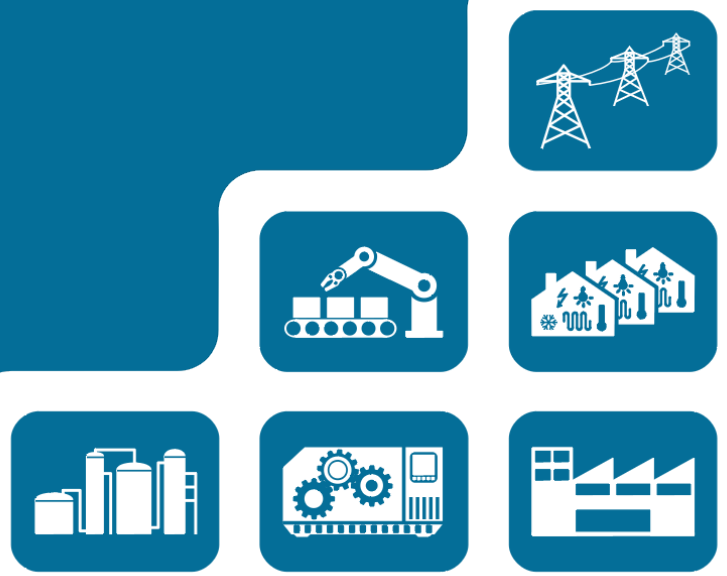
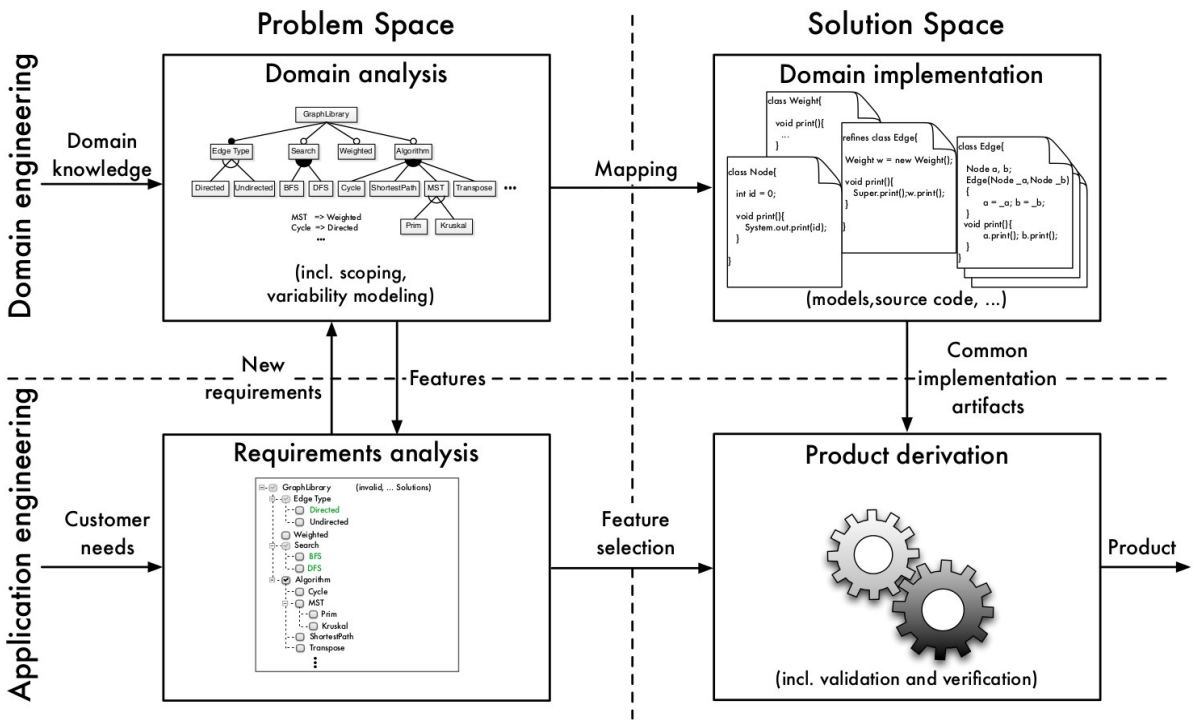
Explaining Why: Explainable SMT-Based Consistency Checking in Variability-Intensive Cyber-Physical Production Systems

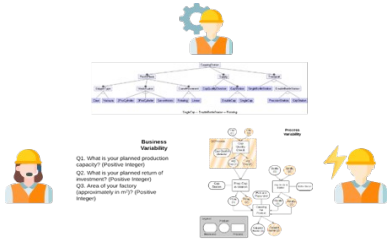
Malte Grave
Christian Doppler Lab VaSiCS
LIT | Cyber-Physical Systems Lab
Johannes Kepler University Linz

PRIMETALS TECHNOLOGIES
Federal Ministry Economy, Energy and Tourism Republic of Austria



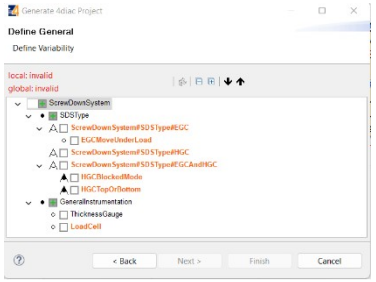
Variability in Cyber-Physical Production Systems

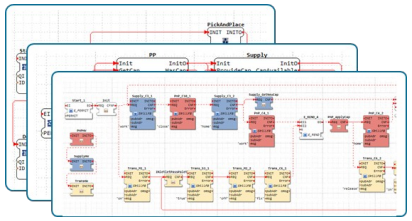




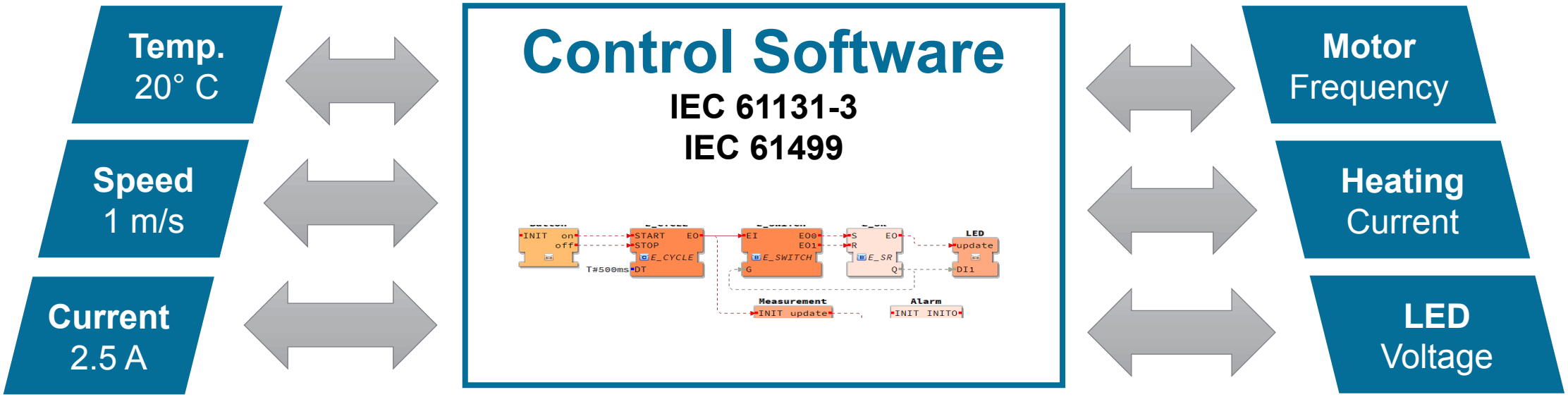
```
delta DApplyCapPresNotReached;
uses Application;

{
    <Modify> Subapplication PnP_ApplyCap {
        <Add> EventOutput Error type=Event;
        <Add> FB PnP_PressureSens_3 type=SkillFB;
        <Add> EventConnection PnP_C5_1.CNF
            PnP_PressureSens_3.REQ;
        <Add> EventConnection PnP_PressureSens_3.CNF
            PnP_PressureSens_2.REQ;
        <Remove> EventConnection PnP_C5_1.CNF
            PnP_PressureSens_2.REQ;
    }
}
```

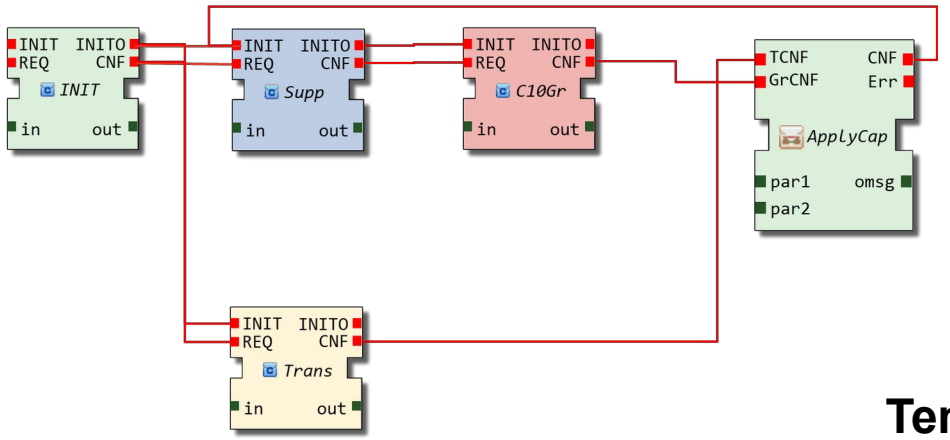




Cyber-Physical Production Systems



Delta Modeling for IEC 61499



Template

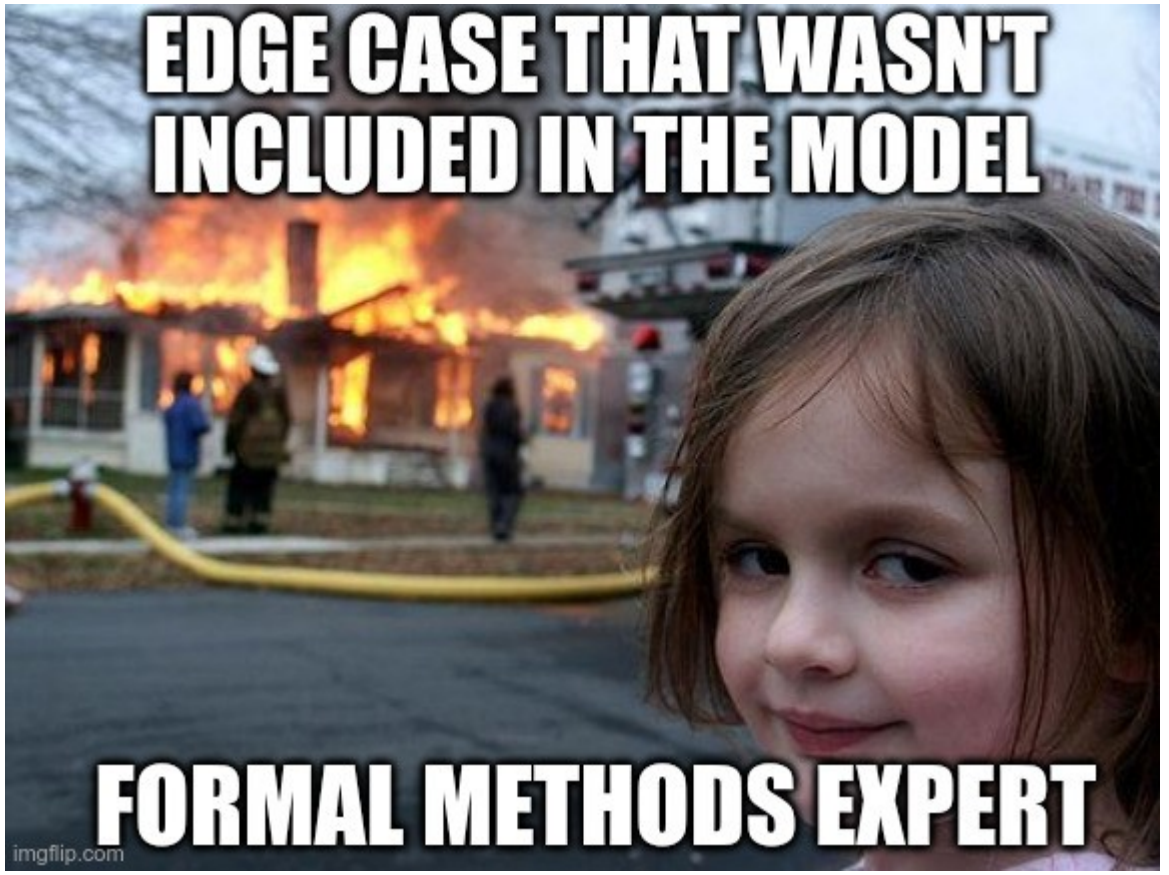
```
delta DModApplyCap;
uses Application.ApplyCap;
{
  <Add> InterfaceElement Output name=Error
  type=Event;
  <Add> EventConnection source=Func2.CNF
                        dest=Error;
}
```

```
delta DRepressCapFunc;
uses Application;
{
  <Create> Subapplication name=RPCap {
    <Add> InterfaceElement Input name=ErrCNF
                                 type=Event;
  }
  <Add> EventConnection source=ApplyCap.Err
                        dest=RPCap.ErrCNF;
}
```

```
delta DRPCap;
uses Application;
{
  <Add> FB name=Func3 type=SkillFB;
  <Remove> FB name=Func4 type=SkillFB;
  <Remove> EventConnection source=Func4.INTTO
                           dest=REST;
}
```

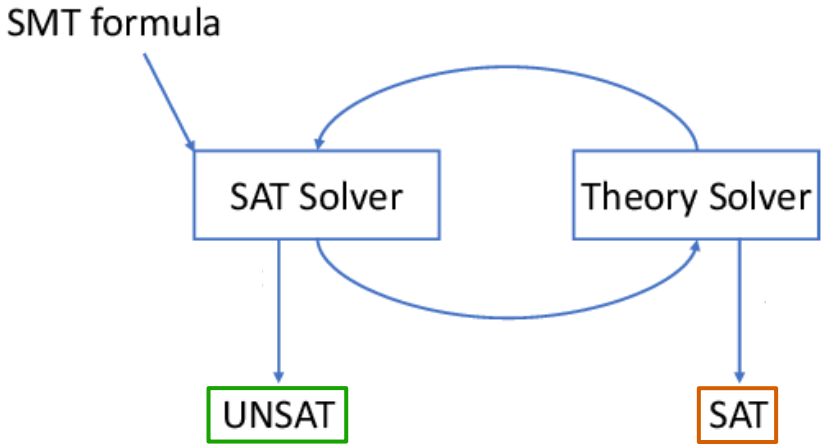
Consistency in Software

- Behaviour changes
- Correctness (structural, functional)
- Formal (proving, SAT, SMT)
- Static code analysis
- Predictability



Consistency Management with SMT Solving

- Deltas may lead to invalid state
- E.g. unknown connection, unknown type, …
- Valid state is key
- Consistency rules
- Global knowledge



Jianhui et al.: Leveraging Control Flow Knowledge in SMT Solving of Program Verification. Software Engineering and Methodology 2021

How to get an SMT Result?

- Suppose **facts** $\mathcal{F}$ where

$$\mathcal{F} = \mathcal{F}_{\exists} \cup \mathcal{F}_{\sim} \cup \mathcal{F}_{\tau}$$

- Which is defined by

$$\mathcal{F}_{\exists} = \{\textsc{Exists}(b) \mid b \in Name\}$$
$$\mathcal{F}_{\sim} = \{\textsc{Connected}(s,t) \mid s,t \in Port\}$$
$$\mathcal{F}_{\tau} = \{\textsc{Type}(b,\tau) \mid b \in Name, \tau \in TypeName\}$$

- Suppose a *fact store defined by* $\mathcal{S} \subseteq \mathcal{F}$
  - S_{bg} a store (**derived facts**)
  - S_q a store for (**queries**)

- Defining the ***background theory***
  - $\Phi_{bg} = \bigwedge_{F \in \mathcal{S}_{bg}} [\![F]\!]$

Grave etl al.: Is it Satisfiable? SMT-Based Consistency Checking in Variability-Intensive Cyber-Physical Production Systems. Variability 2026, (Revision)

How to get an SMT Result?

- A query with a fact $q \in S_q$ is ***consistent*** with S_{bg} if and only if:

$$\Phi_{bg} \models [\![q]\!]$$

  which is checked by asking the SMT solver whether:

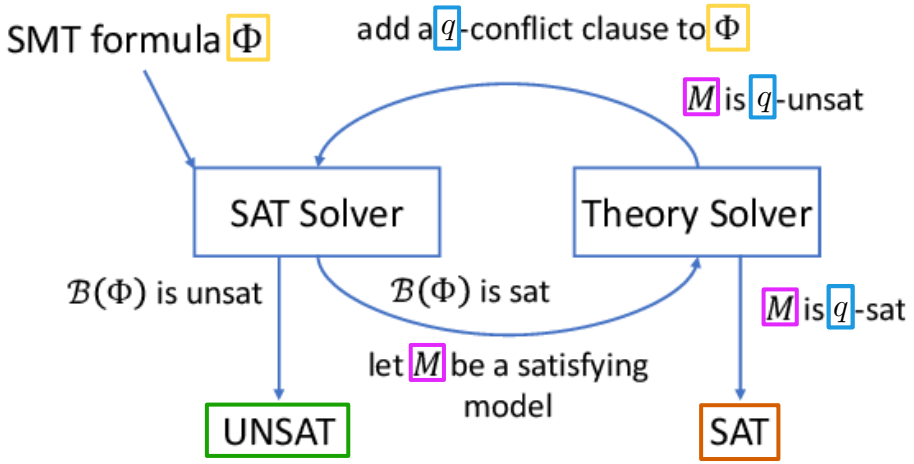
$$\Phi_{bg} \wedge \neg [\![q]\!] \quad \text{is } \mathbf{UNSAT}$$

- If the formula is **SAT**, a counter−example model M exists and q is ***inconsistent***

Grave etl al.: Is it Satisfiable? SMT-Based Consistency Checking in Variability-Intensive Cyber-Physical Production Systems. Variability 2026, (Revision)

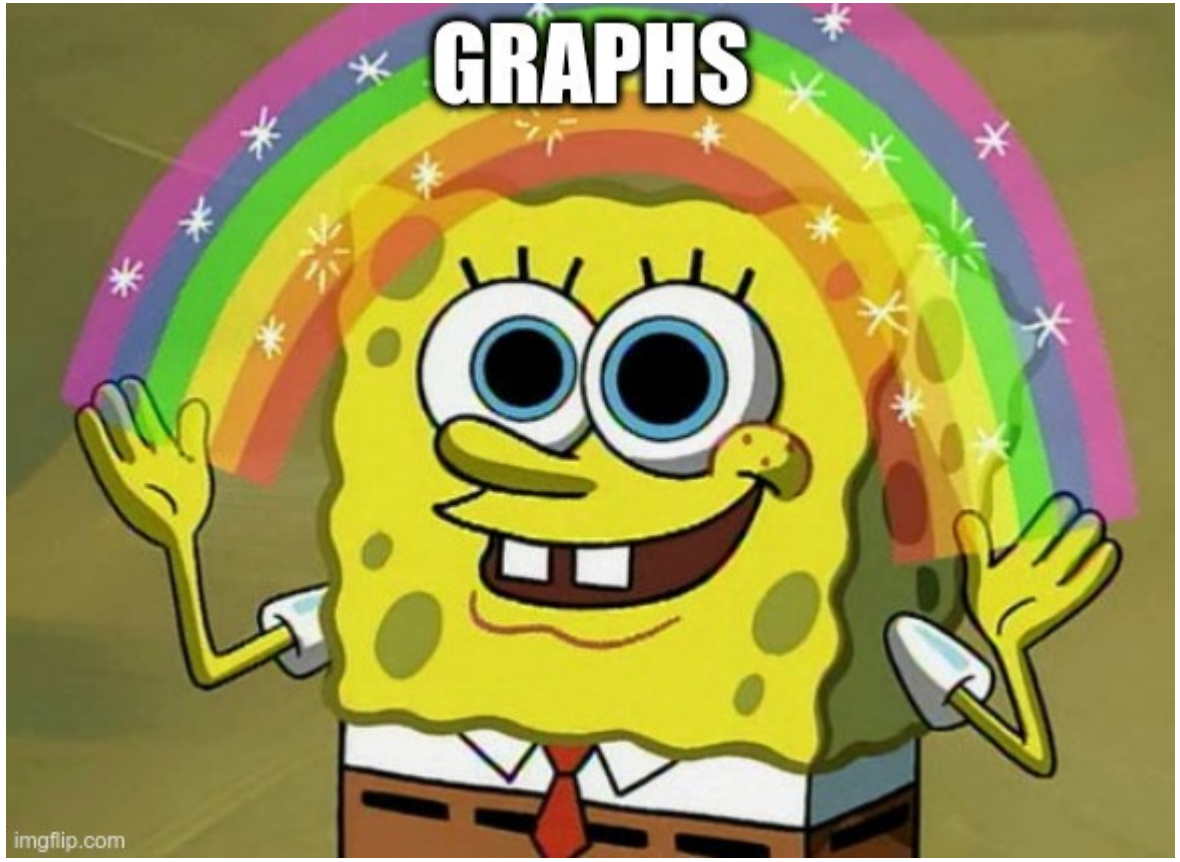
How to Explain the SMT Result?

- Result is either **UNSAT** or **SAT**
- How to check **all facts** and **derive explanations**?



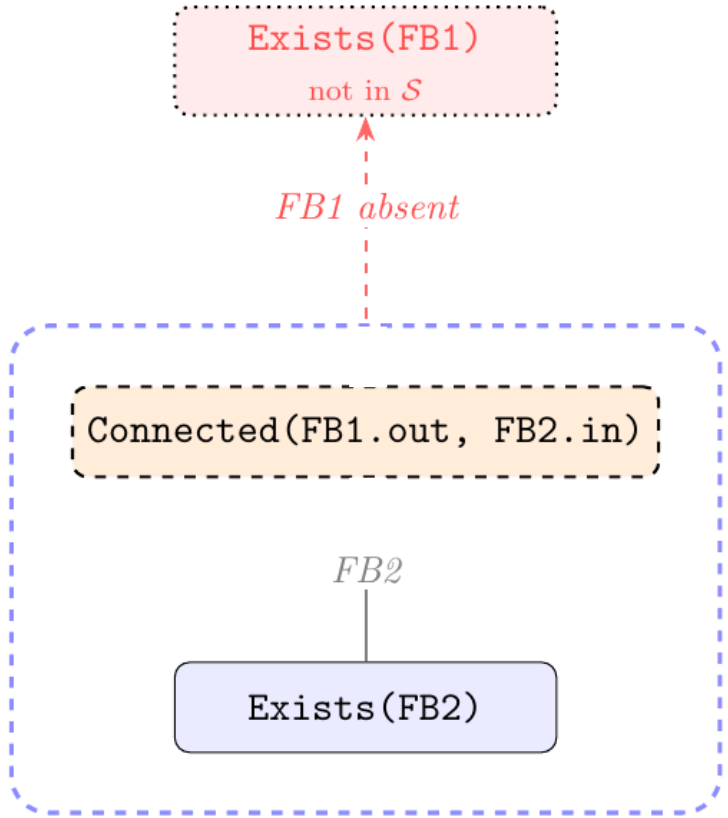
Jianhui et al.: Leveraging Control Flow Knowledge in SMT Solving of Program Verification. Software Engineering and Methodology 2021

How to Explain the SMT Result?



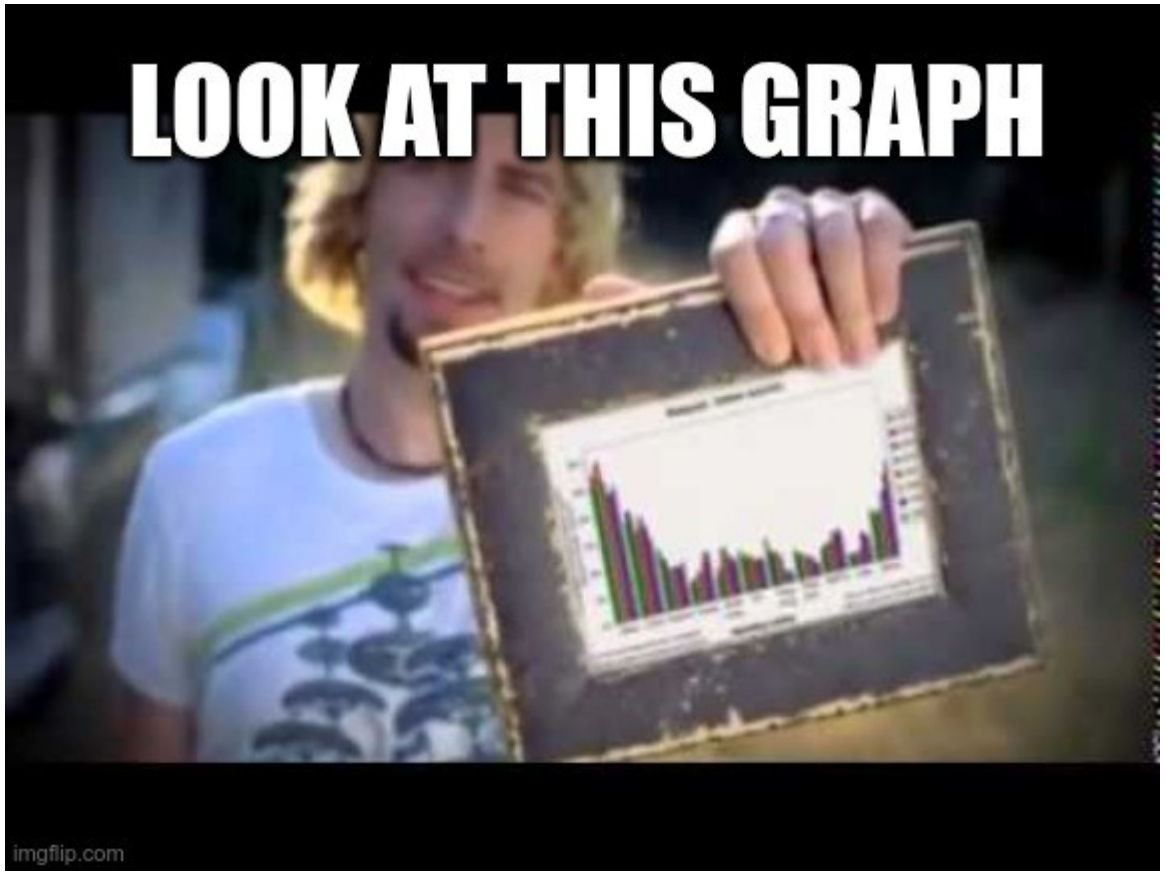
Conflict Graph Resolution (CGR)

- Build one **conflict graph** per **query** (q)
- Deduct with the help of background storage (S_{bg})
- Deduction result is *Exists(FB1)*



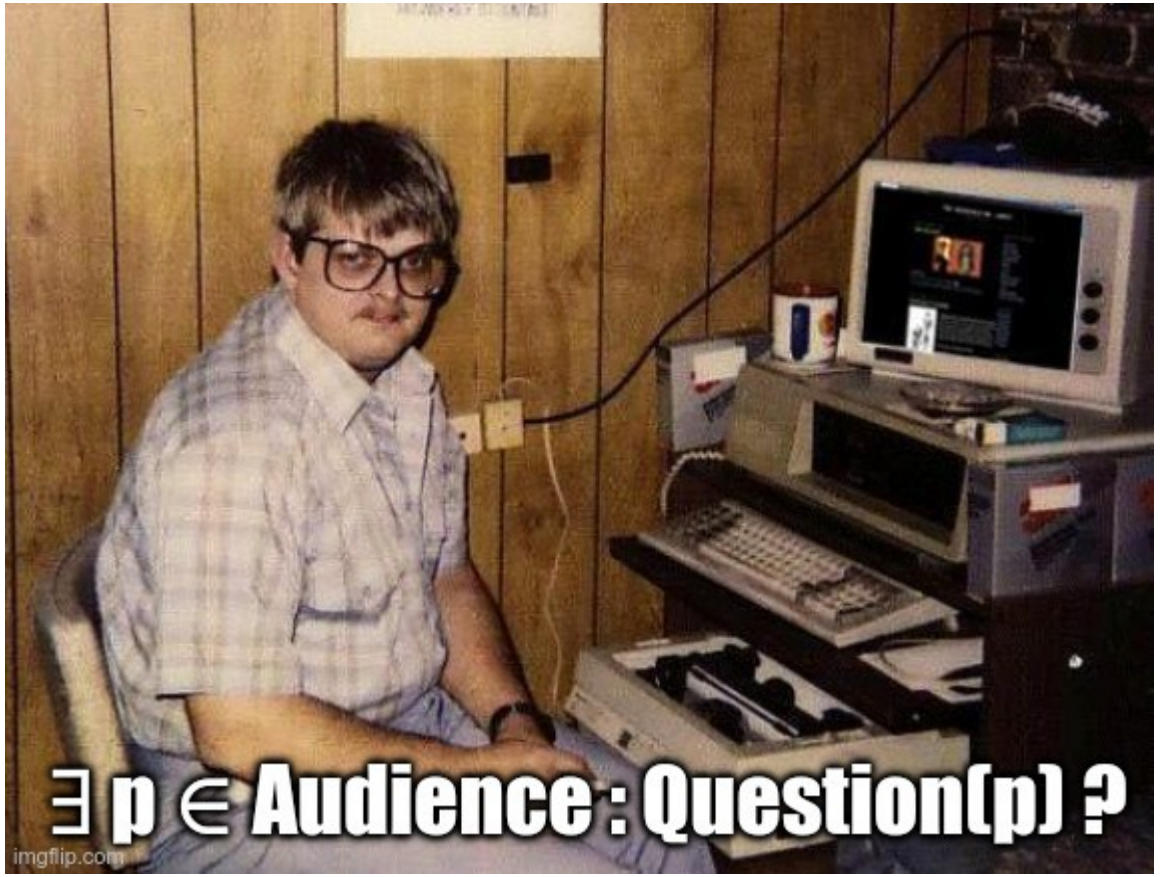
Future Work

- Create a formal specification of the **CGR**
- Implement the **CGR** specification
- Adopt the **CGR** in a tool
- Evaluate the **CGR** based on examples



Feedback and Comments

- Share your **opinion**
- Do you **know** such an approach?



Tak!

Malte Grave
Christian Doppler Lab VaSiCS
LIT | Cyber-Physical Systems Lab
Johannes Kepler University Linz

PRIMETALS TECHNOLOGIES
ober österreich
Federal Ministry Economy, Energy and Tourism Republic of Austria