HEICON
Global Engineering

Software Unit Test:

Autonome Fahrzeuge getestet mit Luftfahrt Best Practice

HEICON Global Engineering
Kreuzweg 22, 88477 Schwendi

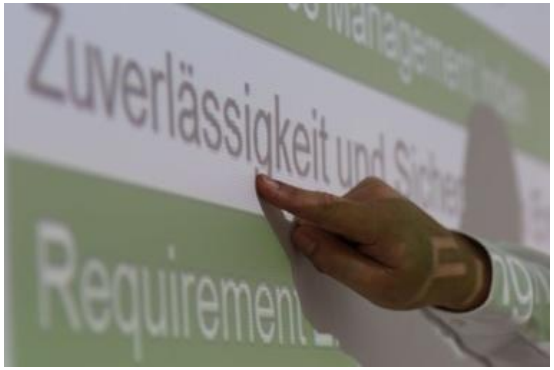
Internet: www.heicon-ulm.de
Blog: http://blog.heicon-ulm.de

HEICON
Global Engineering

- Beobachtungen Unittests
- Vergleich von Luftfahrt und Automotive
- Beispiele unterschiedlicher Interpretationen der Normen
- Werkzeuge
- Best Practice Luftfahrt
- Kontakt - Veröffentlichungen

Vorstellung – Martin Heininger

1993 – 1998 Studium Elektrotechnik
1998 – 2004 Tescom, Ulm
2004 – 2005 Diehl Avionik, Überlingen
2005 – heute Inhaber HEICON



HEICON
Global Engineering

- Beobachtungen Unittests
- Vergleich von Luftfahrt und Automotive
- Beispiele unterschiedlicher Interpretationen der Normen
- Werkzeuge
- Best Practice Luftfahrt
- Kontakt - Veröffentlichungen

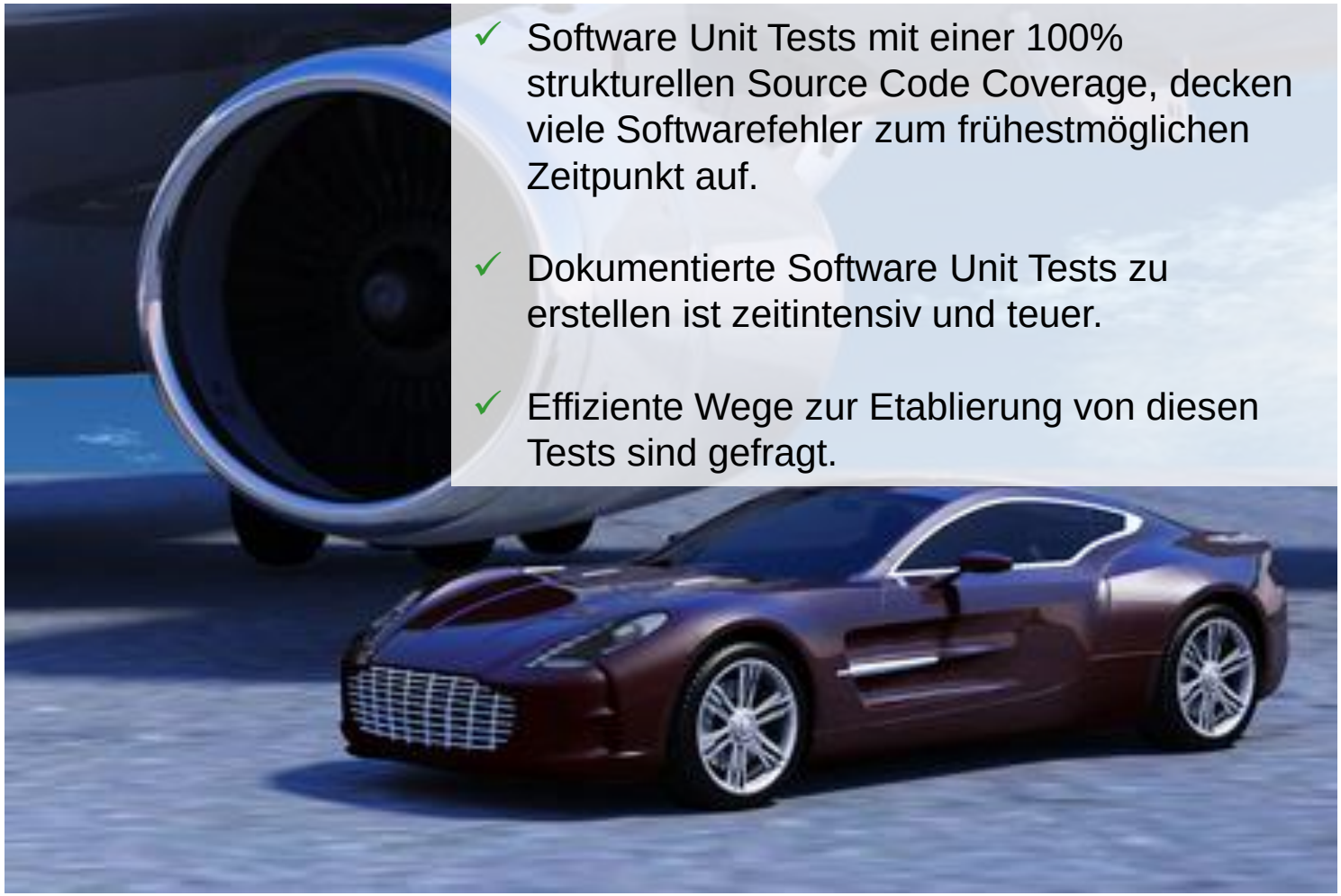
Beobachtungen Unittests

HEICON
Global Engineering

- ✓ Die funktionalen Sicherheitsstandards ISO 26262 und IEC 61508 fordern diese Tests.
- ✓ Die Luftfahrtbranche mit ihrem Standard DO-178C hat jahrzehntelange Praxis-erfahrungen.

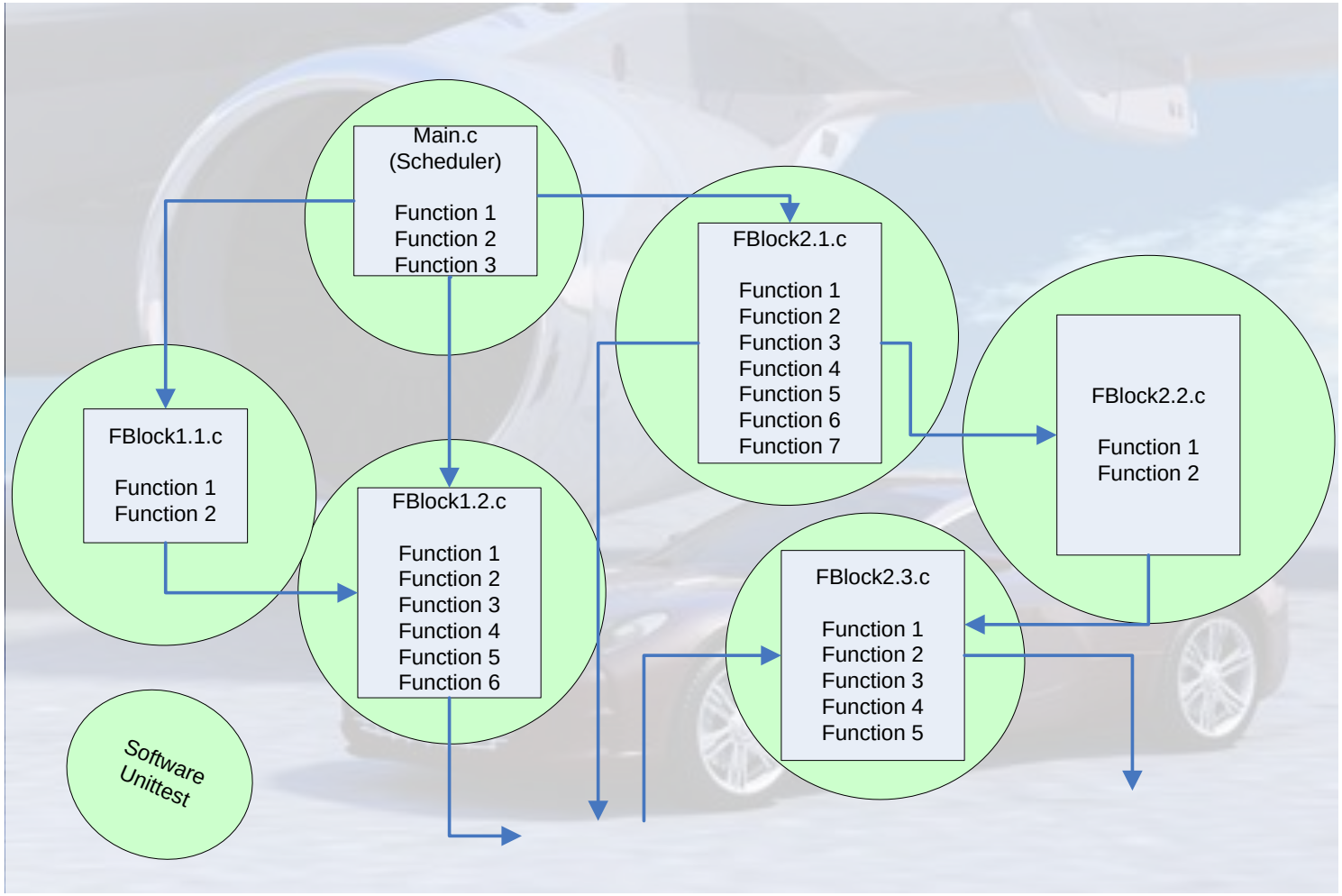
Beobachtungen Unittests

HEICON
Global Engineering

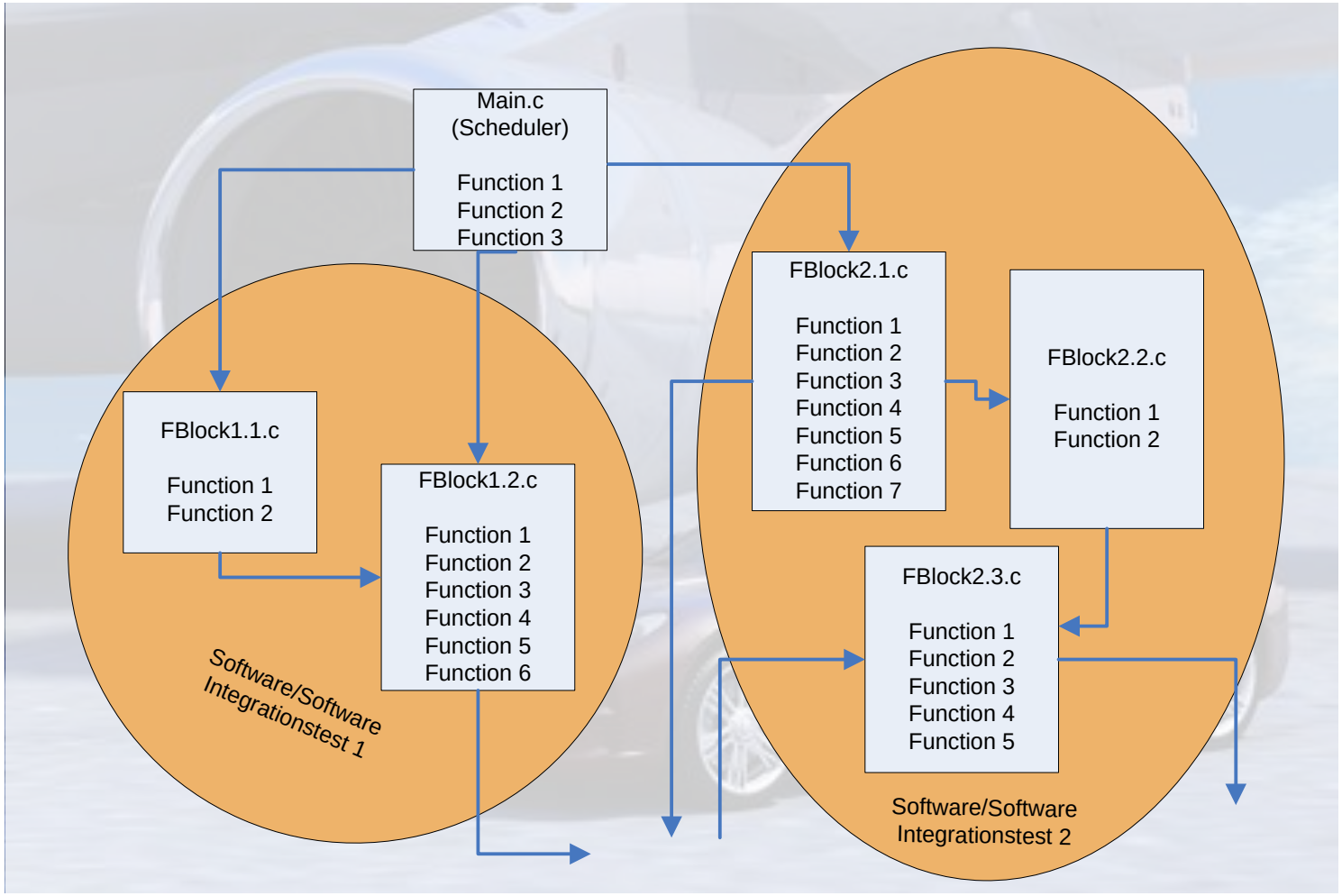


- ✓ Software Unit Tests mit einer 100% strukturellen Source Code Coverage, decken viele Softwarefehler zum frühestmöglichen Zeitpunkt auf.
- ✓ Dokumentierte Software Unit Tests zu erstellen ist zeitintensiv und teuer.
- ✓ Effiziente Wege zur Etablierung von diesen Tests sind gefragt.

Beobachtungen Unittests



Beobachtungen Unittests



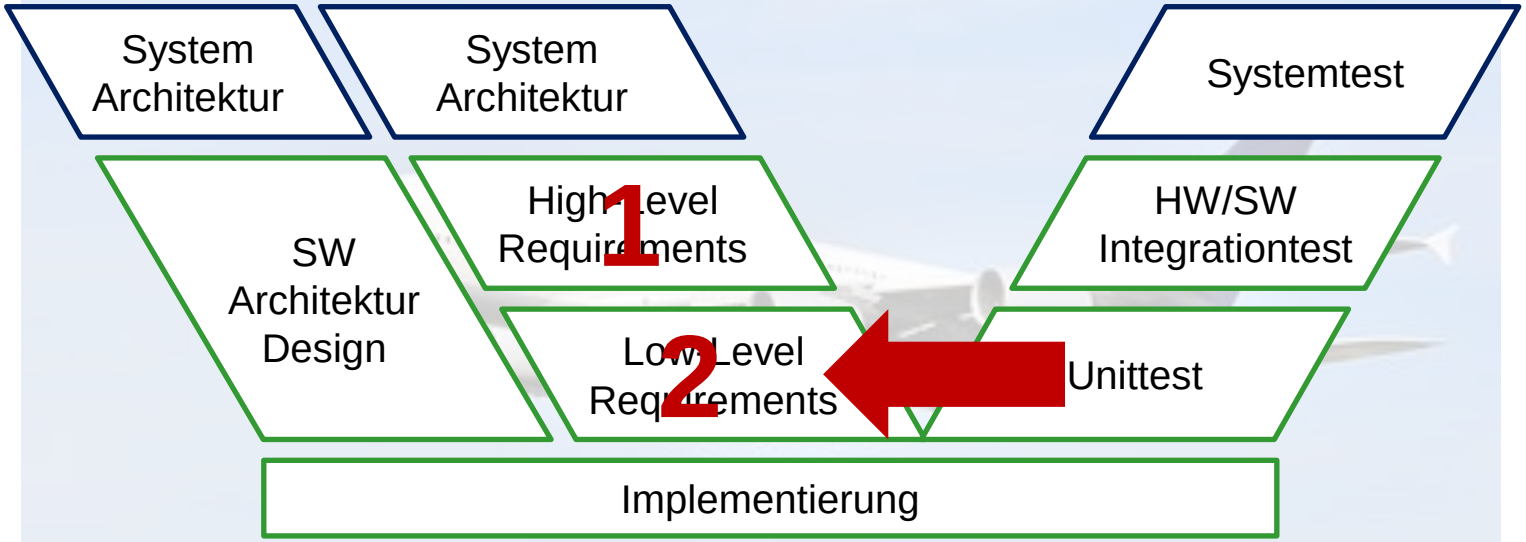
HEICON
Global Engineering

- Beobachtungen Unittests
- **Vergleich von Luftfahrt und Automotive**
- Beispiele unterschiedlicher Interpretationen der Normen
- Werkzeuge
- Best Practice Luftfahrt
- Kontakt - Veröffentlichungen

Vergleich von Luftfahrt und Automotive

HEICON
Global Engineering

Requirements – Luftfahrt:



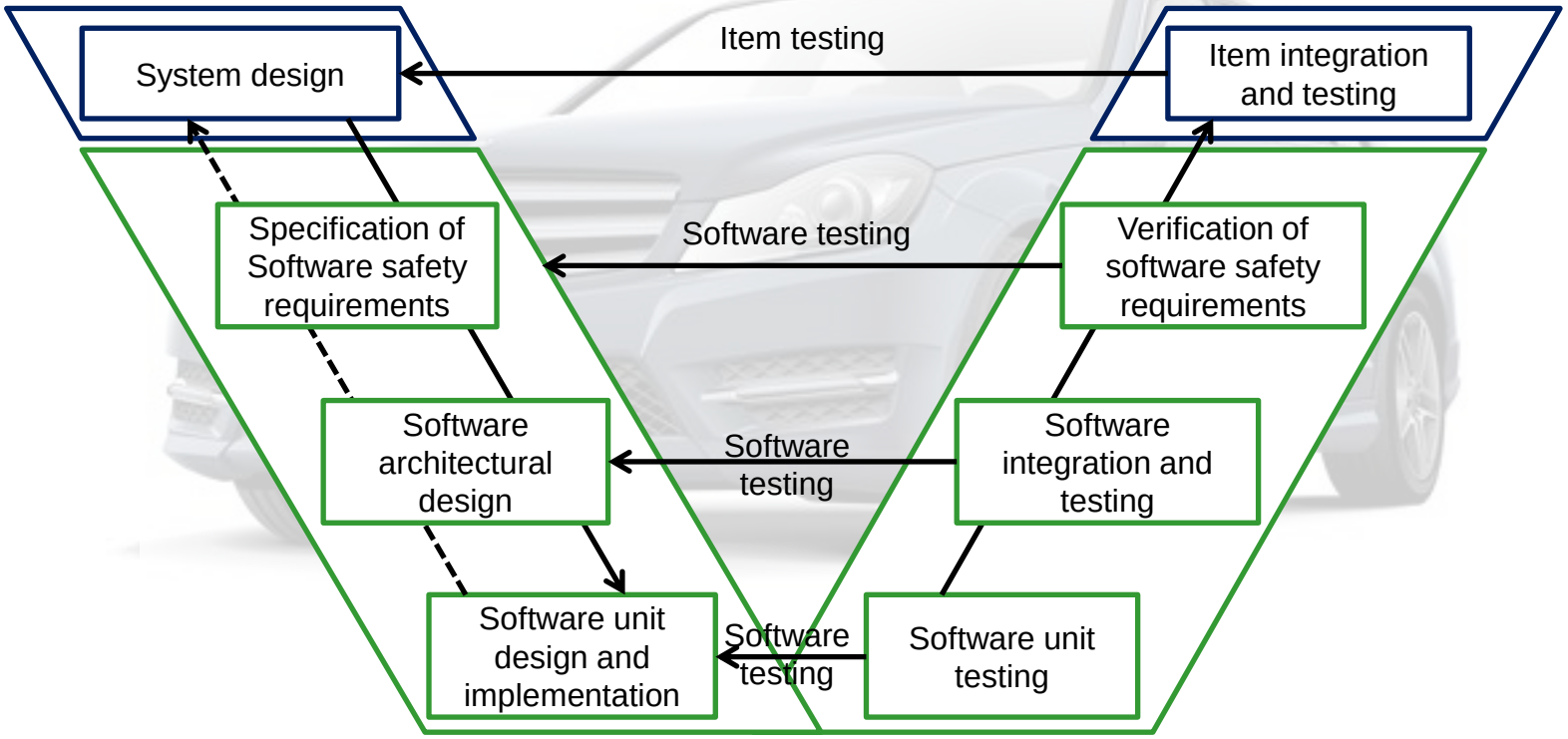
+

- ✓ Normal Test Cases
- ✓ Robustness Test Cases
- ✓ 100% Structural Coverage

Vergleich von Luftfahrt und Automotive

HEICON
Global Engineering

Requirements – Automotive:



Vergleich von Luftfahrt und Automotive

HEICON
Global Engineering

Requirements:

	Luftfahrt - DO-178C	Applicability by SW Level			
	Verification of Outputs of Software Requirements Process	**A**	**B**	**C**	**D**
	High-level requirements comply with system requirements	●	●	○	○
	High-level requirements are accurate and consistent	●	●	○	○
	High-level requirements are compatible with target computer	○	○		
	High-level requirements are verifiable	○	○	○	
	High-level requirements conform to standards	○	○	○	
	High-level requirements are traceable to system requirements	○	○	○	○
	Algorithms are accurate	●	●	○	

Automotive - ISO 26262 –
Part 6 Chapter 6: Specification of software safety requirements

Vergleich von Luftfahrt und Automotive

HEICON
Global Engineering

Requirements:

	Luftfahrt - DO-178C	Applicability by SW Level			
	Verification of Outputs of Software Design Process	**A**	**B**	**C**	**D**
	Low-level requirements comply with high-level requirements	●	●	○	○
	Low-level requirements are accurate and consistent	●	●	○	○
	Low-level requirements are compatible with target computer	○	○		
	Low-level requirements are verifiable	○	○	○	
	Low-level requirements conform to standards	○	○	○	
	Low-level requirements are traceable to high-level requirements	○	○	○	○
	Algorithms are accurate	●	●	○	

	Automotive - ISO 26262 – Notation for software unit design	**ASIL A**	**ASIL B**	**ASIL C**	**ASIL D**
	Natural language	++	++	++	++
	Informal notations	++	++	+	+
	Semi-formal notations	+	++	++	++
	Formal notations	+	+	+	+

Vergleich von Luftfahrt und Automotive

HEICON
Global Engineering

Strukturelle Coverage:

Luftfahrt - DO-178C	Applicability by SW Level			
Verification of Verification Process Results	**A**	**B**	**C**	**D**
Test coverage of software structure (statement coverage) achieved	○	○		
Test coverage of software structure (decision coverage) achieved	●	○	○	
Test coverage of software structure (modified condition/decision coverage) achieved	●	●	○	

Automotive - ISO 26262 – Structural coverage metrics at the software unit level	ASIL A	ASIL B	ASIL C	ASIL D
Statement coverage	++	++	+	+
Branch coverage	+	++	++	++
MC/DC (Modified Condition/Decision Coverage)	+	+	+	++

Vergleich von Luftfahrt und Automotive

HEICON
Global Engineering

Reviews:

	Luftfahrt - DO-178C	Applicability by SW Level			
	Verification of Outputs of Software Coding&Integration	**A**	**B**	**C**	**D**
	Source Code complies with low-level requirements	●	●	○	
	Source Code complies with software architecture	●	○	○	
	Source Code is verifiable	○	○		
	Source Code conforms to standards	○	○	○	
	Source Code is traceable to low-level requirements	○	○	○	
	Source Code is accurate and consistent	●	○	○	
	Output of software integration process is complete and correct	○	○	○	

	Automotive - ISO 26262 – Methods for the verification of software unit design and implementation	**ASIL A**	**ASIL B**	**ASIL C**	**ASIL D**
	Walk-through	++	+	o	o
	Inspection	+	++	++	++
	Static code analysis	+	++	++	++
	Formal Verification	o	o	+	+

Vergleich von Luftfahrt und Automotive

HEICON
Global Engineering

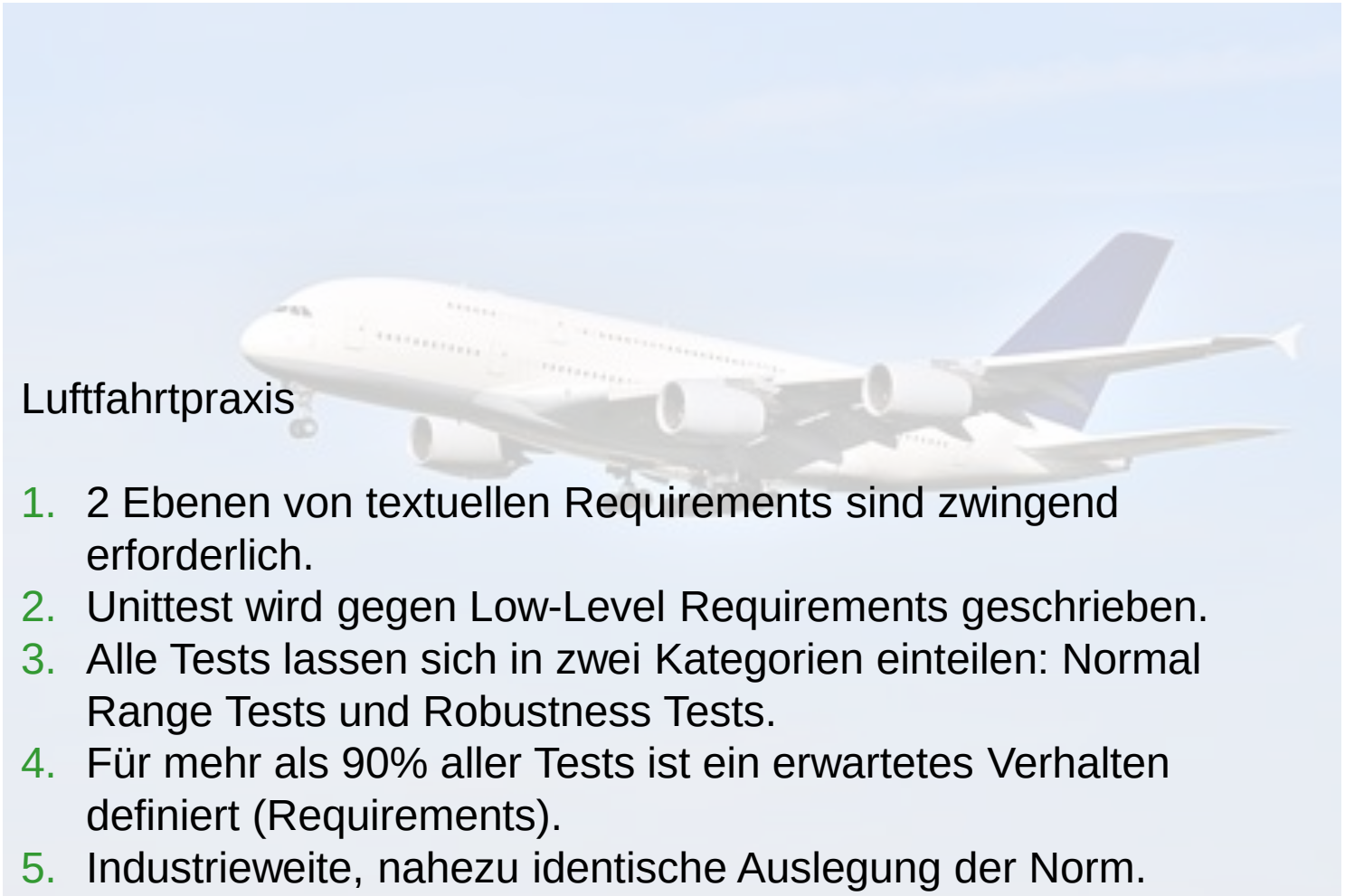
Reviews:

Luftfahrt - DO-178C	Applicability by SW Level			
Verification of Verification Process Results	**A**	**B**	**C**	**D**
Test coverage of software structure (data coupling and control coupling) achieved	●	●	○	

Automotive - ISO 26262 – Methods for the verification of software unit design and implementation	ASIL A	ASIL B	ASIL C	ASIL D
Control flow analysis	+	+	++	++
Data flow analysis	+	+	++	++

Vergleich von Luftfahrt und Automotive

HEICON
Global Engineering

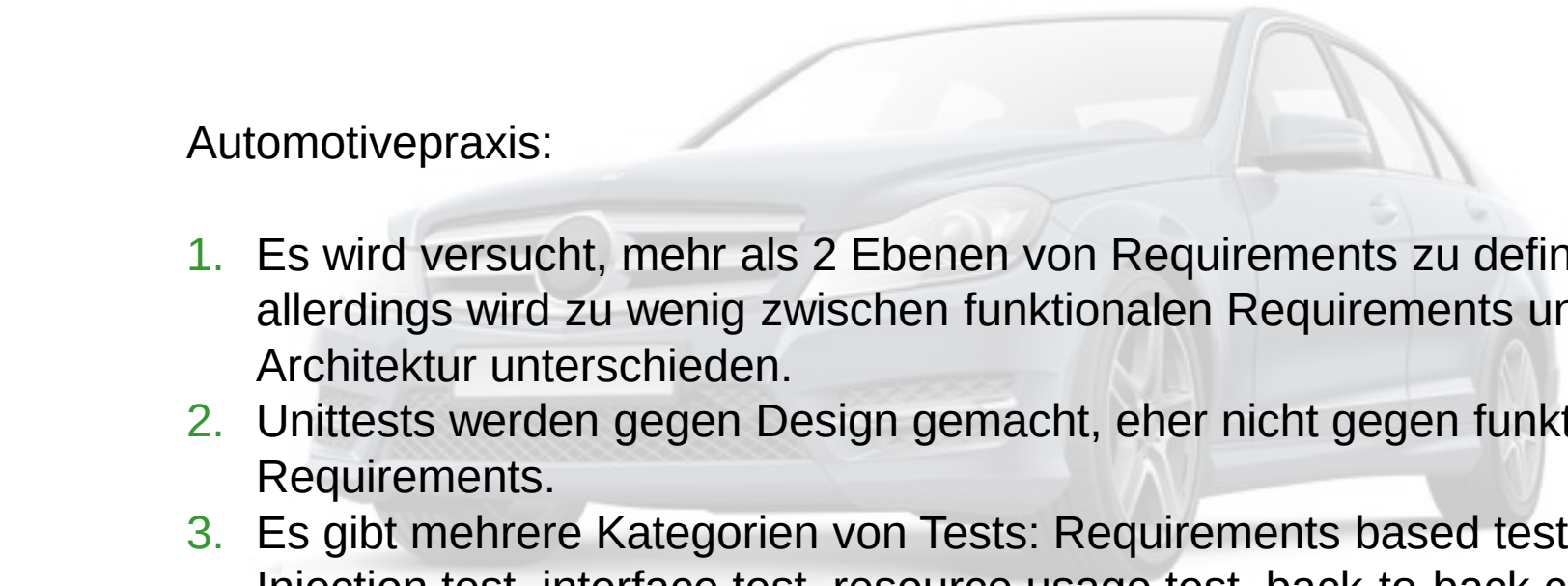


Luftfahrtpraxis

1. 2 Ebenen von textuellen Requirements sind zwingend erforderlich.
2. Unittest wird gegen Low-Level Requirements geschrieben.
3. Alle Tests lassen sich in zwei Kategorien einteilen: Normal Range Tests und Robustness Tests.
4. Für mehr als 90% aller Tests ist ein erwartetes Verhalten definiert (Requirements).
5. Industrieweite, nahezu identische Auslegung der Norm.

Vergleich von Luftfahrt und Automotive

HEICON
Global Engineering



Automotivepraxis:

1. Es wird versucht, mehr als 2 Ebenen von Requirements zu definieren – allerdings wird zu wenig zwischen funktionalen Requirements und Architektur unterschieden.
2. Unittests werden gegen Design gemacht, eher nicht gegen funktionale Requirements.
3. Es gibt mehrere Kategorien von Tests: Requirements based testing, fault Injection test, interface test, resource usage test, back-to-back comparision between model and code.
4. Es sind viele unterschiedliche Interpretationen der Norm in der Branche vorhanden.

HEICON
Global Engineering

- Beobachtungen Unittests
- Vergleich von Luftfahrt und Automotive
- **Beispiele unterschiedlicher Interpretationen der Normen**
- Werkzeuge
- Best Practice Luftfahrt
- Kontakt - Veröffentlichungen

Beispiele unterschiedlicher Interpretationen

HEICON Global Engineering

Umfang von Reviews

Automobil Branche

- ✓ Gefundene Fehler im Review werden oft ohne weitere Dokumentation eingearbeitet.
- ✓ Inhalt einzelner Reviews ist nicht immer nachvollziehbar definiert (Checkliste).

Luftfahrtbranche

- ✓ Durchführung von Code-, Requirements-, Design-Reviews müssen nachgewiesen werden (Überprüfung im Audit!) => nachvollziehbare Dokumentation von Review Findings.
- ✓ Checklisten werden früh im Projekt dem Assessor vorgelegt.

Beispiele unterschiedlicher Interpretationen

HEICON Global Engineering

100% Strukturelle Code Coverage

<u>Automobil Branche</u>

- ✓ Der Anteil der durch Argumentation erreichten Coverage kann 20% und mehr sein.
- ✓ Tests zur Erreichung der Coverage werden oft gegen den Source Code erstellt.

<u>Luftfahrtbranche</u>

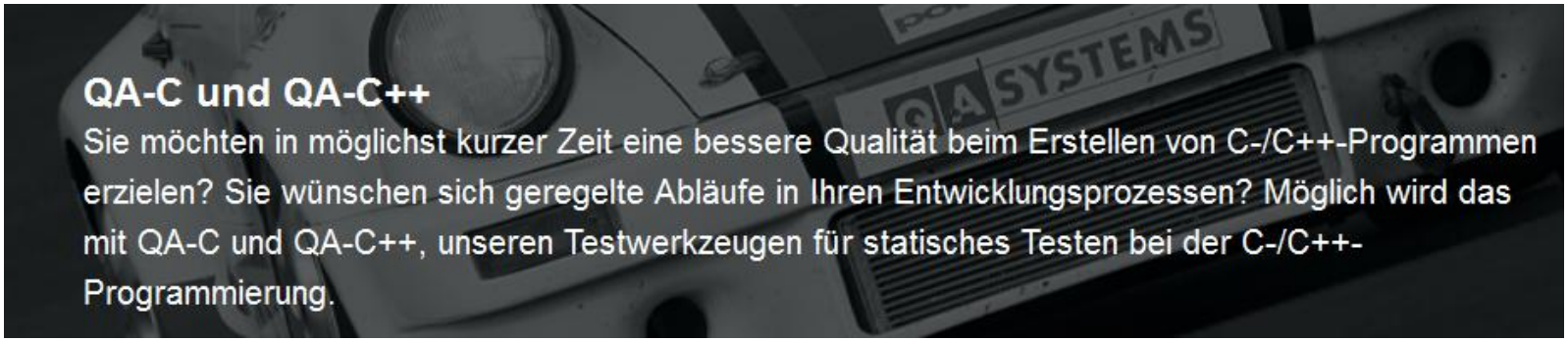
- ✓ Mind. 95% Coverage müssen durch Tests erreicht werden.
- ✓ Tests mit denen die Coverage nachgewiesen wird, müssen gegen Requirements erstellt worden sein (Überprüfung in Audits!).

HEICON
Global Engineering

- Beobachtungen Unittests
- Vergleich von Luftfahrt und Automotive
- Beispiele unterschiedlicher Interpretationen der Normen
- **Werkzeuge**
- Best Practice Luftfahrt
- Kontakt - Veröffentlichungen

Werkzeuge

HEICON
Global Engineering



HEICON
Global Engineering

- Beobachtungen Unittests
- Vergleich von Luftfahrt und Automotive
- Beispiele unterschiedlicher Interpretationen der Normen
- Werkzeuge
- **Best Practice Luftfahrt**
- Kontakt - Veröffentlichungen

Best Practise Luftfahrt

HEICON
Global Engineering

✓ Strukturelle Source Code Coverage	➔ Ideal zum Finden von Req.- und Testlücken
✓ Requirements basiertes Testen	➔ 80% + Strukturelle Source Code Coverage
✓ Funktionale Software Tests	➔ Eine Zielhardware muss nicht immer sein
✓ Traceability	➔ Definieren Sie sich eine Strategie!
✓ Codierrichtlinien	➔ Zuerst Codierstrategie, dann Auswahl von MISRA
✓ Toolqualifikation	➔ Ein gutes Kosten/Nutzen Verhältnis

Kontakt - Veröffentlichungen

Kontaktdaten:

Martin Heininger Dipl.-Ing(FH)

Kreuzweg 22

88477 Schwendi

Tel.: 07353 / 98 17 81

Mobil: 0176 / 24 73 99 60

martin.heininger@heicon-ulm.de

http://www.heicon-ulm.de

Veröffentlichungen:

Leistungselektronik nach ISO 26262 prüfen, ATZ 04/15

Monatlich: Blogbeiträge zu Themen der Funktionalen Sicherheit: http://blog.heicon-ulm.de