Analyzing Unsynthesizable High-Level Robot Specifications in LTLMoP

Vasu Raman and Hadas Kress-Gazit
Autonomous Systems Lab, Cornell University

CAV 2011
Tuesday, July 19

High -Level Tasks:

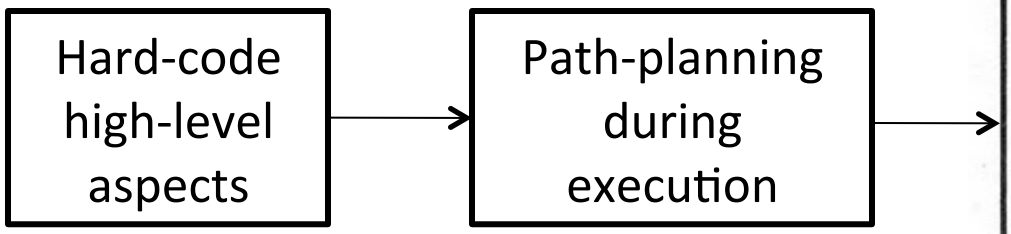
- Patrolling a workspace for an indefinite period
  (**infinite** behaviour)
- Responding to signals or objects of interest
  (**reactive**)

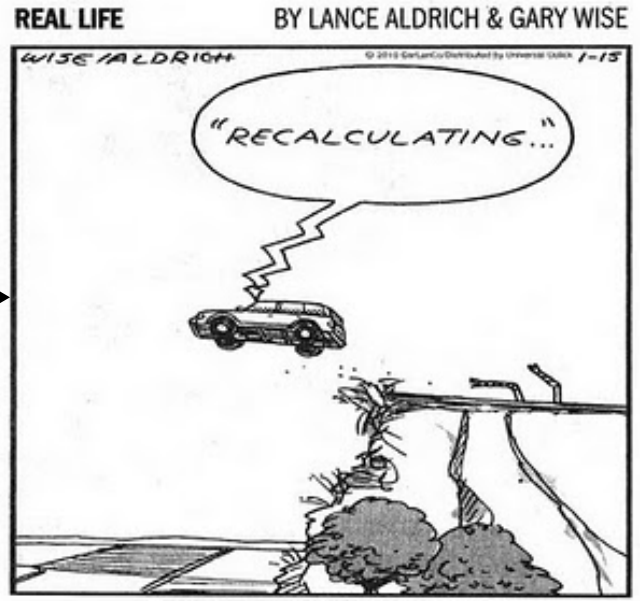
Examples:

Search and rescue missions
Autonomous Unmanned Vehicles
e.g. DARPA Urban Challenge
Firefighting robots
Household chores (laundry, cleanup)
Restocking supermarket shelves

AUTOMATED HIGH-LEVEL ROBOT CONTROL :

Usual Approach





- Need to plan for a large number of contingencies.
- Does the implementation capture the high level requirements?
- Is the intended behavior even achievable?

  Do there exist robot controllers that guarantee fulfillment of the task?

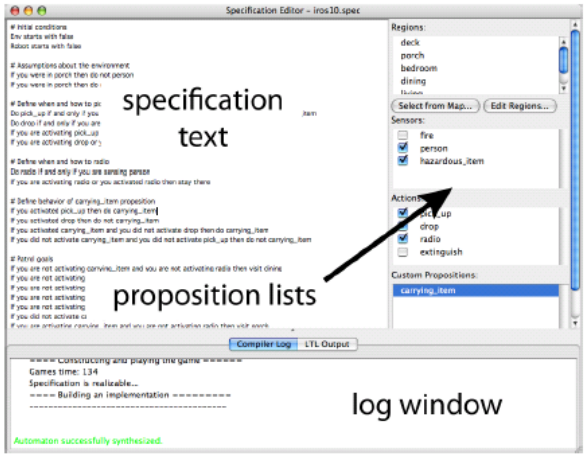
FORMAL GUARANTEES:

Verifiable integration of high-level planning with continuous control.

LINEAR TEMPORAL LOGIC MISSION PLANNING TOOLKIT (LTLMOP)

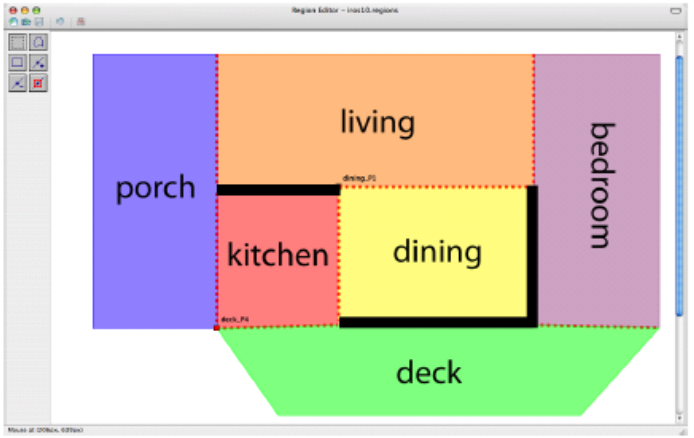
- Discretized problem abstraction
- Structured English specifications ⇔ GR(1) formulas in LTL.
  - environment assumptions
  - desired system behaviour
- Synthesis of correct-by-construction controllers.

LTLMoP Overview



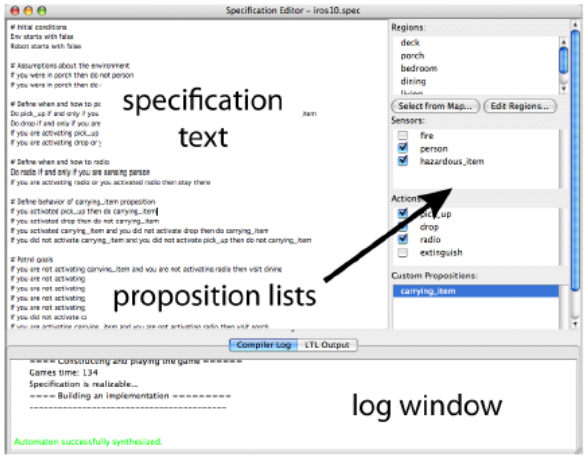
(Specification Editor)

Robot Capability Definitions (Sensors/Actions)



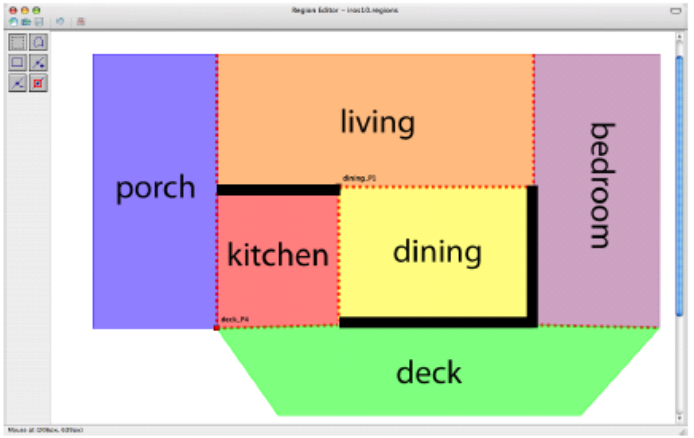
(Region Editor)

LTLMoP Overview



(Specification Editor)

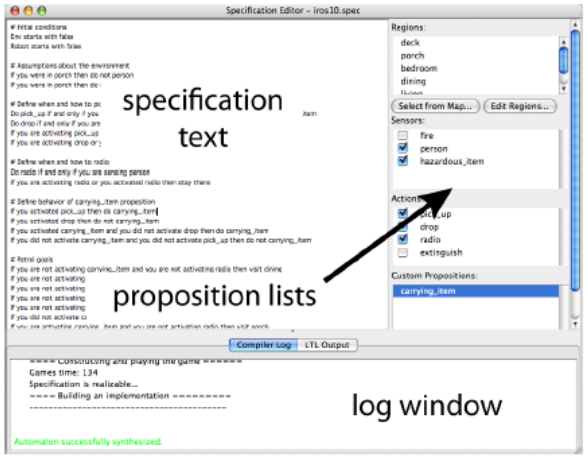
Robot Capability Definitions (Sensors/Actions)



(Region Editor)

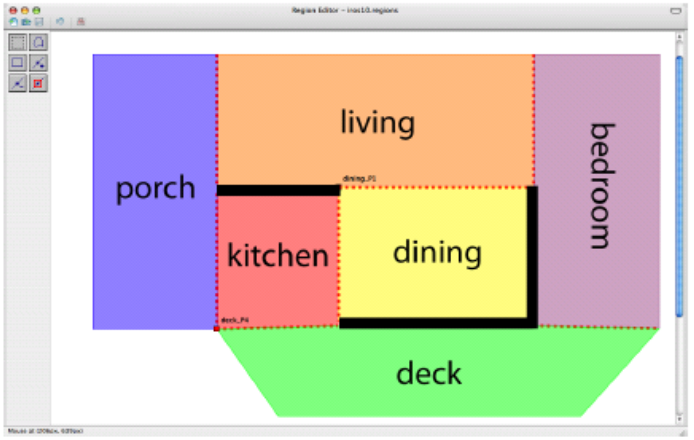
Structured English-to-LTL Parser

LTLMoP Overview



(Specification Editor)

Robot Capability Definitions (Sensors/Actions)

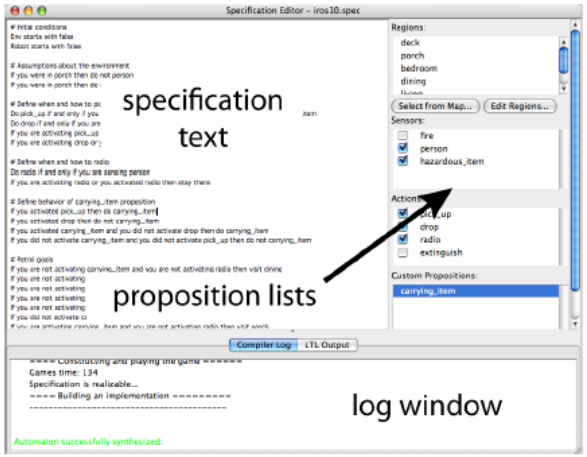


(Region Editor)

Structured English-to-LTL Parser

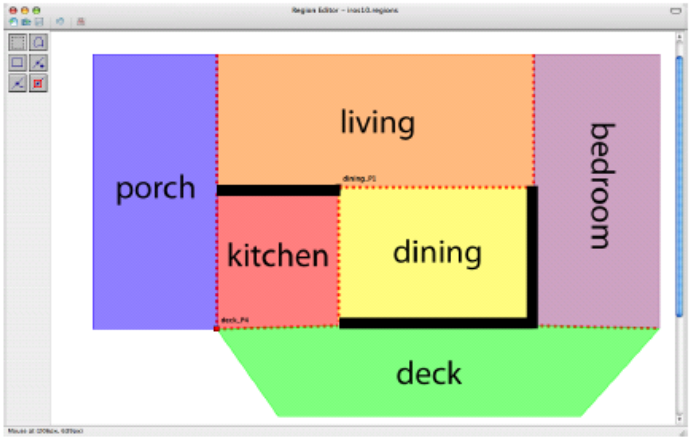
Synthesis

LTLMoP Overview



(Specification Editor)

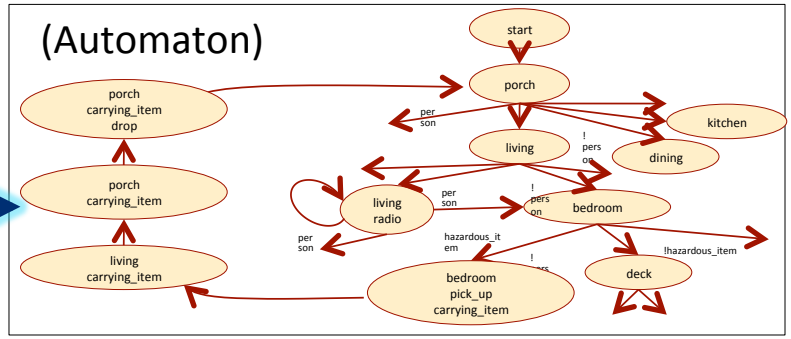
Robot Capability Definitions (Sensors/Actions)



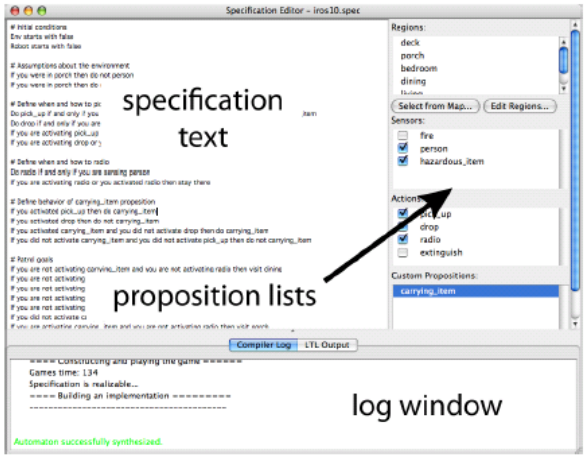
(Region Editor)

Structured English-to-LTL Parser

Synthesis

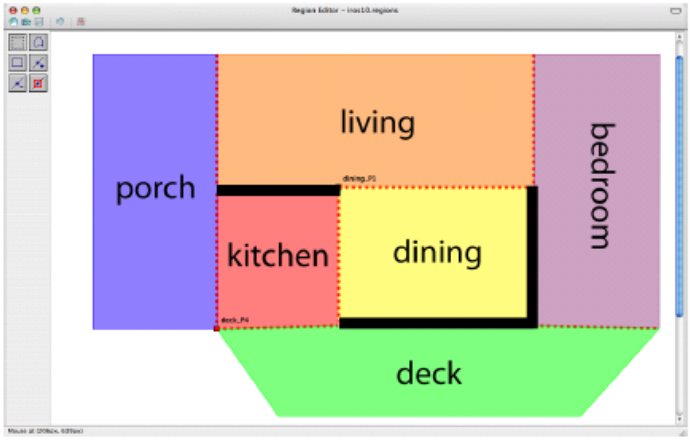


LTLMoP Overview



(Specification Editor)

Robot Capability Definitions (Sensors/Actions)

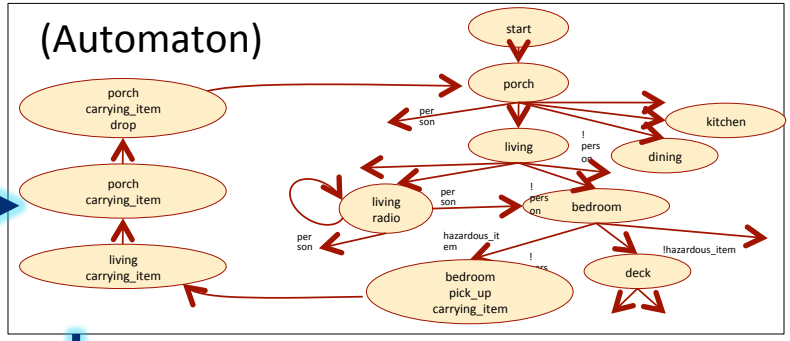


(Region Editor)

Structured English-to-LTL Parser

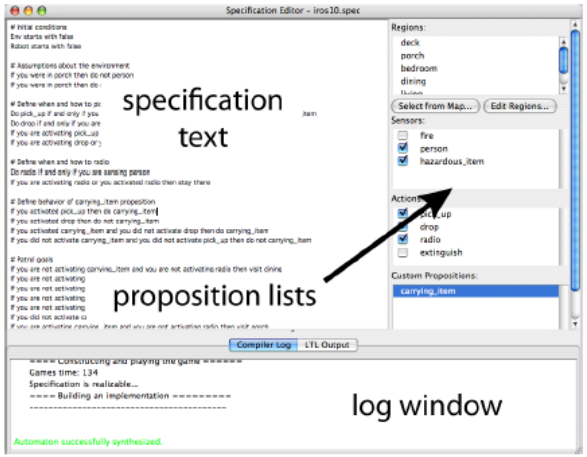
Synthesis

(Automaton)



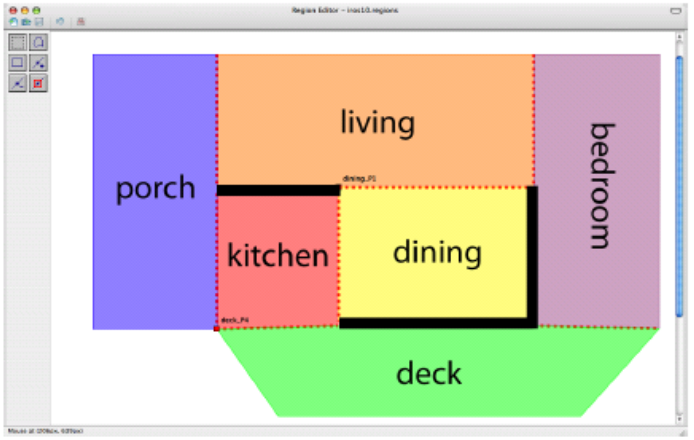
Hybrid Controller

LTLMoP Overview



(Specification Editor)

Robot Capability Definitions (Sensors/Actions)

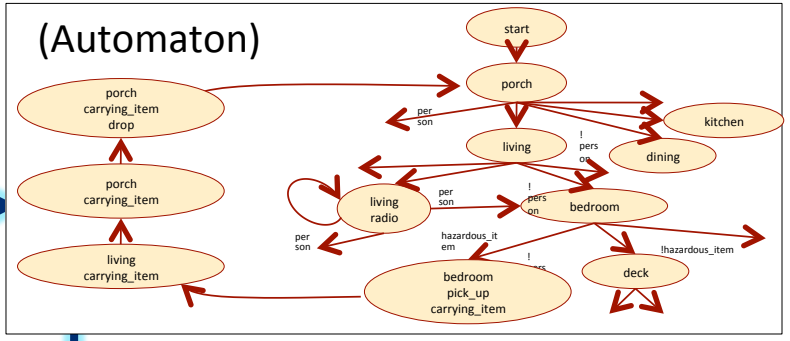


(Region Editor)

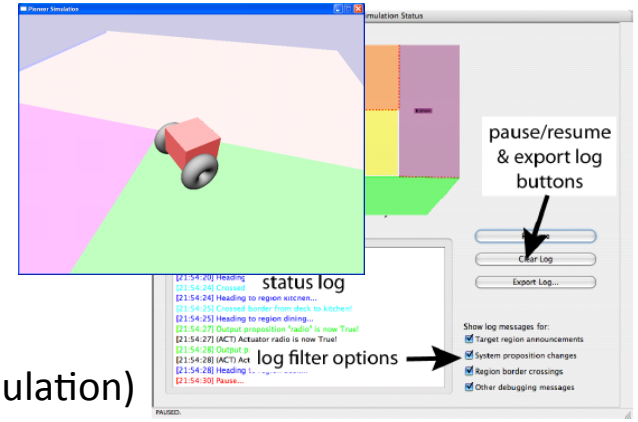
Structured English-to-LTL Parser

Synthesis

(Automaton)

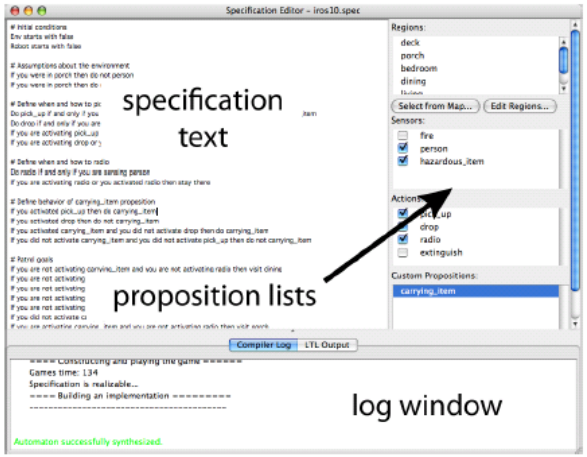


Hybrid Controller



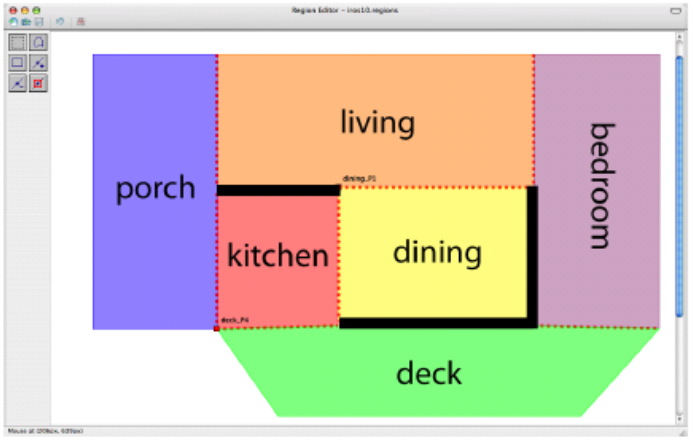
(Simulation)

LTLMoP Overview



(Specification Editor)

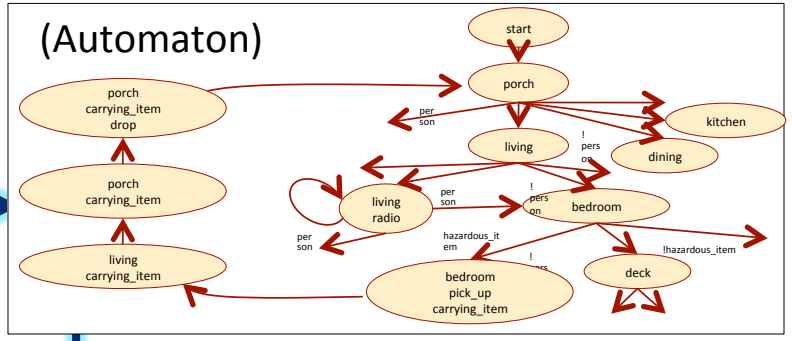
Robot Capability Definitions (Sensors/Actions)



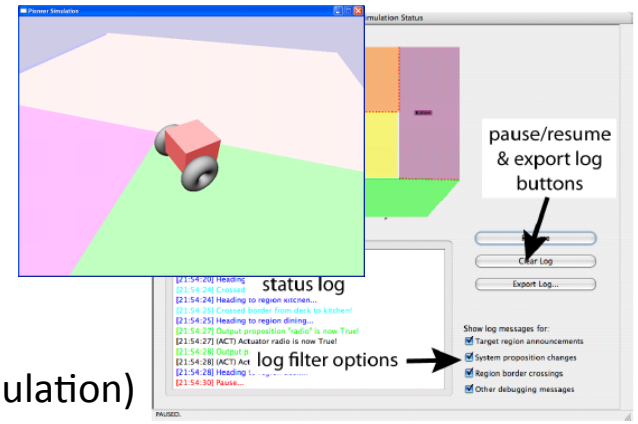
(Region Editor)

Structured English-to-LTL Parser

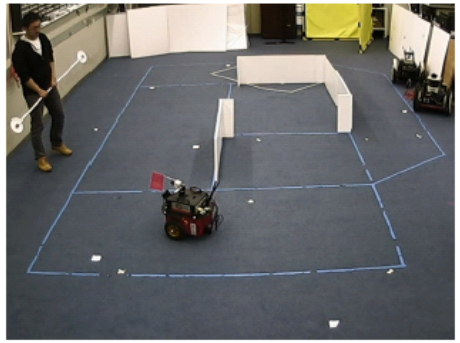
Synthesis



Hybrid Controller



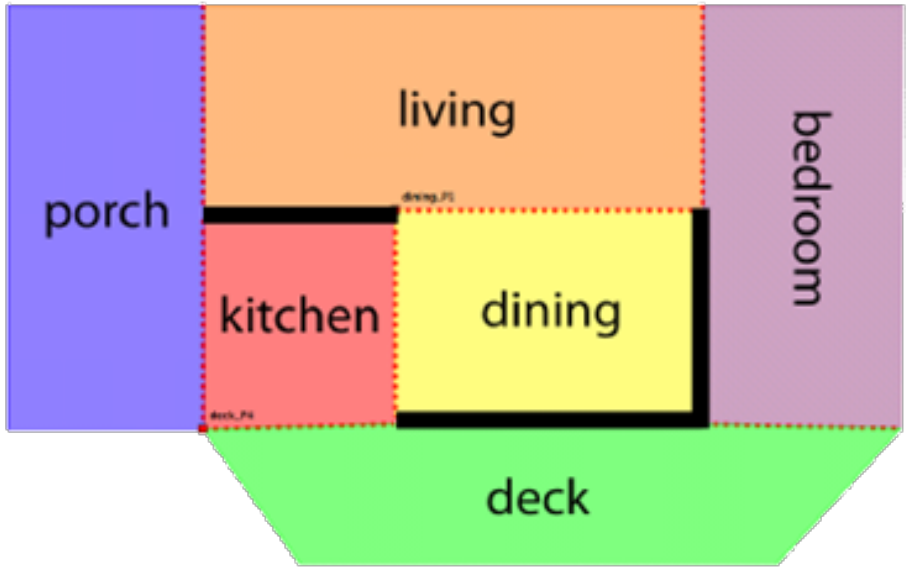
(Simulation)



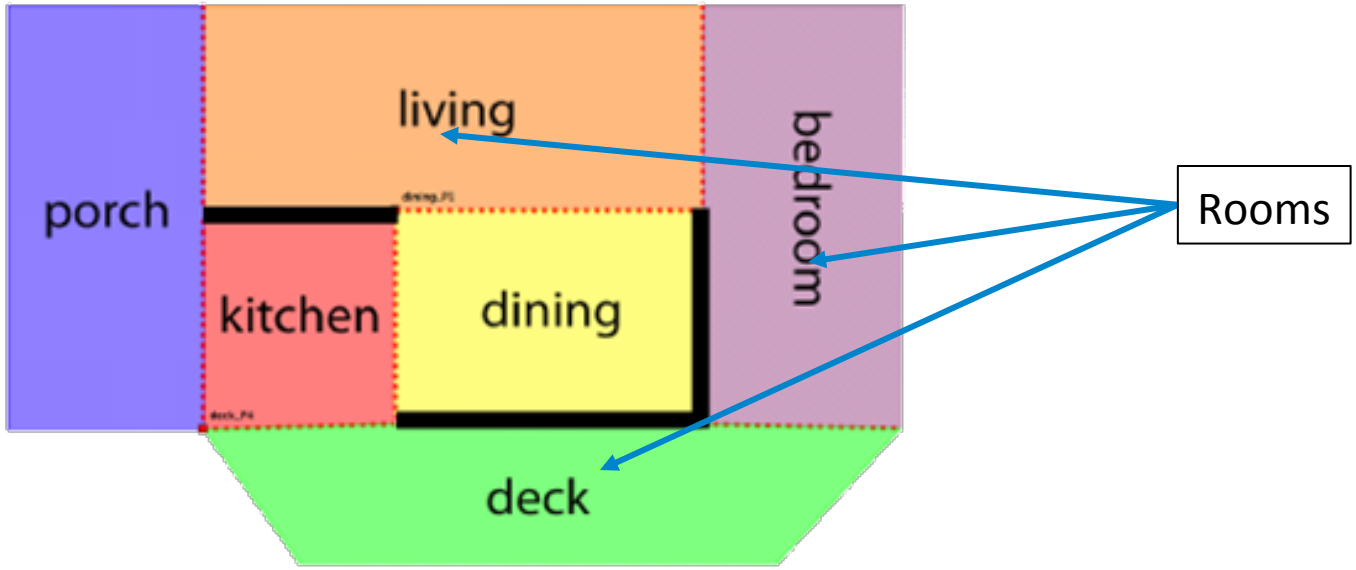
(Physical Robot)

EXAMPLE: FIRE-FIGHTING SCENARIO

FIRE-FIGHTING SCENARIO



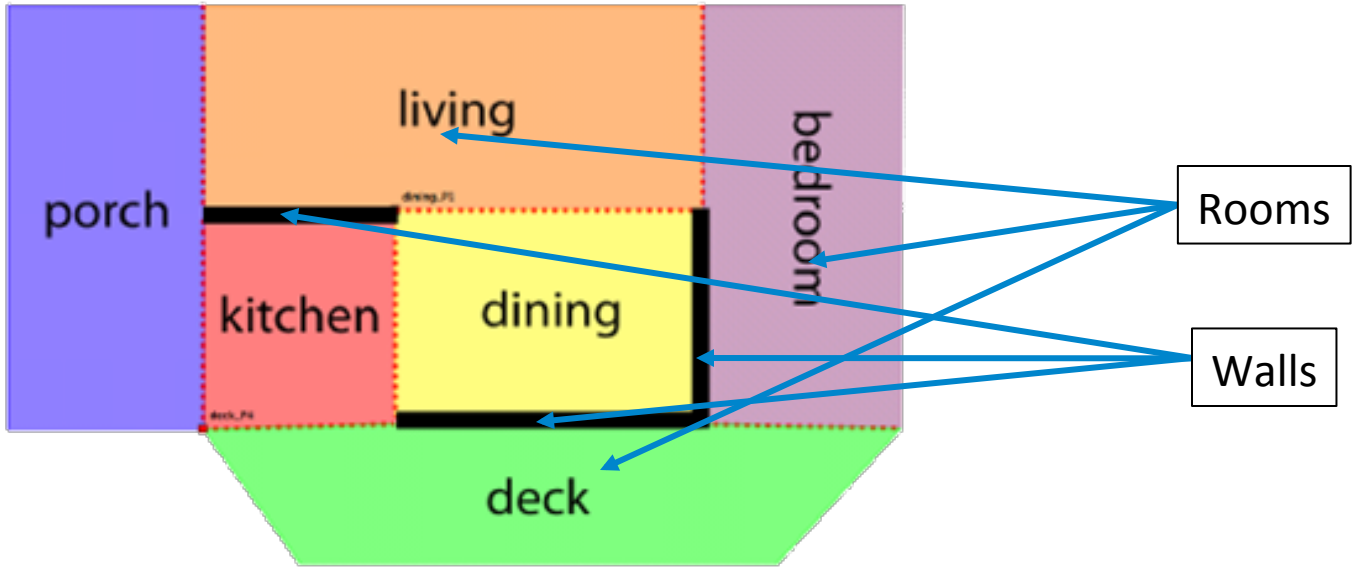
FIRE-FIGHTING SCENARIO



Regions:

- **porch, deck, etc.**

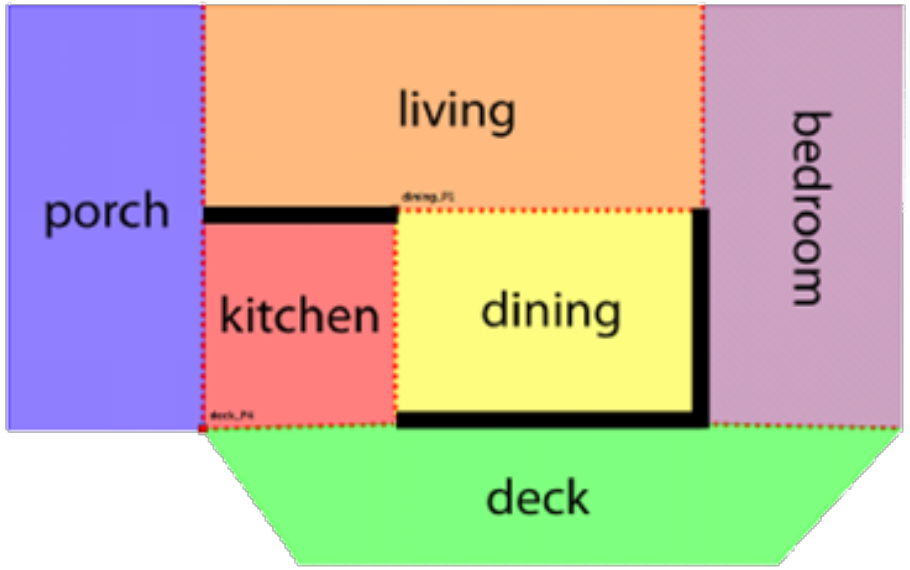
FIRE-FIGHTING SCENARIO



Regions:

- **porch, deck, etc.**

FIRE-FIGHTING SCENARIO



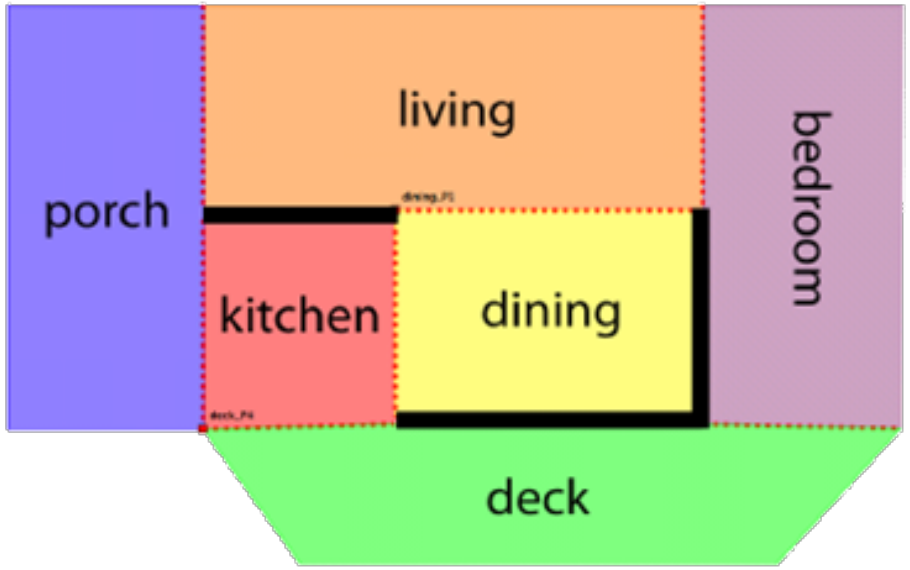
Regions:

- porch, deck, etc.

Robot actions:

- pick_up
- drop
- radio
- carrying_item

FIRE-FIGHTING SCENARIO



Regions:

- porch, deck, etc.

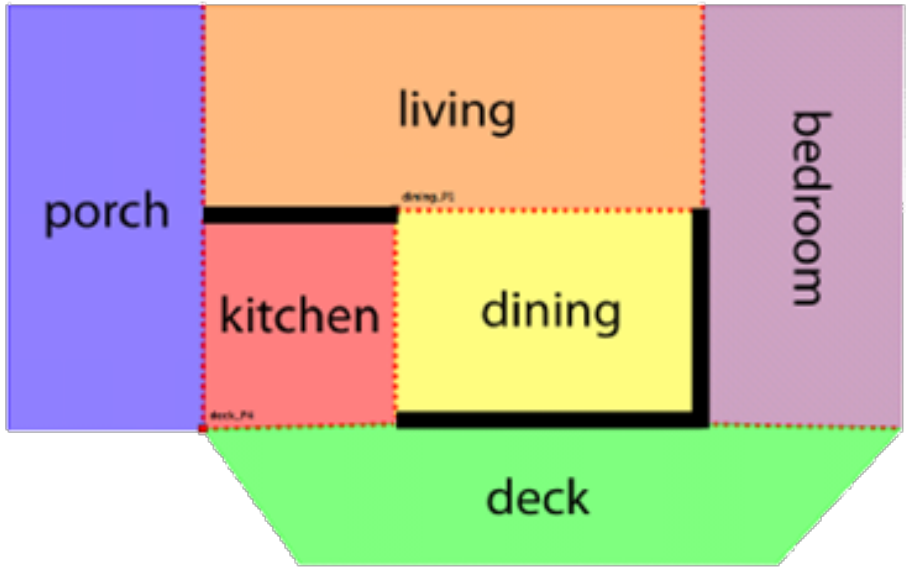
Robot actions:

- pick_up
- drop
- radio
- carrying_item

Sensors:

- hazardous_item
- person

FIRE-FIGHTING SCENARIO



Regions:

- porch, deck, etc.

Robot actions:

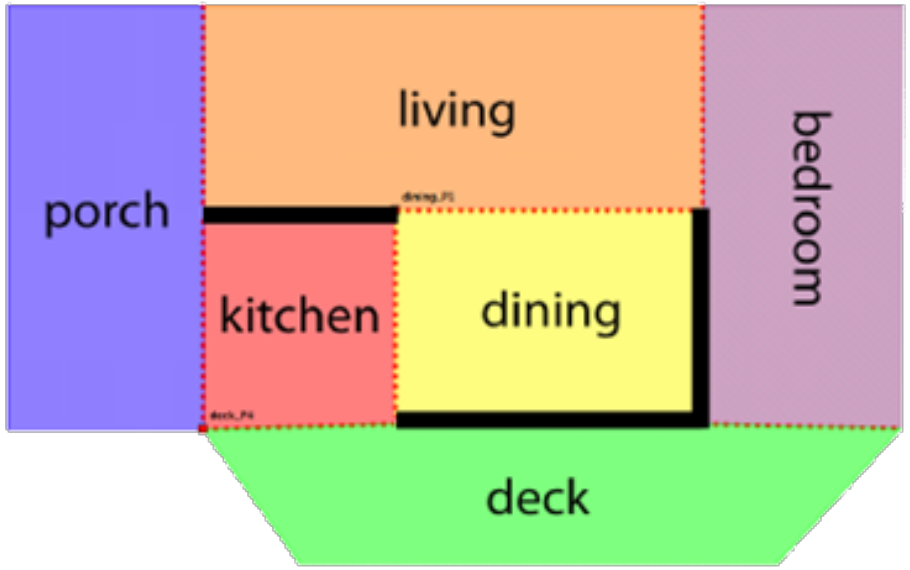
- pick_up
- drop
- radio
- carrying_item

System Propositions

Sensors:

- hazardous_item
- person

FIRE-FIGHTING SCENARIO



Regions:

- porch, deck, etc.

Robot actions:

- pick_up
- drop
- radio
- carrying_item

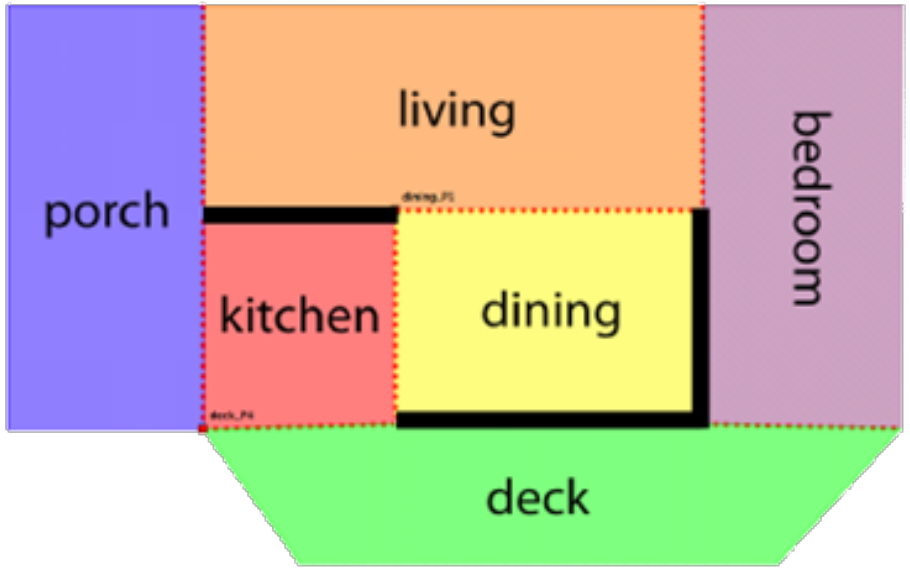
System Propositions

Sensors:

- hazardous_item
- person

Environment Propositions

FIRE-FIGHTING SCENARIO



Regions:

- porch, deck, etc.

Robot actions:

- pick_up
- drop
- radio
- carrying_item

Sensors:

- hazardous_item
- person

Env starts with false
Robot starts with false
Robot starts in **porch**

If you were in **porch** then
do not **hazardous_item**

Do **pick_up** if and only if you are sensing **hazardous_item** and you are not activating **carrying_item**

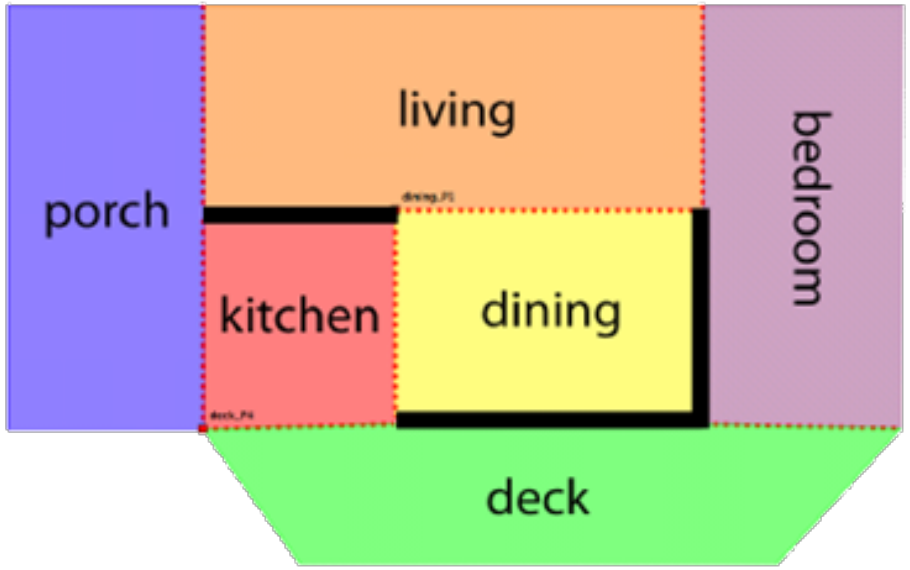
If you did not activate **carrying_item** then always not **porch**

Do **radio** if and only if you are sensing **person**

If you are activating **radio** or you were activating **radio** then stay there

If you are not activating **carrying_item** and you are not activating **radio** then visit **dining**

FIRE-FIGHTING SCENARIO



Regions:

- porch, deck, etc.

Robot actions:

- pick_up
- drop
- radio
- carrying_item

Sensors:

- hazardous_item
- person

Env starts with false
Robot starts with false
Robot starts in **porch**

Initial Conditions

If you were in **porch** then do not **hazardous_item**

Do **pick_up** if and only if you are sensing **hazardous_item** and you are not activating **carrying_item**

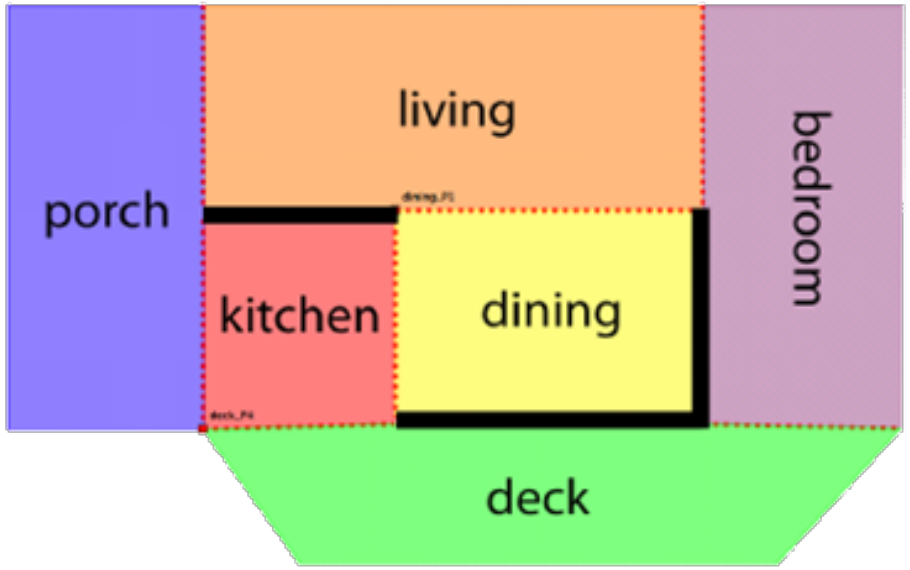
If you did not activate **carrying_item** then always not **porch**

Do **radio** if and only if you are sensing **person**

If you are activating **radio** or you were activating **radio** then stay there

If you are not activating **carrying_item** and you are not activating **radio** then visit **dining**

FIRE-FIGHTING SCENARIO



Regions:

- porch, deck, etc.

Robot actions:

- pick_up
- drop
- radio
- carrying_item

Sensors:

- hazardous_item
- person

Env starts with false
Robot starts with false
Robot starts in **porch**

If you were in **porch** then do not **hazardous_item** } Environment Safety

Do **pick_up** if and only if you are sensing **hazardous_item** and you are not activating **carrying_item**

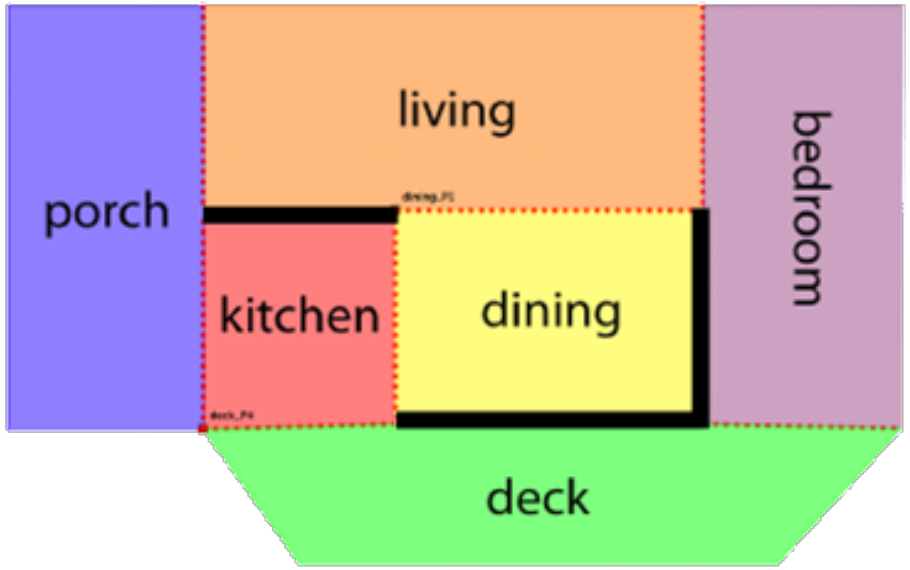
If you did not activate **carrying_item** then always not **porch**

Do **radio** if and only if you are sensing **person**

If you are activating **radio** or you were activating **radio** then stay there

If you are not activating **carrying_item** and you are not activating **radio** then visit **dining**

FIRE-FIGHTING SCENARIO



Env starts with false
Robot starts with false
Robot starts in **porch**

If you were in **porch** then
do not **hazardous_item**

Regions:

- **porch, deck, etc.**

Robot actions:

- **pick_up**
- **drop**
- **radio**
- **carrying_item**

Sensors:

- **hazardous_item**
- **person**

System Safety

Do **pick_up** if and only if you are sensing **hazardous_item** and you are not activating **carrying_item**

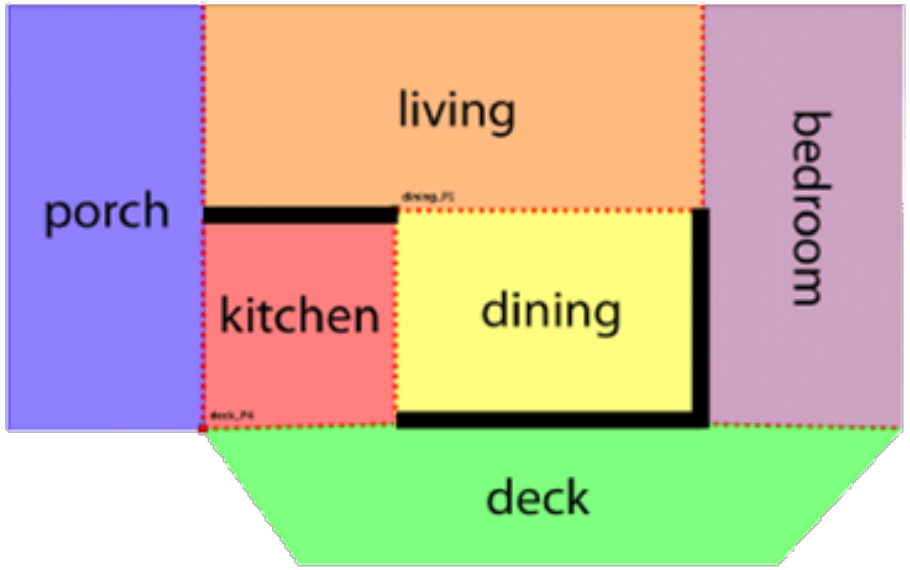
If you did not activate **carrying_item** then always not **porch**

Do **radio** if and only if you are sensing **person**

If you are activating **radio** or you were activating **radio** then stay there

If you are not activating **carrying_item** and you are not activating **radio** then visit **dining**

FIRE-FIGHTING SCENARIO



Regions:

- porch, deck, etc.

Robot actions:

- pick_up
- drop
- radio
- carrying_item

Sensors:

- hazardous_item
- person

Env starts with false
Robot starts with false
Robot starts in **porch**

If you were in **porch** then
do not **hazardous_item**

Do **pick_up** if and only if you are sensing **hazardous_item** and you are not activating **carrying_item**

If you did not activate **carrying_item** then always not **porch**

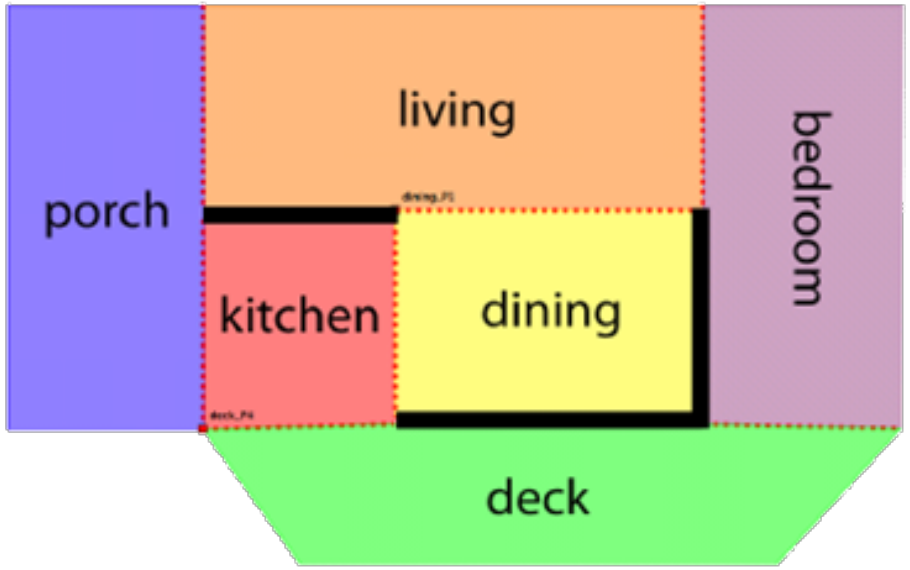
Do **radio** if and only if you are sensing **person**

If you are activating **radio** or you were activating **radio** then stay there

System Liveness

If you are not activating **carrying_item** and you are not activating **radio** then visit **dining**

FIRE-FIGHTING SCENARIO



Regions:

- porch, deck, etc.

Robot actions:

- pick_up
- drop
- radio
- carrying_item

Sensors:

- hazardous_item
- person

Env starts with false
Robot starts with false
Robot starts in **porch**

If you were in **porch** then
do not **hazardous_item**

Do **pick_up** if and only if you are sensing **hazardous_item** and you are not activating **carrying_item**

If you did not activate **carrying_item** then always not **porch**

Do **radio** if and only if you are sensing **person**

If you are activating **radio** or you were activating **radio** then stay there

If you are not activating **carrying_item** and you are not activating **radio** then visit **dining**

Problem: Unsynthesizable Specifications

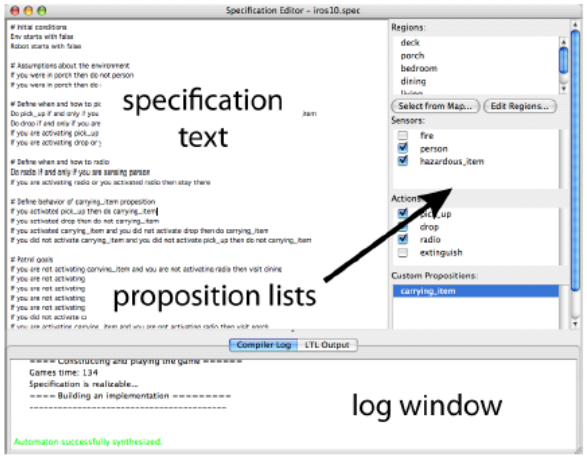
- Unsatisfiable:
  System requirements cannot be fulfilled in **any** environment

- Unrealizable:
  System requirements cannot be fulfilled in **some** admissible environment

Goals:

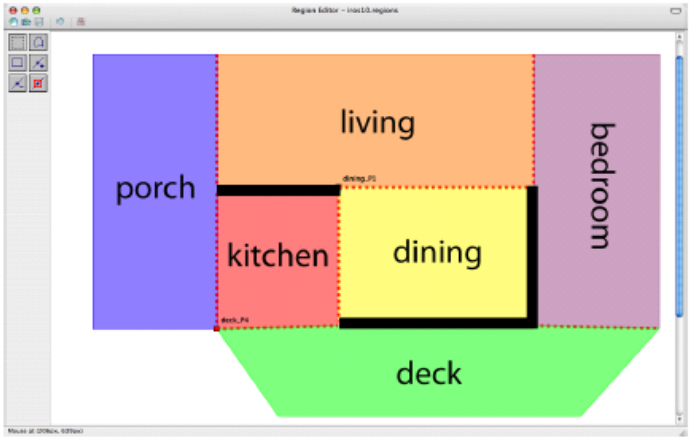
- Identify the cause of failure in the LTL specification
- Map it back to structured English

LTLMoP Overview



(Specification Editor)

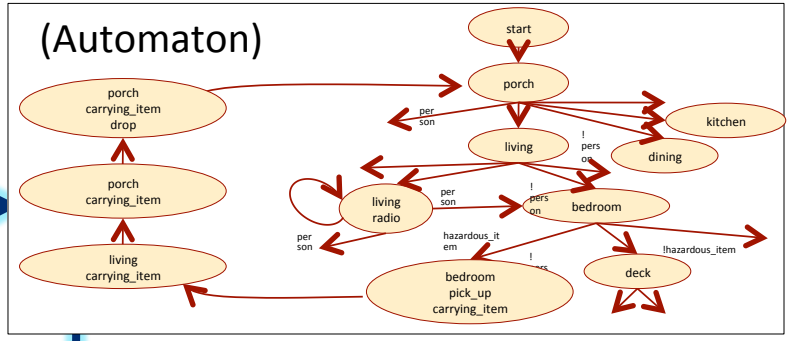
Robot Capability Definitions (Sensors/Actions)



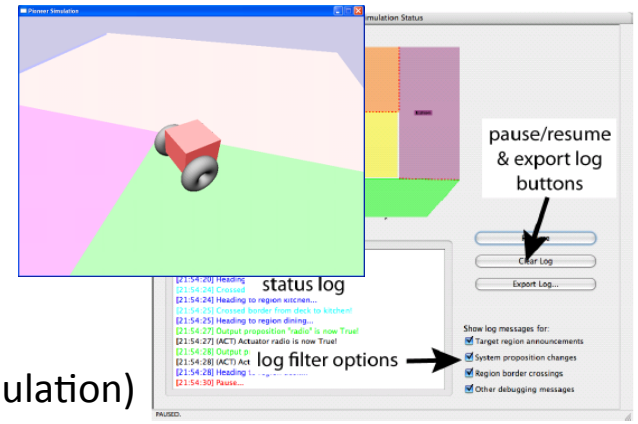
(Region Editor)

Structured English-to-LTL Parser

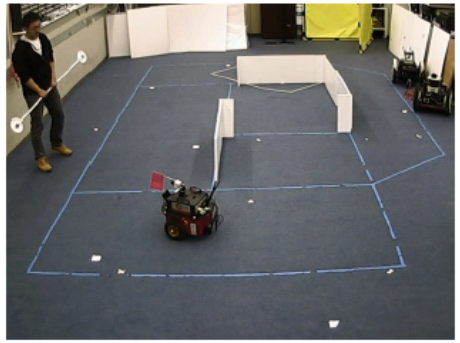
Synthesis



Hybrid Controller

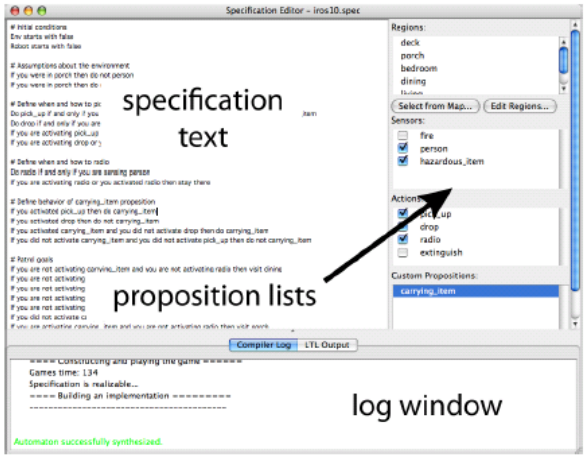


(Simulation)



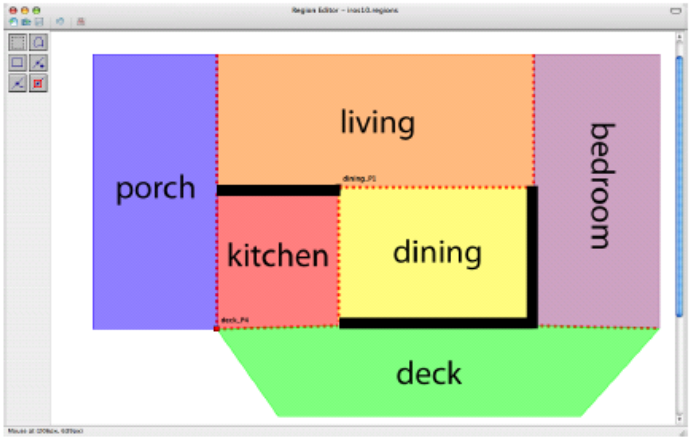
(Physical Robot)

LTLMoP Overview



(Specification Editor)

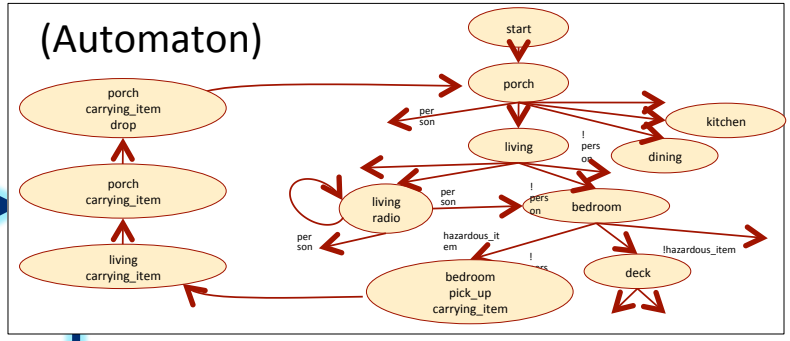
Robot Capability Definitions (Sensors/Actions)



(Region Editor)

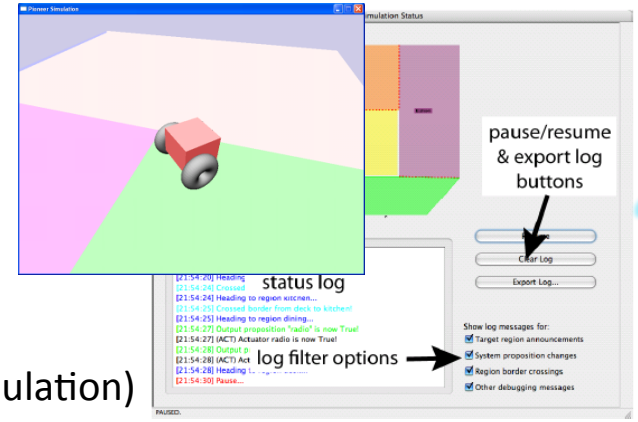
Structured English-to-LTL Parser

Synthesis

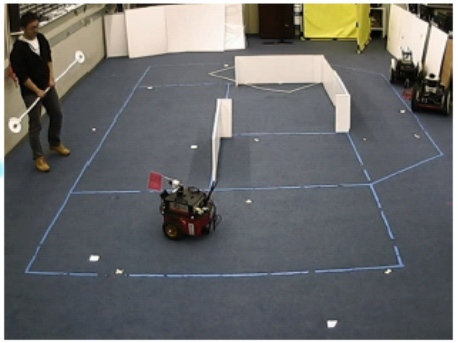


Layer of Analysis for Specifications

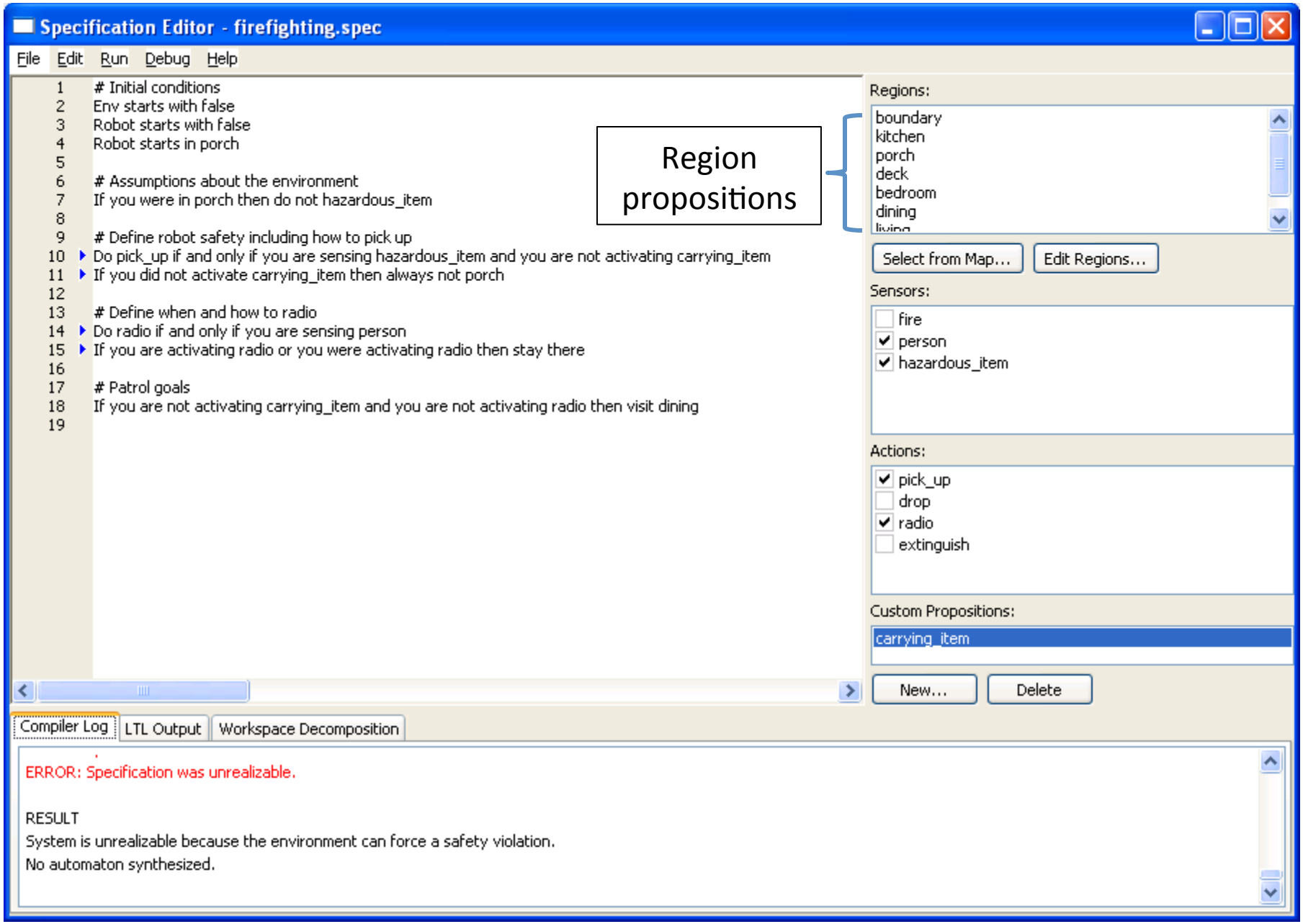
Hybrid Controller

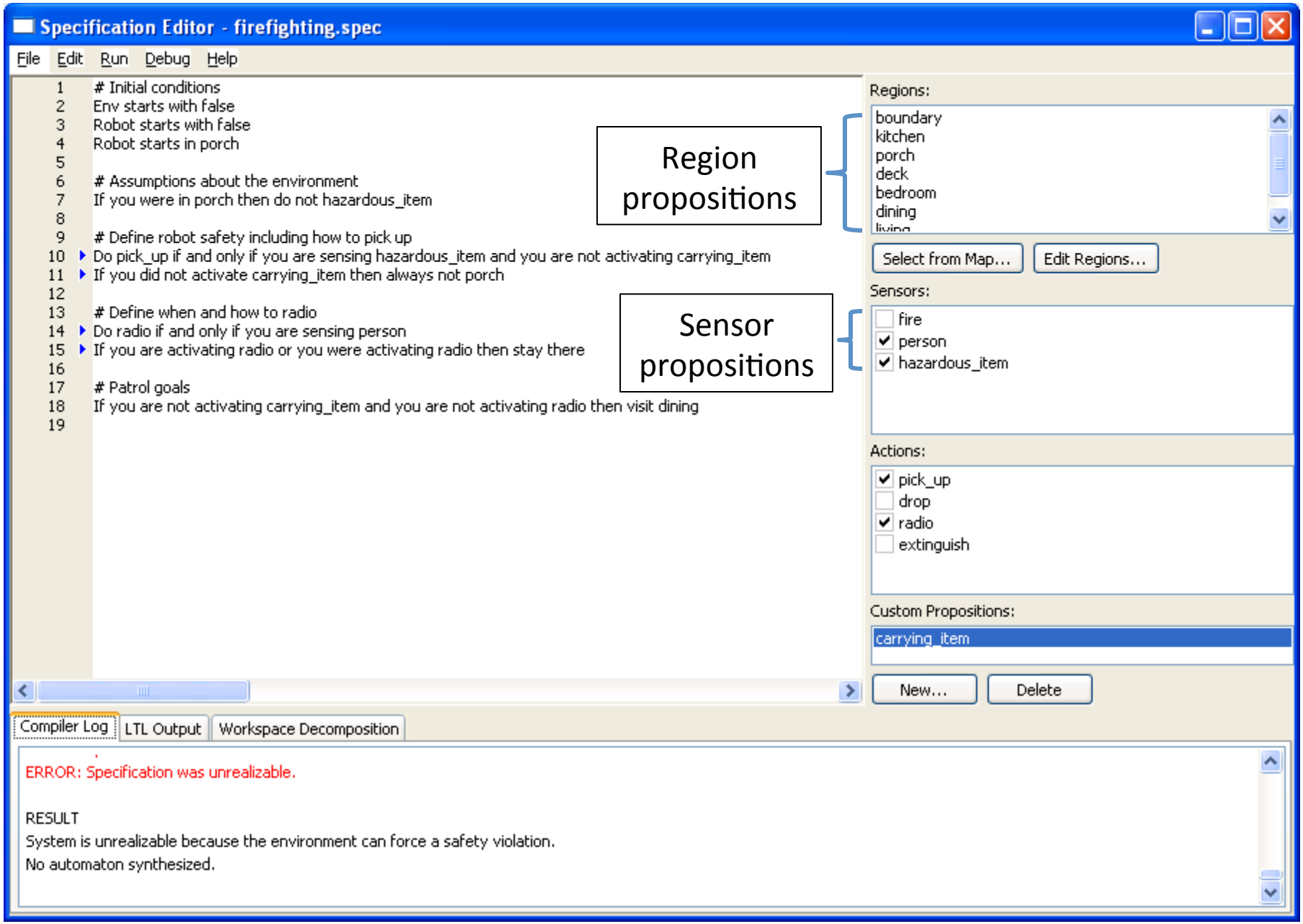


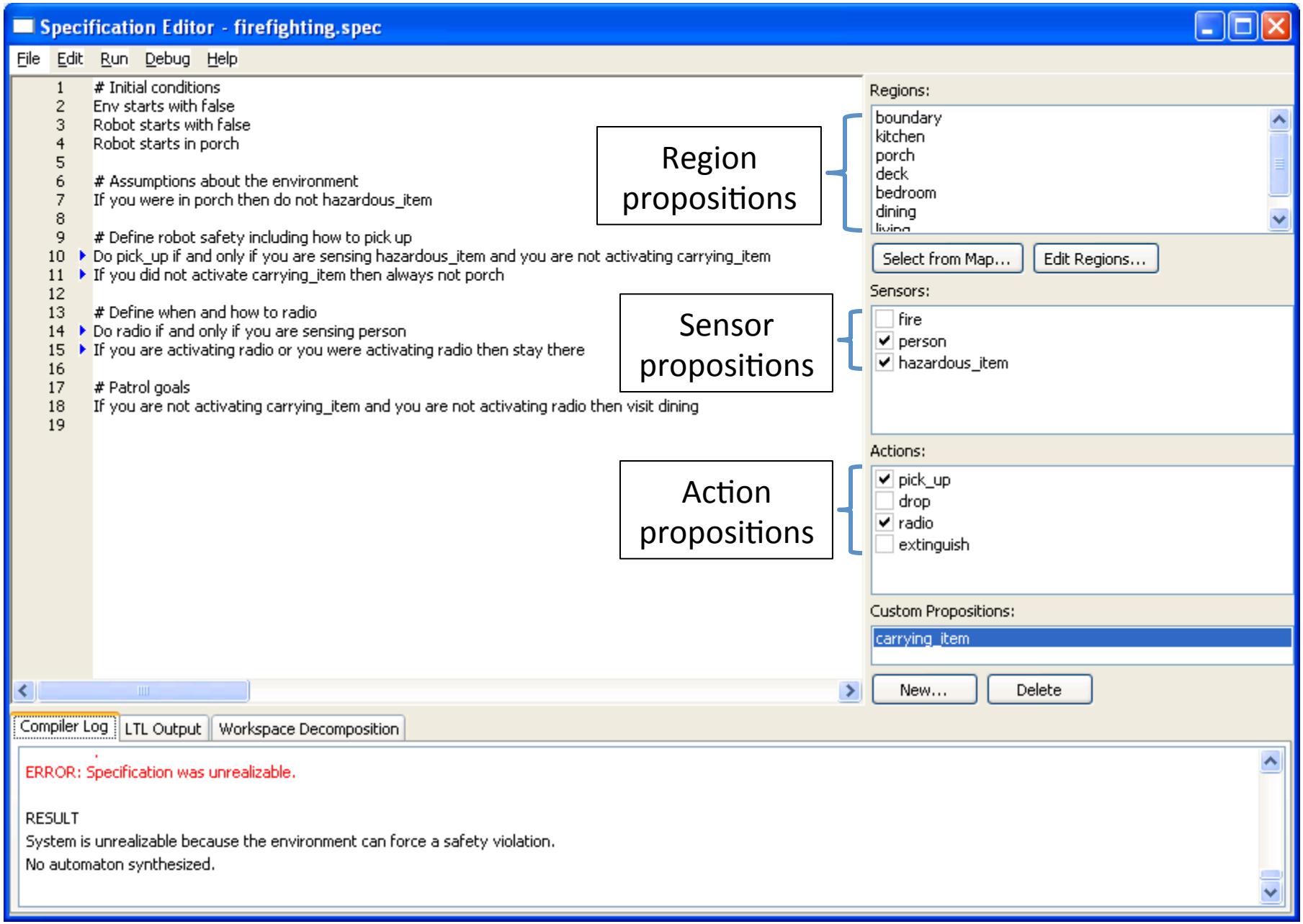
(Simulation)

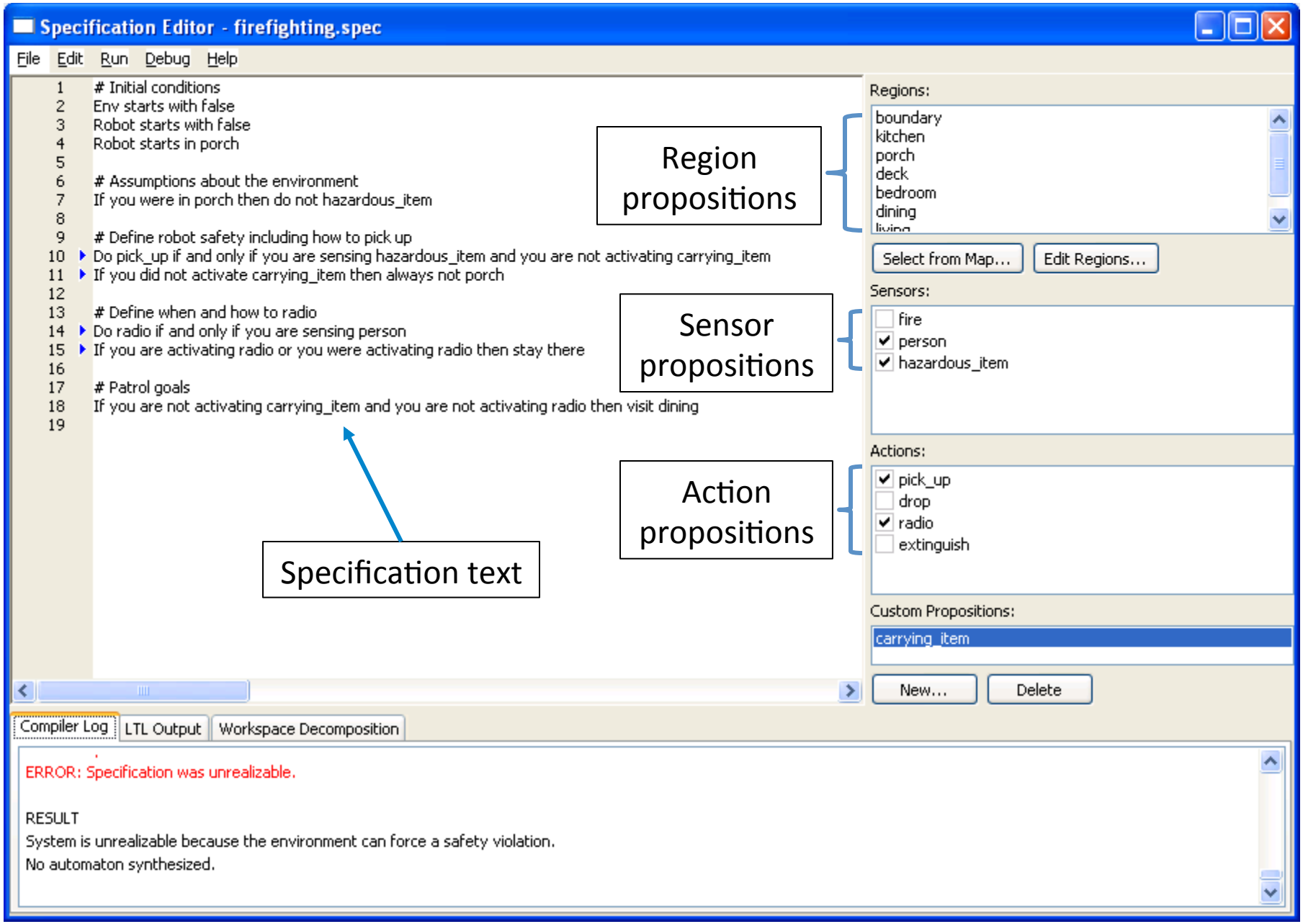


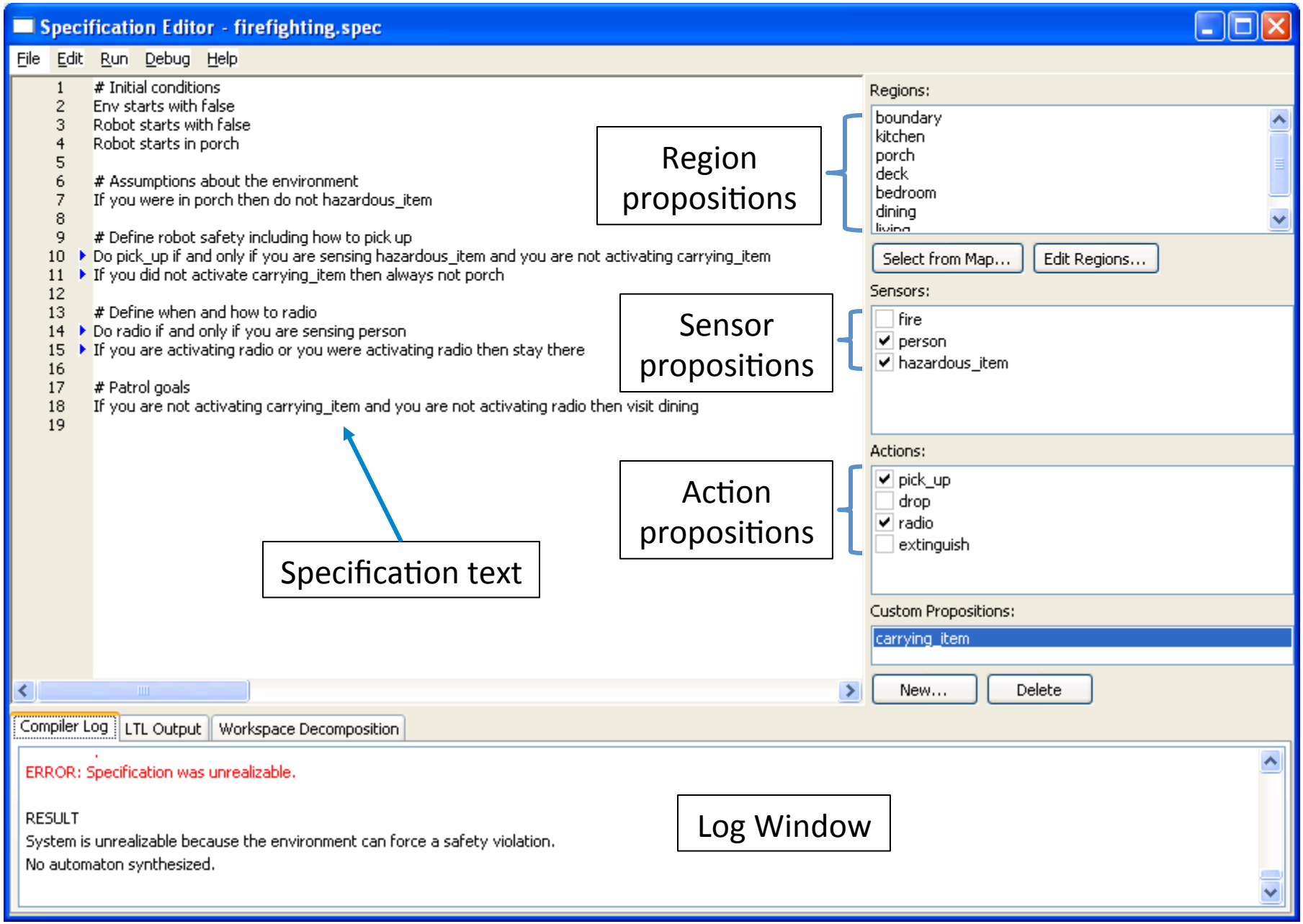
(Physical Robot)

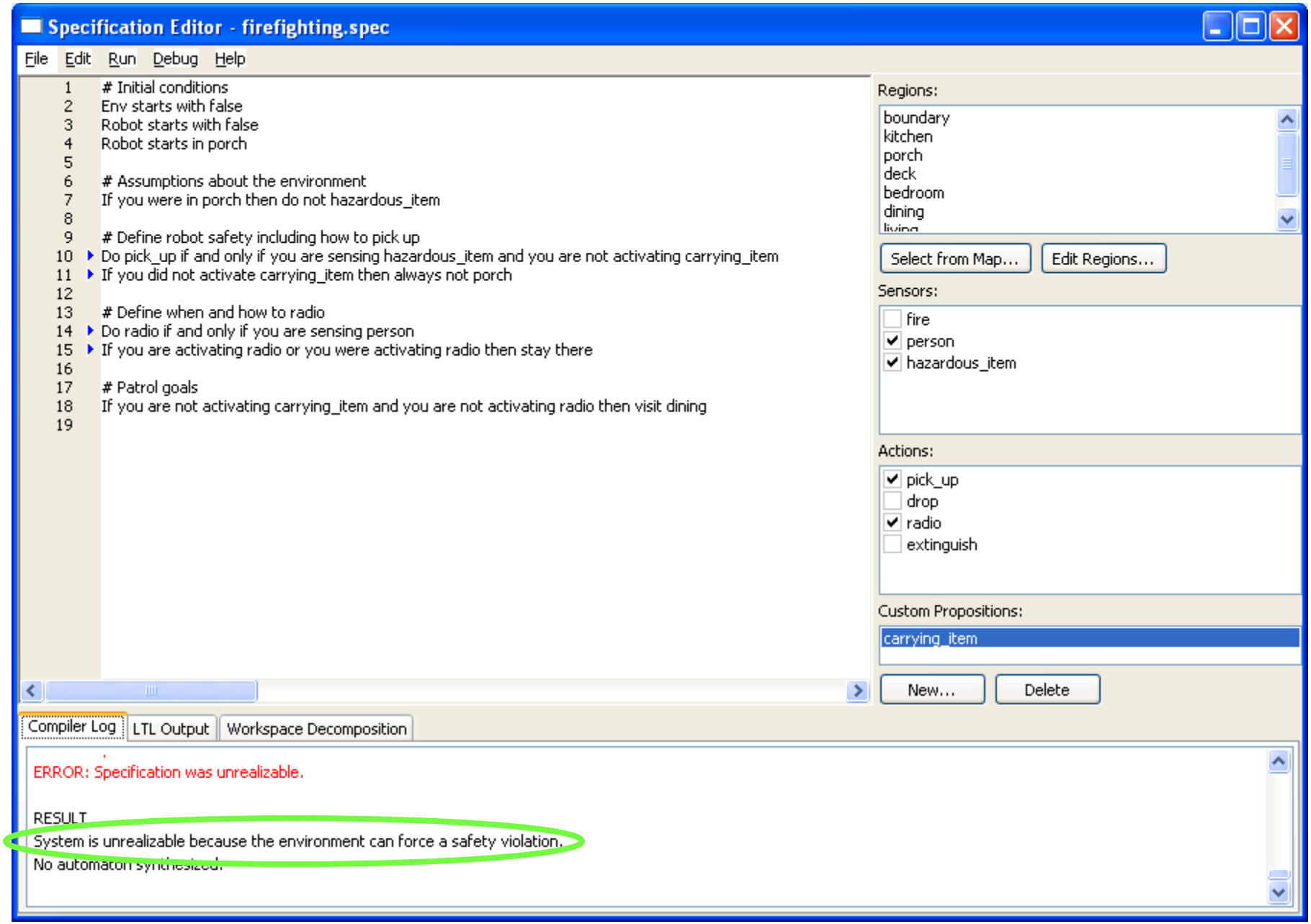

Specification Editor - firefighting.spec
File Edit Run Debug Help
1 # Initial conditions
2 Env starts with false
3 Robot starts with false
4 Robot starts in porch
5
6 # Assumptions about the environment
7 If you were in porch then do not hazardous_item
8
9 # Define robot safety including how to pick up
10 Do pick_up if and only if you are sensing hazardous_item and you are not activating carrying_item
11 If you did not activate carrying_item then always not porch
12
13 # Define when and how to radio
14 Do radio if and only if you are sensing person
15 If you are activating radio or you were activating radio then stay there
16
17 # Patrol goals
18 If you are not activating carrying_item and you are not activating radio then visit dining
19
Region propositions
Regions:
boundary
kitchen
porch
deck
bedroom
dining
Select from Map...
Edit Regions...
Sensors:
fire
person
hazardous_item
Actions:
pick_up
drop
radio
extinguish
Custom Propositions:
carrying_item
New...
Delete
Compiler Log
LTL Output
Workspace Decomposition
ERROR: Specification was unrealizable.
RESULT
System is unrealizable because the environment can force a safety violation.
No automaton synthesized.

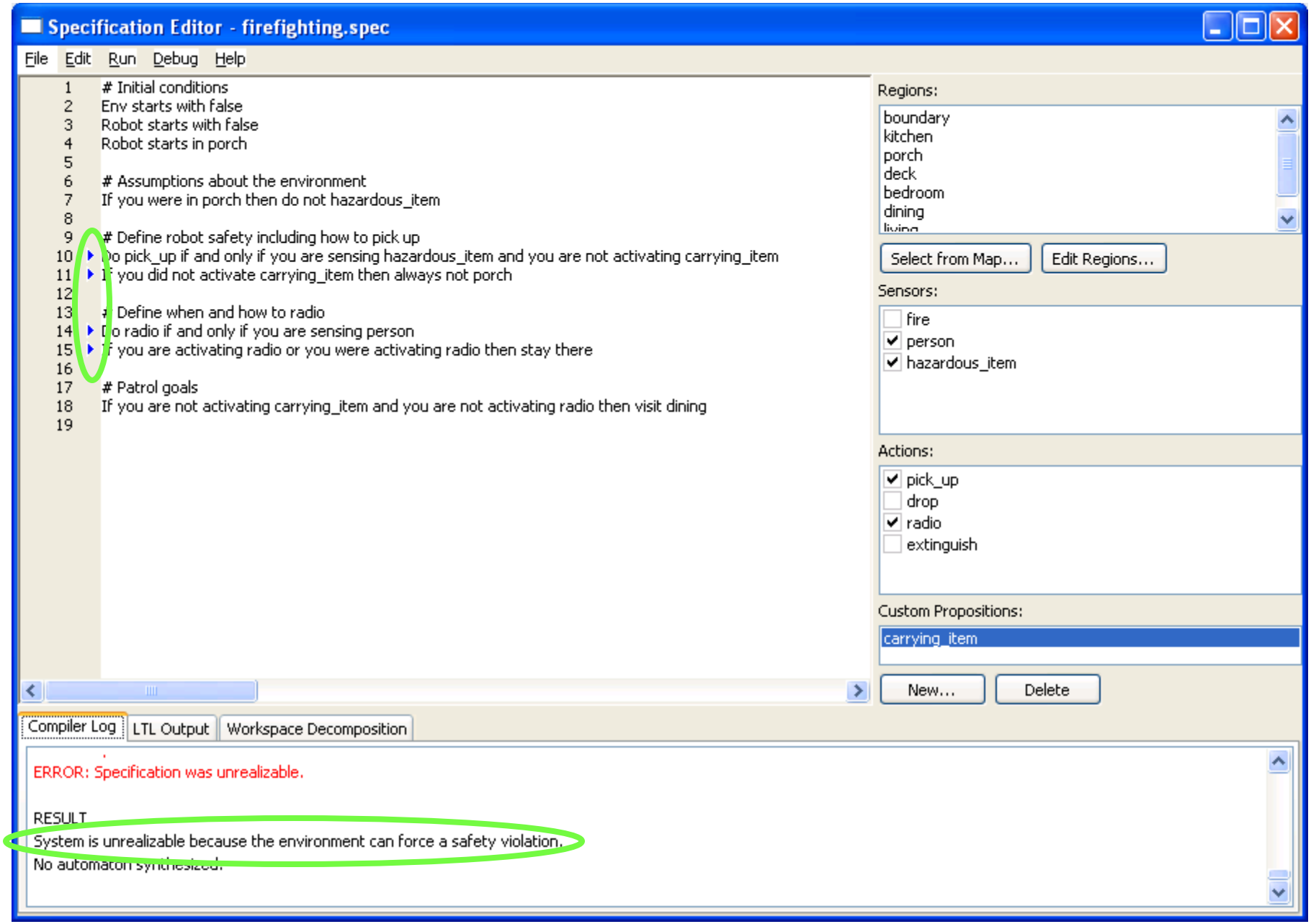

Specification Editor - firefighting.spec
File Edit Run Debug Help
1 # Initial conditions
2 Env starts with false
3 Robot starts with false
4 Robot starts in porch
5
6 # Assumptions about the environment
7 If you were in porch then do not hazardous_item
8
9 # Define robot safety including how to pick up
10 Do pick_up if and only if you are sensing hazardous_item and you are not activating carrying_item
11 If you did not activate carrying_item then always not porch
12
13 # Define when and how to radio
14 Do radio if and only if you are sensing person
15 If you are activating radio or you were activating radio then stay there
16
17 # Patrol goals
18 If you are not activating carrying_item and you are not activating radio then visit dining
19
Region propositions
Regions:
boundary
kitchen
porch
deck
bedroom
dining
Select from Map...
Edit Regions...
Sensor propositions
Sensors:
fire
person
hazardous_item
Actions:
pick_up
drop
radio
extinguish
Custom Propositions:
carrying_item
New...
Delete
Compiler Log
LTL Output
Workspace Decomposition
ERROR: Specification was unrealizable.
RESULT
System is unrealizable because the environment can force a safety violation.
No automaton synthesized.

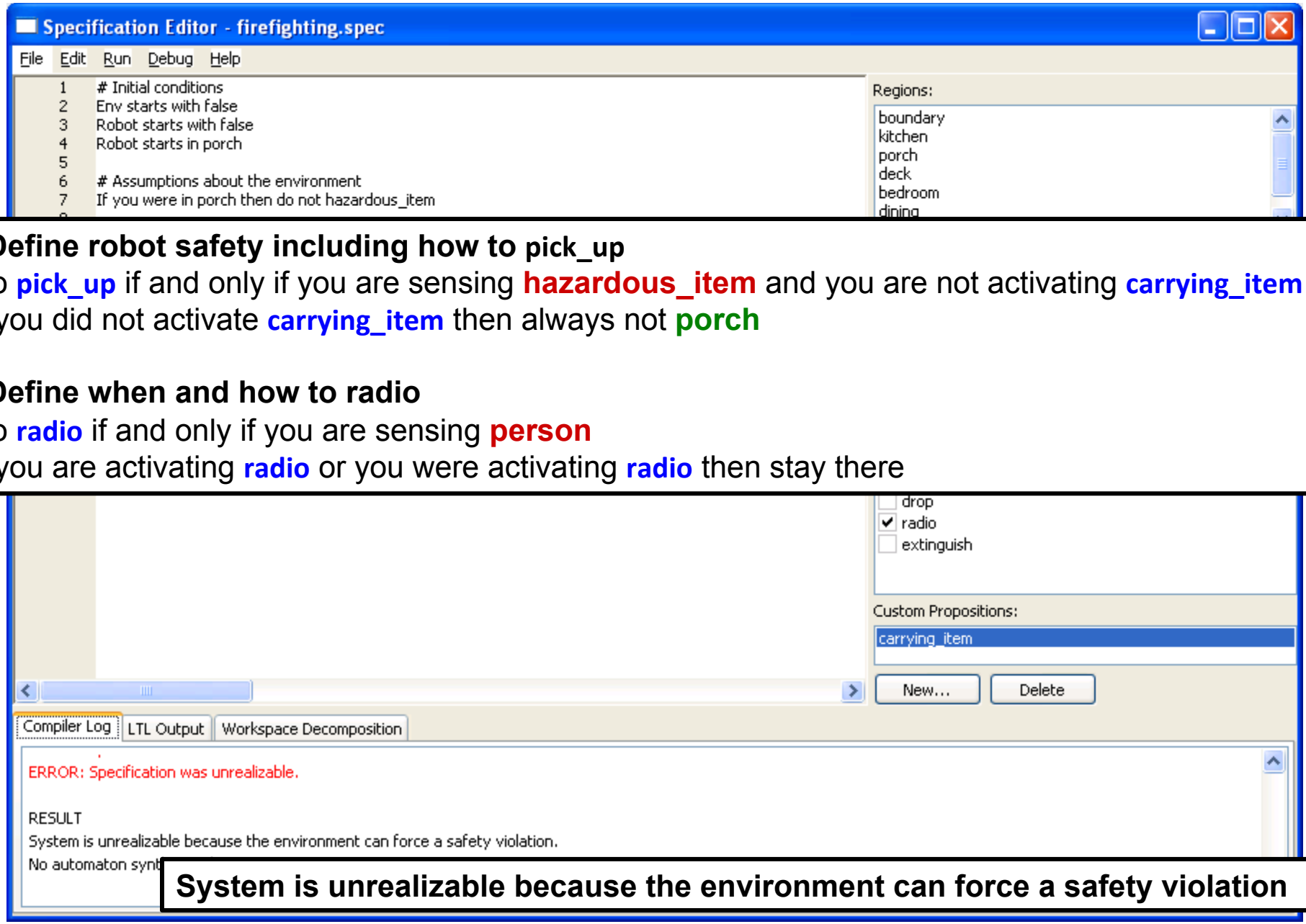

Specification Editor - firefighting.spec
File Edit Run Debug Help
1 # Initial conditions
2 Env starts with false
3 Robot starts with false
4 Robot starts in porch
5
6 # Assumptions about the environment
7 If you were in porch then do not hazardous_item
8
9 # Define robot safety including how to pick up
10 Do pick_up if and only if you are sensing hazardous_item and you are not activating carrying_item
11 If you did not activate carrying_item then always not porch
12
13 # Define when and how to radio
14 Do radio if and only if you are sensing person
15 If you are activating radio or you were activating radio then stay there
16
17 # Patrol goals
18 If you are not activating carrying_item and you are not activating radio then visit dining
19
Region propositions
Sensor propositions
Action propositions
Regions:
boundary
kitchen
porch
deck
bedroom
dining
Select from Map...
Edit Regions...
Sensors:
fire
person
hazardous_item
Actions:
pick_up
drop
radio
extinguish
Custom Propositions:
carrying_item
New...
Delete
Compiler Log
LTL Output
Workspace Decomposition
ERROR: Specification was unrealizable.
RESULT
System is unrealizable because the environment can force a safety violation.
No automaton synthesized.

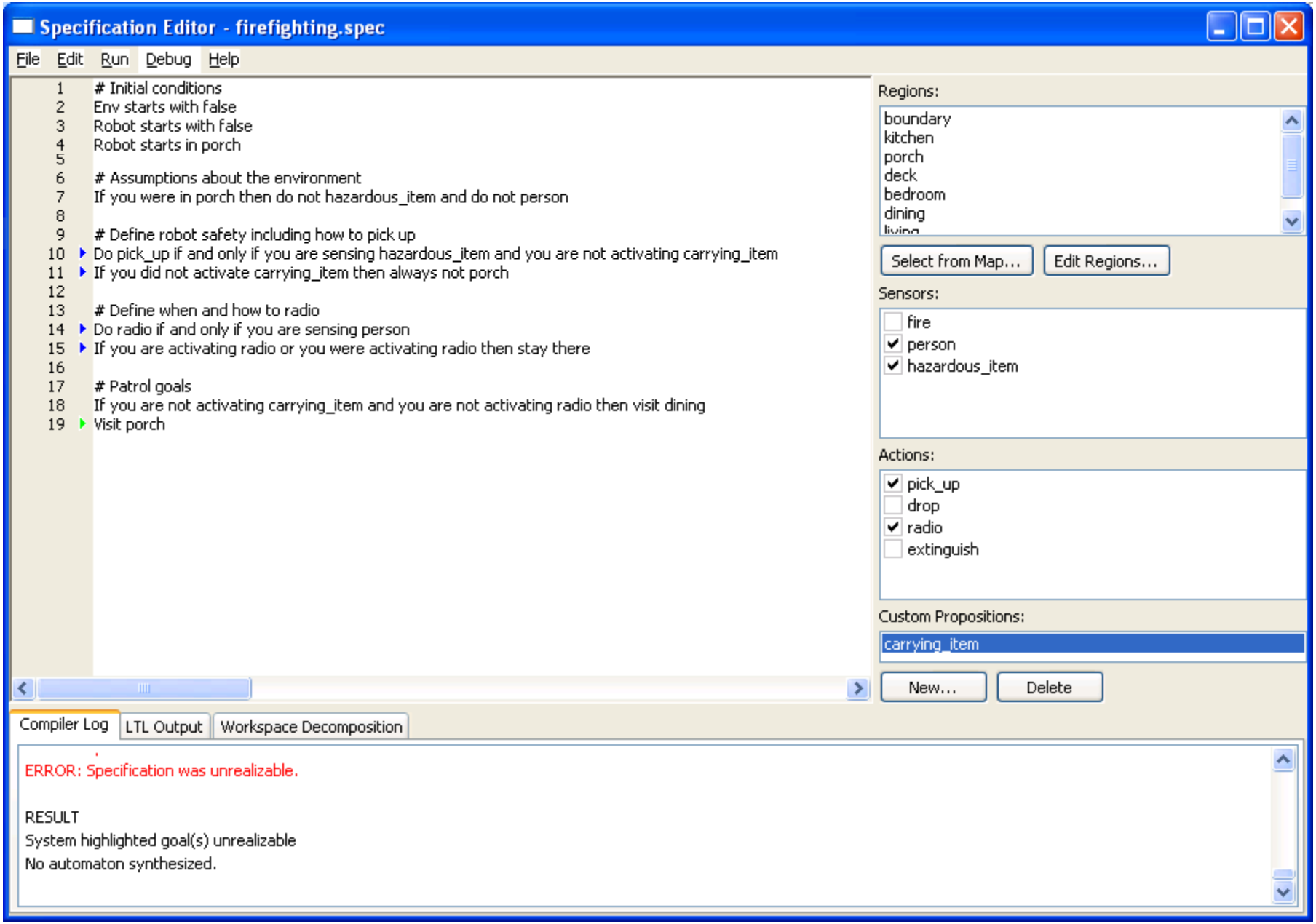

Specification Editor - firefighting.spec
File Edit Run Debug Help
1 # Initial conditions
2 Env starts with false
3 Robot starts with false
4 Robot starts in porch
5
6 # Assumptions about the environment
7 If you were in porch then do not hazardous_item
8
9 # Define robot safety including how to pick up
10 Do pick_up if and only if you are sensing hazardous_item and you are not activating carrying_item
11 If you did not activate carrying_item then always not porch
12
13 # Define when and how to radio
14 Do radio if and only if you are sensing person
15 If you are activating radio or you were activating radio then stay there
16
17 # Patrol goals
18 If you are not activating carrying_item and you are not activating radio then visit dining
19
Region propositions
Regions:
boundary
kitchen
porch
deck
bedroom
dining
Select from Map...
Edit Regions...
Sensor propositions
Sensors:
fire
person
hazardous_item
Action propositions
Actions:
pick_up
drop
radio
extinguish
Specification text
Custom Propositions:
carrying_item
New...
Delete
Compiler Log
LTL Output
Workspace Decomposition
ERROR: Specification was unrealizable.
RESULT
System is unrealizable because the environment can force a safety violation.
No automaton synthesized.

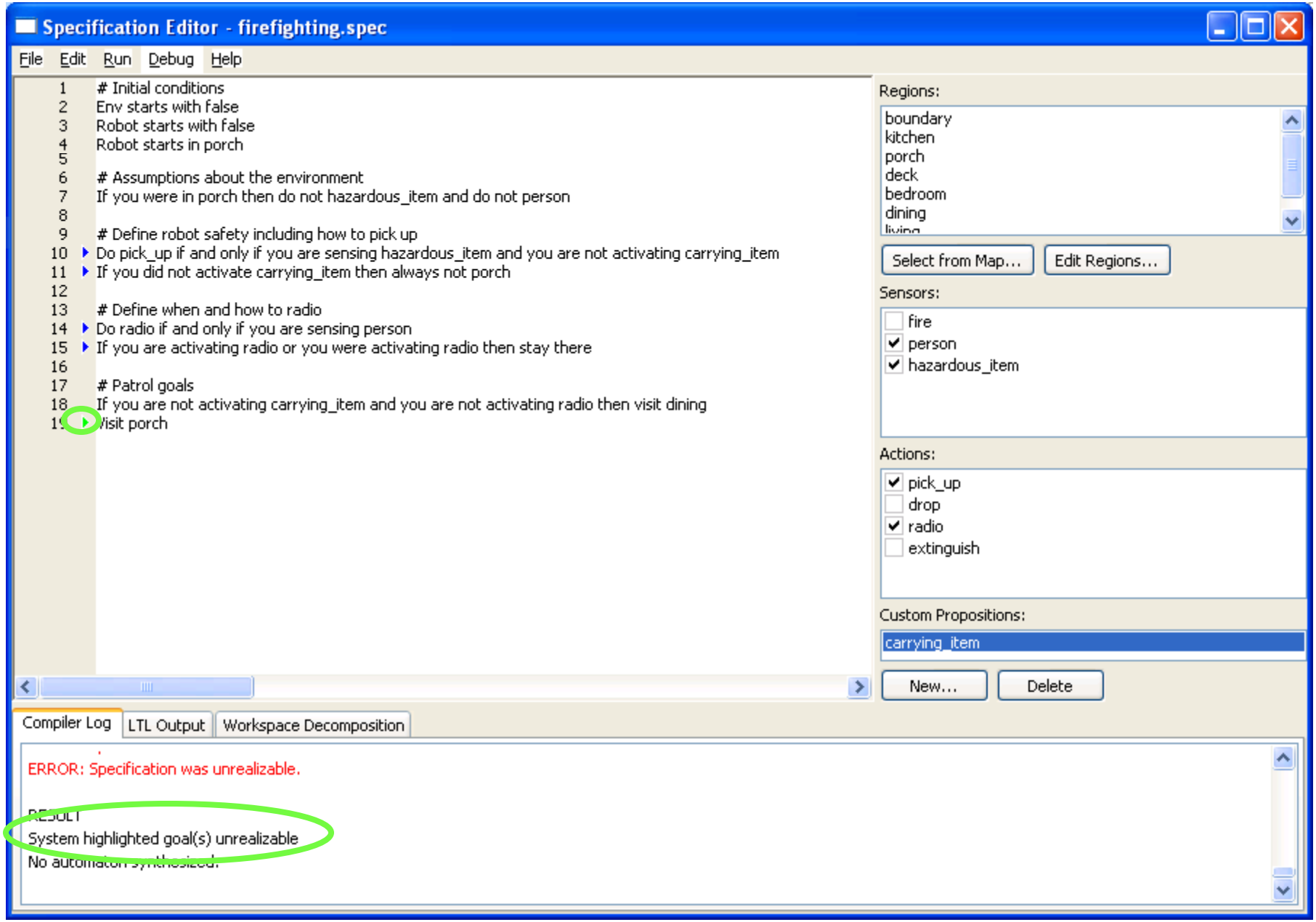

Specification Editor - firefighting.spec
File Edit Run Debug Help
1 # Initial conditions
2 Env starts with false
3 Robot starts with false
4 Robot starts in porch
5
6 # Assumptions about the environment
7 If you were in porch then do not hazardous_item
8
9 # Define robot safety including how to pick up
10 Do pick_up if and only if you are sensing hazardous_item and you are not activating carrying_item
11 If you did not activate carrying_item then always not porch
12
13 # Define when and how to radio
14 Do radio if and only if you are sensing person
15 If you are activating radio or you were activating radio then stay there
16
17 # Patrol goals
18 If you are not activating carrying_item and you are not activating radio then visit dining
19
Region propositions
Regions:
boundary
kitchen
porch
deck
bedroom
dining
Select from Map...
Edit Regions...
Sensor propositions
Sensors:
fire
person
hazardous_item
Action propositions
Actions:
pick_up
drop
radio
extinguish
Specification text
Custom Propositions:
carrying_item
New...
Delete
Compiler Log
LTL Output
Workspace Decomposition
ERROR: Specification was unrealizable.
RESULT
System is unrealizable because the environment can force a safety violation.
No automaton synthesized.
Log Window

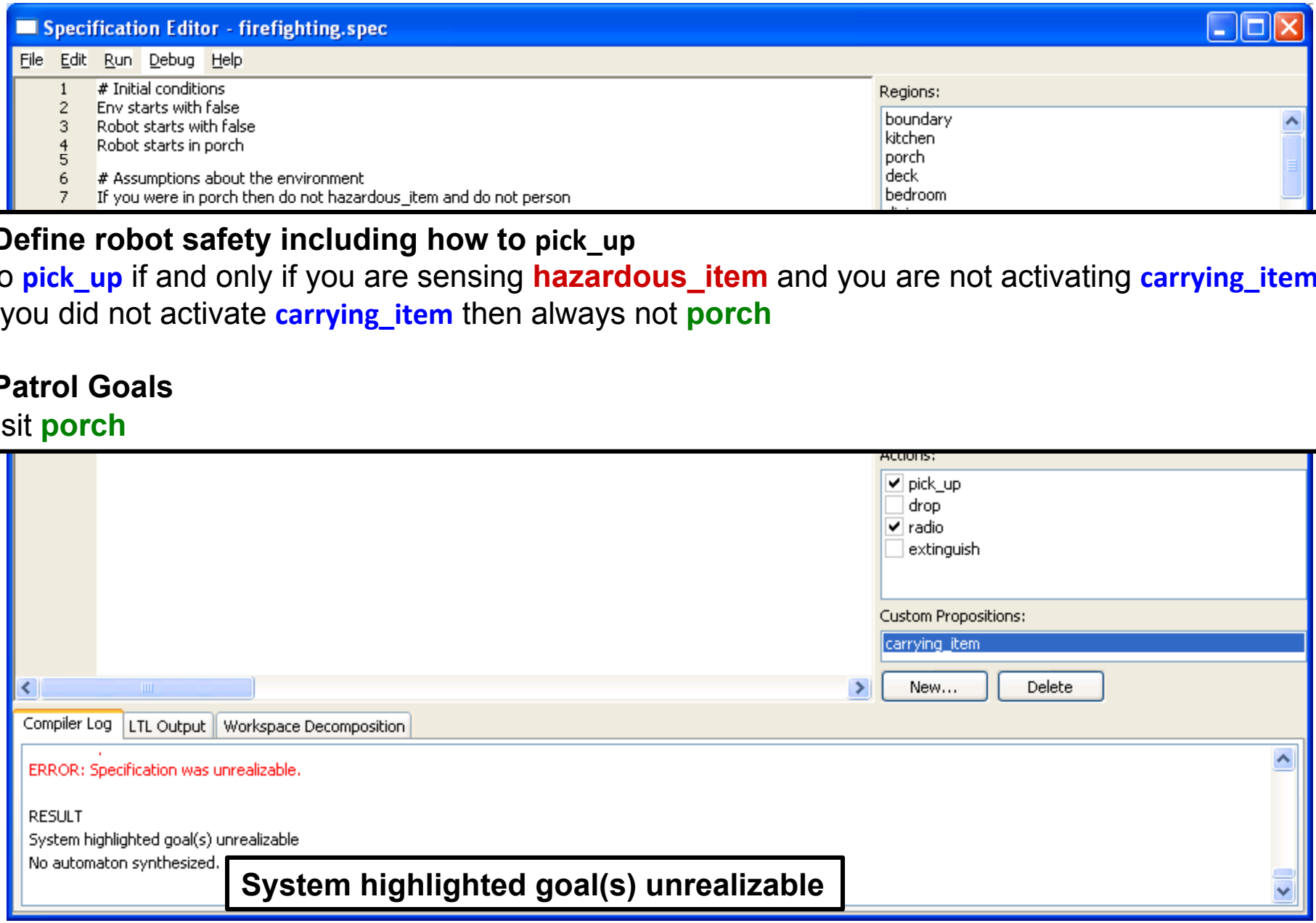

Specification Editor - firefighting.spec
File Edit Run Debug Help
1 # Initial conditions
2 Env starts with false
3 Robot starts with false
4 Robot starts in porch
5
6 # Assumptions about the environment
7 If you were in porch then do not hazardous_item
8
9 # Define robot safety including how to pick up
10 Do pick_up if and only if you are sensing hazardous_item and you are not activating carrying_item
11 If you did not activate carrying_item then always not porch
12
13 # Define when and how to radio
14 Do radio if and only if you are sensing person
15 If you are activating radio or you were activating radio then stay there
16
17 # Patrol goals
18 If you are not activating carrying_item and you are not activating radio then visit dining
19
Regions:
boundary
kitchen
porch
deck
bedroom
dining
Select from Map...
Edit Regions...
Sensors:
fire
person
hazardous_item
Actions:
pick_up
drop
radio
extinguish
Custom Propositions:
carrying_item
New...
Delete
Compiler Log
LTL Output
Workspace Decomposition
ERROR: Specification was unrealizable.
RESULT
System is unrealizable because the environment can force a safety violation.
No automaton synthesized.


Specification Editor - firefighting.spec
File Edit Run Debug Help
1 # Initial conditions
2 Env starts with false
3 Robot starts with false
4 Robot starts in porch
5
6 # Assumptions about the environment
7 If you were in porch then do not hazardous_item
8
9 # Define robot safety including how to pick up
10 Do pick_up if and only if you are sensing hazardous_item and you are not activating carrying_item
11 If you did not activate carrying_item then always not porch
12
13 # Define when and how to radio
14 Do radio if and only if you are sensing person
15 If you are activating radio or you were activating radio then stay there
16
17 # Patrol goals
18 If you are not activating carrying_item and you are not activating radio then visit dining
19
Regions:
boundary
kitchen
porch
deck
bedroom
dining
Select from Map...
Edit Regions...
Sensors:
fire
person
hazardous_item
Actions:
pick_up
drop
radio
extinguish
Custom Propositions:
carrying_item
New...
Delete
Compiler Log
LTL Output
Workspace Decomposition
ERROR: Specification was unrealizable.
RESULT
System is unrealizable because the environment can force a safety violation.
No automaton synthesized.


Specification Editor - firefighting.spec
File Edit Run Debug Help
1 # Initial conditions
2 Env starts with false
3 Robot starts with false
4 Robot starts in porch
5
6 # Assumptions about the environment
7 If you were in porch then do not hazardous_item
Regions:
boundary
kitchen
porch
deck
bedroom
dining
#Define robot safety including how to pick_up
Do pick_up if and only if you are sensing hazardous_item and you are not activating carrying_item
If you did not activate carrying_item then always not porch
#Define when and how to radio
Do radio if and only if you are sensing person
If you are activating radio or you were activating radio then stay there
drop
radio
extinguish
Custom Propositions:
carrying_item
New...
Delete
Compiler Log
LTL Output
Workspace Decomposition
ERROR: Specification was unrealizable.
RESULT
System is unrealizable because the environment can force a safety violation.
No automaton synt
System is unrealizable because the environment can force a safety violation

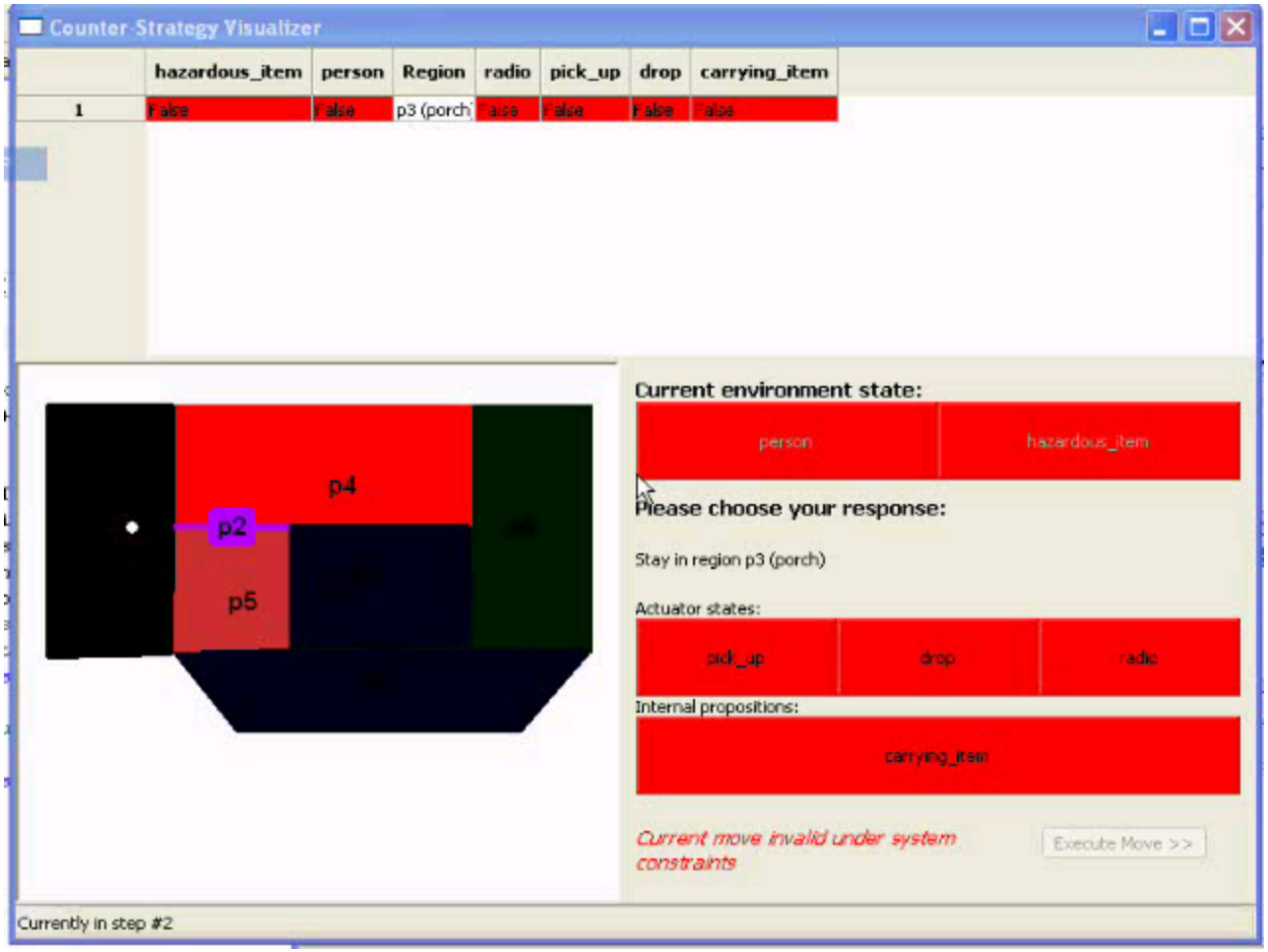

Specification Editor - firefighting.spec
File Edit Run Debug Help
1 # Initial conditions
2 Env starts with false
3 Robot starts with false
4 Robot starts in porch
5
6 # Assumptions about the environment
7 If you were in porch then do not hazardous_item and do not person
8
9 # Define robot safety including how to pick up
10 Do pick_up if and only if you are sensing hazardous_item and you are not activating carrying_item
11 If you did not activate carrying_item then always not porch
12
13 # Define when and how to radio
14 Do radio if and only if you are sensing person
15 If you are activating radio or you were activating radio then stay there
16
17 # Patrol goals
18 If you are not activating carrying_item and you are not activating radio then visit dining
19 Visit porch
Regions:
boundary
kitchen
porch
deck
bedroom
dining
Select from Map...
Edit Regions...
Sensors:
fire
person
hazardous_item
Actions:
pick_up
drop
radio
extinguish
Custom Propositions:
carrying_item
New...
Delete
Compiler Log
LTL Output
Workspace Decomposition
ERROR: Specification was unrealizable.
RESULT
System highlighted goal(s) unrealizable
No automaton synthesized.


Specification Editor - firefighting.spec
File Edit Run Debug Help
1 # Initial conditions
2 Env starts with false
3 Robot starts with false
4 Robot starts in porch
5
6 # Assumptions about the environment
7 If you were in porch then do not hazardous_item and do not person
8
9 # Define robot safety including how to pick up
10 Do pick_up if and only if you are sensing hazardous_item and you are not activating carrying_item
11 If you did not activate carrying_item then always not porch
12
13 # Define when and how to radio
14 Do radio if and only if you are sensing person
15 If you are activating radio or you were activating radio then stay there
16
17 # Patrol goals
18 If you are not activating carrying_item and you are not activating radio then visit dining
19 Visit porch
Regions:
boundary
kitchen
porch
deck
bedroom
dining
Select from Map...
Edit Regions...
Sensors:
fire
person
hazardous_item
Actions:
pick_up
drop
radio
extinguish
Custom Propositions:
carrying_item
New...
Delete
Compiler Log
LTL Output
Workspace Decomposition
ERROR: Specification was unrealizable.
RESULT
System highlighted goal(s) unrealizable
No automaton synthesized.


Specification Editor - firefighting.spec
File Edit Run Debug Help
1 # Initial conditions
2 Env starts with false
3 Robot starts with false
4 Robot starts in porch
5
6 # Assumptions about the environment
7 If you were in porch then do not hazardous_item and do not person
Regions:
boundary
kitchen
porch
deck
bedroom
#Define robot safety including how to pick_up
Do pick_up if and only if you are sensing hazardous_item and you are not activating carrying_item
If you did not activate carrying_item then always not porch
#Patrol Goals
Visit porch
Actions:
pick_up
drop
radio
extinguish
Custom Propositions:
carrying_item
New...
Delete
Compiler Log
LTL Output
Workspace Decomposition
ERROR: Specification was unrealizable.
RESULT
System highlighted goal(s) unrealizable
No automaton synthesized.
System highlighted goal(s) unrealizable

Other Tools for Analysis

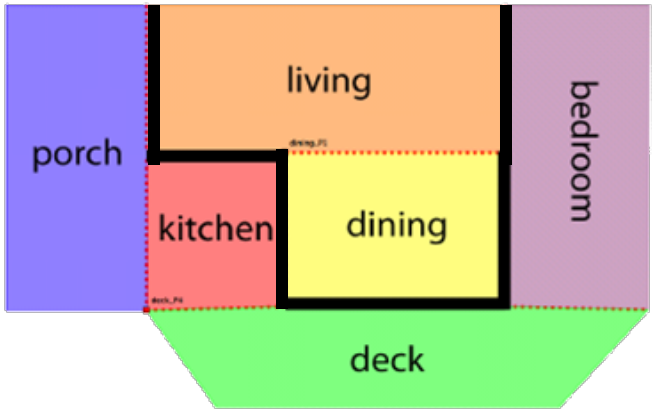
- Interactive game to help explain unrealizability
  - Let the user interact with an environment constructed to thwart the system.
  - Similar to RATSY[1], augmented with domain-specific interface.



[1] R.Bloem, A. Cimatti, K. Greimel, G. Hofferek, R. Könighofer, M. Roveri, V. Schuppan, R. Seeber: ***RATSY - A New Requirements Analysis Tool with Synthesis***. CAV 2010: 425-429

CURRENT AND FUTURE WORK

- Identifying domain-specific special cases of unsatisfiability
  - e.g. disconnected topology



- Further narrowing down the cause of unsynthesizability
  - Unsatisfiable/unrealizable cores

- Suggesting changes to the specification that would allow synthesis
  - Add environment assumptions
  - Weaken system requirements

[1] R.Bloem, A. Cimatti, K. Greimel, G. Hofferek, R. Könighofer, M. Roveri, V. Schuppan, R. Seeber: ***RATSY - A New Requirements Analysis Tool with Synthesis***. CAV 2010: 425-429

?

REMINDER: Tool Demo Session
3:00-6:00pm

LTLMoP: https://github.com/LTLMoP
(GPL)