Cyber Security for Europe

Using statistical model checking for cybersecurity analysis

Carlos E. Budde
Ass. Prof. @ Università di Trento
CS4E: Cybersecurity Skills and Capability Building

Modern cybersecurity: nowhere to run

Cyber Security for Europe

Hack Brief: Hackers Stole $40 Million from Binance Cryptocurrency Exchange

One of the biggest cryptocurrency exchanges got hit, as thieves nabbed $40 million of bitcoin —along with two-factor user codes and API tokens.

"The hackers used a variety of techniques, including phishing, viruses and other attacks," Binance CEO Zhao Changpeng wrote in a blog post. AKIO KON/BLOOMBERG/GETTY IMAGES

Modern cybersecurity: nowhere to run

Cyber Security for Europe

Hack Brief: Hackers Stole $40 Million from Binance Cryptocurrency Exchange

One of the biggest cryptocurrency exchanges got hit, as thieves nabbed $40 million of bitcoin —along with two-factor user codes and API tokens.

"The hackers used a variety of techniques, including phishing, viruses and other attacks," Binance CEO Zhao Changpeng wrote in a blog post. AKIO KON/BLOOMBERG/GETTY IMAGES

… but security is not Boolean,

there is a **degree of resilience to cyberattacks**

Technical Leverage in a Software Ecosystem: Development Opportunities and Security Risks

Fabio Massacci
University of Trento (IT), Vrije Universiteit Amsterdam (NL)
fabio.massacci@ieee.org

Ivan Pashchenko
University of Trento (IT)
ivan.pashchenko@unitn.it

***Abstract*—In finance, *leverage* is the ratio between assets borrowed from others and one's own assets. A matching situation is present in software: by using free open-source software (FOSS) libraries a developer leverages on other people's code to multiply the offered functionalities with a much smaller own**

that third party code inherited through dependencies is four times larger than the size of the own code base as an industry average [9]. It can be up to four orders of magnitude in our FOSS sample.

Measurement of Cyber Resilience from an Economic Perspective

Adam Z. Rose and Noah Miller

Center for Risk and Economic Analysis of Terrorism Events (CREATE), University of Southern California, Los Angeles, CA, USA

10.1 Introduction

All segments of society are becoming increasingly vulnerable to cyber disruptions from malicious actors, natural disasters, and technological accidents. Although significant efforts are being made to protect cyber systems from threats, increasing cyber usage and increasing frequency and potential magnitude of threats appears to be more than offsetting these initiatives. There is a growing realization in the cyber area, as well as in other domains, that we cannot protect complex systems against all threats, so some attention has

It’s a matter of ~~trust~~ $€£¥฿…

How much $€£¥฿ covers the degree of security I want?

How much security I want/need?

It’s a matter of ~~trust~~ $€£¥฿…

How much $€£¥฿ covers the degree of security I want?

How much security I want/need?

How valuable am I?

How vulnerable am I?

It’s a matter of ~~trust~~ $€£¥฿…

How much $€£¥฿ covers the degree of security I want?

How much security I want/need?

How valuable am I?

How vulnerable am I?

Measuring SW security vulnerability

Cyber Security for Europe

Empirical approach: assess existent IT framework

e.g. known vulnerabilities in code

Measuring SW security vulnerability

Cyber Security for Europe

Empirical approach: assess existent IT framework

e.g. known vulnerabilities in code

An Attack Surface Metric

Pratyusa K. Manadhata

CMU-CS-08-152

November 2008

IP address and domains, SSL certificates, ports & services, etc.

Measuring SW security vulnerability

Cyber Security for Europe

Empirical approach: assess existent IT framework

e.g. known vulnerabilities in code

An Attack Surface Metric

Pratyusa K. Manadhata

CMU-CS-08-152

November 2008

IP address and domains, SSL certificates, ports & services, etc.

THE VERGE TECH REVIEWS SCIENCE CREATORS ENTERTAINMENT VIDEO MORE

MOBILE TECH T-MOBILE

Another T-Mobile cyberattack reportedly exposed customer info and SIMs

Documents say the company has contacted impacted customers

By Mitchell Clark | Dec 28, 2021, 6:30pm EST

Dec 28, 2021, 6:30pm EST

Measuring SW security vulnerability

Cyber Security for Europe

Empirical approach: assess existent IT framework

e.g. known vulnerabilities in code

Metrics from known exploits are hard to extrapolate in time

Measuring SW security vulnerability

Empirical approach: assess existent IT framework

e.g. known vulnerabilities in code

Metrics from known exploits are hard to extrapolate in time

How vulnerable ~~am I?~~ shall I be?

Measuring SW security vulnerability

Cyber Security for Europe

Empirical approach: assess existent IT framework

e.g. known vulnerabilities in code

Metrics from known exploits are hard to extrapolate in time

How vulnerable ~~am I?~~ shall I be?

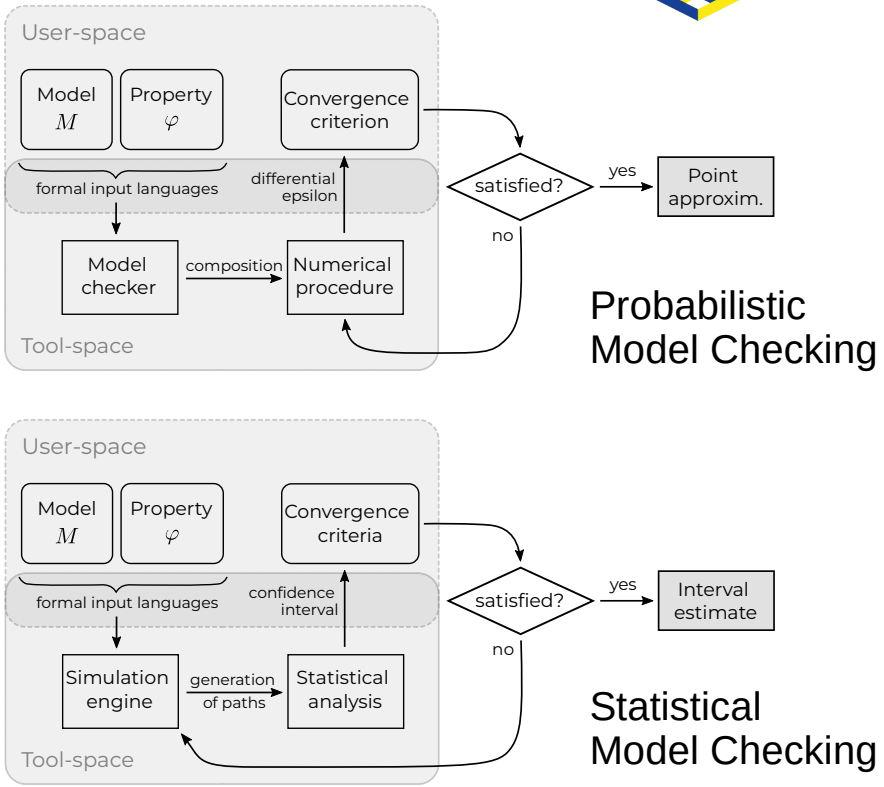
Proposal: let's model & check

Fit attack patterns and distributions within a formal framework

(**model checking** in formal methods)

Model checking for safety, liveness, etc.

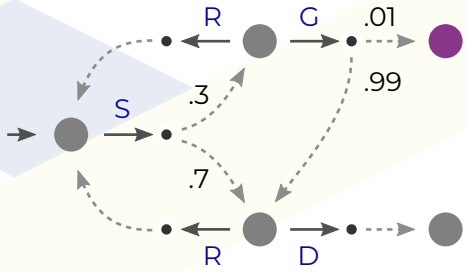
$$M \models \varphi$$

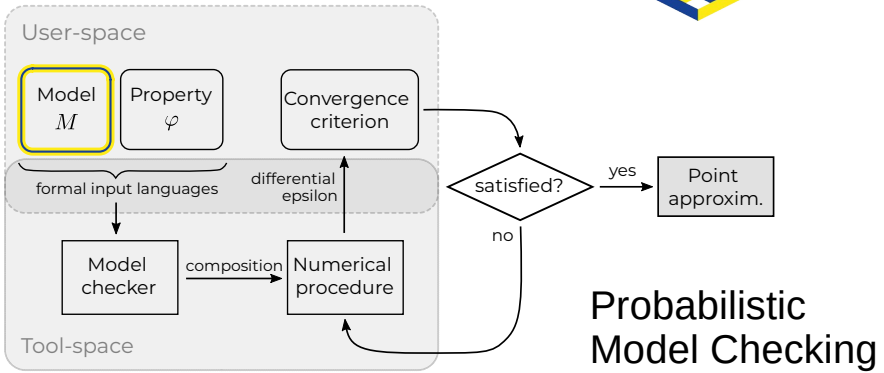


Model checking for safety, liveness, etc.

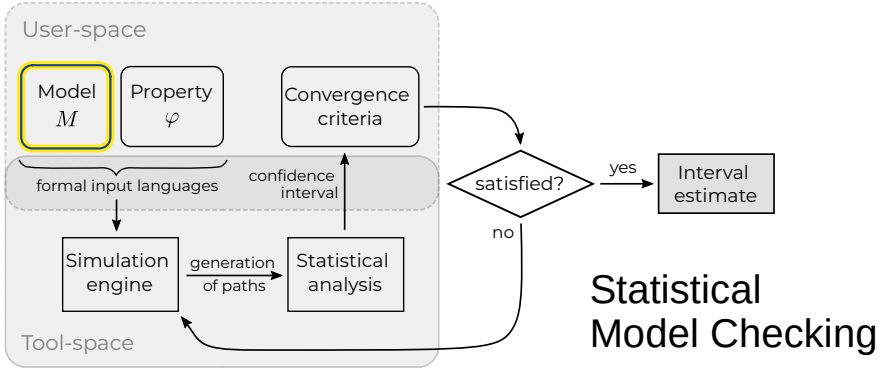
Cyber Security for Europe

$$M \models \varphi$$





Probabilistic Model Checking

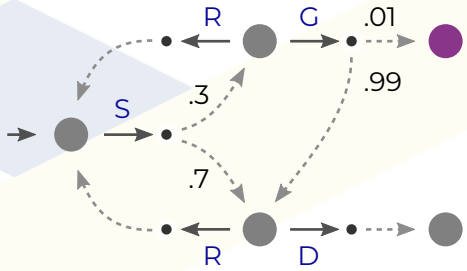


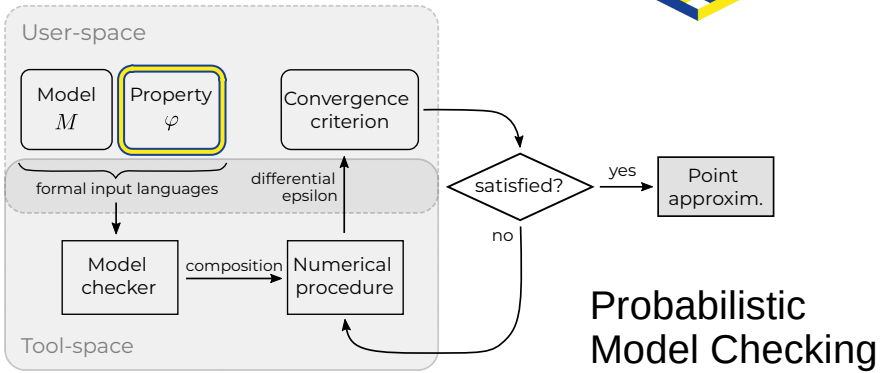
Statistical Model Checking

Model checking for safety, liveness, etc.

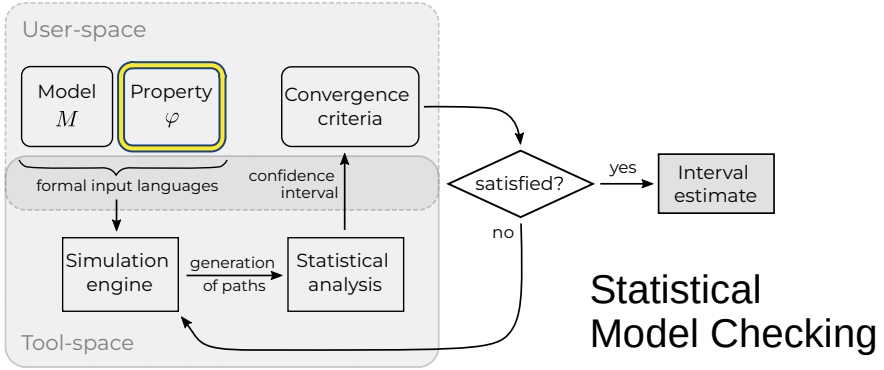
$$M \models \varphi$$

$\square\neg\text{unsafe}$ $\square\Diamond\text{alive}$





Probabilistic Model Checking



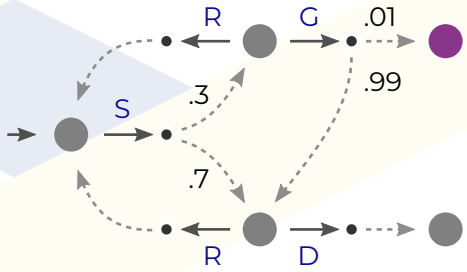
Statistical Model Checking

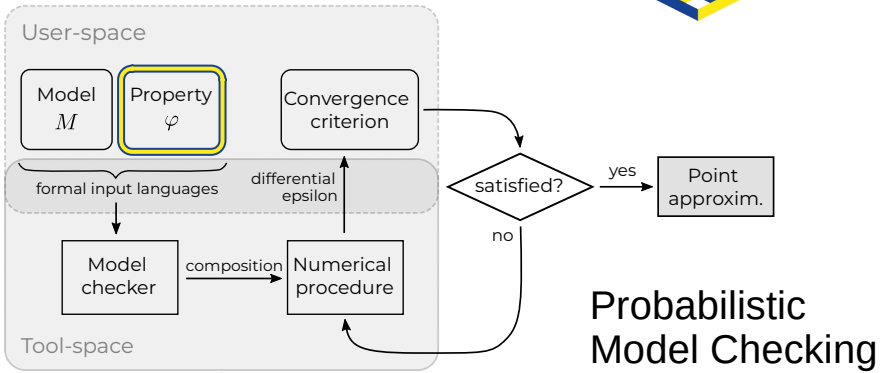
Model checking for safety, liveness, etc.

$$M \models \varphi$$

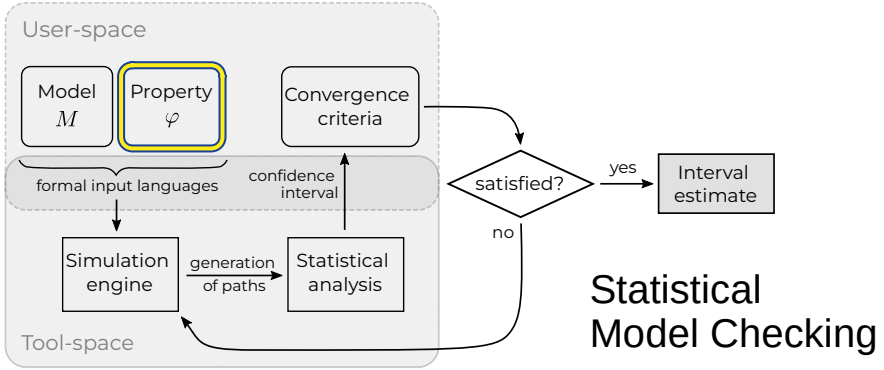
$$P(\text{unsafe}) \leqslant 0.02$$

$$\Box\neg\text{unsafe} \qquad \Box\Diamond\text{alive}$$





Probabilistic Model Checking

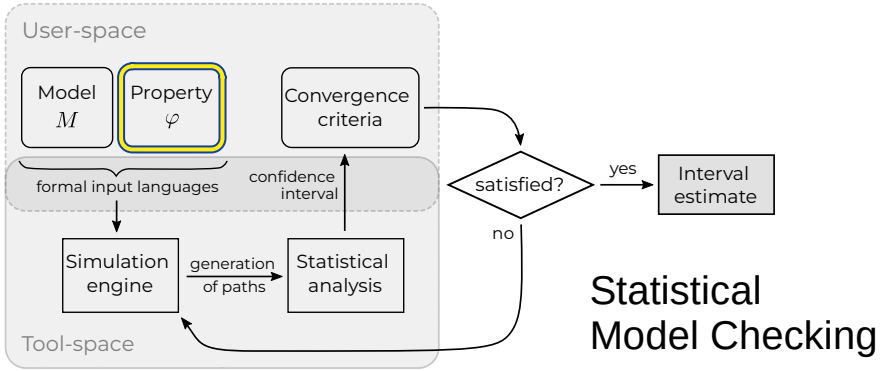


Statistical Model Checking

Model checking for security

$$M \models \varphi$$

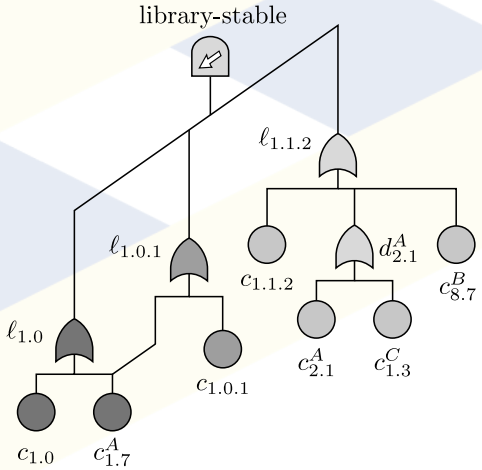
$$P(\text{unsafe}) \leqslant 0.02 \qquad \boxed{P(\text{exploit}) \leqslant 0.02}$$

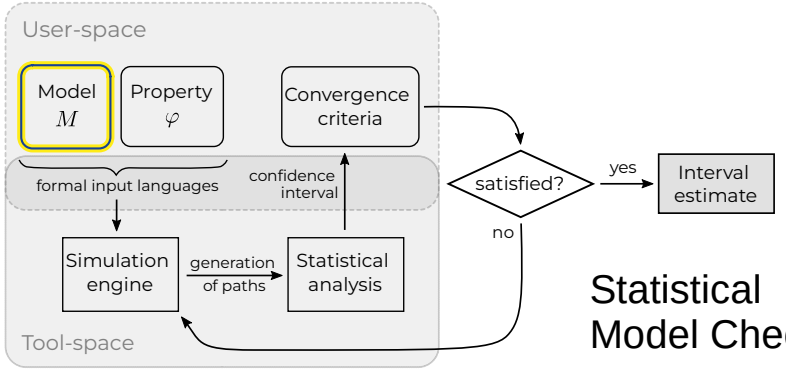


Model checking for security

$$M \models \varphi$$

$$P(\text{unsafe}) \leqslant 0.02 \qquad P(\text{exploit}) \leqslant 0.02$$





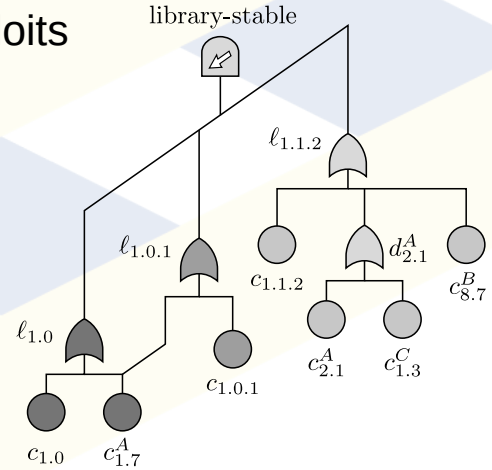
Statistical Model Checking

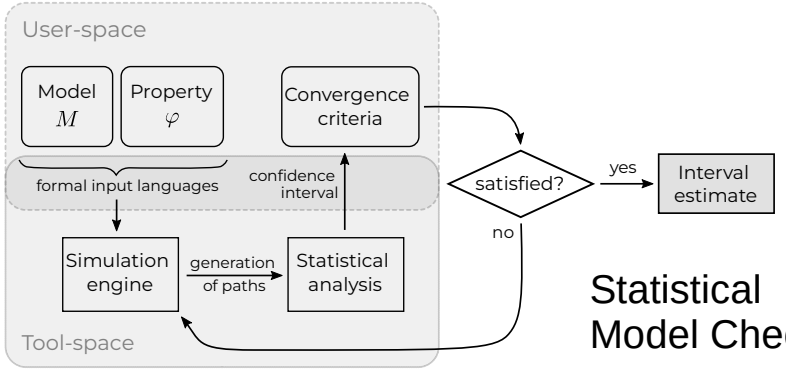
A statistical model checker for are events

$$M \models \varphi$$

$$P(\text{exploit}) \leqslant 0.02$$

Attack Trees to model exploits





Statistical Model Checking

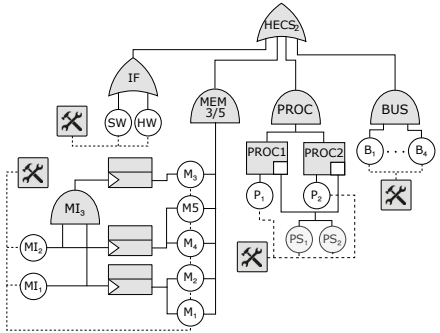
A statistical model checker for are events

Cyber Security for Europe

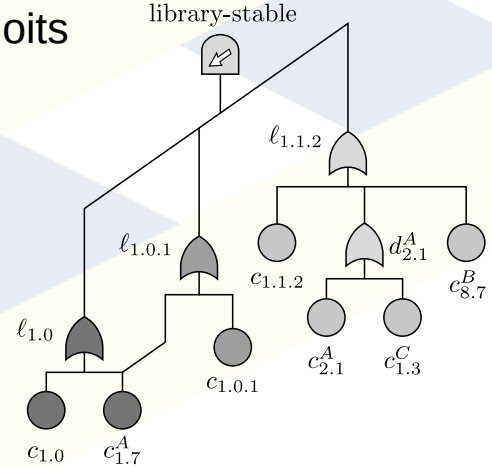
$$M \models \varphi$$

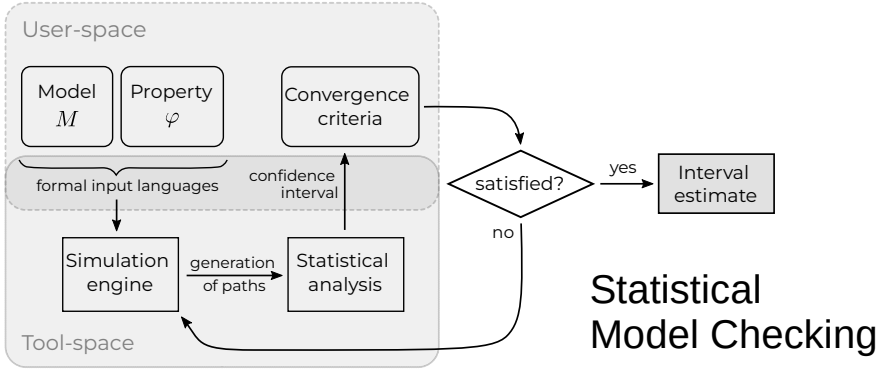
$$P(\text{exploit}) \leqslant 0.02$$

FIG



Attack Trees to model exploits





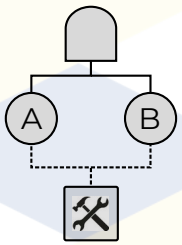
Statistical Model Checking

Cyber Security for Europe

Using statistical model checking for cybersecurity analysis

Carlos E. Budde
CS4E: Cybersecurity Skills and Capability Building (WP6)
https://webapps.unitn.it/du/en/Persona/PER0235360/Curriculum <carlosesteban.budde@unitn.it>

.bkp: FT syntax to IOSA semantics



Kepler:

```
"TLE" and "A" "B";
"A" fail~gamma(9,1) repair~exponential(6);
"B" fail~exponential(1) repair~uniform(1,2);
"R" rbox prio "A" "B";
```

f_A fail_A

r_A rep_A

f_B fail_B

r_B rep_B

Property query:

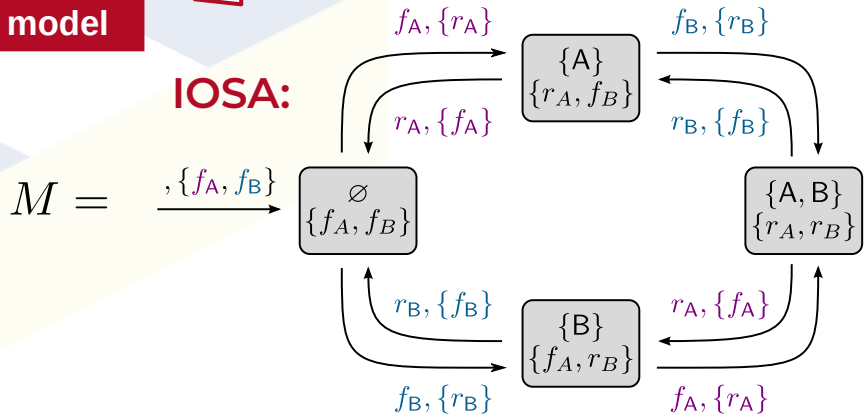
```
P( time<8 U TLE )
```

Formalise the query

$\varphi = Prob(\mathsf{A}_t \wedge \mathsf{B}_t \mid t < 8)$,
where $\mathsf{A}_t, \mathsf{B}_t$ are stochastic processes with Boolean state space

Formalise the model

IOSA:



CTMC: