



# Automotive SPiCE und IEC 61508 – Synergie oder Widerspruch ?

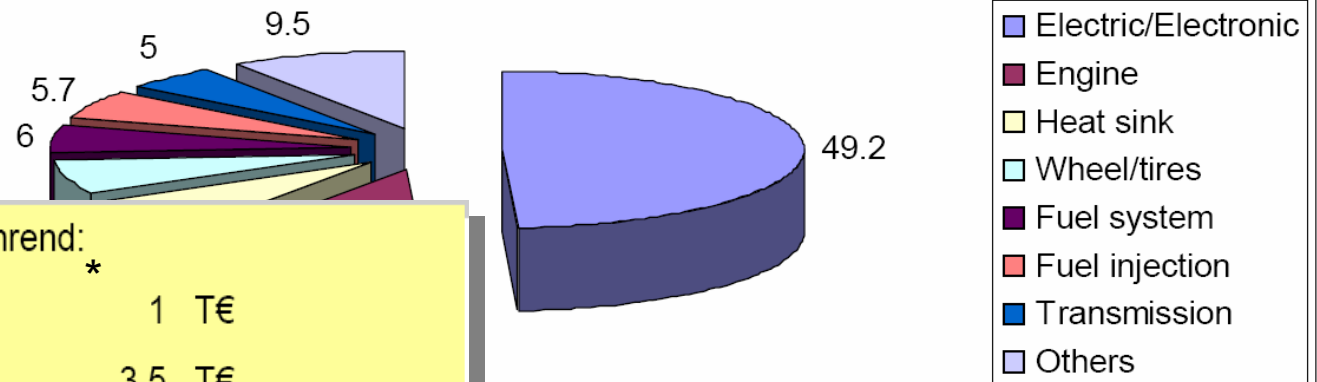
Pierre Metz, Gabriele Schedl

# Problemfelder Produktsicherheit Automotive

Quellen: Der Spiegel, 2001

HIS 2001 (Audi, BMW, DaimlerChrysler, Porsche, Volkswagen)

Distribution of the cause of car problems in Germany (%)



Typische Fehlerbehebung während:

Phase	Cost (T€)
Konzeptphase	1
A-Muster	3,5
B-Muster	4
C-Muster	6
PV-Serie	65
0-Serie	80
Serie	90

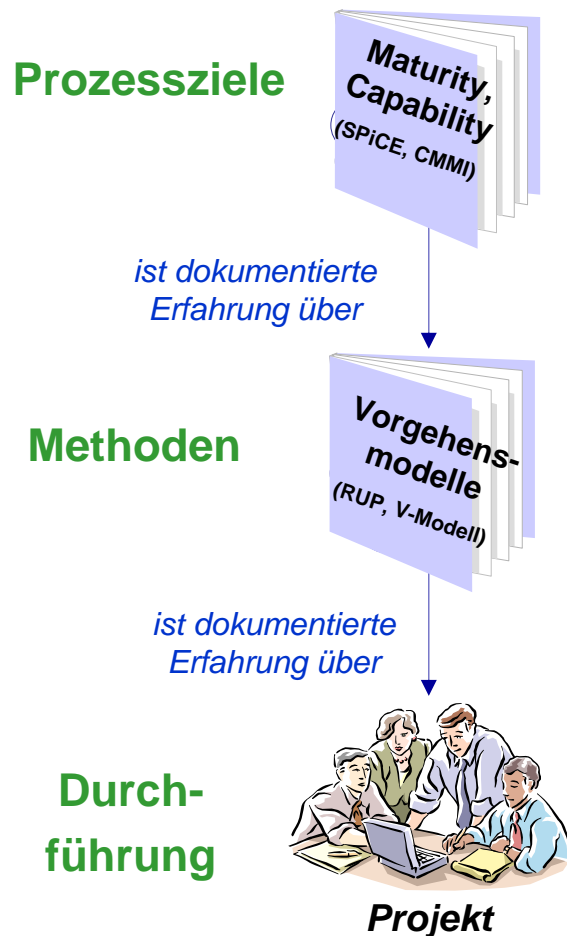
\*) Fahrzeugumrüstung (Umbau, Flashen etc.) nicht berücksichtigt



**Produkthaftung**

# Abstraktionsebenen Standards Systems/SW Engineering

*Beispiel: Sie wollen Automobile herstellen*



**Führe Crashtests durch u. sichere Ergebnisse  
Vergleiche mit Ergebnissen mit Historie !**

## **Methode A:**

**Gegen die Wand fahren und Kraft (N) messen !**

## **Methode B:**

**Mit ganzer Belegschaft gegen Kühlerhaube  
treten und Verformung messen !**

**Peter katapultiert Prototyp 51 um 12:50 bis 13:50  
gegen Crashwand 3.**

# Erfahrung: Gute Prozessqualität führt zu guten Produkten



**Prozessqualität = die Arbeitsweise**

- ✧ Ein Phasen- und Life Cycle Modell einhalten
- ✧ Zusätzliche Tätigkeiten (Review, Planung + Steuerung...)
- ✧ hinreichende Ausbildung + klare Verantwortlichkeiten

...

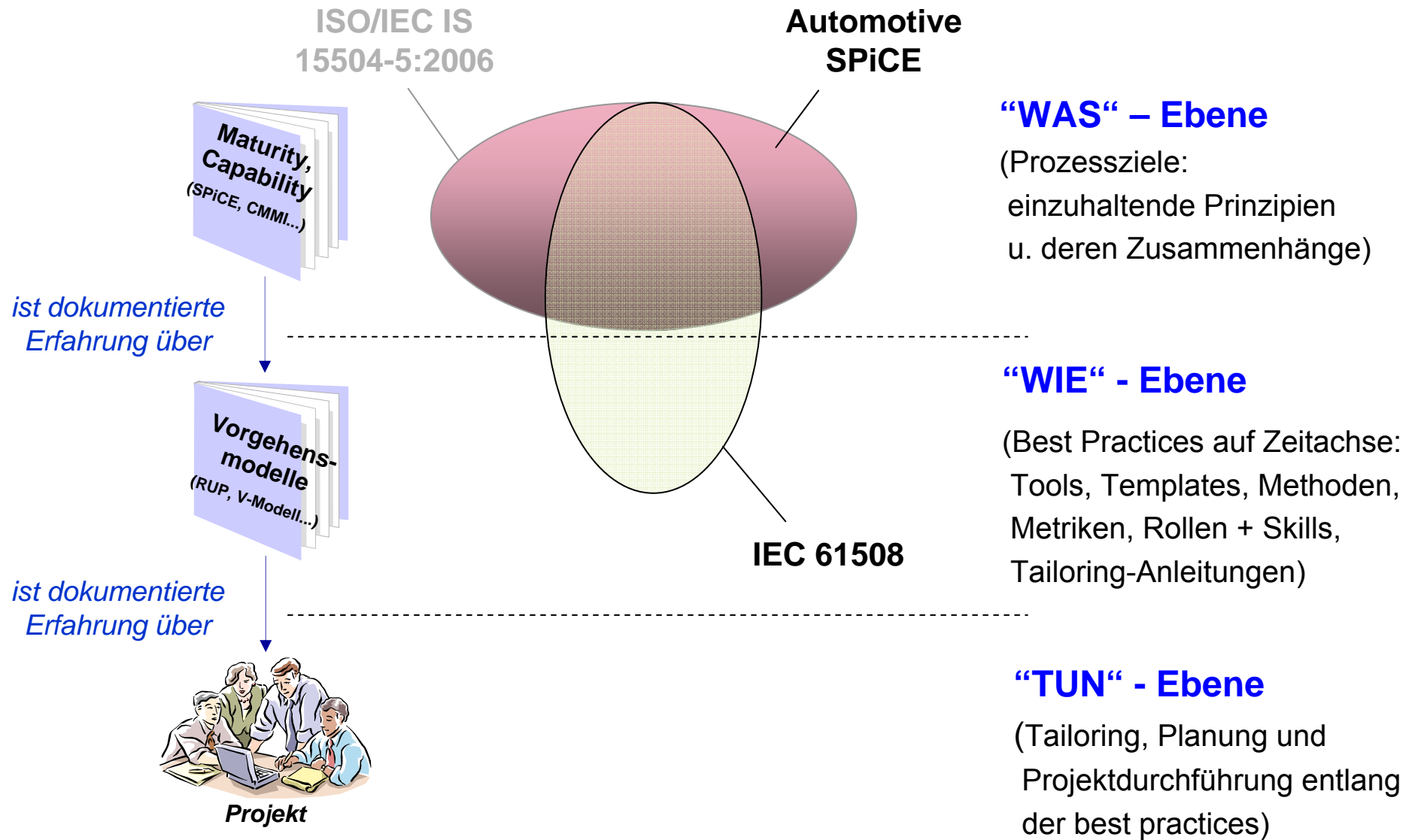


**Produktqualität = das Endergebnis selbst**

- ✧ Erfüllt die Anforderungen (Funktionale & Nicht-Funktionale)
- ✧ Abwesenheit von Fehler
- ✧ Qualität (Robustheit, Wartbarkeit ...)

...

# Automotive SPiCE und IEC 61508 - Konzeptioneller Vergleich



# Automotive SPiCE und IEC 61508 - Konzeptioneller Vergleich

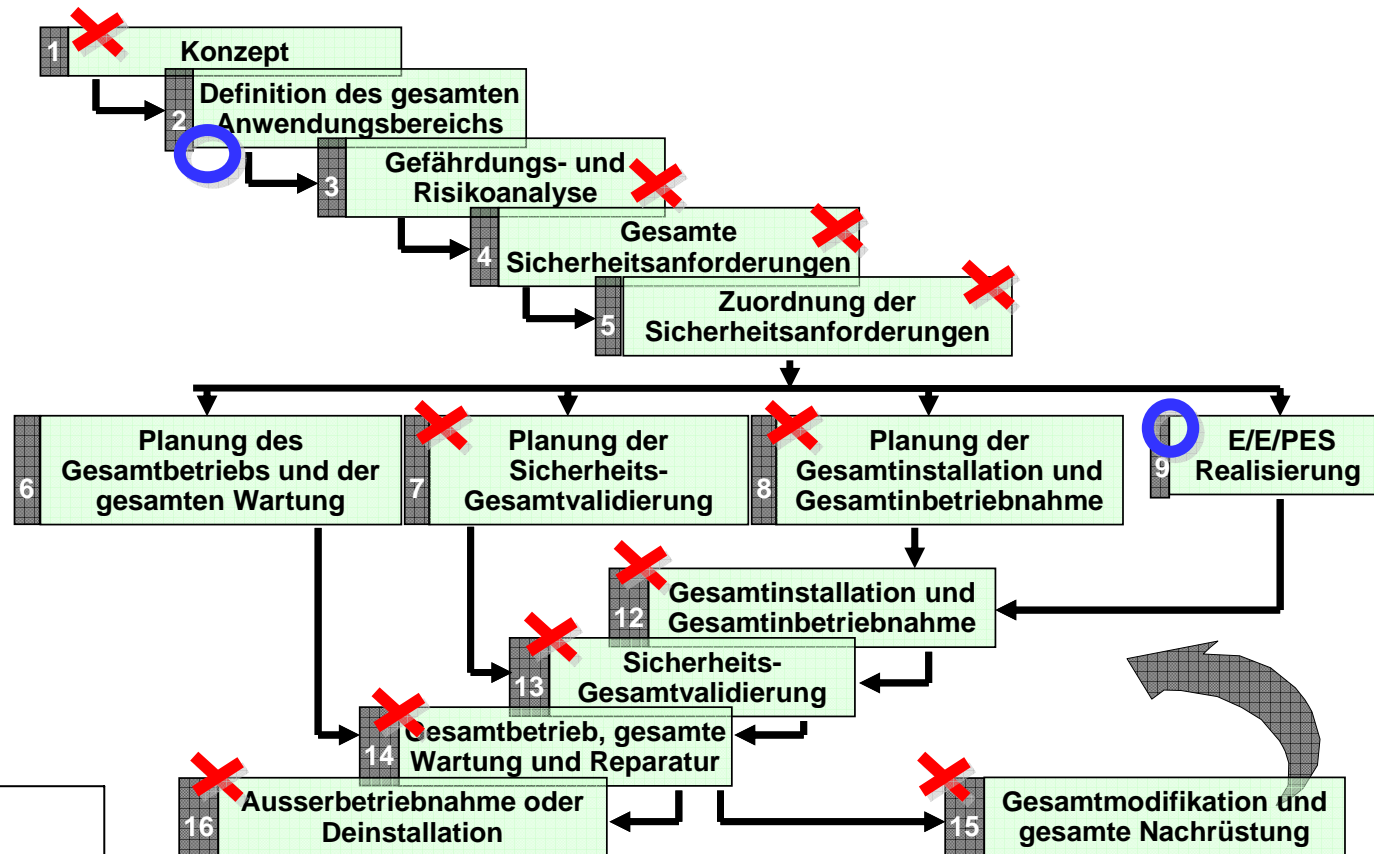
## ISO 15504 / Automotive SPiCE

- Wg. Modellhistorie SW-Fokus, trotzdem hinreichender Systems-Bezug
- Modell für evolutionäre Prozessverbesserung (Capability Dimension)
- Prozessbewertungskriterien und Assessment-Rahmenvorgehen

## IEC 61508

- Gleichberechtigter System und SW-Bezug
- Nur thematisch geordnete, „flache“ Vorgaben, i.e. kein Prozessverbesserungspfad entlang inkrementell zu erklimmender Evolutionsstufen
- Keine Prozessbewertungskriterien, kein Vorgehen für Safety-Assessments

# Inhaltlicher Vergleich – Aus Sicht Sicherheitslebenszyklus 61508





- ✗ Nicht abgedeckt durch Automotive SPiCE
- ◯ partiell abgedeckt durch Automotive SPiCE
- ✓ abgedeckt bei Abdeckung d. entspr. Automotive SPiCE Prozesses


Orthogonal dazu:


- ✧ Functional Safety Management
- ✧ Functional Safety Assessment

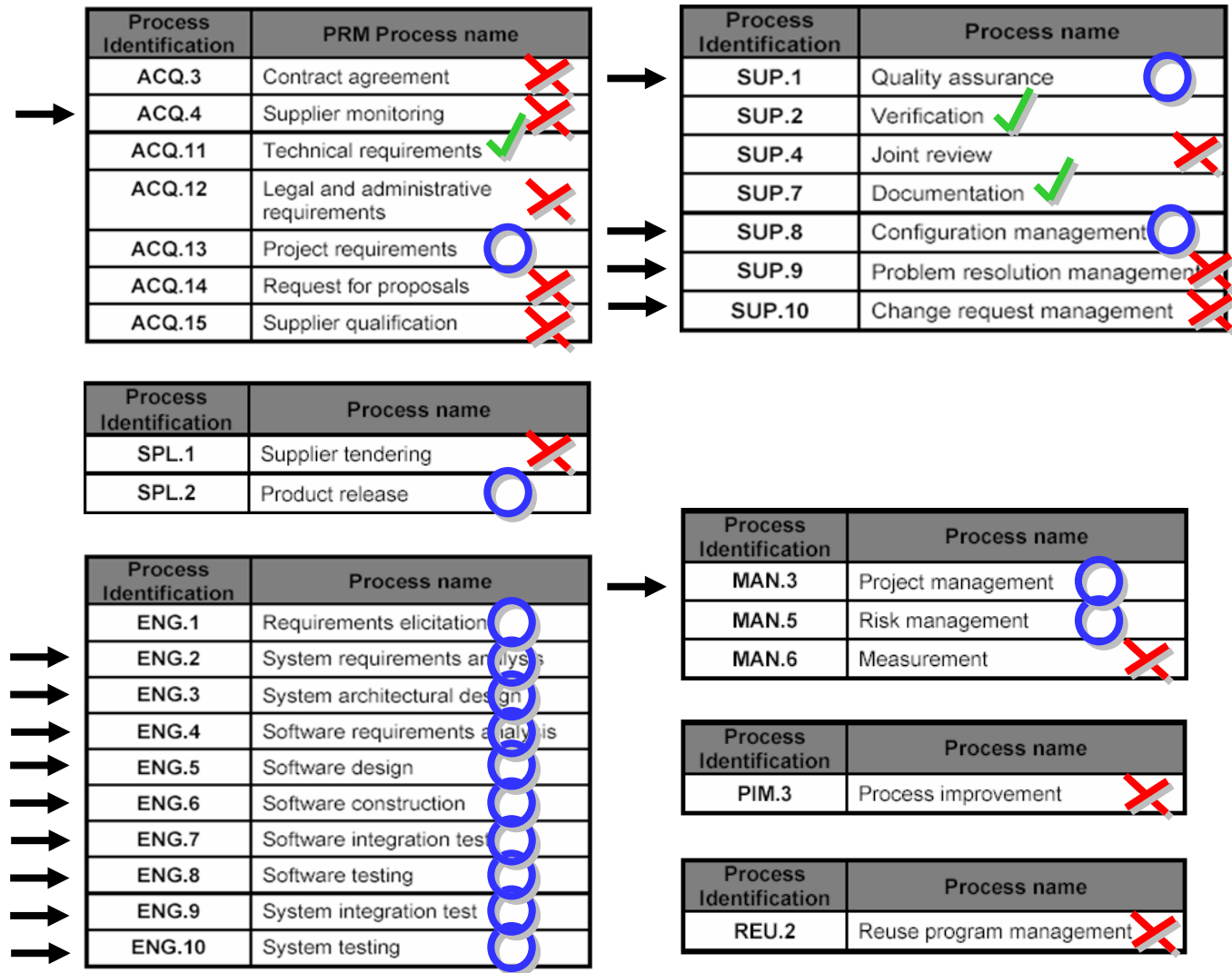
# Inhaltlicher Vergleich – Aus Sicht Automotive SPiCE

 nicht abgedeckt durch IEC 65108

 partiell abgedeckt durch IEC 61508

 abgedeckt bei vollst. Abdeckung d. entspr. IEC 61508 Vorgaben

 HIS Scope



# Prozessfähigkeitsgrade (Capability Levels)

Basierend auf den Messungen werden Standard-Prozesse kontinuierlich verbessert und die Projektarbeit sofort angepasst.

**Level 5 Optimizing**

Prozessdurchführung wird über die Zeit quantitativ gemessen und statistisch ausgewertet, um Vorhersagen zu machen und heute objektiv reagieren zu können.

**Level 4 Predictable**

Set von spez. Standardprozessen im unternehmensweit einheitlich. Anpassungen möglich (Tailoring). Fortentwicklung durch Feedback.

**Level 3 Established**

**Level 2 Managed**

Durchführung wird geplant und gesteuert. Verantwortlichkeiten sind klar definiert. Die Resultate werden konfigurations- u. qualitätsgesichert.

**Level 1 Performed**

Prozessresultate sind vorhanden, kommen aber „irgendwie“ zustande.

**Level 0 Incomplete**

Durchführung und Resultate des Prozesses sind nicht erkennbar oder nicht zielführend.

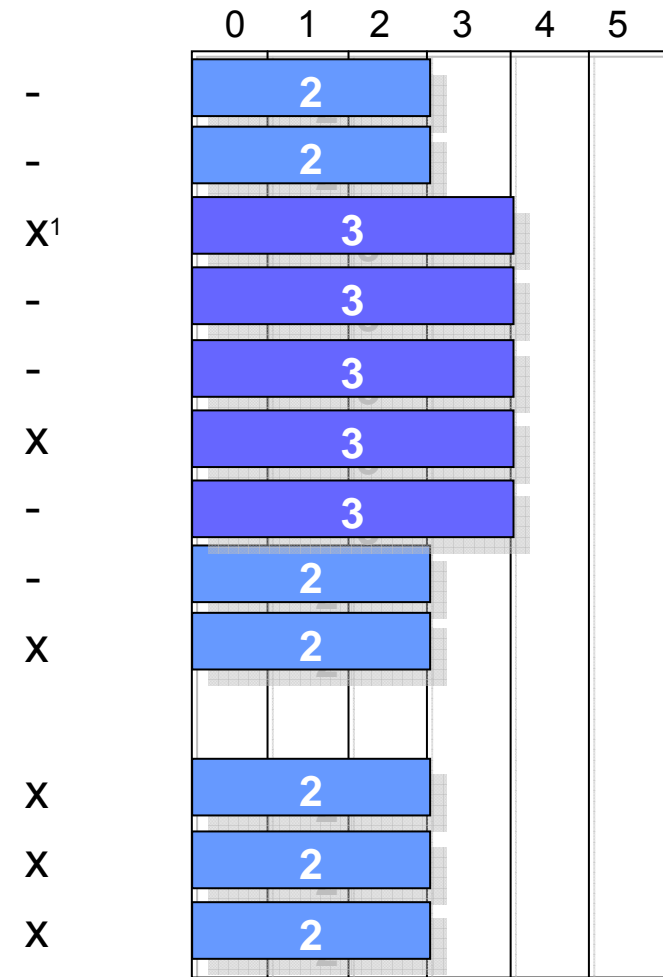
# Target Capability Profile zur Unterstützung safety-kritischer Entwicklung (Vorschlag)

## Automotive SPiCE Prozesse

## HIS-Scope

## Capability Level

- ❖ ACQ.11 – Technical Requirements
- ❖ ACQ.13 – Project Requirements
- ❖ ENG – *alle der ENG-Gruppe*
- ❖ MAN.3 – Project Management
- ❖ MAN.5 – Risk Management
- ❖ SUP.1 – Quality Assurance
- ❖ SUP.2 – Verification
- ❖ SUP.7 – Documentation
- ❖ SUP 8 – Configuration Management
  
- ❖ ACQ.4 – Supplier Monitoring
- ❖ SUP.9 – Problem Resolution Management
- ❖ SUP.10 – Change Request Management



<sup>1</sup> ausgenommen ENG.1 Requirements Elicitation

# Fazit

## Was wir gesehen haben:

- ❖ Automotive SPiCE = *Organisationsentwicklungsmodell*
- ❖ Automotive SPiCE → inkrementell zu hoher Prozessreife
- ❖ IEC 61508 liefert orthogonal Funktionssicherheits-Aspekte

## Man gehe wie folgt vor:

- ❖ Automotive SPiCE als Basis
- ❖ 61508 Inhalte in Automotive SPiCE „integrieren“
- ❖ Nach dieser „Integration“ Ihre(n) Entwicklungsprozesse(e) festlegen (Methodenebene der IEC 61508 beachten)
- ❖ Man betreibe inkrementell Organisational Process Improvement nach dem hier vorgeschlagenen Target Capability Profile

# ...Fragen ?



[gabriele.schedl@frequentis.com](mailto:gabriele.schedl@frequentis.com)



[pierre.metz@synspace.com](mailto:pierre.metz@synspace.com)

