Esempio: door.ads

```
package Door
--# own State : StateType;
--#     in Input;
is
  type T is (Open, Closed);
  --# type StateType is Abstract;
  --#
  --# function prf_alarmTimeout(DoorState : StateType)
  --#    return Clock.TimeT;
  -- non c'è bisogno di esportarlo, a differenza di:
 function TheCurrentDoor return T;
   --# global State;
 function TheDoorAlarm return AlarmTypes.StatusT;
   --# global State;
```


Esempio: lockdoor.ads

```
--# post
--# -- PROOF ANNOTATIONS FOR SECURITY PROPERTY 3
--# -- After each call, the security property holds:
--#
--# ( (TheCurrentDoor(State) = Open and
--#    Latch.IsLocked(Latch.State) and
--#    Clock.GreaterThanOrEqual(
--#          Clock.TheCurrentTime(Clock.CurrentTime),
--#          prf_alarmTimeout(State))
--#   )
--#    <-> TheDoorAlarm(State) = AlarmTypes.Alarming
--# ) and
--# Latch.IsLocked(Latch.State);
```


Esempio: door.adb

```
package body Door
--# own State is CurrentDoor,
--#              AlarmTimeout,
--#              DoorAlarm &
--#     Input is in Door.Interface.Input;
is
   CurrentDoor  : T;
   DoorAlarm    : AlarmTypes.StatusT;
   AlarmTimeout : Clock.TimeT;
```

Esempio: lockdoor.adb

```
--# post
--# -- PROOF ANNOTATIONS FOR SECURITY PROPERTY 3
--# -- After each call, the security property holds:
--#
--# ( (CurrentDoor = Open and
--#    Latch.IsLocked(Latch.State) and
--#    Clock.GreaterThanOrEqual(
--#          Clock.TheCurrentTime(Clock.CurrentTime),
--#          AlarmTimeout)
--#   )
--#    <-> DoorAlarm = AlarmTypes.Alarming
--# ) and
--# Latch.IsLocked(Latch.State);
```


Esempio: lockdoor.adb vs .ads

```
--# ( (CurrentDoor           = Open and
       TheCurrentDoor(State)
--#    Latch.IsLocked(Latch.State) and
--#    Clock.GreaterThanOrEqual(
--#          Clock.TheCurrentTime(Clock.CurrentTime),
--#          AlarmTimeout    )
             prf_alarmTimeout(State)
--#   )
--#    <-> DoorAlarm = AlarmTypes.Alarming
          TheDoorAlarm(State)
--# ) and
--# Latch.IsLocked(Latch.State);
```


Esempio: lockdoor.adb vs .ads

```
--# ( (fld_currentdoor(State) = Open and
       TheCurrentDoor(State)
--#    Latch.IsLocked(Latch.State) and
--#    Clock.GreaterThanOrEqual(
--#          Clock.TheCurrentTime(Clock.CurrentTime),
--#          fld_alarmtimeout(State)
             prf_alarmTimeout(State)
--#   )
--#    <-> fld_dooralarm(State) = AlarmTypes.Alarming
          TheDoorAlarm(State)
--# ) and
--# Latch.IsLocked(Latch.State);
```

Esempio: VC di raffinamento post di lockdoor

```
C1:   latch__islocked(latch__state) and
      thecurrentdoor(state) = open and
      clock__greaterthanorequal(
               clock__thecurrenttime(clock__currenttime),
               prf_alarmtimeout(state))
      <->
      thedooralarm(state) = alarmtypes__alarming .

H9:   fld_currentdoor(state~) = open and
      latch__islocked(latch__state) and
      clock__greaterthanorequal(
              clock__thecurrenttime(clock__currenttime),
              fld_alarmtimeout(state))
      <-> fld_dooralarm(state) = alarmtypes__alarming .
H1:  fld_currentdoor(state~) = fld_currentdoor(state) .
```


Esempio: usando H1

```
C1:   latch__islocked(latch__state) and
      thecurrentdoor(state) = open and
      clock__greaterthanorequal(
               clock__thecurrenttime(clock__currenttime),
               prf_alarmtimeout(state))
      <->
      thedooralarm(state) = alarmtypes__alarming .

H9:   fld_currentdoor(state) = open and
      latch__islocked(latch__state) and
      clock__greaterthanorequal(
              clock__thecurrenttime(clock__currenttime),
              fld_alarmtimeout(state))
      <->
      fld_dooralarm(state) = alarmtypes__alarming .
```


Esempio: è proposizionale

```
C1:    a and
      (thecurrentdoor(state) = open and
       clock__greaterthanorequal(
               clock__thecurrenttime(clock__currenttime),
               prf_alarmtimeout(state))
      )
      <-> thedooralarm(state) = alarmtypes__alarming .

H9:   fld_currentdoor(state) = open and
      (a and
       clock__greaterthanorequal(
              clock__thecurrenttime(clock__currenttime),
              fld_alarmtimeout(state))
      )
      <-> fld_dooralarm(state) = alarmtypes__alarming .
```

Esempio: è proposizionale

```
C1:    a and
      (b and
       clock__greaterthanorequal(
                clock__thecurrenttime(clock__currenttime),
                prf_alarmtimeout(state))
      )
      <-> thedooralarm(state) = alarmtypes__alarming .

H9:   b and
      (a and
       clock__greaterthanorequal(
               clock__thecurrenttime(clock__currenttime),
               fld_alarmtimeout(state))
      )
      <-> fld_dooralarm(state) = alarmtypes__alarming .
```


Esempio: è proposizionale

```
C1:    a and
      (b and
       c)
      )
      <-> thedooralarm(state) = alarmtypes__alarming .

H9:   b and
      (a and
       c)
      )
      <-> fld_dooralarm(state) = alarmtypes__alarming .
```


Esempio: è proposizionale

```
   C1:   a and b and c     H9:   b and a and c
         <-> d .                 <-> d .
```

- per cui

```
lockdoor_user(3):
    B1 and
    (thecurrentdoor(S2) = open and
     clock__greaterthanorequal(T, prf_alarmtimeout(S2)))
    <->
    thedooralarm(S2) = alarmtypes__alarming
 may_be_deduced_from
  [ fld_currentdoor(S) = open and
    (B1 and
     clock__greaterthanorequal(T, fld_alarmtimeout(S2)))
    <->
    fld_dooralarm(S2) = alarmtypes__alarming ,

    fld_currentdoor(S) = fld_currentdoor(S2)  ] .
```