

Project of Formal Methods for Concurrent and Real-time Systems
course (PoliMi/UIC 545)

Model and Report

Ludovico Crotta,

Lorenzo Semeria,

Gabriele Vanoni

Contents

1	Introduction	3
1.1	The environment	3
1.2	The robot	3
1.3	The human operator	3
1.4	Standard robot activities	4
2	List of predicates	4
2.1	Whose state is known by the robot by mean of sensors	4
2.2	Controlled by the robot	5
2.2.1	Cart	5
2.2.2	Arm	5
3	Specification of the system	5
3.1	Specification of the model	5
3.1.1	Environment layout	6
3.1.2	Specification of the cart	6
3.1.3	Specification of the local bin	7
3.1.4	Specification of the arm	8
3.1.5	Specification of the operator	11
3.2	Specification of the behaviour	12
3.2.1	Cart movement	12
3.2.2	Robot Arm working	13
4	Specification of the safety properties	13
5	Conclusion	14

1 Introduction

The aim of this report is to introduce a possible model for the Human-Robot Collaborative (HRC) application shown in class, in terms of modeling both the world and the constraints needed to ensure the safety of the human operator. We will first describe the environment that the robot and the human will work in, along with the assumptions made to simplify the model while keeping it detailed enough to give a meaningful representation of reality.

We then explain the usual actions and related hazards of the robot's operations and their possible interactions with the human operator.

In the later sections we introduce the predicates and the formulae needed for the model introduced.

1.1 The environment

The environment is assumed to be a room, as shown in the section 3.1.1. We decided to position the pallet, where the operator and the robot will work together, on the right side of the room. On the left we put the bin, where the robot will go alone to refill his own "local" bin. The room is divided in squares, according to the natural X and Y axis, allowing us to simply identify the cells via their coordinates. We decided that the path between the bin and the pallet could be a straight line without introducing an oversimplification of the model. This is motivated by the fact that the room does not contain any obstacle and is big enough to for the walls not to interfere with standard robot movement. Therefore – should the path not be a straight line in the first place – a trivial change of basis would make the line straight. The new basis would only be a rotation of the starting one.

1.2 The robot

We modeled the robot as a two-square object, which represents the whole cart. The robotic arm is modeled in more detail and we track the position of the elbow, the arm and the end effector. The cart can move left- and rightward only, since the bin to pallet path is straight and there are no fixed obstacles. Should the operator be in the way, the robot will simply stop moving, as we shall see. The arm is modeled to be retracted (on the same square of the cart) during movement, while its position during activity is modeled accordingly.

We assumed that the robot has sensors to detect his own position in the room as well as the operator's. More specifically, the robot can detect the position of the human operator in terms of distance and direction. This is simply represented by knowing the position of the operator on the grid modeling the room. The robot has also sensors that detect proximity of the human to the robotic arm to ensure the safety conditions. Furthermore, the robot has knowledge of the layout of the room (no physical obstacle is present, the position of the bin and the pallet).

1.3 The human operator

The behaviour of the human operator is assumed not to be constrained by any "common sense" as he might try to hurt himself. This is to ensure that no harm can be done to a human operator even in the event of a human error. The position of the human is modeled as the position of his body and of the arms, all of which occupy a single square of the room. The arms can be stretched out or resting, in which case they occupy the same position of the body.

1.4 Standard robot activities

Expected interactions between the robot and the other parts of the world (the bin and the operator, as we assumed that walls are far enough for not being an issue) have been modeled with formulae describing both the interaction itself and the safety properties, as detailed in further sections. The robot is supposed to move in a straight line, back and forth between the pallet and the bin. The speed is constrained to be “slow” near the pallet to minimize the risk of accidental contact with the operator. The movement is modeled as a straight line, as previously mentioned, since this does not introduce any oversimplification. The regular behaviour is described as the robot moving between the pallet and the bin, while in case of an hazard (the operator being in the way), the robot will stop moving until the hazard is resolved (the operator is far enough to avoid any contact).

When the robot is still, the robotic arm can stretch out to do the required actions (work with the operator when being at the pallet). The arm must be in a resting position during the refill and must not move, while it does move when the operator works on a part. The possible positions at which the operator works on a part are fixed.

The normal functioning of the arm, when refilling, is to pick up the parts and fill the local bin. When the robot is at the pallet, the robotic arm must pick up the part, reach the appropriate final position – which in turn depends on the operator’s current position – and wait for the operator to complete his operations. During any of these operations, it is possible that the operator interferes with the robotic arm’s movement in any way (for example, his arm may be in the way of the robotic arm and would therefore be hit). In this case, considered hazardous, the robotic arm’s movement is stopped until the safety conditions are fulfilled again.

2 List of predicates

We now introduce the predicates needed to properly model the room, the robot, the human and all the events related to the work done by the robot. We split the predicates based on how the robot can know their state: from sensors or directly, since it can control them.

2.1 Whose state is known by the robot by mean of sensors

We shall first introduce the predicates whose state is known by some sensor. This includes the position of the operator as well as the state of the bins (both the “local” and the “remote” ones).

Predicates referring to the operator:

- $\text{isLeftArmAt}(x, y)$
- $\text{isRightArmAt}(x, y)$
- isOpOnTheLeft
- isOpOnTheRight
- $\text{isOperatorAt}(x, y)$

Predicates referring to the robot or the bins:

- isLocalBinEmpty
- isLocalBinFull

- $\text{isJointAt}(x, y)$
- $\text{isEndEffectorAt}(x, y)$
- $\text{isCartAt}(x, y)$
- isRobotResting
- isPieceLoaded

In all above predicates, as well as those that we will introduce later, we indicate with x and y the coordinate of the square describing the room as already explained.

2.2 Controlled by the robot

We now introduce the predicates modeling the robot. We modeled both the movement of the cart – which can move at two different speeds or be still – and the movement of the joint.

2.2.1 Cart

- isCartMoving
- isCartStill
- isCartMovingFast
- isCartMovingSlow
- isCartMovingLeft
- isCartMovingRight

2.2.2 Arm




- isJointMoving
- $\text{isEndEffectorMoving}$
- isRobotPicking
- isRobotHolding
- $\text{isEndEffectorGrabbing}$
- $\text{isEndEffectorClosed}$

3 Specification of the system




3.1 Specification of the model

All formulae have to be indented universally quantified over x and y and over time.

3.1.1 Environment layout

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1																		
2																		
3	B																	
4	I																	
5	N																	
6																		
7																		

Key

- ● : joint
-  : pallet
-  : cart
-  : end effector
- In the area in lilac the cart is allowed to move fast.

3.1.2 Specification of the cart

1. It is impossible that the cart is moving and is still at the same time.

$$\text{isCartMoving} \longleftrightarrow \neg \text{isCartStill}$$

2. The cart is moving if and only if it is moving at some speed.

$$\text{isCartMoving} \longleftrightarrow (\text{isCartMovingFast} \vee \text{isCartMovingSlow})$$

3. It is impossible that the cart is moving at different speeds at the same time.

$$\neg(\text{isCartMovingFast} \wedge \text{isCartMovingSlow})$$

4. The cart is moving if and only if is moving to the bin (left) or to the pallet (right).

$$\text{isCartMoving} \longleftrightarrow (\text{isCartMovingLeft} \vee \text{isCartMovingRight})$$

5. The cart has to be in a cell.

$$\bigvee_{1 \leq x \leq 17, 1 \leq y \leq 7} \text{isCartAt}(x, y)$$

6. The cart can't be in more than one cell.

$$\forall (x, y)(h, k)(x \neq h \vee y \neq k \rightarrow \neg(\text{isCartAt}(x, y) \wedge \text{isCartAt}(h, k)))$$

7. Slow speed is one cell per time step.

$$\begin{aligned} \text{isCartMovingSlow} \wedge \text{isCartAt}(x, y) \rightarrow & \text{Dist}(\text{isCartAt}(x + 1, y) \vee \text{isCartAt}(x, y + 1) \\ & \vee \text{isCartAt}(x - 1, y) \vee \text{isCartAt}(x, y - 1), 1) \end{aligned}$$

8. Fast speed is two cells per time step. We decided that the cart should not be allowed to move of 2 cells per unit of time along the Y axis, therefore the speed “fast” along the Y axis is defined as “moving by one cell per unit of time”.

$$\begin{aligned} \text{isCartMovingFast} \wedge \text{isCartAt}(x, y) \rightarrow & \text{Dist}(\text{isCartAt}(x + 2, y) \vee \text{isCartAt}(x, y + 1) \\ & \vee \text{isCartAt}(x - 2, y) \vee \text{isCartAt}(x, y - 1), 1) \end{aligned}$$

9. The robot is resting if and only if both the joint and the end effector are in the same cell of the cart.

$$\text{isRobotResting} \longleftrightarrow (\text{isCartAt}(x, y) \rightarrow \text{isEndEffectorAt}(x, y) \wedge \text{isJointAt}(x, y))$$

10. The cart is moving left if it is moving on the adjacent left cell at distance one or two.

$$\begin{aligned} \text{isCartMovingLeft} \longleftrightarrow & (\text{isCartAt}(x, y) \rightarrow \text{Dist}(\text{isCartAt}(x - 1, y), 1)) \\ & \vee (\text{isCartAt}(x, y) \rightarrow \text{Dist}(\text{isCartAt}(x - 2, y), 1)) \end{aligned}$$

11. The cart is moving right if is moving on the adjacent right cell at distance one or two.

$$\begin{aligned} \text{isCartMovingRight} \longleftrightarrow & (\text{isCartAt}(x, y) \rightarrow \text{Dist}(\text{isCartAt}(x + 1, y), 1)) \\ & \vee (\text{isCartAt}(x, y) \rightarrow \text{Dist}(\text{isCartAt}(x + 2, y), 1)) \end{aligned}$$

3.1.3 Specification of the local bin

1. It is impossible that the local bin is empty and full at the same time.

$$\neg(\text{isLocalBinEmpty} \wedge \text{isLocalBinFull})$$

3.1.4 Specification of the arm

1. The joint has to be close to the cart.

$$\begin{aligned} \text{isCartAt}(x, y) \rightarrow & \text{isJointAt}(x, y) \vee \text{isJointAt}(x + 1, y) \vee \text{isJointAt}(x, y + 1) \\ & \vee \text{isJointAt}(x + 1, y + 1) \vee \text{isJointAt}(x - 1, y) \vee \text{isJointAt}(x, y - 1) \\ & \vee \text{isJointAt}(x - 1, y - 1) \vee \text{isJointAt}(x + 1, y - 1) \vee \text{isJointAt}(x - 1, y + 1) \end{aligned}$$

2. The joint cannot be in more than one cell at a time.

$$\forall(x, y)(h, k)(x \neq h \vee y \neq k \rightarrow \neg(\text{isJointAt}(x, y) \wedge \text{isJointAt}(h, k)))$$

3. The end effector can be in only one position at a time.

$$\forall(x, y)(h, k)(x \neq h \vee y \neq k \rightarrow \neg(\text{isEndEffectorAt}(x, y) \wedge \text{isEndEffectorAt}(h, k)))$$

4. The end effector has to be close to the joint.

$$\begin{aligned} \text{isJointAt}(x, y) \rightarrow & \text{isEndEffectorAt}(x, y) \vee \text{isEndEffectorAt}(x + 1, y) \vee \text{isEndEffectorAt}(x, y + 1) \\ & \vee \text{isEndEffectorAt}(x + 1, y + 1) \vee \text{isEndEffectorAt}(x - 1, y) \\ & \vee \text{isEndEffectorAt}(x, y - 1) \vee \text{isEndEffectorAt}(x - 1, y - 1) \\ & \vee \text{isEndEffectorAt}(x + 1, y - 1) \vee \text{isEndEffectorAt}(x - 1, y + 1) \end{aligned}$$

5. The joint is moving if and only if it isn't in the same position in next time step.

$$\text{isJointMoving} \longleftrightarrow \text{isJointAt}(x, y) \wedge \text{Dist}(\text{isJointAt}(h, k), 1) \wedge (x \neq h \vee y \neq k)$$

6. The joint can move close to its position.

$$\begin{aligned} \text{isJointMoving} \wedge \text{isJointAt}(x, y) \rightarrow & \text{Dist}(\text{isJointAt}(x + 1, y) \vee \text{isJointAt}(x, y + 1) \\ & \vee \text{isJointAt}(x + 1, y + 1) \vee \text{isJointAt}(x - 1, y) \\ & \vee \text{isJointAt}(x, y - 1) \vee \text{isJointAt}(x - 1, y - 1) \\ & \vee \text{isJointAt}(x + 1, y - 1) \vee \text{isJointAt}(x - 1, y + 1), 1) \end{aligned}$$

7. The end effector is moving if and only if it isn't in the same position in next time step.

$$\text{isEndEffectorMoving} \longleftrightarrow \text{isEndEffectorAt}(x, y) \wedge \text{Dist}(\text{isEndEffectorAt}(h, k), 1) \wedge (x \neq h \vee y \neq k)$$

8. The end effector can move close to its position.

$$\begin{aligned} \text{isEndEffectorMoving} \wedge \text{Dist}(\text{isJointAt}(x, y), 1) \rightarrow & \text{Dist}(\text{isEndEffectorAt}(x + 1, y) \vee \text{isEndEffectorAt}(x, y + 1) \\ & \vee \text{isEndEffectorAt}(x + 1, y + 1) \vee \text{isEndEffectorAt}(x - 1, y) \\ & \vee \text{isEndEffectorAt}(x, y - 1) \vee \text{isEndEffectorAt}(x - 1, y - 1) \\ & \vee \text{isEndEffectorAt}(x + 1, y - 1) \vee \text{isEndEffectorAt}(x - 1, y + 1), 1) \end{aligned}$$

9. The operator is on the left of the cart if it is in the neighboring cells on the left of the cart as shown in the table.

$$\text{isOpOnTheLeft} \longleftrightarrow \text{isCartAt}(x, y) \wedge \bigvee_{x-3 \leq h \leq x+1, y-2 \leq k \leq y+2} \text{isOperatorAt}(h, k)$$

10. The operator is on the right of the cart if it is in the neighboring cells on the right of the cart as shown in the table.

$$\text{isOpOnTheRight} \longleftrightarrow \text{isCartAt}(x, y) \wedge \bigvee_{x-1 \leq h \leq x+3, y-2 \leq k \leq y+2} \text{isOperatorAt}(h, k)$$

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1																		
2																		
3	B																	
4	I																	
5	N																	
6																		
7																		

Table 1: Tabella1 caption

11. Definition of picking.

$$\begin{aligned} \text{isRobotPicking} \longleftrightarrow & (\text{isOperatorAt}(x, y) \wedge y \leq 3 \wedge \neg \text{isRightArmAt}(12, 4) \wedge \neg \text{isLeftArmAt}(12, 4) \\ & \rightarrow \text{Dist}(\text{isJointAt}(13, 5) \wedge \text{isEndEffectorAt}(12, 4), 1)) \\ & \vee (\text{isOperatorAt}(x, y) \wedge y \geq 5 \wedge \neg \text{isRightArmAt}(12, 4) \wedge \neg \text{isLeftArmAt}(12, 4) \\ & \rightarrow \text{Dist}(\text{isJointAt}(13, 3) \wedge \text{isEndEffectorAt}(12, 4), 1)) \vee (\text{isOperatorAt}(14, 4) \\ & \rightarrow \text{Dist}(\text{isJointAt}(13, 4) \wedge \text{isEndEffectorAt}(12, 4), 1)) \end{aligned}$$

While the final position of End Effector is always the Local bin cell, the joint behavior changes accordingly to the position of the Operator in order to prevent collisions or low efficiency.

In the figure above are shown the positions it assume when (1) Op is in the yellow part, (2) Op is in the pink cells and (3) Op is in the green part.

	11	12	13	14	15	16	17
1							
2							
3			● ¹				
4		◻ ◉ ₂		◻			
5			● ³				
6							
7							

12. Definition of holding.

$$\begin{aligned}
\text{isRobotHolding} \longleftrightarrow & (\text{isOperatorAt}(x, y) \wedge y \leq 3 \wedge \neg \text{isRightArmAt}(15, 4) \wedge \neg \text{isLeftArmAt}(15, 4) \\
& \rightarrow \text{Dist}(\text{isJointAt}(14, 5) \wedge \text{isEndEffectorAt}(15, 4), 1)) \\
& \vee (\text{isOperatorAt}(x, y) \wedge y \geq 5 \wedge \neg \text{isRightArmAt}(15, 4) \wedge \neg \text{isLeftArmAt}(15, 4) \\
& \rightarrow \text{Dist}(\text{isJointAt}(14, 3) \wedge \text{isEndEffectorAt}(15, 4), 1)) \vee (\text{isOperatorAt}(x, 4) \\
& \rightarrow \text{Dist}(\text{isJointAt}(14, 4) \wedge \text{isEndEffectorAt}(15, 4), 1))
\end{aligned}$$

While the final position of End Effector is always the Pallet cell, the joint behavior changes accordingly to the position of the Operator in order to prevent collisions or low efficiency.

In the figure above are shown the positions it assume when (1) Op is in the yellow part, (2) Op is in the pink cells and (3) Op is in the green part.

	11	12	13	14	15	16	17
1							
2							
3				● ¹			
4		◻ ◯		● ²	◻		
5				● ³			
6							
7							

13. While the pice is loaded the end effector cannot close or grab another piece.

$$\text{isPieceLoaded} \rightarrow \neg \text{isEndEffectorClosed} \wedge \neg \text{isEndEffectorGrabbing}$$

14. Grabbing takes one time step.

$$\text{isEndEffectorGrabbing} \rightarrow \text{Dist}(\neg \text{isEndEffectorGrabbing}, 1)$$

3.1.5 Specification of the operator

1. The body of the operator has to be somewhere.

$$\bigvee_{1 \leq x \leq 17, 1 \leq y \leq 7} \text{isOperatorAt}(x, y)$$

2. The body of the operator can't be in two cells at a time.

$$\forall(x, y)(h, k)(x \neq h \vee y \neq k \rightarrow \neg(\text{isOperatorAt}(x, y) \wedge \text{isOperatorAt}(h, k)))$$

3. Arms of the operator have to be close to the body.

$$\begin{aligned} \text{isOperatorAt}(x, y) \rightarrow & \text{isRightArmAt}(x, y) \vee \text{isRightArmAt}(x + 1, y) \vee \text{isRightArmAt}(x, y + 1) \\ & \vee \text{isRightArmAt}(x + 1, y + 1) \vee \text{isRightArmAt}(x - 1, y) \\ & \vee \text{isRightArmAt}(x, y - 1) \vee \text{isRightArmAt}(x - 1, y - 1) \\ & \vee \text{isRightArmAt}(x + 1, y - 1) \vee \text{isRightArmAt}(x - 1, y + 1) \end{aligned}$$

$$\begin{aligned} \text{isOperatorAt}(x, y) \rightarrow & \text{isLeftArmAt}(x, y) \vee \text{isLeftArmAt}(x + 1, y) \vee \text{isLeftArmAt}(x, y + 1) \\ & \vee \text{isLeftArmAt}(x + 1, y + 1) \vee \text{isLeftArmAt}(x - 1, y) \\ & \vee \text{isLeftArmAt}(x, y - 1) \vee \text{isLeftArmAt}(x - 1, y - 1) \\ & \vee \text{isLeftArmAt}(x + 1, y - 1) \vee \text{isLeftArmAt}(x - 1, \text{jointy} + 1) \end{aligned}$$

4. Arms of the operator cannot be in more than one cell.

$$\forall(x, y)(h, k)(x \neq h \vee y \neq k \rightarrow \neg(\text{isRightArmAt}(x, y) \wedge \text{isRightArmAt}(h, k)))$$

$$\forall(x, y)(h, k)(x \neq h \vee y \neq k \rightarrow \neg(\text{isLeftArmAt}(x, y) \wedge \text{isLeftArmAt}(h, k)))$$

5. The operator can move by only one cell per time step.

$$\begin{aligned} \text{isOperatorAt}(x, y) \rightarrow & \text{Dist}(\text{isOperatorAt}(x, y) \vee \text{isOperatorAt}(x + 1, y) \vee \text{isOperatorAt}(x, y + 1) \\ & \vee \text{isOperatorAt}(x + 1, y + 1) \vee \text{isOperatorAt}(x - 1, y) \vee \text{isOperatorAt}(x, y - 1) \\ & \vee \text{isOperatorAt}(x - 1, y - 1) \vee \text{isOperatorAt}(x + 1, y - 1) \\ & \vee \text{isOperatorAt}(x - 1, y + 1), 1) \end{aligned}$$

3.2 Specification of the behaviour

3.2.1 Cart movement

1. When the cart is moving, the robot (joint plus end effector) has to be still.

$$\neg(\text{isRobotResting} \wedge \text{Dist}(\text{isRobotResting}, 1)) \rightarrow \neg \text{isCartMoving}$$

2. The cart has to move to the bin when the local bin is empty.

$$\text{isLocalBinEmpty} \wedge \neg \text{isOpOnTheLeft} \wedge \text{isRobotResting} \wedge \neg \text{isCartAt}(2, 4) \rightarrow \text{isCartMovingLeft}$$

3. The cart has to stay at the bin until the local bin is full.

$$\text{isCartAt}(2, 4) \wedge \neg \text{isLocalBinFull} \rightarrow \text{isCartStill}$$

4. The cart has to move to the pallet when the local bin is full.

$$\text{isLocalBinFull} \wedge \neg \text{isOpOnTheRight} \wedge \text{isRobotResting} \wedge \neg \text{isCartAt}(13, 4) \rightarrow \text{isCartMovingRight}$$

5. The cart has to stay at the pallet until the local bin is empty.

$$\text{isCartAt}(13, 4) \wedge \neg \text{isLocalBinEmpty} \rightarrow \text{isCartStill}$$

6. The cart has to move slowly near pallet and near bin.

$$\begin{aligned} &\text{isCartMoving} \wedge (\text{isCartAt}(2, 4) \vee \text{isCartAt}(3, 4) \vee \text{isCartAt}(4, 4) \vee \text{isCartAt}(11, 4) \\ &\vee \text{isCartAt}(12, 4) \vee \text{isCartAt}(13, 4)) \rightarrow \text{isCartMovingSlow} \end{aligned}$$

7. The cart has to move slowly when the operator is close to it.

$$\begin{aligned} &\text{isCartMovingLeft} \wedge \text{isCartAt}(x, y) \wedge (\text{isOperatorAt}(x - 4, y + 2) \vee \text{isOperatorAt}(x - 4, y + 1) \\ &\vee \text{isOperatorAt}(x - 4, y) \vee \text{isOperatorAt}(x - 4, y - 1) \vee \text{isOperatorAt}(x - 4, y - 2)) \rightarrow \text{isCartMovingSlow} \end{aligned}$$

$$\begin{aligned} &\text{isCartMovingRight} \wedge \text{isCartAt}(x, y) \wedge (\text{isOperatorAt}(x + 4, y + 2) \vee \text{isOperatorAt}(x + 4, y + 1) \\ &\vee \text{isOperatorAt}(x + 4, y) \vee \text{isOperatorAt}(x + 4, y - 1) \vee \text{isOperatorAt}(x + 4, y - 2)) \rightarrow \text{isCartMovingSlow} \end{aligned}$$

8. The cart has to move fast if the operator is distant.

$$\begin{aligned} &\text{isCartMovingSlow} \wedge \text{isCartMovingRight} \wedge \text{isCartAt}(x, y) \wedge x \geq 5 \wedge \text{isOperatorAt}(h, k) \\ &\wedge \text{isOperatorAt}(h, k) \wedge (h \geq x + 5 \vee h \leq x - 2 \wedge (k < y - 2 \vee k > y + 2)) \rightarrow \text{Dist}(\text{isCartMovingFast}, 1) \end{aligned}$$

$$\begin{aligned} &\text{isCartMovingSlow} \wedge \text{isCartMovingLeft} \wedge \text{isCartAt}(x, y) \wedge x \leq 10 \wedge \text{isOperatorAt}(h, k) \\ &\wedge \text{isOperatorAt}(h, k) \wedge (h \geq x + 1 \vee h \leq x - 5 \wedge (k < y - 2 \vee k > y + 2)) \rightarrow \text{Dist}(\text{isCartMovingFast}, 1) \end{aligned}$$

3.2.2 Robot Arm working

1. The robot has to set in the right position to grab.

$$\neg \text{isLocalBinEmpty} \wedge \text{isEndEffectorClosed} \wedge \text{isCartAt}(13, 4) \rightarrow \text{isRobotPicking}$$

2. Once the robot has reached the final position, it waits until it has grabbed the piece.

$$\text{isEndEffectorAt}(12, 4) \wedge \neg \text{isRightArmAt}(12, 4) \wedge \neg \text{isLeftArmAt}(12, 4) \rightarrow \text{isEndEffectorGrabbing}$$

3. After the end effector has grabbed, it returns in the base position.

$$\text{isPieceLoaded} \rightarrow \text{Dist}(\text{isEndEffectorAt}(13, 4) \wedge \text{isJointAt}(13, 4), 1)$$

4. If the robot is in the base position and is holding a piece, it has to set in order to let the operator work on it.

$$\text{isPieceLoaded} \wedge \text{isEndEffectorAt}(13, 4) \wedge \text{isJointAt}(13, 4) \wedge \neg \text{isOperatorAt}(14, 4) \rightarrow \text{isRobotHolding}$$

5. Until the piece is held, the robot mustn't move.

$$\text{isPieceLoaded} \wedge \text{isEndEffectorAt}(15, 4) \wedge \text{isJointAt}(x, y) \rightarrow \text{Dist}(\text{isEndEffectorAt}(15, 4) \wedge \text{isJointAt}(x, y), 1)$$

6. If the piece is unloaded, the robot returns to the base position.

$$\neg \text{isPieceLoaded} \wedge \text{isEndEffectorAt}(15, 4) \wedge \neg \text{isOperatorAt}(14, 4) \rightarrow \\ \text{Dist}(\text{isJointAt}(13, 4) \wedge \text{isEndEffectorAt}(13, 4) \wedge \text{isEndEffectorClosed}, 1)$$

4 Specification of the safety properties

1. The cart and the operator cannot be in the same cell of the pallet.

$$\neg \text{isCartAt}(15, 4)$$

2. The cart cannot be in the same cell of the Bin

$$\neg \text{isCartAt}(1, 4)$$

3. The body of the operator cannot be in the same cells of the cart.

$$\text{isCartAt}(x, y) \rightarrow \neg \text{isOperatorAt}(x, y) \wedge \neg \text{isOperatorAt}(x - 1, y)$$

4. Operator left and right arms cannot be in the same cell of the base of the robotic arm.

$$\text{isCartAt}(x, y) \wedge \neg \text{isRobotResting} \rightarrow \neg \text{isLeftArmAt}(x, y) \wedge \neg \text{isRightArmAt}(x, y)$$

5. While the cart is moving, left and right arms cannot be in the same cells of it.

$$\text{isCartMoving} \wedge \text{isCartAt}(x, y) \rightarrow \neg \text{isLeftArmAt}(x, y) \wedge \neg \text{isRightArmAt}(x, y)$$

6. While the joint is in the same cell of the operator arms, it cannot move or work.

$$\begin{aligned} &\text{isJointAt}(x, y) \wedge (\text{isRobotPicking} \vee \text{isRobotHolding}) \\ &\rightarrow \neg \text{isRightArmAt}(x, y) \wedge \neg \text{isLeftArmAt}(x, y) \end{aligned}$$

7. The robotic arm cannot be in the same cell of the operator body.

$$\text{isOperatorAt}(x, y) \rightarrow \neg \text{isJointAt}(x, y) \wedge \neg \text{isEndEffectorAt}(x, y)$$

8. The operator cannot be trapped at the bin.

$$\text{isOperatorAt}(1, 4) \rightarrow \neg \text{isJointAt}(1, 4) \vee \text{isEndEffectorAt}(1, 4)$$

9. The operator cannot be trapped at the pallet.

$$\text{isOperatorAt}(14, 4) \rightarrow \neg \text{isJointAt}(14, 4) \vee \text{isEndEffectorAt}(14, 4)$$

5 Conclusion

Our whole model, especially the safety properties, aims at defining the robot's behaviour and conditions to operate in such way that it is not possible by any means for it to do harm to the human operator. Our choices in creating the model as well as introducing any simplification were mostly driven by this purpose. The core approach was to prevent the robot from moving every time the human was close enough to be potentially harmed. This choice may in some cases (mostly if the operator performs a non-standard movement) restrict the operative effectiveness of the robot but ensures that he cannot be harmed.