AVACS*
Automatic Verification and Analysis of Complex Systems

Werner Damm
AVACS coordinator

*www.avacs.org
Transregional Collaborative Research Center
funded by the German Science Foundation SFB-TR 14
Complex Systems

Source: Aramis Project
The Application Context

• Complex Embedded Systems are key enablers for safe flight and safe ground transportation
• Exponential growth in system complexity is a challenge for quality assurance
• AVACS contributes to meeting forthcoming requirements of pertinent safety standards on use of formal analysis methods
• Methods and tools cover large class of “cyber physical systems” seen to be highly relevant for addressing societal challenges (health, security, green mobility, …)
Automatic Verification of Complex Systems: Models

- Extremely **Heterogeneous Model Space**
  - Systems of Systems
  - ....
  - Cycle Accurate models of HW

- Comprehensive and Scalable Verification requires
  - Relating Models at different Design Levels
  - Identification of typical model characteristic
Requirements

Heterogeneous Requirement Space

- Reliability
  "probability of total a/c failure is less than $10^{-9}$ per flight hour"

- Coordination
  "Crossing will grant access if secured"

- Local Control
  "The train will never run faster than permitted speed"
  "enforce brake profile"

- Real-Time
  "When receiving unconditional emergency stop message the train shall be tripped within 5 msecs"
  "Brake curve control task activated every 30 msecs"
The AVACS model- and requirement space
The AVACS Vision

To **Cover the Model- and Requirement Space of Complex Safety Critical Systems**

with **Automatic Verification Methods**

Giving Mathematical Evidence of Compliance of Models

To **Dependability, Coordination, Control and Real-Time Requirements**
## AVACS Competence Layers

### Complex Systems
- Embedded Transportation Applications

### Models of Complex Systems
- real-time – hybrid – distributed systems – system of systems

### Combining V&A Technology

\[ (x_1 \land x_2 \land \ldots x_n \text{ for } s) \]

\[ x_j \in \text{V&A core technologies}, s \in \text{systems} \]

### V&A Core Technologies
- Abstraction – Decision Diagrams – Constraint Solving – Heuristic Search
- Linear Programming – Model Checking – Lyapunov Method
- Abstract Interpretation – SMT – Decision Procedures