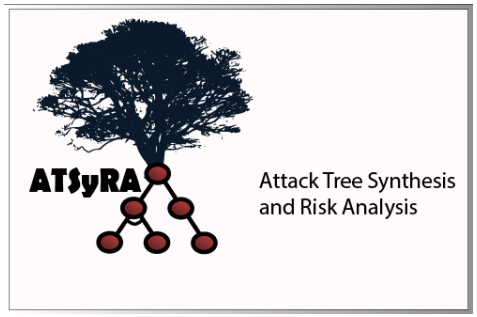
Assisted Generation of Attack Trees : the ATSyRAprototype



Sophie Pinchinat

joint work with Mathieu Acher and Didier Vojtisek

Université de Rennes 1

GraMSec, 13 July 2015

UNIVERSITÉ DE RENNES 1

UMR IRISA

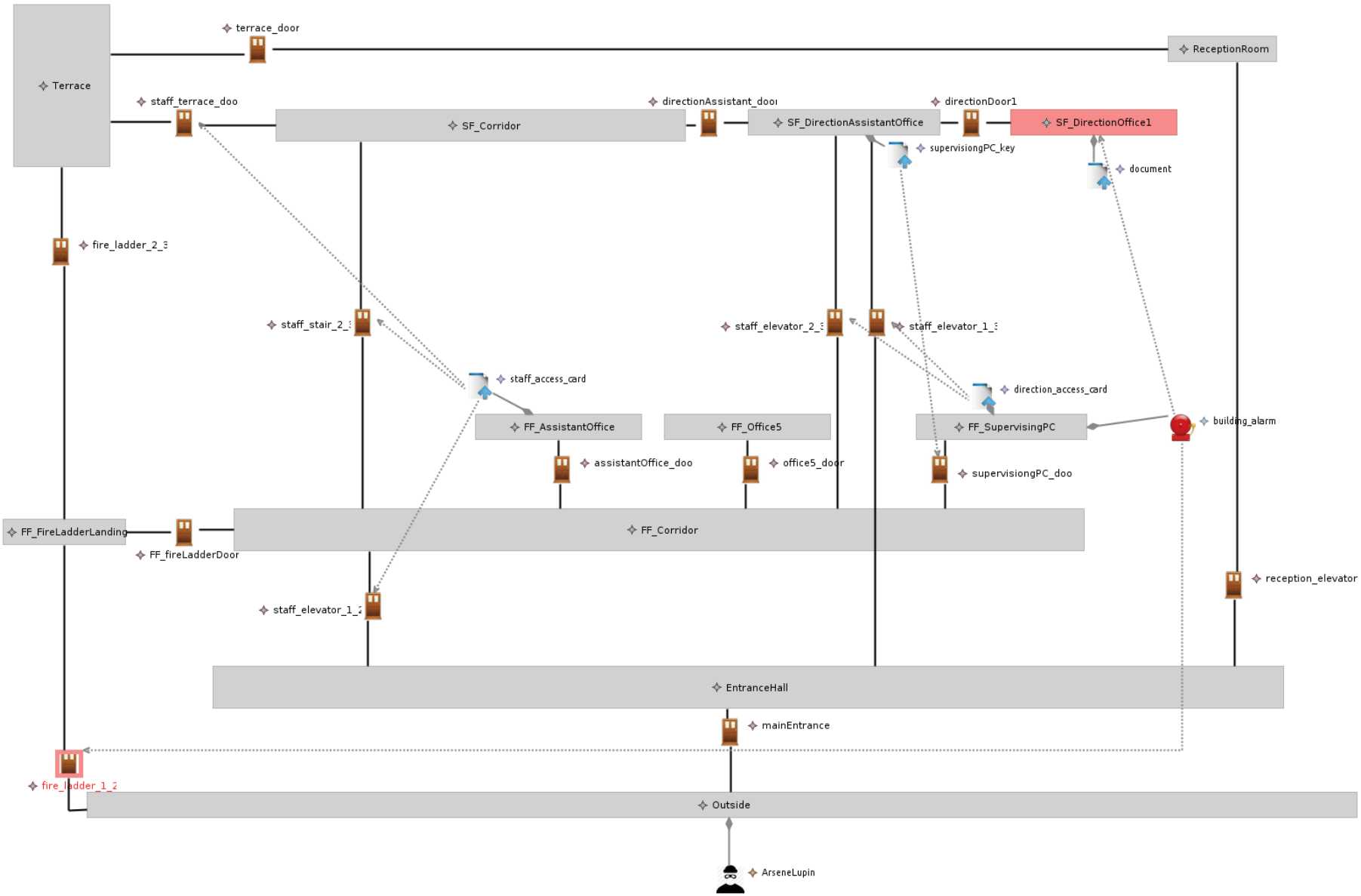
Outline

Outline

A Building Specification

```
building{
    zone
        Outside(noAlarm),
        //****** First Floor
        EntranceHall (noAlarm),
        //****** Second Floor
        FF_Office5(noAlarm),
        FF_AssistantOffice(noAlarm),
        FF_FireLadderLanding(noAlarm),
        FF_SupervisingPC(noAlarm),
        FF_Corridor(noAlarm),
        //***** Third Floor
        SF_Corridor(noAlarm),
        SF_DirectionOffice1([building_alarm]),
        SF_DirectionAssistantOffice(noAlarm),
        ReceptionRoom (noAlarm),
        Terrace(noAlarm);
    access
        //****** First Floor accesses
        mainEntrance (Outside,EntranceHall,open,noAlarm, 0),
        //****** Second Floor accesses
        supervisiongPC_door(FF_Corridor, FF_SupervisingPC, lock, noAlarm,[supervisiongPC_key], 0),
        assistantOffice_door(FF_Corridor, FF_AssistantOffice, open, noAlarm, 0),
        office5_door(FF_Corridor, FF_Office5, open, noAlarm, 0),
        FF_fireLadderDoor(FF_Corridor, FF_FireLadderLanding, open, noAlarm, 0),

        //****** Third Floor accesses
        directionAssistant_door(SF_Corridor, SF_DirectionAssistantOffice, open, noAlarm, 0),
        directionDoor1(SF_DirectionAssistantOffice, SF_DirectionOffice1, open, noAlarm, 0),
        staff_terrace_door(SF_Corridor, Terrace, lock, noAlarm, [staff_access_card], 0),
        terrace_door(ReceptionRoom, Terrace, close, noAlarm, 0),
        //****** Inter Floor accesses
        reception_elevator(EntranceHall, ReceptionRoom, open, noAlarm, 0),
        staff_elevator_1_2 (EntranceHall,FF_Corridor,lock,noAlarm,[staff_access_card], 0),
        staff_elevator_1_3 (EntranceHall,SF_DirectionAssistantOffice,lock,noAlarm,[direction_access_card], 0),
        staff_elevator_2_3 (FF_Corridor,SF_DirectionAssistantOffice,lock,noAlarm,[direction_access_card], 0),
        staff_stair_2_3 (FF_Corridor, SF_Corridor,lock,noAlarm,[staff_access_card], 0),
        fire_ladder_1_2(Outside, FF_FireLadderLanding,close, [building_alarm], 0),
        fire_ladder_2_3( Terrace, FF_FireLadderLanding,  open, noAlarm, 0);

    alarm
        building_alarm  (FF_SupervisingPC, activate, 0);
    item
        supervisiongPC_key(SF_DirectionAssistantOffice),
        staff_access_card(FF_AssistantOffice),
        direction_access_card(FF_SupervisingPC),
        document(SF_DirectionOffice1);
        }
```

A three-level building



The attack objective

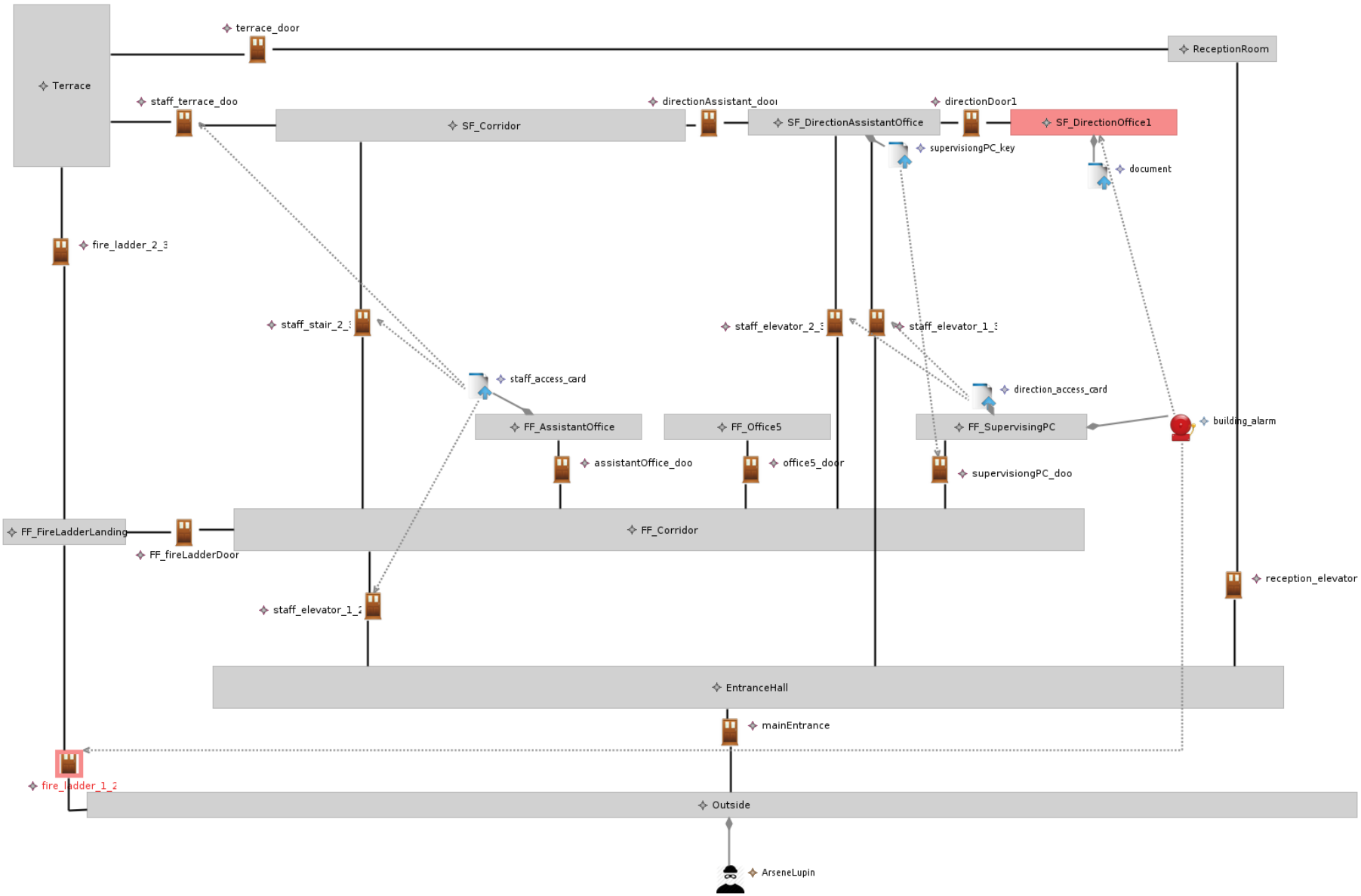
- Item locations

```
item
    supervisiongPC_key(SF_DirectionAssistantOffice),
    staff_access_card(FF_AssistantOffice),
    direction_access_card(FF_SupervisingPC),
    document(SF_DirectionOffice1);
    }
```

- Attacker

```
attack{
    attacker
        ArseneLupin (Outside, 0);
    goal (Outside, document, notDetected);
}
```

Do you think this is possible? How?



ATSyRA response

We analyze a transition system of $\approx 1.6 \times 10^{13}$ states

- Existence of an attack scenarios:

```
ITSReachPath=/donnees/ATSyRA/eclipse/plugins/fr.lip6.move.coloane.tools.its_1.0.0.201403110210/bin/its-reach-linux64
Timeout=60
its-reach command run as :

/donnees/ATSyRA/eclipse/plugins/fr.lip6.move.coloane.tools.its_1.0.0.201403110210/bin/its-reach-linux64  --quiet  -i
Model ,|S| ,Time ,Mem(kb) ,fin. SDD ,fin. DDD ,peak SDD ,peak DDD ,SDD Hom ,SDD cache peak ,DDD Hom ,DDD cachepeak ,SH
OriginalAttacksState,8.16172e+11,17.2077,255600,2,1490,8,1.04742e+06,7,0,247,948006,0
 Total reachable state count : 816172346600

Verifying 1 reachability properties.
Never property goalReached==1 does not hold.
Reachable states that satisfy the never predicate will be exhibited.
There are 183461849936 reachable states that exhibit your property : goalReached==1

Model ,|S| ,Time ,Mem(kb) ,fin. SDD ,fin. DDD ,peak SDD ,peak DDD ,SDD Hom ,SDD cache peak ,DDD Hom ,DDD cachepeak ,SH
goalReached==1,1.83462e+11,17.2088,255656,2,394,8,1.04742e+06,7,0,248,948006,1
```

There is an attack !

ATSyRA response

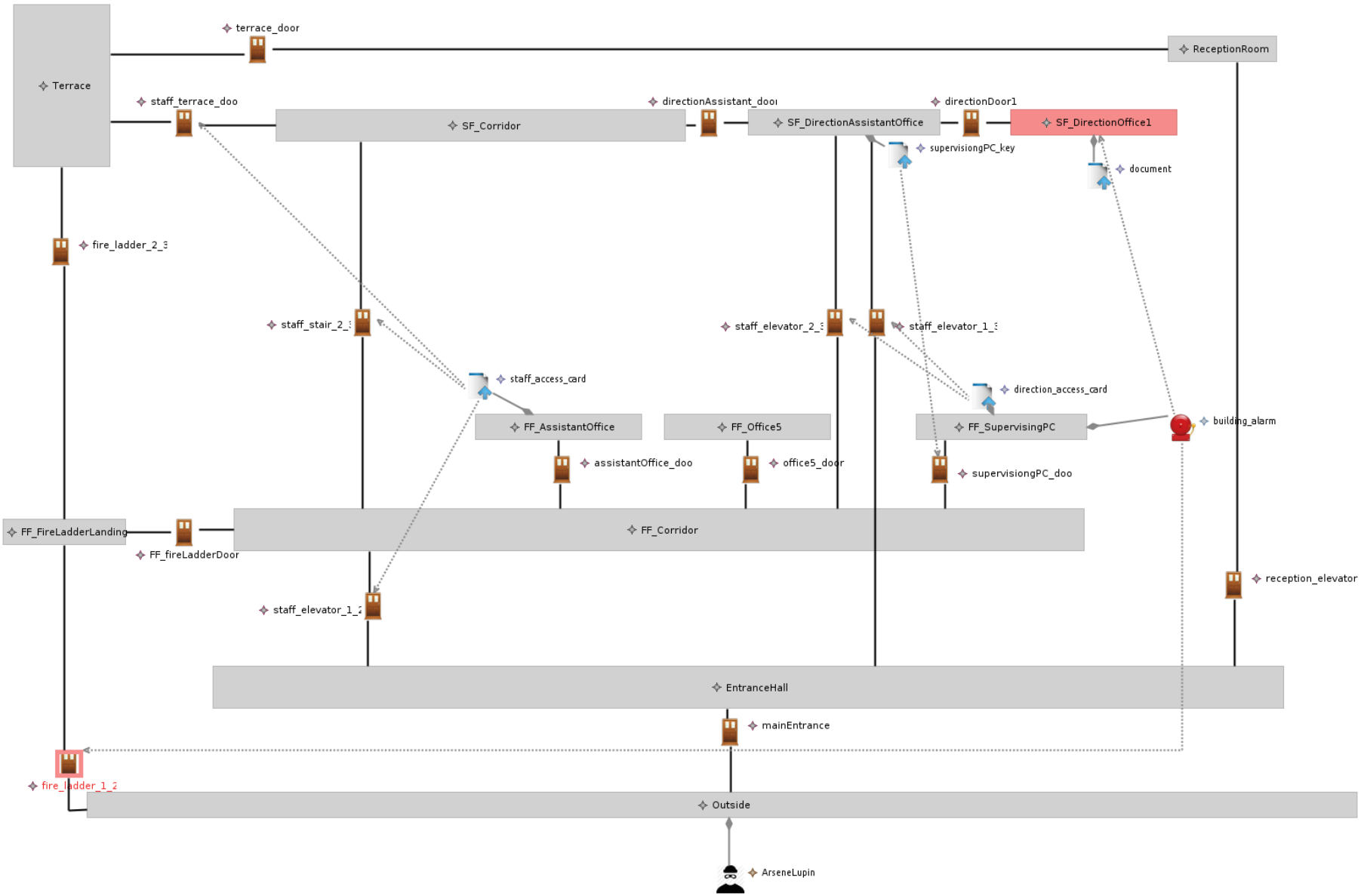
We analyze a transition system of $\approx 1.6 \times 10^{13}$ states

- Attack scenarios generation

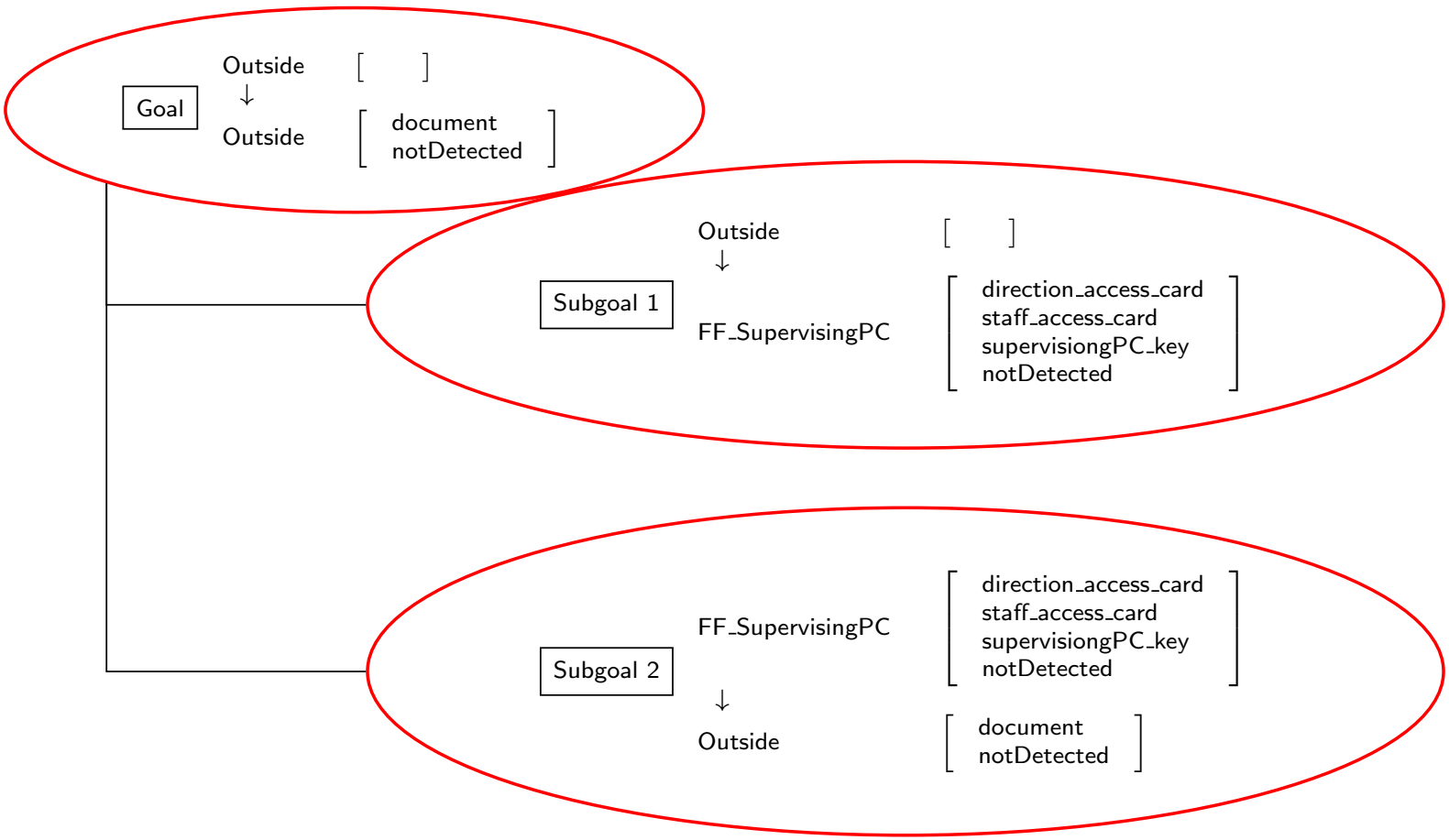
```
Executing Building To GAL on sitemultiniveaux.gtb
GAL model written to file : /donnees/ATSyRA/workspaces/demosite/SiteMultiNiveaux.exemple/atsyra-gen/sitemultiniveaux.g
LLA written to file : sitemultiniveaux_LLA.building_action
ITSReachPath=/donnees/ATSyRA/eclipse/plugins/fr.lip6.move.coloane.tools.its_1.0.0.201403110210/bin/its-reach-linux64
Timeout=120
initial cost 890
final cost 770
position_of_carteacces_direction,state_of_ascenseur_dupersonnel_1_3,state_of_ascenseur_dupersonnel_1_2,state_of_ascens
Reverse transition relation is NOT exact ! Intersection with reachable at each step enabled.

its-reach command run as :

/donnees/ATSyRA/eclipse/plugins/fr.lip6.move.coloane.tools.its_1.0.0.201403110210/bin/its-reach-linux64  --quiet  -i
Model ,|S| ,Time ,Mem(kb) ,fin. SDD ,fin. DDD ,peak SDD ,peak DDD ,SDD Hom ,SDD cache peak ,DDD Hom ,DDD cachepeak ,SH
OriginalAttacksState,8.16172e+11,18.0299,255576,2,1490,8,1.04742e+06,7,0,247,948006,0
 Total reachable state count : 816172346600

Verifying 1 reachability properties.
Never property goalReached==1 does not hold.
Reachable states that satisfy the never predicate will be exhibited.
There are 183461849936 reachable states that exhibit your property : goalReached==1
computing up to 10 traces...

Computation of reachable scenarios from the BuildingAttack did not finish in a timely way. You should try to split you
```

TIMEOUT! even pushing it to a 10mn-long computation

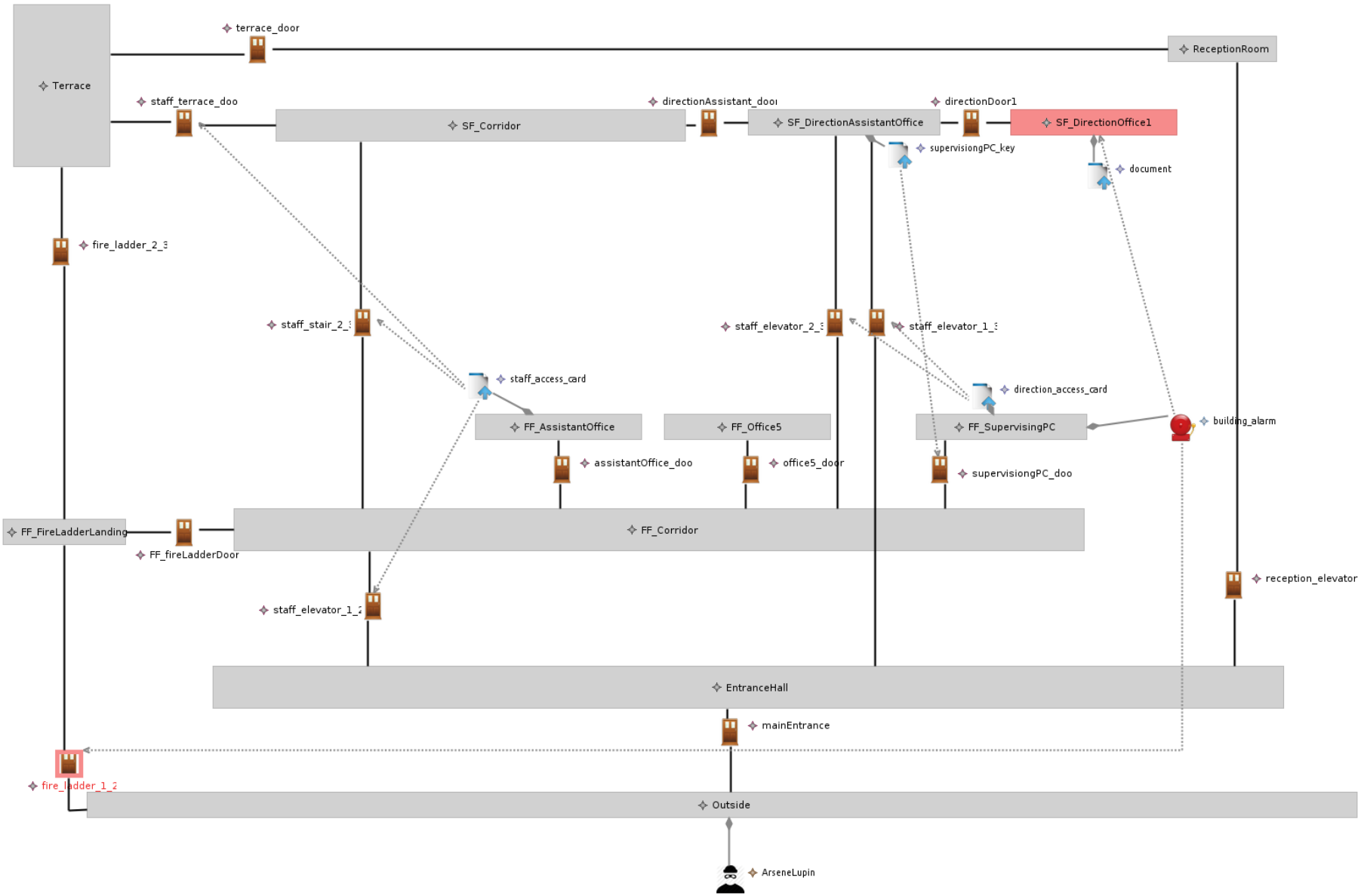
What would the expert do in such a case?



Goal decomposition (similarly to proof assistant tools)



Subgoal 1: Outside [ ] → FF_SupervisingPC [direction_access_card, staff_access_card, supervisiongPC_key, notDetected]



ATSyRA response for Subgoal 1

$$\text{Outside} \begin{bmatrix} \quad \end{bmatrix} \rightarrow \text{FF\_SupervisingPC} \begin{bmatrix} \text{direction\_access\_card} \\ \text{staff\_access\_card} \\ \text{supervisiongPC\_key} \\ \text{notDetected} \end{bmatrix}$$

```
Executing Building To GAL on sitemultiniveaux.gtb
GAL model written to file : /donnees/ATSyRA/workspaces/demosite/SiteMultiNiveaux.exemple/atsyra-gen/sitemultiniveaux.gal
LLA written to file : sitemultiniveaux_LLA.building_action
ITSReachPath=/donnees/ATSyRA/eclipse/plugins/fr.lip6.move.coloane.tools.its_1.0.0.201403110210/bin/its-reach-linux64
Timeout=120
initial cost 890
final cost 725
position_of_carteacces_direction,state_of_ascenseur_dupersonnel_1_3,state_of_ascenseur_dupersonnel_2_3,goalReached,state_of_as
Reverse transition relation is NOT exact ! Intersection with reachable at each step enabled.

its-reach command run as :

/donnees/ATSyRA/eclipse/plugins/fr.lip6.move.coloane.tools.its_1.0.0.201403110210/bin/its-reach-linux64  --quiet  -i  sitemult
Model ,|S| ,Time ,Mem(kb) ,fin. SDD ,fin. DDD ,peak SDD ,peak DDD ,SDD Hom ,SDD cache peak ,DDD Hom ,DDD cachepeak ,SHom cache
OriginalAttacksState,8.30222e+11,27.94,434508,2,1541,8,1.73416e+06,7,0,247,1.79109e+06,0
 Total reachable state count : 830222220280

Verifying 1 reachability properties.
Never property goalReached==1 does not hold.
Reachable states that satisfy the never predicate will be exhibited.
There are 230253264864 reachable states that exhibit your property : goalReached==1
computing up to 10 traces...

Computation of reachable scenarios from the BuildingAttack did not finish in a timely way. You should try to split your goal i
```

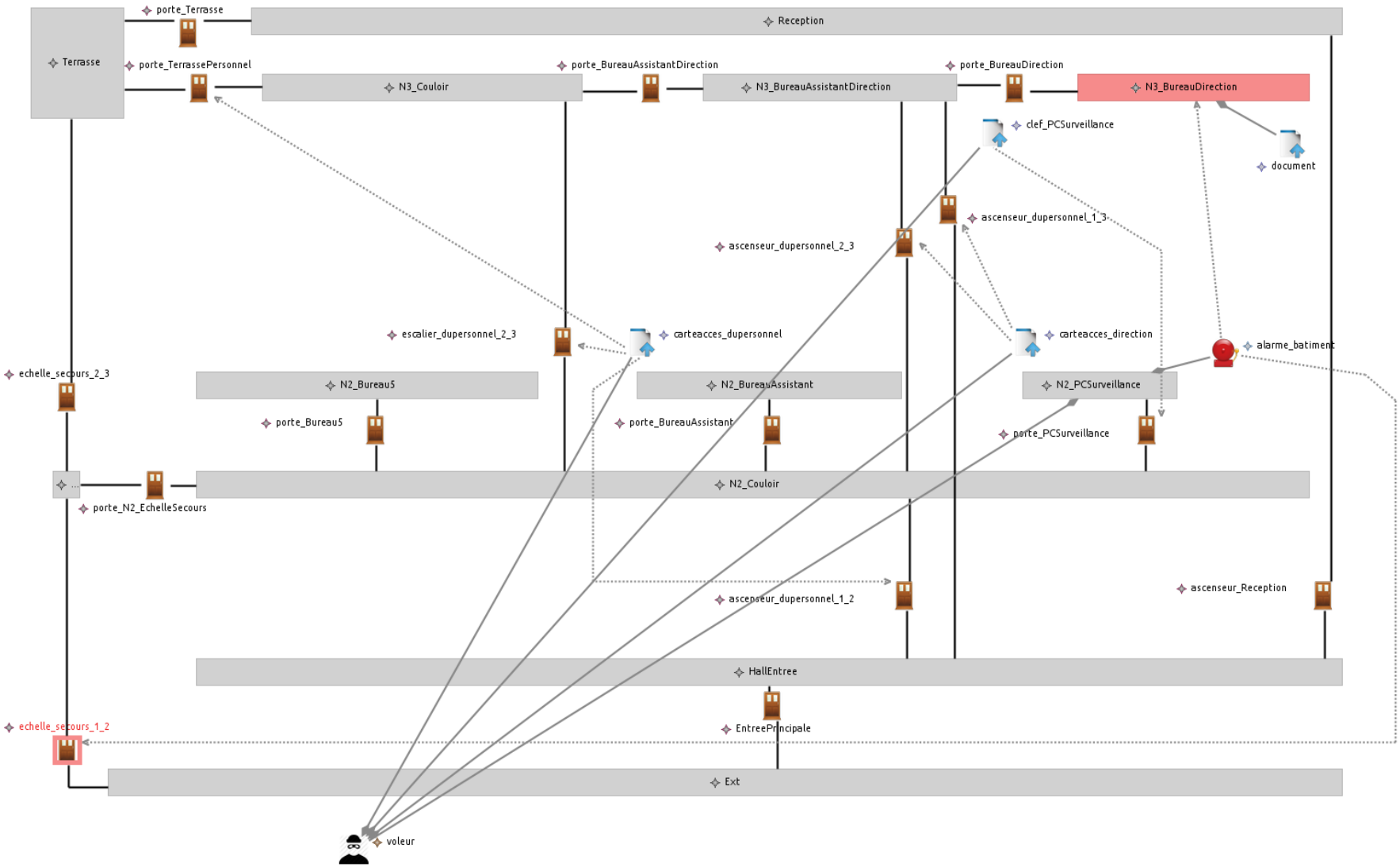
ATSyRA response for Subgoal 1

$$\text{Outside} \left[\quad\right] \rightarrow \text{FF\_SupervisingPC} \left[\begin{array}{l} \text{direction\_access\_card} \\ \text{staff\_access\_card} \\ \text{supervisiongPC\_key} \\ \text{notDetected} \end{array}\right]$$

```
Executing Building To GAL on sitemultiniveaux.gtb
GAL model written to file : /donnees/ATSyRA/workspaces/demosite/SiteMultiNiveaux.exemple/atsyra-gen/sitemultiniveaux.gal
LLA written to file : sitemultiniveaux_LLA.building_action
ITSReachPath=/donnees/ATSyRA/eclipse/plugins/fr.lip6.move.coloane.tools.its_1.0.0.201403110210/bin/its-reach-linux64
Timeout=120
initial cost 890
final cost 725
position_of_carteacces_direction,state_of_ascenseur_dupersonnel_1_3,state_of_ascenseur_dupersonnel_2_3,goalReached,state_of_as
Reverse transition relation is NOT exact ! Intersection with reachable at each step enabled.

its-reach command run as :

/donnees/ATSyRA/eclipse/plugins/fr.lip6.move.coloane.tools.its_1.0.0.201403110210/bin/its-reach-linux64  --quiet  -i  sitemult
Model ,|S| ,Time ,Mem(kb) ,fin. SDD ,fin. DDD ,peak SDD ,peak DDD ,SDD Hom ,SDD cache peak ,DDD Hom ,DDD cachepeak ,SHom cache
OriginalAttacksState,8.30222e+11,27.94,434508,2,1541,8,1.73416e+06,7,0,247,1.79109e+06,0
 Total reachable state count : 830222220280

Verifying 1 reachability properties.
Never property goalReached==1 does not hold.
Reachable states that satisfy the never predicate will be exhibited.
There are 230253264864 reachable states that exhibit your property : goalReached==1
computing up to 10 traces...

Computation of reachable scenarios from the BuildingAttack did not finish in a timely way. You should try to split your goal i
```

STILL TOO COMPLEX

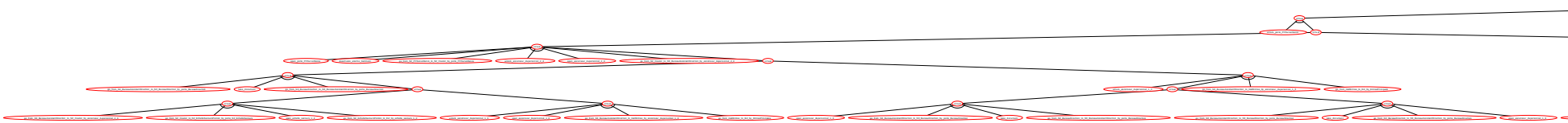
Subgoal 2: FF_SupervisingPC $\begin{bmatrix} \text{direction\_access\_card} \\ \text{staff\_access\_card} \\ \text{supervisiongPC\_key} \\ \text{notDetected} \end{bmatrix}$ $\rightarrow$ Outside $\begin{bmatrix} \text{document} \\ \text{notDetected} \end{bmatrix}$



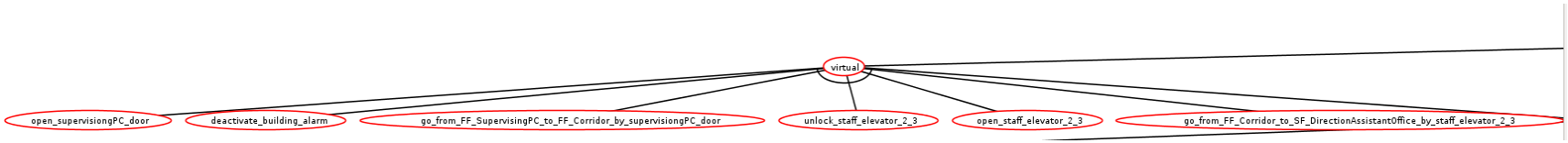
ATSyRA response for Subgoal 2

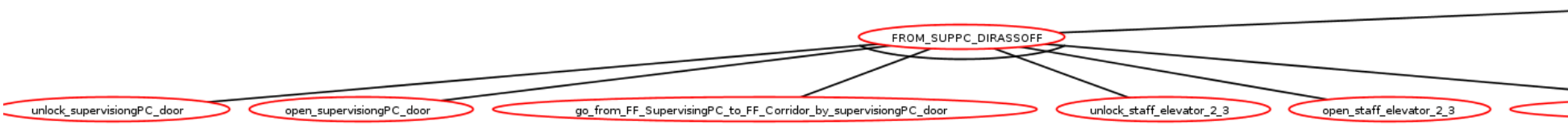
```
Executing Building To GAL on sitemultiniveaux.gtb
GAL model written to file : /donnees/ATSyRA/workspaces/demosite/SiteMultiNiveaux.exemple/atsyra-gen/sitemultiniveaux.gal
LLA written to file : sitemultiniveaux_LLA.building_action
ITSReachPath=/donnees/ATSyRA/eclipse/plugins/fr.lip6.move.coloane.tools.its_1.0.0.201403110210/bin/its-reach-linux64
Timeout=120
its-reach command run as :

/donnees/ATSyRA/eclipse/plugins/fr.lip6.move.coloane.tools.its_1.0.0.201403110210/bin/its-reach-linux64  --quiet  -i  sitemult
Model ,|S| ,Time ,Mem(kb) ,fin. SDD ,fin. DDD ,peak SDD ,peak DDD ,SDD Hom ,SDD cache peak ,DDD Hom ,DDD cachepeak ,SHom cache
OriginalAttacksState,1.42956e+10,5.64958,104156,2,604,6,511907,7,0,247,380715,0
 Total reachable state count : 14295564528

Verifying 1 reachability properties.
Never property goalReached==1 does not hold.
Reachable states that satisfy the never predicate will be exhibited.
There are 4716830720 reachable states that exhibit your property : goalReached==1
computing up to 10 traces...
From initial states :
[ state_of_porte_PCSurveillance=2 state_of_porte_BureauAssistantDirection=1 state_of_porte_BureauAssistant=1 state_of_porte_Te
This shortest transition sequence of length 15 :
unlock_porte_PCSurveillance, open_porte_PCSurveillance, deactivate_alarme_batiment, go_from_N2_PCSurveillance_to_N2_Couloir_by
Leads to final states :
[ 4716830720 states ]From initial states :
[ state_of_porte_PCSurveillance=2 state_of_porte_BureauAssistantDirection=1 state_of_porte_BureauAssistant=1 state_of_porte_Te
This shortest transition sequence of length 15 :
unlock_porte_PCSurveillance, open_porte_PCSurveillance, deactivate_alarme_batiment, go_from_N2_PCSurveillance_to_N2_Couloir_by
Leads to final states :
[ 4716830720 states ]From initial states :
[ state_of_porte_PCSurveillance=2 state_of_porte_BureauAssistantDirection=1 state_of_porte_BureauAssistant=1 state_of_porte_Te
This shortest transition sequence of length 15 :
unlock_porte_PCSurveillance, open_porte_PCSurveillance, deactivate_alarme_batiment, go_from_N2_PCSurveillance_to_N2_Couloir_by
Leads to final states :
[ 4716830720 states ]From initial states :
[ state_of_porte_PCSurveillance=2 state_of_porte_BureauAssistantDirection=1 state_of_porte_BureauAssistant=1 state_of_porte_Te
This shortest transition sequence of length 15 :
unlock_porte_PCSurveillance, open_porte_PCSurveillance, deactivate_alarme_batiment, go_from_N2_PCSurveillance_to_N2_Couloir_by
Leads to final states :
[ 4716830720 states ]From initial states :
[ state_of_porte_PCSurveillance=2 state_of_porte_BureauAssistantDirection=1 state_of_porte_BureauAssistant=1 state_of_porte_Te
```

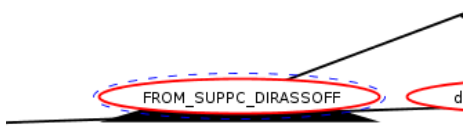
ATSyRA response for Subgoal 2



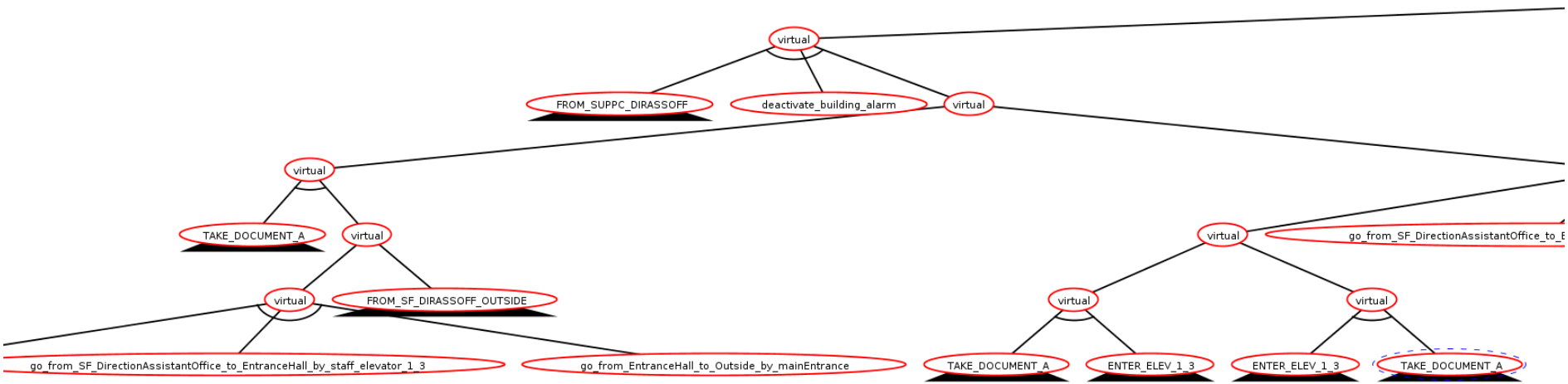
High-level actions for Subgoal 2







High-level actions for Subgoal 2



High-level actions

- Low-level actions are automatically generated

```
{
"go_from_Outside_to_EntranceHall_by_mainEntrance";
"go_from_EntranceHall_to_Outside_by_mainEntrance";
"open_mainEntrance";
"close_mainEntrance";
"go_from_FF_Corridor_to_FF_SupervisingPC_by_supervisiongPC_door";
"go_from_FF_SupervisingPC_to_FF_Corridor_by_supervisiongPC_door";
"open_supervisiongPC_door";
"close_supervisiongPC_door";
"unlock_supervisiongPC_door";
"lock_supervisiongPC_door";
"go_from_FF_Corridor_to_FF_AssistantOffice_by_assistantOffice_door";
"go_from_FF_AssistantOffice_to_FF_Corridor_by_assistantOffice_door";
"open_assistantOffice_door";
"close_assistantOffice_door";
"go_from_FF_Corridor_to_FF_Office5_by_office5_door";
"go_from_FF_Office5_to_FF_Corridor_by_office5_door";
"open_office5_door";
"close office5 door";
```

High-level actions

- Low-level actions are automatically generated
- "Easy" higher-level actions can be generated

```
{
ENTER_ELEV_1_3=unlock_staff_elevator_1_3,open_staff_elevator_1_3;

ENTER_ELEV_1_2=unlock_staff_elevator_1_2,open_staff_elevator_1_2;

ENTER_ELEV2_3=unlock_staff_elevator_2_3,open_staff_elevator_2_3;

// and many others that are to be synthesized
}
```

High-level actions

- Low-level actions are automatically generated
- "Easy" higher-level actions can be generated
- The expert can also develop his vocabulary

```
2 {
TAKE_DOCUMENT_A=go_from_SF_DirectionAssistantOffice_to_SF_DirectionOffice1_by_directionDoor1,
                take_document,
                go_from_SF_DirectionOffice1_to_SF_DirectionAssistantOffice_by_directionDoor1;

FROM_SF_DIRASSOFF_OUTSIDE_FIRELADDER=go_from_SF_DirectionAssistantOffice_to_FF_Corridor_by_staff_elevator_2_3,
                                     go_from_FF_Corridor_to_FF_FireLadderLanding_by_FF_fireLadderDoor,
                                     open_fire_ladder_1_2,
                                     go_from_FF_FireLadderLanding_to_Outside_by_fire_ladder_1_2;

FROM_SF_DIRASSOFF_OUTSIDE_ELEV1_3=ENTER_ELEV_1_3, go_from_FF_Corridor_to_EntranceHall_by_staff_elevator_1_2,
                                  go_from_EntranceHall_to_Outside_by_mainEntrance;

FROM_SUPPC_DIRASSOFF=unlock_supervisiongPC_door,
                     open_supervisiongPC_door,
                     go_from_FF_SupervisingPC_to_FF_Corridor_by_supervisiongPC_door,
                     unlock_staff_elevator_2_3,
                     open_staff_elevator_2_3,
                     go_from_FF_Corridor_to_SF_DirectionAssistantOffice_by_staff_elevator_2_3  ;

ENTER_DIROFF_SAFELY = deactivate_building_alarm,
                      go_from_SF_DirectionAssistantOffice_to_SF_DirectionOffice1_by_directionDoor1;
}
3 {
FROM_SF_DIRASSOFF_OUTSIDE=FROM_SF_DIRASSOFF_OUTSIDE_FIRELADDER | FROM_SF_DIRASSOFF_OUTSIDE_ELEV1_3;
}
```

High-level actions

- Low-level actions are automatically generated
- "Easy" higher-level actions can be generated
- The expert can also develop his vocabulary HLA expressions

$$HLA\_ID = \alpha;$$

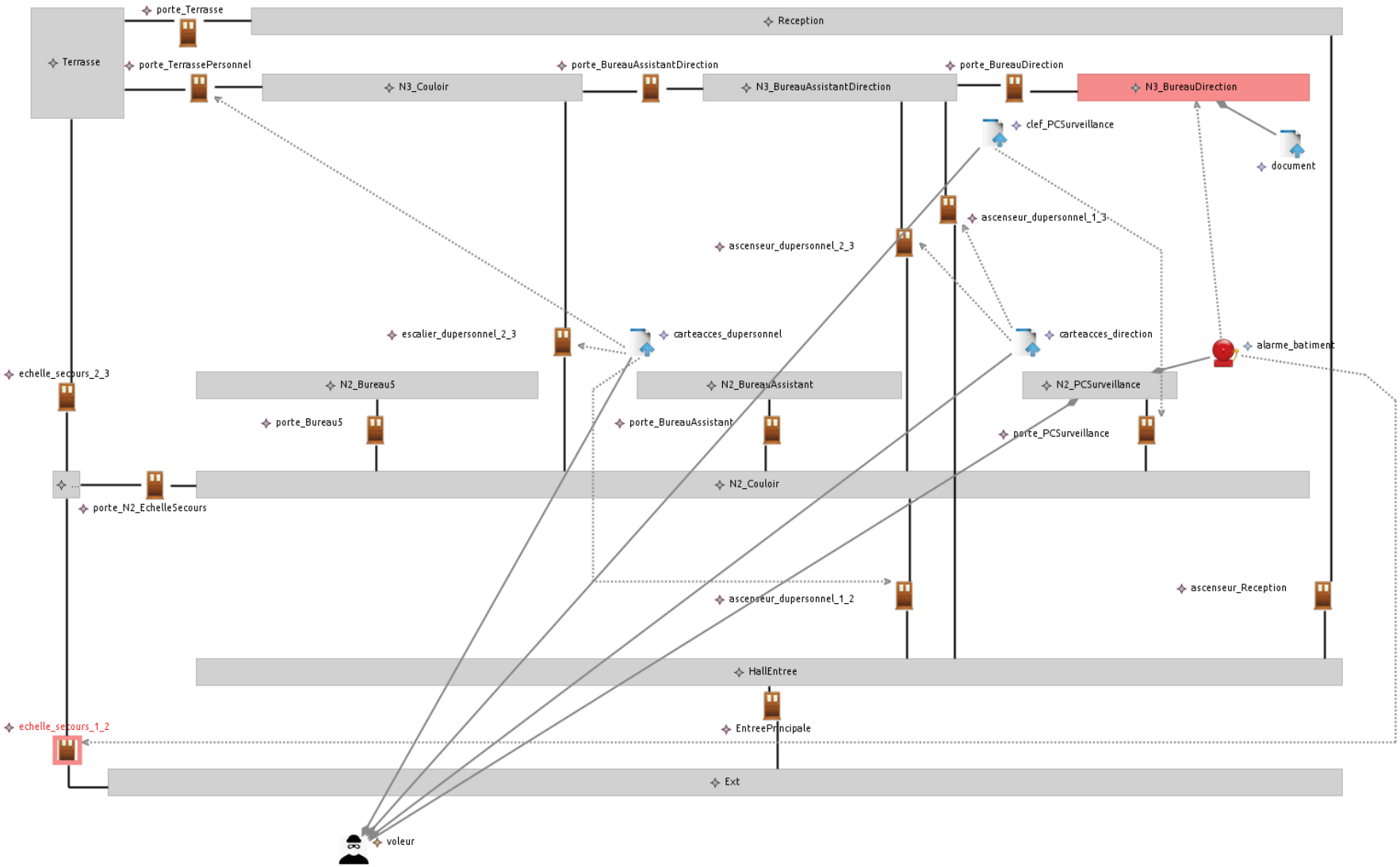
where

$$\alpha ::= a \mid (\alpha|\alpha) \mid \alpha, \alpha \mid \alpha \& \alpha$$

- The expert can also stratify

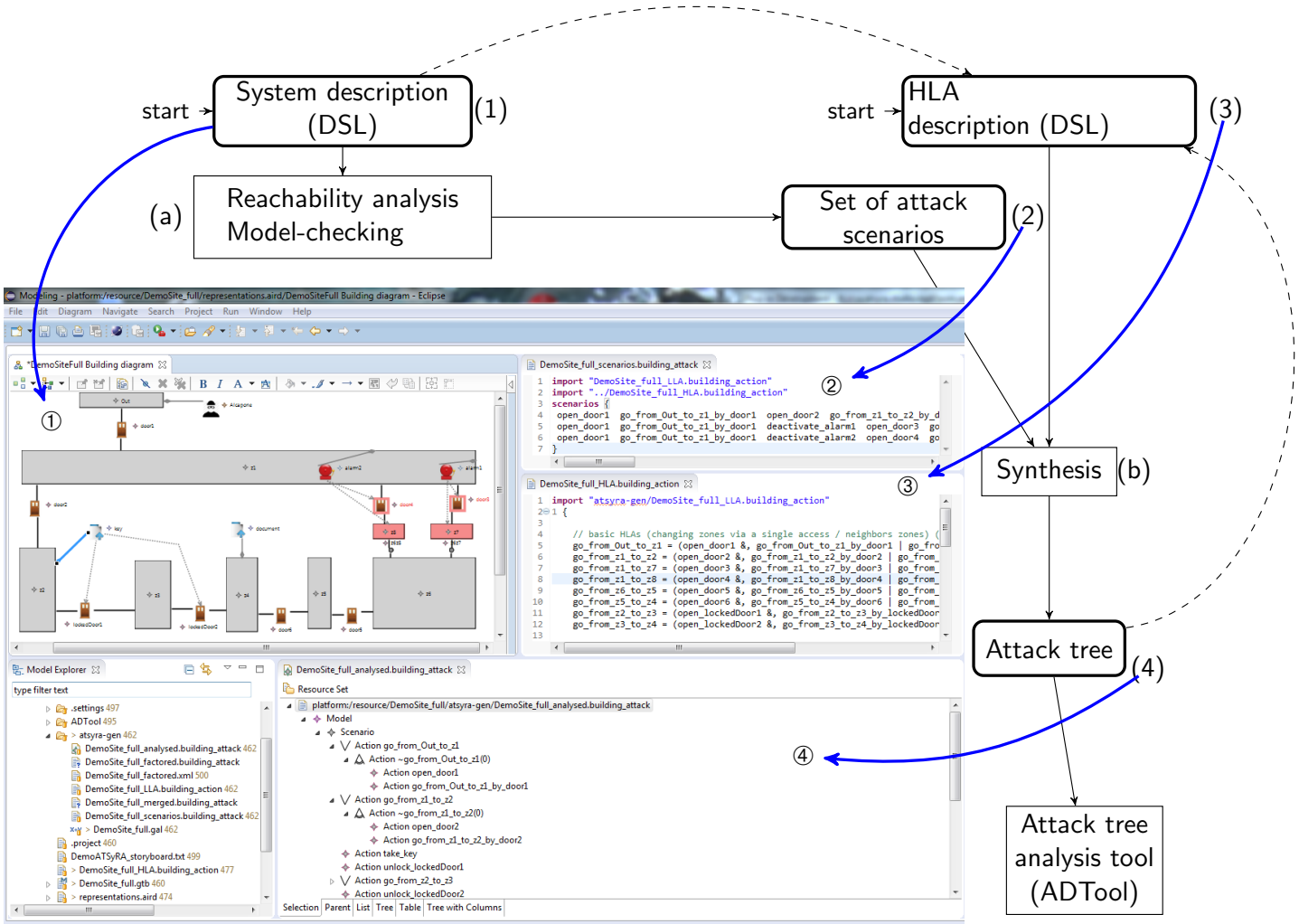
Outline

Subgoal 2: FF_SupervisingPC [direction_access_card, staff_access_card, supervisiongPC_key, notDetected] → Outside [document, notDetected]



Outline

The ATSyRA workflow



Discussion

- Short term
  - Improve both specification languages
    - Easy ways to select a subgoal, a sub-building, etc.
    - Connect subgoals
    - For subgoal: exploit temporal logic from the Model-checker (e.g. $(\neg$staff_access_card.pos=attacker$)\mathbf{U}$(reach_goal).)
    - Select/suggest a virtual node to generate an HLA

Discussion

- Short term
  - Improve both specification languages
    - Easy ways to select a subgoal, a sub-building, etc.
    - Connect subgoals
    - For subgoal: exploit temporal logic from the Model-checker (e.g. $(\neg \text{staff\_access\_card.pos}{=}\text{attacker})\mathbf{U}(\text{reach\_goal})$.)
    - Select/suggest a virtual node to generate an HLA
  - Good tools for editing trees, choose abstract level for display

Discussion

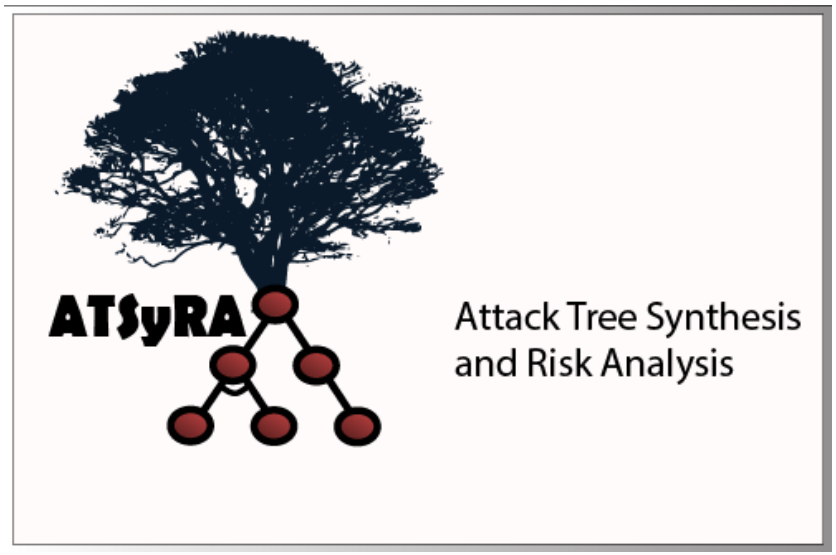
- Short term
  - Improve both specification languages
    - Easy ways to select a subgoal, a sub-building, etc.
    - Connect subgoals
    - For subgoal: exploit temporal logic from the Model-checker (e.g. $(\neg$staff_access_card.pos=attacker$)\mathbf{U}$(reach_goal).)
    - Select/suggest a virtual node to generate an HLA
  - Good tools for editing trees, choose abstract level for display
  - Parsing scenorios with HLA
    - Very combinatorial, currently the rules are not complete enough
    - Need heuristics and backtracking to synthesize even more succinct trees
    - Mathematical characterization of the optimal solutions we want to generate

Discussion

- Short term
  - Improve both specification languages
    - Easy ways to select a subgoal, a sub-building, etc.
    - Connect subgoals
    - For subgoal: exploit temporal logic from the Model-checker (e.g. $(\neg$staff_access_card.pos=attacker$)\mathbf{U}$(reach_goal).)
    - Select/suggest a virtual node to generate an HLA
  - Good tools for editing trees, choose abstract level for display
  - Parsing scenorios with HLA
    - Very combinatorial, currently the rules are not complete enough
    - Need heuristics and backtracking to synthesize even more succinct trees
    - Mathematical characterization of the optimal solutions we want to generate
  - Long term
    - Towards other kinds of systems, typically cyber intrusions
    - Guards, Defense (counter-measures)

The partners

- IRISA
  - LogicA
  - DiversE
  - EMSEC
- LIP6
- DGA



Thank you for your attention!