

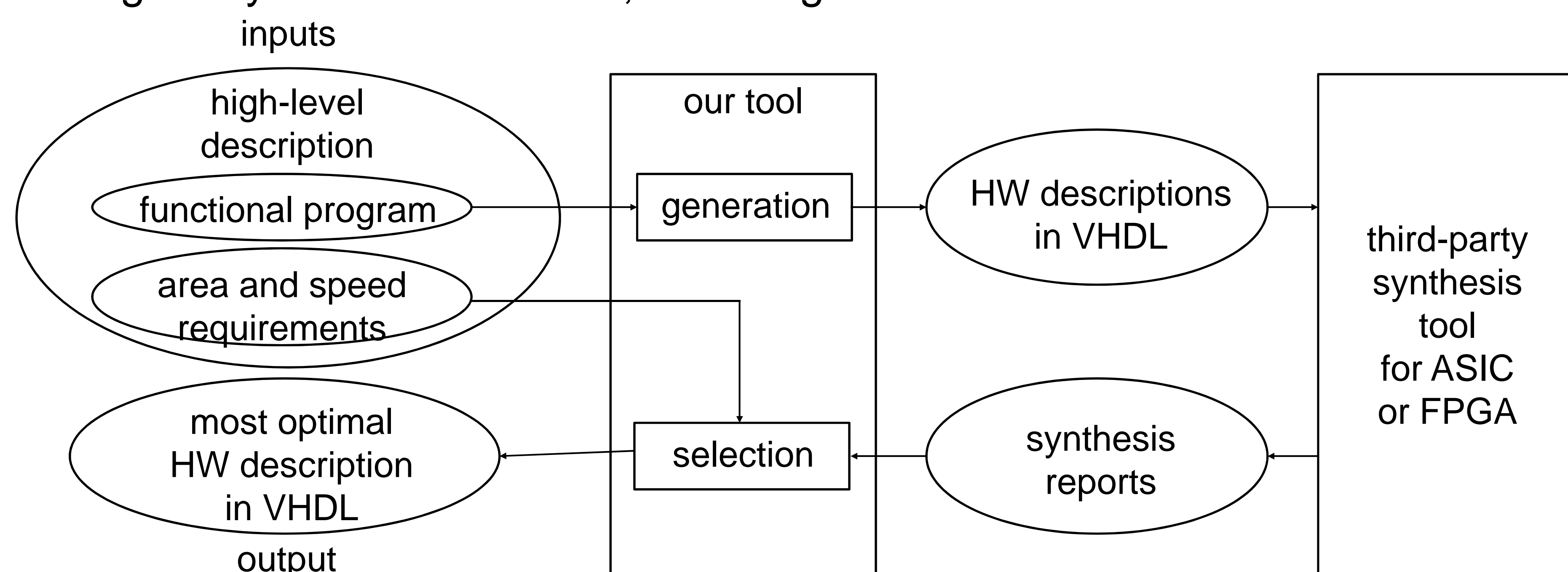
Using FP & Data Mining to Generate Constrained Hardware for Dedicated Algorithms

• Results from a previous ‘risky’ project ^α

- design space exploration of large number modular arithmetic operations using FP and Lava
 - exploration in the generation phase (by exploring different architectures for addition, multiplication, FSM, ...)
 - exploration in the synthesis phase (by exploring options of synthesis tool)
- data path example: 192-bit adder → 32 automatically generated architectures
- control logic example: AES controller → 18 automatically generated architectures

• Current design flow

- Generating many different versions; selecting the solution that best fits the constraints imposed by the user



• Goals of project starting this spring ^β

- demonstrating applicability in a commercial setting by interfacing to industrial tool flow
- expanding from basic building blocks to entire algorithms
- integrating different types of (simple) domain-specific algorithms and libraries

CALL FOR COOPERATION

• Projected follow-up projects

- Adding data mining and machine learning to prune the search tree and speed up generation
- Integrating more domain-specific algorithms and libraries

^α Funded by BOF project CREA/09/016 of the KU Leuven.

Projects are selected on creative, multidisciplinary ideas with uncertain outcome

^β Funded by IOF HB/13/020 of the KU Leuven

Projects are selected on leverage potential for industrial valorisation

K. Aerts^{2,3}, N. Mentens^{1,3}

¹ KU Leuven, ESAT-COSIC, Kasteelpark Arenberg 10, 3001 Leuven, Belgium

² KU Leuven, CS-Informatica/DTAI, 3001 Leuven, Belgium

³ KU Leuven@KHLim, ES&S, Agoralaan Gebouw B/8, 3590 Diepenbeek, Belgium
email: {kris.aerts, nele.mentens}@kuleuven.be