Model-based Testing Strategies for Configurable Software with Unbounded Parametric Real-Time Constraints

ES4CPS (Dagstuhl, January 7, 2019)

TECHNISCHE UNIVERSITÄT DARMSTADT

Lars Luthmann
Timo Gerecht
Andreas Stephan
Johannes Bürdek
Malte Lochau

IMoTEP 2

DFG

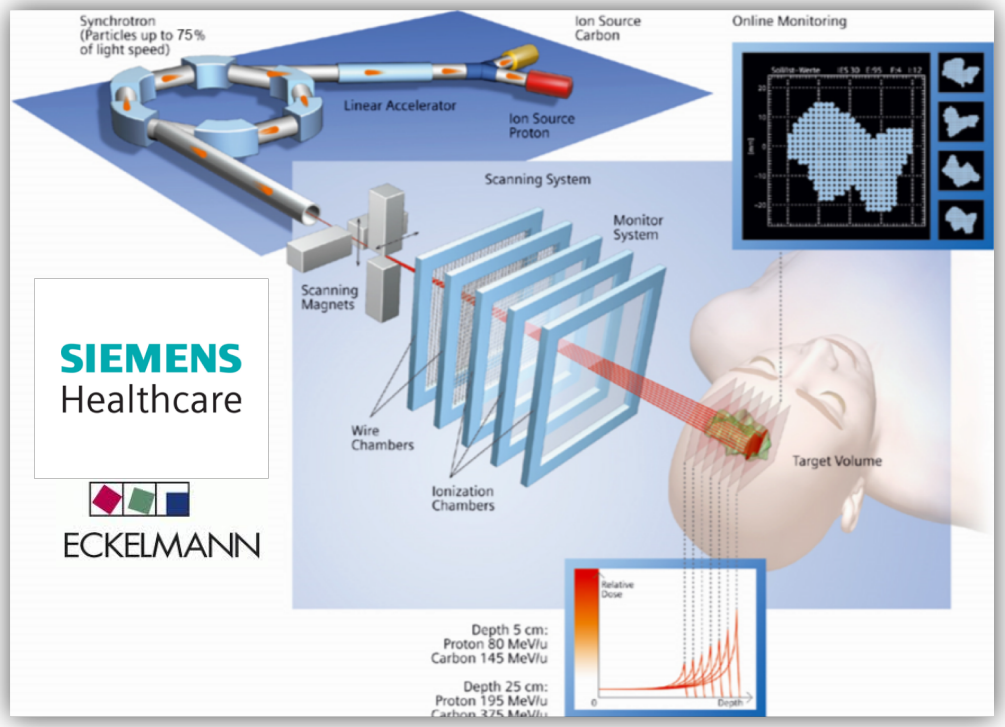
Integrated Model-based Testing of Continuously Evolving Software Product Lines

ES Real-Time Systems Lab
Prof. Dr. rer. nat. Andy Schürr
Dept. of Electrical Engineering and Information Technology
Dept. of Computer Science (adjunct Professor)

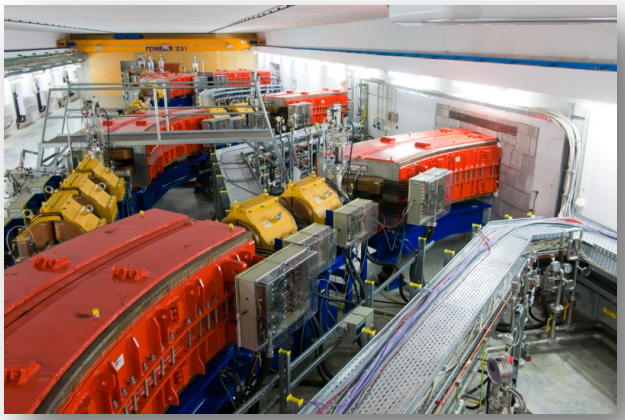
www.es.tu-darmstadt.de

Industrial Case Study: Heidelberg Ion-Beam Therapy Center (HIT)

TECHNISCHE UNIVERSITÄT DARMSTADT



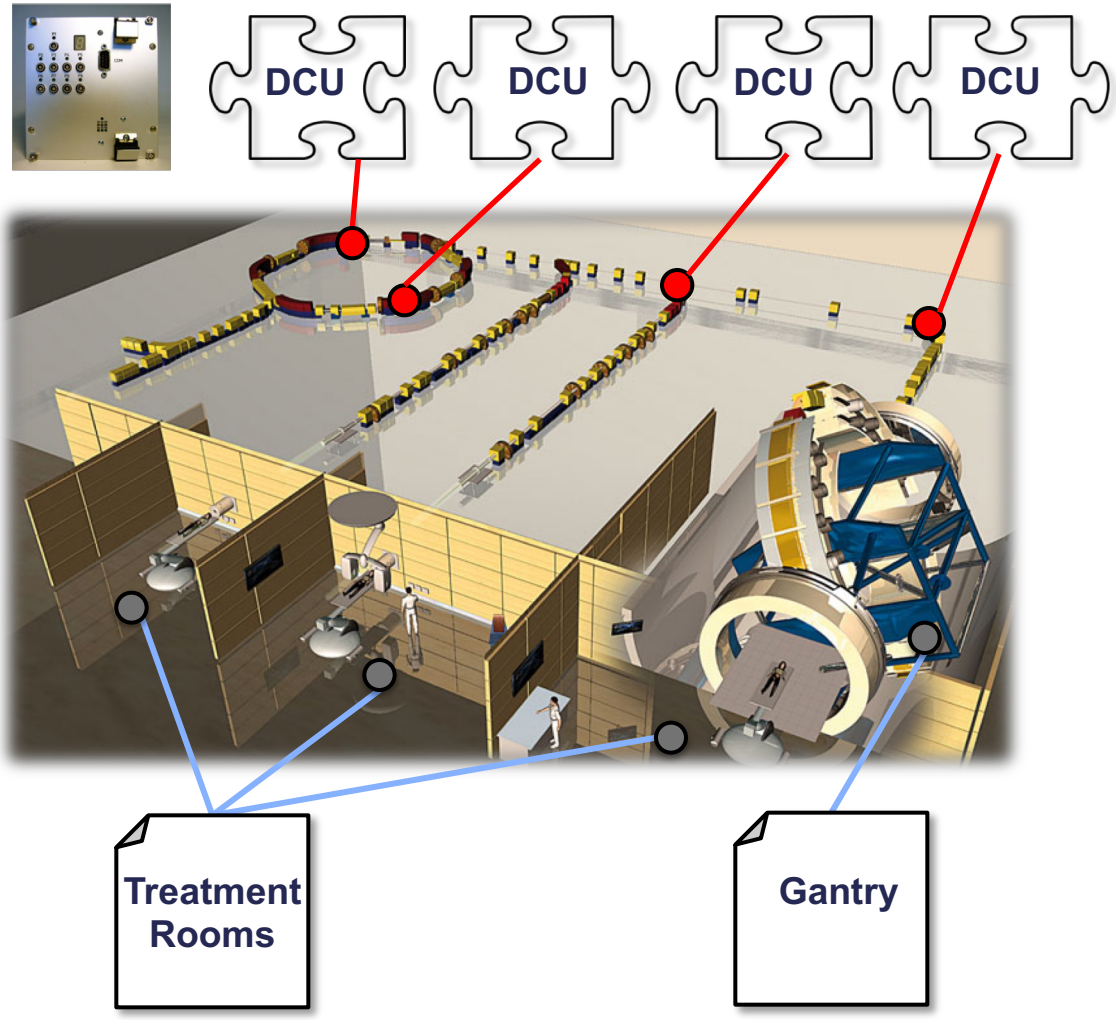
- In operation since 2009
- Novel cancer therapy with very precise heavy ion-beam radiation
- Reduction of collateral damages during radiation



https://www.klinikum.uni-heidelberg.de/

The HIT Cyber-Physical System: An Evolving Dynamic Software Product Line

TECHNISCHE UNIVERSITÄT DARMSTADT



- **Automation** of time-critical **control tasks**, mode switches and error-handling procedures
- Deeply **embedded** and **distributed** software *(~175,000 LOC C-Code)*
- Highly **(re-)configurable** and **evolving** software *(~500 Config. Param.)*
- IEC 62304 for QA of medical device software

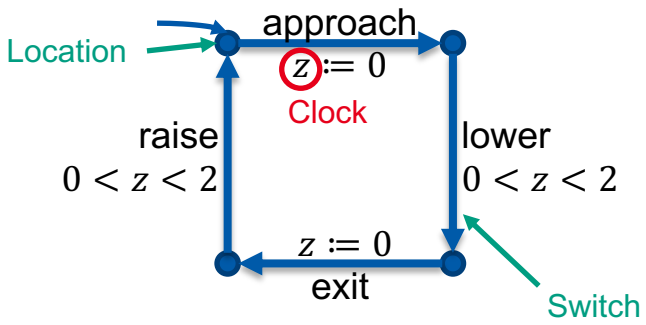
Traceability of test coverage to every possible configuration!

Running Example

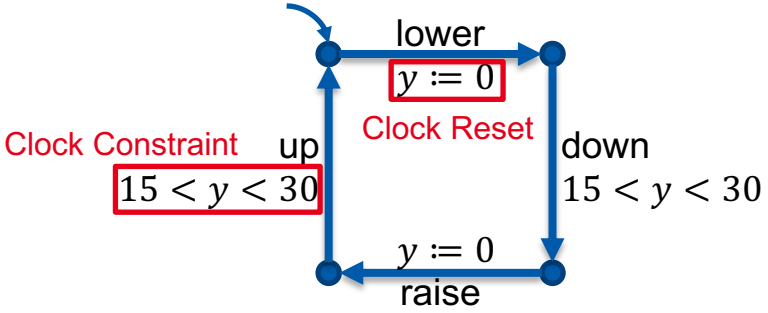
[Alur et al. (1993): Parametric Real-time Reasoning]

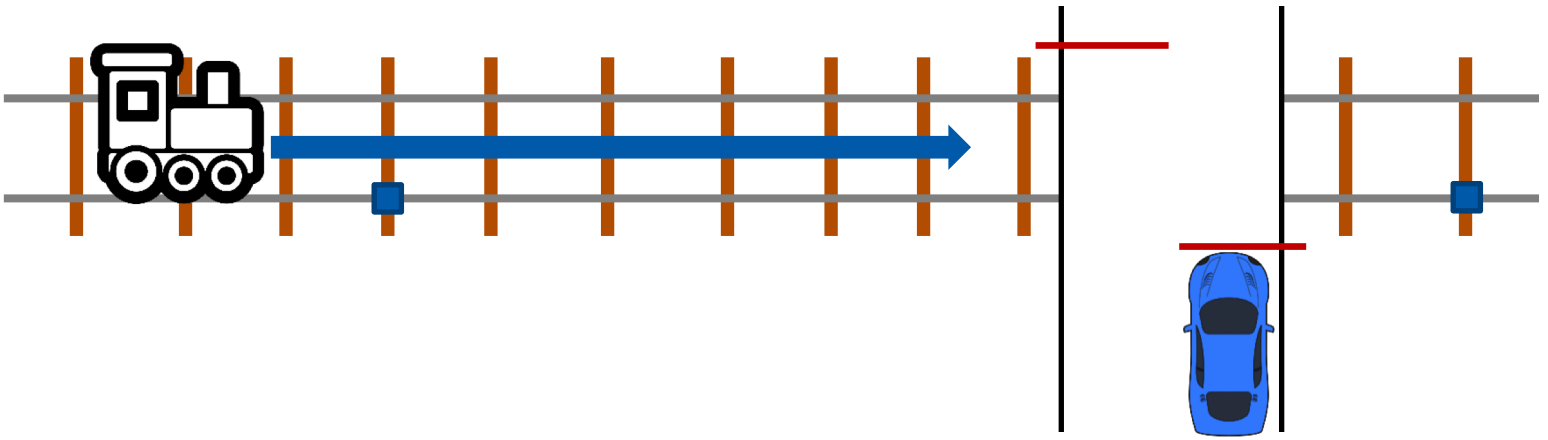
TECHNISCHE UNIVERSITÄT DARMSTADT

Controller

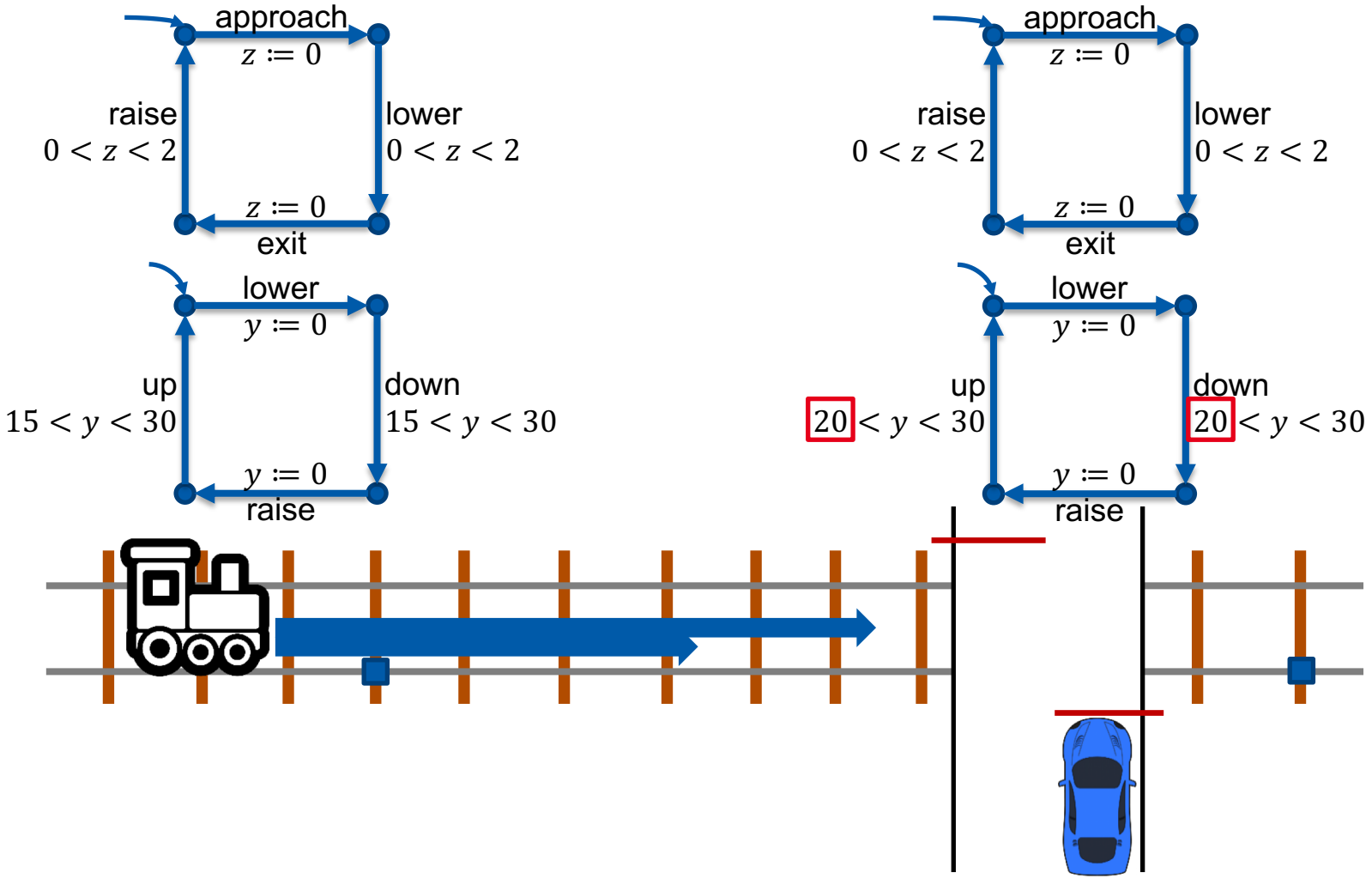


Gate



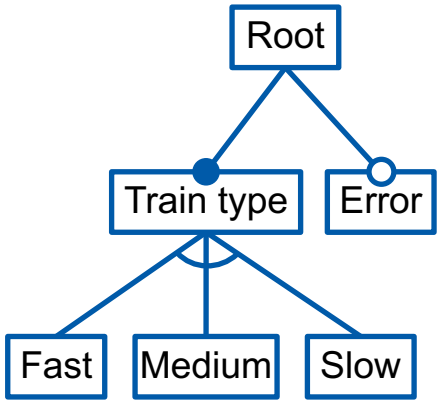


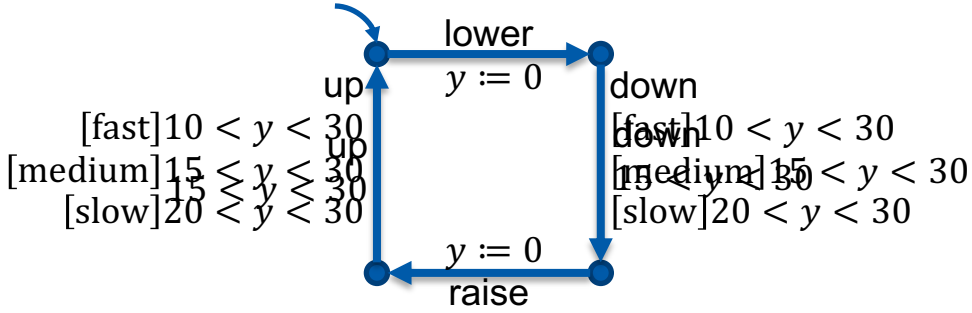
Product Line of TA



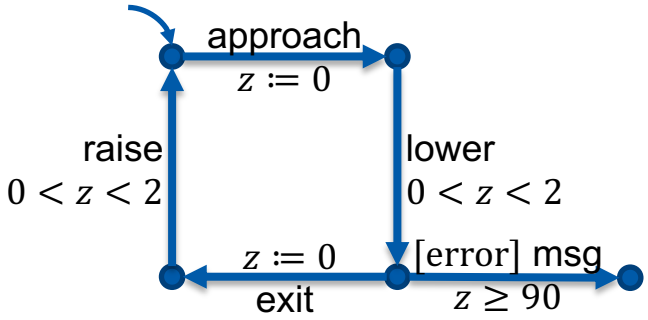
Featured Timed Automata (FTA)

[Cordy et al. (2012): Behavioural Modelling and Verification of Real-Time Software Product Lines]



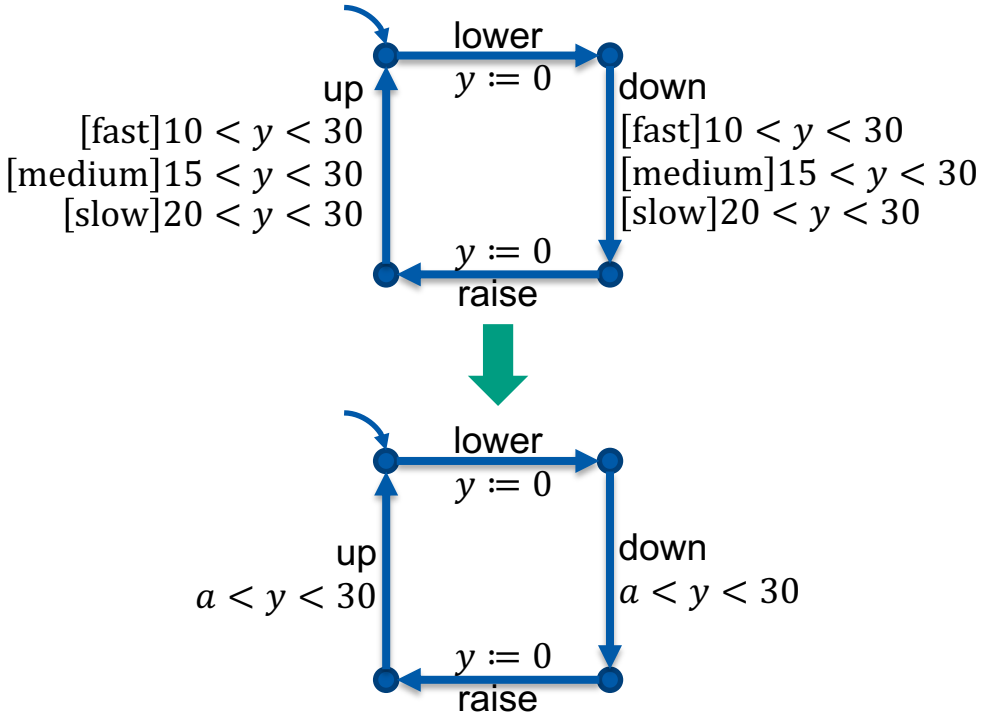


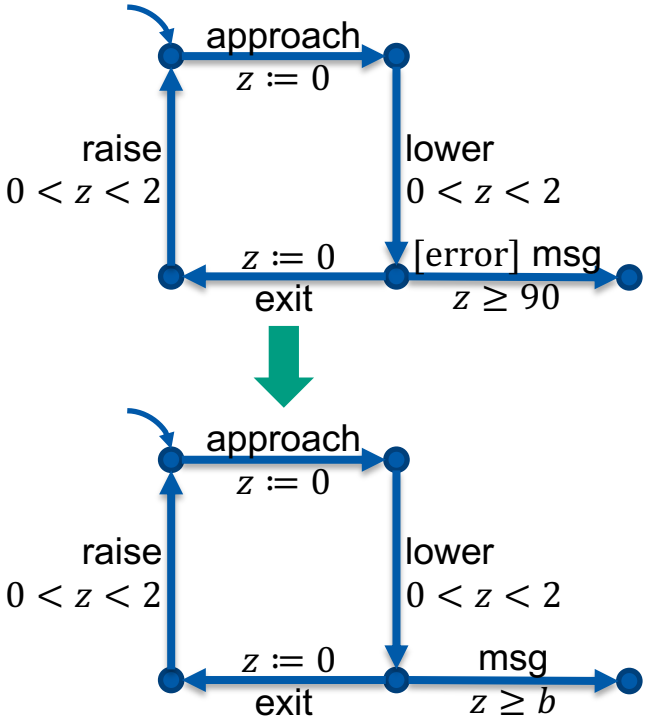
- Presence conditions for clock constraints and switches



Parametric Timed Automata (PTA)

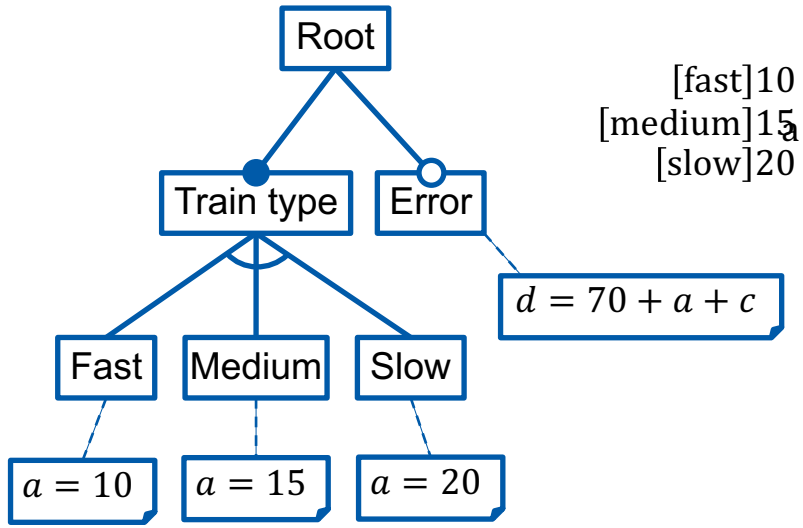
[Alur et al. (1993): Parametric Real-time Reasoning]

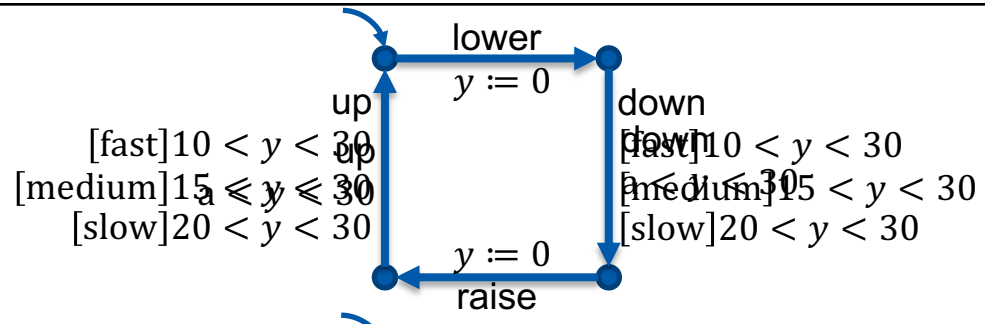


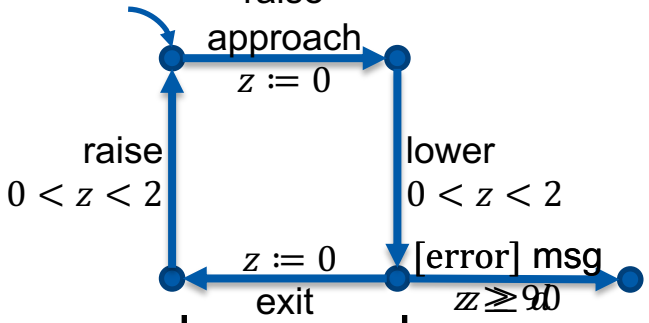


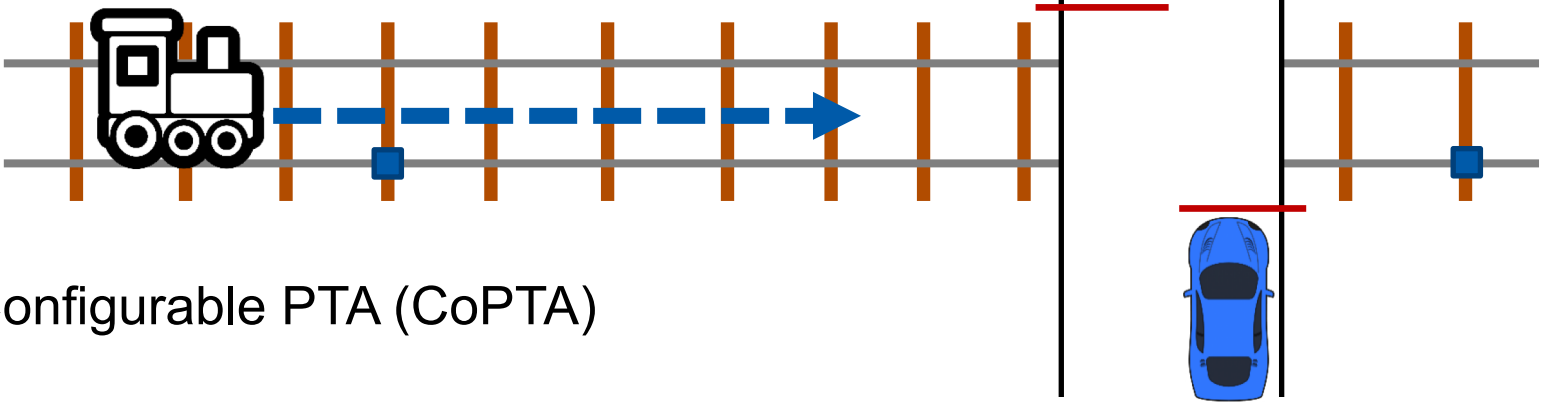
- Unbounded numeric parameters instead of Boolean features
- Results in a (potentially) infinite number of configurations

Unbounded Real-Time Constraints





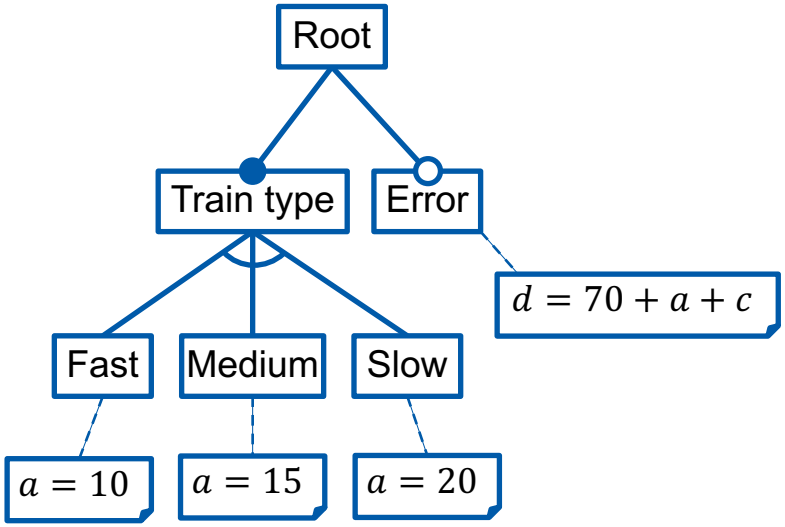


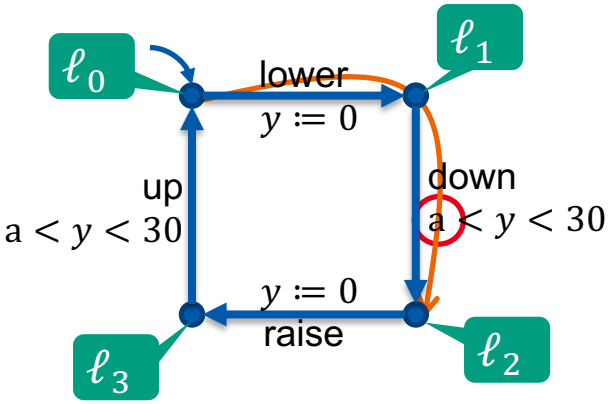


⇒ Configurable PTA (CoPTA)

Test-Case Generation

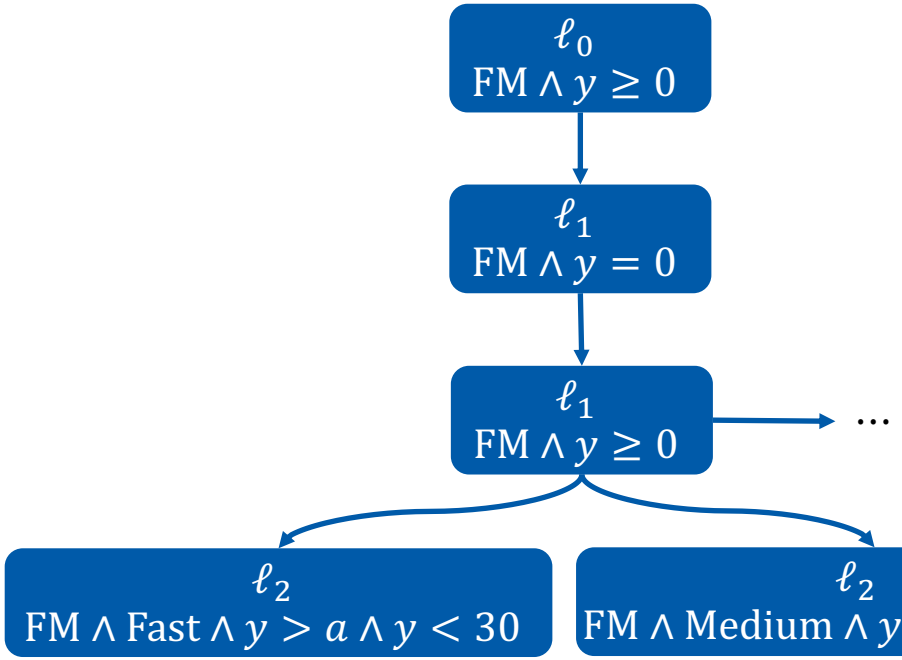
[Bürdek et al. (2015): Facilitating Reuse in Multi-goal Test-Suite Generation for Software Product Lines]
[André (2009): IMITATOR: A Tool for Synthesizing Constraints on Timing Bounds of Timed Automata]

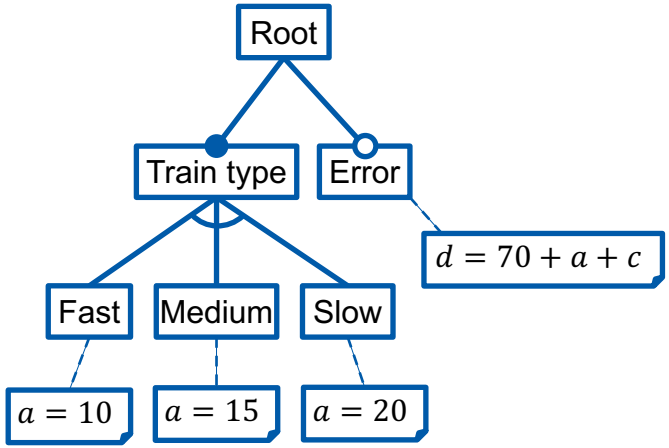


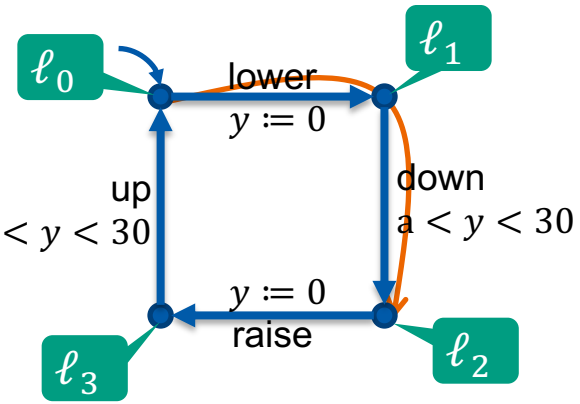


- Test case for ℓ_2: $\ell_0 \xrightarrow{(7,lower)} \ell_1 \xrightarrow{(12,down)} \ell_2$
- May be reused for ℓ_1 [Bürdek et al., 2015]
- May be reused for configurations with feature *Fast* [Bürdek et al., 2015]
- Implementation based on Imitator [André, 2009]

Featured Parametric Zone Graphs

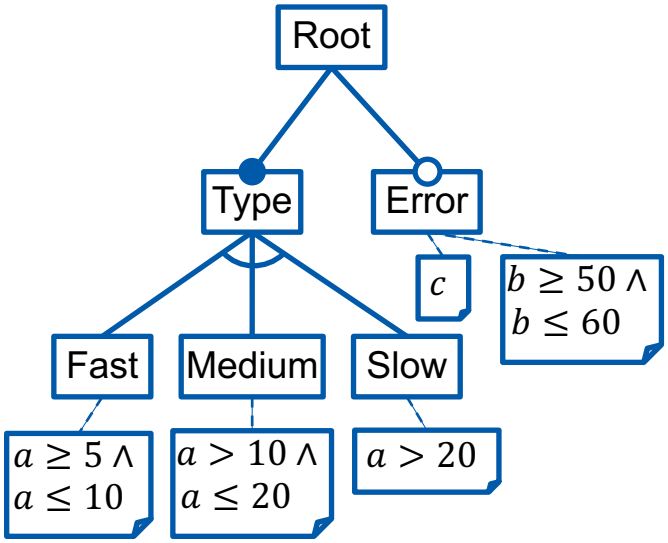


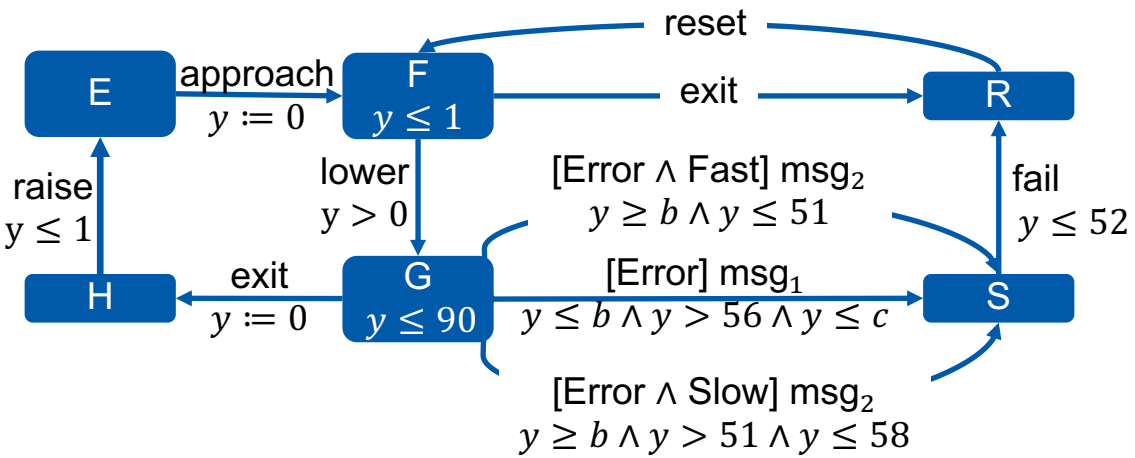




- "Is there a path to ℓ_2?"
- $\ell_2 \colon \ell_0 \xrightarrow{(7,lower)} \ell_1 \xrightarrow{(12,down)} \ell_2$
- Valid for all variants with feature *Fast*

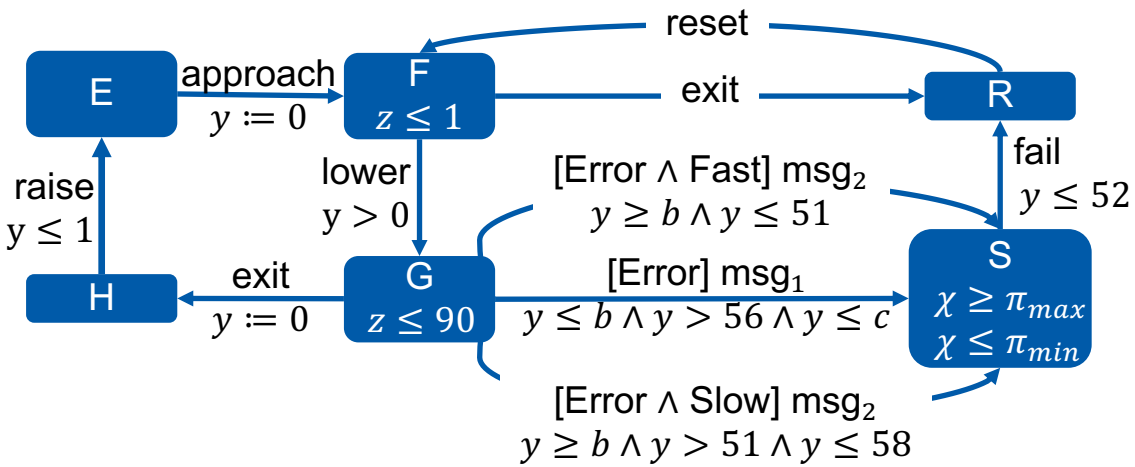
Test-Case Generation for Boundary Cases





- Adapted controller: several error messages
- Solution-space knowledge → boundary cases
- *Minimum/Maximum Delay (M/MD) Coverage*

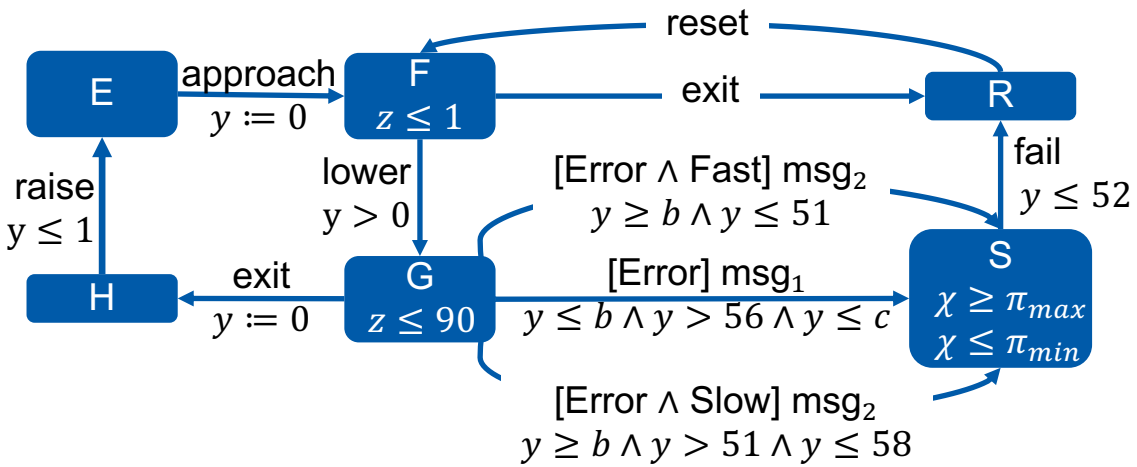
M/MD Instrumentation

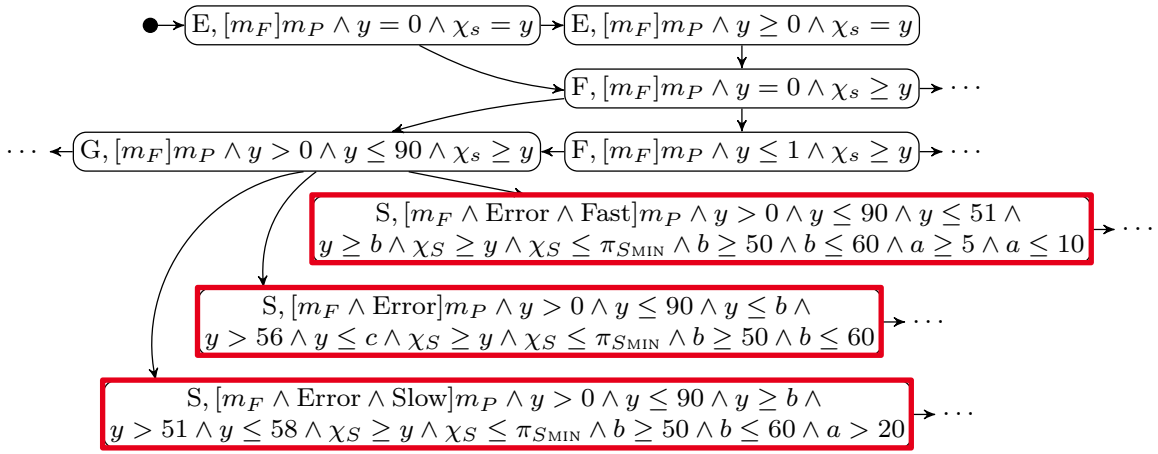


- Additional clock χ and additional parameters π_{min} and π_{max}
- χ is never reset
- Minimize/maximize π_{min}/π_{max}

Generating Test Cases with Minimum/Maximum Delays (1)

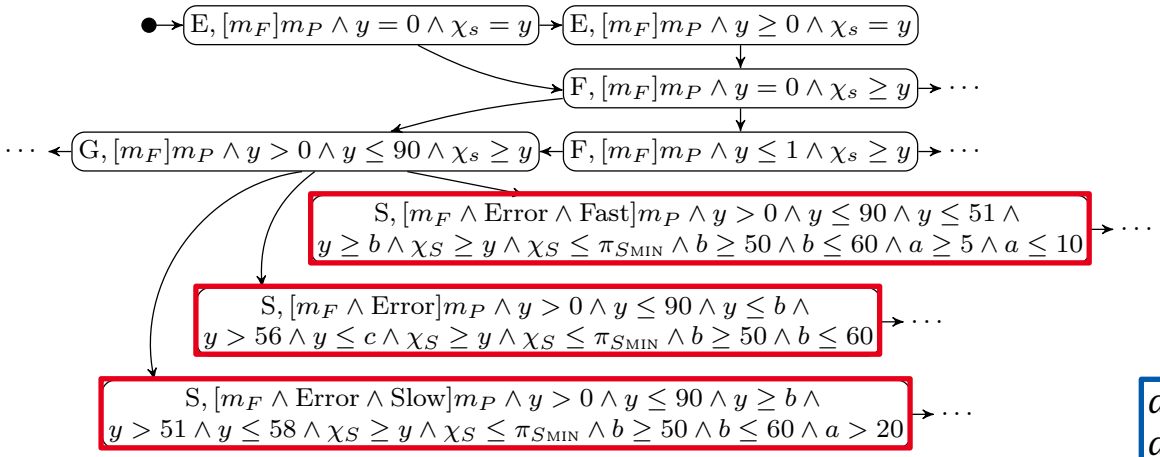
TECHNISCHE UNIVERSITÄT DARMSTADT

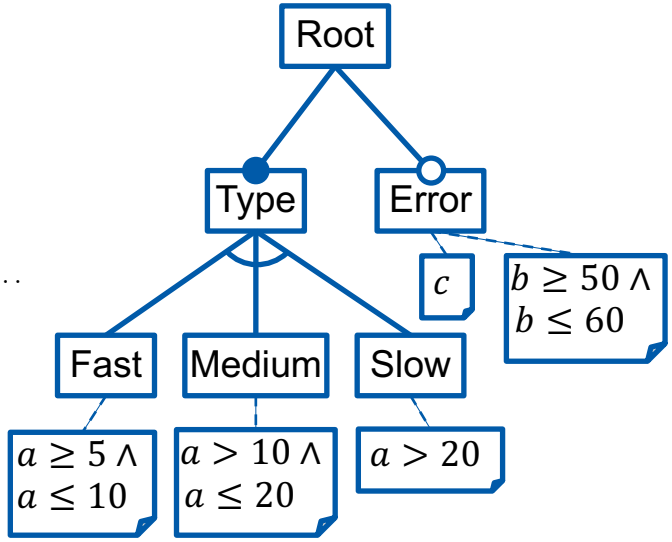




1. Find all paths to the target location (e.g., location *S*)

Generating Test Cases with Minimum/Maximum Delays (2)

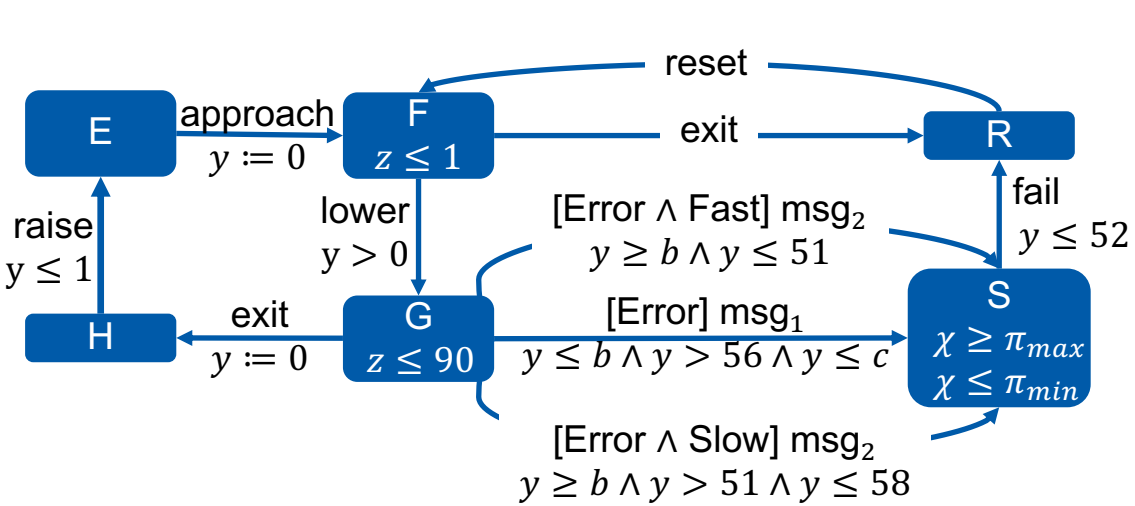


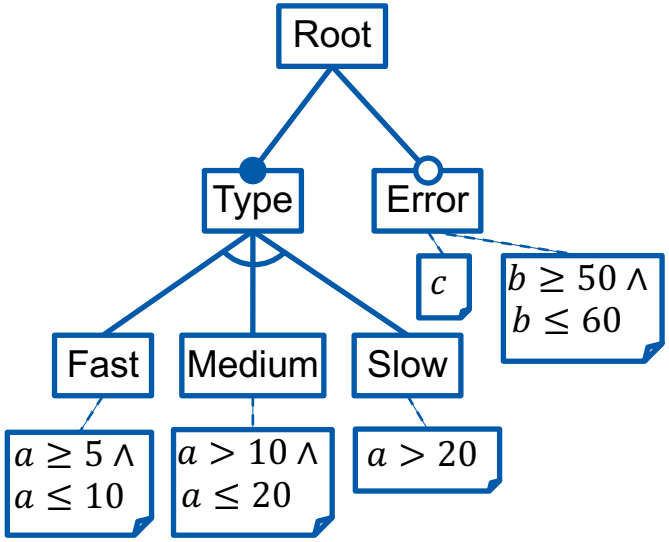


2. Use ILP solver to find parameter valuation with minimal π_{min}

3. Result: $\pi_{min} = 50$

Generating Test Cases with Minimum/Maximum Delays (3)





4. Find path to target location S with $\pi_{min} = 50$

$$E \xrightarrow{(0,approach)} F \xrightarrow{(1,lower)} G \xrightarrow{(49,msg_2)} S$$

5. May be applied to variants satisfying $\text{Error} \wedge \text{Fast} \wedge b = 50$

Workshop-related Questions

TECHNISCHE UNIVERSITÄT DARMSTADT

ES4CPS problems that we are interested in:

- Understand impact of parameters on execution times
- Find a suitable model to express aspects of ES

ES4CPS-related expertise that we can contribute:

- Generate test suites for models of ES
- Generalize concept of M/MD coverage

External expertise that we need:

- Find a suitable hybrid model for (families of) ES
- (Black-box) testing of neural networks
- Generate models (e.g., with a machine-learning approach)