HiPEAC 2020
Adaptive CPS architectures, methods and tools:
the CERBERO project
January 22, 2020


# Formal Methods in the CERBERO Toolchain

**Luca Pulina, Università degli Studi di Sassari**

Horizon 2020
European Union funding
for Research & Innovation

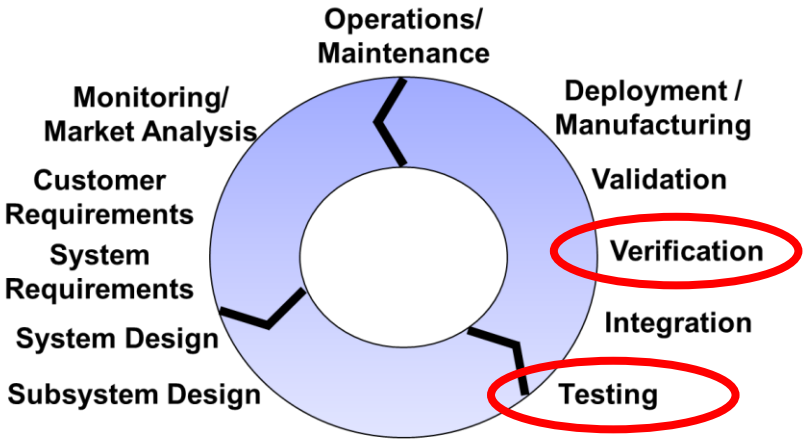
# Formal Methods


From aeronautic standard DO-178C:
*"Descriptive notations and analytical methods used to **construct, develop and reason about mathematical models of system behavior**. A formal method is a **formal analysis** carried out on a formal model"*

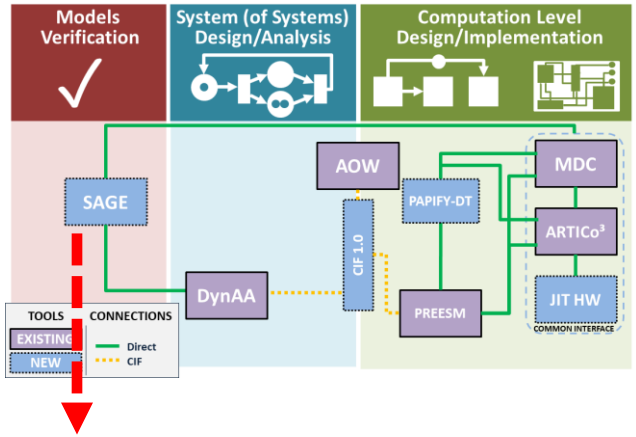
- Mathematically based techniques for the specification, development and verification of SW and HW systems.

- **Appropriate mathematical analysis can contribute to the reliability and robustness of a design**.

# Formal Methods (tools) in CERBERO




Continuous Model Based Engineering

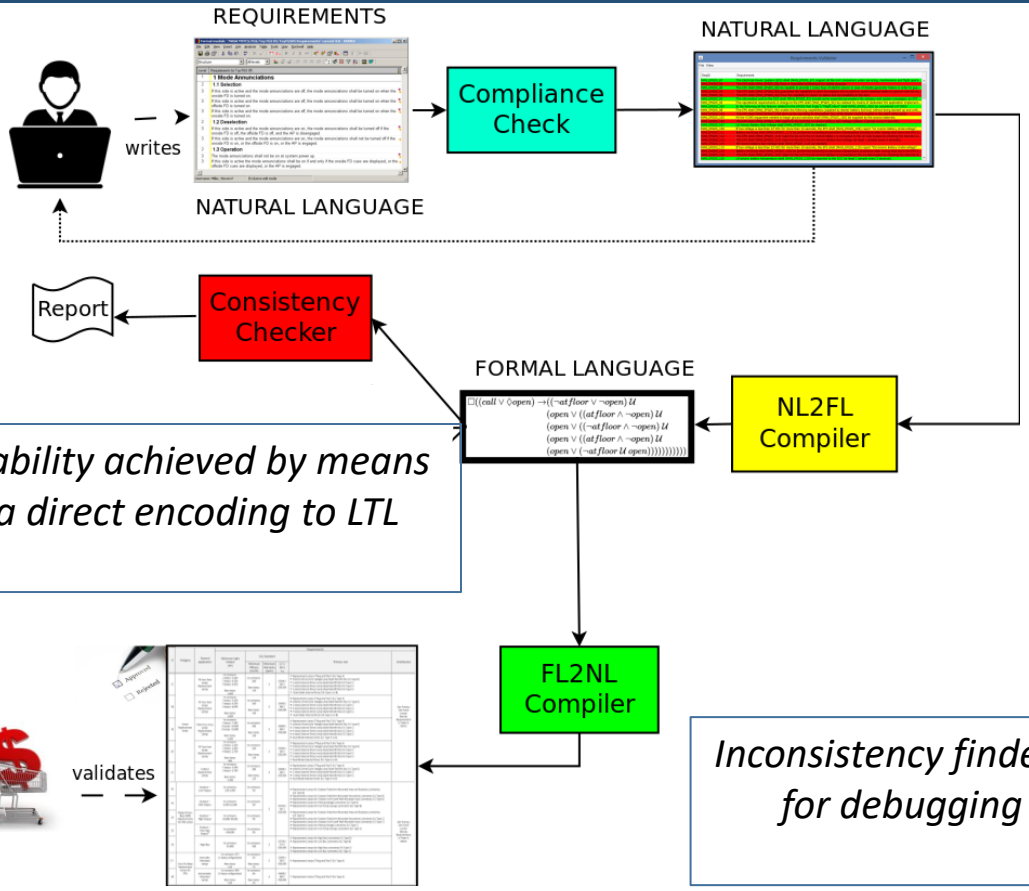



- **ReqV**: automatically check consistency of a set of requirements provided by the user.
- **ReqT**: requirement-based automated test generation.
- **HyDRA**: automated syntesis of high-level policies.

Open-source implementations (see the CERBERO web site)

# ReqV

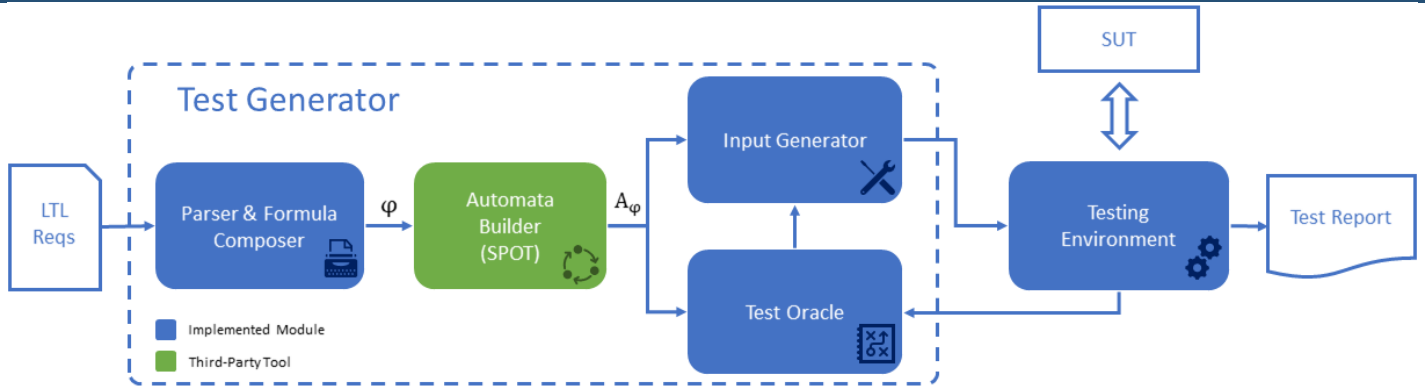
*Property Specification Patterns for Linear Temporal Logic with numerical constraints*



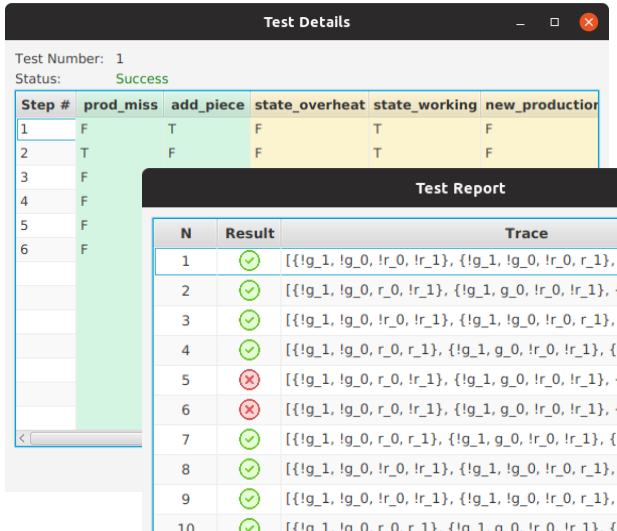

*Scalability achieved by means of a direct encoding to LTL*

*Inconsistency finder procedure for debugging purpose*

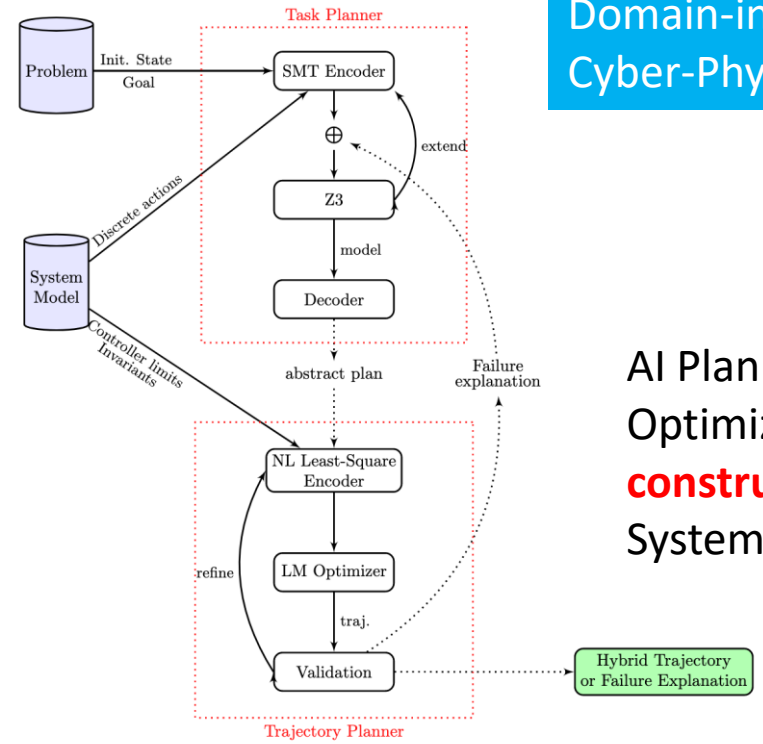
# ReqT




- Focus on black-box testing
- The quality of the generated test suite is comparable to the one obtained with MBT
- Formal assurance of the testing coverage



# Hydra




Domain-independent tool for Goal-Oriented control of Cyber-Physical Systems.

AI Planning + Satisfiability Modulo Theories + Numeric Optimization => derivation of goal-oriented, **correct by construction** strategies from high-level model of Hybrid Systems.

# References


- Narizzano, M., Pulina, L., Tacchella, A., & Vuotto, S. (2019). Property specification patterns at work: Verification and inconsistency explanation. *Innovations in Systems and Software Engineering*, *15*(3-4), 307-323.
- Vuotto, S., Narizzano, M., Pulina, L., & Tacchella, A. (2019, April). Poster: Automatic consistency checking of requirements with reqv. In *2019 12th IEEE Conference on Software Testing, Validation and Verification (ICST)* (pp. 363-366). IEEE.
- Narizzano, M., Pulina, L., Tacchella, A., & Vuotto, S. (2018, April). Consistency of property specification patterns with boolean and constrained numerical signals. In *NASA Formal Methods Symposium* (pp. 383-398). Springer, Cham.
- Vuotto, S., Narizzano, M., Pulina, L., & Tacchella, A. (2019, May). Automata based test generation with SpecPro. In *2019 IEEE/ACM 6th International Workshop on Requirements Engineering and Testing (RET)* (pp. 13-16). IEEE.
- Bit-Monnot, A., Leofante, F., Pulina, L., & Tacchella, A. (2019, July). SMT-based Planning for Robots in Smart Factories. In *International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems* (pp. 674-686). Springer, Cham.
- Bit-Monnot, A., Pulina, L., & Tacchella, A. (2019, July). Cyber-Physical Planning: Deliberation for Hybrid Systems with a Continuous Numeric State. In *Proceedings of the International Conference on Automated Planning and Scheduling* (Vol. 29, No. 1, pp. 49-57).