Our Research Activity

ー From the Viewpoint of Functional Safety ー

Makoto Sugihara

System LSI Research Center

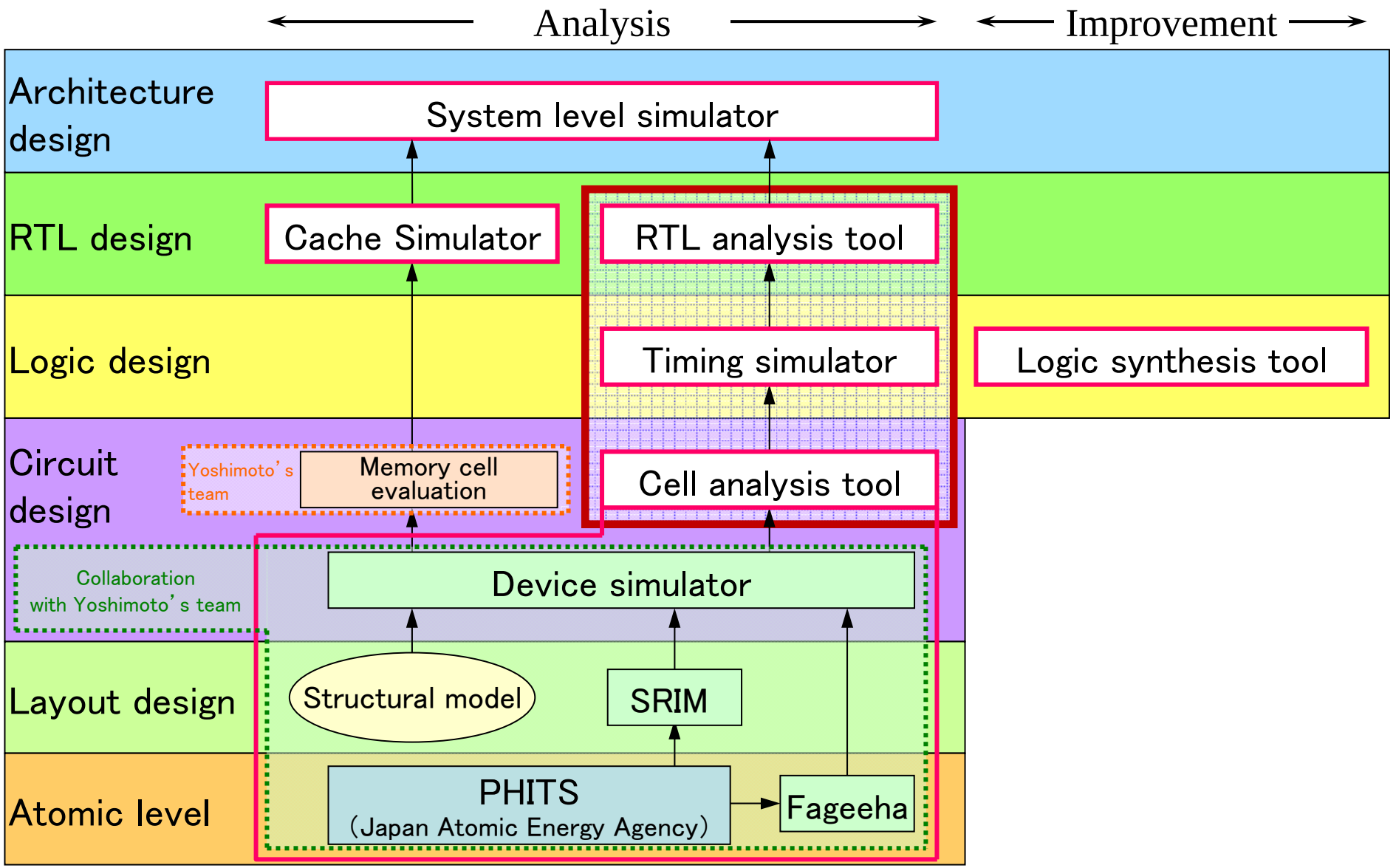
Kyushu University

Our Research Targets

$$dependability = reliability + maintainability + availablity + security + safety$$

Our Team's Targets

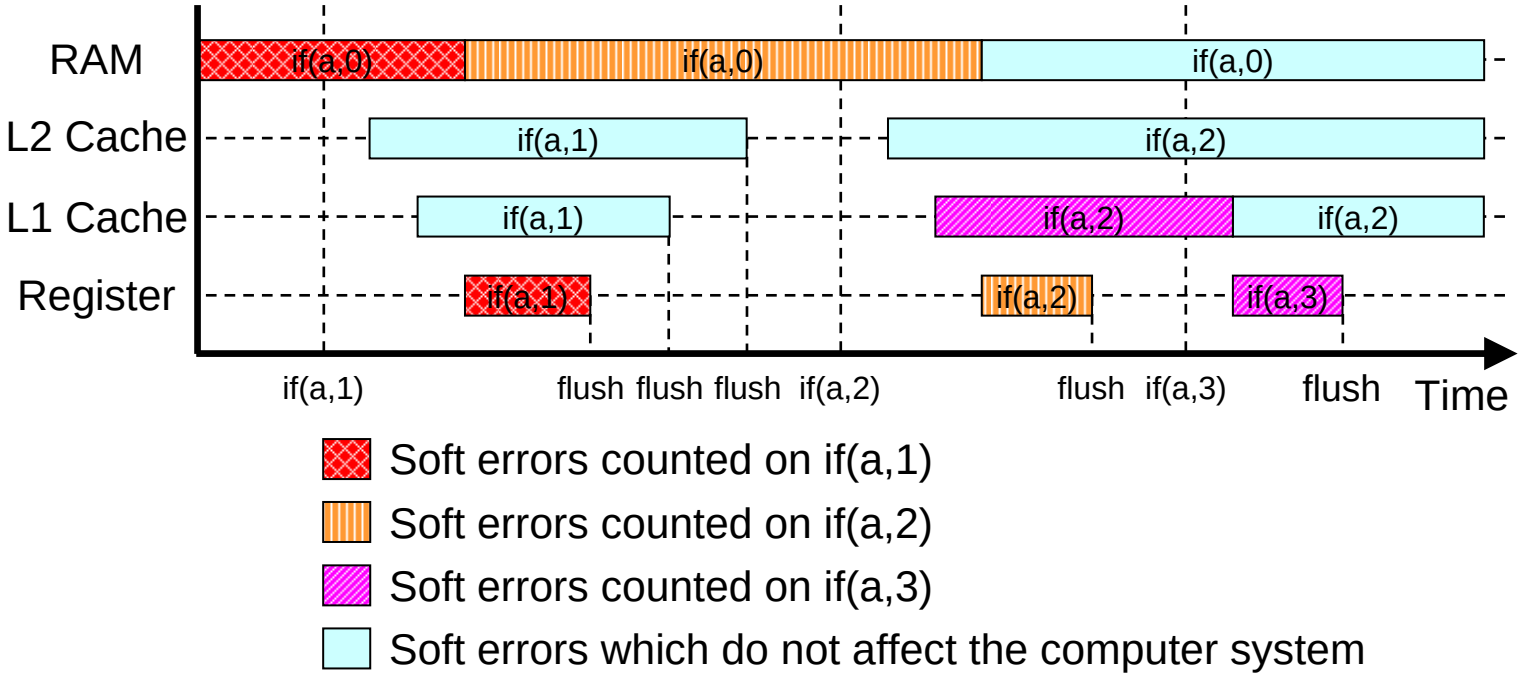
Tool Chain for Soft Error Issue



My Research Activity on Soft Error Issue

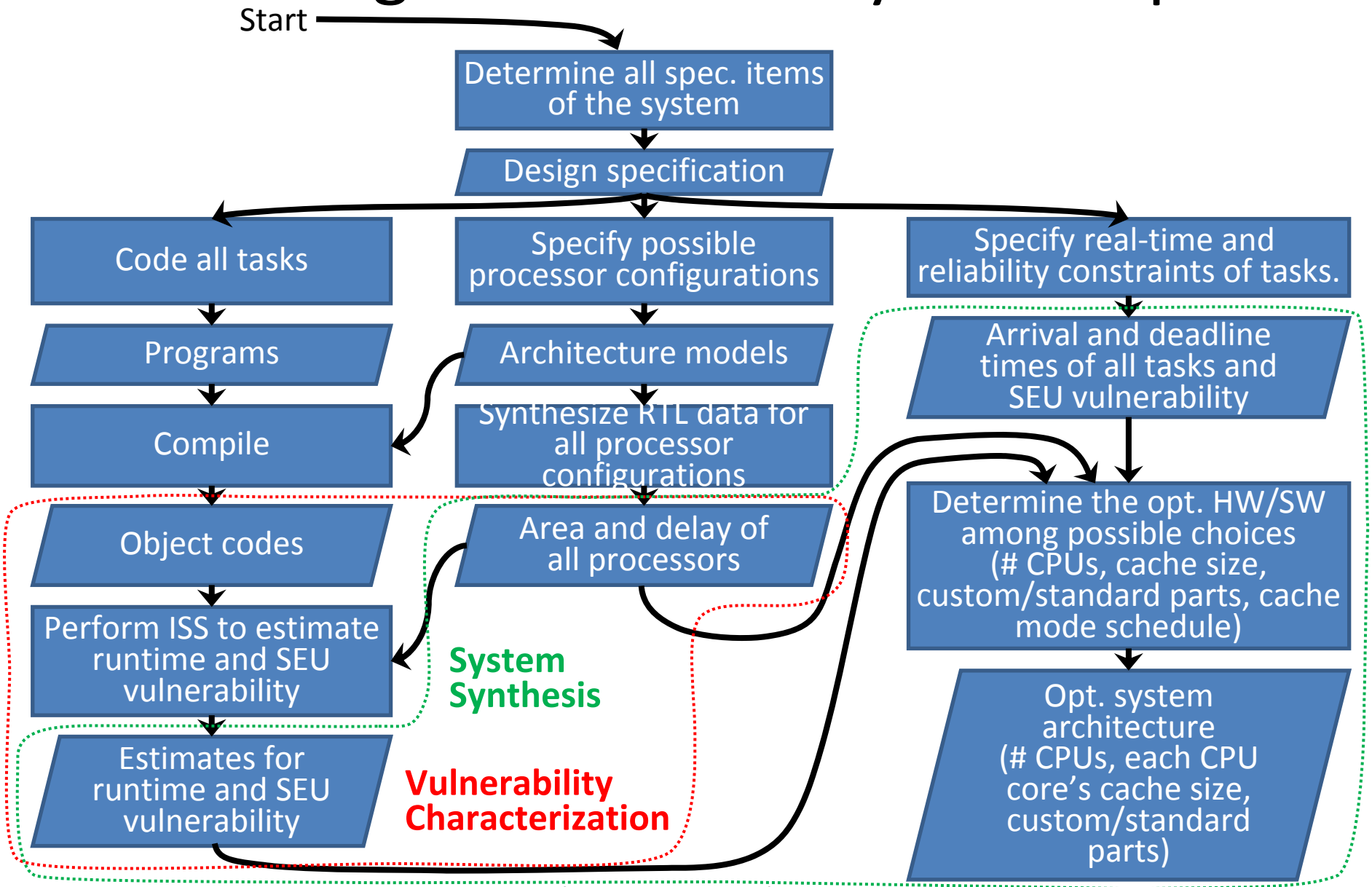
- Reliability analysis:
  - Vulnerability estimation technique for a memory system of a computer (IEICE Trans. 2007).
- Design for reliability:
  - Memory management method for an embedded system (DATE 2007).
  - Memory management method for a multiprocessor system (ISQED 2008).
  - Heterogeneous multiprocessor synthesis (DSD 2009).
  - Continuous signature monitoring technique (DSD 2010).
  - Memory objects allocation for a reliable embedded system (ESS 2011).

Reliability Estimation of a Memory System



Our estimation technique calculates the temporal and spatial use of every data item at each level of memory hierarchy so that we can calculate the number of SEUs on the data time.

Our Design-for-Reliability Techniques



Functional Safety Standards

- Safety of a system is determined by three factors:
  - Frequency (likelihood) of occurrence of a hazardous event.
  - Consequence of a hazardous event.
  - Safety functions applied to a system.
- Safety of a system is typically measured with a safety integrity level (SIL), that is a discrete, rough measure adopted in functional safety standards such as IEC 61508 and ISO 26262.
- Adopting a safety function specified in the standards raises the safety integrity level.
- IEC 61508 is intended to be a basic functional safety standard to all kinds of industry.
- ISO 26262 is a functional safety standard to automotive industry.
- It is not easy to adopt IEC 61508 to all application domains because design requirements vary depending on each domain.
  - Many variants were made.
- We think that functional safety standard of each application domain should be developed.

Impact on Functional Safety Standards

- Our reliability estimation technique helps to quantitatively evaluate how reliable a memory system of a computer is.
  - Our technique helps to invent safety integrity levels to a new application domain.
- Our design-for-reliability techniques help to improve the reliability of a computer system.
  - Our DFR techniques can serve as safety functions that raise the safety integrity level of a system.

Thank you for your attention!