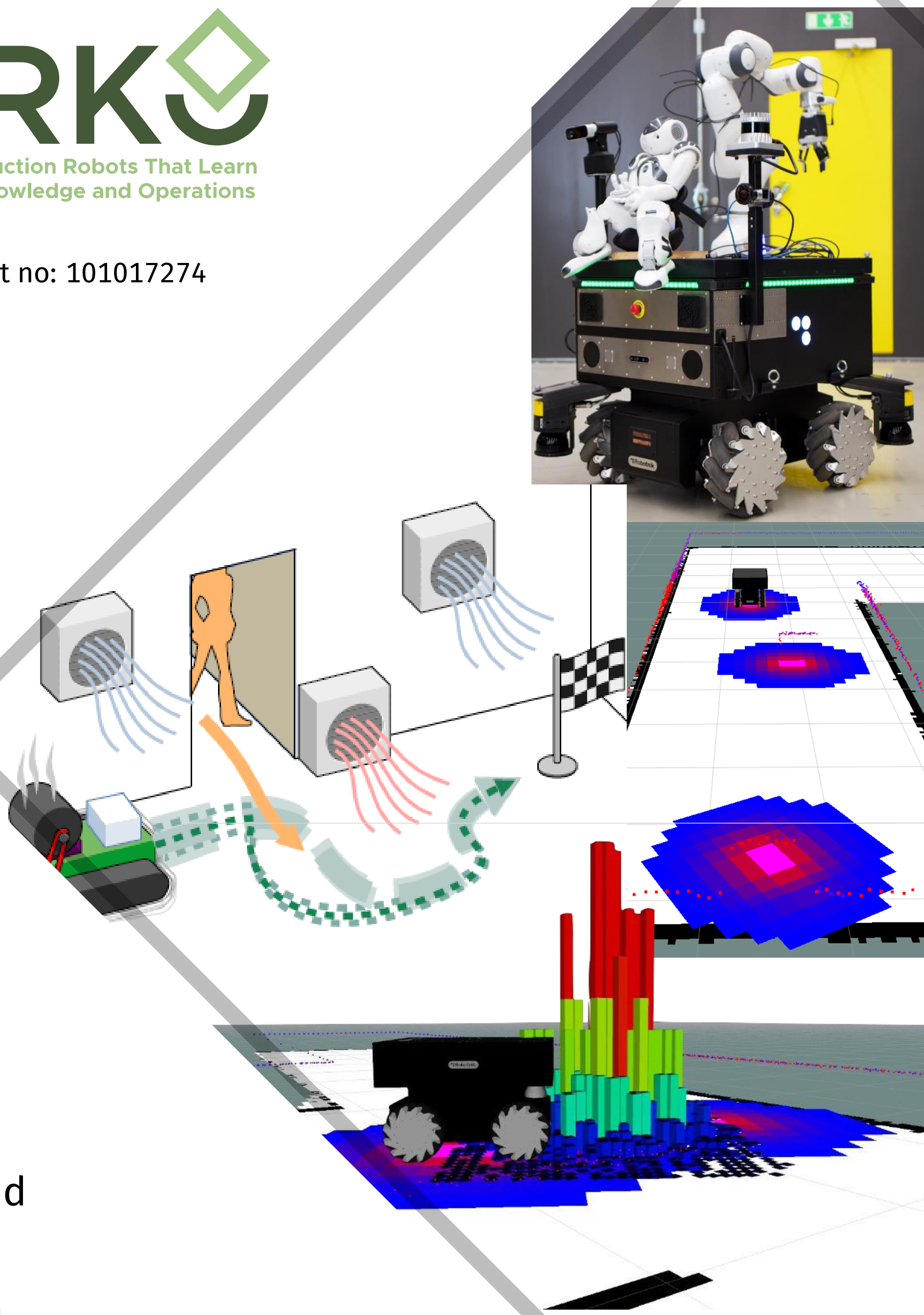
DARKO

Dynamic Agile Production Robots That Learn and Optimise Knowledge and Operations

H2020-ICT-2020-2 Grant agreement no: 101017274



DELIVERABLE 7.1

Risk-space modelling and assessment metrics

Dissemination Level: PUBLIC

Due date: month 19 (July 2022)

Deliverable type: Report

Lead beneficiary: UNIPI

1 Introduction

This deliverable reports results of the works carried on within WP7, in particular within T7.1, for the formal definition of a multi-dimensional risk space able to characterize autonomous agents, the environment in which they strive, and their possibly dynamic relationship, so to endow such agents with a keen sensitivity to uncertainty and to the risk of failure. We break-down such a multi-dimensional risk space into factors, classifying the autonomous agent current state based on the severity and probability of undesired outcomes (hazardous states). Therefore, we analyse how each of these factors relates to the variables defining the state of a robot, to identify the main factors that will serve to introduce a method for the quantification of the risk level.

The described methodology, based on a fuzzy definition of risk levels, outlines a general way to characterize risk for autonomous agents working in unstructured and partially unknown environments, which generalizes to most human-robot collaboration scenarios. The proposed framework is also robust to the introduction of new risk factors.

To apply the outlined methodology to the concrete case study of the DARKO demo scenario, we collect the potential hazards from the output of WP8 reported in D8.1 and group the most relevant risks into categories. The identification of the various risk factors leads to the definition of the dimensions of the multi-dimensional risk space. Then, an analysis of the variables on which each individual risk source may depend leads to the introduction of a fuzzy inference system to quantify the risk level in the particular case study. At the end of each step, we show a comparison with what is prescribed by international standards dealing with risk assessments and risk mitigation.

This work will serve as the main input for T7.2, which would implement a continuous learning approach to identify the most suitable parameter values for the fuzzy inference system proposed in this deliverable. The knowledge of the potential risks of the environment and of the risk map, which will be produced by the union of this work with the outcomes of T7.2, will therefore be used in T6.2 and T6.4 to implement safe and risk-aware motion planning algorithms for mobile and wheeled robots and in T4.2 for safe and risk-aware planning and control for manipulation. The developed risk map will also be used in T7.3 to guide the optimization of tasks planning and temporal scheduling.

The rest of this document is organized as follows. Section 2 reports the general outline of the proposed methodology. Section 3, briefly reports the definition of the demo scenario, as defined in deliverable D8.1, on which we will perform the risk assessment operation. Section 4 identifies the main risks involved in the demo scenario. Section 5 defines the dynamic risk assessment metrics, formalizes the metrics to map the robot state into the risk space, and defines a global risk function to represent the overall level of risk. Finally, Section 6 concludes the report by showing the main results and discussing future developments.

2 Methodology

This work aims to define the theoretical foundation of the DARKO approach for dynamic risk management. To achieve this result, we consider the state-of-the-art by following the steps of a risk management process.

Definition 1: According to Baloi and Price [3] risk is the likelihood of a detrimental event occurring to the project. In the literature, there are other definitions of risk, but there are several characteristics commonly found in all definitions of risk [4]:

- A risk is a future event that may or may not occur.

- Risk must also be an uncertain event or condition that, if it occurs, has an effect on, at least, one of the project objectives, such as scope, schedule, cost, or quality.
- The probability of the future event occurring must be greater than 0% but less than 100%. Future events that have a zero or 100% chance of occurrence are not risks.
- The impact or consequence of the future event must be unexpected or unplanned.

Normative ISO 31000 [9] provides general principles and guidelines for effective risk management and it presents a general approach to risk management that may be applied to various risks (financial, safety, and project risks). The main steps of a risk management process are [15]:

- *Risks identification*: The process of determining which risks may affect the project and documenting their characteristics.
- *Risk assessment*: The process of prioritizing risks for further analysis by assessing and combining, generally, their probability of occurrence and impact.
- *Risk response*: The process of developing options and actions to enhance opportunities and reduce threats to the project objectives.
- *Risk monitoring and review*: The process of implementing a risk response plan, tracking identified risks, monitoring residual risks, identifying new risks, and evaluating the risk process effectiveness throughout the project.

These steps are preceded by the "Establish the context" step. In ISO 31000 establishing the context means defining the purpose of the risk management process, defining the organization's objectives, and establishing the risk evaluation criteria.

This deliverable will deal with the first two points (risks identification and risks assessment) for the DARKO case study (as described in D8.1), and it will outline the methodology for creating a risk space whose factors depend on robot state variables. Figure 1 shows the Australian Standard for Risk Management [1].

The EU norms on industrial machinery are contained in the European Machinery Directive 2006/42/EC. To comply with this regulation, ISO 12100 specifies basic terminology, principles, and a methodology for achieving safety in the design of machinery. Procedures are described for identifying hazards and estimating and evaluating risks during relevant phases of the machine life cycle and for the elimination of hazards or the provision of sufficient risk reduction [5]. According to ISO 12100, the actions to follow to implement risk assessment (1-4) and risk reduction (5) are [5]:

1. Determine the limits of the machinery, which include the intended use and any reasonably foreseeable misuse thereof.
2. Identify the hazards and associated hazardous situations.
3. Estimate the risk for each identified hazard and hazardous situation.
4. Evaluate the risk and take decisions about the need for risk reduction.
5. Eliminate the hazard or reduce the risk associated with the hazard by means of protective measures.

Therefore, they are mostly equivalent to those in [1]. The "Determine the limits of the machinery" step is slightly different from the "Establish the Context" step in ISO 31000 used in the risk management literature. "Determine the limits of the machinery" in ISO

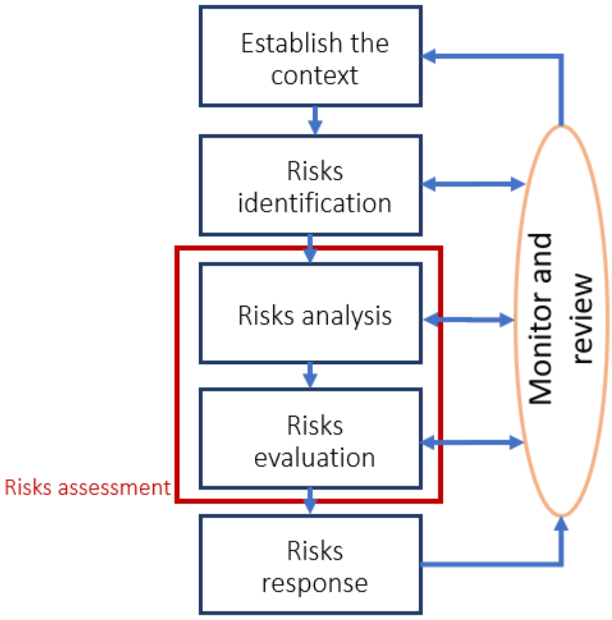


Figure 1: Risk management pipeline. The steps are: establishing the context of risk, identifying risks, analyzing risks, evaluating risks, and monitoring and controlling risk events.

12100 instead aims to identify the use, space, and time limits in which the machine will operate. This means specifying how the machine will be operated, and in which context.

In this work, we apply the risk management process to assess and monitor in real-time the residual risks depending on the robot's movement in a shared environment, relating to the type-C norm for collaborative robots ISO/TS 15066 [8], ISO 10218-1,2 [6][7]. We consider only the hazardous situations arising during the ordinary use phase of the robot (and not for example the setting, testing, and maintenance phase for which a separate specific risk assessment will be needed).

2.1 Context definition

The aim of our risk assessment it's not to design safe machinery and to identify its limits, since we focus on the residual risks during the DARKO application. Therefore, the aim of this phase is to describe the context (the application) in which we need to identify and assess the risk factors. To establish the context in which to perform the hazard identification, we rely on the scenario described in D8.1. The objective that we want to pursue is task success. For task success, we intend that the robot performs all the steps described in D8.1, without colliding with any obstacle or human, not consuming more than scheduled and not draining the battery, not arriving later than the scheduled time, and not causing unnecessary stress to the human operator. Furthermore, the task can be considered successful only if it's not disruptive to the robot's lifespan (e.g., excessive stress on the actuators may cause long-term problems to the robot, and decrease the robot's lifespan).

In section 3 we dissect and describe the DARKO task, and we identify the robot use limits in this context.

2.2 Risks identification

The Collaborative robot safety specification ISO/TS 15066 [8] describes the concepts, terminology, and detailed requirements of human-robot collaboration and complements the traditional industrial robot safety standard ISO 10218-1,2 [6] [7]).

The purpose of these normative specifications is to guarantee human safety and they include a list of significant hazards for collaborative robots (EN ISO 10218-2:2011, Annex A).

There are numerous strategies in the literature for quantifying the level of risk during human-robot collaboration, but they focus only on the risk for the human operator [12]. In DARKO, we want to broaden this concept according to the risk management definition of risk (Definition 1): we will also take care of the self-safety of systems, as about the damages caused by a delay in the operation performed by the robot (for example in the case of a manipulator that has to pick up objects from a conveyor belt). We will catalogue the most relevant risk factors detected within the following families:

- *Performance risks*: Risks concerning the quality of the task execution. (e.g., excessive power consumption leads to increased costs and fewer tasks that can be performed in a charge cycle, and delay in fetching an object from a conveyor belt can cause the assigned task to fail);
- *External risks*: Risks related to the damage that the movement of the robot can cause to other agents involved in the tasks or near the robot (humans, obstacles), in compliance with the ISO/TS 15066;
- *Internal risks*: Risks related to the damage that the robot movement can cause to the robot itself (e.g., damage to the motors due to vibration or overheating, self-collisions between the manipulator and the moving base that can result in damage to the robot).

To identify the involved risks, a questionnaire was administered to the DARKO partners to assess known operational risks in their respective activities. They were asked to report and briefly describe the expected risks, and to enumerate all possible variables that can be used to measure the level of risk. We aggregated the risks identified by the partners with a list developed independently by UNIPI.

2.3 Risks assessment

Risk is measured using two parameters – risk probability and risk consequence [1]. Risk probability (aka likelihood) indicates a chance of a risk event to occur, while risk consequence (aka severity, or impact) represents an outcome generated from the risk event one it occurs. We will, therefore, proceed by analysing the risks found by identifying the variables on which probability and severity depend.

Every detected risk represents a “risk factor” in our multi-dimensional “risk space". The risk level of each risk factor can be expressed quantitatively by combining the probability that the hazardous event occurs and its severity [15, 1]. In the literature, a useful technique that is often used for risk assessment is probability and impact grids: risk events are represented on a grid consisting of probability on one axis and severity on the other. To map probability and severity to a scale that quantifies the risk level, we use a Takagi-Sugeno-Kang fuzzy inference system. In this way, the map on the risk scale is continuous (fig. 3). We defined five levels for probability (Almost Impossible, Low, Medium, High, Almost certain), and four for severity (Minor, Moderate, Severe, Catastrophic). We chose trapezoidal membership functions and a structure-oriented approach to generate the fuzzy rules.

0	1	2	3	4	5	6
Almost impossible + Minor	Almost impossible + Moderate Low + Minor	Almost impossible + Severe Low + Moderate Medium + Minor	Almost impossible + Catastrophic Low + Severe Medium + Moderate High + Minor	Low + Catastrophic Medium + Severe High + Moderate Almost certain + Minor	Medium + Catastrophic High + Severe Almost certain + Moderate	High + Catastrophic Almost certain + Severe/ Catastrophic

Figure 2: Fuzzy rules to map probability and severity to the risk level value

For each risk factor, the risk level span between 0 and 6, resulting from the fuzzy rules shown in fig. 2. To normalize the severity levels on a scale of 0 to 1, we assign 0 to the “minor” level, 0.33 to the “moderate” level, 0.67 to the “severe” level, and finally 1 to the “catastrophic” level.

The probability is the likelihood that the risk occurs. As a consequence, it has the same definition for all hazardous events. On the other hand, severity will have different definitions for each risk. However, the idea is to give a generic definition for each identified degree of severity (minor, moderate, severe, catastrophic), and then decline it for each risk according to its specific characteristics.

We will therefore have that the impact of the occurrence of risk will be:

- *Minor*: Minor damage, resulting in no long-term problems.
- *Moderate*: Damage that has a major immediate impact, like the task failure, but does not result in long-term effects.
- *Severe*: Damage that has a major impact that goes to permanent damages (for the robot or the environment), or involves a plot event of minor medical significance to the human operator.
- *Catastrophic*: Damage that involves major medical issues for the human operator.

To calculate probability and severity values we can still use a fuzzy inference system from the variables that link risk to robot state, or, when available, use other types of assessment (e.g., use more precise metrics for collision risks).

Finally, we propose a global risk index to dynamically quantify the overall level of risk in the system.

2.4 Normative background for human safety

According to ISO 10218-1,2 and ISO/TS 15066, there are four types of collaborative operations [8]:

- Safety-rated monitored stop: in this scenario, the robot is stopped when there is an operator in the collaborative workspace.

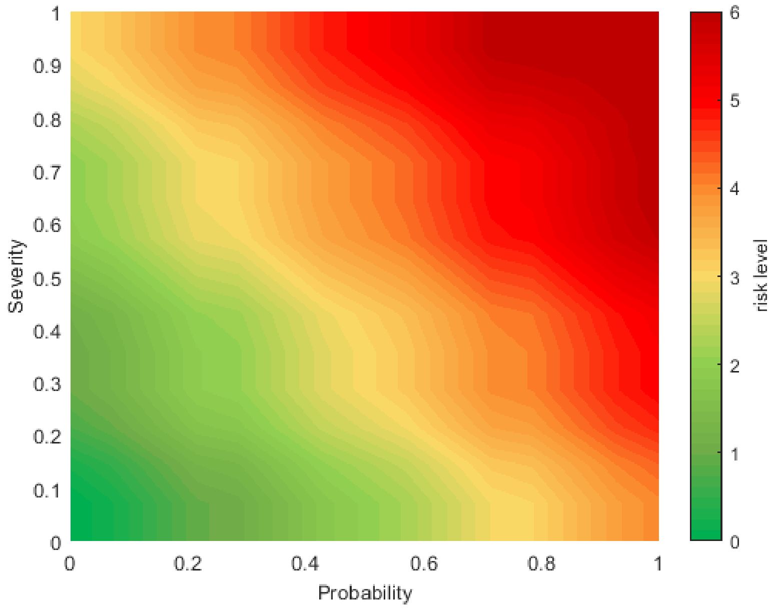


Figure 3: Risk level map from probability and severity values

- Hand guiding: in this case, the robot moves only through direct input from the operator.
- Speed and Separation Monitoring (SSM): In this scenario, the robot and the operator share the same workspace. The risk is reduced by only allowing the robot to move if the separation distance between the robot and the human is greater than the distance required to stop the robot completely.
- Power and Force Limiting (PFL) by inherent design or control: In this case, non-zero speed collisions are possible, but the robot can only impart limited static and dynamic forces, resulting in harmless impacts.

SSM and PFL are considered alternative methods, and the choice between one and the other is at the discretion of the person conducting the risk assessment. However, PFL does not depend on the distance between the robot and the human operator, and SSM is overly conservative when such distance is small.

So in the state of the art have been proposed strategies to adopt PFL near the human operator, and SSM when the distance increases enough, in order to achieve stronger performances [13]. SSM depends on the estimation of the relative distance and velocity, as well as the current needed breaking time and measurement uncertainty in that particular environmental conditions and robot configuration. SSM prevents the collision to happen. PFL, instead, does not guarantee the absence of collisions, but imposes maximum energy transferred during the impact, so, we can see it as a way to reduce the severity part of the collision risk.

To assess the impact severity, in DARKO we can benefit from the extensive injury database collected by TUM. Furthermore, TUM also developed a Safe Motion Unit (SMU) method [10] to define the maximum safe velocity depending on the manipulator's reflective mass, contact geometry, and human body part involved. The SMU controller, that derives the maximum speed, works with safety maps derived with a data-driven experimental approach. On the other hand, PFL relates force/pressure limits ($1cm^2$ contact area) to thresholds in the mass/velocity plane via a simplified contact model, and so there is not a direct connection with experimental observed human injuries [14].

With our approach we will compute a risk value for human safety, that is the combination of the probability that the robot cannot brake in time to avoid the collision (related to the SSM), and its severity (related to the PFL/SMU guideline). In section 5.5 we will show how this approach compared to the guidelines in ISO/TS 15066.

We are currently monitoring the release of the new American standard for autonomous mobile robots ANSI RIA R15.08 [2]. At the time of writing, only part I (Requirements for the Industrial Mobile Robot) of the standard is available, and we believe that part II and III will be particularly interesting for DARKO application, i.e., IMR Type C (AGV & industrial manipulator).

3 Establishment of the context for the DARKO scenario

The DARKO demo scenario is used as a standard use case for identifying typical hazards and their associated risks for the creation of the risk space. This scenario, motivated by the workflow at Bosch Siemens Hausgeräte (BSH Home Appliances group or BSH) and other use cases in agile production, is described in detail in D8.1. The demonstration will be performed at ARENA2036, a multidisciplinary research campus based in Stuttgart (Germany). This will be a near real environment where we are not limited to a single end-user site (which could lead to a kind of "overfitting" the solution to one specific user in a real environment). The robot that will be used in the DARKO scenario consists of the integrated mobile platform selected in T1.1, and the new elastic manipulator that will be developed in T1.3.

As illustrated in D8.1, the robot will receive an order, which is a list of objects and quantities. Items to be picked will be stored in boxes or trays on slanted shelves, and they will have to be placed in trays for further transport on a conveyor belt. Once all the objects in the order are in the tray, the order will be fulfilled.

In this deliverable, we will analyse the risks arising from the hazards to which the robot, the external world (humans, other vehicles, environment) or the task performances may be exposed during the accomplishment of the task.

The fulfilment of the task consists of the following steps (from D8.1):

1. Go to the right shelf containing box A. The robot employs a vehicle safe motion unit [T6.4] to adapt velocities within human-safe limits while carrying out the motion plans. This unit is based on human pose estimation [T2.5] and motion prediction [T5.1]. Furthermore, local modifications to the robot's course due to the presence of nearby people are made using multi-agent interactions [T5.3]. The robot uses a projector to transmit visual information about its planning and perception onto the ground and anthropomorphic signalling, which uses a miniature humanoid robot installed on a movable platform to demonstrate the robot's intentions using head and hand gestures [T5.2].

2. Locate the box and pick up the desired item. The planning and control system for picking [T4.1] makes use of variable stiffness actuation and an elastic manipulator with spring energy storage [T1.2, T1.3] to maximize the success rate and energy efficiency of manipulation. Motion planning and control of the manipulator further takes into account full-body people tracking [T2.5] and a safe motion unit [T4.2] for reaching the best compromise between joint speeds and human safety.

3. Drive to tray B to deliver the object. While navigating to B, the same modules for human-aware and risk-aware navigation and intention communication are active as in step 1.

4. When approaching B, the robot may choose to throw [T4.4] the object into the target tray or to place the object directly in the tray, if the throw failure risk is too high.

The risk computation will benefit from the online assessment of an estimate of the quality of the environment map T3.4 performed during and after the construction of the initial map. The robot also constructs and revises a “map of dynamics” T3.3 in which spatio-temporal patterns of human motion are represented.

We will not consider the risks during the construction of the initial map, as in this phase the robot will not work with the risk-aware motion planning module activated.

To relate to ISO 12100 we specify below the use, time, space, and other limits of the DARKO robots in the described task execution:

- Use limits: The different machine operating modes are described above (a navigation phase (stages 1 and 3), a picking and place phase (stages 2 and 4 if the system decides to place the object directly), and a throwing phase (stage 4)). In contrast to ISO 12100, the purpose of this deliverable is only to consider the regular use of the robots. So, we will not consider the interventions required by maintenance and machine repair.

  The machinery would be used in an industrial environment, sharing its workspace with trained operators, trainees, and apprentices.

  The robot will communicate its intents and will predict human motion and intents with the methods developed in T5.2 and T5.1.

- Space limits: The robot and the human operator will share the same workspace and they will move at a close distance. The robot and the human operator should not touch each other in any part of the task.

  The robot is a mobile manipulator so it could reach any workspace location larger than 1 meter (the Robotnik mobile platform, selected in T1.1, is wide 980 mm). The maximum reachable height is 2 meters.

- Time limits: The robot will need to perform stops to go to the recharge station and recharge its battery.

- Other limits: According to constructors the Robotnik mobile platform has a temperature range between 0 and 50°C.

4 Risks identification for the DARKO scenario

In accordance with the task stages defined in the previous section, we will study the risks involved during the navigation phase (stages 1 and 3), during the picking and placing phase (stages 2 and 4 if the system decides to place the object directly), and during the throwing phase (stage 4).

Tables in figs. 4 to 6, summarize the risks identified, respectively, in the navigation, picking, and throwing stage, dividing them into the families set out in the methodology section of this report (performance, external, and internal risks).

4.1 Risks during the navigation phase

In this phase, the mobile base moves the robot to reach the right shelf or to deliver the items. The manipulator's joints are assumed fixed throughout the process.

Table 1 shows the risks identified during the navigation phase. A brief description of the risk is given in the second column. The third column indicates whether the risk will need to be taken into account by the risk-aware motion planning algorithms that will be developed in T6.2 and T6.4. The fourth column indicates whether the risk will need to be taken into account by the operational scheduling module in T7.3.

The goal of this part of the task is to arrive at a fixed point. The first risk we have to take into account is hence not reaching the final destination because, for example, the mobile robot's battery does not have enough charge. We then have a risk of delay, i.e. if the robot fails to meet the deadline to complete the task, which will have a varying severity depending on the application (e.g., the impact will be greater if an item were fetched from a conveyor belt and this task is not achieved on time, than if it was fetched from a fixed shelf). Then all the risk factors related to the danger of collisions with fixed obstacles, moving obstacles, and human operators, need special attention.

In this regard, solutions will be implemented in T5.1 to predict the behaviour of the human operator. During the motion planning phase, predicted trajectories are taken into account, such that the robot can avoid dense areas, potentially switching to a route following a different homotopy class (e.g. a parallel corridor) [16].

At the same time, using Maps of Dynamics for Global Motion Planning could help the robot avoid dense areas [17] and go along the flow [18], rather than against it, leading to more intelligent robot behaviour perception, reduced obstruction and collision risks. However, it should be kept in mind that the human might take an unexpected sudden action (e.g., she/he turns around quickly and comes back because she/he forgot something). Therefore, we introduce a risk to evaluate whether the motion prediction algorithms are proving effective at that moment. In contrast, methods are proposed in T5.2 to inform the operator about the robot's motion intentions. If the robot is moving with a non-smooth trajectory, with continuous changes in direction, these methods may be ineffective. Having non-smooth robot trajectories could also lead to high energy consumption and the feeling of unsafe interaction on the part of the human operator.

However, it should be also taken into account perception-related risks, as for instance a human not being detected at all or some of its body joints being detected at the wrong location, e.g. due to strong occlusion by other obstacles/objects in the environment or the onboard manipulator, adverse lighting conditions, or a neural network overfitting to a certain environment and performing much worse on unseen environments.

The risk of the robot deviating from the planned path because of an incorrect estimate of its current position, should be also taken into account. In T3.4 we are developing a "localization risk map" that the motion planner can use to actively avoid areas in which there is a higher risk of low localization accuracy.

The operation of the sensors should then be monitored, checking for interference or pieces of carried objects that end on the sensor, precluding sensing.

Finally, levels of motor overheating, system vibration, and power consumption levels during motion need to be monitored.

4.2 Risks during the picking and placing phase

In this phase, the mobile base is supposed fixed, and the robotic arm performs the pick (or place) operation. The identified risks are reported in table 2.

In this case, some risks will depend on variables expressed in the task space, others on the joint variables of the manipulator. As in the previous phase, we will have the risk of

Risk	Description	Minimize during motion planning	Minimize during task scheduling	Minimize online during path execution
Target point not reached	The robot does not arrive in the desired location with the required precision.	✓	✓	✓
Delay	The robot does not complete the task in the scheduled time (e.g., fails to reach the conveyor belt in time)	✓	✓	✓
Not smooth trajectories	The trajectory is not smooth. This can result in increased stress for the operator and in increased energy consumption.	✓		
Intent miscommunication human/robot	The operator performs an unexpected movement. Prediction of human motion fails.			✓
Intent miscommunication robot/human	The methods to transmit visual information about the robot planned intentions fails. Feeling of danger, stress on the operator.			✓
Collisions with fixed obstacles	The robot collides with a fixed known obstacle (e.g., a shelf).	✓	✓	✓
Collisions with moving obstacles	The robot collides with a mobile or unknown obstacle (e.g., a forklift).	✓	✓	✓
Human safety	The robot collides with a human operator.	✓	✓	✓
Sensor's occlusion	Onboard sensors fail in perceiving the surrounding (humans or objects) due to sensor occlusion, adverse light conditions, neural network malfunction with collisions.	✓		✓
Vehicle surrounded by large crowd of people	The robot finds itself in an area with a high density of people, thus having to slow down and/or stop.	✓	✓	✓
Overheating	A motor of the mobile base overheats.	✓	✓	✓
Vibrations	The robot movement can generate vibrations in the system (e.g., because of the mecanum wheels), which can lead to increased stress on the actuators or the fall of the transported object.	✓		✓
Excessive energy consumption	Running a longer route will result in higher energy consumption, which may cause excessive costs and/or battery drain during the task.	✓	✓	✓
Localization failure	The robot should avoid areas in which there is a higher risk of low localization accuracy that may be due to sensing failure. This may cause a higher probability of collisions, an increased risk of not reaching the target point with the required precision or correctly localise humans.	✓	✓	

Table 1: Identified risks during the navigation phase

Risk	Description	Minimize during motion planning	Minimize during task scheduli ng	Minimize online during path execution
Target point not reached	The robot does not arrive in the desired location with the required precision.	✓	✓	✓
Delay	The robot does not complete the task in the scheduled time (e.g., fails to reach the object on a conveyor belt in time)	✓	✓	✓
Not smooth trajectories	The trajectory is not smooth. This can result in increased stress for the operator and in increased energy consumption.	✓		
Grasp failure	Due to a bad grasping or a misperception, the manipulator fails to pick up the object, or the object falls during manipulation.	✓		✓
Collisions with fixed obstacles	The robot collides with a fixed known obstacle (e.g., a shelf).	✓	✓	✓
Collisions with moving obstacles	The robot collides with a mobile or unknown obstacle (e.g., a forklift).	✓	✓	✓
Human safety	The robot collides with a human operator.	✓	✓	✓
Misperception of sensors	Onboard sensors fail in perceiving the surrounding (humans or objects) due to (self) occlusion, adverse light conditions, neural network malfunction with possible collisions.	✓		✓
Self-collisions	The object carried by the end effector may collide with another joint of the manipulator, or with the robot mobile base.	✓		✓
Blocked Joints	The manipulator can enter in singularities during the task. This causes the robot to lose freedom of movement, resulting in an increased risk of collisions or vibrations.	✓		✓
Overheating	A motor of the robotic arm overheats shortening his remaining life time.	✓	✓	✓
Vibrations	The robot movement can generate vibrations in the system, which can lead to increased stress on the actuators or the fall of grasped/transported objects.	✓		✓
Excessive energy consumption	Poor use of stored energy in the elastic actuator system developed in [T1.2, T1.5], or control with excessively high accelerations at the actuator.	✓	✓	✓

Table 2: Identified risks during the picking and placing phase

not reaching the target point. However, in this case, the risk is related to arriving at the desired final configuration with the necessary precision to execute a performant grasp.

The risk factors of delay and not smooth trajectory are the same as in the navigation phase, but related to end-effector (EE) trajectory. Collision risk factors will be evaluated, considering the EE and other points of interest (POI) along the manipulator coordinates in the task space. The grasp failure risk factor expresses the risk that grasping the object will fail or that the item will fall during handling due to an underperforming grasping position or a misperception of sensors because of sensor occlusion or adverse light conditions that do not allow the correct detection or localization of the shelves, the storage bins as well as the objects inside them and so on.

When the manipulator moves, we should consider the risk of self-collisions both between the EE and the mobile base and between the EE and some selected POIs along the manipulator. It should also be considered that the carried object increases the size of the EE.

The blocked joints risk factor is related to the manipulability index of the joints' configuration. A low manipulability decreases the manipulator's dexterity to deviate, if necessary, from the predefined path to avoid a collision with a moving entity. Overheating and vibrations risks have the same definition as in the navigation stage, but referred to the joints' actuators. Excessive energy consumption risk in this phase relates to the effective usage of the stored energy in the elastic actuator system developed in T1.2 and T1.5.

4.3 Risks during the throwing phase

Throwing failure may happen if the thrown item misses the target, or if it collides against something during the in-flight trajectory. Therefore, we will need to evaluate the distance from the fire line and the planned intentions of the humans, and the obstacles around.

Throw success is strictly linked to the grip the manipulator can grasp the object. Only with a performant grip, the manipulator can transmit to the object the desired velocity and flying direction to the object.

In this phase, the manipulator moves to reach the best throwing configuration. Consequently, we will have the risks already identified for the pick and place phase: the risk of self-collisions, blocked joints, vibrations generated by the manipulator actuators, the possible excessive energy consumption made by the elastic actuators, as well as possible misperception of the target tray in terms of position/orientation and velocity (if the tray is on a conveyor belt).

As in the other phases, table 3 reports the list of the identified risk factors.

4.4 Normative comparison – risk factors identification

We compare here briefly the detected risk factors with the list of the significant hazards presented in Annex A of the ISO 10218-2 [7] and Annex A of the ANSI/RIA R15.08-1-2020 [2]. We report only the hazards that apply to the robot movement within the context definition described in section 3. Furthermore, we don't consider the hazards associated with risks to be minimized during the design phase, and with risks to be minimized through operators training and safety rules independent from robot's motion (i.e., loose clothing, long hair). In table 4 we report the relevant hazards identified in the normative, the movement phase in which the hazard is present, and the correspondent identified risk factors in DARKO for that hazard.

Risk	Description	Minimize during motion planning	Minimize during task scheduling	Minimize online during path execution
Target missed	The launched object does not enter the target box or sensors fail in detecting a successful throw.	✓	✓	✓
Delay	The robot does not complete the task in the scheduled time (e.g., fails to throw in time for reaching a moving tray)	✓	✓	✓
Grasp failure	Due to a bad grasping or a misperception, the manipulator fails to pick up the object, or the object falls during throwing.	✓		✓
Collisions with fixed obstacles	The object during the throw hits a fixed known obstacle (e.g., a shelf).	✓	✓	✓
Collisions with moving obstacles	The object during the throw hits a mobile or an unknown obstacle (e.g., a forklift).	✓	✓	✓
Human safety	The object during the throw hits a human operator.	✓	✓	✓
Misperception of sensors	Onboard sensors fail in perceiving the surrounding (humans, objects and trays) due to occlusion, adverse light conditions, neural network malfunction with possible collisions.	✓		✓
Self-collisions	The object carried by the end effector or the end-effector itself collides with another joint/link of the manipulator, or with the mobile base.	✓		✓
Blocked Joints	The manipulator can enter singularity during the operation. This causes the robot to lose freedom of movement, resulting in a worse throwing and vibrations.	✓		✓
Vibrations	The robot movement can generate vibrations in the system, which can lead to increased stress on the actuators or the fall of the transported object or a wrong throw.	✓		✓
Excessive energy consumption	Poor use of stored energy in the elastic actuator system developed in [T1.2, T1.5], or control with excessively high accelerations at the actuator.	✓	✓	✓
Localization failure	The robot should avoid areas in which there is a higher risk of low localization accuracy that may be due to sensing failure. This may cause a higher probability that the target is missed.	✓	✓	

Table 3: Identified risks during the throwing phase

PERFORMANCE RISKS	EXTERNAL RISKS	INTERNAL RISKS
Target point not reached	Collisions with fixed obstacles	Overheating
Delay	Collisions with moving obstacles	Vibrations
Not smooth trajectories	Human safety	Excessive energy consumption
Intent miscommunication human/robot	Misperception of sensors	Slippery floor/ small undetected obstacles on the floor
Intent miscommunication robot/human	Vehicle sorrounded by large crowd of people	

Figure 4: Risks during navigation - Classification

PERFORMANCE RISKS	EXTERNAL RISKS	INTERNAL RISKS
Target point not reached	Collisions with fixed obstacles	Self collisions
Delay	Collisions with moving obstacles	Blocked Joints
Not smooth trajectories	Human safety	Overheating
Grasp failure	Misperception of sensors	Vibrations
		Excessive energy consumption

Figure 5: Risks during pick and place - Classification

PERFORMANCE RISKS	EXTERNAL RISKS	INTERNAL RISKS
Target missed	Collisions with fixed obstacles during the launch	Self collisions
Delay	Collisions with moving obstacles during the launch	Blocked Joints
Grasp failure	Human safety during the launch	Vibrations
	Misperception of sensors	Excessive energy consumption

Figure 6: Risks during the throwing phase - Classification

Type or Group	Description/Origin	DARKO application	Correspondent risk factors
Mechanical hazards	Movements of any part of the robot/ end-effector tool	Navigation Pick and place Throwing	Collisions with fixed obstacles Collision with moving obstacles Human safety
	Movement or rotation of sharp tool on end-effector	Navigation Pick and place	Human safety
	Materials and products falling	Pick and place Throwing	Grasp failure
	Unintended movement of jigs or gripper	Pick and place Throwing	Grasp failure
	Unintended release of tool	Pick and place Throwing	Grasp failure
	Impossibility to avoid mobile platform (entrapment in an area)	Navigation	Human safety Intent miscommunication human/robot
Vibration hazards	Loosening of connections, fasteners, components resulting in unexpected stopping or expulsion of parts	Navigation Pick and place Throwing	Vibrations
Ergonomic hazards	Recognition of hazards and hazardous situations is obscured because of poor area lighting	Navigation Pick and place Throwing	Misperception of sensors
Hazards associated with environment in which the machine is used	Motion pathway on or along inclines, discontinuous or slippery surfaces	Navigation	Slippery floor/Small undetected obstacles on the floor
	Surface or wall characteristics that may affect navigation or safety systems (i.e., transparent, reflection)	Navigation	Misperception of sensors
	In fleet installations, emissive sensors on adjacent robots could potentially compromise the integrity of other robots'	Navigation Pick and place Throwing	Misperception of sensors
	Misidentification of real problem and compound problem by making incorrect or unnecessary actions	Navigation Pick and place	Intent miscommunication human/robot
	One action or failure increases severity of harm, i.e., trying to avoid a sharp edge you came in contact with a hot surface instead	Navigation Pick and place Throwing	Collisions with fixed obstacles Collision with moving obstacles Human safety
Combinations of hazards	Unintended release of holding devices allowing motion under residual forces	Navigation Pick and place Throwing	Collisions with fixed obstacles Collision with moving obstacles Human safety
	Failure of a safeguarding device to function as expected	Navigation Pick and place Throwing	Human safety
	Compromised operation of sensors	Navigation Pick and place Throwing	Misperception of sensors
	Misinterpretation of collaborating robots	Navigation Pick and place Throwing	Intent miscommunication human/robot Intent miscommunication robot/human

Table 4: Comparison Normative hazards - Risk factors

5 Risks assessment for the DARKO scenario

As described in the methodology section, to assess risk values we compute their probability of occurrence and their impact, and we use these variables as inputs for a fuzzy inference system that yields the risk level according to the rules in fig. 2. To compute probability (or severity) for each risk, we propose another fuzzy inference system. This system would have as inputs the variables on which the probability (or severity) of the risk depends. The output will be the sought-after value of probability or severity, which will then enter the risk level inference system, thus creating a fuzzy tree. However, if a more accurate metric to quantify probability or severity for a specific risk is available, the obtained value can be used directly in the risk level inference system. This approach allows a single framework with heterogeneous metrics.

Not all risks have the same maximum severity. Colliding with a human at high speeds is far more disastrous than having non-smooth trajectories. In tables 5 to 7 a definition of when that risk assumes that value of severity is reported. The missing definitions in the tables indicate that risk factors cannot take on that level of severity.

The following sections group the risks identified in the three phases of the task into performance, external and internal risks, going on to expose which variables each risk depends on. If risks are common to multiple phases, it will be specified whether the calculation metrics (and the variables on which the risk depends) are the same for all phases, or whether there are variations.

5.1 Performance risks

The table 8 reports the variables on which the values of probability and severity for each performance risk depend.

Not reaching the target point in the navigation phase because the robot is out of charge is linked with the battery state of charge and with the distance to the target. The robot could fail in reaching the target point also due to a localization problem: the sensor's coverage in the area or the measurement noise is such that there is no guarantee that the robot will reach the endpoint with the required accuracy. This event would be evaluated in the localization failure risk. Its probability would depend on an index, whose values range from 0 to 1, indicating the probability of having low accuracy at that point based on the localization risk map developed in T3.4. Its severity will depend on an index (spanning from 0 to 1) assessing how much precision the current task requires, and on the obstacle density in the area (lower accuracy increases the risk of collisions). A collision could also cause the target not to be reached, but this situation falls under collision risk evaluation. For the manipulation stage, we have the risk of not reaching the target point with the desired precision, which could lead to grasping failure. To minimize this risk, we want to prefer trajectories with low EE velocities near the final grasping position. Severity would depend on the needed grasp precision index, which would span between 0 and 1, according to the type of object to be manipulated (items that are more difficult to catch will require greater precision), and the planned actions after the grasp (if the item has to be thrown after the picking, a higher precision would be required).

The delay risk metric is the same for all the task stages. Probability would depend on the rate between the residual time before the deadline and the estimated time needed to complete the task with the current or predicted human density in the area. Severity, as underlined in table 5, is defined by the delay estimation value (which would depend on the rate between residual time and estimated remaining needed time) and by a parameter representing the time-critical nature of the specific task. This parameter spans between 0 (no time-critical application) and 1 (time-critical application, e.g. picking an object from a

RISK	SEVERITY Minor	Moderate	Severe	Catastrophic
Target point not reached	The robot cannot complete the task, but has enough autonomy to return to the charging base, and there is another robot available to complete the task	Robot gets stuck along the path or no other robots available to complete the task	-	-
Delay	Delay on task time within 10%	Delay on task time above 10% / Delay causes task failure	-	-
Not smooth trajectories	Robot movement perceived as not natural by the operator	Robot movement perceived as not safe by the operator	-	-
Grasp failure	Grip failure, item not damaged	Grip failure comports not meeting a scheduled deadline, item not damaged	Grip failure and item damaged	-
Target missed	Missed target	Missed target involves not meeting a scheduled deadline	-	-
Intent miscommunication human/robot	The robot must slow down due to an increasing collision risk	The robot must stop due to an increasing collision risk	-	-
Intent miscommunication robot/human	The robot must slow down due to an increasing collision risk	The robot must stop due to an increasing collision risk	-	-
Localization failure	The robot needs to slow down due to low localization accuracy	The robot needs to stop due to low localization accuracy/ The task fails because the endpoint is not reached with the precision needed	-	-

Table 5: Severity definitions, performance risks

	SEVERITY			
RISK	Minor	Moderate	Severe	Catastrophic
Collision with fixed known obstacles	The Robot and the obstacle don't report any damage	The robot and the obstacle can report mild damages (scratches)	The robot and/or the obstacle report permanent damages/ broke	-
Collision with mobile obstacle	The Robot and the obstacle don't report any damage	The robot and the obstacle can report mild damages (scratches)	The robot and/or the obstacle report permanent damages/ broke	-
Human safety	-	Painless collision with the human/ The Robot doesn't report any damage	Painful collision with the human/ The robot can report mild damages (scratches)	Severe health problems for the human operator (broken bone)/ Heavy damages for the robot
Misperception of sensors	The robot must slow down due to incomplete vision	The robot must stop because navigation is no longer safe	-	-
Vehicle surrounded by large crowd of people	The robot must slow down because navigation is no longer safe	The robot must stop because navigation is no longer safe	-	-

Table 6: Severity definitions, external risks

RISK	SEVERITY Minor	Moderate	Severe	Catastrophic
Self-collisions	The Robot doesn't report any damage	The robot can report mild damages (scratches)	The robot breaks	-
Blocked Joints	Manipulability compromised. The robot can exit from the singularity without help	The robot can't exit from the singularity without help.	-	-
Overheating	Overheating less than 10% for a short time	Overheating more than 10% for a short time or less than 10 % for a long time	Overheating more than 10% for a long time. Motors can break	-
Vibrations	Slight stress actuators	High stress actuators	Permanent damage for the robot	-
Excessive energy consumption	Operational costs increased by up to 10% compared to what was planned	Operational costs increased by more than 10% compared to what was planned	-	-

Table 7: Severity definitions, internal risks

Performance risk	Stage	Probability	Severity
Target point not reached - navigation	Navigation	- Distance to the final point - Residual battery charge	- Residual battery charge
Target point not reached - manipulation	Pick and place	- Distance to the final point - EE velocity	- Needed grasp precision
Delay	Navigation Pick and place Throwing phase	- Time left - Estimated time to accomplish the task - Predicted human density and other agents' position	- Time left - Estimated time to accomplish the task - Task time critical index
Not smooth trajectory	Navigation Pick and place	- Mobile base/End Effector jerk trajectory values - Average acceleration	- Mobile base / EE jerk trajectory values - Time with high jerk values
Grasp failure	Pick and place Throwing phase	- Grip success index related to approach configuration - Jerks' values (vibrations)	- Type of object manipulated
Target missed	Throwing phase	- Distance from the target - Grip performance index	- Time left
Intent miscommunication human/robot	Navigation	- Human acceleration - Eye-gaze information	- Distance from the human operator - Relative velocity
Intent miscommunication robot/human	Navigation	- Robot acceleration - Parameter to define human/robot visibility	- Distance from the human operator - Planned relative path direction
Localization failure	Navigation Throwing phase	- Localization accuracy index in the area	- Obstacle density in the area - Task required precision

Table 8: Variables from which to compute the probability and severity for each performance risk

conveyor belt).

The risk of non-smooth trajectories is related to the operator's perception of safe collaborative interaction. This risk probability depends on how smooth the mobile base/EE trajectory is, namely on medium acceleration and jerk trajectory values. The severity will also consider the total accumulated time in which the jerks of the robot trajectory overshoot a certain threshold.

The probability of the grasp failure risk factor will be evaluated considering a grip success index spanning between 0 and 1, depending on the approaching manipulator's configuration, and the jerk values during the grasping phase, which may cause vibrations and a consequent increased risk that the object falls. The severity will depend on the type of object manipulated. We define an index between 0 (light, cheap, not breakable objects) and 1 (fragile, expensive objects).

The likelihood of missing the target during the throwing phase will be determined by the distance from the target at which the robot performs the throw and by a grip performance index, spanning between 0 and 1, that assesses how the executed grasp can transmit to the manipulated object the desired motion direction and velocity. Its severity will depend on the time left to complete the task. The robot is allowed to throw only resistant, not breakable objects, so there is no risk that the thrown item breaks.

The probability of miscommunication between humans and robots will be assessed considering the values of not predicted human accelerations by the motion prediction module and on an index depending on If the operator's gaze is in agreement with the motion prediction estimated. Severity would depend on the distance between the robot and the operator when the unforeseen movement happens (the shorter the distance, the more likely it is that the robot will fail to change its planned route in time, thus resulting in a necessary slowdown or forced stop for safety reasons).

On the other hand, the chance of miscommunication between the robot and humans would depend on the magnitude of the robot's acceleration, and on a parameter between 0 and 1 which expresses the operator's ability to see the systems for communicating the robot's motion intent (0 the operator's back is turned, 1 the operator's head is directed in the direction of the robot). Again, the severity of the risk factor will depend on the distance between the operator and the robot and the direction of the robot's planned path (the closer they are, the more the robot will have to slow down to ensure standard safety conditions).

5.2 External risks

The table 9 reports the variables on which the probability and the severity of each external risk depend.

The probability of collisions with fixed objects should be related to the distance and speed of the robot in the direction of the obstacle. Sensor uncertainty should also be considered. For collisions with moving obstacles and with humans, it should be also taken into account the evolution of the distance predicted by the motion prediction module, over a fixed time horizon.

During the navigation and pick-and-place phases, the probability of collision for mobile obstacles and human operators will be the same, but for the same distance and relative speed conditions, the severity of human collisions will be higher, resulting in a higher risk factor value. The severity will depend on the robot velocity, on a parameter between 0 and 1 related to the task application (e.g., 1 if the robot is handling a dangerous sharp item), and on the robot's reflected mass. This quantity represents the mass perceived during a collision [11], and it is dependent on the Jacobian matrix associated with the impact location ($\mathbf{J}(\mathbf{q})$) and the mass matrix $\mathbf{M}(\mathbf{q})$, where $\mathbf{q}$ denotes the joint configurations for a serial manipulator. Mansfeld et al. [14] propose a map that captures human injury

External risk	Stage	Probability	Severity
Collisions with fixed obstacles	Navigation Pick and place	- Robot position - Robot velocity - Quality of perception	- Robot velocity - Reflected mass - Application-related hazards (e.g., handling of fragile objects)
Collisions with moving obstacles	Navigation Pick and place	- Relative position - Relative velocity - Minimum relative distance in the time horizon - Quality of perception	- Relative velocity - Reflected mass - Application-related hazards (e.g., handling of fragile objects)
Human safety	Navigation Pick and place	- Relative position - Relative velocity - Minimum relative distance in the time horizon - Sensing uncertainty - Quality of perception	- Relative velocity - Reflected mass - Application-related hazards (e.g., handling of sharp objects)
Misperception of sensors	Navigation Pick and place Throwing phase	- Distance from the configuration where the sensor would be occluded - Light conditions	- Time since which the misperception starts. - Human/obstacle density in the area
Vehicle surrounded by large crowd of people	Navigation	- Information from the human motion prediction module (predicted relative distance, velocity, probability cloud)	- Time left
Collisions with fixed obstacles	Throwing phase	- Obstacle distance from the throw line - Quality of perception	- Type of object launched - Object launching speed
Collisions with moving obstacles	Throwing phase	- Obstacle distance from the throw line - Obstacle velocity toward the throw line - Quality of perception	- Type of object launched - Object launching speed
Human safety	Throwing phase	- Human distance from the throw line - Human velocity toward the throw line - Target distance	- Type of object launched - Object launching speed

Table 9: Variables from which to compute the probability and severity for each external risk

Internal risk	Stage	Probability	Severity
Overheating	Navigation	- Room temperature - Motor torques values	- Motor temperature - Time in overheating conditions
Vibrations	Pick and place Throwing phase	- Jerks' values	- Time with high jerks' values
Excessive energy consumption	Navigation	- Planned travel distance - Mobile base positive acceleration	- Battery status
Excessive energy consumption	Pick and place Throwing phase	- Joints torques - Elastic actuators exploitation index	- Battery status
Self-collisions	Pick and place Throwing phase	- Relative position - Relative velocity	- Relative velocity
Blocked Joints	Pick and place Throwing phase	- Manipulability index	- Manipulability index

Table 10: Variables from which to compute the probability and severity for each internal risk

occurrences and robot inherent global or task-dependent safety properties in a unified manner, considering reflected mass and maximum velocity.

The human motion prediction module, which will be developed in T5.1, will also be employed to compute the risk of having the vehicle surrounded by a large crowd of people, to identify which areas will be more densely occupied. An index, spanning between 0 and 1, will express the maximum predicted human density in an area up to 3 meters from the proposed planned path. The severity would depend on the margin of time against the deadline by following the currently planned trajectory.

During the throwing phase, the distance to the target will also come into play. In fact, the longer the object's flight lasts, the farther the operator or moving obstacle will have to be from the line of fire to avoid collisions. Severity, on the other hand, should take into account a parameter (between 0 and 1) indicating the danger of the thrown object in the event of a collision (weight, presence of sharp edges, material) and the speed with which the object is thrown.

5.3 Internal risks

The table 10 reports the variables on which the probability and the severity of each internal risk depend.

The chance of overheating is linked to the room temperature and the motor torque values. This risk severity would be related to the motor's temperature and the accumulated time in which the motor exceeds the design temperature.

Vibration risk is strictly related to the joints' jerks values. Prolonged exposure to vibration can cause premature deterioration of manipulator actuators, so the severity level will be computed starting from the accumulated time during the task operation on which the jerks' values overshoot a set threshold proposed at 60% of the manipulator's actuators limits.

The severity of excessive energy consumption will be assessed by comparing the actual operational cost with the one estimated. The operational cost would be assessed by computing or estimating the energy consumed during the task. For the navigation phase, the probability is linked to the length of the planned travel distance, and to the average

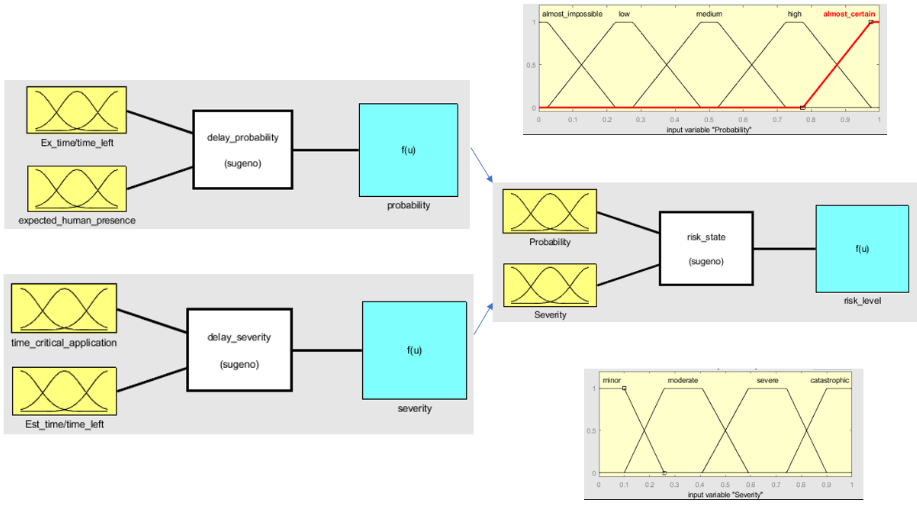


Figure 7: Delay risk level assessment using fuzzy logic. Probability depends on the rate between the estimated time to accomplish the task and the residual time before the deadline, and on the parameter representing the estimated human density in the area near the selected path. Severity depends on the same rate and on a parameter representing how much the application is time critical.

positive acceleration value. For the manipulation phase, the consumed energy, instead, is linked to the joints' torque values and to the effective exploitation of the elastic nature of the actuators.

The self-collisions risk probability would depend on the distance and relative velocity between the EE and a number of points of interest along the manipulator, plus reachable representative points of the moving base. Finally, the blocked joints risk factor is strictly linked to the Yoshikawa manipulability index, depending on the manipulator's joints configuration.

5.4 From identified variables to risk values

To map the identified variables into the discussed probability and severity levels, we can use another Takagi-Sugeno fuzzy inference system. An example of the proposed pipeline for the delay risk factor assessment is reported in fig. 7. Task 7.2 would take care of developing a continuous learning approach to assess the parameters of the membership functions and the fuzzy rules with a data-driven approach. Alternatively, in T7.2 different mapping methodologies can be studied, even if only for some risks: the output values obtained for probability and severity levels will then be equally given as input to the fuzzy inference system to quantify the level of the risk factor.

Fig. 8 shows the trends in the values of collision and non-smooth trajectory risks along three trajectories performed by a 7 DoF PANDA by Franka Emika. An obstacle is represented in the scene as a dark sphere.

Although the probability of collision risks is also manageable with a fuzzy inference system from the identified variables, we also study another approach to be able to use sensor uncertainty explicitly and quantitatively. We assume both the dynamic entity (human or obstacle) and the robot are characterized by position uncertainty having a Gaussian probability density function, we proceed as follows:

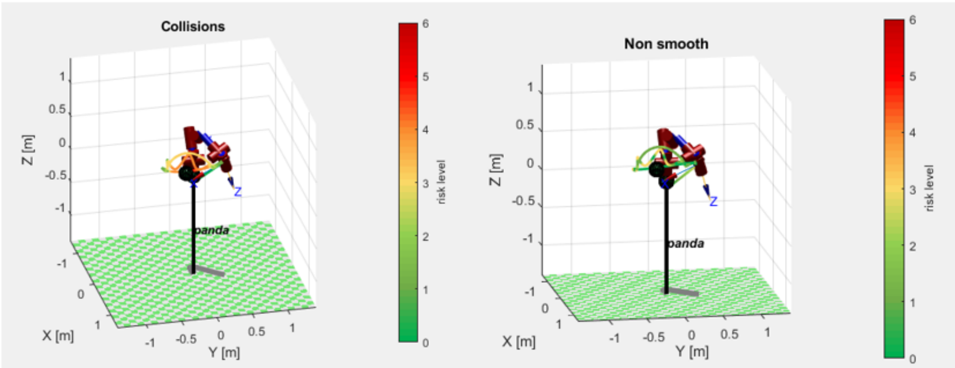


Figure 8: Visualization of the trends in the values of collision and non-smooth trajectory risks along three different trajectories.

- The probability with which the robot and the dynamic entity occupy a cell is plotted on the grid map representing the workspace.
- This occupancy probability is evaluated for all cells in the ellipse, describing the position uncertainty, both at the current time instant and at a predetermined number of prediction steps.

To compute the occupancy probability of a cell, the Gaussian probability density function characterizing the uncertainty of the position variable along each axis is discretized into multiples of its standard deviation σ. The probability with which each position variable takes a value belonging to an interval $[k*\sigma,(k+1)*\sigma]$ with k spanning between 0 and 3 was determined from the distance between the coordinate of the centre of the considered cell and the corresponding component of the robot's position vector. The probability of occupying a cell is calculated as the joint of the probabilities of taking a value along each axis. The same procedure is carried out for the dynamic entity. Next, we consider the kinematic model of the robot and the dynamic obstacles to predicting their future position distributions over time. The probability with which the robot and dynamic entity occupy each of the cells inside the ellipse, gradually increasing as time increases, is calculated, for each step in the prediction interval. The collision hazard occurs when the robot and the dynamic entity occupy the same cell, and it is calculated as the joint of their occupancy probabilities.

The total probability that there is a collision will be $1-\prod p_{\text{cell is free}}$.

Fig. 9 shows the simulation of a mobile base approaching an obstacle (a,b,c). The pink regions correspond to the positions that the robot and the obstacle, respectively, take with a higher probability, while the blue regions are the positions that are occupied by the robot and the obstacle with a lower probability. The collision risk probability increases as the distance between the robot and the obstacle decreases, and it is represented by an increase in the height of the green markers (d,e).

5.5 Normative comparison – human safety

For the human safety risk factor, it's important to compare the results found applying the methodology described in this deliverable with the limits prescribed in ISO/TS 15066. As mentioned in section 2.4, the SSM method imposes that the separation distance is greater than the distance required to stop the robot, and it is related to the probability that the collision happens. So, for this risk factor, we consider as the probability the likelihood that

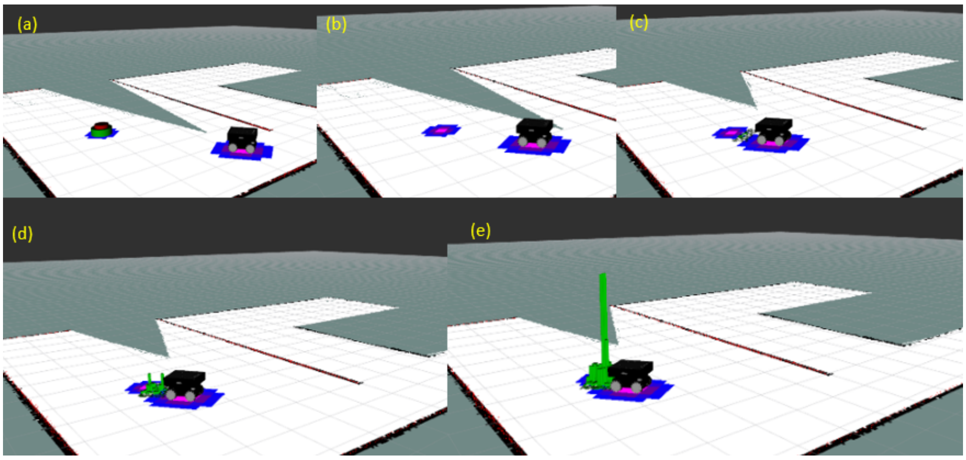


Figure 9: Visualization of collision risk probability using sensors uncertainty

the SSM criterium is not respected (so that the relative distance between the human and the robot is less than the distance the robot needs to stop). For the sake of simplicity, we consider the version used by Lucci et al. [13] where the SSM formulation is simplified as $v_{SSM} = d/T_s$, where v_{SSM} is the maximum allowed relative velocity between the robot and the human operator, d is the relative distance, and T_s is the robot's stopping time. For this example, we suppose the stopping time to be fixed at $0.5s$ and the relative distance to be modeled having a Gaussian distribution of variance $\sigma = 0.1$. In fig. 10 is reported the probability that the SSM criteria is satisfied (namely that the actual distance is higher than the required distance by SSM), for every combination of measured relative distance and relative velocity.

The PFL/SMU methods instead relate to the severity of the impact on the human operator. For this comparison example we consider as a variable the ratio of the relative speed to the limiting velocity that can be obtained by applying the SMU or PFL methodology. A simple type I Sugeno fuzzy inference system maps the value of this ratio, to the severity scale defined in section 2.3. Assuming all other variables fixed the severity values for the combination of velocity and distance are reported in fig. 11. Note that the velocity limit computed with PFL/SMU will not depend on the distance between the robot and the human (it will depend, instead on the reflective mass, type of contact, etc.), but we use the same axis of fig. 10, to then have a clear visualization of the combination of probability and severity in the same conditions.

Finally, Fig. 12 shows, for every combination of measured distance/relative velocity, the correspondent risk level obtained by the fuzzy logic system combining probability and severity from figures 10 and 11 according to the rules in fig. 2. Figures 10, 11, 12 represent the same case study. So, to visualize the corresponding levels of probability and severity to the points of the map in fig. 12, please refer to figures 10 and 11. We can notice from fig. 12 that the obtained risk level is very low when both SSM and PFL velocity requirements are satisfied. When neither constraint is fulfilled the risk value is very high, except when the velocity value is still near the intersection of the two limits. Indeed, in this case, even if neither regulations apply, the action of stopping the robot could eventually result in a collision event (SSM not guaranteed) but will slow the robot's velocity to a threshold for which the PFL is fulfilled (for the example with the method proposed in [13]). When only one of SSM and PFL is respected the computed risk value may vary from low to high values. In particular, we can observe that when the velocity is too high with respect to the limit defined by the severity component the risk level is high

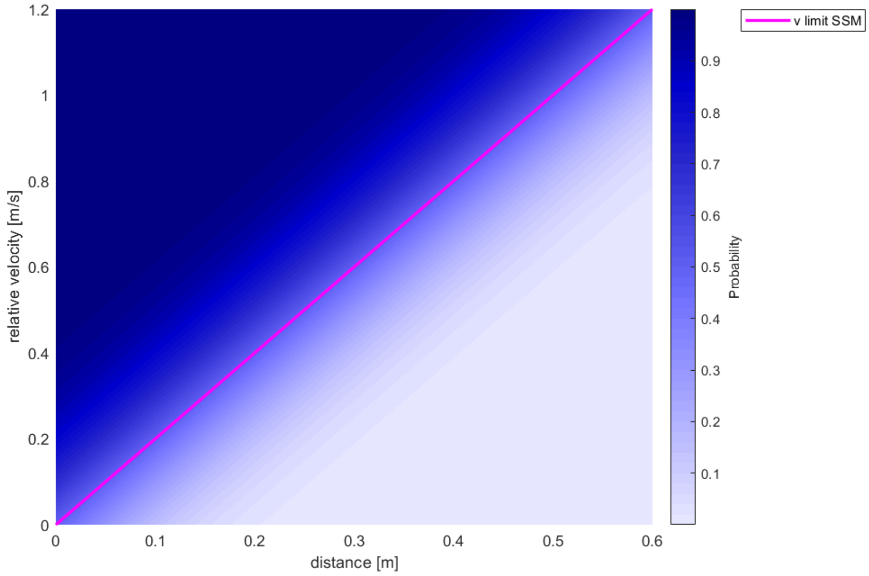


Figure 10: Probability that the relative distance is greater than the one prescribed by the SSM criterion, considering a stopping time of 0.5 s and the measured relative distance uncertainty having a Gaussian distribution with $\sigma = 0.1$

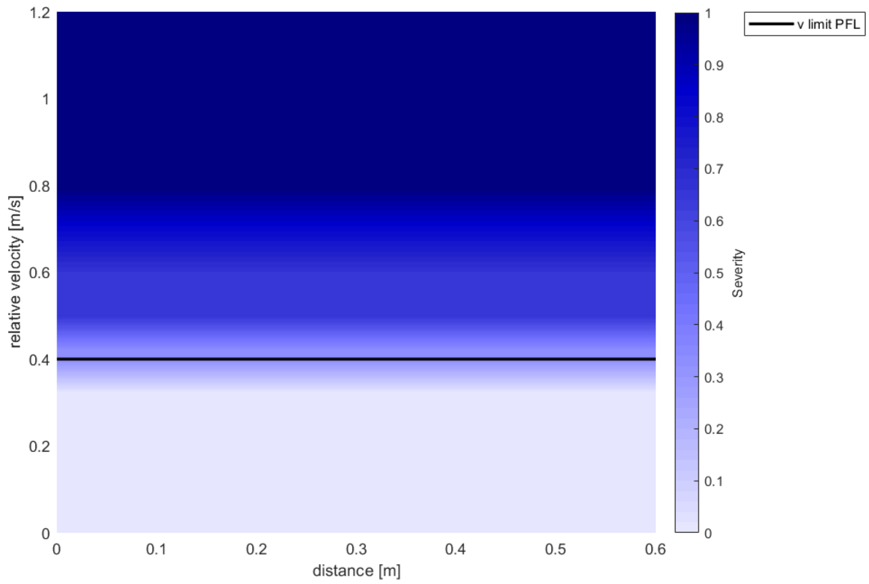


Figure 11: Severity level considering as a variable the ratio of the relative speed to the limiting velocity that can be obtained by applying the SMU or PFL methodology. Note that the severity component does not depend on the collision probability; it only refers to the consequences if a collision occurs. So the severity level is not related to the distance between the robot and the operator.

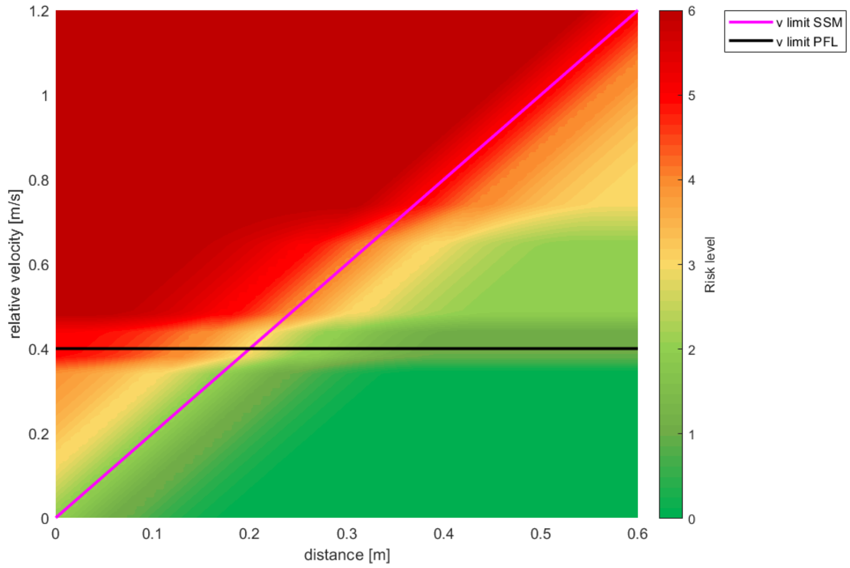


Figure 12: Visualization of risk levels as the distance and relative velocity values vary. Velocity limits prescribed by SSM (pink) and PFL (black).

even if the probability is very low. This is a desired behavior because there is a chance that a high measured distance may result from a blunder (i.e., the sensor fails to recognize the human operator), and so moving an autonomous robot in a shared environment at a speed that may result in catastrophic outcomes is to be carefully monitored.

5.6 Global risk factor

We have so far defined the level of individual risk factors. To conclude, we propose an overall risk index that can be an expression of the overall risk status of the system. A simple sum of the risk indices would not distinguish, for example, between pairs (2,2) and (0,4), so a risk factor at level 4, therefore dangerous, would not be adequately avoided. In the same way, taking as a function an infinite norm of the risk indices would not distinguish between a sequence of risk indices (0, 1, 0, 2, 0 ...) and one (2, 2, 2, 2 ...), with the former leading to a better trajectory. To overcome these issues, we propose to express the global risk factor as the RealSoftMax function of the concurrent risk factors.

$$\text{Global Risk Index} = \log(\sum e^{\text{risk factors}})$$

Minimizing previous overall risk index (or partial indexes where only groups of risks are considered) will provide a strategy for performing risk-aware motion planning in T6.2, T6.4, and T4.2.

6 Conclusions

This document formalizes the “Risk Space" concept, a multidimensional space of Risk Factors, each one combining the probability that that specific hazardous event happens and its impact.

We have identified the main risk factors from the concrete case study of the DARKO demo scenario, illustrated in D8.1. Each risk factor was then analysed, underlining the state variables and the parameters on which each risk depends. Then, we have proposed a method to assess the risk probability and severity from the state variables and parameters values and a map to pass from the severity and probability values to a final risk factor level, spanning from 0 to 6. This report ends with the proposal of a global risk index, which is defined as the real soft max of all the risk factors and represents the total risk state of the system.

References

[1] Ammar Ahmed, Berman Kayis, and Sataporn Amornsawadwatana. A review of techniques for risk management in projects. *Benchmarking: An International Journal*, 2007.

[2] ANSI/RIA. Industrial mobile robots - safety requirements - part 1: Requirements for the industrial mobile robot. Standard ANSI/RIA R15.08-1-2020, 2020.

[3] Daniel Baloi and Andrew DF Price. Modelling global risk factors affecting construction cost performance. *International journal of project management*, 21(4):261–269, 2003.

[4] Eng Seng Chia. Risk assessment framework for project management. In *2006 IEEE International Engineering Management Conference*, pages 376–379. IEEE, 2006.

[5] International Organization for Standardization. Safety of machinery - general principles for design - risk assessment and risk reduction. Standard ISO 12100:2010, Geneva, CH, 2010.

[6] International Organization for Standardization. Robots and robotic devices – safety requirements – part 1: Robots,. Standard ISO 10218-1, Geneva, CH, 2011.

[7] International Organization for Standardization. Robots and robotic devices – safety requirements – part 2: Industrial robot systems and integration. Standard ISO 10218-2, Geneva, CH, 2011.

[8] International Organization for Standardization. Robots and robotic devices – collaborative robots. Standard ISO/TS 15066:2016, Geneva, CH, 2016.

[9] International Organization for Standardization. Risk management – guidelines. Standard ISO 31000:2018, Geneva, CH, 2018.

[10] Sami Haddadin, Simon Haddadin, Augusto Khoury, Tim Rokahr, Sven Parusel, Rainer Burgkart, Antonio Bicchi, and Alin Albu-Schäffer. On making robots understand safety: Embedding injury knowledge into control. *The International Journal of Robotics Research*, 31(13):1578–1602, 2012.

[11] Oussama Khatib. Inertial properties in robotic manipulation: An object-level framework. *The international journal of robotics research*, 14(1):19–36, 1995.

[12] Zhihao Liu, Xinran Wang, Yijie Cai, Wenjun Xu, Quan Liu, Zude Zhou, and Duc Truong Pham. Dynamic risk assessment and active response strategy for industrial human-robot collaboration. *Computers & Industrial Engineering*, 141:106302, 2020.

[13] Niccolò Lucci, Bakir Lacevic, Andrea Maria Zanchettin, and Paolo Rocco. Combining speed and separation monitoring with power and force limiting for safe collaborative robotics applications. *IEEE Robotics and Automation Letters*, 5(4):6121–6128, 2020.

[14] Nico Mansfeld, Mazin Hamad, Marvin Becker, Antonio Gonzales Marin, and Sami Haddadin. Safety map: A unified representation for biomechanics impact data and robot instantaneous dynamic properties. *IEEE Robotics and Automation Letters*, 3(3):1880–1887, 2018.

[15] A. Nieto-Morote and F. Ruz-Vila. A fuzzy approach to construction project risk assessment. *Elsevier*, 29:220–231, feb 2010.

[16] Andrey Rudenko, Luigi Palmieri, and Kai O Arras. Predictive planning for a mobile robot in human environments. In *Proc. of the IEEE Int. Conf. on Robotics and Automation (ICRA), Works. on AI Planning and Robotics*, 2017.

[17] Andrey Rudenko, Luigi Palmieri, Johannes Doellinger, Achim J Lilienthal, and Kai O Arras. Learning occupancy priors of human motion from semantic maps of urban environments. *IEEE Robotics and Automation Letters*, 6(2):3248–3255, 2021.

[18] Chittaranjan Srinivas Swaminathan, Tomasz Piotr Kucner, Martin Magnusson, Luigi Palmieri, and Achim J Lilienthal. Down the cliff: Flow-aware trajectory planning under motion pattern uncertainty. In *2018 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, pages 7403–7409. IEEE, 2018.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101017274