

## Funktionale Sicherheit nach IEC 61508 und ISO 26262

**Software**

00110010100011  
11000011011100  
11100010011001  
11010111111000

**Hardware**

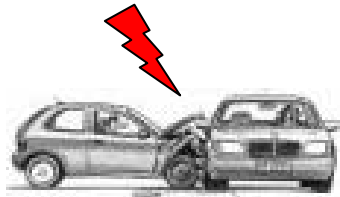


**+** **= ALLES AUTO** | **MOTIVE**

**CLEAR** | **MOTIVE**

# Funktionales Sicherheits Management

CLEAR | MOTIVE

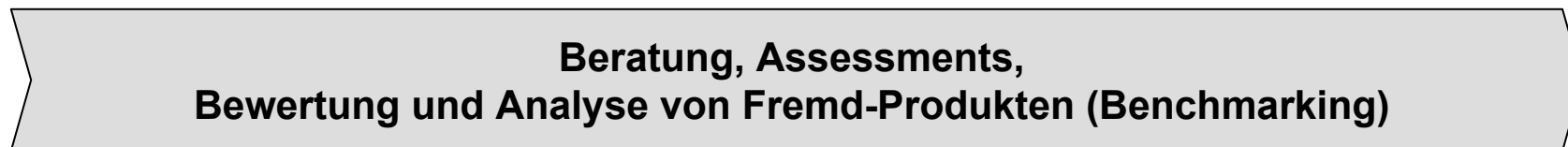


- Gefahren- & Risikoanalyse Ihrer Innovation
- Erstellung der Dokumentation
- Moderation der Safety Aktivitäten
- Nachweis des Safety Cases
- Serienbetreuung der Safetyänderungen




# Funktionales Sicherheits Management

## FSM im Produktlebenszyklus



## Was ist Funktionelle Sicherheit?

Befasst sich mit dem Einfluss von Ausfallrisiken auf Funktionen und somit auf die Sicherheit von Personen und/oder der Umwelt.



***Funktionelle Sicherheit***  
***Bezogenen auf***  
***Elektrisch / Elektronisch /***  
***Programmierbarer Systeme***  
***E/E/EP - Systeme***

**Wurde nach dem Stand der  
Technik entwickelt?**

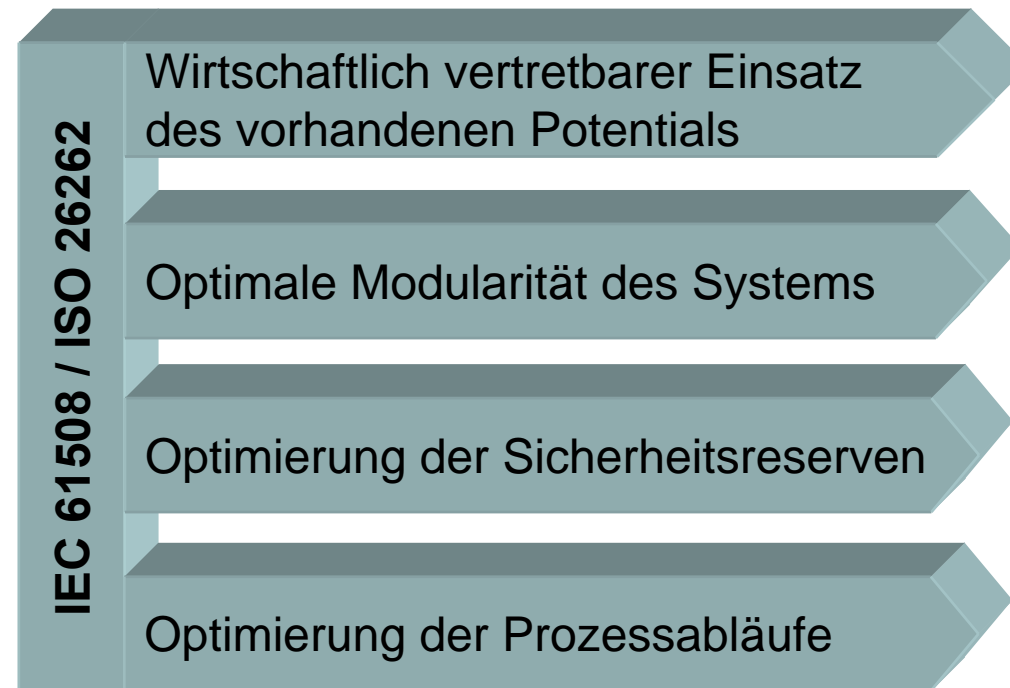
**„Persönlich schuldhaftes  
Verhalten des Entwicklers“  
(§828 BGB-Personenhaftung)**

Ausfälle können auftreten durch:

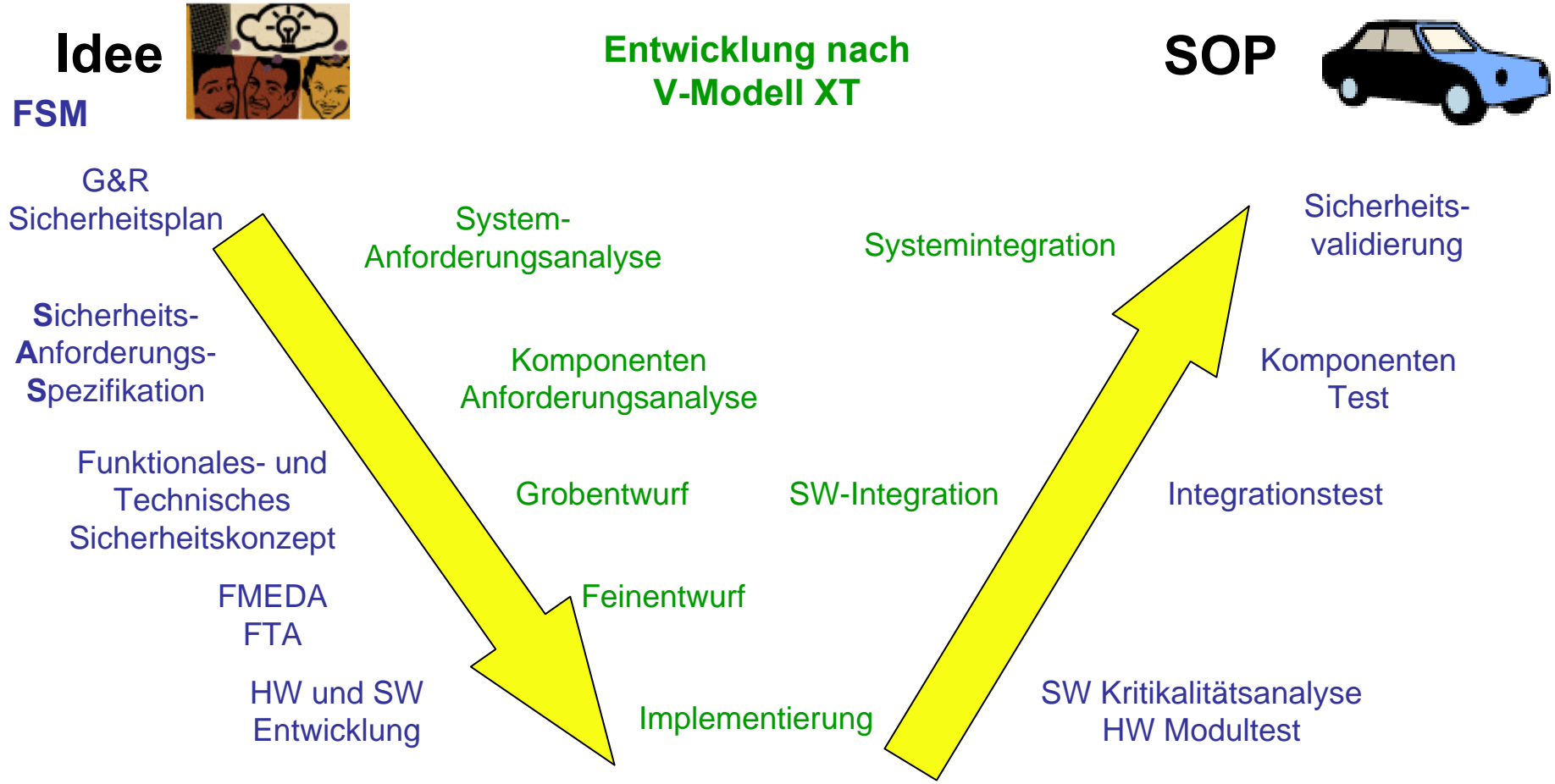


## Ziele: Funktionales Sicherheits Management

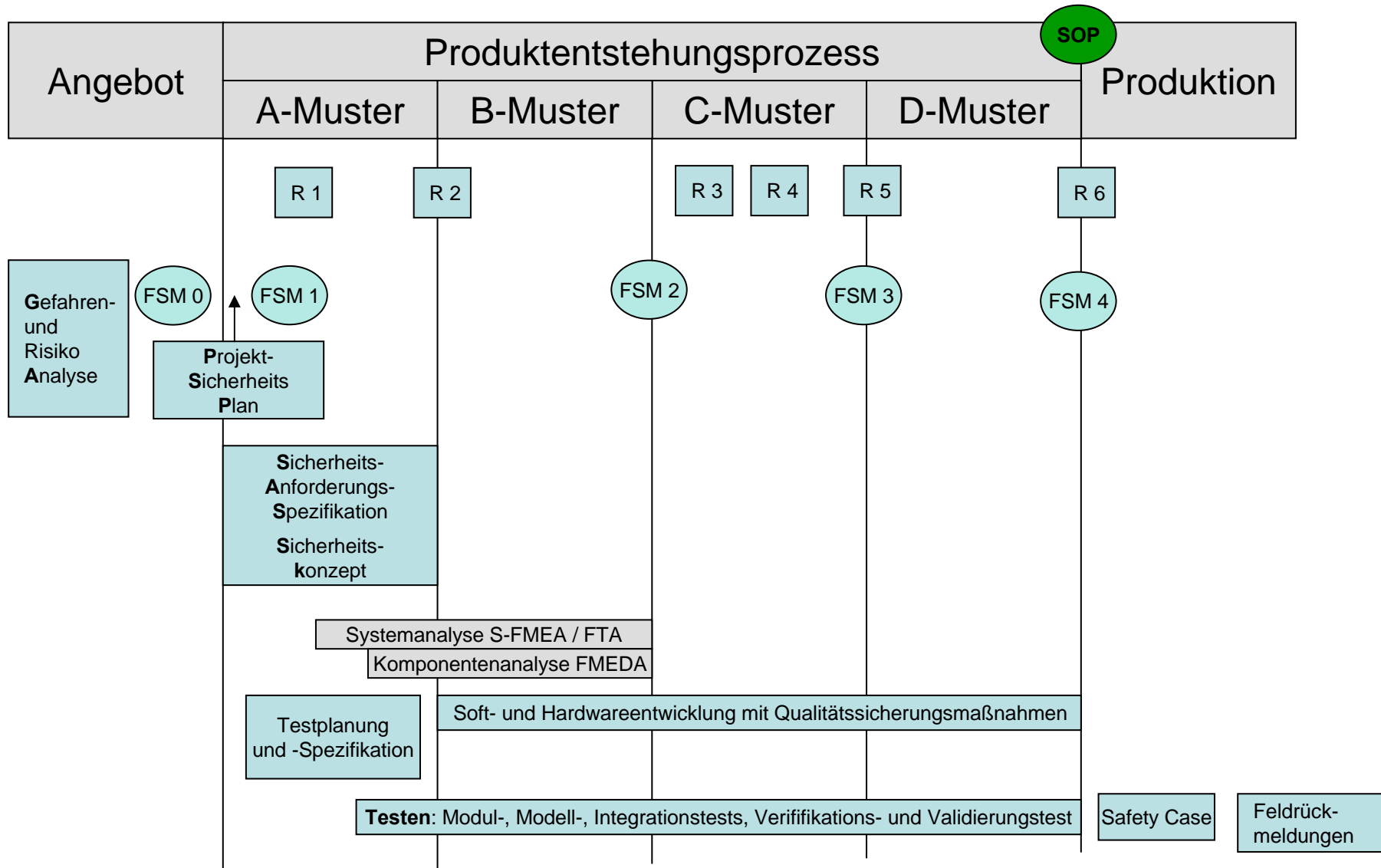
IEC 61508 und ISO 26262 zielen auf:



# Teil 4: FSM orientiert sich am V-Modell XT



# Sachfortschrittsplan



## Teil 5: Gefahren- und Risikoanalyse (GRA) + Sicherheitskonzept (SK)



**Warum ?**

**Erster Schritt: Analyse und  
→ Sicherheitskonzept**

Ziel:

Beurteilung und Bewertung der Gefahr und des Risikos (für z.B. Mensch, Umwelt) das von dem Produkt ausgeht (unter Berücksichtigung aller Rahmenbedingungen)

➡ Bewertung des SIL/ASIL als Grundlage für das weitere Vorgehen

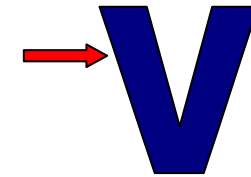
Dokumentation, Ergebnis:

Gefahren- und Risikoanalyse (Review / Unterschrift aller Beteiligten)

Sicherheitskonzept auf Basis der G&R (SIL / ASIL)

## Teil 6: Sicherheits-Anforderungs-Spezifikation (SAS)

CLEAR | MOTIVE



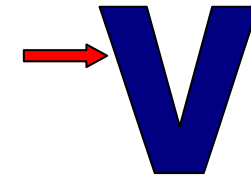
Voraussetzung:  
G&R, Sicherheits Konzept, Anforderungsmanagement

Ziel:  
Übersicht des Gesamtsystems und der Rahmenbedingungen  
Sicherheitsanforderungen und Beschreibung der daraus  
resultierenden Sicherheitsfunktionen (incl. SIL / ASIL)  
Zuordnung der Sicherheitsfunktionen zu den jeweiligen  
Teilsystemen. Erstellung der nach Anforderungsmanagement  
erforderlichen Testfälle

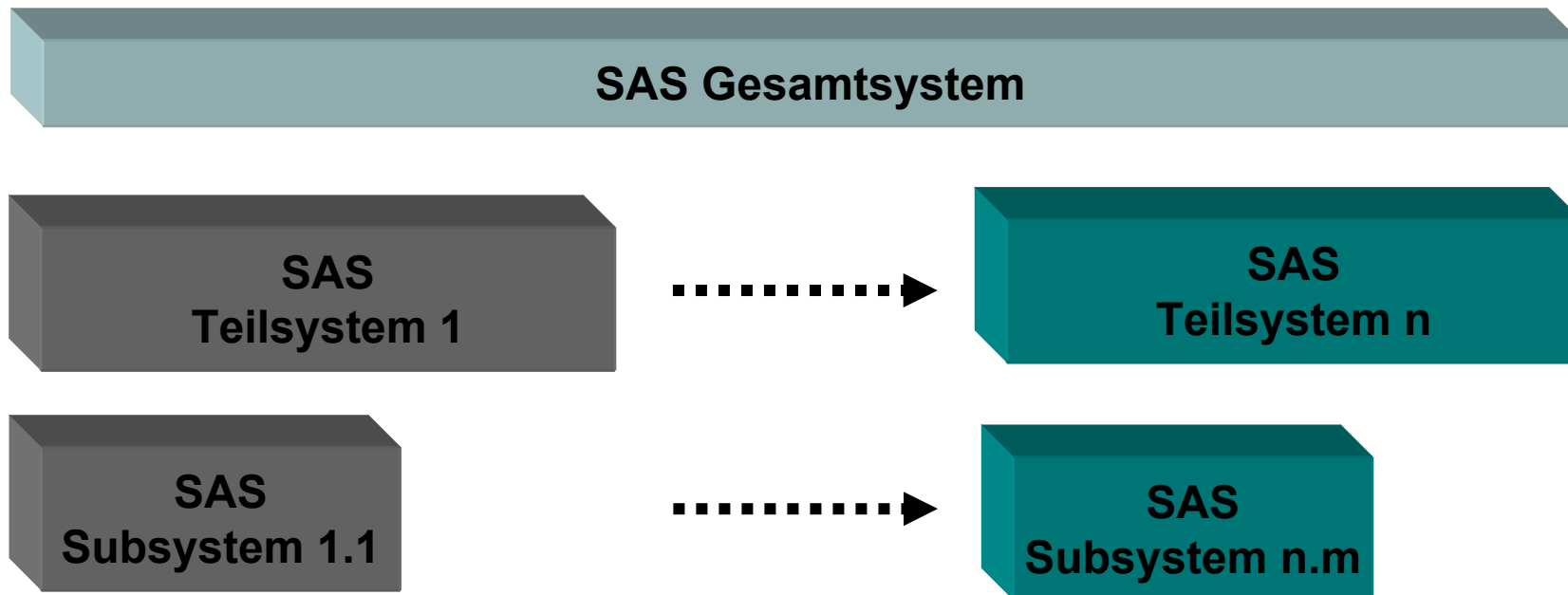
Dokumentation, Ergebnis:  
- Spezifikation der Sicherheitsanforderungen für das System  
- AT Testfiles sind vorhanden

## Teil 6: Sicherheits-Anforderungs-Spezifikation (SAS)

CLEAR | MOTIVE

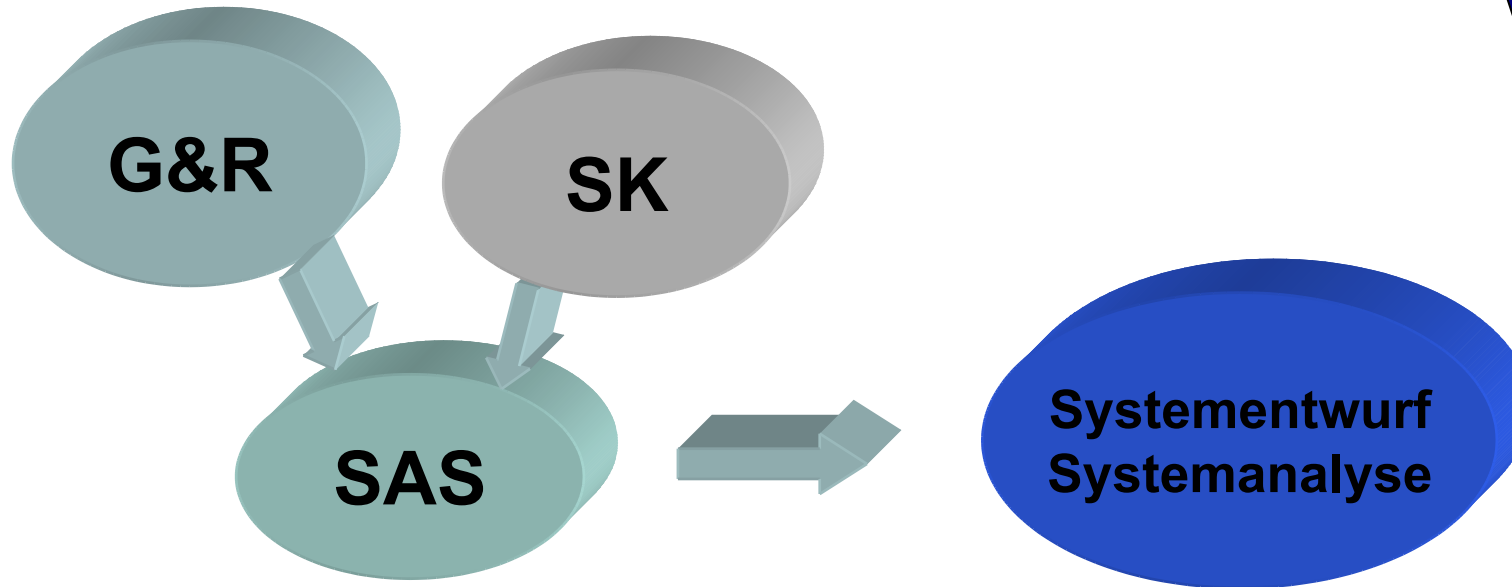
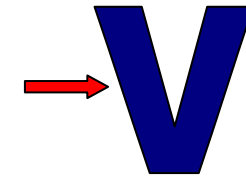


SAS wird auf mehreren Ebenen angewendet, vom Gesamtsystem bis zu den Funktionsebenen im Hardware- und Softwarebereich (Teilsysteme):



## Teil 7: Systementwurf / Systemanalyse

CLEAR | MOTIVE



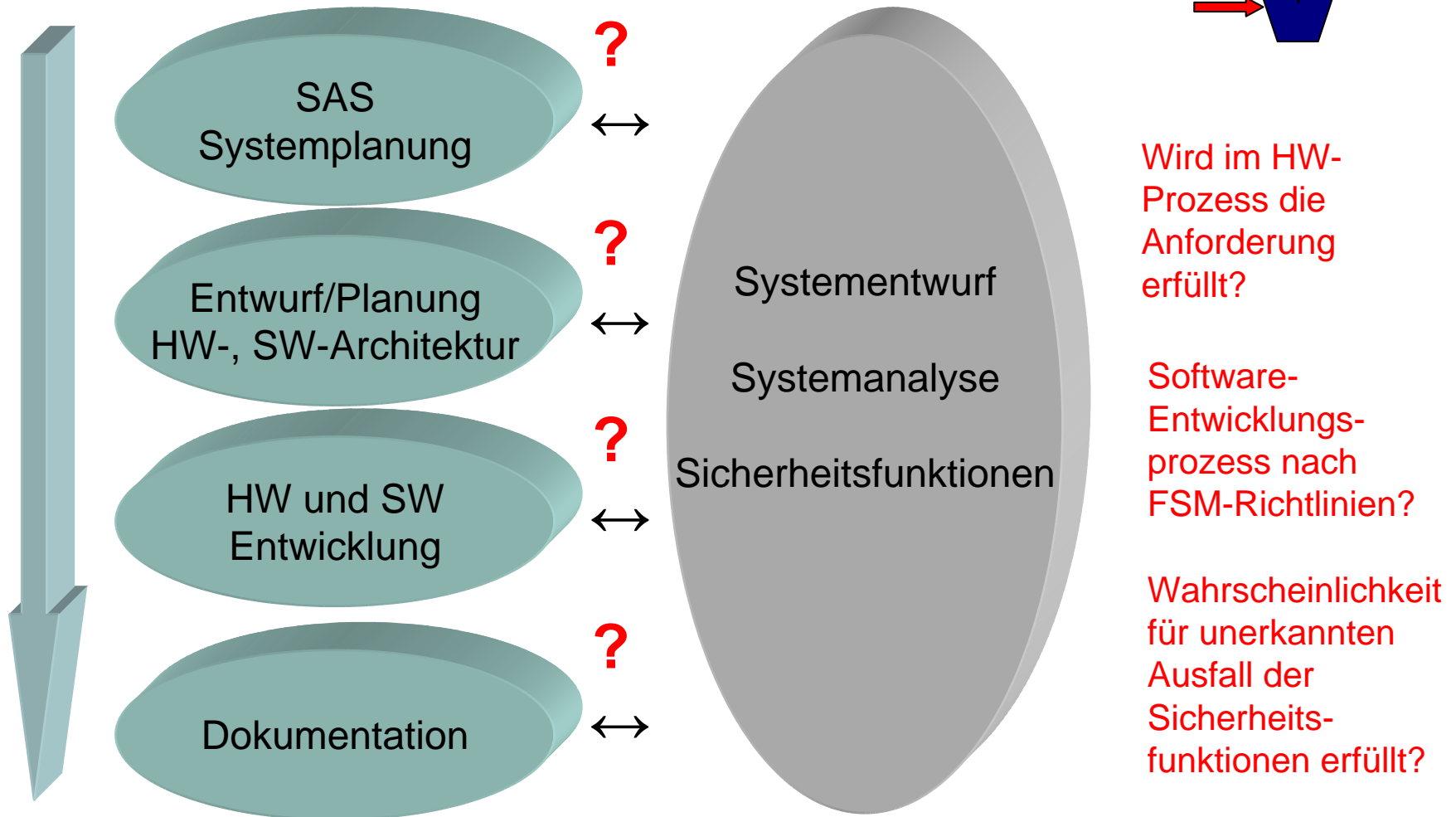
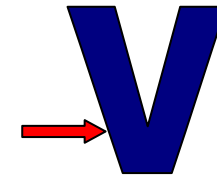
### Ziel:

Überprüfung der Funktionalen Zusammenhänge und Schnittstellen der Teilsysteme und deren Funktionsblöcke

- Untersuchung ob das System gegen Ausfall einzelner Teilsysteme / Funktionsblöcke abgesichert ist

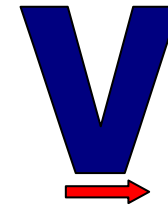
# Teil 8: Hardware Planung und Entwicklung

## Software Analyse, Design und Implementierung



## Teil 9: Implementierung

CLEAR | MOTIVE

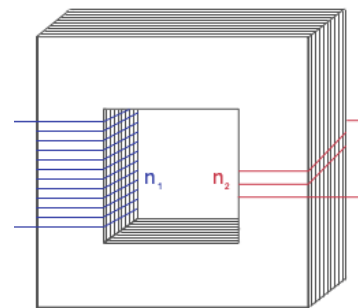


Transformation der Anforderungen

Abstrakte Ebene

Konkrete Ebene

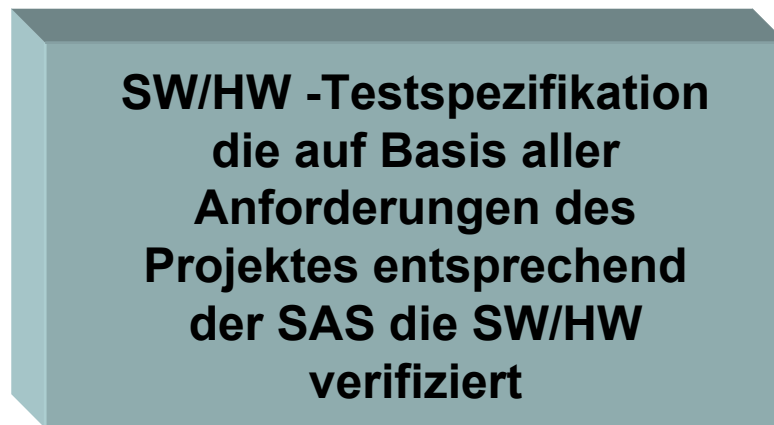
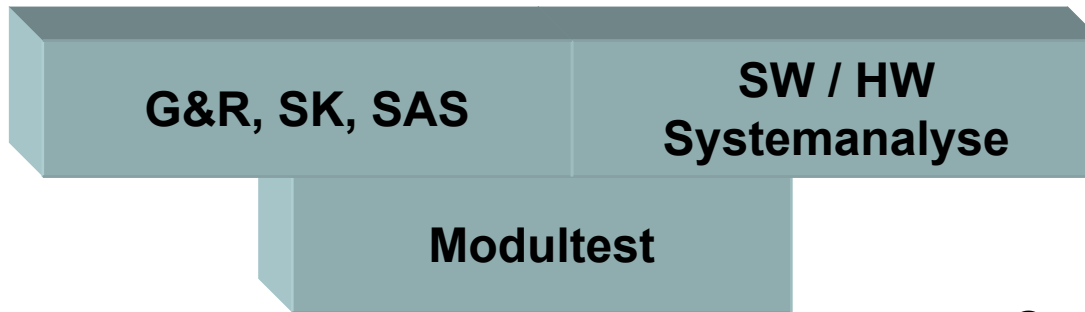
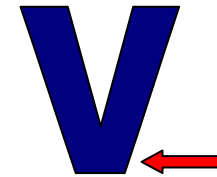
- Hardware  
- Software  
- Prozesse



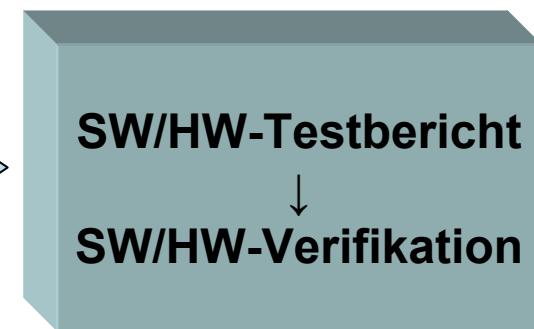
Gesamtsystem

## Teil 10: SW Modultest

CLEAR | MOTIVE

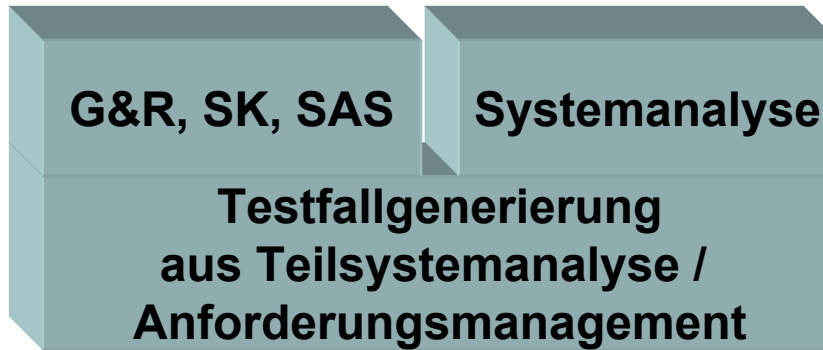
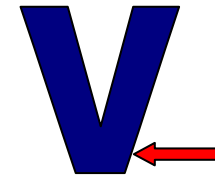


*Spezifizierung und Planung  
des Testkonzeptes durch  
Testspezialisten*

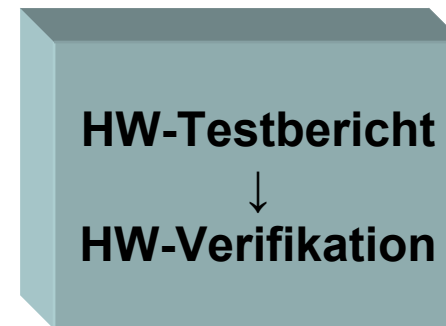
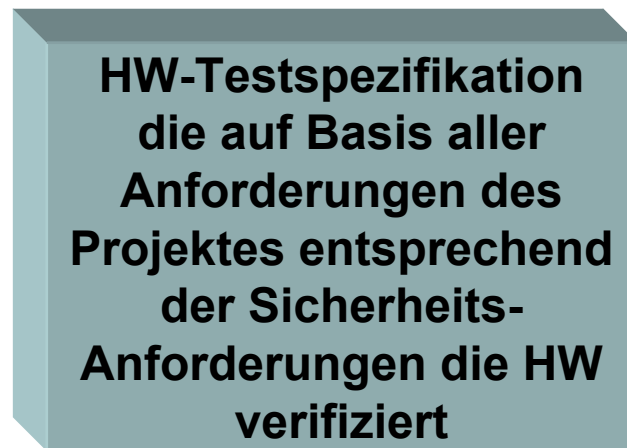


## Teil 11: HW Modultest

CLEAR | MOTIVE

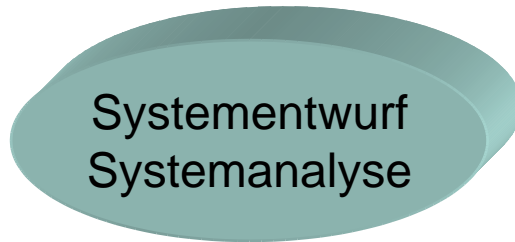
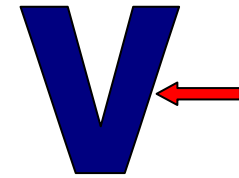


*Spezifizierung und Planung  
des Testkonzeptes durch  
Testspezialisten*



## Teil 12: Systemtest

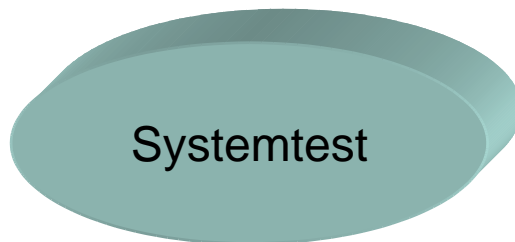
CLEAR | MOTIVE



Grundlage



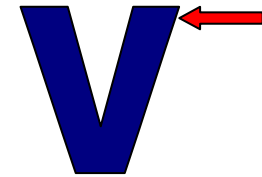
- Planung von Prüfschritten, -kriterien, usw.
- Testfallgenerierung und Vollständigkeitsprüfung



Überprüfung, beispielsweise mittels Funktionstests, ob das System (HW+SW) die Spezifikationen (SAS) erfüllt wurden

## Teil 13: Sicherheitsvalidierung

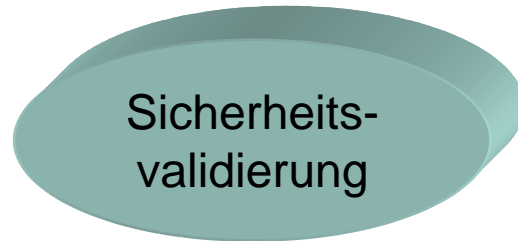
CLEAR | MOTIVE



Grundlage



Testfallgenerierung und Vollständigkeitsprüfung um sicherzustellen das festgelegte Anforderungen erfüllt sind und der Funktionalen Sicherheit entsprechen



- Test von EMV, Umwelt und primärer Sicherheit
- Überprüfung der Anwenderdokumentation
- Abschließende Überprüfung ob alle vorherigen Phasen und deren Anforderungen abgeschlossen und erfüllt wurden

## Unsere Leistungen für Ihre Sicherheit

CLEAR | MOTIVE



### Sicherheitslebenszyklus

- **G**efährdungs- und **R**isikoanalyse
- Definieren der Top Events und Sicherheitszielen
- Erstellung des **S**icherheits-**P**lans
- **S**icherheits-**A**nforderungs-**S**pezifikation
- Funktionales- und Technisches Sicherheitskonzept
- Zuordnung der Sicherheitsanforderungen
- FMEDA, FTA
- Planung und Durchführung Sicherheitsverifikation
- Nachweisversuche und Testberichte
- Sicherheitsnachweis

## Referenzprojekte

CLEAR | MOTIVE



- Zugangs- und Fahrberechtigungssysteme (EZS)
- Elektrische Lenkradverriegelung (ELV)
- Gateways (CGW)
- Getriebesteuerungen
- Hybridsystem für Nutzfahrzeuge (Wechselrichter, E-Maschine, DC/DC-Wandler, Hochvoltsystem, Batteriemanagement, Lilo-Akkus)
- Hybridsteuergeräte (HCU)
- Intardersteuerungen
- Türsteuergeräte (TSG)
- Elektromechanische Lenkung (EPS)

Der CLEAR MOTIVE Funke springt über...

**CLEAR** | **MOTIVE**



CLEAR MOTIVE GmbH  
Am Weichselgarten 8  
91058 Erlangen  
Tel.+49 9131 99 59 730  
Fax.+49 9131 40 75 48  
Mail: [info@clear-motive.de](mailto:info@clear-motive.de)  
Web: [www.clear-motive.de](http://www.clear-motive.de)

[www.clear-motive.de](http://www.clear-motive.de)

**CLEAR** **MOTIVE**  
*Wir haben die zündenden Ideen*