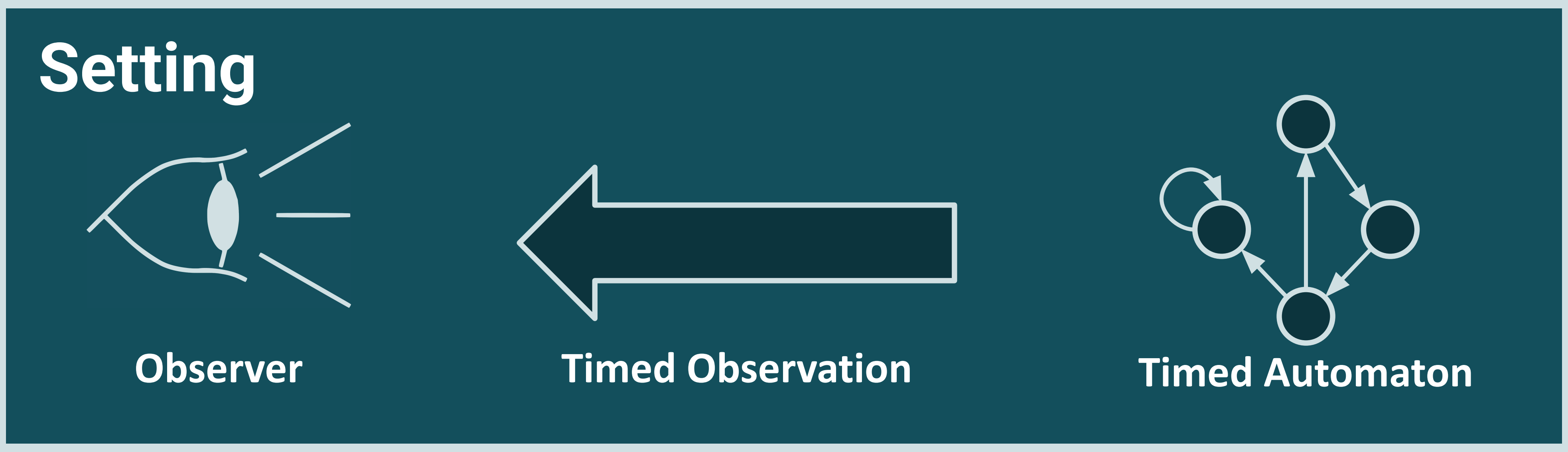
A Unified Method to Guarantee Opacity of Discrete-Timed Automata

Setting



Threat Model

- Observer tries to deduce secret information from
- Timed observations (events with time stamps)
- Structure of timed automaton (state graph)

Opacity Notions

Current-Location Timed Opacity (CLTO)

→ Observer cannot deduce that a secret location is currently active

Initial-Location Timed Opacity (ILTO)

→ Observer cannot deduce that initial location was secret

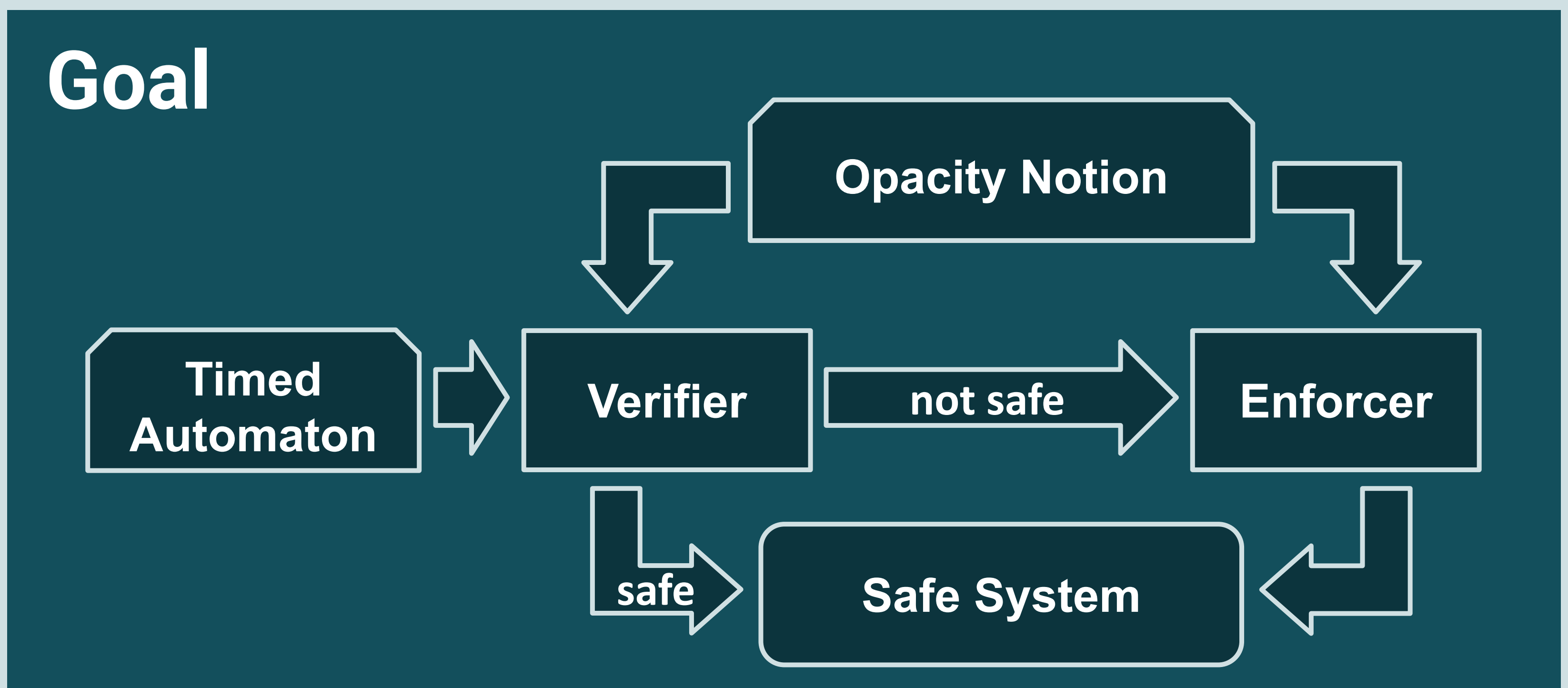
Infinite-Step Timed Opacity (ISTO)

→ Observer cannot deduce that any past location was secret

K-Step Timed Opacity (KSTO)

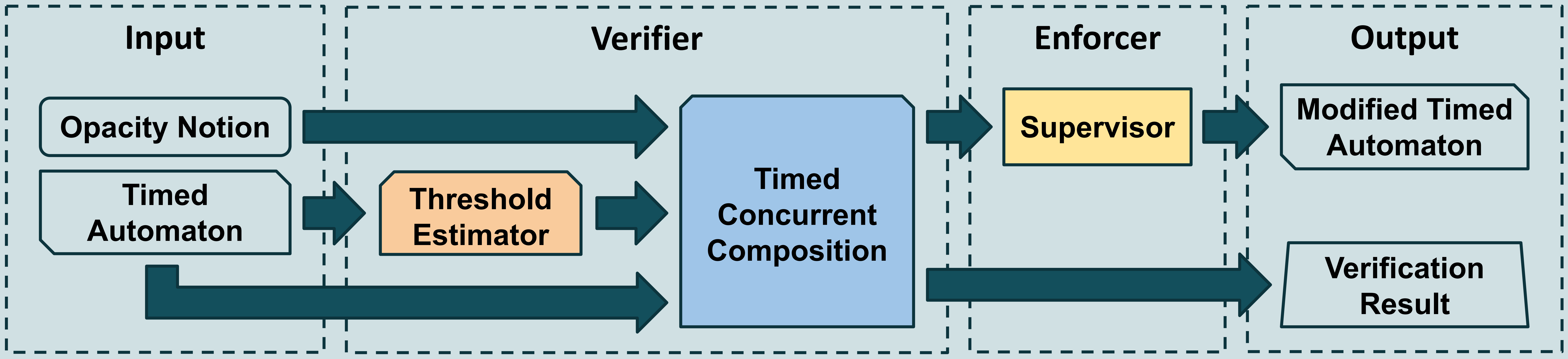
→ Observer cannot deduce that a secret location was active within the last K observations

Goal



- Check if opacity notion holds on original system (**Verifier**)
- Apply changes such that opacity holds (**Enforcer**)
- Terminate if and only if opacity holds

Proposed Method



State Estimation

Compute Threshold Estimator

- **"Deterministic version"** of input timed automaton
- Provides all states that **could be active** after any observation
- Computation is more **efficient** compared to related methods

Opacity Verification

Compute Timed Concurrent Composition

- Composition on **timed automata** and **threshold estimators**
- Can verify **ILTO**, **CLTO**, **ISTO**, and **KSTO**
- Computation is more **efficient** compared to related methods
- Could verify **any** opacity notion (future work)

Opacity Enforcement

Compute Supervisor

- Currently **ongoing work**
- Planned to be based on **timed concurrent composition**
- Joint work with **Kuize Zhang** at the department of mathematics and statistics **Xi'an Jiaotong University**

References

Verifying Opacity of Discrete-Timed Automata
12th International Conference on Formal Methods in Software Engineering (**FormaliSE**), IEEE/ACM,
April 2024, Lisbon, Portugal

Paper Artifact

- Introduces a new **time abstraction**
- **Decreases computation costs** of threshold estimators

Efficient State Estimation of Discrete-Timed Automata
25th International Conference on Formal Engineering Methods (**ICFEM**), Springer,
December 2024, Hiroshima, Japan

Paper Artifact

- Introduction of **threshold estimators**
- **New class** of state estimators for discrete timed automata

A Unified Method to Efficiently Verify Opacity of Discrete-Timed Automata
26th International Conference on Formal Engineering Methods (**ICFEM**), Springer,
November 2025, Hangzhou, China

Will be published in November

Paper Artifact

- **Unified** and **efficient** method to verify four opacity notions
- Will be **extended** to **more opacity notions**

Julian Klein
Technical University of Berlin
j.klein@tu-berlin.de

Prof. Dr. Sabine Glesner (Advisor)
Technical University of Berlin
sabine.glesner@tu-berlin.de

Prof. Dr. Kuize Zhang (Research Partner)
Xi'an Jiaotong University
kuize.zhang@xjtu.edu.cn

SOFTWARE AND EMBEDDED SYSTEMS ENGINEERING

TECHNISCHE UNIVERSITÄT BERLIN

西安交通大學
XI'AN JIAOTONG UNIVERSITY