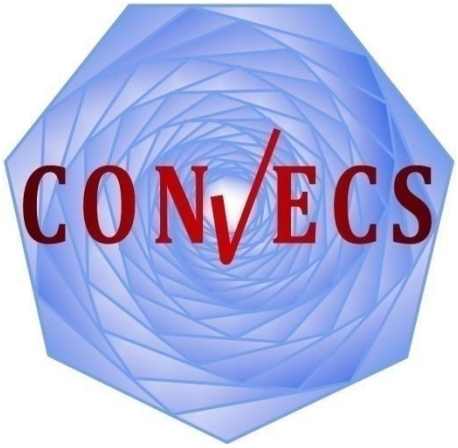
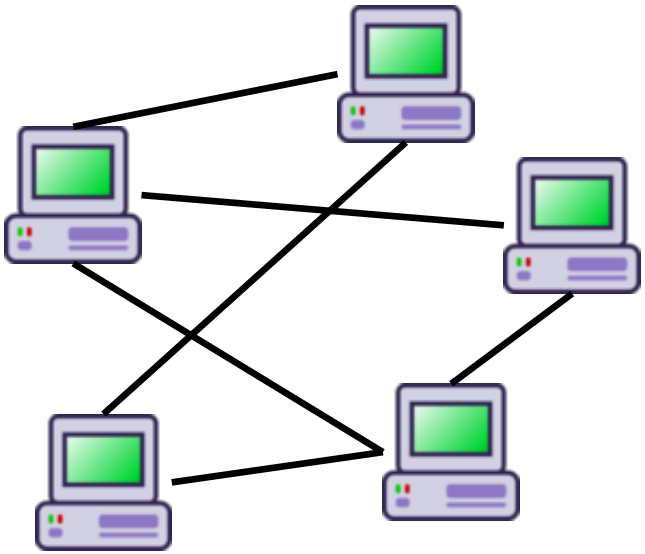
Rapid Prototyping of Formally Verified Distributed Systems

(Officially: “Parallel Code Generation in the Cloud”)

Hugues EVRARD



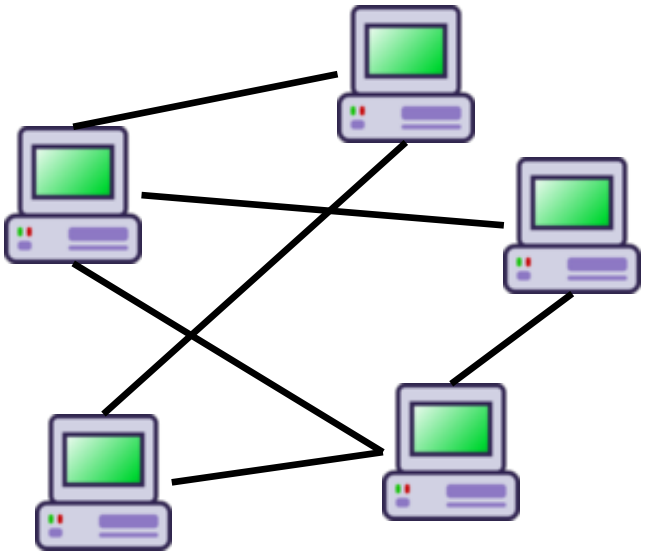
Inria informatics mathematics
LIG



Specifications

- Each component

- Their interactions
  (synchronization on gates)



Specifications

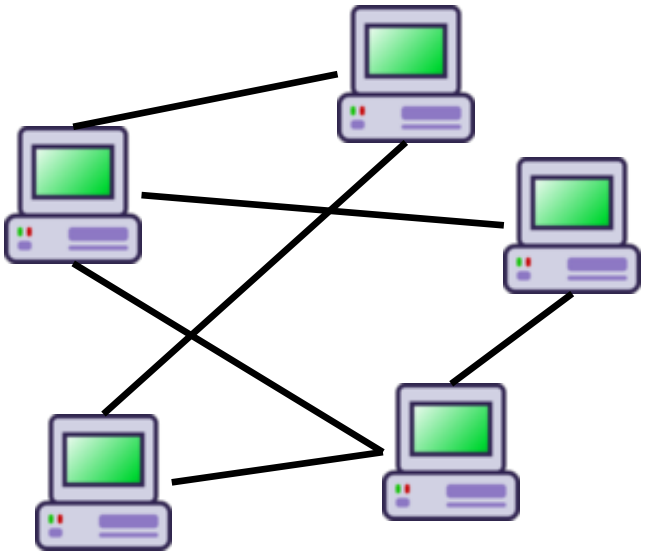
- Each component

- Their interactions
  (synchronization on gates)

Verifications

Formal Methods (model checking…):
- verify properties (no deadlock…)
- equivalence of behaviors…

⇒ **Trustworthy System Specs.**



Specifications

- Each component

- Their interactions
  (synchronization on gates)

Implementation ?

Specification → Executable

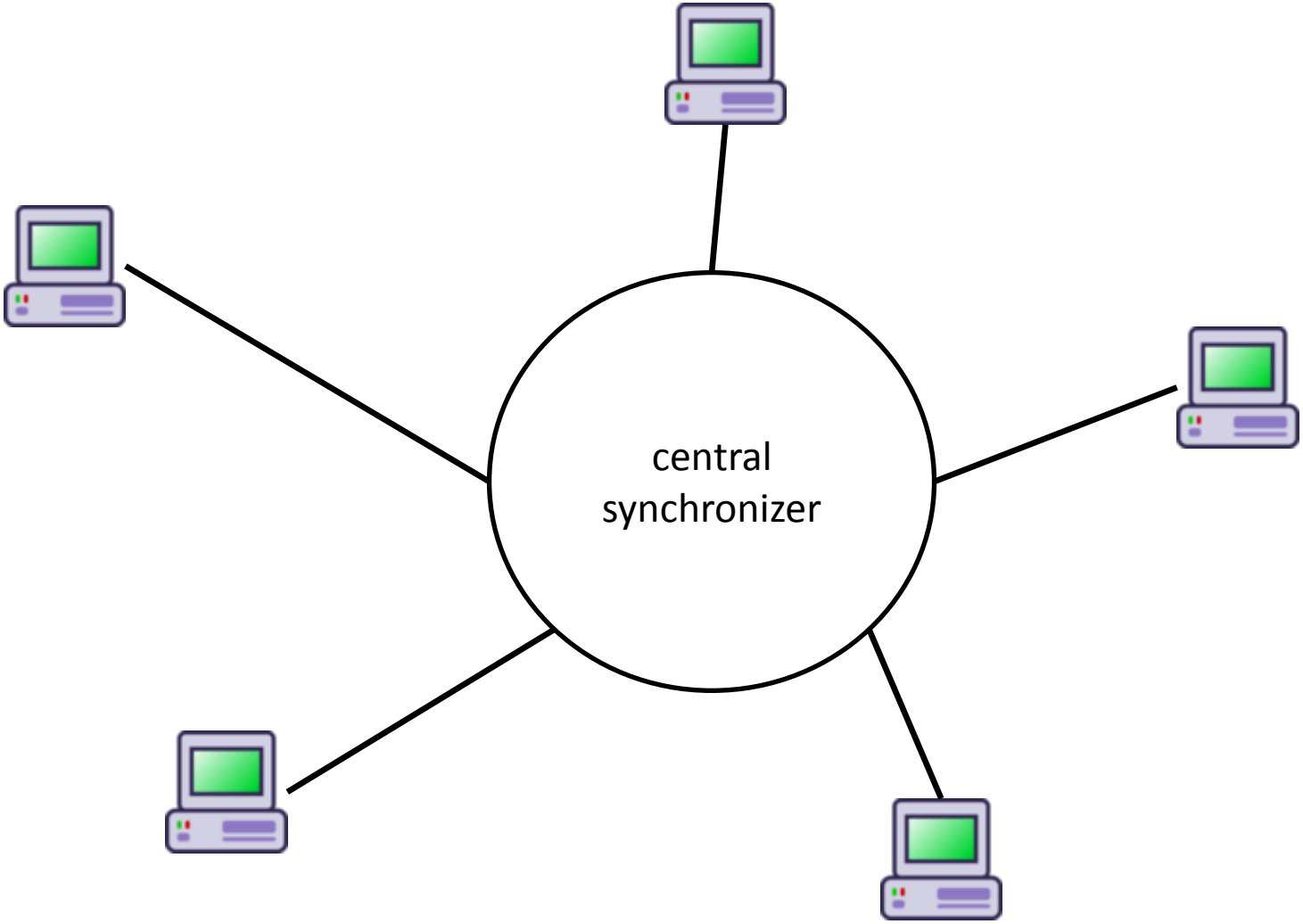
- Component → State Machine (OK)

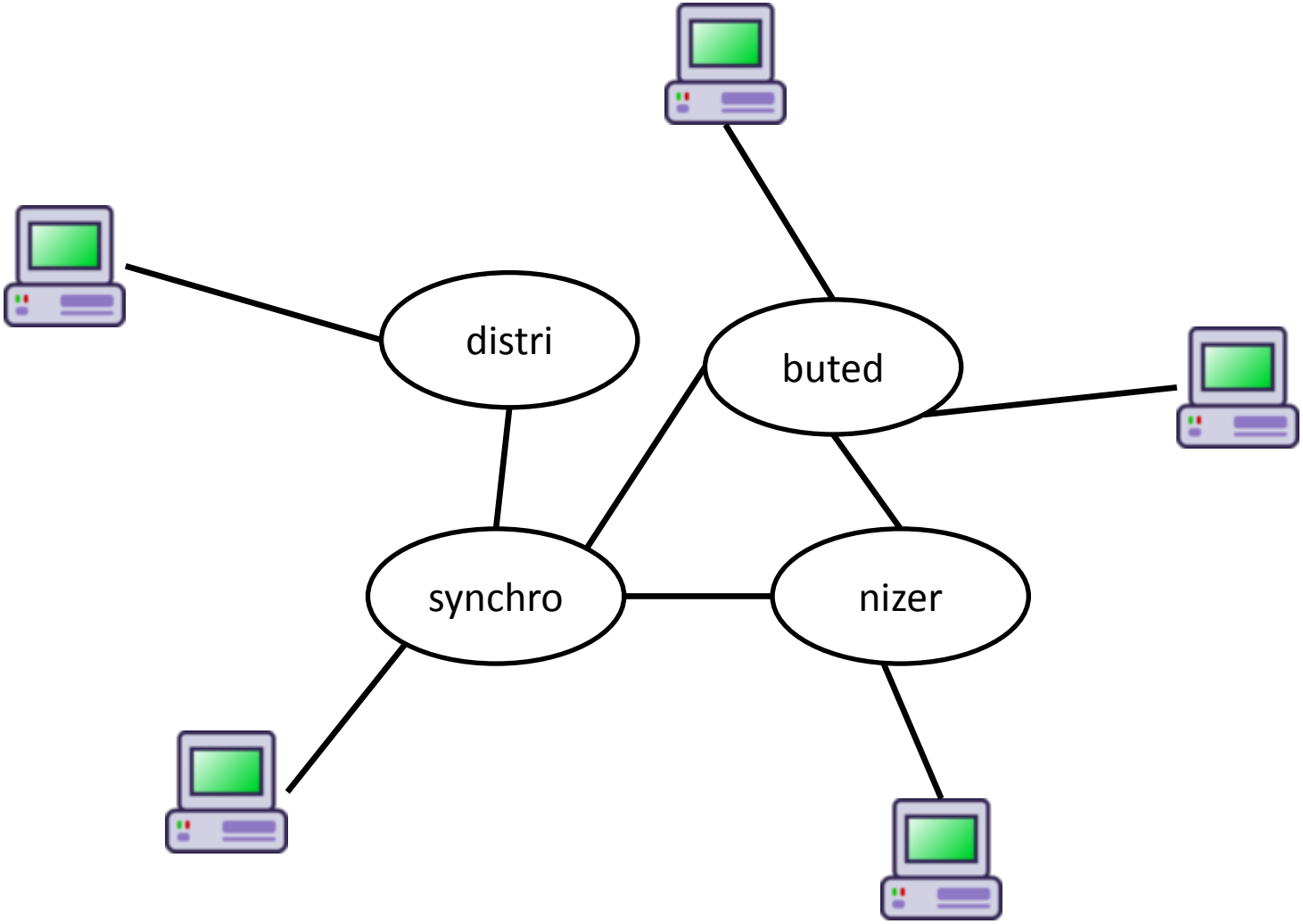
- **Interactions → Synchro Protocol**

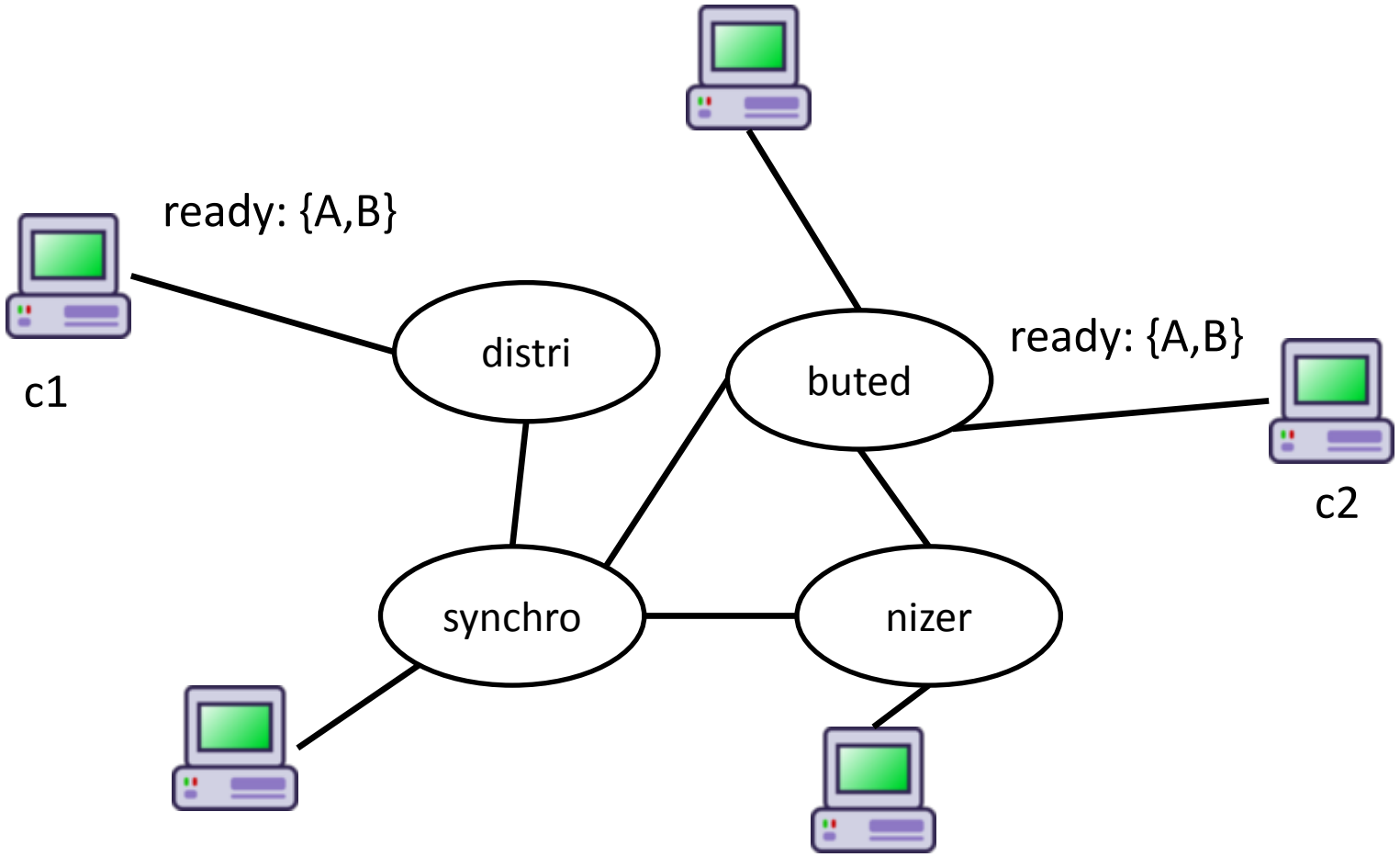
Verifications

Formal Methods (model checking…):
- verify properties (no deadlock…)
- equivalence of behaviors…

⇒ **Trustworthy System Specs.**


central
synchronizer


distri
buted
synchro
nizer



non-determinism:

Components can be ready on **several synchro at the same time**

eg: Both **c1** and **c2** are ready on synchro **A** and **B**

THANKS

- Paper:
  - “Formal Verification of Distributed Branching Multiway Synchronization Protocol” (Evrard, Lang, FORTE’13)
  - (Found a bug in an already published protocol)