TWT GmbH
Science & Innovation

TWT GmbH
Science & Innovation

Introduction to UPPAAL

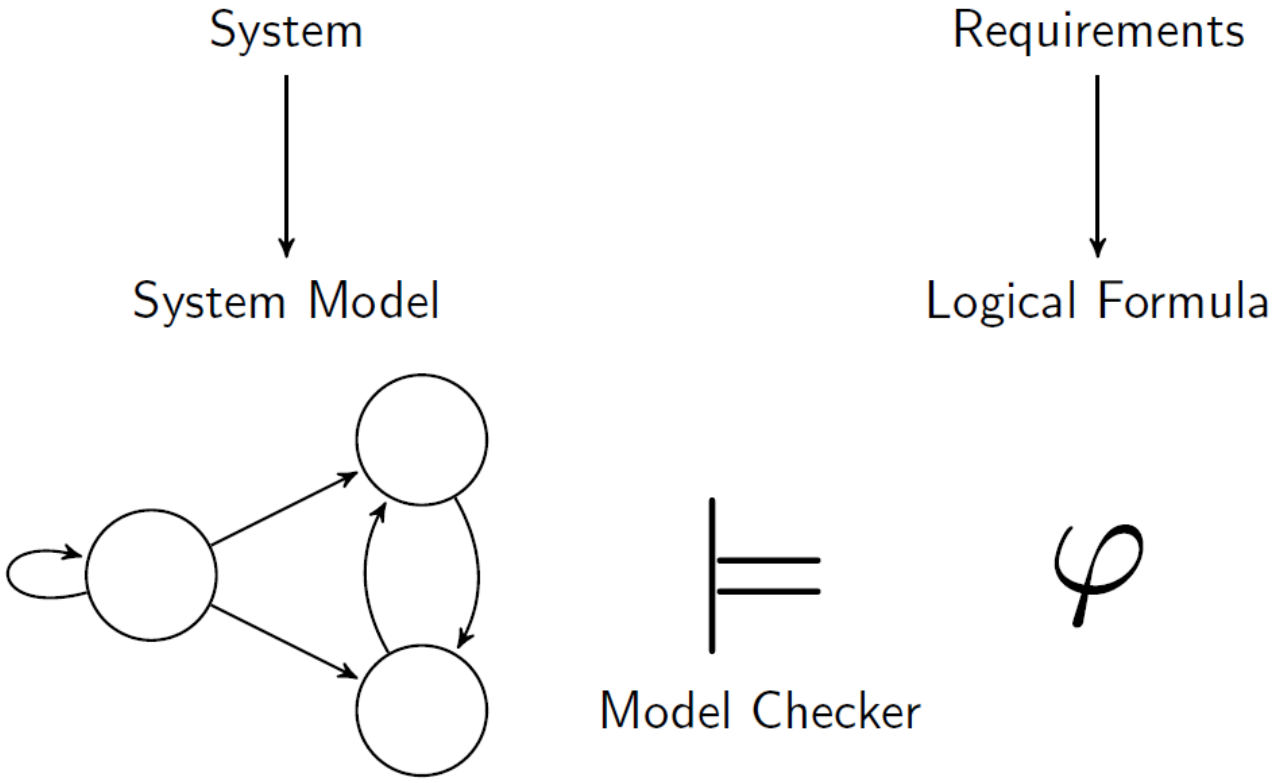
Model Checking of Timed Automata

Stefan Rieger 16/04/2013

Bernhäuser Str. 40-42
73765 Neuhausen
Telefon: +49.71 58.17 15.0
info@twt-gmbh.de
www.twt-gmbh.de

Stuttgart, München,
Friedrichshafen

Model Checking (in General)



TWT

Arguments for/against Model Checking

Advantages

+ Complete (unlike testing)

+ Covers errors difficult to find by testing

+ Fully automatic

+ Failures yield diagnostic error traces

Disadvantages

– Manual model construction intricate and error-prone

– Due to exhaustive search not suitable for large models (State Explosion Problem)

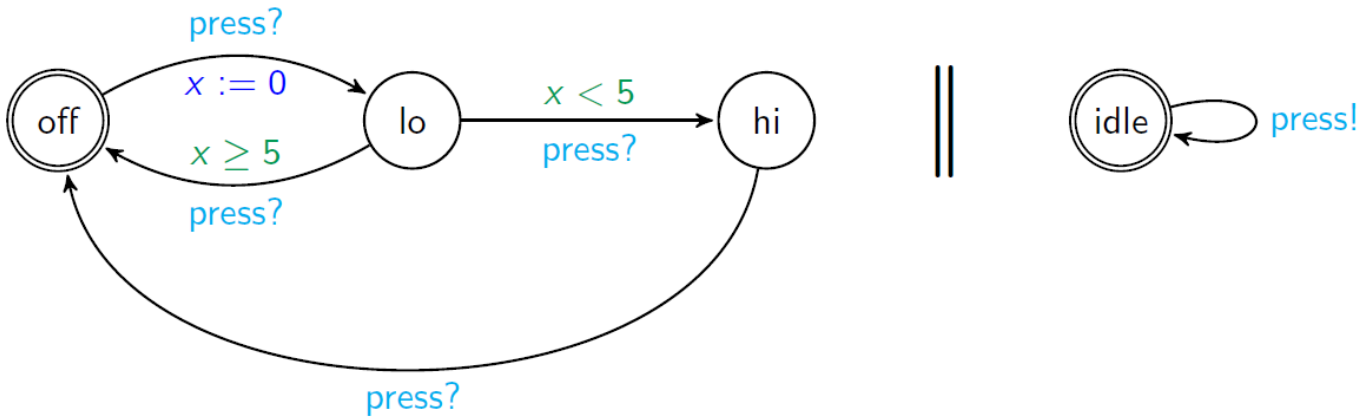
TWT

Application of Model Checking in openETCS

- To be used for critical components in a system, not the system as a whole
- Abstraction from irrelevant details
- **Here: focus on timed model checking**

Timed Automata

- Formal system modelling language
- Takes into account timing and real-time aspects
- Finite automata enriched with clocks

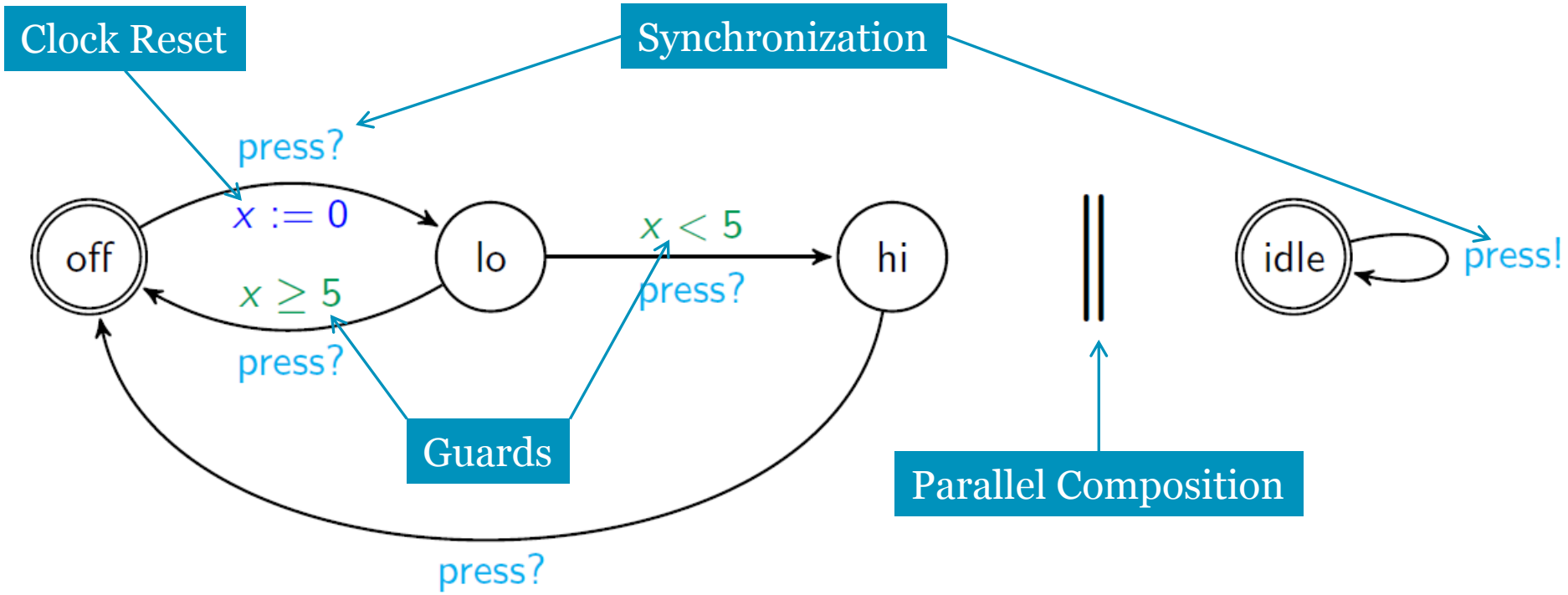


TWT

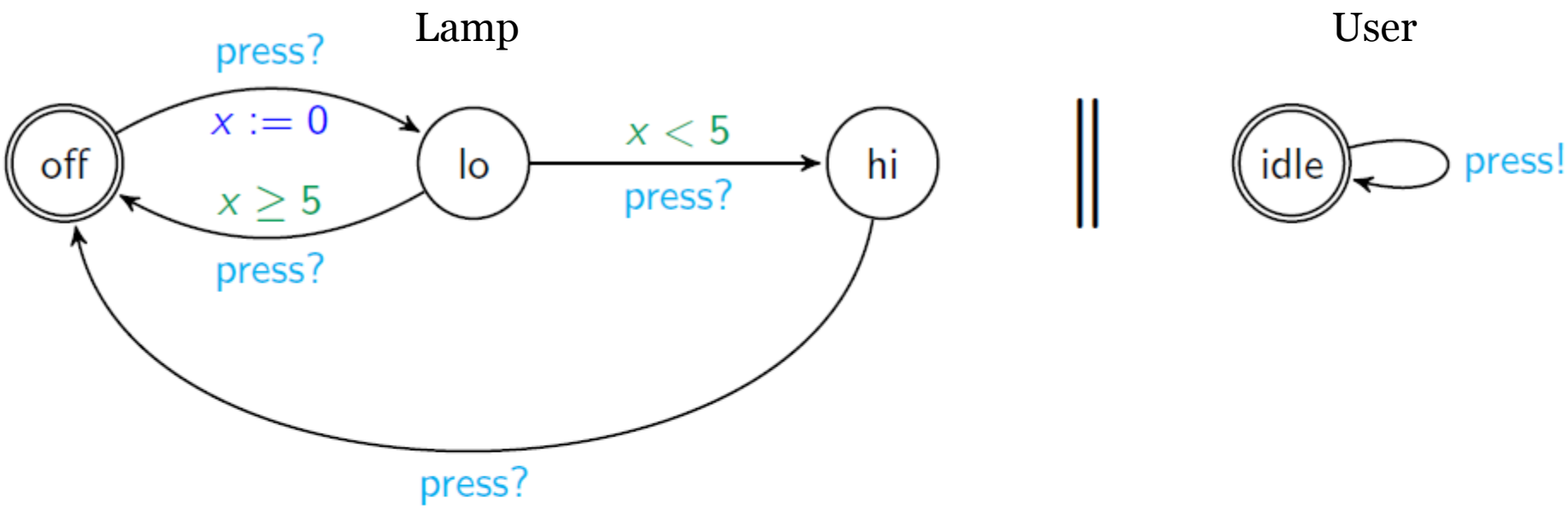
UPPAAL

- Tool for modeling and verifying (model checking) timed automata
- Network of synchronized timed automata
- Subset of TCTL (Timed Computation Tree Logic) for specifying properties
- Developed by the universities of Uppsala und Aalborg
- Currently closed source, free academic license

Example: Lamp Model



Example taken from [1]



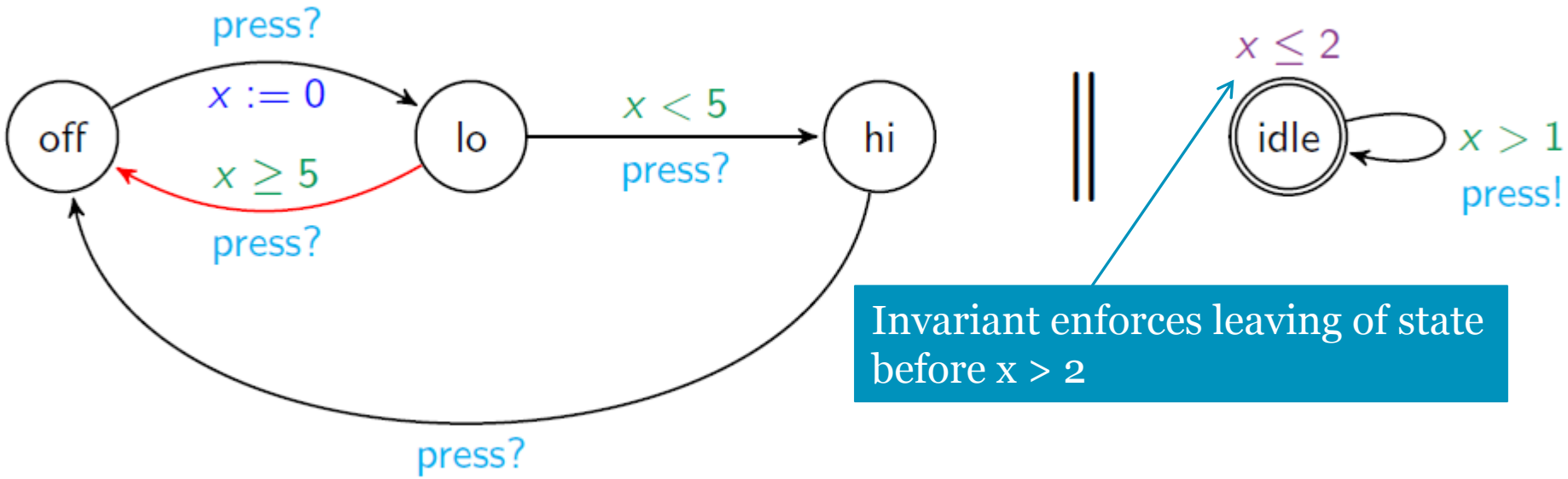
Possible Runs (omitting the user):

$(\text{off}, x = 0) \rightarrow (\text{off}, x = 3) \rightarrow (\text{lo}, x = 0) \rightarrow (\text{lo}, x = 0.5) \rightarrow (\text{hi}, x = 0.5) \rightarrow (\text{hi}, x = 1000) \ldots$

$(\text{off}, x = 0) \rightarrow (\text{off}, x = 2) \rightarrow (\text{lo}, x = 0) \rightarrow (\text{lo}, x = 6) \rightarrow (\text{off}, x = 6) \rightarrow (\text{off}, x = 8) \rightarrow (\text{low}, x = 0) \ldots$

Example taken from [1]

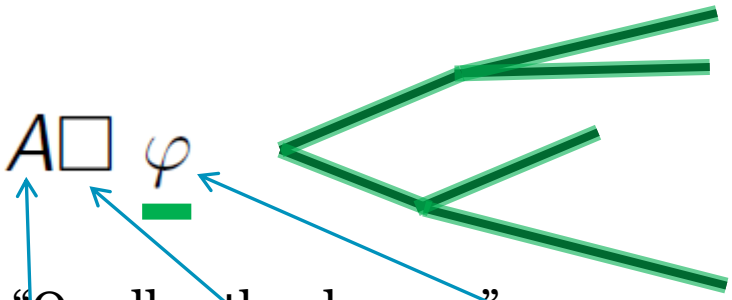
Invariants



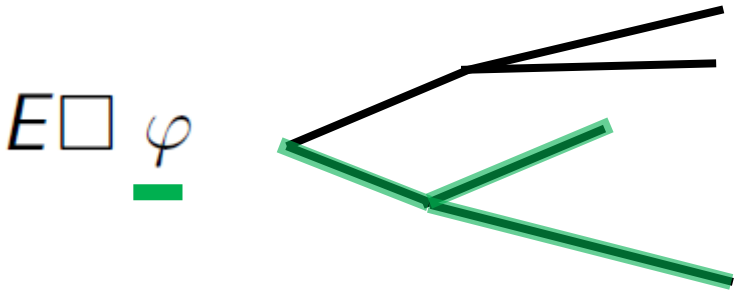
Consequence: red transition will never be taken

Example taken from [1]

Properties in UPPAAL



"On all paths always…"

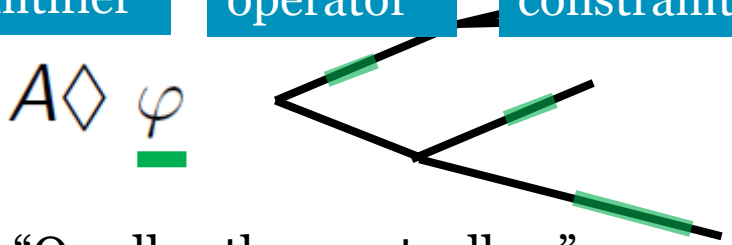


"There is a path where always…"

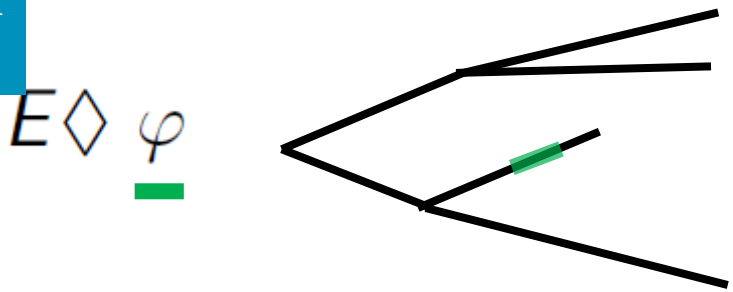
Path quantifier

Temporal operator

May contain clock constraints

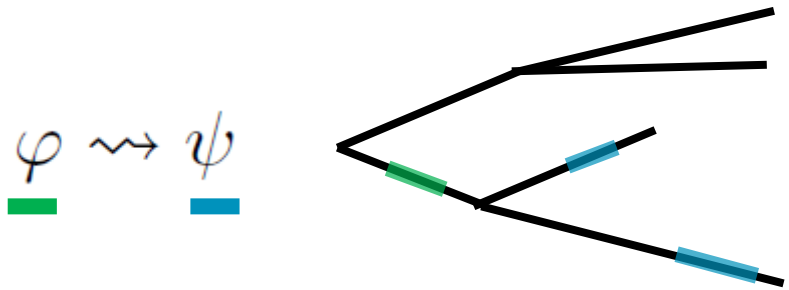


"On all paths eventually…"



"There is a path where eventually…"

Properties (continued)

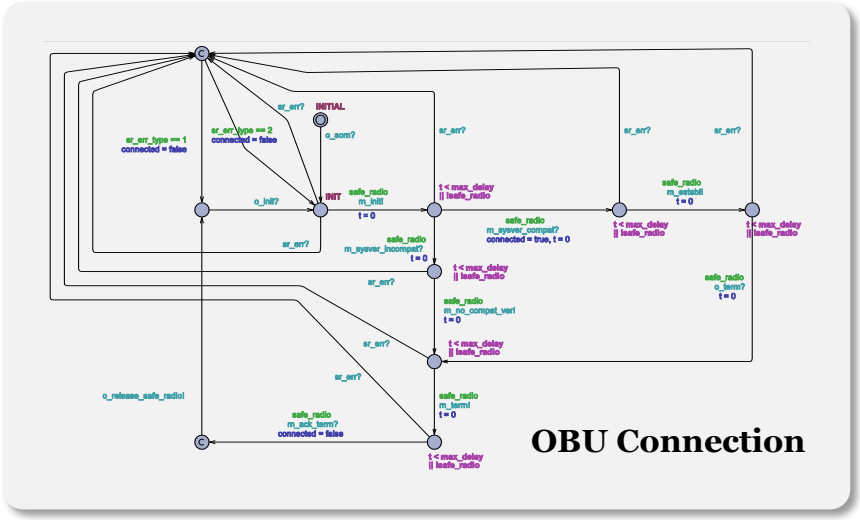


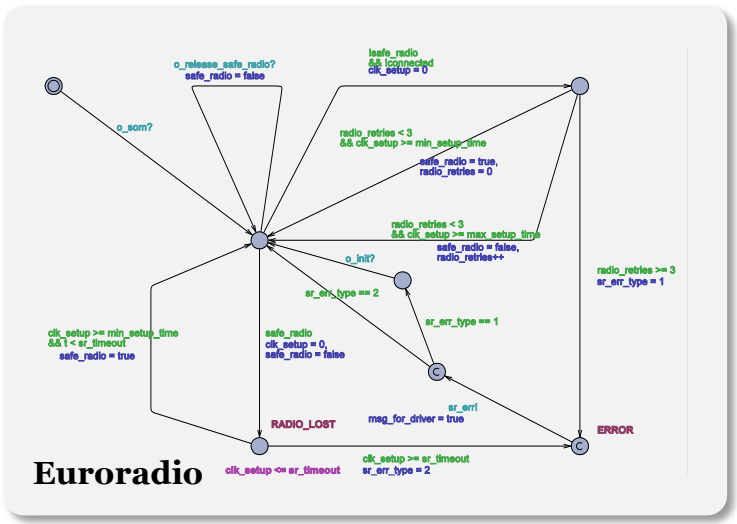
“Whenever φ then eventually ψ…”

Restriction in UPPAAL: No nesting of operators
=> Liveness is restricted

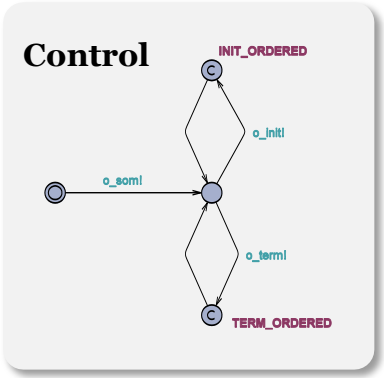
Partial Model of Subset 026
3.5 Radio Communication

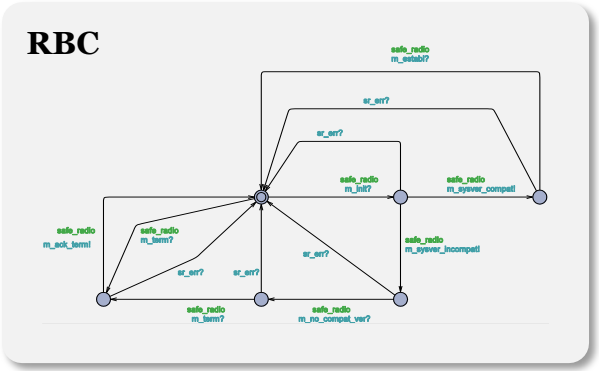
TWT





Synchronization





Radio Communication Model – Covered Aspects

2-stage radio communication setup:

(1) Safe radio connection according to Euroradio (basis for OBU-RBC connection)

- Initially at most 3 retries for setup
- Safe radio connection may fail at any time
- Upon connection loss 5 min timeout for reestablishing connectivity
- Delays and timeouts for safe radio connection

(2) OBU- RBC communication only when safe radio connection established

- Establishing and terminating OBU-RBC connection

Here: Focusing on a single OBU as DUT

TWT

Radio Communication Model – Properties

Verified

- There is no a deadlock in the system
- It is possible to establish a connection
- It is possible that a connection is never established
- Always when the termination of the radio connection is ordered, the connection is eventually terminated

Falsified

- An established RBC connection always implies that there is a safe radio connection.
- When the initiation of a connection is ordered, it is eventually established.

TWT

UPPAAL TOOL DEMO

TWT

Next Steps

- Model still incomplete -> Extension to take into account missing aspects
- Find interesting timing properties in the standard
- Further investigation: transformation of SystemC models to timed automata
    - In the literature approaches exist [2]
    - Not yet suitable for complex models

TWT

Thank you for your attention

Questions?

TWT

References

[1] Behrmann, Gerd, Alexandre David, and Kim G. Larsen. "A Tutorial on UPPAAL 4.0.", *http://www.it.uu.se/research/group/darts/papers/texts/new-tutorial. pdf* (2006).

[2] Herber, Paula, Joachim Fellmuth, and Sabine Glesner. "Model checking SystemC designs using timed automata." *Proceedings of the 6th IEEE/ACM/IFIP international conference on Hardware/Software codesign and system synthesis*. ACM, 2008.