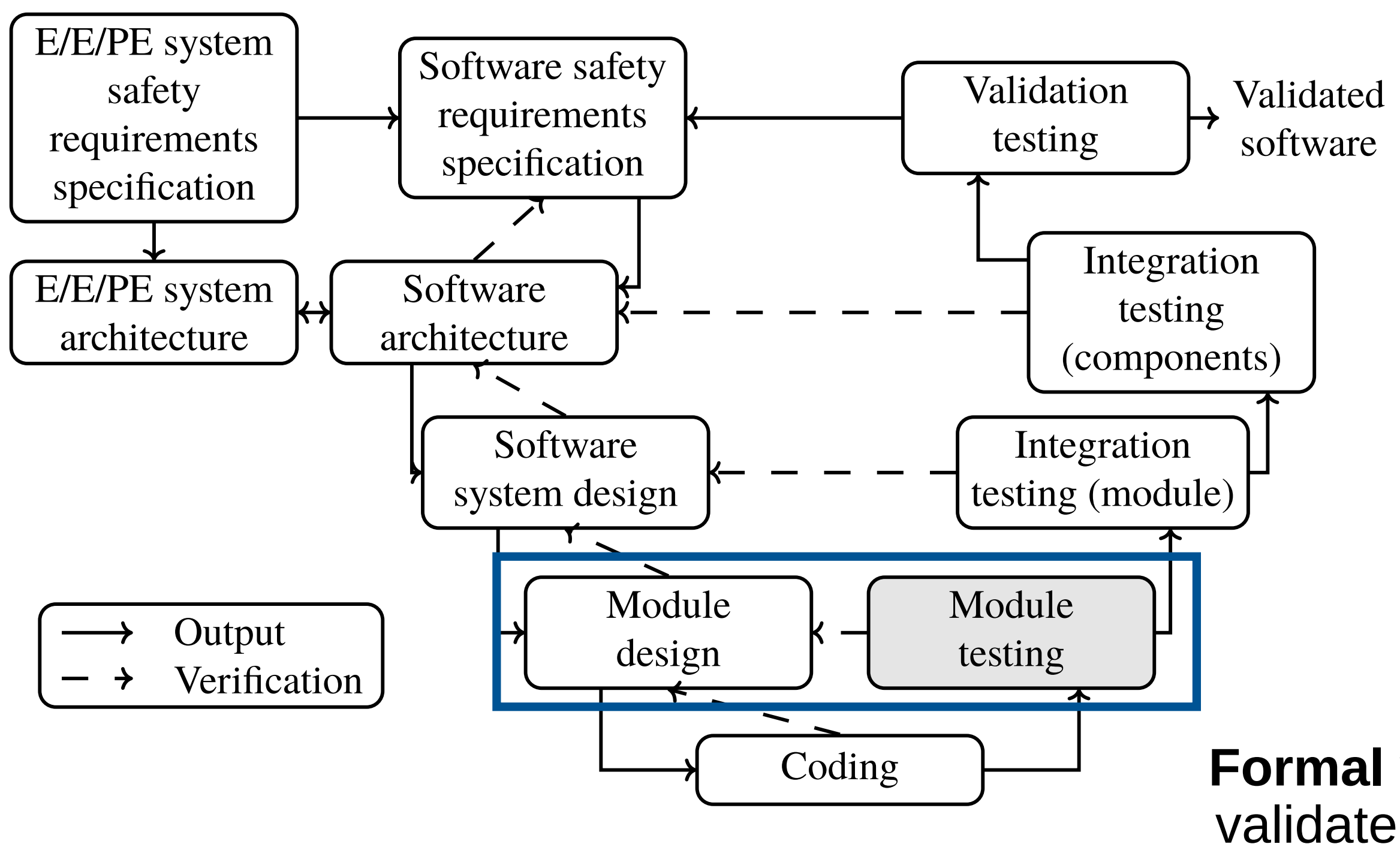
# Working Together for Safer Systems: A Collaboration Model for Verification of PLC Code

**Ignacio D. Lopez-Miguel**, TU Wien, Vienna, Austria
**Borja Fernández Adiego, Enrique Blanco Viñuela**, CERN, Geneva, Switzerland
**Matias Salinas, Christine Betz**, GSI, Darmstadt, Germany
*Ignacio.lopez@tuwien.ac.at, borja.fernandez.adiego@cern.ch, M.Salinas@gsi.de*

*TUPDP001*

## CONTEXT

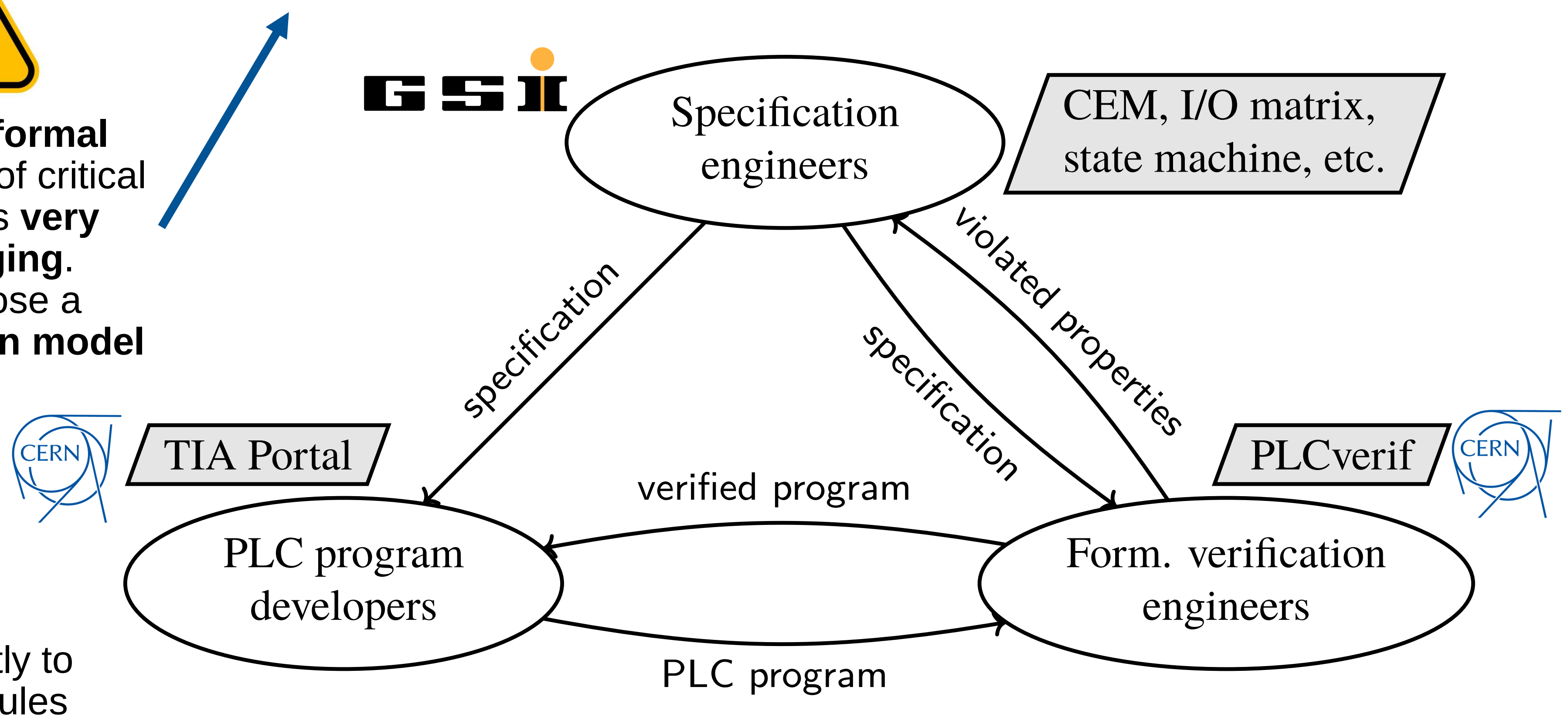
**V-model** recommended by the IEC 61508 standard


E/E/PE system safety requirements specification
Software safety requirements specification
Validation testing
Validated software
E/E/PE system architecture
Software architecture
Integration testing (components)
Software system design
Integration testing (module)
Module design
Module testing
Coding
Output
Verification

**Formal verification** fits perfectly to validate the PLC program modules

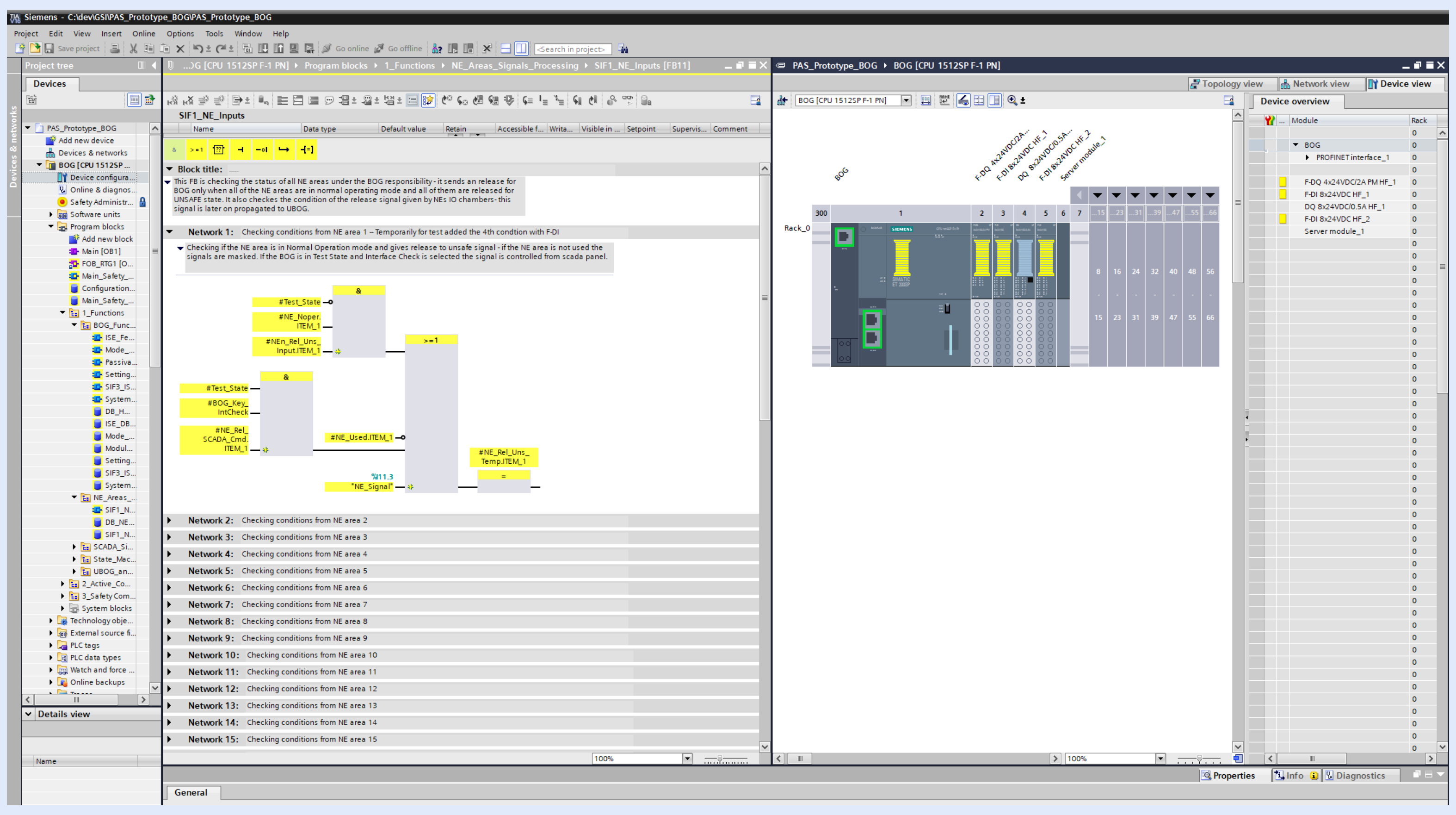
Currently, **formal verification** of critical software is **very challenging**.
We propose a **collaboration model**

## COLLABORATION MODEL

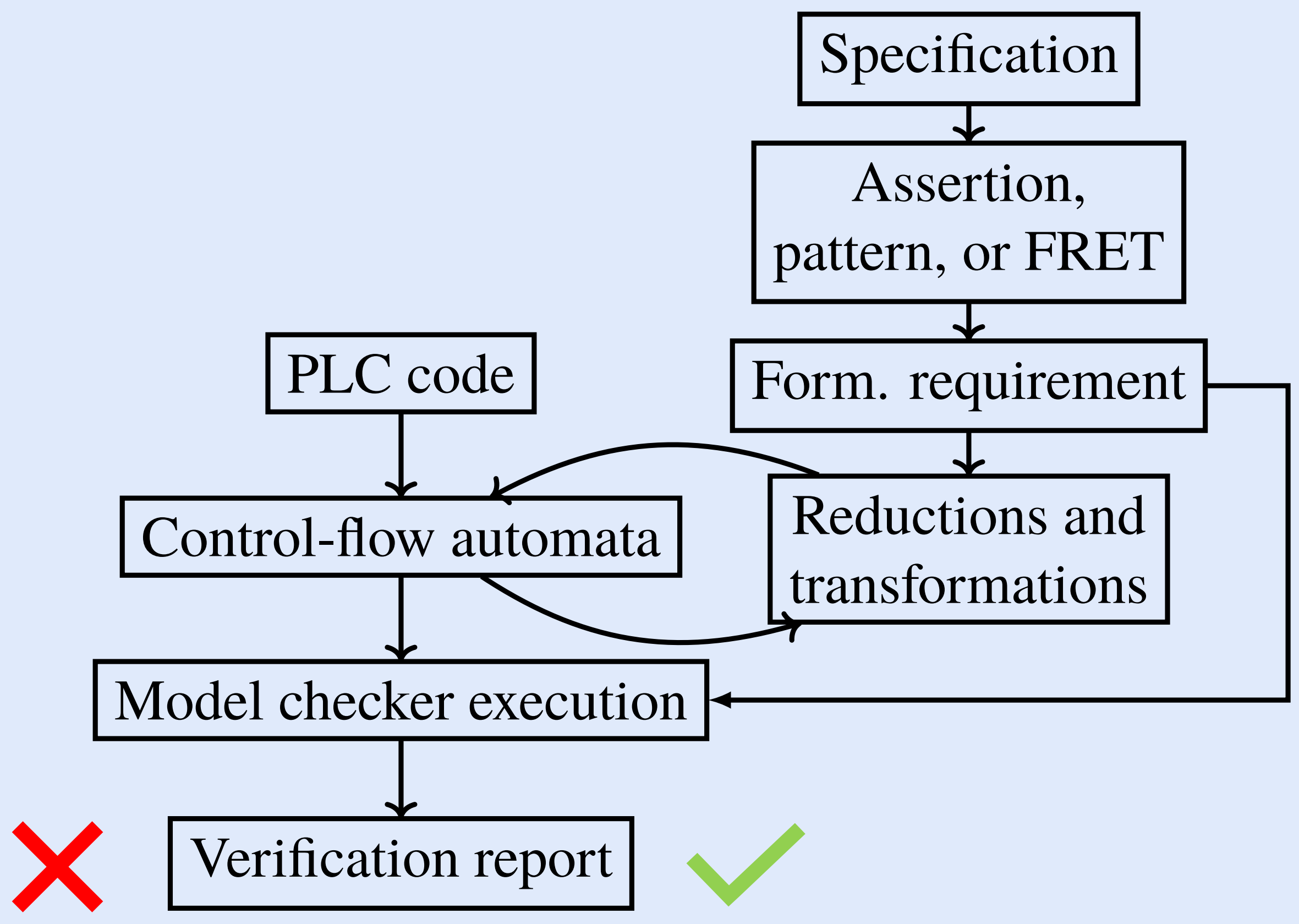


## FORMAL VERIFICATION

### PLC code



### PLCverif

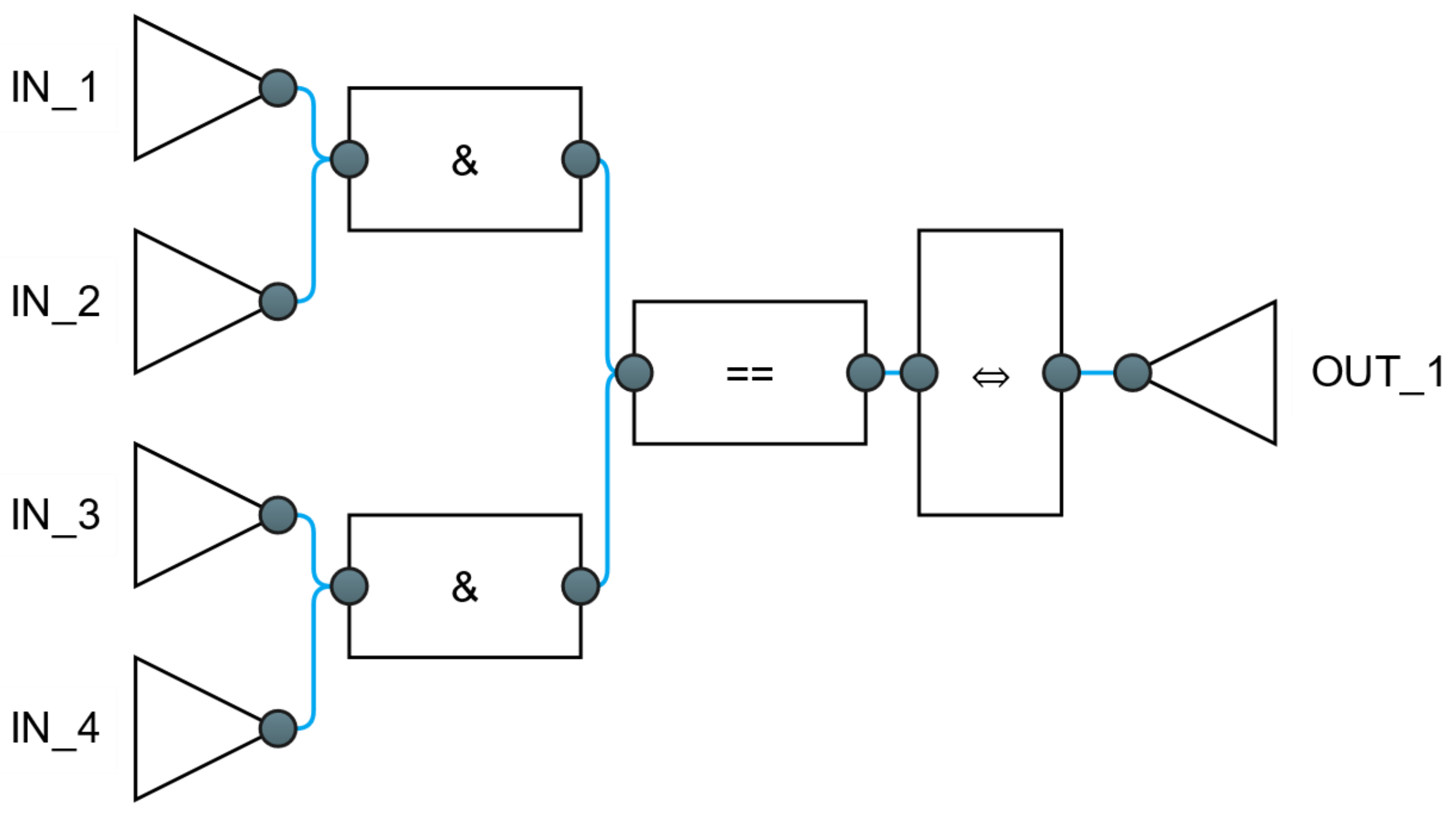


## EXAMPLES OF SPECIFICATION FORMALISMS

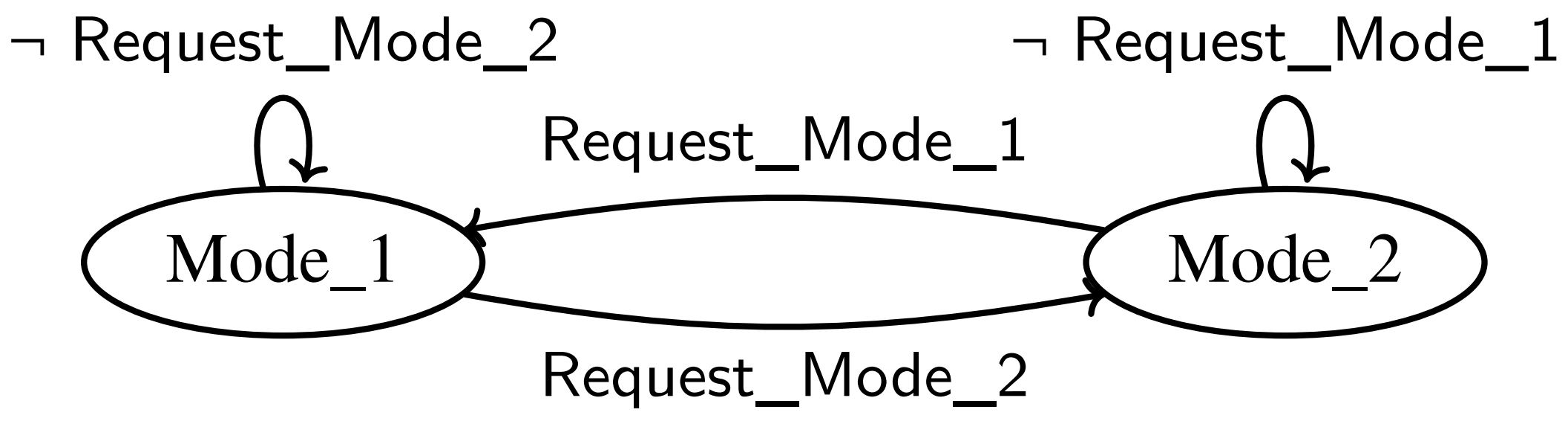
### I/O matrix

| | | Outputs | |
|---|---|---|---|
| | | Out_1 | Out_2 |
| Inputs | In_1 | Reset | Reset |
| | In_2 | Set | Reset |
| | In_3 | Set | Set |

### Logic diagram (grassedit)

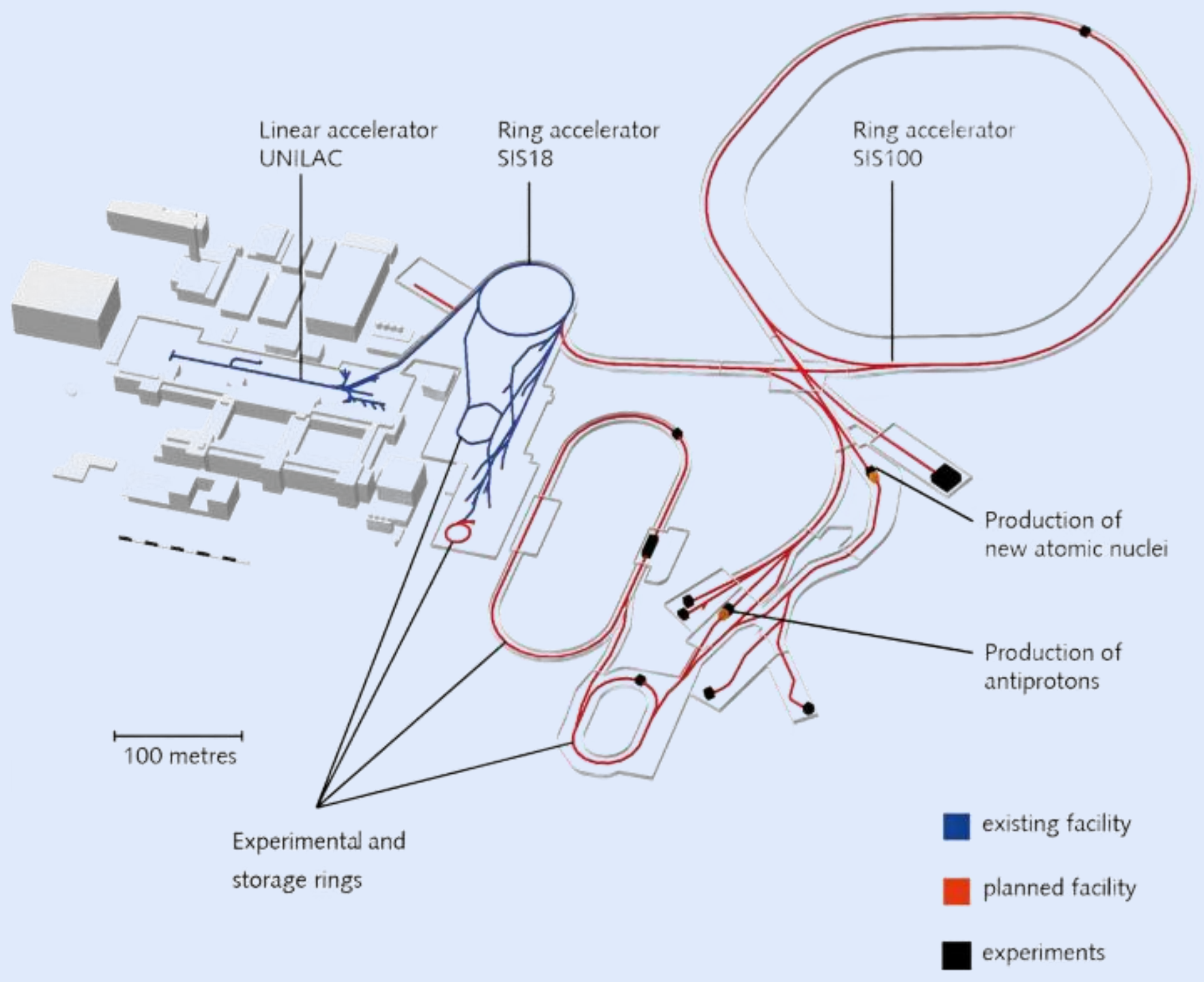


### State machine



Formalisms recommended by the **IEC 61511 standard**

## CASE STUDY: FAIR


Linear accelerator UNILAC
Ring accelerator SIS18
Ring accelerator SIS100
Production of new atomic nuclei
Production of antiprotons
100 metres
Experimental and storage rings
existing facility
planned facility
experiments

### PERSONNEL ACCESS SYSTEM

- **Safety-critical** application
- It prevents personnel from entering areas exposed to particle beams and their **radiation**
- Controls architecture based on **S7-1500F PLCs**
- Developed using **TIA Portal v16** programming environment

### RESULTS

- **Win-win** situation for all counterparts
- **GSI**:
  - Found **discrepancies** between the code and the specification → fixed
  - Improved specification and code
  - Better **understanding** of the code
  - **Knowledge transfer** in formal verification
- **CERN**
  - Improved **PLCverif**