten, die neuprogrammierbar (*flashbar*) sind, kann über die Nachrichten auch eine neue Programmversion zugesendet werden

Kommunikationsmodell der KWP 2000 - Anwendungsschicht

Zusammenfassung

- Automotive:
  - Besondere Bedeutung von Sicherheit
  - Kosteneffizienz

Spezielle Verfahren, die typisch für den Automotive-Bereich sind

Was können wir mit den vorgestellten Mitteln und Methoden anfangen?

Einordnung in die PG

- Unser Vorhaben: Grundstein für ein neues Labor zu legen
  - Entspricht dem Vorhaben ein Laborfahrzeug aufzubauen
  - Vorgestellte Mittel zum Testen von Komponenten, der Integration sowie des Gesamtsystems müssen eingesetzt werden
- Labor wird vermutlich langfristig für Analysen unter realen Lastbedingungen eingesetzt
  - Diagnose wird eine immer größere Rolle spielen

Einordnung in die PG: CANoe 6.1 1/3

- Werkzeug zur Entwicklung, den Test und der Analyse von Netzwerken und Steuergeräten

Quelle: http://www.vector-worldwide.com/

- Anfang des Entwicklungsprozesses werden Simulationsmodelle erstellt, die das Verhalten der Steuergeräte nachbilden (MiL)

Einordnung in die PG: CANoe 6.1 2/3

- Modelle bleiben während der gesamten Steuergeräteentwicklung Grundlage für die Analyse, den Test und die Integration von Bussystemen und Steuergeräten (SiL, HiL)
- Simulation kompletter Systeme möglich sowie Simulation von Nachrichten (noch) nicht vorhandener Steuergeräte (Restbussimulation)
- Ermöglicht automatisierte Durchführung von Tests (dyn. Tests)
- Diagnosekommunikation nach KWP2000 und UDS sowie Einsatz als vollständiger Diagnosetester
- Unterstützung von Modellentwicklung in MATLAB und Statemate
- Unterstützung der Bussysteme CAN, LIN, MOST, FlexRay, J1587 sowie weiterer CAN-basierter Protokolle

Einordnung in die PG: CANoe 6.1 3/3

- Erstellung benutzerdefinierter Oberflächen zur Steuerung der Simulation und Tests oder der Anzeige der Analysedaten
- Freie Programmierbarkeit durch die integrierte C-ähnliche Programmiersprache CAPL zur Unterstützung von Simulation und Analyse
- Arbeitet auf zwei PCs verteilt (für kritische echtzeitrelevante Simulationen)

Quellen

- **Zimmermann, Werner; Schmidgall, Ralf:** Bussysteme in der Fahrzeugtechnik, 2. Auflage, ATZ/MTZ-Fachbuch, Wiesbaden, 2007
- **Schäufelle, Jörg**: Automotive Software Engineering (ATZ-MTZ Fachbuch), 3. Auflage, ATZ/MTZ-Fachbuch, Wiesebaden, 2007
- http://www.vector-worldwide.com/