Environment Models Decomposition

Ilia Zakharov

Ilja.zakharov@ispras.ru

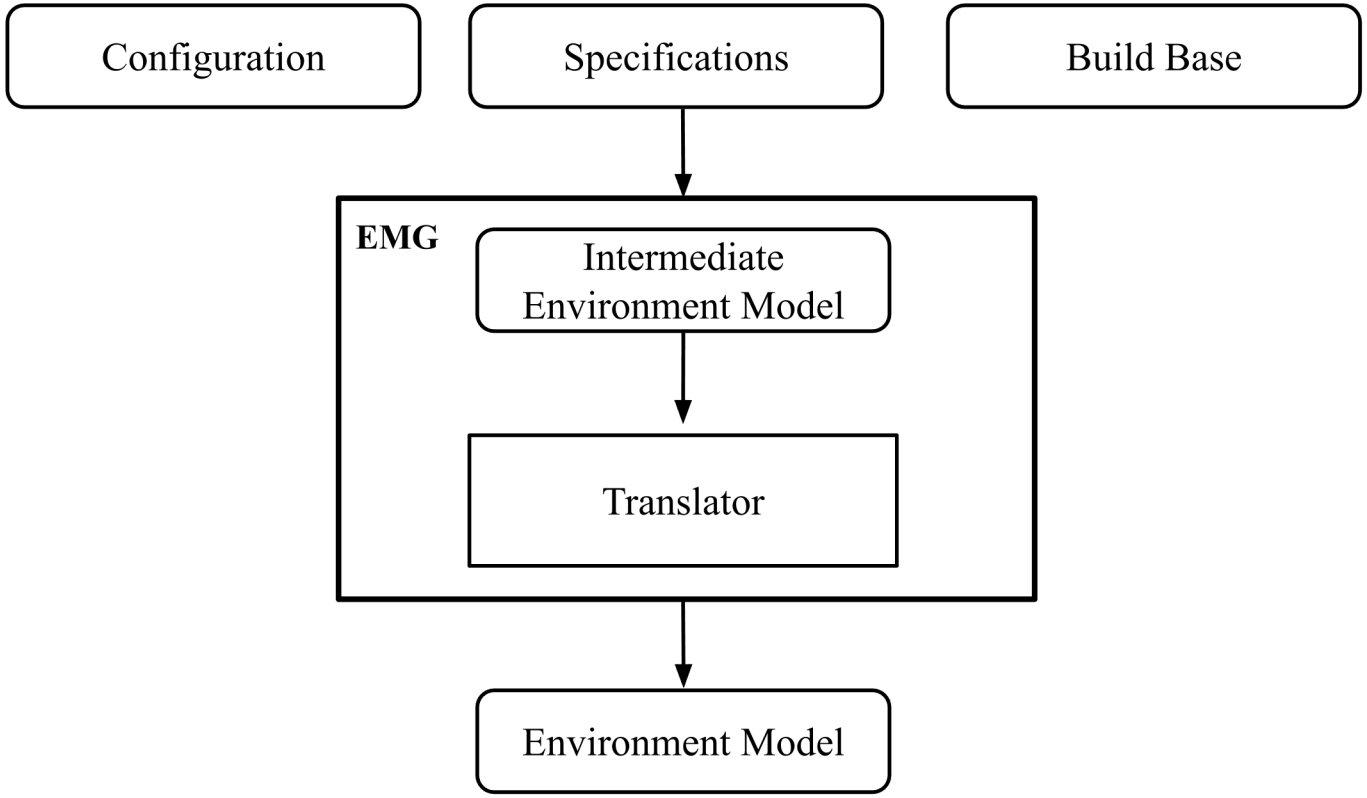
Ivannikov Institute For System Programming of RAS

Motivation

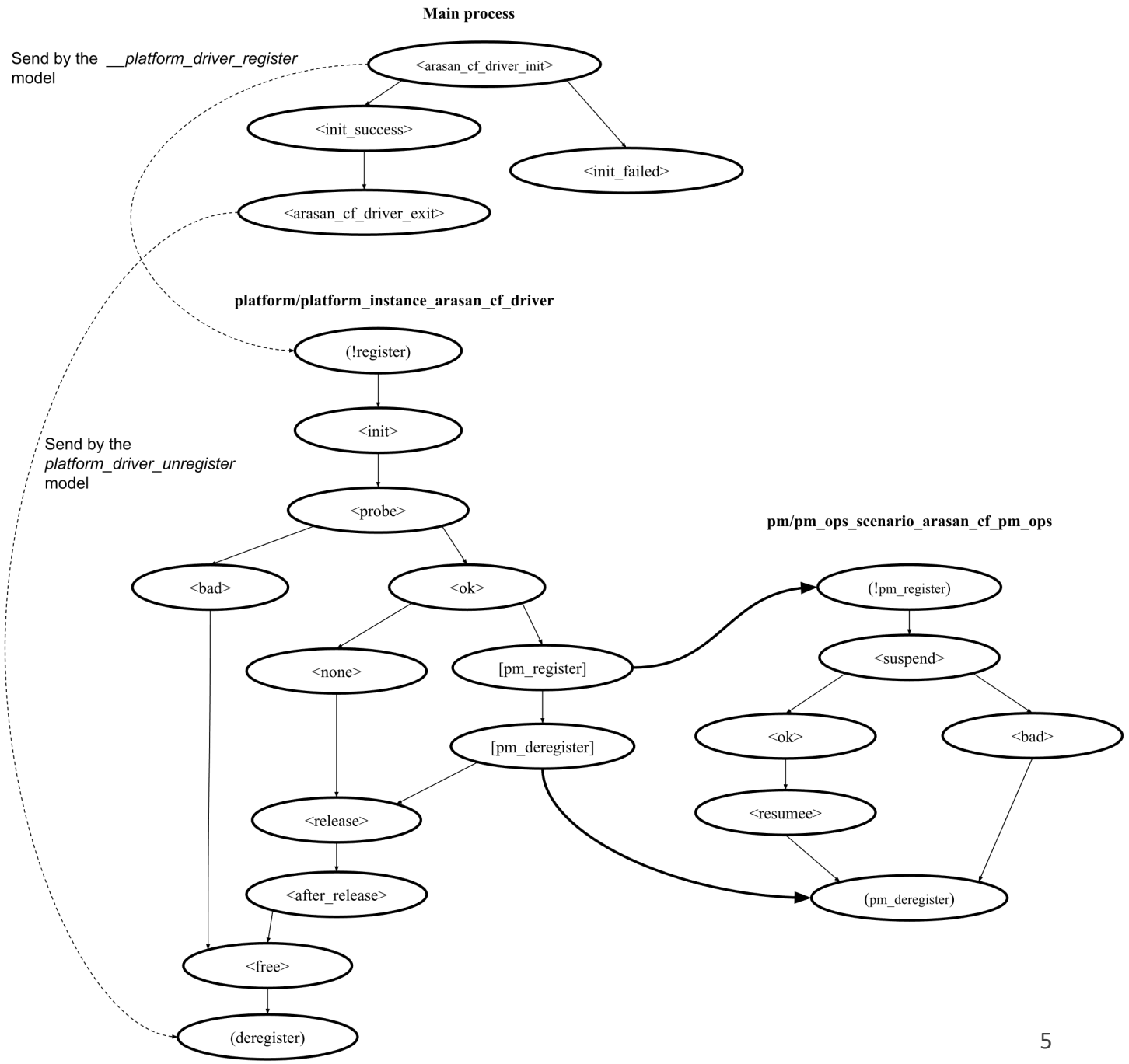
Thorough Verification of a Kernel Module

- Manually designed environment model
  - High verification code coverage
  - Carefully initialized data structures to avoid undefined values
- Functional requirements checking
  - pre- and post- conditions
  - Separated specific sequences of callback calls
  - Different setups of an environment model
    - Enabled or forbidden function models failing
    - Different sets of values for input data structures

Environment Model Generator



Intermediate Environment Model

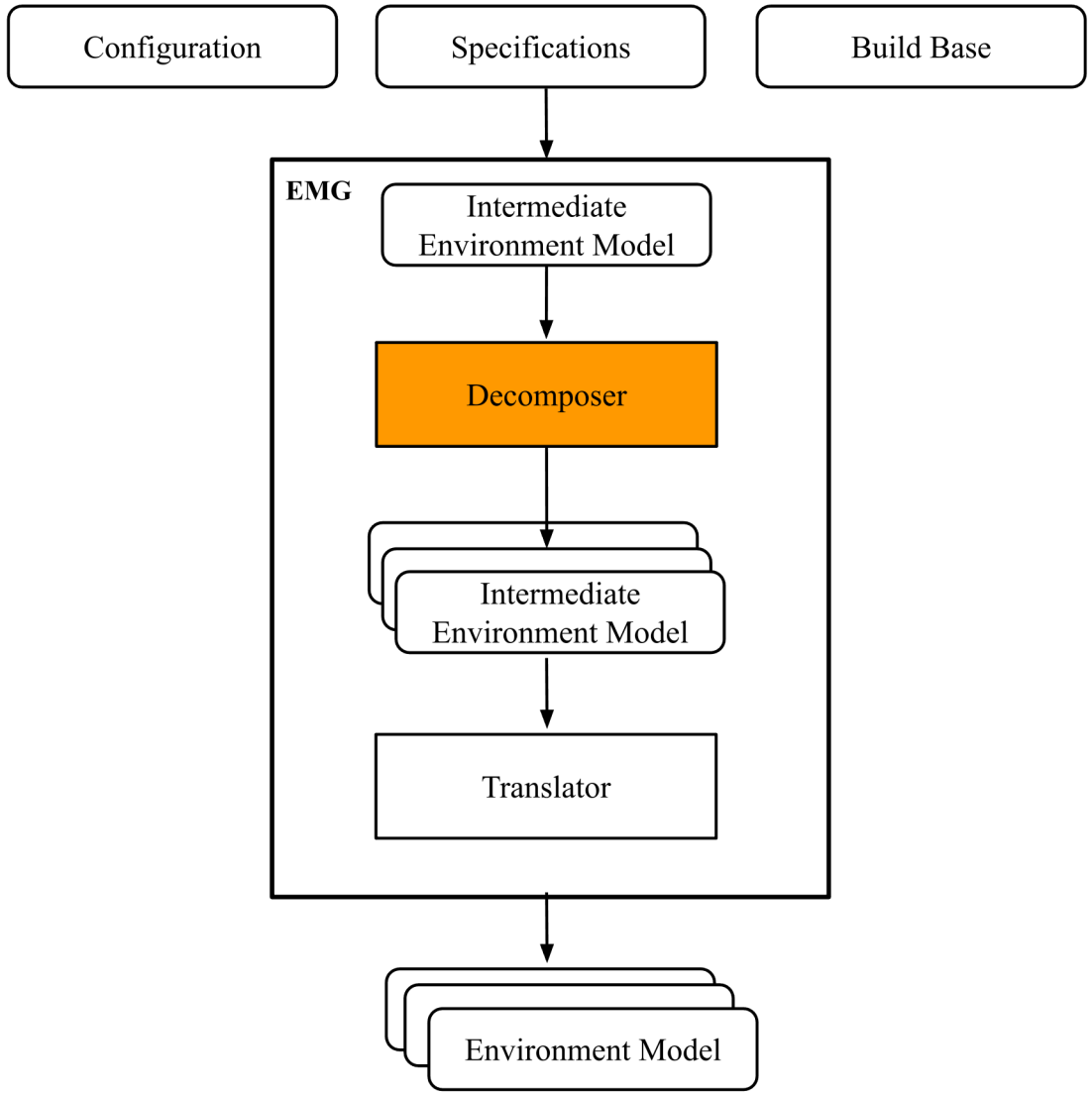


Problems

- Too many options: it obscures the analysis
- Too long time needed to reach “deep code”
- Any revealed error prevents analysis of other paths
- Some environment model setups are incompatible
- Error traces are overloaded

Method

Environment Model Generator with Decomposer



Decomposition

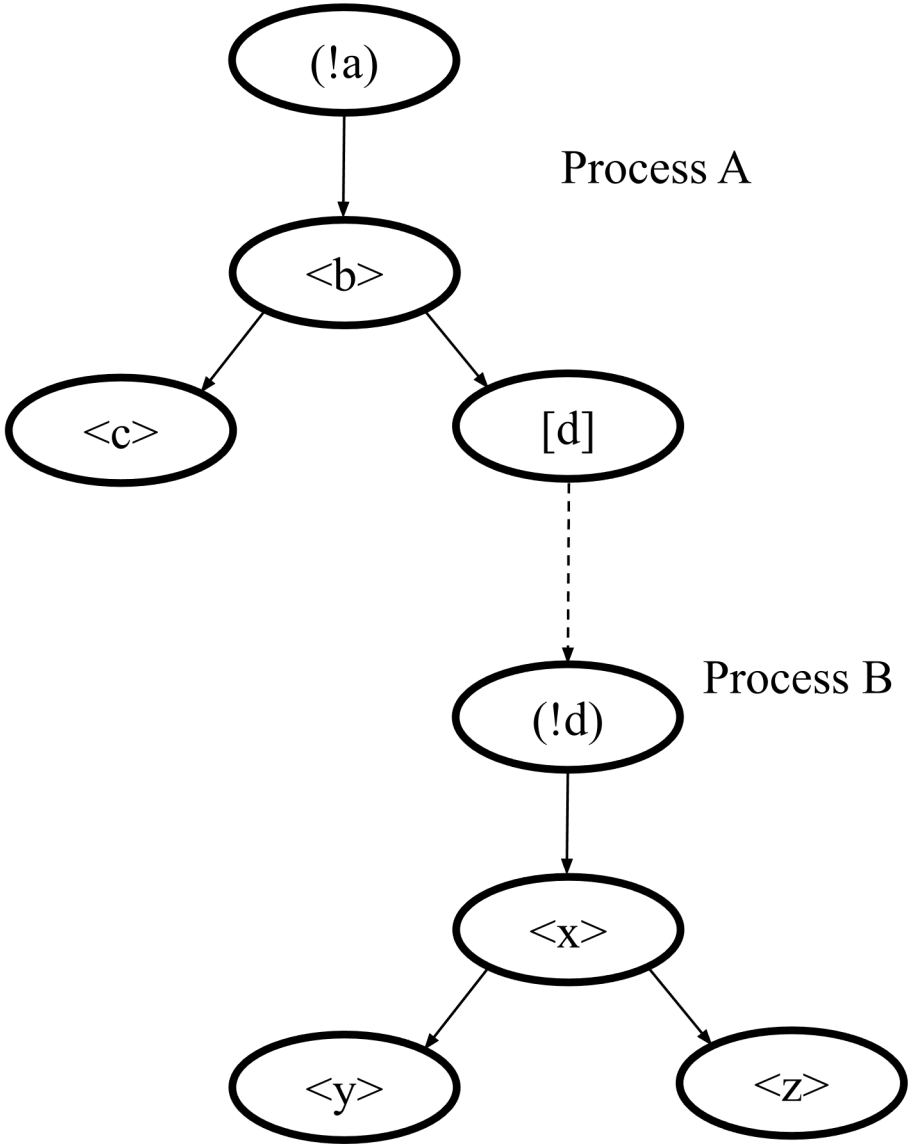
Process Decomposition:

Separate *processes* into *scenarios*

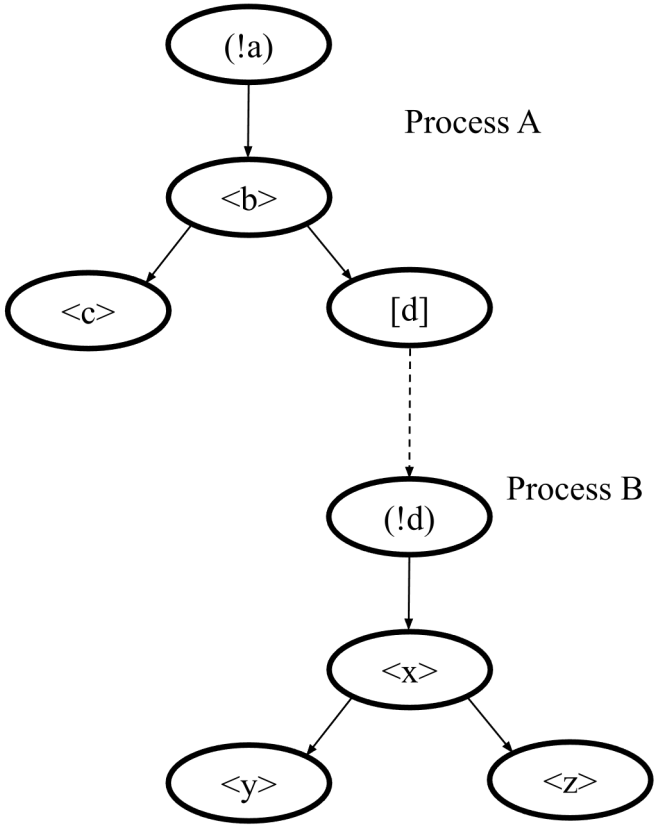
Scenario Selection:

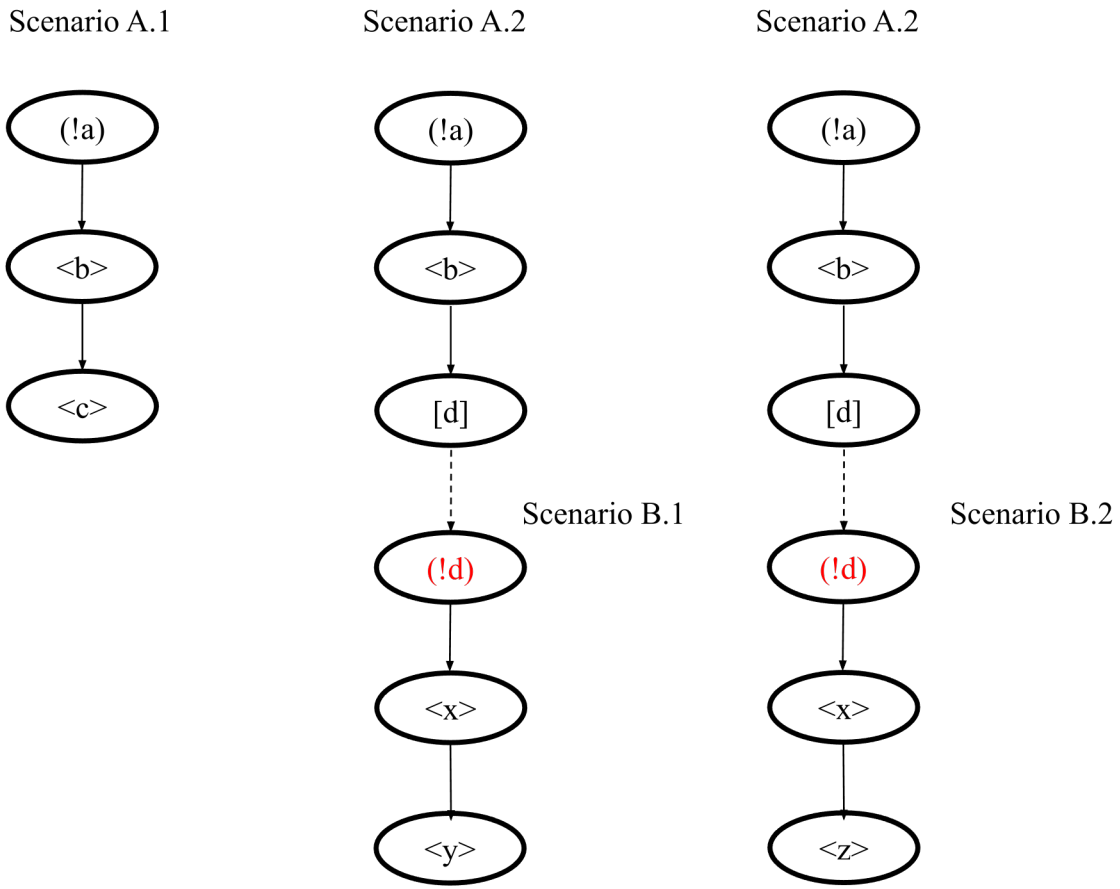
Combine new models by replacing original processes with newly generated scenarios

Example of Process Decomposition



Process Decomposition

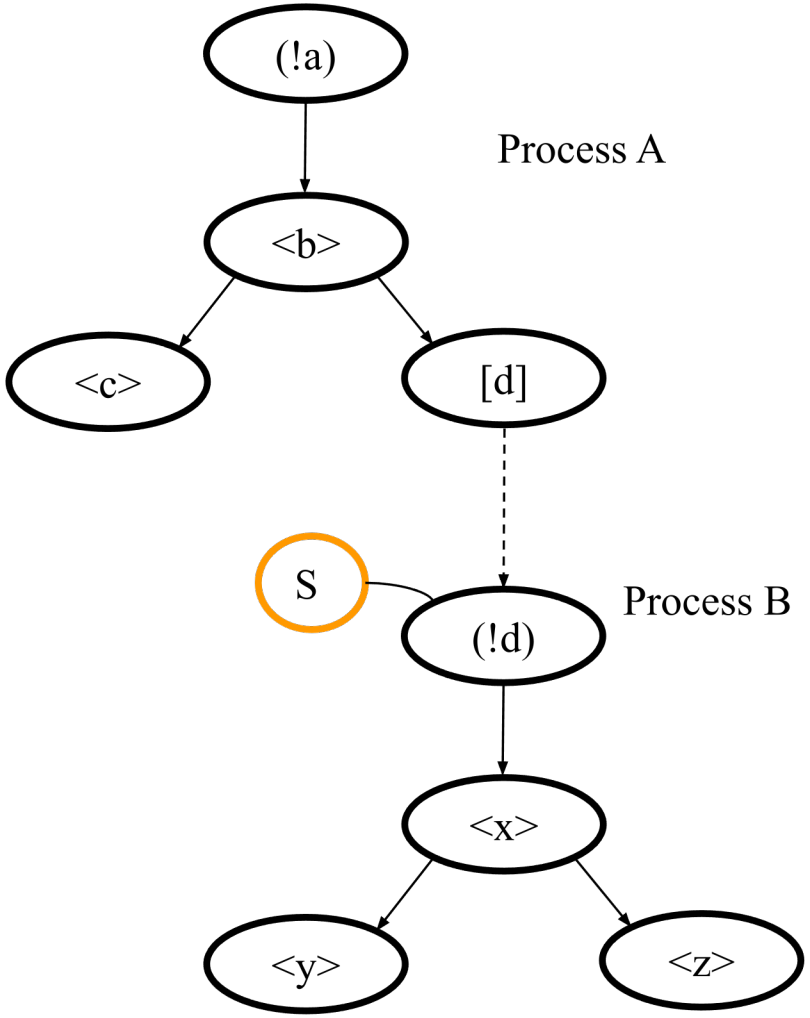




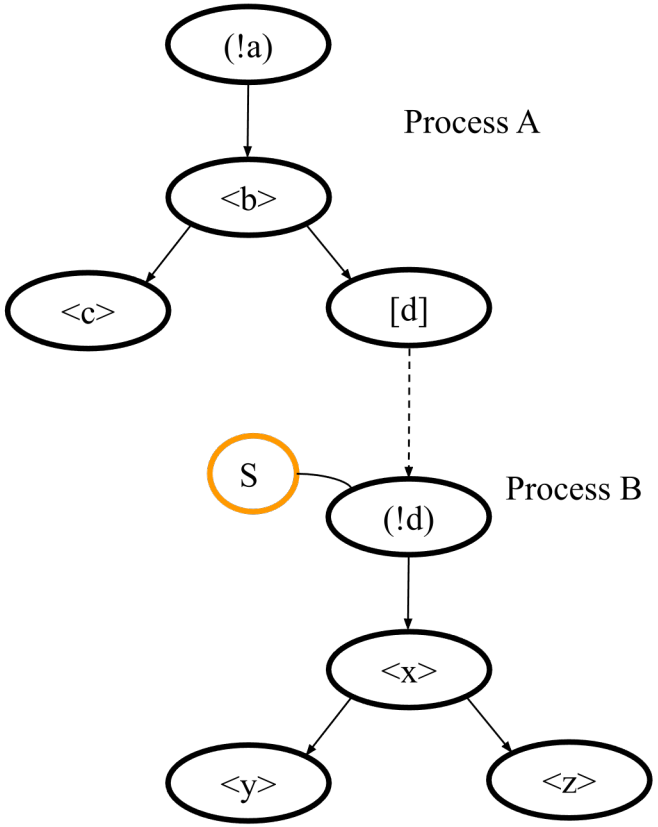
Impact

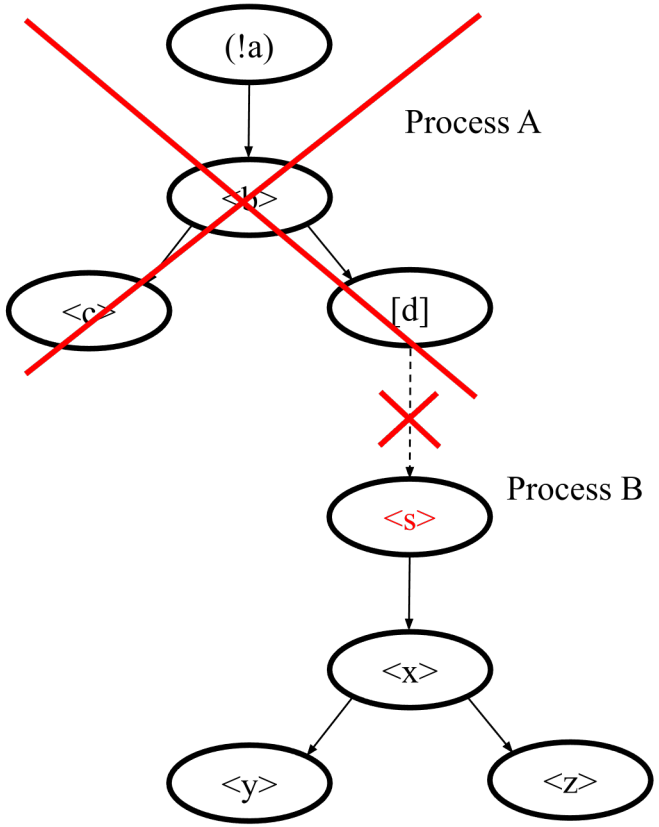
- Less timeout results
- Easy development of environment models
- No more stucking after the first found error

Example with Savepoint



Model with Savepoint

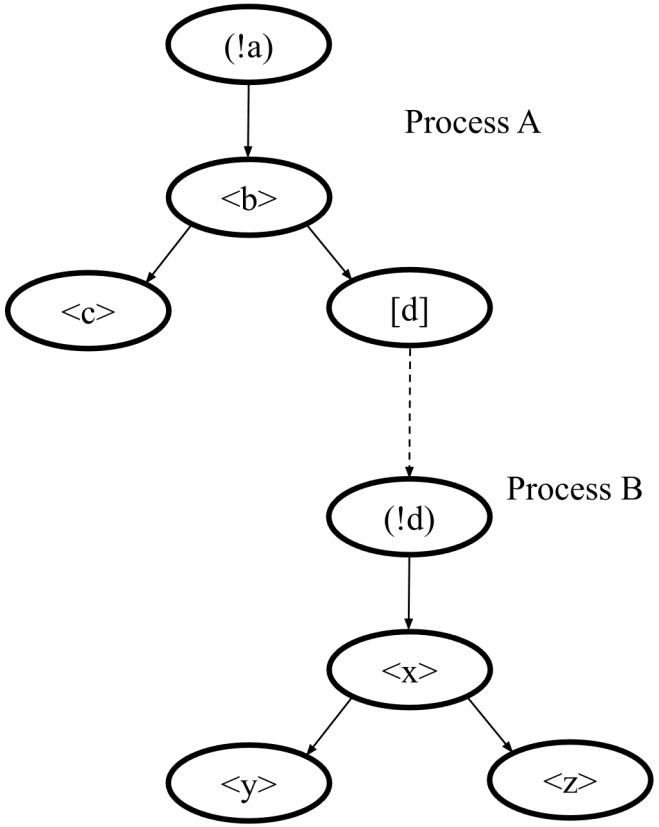


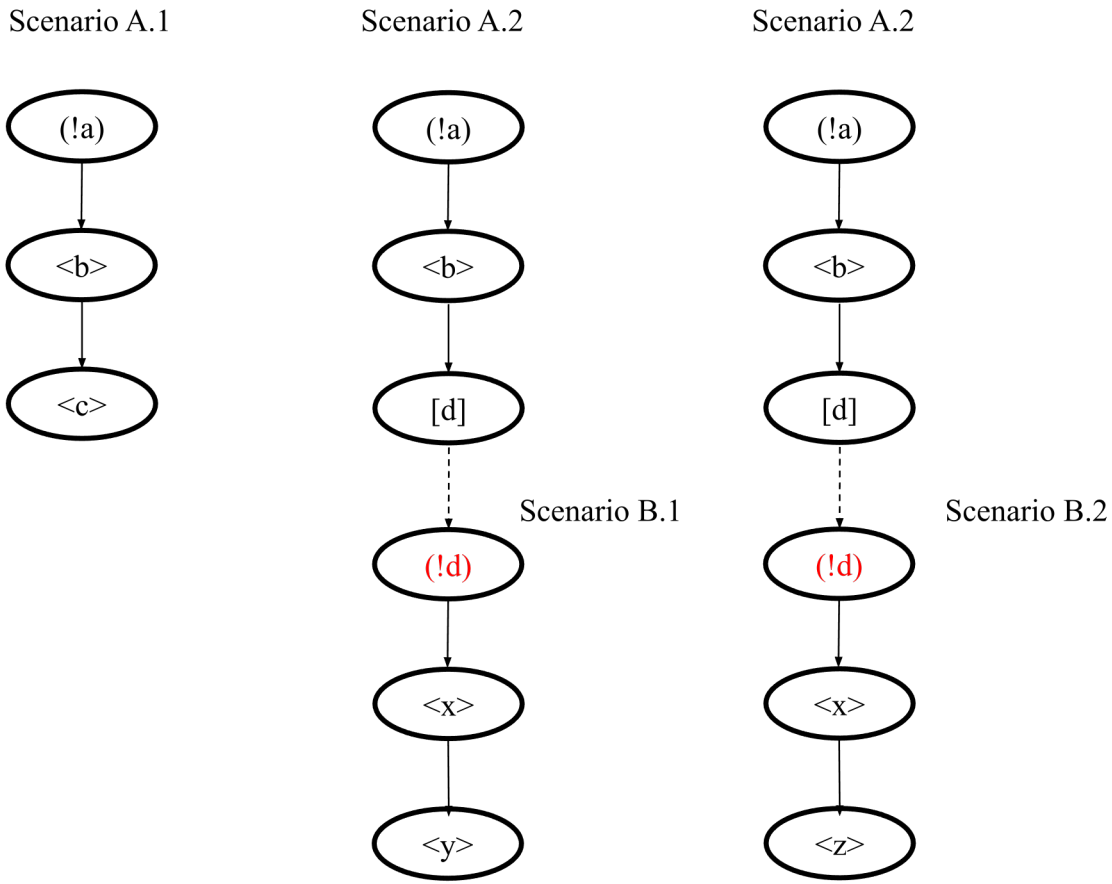


Impact

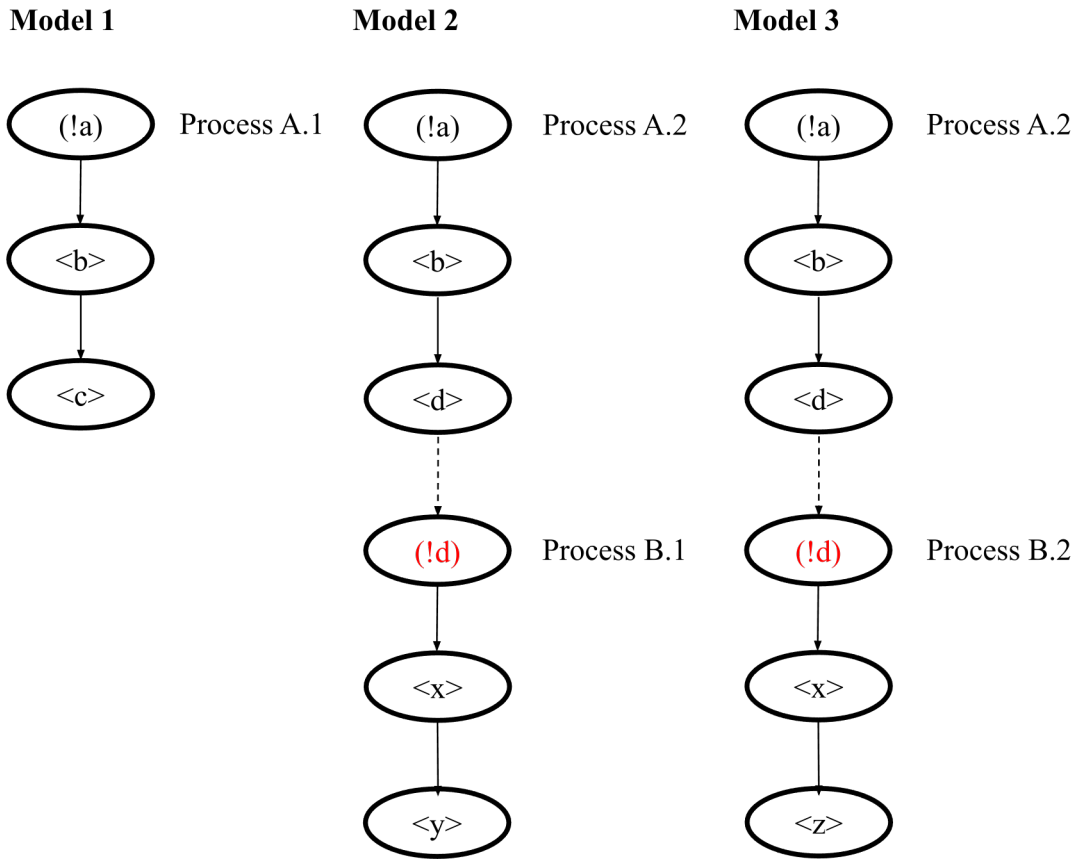
- Less timeout results
- Reduce the number of environment models
- Different setups of an environment model
- Straightforward error traces

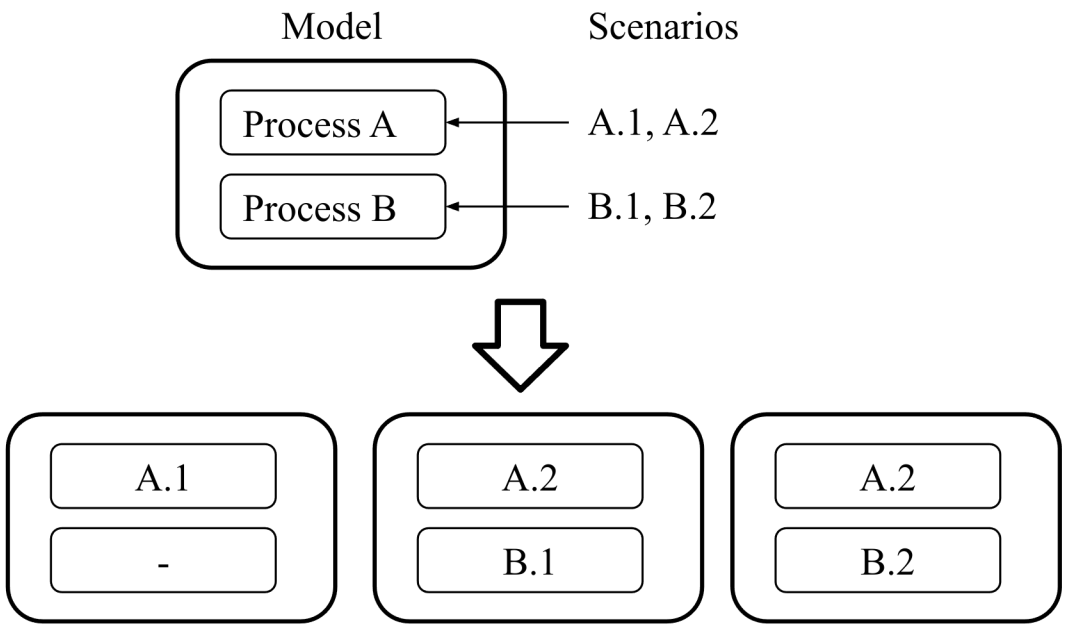
Scenarios


(!a)
Process A
<b>
<c>
[d]
Process B
(!d)
<x>
<y>
<z>

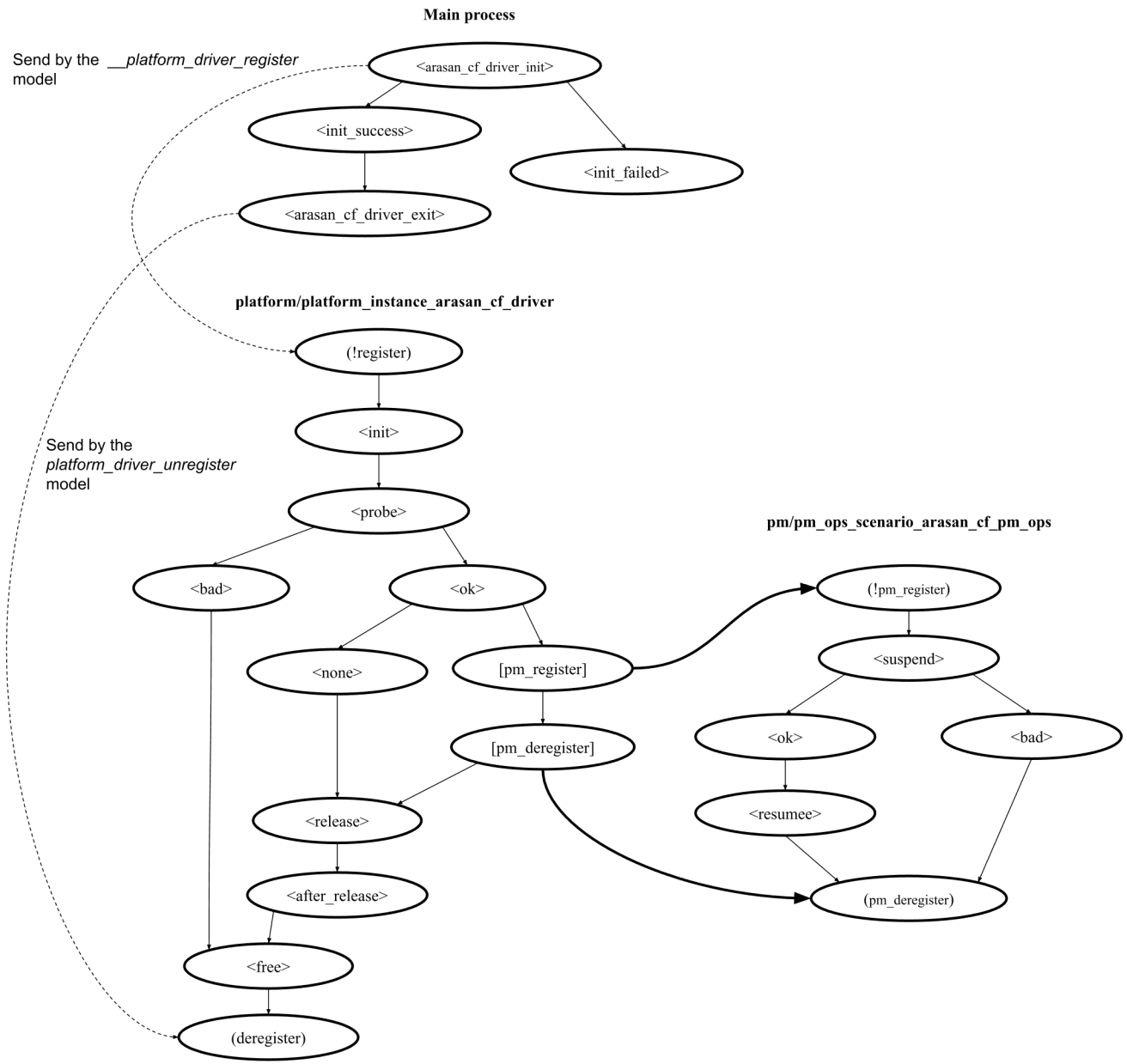

Scenario A.1
Scenario A.2
Scenario A.2
(!a)
<b>
<c>
(!a)
<b>
[d]
Scenario B.1
(!d)
<x>
<y>
(!a)
<b>
[d]
Scenario B.2
(!d)
<x>
<z>

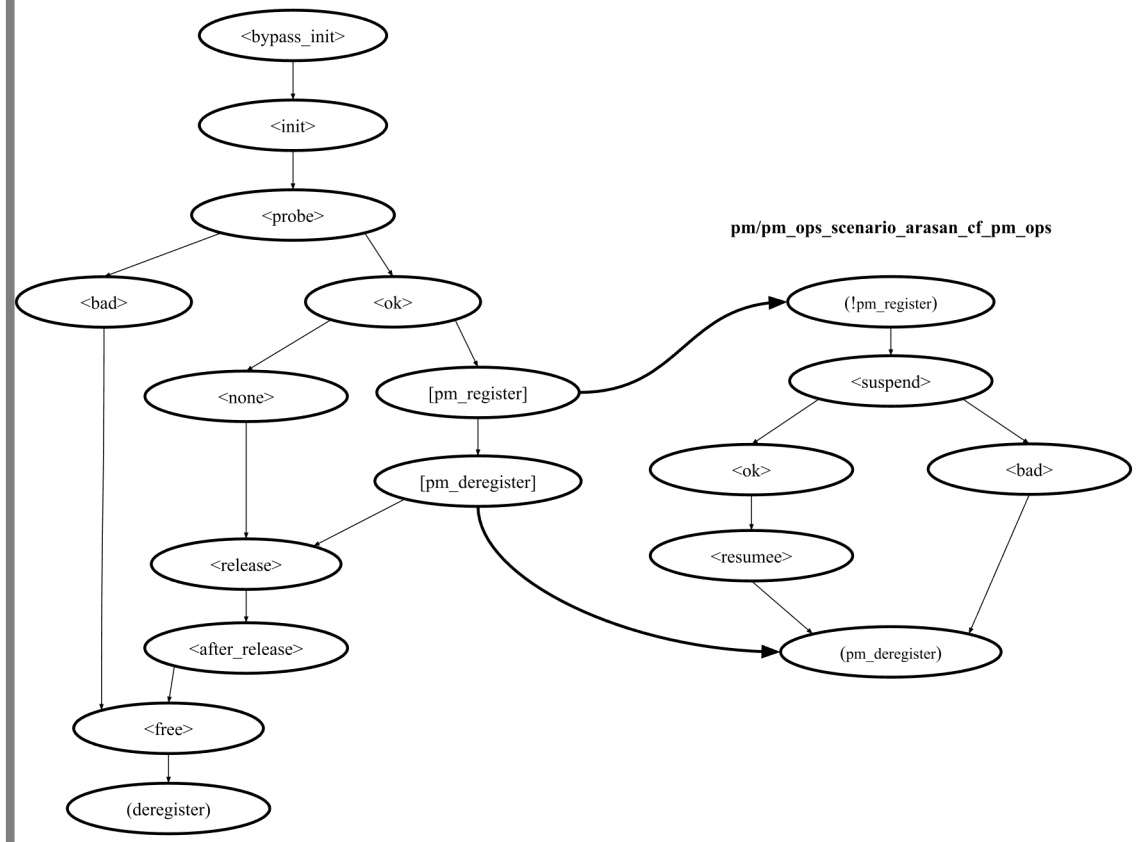
Scenario Selection

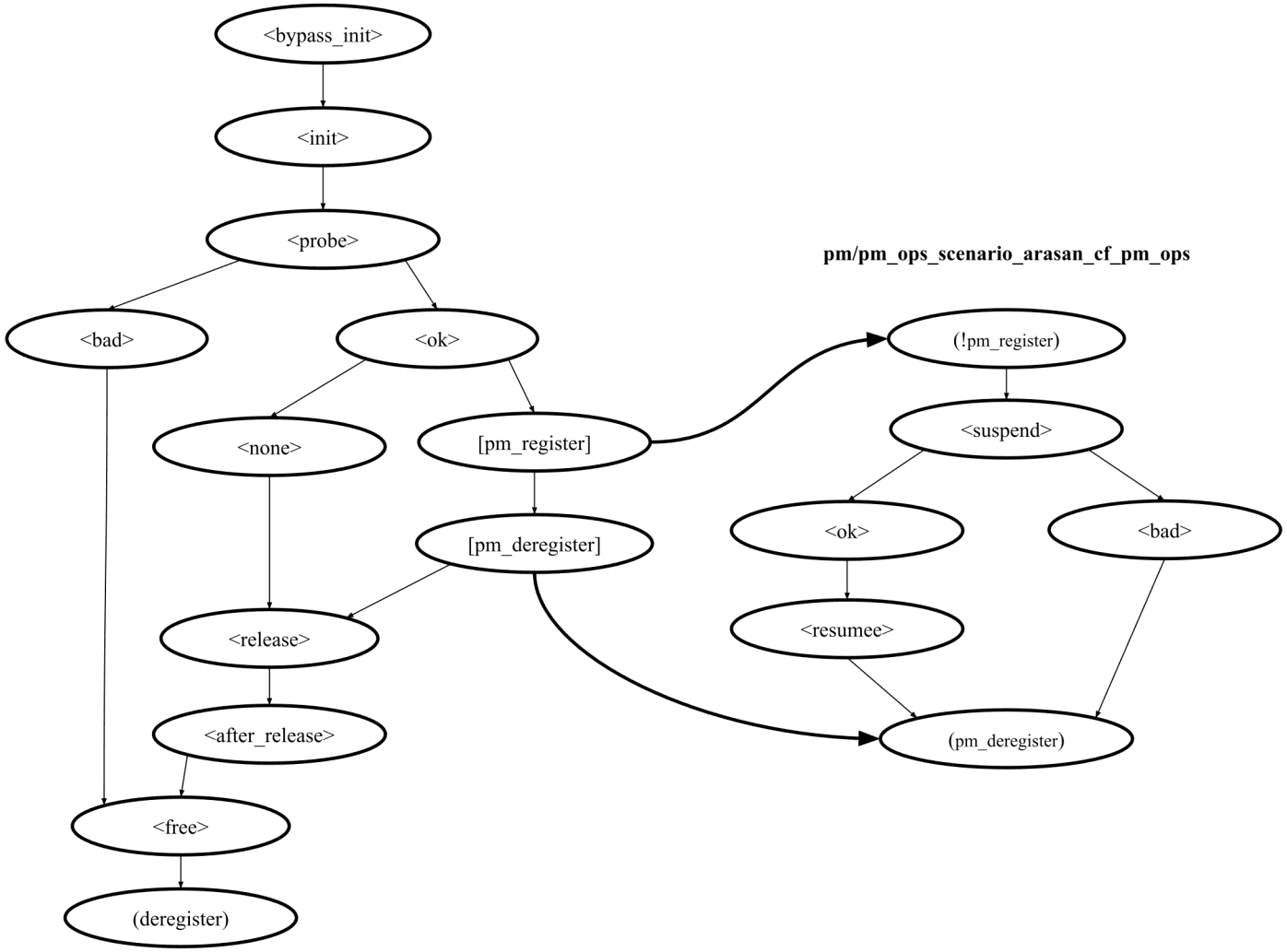


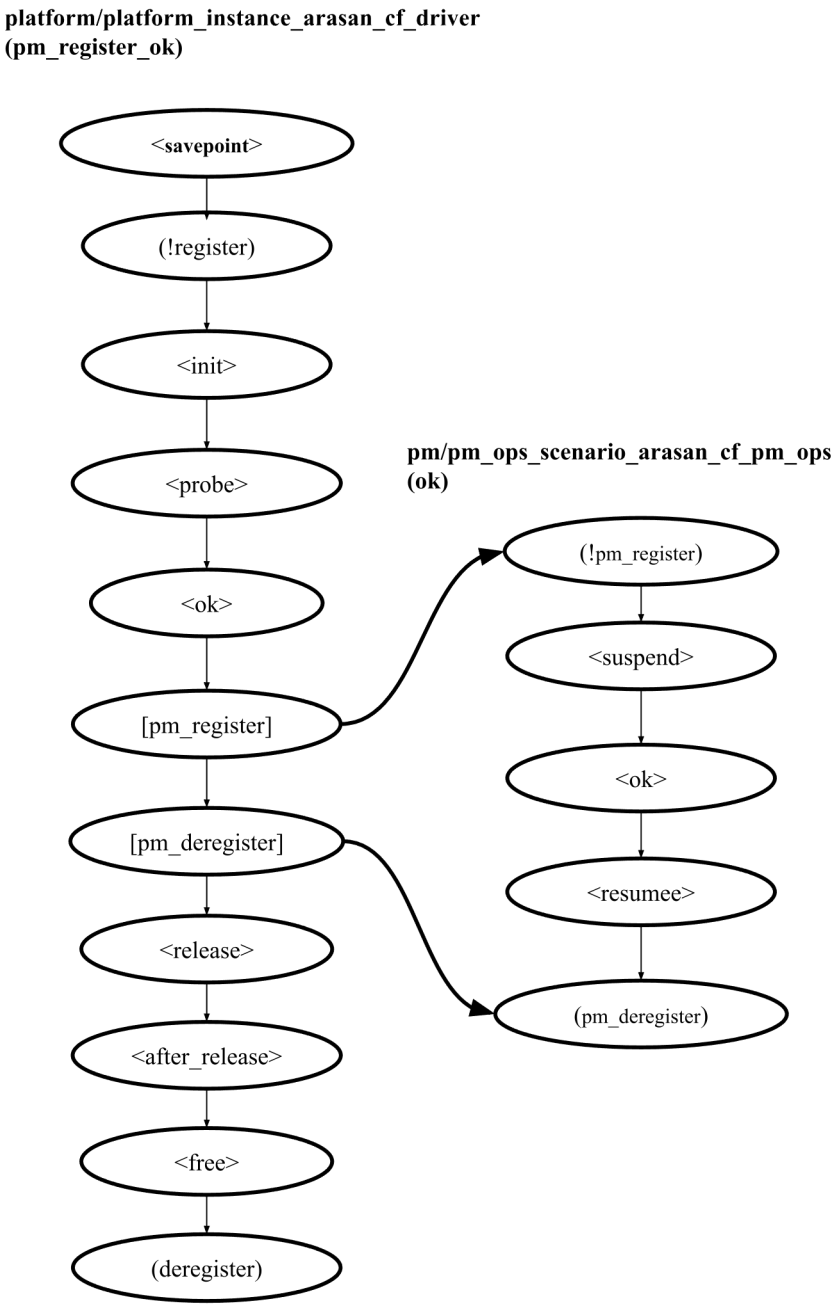


Demo


Main process
Send by the __platform_driver_register model
<arasan_cf_driver_init>
<init_success>
<init_failed>
<arasan_cf_driver_exit>
platform/platform_instance_arasan_cf_driver
(!register)
<init>
Send by the platform_driver_unregister model
<probe>
<bad>
<ok>
<none>
[pm_register]
[pm_deregister]
<release>
<after_release>
<free>
(deregister)
pm/pm_ops_scenario_arasan_cf_pm_ops
(!pm_register)
<suspend>
<ok>
<bad>
<resumee>
(pm_deregister)


pm/pm_ops_scenario_arasan_cf_pm_ops
<bypass_init>
<init>
<probe>
<bad>
<ok>
<none>
[pm_register]
[pm_deregister]
<release>
<after_release>
<free>
(deregister)
(!pm_register)
<suspend>
<ok>
<bad>
<resumee>
(pm_deregister)


pm/pm_ops_scenario_arasan_cf_pm_ops
<bypass_init>
<init>
<probe>
<bad>
<ok>
<none>
[pm_register]
[pm_deregister]
<release>
<after_release>
<free>
(deregister)
(!pm_register)
<suspend>
<ok>
<bad>
<resumee>
(pm_deregister)


platform/platform_instance_arasan_cf_driver
(pm_register_ok)
<savepoint>
(!register)
<init>
<probe>
<ok>
[pm_register]
[pm_deregister]
<release>
<after_release>
<free>
(deregister)
pm/pm_ops_scenario_arasan_cf_pm_ops
(ok)
(!pm_register)
<suspend>
<ok>
<resumee>
(pm_deregister)

Thank You