On Traceability of Informal Specifications for Model-Based Verification

27th of October 2014

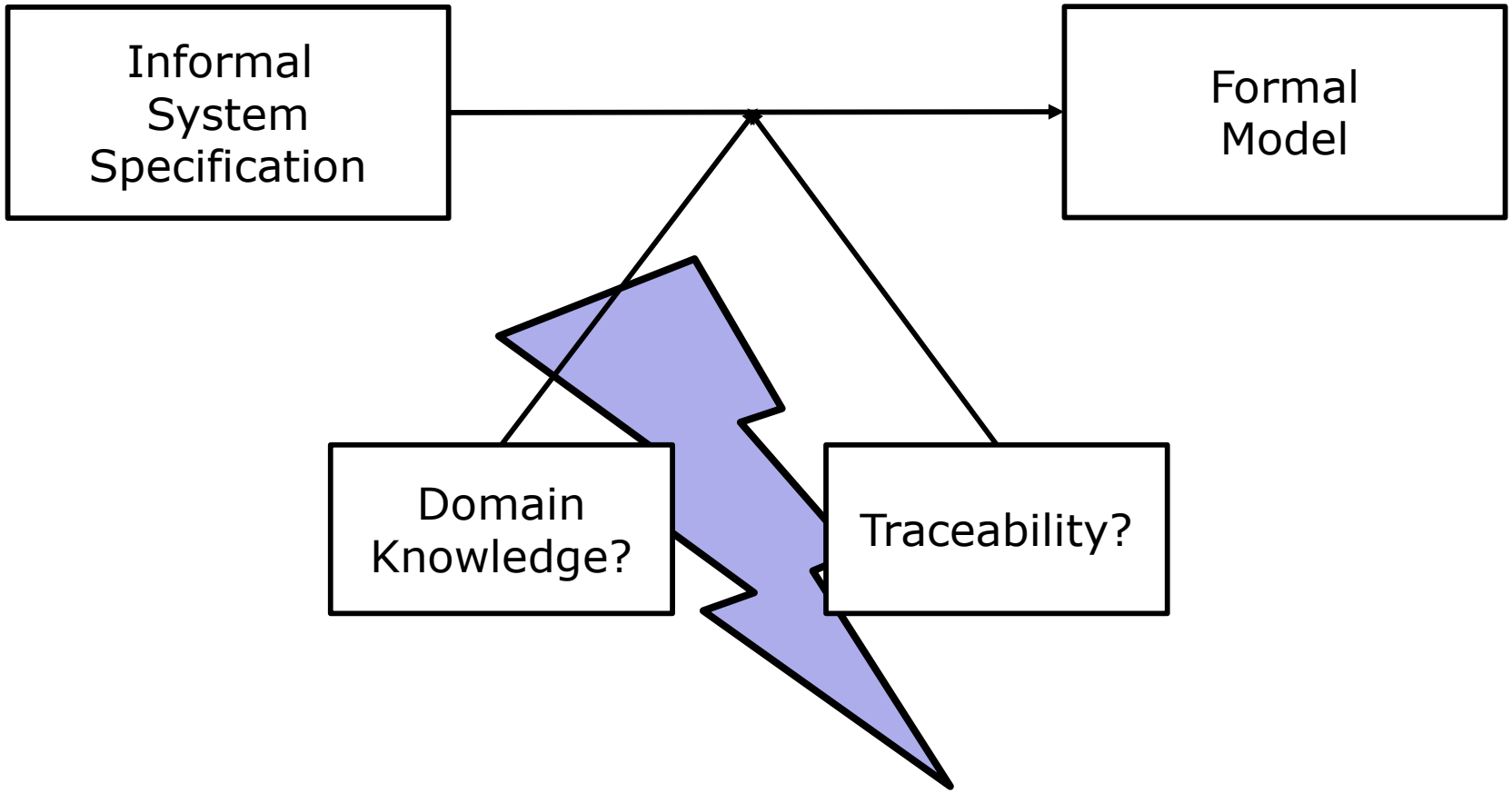
Marco Filax

Formal Verification

- DIN EN 61508
  - Recommends formal verification for different safety integrity levels
- Definition
  - Formal verification requires an abstract model in a language with defined mathematical semantics.
- → How to apply formal methods correctly?

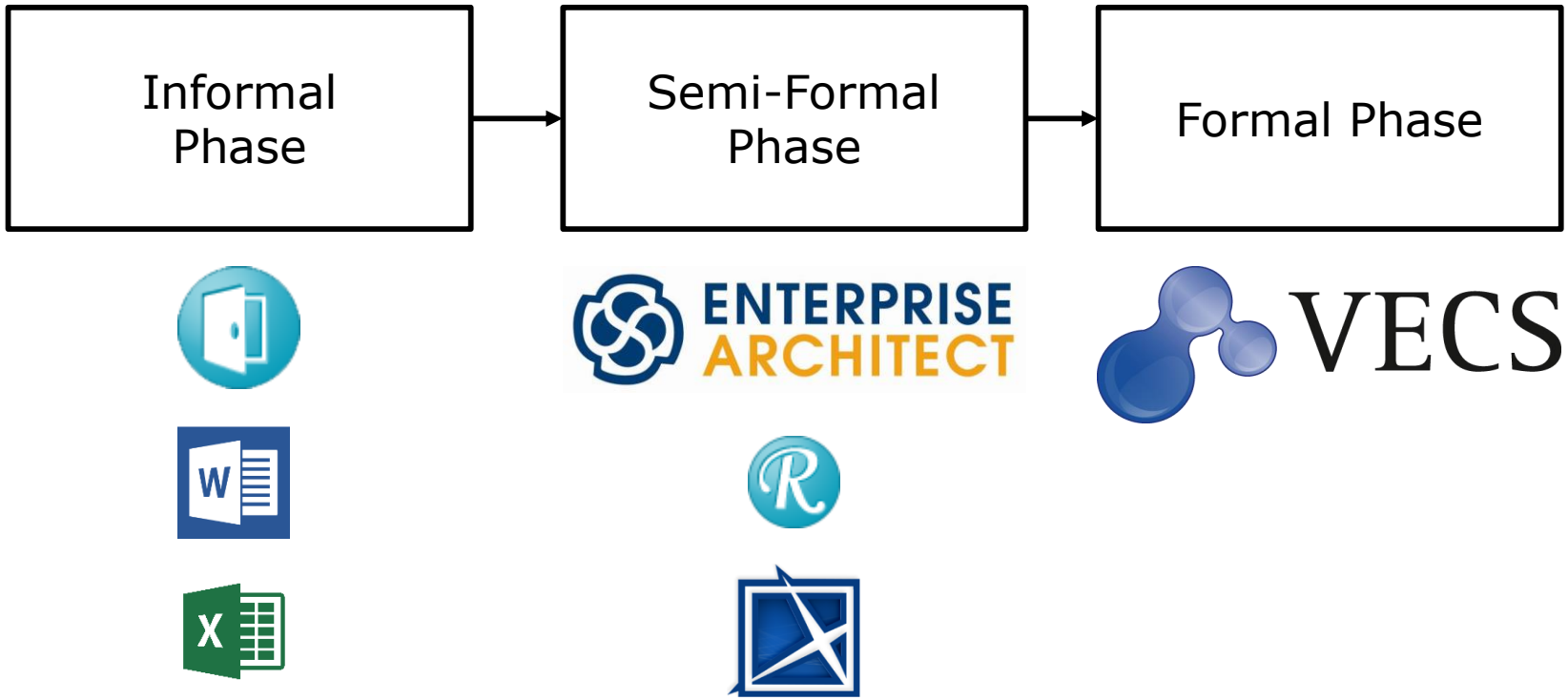
Classic Model-Based Verification

- Direct transformation of informal system specification



Proposed Three Phased Methodology

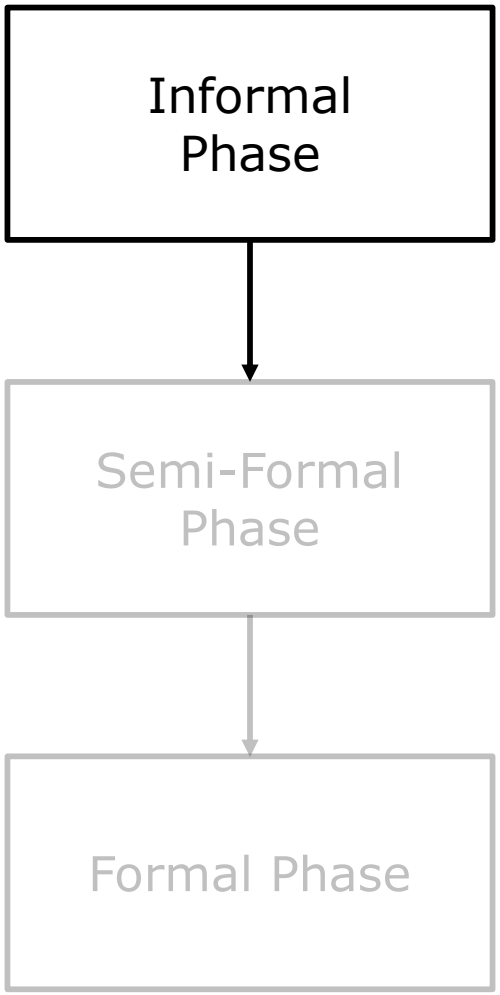
- Distinguish three Sub-Processes



- → Goal: **Preserve traceability through all stages**

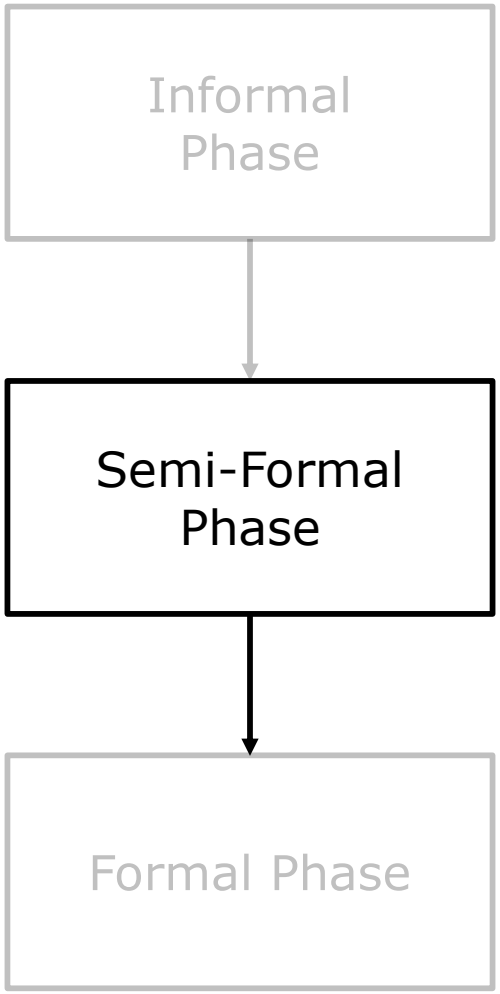
Informal Phase

- Goal
  - Structuring Requirements
- Naive
  - Indexing using IBM Doors
  - Problem: Significance of requirements unclear
- Proposed
  - Structuring requirement using different generic categories
  - Identified 8 different categories
    - Adopted from Cimatti et. al.



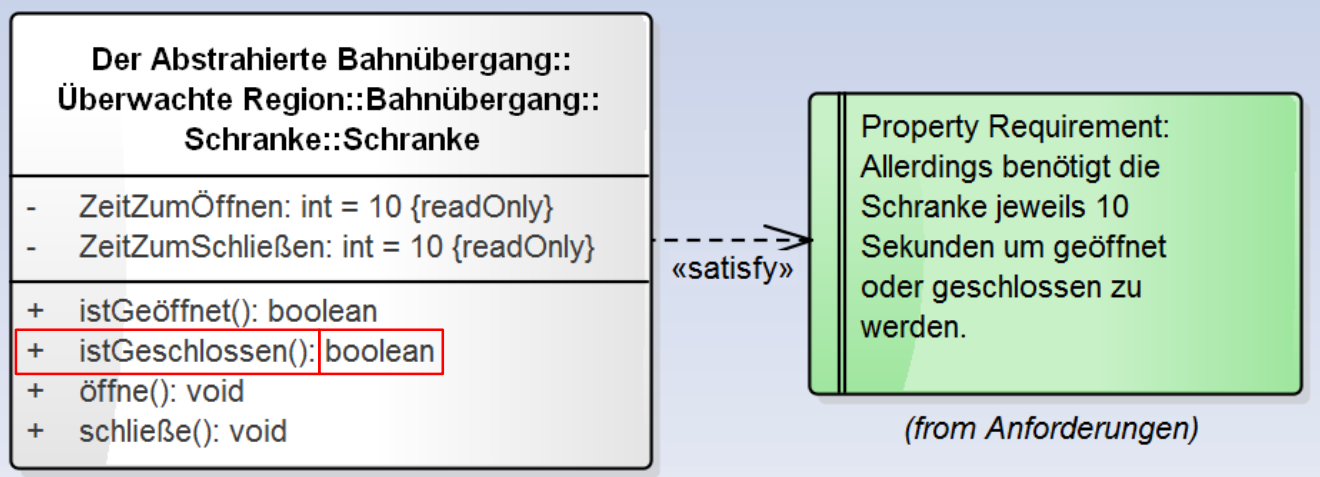
Semi-Formal Phase

Text Fragment	Semi-Formal Artefacts
User Requirement	Use Case Diagram
Glossary Fragment	Component Diagram
Architecture Fragment	Component Diagram
Property Requirement	Class Diagram
Communication Requirement	Sequence Chart
Functional Requirement	- *(formal)*
Safety Requirement	- *(formal)*
Annotation	-

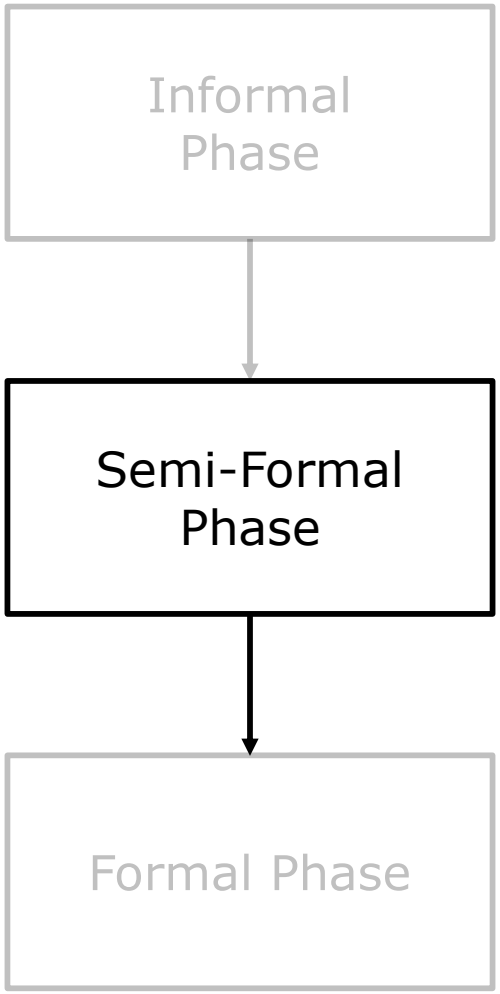


- All Fragments:
  - Requirement Diagrams

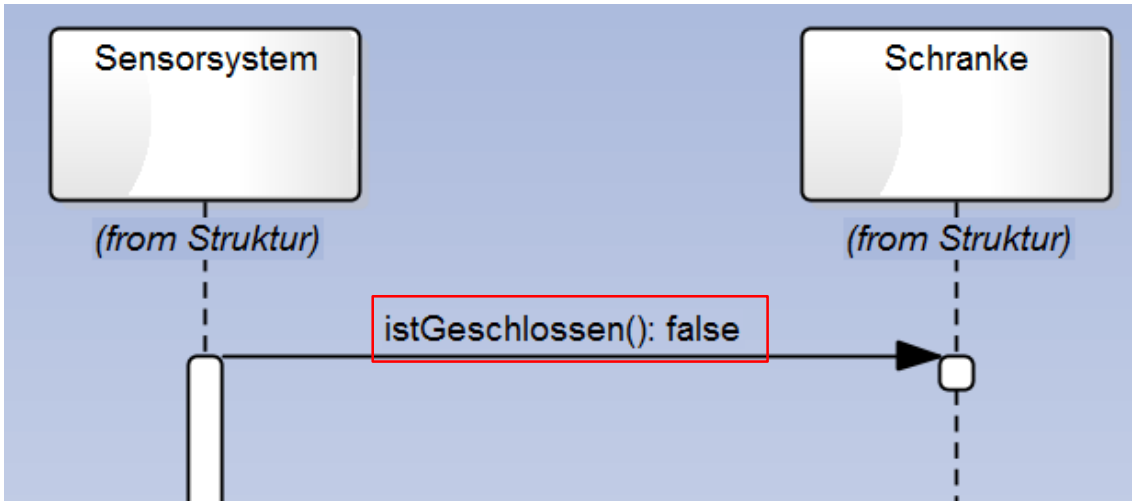
Semi-Formal Phase



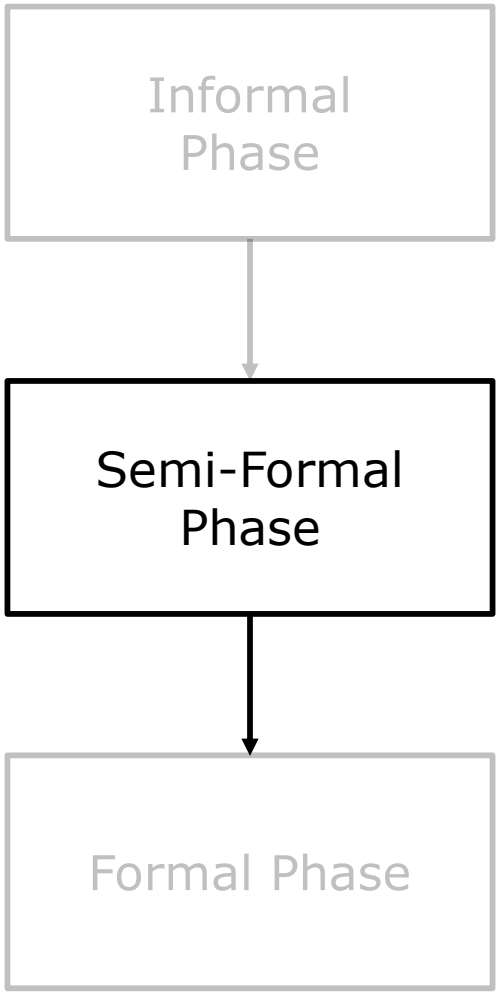

```
/@*
 @ guid: {506B7496-A53E-4e96-AA06-5E9A06966D94};
 @ file: …/Expertenworkshop/DAB.eap;
 @ date: So Okt 25 09:42:15 MESZ 2014;
 @
 @ satisfy DAB46;
*/
template Schranke
    …
    formula bool istGeschlossen;
    formula bool istGeschlossen_return;
endtemplate
```



Semi-Formal Phase

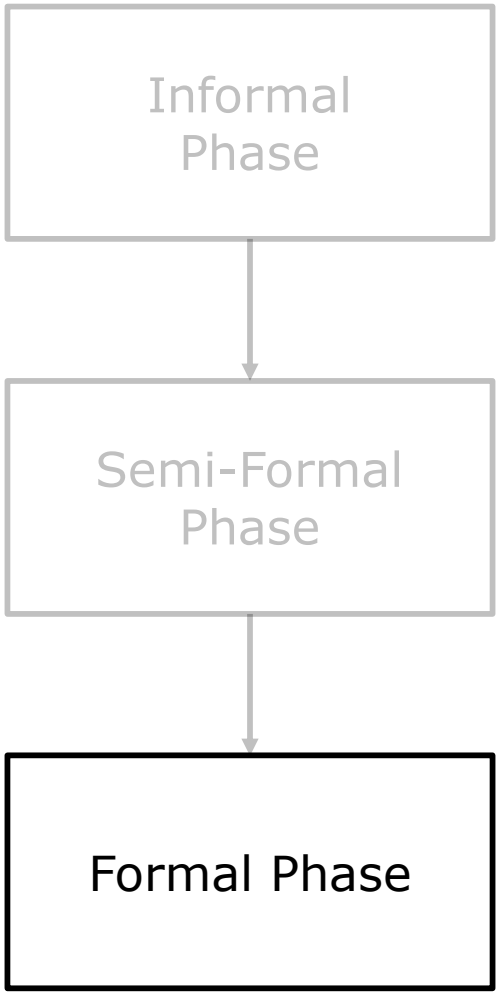



```
NUSMVSPEC EF((EF((EF((EF(((istGeschlossen = true)
& (istGeschlossen_return = true))))&((schliee =
true))))&((schlieeSchranke =
true))))&(((istGeschlossen = true)&
(istGeschlossen_return = false))));
```



Formal Phase

- Completing Partial Formal Model
  - Functional requirements
  - Add requirement links
- Validating the Consistency
  - Using automatic generated formal specifications
- Developing CTL & LTL specifications
  - Safety requirements
  - Add requirement links



Conclusion & Future Work

- Detailed Three Phases Methodology

✓ Reducing required domain knowledge

✓ Preserving traceability
  - Structured approach
  - Requirements & links consistent through all stages

- Precise instructions from first system specification until last verification

Questions?

THANK YOU FOR YOUR ATTENTION!

ANY QUESTIONS?

Literature

- A. Cimatti, M. Roveri, A. Susi, and S. Tonetta. From informal requirements to property-driven formal validation. In Formal Methods for Industrial Critical Systems, Volume 5596 of Lecture Notes in Computer Science, pages 166-181. Springer Berlin / Heidelberg, 2009.

- Deutsche Kommission Elektrotechnik Elektronik Informationstechnik: DIN EN 61508, 2011