

Formalization and Validation

Jörg Desel
Katholische Universität Eichstätt-Ingolstadt

Formalization and Validation

An Iterative Process in Model Synthesis

Jörg Desel
Katholische Universität Eichstätt-Ingolstadt

What is Validation of a system?



Validation: Did we build the right system?

Does the system fulfill the purpose for which it was intended?
Which aspects are missing? What is wrong?

Verification: Did we build the system right?

Automated or manual creation of a proof
showing that the system matches its specification.
Which specification is not satisfied? Counterexample?

Evaluation: Is the system useful?

Will it be accepted by the intended user?
Aspects that cannot be formulated in terms of formal specification.

What is Validation of a model?

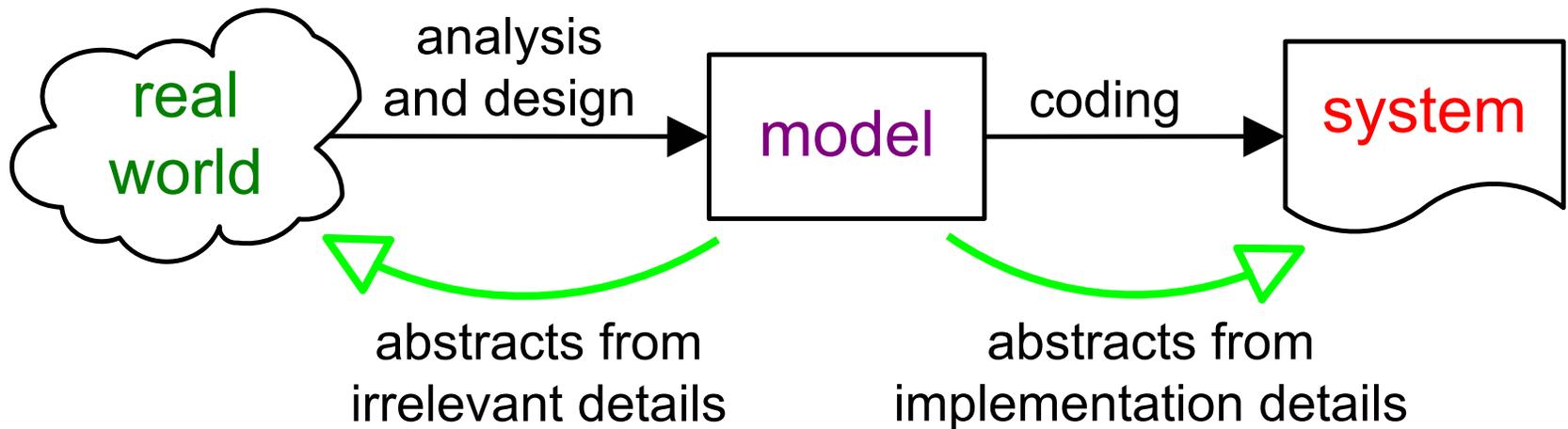
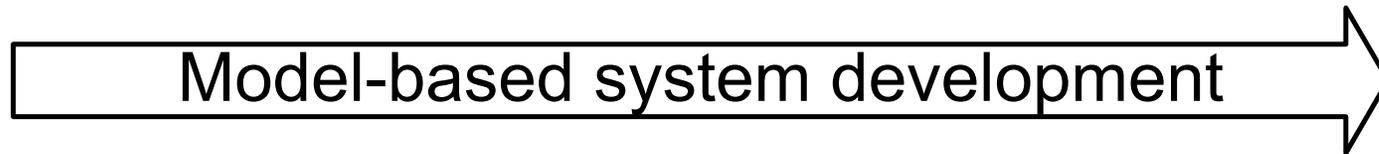


Validation: Did we build the right model?

Does the **model** fulfill the purpose for which it was intended?
Which aspects are missing? What is wrong?

**What is the purpose of a model
in system development?**

Model-based System Development

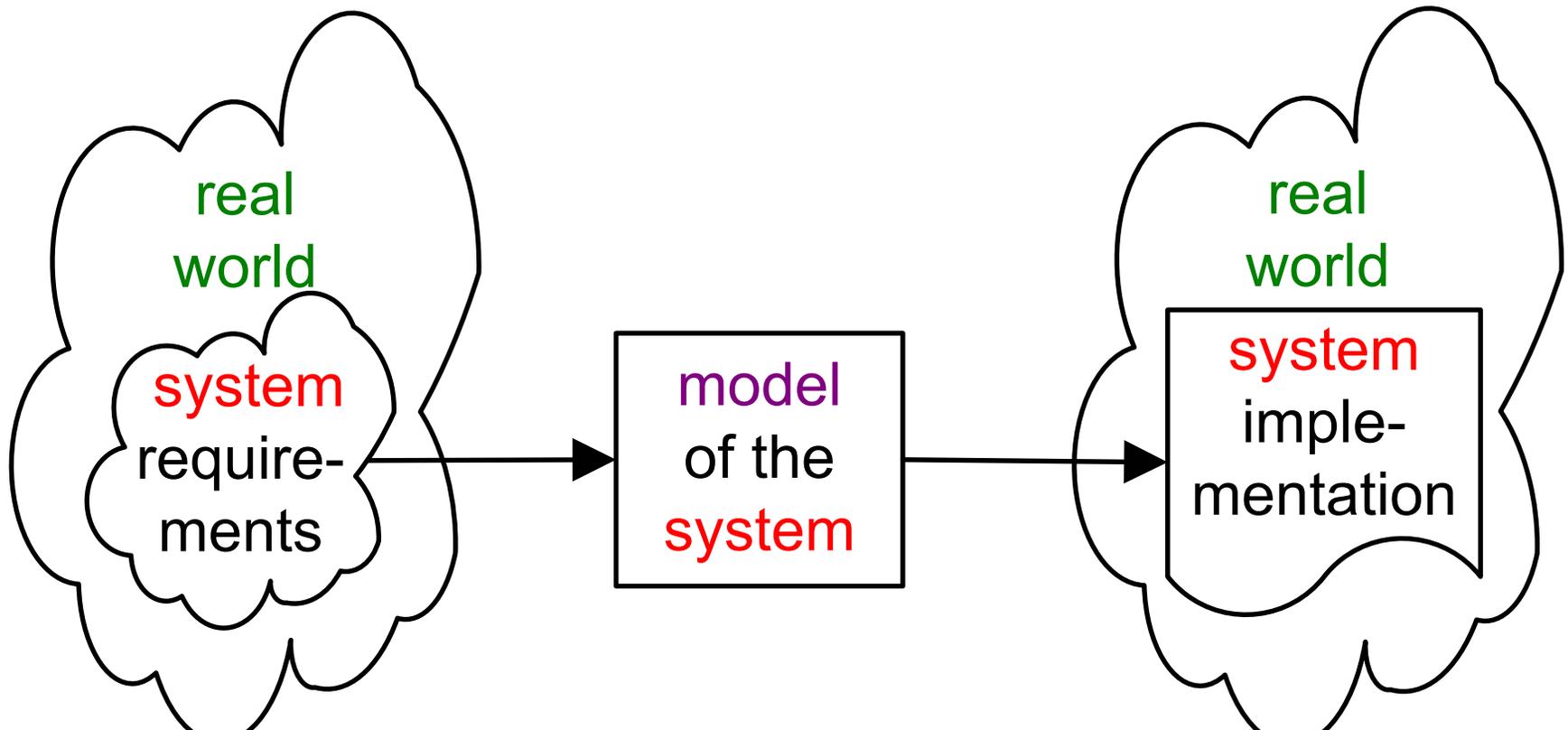


taken from:

Gregor Engels et al.: UML - a universal modeling language?

Invited talk at Petri Nets 2000, Aarhus. LNCS 1825

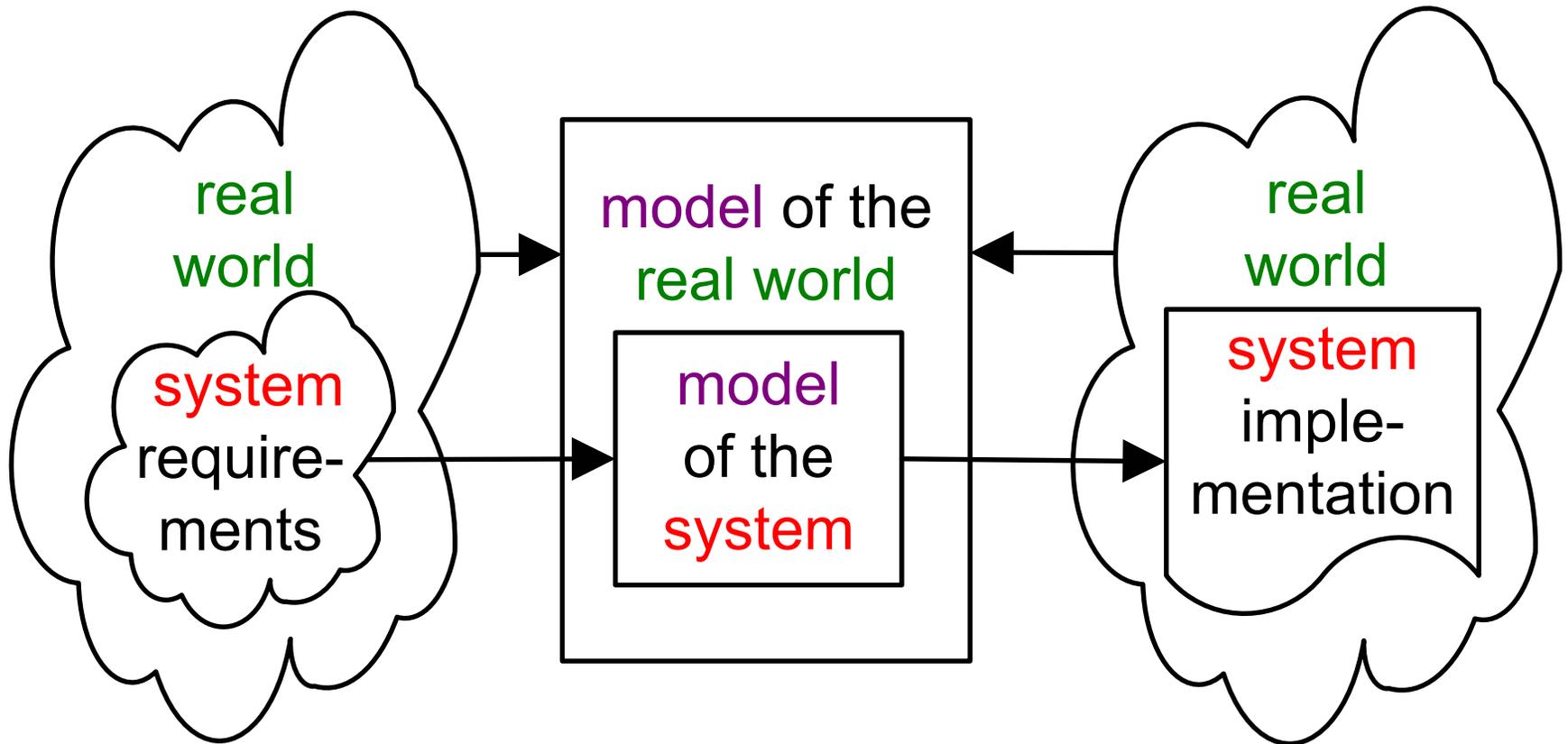
A System in the Real World



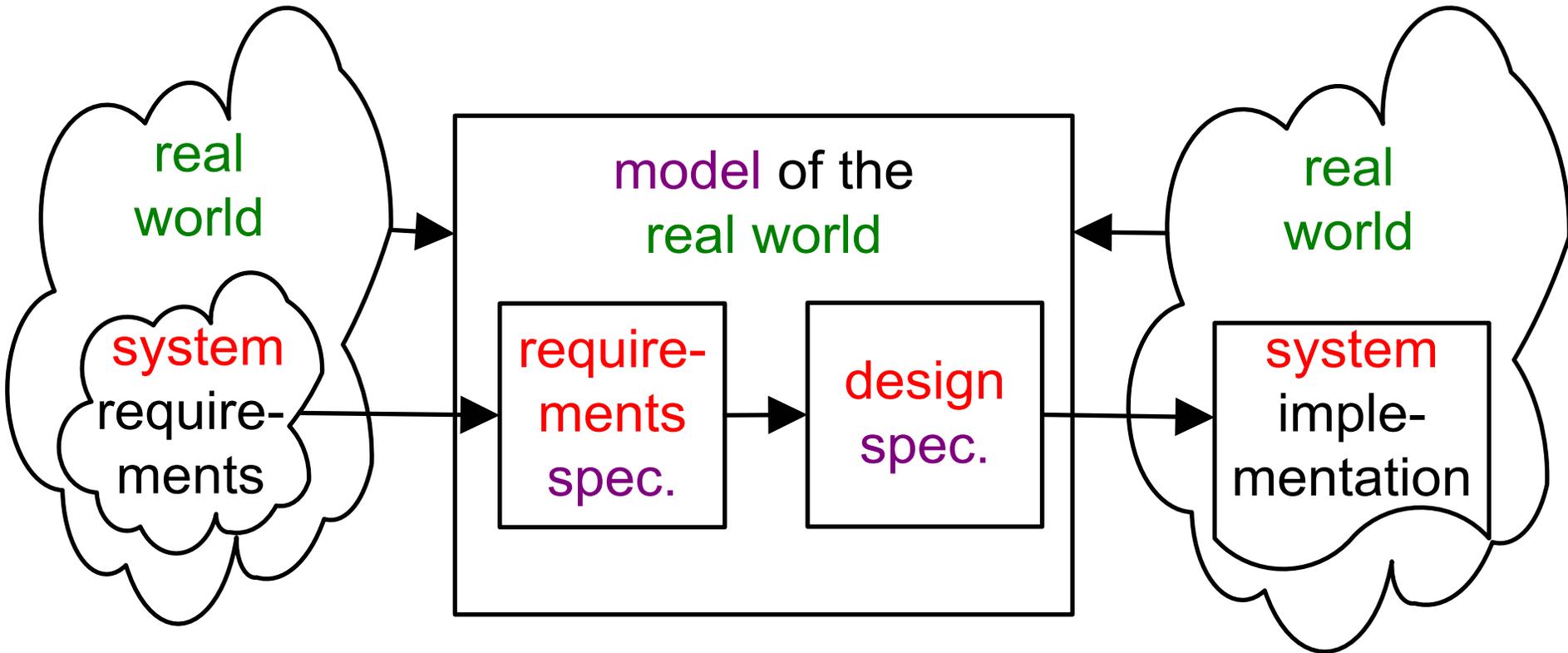
real world:

**plant / environment / assumptions on the environment /
known szenarios / ...**

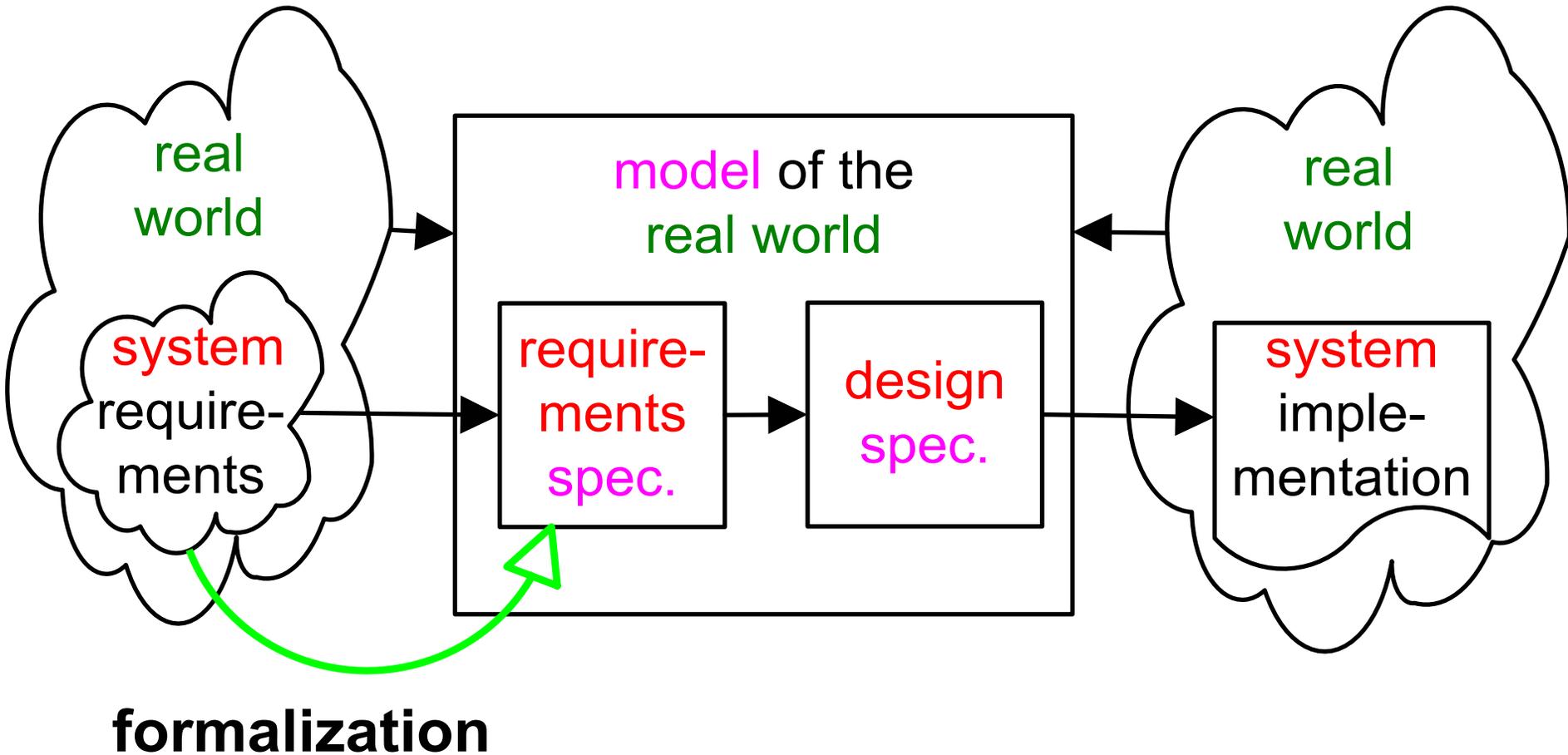
A Model in the Real World's Model



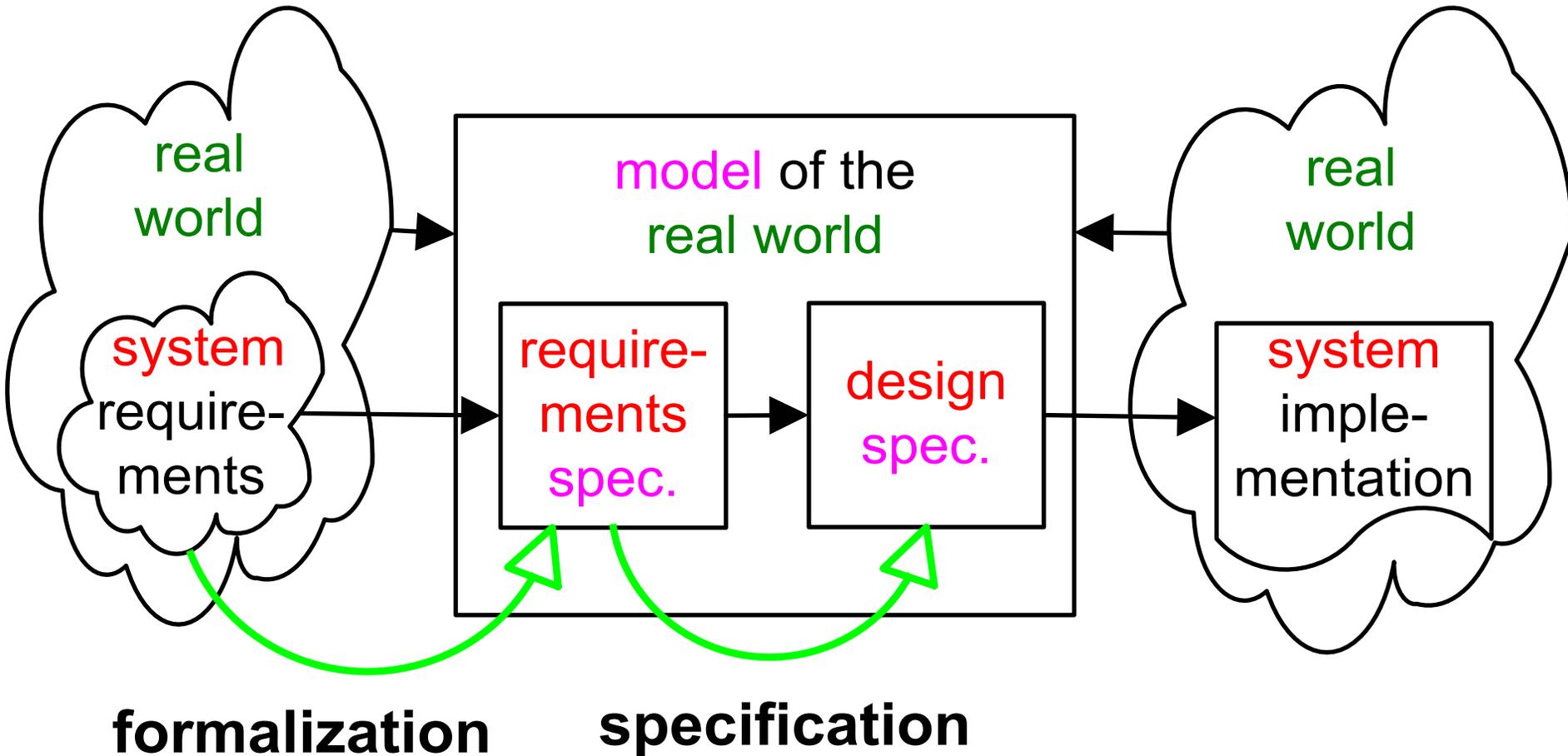
Splitting the System Model



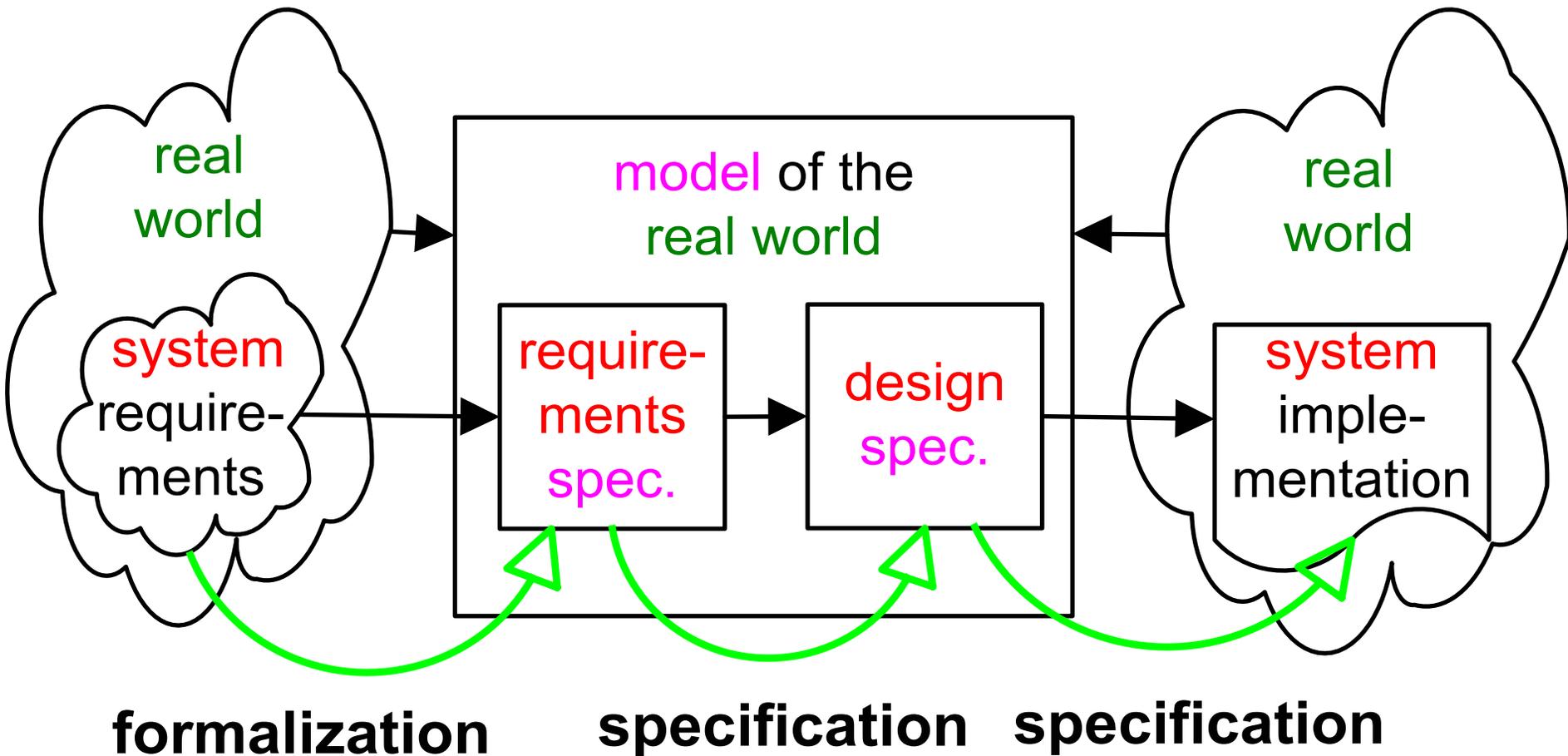
Splitting the System Model



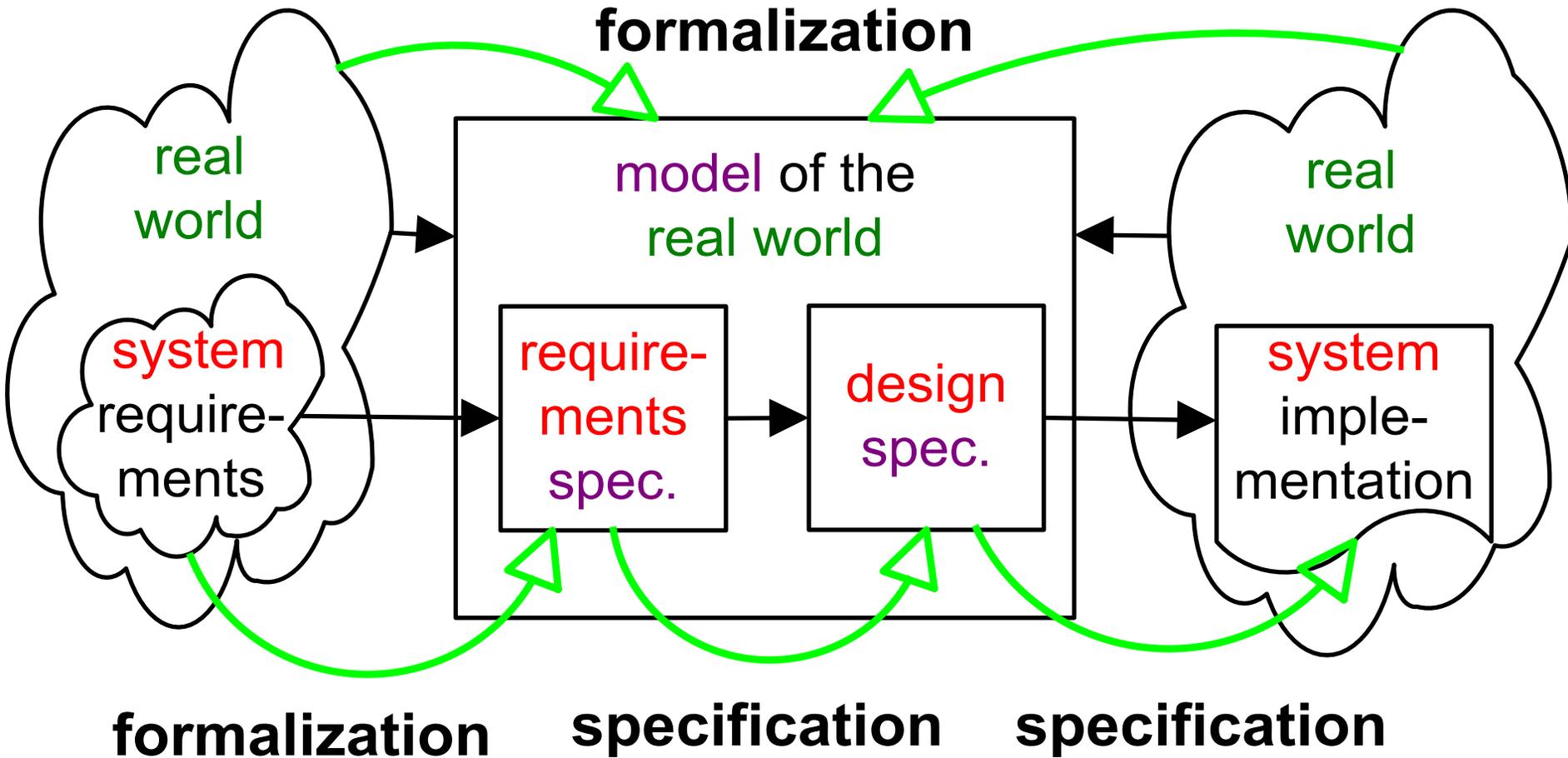
Splitting the System Model



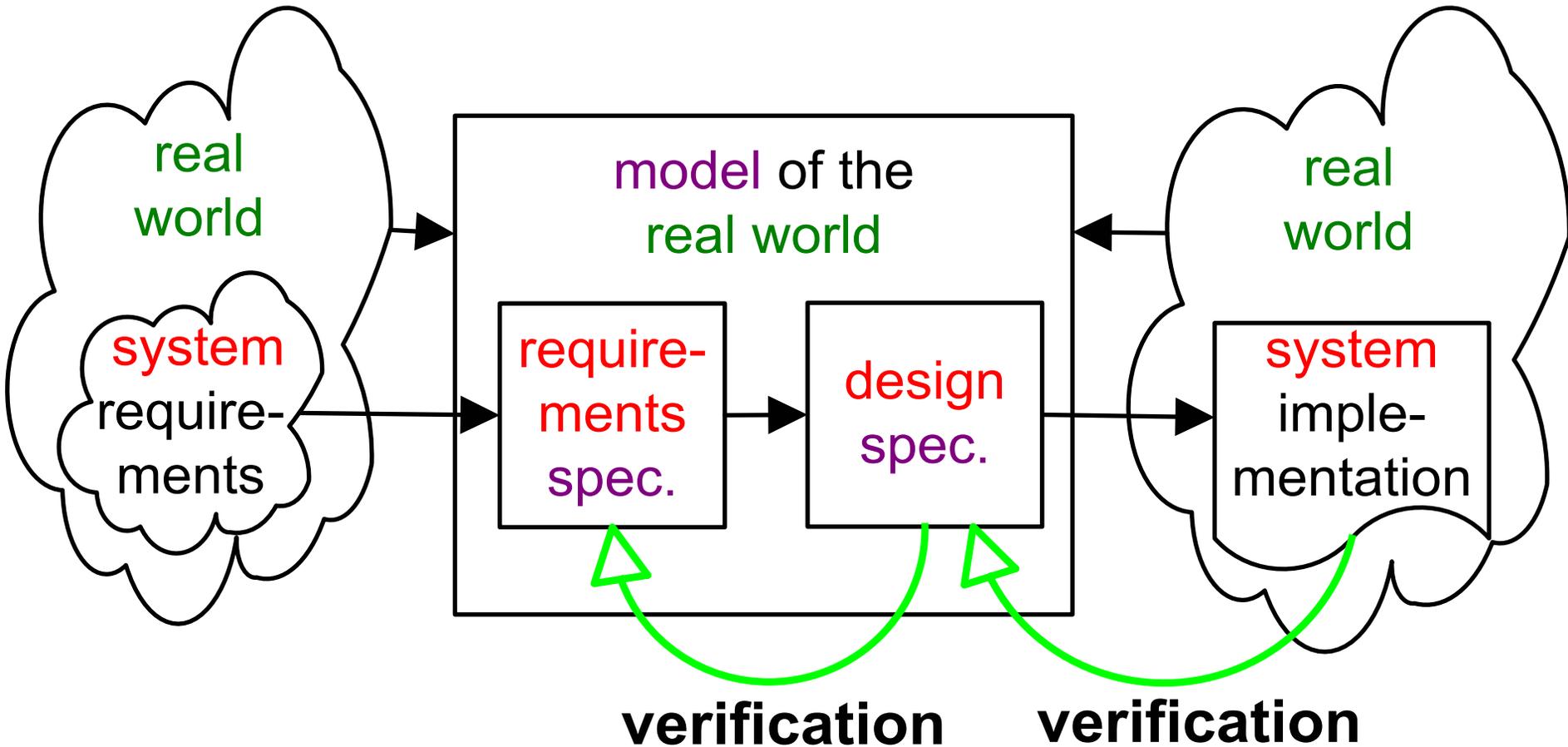
Splitting the System Model



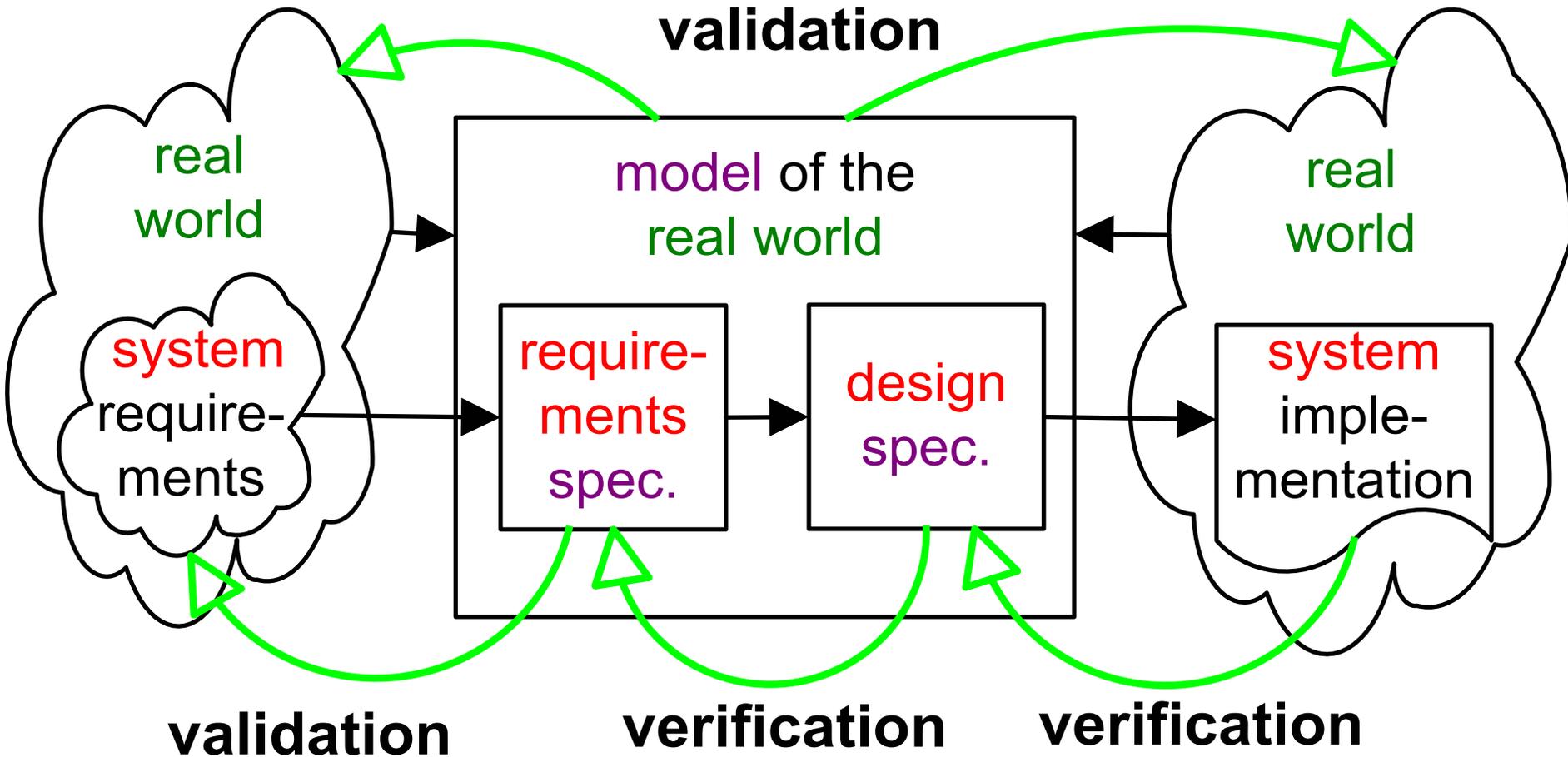
Splitting the System Model



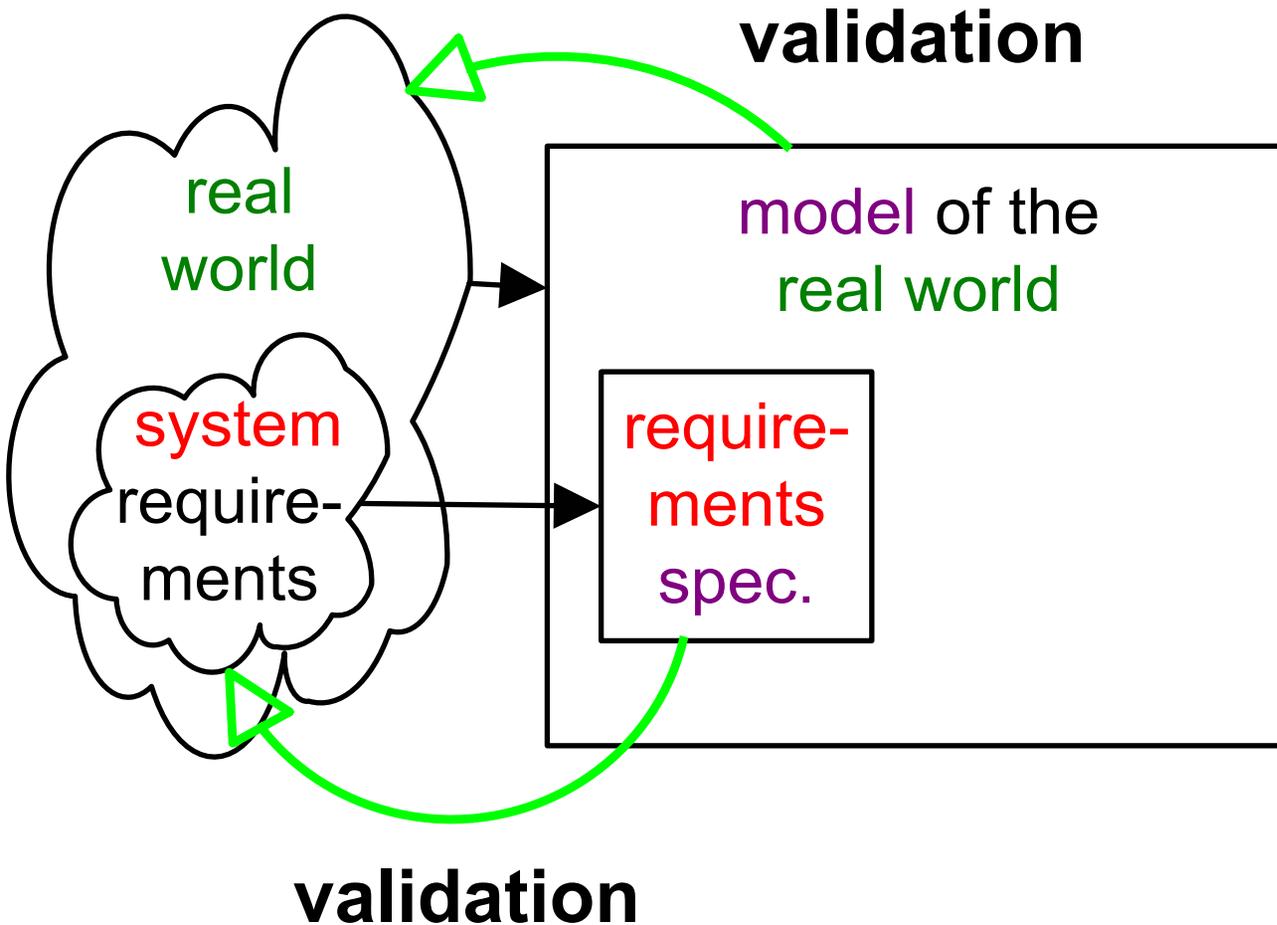
The Reverse of Specification ?



The Reverse of Formalization?



The Reverse of Formalization?

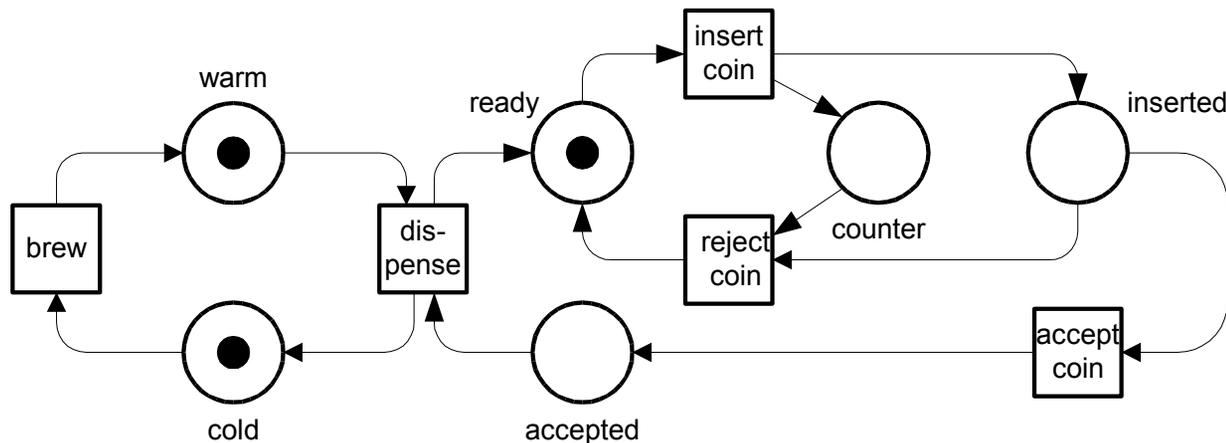


The Modeling Language: Petri Nets



**Graphical representation of
local states (places, circles),
transitions (squares)**

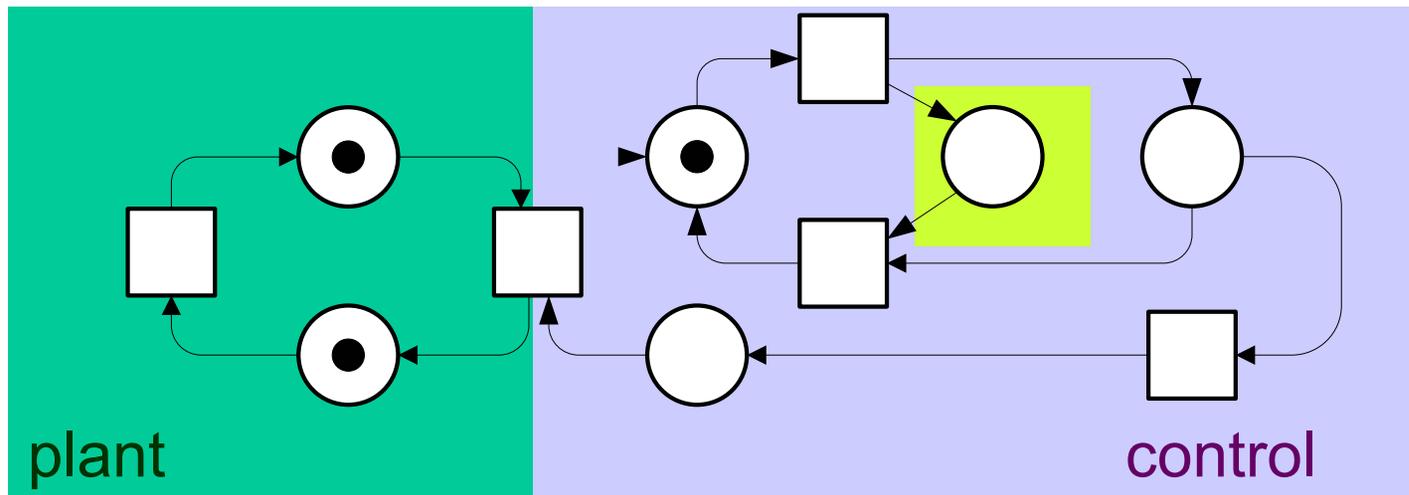
local vicinities (pre- and postconditions, arcs)



The Modeling Language: Petri Nets



System components and communication primitives





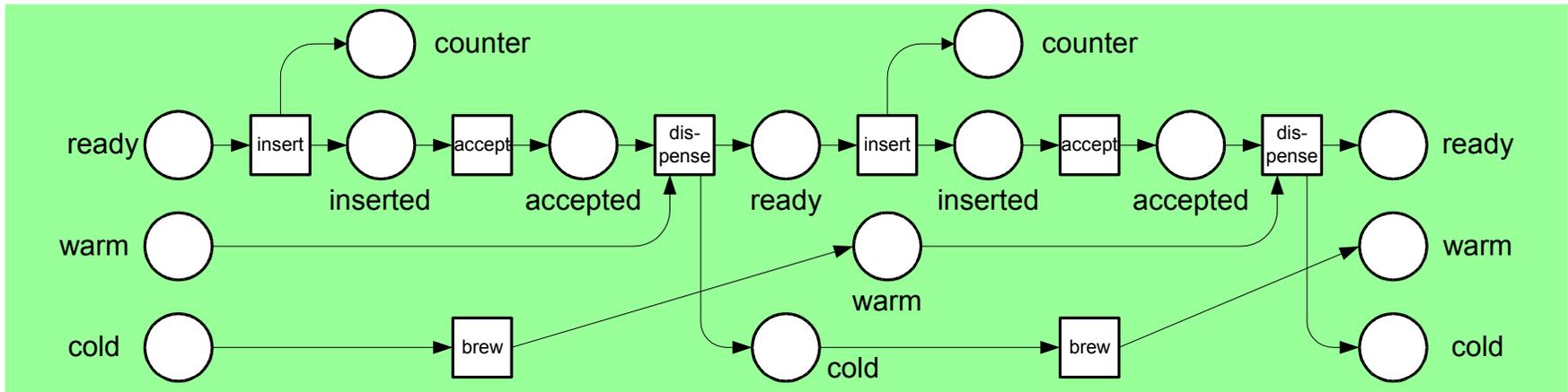
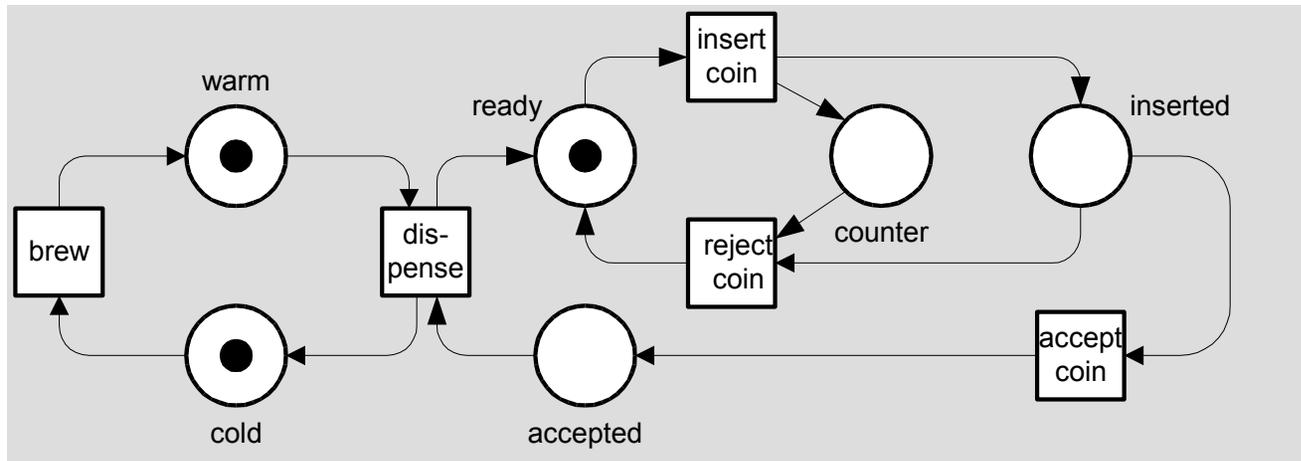
Simulation

means generation of runs.

- **sequential runs** (occurrence sequences),
combined with graphical animation
⇒ the usual approach
- **non-sequential, causal runs** (process nets)
⇒ the **VIP-approach**

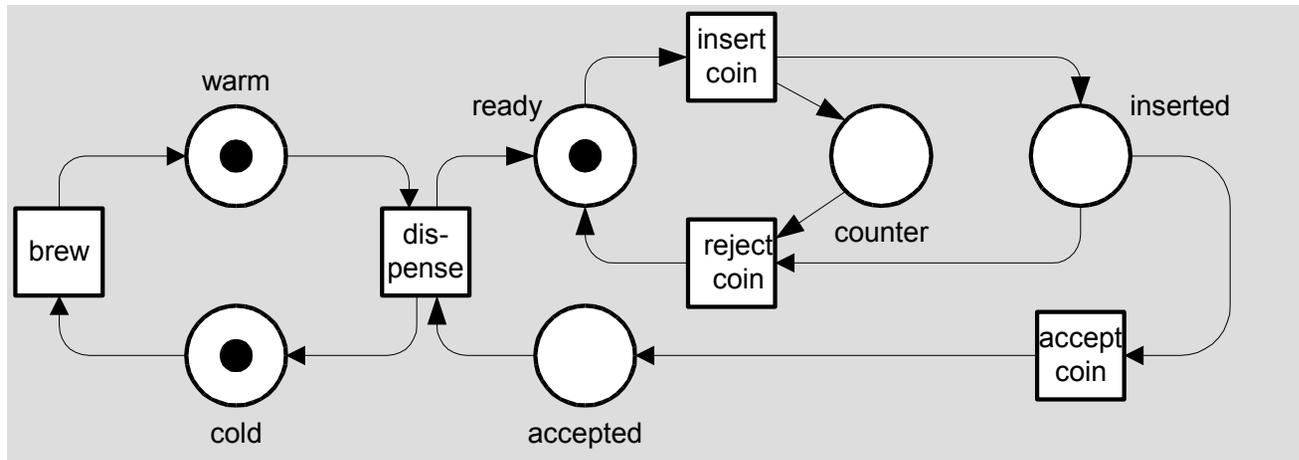


A Coffee Machine with one Process net

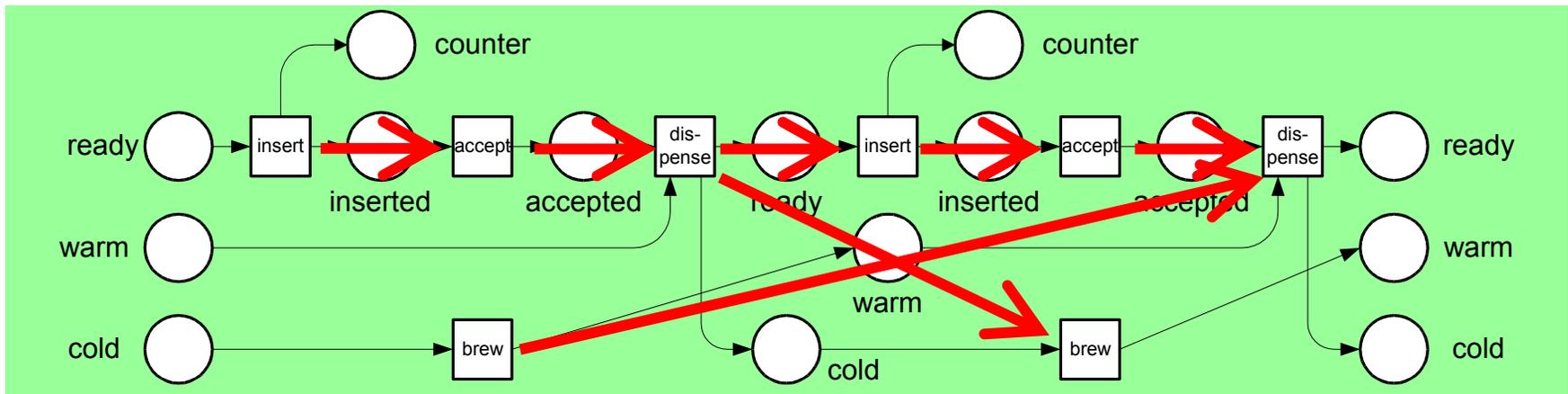




A Coffee Machine with one Process net

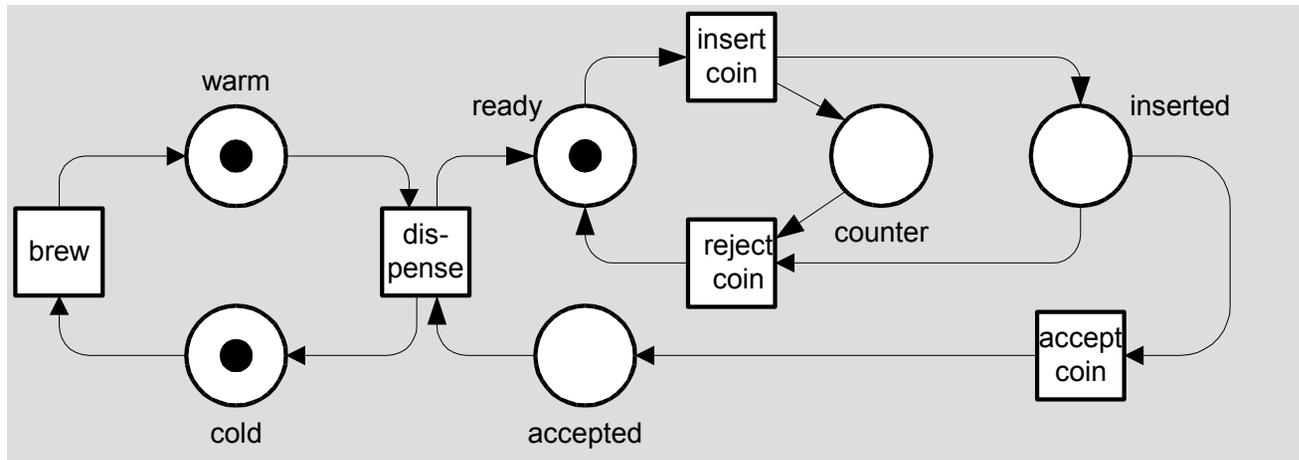


causality between events

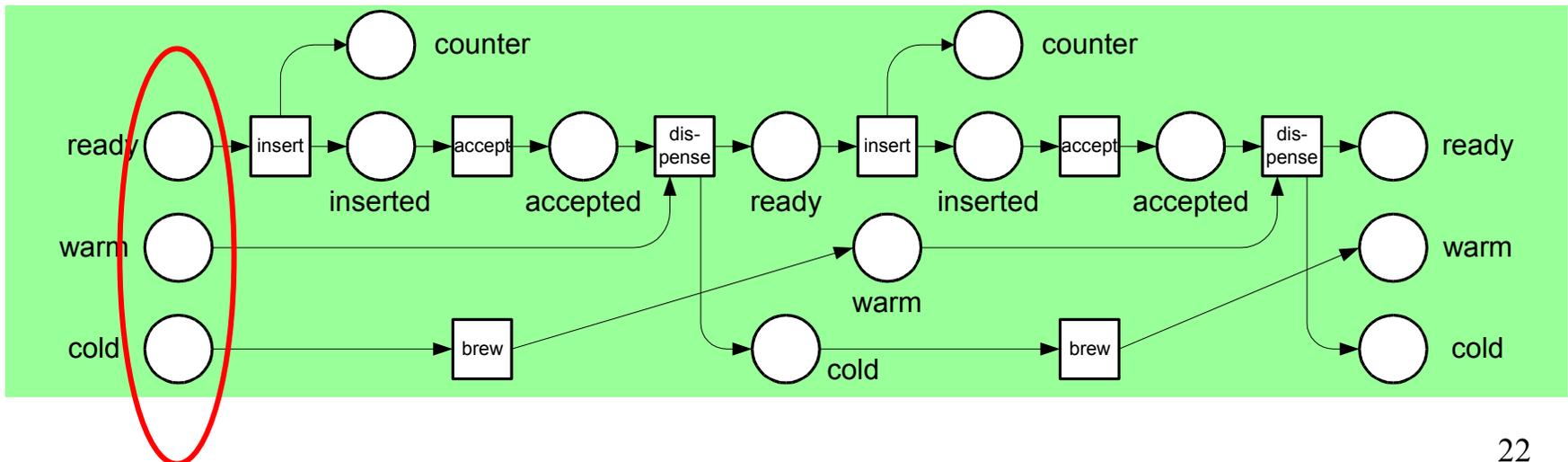




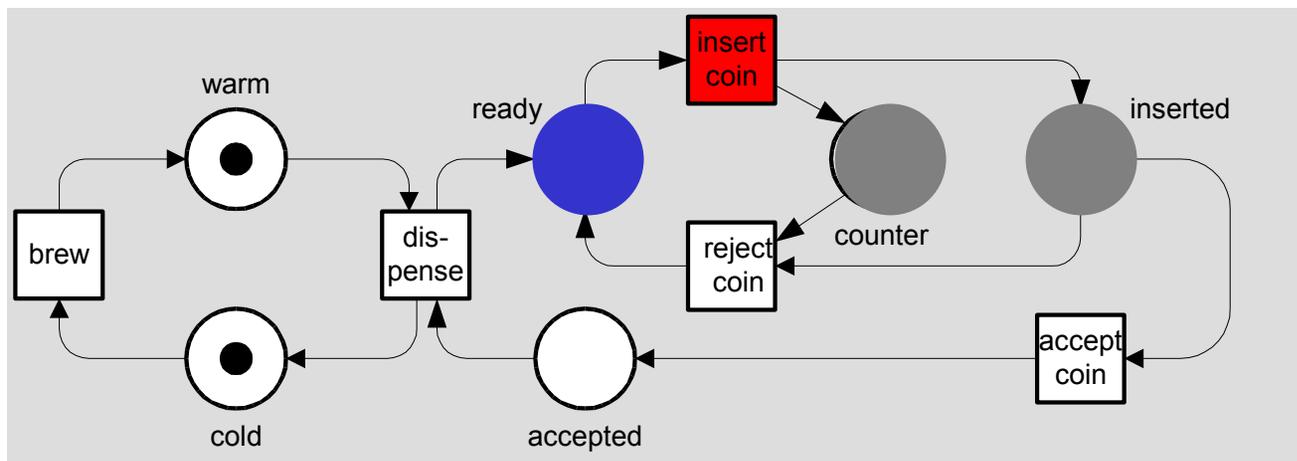
A Coffee Machine with one Process net



initial token distribution



A Coffee Machine with one Process net



respecting pre- and postset of transitions

