Space Software Product Assurance
Research and Development

Rolf Hempel, Dr. Anita Herrmann

German Aerospace Center (DLR)
Simulation and Software Technology (SISTEC)

www.dlr.de/sc/
Simulation and Software Technology (SISTEC)

- Founded 1999
- Central DLR facility for
  - Information Technology
  - Software Product Assurance (standards, assessment, project support)
- Long-term SPA support in space projects (i.e. TerraSAR, Corot, Rosetta) based on ECSS, ESA-PSS
- Own software development experience as basis for professional SPA work. Focus: critical embedded real-time systems, i.e. BIRD satellite ACS)
Simulation and Software Technology (SISTEC)
Current projects and directions of research

- „DLR Software Basis Standards“: DLR intranet application for
  - SPA and SE requirements tailoring (ECSS-E-40, ECSS-Q-80, and other standards IEEE, RTCA/DO 178B, EN 61508)
  - Knowledge base (project documents, links, definitions, publications ...)

- SiLEST: Software in the Loop for Embedded Software Test:
  - Test and safety/dependability analysis of critical embedded real-time software
  - Surrounding system/hardware environment simulated by software
  - Applications: space software (ACS) and automotive control software
Simulation and Software Technology (SISTEC)
Current projects and directions of research (cont.)

- **DataFinder**: Data management in a scientific environment
  - Structured organization of long-term data (from simulation/experiments)
  - Client / Server tool, based on open standards
  - Roll-out at DLR under way

- **Grid Computing**:
  - New paradigm for distributed systems
  - Grown from research applications
  - Great potential for space applications (e.g. mission operation)
  - Important research topic: Security in virtual organisations
Required Development of ECSS-E-40/ECSS-Q-80

- An E40/Q80 requirements tailoring system, based on the specific project characteristics / project context
- Elimination of overlap between ECSS-E-40 and ECSS-Q-80 requirements
- A reference between SPICE for Space (S4S) assessment capability levels (ISO 15504) and ECSS-Q-80 requirements
SPA R&D: Cost Reduction in Space Software Projects

- **Software Reuse**
  - Effective (tool-supported) engineering and SPA processes
  - OO architectural frames / generic architectures for specific technical domains (i.e. ground systems)
  - design evaluation criteria / metrics for software reuseability

- **Formal Code Analysis Methods and Tools**
  - Determination of Worst Case Execution Time (WCET) of real-time software based on the source code only (symbolic code analysis)
  - Automatic code analysis to verify the match of execution pathes with the OO software model
SPA R&D: Safety/Security of Space Systems

- Use of System Simulation (SiL, HiL) to support SPA for critical embedded real-time software
  - Software requirements analysis
    (in particular software-related safety/dependability)
  - Software verification and test
  - Robustness analysis with respect to
    - hardware / environment failure
    - hardware aging
SPA R&D: Safety/Security of Space Systems (cont.)

- Analysis of the relation between
  - software-affected system safety and
  - security
  in critical distributed, internet-based or grid-based systems

- Development of
  - Architectural guidelines for software / system security
  - Test and evaluation approaches for software / system security
    (systematic penetration tests)