Verification of Safety Critical Systems

Software-Workshop Technologiepark Karlsruhe 24.01.2008

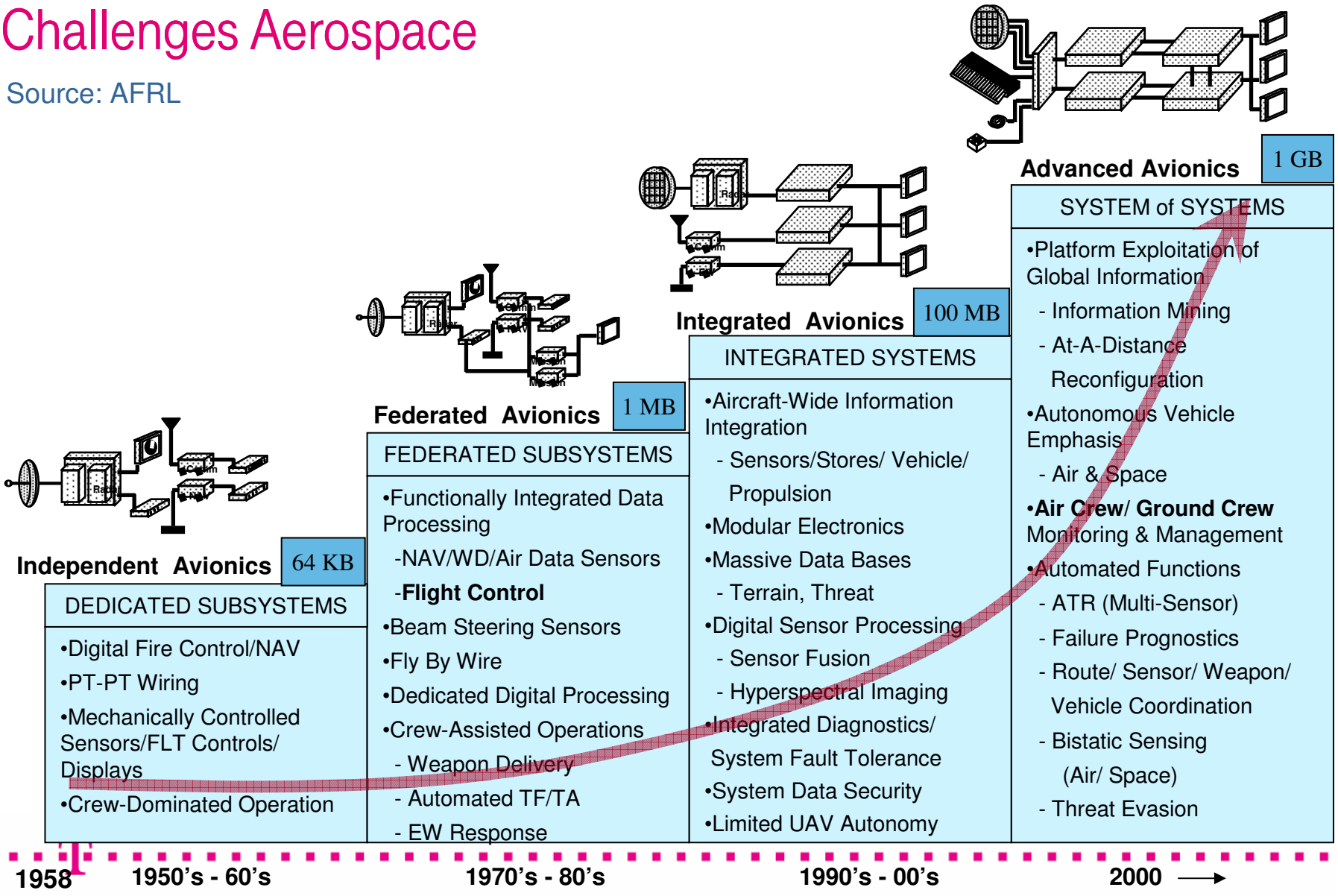
Dr. Christoph Diesch

Verification of Safety Critical Systems
Structure

- Challenges in Aerospace and Automotive
- Fields of Activities
- An Aerospace Example
- V&V Strategy – Theory
  - Requirements
  - Elements of the Strategy
  - Optimization
- V&V Strategy – Experience
  - Effort – Bad Case – Good Case
- Example „Early Verification“
- Example „End-to-End Test“
- 2 Automation Concepts

Verification of Safety Critical Systems
Challenges Aerospace

Source: AFRL



Verification of Safety Critical Systems
Challenges Automotive

Elektronische Einspritzung
Check Control
Geschwindigkeitsregler
Zentralverriegelung
...

1970

Elektronische Getriebesteuerung
Elektronische Klimaregelung
ASC Anti Slip Control
ABS Anti Blocking System
Telefon
Sitzheizungssteuerung
Autom. Spiegelabblendung

1980

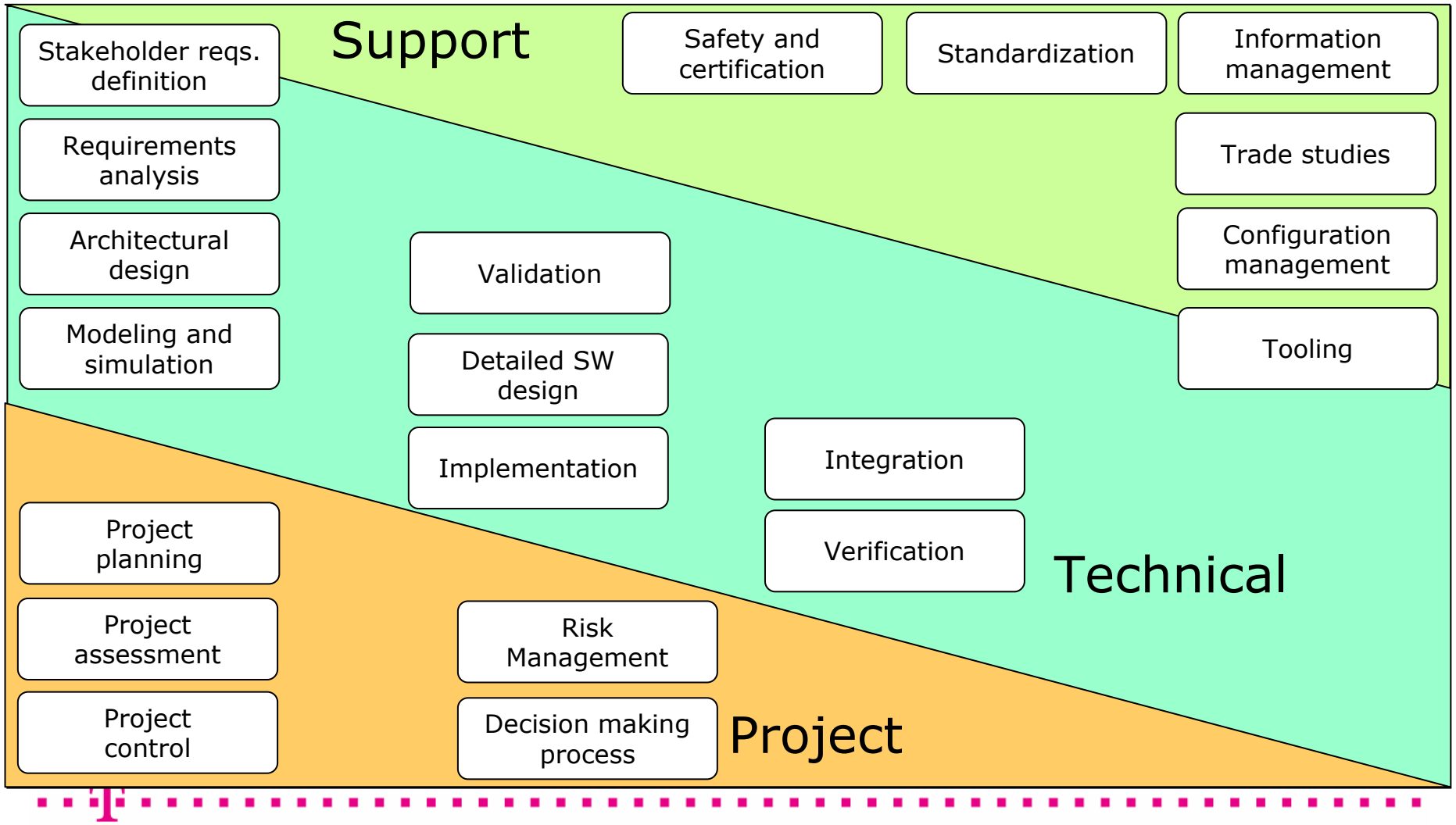
Navigationssystem
CD-Wechsler
ACC Active Cruise Control
Airbags
DSC Dynamic Stability Control
Adaptive Getriebesteuerung
Rollstabilisierung
Xenon Licht
BMW Assist
RDS/TMC
Spracheingabe
Notruf

1990

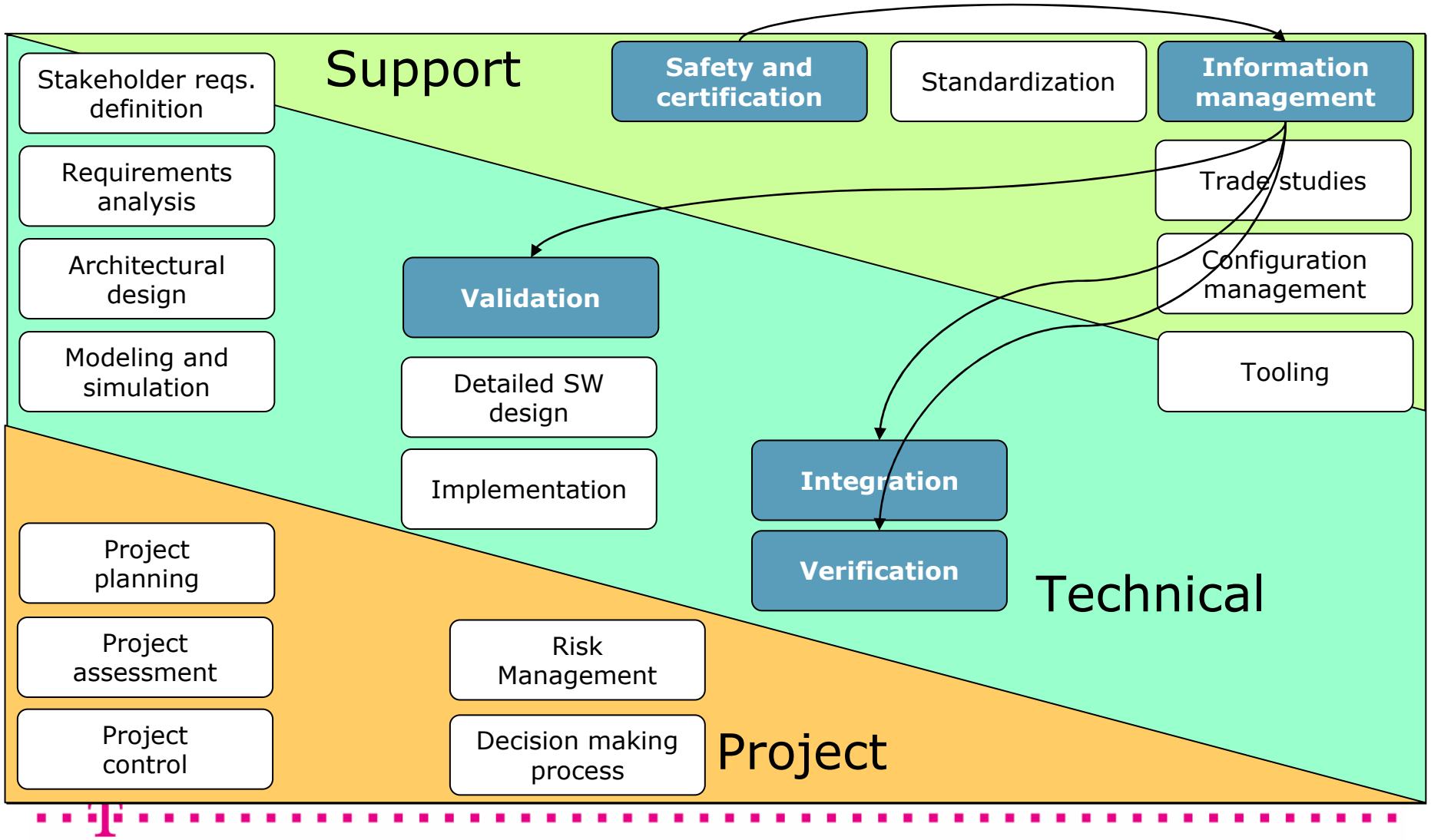
ACC Stop&Go
BFD
ALC
KSG
Internet Portal
GPRS, UMTS
Telematics
Online Services
Blue-Tooth
Car Office
Local Hazard Warning
Integrated Safety System
Steer/Brake-By-Wire
I-Drive
Spurhalteunterstützung
Personalisierung
Force Feedback Pedal

2000

Verification of Safety Critical Systems
Fields of Activities

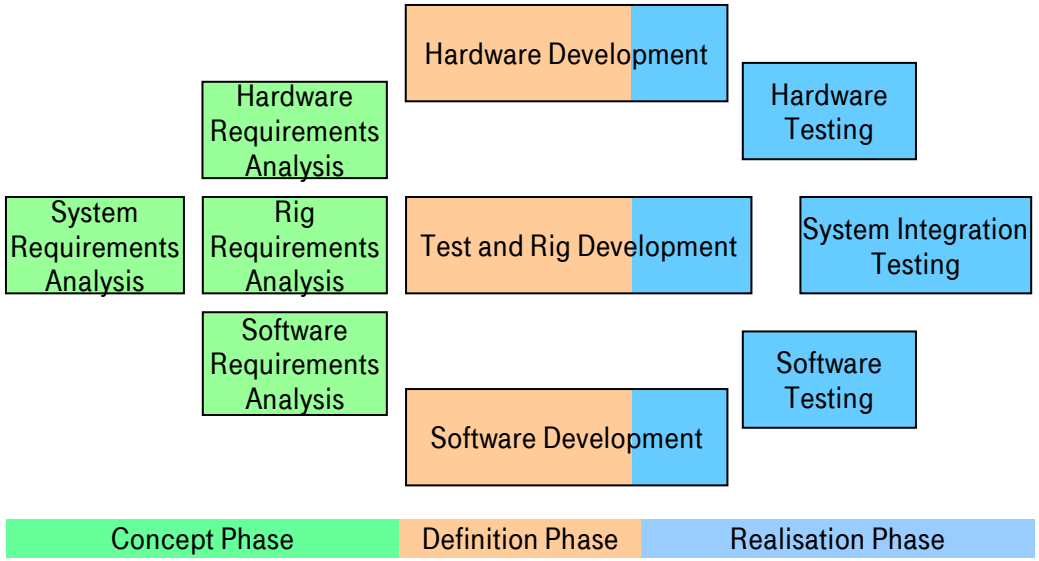


Verification of Safety Critical Systems
Fields of Activities



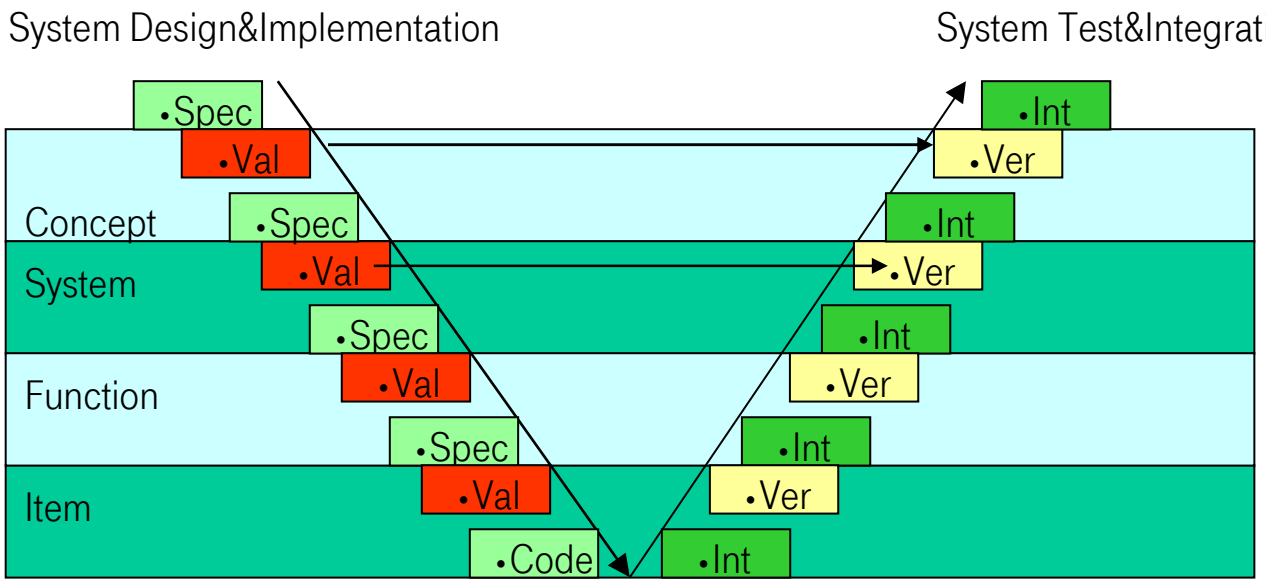
Verification of Safety Critical Systems

Development Process („Classic Approach“ ca. 1985)



- Individual System Development for each Program
- Hierachical System Breakdown (V-Modell)
- Standardized SW-Entwicklungs-modell (e.g. DoD-Std 2167A)
- Strikt tracing Requirements -> Implementation -> Verification
- Documentation of all (Intermediate) Results
- One time execution of the Development Process (Waterfall Model)
- Long Developtimes (10 and more years)

Verification of Safety Critical Systems
Development Process



Verification of Safety Critical Systems

Development Process („New Challanges“ since 1995)

- Significant Extension of functionality and thus complexity
- Development cost reduction by
  - Reduction of development duration (typical 5 years)
  - Utilisation of readily available products (Commercial Off The Shelf)
  - Modifications of readily available products (Modified Off the Shelf)
  - Industrialization of SW-Development (Executable specifications, CASE-Tools)
- Broadening of application base
  - Covering of multiple application scenarios (> 20 variants for military avionic systeme) with configurable Basis-SW
  - Concurrent support for different development / configuration stages in operative use
  - Modularized SW-Design
- Support for SW-Maintenance by
  - Integration of additional functionality
  - Extraction of obsoleten SW-Componentes

Verification of Safety Critical Systems

Concequences for requirements to verification.

Classic requirements	New requirements
Standardized development and verification process	Adaptation of verification process e.g. for COTS/MOTS und reused components
Long lasting verification run (months)	Significant reduced verification run duration (days)
Strict Traceability Requirements -> Implementation -> Verification	
Complete Documentation of all (intermediate) results	
Few (ideal1!) test run for SW-Verification	Multiple (1 per configuration / variant) test runs

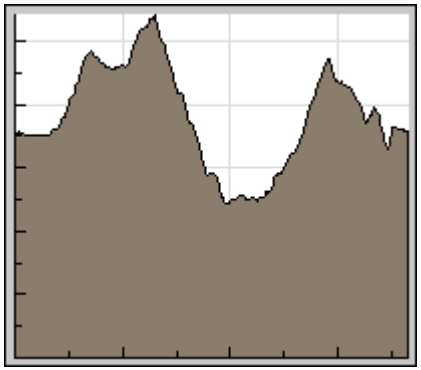
- ARP4754 / DO-178B / DO-254 conformal verification process
- Modular verification concept, close coupling with configuration management
- Reduction of test run duration
- Reduction of test error rate (wrong good, wrong failed)

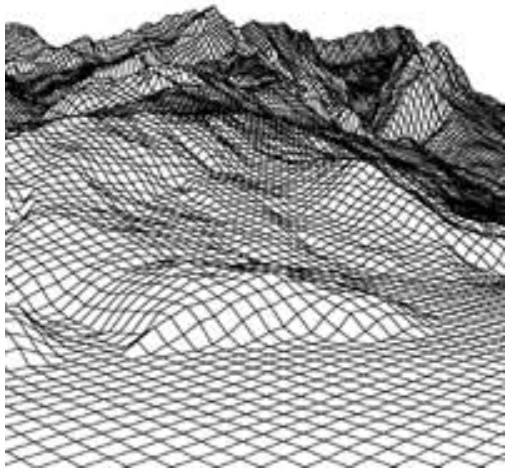
⇒ Utiliztion of Test-Tools (Cantata, VectorCast, TestMATE, ...)

⇒ Automatic test run execution and document generation

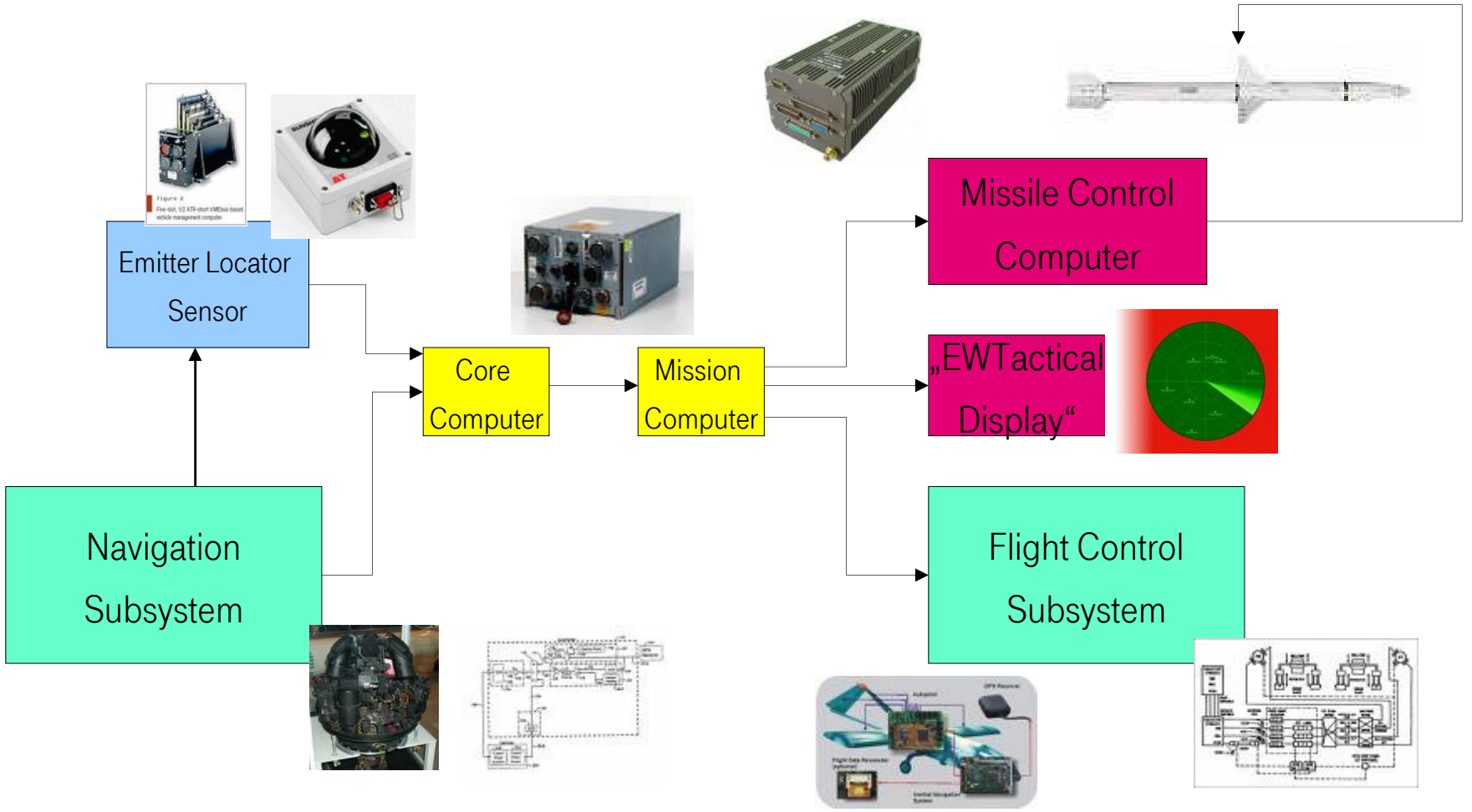
⇒ **Transition from manufactur to industrial testing**

Verification of Safety Critical Systems
An Aerospace Example





Verification of Safety Critical Systems
System Breakdown



Verification of Safety Critical Systems
What to Deal With - Methods of Verification

- Simulation
- Analysis, Engineering Judgement
- Similarity of requirements or design
- Demonstration, Prototyping or Mock-up
- Reviews or Audits
- Inspection
- Test
- Operational Trials

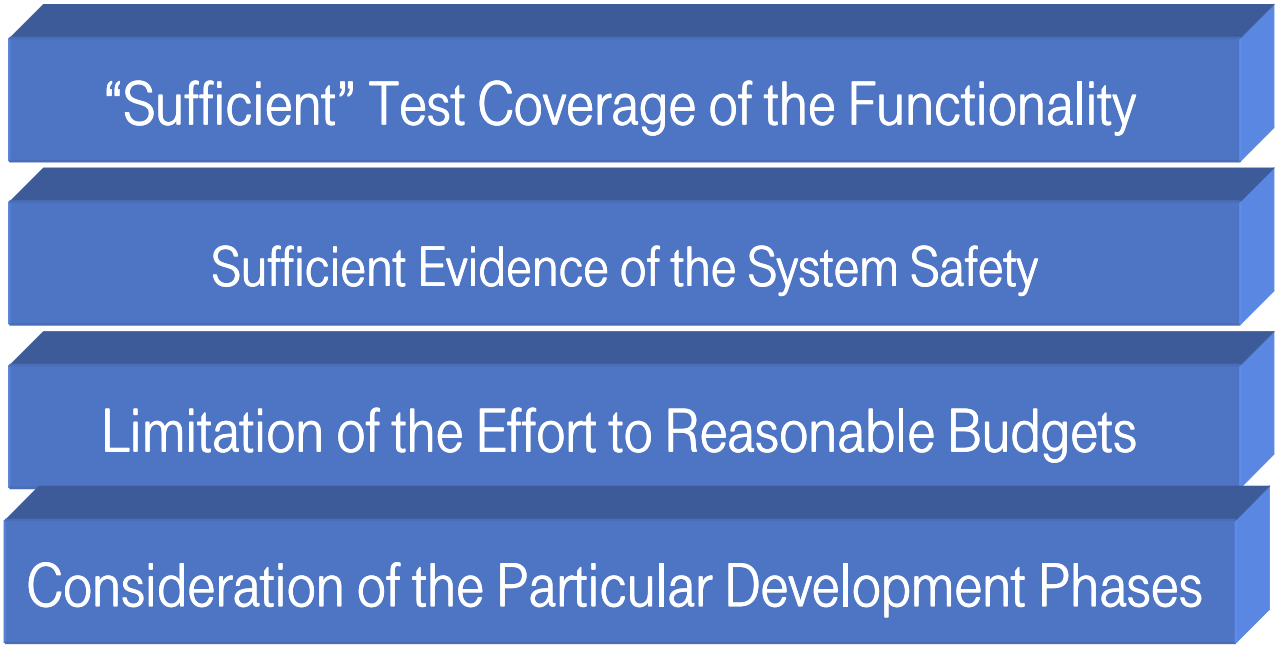
- Flight Test
- Aircraft Ground Test
- System Integration Test
- HW-SW Integration Test (Bench)
- SW-SW Integration Test
- Coding Unit Test

Verification of Safety Critical Systems
Let‘s Find an „Optimized Verification Strategy“

From Theory.....

..... To Experience

Verification of Safety Critical Systems
Requirements on an Optimized Verification Concept



Verification of Safety Critical Systems

Elements of a Good Verification Strategy

- Establish Automated Tests Early
- Realize the Coherence of Functions and Test
- Use Data Bases and Generators
- Coordinate all Test Stages
- Realize End to End Tests
- Verify Requirements &Functions Early

Verification of Safety Critical Systems
Essential Columns of the Verification Strategy - Focusing

Use the specific advantages of each test stage

Automate Tests

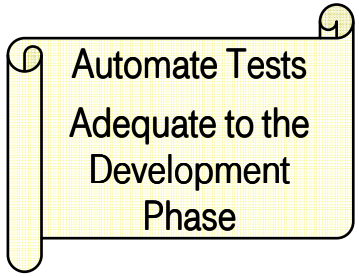
Adequate to the Development Phase

Verification of Safety Critical Systems
Optimized Strategy (1)

Use the specific advantages of each test stage

▪ Verify requirements&functions early	→	Early requirements&design verification
▪ Realize end to end tests	→	User's needs
▪ Coordinate all test stages	→	Integrated test concept
▪ Realize the coherence of functions and test	→	Coverage and traceability

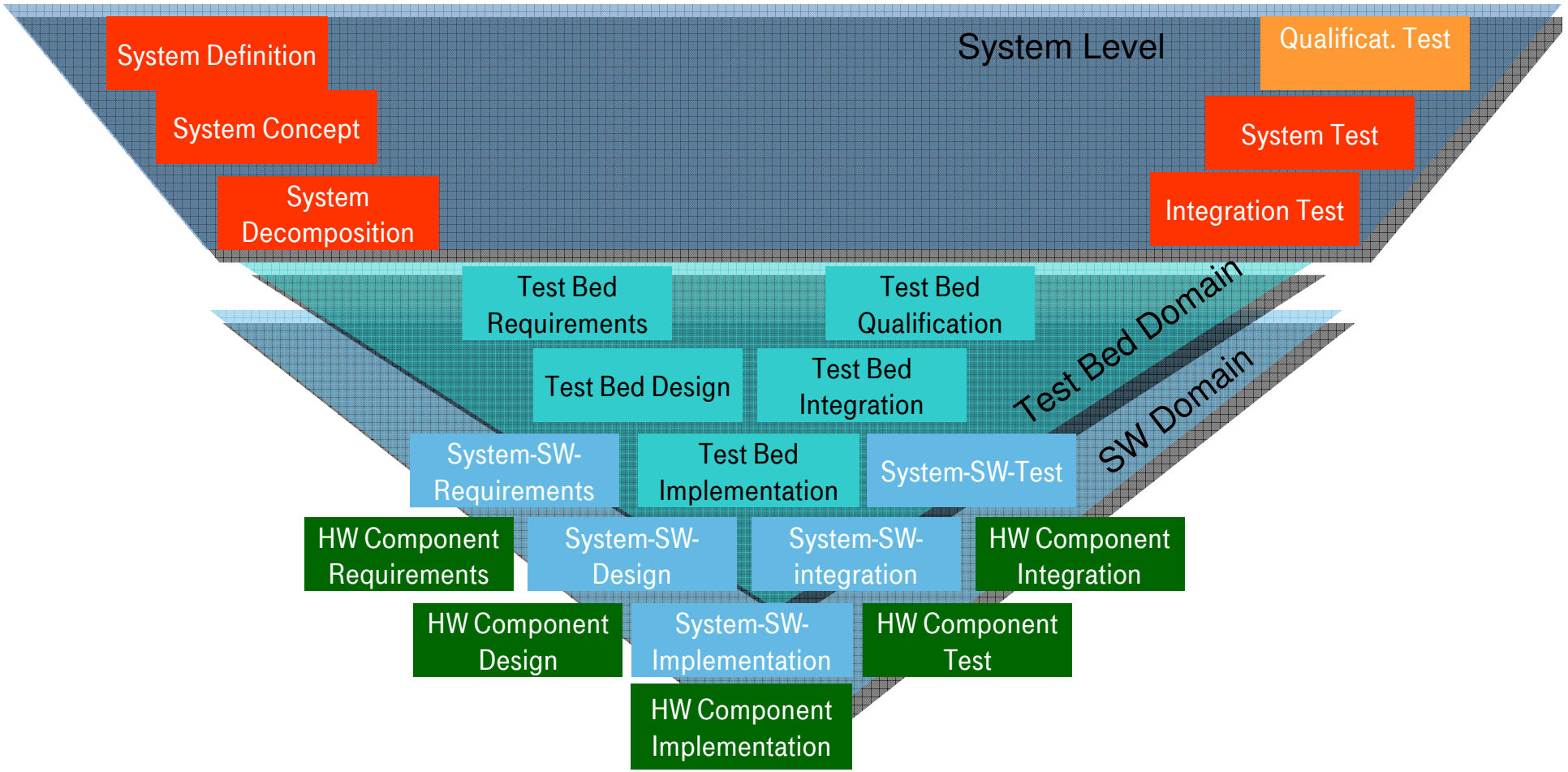
Verification of Safety Critical Systems
Optimized Strategy (2)



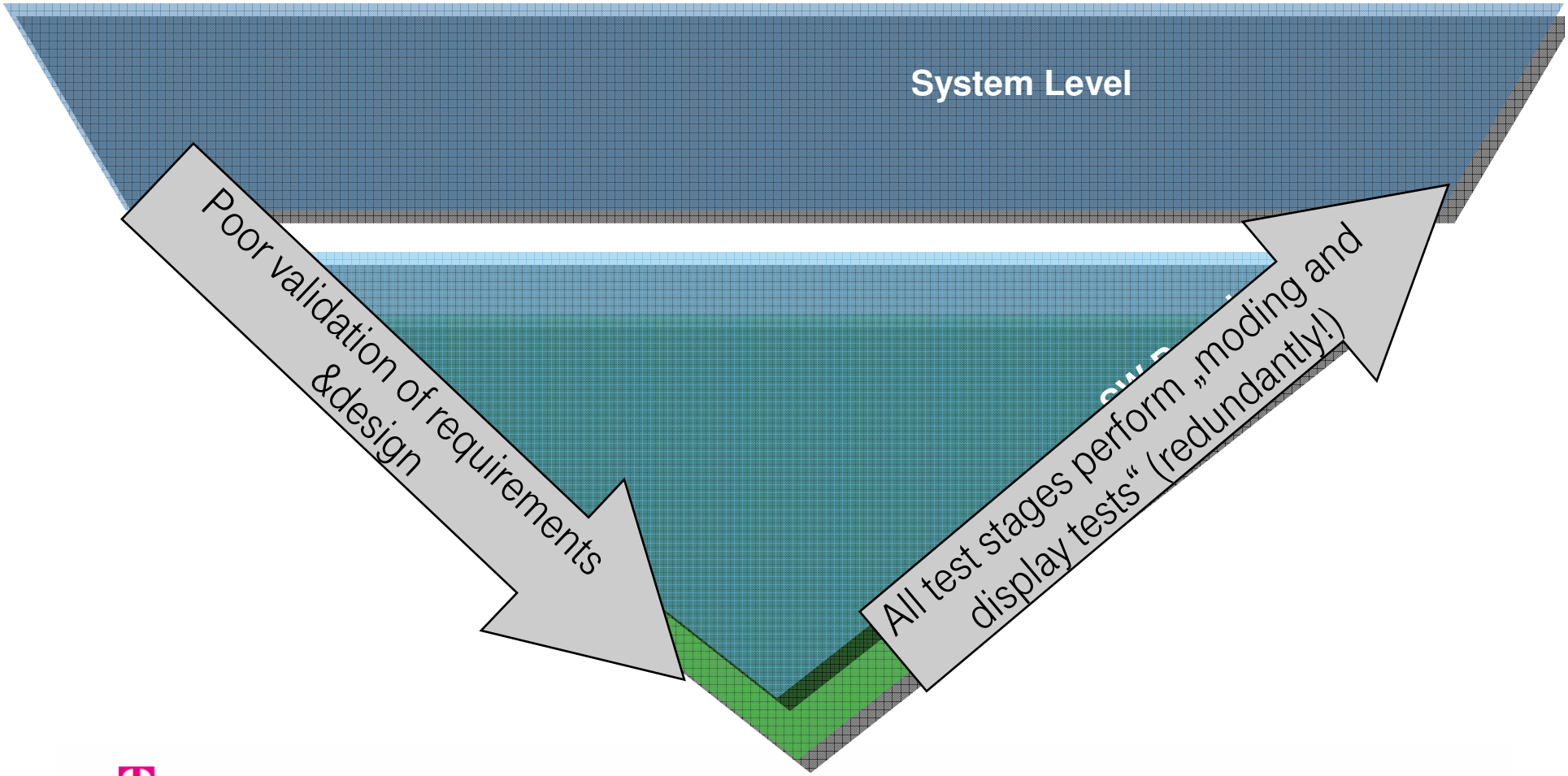
- Establish automated tests early → Reduction of repetitive effort
- Use data bases and document generators → Reduction of document effort

Verification of Safety Critical Systems
Experience

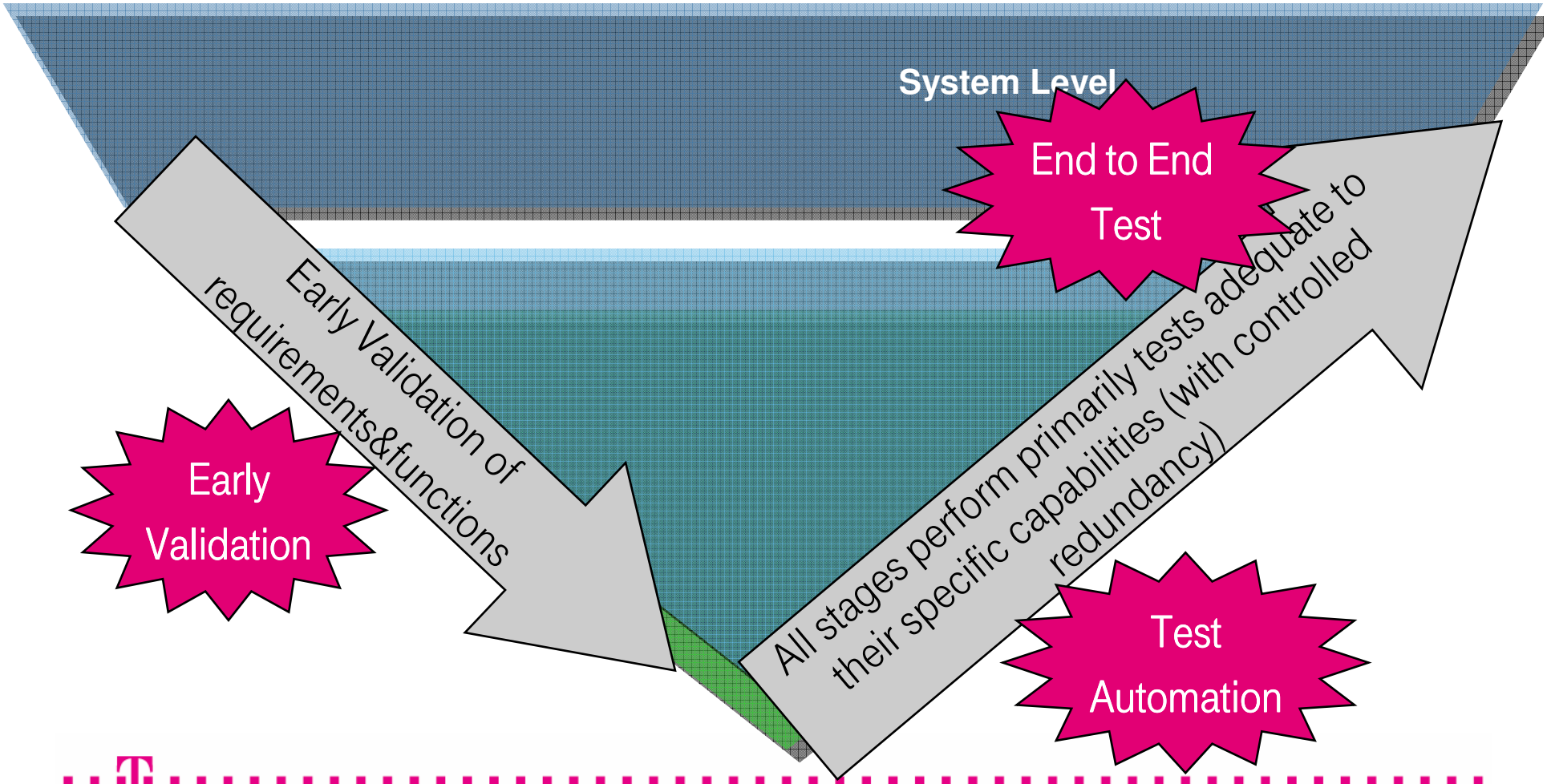
Verification of Safety Critical Systems
Effort



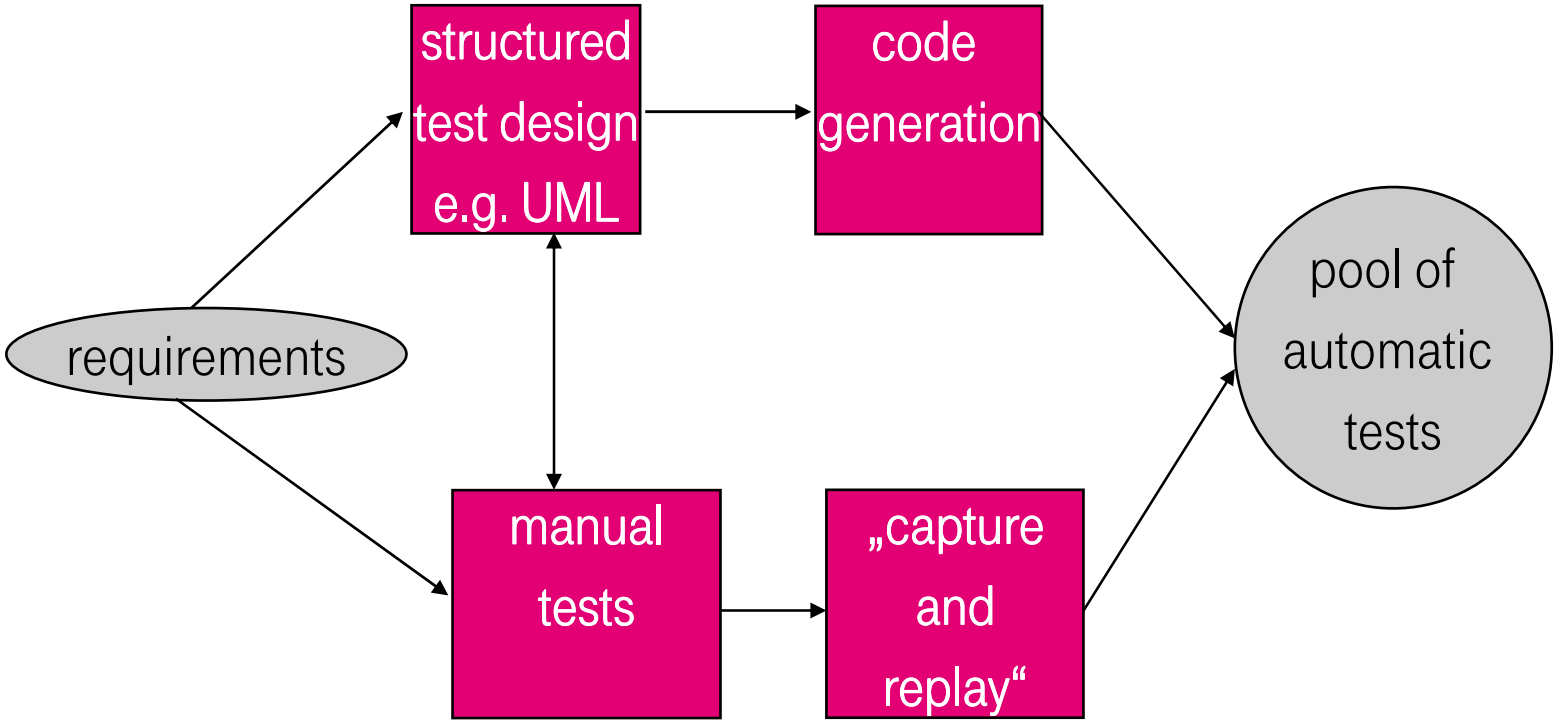
Verification of Safety Critical Systems
„Bad Case“



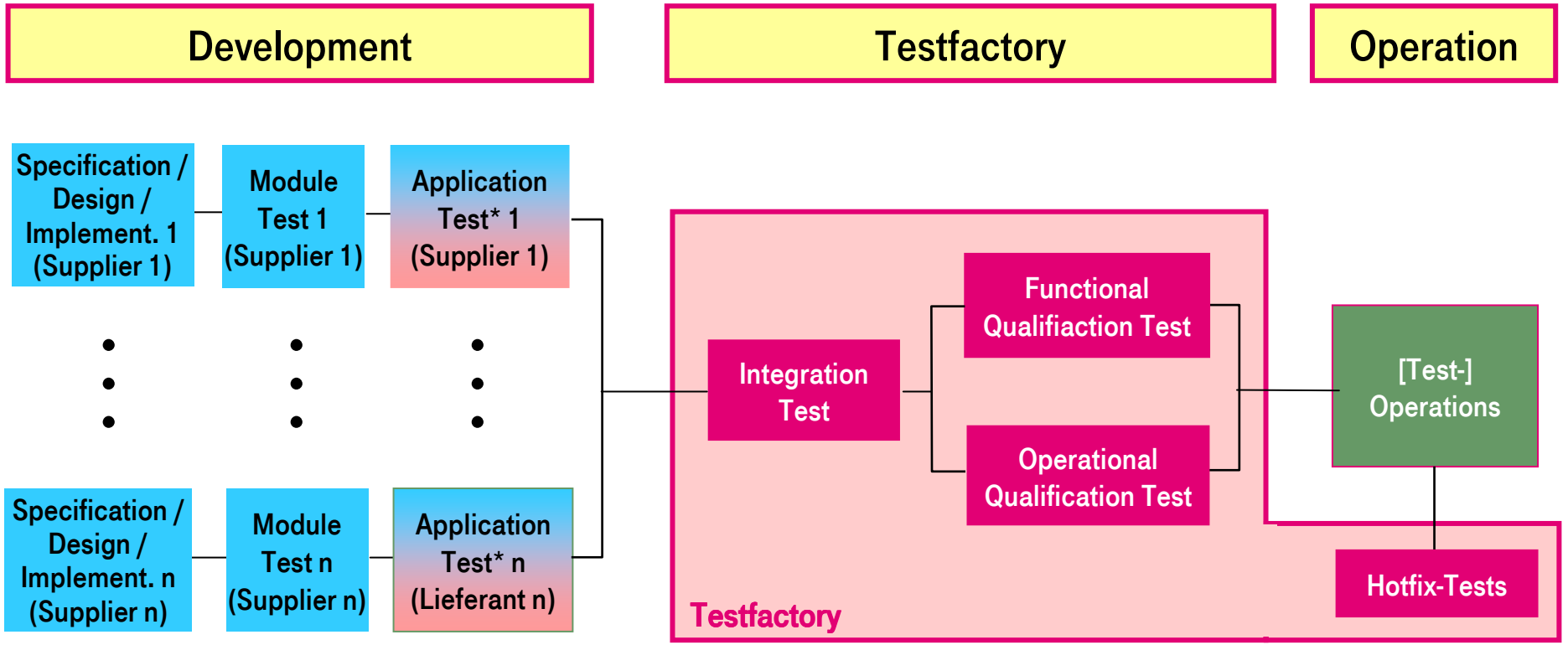
Verification of Safety Critical Systems
„Good Case“



Verification of Safety Critical Systems
Two Automation Concepts



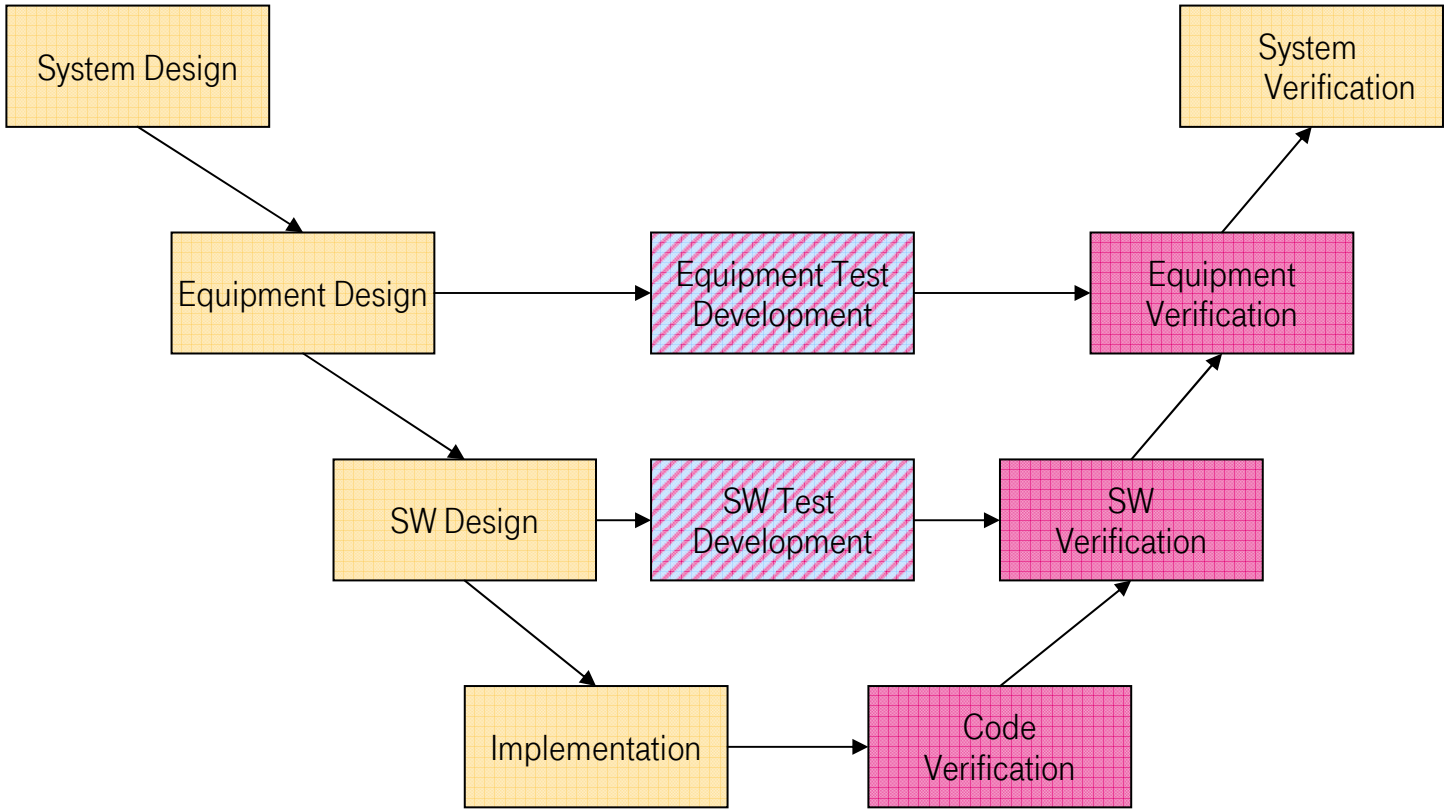
Verification of Safety Critical Systems
Testfactory Concept



*incl. bilateral interfaces

Operational roll out

Verification of Safety Critical Systems
Development Process



Verification of Safety Critical Systems
SW Verification