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

<table>
<thead>
<tr>
<th>DEDICATED SUBSYSTEMS</th>
<th>FEDERATED SUBSYSTEMS</th>
<th>INTEGRATED SUBSYSTEMS</th>
<th>SYSTEM of SYSTEMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Digital Fire Control/NAV</td>
<td>• Functionally Integrated Data Processing</td>
<td>• Aircraft-Wide Information Integration</td>
<td>• Platform Exploitation of Global Information</td>
</tr>
<tr>
<td>• PT-PT Wiring</td>
<td>• - NAV/WD/Air Data Sensors</td>
<td>- Sensors/Stores/ Vehicle/Propulsion</td>
<td>- Information Mining</td>
</tr>
<tr>
<td>• Mechanically Controlled Sensors/FLT Controls/Displays</td>
<td>• - Flight Control</td>
<td>• Modular Electronics</td>
<td>- At-A-Distance Reconfiguration</td>
</tr>
<tr>
<td>• Crew-Dominated Operation</td>
<td>• - Beam Steering Sensors</td>
<td>• Massive Data Bases</td>
<td>• Autonomous Vehicle Emphasis</td>
</tr>
<tr>
<td></td>
<td>• - Fly By Wire</td>
<td>• - Terrain, Threat</td>
<td>- Air &amp; Space</td>
</tr>
<tr>
<td></td>
<td>• - Dedicated Digital Processing</td>
<td>• - Digital Sensor Processing</td>
<td>• Air Crew/ Ground Crew</td>
</tr>
<tr>
<td></td>
<td>• - Crew-Assisted Operations</td>
<td>• - Sensor Fusion</td>
<td>Monitoring &amp; Management</td>
</tr>
<tr>
<td></td>
<td>- Weapon Delivery</td>
<td>• - Hyperspectral Imaging</td>
<td>• Automated Functions</td>
</tr>
<tr>
<td></td>
<td>- Automated TF/TA</td>
<td>• Integrated Diagnostics/System Fault Tolerance</td>
<td>- ATR (Multi-Sensor)</td>
</tr>
<tr>
<td></td>
<td>- EW Response</td>
<td>• System Data Security</td>
<td>- Failure Prognostics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Limited UAV Autonomy</td>
<td>- Route/ Sensor/ Weapon/</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Vehicle Coordination</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Bistatic Sensing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(Air/ Space)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Threat Evasion</td>
</tr>
</tbody>
</table>

Dr. C. Diesch: Verification of safety critical Systems 24.01.2008
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

Local Hazard Warning
Integrated Safety System
Steer/Brake-By-Wire
I-Drive
Spurhalteunterstützung
Personalisierung
Force Feedback Pedal

2000

ACC Stop&Go
BFD
ALC
KSG
Internet Portal
GPRS, UMTS
Telematics
Online Services
Blue-Tooth
Car Office

Dr. C. Diesch: Verification of safety critical Systems

24.01.2008
Verification of Safety Critical Systems
Fields of Activities

Support
- Stakeholder reqs. definition
- Requirements analysis
- Architectural design
- Modeling and simulation
- Validation
- Detailed SW design
- Implementation
- Risk Management
- Decision making process

Technical
- Safety and certification
- Standardization
- Information management
- Trade studies
- Configuration management
- Tooling
- Integration
- Verification

Project
- Project planning
- Project assessment
- Project control
- Safety and certification
- Standardization

Dr. C. Diesch: Verification of safety critical Systems
Verification of Safety Critical Systems

Fields of Activities

Support

Stakeholder reqs. definition
Requirements analysis
Architectural design
Modeling and simulation

Safety and certification
Standardization
Information management

Trade studies
Configuration management
Tooling

Validation
Detailed SW design
Implementation

Integration
Verification
Risk Management
Decision making process

Technical

Project planning
Project assessment
Project control

Information management

Dr. C. Diesch: Verification of safety critical Systems 24.01.2008 6
Verification of Safety Critical Systems
Development Process („Classic Approach“ ca. 1985)

- Individual System Development for each Program
- Hierarchical System Breakdown (V-Modell)
- Standardized SW-Entwicklungsmodell (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 Development times (10 and more years)
Verification of Safety Critical Systems Development Process
Verification of Safety Critical Systems
Development Process („New Challenges“ 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 systems) 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 obsoleted SW-Components
Verification of Safety Critical Systems
Consequences for requirements to verification.

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

- 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)
  ⇒ Utilization 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

Emitter Locator Sensor -> Core Computer -> Mission Computer

Navigation Subsystem

Missile Control Computer

"EWTactical Display"

Flight Control Subsystem
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

“Sufficient” Test Coverage of the Functionality
Sufficient Evidence of the System Safety
Limitation of the Effort to Reasonable Budgets
Consideration of the Particular Development Phases
Verification of Safety Critical Systems
Elements of a Good Verification Strategy

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

<table>
<thead>
<tr>
<th>Action</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify requirements &amp; functions <strong>early</strong></td>
<td>Early requirements &amp; design verification</td>
</tr>
<tr>
<td>Realize <strong>end to end</strong> tests</td>
<td>User's needs</td>
</tr>
<tr>
<td>Coordinate all test stages</td>
<td>Integrated test concept</td>
</tr>
<tr>
<td>Realize the coherence of functions and test</td>
<td>Coverage and traceability</td>
</tr>
</tbody>
</table>

---

Use the specific advantages of each test stage
Verification of Safety Critical Systems
Optimized Strategy (2)

- Establish **automated** tests early
- Use data bases and document **generators**

- Reduction of repetitive effort
- Reduction of document effort

Automate Tests Adequate to the Development Phase
Verification of Safety Critical Systems
Experience

To Experience
Verification of Safety Critical Systems

Effort

System Definition
System Concept
System Decomposition

Test Bed Requirements
Test Bed Design
Test Bed Implementation
Test Bed Integration
Test Bed Qualification

System-SW-Requirements
System-SW-Design
System-SW-Integration
System-SW-Test

 HW Component Requirements
 HW Component Design
 HW Component Implementation
 HW Component Test

System Level
Qualificat. Test
System Test
Integration Test

SW Domain
Test Bed Domain
Verification of Safety Critical Systems
„Bad Case“

- Poor validation of requirements & design
- All test stages perform "moding and display tests" (redundantly!)
Verification of Safety Critical Systems
„Good Case“

24.01.2008 Dr. C. Diesch: Verification of safety critical Systems
Verification of Safety Critical Systems
Two Automation Concepts
Verification of Safety Critical Systems
Testfactory Concept

Development

Testfactory

Operation

Specification / Design / Implement. 1
(Supplier 1)

Module Test 1
(Supplier 1)

Application Test* 1
(Supplier 1)

Specification / Design / Implement. n
(Supplier n)

Module Test n
(Supplier n)

Application Test* n
(Lieferant n)

Integration Test

Functional Qualification Test

Operational Qualification Test

[Test-] Operations

Hotfix-Tests

Operational roll out

*incl. bilateral interfaces
Verification of Safety Critical Systems
Development Process

System Design → Equipment Design → System Verification

Equipment Design → Equipment Test Development → Equipment Verification

SW Design → SW Test Development → SW Verification

Implementation → Code Verification
Verification of Safety Critical Systems

SW Verification

- Source Code
- GUI, IRS, ...
- SRS
- Stub Generation
- Host Simulation
- Test Development
- Design Inspection
- Component Tests
- Unit Tests
- Automated Tasks
- Manuell Tasks
- Input Data
- Output Data
- Test Results
- Test Descriptions
- STD
- STR