Grant agreement No: 101017008

Harmony

Assistive robots for healthcare

Enhancing Healthcare with Assistive Robotic Mobile Manipulation

(HARMONY) | H2020-ICT-2018-20| RIA

Start of the project: 01.01.2021
Duration: 42 months

Deliverable Number	8.1
Deliverable Name	Evaluation of risks associated with the use of mobile manipulator robots in hospitals
WP Number	8
Lead Beneficiary	UT
Dissemination Level	Public
Internal Reviewer	KUH, USZ
Due Date	31-12-2021
Date of Submission	
Version	1.0

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101017008

Revision History

Version	Date	Author(s)	Comments
0.1	17-12-2021	Bob Schadenberg (UT)	First draft
1.0	17-01-2021	Bob Schadenberg (UT)	No comments for revision from KUH and USZ

Table of Contents

1. Summary **4**

2. Introduction **5**

3. Risk Management and Assessment **6**

3.1 Brief Overview on Risk Management 6

3.1.1 Scope and Risk definitions 6

3.1.2 Methods to risk assessment 7

3.1.3 Monitoring and reviewing risk assessments 8

3.2 Risk Assessment in Robotics 9

3.2.1 Robot specific standards 10

3.2.2 Mitigating risks in robotic systems 10

4. HARMONY Risk Assessment **12**

4.1 Method 12

4.2 Results 13

5. Discussion and Conclusion **14**

5.1. Limitations 15

References **16**

Appendix A: Results of the preliminary risk assessment of the Harmony robots **18**

Appendix B: Results of the FMEA for the IDMind Robot **34**

1. Summary

In this deliverable, we describe how we evaluated the risks that are associated with the Harmony robots that are to be used in our user studies. We first briefly describe what risk management and assessment entails, how this relates to risks of robotic systems, and how risks can be mitigated in such systems. We carried out a preliminary risk assessment with the whole consortium to identify potential risks of the Harmony robots in our user studies. This led to the identification of 50 risks, of which two warrant additional mitigation. Firstly, to prevent collisions, the robots will need a robust emergency stop system and cliff detection. Secondly, the user studies should be run with proxy materials, rather than actual bioassay samples, and staff should not rely on the performance of the robot. Given the preliminary nature of the risk assessments, the identified risks should also not be considered an all-inclusive list that guarantees safety. It is therefore important that we monitor and review our risk assessment as the Harmony project progresses and the robots' software and hardware architectures become clear.

2. Introduction

Traditionally, ensuring safety in robotic systems was solved by ensuring that people could not get near the robot (e.g., by putting the robot behind a fence). Nowadays, robots are also being used in environments where they will get in close proximity to people. For such robots, additional safeguards need to be put in place, such as implementing sensors that can be used to detect and respond to people who may be a risk. Other aspects of safety include safety through control, motion planning, prediction, or through consideration of psychological factors (Lasota, Fong & Shah, 2017). However, prior to implementing safety in a novel robot design, we first need to understand what risks are associated with our robots in the Harmony project. In this deliverable, we therefore specifically focus on risk assessment.

The aim of a risk assessment is to identify potential hazards, estimate the associated risks, and come up with mitigation strategies when a risk is estimated to be too big. This is a process that needs to be carried out throughout the design phase of a product. For Harmony, we carried out a preliminary risk assessment, and a risk assessment specific to the IDMind robot, both of which are reported in this deliverable. In addition, ABB will carry out a detailed risk assessment on the hYuMi robot according to industry standards. This assessment will be carried out when the robot is more developed, as the robot's architecture will then be more clear.

In the rest of the deliverable, we will first give a brief overview of risk management and assessment in Section 3. We then discuss how risk assessment applies to robotic systems in Section 4, as well as in what way robots differ from other technology in this regard. In Section 5, we present the results of the risk assessment that we carried out to identify risks associated with the Harmony robots for our user studies. Finally, in Section 6, we discuss our risk assessment and conclude on this deliverable. The full risk assessments can be found in the Appendix.

3. Risk Management and Assessment

3.1 Brief Overview on Risk Management

3.1.1 Scope and Risk definitions

According to the International Standard ISO 31000 "Risk Management –Principles and guidelines", risk management "involves the systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk" (ISO, 2018)(also see Figure 1). Risk management can be applied at different levels (e.g. strategic, operational, programme, project, or other activities), but for the remainder of this deliverable, we set the context of our risk management to the design of the Harmony robots. The goal of our risk management is:

to develop robot prototypes that are safe to be tested in a hospital setting where they carry out tasks related to unpacking and sorting bioassay samples and delivering such samples to other locations within the hospital.

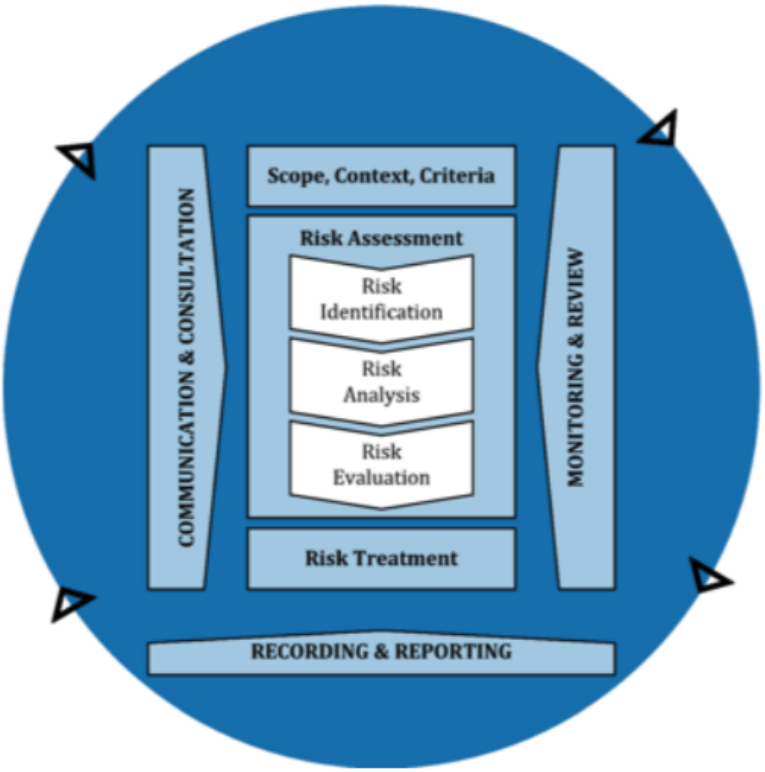

Figure 1. Risk Management process (taken from ISO, 2018).

The Society for Risk Analysis considers the following definitions for risk (SRA, 2018):

1. Risk is the possibility of an unfortunate occurrence.
2. Risk is the potential for realization of unwanted, negative consequences of an event.
3. Risk is exposure to a proposition (e.g.,the occurrence of a loss) of which one is uncertain.
4. Risk is the consequences of the activity and associated uncertainties.
5. Risk is uncertainty about and severity of the consequences of an activity with respect to something that humans value.
6. Risk is the occurrences of some specified consequences of the activity and associated uncertainties.
7. Risk is the deviation from a reference value and associated uncertainties.

Taken together, risk is about adding the uncertainty dimension to events and consequences (Aven, 2016). A common metric for risk is to consider the *likelihood* and *severity* of the consequences of a risk, and the *detectability* of the failure before it causes harm. Sometimes, the knowledge relating to the likelihood and severity estimates are also considered, where less knowledge reflects a greater uncertainty regarding the risk. Given that the Harmony project has little knowledge on which to build the initial risk assessment, we will not consider knowledge in this deliverable.

3.1.2 Methods to risk assessment

To achieve the goal of our risk management (see previous page), we will conduct a risk assessment. Such assessments are generally conducted using brainstorming methods or checklists, both of which are based on experience and expert knowledge. While there are a variety of techniques for conducting risk assessments (see Huck et al., 2021 for a review on risk assessments for robotic systems), they generally involve the following four steps (Aven, 2016). (1) Identify situations and events (hazards/threats/opportunities) that can affect the activity, (2) analyse the consequences of such situation and events, (3) make judgements of the likelihood of the events and their consequences, and establish a risk description or characterisation, (4) evaluate the risk, (5) make recommendations regarding the treatment of the risk.

Giving an overview of all methods for risk assessment is beyond the scope of this deliverable. But there are four common methods for carrying out a risk assessment, namely by conducting a HAZOP (HAZard and OPerability study), FMECA (Failure Mode Effect and Criticality Analysis), Fault Tree Analysis (FTA), or Systems Theoretic Process Analysis (STPA) (Ericson, 2015). Both techniques rely on brainstorming sessions for identifying and assessing risks, with experts from diverse backgrounds, as each expert knows the small intricacies of their part of the system they work on. The multi-disciplinary approach also allows risks to be viewed from different viewpoints, hopefully getting a more holistic overview of all risks.

Of the commonly used methods, HAZOP is a top-down approach which puts hazards central. HAZOP assumes that risk events are caused by deviations from design or operating

intentions. Identification of such deviations is facilitated by using sets of "guide words" (e.g., no, more, less, too much) as a systematic list of deviation perspectives. For each hazard (e.g. hazards related to kinetic energy, usability, security), participants of the brainstorming session will come up with ways that a hazardous situation related to a hazard could occur with the product. For instance, by asking "how can people get physically hurt through kinetic energy from the robot?", or "how can people's privacy get compromised by the robot?". Once a hazardous situation has been identified, participants think of the effect this situation has on the user, the likelihood of the situation occurring, the severity of the consequences, and finally make a decision on whether and how the risk can be mitigated.

In contrast to HAZOP, FMECA is a bottom-up approach that starts at a low-level of the product (e.g. components) and then gradually works its way up to the effects of the subsystem (sets of components) or system level (the full product). Participants think of a way that the component could fail, and what situation this could result in. For instance, "how can the depth camera sensor fail?". Similar to HAZOP, participants then think of what effect this situation has on the user, the likelihood of the situation occurring, the severity of the consequences, and finally make a decision on whether and how the risk can be mitigated.

FTA is typically used to assess probabilities of failures in a quantitative manner. It uses a top-down approach where it starts at a certain failure and then deduces how this failure might come about using a diagram. In this diagram, events that can cause or contribute to a failure are represented by symbols. The relation between the symbols is denoted using boolean logic (e.g., "and", "or"), and statistical probabilities. Given that much is still unsure about the Harmony robots, this technique might be less applicable given its focus on quantification of risks.

STPA is a relatively new hazard analysis technique compared to the other three, and is used to analyse complex systems. Rather than breaking the product into smaller components, examining and analysing each component in isolation (and then combining the results in order to understand the behavior of the composed components), STPA uses a model of the system that consists of a functional control diagram. To apply STPA, this diagram needs to be known, and from it, all control loops in the system are identified. Next, all components that contribute to unsafe behavior of the studied system are identified in each control loop. Thus, STPA considers safety as a system’s control (constraint) problem rather than a component failure problem. At the current stage of the Harmony project, we do not yet have a functional control diagram, making STPA unsuitable at this stage.

3.1.3 Monitoring and reviewing risk assessments

Risk assessment processes are ongoing processes that require periodic reassessment during development (and continues throughout the entire product lifecycle). Reassessment of risk is particularly important whenever significant changes are made to the product or associated manufacturing process. Very early in development and when relatively little experimental

work has been conducted, risk assessment will likely be based primarily on the expected functions of a product and expected use, rather than the product components which are to facilitate the functions and actual use. The primary outcomes of such early risk assessments are generally the need for additional investigation to characterise the source of the risk more fully. However, for initial user studies with the product, the identified risks will already need to be either reduced or accepted.

3.2 Risk Assessment in Robotics

Traditionally, ensuring safety in robotic systems was solved by ensuring that people could not get near the robot (e.g., by putting the robot behind a fence). Nowadays, robots are also being used in environments where they will get in close proximity to people. Safety is typically ensured through various types of safety systems that help to avoid collisions, limit impact severity to the acceptable level in case of collisions, approaches to human-aware navigation, and strategies for safe navigation in dynamic environments. However, according to the Engineering and Physical Sciences Research Council (EPSRC), safety in robotics should not only encompass physical and material safety, but also the avoidance of disruption to psychological, social, moral, and other important values (Boddington, 2017). For instance, psychological discomfort or stress can also be induced by a robot's appearance, embodiment, gaze, speech, posture, and other attributes (Mumm and Mutlu, 2011).

Risk assessments on robotic systems are difficult, as the technology poses several challenges (Huck et al., 2021). Firstly, robots are complex systems with numerous design factors (e.g., type of robot) and dynamic effects (e.g., collision forces). This can lead to hazards being overlooked. Secondly, robots that operate in close proximity to people, or in human-centred environments, are still very novel. There is therefore a lack of safety knowledge and experience with such robots. Thirdly, predicting human behaviour and autonomously responding to this is required for robots in human-centred environments. However, this is also very challenging, and can lead to safety risks when a person's behaviour is incorrectly predicted. Lastly, robots colliding with people is a risk for robots that are to operate in human-centred environments. A collision in itself is not necessarily a risk, but depends on the force and pressure of the collision. Estimating these aspects of collisions, and modelling them in the robot so that it can act accordingly is costly. Even though risk assessments on robotic systems are difficult, there are already many requirements specified that should lead to safe robots. In the remainder of this section, we will discuss what documentation is available for designing safe interactions between humans, and various ways on how we can mitigate risks in robots or our user studies.

3.2.1 Robot specific standards

The International Organization for Standardization (ISO) has been working toward specifying how best to maintain safety during interaction between humans and robots. There are several ISO standards that apply to the Harmony robots. The basic standards are laid out in ISO 10218, which relates to safety standards for *industrial* robots and consists of two parts. Part one (ISO, 2011a) mainly focuses on safety features of the robot itself, whereas part two (ISO, 2011b) specifies requirements for the robot within its application environment (e.g., for its interaction with people) and contains a checklist of potential hazards. While part two specifies some requirements for human-robot collaboration, this is elaborated on in ISO/TS 15066: a technical specification (ISO, 2016). While these ISO reports relate to industrial robots, they are extended by ISO 13482:2014 (ISO, 2014), which specifies requirements and guidelines for the safe design of personal care robots (i.e., mobile servant robot, physical assistant robot, person carrier robot) for non-medical applications, and complements ISO 10218. These are the three international standards that apply to the Harmony robots.

The ISO standards mainly relate to physical and material safety. In addition, Salvini and colleagues (2021) note that conventional risk assessment techniques do not sufficiently address the safety of bystanders and pedestrians for robots that are to work in public spaces. They therefore extended the hazards mentioned in ISO 13482:2014 (ISO, 2014) with a number of additional hazards that focus on bystanders and pedestrians, and on psychological safety.

3.2.2 Mitigating risks in robotic systems

Once the risks associated with a product have been assessed, a decision has to be made to either accept the risk (when the risk is not too critical), or to make recommendations to reduce the risk. There are various ways for doing so, and describing all such ways is beyond the scope of this deliverable. For a review and detailed description on all various ways to mitigate risks for robots that operate in human-centered spaces, we refer to Lasota, Fong & Shah (2017) and Zacharaki et al. (2020). In this section, we will briefly summarise generic ways in which robots can be made more safe, based on software control methods, hardware design, and user study protocol design.

One of the most common ways is through controlling robot motion at a low-level (i.e., that does not rely on complicated prediction models or planners). The simplest way of doing so is by enforcing limits on the robot's speed or energy, by monitoring the physical distance between the human and robot and adjusting robot speed accordingly. More advanced methods have also been investigated. For instance, there are methods that aim to prevent collisions by gradually slowing a robot's motion based on safety zones, separation distance from the human, and human behaviour (e.g., gaze) (Polverini et al., 2014; ABB, 2015). In some cases, collisions (i.e., physical contact) are required for a task, such as can be the case in human-robot collaboration. It is then important to limit the severity of the impact, rather

than preventing collisions. "Post-collision" methods can be implemented in this case, which aim to detect a collision, localise where on the robot contact was made, and then decide on how to proceed.

The downside of controlling robot motion at a low-level is that it can have a negative impact on the effectiveness of the robot by making it overly conservative. There are also more complex ways of ensuring human safety that have less impact on the effectiveness of a robot, and can deal with more complex or proximate interactions. Such methods are based on models that predict human motion (and make the robot respond accordingly), or plan the robot's motion trajectories. These methods can not only prevent collisions, but do so in a manner that does not negatively impact the perceived safety and comfort of users (Lasota and Shah, 2015). In the design of robot behaviour, it is also possible to improve the physical and psychological safety of users. For instance, people can anticipate the robot's motions by designing behaviour to quickly communicate its intent with its action (legibility), as well as what it intends to do afterwards (predictability). Such behaviour can also reduce people's discomfort when seeing the robot (Schadenberg et al., 2021).

A different approach to the one described above is making robots more safe, and be perceived as such, by designing the robot's appearance to that end (Zacharaki et al., 2020). By using user-friendly materials, such as soft-bodied robots (not unlike Baymax from the movie Big Hero Six), the impact of a collision can be mitigated. While soft robotics is a hot topic, using soft materials brings a host of challenges regarding the deformation, kinematics, and the control of the soft joints.

In the case of Harmony user studies, another way of mitigating risk is by changing the research protocols. For instance, we could opt to use a Wizard-of-Oz paradigm (Riek, 2012) where a researcher sees the robot's surroundings and is controlling the robot (unbeknownst to any participants). Such a research method would circumvent the need to rely on the robot's perception, reasoning, and action selection. The downside of this method is that it can reduce the impact of the results, because in the end robots will need to work autonomously in the Harmony scenarios. To that end, we will need to assess the robot's perception, reasoning, and action selection *in situ*. Alternatively, to increase safety through the research protocol could involve using an empty hallway, informing people about the robot and how to make it stop, or use protective gear for participants in human-robot collaborations.

4. Harmony Risk Assessment

4.1 Method

At this stage in Harmony (M11), we do not yet know all the components of the Harmony robots. These will be defined as the project progresses. The risk assessment that we carried out therefore focuses on functions (e.g. object recognition). For the same reason, we also opted to do a preliminary HAZOP.

The risk assessment was carried out in three sessions with delegates from each of the Harmony partners, including the Ethical and Safety Board. In each session, we looked at various hazards that might be relevant to the Harmony robots, and had a brainstorm on what series of events could lead to a hazard. To this end, we used the hazards specified in ISO 13482:2014, with the addition of those specified by Salvini, Paez-Granados & Billard (2021). To denote the severity, occurrence, detectability, and calculate the resulting criticality index, and interpret its value to quantify the risk, we used the definitions in Figure 2. To check whether we did not miss any obvious risks. In one of the sessions, we also did an unstructured brainstorm on risks related to one of the use cases.

Severity

Effect	Criteria	Score
Catastrophic	Results in death or device does not comply to Annex I of MDR (EU) 2017/745 (see 4.01.x GSPR checklist).	5
Critical	Affects performance of the product, may result in serious adverse effects like permanent impairment or life-threatening injury.	4
Serious	Highly likely to affect the performance of the product, may result in injury or impairment requiring professional medical intervention	3
Minor	May affect the performance of the product, may result in temporary injury or impairment not requiring professional medical intervention	2
Negligble	No effect on the product or related application(s). No effect on safety of the user. Minor/no inconvenience or temporary discomfort for the patient.	1

Occurance

Degree	Criteria	Score
Very often	All of the uses (100%)	10
Often	30% to 100% of uses	9
Regular	10% to 30% of uses	8
Very likely	3% - 10% of uses	7
Likely	1% to 3% of uses	6
Unlikely	0.1% to 1% of uses	3
Very unlikely	< 0.1% of uses	1

Figure 2. Criteria used to denote severity, occurrence, detectability, and risk.

Detectability

Degree	Criteria	Score
Impossible	Failure detection is not possible	10
Very low	Failure is almost certainly not possible to detect	9
Low	Failure is difficult to detect	8
High	Failure can be detected	5
Very high	Failure is usually detected	3
Almost certain	Failure is almost certainly detected	1

Criticality Index

Risk is expressed as Criticality Index (CI):
CI = Severity * Occurrence * Detectability

Risk determination

Result value	Risk determination
0 - 199	Negligible
200 - 499	Tolerable
500 - 799	Undesired
> 800	Intolerable

Figure 2. Figure 2 continued.

4.2 Results

The notable results from the risk assessment are discussed in Section 5. For *all* safety risks that were identified, please see Appendix A. The results for the FMEA carried out on the IDMind robot can be seen in Appendix B.

5. Discussion and Conclusion

Through our risk assessment, we identified 50 events, or sequences of events, that may lead to risks to users. Both physical and psychological risks. All risks, however, were estimated with a criticality index of below 200, and are therefore classified as negligible. There were certain risks that we estimated could have a high severity of harm when they occur. These had to do with collisions, where people might get hit or crushed by the robot. In particular, a robot falling from the stairs is a dangerous situation. The occurrence of risks of collision were rated as very low however, as the safety stop system should become active in time and thus prevent these situations.

To prevent collisions, it is critical that the robots are equipped with robust sensors that can detect when people are too close, and cause the robot to stop. These are well known requirements and are also well described in the relevant ISO documentation (ISO 2011a, 2011b, 2014) as emergency or protective stop. Similarly, the robots will need to be able to detect cliffs so that the robot does not drive off one. In case of stairs, such detection is required to prevent the robot from falling off the stairs and potentially colliding with people on the stairs. We estimated that robust sensors, that run outside of the normal control system (i.e. ROS2) (in case this system gets overloaded) should be sufficient to prevent collisions when the robot is driving around the hospital. Additionally, a remote (observed by a researcher) or on-board button that shuts off the robot may be useful in further preventing collisions. One notable exception is when a person runs too fast for the sensor to keep up. When this person does not notice the robot, a collision could occur. However, we deem this unlikely to occur during our user studies.

One of the hazards that was identified in the free brainstorming session was the hazard of the robot not completing its task. As a result, the whole bioassay sample flow could come to a halt were it to rely completely on the robot(s) to perform this task. Given that most systems will have a Technology Readiness Level of 5 at the end of the project, it is very likely that the robot will not always be able to carry out its tasks. To mitigate this risk in our user studies, we propose that the robots will only carry out non-emergency tasks, and do them in parallel to the current bioassay sample flow, so as not to disrupt this chain. Furthermore, there is no need for the robots to carry actual bioassay samples, as we could fill the tubes with a proxy material. This will prevent any potential risks of bioassay samples being exposed and lost due to breaking of samples.

To conclude, we propose two risk mitigation actions. First, the Harmony robots will need a robust emergency stop system. Through the use of robust sensors that stop the robot when a person gets too close, or when a cliff is detected, and a physical/remote-controlled button to stop the robot. Secondly, the user studies should use proxy materials for the scenarios, and hospital staff should not rely on the robot's performance in the study. As a final remark, we should be mindful of participant safety when designing our research

protocols. If there are actions we can take that won't impact the results of a study, but increase the safety of participants, we should consider implementing those actions.

5.1. Limitations

At the time of the risk assessments, much is still unclear about the exact hard and software that the Harmony robots will have. We therefore stress that this is a *preliminary* risk assessment. The identified risks should also not be considered an all-inclusive list that guarantees safety. It is therefore important that we monitor and review our risk assessment as the Harmony project progresses and the robots' software and hardware architectures become clear.

An additional limitation of the risk assessment that we carried out is the limited experience of the participants in conducting them. Most had no experience with risk assessment, which could result in the identification of fewer risks.

References

ABB (2015). *Yumi - creating an automated future together*. ABB, http://new.abb.com/products/robotics/yumi.

Aven, T., Ben-Haim, Y., Boje Andersen, H., Cox, T., Droguett, E. L., Greenberg, M., Guikema, S., Kröger, W., Renn, O., Thompson, K. M., & Zio, E. (2018). *Society for risk analysis glossary*. Society for Risk Analysis, August.

Boddington, P. (2017). EPSRC Principles of Robotics: commentary on safety, robots as products, and responsibility. *Connection Science*, *29*(2), 170–176. https://doi.org/10.1080/09540091.2016.1271396

Dogramadzi, S., Giannaccini, M. E., Harper, C., Sobhani, M., Woodman, R., & Choung, J. (2014). Environmental hazard analysis-a variant of preliminary hazard analysis for autonomous mobile robots. *Journal of Intelligent & Robotic Systems*, 76(1), 73-117.

Ericson, C. A. (2015). *Hazard analysis techniques for system safety*. John Wiley & Sons.

ISO (2011a). *Robots and robotic devices - Safety requirements for industrial robots - Part 1: Robots*, International Organization for Standardization, Geneva.

ISO (2011b). *Robots and robotic devices - Safety requirements for industrial robots - Part 2: Robot systems and integration*, International Organization for Standardization, Geneva.

ISO. (2014). *Robots and robotic devices - Safety requirements for personal care robots*, International Organization for Standardization, Geneva.

ISO (2016). *ISO/TS 15066 - Robots and robotic devices - Collaborative robots*, International Organization for Standardization, Geneva.

ISO (2018). *ISO 31000:2018 Risk management - Principles and guidelines*, International Organization for Standardization, Geneva.

Lasota, P. A., & Shah, J. A. (2015). Analyzing the Effects of Human-Aware Motion Planning on Close-Proximity Human–Robot Collaboration. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *57*(1), 21–33. https://doi.org/10.1177/0018720814565188

Lasota, P. A., Fong, T., & Shah, J. A. (2017). A Survey of Methods for Safe Human-Robot Interaction. *Foundations and Trends in Robotics*, *5*(3), 261–349. https://doi.org/10.1561/2300000052

Mumm, J., & Mutlu, B. (2011). Human-robot proxemics: Physical and Psychological Distancing in Human-Robot Interaction. *Proceedings of the 6th International Conference on Human-Robot Interaction - HRI '11*, 331. https://doi.org/10.1145/1957656.1957786

Polverini, M. P., Zanchettin, A. M., & Rocco, P. (2014). Real-time collision avoidance in human-robot interaction based on kinetostatic safety field. In *2014 IEEE/RSJ International Conference on Intelligent Robots and Systems* (pp. 4136-4141).

Salvini, P., Paez-Granados, D., & Billard, A. (2021). On the Safety of Mobile Robots Serving in Public Spaces. *ACM Transactions on Human-Robot Interaction*, *10*(3), 1–27. https://doi.org/10.1145/3442678

Schadenberg, B. R., Reidsma, D., Heylen, D. K. J., & Evers, V. (2021). "I See What You Did There": Understanding People's Social Perception of a Robot and Its Predictability. *ACM Transactions on Human-Robot Interaction*, *10*(3), 1–28. https://doi.org/10.1145/3461534

SRA (2018). *Glossary society for risk analysis*. https://www.sra.org/risk-analysis-introduction/risk-analysis-glossary/ (accessed 18 November 2021).

Riek, L. D. (2012). Wizard of Oz Studies in HRI: A Systematic Review and New Reporting Guidelines. *Journal of Human-Robot Interaction*, *1*(1), 119–136. https://doi.org/10.5898/JHRI.1.1.Riek

Rouff, C.A., Hinchey, M., Rash, J., Truszkowski, W., Gordon-Spears, D. (2006). *Agent Technology from a Formal Perspectiv*e. Springer

Zacharaki, A., Kostavelis, I., Gasteratos, A., & Dokas, I. (2020). Safety bounds in human robot interaction: A survey. *Safety Science*, *127*, 104667. https://doi.org/10.1016/j.ssci.2020.104667

Appendix A: Results of the preliminary risk assessment of the Harmony robots

ID #	Hazard	Reasonably foreseeable sequence or combination of events	Hazardous situation	Harm	Notes	Occurrence	Severity	Detectability	**Criticality Index**
	Hazards due to energy storage and supply								
	Contact with hazardous energy parts								
1	Harmful contact with high mechanical energy sources	A large object collides with the robot, destroying the casing around the battery and exposing it.	The battery is hazardous to touch	Biochemical harm, equipment damage		1	4	10	40
	Uncontrolled release of stored energy								
2	Unintended shutdown	When the robot's power supplies stops providing power, the robot's arms may fall down, potentially colliding with a person	Robot arm colliding with a person due to loss of power	Physical harm		1	5	10	50
	Power failure or shutdown								

ID #	Hazard	Reasonably foreseeable sequence or combination of events	Hazardous situation	Harm	Notes	Occurrence	Severity	Detectability	**Criticality Index**
3	Power failure	When an object is stuck on the wheels, it could provoke an overcurrent, causing the battery to shut down, which causes the robot to stop.	Robot arm colliding with a person due to loss of power	Physical harm		1	5	10	50
	Hazards due to robot shape								
4	The robot's appearance does not elicit an acceptable level of perceived safety	Robot too big/heavy	Perceived loss of safety	Psychological safety		6	1	10	60
5	,,	Robot has the ability to change its shape (e.g. move its arms), which could be perceived as the potential to be hit by the robot	Perceived loss of safety	Psychological safety		3	1	10	30
6	,,	Robot looks dirty, or be perceived as unclean	Perceived loss of safety	Psychological safety		6	1	10	60

ID #	Hazard	Reasonably foreseeable sequence or combination of events	Hazardous situation	Harm	Notes	Occurrence	Severity	Detectability	**Criticality Index**
7	The robot's appearance does not elicit an acceptable level of perceived privacy	Entering patients room	Perceived loss of privacy	Psychological safety		1	3	4	12
8	Hazardous robot shape profile during collisions	Robot's cabling might dislodge a bioassay sample, which then could be spilled	Contamination	Biochemical harm		6	3	3	54
	Hazards due to stress, posture and usage								
	Physical stress and posture hazards								
9	Stressful posture required for robot operation	Reading the tablet interface might cause stress on the body	Repetitive stress on the body	Musculoskeletal disorder		6	3	10	180
10	,,	Loading the robot, or learning from demonstration	Repetitive stress on the body	Musculoskeletal disorder		6	3	10	180
11	Poor user interface design and/or location of indicators and visual displays units	Difficult to read the user interface	strain on the eyes	Tiring, eye problems		6	2	10	120

ID #	Hazard	Reasonably foreseeable sequence or combination of events	Hazardous situation	Harm	Notes	Occurrence	Severity	Detectability	**Criticality Index**
12	Poor visibility of robot	Robot could block the view of a child	run into child	Physical harm		1	1	10	10
	Mental stress and usage hazards								
13	Unclear method for communicating with robot	Robot's appearance signal incorrect ways of communicating with it, or the robot does not communicate clearly with the user	Distress	Psychological discomfort		9	1	8	72
14	Robot performs behaviour that is perceived as unsafe	Robot drives too close to a person (invade personal space)	Distress	Psychological safety		9	1	10	90
15	Robot is not performing well enough	Robot is not performing its task well enough, and will need user involvement to perform well	Annoyance, stress, additional workload	Psychological discomfort		7	1	1	7
	Hazards due to robot motion								
	Mechanical instability								

ID #	Hazard	Reasonably foreseeable sequence or combination of events	Hazardous situation	Harm	Notes	Occurrence	Severity	Detectability	**Criticality Index**
16	Mechanical instability – over-turning while handling loads	Robot grabs something that is too heavy	Robot falls onto a person	Crushing	Payment load is about 1kg, which is not enough to cause mechanical instability	1	3	10	30
	Collision with safety-related obstacles								
17	Collision with safety-related objects	Collision with a person because the person is running too fast for the robot to stop in time	Person collides with robot	Impact injuries	In this case, the safety-stop might not stop the robot in time	2	4	8	64
18	,,	Collision because person is out of view (e.g. coming from a stairwell)	Person collides with robot	Impact injuries	Safety-stop will stop the robot when a person gets too close	5	2	5	50

ID #	Hazard	Reasonably foreseeable sequence or combination of events	Hazardous situation	Harm	Notes	Occurrence	Severity	Detectability	**Criticality Index**
19	,,	Collision because robot hardware is overloaded and does not recognise safety-related objects in time	Safety-related object collides with robot	Impact injuries	Safety-stop is running locally and not integrated in ROS, which should prevent such overloads of the system	2	4	8	64
20	,,	Collision due to arms might move out of the visual sensor suite (exc. proprioceptive)	Safety-related object collides with robot	Impact injuries	The robot then has to rely on its proprioceptive sensors.	5	2	5	50
21	Collision with safety-related objects	Collision because robot motion might have an offset causing them to end up in an unintended position, which can then cause a collision with a safety-related object	Safety-related object collides with robot	Impact injuries		6	2	2	24

ID #	Hazard	Reasonably foreseeable sequence or combination of events	Hazardous situation	Harm	Notes	Occurrence	Severity	Detectability	**Criticality Index**
22	Collision with safety-related objects	Collision because the reconstruction of the scene is incorrect, which can cause the robot's actuators to be in an unintended position. This then can cause a collision.	Safety-related object collides with robot	Impact injuries		7	2	2	28
23	Collision with fragile safety-related objects	Fragile items might break because the perception of the fragility might not be correct	The contents of the item, or the material (e.g. glass) may get into contact with people	Biochemical, cutting	For instance, the bioassay samples themselves	6	3	5	90
24	Collision with walls, permanent/ unmovable barriers	Collision with glass door/panels because sensor has difficulty with glass surfaces	Robot collides with glass door/panels	Damage to robot and environment		6	3	5	90
	Hazardous psychological effects due to robot motion								

ID #	Hazard	Reasonably foreseeable sequence or combination of events	Hazardous situation	Harm	Notes	Occurrence	Severity	Detectability	**Criticality Index**
25	The robot motion does not elicit an acceptable level of perceived safety	Navigation style might be seen as unsafe, or unpredictable	People might feel unsafe near the robot, or experience discomfort	Psychological safety		8	2	10	160
26	„	Invading personal space	People might feel unsafe near the robot, or experience discomfort	Psychological safety		7	2	10	140
27	„	Robot might move too fast	People might feel unsafe near the robot, or experience discomfort	Psychological safety	IDMind's robot might drive at max 1.8m per second	6	2	10	120
28	„	Arm motions may be perceived as going to fast, or making dangerous movements	People might feel unsafe near the robot, or experience discomfort, or stop wanting to	Psychological safety		6	2	10	120

ID #	Hazard	Reasonably foreseeable sequence or combination of events	Hazardous situation	Harm	Notes	Occurrence	Severity	Detectability	**Criticality Index**
			work with the robot						
	Hazards due to incorrect autonomous decisions and actions								
29	Harmful action taken in performing tasks	Perception does not reach, or is delayed, decision making modules, causing incorrect decisions	Robot does not plan a collision-free path	Impact injuries	Robot failsafe to stop the robot automatically will kick-in	4	3	3	36
30	,,	,,	Robots drives off the stairs or elevator	Impact injuries	Sensor (processing) overloaded, does not work correctly, and the cliff-detector of the robot does not detect a cliff in time	3	5	3	45

ID #	Hazard	Reasonably foreseeable sequence or combination of events	Hazardous situation	Harm	Notes	Occurrence	Severity	Detectability	**Criticality Index**
31	Items are displaced	Robot unloads bioassay samples in the wrong place, because user input the wrong room on the box, or the room is not scanned correctly	Misplaced items can cause privacy issues, possible theft, loss of the item (e.g. bioassay sample that expires)	Privacy, performance, patient safety, loss of trust in the hospital	Robot scans the room where it needs to deliver, and should not deliver at the wrong place, but user could input the wrong room	3	3	1	9
	Hazards due to contact with moving components								
32	Harmful contact with moving mechanical parts	Arms might block camera sensors, and then a person can get into contact with moving mechanical parts	Collision with person	Physical harm	Force sensor will likely still block the robot's movement	2	3	3	18
33	,,	Threshold for force sensor to detect collisions with the arms are set too high	Collision with person	Physical harm		3	3	3	27

ID #	Hazard	Reasonably foreseeable sequence or combination of events	Hazardous situation	Harm	Notes	Occurrence	Severity	Detectability	**Criticality Index**
	Hazards due to lack of awareness of robots by humans								
34	Lack of social awareness in the robot control system	Staff does not know how to communicate with the robot and make it clear the path	Path is blocked for emergency situations	Physical and psychological		2	5	10	100
35	,,	Users do not know how to communicate with the robot	Human-robot interaction fails	Loss of acceptance		9	1	3	27
36	Lack of legibility of robot intentions	User does not know what the robot tries to communicate due to illegible robot behaviours	Human-robot interaction fails	Physical and psychological		8	1	5	40
	Hazardous environmental conditions								
37	Exposure of robot to snow, ice	Melting snow can cause wet floors	Wet floor which could make the robot slip	Impact injuries		1	3	10	30

ID #	Hazard	Reasonably foreseeable sequence or combination of events	Hazardous situation	Harm	Notes	Occurrence	Severity	Detectability	**Criticality Index**
38	Exposure of robot to water, moisture	Cleaning the floor can leave a wet floor	Wet floor which could make the robot slip	Impact injuries		1	3	10	30
39	,,	Drinks spilled on the ground	Wet floor which could make the robot slip	Impact injuries		1	3	10	30
40	Exposure of robot to saline atmosphere or salt-water sprays (e.g. in marine or coastal environments)	Cleaning the robot might leave detergents and water on the robot	This can damage the robot, can no longer perform its task, and staff have to step in	Stress		8	2	10	160
41	Small objects lying on the floor	Plastic cups, tie-wraps, boxes lying on the floor	Items get stuck in the wheels of the robot, or could make a slip, or block part of the hallway	Impact injuries		3	3	5	45

ID #	Hazard	Reasonably foreseeable sequence or combination of events	Hazardous situation	Harm	Notes	Occurrence	Severity	Detectability	**Criticality Index**
42	Large objects on the floor	beds, boxes lying on the floor	Items get stuck in the wheels of the robot, or could make a slip, or block part of the hallway	Collision, stress		9	3	1	27
	Hazards due to localization and navigation errors								
43	Localization errors causing unexpected movement of the robot	Errors in interpreting sensor data, or incorrect sensor data, may cause the robot to make a turn when this is not expected.	The unexpected movement of the robot could cause a collision with a person who does not anticipate it. May also impact how safe people feel around the robot	Physical harm, psychological safety	Collision avoidance/safety-stop can be handled in a reactive manner based on current 2D LiDAR measurements	6	2	8	96
44	Localization errors causing entry of forbidden zone	Delocalized robot enters stairway (negative obstacles)	Robot can enter a room with patients and	Loss of trust, loss of privacy		3	3	10	90

ID #	Hazard	Reasonably foreseeable sequence or combination of events	Hazardous situation	Harm	Notes	Occurrence	Severity	Detectability	**Criticality Index**
			invade their privacy						
45	Localization errors causing mechanical instability	Wrong pose estimate underestimates the distance to obstacles in the surrounding	Delocalized robot crashes into objects or structure, making it unstable	Impact injuries	Collision avoidance/safety-stop can be handled in a reactive manner based on current 2D LiDAR measurements	1	2	8	16
46	Navigation errors preventing reaching of goal locations or avoiding safety-related obstacles	Delocalized robot enters the wrong room	Robot can enter a room with patients and invade their privacy	Loss of trust, loss of privacy		3	3	5	45
	Security hazards due to external vulnerabilities								

ID #	Hazard	Reasonably foreseeable sequence or combination of events	Hazardous situation	Harm	Notes	Occurrence	Severity	Detectability	**Criticality Index**
47	Vandalism: damaging the robot or its components	An unattended robot may be vandalised by people.	Damage to the robot	Physical and psychological safety		1	3	4	12
48	Bullying, compromising the robot behaviours by exploiting external properties (behaviour violation)	People are known to intentionally see how a robot responds to certain kinds of input. For instance, standing in front of the robot to make it stop.	Robot cannot perform its task, and may be damaged by people	Physical and psychological safety		1	1	4	4
	Security hazards due to internal vulnerabilities								
49	Hacking robot database for stealing information/sensitive data (privacy violation)	Hacker might steal camera footage of people or of bioassay samples	Loss of privacy, loss of feeling safe around robots	Psychological safety and privacy	Hackers attempting to hack the robot during a user study is very small	1	3	10	30

ID #	Hazard	Reasonably foreseeable sequence or combination of events	Hazardous situation	Harm	Notes	Occurrence	Severity	Detectability	**Criticality Index**
50	Hacking the robot control system for altering the robot behaviours (behaviours violation)	Hacker might take-over control over the robot's motions and cause collisions	Collisions	Impact injuries	Hackers attempting to hack the robot during a user study is very small	1	3	10	30

Appendix B: Results of the FMEA for the IDMind Robot

COMPONENT	POTENTIAL FAILURE MODE	POTENTIAL EFFECTS OF FAILURE	OCCURRENCE	SEVERITY	CURRENT PROCESS CONTROLS	DETECTABILITY	CRITICALITY INDEX	RECOMMENDED ACTION
BUMPER	Robot - Human collision	Damage of robot and/or injury of person	4	5	Collision sensors / visual	1	20	Introduction of collision sensors around the robot
SHELL	Children try to climb the robot	Damage of shell and / or injury of child	8	4	Visual	1	32	Design the shell to reduce the possibility of climbing over
MATERIALS	Can´t be cleaned properly	Contact with toxic residue / staining / looks bad in an hospital environment	6	2	Visual	3	36	Choose cleanable materials
ARM	Collision with something	Damage to the arm	4	3	Collision sensors / visual	3	36	Design armrest / sensors to determine safe

								area
STORAGES	Do not open / do not close	Unable to access to the deliverables / safety of materials	2	4	Visual	1	8	Override system
TOUCHSCREEN	Doesn´t turn on	Unable to establish communicati on robot-person	1	5	Visual	1	5	Override system
PLATFORM	Doesn´t stop	Crashes into something / someone	3	5	Collision sensors / visual	1	15	Emergency stop button to cut the power
BATTERIES	Battery detection	Robot is totally (or partially) not powered	2	5	Voltage converters on the board	1	10	Regular checking of battery voltage, fuses and connectors
NAVIGATION COMPUTER	Communication	Robot doesn't move	4	5	Visual	2	40	Assure a proper shutdown of the pc

MANIPULATION COMPUTER	Communication	Arm doesn't move	4	2	Visual	2	16	Assure a proper shutdown of the pc
DOCKING STATION	Power overload	Burns batteries / components	1	5	Measures	8	40	Regular checking of tension levels, fuses and connectors