Computers and Electronics in Agriculture 222 (2024) 108987

Contents lists available at ScienceDirect

Computers and Electronics in Agriculture

journal homepage: www.elsevier.com/locate/compag

Original papers

Probabilistic model-checking of collaborative robots: A human injury assessment in agricultural applications ☆

Leonardo Guevara [a,b,*], Muhammad Khalid [c], Marc Hanheide [a], Simon Parsons [a]

[a] University of Lincoln, Lincoln Centre for Autonomous Systems (L-CAS), Lincoln, LN6 7TS, UK
[b] University of Lincoln, Lincoln Institute for Agri-Food Technology (LIAT), Lincoln, LN2 2LF, UK
[c] University of Hull, Department of Computer Science and Technology, Hull, UK

ARTICLE INFO

Keywords:
Agricultural robotics
Safety systems
Probabilistic model-checking
Sensitivity analysis
HRI
PRISM

ABSTRACT

Current technology has made it possible to automate a number of agricultural processes that were traditionally carried out by humans and now can be entirely performed by robotic platforms. However, there are certain tasks like soft fruit harvesting, where human skills are still required. In this case, the robot's job is to cooperate/collaborate with human workers to alleviate their physical workload and improve harvesting efficiency. To accomplish that in a safe and reliable way, the robot should incorporate a safety system whose main goal is to reduce the risk of harming human co-workers during close human–robot interaction (HRI). In this context, this paper presents a theoretical study, addressing the safety risks of using collaborative robots in agricultural scenarios, especially in HRI situations when the robot's safety system is not completely reliable and a component may fail. The agricultural scenarios discussed in this paper include automatic harvesting, logistics operations, crop monitoring, and plant treatment using UV-C light. A human injury assessment is conducted based on converting the HRI in each agricultural scenario into a formal mathematical representation. This representation is later implemented in a probabilistic model-checking tool. We then use this tool to perform a sensitivity analysis that allows us to determine the probability that a human may get injured according to the occurrence of failures in the robot's safety or perception systems. Results of the sensitivity analysis show that an agricultural robot with a robust human perception system can still harm people if they are not well-trained to interact with the robot for certain scenarios. This illustrates how the probabilistic modeling methodology presented in this work can be used by safety engineers as a guideline to construct their own HRI models and then use the results of the model-checking to enhance the safety and reliability of their robot's safety system architectures and on-site safety policies.

1. Introduction

In 2021, the UK agricultural economy suffered a shortage of British and Eastern European workers compounded by Brexit and the Covid pandemic. The shortage of workers who could complete specialized harvesting tasks made UK farmers consider scaling back production as crops were left rot in fields (The Daily Mail, 2021). To attenuate the economic impact of pickers shortage, it is expected that for the next decades, the traditional fully manual harvesting operations will be transformed to semi or fully automated operations where robotic platforms are used to pick fruits and vegetables (Zhou et al., 2022). However, the performance of current picking robots has not yet been able to surpass the efficiency of experienced human pickers. This is why in the next few years, it is expected that fruit harvesting will see the use of cooperative/collaborative robots that must interact with human co-workers to complete harvesting tasks in a coordinated manner (Banjanović-Mehmedović and Gurdić, 2021).

The use of cooperative/collaborative robots, such as the ones conceptualized in Peng and Vougioukas (2020), Guevara et al. (2021) and Vásconez and Auat Cheein (2022), involves an additional technological challenge over and above those that must be normally faced by robots that navigate autonomously without interacting with humans. For instance, the existence of human–robot interaction (HRI) forces the robot to incorporate a perception system able to determine where the humans are located and what actions they perform (Vasconez et al., 2021). Additionally, and more importantly, is to incorporate a safety system (which uses the information taken from the perception system)

☆ This project is supported by the Assuring Autonomy International Programme, a partnership between Lloyd's Register Foundation and the University of York.
* Correspondence to: Lincoln Institute for Agri-food Technology (LIAT), LN2 2LF.
E-mail addresses: lguevara@lincoln.ac.uk (L. Guevara), m.khalid@hull.ac.uk (M. Khalid), mhanheide@lincoln.ac.uk (M. Hanheide), sparsons@lincoln.ac.uk (S. Parsons).

https://doi.org/10.1016/j.compag.2024.108987
Received 17 July 2023; Received in revised form 14 April 2024; Accepted 25 April 2024
Available online 13 May 2024

to be able to activate safety stops in conditions where it is not safe for the robot to continue to operate.

In the last decade, safety solutions and considering HRI for collaborative robots have been focused mostly on industrial manufacturing environments (Robla-Gómez et al., 2017; Wang and Wang, 2021). In these environments, commercial robotic platforms follow standards in their kinematic/mechanical design to satisfy safety requirements and risk assessment methodologies that have been previously established, for example, International Organization for Standardization (2018a, 2015) and Huck et al. (2021). On the other hand, for agricultural environments, there are only safety standards for traditional agricultural machinery and tractors (International Organization for Standardization, 2018b), but there is not yet any standard for designing safe agricultural robots, a.k.a. agri-robotics. This lack of standards is one of the main reasons why studies related to safety systems or HRI in agri-robotics have been sparse. As far as our knowledge, the authors in Mayoral et al. (2021, 2023) are one of the pioneers in incorporating a safety module into an open-field robot used for grass cutting. This safety module consists of a human-aware braking system that allows the robot to perform safety stops according to the level of risk in unplanned HRIs. These works were tested in a simulated version of a Thorvald II robot commercialized by SAGA robotics.[1] This is a modular platform whose mechanical design can be easily modified according to the user's requirements. The modularity of Thorvald II robots makes them suitable platforms for designing a generic safety system that can be applied to a wide range of agricultural scenarios. We have been building such a generic safety system, one that is constructed as a wrapper around the software that is responsible for Thorvald II autonomous navigation (Grimstad and From, 2018), and that can be valid for different agricultural scenarios compatible with the Thorvald II standard kinematic design. These scenarios include crop monitoring (Kirk et al., 2020), UV-C treatment of plants (Gadoury, 2021), fruit harvesting (Parsa et al., 2023), and logistics operations (Ravikanna et al., 2023; Guevara et al., 2023).

In this context, the aim of the work in this paper is to perform a theoretical human injury assessment on the safety system proposed in Guevara et al. (2023) in case a component of the safety system fails. A critical failure may cause the robot to be unaware of the presence of nearby people and injure them by colliding with them. Moreover, there is the possibility of injuring people without being in contact with them. This can happen when a robot is equipped with UV-C LEDs used for plant treatment (Guettari et al., 2021). To perform a human injury assessment, planned and unplanned HRIs from a range of different agricultural scenarios covered by the Thorvald II robot are modeled as discrete-time automata processes and then translated to an equivalent representation based on a probabilistic modeling language that can be used for model-checking purposes.

In the literature, model-checking tools such as UPPAAL (Bengtsson et al., 1996), NuSMV (Cimatti et al., 2002), or PRISM (Kwiatkowska et al., 2011) have been successfully used to evaluate the effectiveness of theoretical models and analyze quantitative properties of systems across a variety of application domains, including robotic systems. For instance (Dakwat and Villani, 2018) presented a safety assessment based on the concepts of Systems Theory Process Analysis (STPA) and model-checking using UPPAAL applied to a robotic flight simulator; Vicentini et al. (2020) presented a safety assessment methodology based on model-checking for collaborative robots used to assist operators in tasks such as carrying/loading tools during industrial assembly processes. These works introduced important contributions to industrial robots safety systems, however, the applicability of the safety assessments in these works is limited by the deterministic nature of their models, which in terms of HRI, constrains the human behavior to a small number of realistic situations since it does not include the probability of erroneous human behavior as was done for instance in Bolton et al. (2021, 2019). On the other hand, works such as Araújo et al. (2017), Zhao et al. (2019) and Lacerda et al. (2019) used the PRISM tool to evaluate probabilistic representations of robotic systems which addressed the uncertainty of unexpected situations by introducing the probabilities of making state transitions. These kinds of models are better suited to perform a sensitivity analysis and obtain statistical metrics of reaching a specific critical model state as was presented in Mazzeo et al. (2018) and Cheng et al. (2021).

The work mentioned above contains important contributions in the context of model-checking methodologies and safety assessments for cooperative/collaborative robots in structured environments. However, those studies cannot be completely translated to agri-robotics since agricultural applications typically involve environmental conditions that are either unstructured or are not fully controlled. Moreover, so far, there are no studies about the potential hazards (in terms of producing human injuries) of modular robots like the Thorvald II that can be used in several kinds of agricultural scenarios, as opposed to studies that concentrate on a single function. Given this, the work presented here aims to contribute to the state of the art by:

- Defining safety requirements and modeling the planned/unplanned HRIs of four agricultural scenarios where commercial modular platforms like Thorvald II robots are planned to be used in the next decades. The scenarios that we model cover crop monitoring, UV-C treatment of plants, fruit harvesting, and logistics operations.
- Performing a human injury assessment based on the model proposed above. Probabilities of human injury are calculated by performing a sensitivity analysis using a probabilistic model-checking tool. The resulting probabilities can then be used as metrics to evaluate what kind of failure in a proposed safety system architecture can cause the most chance of human injury.

We hope that this can be useful to safety engineers in two ways. First, by showing how tools such as PRISM can be used to measure the reliability of safety systems, we hope to convince safety engineers that the use of model-checking techniques can help them in their work. Second, by providing example models that can be the basis for applying model-checking techniques in other situations we hope to make the use of such techniques easier.

This paper is organized as follows. The prerequisites, main concepts, and safety requirements are introduced in Section 2. The probabilistic modeling of HRI in agricultural scenarios is described in Section 3, showing an example of how to implement a simplified model of a UV-C treatment scenario using the PRISM modeling language. The results of the sensitivity analysis of each scenario, generated by the PRISM model-checking tool, are presented in Section 4, and these results are discussed in Section 5. Finally, the conclusions are presented in Section 6.

2. Background

This section briefly introduces the agricultural context of the work and the key elements from the safety system implemented in Guevara et al. (2023) on which this paper builds.

2.1. Agricultural scenarios

This work covers HRIs in four agricultural scenarios: UV-C treatment, scouting for data collection, and harvesting operations divided into logistics support and automated picking. For all the scenarios, it is intended to use Thorvald II robots whose configuration can be easily modified to fit the requirements of each agricultural scenario. As can be seen in the examples in Fig. 1, the Thorvald II has four steerable wheels which allow it to move in any direction without restrictions unlike a typical car-like or differential-drive robot.

[1] SAGA robotics website https://sagarobotics.com/.

2.1.1. Logistics

We use the term *logistics* to refer to a scenario in which a service robot assists human pickers in transporting fruit that has been picked, allowing human pickers to concentrate on picking fruit as was presented in Ravikanna et al. (2023). As in a traditional picking operation, human pickers remove the fruit from the plant and place them in small containers, the punnets that are familiar from the supermarket. These containers are then placed in larger trays. The picker works with a given tray until it is full, and then summons a robot. The full tray is placed on the robot, which also brings a new tray, and the robot then leaves the current picker location, moves to the end of the row of plants, and waits there until a new picker summons it. When the robot is fully loaded, it transports the full trays to the collection point. To do this the robot has to navigate along paths outside the polytunnel. The Thorvald II robot configuration used during the logistics is presented in Fig. 1(a) where it can be seen that the robot moves between the crop rows transporting trays with fruits.

2.1.2. Picking

The picking refers to the scenario when a harvesting robot performs automatic picking operations as was presented in Parsa et al. (2023). In this scenario, the robot is moving slowly along the rows while a manipulator on it is picking the fruits and placing them on the trays. During this operation, the Thorvald II robot uses the same configuration showed in Fig. 1(a) (i.e it is moving between the crop rows), but the harvesting platform includes a robotic manipulator which performs the picking task.

Since the current harvesting robots do not have good enough harvesting rates to be an efficient solution on their own, then the harvesting operations still require human pickers. Thus, similar to the logistic scenario, in the picking scenario the robots share the workspace with humans but unlike the logistics scenario, they do not require human interaction during the picking process to accomplish their tasks. The only situation when robots require human interaction is for loading/unloading of trays of harvested fruit at collection points. Thus, we can treat this scenario as a complementary operation to the logistics scenario.

2.1.3. UV-C treatment

In commercial growing operations, plants are typically sprayed with various pesticides in order to keep diseases, such as powdery mildew, at bay. However, with a growing interest in reducing the use of chemicals, there is interest in using robots that can treat strawberry crops with UV-C light which has been demonstrated to be effective against powdery mildew according to Hall and Jin (2017) and Gadoury (2021).

The Thorvald II robot configuration used during the UV-C treatment is presented in Fig. 1(b), where the robot is moving along the rows and straddles the tables on which the strawberries grow so that the UV-C emissions are directed inwards. The UV-C dose is carefully calibrated to not damage the strawberry plants but it can harm any other living thing that comes closer than 7 m to the robot. Thus, it is mandatory to restrict access to the polytunnels during UV-C treatment. However, it is always possible that untrained people (visitors) decide to come close to the robot to have a look, or accidentally find themselves too close to the robot. For these unplanned HRIs it is crucial that the robot safety system can get an early human detection in order to alert the human of the danger and stop UV-C operations immediately.

2.1.4. Scouting

The term *scouting* refers to the scenario when the robot operates in an autonomous way, following a predefined pattern inside the polytunnel, in which the fruit is typically grown in the UK, in order to collect data about the crop. For example, in Kirk et al. (2020) the robot was used to count fruit in order to make yield forecasts. The robot can traverse the polytunnel using: (i) the same configuration and pattern as for UV-C application allowing each plant to be imaged from both sides simultaneously, or (ii) using the same configuration and pattern as for harvesting operations imaging the plants from one side at a time. Currently, scouting is performed using a robot in the UV-C treatment configuration. Typically, the data collection is an independent task, however, it is possible to perform the data collection in parallel with the picking or logistics operations. The latter means that from a safety perspective, the scouting scenario does not introduce hazards that are not already covered by the other scenarios. For this reason, in the following sections, we will only deal with UV-C treatment, picking, and logistics operations.

2.2. Safe human–robot interaction

In order to determine if a HRI is safe or not, we can follow the methodologies used by previous work such as Herrera et al. (2017), Vasconez et al. (2019) and Liu et al. (2019). These works were based on concepts of social interactions which divide the personal space around people into four zones according to the relative distance, denoted by d, between the robot and a person where: (i) the *public zone* is the region that is $d \geq 3.6$ m away from the person, (ii) the *social zone* is the region that is $1.2\ \text{m} \leq d < 3.6$ m away from the person, (iii) the *personal zone* is the region that is $0.45\ \text{m} < d < 1.2$ m away from the person, (iv) and the *intimate zone* is the region that is $d \leq 0.45$ m away from the person.

Thus, based on these four zones, in this work, we constrain robot motion to be permitted only if the robot is either within the social zone or the public zone of the nearest person, i.e $d > 1.2$ m. The latter is a general rule for all the agricultural scenarios studied here in order to reduce the chance of causing human injury through some undesired physical contact with the robot. However, during UV-C treatment the people need to stay at least 7 m from the robot to avoid any skin or eye injuries (Lucas et al., 2019). Thus, a stronger safety rule is required for this specific scenario. This rule is that the robot that is carrying out UV-C treatment is allowed to operate only if it is within the public zone of the nearest person, and the robot is also more than 7 m away from him/her.

Fig. 2 shows illustrative examples of possible HRIs that may happen when Thorvald II robots are performing logistics tasks and UV-C treatment. The example on the left shows three pickers (H1, H2, H3) sharing the workspace with robot R1 (in logistics configuration). Pickers H1 and H2 are working in the same row as the robot R1 while picker H3 is working in another row. According to the safety distances mentioned above, robot R1 is considered within the public zone of picker H1, and within the personal zone of pickers H2 and H3. Then, in order to ensure a safe HRI, the robot is not allowed to move while H2 continues to be detected as being within 1.2 m of the robot. However, the robot is allowed to operate next to H3 since any people detected in another row are not considered at risk. This is because the maneuverability constraints of the Thorvald II robot inside the polytunnels do not allow it to move sideways. In the case of picker H1, they are located far enough from the robot to not be considered in danger, thus the robot can move without restriction with respect to them.

The example in the middle considers the same robot R1, but this time moving on paths outside the polytunnel with the collection point as a goal. Since the footpaths are wider than polytunnel rows, in this scenario the Thorvald II is allowed to perform sideways movements, thus the worker H5 is at risk of a potential collision. On the other hand, worker H6 located at the collection point is far enough to let the robot continue with the motion without safety restrictions.

In the example on the right, there are three untrained people (H6, H7, H8) approaching the robot R2 while it is performing UV-C treatment. In this case, the human H6 is located at the same distance from robot R2 as H1 was from robot R1 in the first example, however for a UV-C treatment scenario, any people detected within 7 m from the robot, make the robot stop operation in order to avoid potential human injuries due to UV-C light radiation. Moreover, unlike logistics operations, for UV-C treatment, even if a human is located in a row

(a) (b)

Fig. 1. The Thorvald II configuration used to: (a) perform logistics and picking during fruit harvesting operations; and (b) perform the UV-C treatment and crop monitoring.

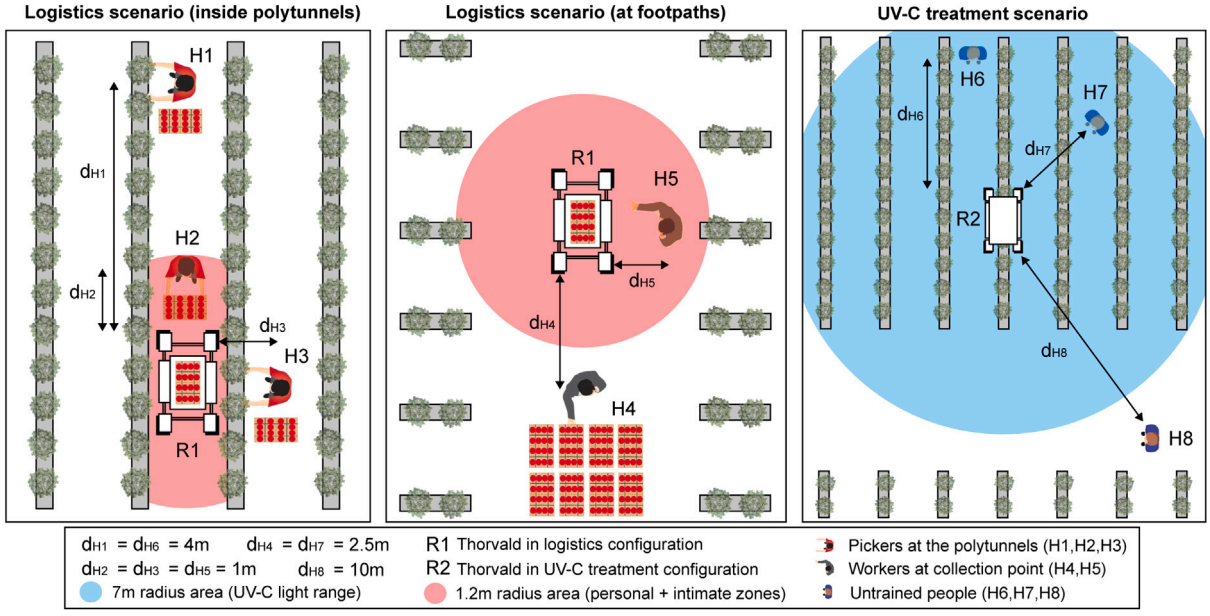

Fig. 2. Illustrative examples of possible HRIs that may happen when Thorvald II robots are performing logistics tasks inside polytunnels (left), at footpaths next to the collection point (middle) and while performing UV-C treatment (right).

next to the robot (as the human H7 in this example), the robot must stop operations since the human is still at risk. The only human who is at a safe distance is H8, however, if an untrained person is not aware of the danger, he/she may decide to get closer at some point in the future.

2.3. Safety system requirements and policies

According to the descriptions of the agricultural scenarios given above, the safety system implemented in the robot should include at least the following components[2]:

SR-1 Audiovisual Feedback Alert System (AVFAS): The robots must be equipped with colored beacons and speakers to periodically or explicitly inform people of the current robot's behavior/intentions (Al-Hussaini et al., 2020).

SR-2 Human Detection System (HDS): The robots must be equipped with sensors such as LiDARs, RBG-D Cameras or IR Cameras that allow it to detect people in a range above 7 m (necessary in the UV-C treatment) (Islam et al., 2019).

SR-3 Human Tracking and Motion Inference System (HTMIS): Based on the HDS, the robot must be able to keep track of the position of the person detected by the HDS and use this information to try to infer the current person's movements (Unhelkar et al., 2018).

SR-4 Human Action Recognition System (HARS): By using the information taken from the HDS, the robot must be able to recognize certain body gestures (used to control the robot) as well as common actions that pickers perform during harvesting operations (see Vasconez et al. (2019) and Vasconez et al. (2021)).

SR-5 Collision Avoidance System (CAS): The robot must be able to perform human-aware maneuvers while evading unexpected people (for example where the robot crosses footpaths) and while approaching a worker to unload/load trays (Hou et al., 2020; Fan et al., 2020).

[2] The policies and safety system components presented in this work are being implemented on a Thorvald II robot as part of the Medium-Sized AGV for soft-fruit Production (MeSAPro) project. A demo video can be seen at https://www.youtube.com/watch?v=WLEGSuPtYJU.

SR-6 Safety Contact System (SCS): In case of imminent contact (either by robot failures or human mistakes), the severity of the human injuries can be reduced by implementing a sensorized flexible skin (such as the one presented in Cirillo et al. (2016)) that could be mounted on strategic areas on the robot structure to detect pressure changes and stop the robot immediately.

Based on these six components and the safety requirements of each agricultural scenario, the following safety policies are proposed with the aim of reducing the severity and/or occurrence of potential human injuries.

SP-1 The AVFAS must activate visual alerts with the aim of making the people who were planning to approach the robot aware of the potential danger without the need to stop robot operations. Moreover, the AVFAS can also activate auditory alerts with explicit prerecorded voice messages to make the robot's intentions easier to understand for untrained people.

SP-2 The AVFAS must activate audiovisual alerts periodically to warn people of the robot's current intentions, especially useful when the robot is going to perform row transitions inside the polytunnels. (When transitioning between rows the robot moves sideways, and, given the position of the sensors, moves blind.)

SP-3 The AVFAS must activate visual alerts when a human is detected within the public zone ($d > 3.6$ m) in order to make them aware of the robot's presence and potential danger. Moreover, the robot must activate audiovisual alerts when a human is within the social zone ($1.2\text{ m} \leq d < 3.6\text{ m}$) to ask if they need the robot's service (in case of operations inside polytunnels) or to inform them that the robot yields priority to the human by default (in case of operations outside polytunnels). According to the replying body gesture, the robot has to pause the operation, re-plan another route, or approach the human.

SP-4 The CAS can be used to slowly approach a picker to load/unload trays only if the HTMIS infers that the picker is mostly stationary or if the HARS recognizes a specific body gesture indicating it.

SP-5 The CAS can be used to perform safety evasion maneuvers outside the polytunnels only if the maneuverability space is wide enough and the HTMIS infers that the human detected is going to be stationary.

SP-6 A body gesture with the directive of pause/continue robot operations can be recognized by the HARS at any moment, inside or outside the polytunnels.

SP-7 A safety stop can be automatically triggered by the HDS when a human is detected within an unsafe distance from the robot ($d \leq 7$ m for UV-C treatment, or $d \leq 1.2$ m for the remaining scenarios) or by SCS if a physical contact is detected.

SP-8 As in-site safety policy, the farm workers and visitors must receive basic training about robot operation modes, the meaning of visual and auditory alerts, and the potential hazards of approaching them (especially critical for UV-C treatment scenarios).

2.4. Model-checking for safety analysis

Safety-critical systems are systems that cannot be allowed to fail. Such systems, if they fail, may cause either economic damage or even loss of life (Guha et al., 2021). To address this critical problem, formal verification by model checking can be used to unearth deficiencies in a system (software, hardware, or safety policies) and then improve it.

The so-called model checking is an algorithmic approach that verifies whether a finite-state model of a system meets a given specification (also known as property) through an exhaustive search of the state space. In the context of robotic systems, formal verification has been widely used to deal with safety issues in different ways. For instance, authors in Xin et al. (2022) presented a run-time verification framework combining sensor-level fault detection and system-level probabilistic model checking. Authors in Ozkan et al. (2023) presented a safety verification of multiple industrial robot manipulators with path conflicts using model-checking. Although those works are valid for formal verification of solely robotic systems, they lack in analyzing the consequences on human co-workers' safety due to either robot failures or human stochastic behavior.

For robotic applications that require HRI, a few works such as Askarpour et al. (2019) presented a formal model of human erroneous behavior for safety analysis in collaborative robotics. Later, the same authors proposed in Vicentini et al. (2020) a risk analysis methodology for collaborative robotic applications, which uses formal verification techniques to automate the traditional risk analysis methods. The main limitation of those two works is that the models used are deterministic which may capture some of the robot behaviors (under certain conditions) but do not fully capture human stochastic behavior. In this context, only a few works such as Gleirscher et al. (2022) and Zacharaki et al. (2021) have addressed the formal verification in HRI scenarios by using probabilistic models for both human and robot agents.

3. Modeling

To model the planned/unplanned HRIs in the agricultural scenarios studied in this work, it was decided to model the behavior of each component involved in the interaction as a Markov decision process (MDP) as in Liang et al. (2022). The MDP is a discrete-time formalism widely used to model sequential decision-making problems where there is inherent uncertainty about the system's evolution. The use of MDPs makes it possible for us to use a probabilistic model-checking tool such as PRISM (Kwiatkowska et al., 2020; Lu et al., 2015) which already has support for solving MDPs against properties in Linear Temporal Logic (LTL), in particular allowing for the maximization of the probability of satisfying an LTL formula. This, in turn, means that the model of system behavior, in the form of an MDP, can be checked against conditions, expressed in LTL, that correspond to states that we wish to achieve (such as "the robot stops when the human makes the appropriate signal") or wish to avoid (such as "the robot collides with the human"). This section first introduces the assumptions used to construct the proposed HRI model, then the discrete states that define the MDP representation of the proposed model are shown, and finally, a case study is presented to illustrate how to implement each component of the proposed model using the PRISM modeling language.

3.1. Modeling assumptions

In order to construct a simplified but realistic HRI model, the following assumptions were used to describe the agricultural tasks, robot operation modes, human behavior, and hazard situations.

3.1.1. Defining the robot agricultural tasks as sequence of steps

To determine whether the agricultural scenarios described in Section 2.1 are completed or not, they can be divided into a sequence of steps. The robot finishes a specific agricultural task when it has successfully completed all the steps. For instance, the sequence of steps to complete the UV-C treatment scenario corresponds to a closed loop in which the robot starts operation from its home location at the storage shed, the robot moves from the shed to the polytunnel, the robot performs the UV-C treatment, the robot moves back to the shed, and finally, the robot is back at the shed. Thus, as it can be seen in Fig. 3, for every agricultural scenario studied here, the sequence of

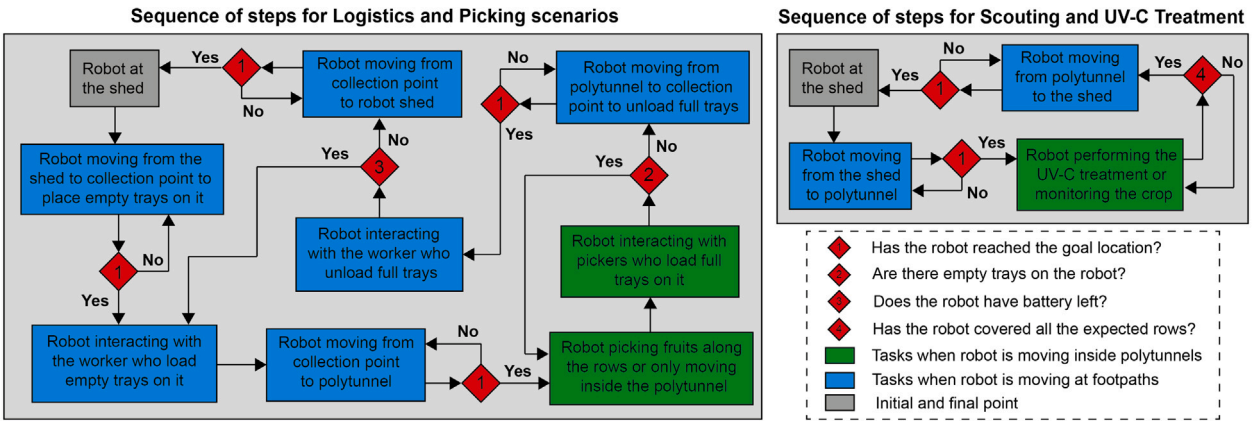

Fig. 3. Diagrams with the sequence of steps that define all the agricultural scenarios.

steps corresponds to a closed loop that starts and finishes with the robot at the shed. The number of steps and complexity depends on the level of HRI expected in each scenario. For instance, in the case of performing the logistics tasks, the corresponding sequence of steps is more complex than for UV-C treatment (where it is not expected to have HRI) since now it is possible to interact with human workers on footpaths between the shed and the polytunnels or with pickers inside polytunnels. Additionally, as can be seen in Fig. 3 (highlighted in red), in order to determine when a robot has completed a specific step within the sequence, there are conditions to be satisfied such as traversing a specific distance or completing the harvesting of a certain amount of fruit placed on trays. Thus since a planned/unplanned HRI may happen each time the robot traverses a new polytunnel row or footpath segment, then the inclusion of these conditions exponentially increases the chances of having human injuries.

3.1.2. Robot operation modes

In order to successfully complete each of the sequential steps defined above, the robot must have the ability to operate in different modes and with different levels of autonomy to adapt to possible unexpected situations. Therefore, we describe the robot motion during the above-mentioned scenarios by 11 different modes divided into 3 groups:

- **Standard operation modes:** The operation modes in common for all agricultural scenarios include: (1) Robot in pause mode, (2) Robot moving along footpaths, (3) Robot performing a transition between footpath segments, (4) Robot performing a transition between rows inside the polytunnel.
- **Custom operation modes:** In order to perform certain agricultural tasks, the robot must be configured in different ways (see Fig. 1) and move at different speeds. Thus, while operating inside the polytunnel, the robot can be working in three custom modes: (5) Robot moving along a row transporting trays (normal speed), (6) Robot moving along a row while picking fruit (slow motion) (7) Robot moving along a row performing UV-C treatment (same configuration used for scouting).
- **Human-aware operation modes:** The implementation of the safety system components described in Section 2.3 aims to ensure a safe HRI during planned and unplanned interactions. Thus, the operation modes which make use of these safety components include: (8) Robot stopping the current action because of human detected within a dangerous distance or because a collision was detected, (9) Robot approaching the human worker's position (reducing the speed) to load/unload trays, (10) Robot moving away from the human's position after loading/unloading trays, (11) Robot performing evasive maneuvers on a footpath.

3.1.3. Human decision-making

In order to emulate human decision-making during planned and unplanned HRI, the following assumptions were considered according to the human's training level:

- If the HRI happens with the picker who summoned the robot, then the picker starts the interaction being stationary, but they can decide to stay stationary or move towards the robot if they are within the social zone.
- If the HRI happens with a picker who did not call the robot, then they start the interaction being stationary, but they can decide to approach or move away when the robot is within the social zone.
- Untrained people inside polytunnels and workers at the end of the rows are always moving to the robot position until they become aware of the danger. If they become aware of the danger, then they move away.
- Workers and untrained people on footpaths move toward the robot until they become aware of the danger. If they become aware of the danger, then they can decide to stop or move away.
- If workers or untrained people decide to remain stationary before the robot enters their social zone, then the robot starts evading them and the human can decide to keep stationary or walk next to the robot.
- Only workers can perform hand gestures, and this can happen only when the robot is within their social zone and the workers are aware of the robot's presence.
- If a person (independent of the training level) is injured, or if the robot performs a safety stop, then the person becomes aware of the danger and decides to move away from the robot.
- Workers who are supposed to place trays on the robot (inside and outside polytunnel) are assumed to always be aware of the danger of HRI.
- An untrained person who is going to interact with a robot can become aware of the danger only if he/she is able to interpret the audiovisual alerts activated by the AVFAS. If he/she is not able to interpret the alerts, then he/she decides to continue approaching till reaches an unsafe distance.

3.1.4. Hazard situations

Based on the agricultural scenarios described in Section 2.1 and the safety system components defined in Section 2.3, it is necessary to identify the potential hazards product of failures in any of the components of the safety system. In this context, following the guidelines of traditional risk assessment techniques such as Failure Mode and Effects Analysis (FMEA) (Chi et al., 2020) and System Theoretic Process Analysis (STPA) (Sun et al., 2021; Huck et al., 2021), Table 1 summarizes a list of 8 critical situations expected to happen during the robot operations in all agricultural scenarios studied here. The table

Table 1
List of relevant failures modes which may happen in every agricultural scenario.

Scenarios	Possible situations	Failure code	Possible failures	Potential effect	Consequence
UV-C scouting logistics picking	Imminent collision is about to happen	**F-1**	Robot fails to detect physical contact	Robot keeps moving after collision	Human is injured after collision
Logistics picking	A human is in the robot's way	**F-2**	Robot fails to detect the human further away than 3.6 m	Audiovisual alerts are not activated so the human is not altered to the robot's presence	Potential human injuries due to collisions
		F-3	Robot fails to interpret a body gesture performed by the human	Robot performs a different action than the directive given by the human	Potential human injuries due to collisions
UV-C scouting logistics picking	Untrained human approaching the robot	**F-4**	Human cannot interpret the audiovisual alerts	Untrainned human is still approaching without being aware of the danger	Potential human injuries due to collisions or UV-C light
Logistics picking	Robot at the end of the rows when a human is approaching laterally (inside polytunnel)	**F-5**	Robot detects the humans only when they are too close (less than 3.6 m)	Robot and human are not aware of each other's presence in time	Potential human injuries due to collisions
		F-2	Robot fails to detect the human further away than 3.6 m	Audiovisual alerts are not activated and then human is not made aware of the robot presence	Potential human injuries due to collisions
UV-C scouting logistics picking	Robot tries to evade a human in its way (only at footpaths)	**F-6**	Robot fails to accurately track the human position	Robot fails to stop safely at 1.2 m from the human	Potential human injuries due to collisions
Logistics picking	Robot starts reducing speed to finally stop next to a human to load/unload trays	**F-6**	Robot fails to track accurately the human position	Robot fails to stop safely at 1.2 m from the human	Potential human injuries due to collisions
UV-C	Robot moving along a row while a human is approaching frontally (inside polytunnel)	**F-7**	Robot fails to detect the human further away than 7 m	Audiovisual alerts are not activated and then human is not made aware of danger	Potential human injuries due to UV-C light
		F-8	Robot fails to detect the human on time when they are within 7 m	Safety stop is not activated and then robot keeps using UV-C light	Potential human injuries due to UV-C light
	Robot at the end of the rows when a human is approaching laterally (inside polytunnel)	**F-5**	Robot detects the human only when they are too close (less than 3.6 m)	Robot stops using UV-C light when it is too late	Potential human injuries due to UV-C light

also shows the possible failures that can occur in each situation along with their consequence in terms of human injuries.

Considering all the situations and failure modes presented in Table 1, we can conclude that there are basically five kinds of ways to produce human injuries:

HI-1 Actual human injuries when $d \leq 7$ m and the robot continues to carry out UV-C treatment in the polytunnels (UV-C treatment scenario).
HI-2 Actual human injuries when the human collides with the robot but the robot stops just after the contact (in any agricultural scenario).
HI-3 Actual human injuries when the human collides with the robot and it is still moving after contact (in any agricultural scenario).
HI-4 Potential human injuries when $1.2 \text{ m} \leq d < 3.6$ m (social zone) and the robot is not aware of the human's intentions during logistics and picking operations (logistics and picking scenarios).
HI-5 Potential human injuries when $1.2 \text{ m} \leq d < 3.6$ m (social zone) and the human is not aware of the presence of the robot (in any agricultural scenario).

HI-2 and **HI-3** are hazards that represent real physical human injuries where the severity level depends on the robot's motion state after the collision. The remaining hazards represent only potential or virtual injuries. In the case of **HI-1**, it is a virtual injury but may produce real injuries if the human is exposed to UV-C radiation at an unsafe distance for a long enough period of time (Lucas et al., 2019). In the case of **HI-5**, since the robot is getting close to the intimate zone, any failure in the HDS, or the HTMIS can produce delays in the activation of safety stops which subsequently may lead to **HI-2** or **HI-3**. In the same way with **HI-4**, if HARS fails to interpret a body gesture performed by a trained worker located next to the robot, an incorrect action by the robot may lead to **HI-2** or **HI-3**.

As was initially mentioned in Section 2.1.4 and later was shown in Table 1, the hazards identified for the scouting scenario overlap with the hazards covered by the rest of the scenarios. Thus, to simplify the modeling and human injury assessment, the following sections will cover only the first three scenarios described in Section 2.1.

3.2. The PRISM language

To facilitate the representation of the MDPs, we decided to follow the methodology presented in Lacerda et al. (2019), using the so-called probabilistic STRIPS-like representation of factored MDPs (see Figs. 4–8), based on the PRISM modeling language as the example in (1).

The fundamental components of the PRISM language are modules, variables, and constants. A model is composed of a number of modules that can interact with each other. A module contains a number of local variables. The values of these variables at any given time constitute the state of the module. The global state of the whole model is determined by the local state of all modules. The behavior of each module is described by a set of commands. A command takes the form:

$$[action]\ (guard\_1 \mid guard\_2)\ \&\ \ldots\ \&\ guard\_m$$
$$-> \ prob\_1 : update\_1 + \cdots + prob\_n : update\_n \quad (1)$$

The ith guard denoted by $guard\_i$ for $i \in \{1, 2, \ldots, m\}$ is a predicate over all the variables in the model (including those belonging to other modules) which may be related to other guards by logical operators such as AND (&), OR (|), Not Equal (!=), among others. Each i-th update denoted by $update\_i$ for $i \in \{1, 2, \ldots, n\}$ describes a transition that the module can make if all the guards are true. A transition is specified by giving the new values of the variables in the module, possibly as a function of other variables or constants. Each update

is assigned a probability (or in some cases a rate) which will be assigned to the corresponding transition. The sum of all probabilities of transitions written on the second side of (1) must be equal to 1. The command also optionally includes an action, either just to annotate it, or for synchronization.

With this base, the following subsections aim to introduce the variables and probabilities (constants) needed to construct commands as the one in (1) which represents the state transitions of the proposed HRI model.

3.3. Modeling the agricultural tasks

As was mentioned in Section 3.1.1, the agricultural tasks are divided into a sequence of steps. In order to define in which step of each scenario we are, the variables *x_uvc*, *x_logistics* and *x_picking* were introduced. Table 7 in the Appendix lists and describes the 4 discrete values that variables *x_uvc* can take as well as the possible transitions between them. On the other hand, Table 7 lists 9 values that the variable *x_logistic* can take where 8 of them overlap with the values that the variable *x_picking* can take. For these three variables related to the agricultural tasks, the transition between two different values is always deterministic, thus it is not necessary to introduce any probabilistic term to model the transitions. However, it is necessary to introduce some auxiliary variables to determine when an agricultural step has been completed and a transition can be carried out. These auxiliary variables are also listed in Table 7 and include: the number of full trays that the robot is carrying represented by *x_trays*; the number of times the robot performed two-way trips from polytunnel to collection point represented by *x_runs*; and the number of rows and footpaths that have been traversed by the robot represented by *x_rows* and *x_segments* respectively.

The range of values that the auxiliary variables can take is constrained by the constants described in Table 8, which basically define the scale of the field to be covered and the capacity of the robot to transport full trays.

3.4. Modeling the robot operations

Depending on the agricultural scenario, the robot is expected to perform specific operation modes that may or may not overlap with another scenario. Thus, based on the robot operation modes introduced in Section 3.1.2, the robot operation is defined by the variable *x_robot* which can take 11 values listed in Table 9. Similar to the variables related to the agricultural tasks presented in Table 7, the variable *x_robot* is purely deterministic, thus, it does not depend on any probabilistic term to make transitions between two values.

3.5. Modeling the safety system components

According to the safety requirements presented in Section 2.3, the proposed safety system is made up of 6 main components which include: AVFAS, HDS, HTMIS, HARS, CAS, and SCS. To implement these components in PRISM, their behavior has been characterized by 6 variables and 16 constants that are used to define the probability of success/failure (i.e. the reliability) of each component.

Table 10 summarizes the values that the 6 variables *x_hds*, *x_htmis*, *x_hars*, *x_scs*, *x_visual* and *x_voice* can take, highlighting with * the transitions that depend on probabilities. Table 11 shows a list of constants that are introduced to define the probabilities to make transitions. These constants can take any value between 0 and 1 depending on the actual effectiveness of the safety system implemented. For instance, if the HDS is considered "virtually perfect" (0% probability of failure) to detect a human above 7 m, then, the constants *x_hds_fail_1* and *x_hds_fail_5* are set as 0 while they are set as 0.9 if 90% of times the HDS fails to detect a human on time. Notice that the performance of HDS in terms of failures may be different inside the polytunnel than at footpaths due to the different levels of occlusion in each environment. Thus, Table 11 shows independent constants for define the probability of failure in each environment.

It is important to notice that in Tables 10–11 no variables or constants were introduced to implicitly define the CAS, but its behavior was included when *x_robot* = 3,8 and the success of the collision-free maneuvering depends indirectly on the success of the remaining safety system components.

Finally, the behavior of the AVFAS was defined by introducing two independent variables for audio and visual alerts. According to Table 10, the transitions of these variables are mostly deterministic, but due to the probabilistic behavior of their potential failures, they are modeled as part of the human side instead of the AVFAS itself.

3.6. Modeling human behavior

For PRISM implementation purposes, human behavior is described by 5 variables whose possible values are listed in Table 12. The first variable is denoted by *x_human* and determines if the human decides to interact with the robot or not and captures what the human's training level is (trained or untrained). The second variable denoted by *x_motion* represents the most relevant actions that trained farm workers typically perform during harvesting operations and the expected actions from untrained people who approach the robot without being aware of the danger. The third variable is denoted by *x_aware* and represents the human knowledge about the robot's intentions or potential danger. The fourth variable denoted by *x_gesture* determines if the human performs or not a body gesture to make the robot knows about his/her intentions. Finally, the fifth variable denoted by *x_dist* represents the distance between the human and the robot in discrete steps according to the safety distances explained in Section 2.2. In order to introduce probabilistic human behavior, 5 constants are used to define the probability of making a decision or another (see Section 3.1.3). Table 13 summarizes the list of probabilities used that include the probabilities that unplanned HRI are going to happen, the probabilities that the human gets aware of the robot's presence or potential danger, the probability that the human decides to perform a risky movement during close HRI, and the probability that a trained worker performs a body gesture to communicate him/her intentions to the robot.

It is important to notice that the transition probabilities may vary according to the training level of the human interacting with the robot. This can be seen in Table 13 where was used different constants to characterize the behavior of untrained visitants and trained farm workers.

3.7. Modeling the hazard situations

Finally, since the values of the variables at a given time constitute the state of the whole HRI, then the PRISM model checker tool should be able to determine if a potential hazard situation is happening or not when a failure is introduced into the robot safety system. The failure modes to be evaluated in PRISM were identified previously in Table 1. Moreover, in Section 3.1.4, it was identified the hazard scenarios which may lead to actual human injuries, remarking **HI – 1**, **HI – 2** and **HI – 3**. These three possible human injuries can be evaluated in PRISM by introducing the following conditions:

HI-1 Pmax=? [F task_finished=false & (x_dist≥2 & x_robot!=10 & x_uvc=2)].
HI-2 Pmax=? [F task_finished=false & (x_dist=5 & x_scs=1)].
HI-3 Pmax=? [F task_finished=false & (x_dist=5 & x_scs=2)].

where Pmax=? [F<t task_finished=false (<condition>)] is the notation of LTL properties to verify in PRISM. This particular notation determines the maximum probability of satisfying a specific condition before the simulated agricultural process ended. The auxiliary variable *task_finished* becomes true when the variables *x_uvc*, *x_logistics*, and *x_picking* have taken all their possible values and return to the initial value 0.

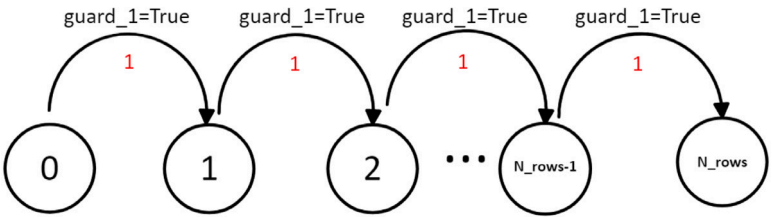

Fig. 4. Diagram with the states transition for variable *x_rows*.

3.8. PRISM implementation: UV-C treatment case study

In the previous Subsections, all the variables, possible values and transition probabilities were introduced in order to model the agricultural scenarios defined in Section 2.1. This Subsection aims to illustrate with an example how to use these elements to construct a simplified UV-C treatment model in PRISM by using commands of the form (1).

Since this example is only for illustration purposes, a simplified version of the UV-C treatment scenario is presented here, where only the robot operations inside the polytunnels are modeled, i.e when *x_uvc* = 2. The complete model with all the transitions presented in Tables 7, 9, 10, and 12 will be used in Section 4.

3.8.1. Commands to model the agricultural task

Since only operations inside the polytunnel are considered, then the variable *x_uvc* does not need to be updated. However, the auxiliary variable *x_rows* needs to be updated each time the robot covers a row. Thus, in order to cover the possible transitions for the variable *x_rows*, the following command is needed:

$$(guard\_1 \ \&\ x\_rows < N\_rows) -> \ (x\_rows' = x\_rows + 1); \tag{2}$$

where the guard expression is defined by:

$$guard\_1 = (x\_uvc = 2 \ \&\ x\_human = 0 \ \&\ x\_robot = 8) \tag{3}$$

The command in (2) updates *x_rows* starting from 0 and increasing in steps of 1 till reach *x_rows* = *N_rows* which represents the condition when the robot has covered all the rows that are expected to be treated. To better understand how the command (2) is executed in PRISM, Fig. 4 illustrates the transition between states, where the number inside the circles are the possible values of variable *x_rows* from 0 to *N_rows*, and the numbers in red represent the probabilities of transition if the condition *guard_1* is satisfied.

3.8.2. Commands to model the robot operation

In order to make all possible transitions for the variable *x_robot* during the UV-C treatment operation, the following commands are needed:

$$(guard\_2 \ \&\ x\_robot = 7) -> \ (x\_robot' = 4); \tag{4}$$

$$(guard\_2 \ \&\ (x\_robot = 4 \mid x\_robot = 10)) -> \ (x\_robot' = 7); \tag{5}$$

$$(guard\_3 \ \&\ x\_robot! = 10) -> \ (x\_robot' = 10) \ \&\ (x\_aware' = 1); \tag{6}$$

where the guards are defined by:

$$guard\_2 = (x\_uvc = 2 \ \&\ x\_human = 0) \tag{7}$$

$$guard\_3 = (x\_uvc = 2 \ \&\ x\_human! = 0 \ \&\ x\_hds = 2) \tag{8}$$

Commands (4)–(5) aim to update the value of *x_robot* between moving along a row and making transition between rows when no human presence is detected. The command in (6) activates a safety stop (i.e. stop motion and turning off the UV-C light) in case a human is detected within the range 3.6 m $\leq d \leq$ 7 m. This command also updates the variable *x_aware* to make the human aware of the danger. To reactivate the robot operation after a safety stop, the condition (*guard_2* & *x_robot* = 10) has to be satisfied in command (5) which makes the robot resume the operation from a transition between rows. Fig. 5(a) illustrates the execution of commands (4)–(6) where the color used on each arrow indicates which condition/guard has to be satisfied to make a transition.

3.8.3. Commands to model the safety system

To simplify this example, the safety system during the UV-C treatment only includes the AVFAS and HDS. Thus, in order to make transitions for the variable *x_hds* when the robot is inside the polytunnels, the following commands need to be implemented:

$$(guard\_4 \ \&\ x\_hds = 0) -> 1 - p\_hds\_1 : (x\_hds' = 1) + p\_hds\_1 : (x\_hds' = x\_hds); \tag{9}$$

$$(guard\_5 \ \&\ x\_hds = 0) -> 1 - p\_hds\_5 : (x\_hds' = 1) + p\_hds\_5 : (x\_hds' = x\_hds); \tag{10}$$

$$(guard\_6 \ \&\ x\_hds \leq 1) -> 1 - p\_hds\_2 : (x\_hds' = 2) + p\_hds\_2 : (x\_hds' = x\_hds); \tag{11}$$

$$(guard\_7 \ \&\ x\_hds \leq 1) -> 1 - p\_hds\_6 : (x\_hds' = 2) + p\_hds\_6 : (x\_hds' = x\_hds); \tag{12}$$

$$(guard\_8 \ \&\ x\_hds \leq 2) -> 1 - p\_hds\_3 : (x\_hds' = 3) + p\_hds\_3 : (x\_hds' = x\_hds); \tag{13}$$

$$(guard\_9 \ \&\ x\_hds \leq 2) -> 1 - p\_hds\_7 : (x\_hds' = 3) + p\_hds\_7 : (x\_hds' = x\_hds); \tag{14}$$

$$(guard\_10 \ \&\ x\_hds \leq 3) -> 1 - p\_hds\_4 : (x\_hds' = 4) + p\_hds\_4 : (x\_hds' = x\_hds); \tag{15}$$

$$(guard\_11 \ \&\ x\_hds \leq 3) -> 1 - p\_hds\_8 : (x\_hds' = 4) + p\_hds\_8 : (x\_hds' = x\_hds); \tag{16}$$

$$(guard\_12 \ \&\ x\_hds = 4) -> (x\_hds' = 3); \tag{17}$$

$$(guard\_13 \ \&\ x\_hds = 3) -> (x\_hds' = 2); \tag{18}$$

$$(guard\_14 \ \&\ x\_hds = 2) -> (x\_hds' = 1); \tag{19}$$

$$(guard\_15 \ \&\ x\_hds = 1) -> (x\_hds' = 0); \tag{20}$$

where the guards are defined by:

$$guard\_4 = (x\_uvc = 2 \ \&\ x\_human! = 0 \ \&\ x\_robot! = 7 \ \&\ x\_dist = 1) \tag{21}$$

$$guard\_5 = (x\_uvc = 2 \ \&\ x\_human! = 0 \ \&\ x\_robot = 7 \ \&\ x\_dist = 1) \tag{22}$$

$$guard\_6 = (x\_uvc = 2 \ \&\ x\_human! = 0 \ \&\ x\_robot! = 7 \ \&\ x\_dist = 2) \tag{23}$$

$$guard\_7 = (x\_uvc = 2 \ \&\ x\_human! = 0 \ \&\ x\_robot = 7 \ \&\ x\_dist = 2) \tag{24}$$

$$guard\_8 = (x\_uvc = 2 \ \&\ x\_human! = 0 \ \&\ x\_robot! = 7 \ \&\ x\_dist = 3) \tag{25}$$

$$guard\_9 = (x\_uvc = 2 \ \&\ x\_human! = 0 \ \&\ x\_robot = 7 \ \&\ x\_dist = 3) \tag{26}$$

$$guard\_10 = (x\_uvc = 2 \ \&\ x\_human! = 0 \ \&\ x\_robot! = 7 \ \&\ x\_dist = 4) \tag{27}$$

$$guard\_11 = (x\_uvc = 2 \ \&\ x\_human! = 0 \ \&\ x\_robot = 7 \ \&\ x\_dist = 4) \tag{28}$$

$$guard\_12 = (x\_uvc = 2 \ \&\ x\_human! = 0 \ \&\ x\_dist = 3) \tag{29}$$

$$guard\_13 = (x\_uvc = 2 \ \&\ x\_human! = 0 \ \&\ x\_dist = 2) \tag{30}$$

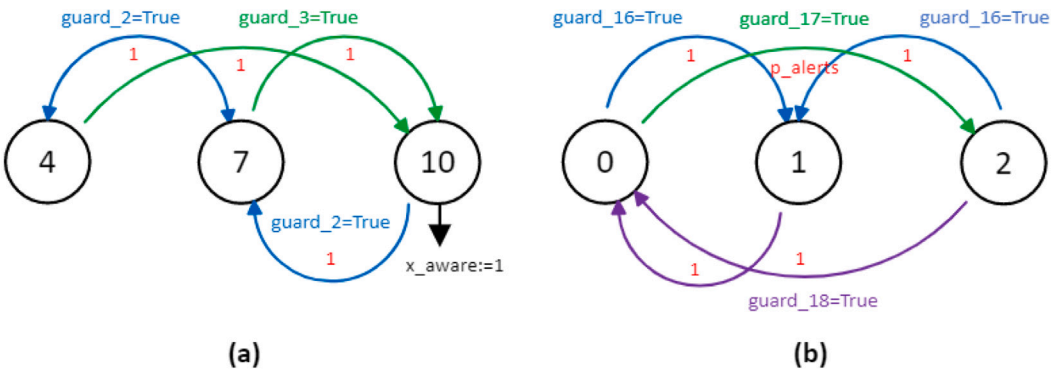

Fig. 5. Diagrams with the states transition for variables: (a) *x_robot*, considering only operations inside the polytunnels during UV-C treatment (b) *x_voice* and *x_visual*.

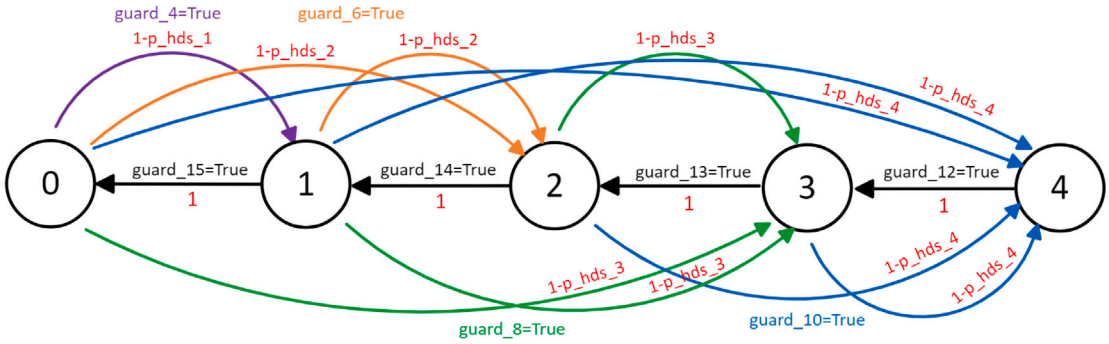

Fig. 6. Diagram with the states transition for variable *x_hds*, without considering transitions when robot operation *x_robot* = 7.

$$guard\_14 = (x\_uvc = 2 \ \& \ x\_human! = 0 \ \& \ x\_dist = 1) \quad (31)$$

$$guard\_15 = (x\_uvc = 2 \ \& \ x\_human = 0 \ \& \ x\_dist = 0) \quad (32)$$

Commands in (9)–(16) cover the updates of *x_hds* from 0 to 4 which depend of the probabilities of failure defined in Table 11. On the other hand, commands in (17)–(20) cover the updates of *x_hds* from 4 to 0 which in this case are purely deterministic. Fig. 6 illustrates the transitions of variable *x_hds*. However, for readability, the transitions whose conditions depend on *x_robot* = 7 are not illustrated in this diagram (i.e when the robot is making transitions between rows).

Then, in order to make the transitions for the two variables related to AVFAS, the following commands are needed:

$$(guard\_16 \ \& \ (x\_visual! = 1 \mid x\_voice! = 1)) \\ -> (x\_visual' = 1)\&(x\_voice' = 1); \quad (33)$$

$$(guard\_17 \ \& \ x\_voice = 0) -> p\_alerts : (x\_voice' = 2) \\ + 1 - p\_alerts : (x\_voice' = x\_voice); \quad (34)$$

$$(guard\_17 \ \& \ x\_visual = 0) -> p\_alerts : (x\_visual' = 2) \\ + 1 - p\_alerts : (x\_visual' = x\_visual); \quad (35)$$

$$(guard\_18 \ \& \ (x\_visual! = 0 \mid x\_voice! = 0)) \\ -> (x\_visual' = 0)\&(x\_voice' = 0); \quad (36)$$

where the guards are defined by:

$$guard\_16 = (x\_uvc = 2 \ \& \ x\_hds \geq 1) \quad (37)$$

$$guard\_17 = (x\_uvc = 2\&(x\_robot = 7 \mid x\_robot = 1 \mid x\_robot = 4)) \quad (38)$$

$$guard\_18 = (x\_uvc = 2 \ \& \ x\_hds = 0) \quad (39)$$

Command (33) activates the audiovisual alerts (visual and voice alerts in parallel) when the HDS detects a human above 7 m. Commands (34)–(35) can also activate the audiovisual alerts, but in this case without the need to detect a human, this activation depends on the probability that at this specific moment a periodic alert was programmed to happen. In any case, after alerts were activated, they can be deactivated only if the condition in (36) is satisfied. The execution of commands (33)–(36) is illustrated in Fig. 5(b).

3.8.4. Commands to model the human behavior

To simplify this example, human behavior considers only the actions performed by untrained people (since farm workers are aware of the UV-C danger). Thus, the transitions of the variable *x_gesture* were not included since only trained people are able to perform body gestures.

In order to update the value of *x_human*, the following commands are required:

$$(guard\_19 \ \& \ x\_human = 0) -> p\_int\_1 : (x\_human' = 1) \\ + 1 - p\_int\_1 : (x\_human' = x\_human); \quad (40)$$

$$(guard\_20 \ \& \ x\_human! = 0) -> (x\_human' = 0); \quad (41)$$

where the guards are defined by:

$$guard\_19 = (x\_uvc = 2 \ \& \ x\_rows < N\_rows) \quad (42)$$

$$guard\_20 = (x\_uvc = 2 \ \& \ x\_dist = 0 \ \& \ x\_motion = 2 \ \& \ x\_aware = 1) \quad (43)$$

Command (40) is used to determine if an untrained person is going to interact with the robot inside the polytunnels or not. Once an HRI has happened, the variable *x_human* returns to the default value of 0 if the condition in command (41) is satisfied.

Once we know that an untrained person is going to interact with a robot, the actions which govern the human motion are represented by the variable *x_motion*, which transitions are defined by the following commands:

$$(guard\_21 \ \& \ x\_motion = 0) -> (x\_motion' = 1); \quad (44)$$

$$(guard\_22\&x\_motion = 1) \mid (guard\_23\&x\_motion! = 2) \mid (guard\_24 \\ \&x\_motion! = 2) -> (x\_motion' = 2); \quad (45)$$

$$(x\_human = 0\& \ x\_motion = 2) -> (x\_motion' = 0); \quad (46)$$

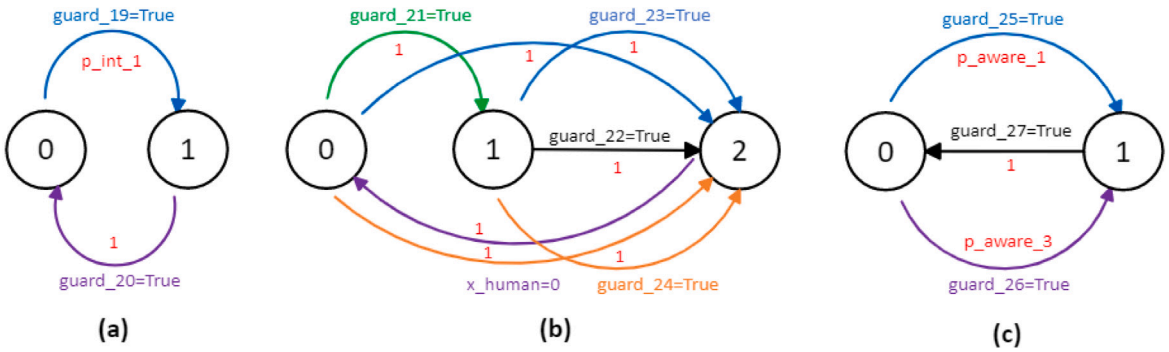

Fig. 7. Diagrams with the states transition for variables: (a) x_human (b) x_motion and (c) x_aware.

where the guards are defined by:

$$guard\_21 = ((x\_robot = 4 \mid x\_robot = 7)\ \&\ (x\_human = 1 \& x\_dist! = 5 \& x\_aware = 0)) \quad (47)$$

$$guard\_22 = ((x\_robot = 4 \mid x\_robot = 7)\ \&\ (x\_human = 1\ \&\ x\_aware = 1)) \quad (48)$$

$$guard\_23 = (x\_dist = 5\ \&\ x\_human! = 0) \quad (49)$$

$$guard\_24 = (x\_human! = 0\ \&\ x\_robot = 10) \quad (50)$$

Then, to make the untrained people aware of danger of approaching the robot, the following commands are included to update *x_aware*:

$$(guard\_25\ \&\ x\_aware = 0) -> p\_aware\_1 : (x\_aware' = 1) + 1 - p\_aware\_1 : (x\_aware' = x\_aware); \quad (51)$$

$$(guard\_26\ \&\ x\_aware = 0) -> p\_aware\_3 : (x\_aware' = 1) + 1 - p\_aware\_3 : (x\_aware' = x\_aware); \quad (52)$$

$$(guard\_27\ \&\ x\_aware = 1) -> (x\_aware' = 0); \quad (53)$$

where the guards are defined by:

$$guard\_25 = (x\_uvc = 2 \& x\_robot! = 10 \& x\_dist \geq 1 \& x\_visual \geq 1 \& x\_human = 1) \quad (54)$$

$$guard\_26 = (x\_uvc = 2 \& x\_robot! = 10 \& x\_dist \geq 2 \& x\_voice \geq 1 \& x\_human! = 0) \quad (55)$$

$$guard\_27 = (x\_uvc = 2 \& x\_human = 0) \quad (56)$$

Commands (51)–(52) update the variable *x_aware* in case of any of the audiovisual alerts were activated at a specific *x_dist*. The variable *x_aware* returns to the default value of 0 by using the command (53).

Finally, to fully model human behavior in this case, the variable *x_dist* needs to be updated according to the relative distance between the human and the robot. The latter is done by introducing the following commands:

$$(guard\_28\ \&\ x\_dist \leq 3) -> (x\_dist' = x\_dist + 1); \quad (57)$$

$$(guard\_29\ \&\ x\_dist \leq 3) -> (x\_dist' = x\_dist + 1); \quad (58)$$

$$(guard\_30\ \&\ x\_dist = 4) -> (x\_dist' = 5)\ \&\ (x\_aware' = 1); \quad (59)$$

$$(guard\_31\ \&\ x\_dist \geq 1) -> (x\_dist' = x\_dist - 1); \quad (60)$$

where the guards are defined by:

$$guard\_28 = (x\_human! = 0 \& x\_motion = 1) \quad (61)$$

$$guard\_29 = (x\_human! = 0 \& x\_motion = 0 \& (x\_robot = 1 \mid x\_robot = 2 \mid x\_robot = 4)) \quad (62)$$

$$guard\_30 = (x\_robot! = 10 \& x\_human! = 0) \quad (63)$$

$$guard\_31 = (x\_human! = 0 \& x\_motion = 2) \quad (64)$$

Commands (57)–(58) update the variable *x_dist* from 0 to 4 in case the robot or the human are approaching each other. The command (59) covers the remaining transition from 4 to 5 in case a safety stop was not activated on time, and the command (60) makes the variable *x_dist* update from 5 to 0 by steps of 1.

The state transitions of variables *x_human*, *x_motion* and *x_aware* are illustrated in Fig. 7, and the transitions of variable x_dist are shown in Fig. 8.

3.8.5. Synchronization

After defining the commands to update all the variables within a PRISM module. We need to ensure that the commands are executed in a specific order to emulate the behavior of the real system. One way to synchronize the execution of the commands presented above is to label each command with actions as illustrated in expression (1). However, this kind of synchronization method depends on the product of the individual rates of transition of all commands with the same label. Thus, for synchronization purposes, we decided to use auxiliary Boolean variables called flags which restrict the execution of commands in a specific order each simulation cycle.

A flag can be assigned to one or more local variables within the model. A flag is always initiated as false and can be updated to true only after the corresponding variable was updated. Thus, a simulation cycle starts with all the flags set as false and ends when all of them are true (being reset as false after that). The order of updating these flags is shown in Fig. 9 starting with the flag related with either *x_uvc*, *x_logistics*, and *x_picking*, and ending with the flag related with variables *x_trays*, *x_runs*, *x_rows*, and *x_seg*.

For instance, in order to execute the command in (4) to make the variable *x_robot* change from 7 to 4, the command should be modified as follows:

$$(guard\_2\ \&\ flag\_hars = true\ \&\ flag\_robot = false) -> (x\_robot' = 4)\ \&\ (flag\_robot' = true); \quad (65)$$

Apart from this modification, it is necessary to include an additional command per each variable in order to avoid being stuck in the execution of the same flag forever when no update is required. By considering again the *x_robot* as an example, the extra command has to make *flag_robot* = true when none of the conditions in (7)–(8) are satisfied. Thus, the extra command for the *x_robot* example takes the following form.

$$(flag\_hars = true\ \&\ flag\_robot = false\ \&\ guard\_sync = false) -> (flag\_robot' = true); \quad (66)$$

where $guard\_sync = (guard\_2 \mid guard\_3)$.

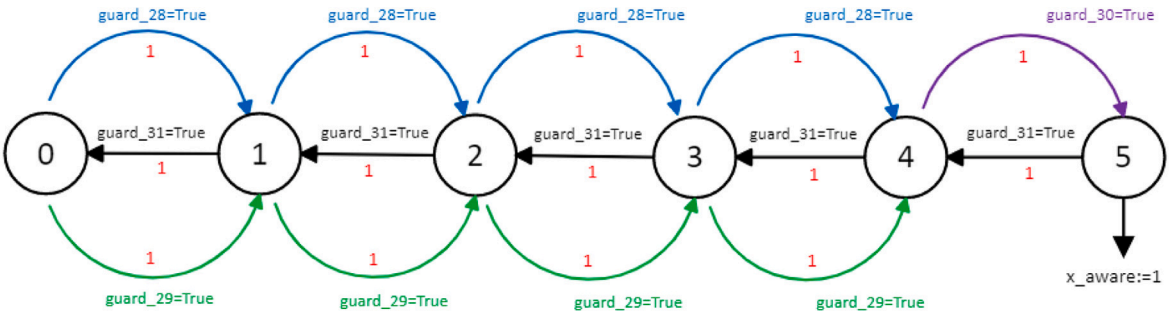

Fig. 8. Diagram with the states transition for variable x_dist.

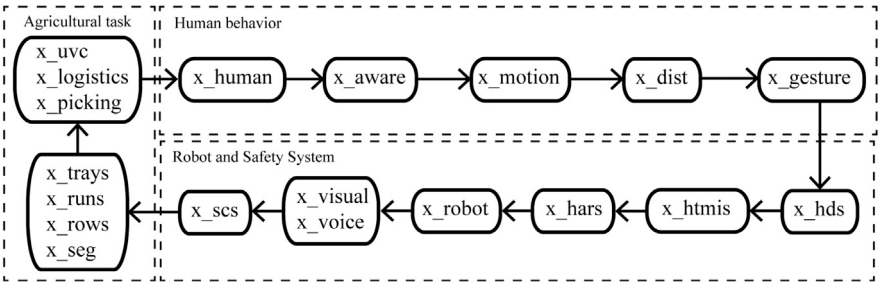

Fig. 9. Diagram with the order in which the local variables are updated in PRISM.

4. Results

Using a more completed PRISM-based model[3] than the one presented in Section 3, this section presents a sensitivity analysis that evaluates the probability of producing any of the three human injuries modeled in Section 3.7 in the presence of any of the eight failure modes identified in Table 1. The evaluation considers three cases where we assumed three different overall performances of the robot safety system. These three cases are called:

Ideal : when the safety system performance is as a much robust as possible.

Regular : when the safety system is as reliable as would be expected in normal conditions.

Worst : when the safety system is not reliable at all.

Note that in the *ideal* case there is still a low probability of having failures since a "virtually perfect" performance with a probability of failure equal to zero is not realistic. Table 14 shows the values of the constants (used as probabilities of transition) that were chosen to characterize the three cases evaluated. See Tables 11 and 13 for more information about the constants listed in Table 14.

Then, the sensitivity analysis for each case was performed as follows. Table 2 indicates with X which constants (used as probabilities of transition) influence a specific safety system failure mode. Thus, to evaluate the consequences of a specific failure mode (see Table 1 for more information about the failure modes), the constant(s) marked with X in the same column of Table 2 were varied from 0% to 100% (in steps of 10%). The value of the rest of the probabilities needed for modeling the safety system and human behavior were set according to which case is evaluated (i.e. *ideal*, *regular*, or *worst*) as indicated in Table 14. For the three cases evaluated, the agricultural tasks were defined by using the following constant values: N_rows = N_runs = 5, N_segments_shed = 2, N_segments_collect = 1, and N_trays = 2 (see Table 8 for more information about these constants).

[3] The PRISM-based model and properties used for the sensitivity analysis can be found at https://github.com/LCAS/PRISM-HRI-model.

Sections 4.1–4.2 show graphically the results of the sensitivity analysis but only from the *ideal* case. Later, Section 4.3 summarizes numerically the results of evaluating all three cases in order to compare the performance of the proposed safety system in each case. Figs. 10–16 show 3D plots that give an idea of the consequences of introducing different probabilities of a failure occurring (from 0 to 100%) as well as varying the probability of having unplanned HRI (from 0 to 100%) with trained farm workers and/or untrained visitors. In these plots, the probabilities were given values of 0% only for visualization purposes, however as mentioned before, even in an *ideal* case, there should still be a low probability of having a failure (to keep it realistic).

As an example to understand how every resultant probability in Figs. 10–16 was generated, let us consider that we want to know the probability of having human injuries of type **HI-3**, if there is a probability of 50% of having a failure of type **F-1** with a 20% probability of encountering with an untrained person. Thus, to generate the resultant probability for this specific example, the constants marked with X in the column **F-1** of Table 2 are set as 0.5, while the rest of the constants in Table 14 are set with the values in the *ideal* case column. Finally, to introduce unplanned HRIs with untrained/trained people, at least one of the four constants related to the variable *x_human* indicated in Table 13 needs to be configured accordingly. In this example, the constants *p_int*_1 (for untrained people inside polytunnels) and *p_int*_3 (for untrained people outside polytunnels) need to be set as 0.2 while the other two (related to trained workers) are set as 0.

It is important to clarify that the resultant probabilities of human injuries in the sensitivity analysis does not represent a metric to quantify the severity of human injuries after each HRI, but a metric to quantify the probability of having at least a human injury after an entire agricultural scenario (UV-C treatment, logistics or picking) is fully completed.

4.1. Assessment of human injuries due to unplanned physical contact

This subsection shows the resulting probabilities of getting human injuries after collisions. Injury **HI-2** is the least critical since the robot tries to minimize the impact by stopping immediately just after detecting the physical contact. On the other hand, injury **HI-3** represents the

Table 2
List of constants belonging to different safety components that influence specific failure modes.

Safety system component	Constant name	Influence over each failure mode[a]							
		F-1	F-2	F-3	F-4	F-5	F-6	F-7	F-8
Human Detection System (HDS)	p_hds_1		X					X	
	p_hds_2		X						X
	p_hds_3					X			
	p_hds_4					X			
	p_hds_5		X					X	
	p_hds_6		X						X
	p_hds_7					X			
	p_hds_8					X			
	p_hds_9		X						
	p_hds_10					X			
	p_hds_11					X			
Human Tracking and Motion Inference System (HTMIS)	p_htmis_1						X		
	p_htmis_2						X		
Human Action Recognition System (HARS)	p_hars			X					
Audiovisual Feedback Alert System (AVFAS)	p_alerts				X				
Safety Contact System (SCS)	p_scs	X							

[a] See Table 1 for more information about the failure modes and Table 11 for more information about the constants listed here.

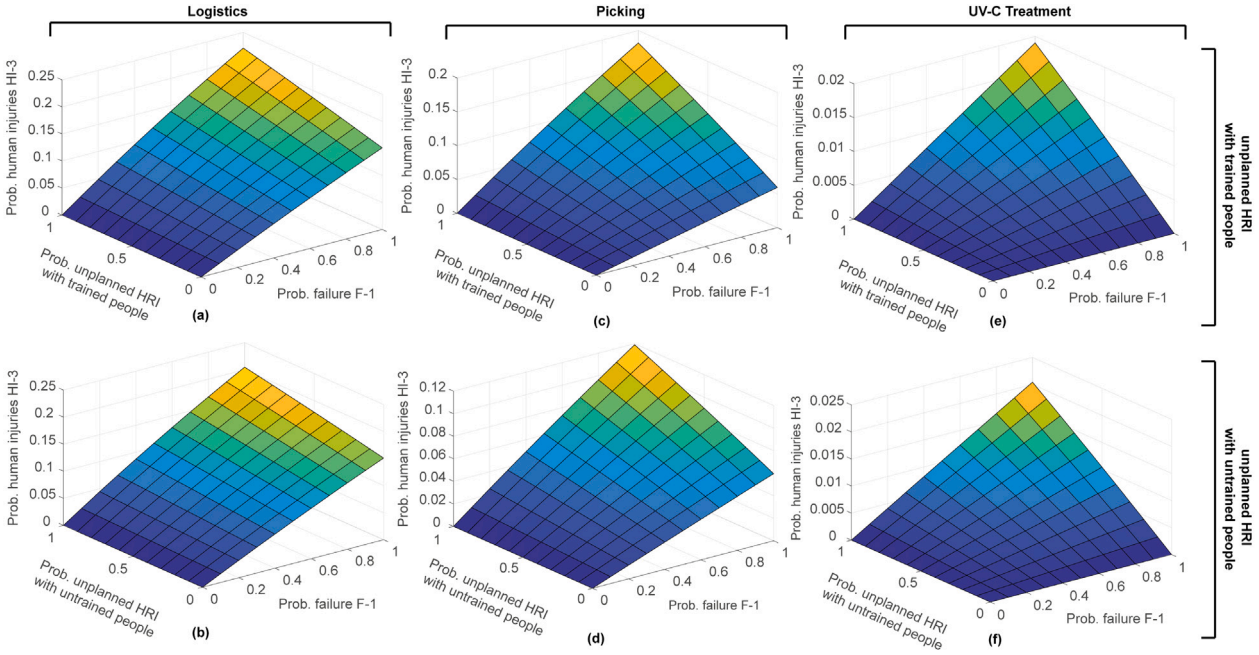

Fig. 10. Probability of human injury **HI-3** in the *ideal* case due to failure **F-1** during: (a,b) Logistics, (c,d) Picking, (e,f) UV-C treatment at footpaths. Evaluating different probabilities of having unplanned interaction with: (a,c,e) trained workers, (b,d,f) untrained people. See Section 3.1.4 for more information about the failure modes and human injuries evaluated here.

most critical scenario since the robot fails to detect the collision on time and continues moving once it has hit the person.

See Sections 3.1.4 and 3.7 for more information about the human injuries **HI-2** and **HI-3**, and Table 1 for more information about the failure modes **F-1** to **F-6**.

4.1.1. Human injuries due to robot failing to detect physical contact (F-1)

According to Fig. 10, considering *ideal* performance of the overall safety system but with a high probability of SCS failing to detect a collision, the maximum probability of human injuries of type **HI-3** is 2% when the robot is moving along footpaths in the UV-C treatment scenario. These results show that the HDS and the AVFAS successfully avoid unnecessarily close HRIs. On the other hand, in the picking scenario, even if the HDS and the AVFAS have the same performance as before, human injuries represent a probability of about 20%. This increment in human injuries happens mainly during planned close HRI when workers approach the robot to load/unload trays. In the same way, since the logistic robots are expected to have even more HRI with human workers than for picking robots, the probability of injury reaches almost 25% for the logistics scenario.

4.1.2. Human injuries due to robot failing to detect the human further away than 3.6 m (F-2)

According to Fig. 11, if the robot fails to detect a human (trained or untrained) further away than 3.6 m, then the human injuries of type **HI-2** can reach a probability of around 30% in both cases logistics and picking scenarios. Moreover, according to these graphical results, the human training level is not a key factor that affects the consequences of having an unplanned HRI. In both cases, trained and untrained people interacting with the robot, the probability of injury is similar, though the interaction with trained people is more dangerous due to the trained people being expected to approach to the robot to load/unload trays.

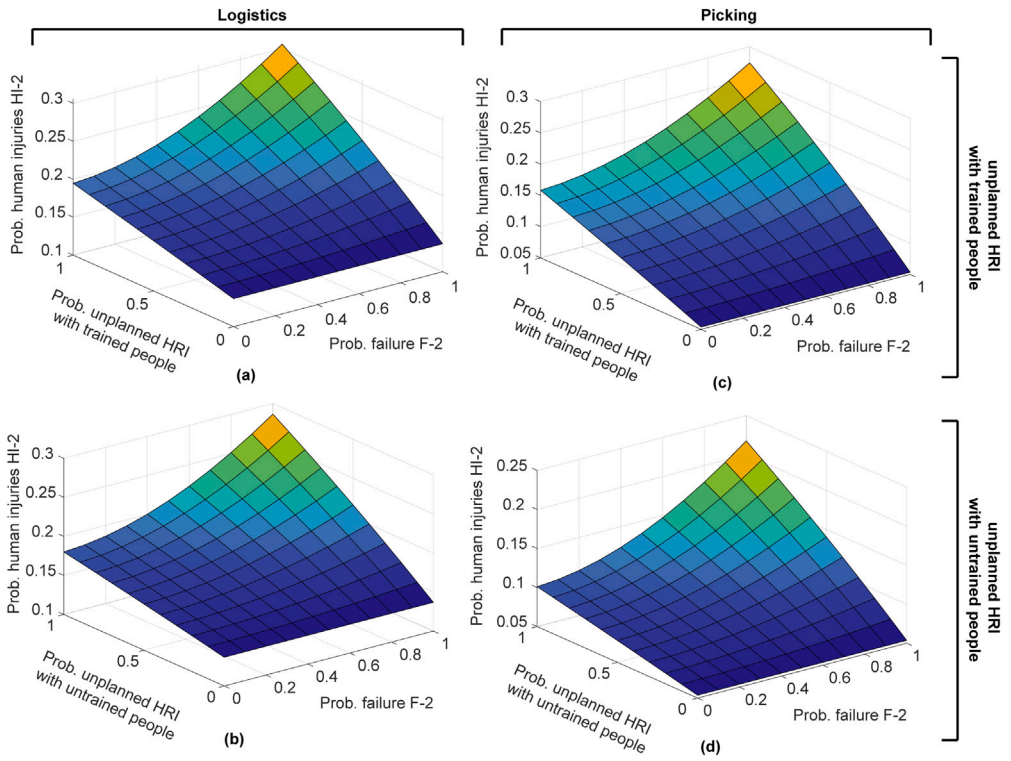

Fig. 11. Probability of human injury **HI-2** in the *ideal* case due to failure **F-2** during: (a,b) Logistics, (c,d) Picking. Evaluating different probabilities of having unplanned interaction with: (a,c) trained workers, (b,d) untrained people. See Section 3.1.4 for more information about the failure modes and human injuries evaluated here.

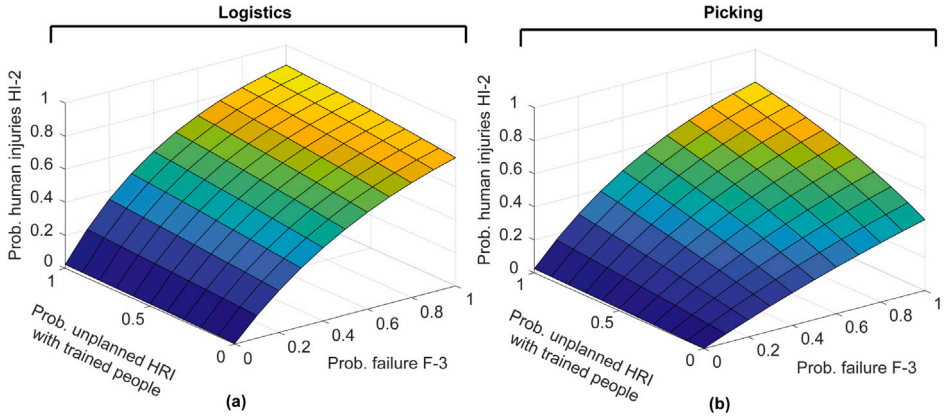

Fig. 12. Probability of human injury **HI-2** in the *ideal* case due to failure **F-3** during: (a) Logistics, (b) Picking. See Section 3.1.4 for more information about the failure modes and human injuries evaluated here.

4.1.3. Human injuries due to robot failing to interpret a body gesture performed by the human (F-3)

According to Fig. 12, in case the robot fails to interpret correctly a body gesture performed by a worker (during planned and unplanned close HRI), then the consequences represent a high probability of human injury of the type **HI-2** with around 90% in case of logistics and 80% in case of picking scenario. These results are due to the fact that if a worker performs a hand gesture to command the robot to stop when they are closely interacting, the HARS could interpret the gesture as another command, which could make the robot move unexpectedly toward the worker.

4.1.4. Human injuries due to human unable to interpret the audiovisual alerts (F-4)

According to Fig. 13, when an untrained person is not able to interpret the audiovisual alerts of the robot, the results are as critical as the results shown for **F-3**. Since the human is not aware of the robot's presence/intention, then the human tends to get closer and closer, producing probabilities of human injury of almost 100% in the *worst* case for logistics, 90% for picking, and around 40% for UV-C treatment when the robot is moving along the footpaths. These results evidence the importance of properly implementing an AVFAS. The visual alerts may not be clear enough for untrained people, and voice messages are not always understandable for the pickers who may speak a different language than the one used in the prerecorded messages.

4.1.5. Human injuries due to robot detecting the humans only when they are too close (F-5)

According to Fig. 14, if the robot can detect people only when they are already closer than 3.6 m, then the consequences can produce human injuries of type **HI-2** with up to 21% for logistics and 16% for picking. Another important thing to highlight from the results

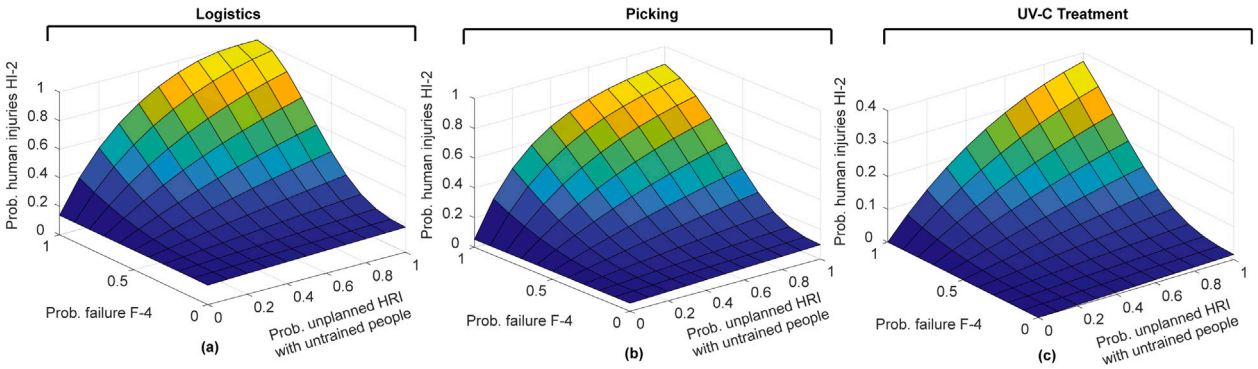

Fig. 13. Probability of human injury **HI-2** in the *ideal* case due to failure **F-4** during: (a) Logistics, (b) Picking, (c) UV-C treatment at footpaths.

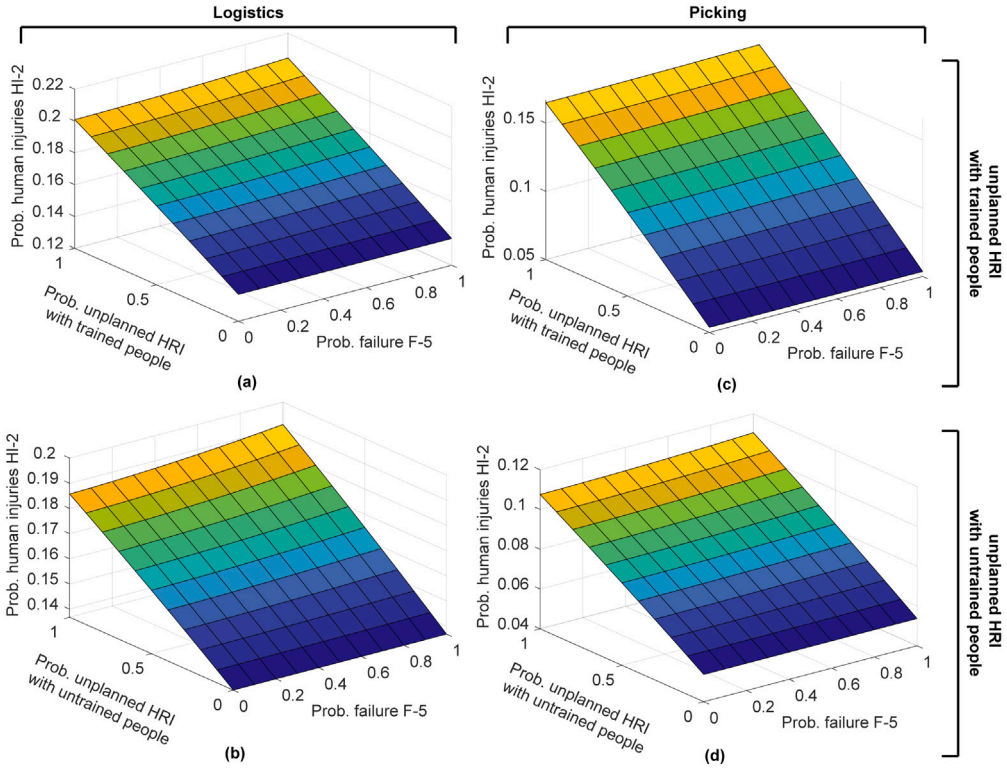

Fig. 14. Probability of human injury **HI-2** in the *ideal* case due to failure **F-5** during: (a,b) Logistics, (c,d) Picking. Evaluating different probabilities of having unplanned interaction with: (a,c) trained workers, (b,d) untrained people. See Section 3.1.4 for more information about the failure modes and human injuries evaluated here. See Section 3.1.4 for more information about the failure modes and human injuries evaluated here.

in Fig. 14 is that varying the probability of failure but keeping the same probability of having unplanned interactions produces almost no changes in the resulting injuries. This can be explained by the fact that when a human approaches the robot at the end of the rows, the AFVAS can still activate periodic alerts even if the HDS was not able to detect a human on time. Thus, even if the HDS performance at the end of the rows is bad, the periodic alerts of the AFVAS can keep the probability of human injuries almost the same as when the HDS is working properly.

4.1.6. Human injuries due to robot failing to track the human position (F-6)

According to Fig. 15, when the robot fails to track accurately the human's position during close interactions with untrained people, the resultant potential injuries **HI-2** probabilities are of up to 28%, 20% and 6% for logistics, picking and UV-C treatment respectively. The results for trained workers are very similar but slightly lower since the behavior of trained people is less unpredictable, making it easier to track it.

4.2. Assessment of potential human injuries due to UV-C light side effects

This subsection shows the probabilities of producing potential human injuries due to UV-C exposure denoted by **HI-1**. These potential injuries can be serious if the UV-C light is directly exposed to a human for a prolonged time, causing severe burns of the skin and eye injuries (photokeratitis) (Lucas et al., 2019).

See Sections 3.1.4 and 3.7 for more information about the human injury **HI-1**, and Table 1 for more information about the failure modes **F-4**, **F-5**, **F-7**, and **F-8**.

4.2.1. Human injuries due to human unable to interpret the audiovisual alerts (F-4)

According to Fig. 16(a), the consequences of having unplanned HRI with untrained people who cannot interpret the audiovisual alerts of the robot are really critical in terms of UV-C treatment. Since, under these conditions, the human is not aware of the danger, then they

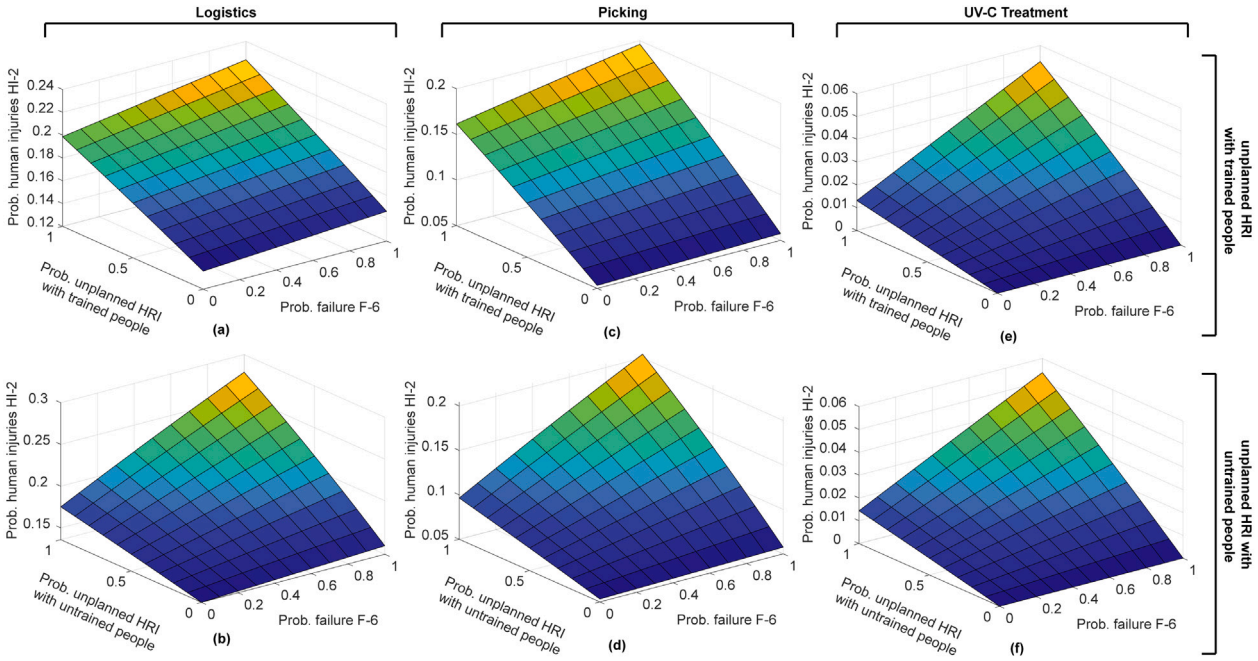

Fig. 15. Probability of human injury **HI-2** in the *ideal* case due to failure **F-6** during: (a,b) Logistics, (c,d) Picking, (e,f) UV-C treatment at footpaths. Evaluating different probabilities of having unplanned interaction with: (a,c,e) trained workers, (b,d,f) untrained people. See Section 3.1.4 for more information about the failure modes and human injuries evaluated here.

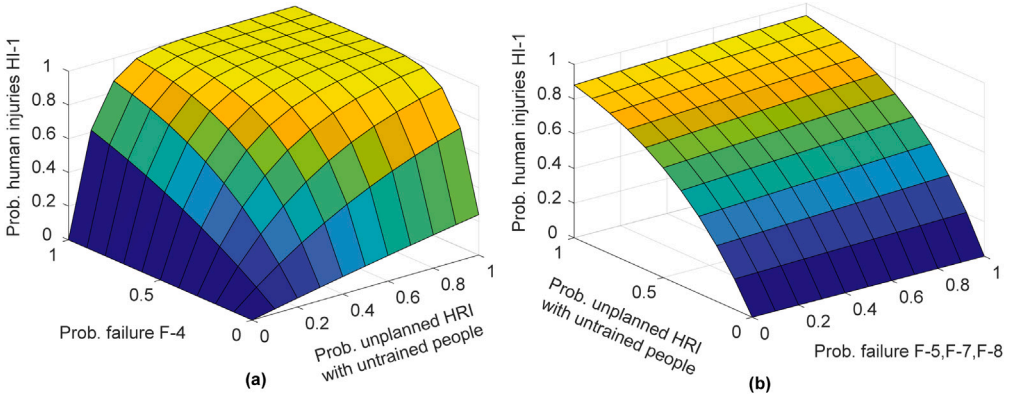

Fig. 16. Probability of human injury **HI-1** in an *ideal* case due to UV-C light side effects evaluating: (a) Failure **F-4**, (b) Failures **F-5**, **F-7** and **F-8**. See Section 3.1.4 for more information about the failure modes and human injuries evaluated here.

decide to get closer than 7 m from the robot to have a look at it, producing a probability of human injuries **HI-1** of almost 90% even when the probability of unplanned HRI is only 20%. This means that if the unplanned HRI probability is higher than 20% then the human injuries are basically unavoidable even if the overall safety system performance is *ideal* (according to probabilities in Table 14).

4.2.2. Human injuries due to robot failing to detect the human on time (F-5, F-7 and F-8)

According to Table 1, the failures in the HDS described in **F-5**, **F-7** and **F-8** can all produce human injuries **HI-1** where the severity of the consequences of each failure may be different due to the time of UV-C exposure. Despite this, the model implemented in PRISM was simplified to consider a potentially dangerous situation when a human gets closer than 7 m to the robot without considering the exposure time. Then, the consequences of the failures **F-5**, **F-7**, and **F-8** are equivalent and were treated as the same kind of failure for our analysis.

Thus, according to Fig. 16(b), if an unplanned HRI is going to happen with a 100% probability, then there is a probability of getting injured of almost 90% which remains constant independently of the probability of a failure in the HDS (**F-5**, **F-7**, or **F-8**). These results show the importance of ensuring that the polytunnel area is free of people during UV-C treatment. In this case, even by assuming that the overall safety system performance was *ideal*, the consequences of having unplanned HRI cannot be fully compensated. Thus, the only way for the safety system to attenuate the human injuries **HI-1** is by ensuring that the performance of the HDS and AVFAS is "virtually perfect" (0% probability of failure), but since this is not realistic, then the solution has to be addressed by changing the workspace usage policies and increasing the security on the field to control unauthorized access to polytunnels during UV-C treatment.

4.3. Summary of results for all cases

This subsection summarizes in Tables 3–5 the numerical results of testing all three cases (*ideal*, *regular*, and *worst*) of overall safety system performance. The results in these tables show the consequences of: (i) having or not unplanned HRI, (ii) having HRI with trained or untrained people, and (iii) having different failures. The columns "probability of unplanned HRI" and "probability of failure" have two levels being the

Table 3
Probabilities of human injuries (see Section 3.1.4) during UV-C treatment operations (see Section 2.1.3) due to failures in the safety system (see Table 1).

Scenario	Overall safety system performance	Human training level	Probability of unplanned HRI (%)	Probability of failure (%)	Probability of getting human injuries according to the failure evaluated (%)				
					HI-3	HI-2		HI-1	
					F-1	F-4	F-6	F-4	F-5,7,8
UV-C treatment	Ideal case[a]	Untrained	10	10	0.021	0.186	0.19	10.86	17.77
				100	0.21	6.581	0.566	61.25	20.75
			100	10	0.2	1.523	1.839	70.54	88.7
				100	2	37.37	5.385	100	92.98
		Trained	10	10	0.019	–	0.177	–	–
				100	0.19	–	0.557	–	–
			100	10	0.19	–	1.715	–	–
				100	1.9	–	5.299	–	–
	Regular case[a]	Untrained	10	10	0.072	0.486	0.46	17.23	27.36
				100	0.727	5.721	0.9	61.25	34.18
			100	10	0.679	4.495	4.24	87.73	97.92
				100	6.645	32.72	8.17	100	99.59
		Trained	10	10	0.068	–	0.427	–	–
				100	0.68	–	0.873	–	–
			100	10	0.638	–	3.962	–	–
				100	6.257	–	7.947	–	–
	Worst case[a]	Untrained	10	10	1.526	2.496	3.653	25.72	41
				100	7.44	8.879	4.22	61.25	47.68
			100	10	6.05	19.64	26.53	97.09	99.95
				100	48.22	46.5	30.14	100	99.99
		Trained	10	10	0.6	–	2.89	–	–
				100	5.97	–	3.46	–	–
			100	10	4.88	–	21.83	–	–
				100	41.33	–	25.67	–	–

[a] See Table 14 to know the transition probabilities used in each case.

10% lowest value and 100% as the highest value. The 10% was chosen as the minimum threshold instead of 0% just to show a more realistic numerical result. If interested anyways in the results of having 0% as the minimum probability of having unplanned HRI and/or failures, these results were shown graphically in Figs. 10–16, only for the *ideal* case.

4.4. UV-C treatment

Table 3 shows the probability of getting injuries of types **HI-1**, **HI-2** and **HI-3** according to the specific failure evaluated. The failures **F-2** and **F-3** are not evaluated in the UV-C treatment since those are failures related to farm workers, and it was established in **SP-8** that trained workers know that they cannot interact with robots inside the polytunnel during UV-C treatment.

As was expected, the highest probabilities of getting human injuries happen under the condition of 100% of probability of failure with 100% of probability of unplanned HRI with untrained people. In the *worst* case, the highest probability of getting human injuries reaches 48.22%, 46.5% and 100% for injuries of type **HI-3**, **HI-2** and **HI-1** respectively. In contrast, when comparing these results with the *ideal* case, the human injuries related to physical contact are almost negligible but the injuries due to UV-C light exposure remain as dangerous as in the *worst* case. This result demonstrates the importance of training everybody on the farm about the dangers of approaching a robot during UV-C treatment but also the importance of the AVFAS to alert untrained people of the danger in case the training fails.

4.4.1. Logistics and picking

Unlike for UV-C treatment, for logistics and picking, the failures **F-7** and **F-8** are not evaluated but the failures **F-2** and **F-3** are included instead. Thus, Tables 4–5, show probabilities of injuries of types **HI-2** and **HI-3** only.

According to these results, the probability of injury, when SCS fails during both logistics or picking, can reach above 90% in the *worst* case and around 20% in the *ideal* case. In general, the probabilities of getting human injuries during logistics operations have similar magnitudes but are always higher than when the robot is on picking operations. For instance, the probability of getting human injuries of type **HI-2** can reach 100% during logistics (due to **F-4**), but for picking the resultant probability is up to 92.35%. They both are really critical results, and the slight difference is due to in logistics the robot performs more two-way trips from polytunnel to the collection point, so the chances of having unplanned HRI are higher.

As was mentioned for UV-C treatment, mandatory training and proper AVFAS design are crucial factors to attenuate the consequences of **F-4**. Moreover, for logistics and picking, the HARS performance is another crucial factor to be considered since if **F-3** happens with 100% of probability, then it may produce human injuries of around 80% even in *ideal* conditions.

5. Discussion

5.1. Performance of the safety system under failure modes

The sensitivity analysis in Section 4 showed that by evaluating eight potential failures in the safety system, the probability of having human injuries even in *ideal* conditions may be 100%. These critical situations occur when the robot or the human is not aware of the intentions or actions of the other one. The latter means that it is crucial to ensure that only trained people are going to interact with the robot closely (in logistics and picking scenarios), in order to reduce the likelihood that the human is not aware of the robot's intentions, but also to ensure that people are not going to approach the robot in critical operations (during the UV-C treatment) since the human can get harmed by staying at 7 m from the robot for a long time.

Table 4
Probabilities of human injuries (see Section 3.1.4) during logistics operations (see Section 2.1.1) due to failures in the safety system (see Table 1).

Scenario	Overall safety system performance	Human training level	Probability of unplanned HRI (%)	Probability of failure (%)	Probability of getting human injuries according to the failure evaluated (%)					
					HI-3	HI-2				
					F-1	F-2	F-3	F-4	F-5	F-6
Logistics	Ideal case[a]	Untrained	10	10	1.681	14.15	–	14.16	14.19	14.2
				100	15.65	15.33	–	36.20	14.25	16.06
			100	10	2.255	18.21	–	18.3	18.59	18.61
				100	20.46	28.63	–	100	19.11	27.89
		Trained	10	10	1.7	14.3	14.35	–	14.35	14.35
				100	15.82	15.54	78.93	–	14.38	15.4
			100	10	2.45	19.68	20.11	–	20.10	20.11
				100	22.09	30.57	87.92	–	20.44	22.3
	Regular case[a]	Untrained	10	10	3.549	22.32	–	22.4	22.44	22.13
				100	30.56	23.74	–	37.73	22.78	25.14
			100	10	5.376	30.96	–	31.7	31.97	31.08
				100	42.73	42	–	100	35.12	40.8
		Trained	10	10	3.574	22.44	13.28	–	22.58	22.34
				100	30.74	24.05	69.71	–	22.88	24.7
			100	10	5.682	32.31	22.42	–	33.54	33.22
				100	44.58	44.73	81.93	–	36.18	37.92
	Worst case[a]	Untrained	10	10	27.27	54.67	–	52.89	55.08	53.77
				100	80.6	57.07	–	63.65	56.13	60.97
			100	10	31	82.54	–	73.97	83.7	83.82
				100	97.85	89.65	–	100	89.7	87.8
		Trained	10	10	27.21	54.51	42	–	54.96	53.62
				100	80.4	57.17	82.29	–	56.01	60.22
			100	10	51.75	81.18	77.39	–	82.29	81.72
				100	96.3	88.08	93.84	–	87.95	88.5

[a] See Table 14 to know the transition probabilities used on each case.

Table 5
Probabilities of human injuries (see Section 3.1.4) during picking operations (see Section 2.1.2) due to failures in the safety system (see Table 1).

Scenario	Overall safety system performance	Human training level	Probability of unplanned HRI (%)	Probability of failure (%)	Probability of getting human injuries according to the failure evaluated (%)					
					HI-3	HI-2				
					F-1	F-2	F-3	F-4	F-5	F-6
Picking	Ideal case[a]	Untrained	10	10	0.675	5.89	–	5.9	5.936	5.938
				100	6.578	7.176	–	29.13	5.966	7.365
			100	10	1.255	10.33	–	10.43	10.76	10.77
				100	11.9	21.75	–	88.11	11.04	20.41
		Trained	10	10	0.747	6.497	6.548	–	6.547	6.548
				100	7.252	7.85	48.59	–	6.567	7.232
			100	10	1.976	16.04	16.5	–	16.49	16.5
				100	18.16	27.44	80.42	–	16.65	19.61
	Regular case[a]	Untrained	10	10	1.485	9.826	–	9.927	9.983	9.768
				100	14	11.47	–	26.95	10.18	11.83
			100	10	3.348	19.86	–	20.71	21.17	20.12
				100	29.07	32.61	–	81.47	22.87	30.26
		Trained	10	10	1.629	10.71	6.466	–	10.9	10.73
				100	15.25	12.59	40.29	–	11.06	12.32
			100	10	4.798	27.72	20.33	–	29.19	28.55
				100	39.13	40.98	73.37	–	30.21	34.83
	Worst case[a]	Untrained	10	10	7.261	30.81	–	28.12	31.57	30.69
				100	53.93	34.41	–	43.73	32.31	35.19
			100	10	23.44	71.6	–	60.23	74.02	73.31
				100	93.97	80.97	–	92.35	76.24	78.16
		Trained	10	10	7.564	31.94	25.27	–	32.67	31.61
				100	55.35	35.6	54.19	–	33.37	36.88
			100	10	24.83	73.63	70.5	–	75.26	73.17
				100	92.98	80.67	87	–	76.62	83.33

[a] See Table 14 to know the transition probabilities used on each case.

Table 6
Metrics of PRISM model built for experiments.

Scenario modeled	Human training level	States	Transitions	Model construction time (s)	Property[a] verification time (s)		
					HI-1	HI-2	HI-3
UV-C treatment	Untrained	18 003	19 276	0.163	0.243	0.325	0.316
	Trained	11 561	12 371	0.097	0.001	0.161	0.156
Picking	Untrained	67 965	72 516	0.676	0.013	3.989	3.913
	Trained	155 035	165 501	1.586	0.014	5.144	4.944
Logistics	Untrained	94 265	100 376	0.909	0.011	7.852	8.183
	Trained	172 970	183 981	1.723	0.014	8.986	7.12

[a] See Section 3.7 for more information about the properties to verify.

Then, if there is always a chance of having unplanned interactions, a key factor in avoiding human injuries is designing and implementing an adequate audiovisual feedback system that alerts untrained people to the danger before they get closer. This system must include intuitive visual signals and explicit voice messages to make the robot's operation as transparent as possible for humans.

If these audiovisual alerts do not make the human move away, the last safety barrier relies on the robot's perception system. The perception includes human detection/tracking, collision detection, and action recognition, which performances are highly dependent on the sensors used and the capacity to process the sensor's data online.

The consequences of having failures in any of the components of the perception system vary between agricultural scenarios. For example, for logistics and picking, it is not very critical if the robot fails to detect people more than 3.6 m away, but it is more critical if the robot fails to track the position of people, or if the robot infers motion incorrectly or recognizes body gestures incorrectly. These failures during close interactions can lead to injuries (due to physical contact) with a probability of up to 93% in the *worst* case.

On the other hand, for UV-C treatment, tracking, motion inference, and gesture recognition are not even components required by the perception system, since only the early detection of people at distances greater than 7 m is required. However, even if detection within this distance range is assumed robust (up to 10% probability of failure), the potential injuries from exposure to UV-C light can still be around 41%, due to HRI with untrained people. In fact, in all cases evaluated in this work, it was assumed a non-perfect robot perception performance to make it realistic, and that is why there was always a chance of having human injuries. In theory, if the on-site training policy, audiovisual alerts, and robot perception accomplish their goals in conjunction, the probability of getting human injuries could be minimized.

5.2. Interpretation of resultant human injury probability

As mentioned at the beginning of Section 4, the resultant probabilities from the sensitivity analysis do not represent a metric to quantify the severity of human injuries after each HRI, but a metric to quantify the probability of having at least a human injury (independent of the severity). Then, taking as an example the results from Section 4.1.1, a probability of having human injuries of 20% means that one per every five times a robot operates in *picking mode*, it causes at least a human injury (unknown severity). This is of course unacceptable and alerts safety engineers that additional mitigation strategies need to be put in place to minimize it.

5.3. Granularity of the model

In this work, we used simplified models to describe the HRI and the agricultural tasks to be performed by the robots. Thus, it is important to mention that these simplifications do not reduce the validity of the proposed models to determine if a human injury occurred but may reduce the granularity of the output (i.e. injury severity level). The main limitation of the models used in this work is related to the assumptions used for modeling human injuries.

According to Section 3.1.4, **HI-2** and **HI-3** are hazards that represent physical human injuries where the severity level depends on the robot's motion state after the collision. Those are the only two levels of severity considered by the models proposed, however, if more realistic/complete results are needed, a more granular output that considers different robot speed levels before collision should be modeled. The same limitation is present in **HI-1** which is a hazard present during UV-C treatments, in the proposed models we consider a human to be injured at the moment a robot enters the 7 m safety threshold, however, to get a more realistic measure of the injury severity, it will be required to include in the modeling the distance and especially the time of being exposed to UV-C radiation.

As stated in Vicentini et al. (2020), as the model gets more complex, the formal verification tool needs more time to exhaustively explore the corresponding state-space, leading to the well-known state-space explosion issue of formal verification approaches. Thus, finding the right level of detail for models representing systems is an open issue, which inevitably involves using some level of abstraction.

Table 6 summarizes some metrics of the model built in PRISM that generated the results in Section 4. The table includes the number of states, number of transitions, time for model construction, and time for property verification for every scenario. It is important to highlight how the level of training (untrained vs trained) influences the size of the model built. Overall, the model did not require extensive computations, which means it can potentially be used for online formal verification. However, the number of states and transitions will increase according to the scale of the farming scenario modeled by the constants x_rows, $x\_segments$, x_runs and x_trays (see Section 3.3).

5.4. Scalability and versatility of the model

In the literature, models used for formal verification are usually very case-specific and may not be reused for applications of the same type (Askarpour et al., 2019). In this sense, in our work, the level of abstraction for modeling the agricultural tasks as a sequence of steps illustrated in Fig. 3, and the simplicity of state discretization of human, robot, and safety systems, allow the proposed model to be adapted to different applications/tasks within the agricultural domain. The results shown in Section 4.3 exemplify this statement since they all were generated by a single PRISM model file which describes three agricultural scenarios (UV-C treatment, picking, logistics). These scenarios share most of the variables, constants, and commands. The key differences between scenarios are the type of human injury being evaluated and the number of safety components in place. Depending on the agricultural scenario chosen for testing, one of the variables x_uvc, $x\_logistics$, and $x\_picking$ (described in Section 3.3) are used to only allow commands related to that particular scenario to be executed.

Finally, if a different application is being modeled, where there are additional safety requirements (e.g. additional components in the safety system), then the sequential approach to execute the model components (described in Section 3.8.5) allows easy adaptation and scalability.

Table 7
List of variables used to model the agricultural tasks (see Section 3.3).

Variable name	Initial value	Possible values	Description	Transitions					
				Previous values			Next values		
				UV-C	Logistics	Picking	UV-C	Logistics	Picking
x_uvc	0	0	Robot at the shed	3	–	–	1	–	–
		1	Robot moving from the shed to polytunnel	0	–	–	2	–	–
		2	Robot performing the UV-C treatment	1	–	–	3	–	–
		3	Robot moving from polytunnel to the shed	2	–	–	0	–	–
x_logistics x_picking	0	0	Robot at the shed	–	8		–	1	
		1	Robot moving from the shed to collection point to place empty trays on it	–	0		–	2	
		2	Robot interacting with the worker who load empty trays on it	–	1		–	3	
		3	Robot moving from collection point to polytunnel	–	2,7		–	4	
		4	Robot picking fruits along the rows or only moving inside the polytunnel	–	3,5	3	–	5	6
		5	Robot interacting with the worker who summoned it inside the polytunnel	–	4	–	–	4,6	–
		6	Robot moving from polytunnel to collection point to unload full trays	–	5	4	–	7	
		7	Robot interacting with the worker who unload full trays	–	6		–	8	
		8	Robot moving from collection point to robot shed	–	7		–	0	
x_runs	0	0,1,2, …	Number of times that the robot performed a two-way trip from polytunnel to the collection point	–	x_runs-1		–	x_runs+1	
		N_runs	The robot completed the maximum number of runs before the robot battery requires to be recharged	–	N_runs-1		–	0	
x_seg	0	0,1,2, …	Number of footpath segments traversed by the robot before reaching the goal point	N_seg-1			N_seg+1		
		N_seg_shed-N_seg_collect	The robot traversed all the footpaths segments between the shed and the collection point, assuming that N_seg_shed > N_seg_collect	N_seg_shed-N_seg_collect-1			N_seg_shed-N_seg_collect+1		0
		N_seg_shed	Robot traversed all the footpaths segments between the shed and the polytunnel	N_seg_shed-1				0	
		N_seg_collect	Robot traversed all the footpaths segments between the shed and the polytunnel	N_seg_collect-1			N_seg_collect+1		0
x_rows	0	0,1,2, …	Number of rows traversed by the robot	N_rows-1		–	N_rows+1		–
		N_rows	Robot covered all the rows in the polytunnel	N_rows-1			0		
x_trays	0	0,1,2, …	Number of times the robot replaced the trays	–	N_trays-1		–	N_trays+1	
		N_trays	All the trays on the robot are full of fruit		N_trays-1				0

5.5. Comparison with related work

As mentioned in Section 2.4 only a few existing works have addressed the safety analysis of human–robot collaboration scenarios by considering probabilistic model-checking approaches. Among those works, the approach in Gleirscher et al. (2022) is the closest one to our work. Similar to our work, the application, the robotic system, and human behavior are modeled as MDPs using PRISM as a probabilistic model-checking tool. However, in Gleirscher et al. (2022), the authors investigate what is the likelihood of accident-free operation under the control of a synthesized safety controller. Thus, their goal in the results analysis is to demonstrate the correctness of safety controllers under explicit conditions. In our case, the goal in the analysis of the results is not to verify the correctness of the proposed safety system

Table 8
List of constants used to define the scale of the agricultural tasks (see Section 3.3).

Constant name	Possible values	Description	Related to variable
N_rows	1,2,3, ...	Number of rows that the robot is able to cover before it has to come back to the robot shed to charge the battery	x_rows x_uvc
N_seg_shed	1,2,3, ...	Number of footpath segments required to be traversed when moving from robot shed to the polytunnel	x_seg x_uvc x_logistics x_picking
N_seg_collect	1,2,3, ...	Number of footpath segments required to be traversed when moving from collection point to the polytunnel	x_seg x_logistics x_picking
N_runs	1,2,3, ...	Number of times a robot can perform two-way trips from polytunnel to collection point before it has to come back to robot shed to charge the battery	x_runs x_logistics x_picking
N_trays	1,2,3, ...	Number of times a robot can place full trays on it before it has to come back to collection point to replace with empty trays	x_trays x_logistics x_picking

Table 9
List of values that the variable x_robot can take according to the agricultural scenario (see Section 3.4).

Variable name	Initial value	Possible values	Description	Transitions					
				Previous values			Next values		
				UV-C	Logistics	Picking	UV-C	Logistics	Picking
x_robot	0	0	Robot operation is paused (starting mode at the shed)	1	1	1	1	1	1
		1	Robot moving along footpaths	2	2	2	2,3,10	2,3,8,10	
		2	Robot performing a transition between footpath segments		1,9,10		1,3,10		
		3	Robot evading a human at footpaths		1,2		9,10		
		4	Robot moving along the row performing UV-C treatment	7	–	–	7,10	–	–
		5	Robot moving along a row transporting trays	–	7	–	–	7,8,10	–
		6	Robot moving along a row while picking fruits	–	–	7	–	–	7,10
		7	Robot performing a transition between rows	4,10	5,9,10	6,10	4,10	5,10	6,10
		8	Robot approaching to the worker position (reducing speed)	–	1,5		–	9,10	
		9	Robot moving away from the worker position	3	3,8		2,10	2,7,10	2,10
		10	Robot stops because of safety purposes		1,2, ...,8,9			2,7	

Table 10
List of variables used to model the safety system (see Section 3.5).

Variable name	Initial value	Possible values	Description	Transitions	
				Previous values	Next values
x_hds	0	0	No human detected	1	1,2,3,4
		1	Human detected when $d > 7$ m	0,2	0,2,3,4
		2	Human detected when 3.6 m$\leq d \leq$ 7 m	0,1,3	1,3
		3	Human detected when 1.2 m$< d <$ 3.6 m	0,1,2,4	2,4
		4	Human detected when 0 m$< d \leq$ 1.2 m	0,1,2,3	3
x_htmis	0	0	No human tracked	1,2	1[a],2[a]
		1	Accurate human motion inference	0	0
		2	Not reliable human motion inference	0	0
x_hars	0	0	No human gesture detected	1,2	1[a],2[a]
		1	Correct human gesture/action recognition	0	0
		2	Wrong human gesture/action recognition	0	0
x_scs	0	0	No contact	1,2	1[a],2[a]
		1	Collision is detected	0	0
		2	Collision is not detected on time	0	0
x_visual x_voice	0	0	Audiovisual alerts are not activated	1,2	1,2[a]
		1	Audiovisual indicators are activated when a human is detected	0,2	0
		2	Periodic audiovisual indicators are activated (even when there is not a human detected)	0	0,1

[a] Probabilistic transition (see Table 11).

(taken from Guevara et al. (2023)), but to perform a sensitivity analysis that shows the consequences of explicit conditions (failure modes) translated into probabilities of human injuries.

Most of the studies on safety for human–robot collaboration including Zacharaki et al. (2021) and Vicentini et al. (2020) have focused on manufacturing settings which, unlike agricultural settings, are more structured and have well-established safety standards and regulations. Moreover, as mentioned in Section 5.4, most of the existing works use models that are case-specific and are not suited to be re-used even for applications of the same type. Here we have illustrated that the same modeling abstraction level can be used for different applications within the agricultural domain.

6. Conclusions

This paper has discussed the use of a probabilistic model-checking tool, in particular PRISM, to provide a theoretical assessment of the probability of human injuries occurring during planned and unplanned

Table 11
List of constants used to define the probability of failure of each safety system component (see Section 3.5).

Constant name	Possible values	Description	Related to variable
p_alerts	[0,1]	Probability that at this specific moment a periodic audiovisual alert is activated to warn nearby human about danger	x_visual x_voice
p_scs	[0,1]	Probability that the SCS fails to detect a collision	x_scs
p_hds_1	[0,1]	Probability that HDS fails in detect a human in the same row farther than 7 m	x_hds
p_hds_2	[0,1]	Probability that HDS fails in detect on time a human at 7 m in the same row	
p_hds_3	[0,1]	Probability that HDS fails in detect on time a human at 3.6 m in the same row	
p_hds_4	[0,1]	Probability that HDS fails in detect on time a human at 1.2 m in the same row	
p_hds_5	[0,1]	Probability that HDS fails in detect a human at the end of the rows farther 7 m when the robot is going to perform row transitions	
p_hds_6	[0,1]	Probability that HDS fails in detect on time a human at the end of the row at 7 m when the robot is going to perform row transitions	
p_hds_7	[0,1]	Probability that HDS fails in detect on time a human at the end of the row at 3.6 m when the robot is going to perform row transitions	
p_hds_8	[0,1]	Probability that HDS fails in detect on time a human at the end of the row at 1.2 m when the robot is going to perform row transitions	
p_hds_9	[0,1]	Probability that HDS fails in detect a human on time in the same footpath above 3.6 m	
p_hds_10	[0,1]	Probability that HDS fails in detect a human on time in the same footpath at 3.6 m	
p_hds_11	[0,1]	Probability that HDS fails in detect a human on time in the same footpath at 1.2 m	
p_htmis_1	[0,1]	Probability that HTMIS fails to track accurately a human in the same row	x_htmis
p_htmis_2	[0,1]	Probability that HTMIS fails to track accurately a human in the same footpath	
p_hars	[0,1]	Probability that the HARS fails to detect the correct hand gesture	x_hars

Table 12
List of variables used to model the human behavior (see Section 3.6).

Variable name	Initial value	Possible values	Description	Transitions	
				Previous values	Next values
x_human	0	0	No human presence	1,2	1[a],2[a]
		1	Untrained human is interacting with the robot	0	0
		2	Trained human is interacting with the robot	0	0
x_human_motion	0	0	Human stays stationary	0,1,2	1,2[a],3[a],4[a]
		1	Human is moving to the robot position	0	0[a],2[a]
		2	Human is moving away from the robot position	0,1,3,4	0
		3	Human approaching to the robot to place trays on it	0	2
		4	Human walking next to the robot along the footpath	0	2
x_human_aware	0	0	Human is not aware of robot presence or potential danger of approaching to the robot	1	1[a]
		1	Human is aware of robot intentions or danger of approaching to the robot	0	0
x_human_gesture	0	0	Human is not performing any specific body gesture	1	1[a]
		1	Human performing a body gesture to make the robot knows about his/her intentions	0	0
x_human_distance	0	0	$d >> 7$ m	1	1
		1	$d > 7$ m	0,2	0,2
		2	3.6 m $\leq d \leq$ 7 m	1,3	1,3
		3	1.2 m $< d <$ 3.6 m	2,4	2,4
		4	0 m $< d \leq$ 1.2 m	3,5	3,5
		5	$d = 0$ m	4	4

[a] Probabilistic transition (see Table 13).

Table 13
List of constants used to model the probabilistic human behavior (see Section 3.6).

Constant name	Possible values	Description	Related to variable
p_int_1	[0,1]	Probability that an unplanned interaction is going to happen inside the polytunnels with an untrained person	x_human
p_int_2	[0,1]	Probability that an unplanned interaction is going to happen inside the polytunnels with an trained person	
p_int_3	[0,1]	Probability that an unplanned interaction is going to happen outside the polytunnels with an untrained person	
p_int_4	[0,1]	Probability that an unplanned interaction is going to happen outside the polytunnels with an trained person	
p_aware_1	[0,1]	Probability that visual alerts are correctly interpreted by untrained people	x_aware
p_aware_2	[0,1]	Probability that visual alerts are correctly interpreted by trained people	
p_aware_3	[0,1]	Probability that voice alerts are correctly interpreted by trained and untrained people	
p_decision	[0,1]	Probability that the human decides to perform a risky movement or not	x_motion
p_reply	[0,1]	Probability that the human performs or not a body gesture to make the robot knows about his/her intentions	x_gesture

Table 14
Values of the constants (used as probabilities of transition) that were chosen to characterize the three cases tested (*ideal*, *regular*, and *worst*) in the Section 4.

Model component	Constant name	Values for specific cases evaluated		
		Ideal case	Regular case	Worst case
Safety system	p_hds_1	0.3	0.4	0.5
	p_hds_2	0.2	0.3	0.4
	p_hds_3	0.1	0.2	0.3
	p_hds_4	0.1	0.1	0.2
	p_hds_5	0.3	0.4	0.5
	p_hds_6	0.2	0.3	0.4
	p_hds_7	0.1	0.2	0.3
	p_hds_8	0.1	0.1	0.2
	p_hds_9	0.2	0.3	0.4
	p_hds_10	0.1	0.2	0.3
	p_hds_11	0.1	0.1	0.2
	p_htmis_1	0.1	0.2	0.3
	p_htmis_2	0.1	0.2	0.3
	p_hars	0.1	0.2	0.3
	p_alerts	0.9	0.7	0.5
	p_scs	0.1	0.3	0.5
Human behavior	p_int_1		0,0.1,0.2,...,0.9,1	
	p_int_2		0,0.1,0.2,...,0.9,1	
	p_int_3		0,0.1,0.2,...,0.9,1	
	p_int_4		0,0.1,0.2,...,0.9,1	
	p_aware_1	0.8	0.7	0.5
	p_aware_2	0.9	0.8	0.5
	p_aware_3	0.9	0.9	0.5
	p_decision	0.9	0.8	0.5
	p_reply	0.9	0.8	0.5

See Tables 11 and 13 for more information about the constants listed here.

HRI in four specific agricultural scenarios, focusing on the consequences of failures in unreliable robot safety systems. The paper illustrated how by performing a sensitivity analysis, the safety engineers can obtain metrics to evaluate how reliable their safety system architectures are and based on those preliminary results, make changes accordingly before implementation in the real robots. Moreover, the results demonstrated that minimizing the probability of human injuries depends not only on the performance and reliability of the technology within the safety system but also on in-site safety policies to ensure no human errors. For instance, one of the agricultural scenarios evaluated was the UV-C treatment, where no humans are allowed to interact closely with robots. In this scenario, the human injury assessment demonstrated that an agricultural robot with a robust human perception system (up to 10% probability of failure) can still harm untrained people (from exposure to UV-C light) with a probability of around 41%. Thus, the only way to minimize the chances of producing human injuries in these safety-critical applications is to ensure that only trained people interact with agricultural robots, which is part of the in-site safety policies.

Finally, although the model-checking analysis presented here uses simplified probabilistic models that are limited in granularity level, their advantages include easily adapting to multiple scenarios and being able to be used for online formal verification. If used for online model-checking analysis, then the number of state transitions in the model will be reduced due to requiring a shorter prediction time window, and the probabilities of failures should not come from a sensitivity analysis but must be extracted from real-time robot sensing data such as the level of noise in human detection/tracking readings. The online model-checking analysis is going to be addressed in future work.

CRediT authorship contribution statement

Leonardo Guevara: Writing – original draft, Visualization, Validation, Software, Investigation, Formal analysis, Data curation, Conceptualization. **Muhammad Khalid:** Writing – review & editing, Resources, Investigation. **Marc Hanheide:** Supervision, Methodology, Conceptualization. **Simon Parsons:** Writing – review & editing, Supervision, Project administration, Funding acquisition.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Marc Hanheide owns shares in SAGA Robotics who manufactures the Thorvald II robot used in the research described in the paper and delivers autonomous services for the soft-fruit agricultural industry.

Data availability

No data was used for the research described in the article.

Appendix

See Tables 7–14.

References

Al-Hussaini, S., Gregory, J.M., Guan, Y., Gupta, S.K., 2020. Generating alerts to assist with task assignments in human-supervised multi-robot teams operating in challenging environments. In: 2020 IEEE/RSJ International Conference on Intelligent Robots and Systems. IROS, IEEE, pp. 11245–11252.

Araújo, R., Mota, A., Nogueira, S., 2017. Analyzing cleaning robots using probabilistic model checking. In: International Conference on Information Reuse and Integration. Springer, pp. 23–51.

Askarpour, M., Mandrioli, D., Rossi, M., Vicentini, F., 2019. Formal model of human erroneous behavior for safety analysis in collaborative robotics. Robot. Comput.-Integr. Manuf. (ISSN: 0736-5845) 57, 465–476. http://dx.doi.org/10.1016/j.rcim.2019.01.001.

Banjanović-Mehmedović, L., Gurdić, A., 2021. Collaborative service robots: Challenges, paradigms and applications. Serv. Robot.: Adv. Res. Appl. 139–163.

Bengtsson, J., Larsen, K., Larsson, F., Pettersson, P., Yi, W., 1996. UPPAAL—a tool suite for automatic verification of real-time systems. In: Proceedings of the DIMACS/SYCON Workshop on Hybrid Systems III: Verification and Control: Verification and Control. Springer-Verlag, Berlin, Heidelberg, ISBN: 354061155X, pp. 232–243.

Bolton, M.L., Molinaro, K.A., Houser, A.M., 2019. A formal method for assessing the impact of task-based erroneous human behavior on system safety. Reliab. Eng. Syst. Saf. (ISSN: 0951-8320) 188, 168–180. http://dx.doi.org/10.1016/j.ress.2019.03.010.

Bolton, M.L., Zheng, X., Kang, E., 2021. A formal method for including the probability of erroneous human task behavior in system analyses. Reliab. Eng. Syst. Saf. (ISSN: 0951-8320) 213, 107764. http://dx.doi.org/10.1016/j.ress.2021.107764.

Cheng, R., Cheng, Y., Chen, D., Song, H., 2021. Online quantitative safety monitoring approach for unattended train operation system considering stochastic factors. Reliab. Eng. Syst. Saf. (ISSN: 0951-8320) 216, 107933. http://dx.doi.org/10.1016/j.ress.2021.107933, URL: https://www.sciencedirect.com/science/article/pii/S095183202100449X.

Chi, C.-F., Sigmund, D., Astardi, M.O., 2020. Classification scheme for root cause and failure modes and effects analysis (FMEA) of passenger vehicle recalls. Reliab. Eng. Syst. Saf. (ISSN: 0951-8320) 200, 106929. http://dx.doi.org/10.1016/j.ress.2020.106929.

Cimatti, A., Clarke, E., Giunchiglia, E., Giunchiglia, F., Pistore, M., Roveri, M., Sebastiani, R., Tacchella, A., 2002. NuSMV 2: An OpenSource tool for symbolic model checking. In: Brinksma, E., Larsen, K.G. (Eds.), Computer Aided Verification. Springer Berlin Heidelberg, Berlin, Heidelberg, ISBN: 978-3-540-45657-5, pp. 359–364.

Cirillo, A., Ficuciello, F., Natale, C., Pirozzi, S., Villani, L., 2016. A conformable force/tactile skin for physical human–robot interaction. IEEE Robot. Autom. Lett. 1 (1), 41–48. http://dx.doi.org/10.1109/LRA.2015.2505061.

Dakwat, A.L., Villani, E., 2018. System safety assessment based on STPA and model checking. Saf. Sci. (ISSN: 0925-7535) 109, 130–143. http://dx.doi.org/10.1016/j.ssci.2018.05.009.

Fan, T., Long, P., Liu, W., Pan, J., 2020. Distributed multi-robot collision avoidance via deep reinforcement learning for navigation in complex scenarios. Int. J. Robot. Res. 39 (7), 856–892.

Gadoury, D.M., 2021. The potential of ultraviolet light to suppress grapevine powdery mildew. Progress. Crop Consult. 38–44.

Gleirscher, M., Calinescu, R., Douthwaite, J., Lesage, B., Paterson, C., Aitken, J., Alexander, R., Law, J., 2022. Verified synthesis of optimal safety controllers for human-robot collaboration. Sci. Comput. Program. (ISSN: 0167-6423) 218, 102809. http://dx.doi.org/10.1016/j.scico.2022.102809.

Grimstad, L., From, P.J., 2018. Software Components of the Thorvald II Modular Robot. Model. Identif. Control 39 (3), 157–165. http://dx.doi.org/10.4173/mic.2018.3.2.

Guettari, M., Gharbi, I., Hamza, S., 2021. UVC disinfection robot. Environ. Sci. Pollut. Res. 28 (30), 40394–40399.

Guevara, L., Hanheide, M., Parsons, S., 2023. Implementation of a human-aware robot navigation module for cooperative soft-fruit harvesting operations. J. Field Robotics 1–31. http://dx.doi.org/10.1002/rob.22227.

Guevara, L., Rocha, R.P., Cheein, F.A., 2021. Improving the manual harvesting operation efficiency by coordinating a fleet of N-trailer vehicles. Comput. Electron. Agric. (ISSN: 0168-1699) 185, 106103. http://dx.doi.org/10.1016/j.compag.2021.106103.

Guha, S., Nag, A., Karmakar, R., 2021. Formal verification of safety-critical systems: A case-study in airbag system design. In: Intelligent Systems Design and Applications. Springer International Publishing, Cham, ISBN: 978-3-030-71187-0, pp. 107–116.

Hall, A.M., Jin, X., 2017. Integrated control of strawberry powdery mildew. Acta Hortic. 1156, 771–776.

Herrera, D., Monllor, M., Santiago, D., Roberti, F., Carelli, R., 2017. Null-space based control for human following and social field avoidance. In: 2017 XVII Workshop on Information Processing and Control. RPIC, pp. 1–6. http://dx.doi.org/10.23919/RPIC.2017.8214358.

Hou, Y.C., Mohamed Sahari, K.S., Weng, L.Y., Foo, H.K., Abd Rahman, N.A., Atikah, N.A., Homod, R.Z., 2020. Development of collision avoidance system for multiple autonomous mobile robots. Int. J. Adv. Robot. Syst. 17 (4), 1729881420923967.

Huck, T.P., Münch, N., Hornung, L., Ledermann, C., Wurll, C., 2021. Risk assessment tools for industrial human-robot collaboration: Novel approaches and practical needs. Saf. Sci. (ISSN: 0925-7535) 141, 105288. http://dx.doi.org/10.1016/j.ssci.2021.105288.

International Organization for Standardization, 2015. ISO-13489 Safety of Machinery - Safety-related parts of control systems - Part 1: General principles of design.

International Organization for Standardization, 2018a. ISO-10218 Robots and Robotic Devices - Safety requirements for industrial robots - Part 1: Robots.

International Organization for Standardization, 2018b. ISO-18497 Agricultural machinery and tractors - Safety of highly automated agricultural machines - Principles for design.

Islam, M.J., Hong, J., Sattar, J., 2019. Person-following by autonomous robots: A categorical overview. Int. J. Robot. Res. 38 (14), 1581–1618.

Kirk, R., Cielniak, G., Mangan, M., 2020. L*a*b*Fruits: A rapid and robust outdoor fruit detection system combining bio-inspired features with one-stage deep learning networks. Sensors (ISSN: 1424-8220) 20 (1), http://dx.doi.org/10.3390/s20010275.

Kwiatkowska, M., Norman, G., Parker, D., 2011. PRISM 4.0: Verification of probabilistic real-time systems. In: Gopalakrishnan, G., Qadeer, S. (Eds.), Proc. 23rd International Conference on Computer Aided Verification. CAV'11, In: LNCS, Vol. 6806, Springer, pp. 585–591.

Kwiatkowska, M., Norman, G., Parker, D., Santos, G., 2020. PRISM-games 3.0: Stochastic game verification with concurrency, equilibria and time. In: International Conference on Computer Aided Verification. Springer, pp. 475–487.

Lacerda, B., Faruq, F., Parker, D., Hawes, N., 2019. Probabilistic planning with formal performance guarantees for mobile service robots. Int. J. Robot. Res. 38 (9), 1098–1123. http://dx.doi.org/10.1177/0278364919856695.

Liang, Q., Yang, Y., Zhang, H., Peng, C., Lu, J., 2022. Analysis of simplification in Markov state-based models for reliability assessment of complex safety systems. Reliab. Eng. Syst. Saf. (ISSN: 0951-8320) 221, 108373. http://dx.doi.org/10.1016/j.ress.2022.108373.

Liu, M., Zhou, L., Sun, Y., Liu, J., 2019. Robot comfort following based on extended social force model in dynamic environment. In: 2019 IEEE 9th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems. CYBER, pp. 30–35. http://dx.doi.org/10.1109/CYBER46603.2019.9066624.

Lu, Y., Peng, Z., Miller, A.A., Zhao, T., Johnson, C.W., 2015. How reliable is satellite navigation for aviation? Checking availability properties with probabilistic verification. Reliab. Eng. Syst. Saf. (ISSN: 0951-8320) 144, 95–116. http://dx.doi.org/10.1016/j.ress.2015.07.020.

Lucas, R., Yazar, S., Young, A., Norval, M., De Gruijl, F., Takizawa, Y., Rhodes, L., Sinclair, C., Neale, R., 2019. Human health in relation to exposure to solar ultraviolet radiation under changing stratospheric ozone and climate. Photochem. Photobiol. Sci. 18 (3), 641–680.

Mayoral, J.C., From, P.J., Cielniak, G., 2023. Towards safe robotic agricultural applications: Safe navigation system design for a robotic grass-mowing application through the risk management method. Robotics (ISSN: 2218-6581) 12 (3), http://dx.doi.org/10.3390/robotics12030063, URL: https://www.mdpi.com/2218-6581/12/3/63.

Mayoral, J.C., Grimstad, L., From, P.a.J., Cielniak, G., 2021. Integration of a human-aware risk-based braking system into an open-field mobile robot. In: 2021 IEEE International Conference on Robotics and Automation. ICRA, pp. 2435–2442. http://dx.doi.org/10.1109/ICRA48506.2021.9561522.

Mazzeo, G., Coppolino, L., D'Antonio, S., Mazzariello, C., Romano, L., 2018. SIL2 assessment of an active/standby COTS-based safety-related system. Reliab. Eng. Syst. Saf. (ISSN: 0951-8320) 176, 125–134. http://dx.doi.org/10.1016/j.ress.2018.04.009.

Ozkan, M., Demirci, Z., Aslan, Ö., Yazı cı, A., 2023. Safety verification of multiple industrial robot manipulators with path conflicts using model checking. Machines (ISSN: 2075-1702) 11 (2), http://dx.doi.org/10.3390/machines11020282, URL: https://www.mdpi.com/2075-1702/11/2/282.

Parsa, S., Debnath, B., Khan, M.A., E., A.G., 2023. Modular autonomous strawberry picking robotic system. J. Field Robotics http://dx.doi.org/10.1002/rob.22229.

Peng, C., Vougioukas, S.G., 2020. Deterministic predictive dynamic scheduling for crop-transport co-robots acting as harvesting aids. Comput. Electron. Agric. (ISSN: 0168-1699) 178, 105702. http://dx.doi.org/10.1016/j.compag.2020.105702.

Ravikanna, R., Heselden, J., Khan, M.A., Perrett, A., Zhu, Z., Das, G., Hanheide, M., 2023. Smart parking system using heuristic optimization for autonomous transportation robots in agriculture. In: Towards Autonomous Robotic Systems. Springer Nature Switzerland, ISBN: 978-3-031-43360-3, pp. 38–50. http://dx.doi.org/10.1007/978-3-031-43360-3_4.

Robla-Gómez, S., Becerra, V.M., Llata, J.R., González-Sarabia, E., Torre-Ferrero, C., Pérez-Oria, J., 2017. Working together: A review on safe human-robot collaboration in industrial environments. IEEE Access 5, 26754–26773. http://dx.doi.org/10.1109/ACCESS.2017.2773127.

Sun, L., Li, Y.-F., Zio, E., 2021. Comparison of the HAZOP, FMEA, FRAM, and STPA methods for the hazard analysis of automatic emergency brake systems. ASCE-ASME J. Risk Uncertain. Eng. Syst. B: Mech. Eng. 8 (3), 031104.

The Daily Mail, 2021. Britain's far-flung army of fruit-pickers: How 16,000 workers flew in for 2021 season from 37 countries including Barbados, Nepal, Tajikistan and Kenya. URL: https://www.dailymail.co.uk/news/article-9982957/UKs-far-flung-army-fruit-pickers-16-000-workers-flew-2021-season-37-countries.html. (Accessed 23 April 2022).

Unhelkar, V.V., Lasota, P.A., Tyroller, Q., Buhai, R.-D., Marceau, L., Deml, B., Shah, J.A., 2018. Human-aware robotic assistant for collaborative assembly: Integrating human motion prediction with planning in time. IEEE Robot. Autom. Lett. 3 (3), 2394–2401.

Vasconez, J., Admoni, H., Auat Cheein, F., 2021. A methodology for semantic action recognition based on pose and human-object interaction in avocado harvesting processes. Comput. Electron. Agric. (ISSN: 0168-1699) 184, 106057. http://dx.doi.org/10.1016/j.compag.2021.106057.

Vásconez, J.P., Auat Cheein, F.A., 2022. Workload and production assessment in the avocado harvesting process using human-robot collaborative strategies. Biosyst. Eng. (ISSN: 1537-5110) 223, 56–77. http://dx.doi.org/10.1016/j.biosystemseng.2022.08.010.

Vasconez, J.P., Guevara, L., Cheein, F.A., 2019. Social robot navigation based on HRI non-verbal communication: A case study on Avocado Harvesting. In: Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing. SAC '19, Association for Computing Machinery, New York, NY, USA, ISBN: 9781450359337, pp. 957–960. http://dx.doi.org/10.1145/3297280.3297569.

Vicentini, F., Askarpour, M., Rossi, M.G., Mandrioli, D., 2020. Safety assessment of collaborative robotics through automated formal verification. IEEE Trans. Robot. 36 (1), 42–61. http://dx.doi.org/10.1109/TRO.2019.2937471.

Wang, X.V., Wang, L., 2021. Safety strategy and framework for human–robot collaboration. In: Wang, L., Wang, X.V., Váncza, J., Kemény, Z. (Eds.), Advanced Human-Robot Collaboration in Manufacturing. Springer International Publishing, Cham, ISBN: 978-3-030-69178-3, pp. 69–87. http://dx.doi.org/10.1007/978-3-030-69178-3_3.

Xin, X., Keoh, S.L., Sevegnani, M., Saerbeck, M., 2022. Run-time probabilistic model checking for failure prediction: A smart lift case study. In: 2022 IEEE 8th World Forum on Internet of Things (WF-IoT). IEEE, pp. 1–7.

Zacharaki, A., Kostavelis, I., Dokas, I., 2021. Decision making with STPA through Markov decision process, a theoretic framework for safe human-robot collaboration. Appl. Sci. (ISSN: 2076-3417) 11 (11), http://dx.doi.org/10.3390/app11115212, URL: https://www.mdpi.com/2076-3417/11/11/5212.

Zhao, X., Robu, V., Flynn, D., Dinmohammadi, F., Fisher, M., Webster, M., 2019. Probabilistic model checking of robots deployed in extreme environments. In: Proceedings of the AAAI Conference on Artificial Intelligence. Vol. 33, pp. 8066–8074.

Zhou, H., Wang, X., Au, W., Kang, H., Chen, C., 2022. Intelligent robots for fruit harvesting: Recent developments and future challenges. Precis. Agric. 23 (5), 1856–1907. http://dx.doi.org/10.1007/s11119-022-09913-3.