Case Study Mutex – Liveness analysis

(distributed in https://idcm.wp.mines-telecom.fr/idcm-tool/)

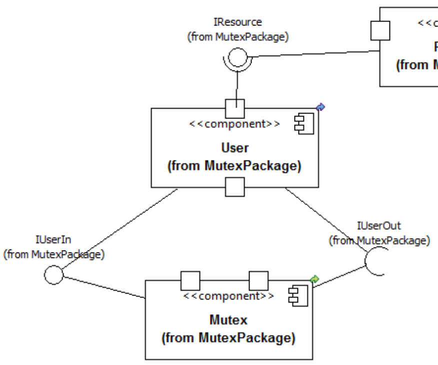
This case study models a system of two users who get in a task and get out the performed task using a tool. In a first version, the resource is modelled in a non-exclusive way. Conformance relation demonstrates that this model fits two requirements (sequential or parallel treatment of two tasks).

A second version of the Resource named ResourceExclusive is proposed in order to model an exclusive use. Conformance relation demonstrates that the new model fits again the two specifications.

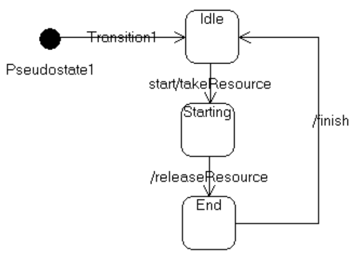
All diagrams and files refer to the MUTEX model downloaded on idcm.wp.mine-telecom/idem-tool. LTS, EXP.OPEN and BIP models are automatically generated using IDCM. For IDCM W1.0, LTS associated with architectures (EXP.OPEN models) are provided in the LTS directory since IDCM needs CADP toolbox to generate them.

1. Modelling a non-exclusive resource

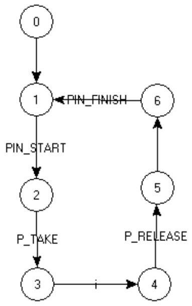
Component Diagrams :



State Machine of User:



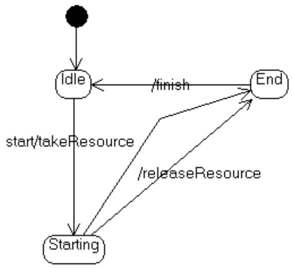
LTS of User:



BIP model of User[1]

```
package User
atomic type User
      export port Port PIN_START
      export port Port P_TAKE
      export port Port P_RELEASE
      export port Port PIN_FINISH
      port Port i
      place Pseudostate1,Idle,Idle_0,Starting,Starting_0,End,End_0
      initial to Pseudostate1
      on i from Pseudostate1 to Idle
      on PIN_START from Idle to Idle_0
      on P_TAKE from Idle_0 to Starting
      on i from Starting to Starting_0
      on P_RELEASE from Starting_0 to End
      on i from End to End_0
      on PIN_FINISH from End_0 to Idle
end
```

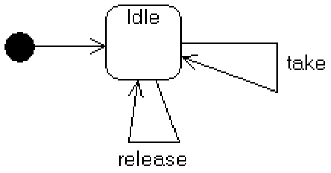
Let us consider the following model (Bad User) that have a non-deterministic behaviour implying that the tool is not systematically released.



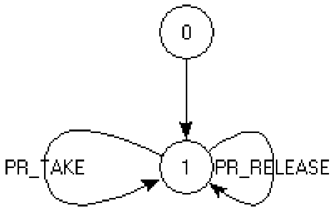
IDCM demonstrates that BadUser does not conform to User

[1] BIP models are not handled in IDCM1.0. and will be used for safety analysis

State machine of Resource:



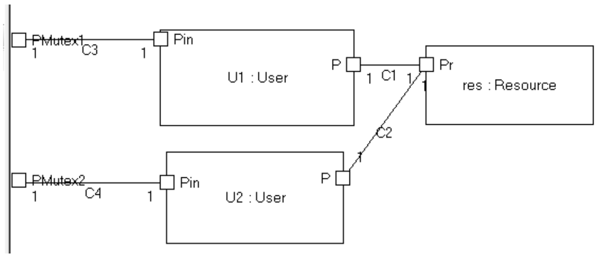
LTS of Resource :



BIP model of Resource:

```
package Resource

atomic type Resource
     export port Port PR_TAKE
     export port Port PR_RELEASE
     port Port i

     place Pseudostate1,Idle

     initial to Pseudostate1

     on i from Pseudostate1 to Idle
     on PR_TAKE from Idle to Idle
     on PR_RELEASE from Idle to Idle
end
```

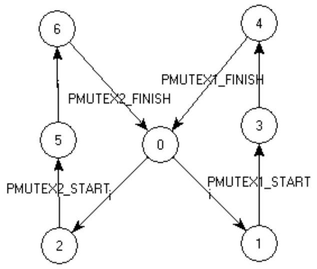
Composite Component Mutex:



EXP.OPEN model of the architecture Mutex:

```
hide C1_RELEASE, C1_TAKE, C2_RELEASE, C2_TAKE in
gate par using
_ * PIN_FINISH * _ -> PMUTEX1_FINISH,
_ * PIN_START * _ -> PMUTEX1_START,
_ * _ * PIN_FINISH -> PMUTEX2_FINISH,
_ * _ * PIN_START -> PMUTEX2_START,
PR_RELEASE * P_RELEASE * _ -> C1_RELEASE,
PR_TAKE * P_TAKE * _ -> C1_TAKE,
PR_RELEASE * _ * P_RELEASE -> C2_RELEASE,
PR_TAKE * _ * P_TAKE -> C2_TAKE
in
"Resource.bcg" || "User.bcg" || "User.bcg"
end par
end hide
```

Let us consider a specification (SpecMutexSequentialUsers.aut) where tasks may arrive on user U1 or user U2 but not on both. The specification is expressed with the following LTS:



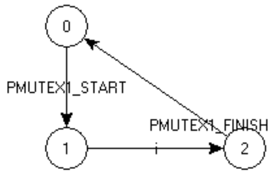
IDCM demonstrates that Mutex conforms to specification SpecMutexSequentialUsers

Let us consider a specification that allows two users to get task in parallel. The specification is expressed with the LTS obtained by the following specification (SpecMutex2ParallelUsers.exp):

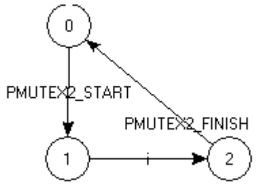
```
SpecUser1.bcg ||| SpecUser2.bcg
```

with

SpecUser1 (SpecUser1.aut) is:



SpecUser2 (SpecUser.aut) is:

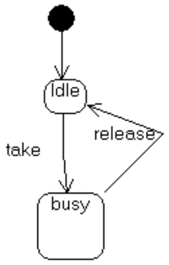


IDCM demonstrates that Mutex conforms to specification SpecMutex2ParallelUsers

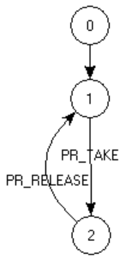
It implies that this model allows two tasks to be treated in parallel. It is not possible to conclude about the use of the tool in an exclusive or non-exclusive way. A safety property analysis is required for this evaluation. (see IDCM 2.0)

2. Modelling an exclusive resource

State machine of ResourceExclusive:



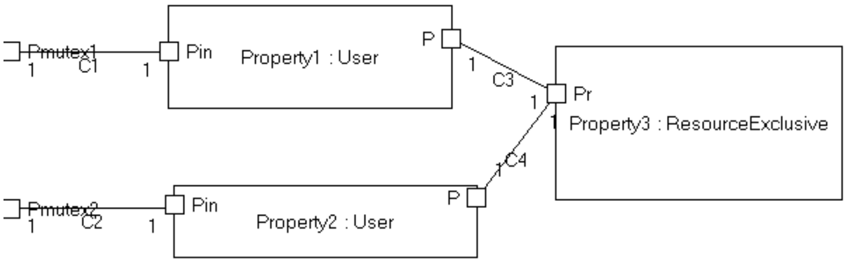
LTS of ResourceExclusive:



BIP model of ResourceExclusive:

```
package ResourceExclusive

atomic type ResourceExclusive
      export port Port PR_TAKE
      export port Port PR_RELEASE
      port Port i

      place Pseudostate1,Idle,busy

      initial to Pseudostate1

      on i from Pseudostate1 to Idle
      on PR_TAKE from Idle to busy
      on PR_RELEASE from busy to Idle
end
```

Composite component MutexResourceExclusive:



EXP.OPEN model of the architecture MutexResourceExclusive:

```
hide C3_RELEASE, C3_TAKE, C4_RELEASE, C4_TAKE in
gate par using
PIN_FINISH * _ * _ -> PMUTEX1_FINISH,
PIN_START * _ * _ -> PMUTEX1_START,
_ * PIN_FINISH * _ -> PMUTEX2_FINISH,
_ * PIN_START * _ -> PMUTEX2_START,
P_RELEASE * _ * PR_RELEASE -> C3_RELEASE,
P_TAKE * _ * PR_TAKE -> C3_TAKE,
_ * P_RELEASE * PR_RELEASE -> C4_RELEASE,
_ * P_TAKE * PR_TAKE -> C4_TAKE
in
"User.bcg" || "User.bcg" || "ResourceExclusive.bcg"
end par
end hide
```

IDCM demonstrates:

MutexResourceExclusive conforms to specification SpecMutexOneUser

MutexResourceExclusive conforms to specification SpecMutex2ParallelUsers

Conformance analysis is based on liveness properties and is not powerful enough to demonstrate safety properties of the system. For example, it cannot be demonstrated here that when the tool is used by an user, it cannot be used by another one.

Such analysis requires safety property analysis. See IDCM2.0 to get more information.