Exact schedulability test for sporadic mixed-criticality real-time systems using antichains and oracles

Simon Picard, Antonio Paolillo, Gilles Geeraerts, Joël Goossens

Ourway, Vrije Universiteit Brussel, Université libre de Bruxelles

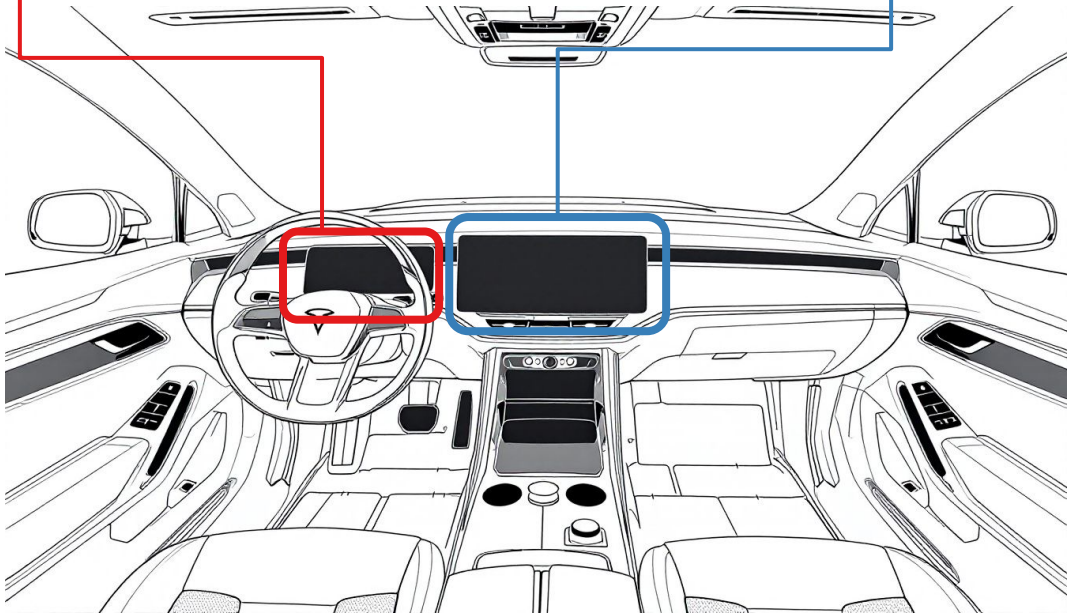
RTNS 2024, November 6-8

67 10 96 5

Introduction to mixed-criticality systems

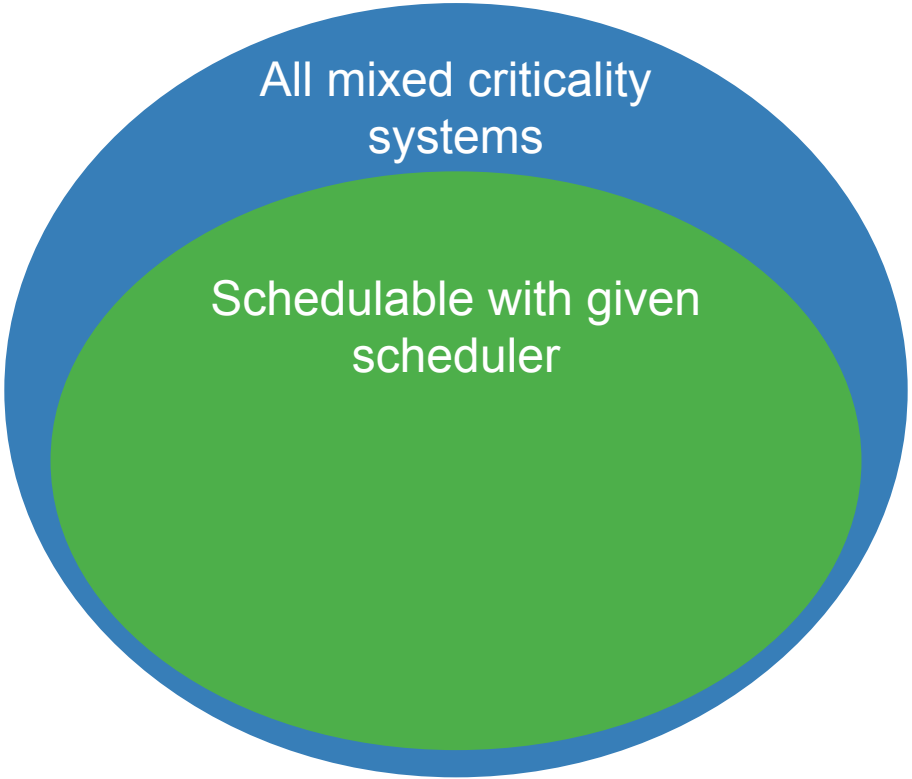
automated driving

passenger entertainment

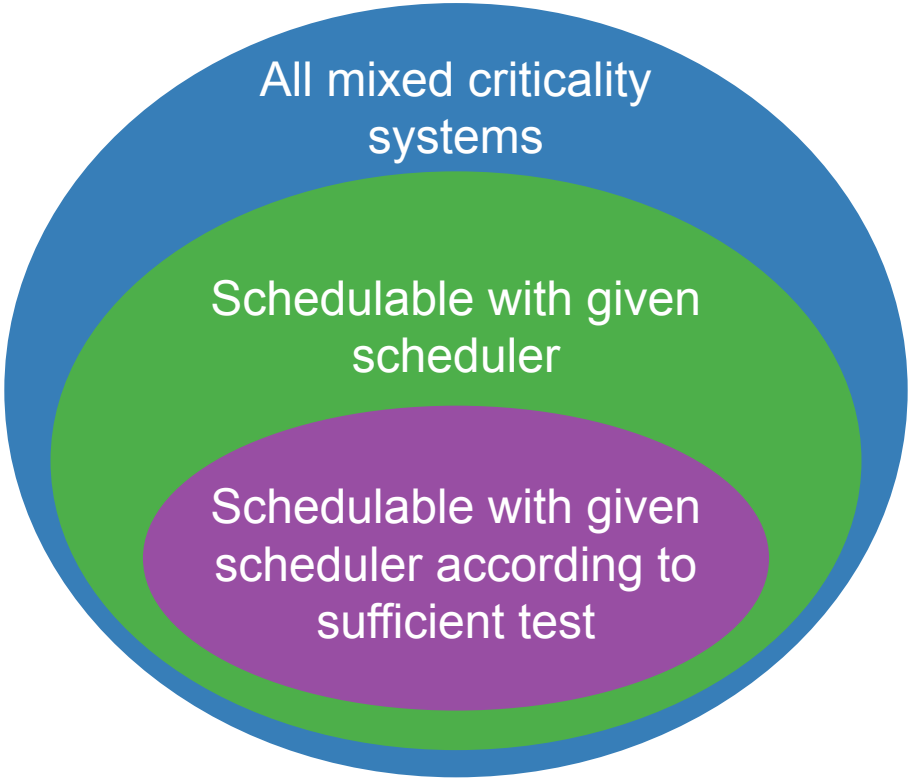


S. Vestal. Preemptive scheduling of multi-criticality systems with varying degrees of execution time assurance. 2007.

Problem statement



Problem statement



Sporadic dual-criticality systems

Task set $\tau = \{\tau_1, \tau_2, ..., \tau_n\}$

Task $\tau_i = \langle\langle L_i, T_i, D_i, C_i(LO), C_i(HI)\rangle\rangle$

L_i : criticality level (**LO** or **HI**)

T_i : minimum interarrival time (**period**) between jobs released **sporadically**

D_i : relative **deadline** (constrained)

C_i : worst-case execution time (WCET) **per criticality level**

Single processor

Lifecycle of a sporadic dual-criticality system

At each **clock tick**:

1. **Potential** job release
2. Scheduling
3. Execution
4. **Potential** completion signal
5. Possible criticality mode change

Non-deterministic job **release** and **completion** signal → **multiple scenarios**

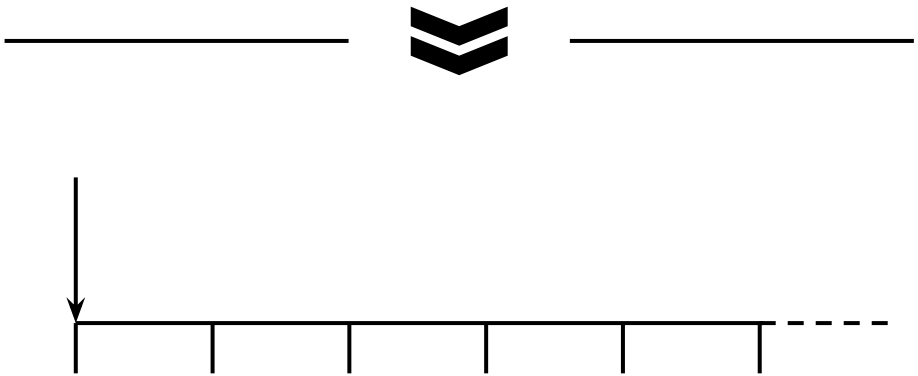
Sporadic dual-criticality task chronogram

	C(LO)	C(HI)	D	T	L
τ_1	2	3	3	4	HI

Sporadic dual-criticality task chronogram

↓ : release

	C(LO)	C(HI)	D	T	L
τ_1	2	3	3	4	HI

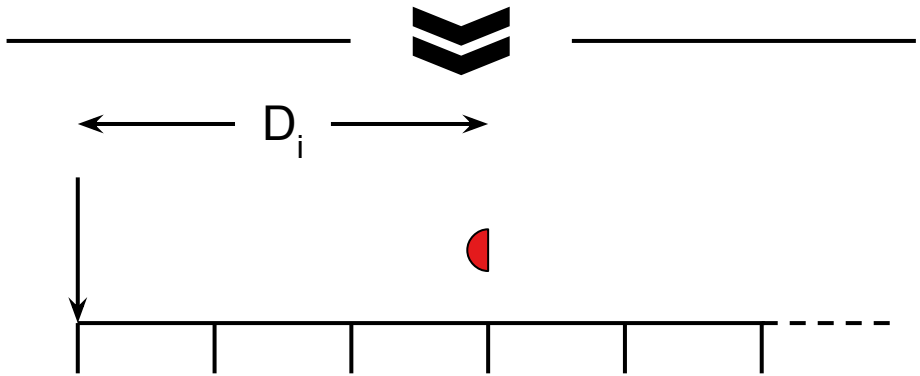


Sporadic dual-criticality task chronogram

: release

: absolute deadline

	C(LO)	C(HI)	D	T	L
τ_1	2	3	3	4	HI



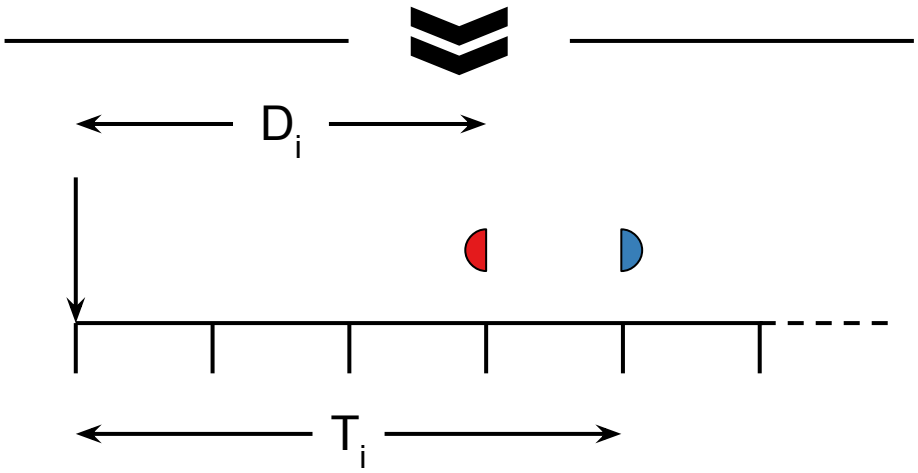
Sporadic dual-criticality task chronogram

: release

: absolute deadline

: earliest next arrival time

	C(LO)	C(HI)	D	T	L
τ_1	2	3	3	4	HI



Sporadic dual-criticality task chronogram

: release

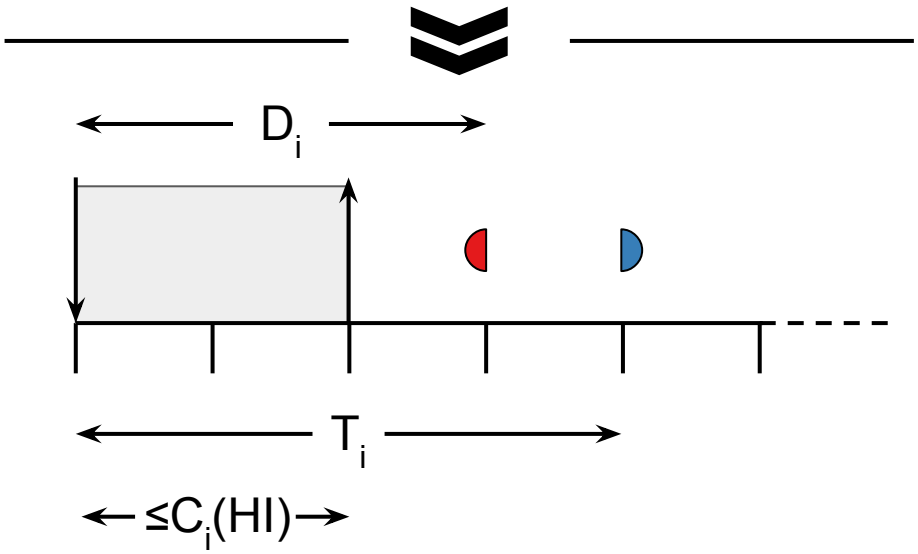
: absolute deadline

: earliest next arrival time

: execution

: completion signal

	C(LO)	C(HI)	D	T	L
τ_1	2	3	3	4	HI

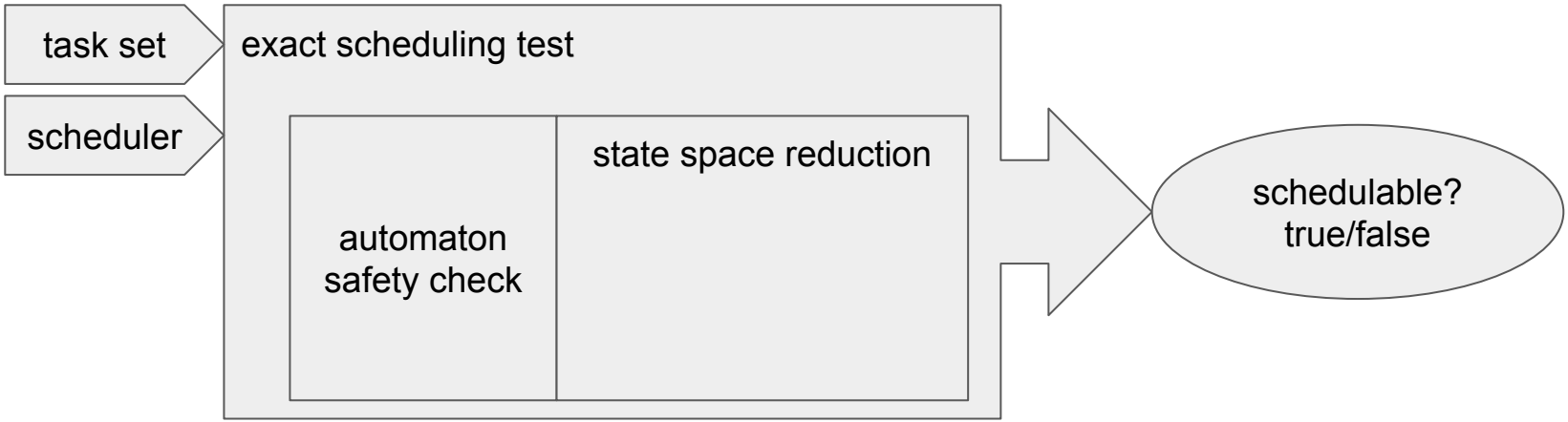


Objective of the work

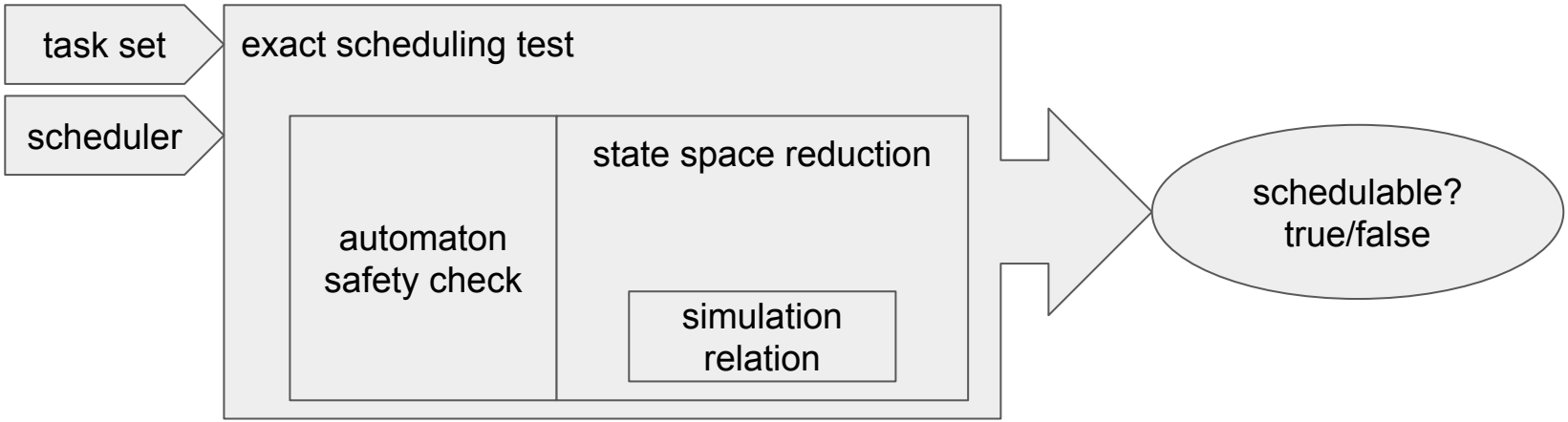
Objective of the work

Theodore P. Baker and Michele Cirinei. 2007. Brute-Force Determination of Multiprocessor Schedulability for Sets of Sporadic Hard-Deadline Tasks.

Objective of the work

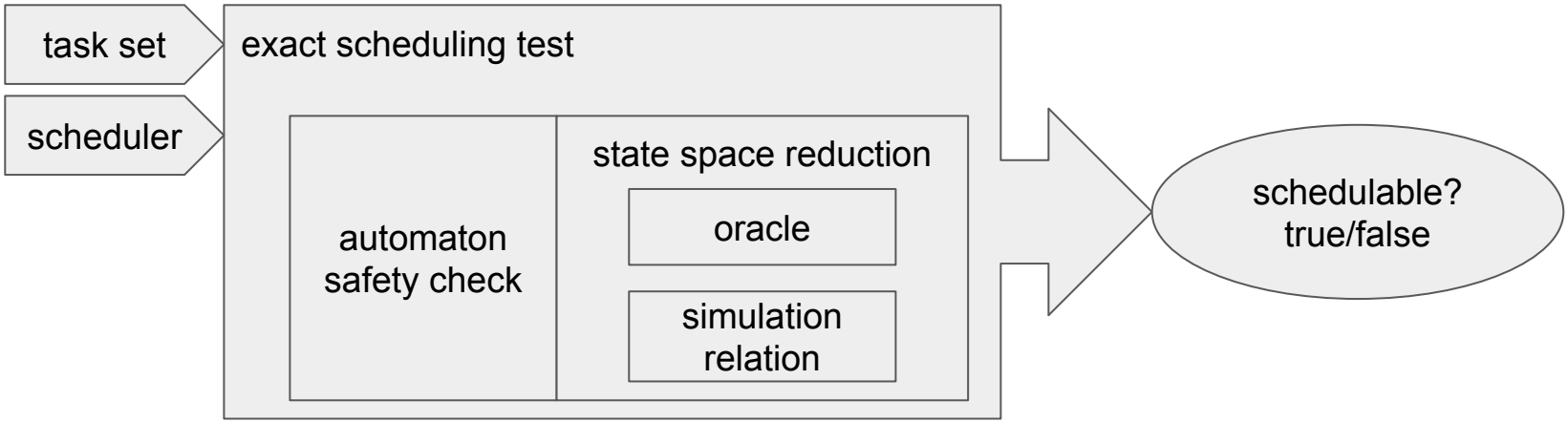


Objective of the work

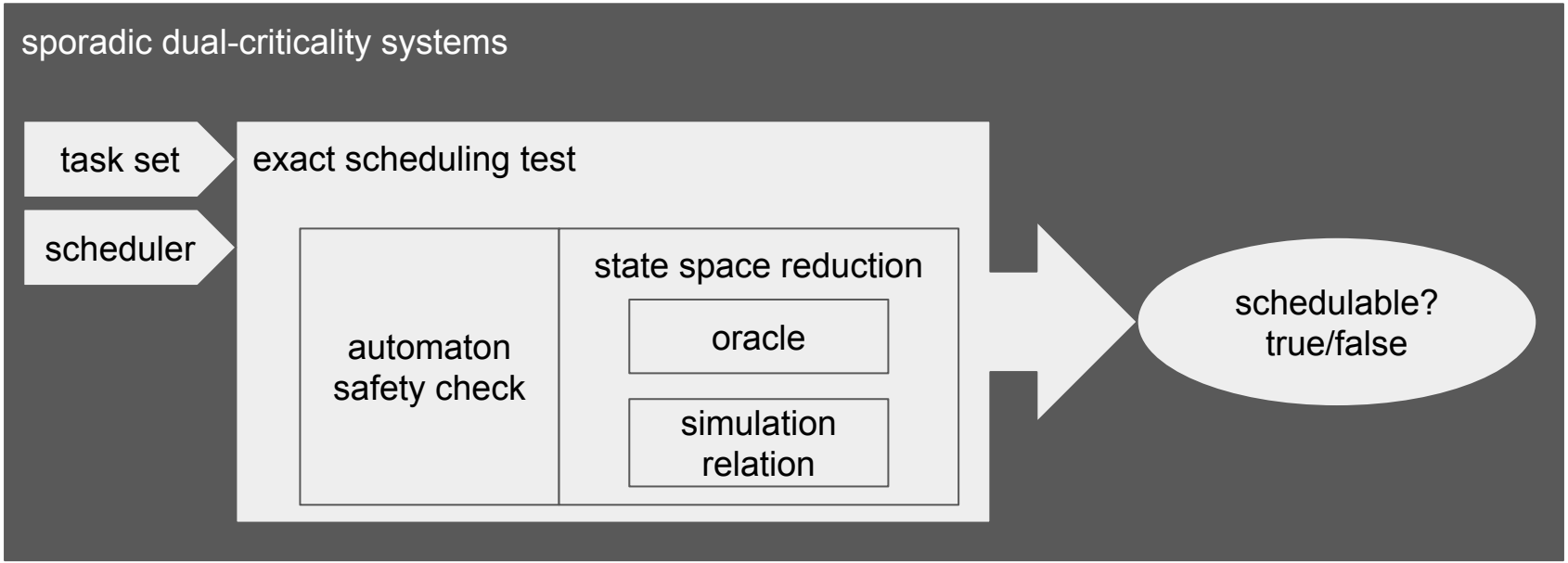


Markus Lindström, Gilles Geeraerts, and Joël Goossens. 2011. A faster exact multiprocessor schedulability test for sporadic tasks.

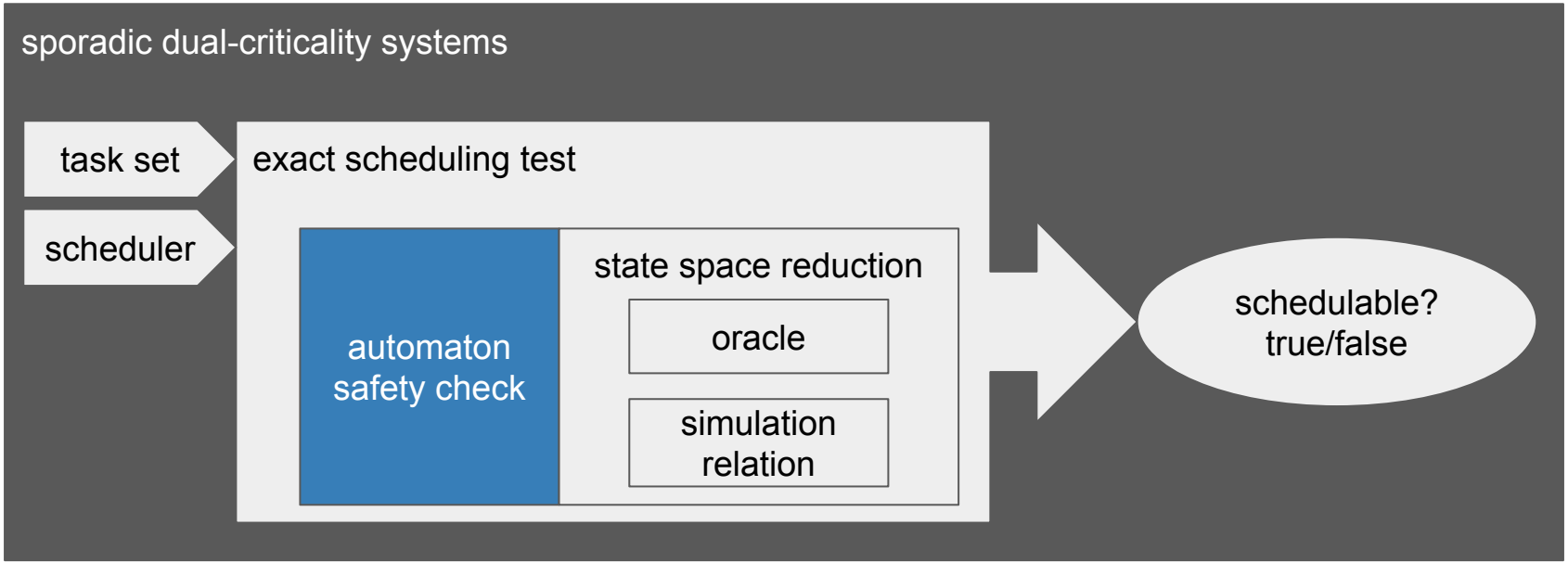
Objective of the work



Objective of the work

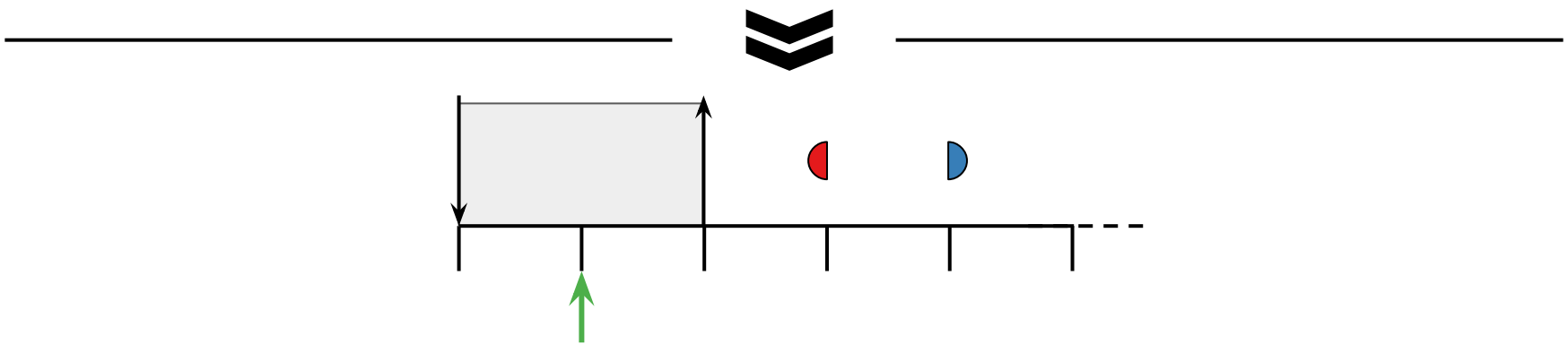


Objective of the work



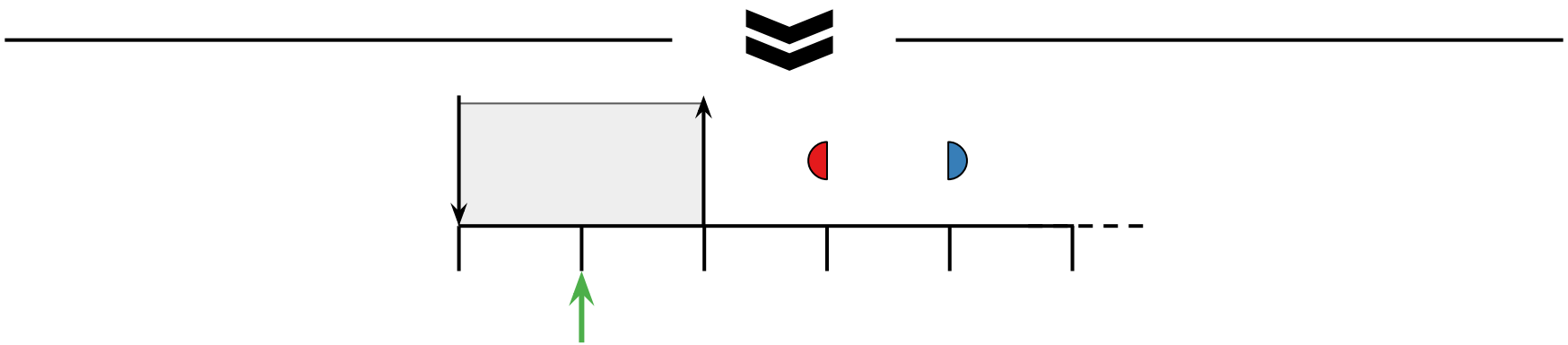
States of the automaton

	C(LO)	C(HI)	D	T	L
τ_1	2	3	3	4	HI



Criticality (cri)

	C(LO)	C(HI)	D	T	L
τ_1	2	3	3	4	HI

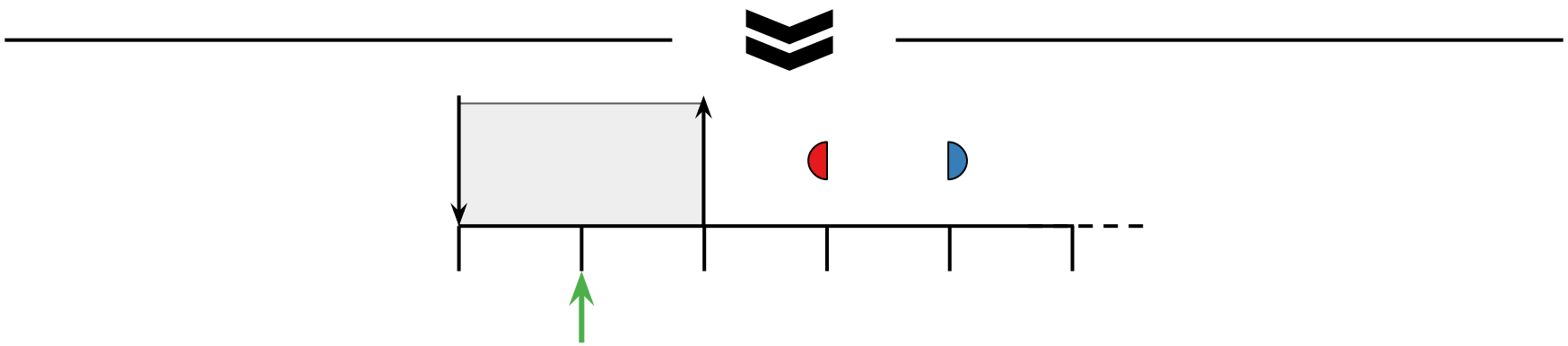


cri = HI if a mode change happened, LO otherwise

cri = LO

Next Arrival Time (nat)

	C(LO)	C(HI)	D	T	L
τ_1	2	3	3	4	HI

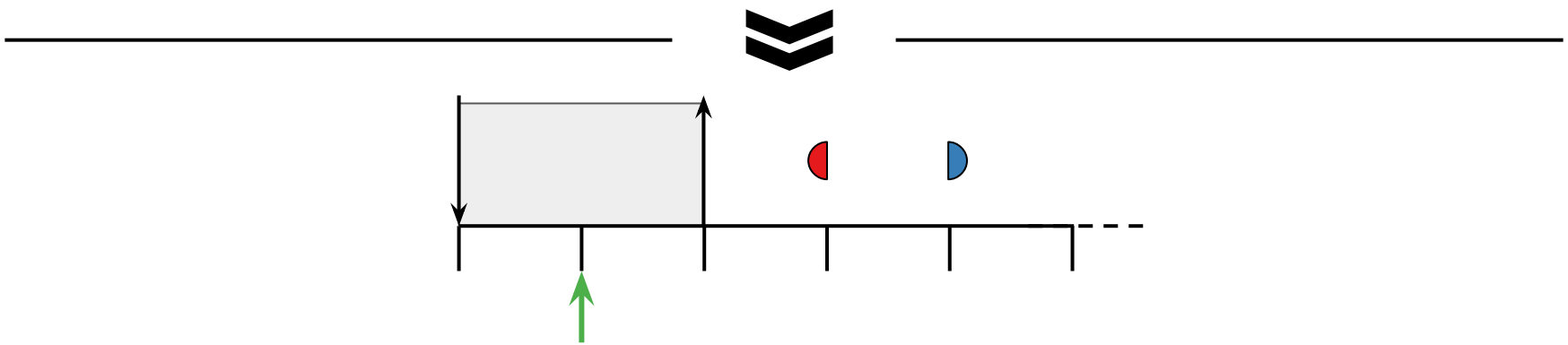


nat =

nat = 3

Remaining Computing Time (rct) for the current criticality

	C(LO)	C(HI)	D	T	L
τ_1	2	3	3	4	HI

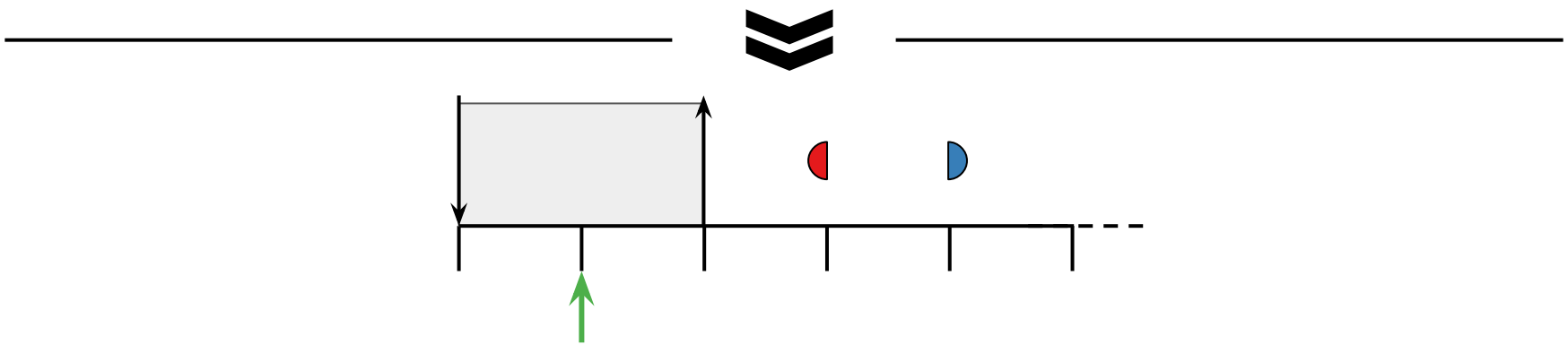


rct = - |——| + C(cri)

rct = - 1 + 2 = 1

States of the automaton

	C(LO)	C(HI)	D	T	L
τ_1	2	3	3	4	HI

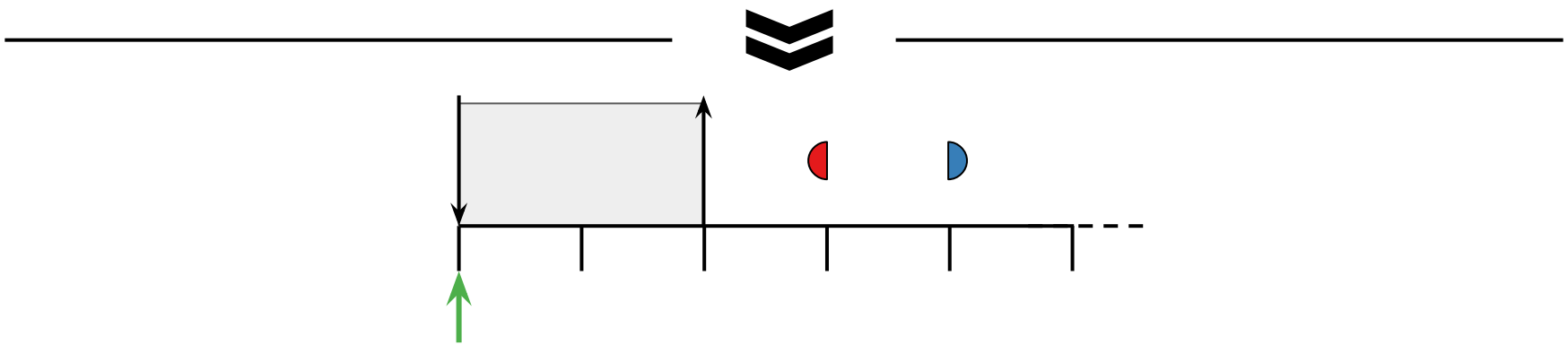


cri (rct_i, nat_i)

LO (1, 3)

From chronogram to path

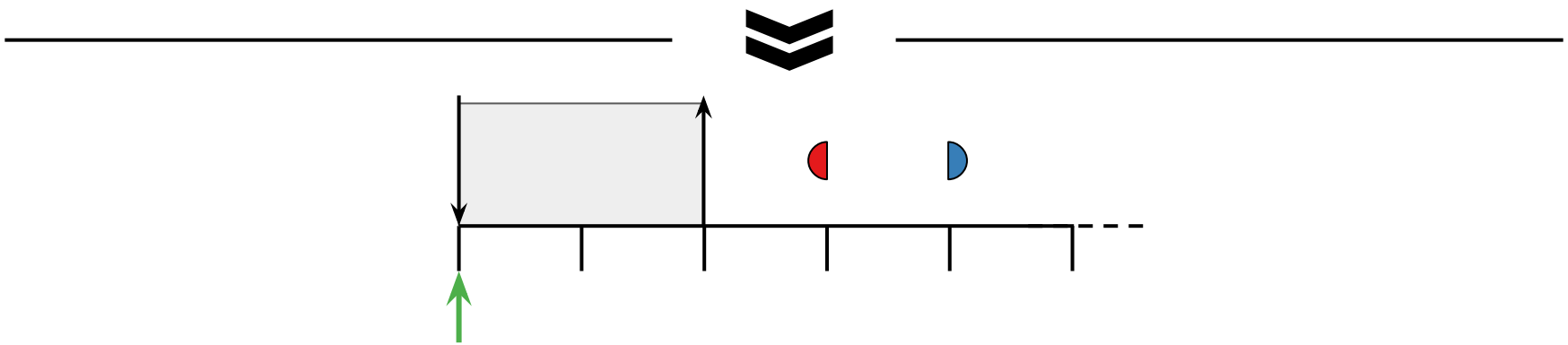
	C(LO)	C(HI)	D	T	L
τ_1	2	3	3	4	HI



cri
(rct_1, nat_1)

From chronogram to path

	C(LO)	C(HI)	D	T	L
τ_1	2	3	3	4	HI

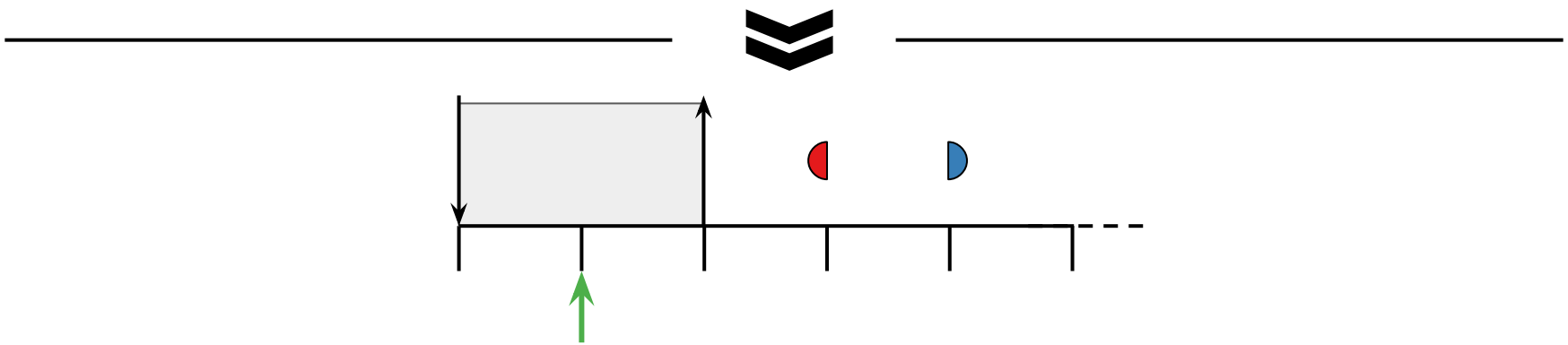


cri
(rct_1, nat_1)

LO
(0, 0)

From chronogram to path

	C(LO)	C(HI)	D	T	L
τ_1	2	3	3	4	HI



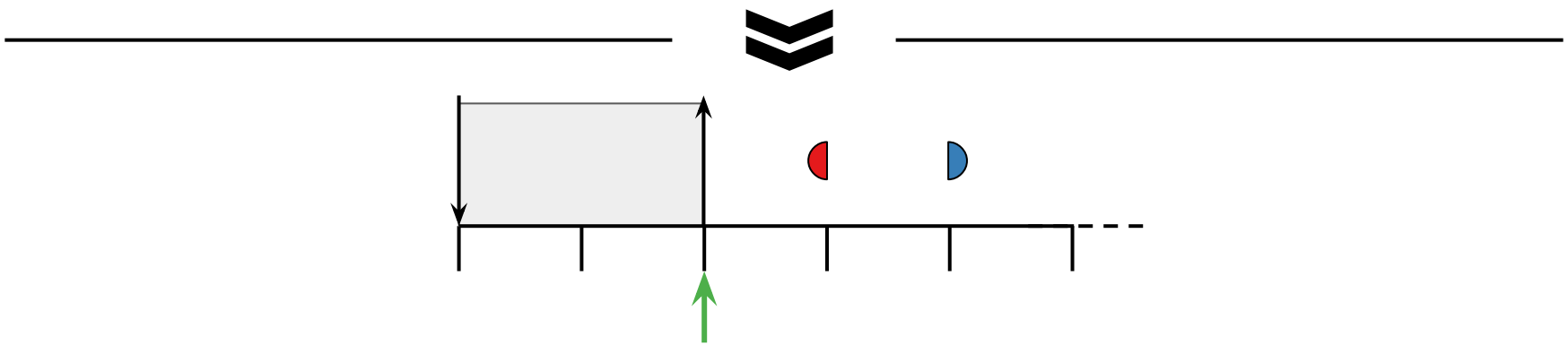
cri
(rct_1, nat_1)

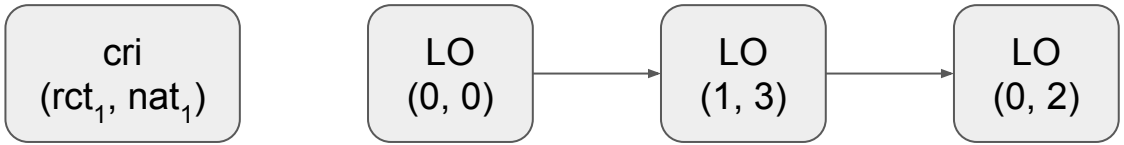
LO
(0, 0)

LO
(1, 3)

From chronogram to path

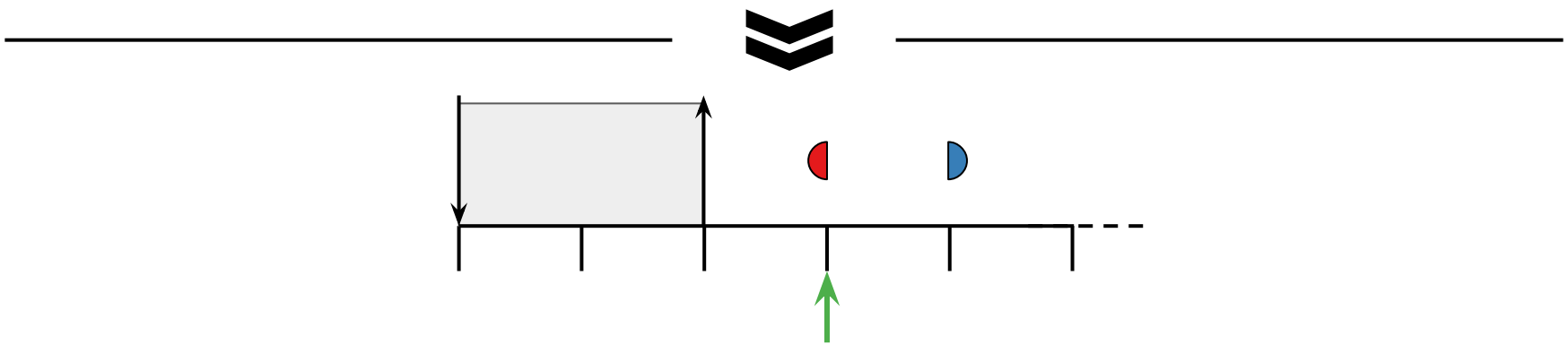
	C(LO)	C(HI)	D	T	L
τ_1	2	3	3	4	HI

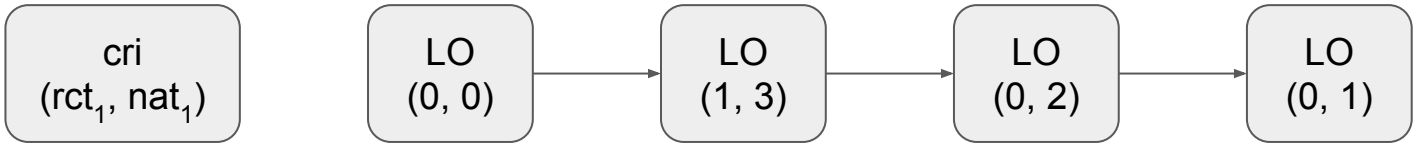




From chronogram to path

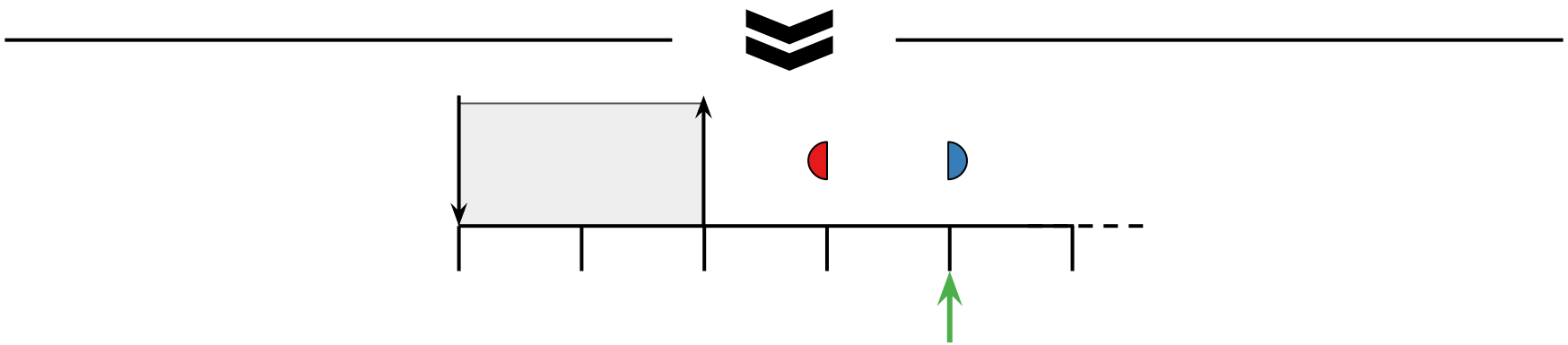
	C(LO)	C(HI)	D	T	L
τ_1	2	3	3	4	HI





From chronogram to path

	C(LO)	C(HI)	D	T	L
τ_1	2	3	3	4	HI



cri
(rct_1, nat_1)

LO
(0, 0)

LO
(1, 3)

LO
(0, 2)

LO
(0, 1)

LO
(0, 0)

From task set and scheduler to automaton

	τ_1
C(LO)	2
C(HI)	3
D	3
T	4
L	HI

From task set and scheduler to automaton

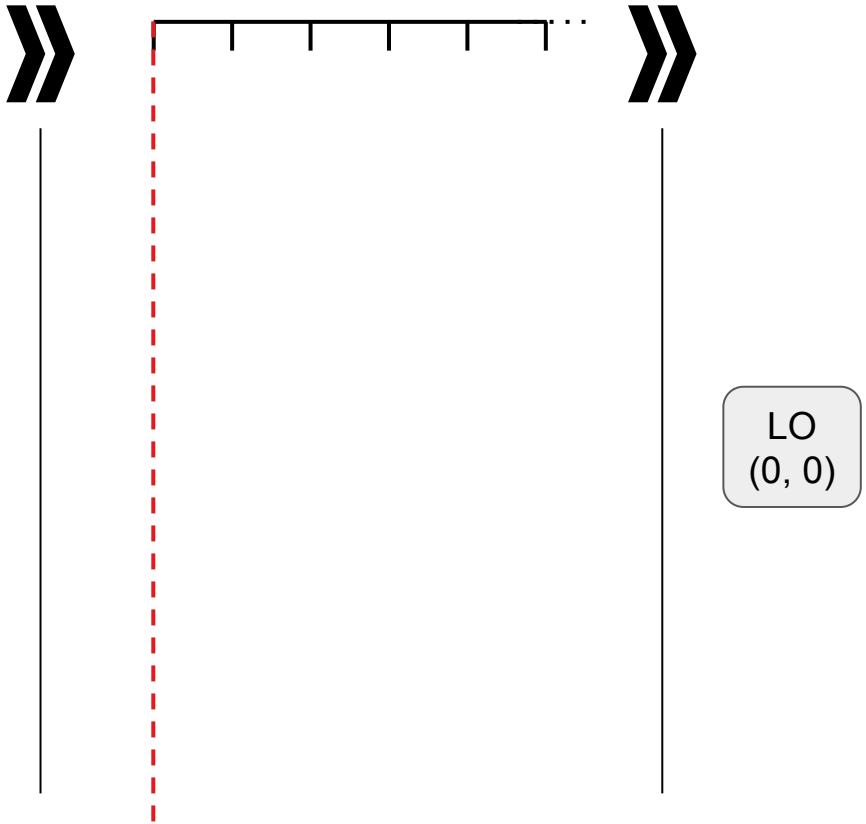
	τ_1
C(LO)	2
C(HI)	3
D	3
T	4
L	HI

EDF-VD

From task set and scheduler to automaton

	τ_1
C(LO)	2
C(HI)	3
D	3
T	4
L	HI

EDF-VD

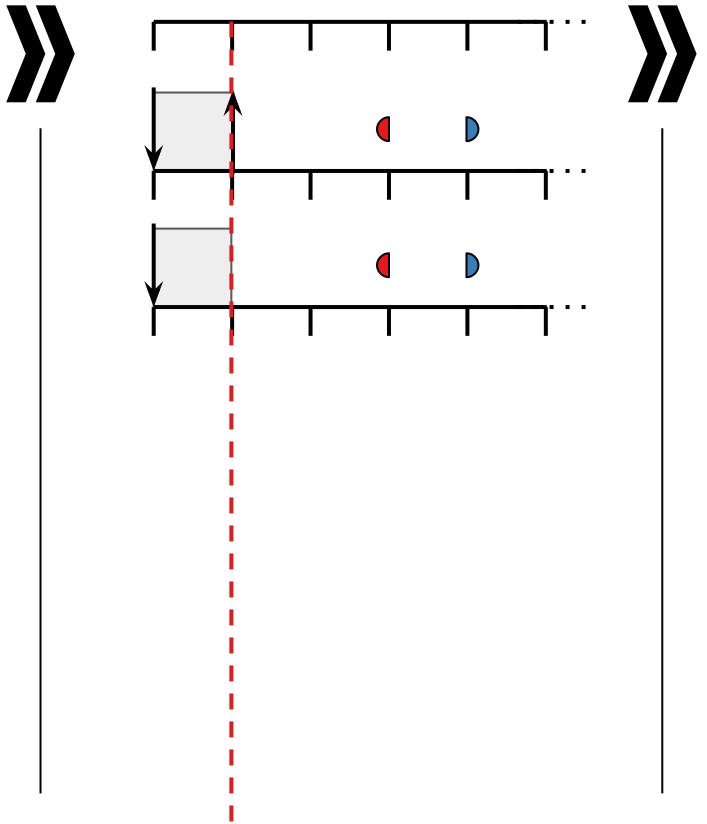


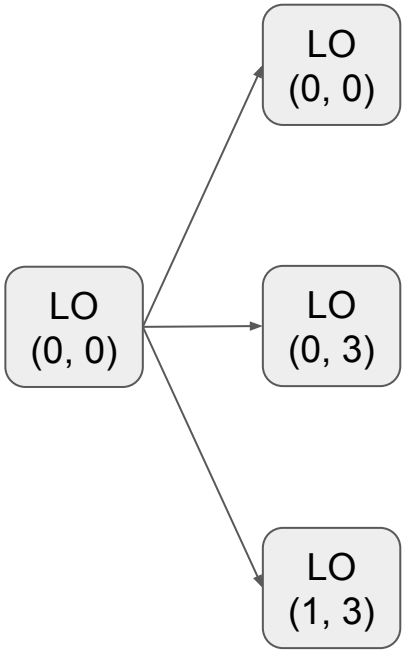
LO
(0, 0)

From task set and scheduler to automaton

	τ_1
C(LO)	2
C(HI)	3
D	3
T	4
L	HI

EDF-VD

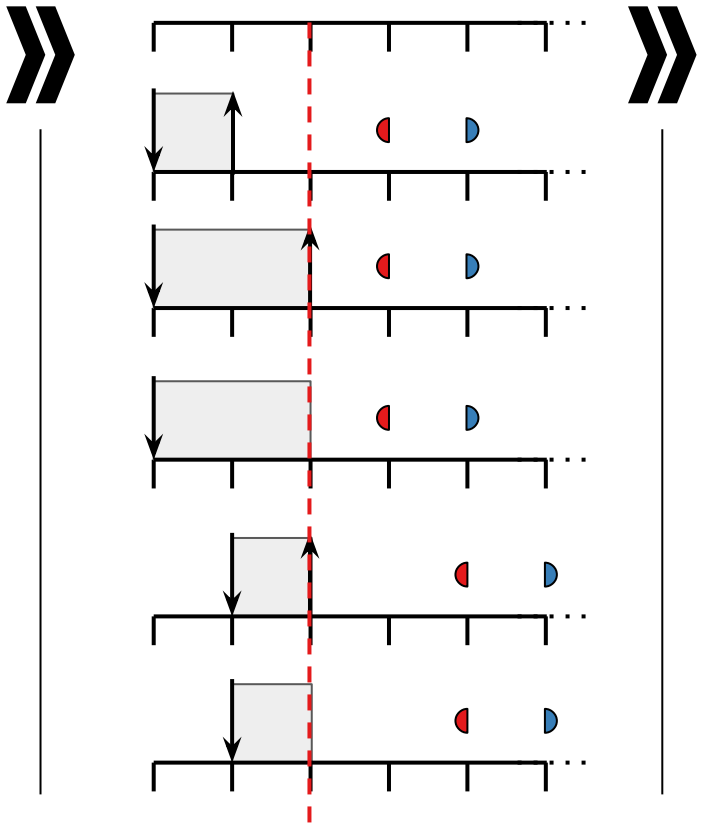


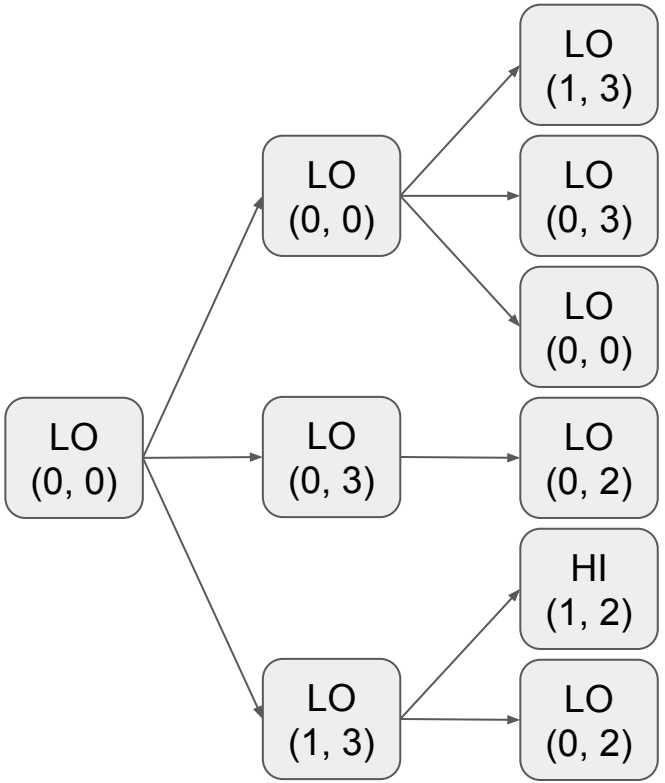


From task set and scheduler to automaton

	τ_1
C(LO)	2
C(HI)	3
D	3
T	4
L	HI

EDF-VD

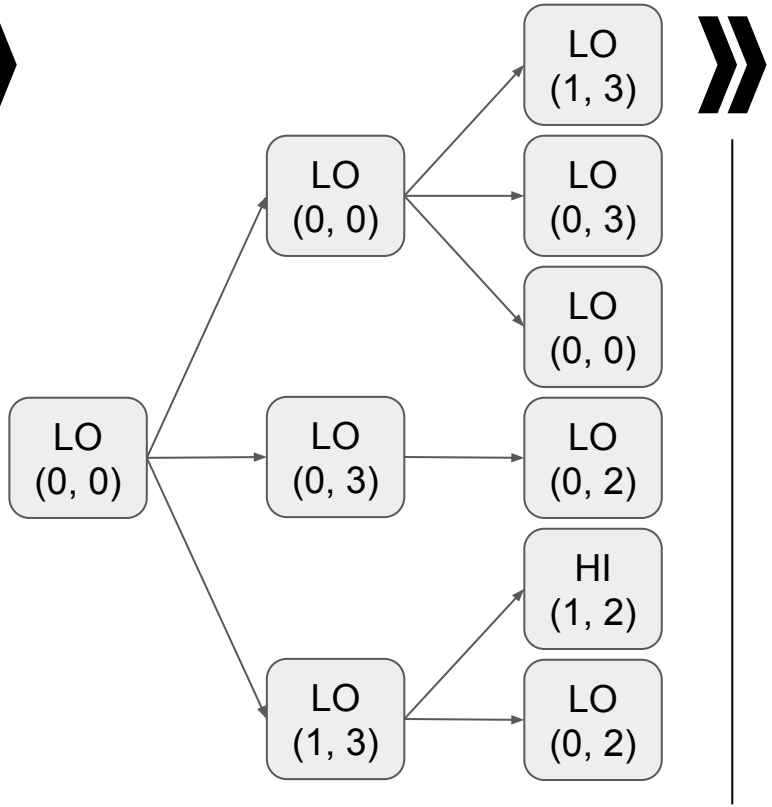


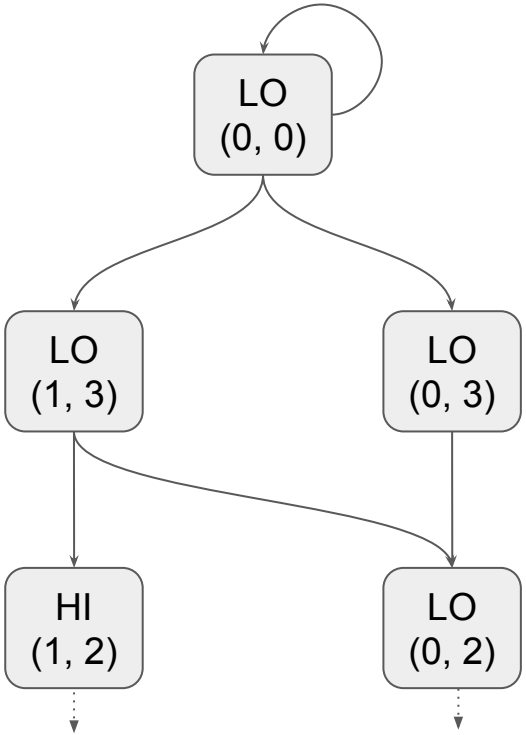


From task set and scheduler to automaton

	τ_1
C(LO)	2
C(HI)	3
D	3
T	4
L	HI

EDF-VD

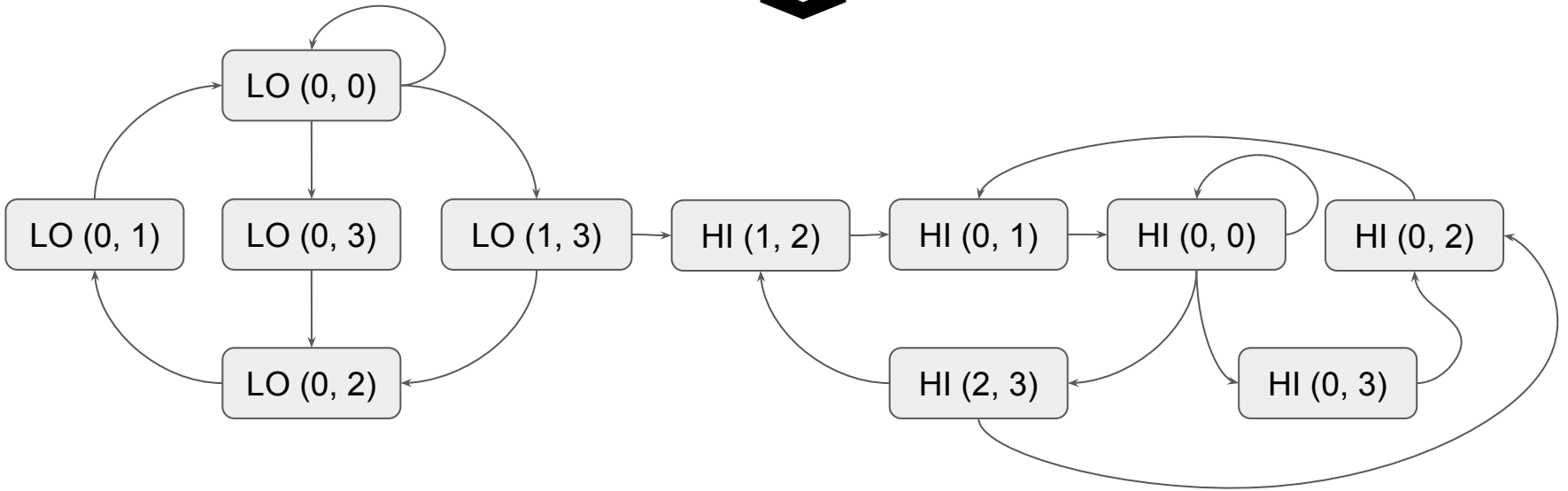




From task set and scheduler to automaton

	C(LO)	C(HI)	D	T	L
τ_1	2	3	3	4	HI

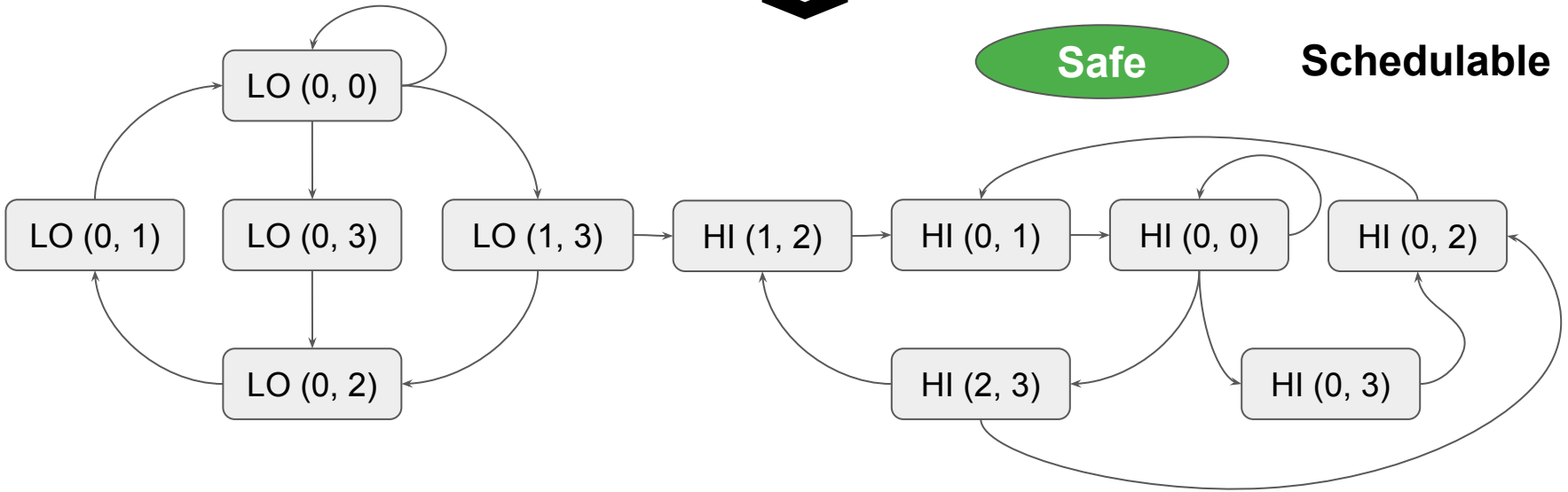
EDF-VD



From task set and scheduler to automaton

	C(LO)	C(HI)	D	T	L
τ_1	2	3	3	4	HI

EDF-VD



Safe

Schedulable

Unschedulable task set

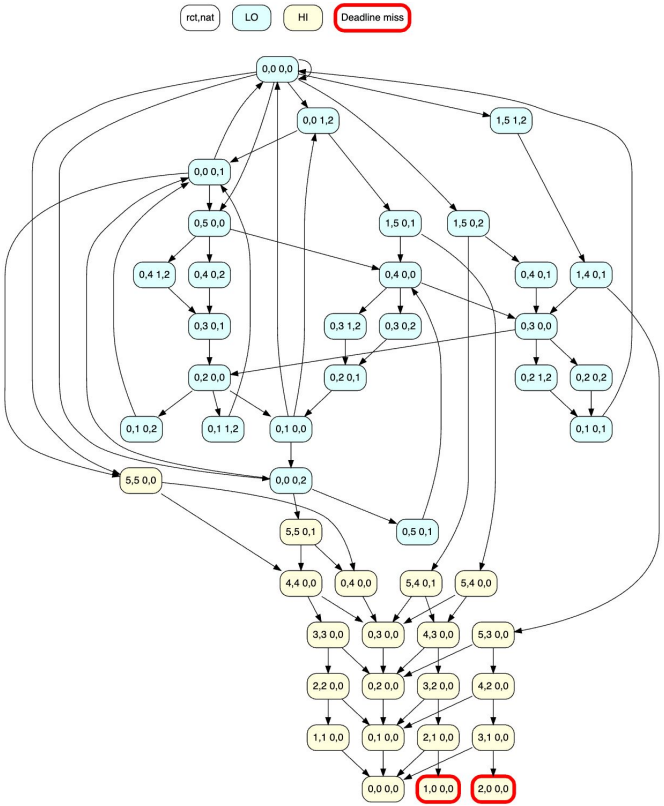
	τ_1	τ_2
C(LO)	1	2
C(HI)	6	2
D	6	3
T	6	3
L	HI	LO

EDF-VD

Unschedulable task set

	τ_1	τ_2
C(LO)	1	2
C(HI)	6	2
D	6	3
T	6	3
L	HI	LO

EDF-VD



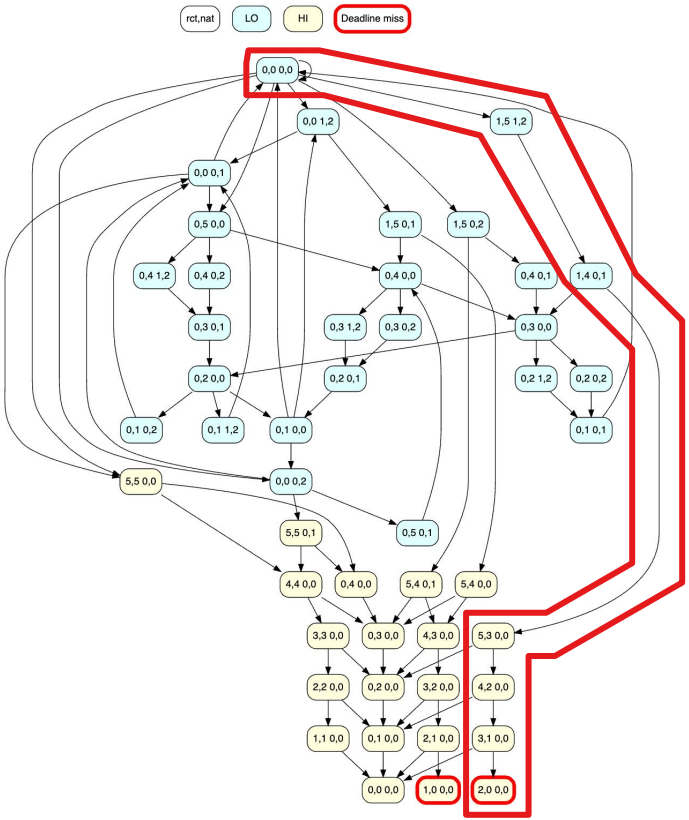
Unsafe

Unschedulable

Unschedulable task set

	τ_1	τ_2
C(LO)	1	2
C(HI)	6	2
D	6	3
T	6	3
L	HI	LO

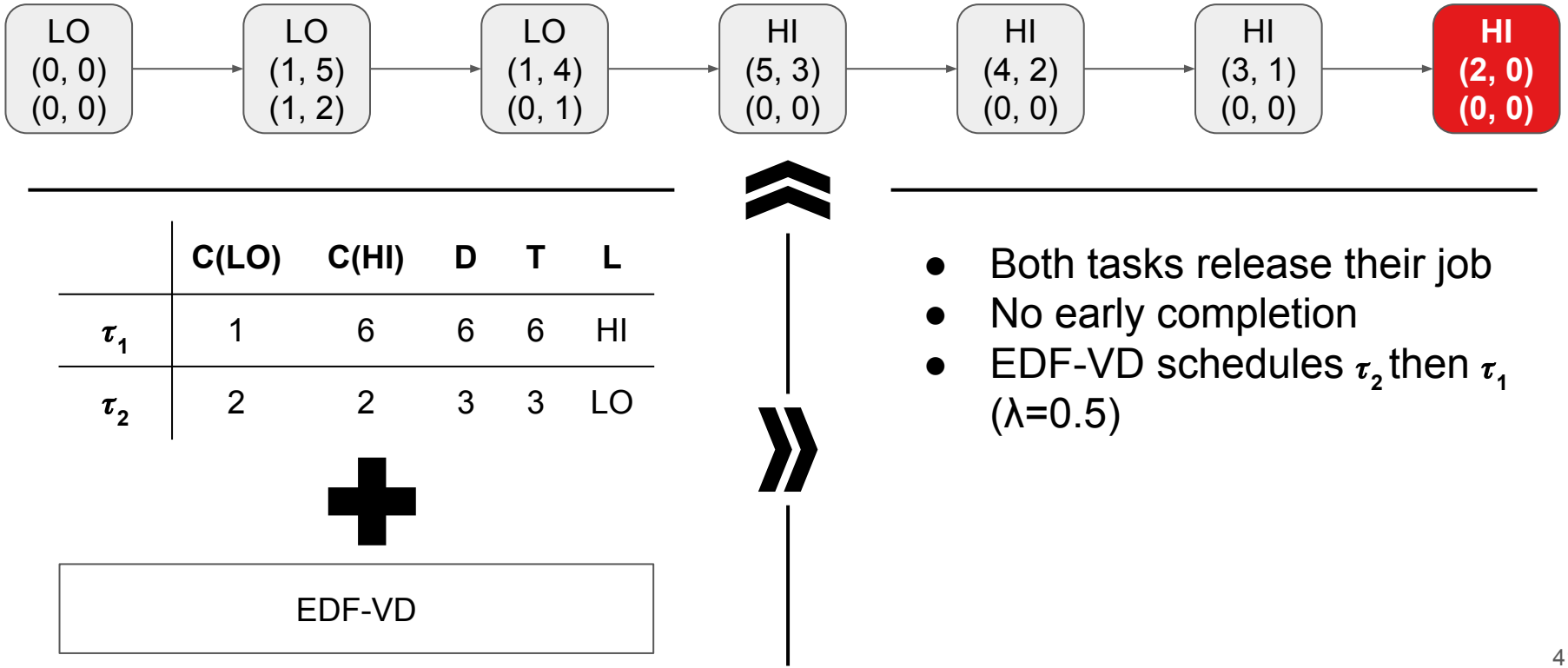
EDF-VD



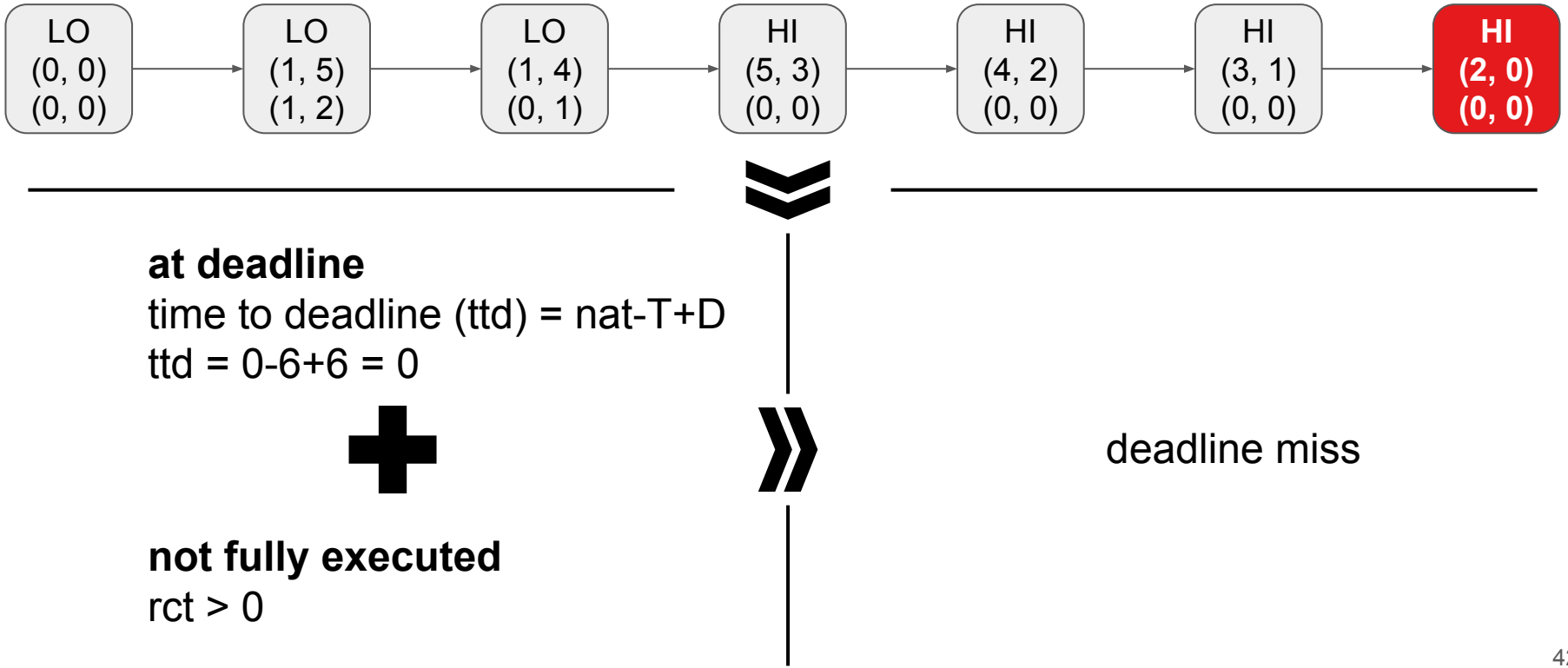
Unsafe

Unschedulable

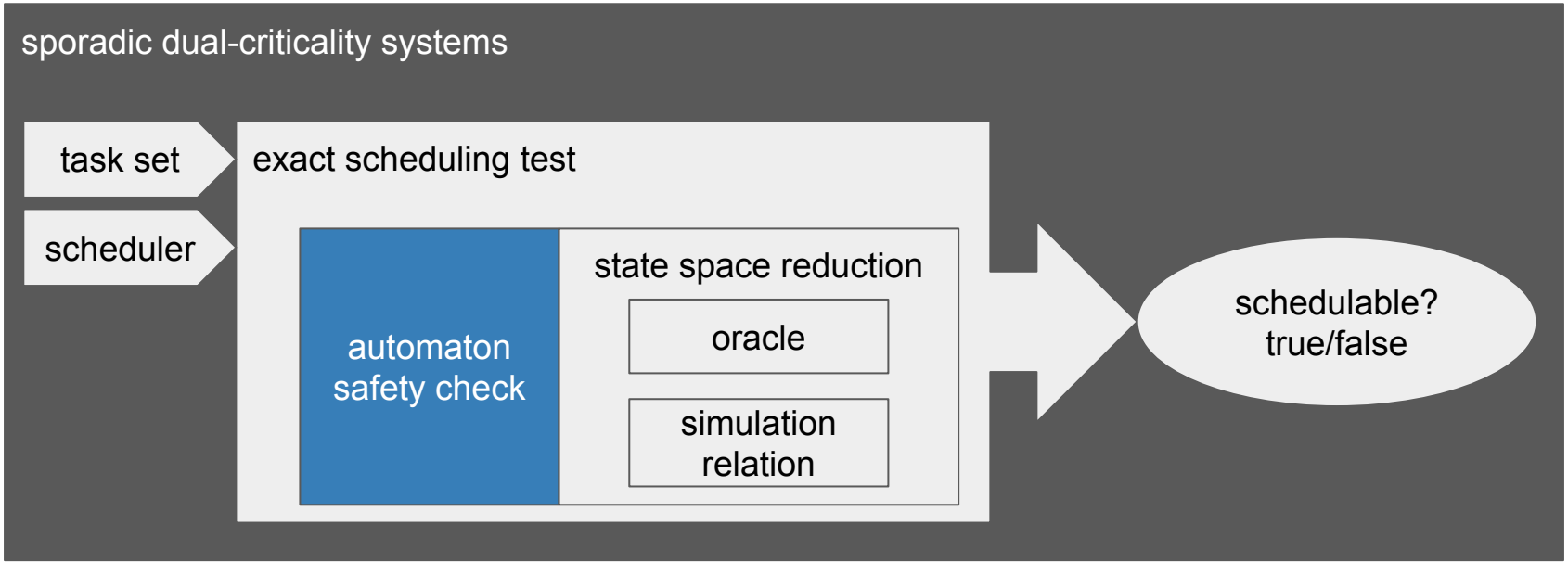
Encountering a deadline miss (with EDF-VD)



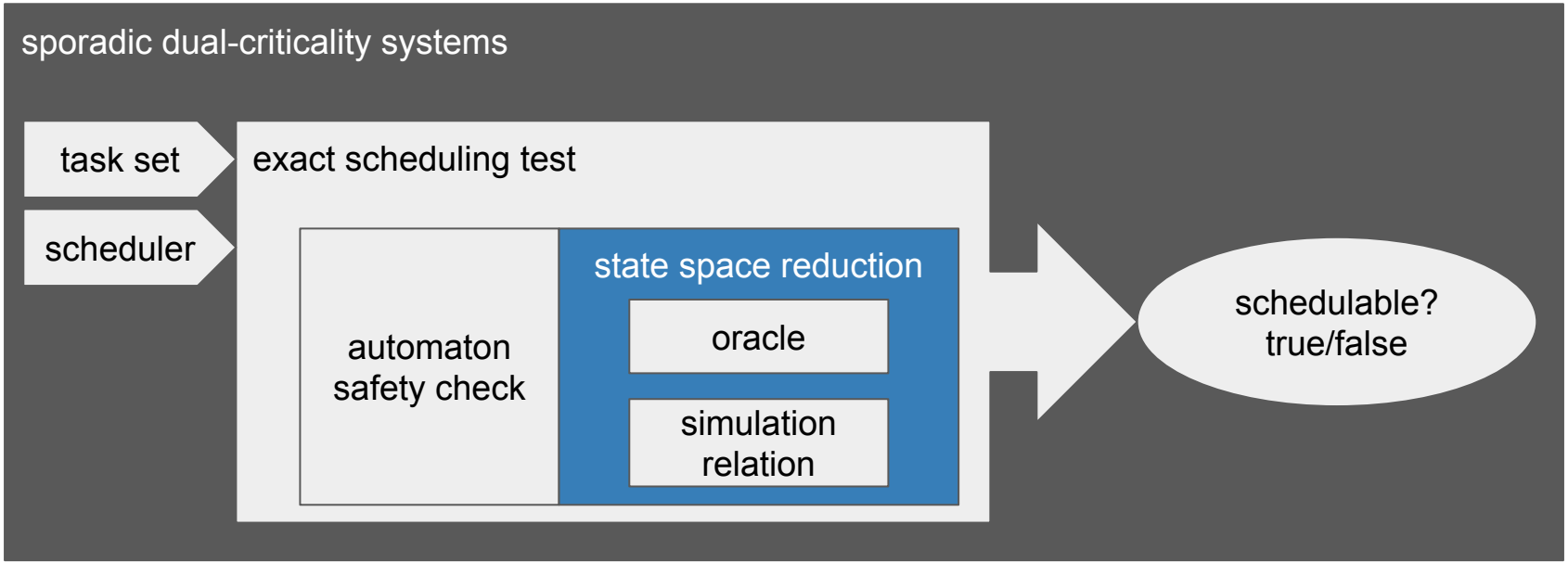
Encountering a deadline miss (with EDF-VD)



Objective of the work



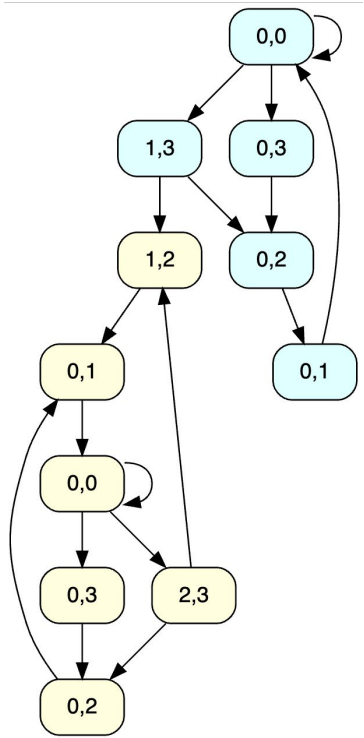
Objective of the work



State space exponential on the number of tasks

1 task

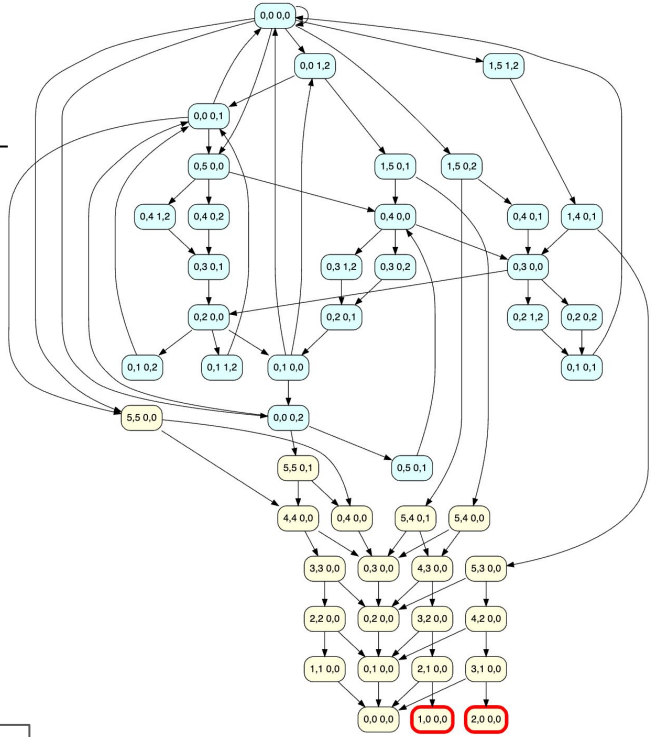
	τ_1
C(LO)	2
C(HI)	3
D	3
T	4
L	HI



EDF-VD

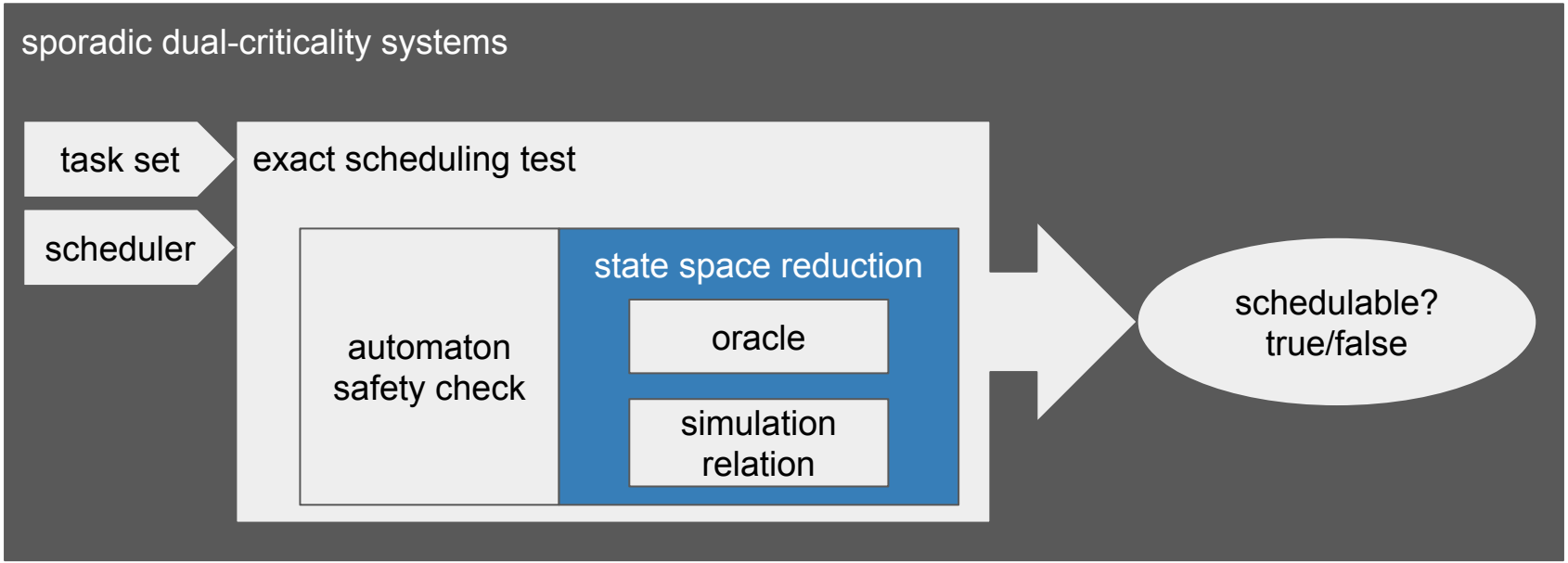
2 tasks

	τ_1	τ_2
C(LO)	1	2
C(HI)	6	2
D	6	3
T	6	3
L	HI	LO

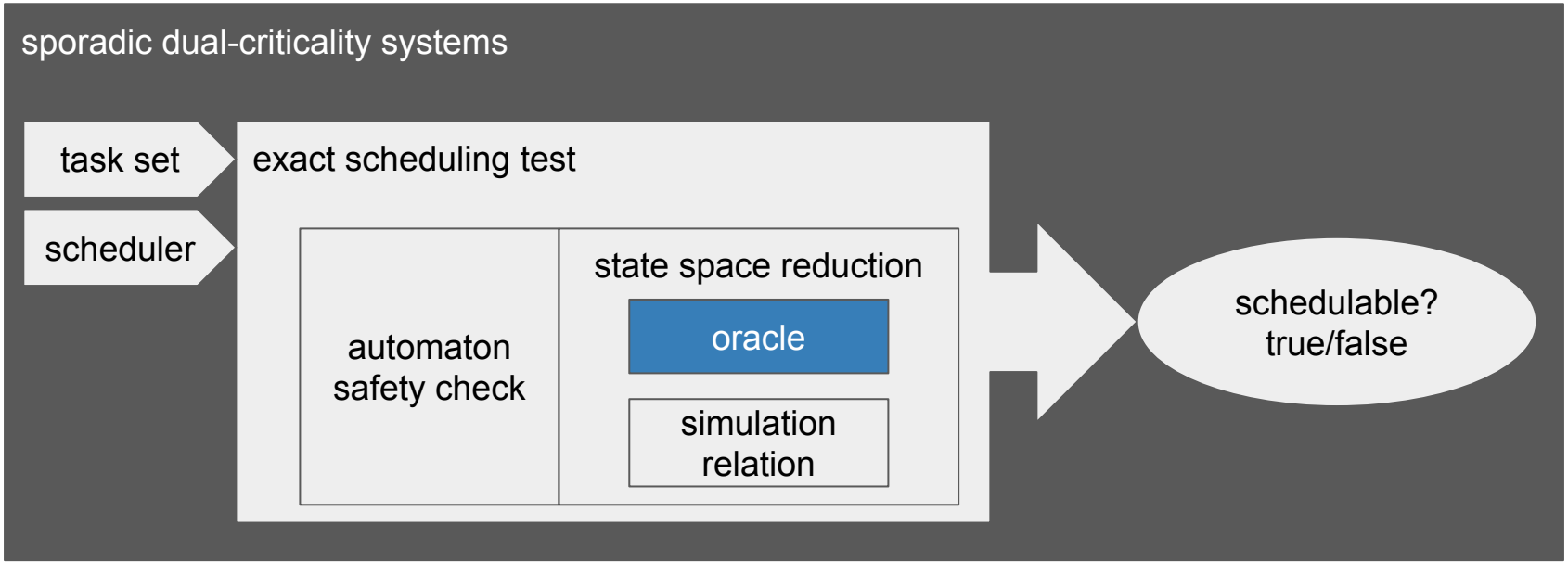


EDF-VD

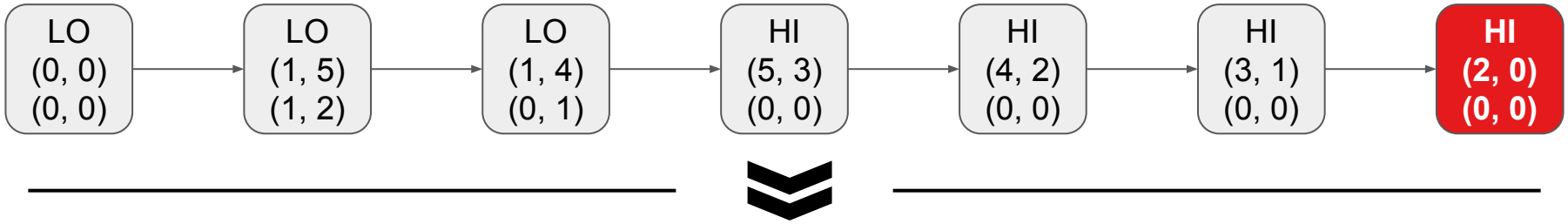
Objective of the work



Objective of the work

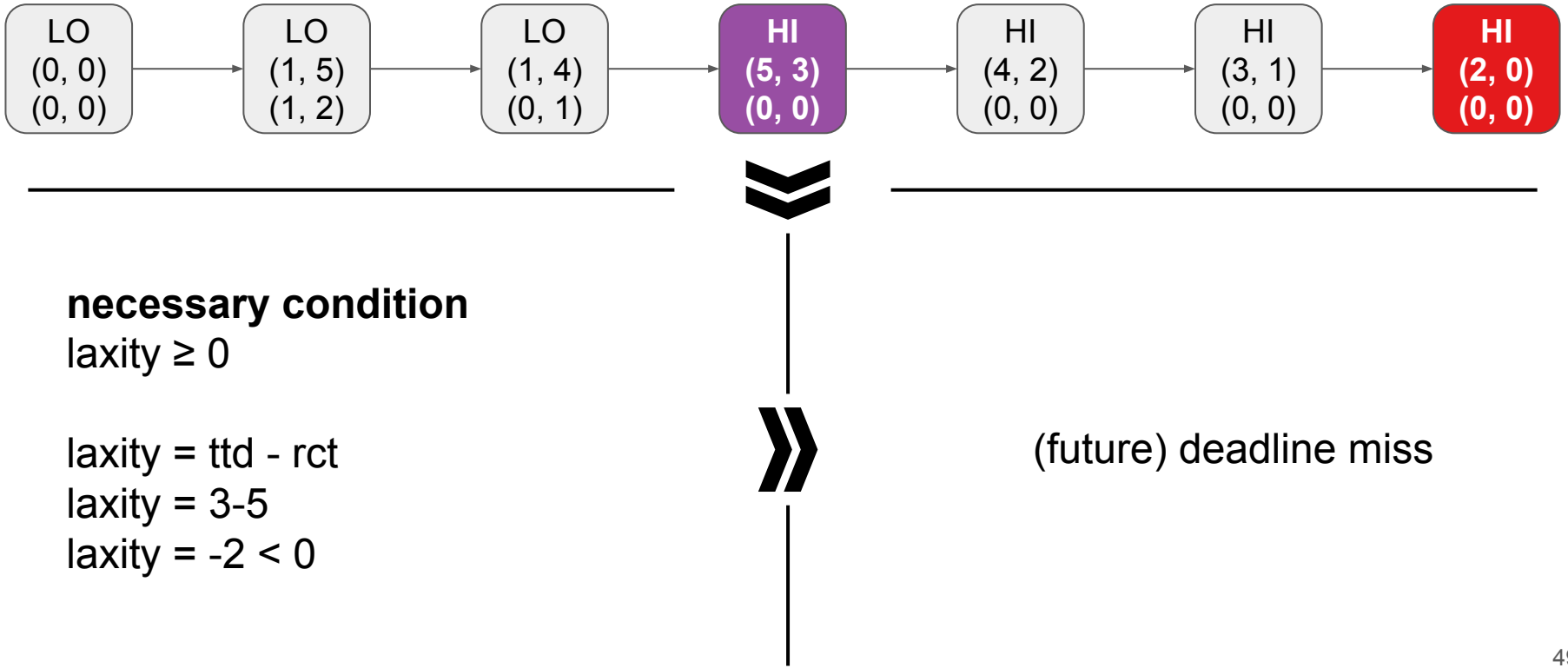


Encountering a deadline miss (with EDF-VD)

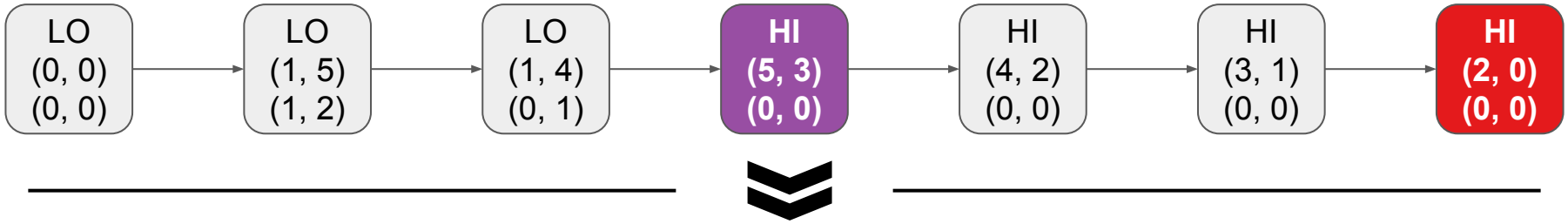


Can an **oracle predict** a future deadline miss?

Necessary condition to predict deadline miss (oracle)

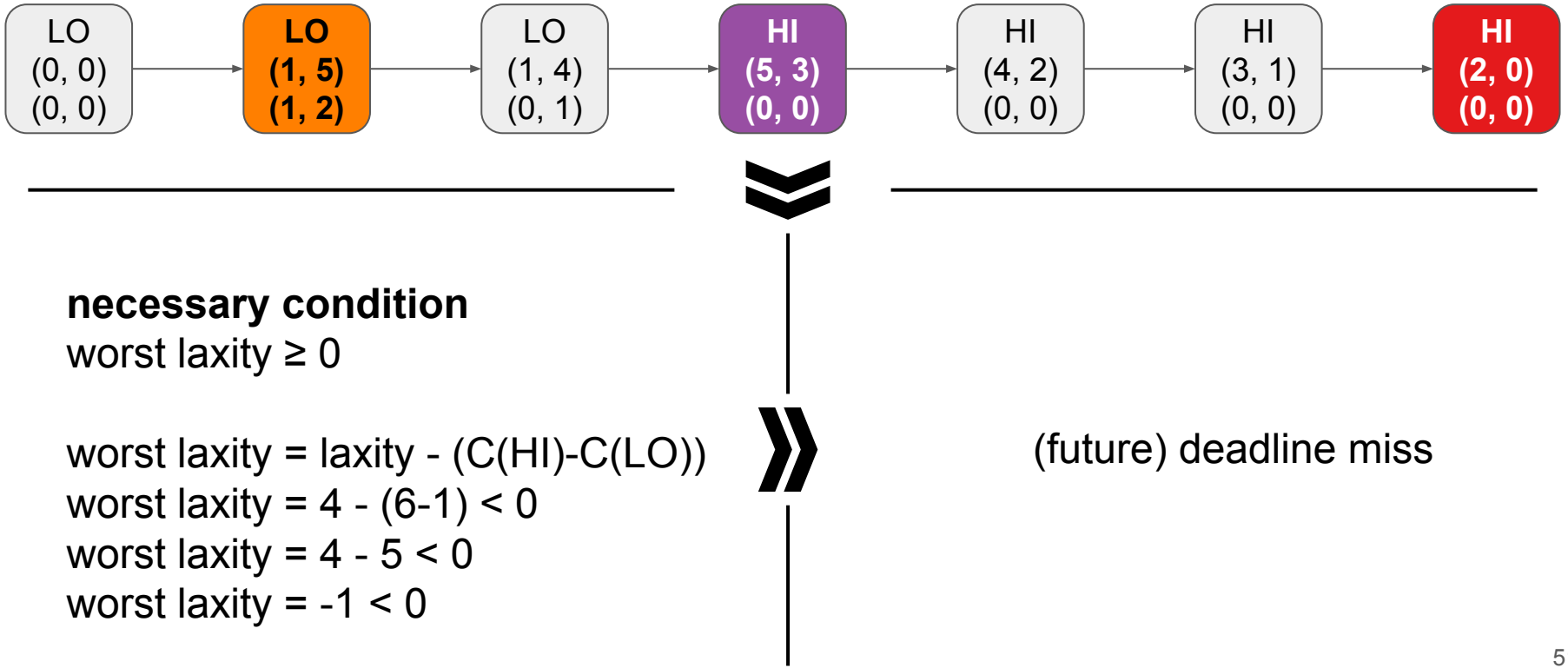


Predicting the deadline miss earlier?

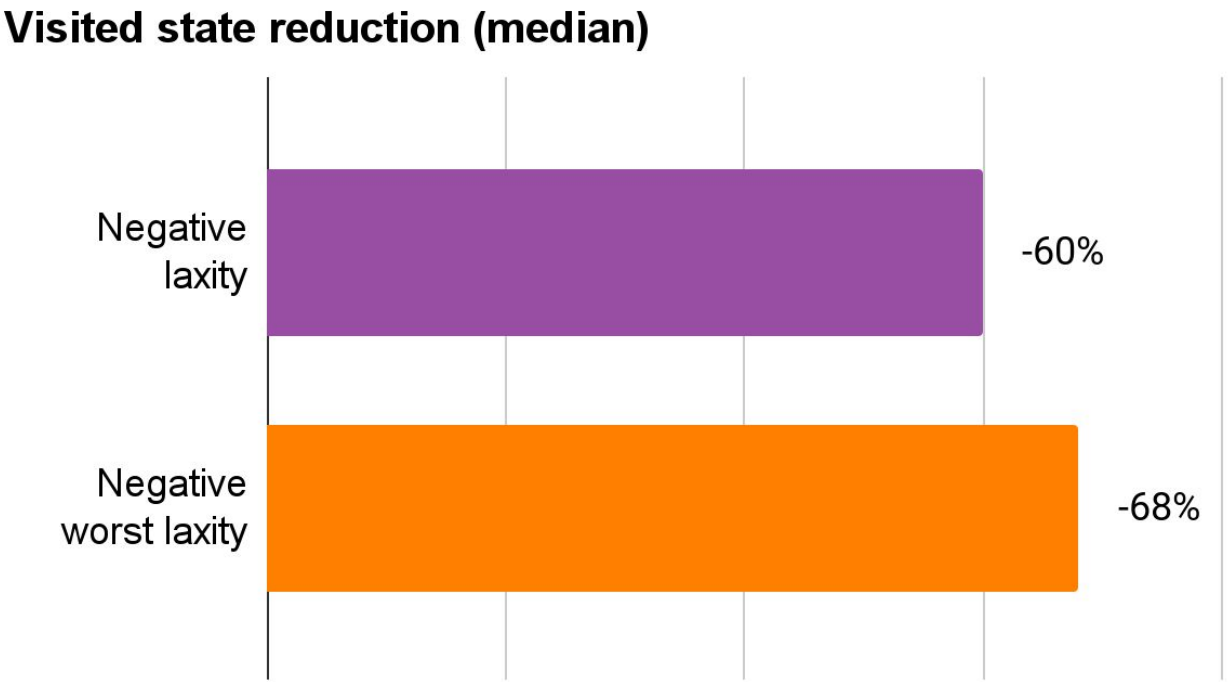


Can another **oracle predict** a future deadline miss **even earlier**?

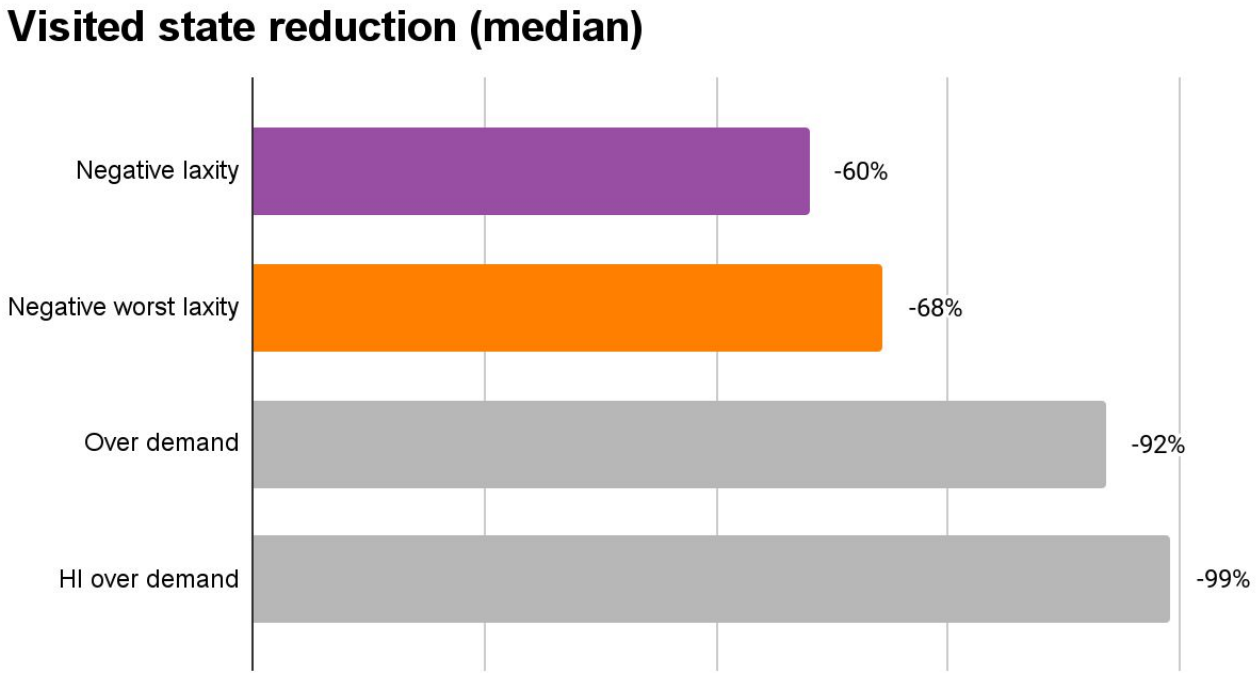
Anticipating a future mode change for a stronger oracle



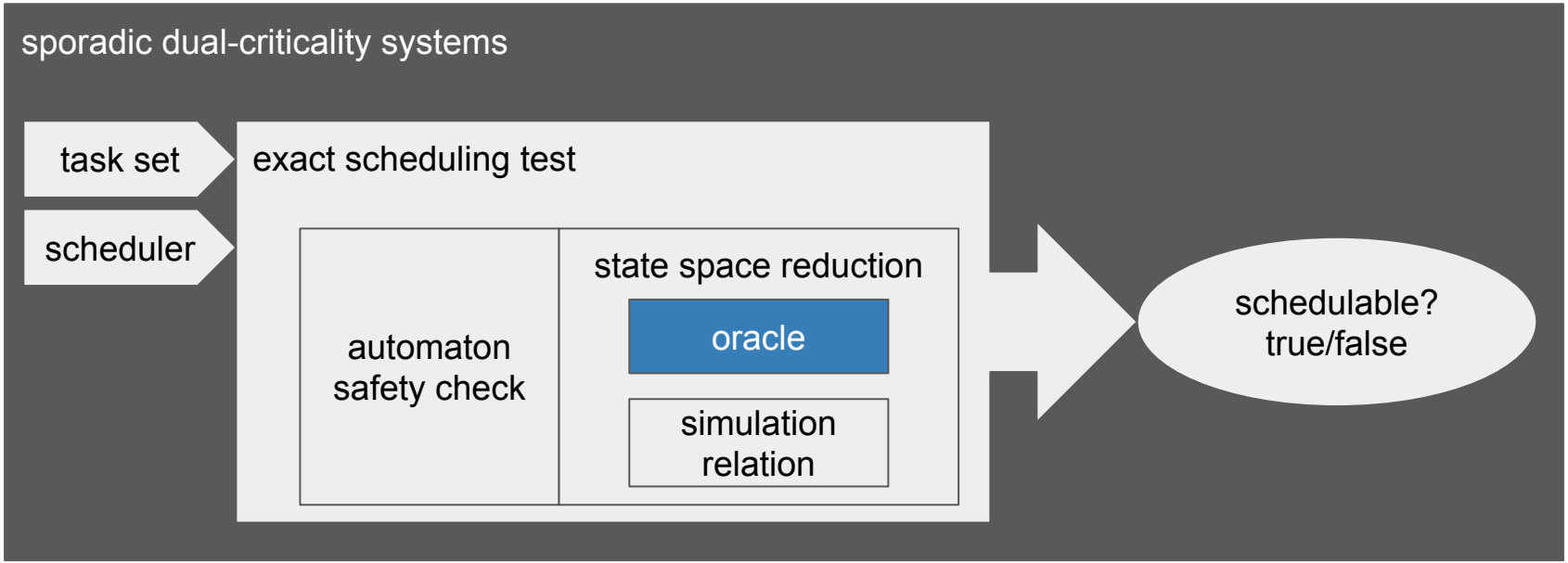
Oracles’ impact on unschedulable task sets



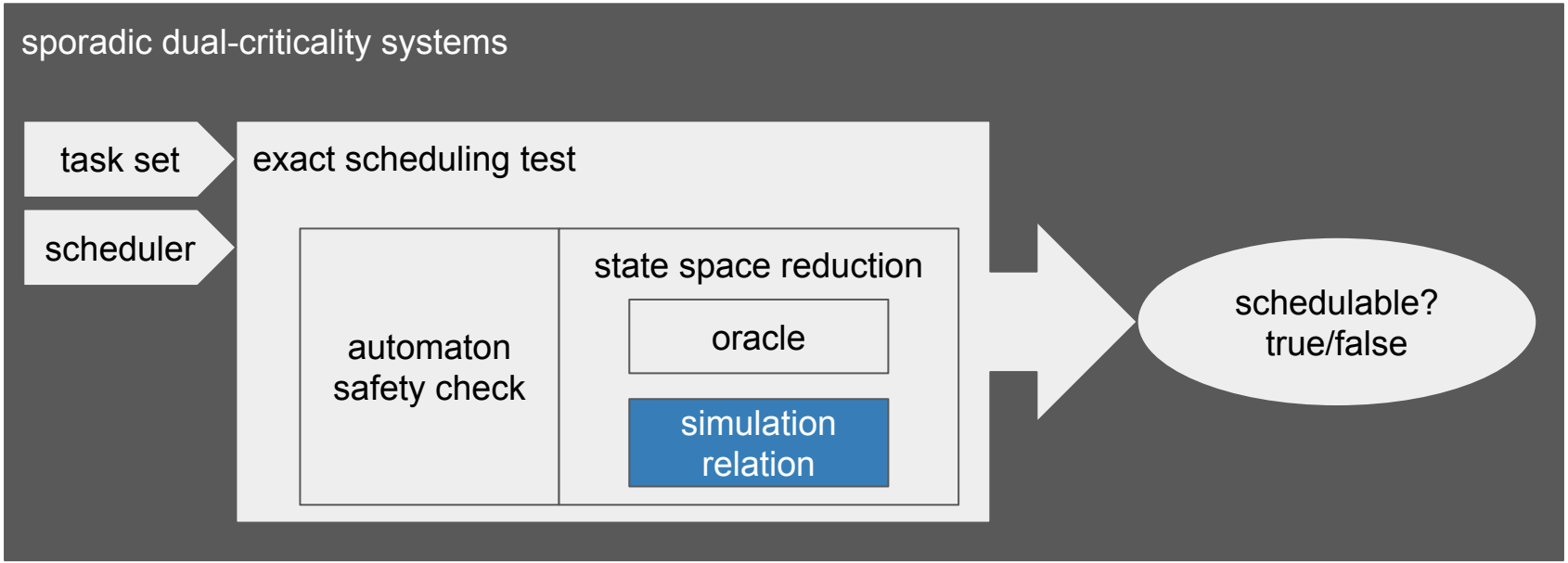
Paper only oracles' impact on unschedulable task sets



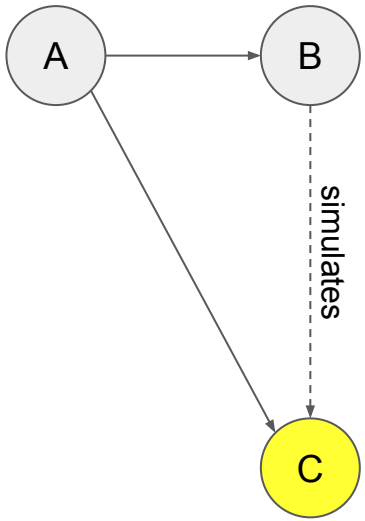
Objective of the work



Objective of the work



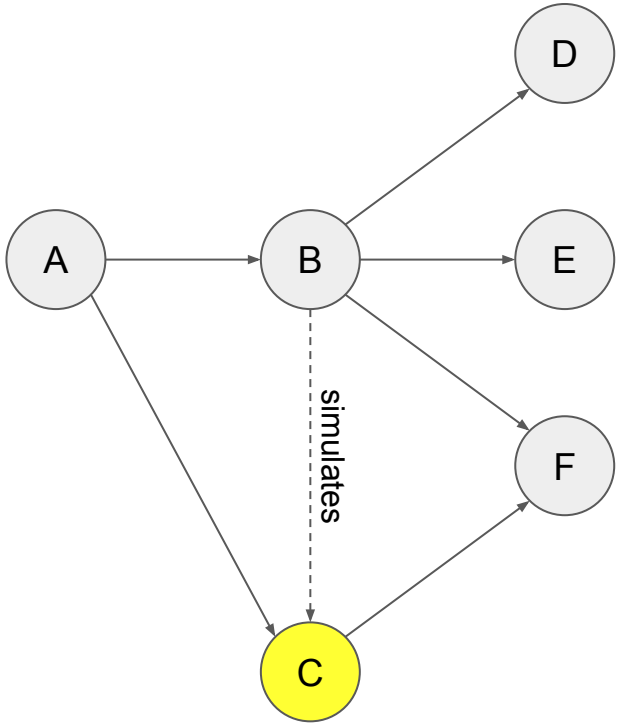
A simulation relation is a relationship between states



»

state B simulates state C

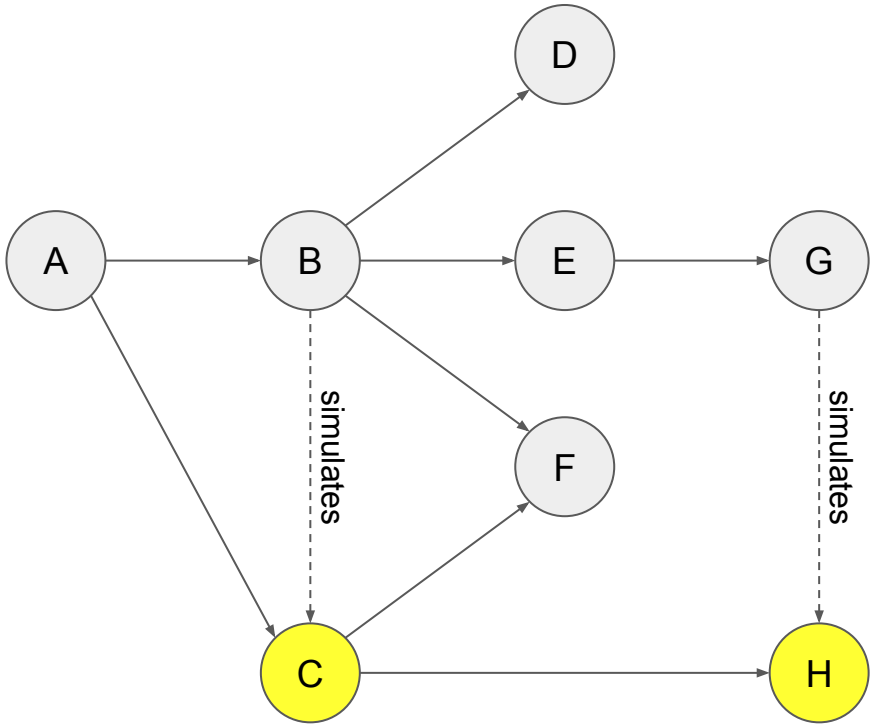
Implication of the simulation relation



Simulation implies:

1. Can reach all states

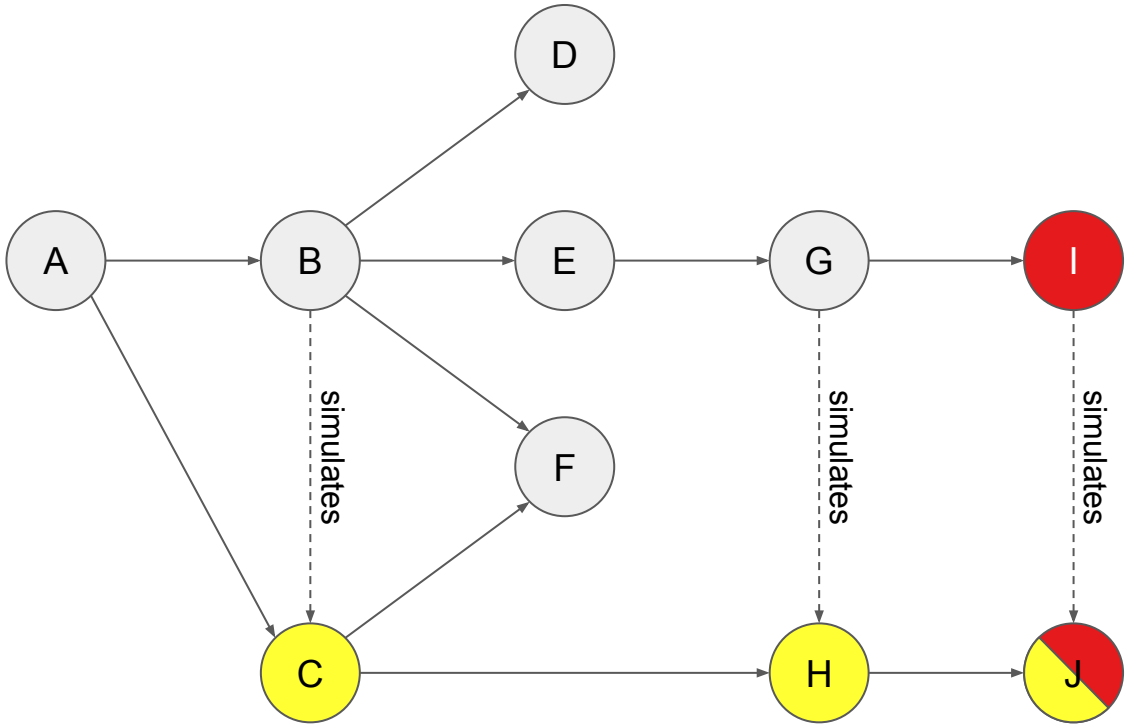
Implication of the simulation relation



Simulation implies:

1. Can reach all states
2. Or a state simulating it

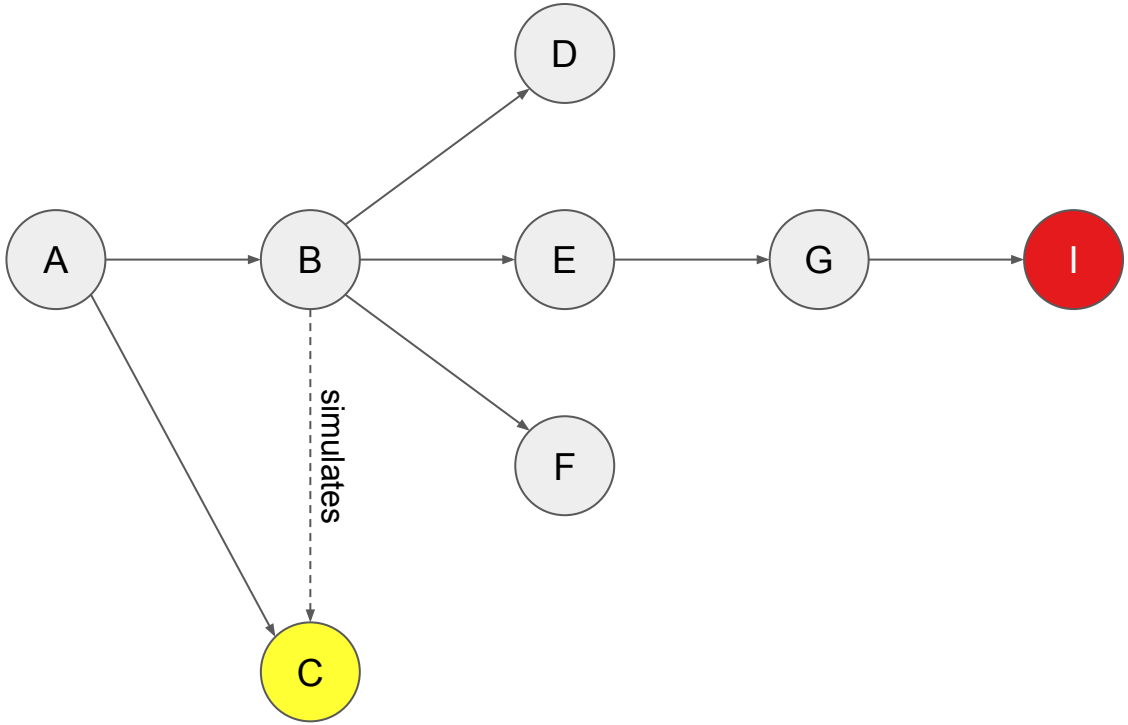
Implication of the simulation relation



Simulation implies:

1. Can reach all states
2. Or a state simulating it
3. Simulated fail states remains fail states

Do not explore simulated states and reduce state space



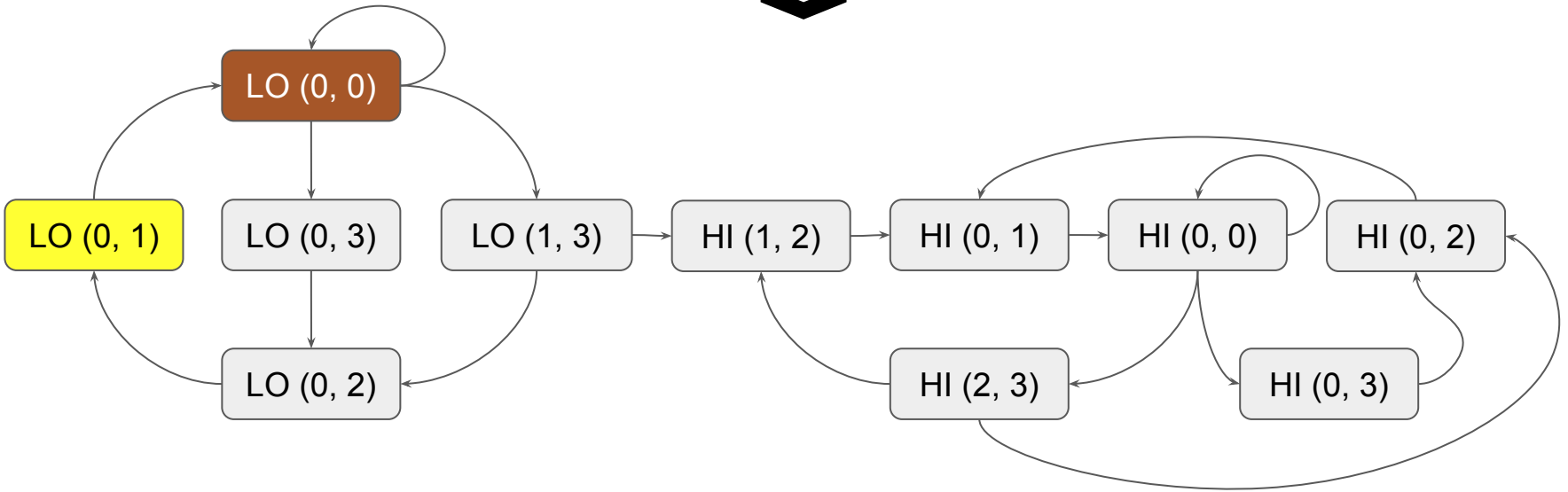
Simulation implies:

1. Can reach all states
2. Or a state simulating it
3. Simulated fail states remains fail states

Some states are simulated by the idle state

	C(LO)	C(HI)	D	T	L
τ_1	2	3	3	4	HI

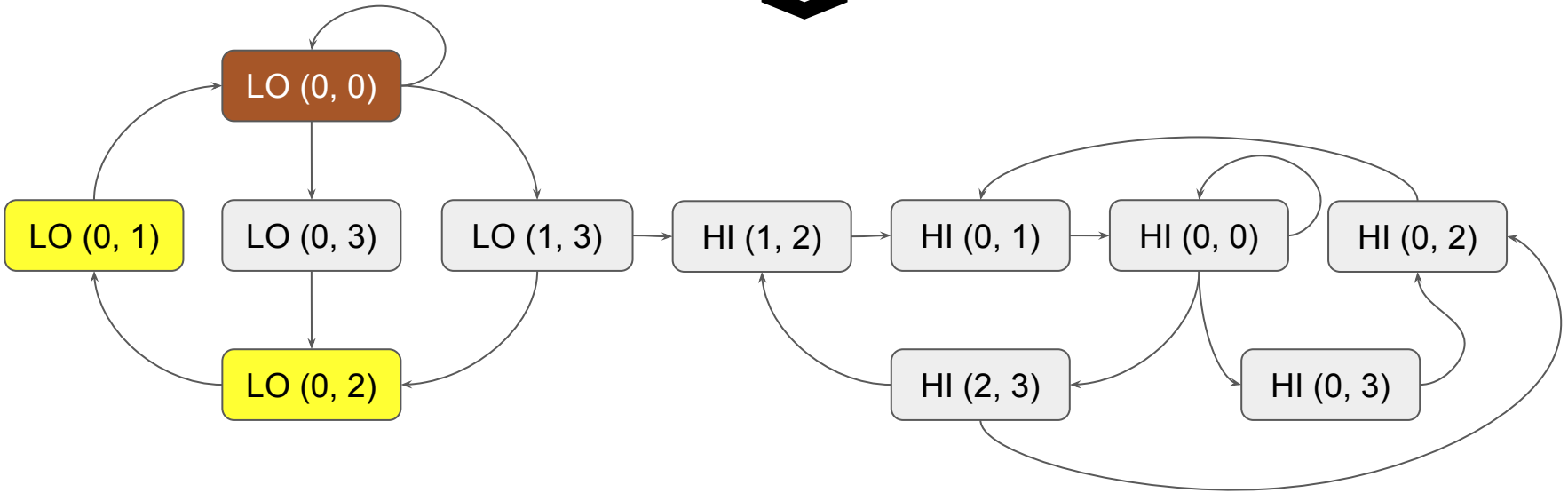
EDF-VD



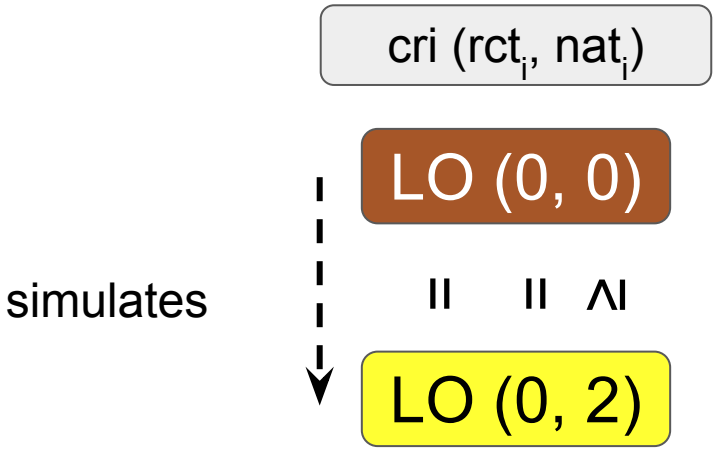
Some states are simulated by the idle state

	C(LO)	C(HI)	D	T	L
τ_1	2	3	3	4	HI

EDF-VD

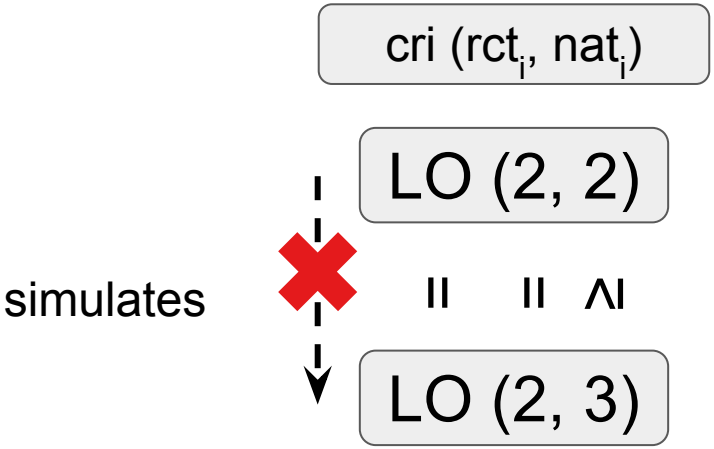


Idle tasks simulation



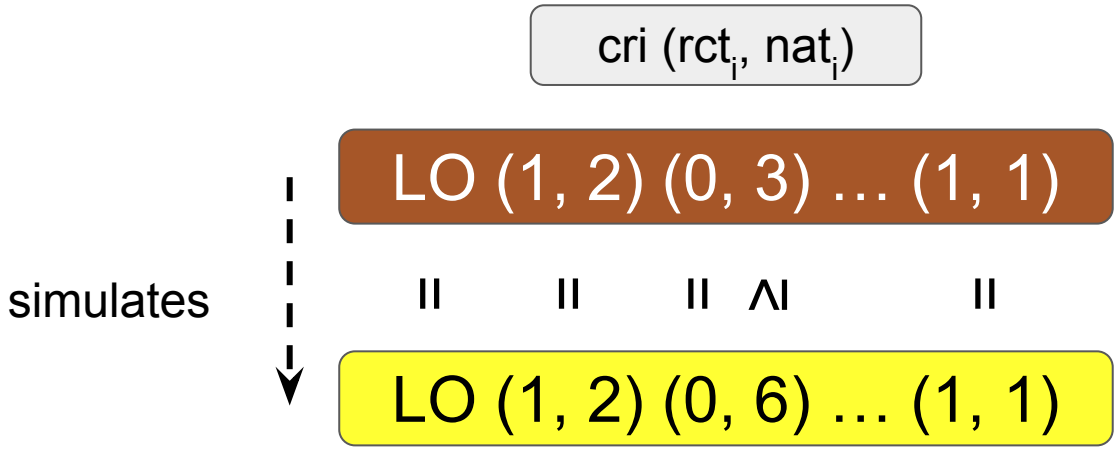
- Same criticality
- Task has no active jobs
- Next arrival time is sooner

Idle tasks simulation



- Same criticality
- Active tasks are identical

Idle tasks simulation

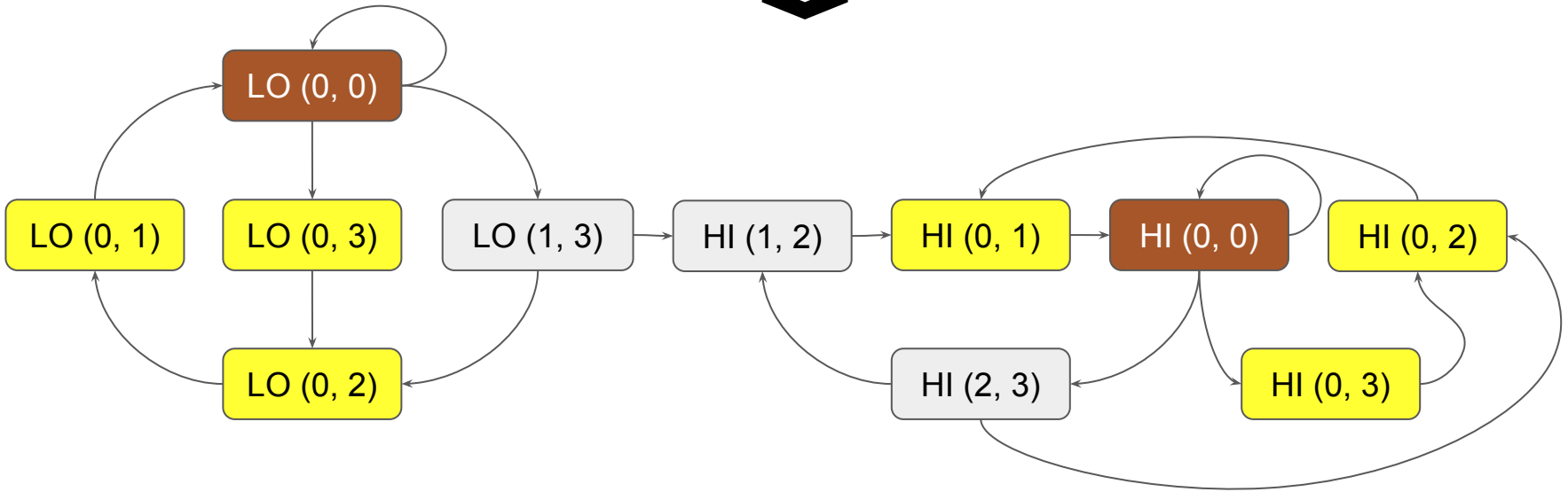


- Same criticality
- Active tasks are identical
- Idle task can release earlier

Simulated states can be omitted from the exploration

	C(LO)	C(HI)	D	T	L
τ_1	2	3	3	4	HI

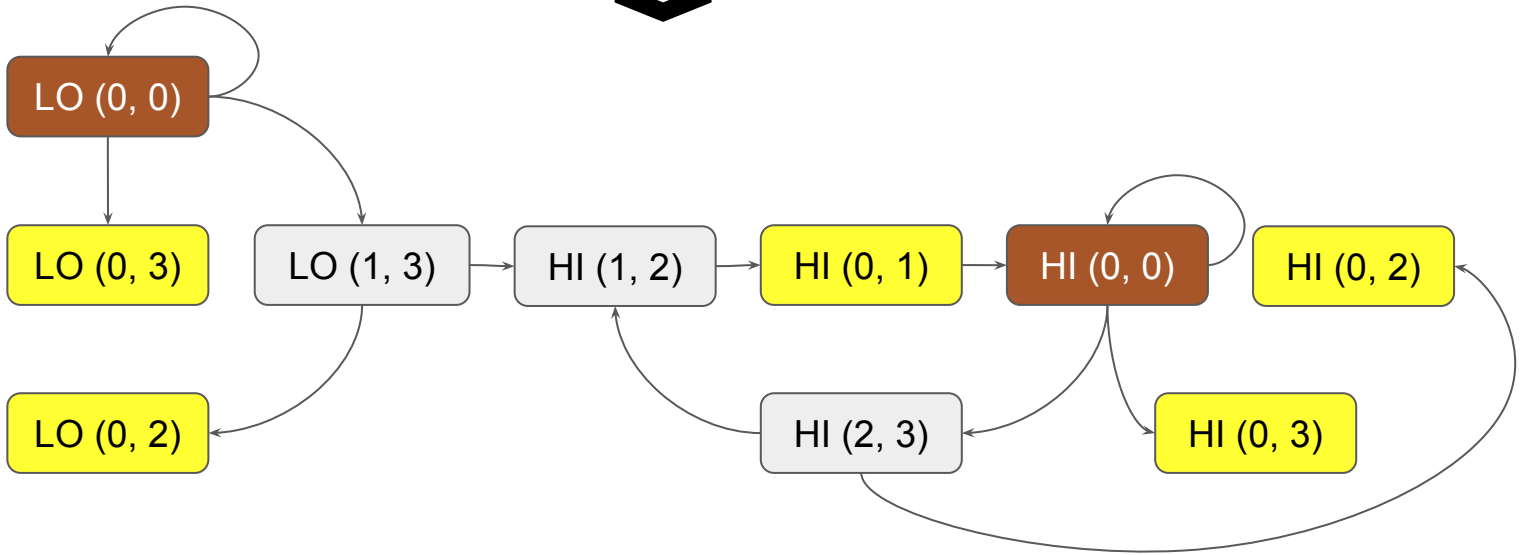
EDF-VD



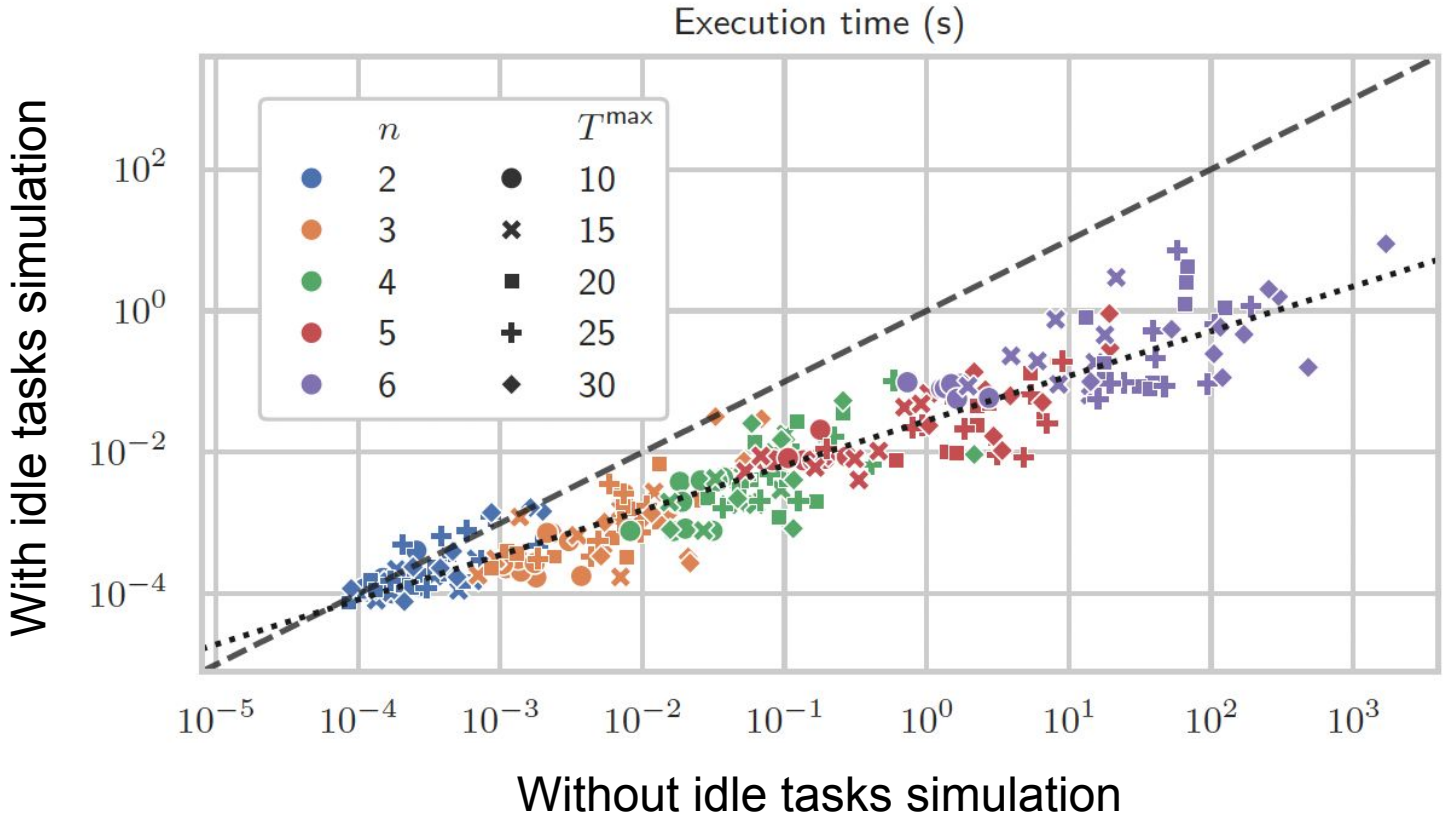
Simulated states can be omitted from the exploration

	C(LO)	C(HI)	D	T	L
τ_1	2	3	3	4	HI

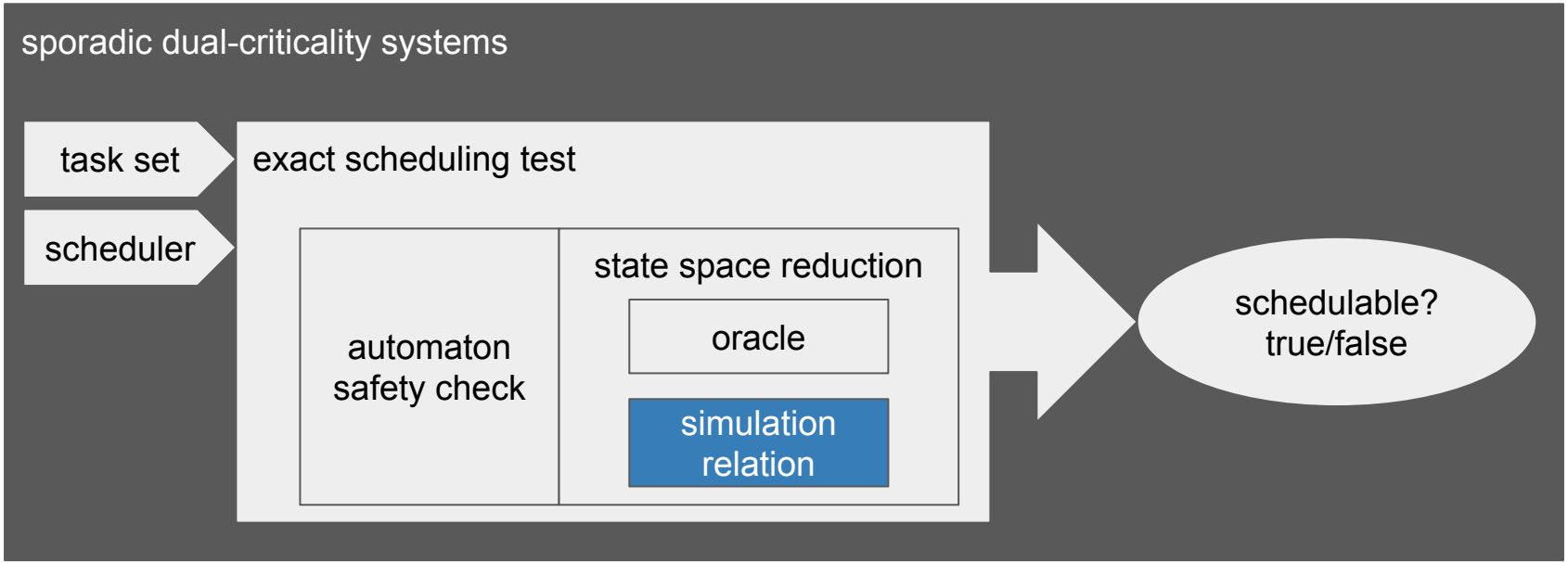
EDF-VD



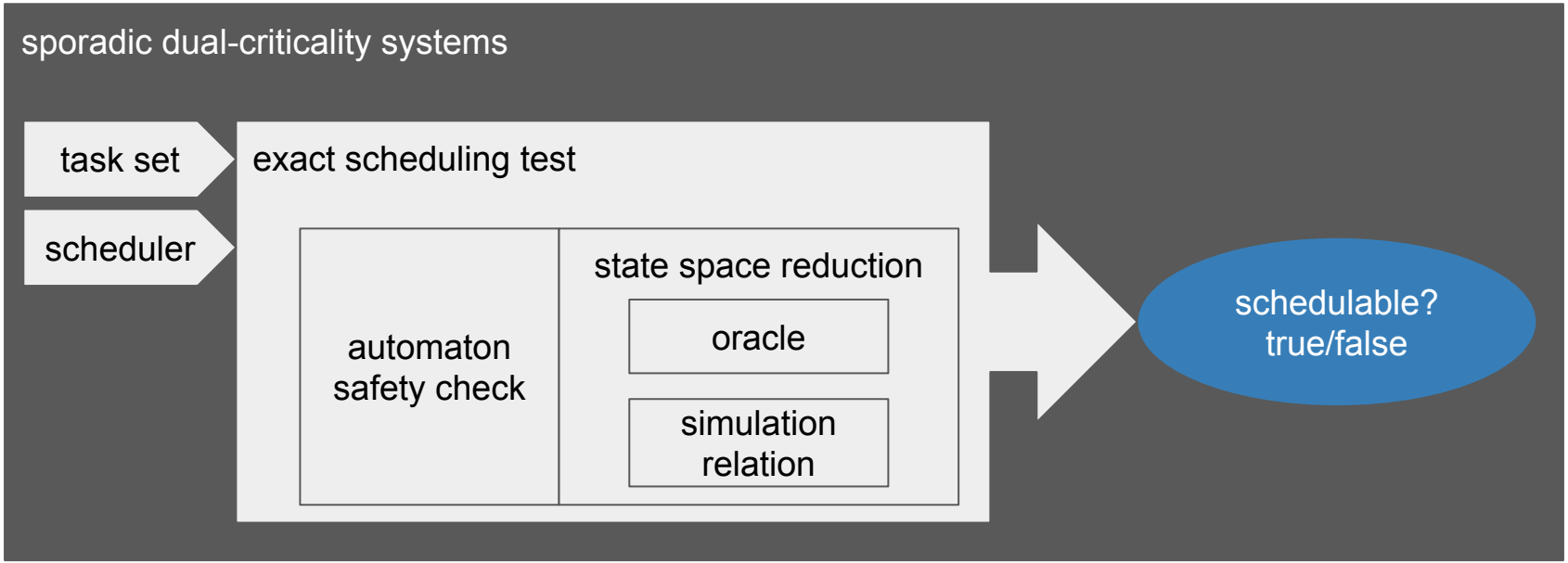
Idle tasks simulation impact on exploration duration



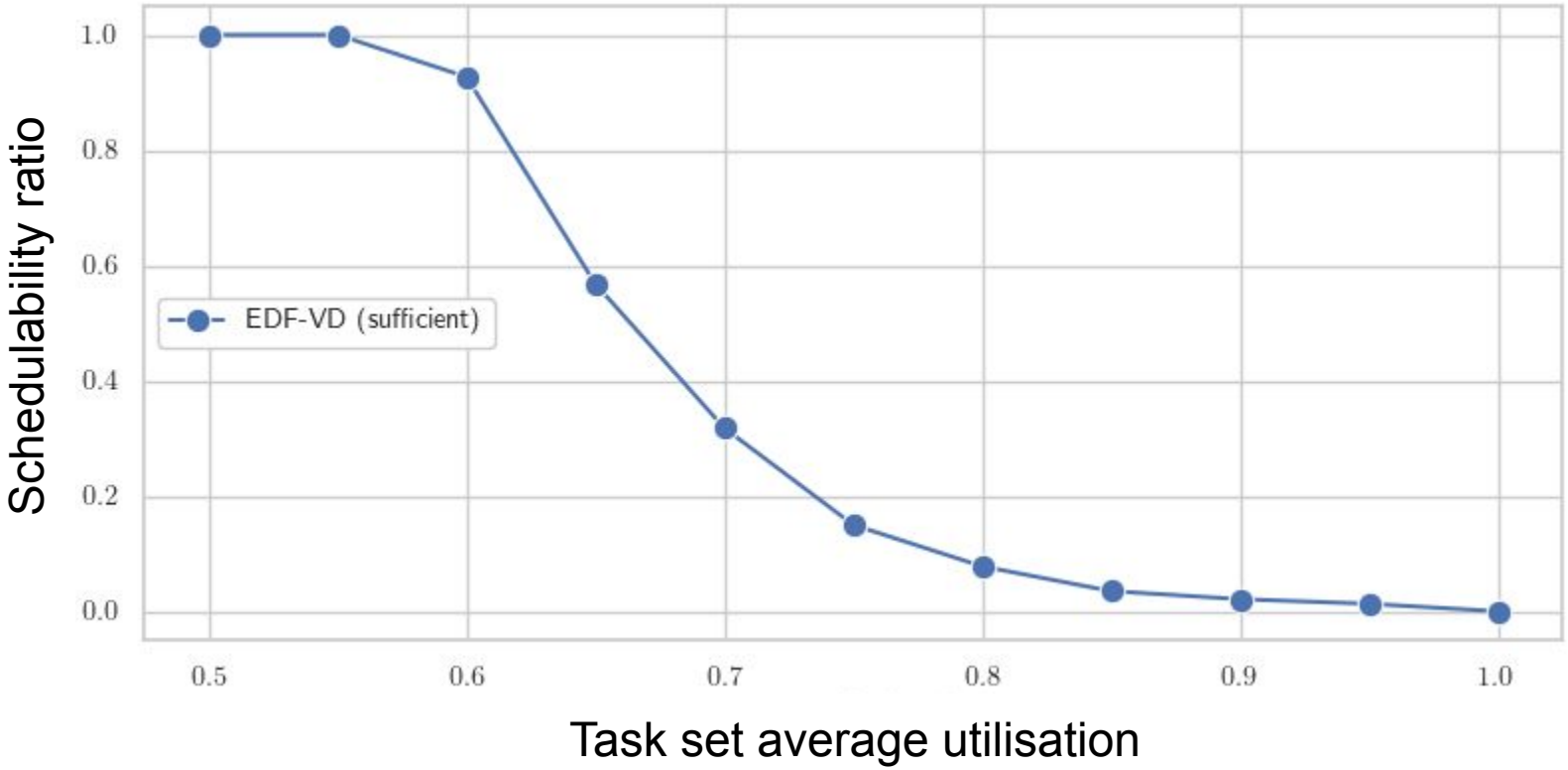
Objective of the work



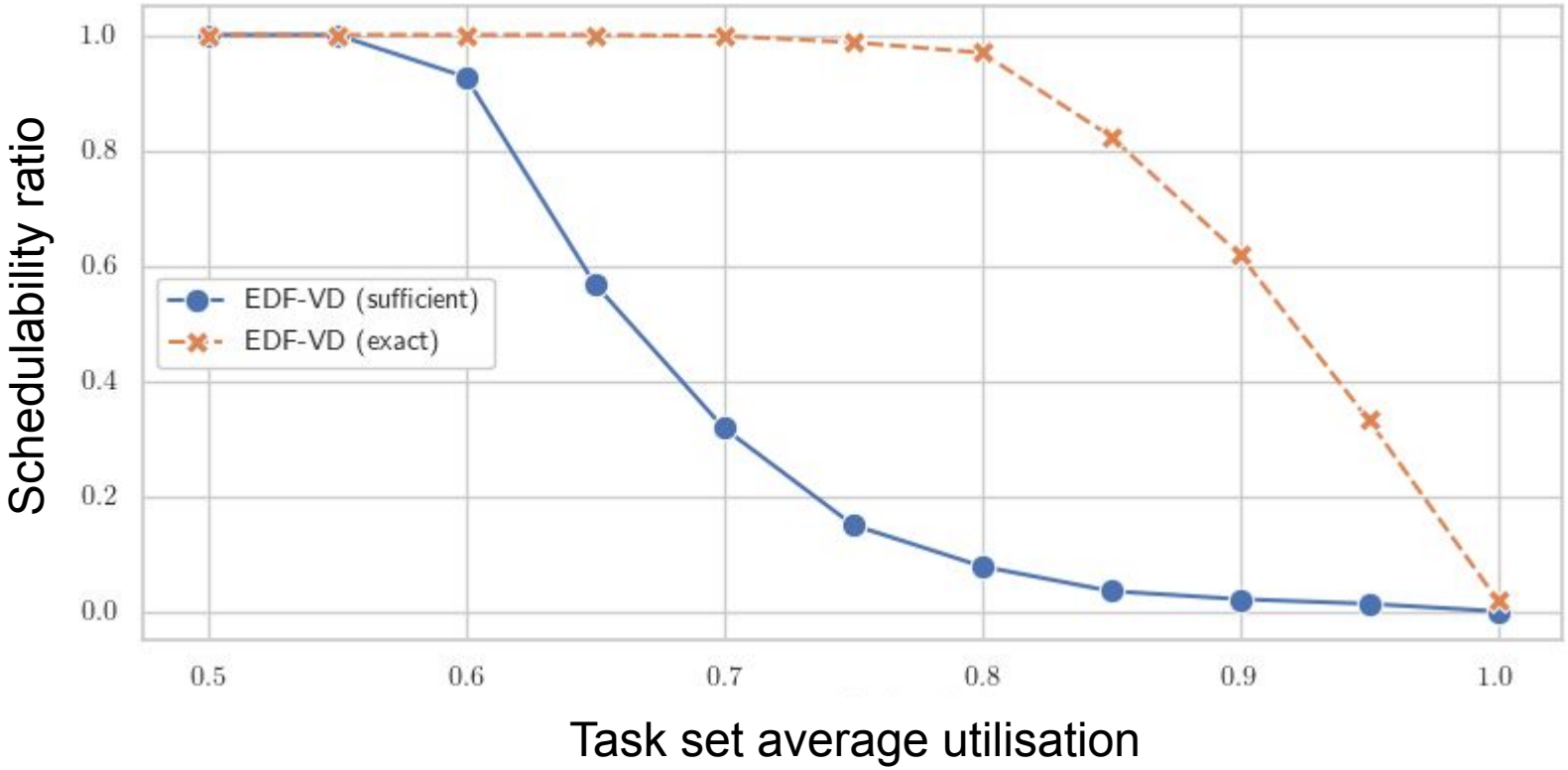
Objective of the work



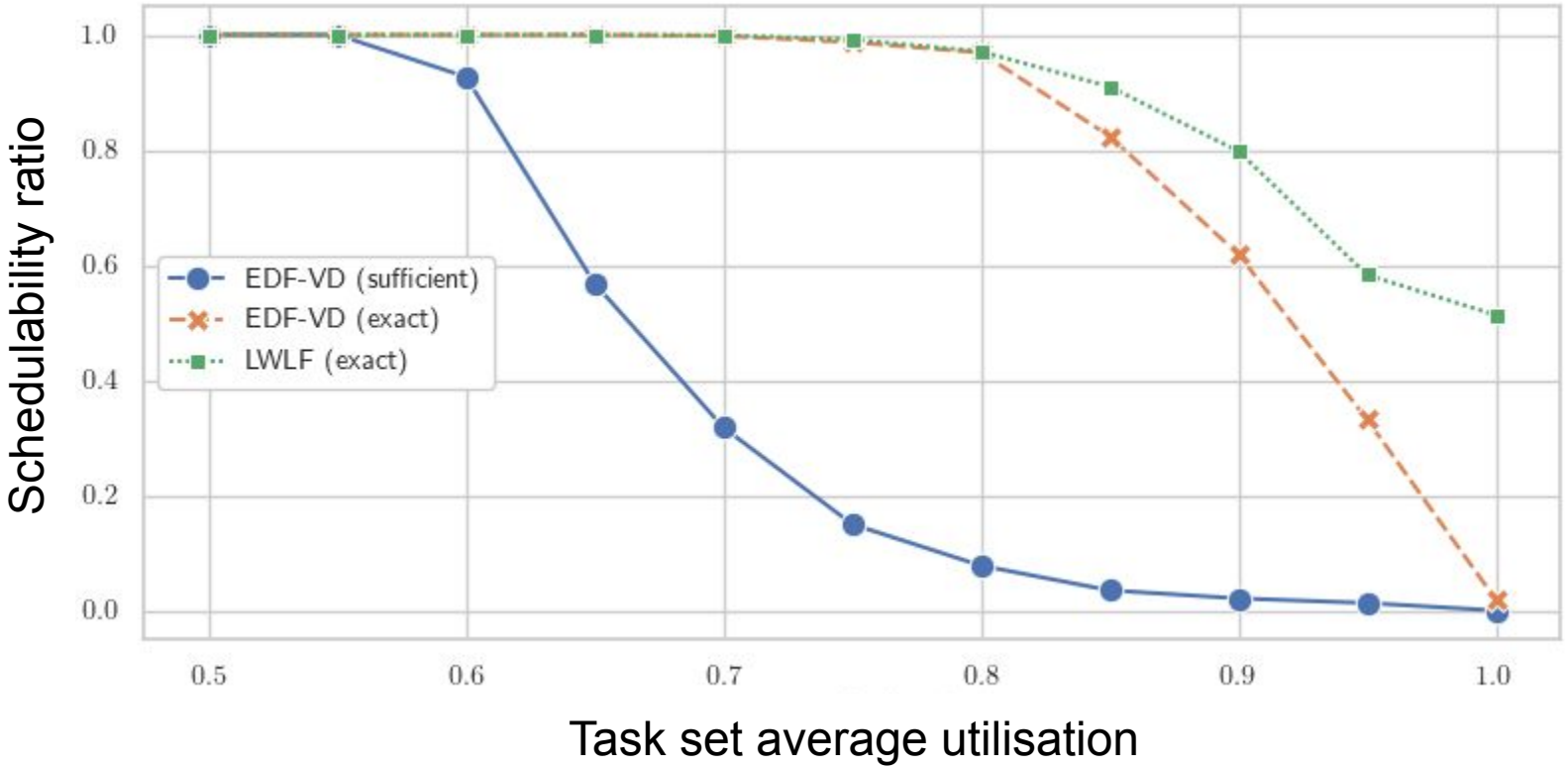
Assessing the schedulability for varying utilisation



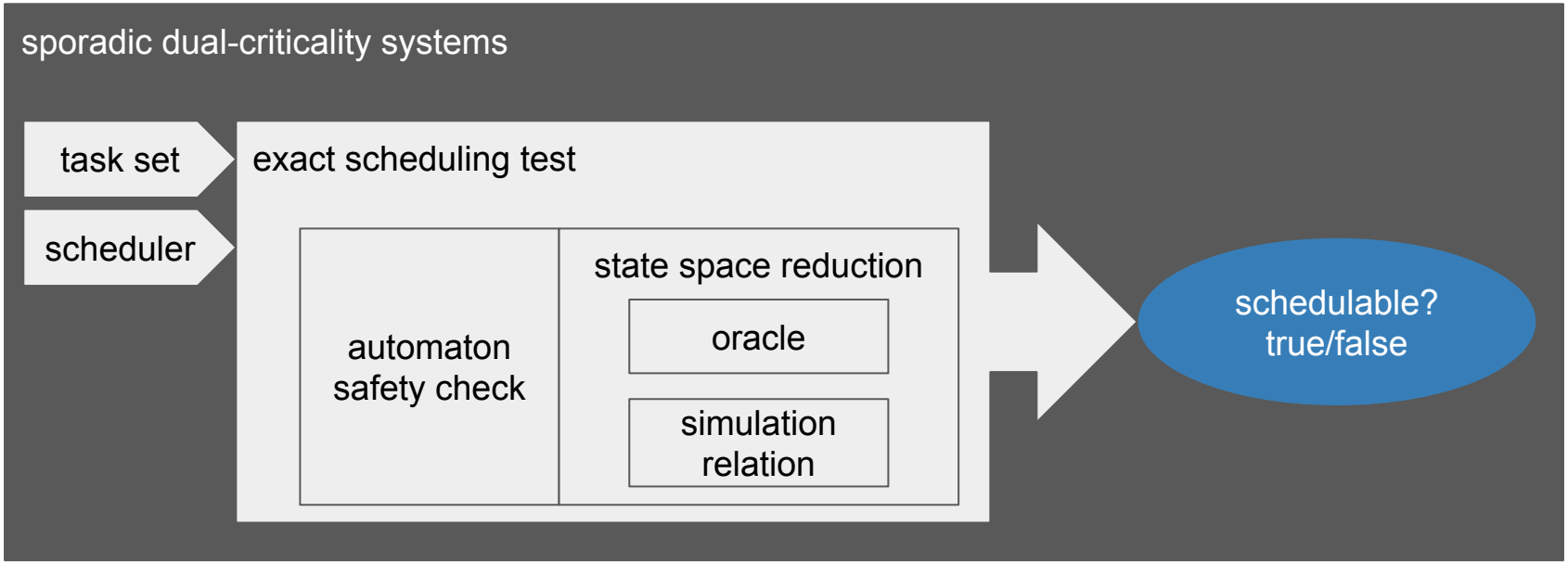
Quantifying the pessimism of sufficient tests



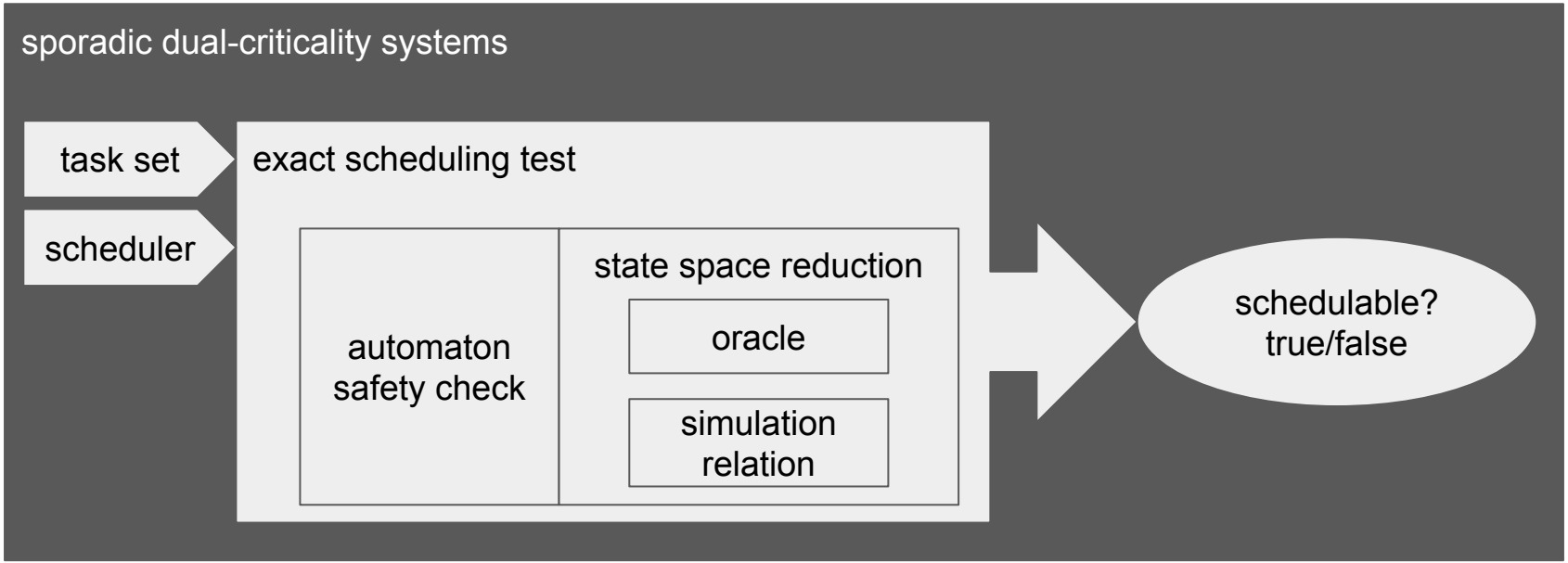
Empirical scheduler evaluation



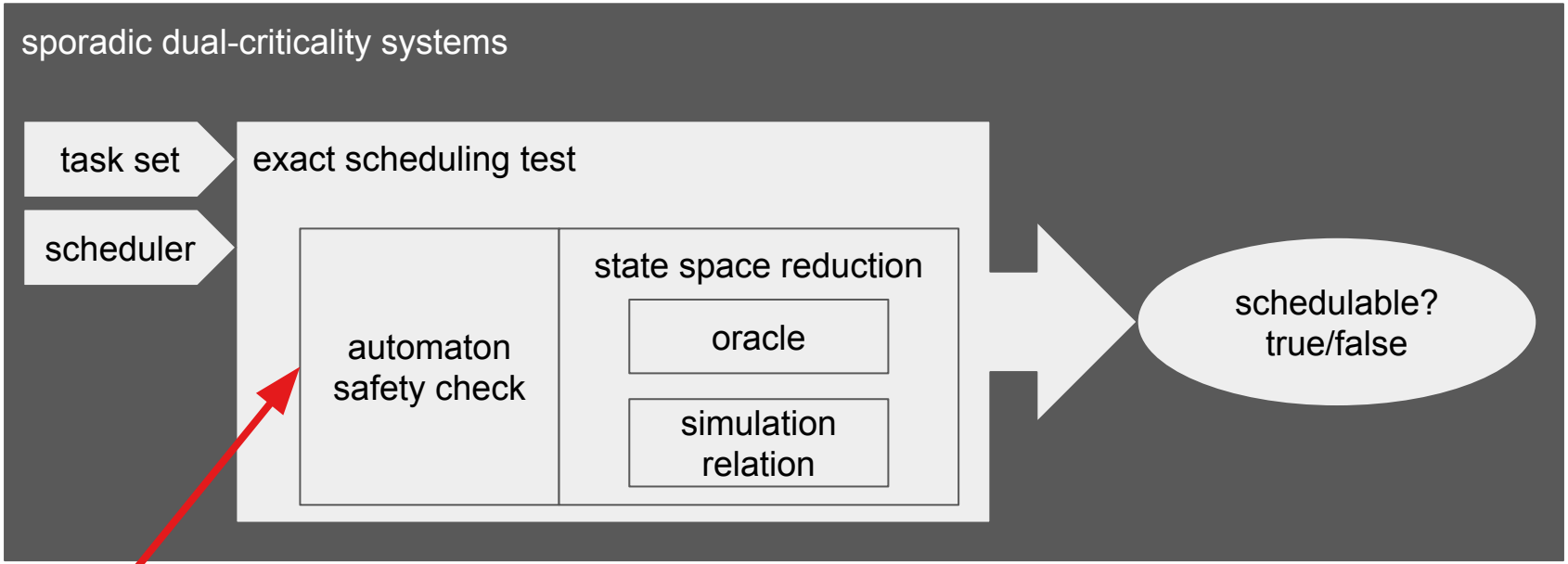
Objective of the work



Objective of the work

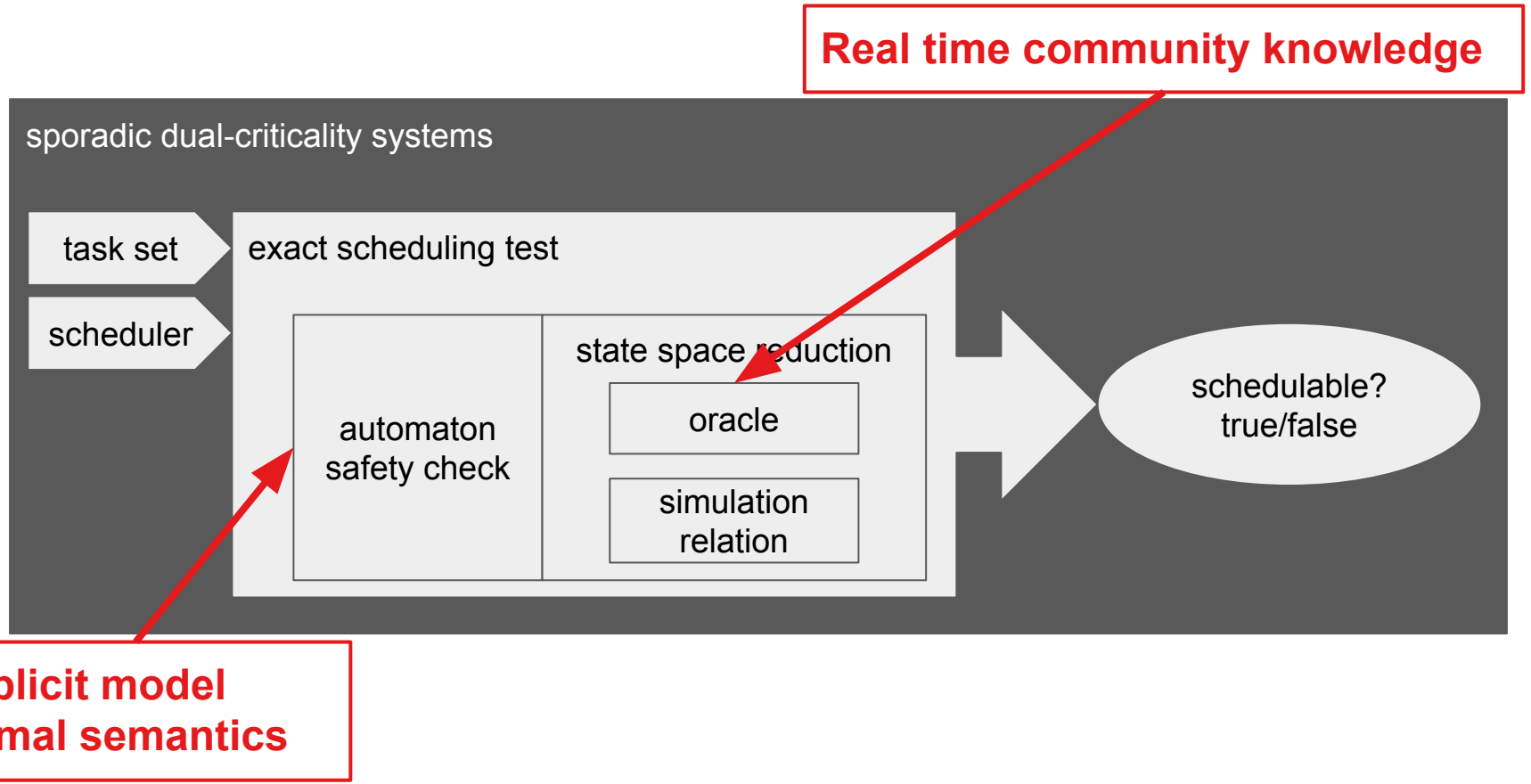


Objective of the work

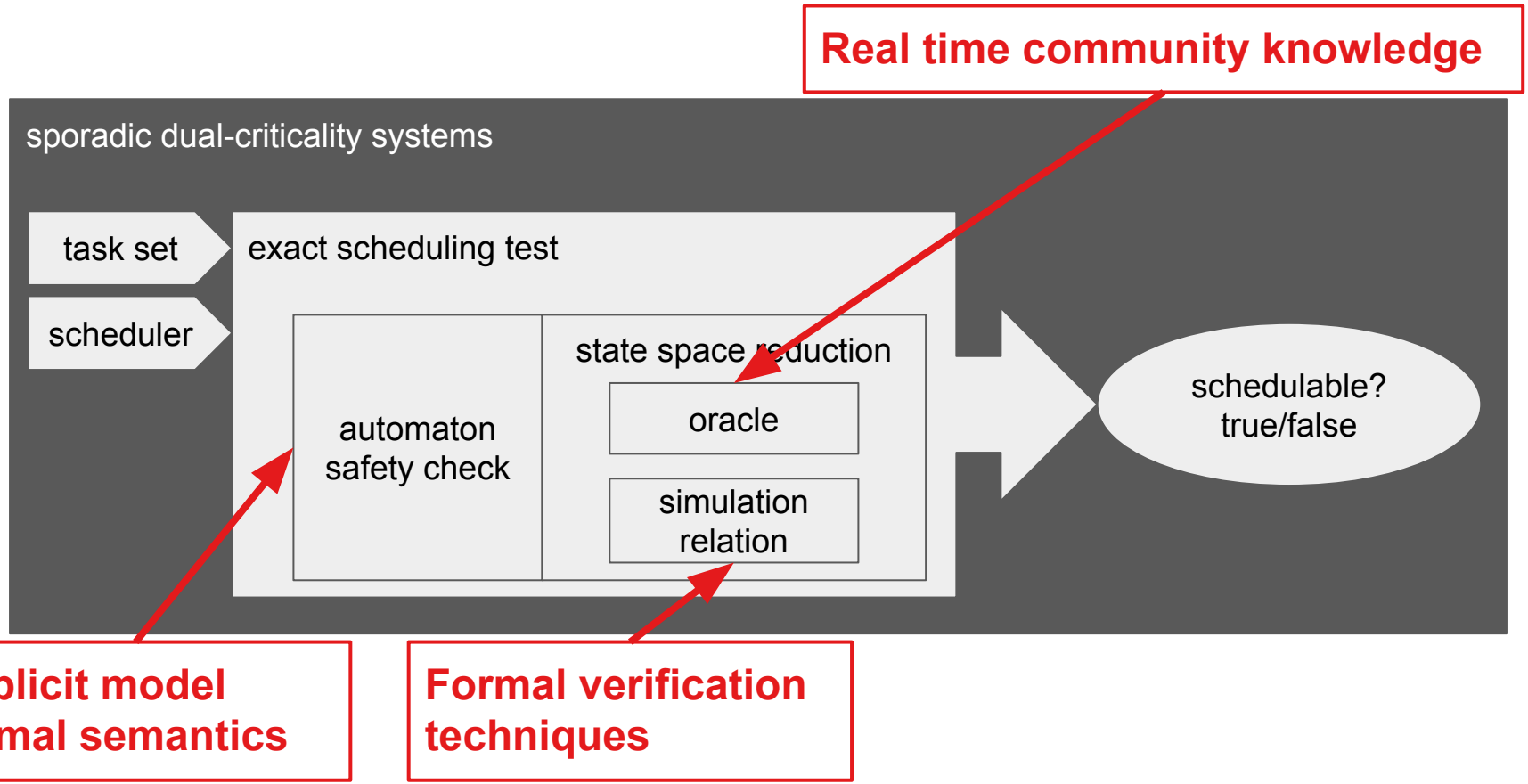


Explicit model
formal semantics

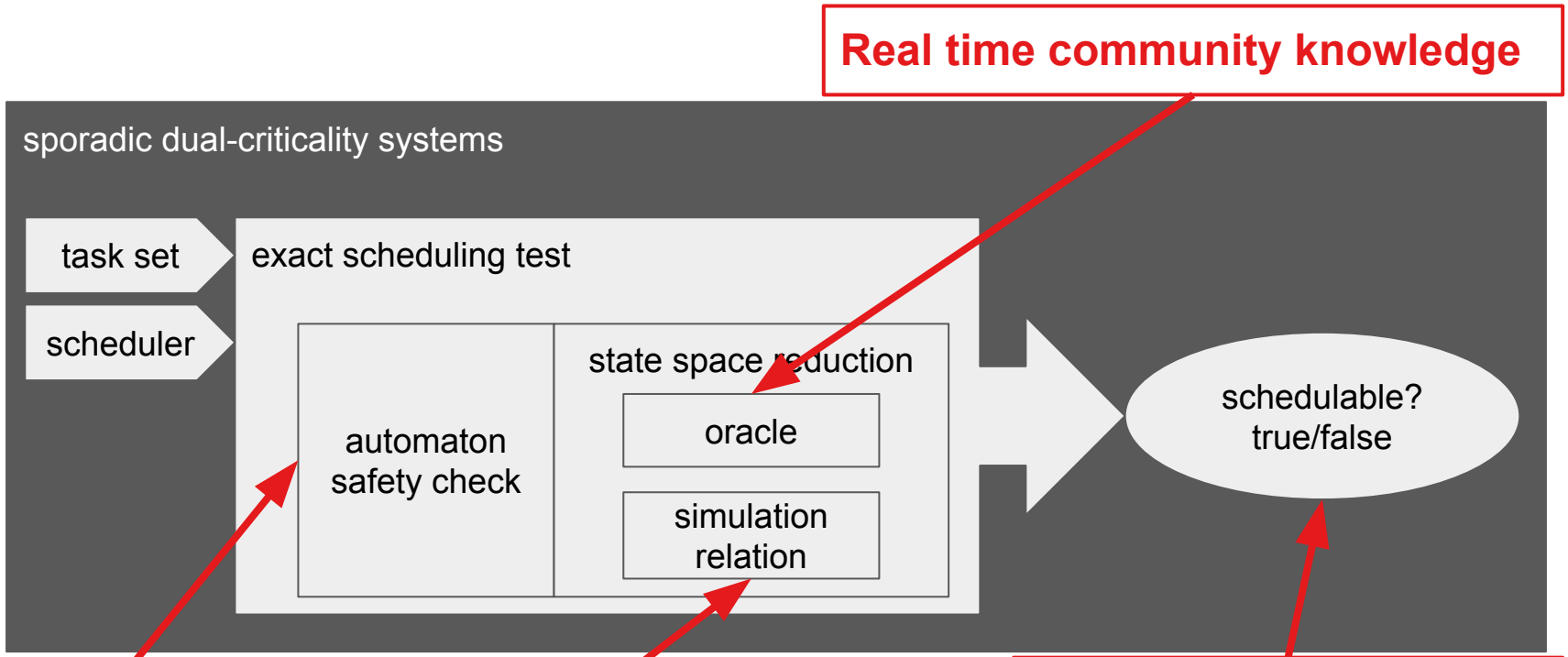
Objective of the work



Objective of the work



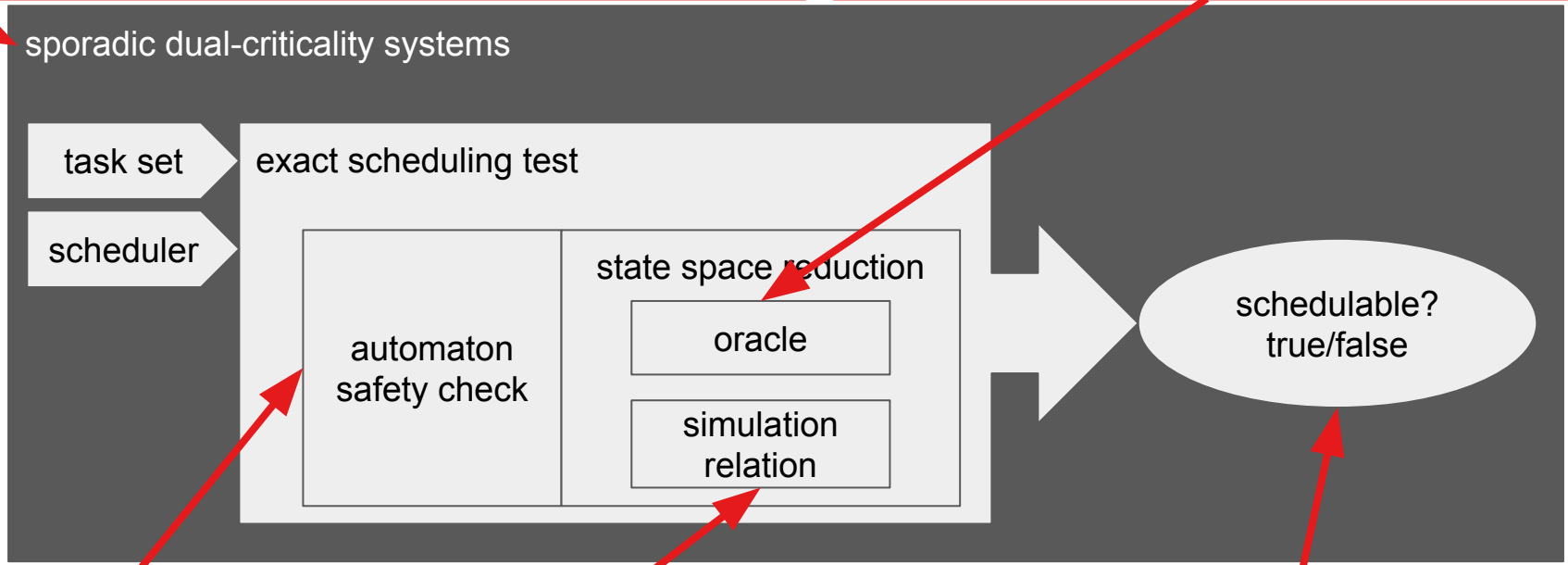
Objective of the work



Objective of the work

Framework applicable to other models

Real time community knowledge



Explicit model formal semantics

Formal verification techniques

No pessimism and scheduler exploration

Future work

Model extension

- multi-processor
- varying CPU speed
- preemption delay considerations
- arbitrary deadlines

Enhanced scalability

- new oracles
- new simulation relations
- implement meta transitions

Framework extension

- Feasibility as game on the automaton

Questions & voting

Model extension

- multi-processor
- varying CPU speed
- preemption delay considerations
- arbitrary deadlines

Enhanced scalability

- new oracles
- new simulation relations
- implement meta transitions

Framework extension

- Feasibility as game on the automaton

67 10 96 5

Backup

Related work

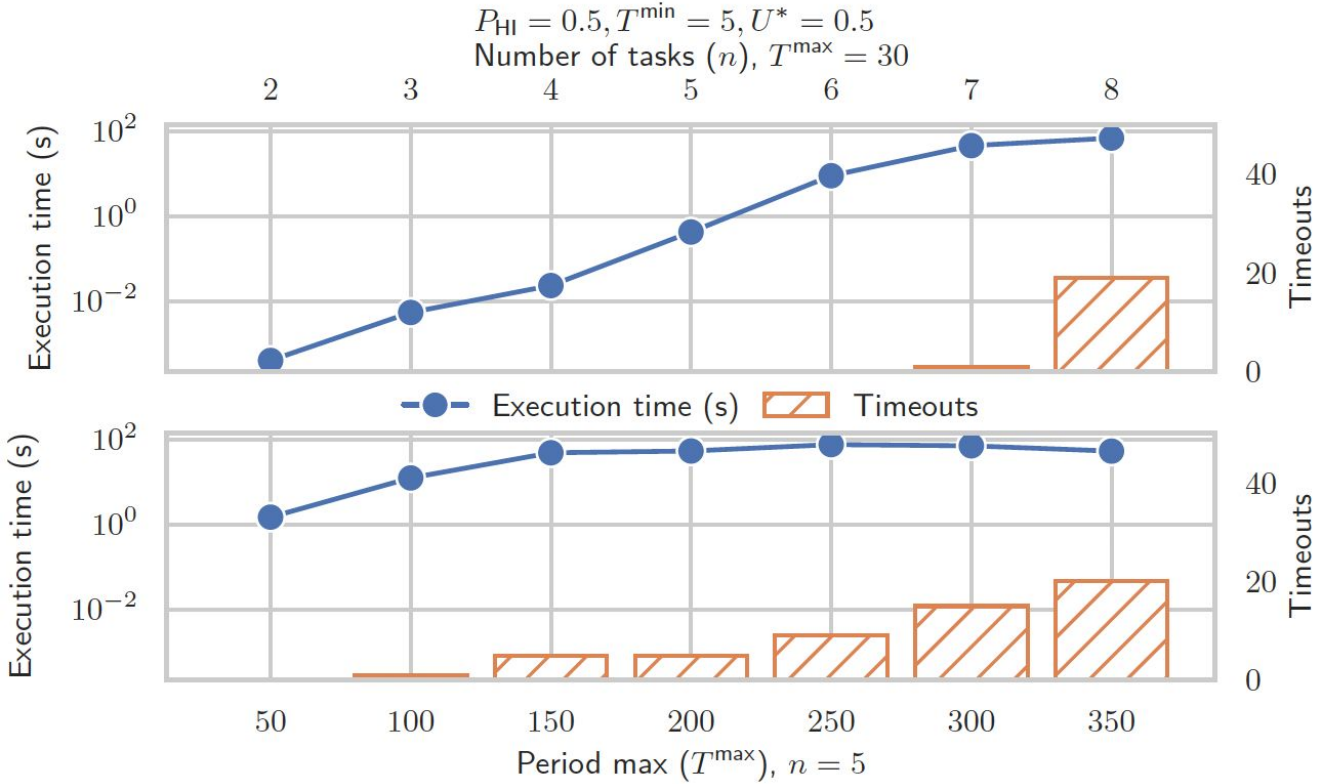
Table 1: Comparing with the related work.

	[5]	[4]	[29]	Us
Criticality	Single	**Dual**	Single	**Dual**
Priority classes	**Any**	FTP	**Any**	**Any**
Pruning rules	✖	✔	✖	✖
Antichains	✖	✖	✔	✔
Oracles	✖	✖	✖	✔
Multi-processor	✔	✖	✔	✖

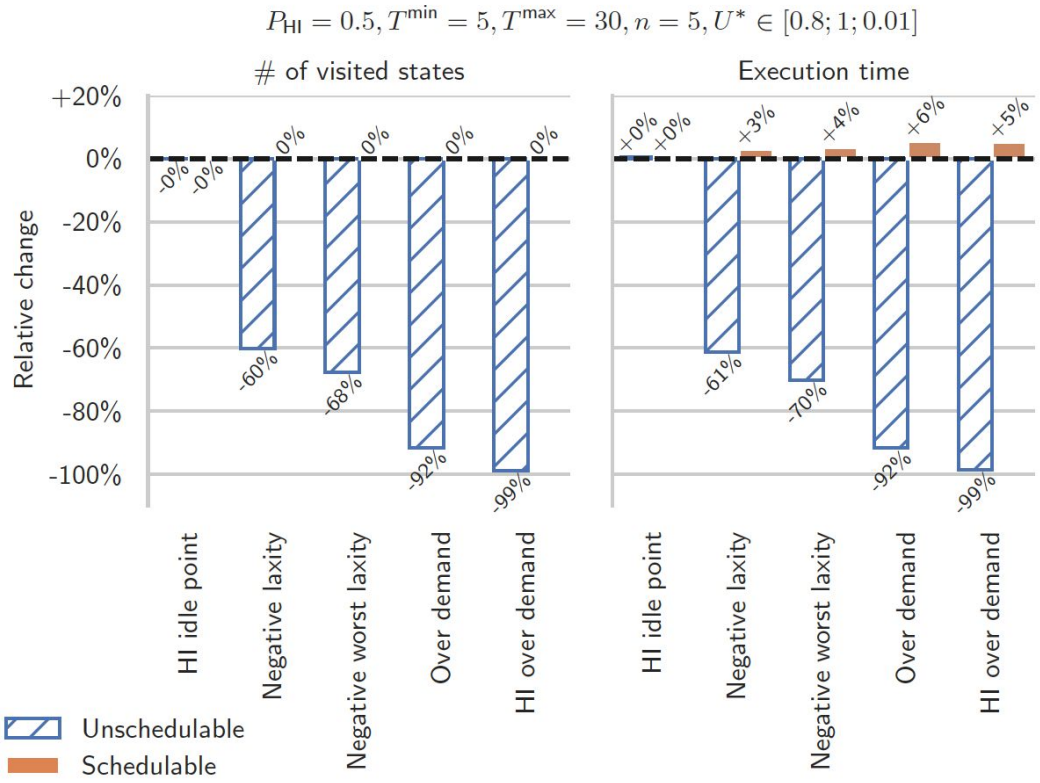
Related work (extended, tentative)

Category		Baker 2007	Lindstrom 2011	Nasri 2017	Asyaban 2018	Yalcinkaya 2019	Abdeddaïm 2020	Ranjha 2023	Nasri 2024	Gohari 2024	This paper 2024
Framework	FSM	x	x		x						x
	Timed automata					x	x				
	SAG			x				x	x	x	
Execution time	Varying execution time			x		x		x	x	x	
	Dual-crit				x		x				x
Scheduler	FTP	x	x	x	x	x	x	x	x	x	x
	FJP	x	x	x			x	x	x	x	x
	DP	x	x								x
	Preemptive	x	x		x		x		x	x	x
Multi proc	Multi proc	x	x	x		x		x	x	x	
Release model	Release jitter			x		x		x	x	x	
	Periodic task		x	x		x	x		x	x	
	Sporadic task	x	x		x	x	x				x
Constraints	DAG							x			
	Self-suspending					x					
Optimisation	Pruning rules				x			x			
	Partial-order							x		x	
	Antichain		x								x
	Oracles										x

Scalability experiment



Extended oracle experiment

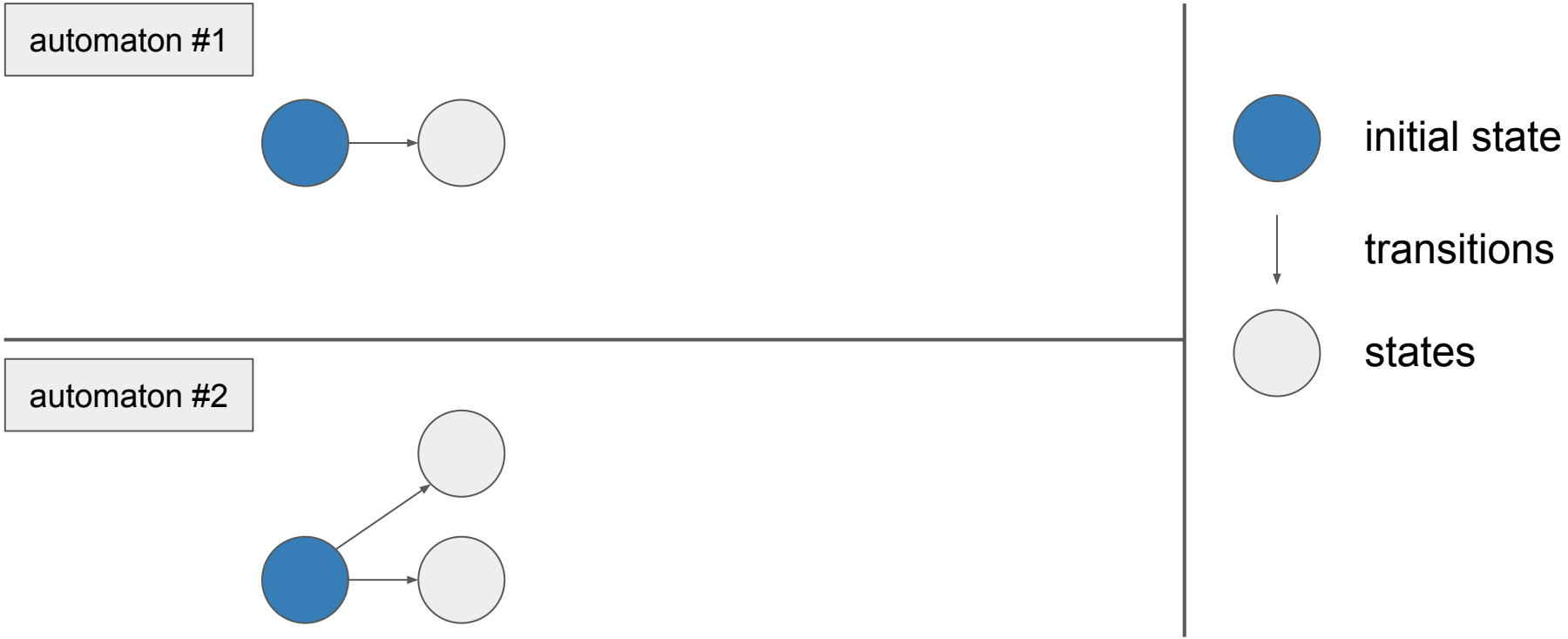


Statistics on the number of visited states

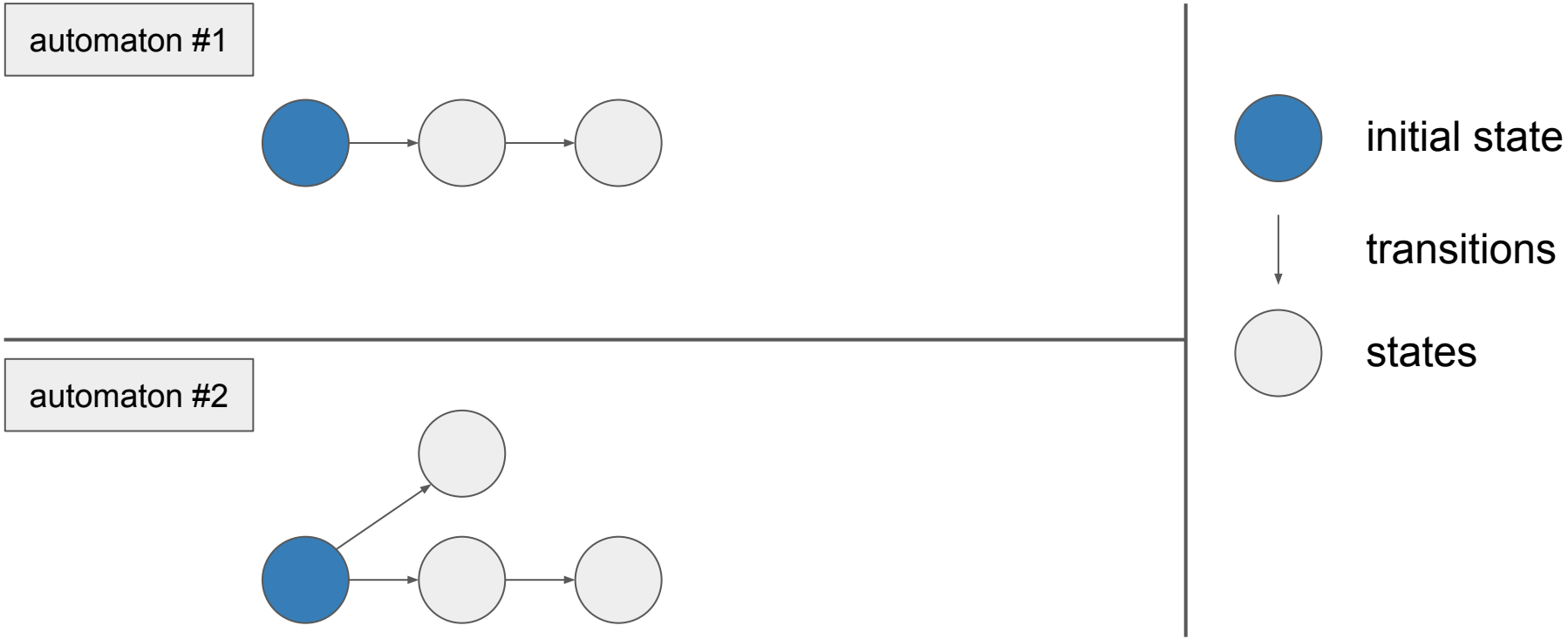
$P_{\mathsf{HI}} = 0.5, T^{\mathsf{min}} = 5, T^{\mathsf{max}} = 20, n = 5, U^* \in [0.8; 1; 0.01]$				
Search	BFS		ACBFS	
Oracle	None	HI over demand	None	HI over demand
min	9905	35 (-100%)	668 (-93%)	29 (-100%)
mean	746974	480688 (-36%)	75374 (-90%)	46024 (-94%)
std	999984	819378 (-18%)	126110 (-87%)	107731 (-89%)
median	410063	217928 (-49%)	35888 (-91%)	15459 (-96%)
max	11875126	11875126 (-0%)	2687577 (-77%)	2687577 (-77%)

Safety check in an automaton

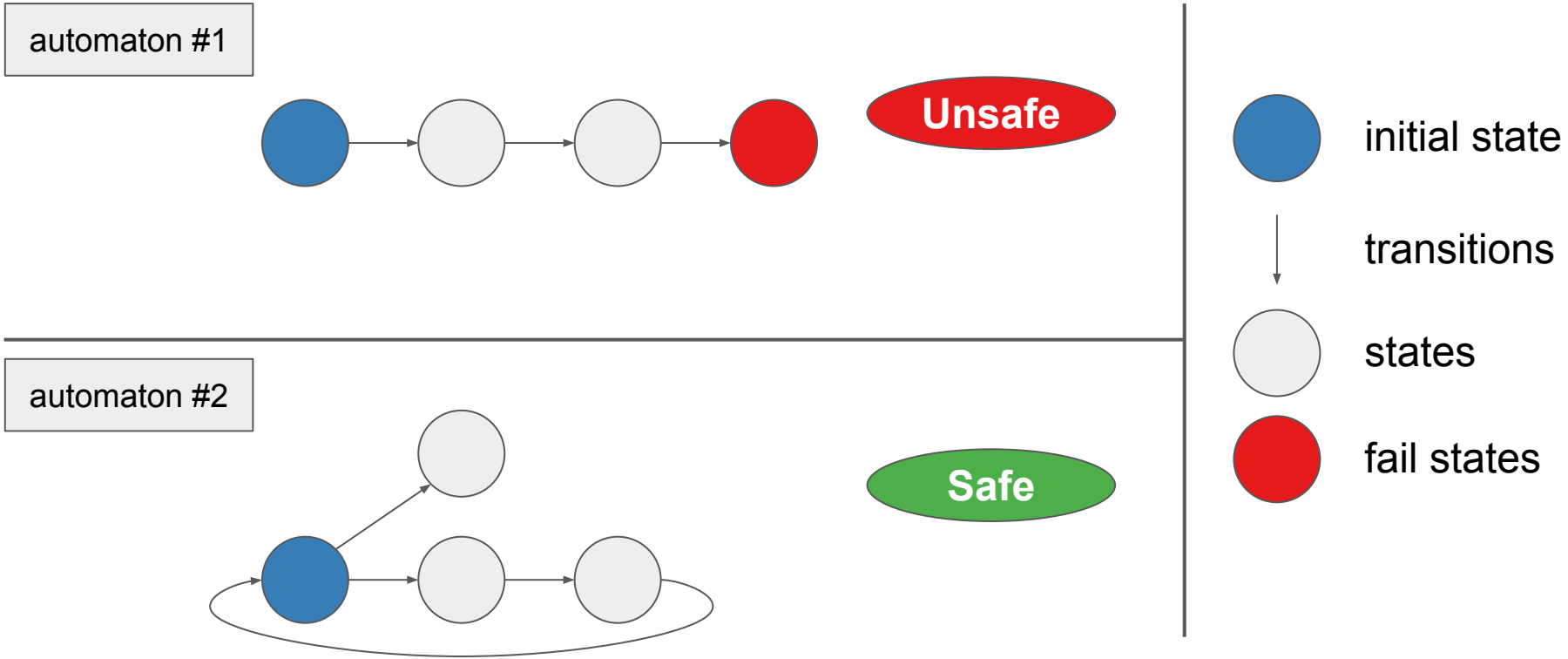
Safety check in an automaton



Safety check in an automaton



Safety check in an automaton



Scheduling test to automaton safety