Formal Property Verification of the Digital Section of an Ultra-Low Current Digitizer ASIC

K. Ceesay-Seitz, S. Kundumattathil Mohanan, H. Boukabache, D. Perrin

CERN, European Organization of Nuclear Research, Geneva, Switzerland

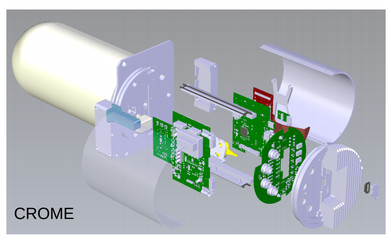
accellera SYSTEMS INITIATIVE™

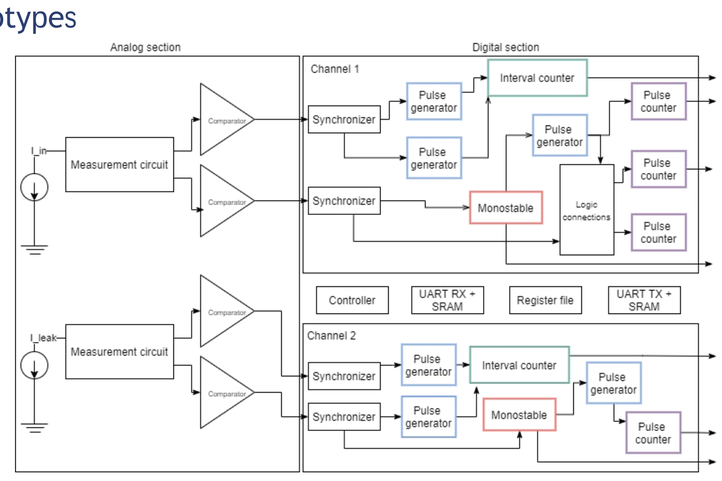
2021 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION EUROPE OCTOBER 26-27, 2021

INTRODUCTION

- CERN (European Organization for Nuclear Research) conducts particle physics experiments which produce radiation
- Radiation Protection Group is responsible for measuring levels of ionizing radiation and for ensuring radiological safety of people

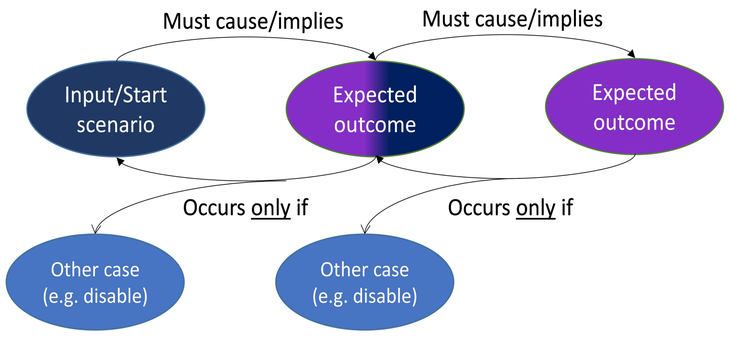
- Aim of this work: Demonstrate examples of Formal Property Verification of the digital section of the ASIC prototypes for the future front end of the CERN RadiatiOn Monitoring Electronics (CROME)

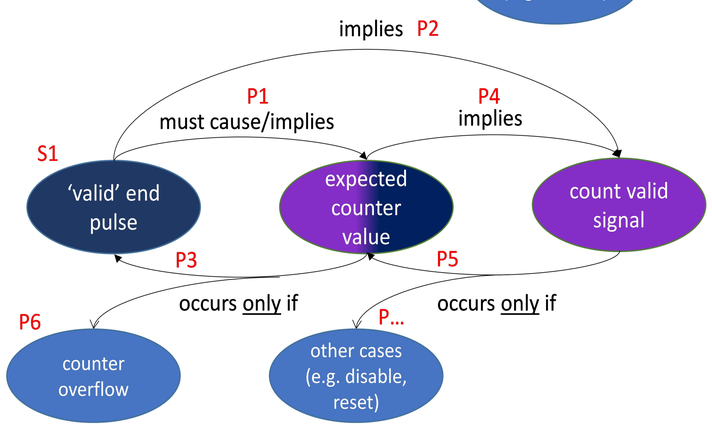




Chain of Events

- Challenges:
  1. Sequential nature - Input current is determined by several counters of up to 40 bits
  2. Many corner cases





- Analyze requirements as chain of events
- Use properties of short sequential depth to express relationship between 2 events

Proving the Current Counters

Counting with Local Variables

```
assert property(
 reg[`Bit_Width - 1:0] lCnt; // local counter
 (((cond1, lCnt = 1) or (cond2 or cond3, lCnt = 0))[*0:$]
    ##1
 ((cond4, lCnt++) or (cond5, lCnt = lCnt))[*0:$]
    ##1
 ((cond6, lCnt = lCnt) or (cond7, lCnt = 1)))
 |=> (lCnt == duvCnt);
);
```

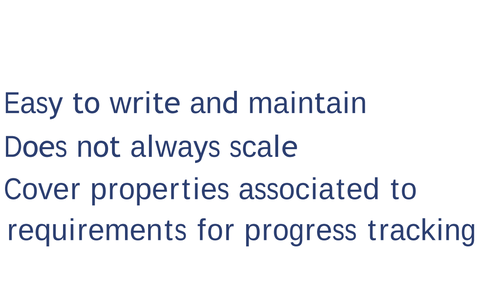
- Hard to write, read and debug
- Scaled better than Reference Models
- Cover properties to ensure that all 'or' branches in antecedent are reachable

Two Clock Cycle Property

```
assert property(
  // Normal counting
    counter == $past(counter) + 1 ||
  // Case 1: counting not started
    ( ($past(counter) == 0 ||
  // Case 2/3: counter should reset
     $past(counter) == $past(targetValue) ||
     otherCondition)
    && counter == 0 )
);
```

- Property describes full requirement
- Very efficient, exhaustive proof within seconds
- Only for counters with few input dependencies

Reference Models



- Easy to write and maintain
- Does not always scale
- Cover properties associated to requirements for progress tracking

CONCLUSIONS

- Safety standard compliant methodology including
  - detailed specification
  - requirements based progress tracking
  - regular review meetings
  → lead to early fault discoveries and less debugging effort
- Wrong property affects larger part of the functionality than a wrong test case
  → quality assurance techniques necessary
- Structural coverage with reduced bit-width does not reveal cases where small values/bit-widths are mistakenly hard-coded → add functional coverage
- Counter examples recreated in simulation by designer for analysis and bug fixing

- Chain-of-Events-based requirements analysis lead to efficient properties
- Properties with small structural size and short sequential depth do not guarantee fast proof results
- Counters: Each method has its strengths/weaknesses and applicability
- Formal with synthesis semantics is closer to silicon than simulation
  → revealed 'X' values inside the design

- Found 30 faults, many corner cases
- Proved 70 properties
- Detailed examples of properties and results in the paper

REFERENCES

[1] H. Foster, Wilton Research Group and Mentor, A Siemens Business, "2020 Functional Verification Study"
[2] H. Boukabache, M. Pangallo, G. Ducos, N. Cardines, A. Bellotta, C. Toner, D. Perrin, D. Forkel-Wirth, "Towards a novel modular architecture for CERN radiation monitoring," Radiat. Prot. Dosim. 173 (2017), pp.240-244, 2017
[3] S. Kundumattathil Mohanan, An Accurate Ultra-low Current Measurement ASIC for Ionization Chamber Readout, PhD thesis (to be published)
[4] E. Seligman, T. Schubert, M V A.K. Kumar, "Formal Verification: An Essential Toolkit for Modern VLSI Design", Morgan Kaufmann, 2015, ISBN-13: 978-0128007273
[5] C. Krieg, M. Rathmair, F. Schupfer, "A Process for the Detection of Design-Level Hardware Trojans Using Verification Methods", 2014 IEEE Intl Conf on High Performance Computing and Communications, 2014 IEEE 6th Intl Symp on Cyberspace Safety and Security, 2014 IEEE 11th Intl Conf on Embedded Software and Syst (HPCC,CSS,ICESS), 2014, pp. 729-734, doi: 10.1109/HPCC.2014.112.
[6] A. Li, H. Chen, J.K. Yu, E.L. Teoh, I.P. Anand, "A Coverage-Driven Formal Methodology for Verification Sign-off", Design and Verification Conference and Exhibition (DVCon) United States, 2019
[7] A. Gaur, G. Jain, R. Singh, "Metrics Driven Sign-off for SoC Specific Logic (SSL) Using Formal Techniques", Design and Verification Conference and Exhibition (DVCon) United States, 2021
[8] Ceesay-Seitz K., Boukabache H., Perrin D. (2020) A Functional Verification Methodology for Highly Parametrizable, Continuously Operating Safety-Critical FPGA Designs: Applied to the CERN RadiatiOn Monitoring Electronics (CROME). In: Casimiro
[9] A., Ortmeier F., Bitsch F., Ferreira P. (eds) Computer Safety, Reliability, and Security. SAFECOMP 2020. Lecture Notes in Computer Science, vol 12234. Springer, Cham. https://doi.org/10.1007/978-3-030-54549-9_5
[10] A. Darbari, I. Singleton, "Industrial Strength Formal Using Abstractions", In: CoRR (2016), https://arxiv.org/abs/1606.02347
[11] A. Darbari, "Smart Formal for Scalable Verification", Design and Verification Conference and Exhibition (DVCon) United States, 2019
[12] S. Sutherland, I'm Still In Love With My X!, Design and Verification Conference and Exhibition (DVCon) United States, 2013 European Committee for Electrotechnical Standardization, "Functional safety of electrical/electronic/programmable electronic safety-related systems," May 2010
[13] X. Yhang, M. Tehranipoor, "Case Study: Detecting Hardware Trojans in Third-Party Digital IP Cores", 2011 IEEE International Symposium on Hardware-Oriented Security and Trust, 2011, pp. 67-70, doi: 10.1109/HST.2011.5954998.

Instrumentation & Logistics Section, Radiation Protection Group, Health & Safety and Environmental Protection Unit
CERN, European Organization of Nuclear Research, Geneva, Switzerland