

Gilles Dowek's Contributions to the Development of Safety-Critical Systems at NASA

César Muñoz
(premier doctorant et collaborateur)



Colloque en hommage à Gilles Dowek (1966-2025)
June 19, 2026

- Computer scientist and logician: type theory, proof theory, higher-order logic, rewriting, quantum computing, proof systems interoperability, philosophy, ethics, education, popularization of science, ...
- and **NASA consultant**¹
 - ⇒ 21 publications (<https://shemesh.larc.nasa.gov/fm/fm-pubs-larc.html>)

¹... through the Institute for Computer Applications in Science and Engineering (ICASE) and the National Institute of Aerospace (NIA).

- Advanced Air Transportation Technologies (AATT) & Next Generation of Air Traffic Management Systems (NextGen):
 - ⇒ Formal framework for verification of aircraft separation systems
- Small Air Transportation System (SATS):
 - ⇒ Formal verification of operational concept
- Spacecraft Autonomy for Vehicles and Habitats (SAVH) & Autonomy for Operations (A4O):
 - ⇒ Semantics of synchronous language for autonomous spacecraft operations
- Theorem proving technology

- Minimal Operational Standard for Detect and Avoid of Unmanned Aircraft Systems (RTCA DO-365)
- Programming language for current and future space missions
- Operational concept for Urban Air Mobility
- Several libraries, hundreds of proofs, several strategies in the NASA PVS Library

Dedukti and Logipedia



Gilles, A Visionary



NASA Formal Methods 2018 (I)

Gilles delivered the keynote speech “*Formal methods: a plea for knowing what computers do*”.

The Nasa formal method team is 30 years old

This talk: formal methods in the next 30 years

We shall need more formal methods because we shall need more
and more to understand **what computers do**

A lot of work for the coming 30 years

Gilles, ta passion pour la science continuera de nous inspirer



- C. Rocha, C. Muñoz, and **G. Dowek**, *A formal library of set relations and its application to synchronous languages*, Theoretical Computer Science, 412, 37, 2011, pp. 4853-4866.
- **G. Dowek**, C. Muñoz, and C. Rocha, *Rewriting Logic Semantics of a Plan Execution Language*, 2010.
- **G. Dowek**, C. Muñoz, and C. Păsăreanu, *A Small-Step Semantics of PLEXIL*, Technical Report, 2008-11, National Institute of Aerospace, 2008.
- **G. Dowek**, C. Muñoz, and Corina S. Păsăreanu, *A Formal Analysis Framework for PLEXIL*, Third Workshop on Planning and Plan Execution for Real-World Systems, 2007.

- **G. Dowek**, C. Muñoz, and V. Carreño, *Formal Analysis of the Operational Concept for the Small Aircraft Transportation System*, *Rigorous Engineering of Fault-Tolerant Systems*, LNCS 4157, 2006, pp. 306-325.
- C. Muñoz and **G. Dowek**, *Hybrid Verification of an Air Traffic Operational Concept*, IEEE ISoLA Workshop on Leveraging Applications of Formal Methods, Verification, and Validation, 2005.
- **G. Dowek**, C. Muñoz, and V. Carreño, *Abstract Model of the SATS Concept of Operations: Initial Results and Recommendations*, NASA/TM-2004-213006, 2004.
- C. Muñoz, **G. Dowek**, and V. Carreño, *Modeling and Verification of an Air Traffic Concept of Operations*. *International Symposium on Software Testing and Analysis*, Software Engineering Notes, 29, 4, 2004, pp. 175-182.

References – AATT & NextGen I

- A. Narkawicz, C. Muñoz, and **G. Dowek**, *Provably Correct Conflict Prevention Bands Algorithms*, Science of Computer Programming, 77, 10-11, 2012, pp. 1039-1057.
- A. Narkawicz, C. Muñoz, and **G. Dowek**, *Formal verification of air traffic prevention bands algorithms*, Technical Memorandum, NASA/TM-2010-216706, 2010.
- R. Butler, G. Hagen, J. Maddalon, C. Muñoz, A. Narkawicz, and **G. Dowek**, *How Formal Methods Impels Discovery: A Short History of an Air Traffic Management Project*, Technical Memorandum, NASA/CP-2010-216215, 2010.
- J. Maddalon, R. Butler, C. Muñoz, and **G. Dowek**, *A Mathematical Analysis of Conflict Prevention Information*, 9th AIAA Aviation Technology, Integration, and Operations Conference, 2009. Extended version: Technical Memorandum, NASA TM-2009-215768, 2009.
- **G. Dowek** and C. Muñoz, *Conflict Detection and Resolution for 1, 2, ..., N Aircraft*, 7th AIAA Aviation Technology, Integration and Operations Conference, 2007.
- C. Muñoz, R. Siminiceanu, V. Carreño, and **G. Dowek**, *KB3D Reference Manual - Version 1.a*, NASA/TM-2005-213769, 2005.

References – AATT & NextGen II

- **G. Dowek**, C. Muñoz, and V. Carreño, *Provably Safe Coordinated Strategy for Distributed Conflict Resolution*, AIAA Guidance Navigation, and Control Conference and Exhibit, 2005.
- C. Muñoz, R. Butler, V. Carreño and **G. Dowek**, *Formal verification of conflict detection algorithms*, International Journal on Software Tools for Technology Transfer, 4, 3, 2003, pp. 371-380. Extended version: Technical report NASA/TM-2001-210864.
- A. Geser, C. Muñoz, **G. Dowek**, and F. Kirchner, *Air Traffic Conflict Resolution and Recovery*, ICASE Report 2002-12, 2002.
- **G. Dowek**, C. Muñoz, and A. Geser, *Tactical conflict detection and resolution in a 3-D airspace*, Proceedings of Air Traffic Management R & D Seminar, 2001. Extended version: Technical Report, NASA/CR-2001-210853 and ICASE 2001-7, 2001.