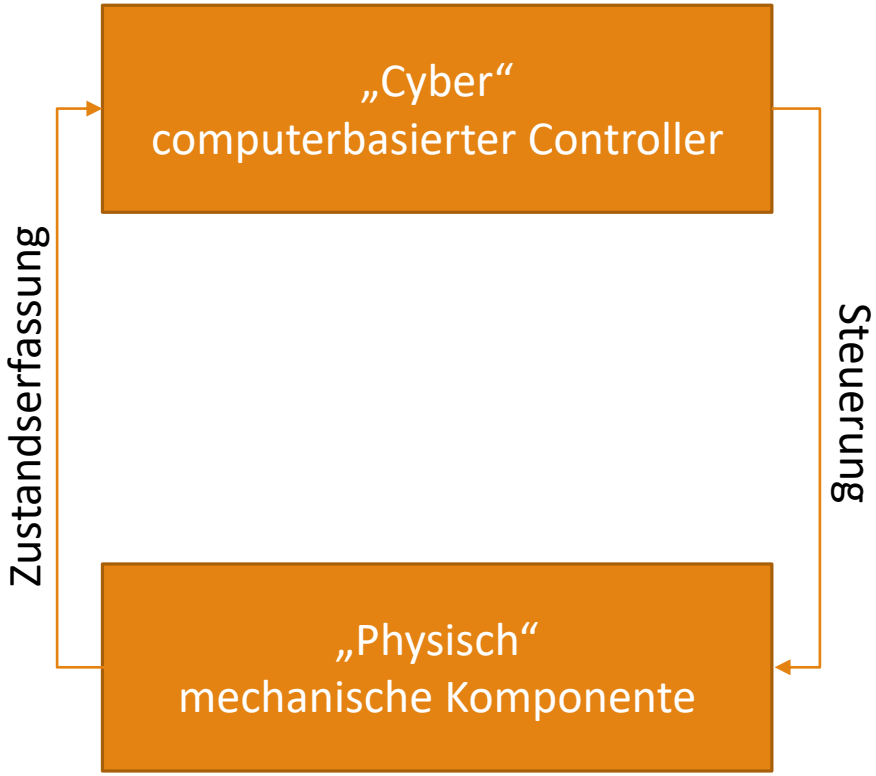
SW-Qualitätssicherung in Cyber-Physischen Systemen

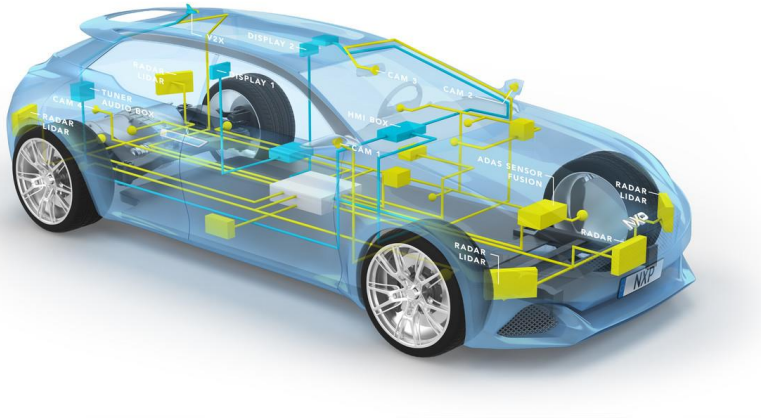
FRAMEWORKS & METHODEN

FOLIEN: HTTPS://WWW.STEFAN-WINTER.NET/APPLICATION-MATERIALS/

Cyber-Physische Systeme (CPS)



Cyber-Physische Systeme



Domänenspezifische Standards

- Luft- und Raumfahrt: DO-178B/C
- Industrie: IEC 61508
  - Schienenverkehr: CENELEC EN 50128
  - Kernkraft: IEC 61513
  - Automobile: ISO 26262
  - Medizintechnik: IEC 62304
  - Verfahrenstechnik: IEC 61511

→ Keine einheitlichen Qualitätsanforderungen → domänenspezifische Methoden & Frameworks

Hier:

- Allgemeine Orientierungshilfe zu QS-Methoden in den Standards
- Konkrete Methodendiskussion für spezifische Problemstellung in CPS-QS

Klassen von Qualitätssicherungsmethoden

1. Präventive oder pro-aktive Methoden

Ziel: Vermeidung von (Qualitäts-)Problemen

Formen: Prozessorientiert

2. Reaktive Methoden

Ziel: Aufspüren und Beseitigen von (Qualitäts-)Problemen

Formen: Produktorientiert

Präventive Qualitätssicherung

- Auswahl geeigneter Prozessmodelle
- Prozess-Qualitätsmanagement (z.B. ISO 9001, CMMI, SPICE)
- Mitarbeiter-Schulungen
- Auswahl geeigneter Programmiersprachen, Frameworks, Bibliotheken, etc.
- …

\+ Großer Einfluss auf Softwarequalität

– Keine spezifische Werkzeugunterstützung

– Gute Entscheidungen erfordern v.a. Erfahrung,
teils Vorgaben/Empfehlungen durch domänenspezifische Standards

Beispiel: Empfehlungen nach ISO 26262

Topic
Enforcement of low complexity
Use of language subsets
Enforcement of strong typing
Use of defensive implementation techniques
Use of established design principles
Use of unambiguous graphical representation
Use of style guides
Use of naming conventions

ISO 26262, Part 6: Product development at the software level
Table 1 — Topics to be covered by **modelling and coding guidelines**

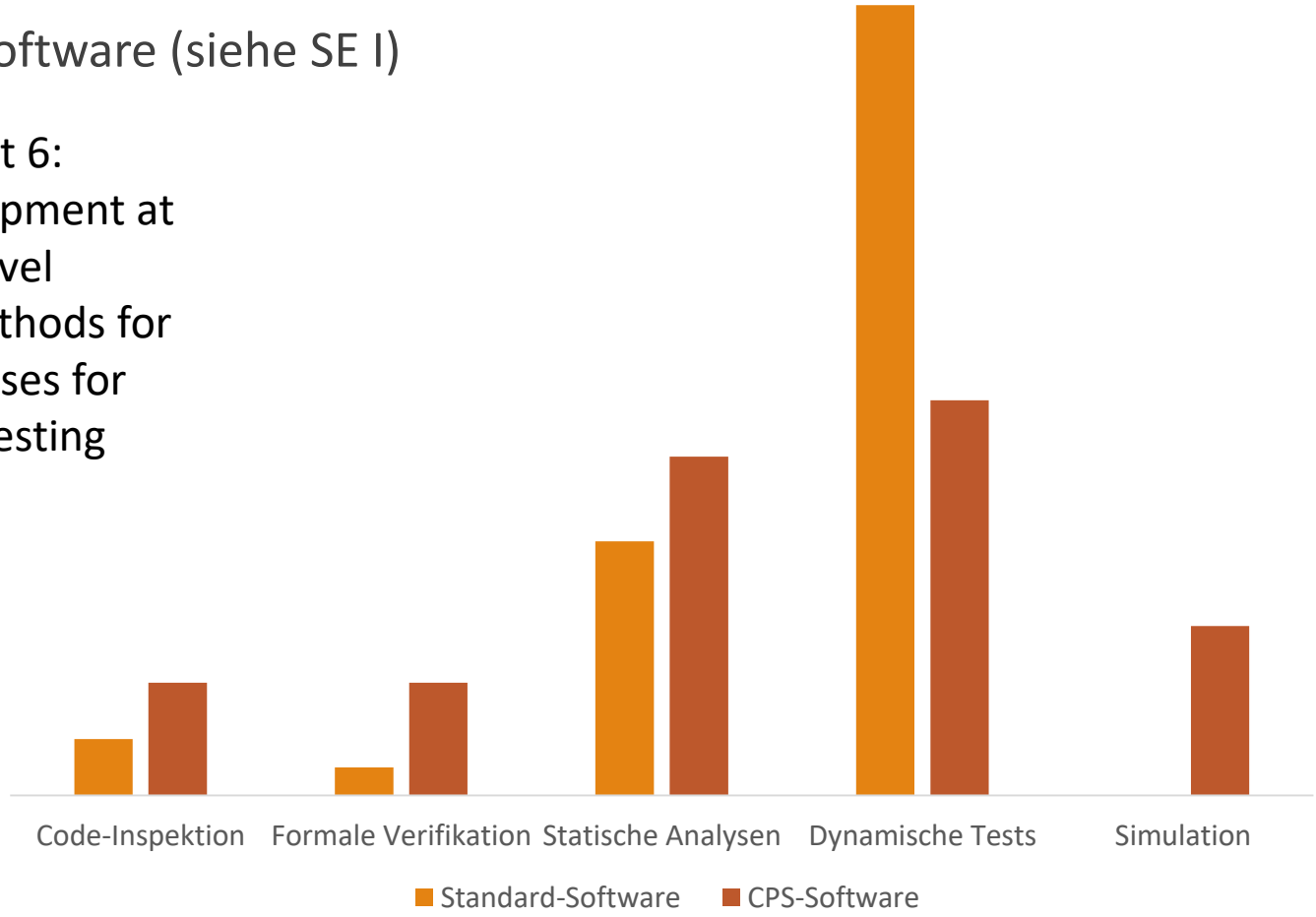
Reaktive Methoden der Software-Qualitätssicherung

- CPS-Software ist zunächst einmal Software
- Qualitätssicherungsmethoden für Standardsoftware (siehe SE I)

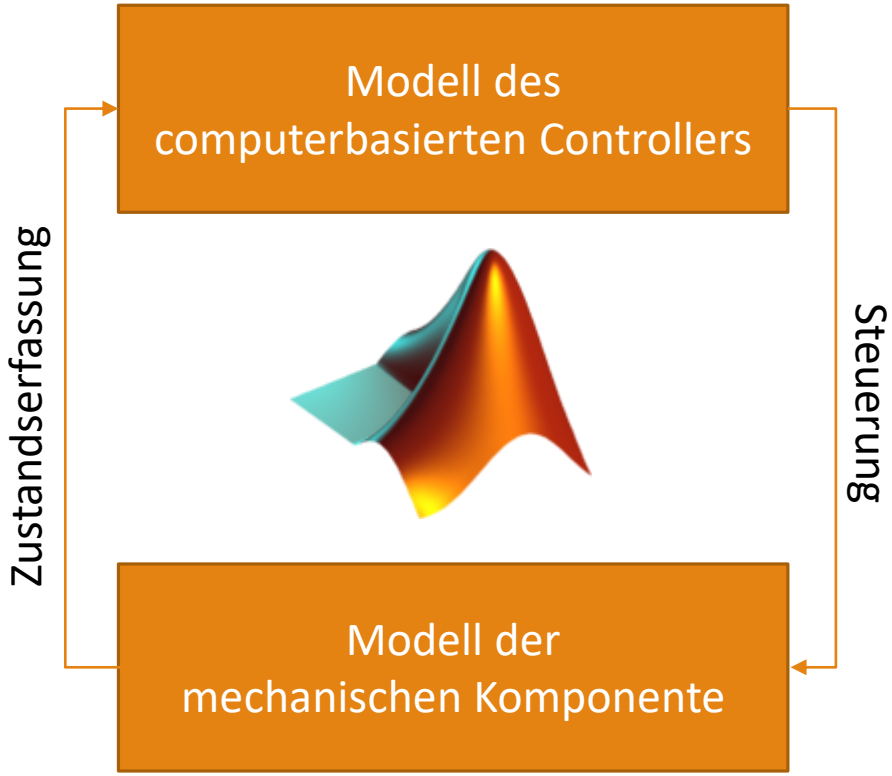
Topic
Analysis of requirements
Generation & analysis of equivalence classes
Analysis of boundary values
Error guessing

ISO 26262 , Part 6:
Product development at the software level
Table 11 — Methods for deriving test cases for software unit testing

- Aber:
  - Verschiebung der Gewichtung
  - Simulation noch nicht vorhandener Hardware

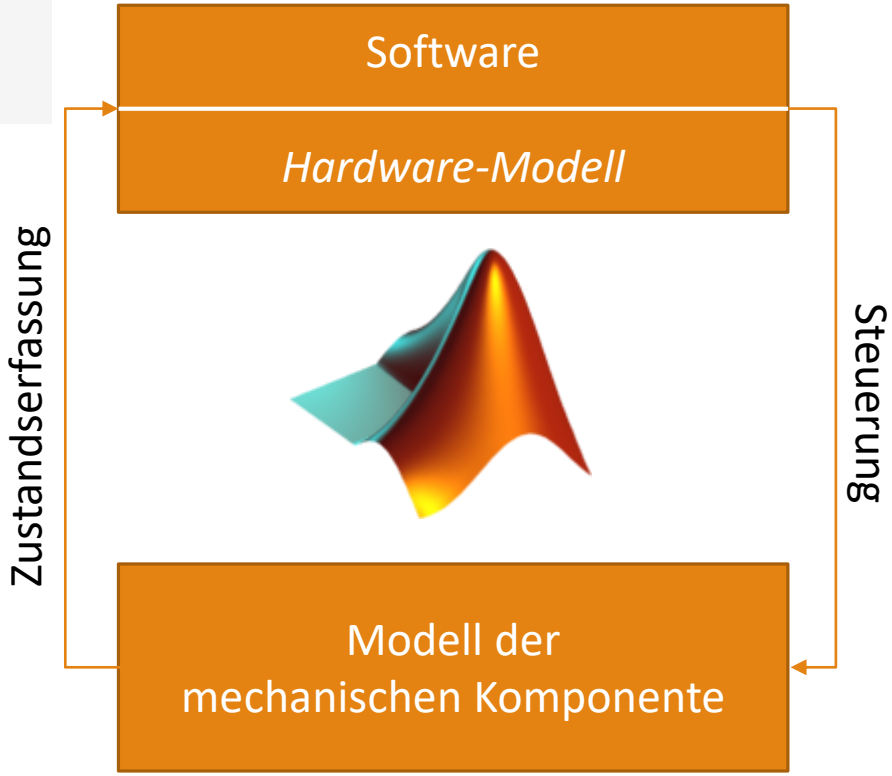


Software-QS ohne Hardware: Modellgetriebene Entwicklung

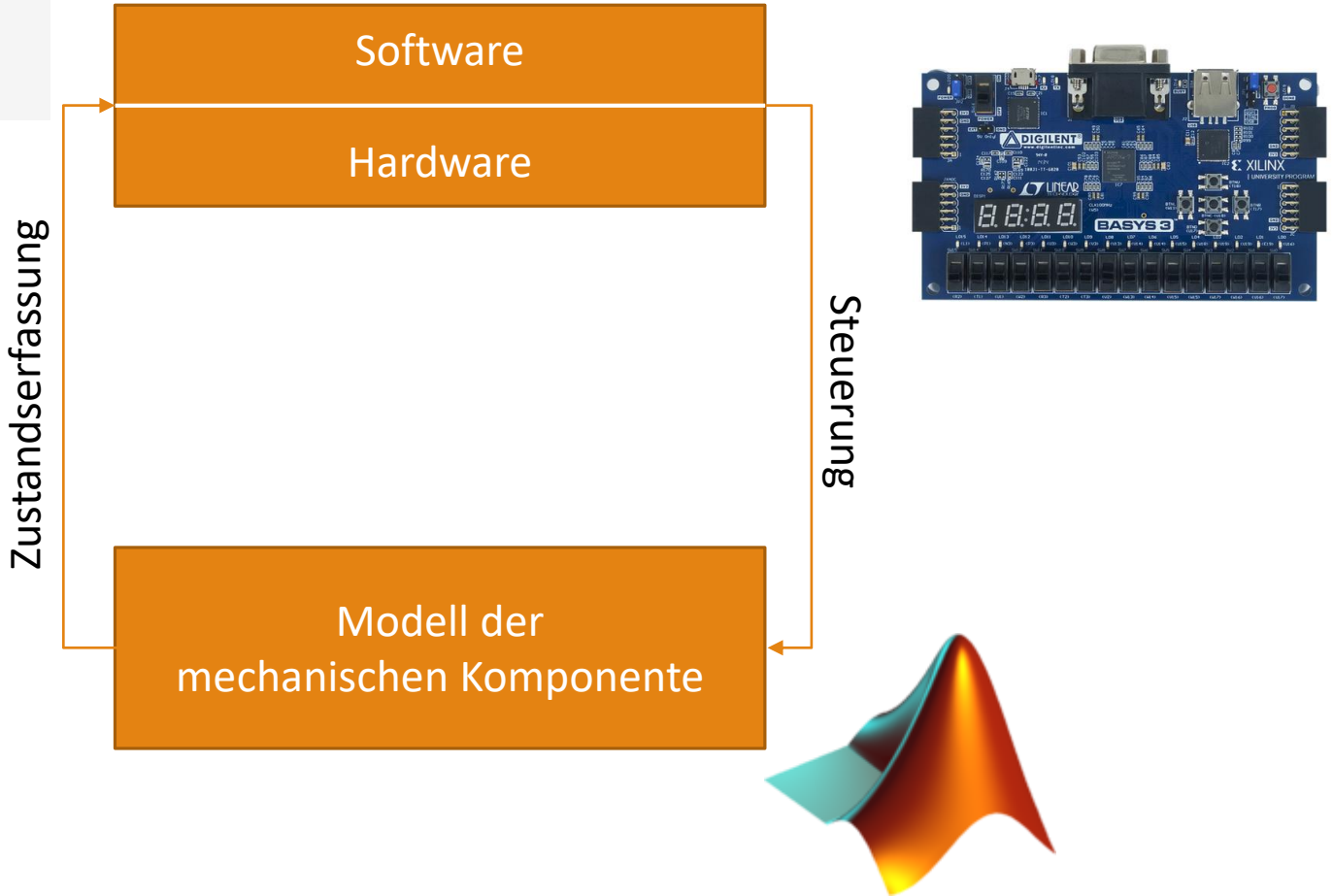


Model in the loop (MIL)

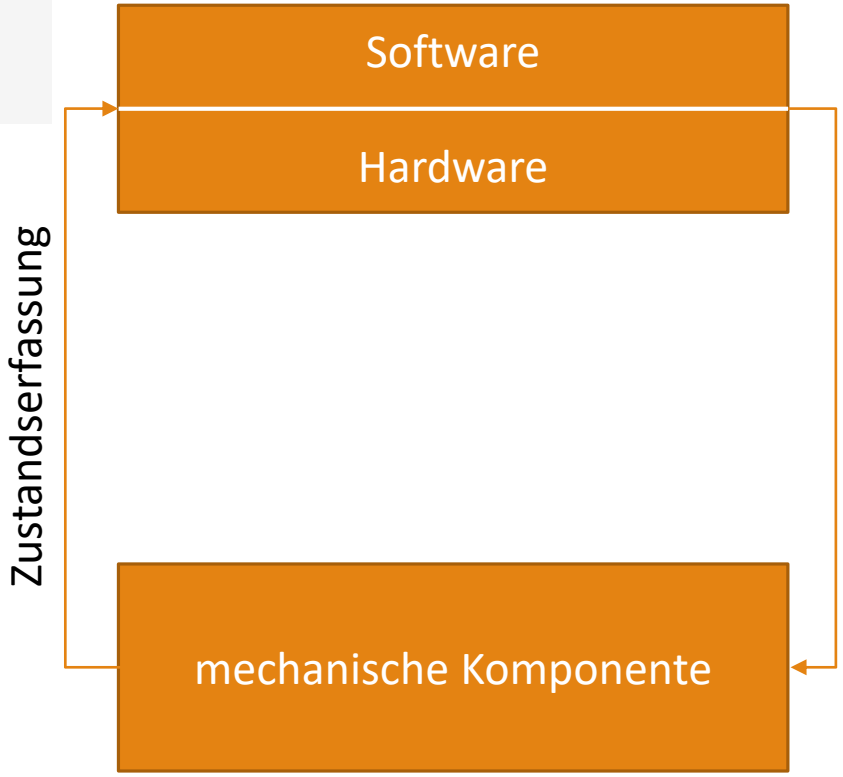
Software in the loop (SIL)

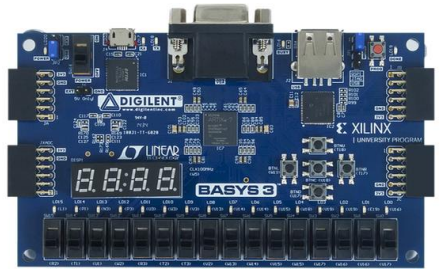


Processor in the loop (PIL)



Hardware in the loop (HIL)





Bewertung des modellbasierten Ansatzes

Kosten:

– Modellerstellung teils sehr komplexer Komponenten

– Fehler im Modell können die Vorteile des Ansatzes zunichte machen

– Ggf. Wiederholung von Tests über die verschiedenen Abstraktionsstufen

Nutzen:

+ Frühestmögliche Fehleridentifikation

+ Inkrementelle Integration des Systems und der Tests → beherrschbare Komplexität

+ Quasi-Industriestandard mit exzellenter Werkzeugunterstützung (z.B. Matlab/Simulink)

Zusammenfassung

1. Was sind Anwendungsgebiete cyber-physische Systeme und aus welchen Komponenten bestehen sie?
2. Welche grundlegenden Arten von Qualitätssicherungsmethoden werden in Standards für CPS vorgegeben/empfohlen?
3. Beschreiben sie den inkrementellen modellbasierten Testansatz für cyber-physische Systeme.
4. Sie werden von einem Automobilzulieferer mit der Software-Qualitätssicherung für ein Adaptive-Cruise-Control-System beauftragt. Wie ermitteln Sie geeignete Methoden und Frameworks?

Weiterführende Literatur:

Stephan Grünfelder: Software-Test für Embedded Systems. dpunkt.verlag

Robert Oshana, Mark Kraeling (eds.): Software Engineering for Embedded Systems – Methods, Practical Techniques, and Applications. Elsevier