中国科学院软件研究所学术年会'2023
暨计算机科学国家重点实验室开放周

# mcp f f

Changwen Li, Joseph Sifakis, Qiang Wang, Rongjie Yan, Jian Zhang

学术会议： International Symposium on Software Testing and Analysis

联系方式： 晏荣杰 yrj@ios.ac.cn 李昌文 licw@ios.ac.cn

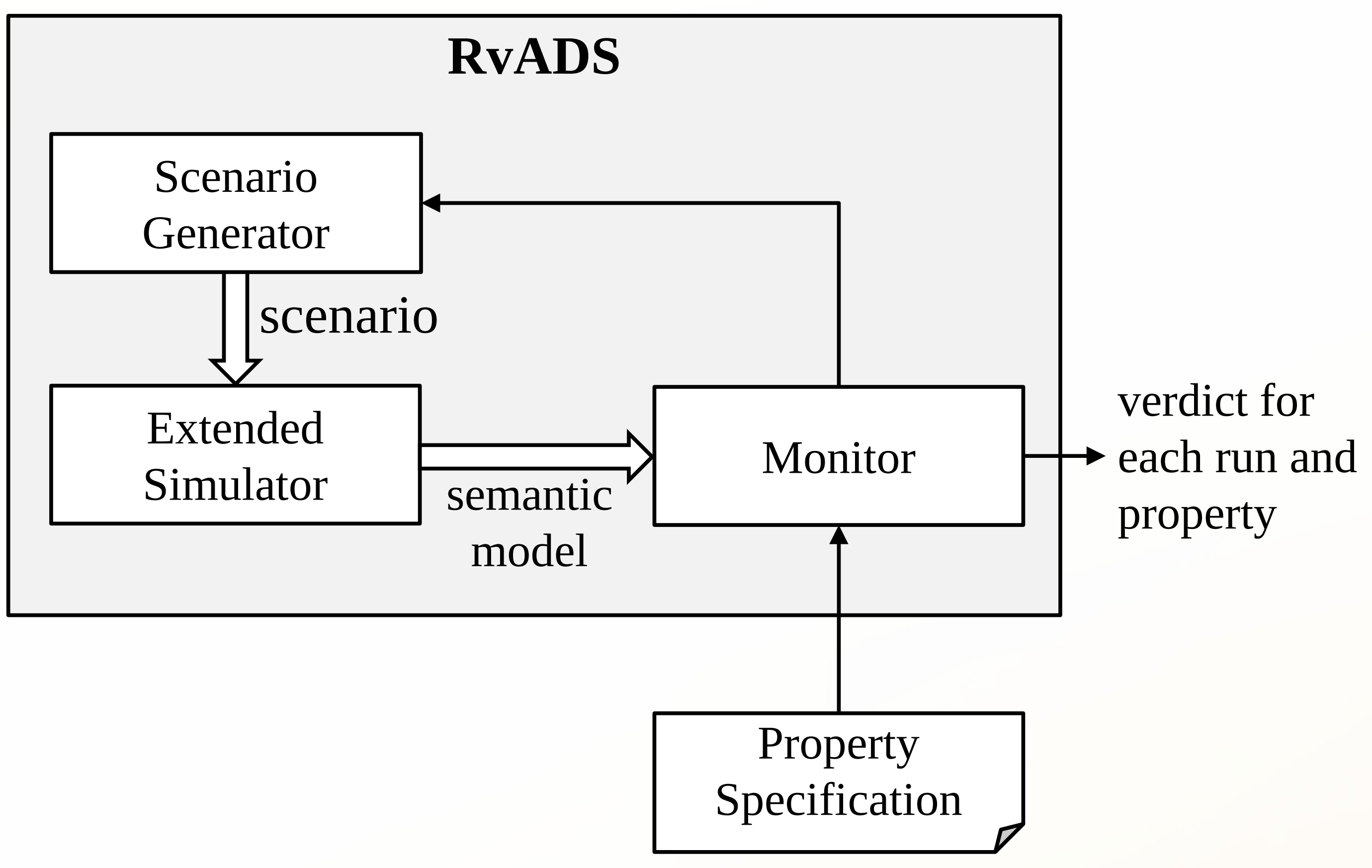
We investigate a rigorous simulation and testing-based validation method for autonomous driving systems that integrates an existing industrial simulator and a formally defined testing environment. The environment includes a scenario generator that drives the simulation process and a monitor that checks at runtime the observed behavior of the system against a set of system properties to be validated. The validation method consists in extracting from the simulator a semantic model of the simulated system including a metric graph, which is a mathematical model of the environment in which the vehicles of the system evolve. The monitor can verify properties formalized in a first-order linear temporal logic and provide diagnostics explaining their non-satisfaction. Instead of exploring the system behavior randomly as many simulators do, we propose a method to systematically generate sets of scenarios that cover potentially risky situations, especially for different types of junctions where specific traffic rules must be respected. We show that the systematic exploration of risky situations has uncovered many flaws in the real simulator that would have been very difficult to discover by a random exploration process.

## f c f f m

The Scenario Generator drives the simulation process. It generates scenarios as the coordinated sequences of actions executed by the agents in the Simulator.

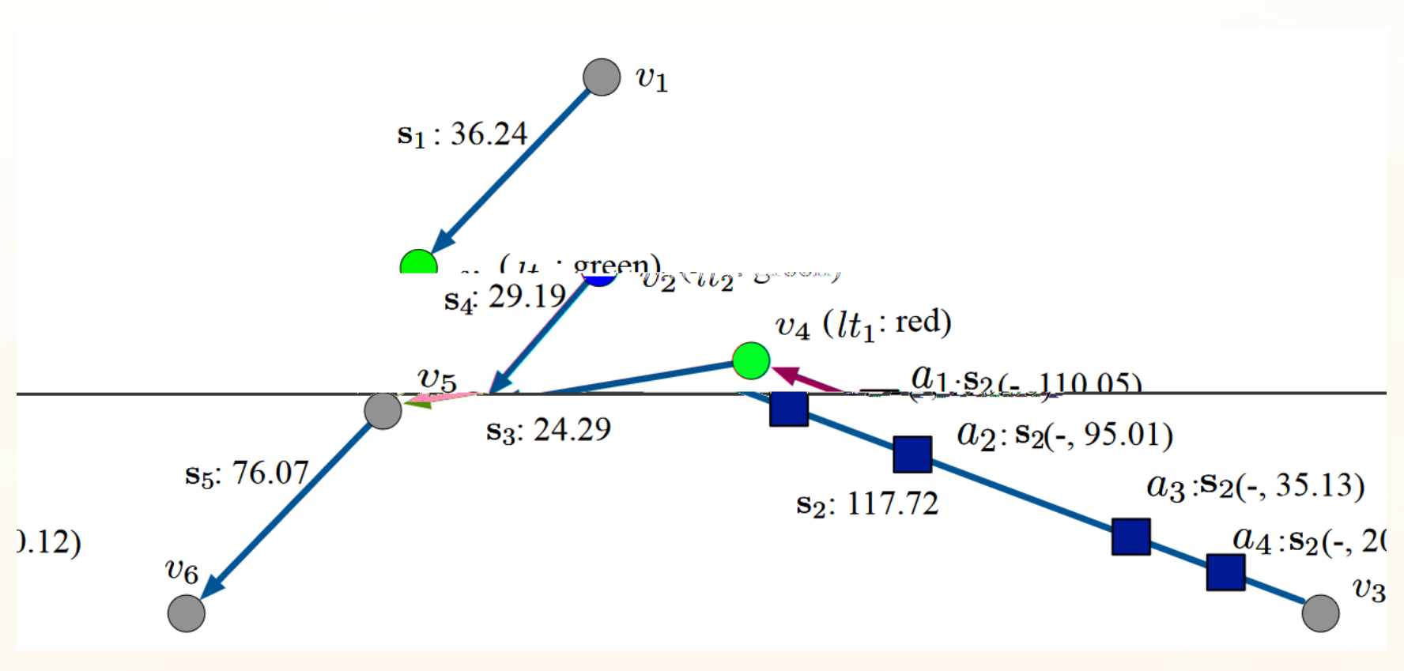
The Simulator executes an ADS model obtained as the composition of the world model and the behavior model.

The Monitor observes the system behavior as sequences of global states and applies a runtime verification method of the properties

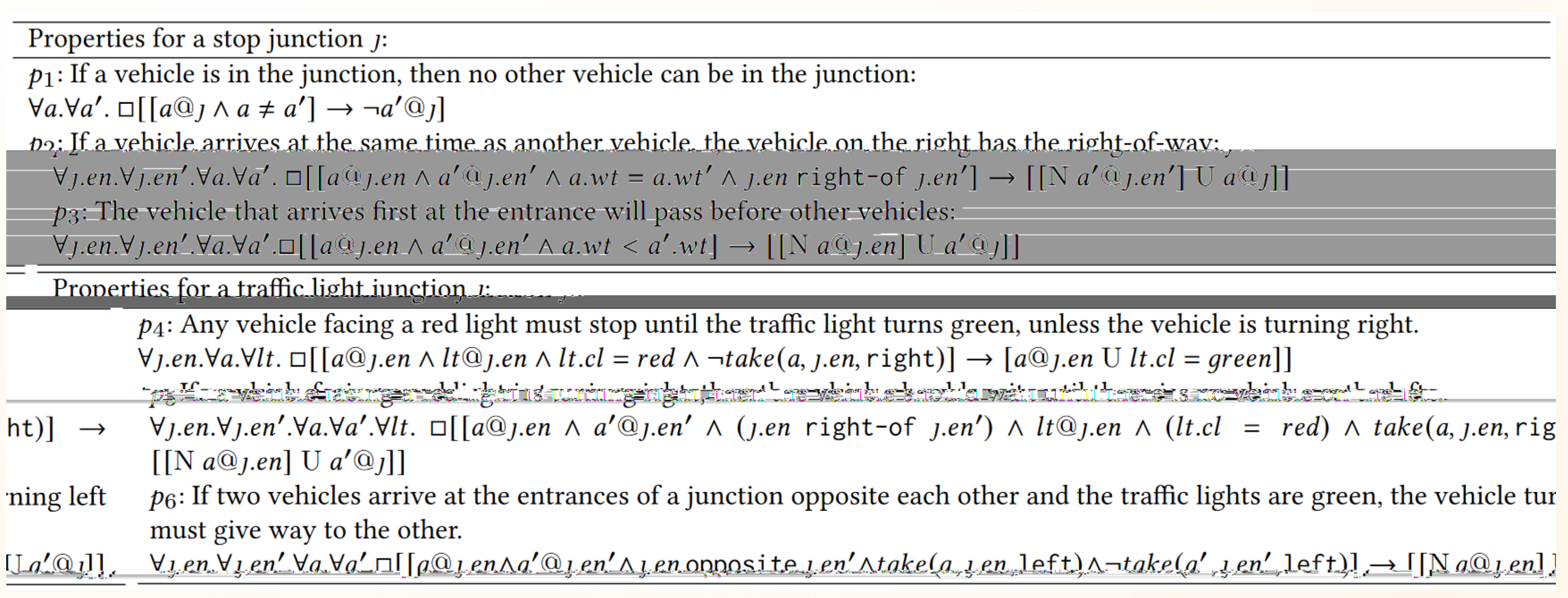


## f c

The system is modeled as a semantic model with a well-defined notion of system state as the distribution of vehicles and objects on a map with all their kinetic and time attributes.



## f p f


Properties for a stop junction $\jmath$:

$p_1$: If a vehicle is in the junction, then no other vehicle can be in the junction:
$\forall a.\forall a'.\ \Box[[a@\jmath \land a \neq a'] \rightarrow \neg a'@\jmath]$

$p_2$: If a vehicle arrives at the same time as another vehicle, the vehicle on the right has the right-of-way:
$\forall \jmath.en.\forall \jmath.en'.\forall a.\forall a'.\ \Box[[a@\jmath.en \land a'@\jmath.en' \land a.wt = a.wt' \land \jmath.en\ \texttt{right-of}\ \jmath.en'] \rightarrow [[\mathrm{N}\ a'@\jmath.en'] \ \mathrm{U}\ a@\jmath]]$

$p_3$: The vehicle that arrives first at the entrance will pass before other vehicles:
$\forall \jmath.en.\forall \jmath.en'.\forall a.\forall a'.\Box[[a@\jmath.en \land a'@\jmath.en' \land a.wt < a'.wt] \rightarrow [[\mathrm{N}\ a@\jmath.en]\ \mathrm{U}\ a'@\jmath]]$

Properties for a traffic light junction $\jmath$:

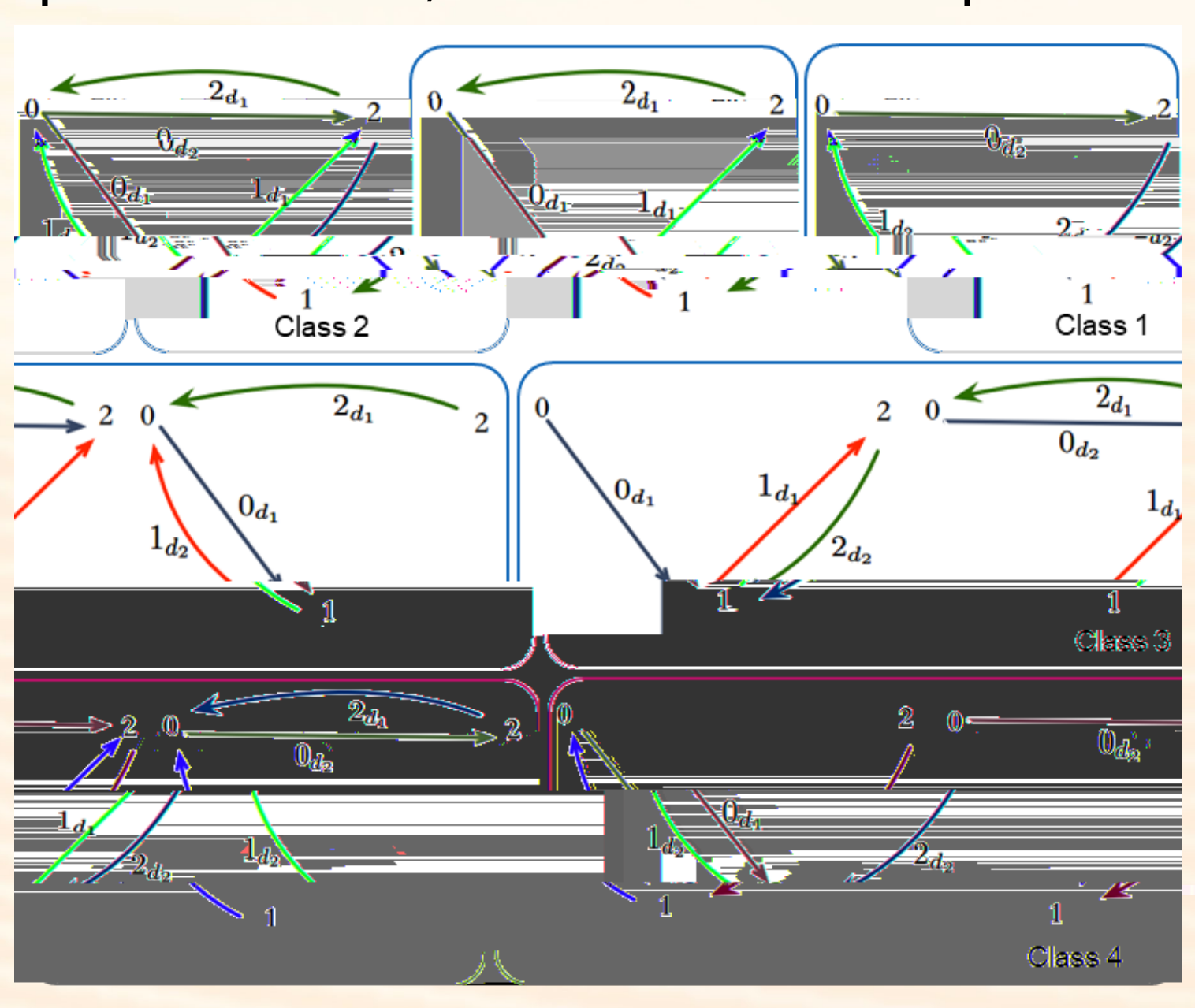
$p_4$: Any vehicle facing a red light must stop until the traffic light turns green, unless the vehicle is turning right.
$\forall \jmath.en.\forall a.\forall lt.\ \Box[[a@\jmath.en \land lt@\jmath.en \land lt.cl = red \land \neg take(a, \jmath.en, \mathrm{right})] \rightarrow [a@\jmath.en\ \mathrm{U}\ lt.cl = green]]$

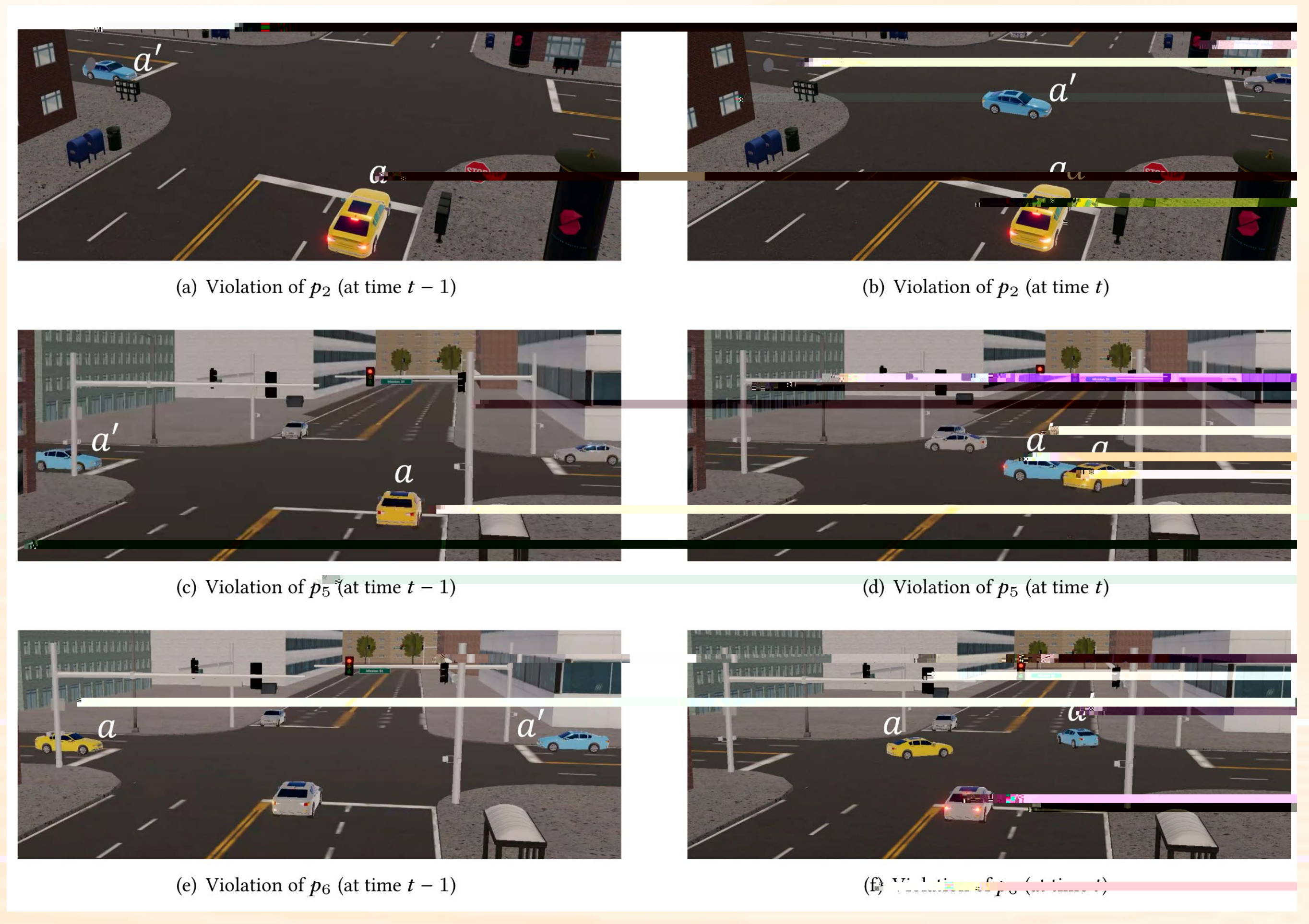
$p_5$: [illegible]
ht)] $\rightarrow$ $\forall \jmath.en.\forall \jmath.en'.\forall a.\forall a'.\forall lt.\ \Box[[a@\jmath.en \land a'@\jmath.en' \land (\jmath.en\ \texttt{right-of}\ \jmath.en') \land lt@\jmath.en \land (lt.cl = red) \land take(a, \jmath.en, \mathrm{rig}$
$[[\mathrm{N}\ a@\jmath.en]\ \mathrm{U}\ a'@\jmath]]$

ning left $p_6$: If two vehicles arrive at the entrances of a junction opposite each other and the traffic lights are green, the vehicle tur must give way to the other.
$\mathrm{U}\ a'@\jmath]]$, $\forall \jmath.en.\forall \jmath.en'.\forall a.\forall a'.\Box[[a@\jmath.en \land a'@\jmath.en' \land \jmath.en\ \mathrm{opposite}\ \jmath.en' \land take(a, \jmath.en, \mathrm{left}) \land \neg take(a', \jmath.en', \mathrm{left})] \rightarrow [[\mathrm{N}\ a@\jmath.en]$

## f f c f f p f c f

We define structurally equivalent abstract scenarios by simply rotating the inputs and preserving the symbolic directions based on the assumption that the traffic rules do not particularize the inputs of the junction according to their positions.
It is sufficient to apply one test case per equivalence class for the system that is assumed to be consistent. If equivalent test scenarios differ in the properties tested, it means that test process is inconsistent.




(a) Violation of $p_2$ (at time $t-1$)
(b) Violation of $p_2$ (at time $t$)
(c) Violation of $p_5$ (at time $t-1$)
(d) Violation of $p_5$ (at time $t$)
(e) Violation of $p_6$ (at time $t-1$)
(f) [illegible]