Formal Verification of HILECOP: A Process to Design and Implement Critical Digital Systems.

V. Iampietro[1], D. Andreu[1,2], D. Delahaye[1]

[1] *LIRMM, Université de Montpellier, CNRS, Montpellier, France.*
[2] *NEURINNOV, Montpellier, France.*

Key words — Critical Digital Systems, Formal Verification, Petri Nets, HILECOP Methodology, Coq Proof Assistant.

Abstract :

Digital systems are said to be critical when a malfunction on their side puts human lifes at risk. The design of such systems often relies on formal models from which safety and correctness properties can be checked. The HILECOP methodology for the design and implementation of critical digital systems proposes Synchronously executed Petri Nets (SPNs) as a formalism to model the behavior of systems. In the HILECOP workflow, source code for hardware description (VHDL) is generated from Petri net models to finally implement the digital system on a physical circuit. Then, it remains to be proved that the behavior of the digital system described with Petri nets is preserved in the generated VHDL code. In this poster, we present, as a first step towards the establishment of this proof, our modeling of SPNs and their semantics, i.e their evolution rules, using the Coq proof assistant.

References

[1] Andreu, D. and Guiraud, D. and Souquet G. *A distributed architecture for activating the peripheral nervous system*, Journal of Neural Engineering, vol. 6(2), feb. 2009.