Panel CPS for Aviation: Looking Forward

César A. Muñoz
munoz@nianet.org

National Institute of Aerospace

November 2008

Transportation CPS Workshop

NIA
NATIONAL INSTITUTE OF AEROSPACE

- NIA is a non-for-profit research and education organization formed by a consortium of universities and the AIAA Foundation.

- NIA is a strategic partner to NASA Langley Research Center.

LANGLEY FORMAL METHODS

- `http://shemesh.larc.nasa.gov/fm`
- `http://research.nianet.org/fm-at-nia`

As for the future, your task is not to foresee it, but to enable it.

Antoine de Saint-Exupery (1900-1944)

Formal Methods Research at NIA

(Past)

- Airborne Information for Lateral Spacing (AILS): Formal verification of an alerting algorithm for parallel landing.
- Distributed Air/Ground Traffic Management (DAG/TM): Design and formal verification of a tactical conflict detection and resolution algorithm.
- Small Aircraft Transportation Systems (SATS): Formal analysis of an operational concept for non-towered non-radar small airports.
- Enhanced Oceanic Operations (EOO): Design and safety analysis of an oceanic in-trail climb and descend procedure.

Formal Methods Research at NIA

(Present)

- Next Generation of Air Traffic Management Systems (NGATS): Design and verification of distributed conflict prevention, detection, resolution systems.
- Integrated Vehicle Health Management (IVHM):
  - Compositional verification of complex systems.
  - Symbolic model checking of hybrid systems.
  - Monitor synthesis from formal models of fault tolerant architectures.

State of the Art of Formal Methods in Aviation Systems

(Personal Assessment)

- Basic capabilities in theorem proving, model-checking, and software verification are well-developed.
- Formal verification of algorithms and traditional software is becoming routine:
  - but still a complex and time consuming activity for highly trained experts,
  - a huge barrier in establishing that capability in practice.
- Enormous progress in promising new technologies:
  - Hybrid abstraction and model checking.
  - Constraint solving.
  - Run-time verification and monitoring.
  - Compositional verification.

State of the Art of Formal Methods in Aviation Systems

(Personal Assessment)

- Basic capabilities in theorem proving, model-checking, and software verification are well-developed.
- Formal verification of algorithms and traditional software is becoming routine:
  - but still a complex and time consuming activity for highly trained experts,
  - a huge barrier in establishing that capability in practice.
- Enormous progress in promising new technologies:
  - Hybrid abstraction and model checking.
  - Constraint solving.
  - Run-time verification and monitoring.
  - Compositional verification.

State of the Art of Formal Methods in Aviation Systems

(Personal Assessment)

- Basic capabilities in theorem proving, model-checking, and software verification are well-developed.
- Formal verification of algorithms and traditional software is becoming routine:
  - but still a complex and time consuming activity for highly trained experts,
  - a huge barrier in establishing that capability in practice.
- Enormous progress in promising new technologies:
  - Hybrid abstraction and model checking.
  - Constraint solving.
  - Run-time verification and monitoring.
  - Compositional verification.

Technical Challenges in NextGen

(From a Formal Methods Perspective)

NextGen is a non-traditional formal methods domain:

- Formal methods for system engineering rather than for software engineering.
- Significant human factors component.
- New software technology such as adaptive and biological inspired systems.
- Different sources of uncertainty.
- Massively critical system.

Practical Challenges

- Human resources to solve the problem is scarce.
- Lack of tractable but relevant examples.
- Too many difficult problems.

Let's Not Fear the Future

Development of *common models and challenge problems*:

- Coordination and cooperation between different groups and stake holders.
- Models for teaching and researching relevant issues in NextGen.
- Common language of discourse between academia, industry, certification authorities.