Introduction to runtime monitoring

Jonathan Julián Huerta y Munive
Industrial Test and Verification

Checking a system

Model checking

input: system model
input: specification
output: counterexample

guarantee:
any **modelled** behaviour of the system satisfies the specification

Runtime monitoring

input: system trace
input: specification
output: verdict

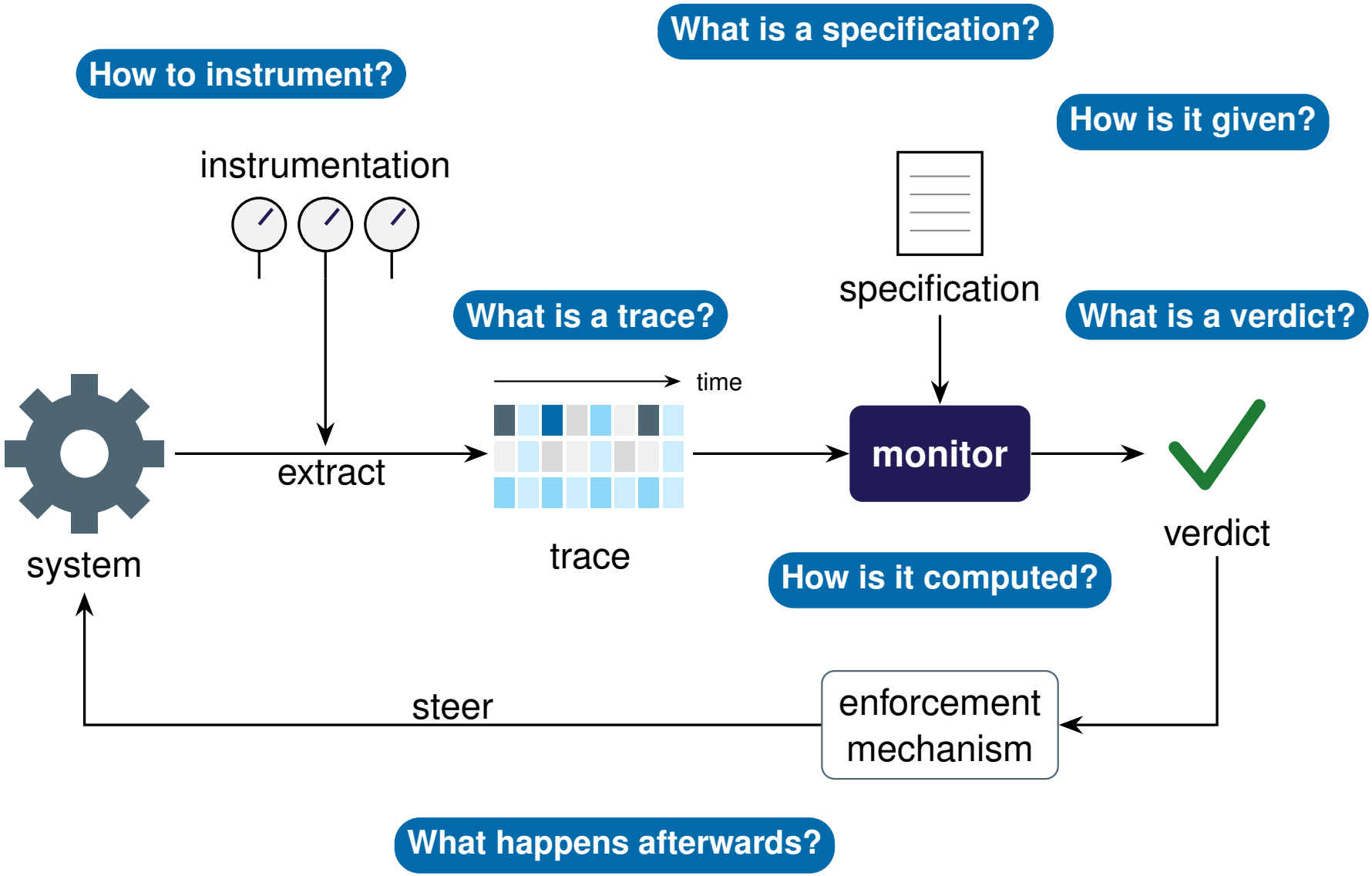
guarantee:
on the **real inputs** the behaviour of the system satisfies the specification

Software testing

input: system
input: test cases
output: failed assertion

guarantee:
on the **test inputs** the behaviour of the system satisfies the specification

Monitoring and enforcement



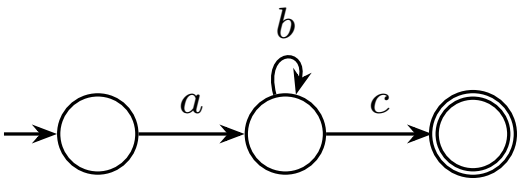
Specification: paradigms

ab^*c

regular expression

$p \rightarrow \mathrm{F}\, q$

logic



automaton



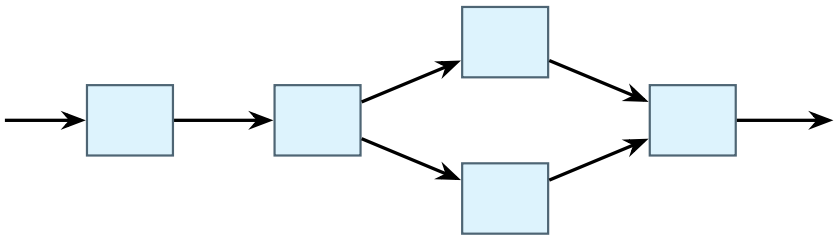
implicit

```
SELECT * FROM
```

SQL

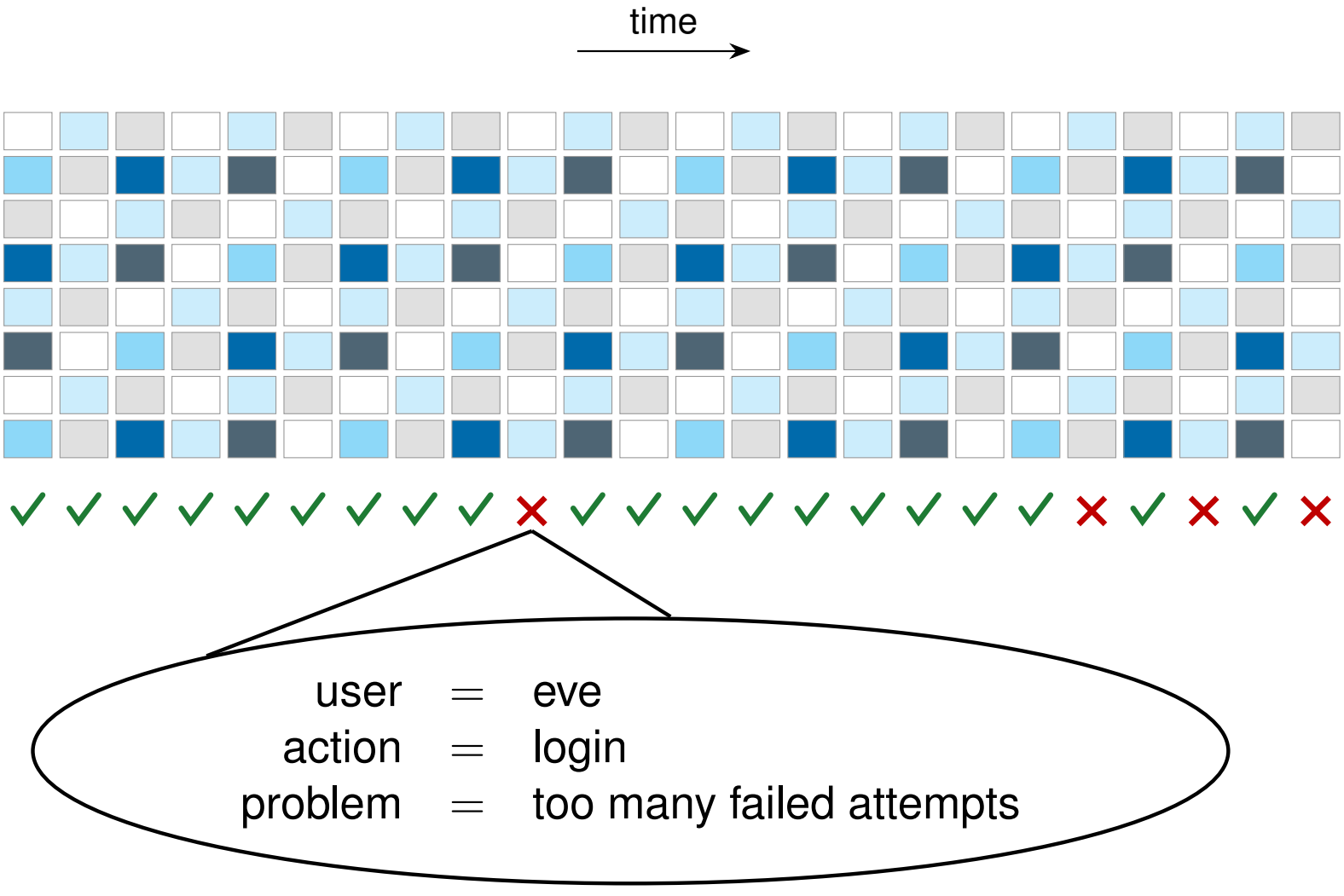
```
if (fails[u] > 3)
  alarm(u);
if (login(u))
  fails[u] = 0;
```

code



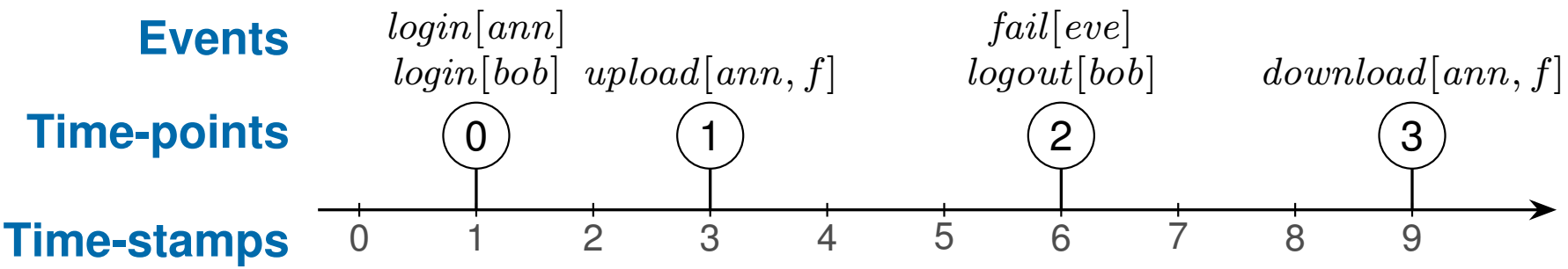
stream processor

Verdicts


time
user = eve
action = login
problem = too many failed attempts

Trace model

- `12:00:01  INFO login user=ann`
- `12:00:01  INFO login user=bob`
- `12:00:03  INFO upload user=ann file=f`
- `12:00:06  WARN failed login user=eve`
- `12:00:06  INFO logout user=bob`
- `12:00:09  INFO download user=ann file=f`



References

Slides 2–6 are adapted from:

Srđan Krstić. *Runtime Monitoring*. Lecture slides, FMSEC Modules 10 & 11. Institute of Information Security, ETH Zurich, 2020.