HybridSynchAADL

Tutorial

Outline

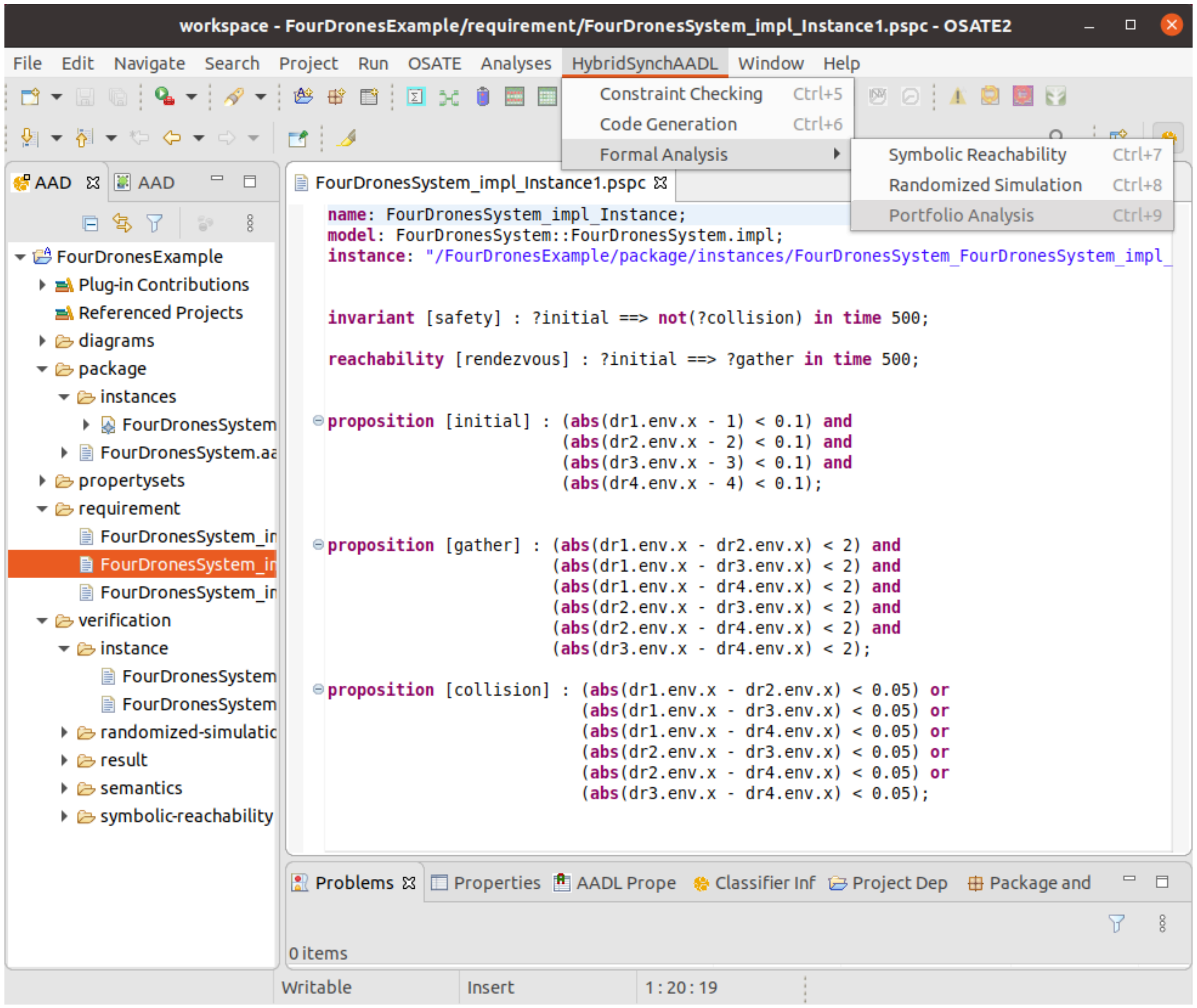
1. Short Tutorial
2. Basic OSATE
3. Creating Property Specification Files (PSPC)
4. HybridSynchAADL Constraints Checker
5. Rewriting-Modulo-SMT Code Generation
6. Formal Analysis

Outline

1. Short Tutorial
2. Basic OSATE
3. Creating Property Specification Files (PSPC)
4. HybridSynchAADL Constraints Checker
5. Rewriting-Modulo-SMT Code Generation
6. Formal Analysis

Short Tutorial

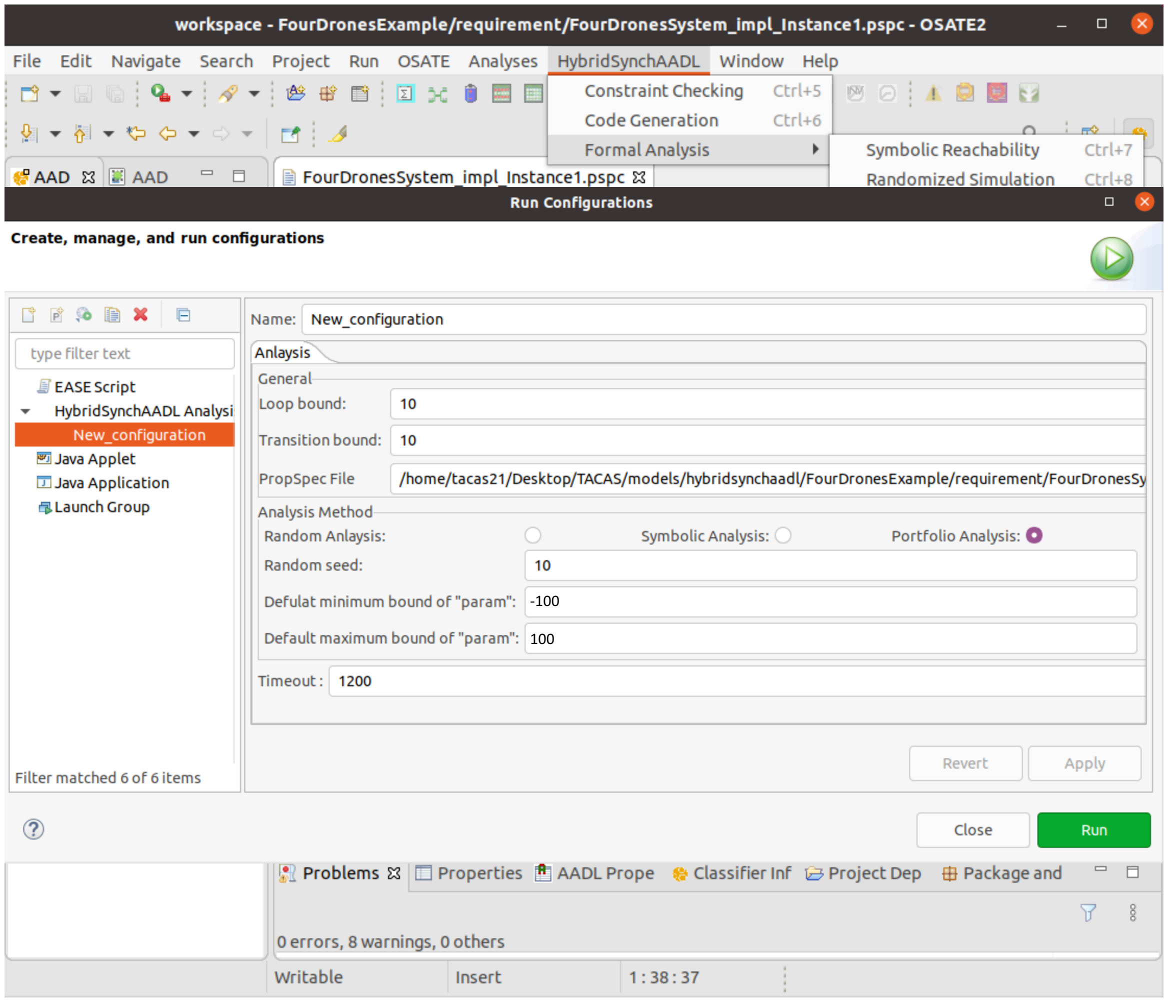
- See `Readme.txt` for instructions on how to set the virtual machine environment and run OSATE.
- Click `Portfolio Analysis` to perform symbolic reachability and randomized simulation simultaneously using rewriting-modulo-SMT.



```
name: FourDronesSystem_impl_Instance;
model: FourDronesSystem::FourDronesSystem.impl;
instance: "/FourDronesExample/package/instances/FourDronesSystem_FourDronesSystem_impl_

invariant [safety] : ?initial ==> not(?collision) in time 500;

reachability [rendezvous] : ?initial ==> ?gather in time 500;

proposition [initial] : (abs(dr1.env.x - 1) < 0.1) and
                        (abs(dr2.env.x - 2) < 0.1) and
                        (abs(dr3.env.x - 3) < 0.1) and
                        (abs(dr4.env.x - 4) < 0.1);

proposition [gather] : (abs(dr1.env.x - dr2.env.x) < 2) and
                       (abs(dr1.env.x - dr3.env.x) < 2) and
                       (abs(dr1.env.x - dr4.env.x) < 2) and
                       (abs(dr2.env.x - dr3.env.x) < 2) and
                       (abs(dr2.env.x - dr4.env.x) < 2) and
                       (abs(dr3.env.x - dr4.env.x) < 2);

proposition [collision] : (abs(dr1.env.x - dr2.env.x) < 0.05) or
                          (abs(dr1.env.x - dr3.env.x) < 0.05) or
                          (abs(dr1.env.x - dr4.env.x) < 0.05) or
                          (abs(dr2.env.x - dr3.env.x) < 0.05) or
                          (abs(dr2.env.x - dr4.env.x) < 0.05) or
                          (abs(dr3.env.x - dr4.env.x) < 0.05);
```

Portfolio Analysis

- Create a new configuration file
- Set PSPC file "FourDronesSystem_impl_Instance1.pspc" path
- Click `Portfolio Analysis` radio button
- Set positive integer value in `Random Seed`
- Set proper range value for parameterized variables.
- Set positive integer value in `Timeout`
  - `-1` can be set for infinite time.


workspace - FourDronesExample/requirement/FourDronesSystem_impl_Instance1.pspc - OSATE2
File Edit Navigate Search Project Run OSATE Analyses HybridSynchAADL Window Help
Constraint Checking Ctrl+5
Code Generation Ctrl+6
Formal Analysis
Symbolic Reachability Ctrl+7
Randomized Simulation Ctrl+8
AAD
AAD
FourDronesSystem_impl_Instance1.pspc
Run Configurations
Create, manage, and run configurations
type filter text
EASE Script
HybridSynchAADL Analysi
New_configuration
Java Applet
Java Application
Launch Group
Filter matched 6 of 6 items
Revert
Apply
Close
Run
Problems
Properties
AADL Prope
Classifier Inf
Project Dep
Package and
Writable
Insert
1 : 38 : 37

Name: New_configuration

Anlaysis

General

Loop bound: 10

Transition bound: 10

PropSpec File: /home/tacas21/Desktop/TACAS/models/hybridsynchaadl/FourDronesExample/requirement/FourDronesSy

Analysis Method

Random Anlaysis: ○ Symbolic Analysis: ○ Portfolio Analysis: [✓ ●]

Random seed: 10

Defulat minimum bound of "param": -100

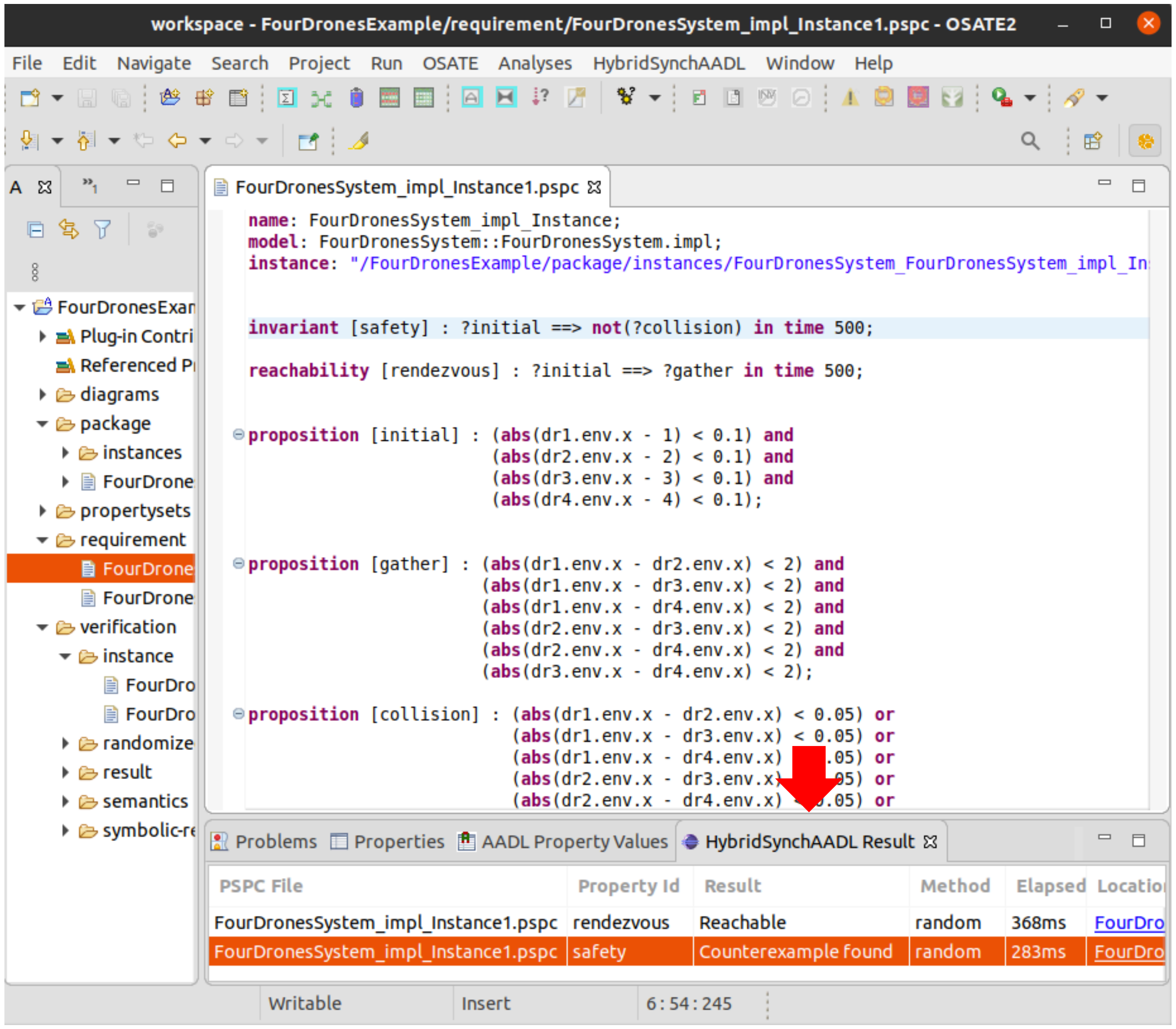
Default maximum bound of "param": 100

Timeout : 1200

0 errors, 8 warnings, 0 others

Analysis Results (1)

- The HybridSynchAADL Result view shows the analysis results.

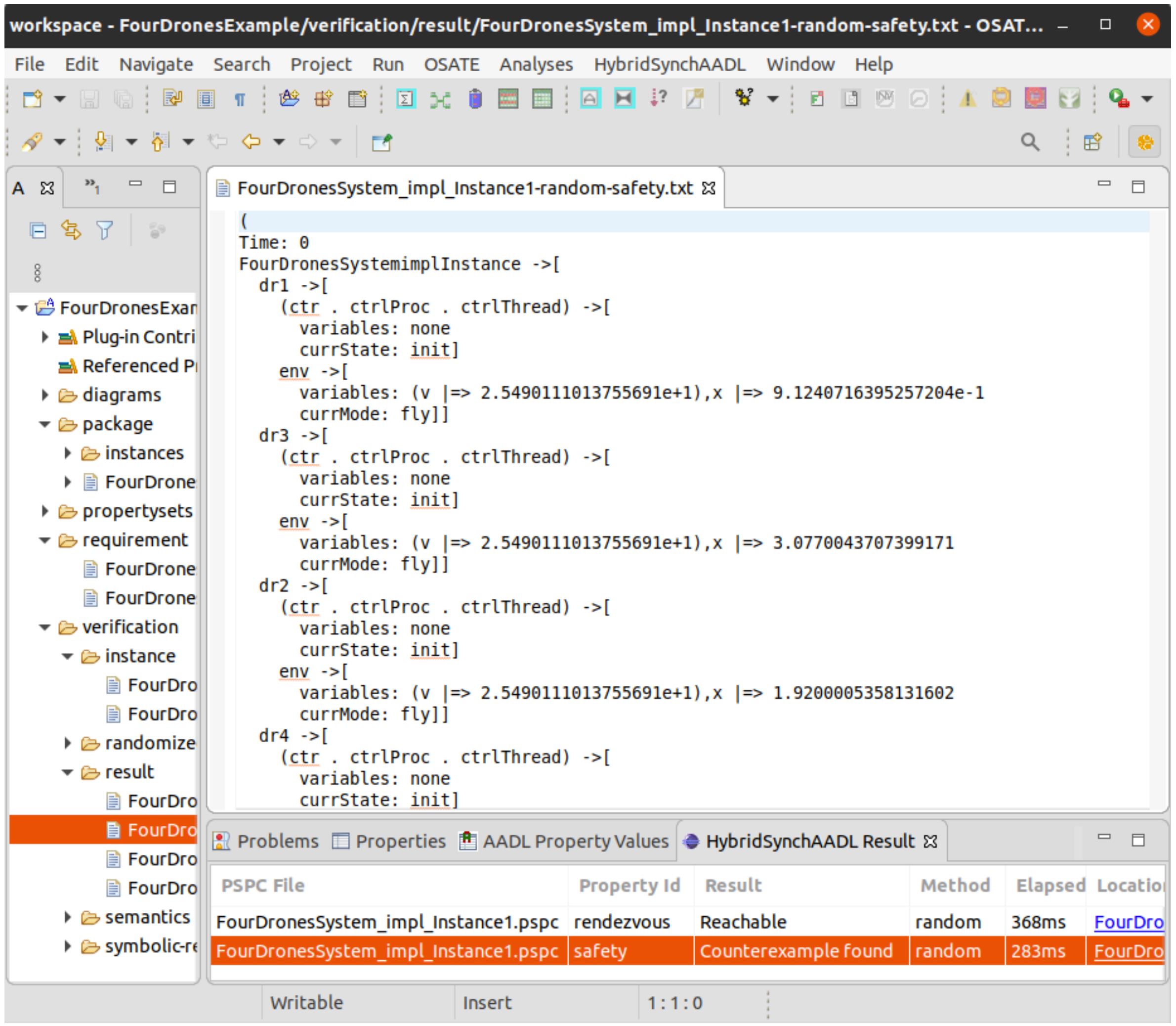


```
name: FourDronesSystem_impl_Instance;
model: FourDronesSystem::FourDronesSystem.impl;
instance: "/FourDronesExample/package/instances/FourDronesSystem_FourDronesSystem_impl_In


invariant [safety] : ?initial ==> not(?collision) in time 500;

reachability [rendezvous] : ?initial ==> ?gather in time 500;

proposition [initial] : (abs(dr1.env.x - 1) < 0.1) and
                        (abs(dr2.env.x - 2) < 0.1) and
                        (abs(dr3.env.x - 3) < 0.1) and
                        (abs(dr4.env.x - 4) < 0.1);


proposition [gather] : (abs(dr1.env.x - dr2.env.x) < 2) and
                       (abs(dr1.env.x - dr3.env.x) < 2) and
                       (abs(dr1.env.x - dr4.env.x) < 2) and
                       (abs(dr2.env.x - dr3.env.x) < 2) and
                       (abs(dr2.env.x - dr4.env.x) < 2) and
                       (abs(dr3.env.x - dr4.env.x) < 2);

proposition [collision] : (abs(dr1.env.x - dr2.env.x) < 0.05) or
                          (abs(dr1.env.x - dr3.env.x) < 0.05) or
                          (abs(dr1.env.x - dr4.env.x)   .05) or
                          (abs(dr2.env.x - dr3.env.x)   05) or
                          (abs(dr2.env.x - dr4.env.x)   .05) or
```

PSPC File	Property Id	Result	Method	Elapsed	Locatio
FourDronesSystem_impl_Instance1.pspc	rendezvous	Reachable	random	368ms	FourDro
FourDronesSystem_impl_Instance1.pspc	safety	Counterexample found	random	283ms	FourDro

Counterexamples and Witnesses

- Each file in Location in the result view contains a counterexample of an invariant property or a witness of a reachability property, if it exists.

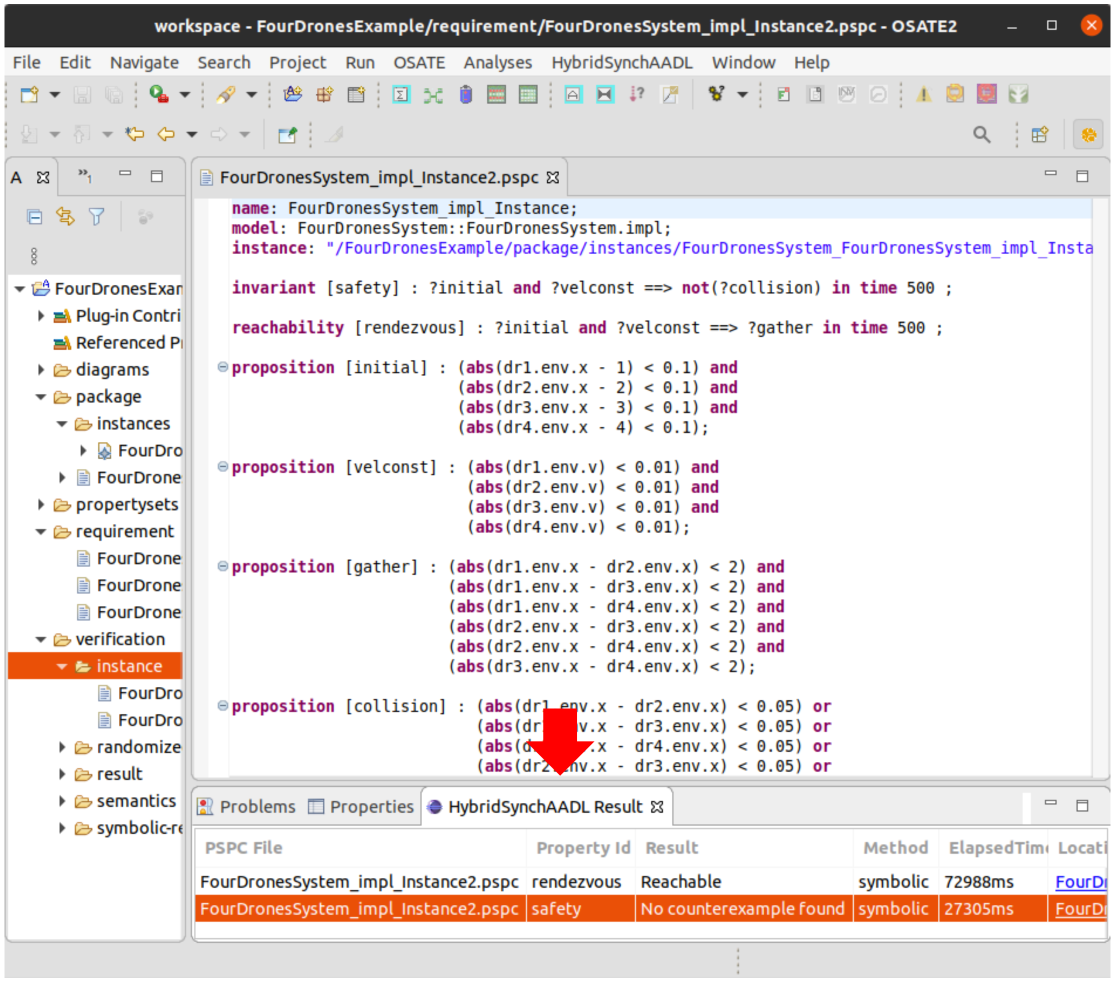

workspace - FourDronesExample/verification/result/FourDronesSystem_impl_Instance1-random-safety.txt - OSAT...
File Edit Navigate Search Project Run OSATE Analyses HybridSynchAADL Window Help
FourDronesExar
Plug-in Contri
Referenced P
diagrams
package
instances
FourDrone
propertysets
requirement
FourDrone
FourDrone
verification
instance
FourDro
FourDro
randomize
result
FourDro
FourDro
FourDro
FourDro
semantics
symbolic-re
FourDronesSystem_impl_Instance1-random-safety.txt
Problems Properties AADL Property Values HybridSynchAADL Result
Writable Insert 1 : 1 : 0

```
(
Time: 0
FourDronesSystemimplInstance ->[
  dr1 ->[
    (ctr . ctrlProc . ctrlThread) ->[
      variables: none
      currState: init]
    env ->[
      variables: (v |=> 2.549011101375569le+1),x |=> 9.1240716395257204e-1
      currMode: fly]]
  dr3 ->[
    (ctr . ctrlProc . ctrlThread) ->[
      variables: none
      currState: init]
    env ->[
      variables: (v |=> 2.549011101375569le+1),x |=> 3.077004370739917l
      currMode: fly]]
  dr2 ->[
    (ctr . ctrlProc . ctrlThread) ->[
      variables: none
      currState: init]
    env ->[
      variables: (v |=> 2.549011101375569le+1),x |=> 1.9200005358131602
      currMode: fly]]
  dr4 ->[
    (ctr . ctrlProc . ctrlThread) ->[
      variables: none
      currState: init]
```

PSPC File	Property Id	Result	Method	Elapsed	Locatio
FourDronesSystem_impl_Instance1.pspc	rendezvous	Reachable	random	368ms	FourDro
FourDronesSystem_impl_Instance1.pspc	safety	Counterexample found	random	283ms	FourDro

Analysis Results (2)

- In the case of “FourDronesSystem_impl_Instsance2.pspc”
- The result shows there is no counterexample found and a reachability of witness found



```
name: FourDronesSystem_impl_Instance;
model: FourDronesSystem::FourDronesSystem.impl;
instance: "/FourDronesExample/package/instances/FourDronesSystem_FourDronesSystem_impl_Insta

invariant [safety] : ?initial and ?velconst ==> not(?collision) in time 500 ;

reachability [rendezvous] : ?initial and ?velconst ==> ?gather in time 500 ;

proposition [initial] : (abs(dr1.env.x - 1) < 0.1) and
                        (abs(dr2.env.x - 2) < 0.1) and
                        (abs(dr3.env.x - 3) < 0.1) and
                        (abs(dr4.env.x - 4) < 0.1);

proposition [velconst] : (abs(dr1.env.v) < 0.01) and
                         (abs(dr2.env.v) < 0.01) and
                         (abs(dr3.env.v) < 0.01) and
                         (abs(dr4.env.v) < 0.01);

proposition [gather] : (abs(dr1.env.x - dr2.env.x) < 2) and
                       (abs(dr1.env.x - dr3.env.x) < 2) and
                       (abs(dr1.env.x - dr4.env.x) < 2) and
                       (abs(dr2.env.x - dr3.env.x) < 2) and
                       (abs(dr2.env.x - dr4.env.x) < 2) and
                       (abs(dr3.env.x - dr4.env.x) < 2);

proposition [collision] : (abs(dr1 env.x - dr2.env.x) < 0.05) or
                          (abs(dr[illegible]v.x - dr3.env.x) < 0.05) or
                          (abs(d[illegible].x - dr4.env.x) < 0.05) or
                          (abs(dr2[illegible]nv.x - dr3.env.x) < 0.05) or
```

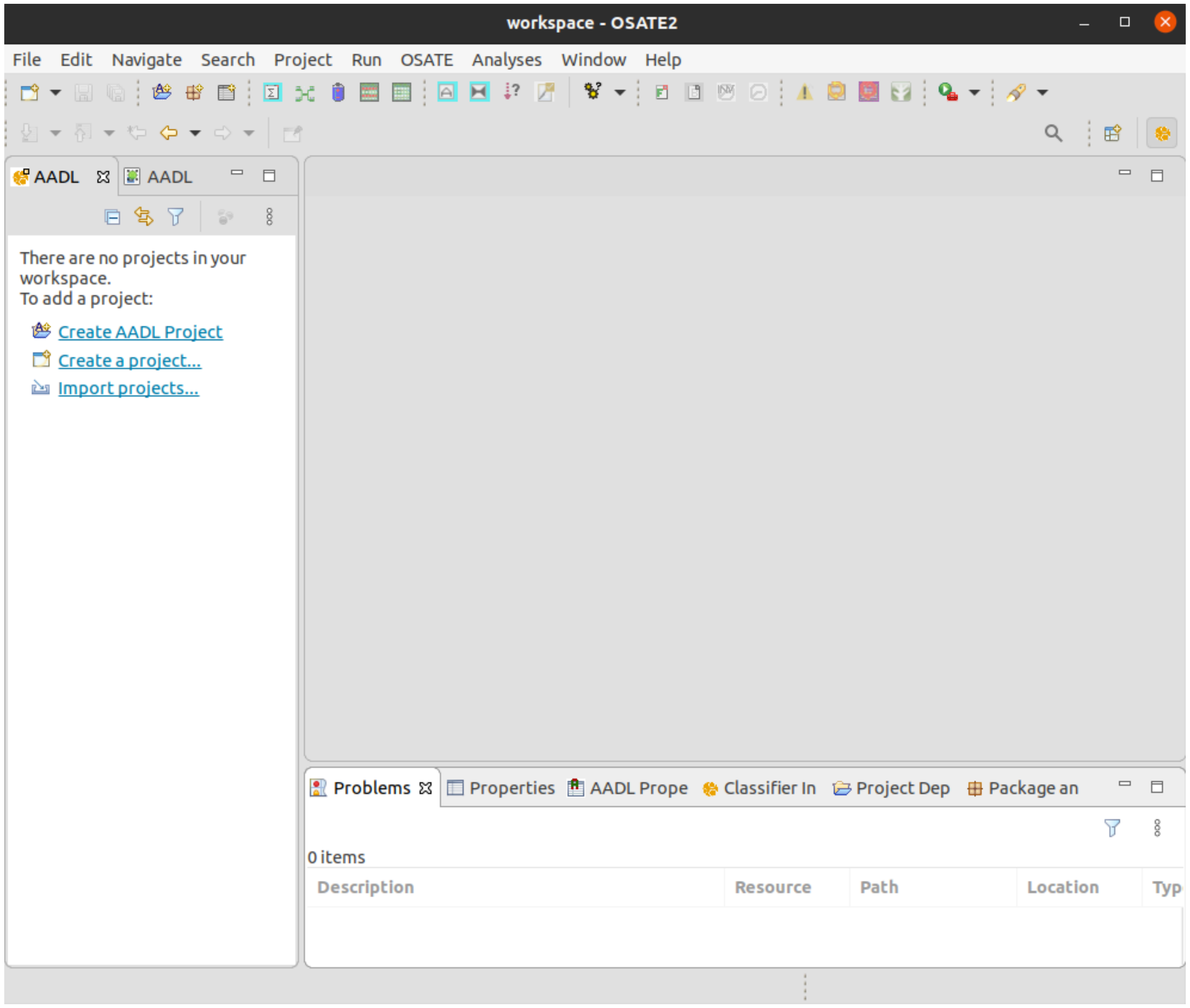
PSPC File	Property Id	Result	Method	ElapsedTim	Locati
FourDronesSystem_impl_Instance2.pspc	rendezvous	Reachable	symbolic	72988ms	FourDı
FourDronesSystem_impl_Instance2.pspc	safety	No counterexample found	symbolic	27305ms	FourDı

Outline

1. Short Tutorial
2. Basic OSATE
3. Creating Property Specification Files (PSPC)
4. HybridSynchAADL Constraints Checker
5. Rewriting-Modulo-SMT Code Generation
6. Formal Analysis

Running OSATE

- Let's look at more details
- You will see this window when you execute OSATE.


workspace - OSATE2
File Edit Navigate Search Project Run OSATE Analyses Window Help
AADL
AADL

There are no projects in your workspace.
To add a project:

- Create AADL Project
- Create a project...
- Import projects...

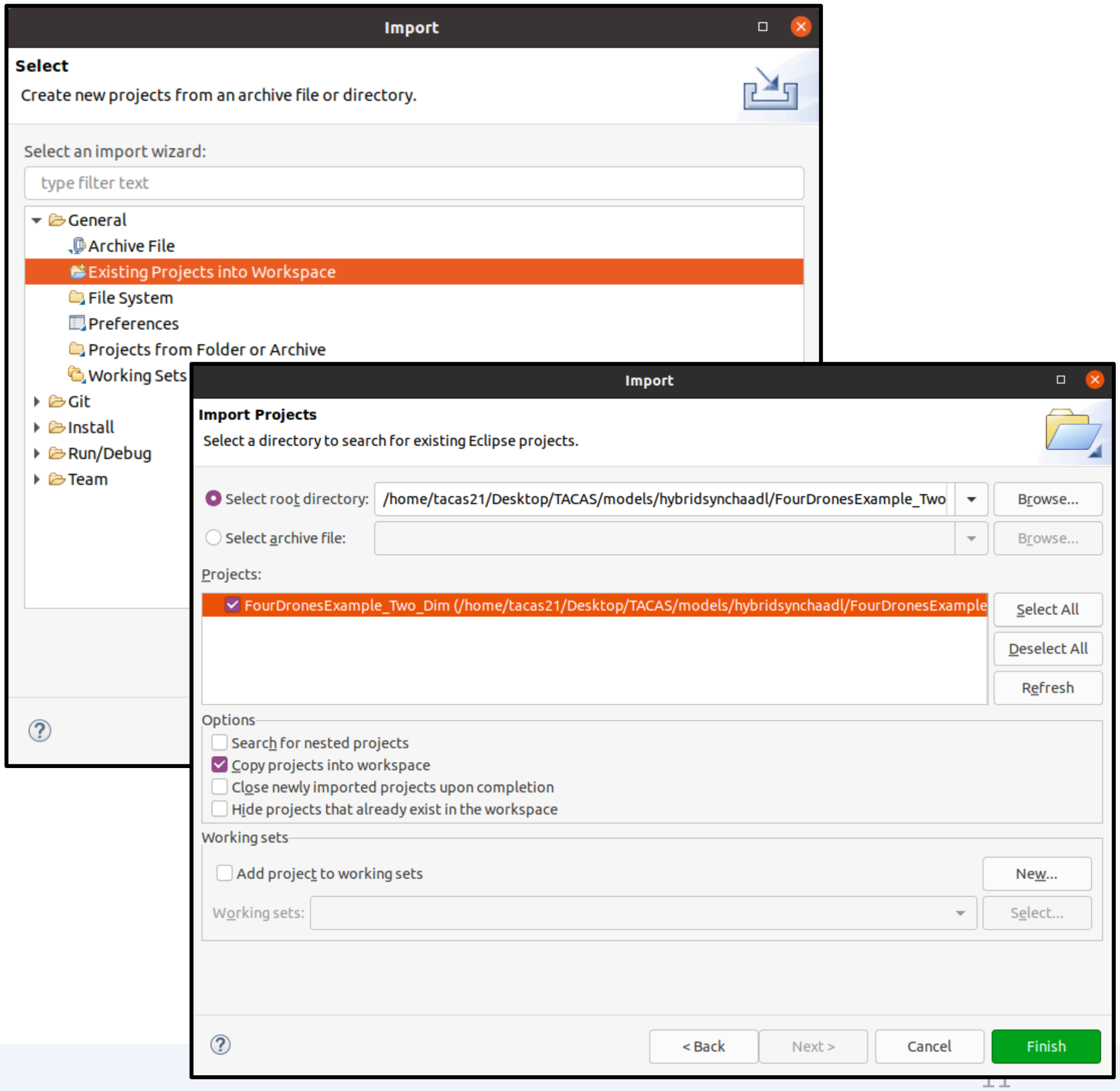
0 items

Description	Resource	Path	Location	Typ

OSATE - Importing an Example

- We start with a simple example, namely, `FourDronesExample_Two_Dim` in the directory `models/hybridsynchaadl`.

- To import the example, choose
  - Menu → File → Import → General → Existing Projects into Workspace.



Import

Select

Create new projects from an archive file or directory.

Select an import wizard:

type filter text

- General
  - Archive File
  - Existing Projects into Workspace
  - File System
  - Preferences
  - Projects from Folder or Archive
  - Working Sets
- Git
- Install
- Run/Debug
- Team

Import

Import Projects

Select a directory to search for existing Eclipse projects.

[✓ Select root directory:] /home/tacas21/Desktop/TACAS/models/hybridsynchaadl/FourDronesExample_Two

Select archive file:

Projects:

[✓] FourDronesExample_Two_Dim (/home/tacas21/Desktop/TACAS/models/hybridsynchaadl/FourDronesExample

Options

- [ ] Search for nested projects
- [✓] Copy projects into workspace
- [ ] Close newly imported projects upon completion
- [ ] Hide projects that already exist in the workspace

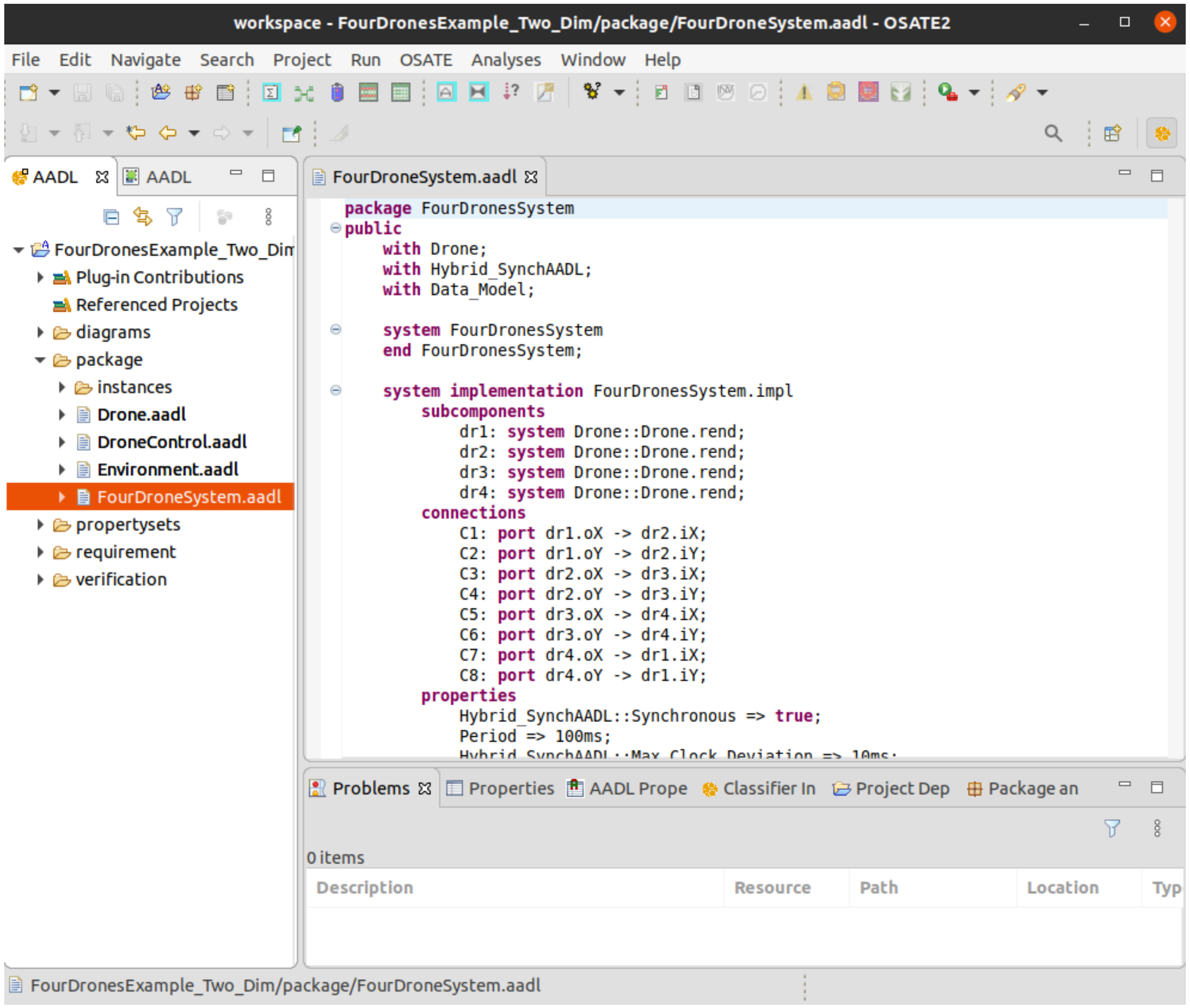
Working sets

- [ ] Add project to working sets

Working sets:

FourDronesSystem – Text

- `FourDroneSystem.aadl` contains the top-level system component.

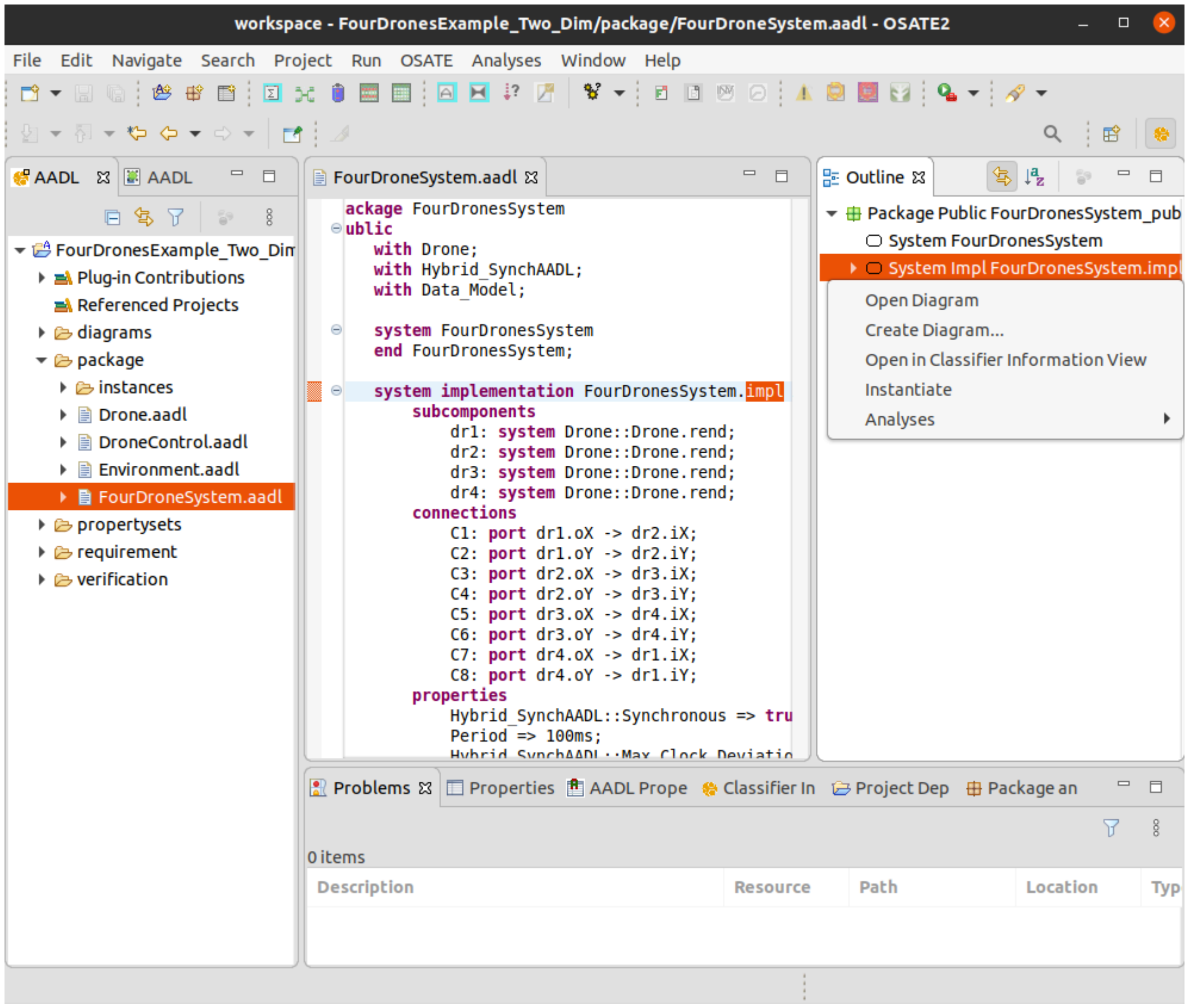


```
package FourDronesSystem
public
    with Drone;
    with Hybrid_SynchAADL;
    with Data_Model;

    system FourDronesSystem
    end FourDronesSystem;

    system implementation FourDronesSystem.impl
        subcomponents
            dr1: system Drone::Drone.rend;
            dr2: system Drone::Drone.rend;
            dr3: system Drone::Drone.rend;
            dr4: system Drone::Drone.rend;
        connections
            C1: port dr1.oX -> dr2.iX;
            C2: port dr1.oY -> dr2.iY;
            C3: port dr2.oX -> dr3.iX;
            C4: port dr2.oY -> dr3.iY;
            C5: port dr3.oX -> dr4.iX;
            C6: port dr3.oY -> dr4.iY;
            C7: port dr4.oX -> dr1.iX;
            C8: port dr4.oY -> dr1.iY;
        properties
            Hybrid_SynchAADL::Synchronous => true;
            Period => 100ms;
            Hybrid_SynchAADL::Max_Clock_Deviation => 10ms;
```

Instance Model

- Open the Outline view by clicking Menu → Window → Show view → Outline.

- Create an instance model from a system implementation as follows:
  - Right click on `System Impl FourDronesSystem.impl` and choose `Instantiate`.

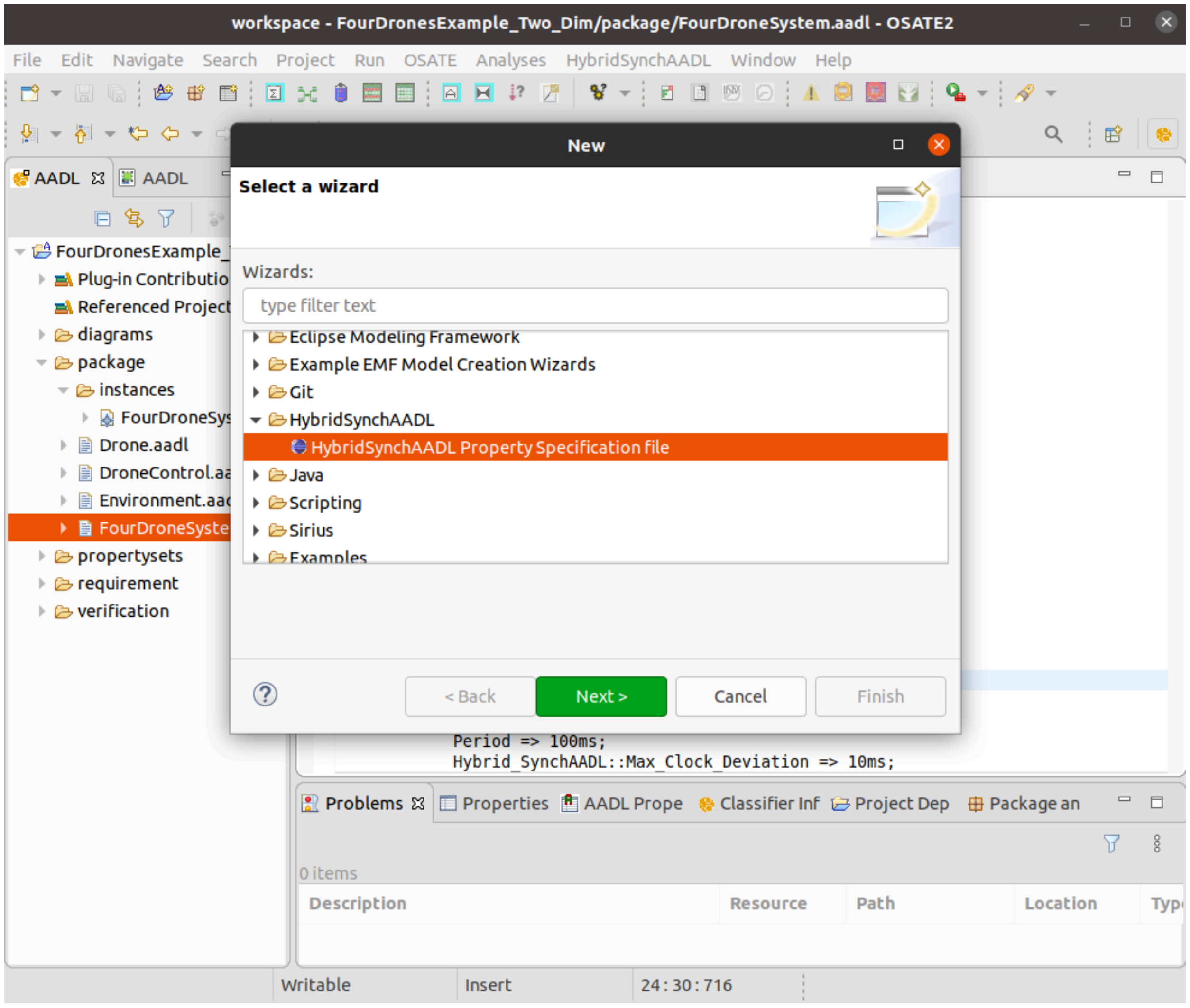


```
ackage FourDronesSystem
ublic
   with Drone;
   with Hybrid_SynchAADL;
   with Data_Model;

   system FourDronesSystem
   end FourDronesSystem;

   system implementation FourDronesSystem.impl
      subcomponents
         dr1: system Drone::Drone.rend;
         dr2: system Drone::Drone.rend;
         dr3: system Drone::Drone.rend;
         dr4: system Drone::Drone.rend;
      connections
         C1: port dr1.oX -> dr2.iX;
         C2: port dr1.oY -> dr2.iY;
         C3: port dr2.oX -> dr3.iX;
         C4: port dr2.oY -> dr3.iY;
         C5: port dr3.oX -> dr4.iX;
         C6: port dr3.oY -> dr4.iY;
         C7: port dr4.oX -> dr1.iX;
         C8: port dr4.oY -> dr1.iY;
      properties
         Hybrid_SynchAADL::Synchronous => tru
         Period => 100ms;
         Hybrid_SynchAADL::Max_Clock_Deviatio
```

Outline

Creating PSPC Files

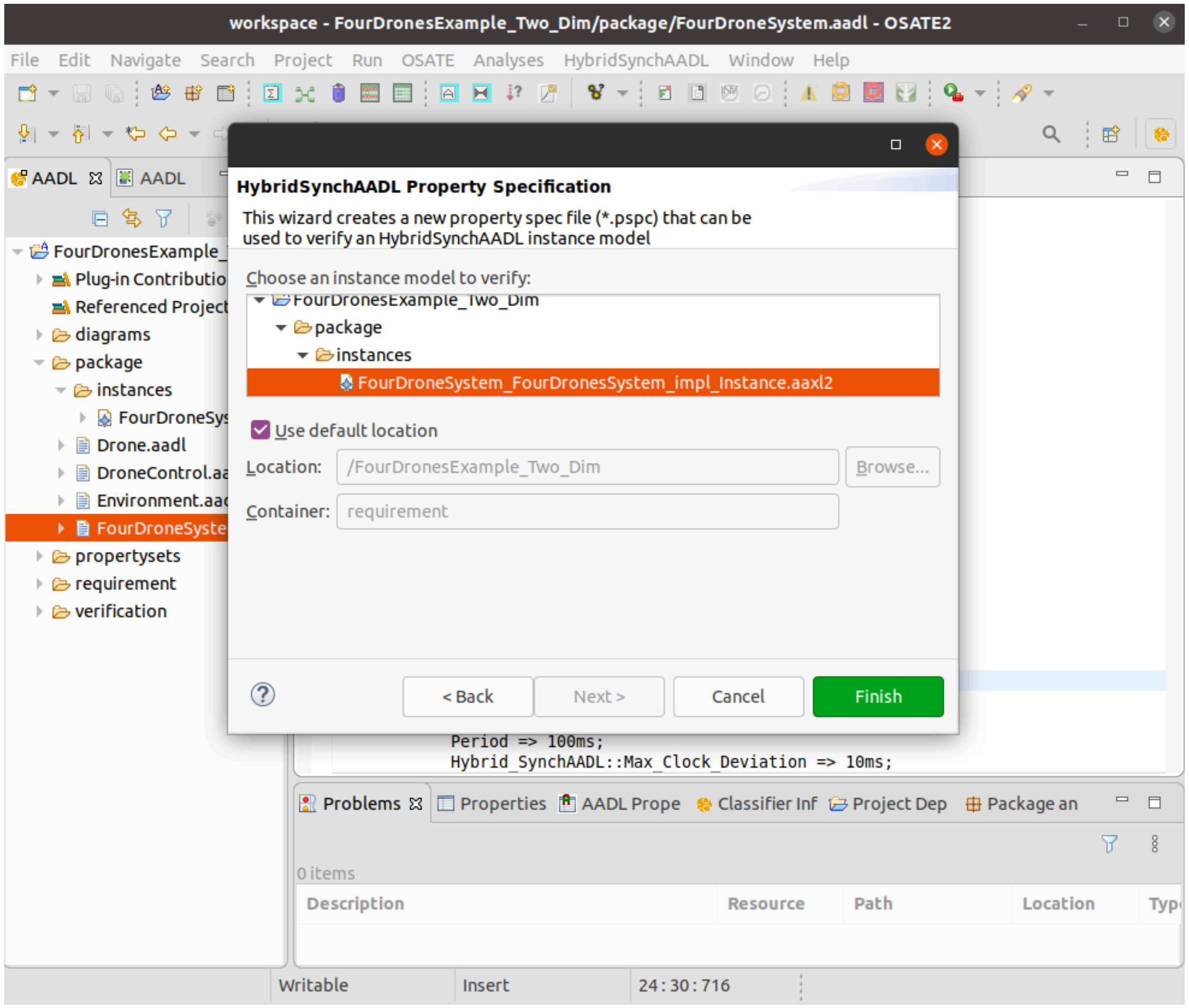
- To create a PSPC file, choose
  - Menu → File → New → Other → HybridSynchAADL → HybridSynchAADL Property Specification file.



```
Period => 100ms;
Hybrid_SynchAADL::Max_Clock_Deviation => 10ms;
```

Creating PSPC Files

- Any valid AADL instance model can be chosen in the wizard.
- Choose the instance model we have created in the previous slides.


workspace - FourDronesExample_Two_Dim/package/FourDroneSystem.aadl - OSATE2

HybridSynchAADL Property Specification

This wizard creates a new property spec file (*.pspc) that can be used to verify an HybridSynchAADL instance model

Choose an instance model to verify:

- FourDronesExample_Two_Dim
  - package
    - instances
      - FourDroneSystem_FourDronesSystem_impl_Instance.aaxl2

☑ Use default location

Location: /FourDronesExample_Two_Dim

Container: requirement

```
Period => 100ms;
Hybrid_SynchAADL::Max_Clock_Deviation => 10ms;
```

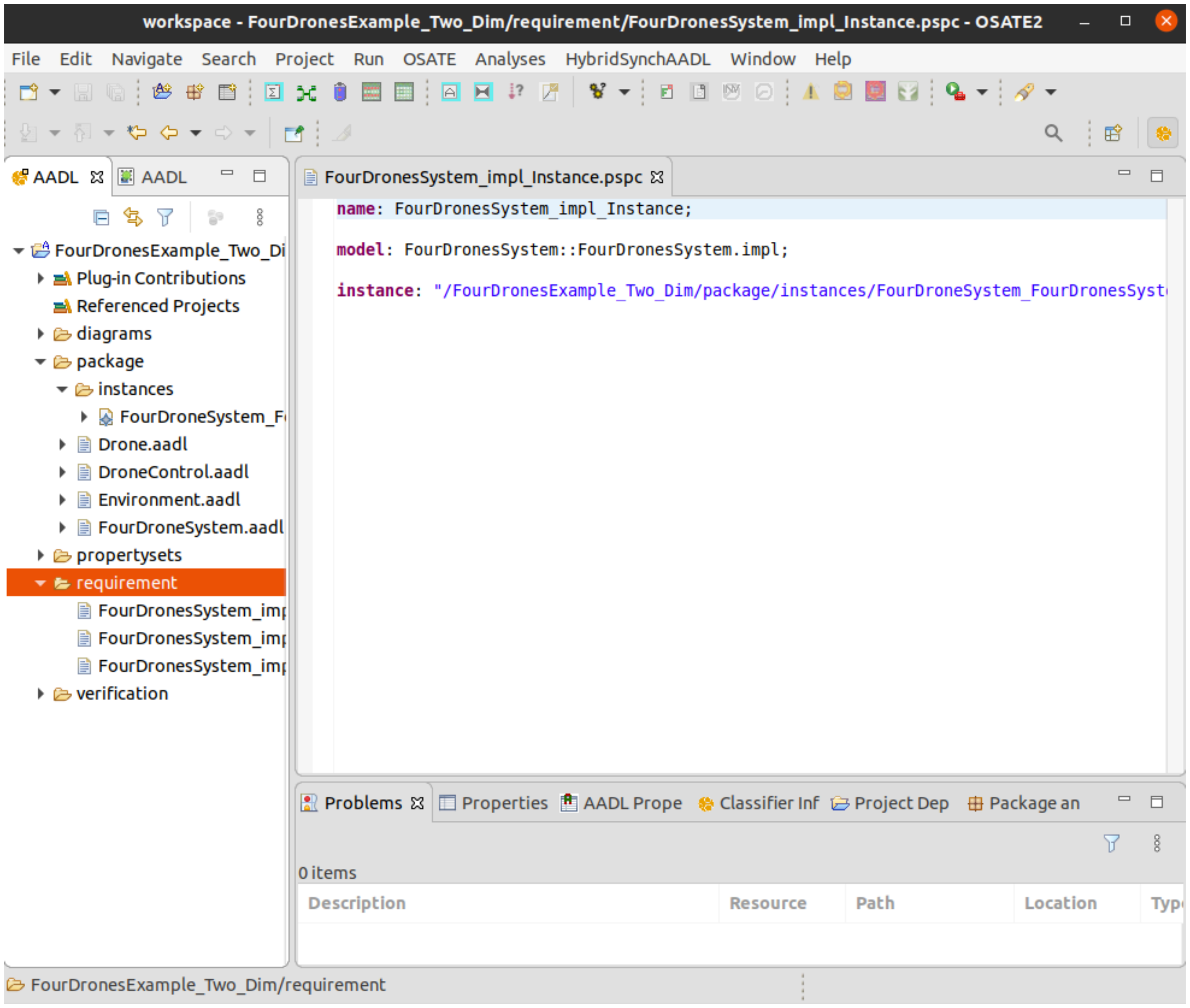
0 items

Description	Resource	Path	Location	Typ

Writable | Insert | 24 : 30 : 716

Creating PSPC Files

- This screen shows the generated (empty) PSPC file.
- There are two sample PSPC files in this project.



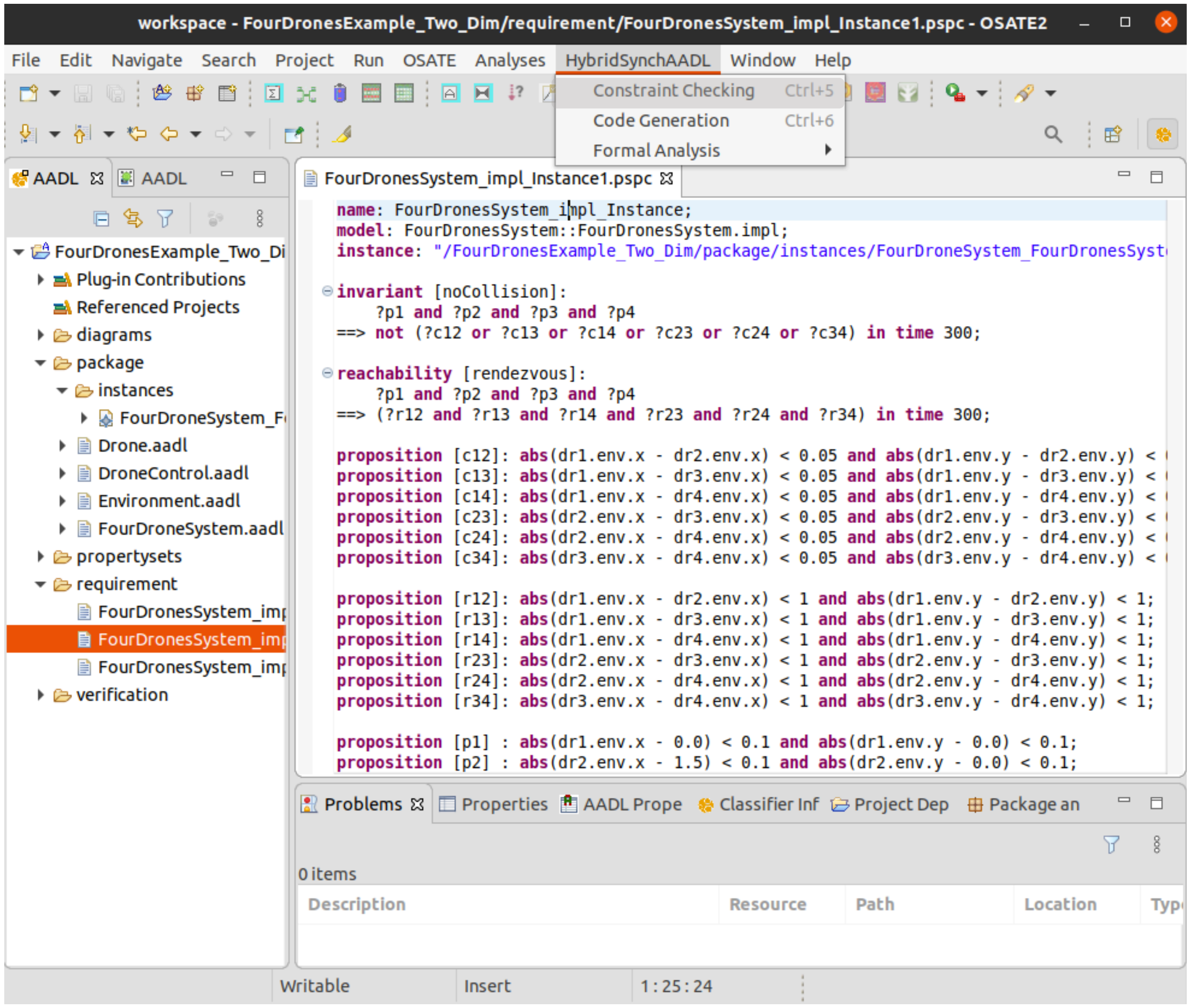
```
name: FourDronesSystem_impl_Instance;

model: FourDronesSystem::FourDronesSystem.impl;

instance: "/FourDronesExample_Two_Dim/package/instances/FourDroneSystem_FourDronesSyst
```

Outline

1. Short Tutorial
2. Basic OSATE
3. Creating Property Specification Files (PSPC)
4. HybridSynchAADL Constraints Checker
5. Rewriting-Modulo-SMT Code Generation
6. Formal Analysis

Checking HybridSynchAADL Constraints

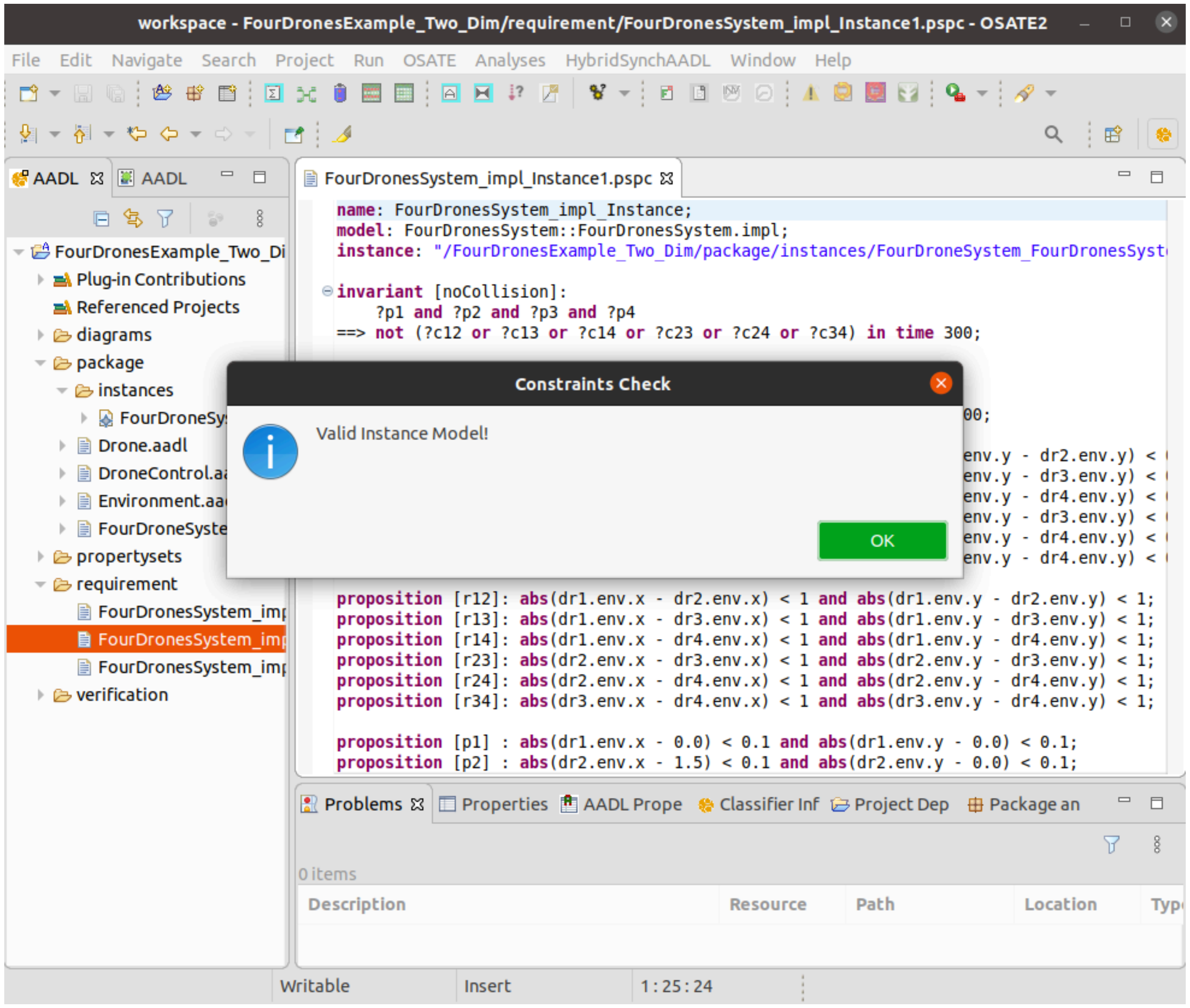
- There are three menu items in HybridSynchAADL: `Constraints Check`, `Code Generation`, and `Formal Analysis`.
- Click `Constraints Check` to perform constraints checking.
- Click `Initial Mode`



```
name: FourDronesSystem_impl_Instance;
model: FourDronesSystem::FourDronesSystem.impl;
instance: "/FourDronesExample_Two_Dim/package/instances/FourDroneSystem_FourDronesSyst

invariant [noCollision]:
    ?p1 and ?p2 and ?p3 and ?p4
==> not (?c12 or ?c13 or ?c14 or ?c23 or ?c24 or ?c34) in time 300;

reachability [rendezvous]:
    ?p1 and ?p2 and ?p3 and ?p4
==> (?r12 and ?r13 and ?r14 and ?r23 and ?r24 and ?r34) in time 300;

proposition [c12]: abs(dr1.env.x - dr2.env.x) < 0.05 and abs(dr1.env.y - dr2.env.y) <
proposition [c13]: abs(dr1.env.x - dr3.env.x) < 0.05 and abs(dr1.env.y - dr3.env.y) <
proposition [c14]: abs(dr1.env.x - dr4.env.x) < 0.05 and abs(dr1.env.y - dr4.env.y) <
proposition [c23]: abs(dr2.env.x - dr3.env.x) < 0.05 and abs(dr2.env.y - dr3.env.y) <
proposition [c24]: abs(dr2.env.x - dr4.env.x) < 0.05 and abs(dr2.env.y - dr4.env.y) <
proposition [c34]: abs(dr3.env.x - dr4.env.x) < 0.05 and abs(dr3.env.y - dr4.env.y) <

proposition [r12]: abs(dr1.env.x - dr2.env.x) < 1 and abs(dr1.env.y - dr2.env.y) < 1;
proposition [r13]: abs(dr1.env.x - dr3.env.x) < 1 and abs(dr1.env.y - dr3.env.y) < 1;
proposition [r14]: abs(dr1.env.x - dr4.env.x) < 1 and abs(dr1.env.y - dr4.env.y) < 1;
proposition [r23]: abs(dr2.env.x - dr3.env.x) < 1 and abs(dr2.env.y - dr3.env.y) < 1;
proposition [r24]: abs(dr2.env.x - dr4.env.x) < 1 and abs(dr2.env.y - dr4.env.y) < 1;
proposition [r34]: abs(dr3.env.x - dr4.env.x) < 1 and abs(dr3.env.y - dr4.env.y) < 1;

proposition [p1] : abs(dr1.env.x - 0.0) < 0.1 and abs(dr1.env.y - 0.0) < 0.1;
proposition [p2] : abs(dr2.env.x - 1.5) < 0.1 and abs(dr2.env.y - 0.0) < 0.1;
```

Checking HybridSynchAADL Constraints

- When the model has no constraints error, the tool notifies that the model is valid.



```
name: FourDronesSystem_impl_Instance;
model: FourDronesSystem::FourDronesSystem.impl;
instance: "/FourDronesExample_Two_Dim/package/instances/FourDroneSystem_FourDronesSyst

invariant [noCollision]:
    ?p1 and ?p2 and ?p3 and ?p4
==> not (?c12 or ?c13 or ?c14 or ?c23 or ?c24 or ?c34) in time 300;
```

Valid Instance Model!

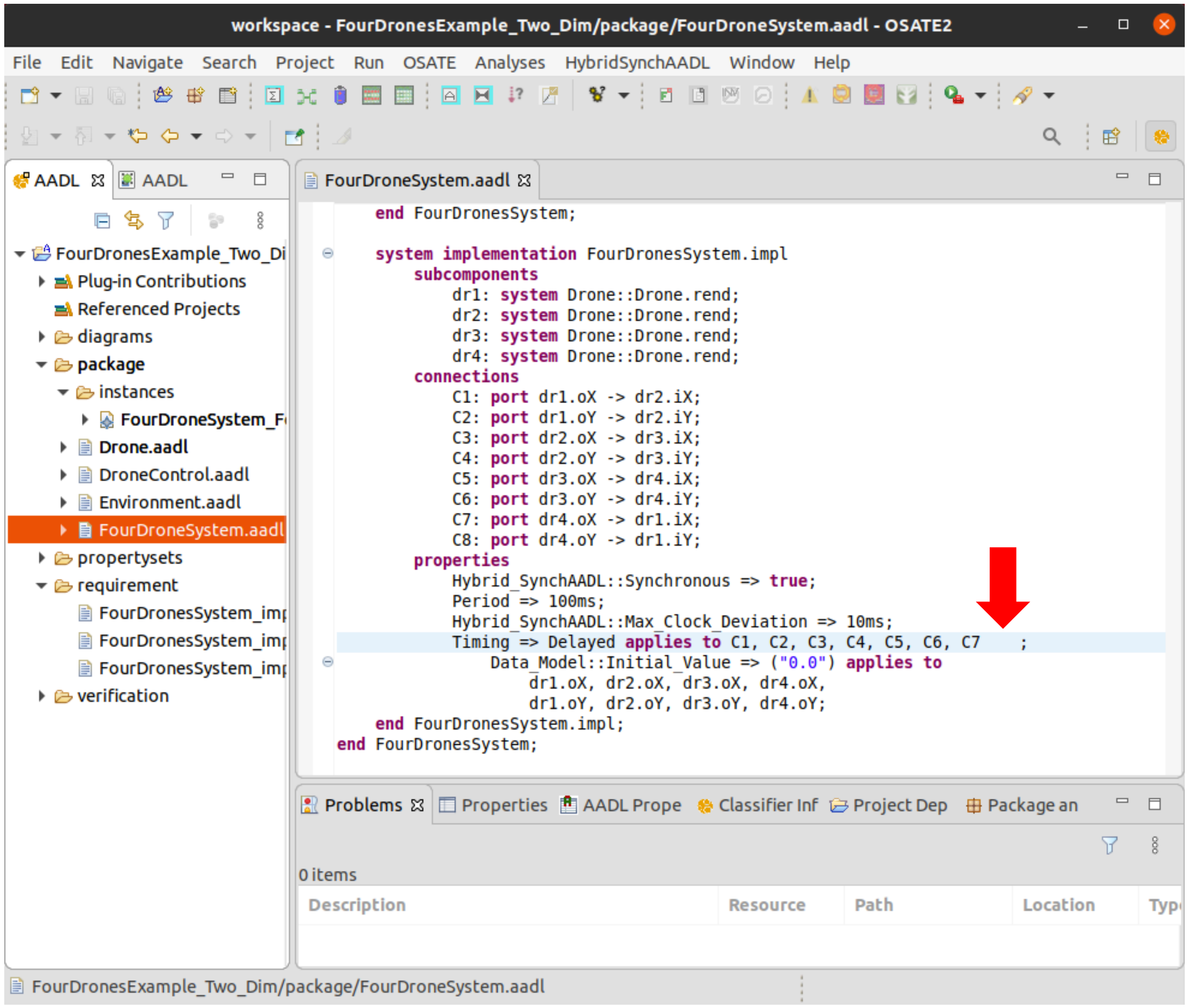
```
00;

env.y - dr2.env.y) <
env.y - dr3.env.y) <
env.y - dr4.env.y) <
env.y - dr3.env.y) <
env.y - dr4.env.y) <
env.y - dr4.env.y) <

proposition [r12]: abs(dr1.env.x - dr2.env.x) < 1 and abs(dr1.env.y - dr2.env.y) < 1;
proposition [r13]: abs(dr1.env.x - dr3.env.x) < 1 and abs(dr1.env.y - dr3.env.y) < 1;
proposition [r14]: abs(dr1.env.x - dr4.env.x) < 1 and abs(dr1.env.y - dr4.env.y) < 1;
proposition [r23]: abs(dr2.env.x - dr3.env.x) < 1 and abs(dr2.env.y - dr3.env.y) < 1;
proposition [r24]: abs(dr2.env.x - dr4.env.x) < 1 and abs(dr2.env.y - dr4.env.y) < 1;
proposition [r34]: abs(dr3.env.x - dr4.env.x) < 1 and abs(dr3.env.y - dr4.env.y) < 1;

proposition [p1] : abs(dr1.env.x - 0.0) < 0.1 and abs(dr1.env.y - 0.0) < 0.1;
proposition [p2] : abs(dr2.env.x - 1.5) < 0.1 and abs(dr2.env.y - 0.0) < 0.1;
```

0 items

Description	Resource	Path	Location	Typ

Constraints Check – Erroneous Model

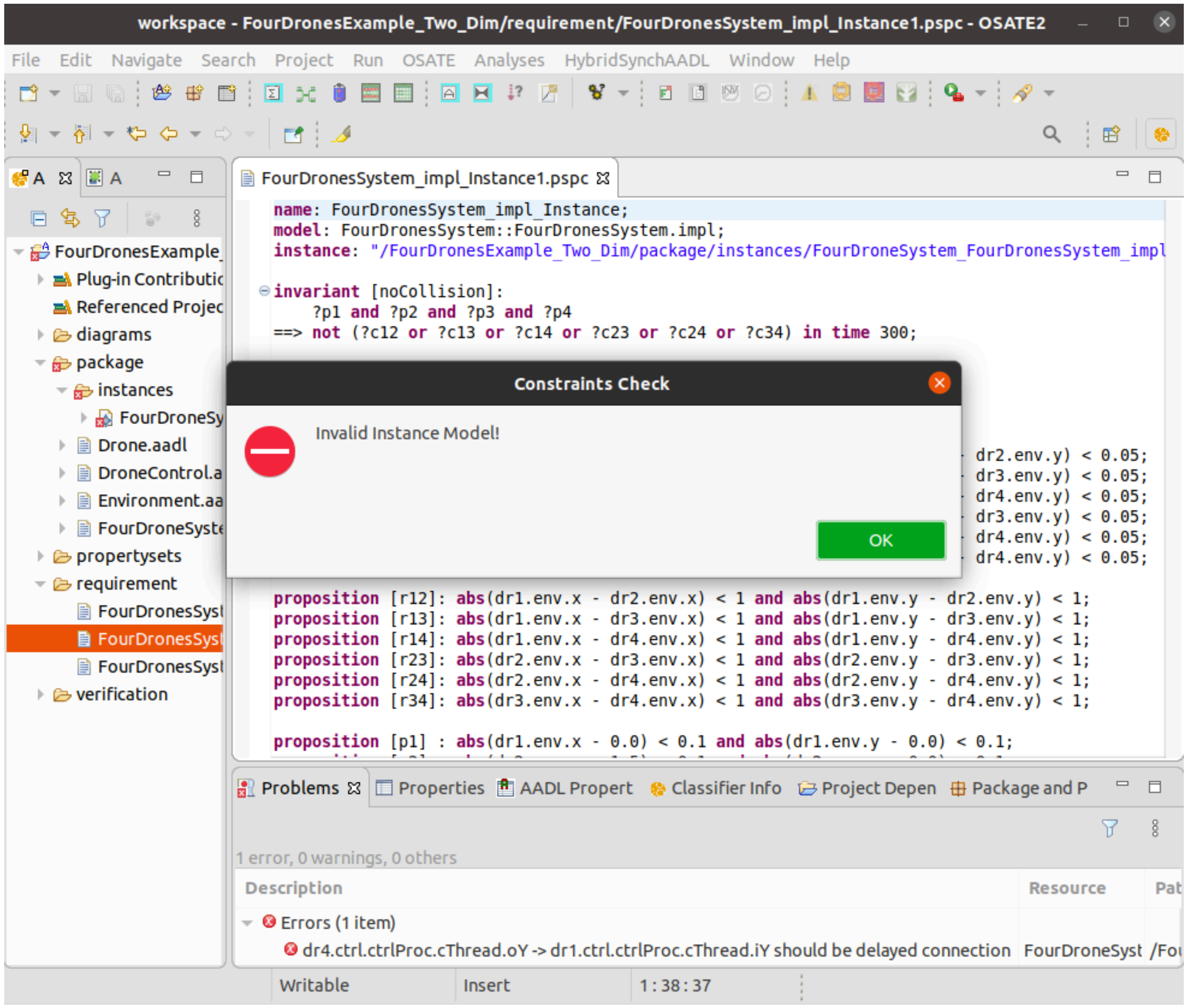
- What if some HybridSynchAADL constraints is not satisfied?
- Let us add an invalid immediate connection and see what happened.
  - by removing the property `Timing => Delayed` from the connection `C8`.



```
    end FourDronesSystem;

    system implementation FourDronesSystem.impl
        subcomponents
            dr1: system Drone::Drone.rend;
            dr2: system Drone::Drone.rend;
            dr3: system Drone::Drone.rend;
            dr4: system Drone::Drone.rend;
        connections
            C1: port dr1.oX -> dr2.iX;
            C2: port dr1.oY -> dr2.iY;
            C3: port dr2.oX -> dr3.iX;
            C4: port dr2.oY -> dr3.iY;
            C5: port dr3.oX -> dr4.iX;
            C6: port dr3.oY -> dr4.iY;
            C7: port dr4.oX -> dr1.iX;
            C8: port dr4.oY -> dr1.iY;
        properties
            Hybrid_SynchAADL::Synchronous => true;
            Period => 100ms;
            Hybrid_SynchAADL::Max_Clock_Deviation => 10ms;
            Timing => Delayed applies to C1, C2, C3, C4, C5, C6, C7    ;
                Data_Model::Initial_Value => ("0.0") applies to
                    dr1.oX, dr2.oX, dr3.oX, dr4.oX,
                    dr1.oY, dr2.oY, dr3.oY, dr4.oY;
    end FourDronesSystem.impl;
end FourDronesSystem;
```

Constraints Check – Erroneous Model

- After re-instantiating the model, click `Constraints Check` to perform constraints checking.
- Click `Initial Mode`
- Our tool then shows an error message in the Problems view.



```
name: FourDronesSystem_impl_Instance;
model: FourDronesSystem::FourDronesSystem.impl;
instance: "/FourDronesExample_Two_Dim/package/instances/FourDroneSystem_FourDronesSystem_impl

invariant [noCollision]:
    ?p1 and ?p2 and ?p3 and ?p4
==> not (?c12 or ?c13 or ?c14 or ?c23 or ?c24 or ?c34) in time 300;

                                                                        dr2.env.y) < 0.05;
                                                                        dr3.env.y) < 0.05;
                                                                        dr4.env.y) < 0.05;
                                                                        dr3.env.y) < 0.05;
                                                                        dr4.env.y) < 0.05;
                                                                        dr4.env.y) < 0.05;

proposition [r12]: abs(dr1.env.x - dr2.env.x) < 1 and abs(dr1.env.y - dr2.env.y) < 1;
proposition [r13]: abs(dr1.env.x - dr3.env.x) < 1 and abs(dr1.env.y - dr3.env.y) < 1;
proposition [r14]: abs(dr1.env.x - dr4.env.x) < 1 and abs(dr1.env.y - dr4.env.y) < 1;
proposition [r23]: abs(dr2.env.x - dr3.env.x) < 1 and abs(dr2.env.y - dr3.env.y) < 1;
proposition [r24]: abs(dr2.env.x - dr4.env.x) < 1 and abs(dr2.env.y - dr4.env.y) < 1;
proposition [r34]: abs(dr3.env.x - dr4.env.x) < 1 and abs(dr3.env.y - dr4.env.y) < 1;

proposition [p1] : abs(dr1.env.x - 0.0) < 0.1 and abs(dr1.env.y - 0.0) < 0.1;
```

Constraints Check

Invalid Instance Model!

OK

1 error, 0 warnings, 0 others

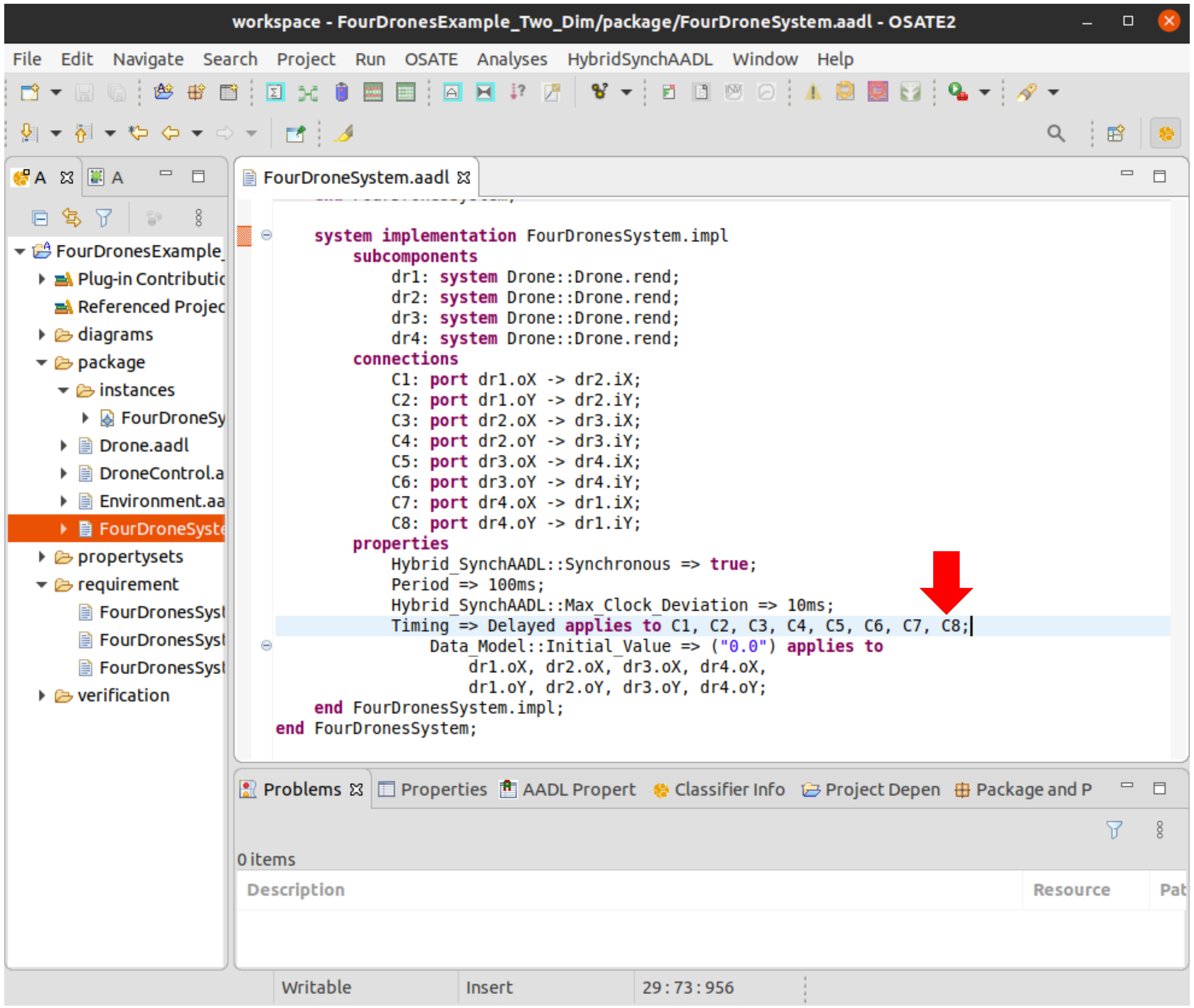
Description	Resource	Pat
Errors (1 item)		
dr4.ctrl.ctrlProc.cThread.oY -> dr1.ctrl.ctrlProc.cThread.iY should be delayed connection	FourDroneSyst	/Fo

Outline

1. Short Tutorial
2. Basic OSATE
3. Creating Property Specification Files (PSPC)
4. HybridSynchAADL Constraints Checker
5. Rewriting-Modulo-SMT Code Generation
6. Formal Analysis

The FourDronesSystem Example

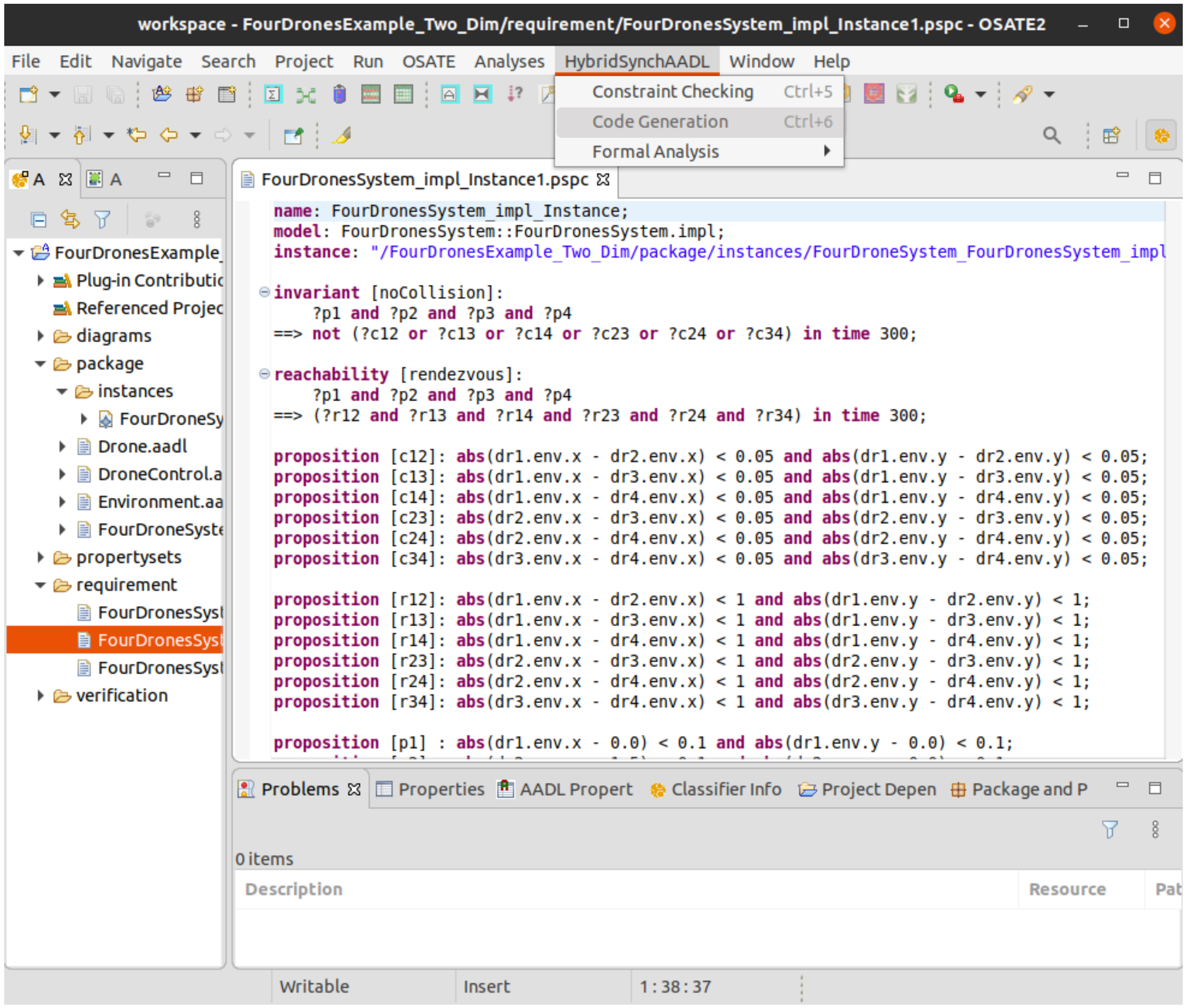
- Let us go back to the correct model.
- Don't forget to instantiate the model again.



```
    system implementation FourDronesSystem.impl
        subcomponents
            dr1: system Drone::Drone.rend;
            dr2: system Drone::Drone.rend;
            dr3: system Drone::Drone.rend;
            dr4: system Drone::Drone.rend;
        connections
            C1: port dr1.oX -> dr2.iX;
            C2: port dr1.oY -> dr2.iY;
            C3: port dr2.oX -> dr3.iX;
            C4: port dr2.oY -> dr3.iY;
            C5: port dr3.oX -> dr4.iX;
            C6: port dr3.oY -> dr4.iY;
            C7: port dr4.oX -> dr1.iX;
            C8: port dr4.oY -> dr1.iY;
        properties
            Hybrid_SynchAADL::Synchronous => true;
            Period => 100ms;
            Hybrid_SynchAADL::Max_Clock_Deviation => 10ms;
            Timing => Delayed applies to C1, C2, C3, C4, C5, C6, C7, C8;
                Data_Model::Initial_Value => ("0.0") applies to
                    dr1.oX, dr2.oX, dr3.oX, dr4.oX,
                    dr1.oY, dr2.oY, dr3.oY, dr4.oY;
    end FourDronesSystem.impl;
end FourDronesSystem;
```

Rewriting-Modulo-SMT Code Generation

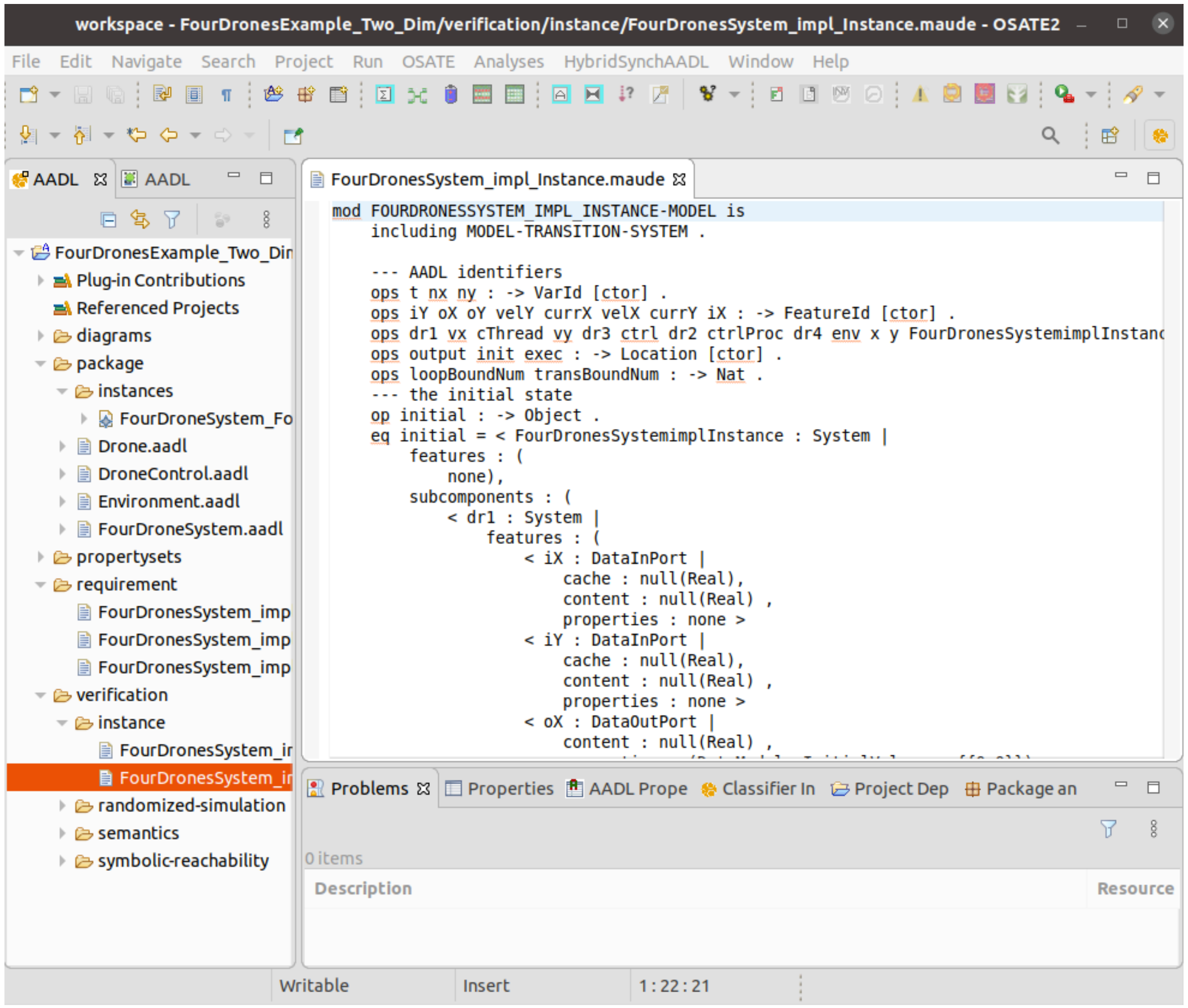
- Click `Code Generation` to automatically generate the rewriting-modulo-SMT model from the HybridSynchAADL model.



```
name: FourDronesSystem_impl_Instance;
model: FourDronesSystem::FourDronesSystem.impl;
instance: "/FourDronesExample_Two_Dim/package/instances/FourDroneSystem_FourDronesSystem_impl

invariant [noCollision]:
    ?p1 and ?p2 and ?p3 and ?p4
==> not (?c12 or ?c13 or ?c14 or ?c23 or ?c24 or ?c34) in time 300;

reachability [rendezvous]:
    ?p1 and ?p2 and ?p3 and ?p4
==> (?r12 and ?r13 and ?r14 and ?r23 and ?r24 and ?r34) in time 300;

proposition [c12]: abs(dr1.env.x - dr2.env.x) < 0.05 and abs(dr1.env.y - dr2.env.y) < 0.05;
proposition [c13]: abs(dr1.env.x - dr3.env.x) < 0.05 and abs(dr1.env.y - dr3.env.y) < 0.05;
proposition [c14]: abs(dr1.env.x - dr4.env.x) < 0.05 and abs(dr1.env.y - dr4.env.y) < 0.05;
proposition [c23]: abs(dr2.env.x - dr3.env.x) < 0.05 and abs(dr2.env.y - dr3.env.y) < 0.05;
proposition [c24]: abs(dr2.env.x - dr4.env.x) < 0.05 and abs(dr2.env.y - dr4.env.y) < 0.05;
proposition [c34]: abs(dr3.env.x - dr4.env.x) < 0.05 and abs(dr3.env.y - dr4.env.y) < 0.05;

proposition [r12]: abs(dr1.env.x - dr2.env.x) < 1 and abs(dr1.env.y - dr2.env.y) < 1;
proposition [r13]: abs(dr1.env.x - dr3.env.x) < 1 and abs(dr1.env.y - dr3.env.y) < 1;
proposition [r14]: abs(dr1.env.x - dr4.env.x) < 1 and abs(dr1.env.y - dr4.env.y) < 1;
proposition [r23]: abs(dr2.env.x - dr3.env.x) < 1 and abs(dr2.env.y - dr3.env.y) < 1;
proposition [r24]: abs(dr2.env.x - dr4.env.x) < 1 and abs(dr2.env.y - dr4.env.y) < 1;
proposition [r34]: abs(dr3.env.x - dr4.env.x) < 1 and abs(dr3.env.y - dr4.env.y) < 1;

proposition [p1] : abs(dr1.env.x - 0.0) < 0.1 and abs(dr1.env.y - 0.0) < 0.1;
```

Rewriting-Modulo-SMT Code Generation

- The generated Maude files, including Maude files for properties, are in the `verification/instance` directory.



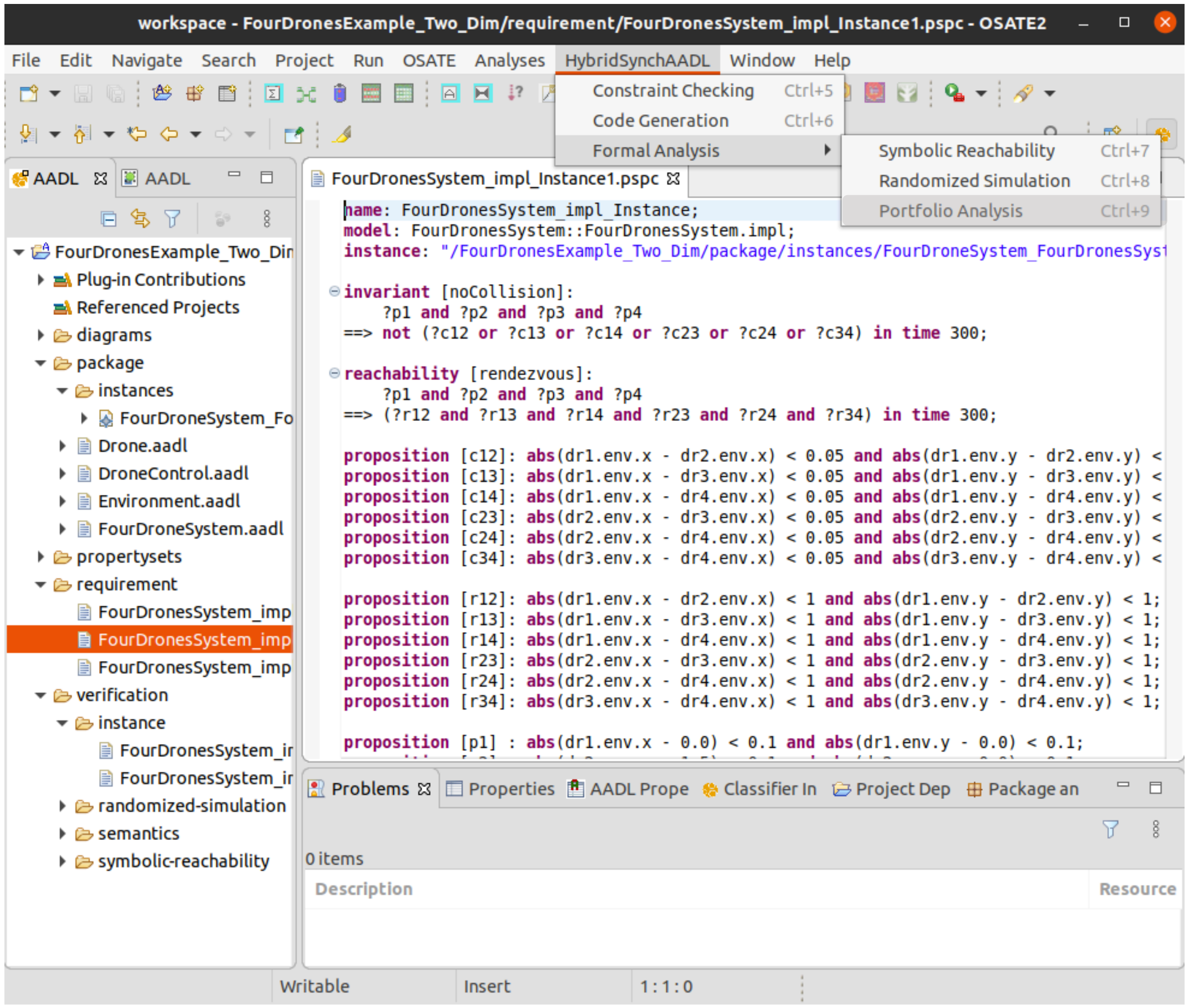
```
mod FOURDRONESSYSTEM_IMPL_INSTANCE-MODEL is
    including MODEL-TRANSITION-SYSTEM .

    --- AADL identifiers
    ops t nx ny : -> VarId [ctor] .
    ops iY oX oY velY currX velX currY iX : -> FeatureId [ctor] .
    ops dr1 vx cThread vy dr3 ctrl dr2 ctrlProc dr4 env x y FourDronesSystemimplInstanc
    ops output init exec : -> Location [ctor] .
    ops loopBoundNum transBoundNum : -> Nat .
    --- the initial state
    op initial : -> Object .
    eq initial = < FourDronesSystemimplInstance : System |
        features : (
            none),
        subcomponents : (
            < dr1 : System |
                features : (
                    < iX : DataInPort |
                        cache : null(Real),
                        content : null(Real) ,
                        properties : none >
                    < iY : DataInPort |
                        cache : null(Real),
                        content : null(Real) ,
                        properties : none >
                    < oX : DataOutPort |
                        content : null(Real) ,
```

Outline

1. Short Tutorial
2. Basic OSATE
3. Creating Property Specification Files (PSPC)
4. HybridSynchAADL Constraints Checker
5. Rewriting-Modulo-SMT Code Generation
6. Formal Analysis

Portfolio Analysis

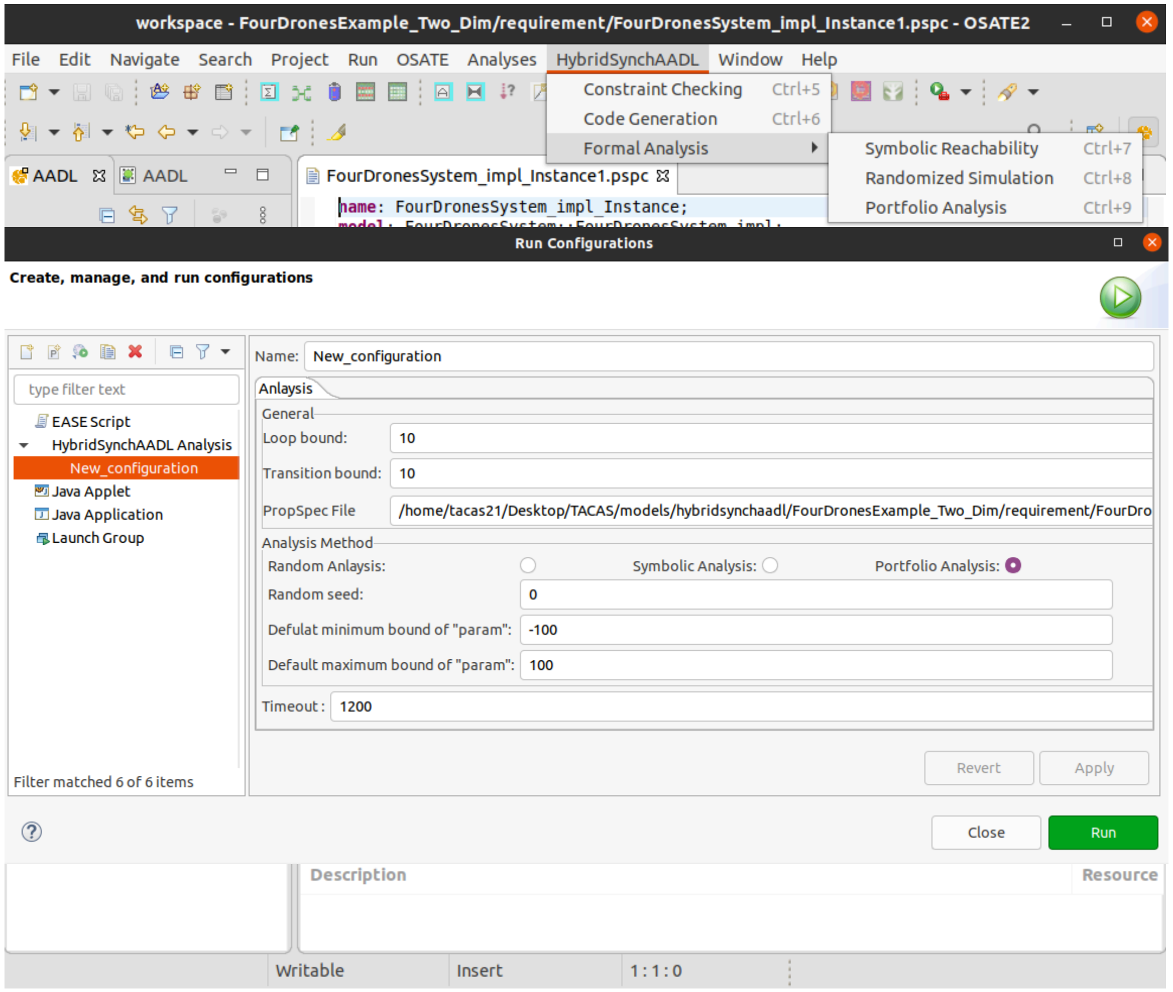
- Click `Portfolio Analysis` to perform symbolic reachability and randomized simulation simultaneously using rewriting-modulo-SMT.



```
name: FourDronesSystem_impl_Instance;
model: FourDronesSystem::FourDronesSystem.impl;
instance: "/FourDronesExample_Two_Dim/package/instances/FourDroneSystem_FourDronesSyst

invariant [noCollision]:
    ?p1 and ?p2 and ?p3 and ?p4
==> not (?c12 or ?c13 or ?c14 or ?c23 or ?c24 or ?c34) in time 300;

reachability [rendezvous]:
    ?p1 and ?p2 and ?p3 and ?p4
==> (?r12 and ?r13 and ?r14 and ?r23 and ?r24 and ?r34) in time 300;

proposition [c12]: abs(dr1.env.x - dr2.env.x) < 0.05 and abs(dr1.env.y - dr2.env.y) <
proposition [c13]: abs(dr1.env.x - dr3.env.x) < 0.05 and abs(dr1.env.y - dr3.env.y) <
proposition [c14]: abs(dr1.env.x - dr4.env.x) < 0.05 and abs(dr1.env.y - dr4.env.y) <
proposition [c23]: abs(dr2.env.x - dr3.env.x) < 0.05 and abs(dr2.env.y - dr3.env.y) <
proposition [c24]: abs(dr2.env.x - dr4.env.x) < 0.05 and abs(dr2.env.y - dr4.env.y) <
proposition [c34]: abs(dr3.env.x - dr4.env.x) < 0.05 and abs(dr3.env.y - dr4.env.y) <

proposition [r12]: abs(dr1.env.x - dr2.env.x) < 1 and abs(dr1.env.y - dr2.env.y) < 1;
proposition [r13]: abs(dr1.env.x - dr3.env.x) < 1 and abs(dr1.env.y - dr3.env.y) < 1;
proposition [r14]: abs(dr1.env.x - dr4.env.x) < 1 and abs(dr1.env.y - dr4.env.y) < 1;
proposition [r23]: abs(dr2.env.x - dr3.env.x) < 1 and abs(dr2.env.y - dr3.env.y) < 1;
proposition [r24]: abs(dr2.env.x - dr4.env.x) < 1 and abs(dr2.env.y - dr4.env.y) < 1;
proposition [r34]: abs(dr3.env.x - dr4.env.x) < 1 and abs(dr3.env.y - dr4.env.y) < 1;

proposition [p1] : abs(dr1.env.x - 0.0) < 0.1 and abs(dr1.env.y - 0.0) < 0.1;
```

Portfolio Analysis

- Create a new configuration file
- Set PSPC file "FourDronesSystem_impl_Instance1.pspc" path
- Click `Portfolio Analysis` radio button
- Set positive integer value in `Random Seed`
- Set proper range value for parameterized variables.
- Set positive integer value in `Timeout`
    - `-1` can be set for infinite time.

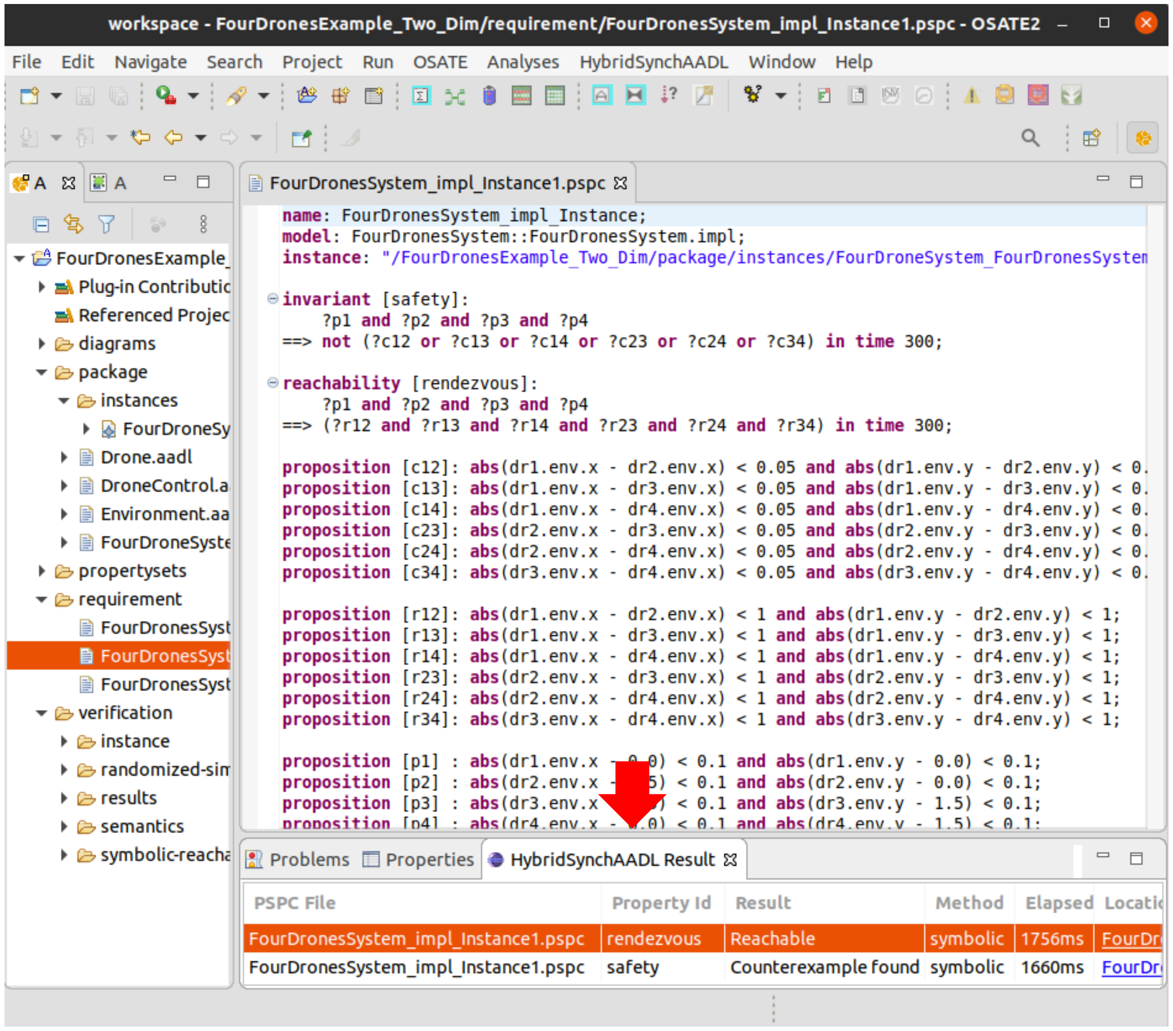

workspace - FourDronesExample_Two_Dim/requirement/FourDronesSystem_impl_Instance1.pspc - OSATE2
File Edit Navigate Search Project Run OSATE Analyses HybridSynchAADL Window Help
Constraint Checking Ctrl+5
Code Generation Ctrl+6
Formal Analysis
Symbolic Reachability Ctrl+7
Randomized Simulation Ctrl+8
Portfolio Analysis Ctrl+9
AADL
AADL
FourDronesSystem_impl_Instance1.pspc
Run Configurations
Create, manage, and run configurations
type filter text
EASE Script
HybridSynchAADL Analysis
New_configuration
Java Applet
Java Application
Launch Group
Filter matched 6 of 6 items
Revert
Apply
Close
Run
Description
Resource
Writable
Insert
1 : 1 : 0

```
name: FourDronesSystem_impl_Instance;
```

Name:	New_configuration
Anlaysis	
General	
Loop bound:	10
Transition bound:	10
PropSpec File	/home/tacas21/Desktop/TACAS/models/hybridsynchaadl/FourDronesExample_Two_Dim/requirement/FourDro
Analysis Method	
Random Anlaysis: ○ Symbolic Analysis: ○	[✓ Portfolio Analysis: ●]
Random seed:	0
Defulat minimum bound of "param":	-100
Default maximum bound of "param":	100
Timeout :	1200

Analysis Results (1)

- The HybridSynchAADL Result view shows the analysis results.

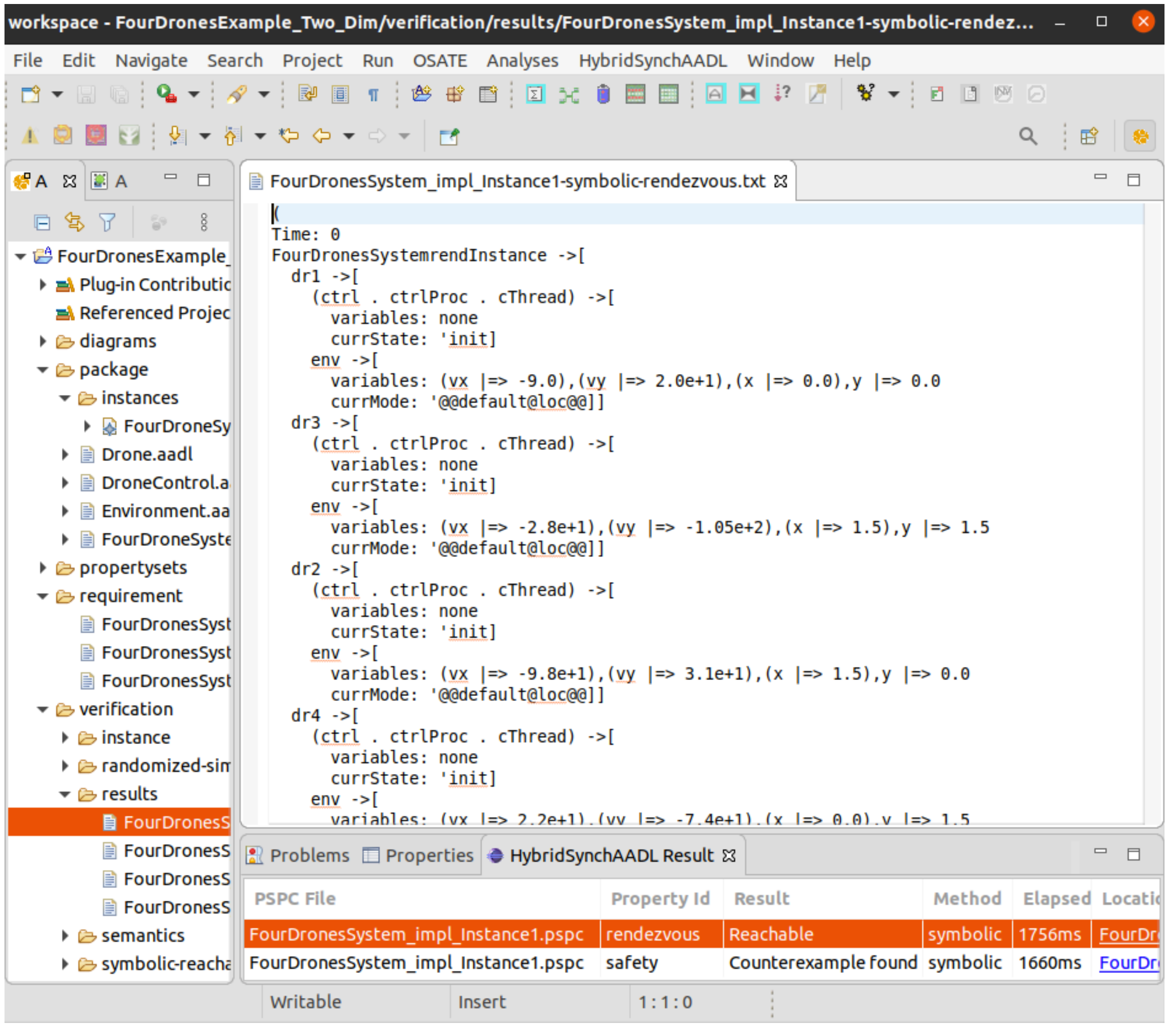


```
name: FourDronesSystem_impl_Instance;
model: FourDronesSystem::FourDronesSystem.impl;
instance: "/FourDronesExample_Two_Dim/package/instances/FourDroneSystem_FourDronesSysten

invariant [safety]:
    ?p1 and ?p2 and ?p3 and ?p4
==> not (?c12 or ?c13 or ?c14 or ?c23 or ?c24 or ?c34) in time 300;

reachability [rendezvous]:
    ?p1 and ?p2 and ?p3 and ?p4
==> (?r12 and ?r13 and ?r14 and ?r23 and ?r24 and ?r34) in time 300;

proposition [c12]: abs(dr1.env.x - dr2.env.x) < 0.05 and abs(dr1.env.y - dr2.env.y) < 0.
proposition [c13]: abs(dr1.env.x - dr3.env.x) < 0.05 and abs(dr1.env.y - dr3.env.y) < 0.
proposition [c14]: abs(dr1.env.x - dr4.env.x) < 0.05 and abs(dr1.env.y - dr4.env.y) < 0.
proposition [c23]: abs(dr2.env.x - dr3.env.x) < 0.05 and abs(dr2.env.y - dr3.env.y) < 0.
proposition [c24]: abs(dr2.env.x - dr4.env.x) < 0.05 and abs(dr2.env.y - dr4.env.y) < 0.
proposition [c34]: abs(dr3.env.x - dr4.env.x) < 0.05 and abs(dr3.env.y - dr4.env.y) < 0.

proposition [r12]: abs(dr1.env.x - dr2.env.x) < 1 and abs(dr1.env.y - dr2.env.y) < 1;
proposition [r13]: abs(dr1.env.x - dr3.env.x) < 1 and abs(dr1.env.y - dr3.env.y) < 1;
proposition [r14]: abs(dr1.env.x - dr4.env.x) < 1 and abs(dr1.env.y - dr4.env.y) < 1;
proposition [r23]: abs(dr2.env.x - dr3.env.x) < 1 and abs(dr2.env.y - dr3.env.y) < 1;
proposition [r24]: abs(dr2.env.x - dr4.env.x) < 1 and abs(dr2.env.y - dr4.env.y) < 1;
proposition [r34]: abs(dr3.env.x - dr4.env.x) < 1 and abs(dr3.env.y - dr4.env.y) < 1;

proposition [p1] : abs(dr1.env.x - 0.0) < 0.1 and abs(dr1.env.y - 0.0) < 0.1;
proposition [p2] : abs(dr2.env.x [illegible]5) < 0.1 and abs(dr2.env.y - 0.0) < 0.1;
proposition [p3] : abs(dr3.env.x [illegible]) < 0.1 and abs(dr3.env.y - 1.5) < 0.1;
proposition [p4] : abs(dr4.env.x - [illegible].0) < 0.1 and abs(dr4.env.y - 1.5) < 0.1;
```

PSPC File	Property Id	Result	Method	Elapsed	Locatic
FourDronesSystem_impl_Instance1.pspc	rendezvous	Reachable	symbolic	1756ms	FourDr
FourDronesSystem_impl_Instance1.pspc	safety	Counterexample found	symbolic	1660ms	FourDr

Counterexamples and Witnesses

- Each file in Location in the result view contains a counterexample of an invariant property or a witness of a reachability property, if it exists.



workspace - FourDronesExample_Two_Dim/verification/results/FourDronesSystem_impl_Instance1-symbolic-rendez...

FourDronesSystem_impl_Instance1-symbolic-rendezvous.txt

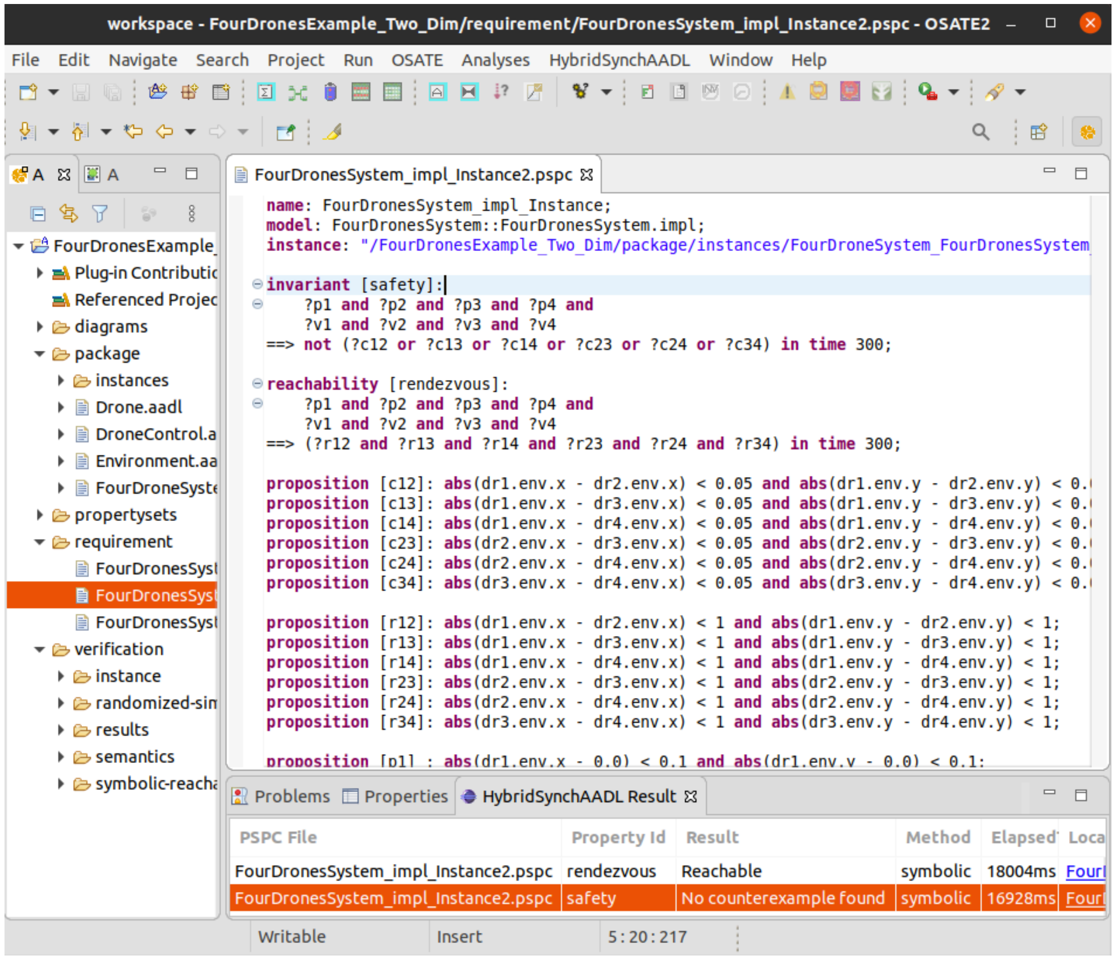
```
(
Time: 0
FourDronesSystemrendInstance ->[
  dr1 ->[
    (ctrl . ctrlProc . cThread) ->[
      variables: none
      currState: 'init]
    env ->[
      variables: (vx |=> -9.0),(vy |=> 2.0e+1),(x |=> 0.0),y |=> 0.0
      currMode: '@@default@loc@@]]
  dr3 ->[
    (ctrl . ctrlProc . cThread) ->[
      variables: none
      currState: 'init]
    env ->[
      variables: (vx |=> -2.8e+1),(vy |=> -1.05e+2),(x |=> 1.5),y |=> 1.5
      currMode: '@@default@loc@@]]
  dr2 ->[
    (ctrl . ctrlProc . cThread) ->[
      variables: none
      currState: 'init]
    env ->[
      variables: (vx |=> -9.8e+1),(vy |=> 3.1e+1),(x |=> 1.5),y |=> 0.0
      currMode: '@@default@loc@@]]
  dr4 ->[
    (ctrl . ctrlProc . cThread) ->[
      variables: none
      currState: 'init]
    env ->[
      variables: (vx |=> 2.2e+1),(vy |=> -7.4e+1),(x |=> 0.0),y |=> 1.5
```

HybridSynchAADL Result

PSPC File	Property Id	Result	Method	Elapsed	Locatic
FourDronesSystem_impl_Instance1.pspc	rendezvous	Reachable	symbolic	1756ms	FourDr
FourDronesSystem_impl_Instance1.pspc	safety	Counterexample found	symbolic	1660ms	FourDr

Analysis Results (2)

- In the case of “FourDronesSystem_impl_Instsance2.pspc”
- The result shows there is no counterexample found and a reachability of witness found



workspace - FourDronesExample_Two_Dim/requirement/FourDronesSystem_impl_Instance2.pspc - OSATE2

```
name: FourDronesSystem_impl_Instance;
model: FourDronesSystem::FourDronesSystem.impl;
instance: "/FourDronesExample_Two_Dim/package/instances/FourDroneSystem_FourDronesSystem

invariant [safety]:
    ?p1 and ?p2 and ?p3 and ?p4 and
    ?v1 and ?v2 and ?v3 and ?v4
==> not (?c12 or ?c13 or ?c14 or ?c23 or ?c24 or ?c34) in time 300;

reachability [rendezvous]:
    ?p1 and ?p2 and ?p3 and ?p4 and
    ?v1 and ?v2 and ?v3 and ?v4
==> (?r12 and ?r13 and ?r14 and ?r23 and ?r24 and ?r34) in time 300;

proposition [c12]: abs(dr1.env.x - dr2.env.x) < 0.05 and abs(dr1.env.y - dr2.env.y) < 0.
proposition [c13]: abs(dr1.env.x - dr3.env.x) < 0.05 and abs(dr1.env.y - dr3.env.y) < 0.
proposition [c14]: abs(dr1.env.x - dr4.env.x) < 0.05 and abs(dr1.env.y - dr4.env.y) < 0.
proposition [c23]: abs(dr2.env.x - dr3.env.x) < 0.05 and abs(dr2.env.y - dr3.env.y) < 0.
proposition [c24]: abs(dr2.env.x - dr4.env.x) < 0.05 and abs(dr2.env.y - dr4.env.y) < 0.
proposition [c34]: abs(dr3.env.x - dr4.env.x) < 0.05 and abs(dr3.env.y - dr4.env.y) < 0.

proposition [r12]: abs(dr1.env.x - dr2.env.x) < 1 and abs(dr1.env.y - dr2.env.y) < 1;
proposition [r13]: abs(dr1.env.x - dr3.env.x) < 1 and abs(dr1.env.y - dr3.env.y) < 1;
proposition [r14]: abs(dr1.env.x - dr4.env.x) < 1 and abs(dr1.env.y - dr4.env.y) < 1;
proposition [r23]: abs(dr2.env.x - dr3.env.x) < 1 and abs(dr2.env.y - dr3.env.y) < 1;
proposition [r24]: abs(dr2.env.x - dr4.env.x) < 1 and abs(dr2.env.y - dr4.env.y) < 1;
proposition [r34]: abs(dr3.env.x - dr4.env.x) < 1 and abs(dr3.env.y - dr4.env.y) < 1;

proposition [p1] : abs(dr1.env.x - 0.0) < 0.1 and abs(dr1.env.y - 0.0) < 0.1;
```

PSPC File	Property Id	Result	Method	Elapsed	Loca
FourDronesSystem_impl_Instance2.pspc	rendezvous	Reachable	symbolic	18004ms	Four
FourDronesSystem_impl_Instance2.pspc	safety	No counterexample found	symbolic	16928ms	Four

Writable Insert 5 : 20 : 217

Thank you!