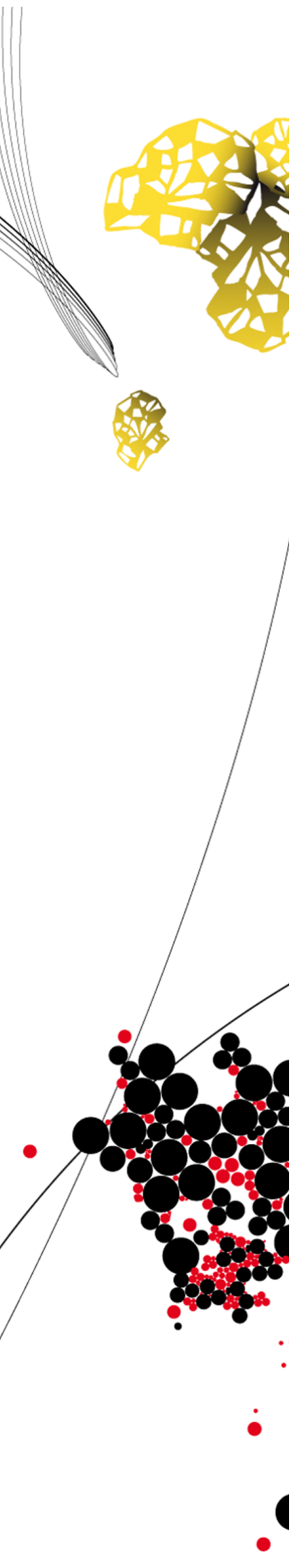

# UNIVERSITY OF TWENTE.


**Faculty of Electrical Engineering, Mathematics & Computer Science**


# Risk Assessment of a Humanoid Robot EVE-R3


**Joshua Anith Singh Jeeva**
**Master of Science Computer Science**

**July 2023**


**Supervisors:**
PROF.DR. M.I.A. Stoelinga
DR.IR. M. Vlutters
MSC. SM. Nicoletti

Formal Methods & Tools research Group
Faculty of Electrical Engineering,
Mathematics and Computer Science
University of Twente
P.O. Box 217
7500 AE Enschede
The Netherlands

# Acknowledgement

I would like to express my gratitude to my primary supervisor Marielle Stoelinga, external supervisor Mark Vlutters, and daily supervisor Stefano Nicoletti for their guidance and support throughout the entire process of working on this thesis.

Marielle's knowledge and expertise in the field of risk management helped me in shaping and refining my research, and her patience and encouragement was essential in helping me overcome the challenges that I faced. Mark's and Stefano's valuable feedback and constructive criticism, dedication, and commitment to my project was truly inspiring, and their insights enhanced the quality of my thesis.

Furthermore, I am grateful to the staff and faculty of the University of Twente for providing me with the necessary resources and facilities to complete my research. Their support and encouragement helped me achieve my academic goals.

Lastly, I would like to thank my family and friends, who stood by me throughout this academic journey. Their encouragement and belief in me was a constant source of motivation, and I am forever grateful for their presence in my life.

To everyone who has played a part in my Master's thesis, I express my deepest gratitude. Thank you for your support, guidance, and encouragement, and for making this a truly enriching and rewarding experience.

# Summary

This thesis report presents a project that involves a fully functioning humanoid robot, EVE-r3, to be used in a healthcare setting to assist healthcare workers in performing general tasks. As the ratio of the elderly people who need healthcare to the amount of healthcare workers increases, there is a decline in the quality of the Dutch healthcare. This project aims to conduct a risk assessment of a humanoid robot which is aimed to provide an extra helping hand to address the decline in the quality of the Dutch healthcare.

The primary focus of this project is to ensure the safety usage of the robot and its interaction with the users and the environment. To achieve this, a risk assessment is performed on the EVE-r3 humanoid robot using the combination of FMEA and STPA risk analysis methods. The analysis is conducted by identifying risk sources, failure modes, potential injuries, and their causal relationships. The STPA-FMEA analysis considers the *user ability*, *natural environment*, and the *social environment* of the robot as additional factors contributing to the analysis when compared to its traditional counterparts, the classical FMEA analysis, which considers the *severity*, *occurrence*, and *detection* of hazard present in the robot. The analysis also considers a classification of different relevant user groups under user ability such as *elderly patients, healthcare workers*, and *other stakeholders*, as the ability of a user to handle the risks may differ amongst different users. The same goes with the environmental settings where the environments considered are *nursing centre, residential care*, *and home care*. The evaluation of all these mentioned factors are performed by the experts via questionnaires and interviews.

The results obtained from the questionnaires by the experts were used to calculate the risk priority number (RPN) for all the identified hazard scenarios. The STPA-FMEA analysis retrieved a range of risk values which shows that the ranking of the most hazardous risks in STPA-FMEA is different from that of the traditional FMEA analysis. Overall, this study aims to provide insights about the risks and causes associated with the humanoid robot EVE and prioritize them according to the RPN which would in-turn improve the robot's safety in the healthcare setting.

# Contents

# List of acronyms

| | |
|---|---|
| **ADL** | Activities of daily living |
| **VR** | Virtual Reality |
| **ADA** | Americans with Disabilities Act |
| **FMEA** | Failure Modes and Effects Analysis |
| **STPA** | Systems Theoretic Process Analysis |
| **SSR** | Social Service Robots |
| **HFACS** | Human Factors Analysis and Classification System |
| **HAZOP** | Hazard and Operability Analysis |
| **FTA** | Fault Tree Analysis |
| **STAMP** | Systems Theoretic Accident Model and Process |
| **m-HFMEA** | modified healthcare FMEA |
| **RIFMEA** | Robot Inclusive FMEA |
| **PRAT** | Proportional Risk Assessment technique |
| **ETA** | Event Tree Analysis |
| **RPN** | Risk Priority Number |
| **HFMEA** | healthcare FMEA |
| **HCS** | Hierarchical Control Structure |
| **CF** | consumer factor |
| **EF** | environmental factor |
| **UML** | Unified Modeling Language |
| **HSS** | Hazard Scenario Symbol |

# Chapter 1

# Introduction

In light of a shortage of healthcare workers to support the aging population in the Netherlands, there is a decline in the quality of the Dutch healthcare [1]. To address this issue, the study [1] proposed the use of Social service robots which is aimed to provide an extra hand to the healthcare officials and has the potential to increase the quality of the dutch healthcare system. To envision the use of Social Service Robots (SSR) in the healthcare sector, a thorough safety analysis of one such robot needs to be performed which considers the robot's interaction with the users and the environment along with the robot's components. This thesis performs risk assessment on one such humanoid robot EVE - r3 that can learn and function to physically interact with the environment. The humanoid robot may use its skillset in assisting humans in numerous tasks, for example, by looking for and bringing in a requested tool. EVE is aimed to be similar to a supporting nursing staff.

## 1.1 Why a humanoid robot?

The purpose of the humanoid robot in our case is to address in aiding the healthcare sector by potentially lending an extra hand to the healthcare workers by performing the general aiding tasks such as Activities of daily living (ADL) tasks, housekeeping tasks like general cleaning activities, tidying up the kitchen/living room space etc., reporting and administrative tasks like recording reports and relaying messages, daily structuring tasks like conversing or entertaining the client etc., and peak intensity tasks like making or clearing the tables, dispersing medicine among clients etc. This is because the number of workers does not grow as rapidly as its necessity to uphold the current requirement of the aging population in the Netherlands. As the ratio of the elderly people who need healthcare to the amount of healthcare workers is increasing, there is a decline in the quality of the Dutch healthcare as mentioned in [1].

The humanoid robot EVE – r3 considered for the thesis is owned by the Nakama Robotics lab which was established in 2021 in partnership with the University of Twente. As mentioned in a study conducted [1], the SSR, in this case, the humanoid robot EVE may potentially address the problem of aiding the growing number of elderly patients and help tackle the issue of a potential healthcare worker shortage in the future. There are numerous benefits associated with deploying a humanoid robot as for social service. A social service robot can not only assist the healthcare workers by performing general daily tasks, but also provide a companionship and a form of social interaction to the respective patients. Using a social service robot can improve the efficiency in a healthcare setting by freeing up the staff to focus on more complex tasks and prove to be cost efficient by achieving automation of certain tasks. All of this can prove to be beneficial to both the healthcare sector and to the patients and may also improve the patient outcomes. Details of the humanoid robot EVE specifics are as follows.

## 1.2 EVE

In this case study, the robot chosen to assess its risks is the EVE – r3 humanoid robot [2]. The EVE - r3 humanoid robot is a highly advanced robot developed by Halodi Robotics, known for its full human size appearance and ability to display a wide range of activities and movements. The robot is powered by fully integrated platform that utilizes direct force control technology [3] for natively compliant operation, which allows it to interact with people in a natural way.

One of the main goal of EVE-r3 is to provide as a solution for the industry needs. This could mean for security purposes, retail, logistics or healthcare. The robot can even be controlled remotely with the help of Virtual Reality (VR) control in avatar mode apart from its autonomous navigation, door opening and elevator travel. The additional VR control enables the robot to be controlled remotely to perform some precision tasks which the robot might not be able to perform autonomously. Its life-like structure and ability to lift a payload of 8kg per arm makes it well-suited for industrial usage, as well as in studies to help the robot improve according to human perception and cognition.

This robot can learn and function to physically interact with the environment and is aimed to be used in a healthcare setting. Specific information regarding the robot which would help in the risk assessment is mentioned in [4]. In order to keep the users and the environment safe, the EVE must operate in a space which is hazard

free. This includes knives, sources of fire, hazardous chemicals or furniture that could be knocked over. Sufficient space is necessary for the EVE to move around and perform tasks. The robot EVE is Americans with Disabilities Act (ADA) compliant i.e., it is wheelchair friendly which means stairways and other drop offs must not be present in EVE's working environment or it could pose danger [3].

Some of the notable technologies present in EVE are, surveillance and autonomy, whole body torque control to aid in pushing the robot back and forth to avoid any harsh contact, force and impedance control on all joints and a platform provision to add deep learning compute as an add-on.

EVE is equipped with a wheeled base for movement and is powered by highly backdrivable motors for safe human interaction. This enables the person to push the robot against its motion easily and without actually harming the robot so that the human can move aside safely in case to avoid any possible hard contact being made with the robot's rigid and heavy components.

The robot also requires a gantry to lift and initialize the robot. The gantry along with a support tether is recommended to help perform EVE with high-risk tasks that could cause EVE to fall. The gantry must be able to withstand an impulse load of at least 500kg in an unlikely event if EVE falls while tethered. Although once initialized, the gantry system may not be necessary for the EVE to perform its general operations.

The specification of the EVE is as follows. The EVE weighs about 89kg with a height of 1.83 meters and a shoulder width of 55 cm. The EVE can achieve a top speed of 6.2 km/h with a remote-control capability of autonomous navigation or VR avatar mode. The charging mode of EVE is manual, and the robot runs on Li-ion batteries. EVE consists of various sensors namely ZED2 stereo camera (Head), audio recording, two-way intercom/ PA sensor and lighting. EVE is also capable to store any received data including audio and video storage. Also, the EVE can withstand temperatures up to 50 degrees Celsius and is meant for indoor use purpose only.

The battery packs are located in the wheelbase and should be taken care from exposing to high temperatures or anything that could cause them to short, creating a hazard. The EVE is also equipped with an E-Stop button which blocks the robot from powering its motors when turned on. Triggering the E-Stop would require the robot to be suspended from the support system as the robot would collapse to the ground

if it were not suspended whilst action. The EVE has a motor overtemp and battery low voltage detector which gives warning beeping sound if in case the motor is overheated, or the batteries provide insufficient voltage. If the robot at this situation is not connected to the overhead tether, there might be a significant damage from the robot powering off unexpectedly and collapsing. The EVE battery system includes pre-programmed voltage, current and temperature limits that will safely power down the system in case the set limits are exceeded.

EVE's joints make use of cable-based power transmissions known as capstan drive transmissions and couple these transmissions with a differential cable transmission to combine the torque of two electric motors for either of the two joint axes they are connected to. This allows the motors to deliver two to three times the torque of a single serial transmission.

EVE R3 has potential in the healthcare sector. The robot could be used in hospitals, nursing homes, and other healthcare settings to provide companionship and assistance to patients, as well as to perform tasks such as taking vital signs or reminding patients to take their medication.

On the whole, EVE-r3 is an advanced humanoid robot that has a wide range of potential uses, from research and industry to customer service and social service, and also in healthcare sector as a companion and helper for patients and healthcare workers.

## 1.3 Problem Statement

With the main aim to keep the humanoid robot safe from not disturbing or harming its interacting users or the environment, safety analyses needs to be performed which is the primary reason for this project.

A study [5] based on analysis of multiple accidents for different robots show that robot operators (72 percent), maintenance workers (19 percent) and programmers (9 percent) suffered various injuries which includes pinch injuries (56 percent) occurring when a robot traps a worker between itself and an object and impact injuries (44 percent) occurring when a robot and worker collide. The causes of injuries included unexpected robot behavior, human errors (e.g., a second worker activating the robot when one worker is close to the robot) and unexpected software problems. The harm ranges from slight injuries with no loss time, to fatal injuries. To avoid such risks and create a safe environment for the robot and its environment, a thorough

risk assessment is required. This M.Sc. project will perform such a risk assessment for the robot EVE, by combining two risk assessment frameworks namely the FMEA, and the STPA in order to provide a thorough and complete risk analysis with respect to the robot, user, and environment.

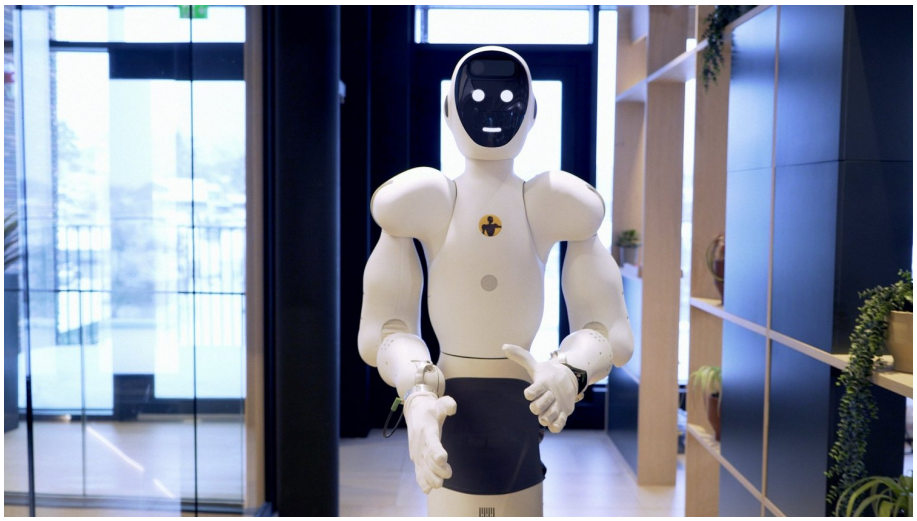

**Figure 1.1:** EVE

## 1.4 Research Objective

The goal of this study is to perform a risk assessment on the EVE – r3 humanoid robot in a healthcare setting by identifying and prioritizing the hazardous components or potential hazard scenarios with respect to the robot, its interacting users and working environment. Performing such a risk assessment would lead to proposing and implementing mitigation strategies for the betterment of the robot and its environment.

To attain this goal, the combination of the FMEA and STPA risk analysis methods is selected for this case study. With the selected methodologies, risk analysis will be performed from which, it will be certain to identify and quantify some of the most hazardous risks. The further procedure is to consider different user groups and environmental settings and re-iterate the risks analysis process. A comparative analysis can then be performed to confirm if there are significant changes in risks with different user groups and environmental settings when compared against the initial risk assessment.

## 1.5 Research questions

The research objective can be further broken down to the following research questions to attain the primary goal.

1. What are the identified hazards associated with the EVE-r3 humanoid robot used in a healthcare setting using the STPA-FMEA risk analysis method?

2. How do different user groups and environmental settings impact the identified risks and hazards associated with the EVE-r3 humanoid robot in a healthcare setting?

3. Is there a significant difference in the level of risk associated with the EVE-r3 humanoid robot in a healthcare setting between the classical FMEA analysis, and the STPA-FMEA analysis which takes into consideration the external factors like user ability, and the environment?

*Research question 1* will be answered by using the FMEA analysis which can consider risk quantification on a component level and the STPA analysis which considers the system as a whole, and can come up with a system structure which would take into account the various sub-systems of the product (the robot in this case) along with its interaction with the environment and other humans to give a list of unsafe behaviors of the product in terms of hazard scenarios. The goal is to couple the FMEA's component level risk identification with the hazard scenarios identified by the STPA to give a more detailed and well covered risk identification for a certain component or a sub-system as a risk identification process of the STPA-FMEA methodology. These hazard scenarios identified by the above mentioned process may be constructed based on factors like, the component, risk sources, risk consequences etc.,

*Research question 2* will be answered by performing a risk quantification with respect to the FMEA methodology, but also include the human and the environment factors for the quantification which is the ideology of the STPA framework. This may include a way to quantify different factors like the user or the environmental perspective along with the degree by which these factors may affect the identified hazard scenario.

*Research question 3* will be answered by further identifying the results of the risk quantification of the STPA-FMEA methodology. A comparison may be plotted showing if there is a significant difference between the risk quantification of the STPA-FMEA methodology which considers the user and the environmental perspective

against the FMEA's traditional risk quantification methodology.

# Chapter 2

# Literature Survey

In order to execute the experiment using the FMEA-STPA approach, a list of different risk assessment techniques were researched on. It was then decided that the FMEA-STPA methodology covers all aspects by considering the robot and its working environment to identify and evaluate possible risks, and improve the safety of the humanoid robot and its surroundings in a healthcare context. The following sections will outline the methodologies that were taken into consideration and why the FMEA-STPA methodology was chosen after careful consideration of all available options.

The first step would be to determine whatever approaches are available that would work for the case study 2.1. Section 2.2 will discuss why the STPA-FMEA methodology is sufficient and what benefits it has to be chosen for this case study after focusing on the most suitable risk assessment for the current case study. The FMEA approach, STPA approach, and any shortcomings with the methodologies under consideration will all be shown in section 2.3, along with any pertinent extensions and any combination analyses. These sections make it abundantly evident why the FMEA-STPA combination is a comprehensive analysis applicable to the case study and why it is the most appropriate for the case study.

## 2.1 A Hunt for the more appropriate analyses

The current techniques for analyzing the safety of robots and their interactions with people and the environment are explained in this section. The study [6] presents its research on several of the conventional hazard analysis methods that are frequently employed. They include Fault Tree Analysis (FTA) [7], failure mode and effects analysis FMEA [8], and Human Factors Analysis and Classification System (HFACS) [9]. According to the study [6], one of the main drawbacks of these current method-

ologies is that they primarily focus on the system rather than the safety violations brought on by human activity and interactions with the environment. It also notes that there aren't many published papers on the topic of identifying accident early warning signs in the context of collaborative robots. As their frameworks provide hazard identification and safety design for the system, informal approaches like Hazard and Operability Analysis (HAZOP) [10] and STPA [11] frameworks are helpful in this situation. To give a more extensive and comprehensive risk analysis in terms of hazard identification and risk quantification, these informal frameworks are typically combined with additional formal or semi-formal risk assessment methodologies. In the works [12] [13], where HAZOP and Unified Modeling Language (UML) are merged and used, examples may be discovered. Human-robot interactions are described using use-case and sequence diagrams from the UML, and risk analysis is carried out using HAZOP by applying the approach to each component of the UML model. Another instance of such a combination may be found in the work [14], where risk assessment and hazard analysis are conducted for vehicle safety using the STPA hazard analysis in conjunction with the FMEA analysis. In this work, the STPA analysis focuses on gathering more detailed cause factors for those identified components in order to provide a variety of system hazard instances, while the FMEA analysis continues to focus on finding and evaluating the low-level components. In order to clearly explain a piece of equipment in terms of system function and system boundary for a high-level understanding of the complete system, the information offered by STPA is also important in developing safety or hierarchical control structures.

The objective of the current case study is to carry out a comprehensive risk evaluation that takes into account both the robot's system and the external human-robot interaction factor. This can be accomplished by using a mix of analyses that support one another. This would aid in assessing the risk and in providing a broader range of hazards' causes. More details about the case study should be taken into account when choosing the best risk evaluation methods. This may be in relation to the information supplied in order to carry out the risk evaluation. This case study lacks historical information on failures or the likelihood of hazards, which forces the risk assessment of the humanoid robot to rely on the expert's judgment in each instance where a risk or hazard has been identified. The FMEA analysis was deemed the most appropriate for this case study out of the well-known failure analysis techniques like FMEA and FTA to find the system risks. This is primarily because the research [15] that compared the results of FMEA and FTA for a common case study reveals that there were differences between the two when compared in its findings. It claims that while the FMEA methodology is frequently used for a single random failure analysis, the FTA methodology has the capacity to incorporate the fundamen-

tal causes of a variety of failure situations. The FMEA method, however, proves to be quite useful during the preliminary design stages of the case study when there is a lack of quantitative failure data. The FTA is also suitable in situations where some historical data, such as probability of failure or rate of occurrence of failures, are available.

One of the major objectives for the present case study is to also take into account external factors for the risk assessment, such as stakeholders and the product environment that the robot will interact with. Numerous studies [12] [16] [17] show that traditional hazard analysis methods like FTA and FMEA are inadequate for analyzing human-robot interactions and that they oversimplify the role of humans in instances of hazards or accidents. HAZOP, STPA, and HFACS techniques are taken into consideration to be possibly combined with the already shortlisted FMEA analysis in order to support this scenario and provide the best risk assessment possible. The study [18] claims that HFACS is more focused on the human factor in accident analysis, but the HFACS model is too rigid and constrained on its own to categorize all the failures involved, particularly when this model is used outside of the aviation industry. The HAZOP analysis is a commonly used hazard identification method that breaks down a system into smaller components and analyzes each one separately in order to systematically look for potential hazards. The project [19] demonstrates how analysis aims to identify potential hazards and reduce them. The analysis takes into account both the operational view and the component centric view in order to encompass all aspects of the robot's operation. Human factors can also be taken into account with HAZOP, which is not feasible with the standard conventional risk analysis techniques like FMEA and FTA. STPA analysis, on the other hand, is a more recent method of hazard analysis that is founded on a systems-theoretical strategy. In order to control or mitigate those factors, STPA analysis first concentrates on identifying the causal factors that can result in a hazard. STPA takes into account the system's operating environment as well as the social, organizational, and environmental variables that may be associated with risks. This is supported by the research [17], according to which HAZOP is advised for simple function system analysis while STPA is advised for complex system analysis because it focuses on the accuracy of control actions and produces a complex result. Another research, [16] asserts that HAZOP may be more appropriate for complex systems due to its simplicity and shorter time requirement than STPA for highly automated systems and numerous component interactions. Overall, STPA maintains a more comprehensive perspective of the system and is regarded as a more thorough and efficient method of hazard analysis than HAZOP in terms of the inventory of hazards [20].

It was decided to dig deep to find some pertinent combinations of the FMEA and the STPA analysis and how they complement each other to be the right fit for the current case study analysis based on the aforementioned findings and while taking into account the case study at hand.

## 2.2 A relevant combination of FMEA and STPA analysis for a more complete risk analysis

This section includes some of the most current research on the benefits of combining FMEA with STPA. A standalone STPA is built to handle the hazard analysis of any modern complex systems, but it does not include the risk evaluation required by the majority of safety-related international standards. This is one of the main benefits of combining STPA and FMEA method analysis, in addition to the potential benefits discussed in section. The FMEA technique, which is typically focused on the risk evaluation of the low-level components, enters the picture at this point. The STPA will be able to provide a list of product hazards and their interactions with external factors as a result of this combination, while the FMEA can assist in quantifying and prioritizing the identified risks as part of risk quantification in the risk assessment, which would be helpful in reaching the necessary conclusions.

The research [21] presents a novel method for assessing consumer product risks along with a comprehensive five-level complex index system. One example of intelligent home appliances that has created new safety concerns is autonomous sweeping robots. STPA-FMEA is a novel method of risk assessment for consumer goods that is introduced in the research in [21]. This method considers the ”person-product environment” elements as well as the intricate processes of developing consumer goods. The results suggest that this methodology is capable of identifying all injury scenarios, failure modes among product components, and safety limits within the hierarchical control structure of the interactive system.

Traditional methodologies, which mainly focus on the product itself, give comparatively less thought to the interactions between people, products, and the environment. The limitations between the various levels of complex systems and their effects on people and the environment are not taken into account by the conventional FMEA method, nor are the risks related to consumer goods when they are being used. Because of how the various system components interact with one another impacts how safe the system is, the Systems Theoretic Accident Model and Process (STAMP) views the system as a whole. This addresses the lack of interac-

tion in the FMEA technique. Although, the singular STPA method does not take into account the risk of potential component defects, in particular consumer goods, the accuracy of the analysis is greatly influenced by the subjective judgment and analytical skill of the person(s) conducting the assessment. The findings are therefore unsupported by factual information.

Accidents are primarily caused by the product, the user, the environment, and different levels of safety restrictions. Utilizing the STPA-FMEA method, emerging risks can be evaluated.

As systems become more complex, traditional top-down and bottom-up safety assessment techniques, like FTA and the FMEA method, are no longer sufficient to ensure product safety while taking into account external factors of the product, such as the stakeholders and its environment. This is because, compared to the current state-of-the-art method, STPA, finding and investigating all damage scenarios when a product interacts with people or the environment is much more difficult in a standalone FMEA or FTA. The characteristics and shortcomings of the FMEA and STPA methodologies are carefully investigated, and it is found that they can be combined to meet the requirements of a person-product-environment risk assessment. This enables more objective quantification and visualization of risk factors and potential damage scenarios using Risk Priority Number (RPN).

It is clear from the analysis performed using the STPA-FMEA method [21], that the ranking differs depending on whether user and environmental factors are taken into account. In the risk assessment of consumer goods, users and the environment typically have a comparatively significant effect on the event risk. After analyzing the current unsafe control behaviors and their causes, it is necessary to further reinforce the safety limits in order to reduce the risks of damage scenarios.

Similar to this, the authors of [14] presented a brand-new technique called STPAFT that is applied to risk assessment and hazard analysis in the case study of vehicle functional safety. STPAFT is nothing more than the combination of a hazard analysis conducted by STPA and a risk evaluation conducted by FMEA. By concentrating on the low-level components in this research, the FMEA methodology also assists STPA in systematically identifying causal factors, making it superior in the identification of causal factors. In turn, this is quite favorable for the functional safety requirements derivation that is required for the aforementioned case study. It implies STPAFT can obtain more detailed causal factors. When describing a piece of equipment in terms of system function and system boundary, the knowledge obtained

from the STPA analysis can be used on safety control structures. The STPAFT methodology used in this research emphasizes the benefits of both STPA and FMEA analysis as a result. This indicates that, when compared to the standalone STPA, this methodology not only broadens the range of hazards that can be found, but also allows for the risk assessment of those hazards through FMEA.

The studies FMEA and STPA research are compared qualitatively in another study cited as [22]. These techniques have been used on a single case study, the forward collision avoidance system, in order to compare and contrast the methods' major strengths and weaknesses, as well as to look into their main differences. As both methods produced the same kinds of recognized hazards, there were no significant differences between them when the analysis of the two methods was conducted. A crucial point was that both approaches had a few distinctive risks that their counterparts had not noted. In terms of numbers, STPA analysis discovered 9 distinct risks, while FMEA discovered 8 distinct hazards. The studies also point out that in their case study, the STPA was more concerned with the delivery of control instructions and their feedback, whereas the FMEA analysis was more concerned with components, their failures, and risk mitigation strategies. Additionally, compared to other conventional hazard analysis techniques, STPA took into account a wider variety of hazard causes, whereas FMEA is thought to be more robust with regard to risk evaluation through the determination of a risk priority number. The study's conclusion emphasizes how both methods worked well together in the study, stating that no kinds of hazards were missed by either of the two methods and that neither method was sufficient to identify all identified hazards.

However, it was also discovered that the STPA-FMEA method had some shortcomings. First, the STPA-FMEA approach still incorporates subjective elements, such as expert scoring, despite having some objective elements in the analysis of the STAMP model. Second, even when the suggested technique is built into a platform for network assessment, it still isn't intelligent or automated enough. To enhance the objectivity of the STPA-FMEA methodology and to automate or improve the intelligence of the expert scoring process by determining how to combine the risk identification and quantification steps of the STPA-FMEA method with computer techniques like semantic matching, web data crawlers, machine learning, dynamic simulation, agent-based modeling, other complexity theories, and various modelling-related technologies, more research is required.

## 2.3 Other valuable alternatives extending the FMEA or STPA

A few other options regarding FMEA, STPA, their extensions, or a combination of FMEA or STPA with another complementing analysis were considered, in addition to choosing the combination of STPA-FMEA analysis for the present case study on risk assessment of a humanoid robot. The modified healthcare FMEA (m-HFMEA) was one of these analyses. Using FMEA and healthcare FMEA (HFMEA) separately as a comparative study, the work [23] performed analysis on an advanced radiotherapy procedure—linac-based, intracranial radiosurgery. The m-HFMEA is based on risk inventory matrix and decision tree analysis, whereas the FMEA is based on RPN values and creating actions and outcomes. The lesson learned from this case study was that 17 failure modes shared by RPN and HFMEA were discovered during the risk evaluation of the top 20 failure modes. The work concluded by stating that healthcare services should not rely solely on a single FMEA or m-HFMEA to ensure that all risks have been identified for a given process.

Another study, called Robot Inclusive FMEA (RIFMEA) [24], developed an FMEA framework that was specially designed for build settings that were robot-inclusive. The RIFMEA is a type of FMEA in which the robot itself is regarded as a partner. This study's primary objective is to take into account the structures and environment in which the robots will operate and analyze the risks associated with those environments in order to improve, make safer, and more effective robot operations that will further their intended goals without endangering people and maintain the highest level of human priorities. While other studies typically only considers the hazards in the robot operating environment, making it less detailed than the approach of RIFMEA, this can be used to point out hazards for the service robots in built environments to enhance safety of robots for humans, robots, and the environment. A modified severity, occurrence, and detection measure, which has a 5-point scale, is used by RIFMEA. The severity takes into account three distinct things: robots, people, and the environment. The probability of occurrence, which ranges from 0 to 1, is taken into account when determining the likelihood of failure under the considered environmental conditions. This value is then classified into one of the five parts, which corresponds to a five-point scale. The degree of robot autonomy affects the detection values. This can work remotely, partially automatically, or entirely on its own. Based on these values, suggested actions can be taken to address the list of hazards and lessen or eliminate the effects of harm done to or by the robots during operation. While the RIFMEA framework is generally quite detailed when it comes to the environment that the robot will operate in, it only takes that into account from an

environmental standpoint. Since this use case is outside the purview of RIFMEA's analysis, specific robot component-based hazards are not covered in this analysis. As a result, the risk identification process is conducted exclusively from an environmental viewpoint while taking the robot into account as a stakeholder. In order to perform a thorough risk analysis of the humanoid robot, just as the current thesis calls for hazard identification from an environmental or user perspective, it also calls for hazard identification within the robot's components. This work [24] has provided a thorough knowledge of how the robot operation environments can be taken into account in a robot risk analysis.

In a risk evaluation involving a collaborative brick lifter robot, FMEA and Proportional Risk Assessment technique (PRAT) analysis are combined [25]. This work was carried out as an exploratory analysis coupled with the well-known risk assessment framework, FMEA, because the use of PRAT was not among the most commonly used methods for the risk assessment of HRC applications but was capable of one. Similar to the FMEA framework, PRAT has its own RPN dubbed the PRAT RPN, where the risks are scaled from 1 to 1000, as in FMEA. The factors—probability of failure, seriousness of harm, and exposure—are quite comparable as well. Different groups of evaluators separately complete both analyses, which are then paired to rank the risk priority from each RPN. The main reason this method is not taken into consideration for the experiment of risk analysis of the humanoid robot in this thesis is that the merging of FMEA and PRAT into one combined analysis is mentioned as a future work, and the analysis of PRAT and FMEA in the case study mentioned is quite similar without different factors being involved.

A different strategy that was taken into consideration was a STPA and bowtie analysis combination for assessing a multi-agent system and contrasting various control strategies [26]. While the bowtie analysis handles the risk assessment of the scenarios obtained by the STPA analysis, the STPA analysis is used in the research to identify risks and extract a set of risk scenarios with various hierarchical coordination architectures. For the STPA analysis used in this research to identify risks, 3 different control architectures are taken into account. These are the centralized strategy, the hierarchical approach, and the modified hierarchy approach principles. In this study, the bowtie method is thought to be a good complement to the STPA analysis because it combines the FTA and Event Tree Analysis (ETA) tools for identifying events, their causes, and effects. It also provides a clear visualization of STPA results and has the ability to assess the hazard scenarios that the STPA analysis has identified. The severity of each hazard was combined with the frequency of the causal event to analyze the hazards using the risk classification matrix. The bowtie

method is not very useful for control approaches, but when combined with STPA, an improved and more fruitful analysis is created, which is why these methodologies were combined. The applications of STPA provide a wide range of hazard scenarios and causal variables, including software, human, environmental, and technical problems. Additionally, the scenarios obtained from STPA are more detailed than those obtained from other traditional techniques. The study had limitations, so it was agreed to continue looking for alternative approaches. It was difficult to quantitatively distinguish between some scenarios and their causal factors because they were so similar, and as a result, they were ultimately considered the same rather than being able to differentiate the scenarios. Also, the bowtie methodology is not quite capable of quantifying all of the potential scenarios and the causal factors identified by the STPA analysis.

# Chapter 3

# Theory and Background

To answer the research questions and attain the objective of this case study of risk assessment of EVE, two risk analysis methodologies were selected. These are FMEA [8] and STPA [11] frameworks. FMEA and STPA are complementary methods for identifying and analysing hazards and risks in complex systems. FMEA follows a bottom-up approach and focuses on the potential failures of individual components or subsystems within a system, and the effects of those failures on the system as a whole. STPA, on the other hand, focuses on the interactions and dynamics between actors within a system, and the potential hazards that may be initiated or triggered by those interactions.

A study [22] also states that the STPA and the FMEA analysis left no types of hazard unfound and complemented each other well in the study. Combining these two methods can provide a more comprehensive and robust approach to risk assessment, because it allows organizations to identify and analyse both the individual components and the overall system dynamics which, in this case would be considering the user and the environmental factors along with the robot system's risks. Hence, reduce or eliminate the root cause of accidents and injuries. This can help organizations identify potential hazards that may not be apparent using one method alone, and develop more effective strategies for preventing or mitigating those hazards.

In addition, FMEA and STPA are both systematic and structured methods, which makes it easier to document and communicate the results of the risk assessment process. This can be especially useful for organizations that need to demonstrate compliance with relevant regulations and standards. Overall, the combination of FMEA and STPA can provide organizations with a powerful tool for improving the safety and reliability of their complex systems.

## 3.1 Failure mode effects analysis (FMEA)

Failure Modes and Effects Analysis (FMEA) [8] is a methodology designed to identify potential failure modes for a product or process before the problems occur, to assess the risk. FMEA's are conducted in the product design or process development stages, although conducting an FMEA on existing products or processes also yields benefits. Currently, FMEA has developed into a set of thorough and scientific risk methodologies in engineering practice and has grown to be a robust technique for reliability analysis and risk assessment. FMEA has been used in studies to evaluate project risks.

The FMEA is a defined yet subjective analysis used to systematically identify potential Root Causes and Failure Modes and estimate the risks associated with each. The fundamental objective is to detect risk in a design, then to reduce or eliminate it. As a result, the FMEA strives for improved safety, reliability, and quality. It can also be applied to evaluate and improve maintenance schedules.

To improve the subjective nature of the traditional risk priority number (RPN) method, a study [27] describes numerous methods like (i) A FMEA method based on fuzzy set theory and gray correlation theory, and put forward an improved FMEA method by mixing fuzzy rule base with grey correlation theory, (ii) A possibilistic hesitant fuzzy linguistic information to evaluate failure modes and applied an interactive consensus-driven FMEA method to cluster the failure modes and (iii) An adopted fuzzy set theory to analyze the identified potential failure modes in FMEA.
A team of design and maintenance people who have experience with all the aspects to be taken into account in the analysis often conducts an FMEA. The mechanisms that create failures are known as Root Causes and can be thought of as the causes of failure. Although the term ”failure” has been established, it does not indicate how the component failed. The various ways in which a component could malfunction are known as failure modes. It is crucial to understand that a Failure Mode is the manner in which a failure has occurred rather than its underlying cause. Often, the Root Causes of one failure might be connected to the impacts of another failure.

The FMEA technique uses severity, occurrence, and detection as metrics to assign a numerical number to each risk related to triggering a failure. The values of the ranking rise as the risk does. A RPN, which can be used to examine the system, is created by combining these. The most dangerous aspects of the design can be handled by focusing on high value RPNs. RPN is derived by multiplying the risk's severity, occurrence, and detection.

The degree of a system failure's End Effect is referred to as its Severity. The severity value attributed to the effect will be higher the more sever the consequence. The term "occurrence" refers to a qualitative description of how frequently a Root Cause is expected to occur. That is expressed in words other than a time frame, such as remote or occasional. The possibility of finding a Root Cause before a failure may happen is referred to as detection. Specific standards have been developed for the usage of FMEA because it is used by many different sectors, including the automotive, aerospace, military, nuclear, and electro-technical ones. A typical standard will provide samples of an FMEA spreadsheet structure as well as descriptions of the Severity, Occurrence, and Detection rating scales.

For calculating the risk in FMEA method, the three components are multiplied to produce a RPN is described on a 10-point scale where 10 is highest.

$$RPN = S \times O \times D$$

$RPNmin = 1$ while $RPNmax = 1000$ [28]

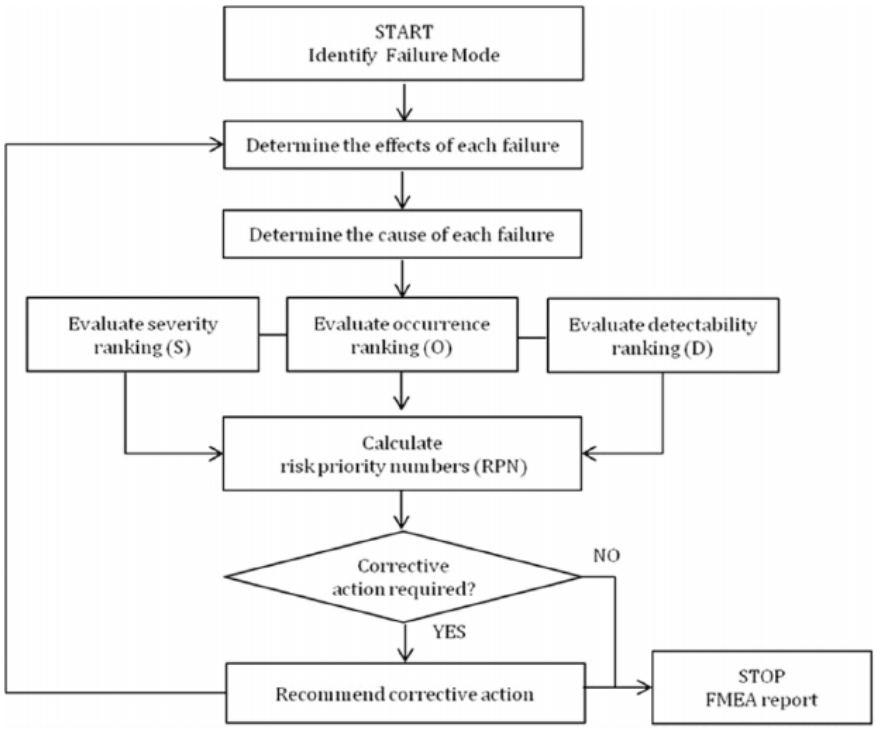


**Figure 3.1:** The FMEA Process [23]

## 3.2 Systems theoritic process analysis (STPA)

The System Theoretic Process Analysis (STPA) method [11] for hazard analysis focuses on analysing the dynamic behaviour of systems, and in this way provides significant advantages over the traditional hazard analysis methods. STPA employs a top-down analysis methodology. Instead of the physical component diagram that is utilized by conventional hazard analysis techniques, STPA uses a model of the system made up of a functional control diagram. System theory serves as the foundation for STPA, which views safety as a problem of system control (constraints), as opposed to component failure.

Safety constraints, hierarchical safety control structures, and process models are three essential parts of a STPA analysis. In order to assure safety, safety limitations must be imposed on the system's behavior. According to STPA, unsafe control actions or a lack of controls results in unsafe states due to insufficient enforcement of safety regulations. Constraints on safety are measures that should be taken to ensure the avoidance of risks, unintended consequences, or accidents. A hierarchy of controllers is depicted in a hierarchical safety control structure diagram, with each level enforcing safety limits. By recognizing system behaviors and interactions, the safety control structure of STPA offers a thorough method for identifying potentially hazardous control actions.

The process model illustrates how system control is carried out by human operators, or controllers. In order to manage the system, the controller must be aware of its current status, the appropriate control measures, and the impact of various control outputs on the network. For both computerized and human controllers, this statement is valid.

It is important to mention that STPA can be applied at any stage, such as in the design phase and in the operational phase. It is carried out in the following two steps:

- Determine the possibility of inadequate system control that might result in a hazardous state. A hazardous state is one that transgresses the safety limitations or requirements of the system and may result in a loss.
- Determine the likely outcomes of each potentially hazardous control action listed in step 1. A system can enter a hazardous state as a result of insufficient control action in the following ways:
    1. a control action required is not provided,

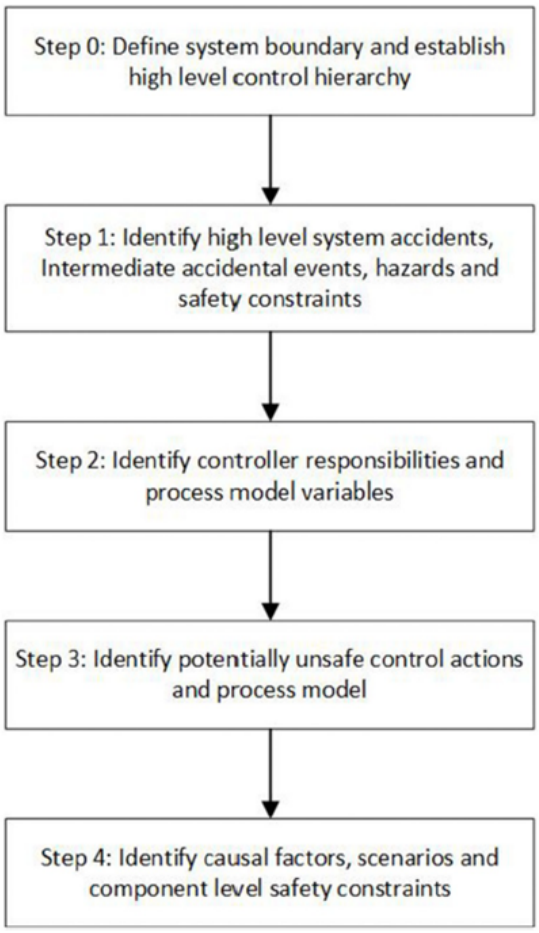


**Figure 3.2:** The STPA Process [16]

2. an unsafe (incorrect) control action is provided,
3. a control action is provided too early or too late (wrong time or sequence),
4. a control action is stopped too early or applied too long.

The process flow of the STPA analysis is shown in figure 3.2.

With the process flow being performed, appropriate and relevant strategies can be developed in order to prevent or mitigate the hazards, and evaluate their effectiveness. In result, STPA is a useful tool for ensuring the safety and reliability of complex systems by identifying and addressing potential hazards before they can cause harm. It can also help organizations comply with relevant regulations and standards, and improve the overall performance of their systems.

An extensive literature review on these methods, valuable alternatives, and their applications is proposed in chapter 2.

# Chapter 4

# Methodology

Risk analysis is performed by identifying potential consequences of a risk event, their probability, as well as other risk characteristics, while taking into account the already existing control measures, their effectiveness, and efficiency. The Hierarchical Control Structure (HCS) and current safety limitations are taken into account in this phase, which leads to the analysis step of the proposed STPA-FMEA technique. The process model that embodies each safety restriction is examined using the HCS.

## 4.1 STPA-FMEA : the framework

From section 2.2 of the literature study, it was evident that the STPA and FMEA methods can be generally used in interactive situations for the risk assessment methods that supports person-product-environment interactions.

As the systems become more complex, the traditional risk analysis methods such as the FMEA or the Fault tree analysis are now not sufficient to ensure product safety [29]. This is because with a standalone method, it is more difficult to showcase all possible hazards and risk sources especially when a product interacts with its environment or the users.

A system, process, or product's potential failure modes are identified, along with their potential effects, using a bottom-up approach technique called FMEA. The objective of an FMEA is to identify potential hazards, assess the effectiveness of already-in-place controls, and plan for new controls to diminish or eliminate those hazards. It is a methodical process where an expert or group of experts collaborate to determine potential failure modes, causes, and effects as well as to assess the risk related to each failure mode.

Contrarily, STPA is a top-down analysis that concentrates on finding threats and hazards in the overall system as opposed to specific parts or subsystems. It is built on the idea of ”control domains,” or system components with the capability to influence how the system behaves. In order to develop methods to reduce or eliminate these hazards and risks, STPA aims to identify the threats and hazards connected to the interactions between various control domains.

When paired, FMEA and STPA offer a thorough method for detecting and managing hazards and risks in intricate systems. While STPA is intended to identify hazards and risks in the entire system, FMEA is used to detect potential failure modes in specific components or subsystems. Combining these two approaches enables a more all-encompassing and complete approach to risk analysis. It can provide a more thorough understanding of the potential risks and solutions to mitigate them by using both a bottom-up and top-down approach.

In a product-environment situation, users are able to perform risk assessments from the perspectives of components and their failure modes, as well as from the perspectives of interactions between people, products, and its environments, and the hierarchical control systems. In addition to the component-based risks discovered by the FMEA technique, the possible dangers of an in-use scenario is detected by the STPA methodology.

A risk analysis framework is a methodical strategy that directs the risk analysis process and facilitates in identifying and assessing all relevant and important risks. A risk analysis framework generally includes risk identification, risk assessment, risk management and risk review. Considering the two risk assessment techniques and their process flow, and taking into consideration, the risk analysis frameworks from [30], [21] and [31], the STPA-FMEA risk assessment framework was processed as shown in figure 4.1.

### 4.1.1 Method procedure

As mentioned earlier, the goal of this study is to conduct a thorough risk analysis of the humanoid robot EVE using the STPA-FMEA methodology. This means, the case is aimed to follow a specific set of implementation steps.

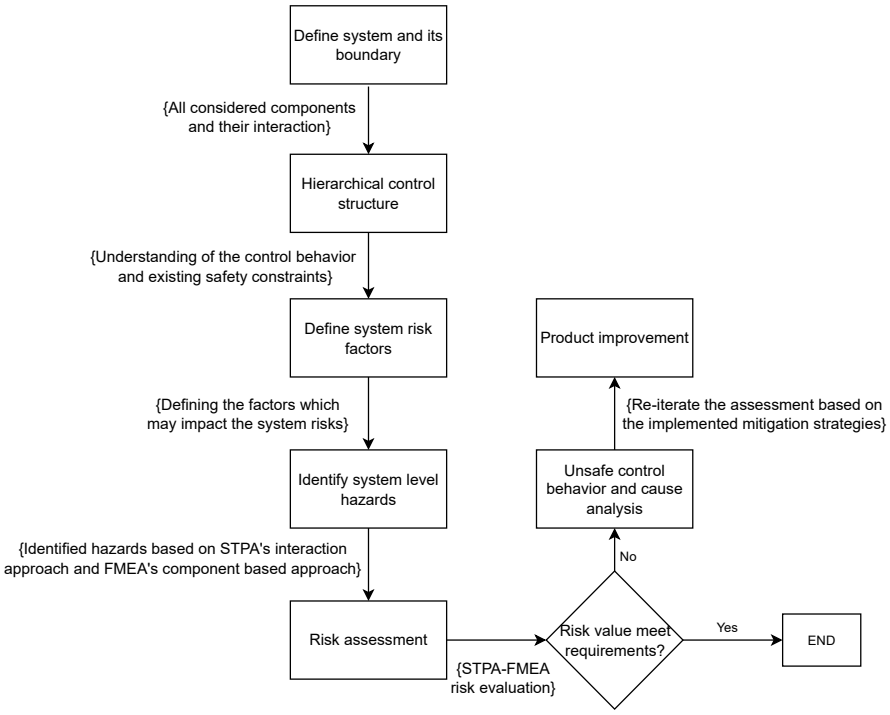


**Figure 4.1:** Risk Management Process Framework

**System scope and system boundary.** The implementation steps start with defining the scope of the system and the system boundaries. Once all the relevant components and their processes are known, it can be constructed in the format of a HCS. The HCS is used to detect various risks or hazards connected to a certain system, process, or their interactions for the risk identification phase. With the control structure in place, there is now an understanding of the different process layers, their control behavior, and a possible understanding on the existing safety constraints present in the system.

**Definition of system risk factors and identification of system level hazards.** From the HCS, one can also examine to understand the risk characteristics and the different types of risk factors which may impact the system. This can be interaction with another component, interaction with a user or the environment. The identification of hazards in the FMEA approach identifies risks in a component based systematic approach, component level hazards can be identified for the system which is present and relevant within the system boundary. It focuses on the likelihood of a failure, its potential failure modes of the system and effects of the failures whereas, with the STPA approach, identification of hazard involves in a more holistic fashion of the system. This means it considers the interactions between components and the broader system context in which the robot operates. From this, the identification of risk sources, failure modes, potential injuries, and their causal relationships are

performed in order to find the risks associated with the humanoid robot EVE.

**Risk assessment.** The risk assessment of the humanoid robot uses the STPA-FMEA methodology which assesses the product including its interaction with the users and the environment. The assessment also involves different user groups and environmental settings as the robot may interact with a variety of users and environments. This thesis also highlights the risks considering the three user groups namely the elderly patients, healthcare workers, and other stakeholders who interact with the robot on a regular basis, and three environmental settings namely, the nursing centre, the residential care, and home care setting. The results of this assessment will provide with insights about the risks and causes associated with the humanoid robot EVE considering the users and environments.

**Product improvement.** The product improvement can be performed later on to improve the system and avoid certain hazard scenarios. This can start with identifying mitigation strategies from the prioritization of the most hazardous risk scenarios. A re-iterated risk quantification can further be performed with the usage of a new risk correction factor to verify and update the risk assessment considering the proposed mitigation strategies to achieve latest results for the STPA-FMEA analysis.

### 4.1.2 Data collection

To conduct this risk assessment, there is a requirement of evaluations of the identified hazard scenarios and their impact whilst considering the interaction with users and the environment, evaluations of different user groups, and environmental settings. As this case study involves a humanoid robot which is aimed at working in a healthcare setting, there is no concrete real-time data as to which this analysis and evaluation has to be performed on. This leads to gathering all the required values from the subject experts.

The data values needed for this risk assessment will be gathered from two experts who have worked with the humanoid robot EVE. The data collection process will be collected on an questionnaire and interview basis. This will help collect all relevant data in order to proceed with the risk assessment using the STPA-FMEA methodology. The figure 4.2 depicts the need for the expert based data collection for this risk assessment.

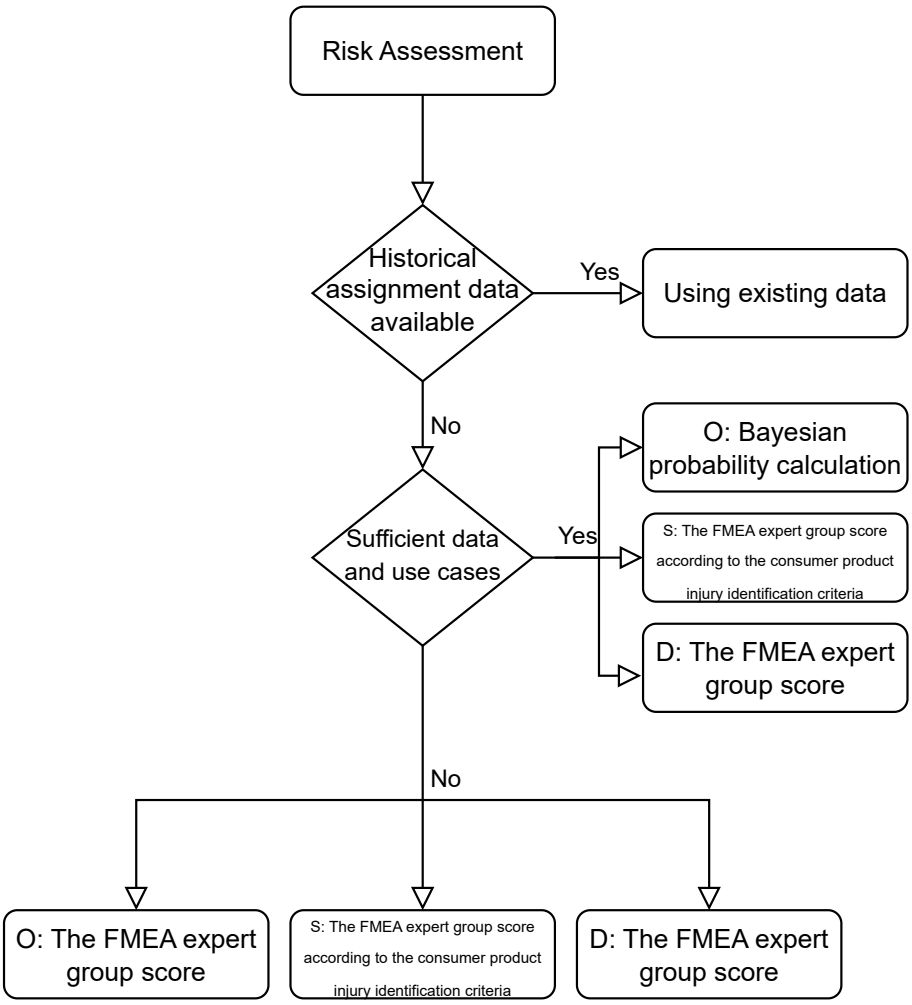


**Figure 4.2:** Risk Management Flowchart [21]

## 4.2 The hierarchical control structure (HCS)

This stage in the STPA-FMEA methodology identifies safety-related controls or limitations that may not be appropriately implemented to harm throughout the design and operation of the system at each level of the control structure. The hazards related to a system or process can be organized and analyzed in risk analysis using a hierarchical control structure. It enables a logical and systematic organization of the risks and offers a precise framework for identifying and managing the most important issues.

In the STPA-FMEA methodology, the hierarchical control structure is used to detect various risks or hazards connected to a certain system, process, or activity during the risk identification phase. This helps the experts to better comprehend the potential repercussions and possibility of each risk by classifying them into distinct categories, which may ultimately aid them in creating effective risk mitigation plans.

In general, a hierarchical control structure is a helpful tool for systematic, logical risk organization and analysis, as well as for identifying and prioritizing the most important risks so they can be efficiently controlled. With respect to the relevant literature [32] [33], the risk analysis takes the user, product, and environment factor into consideration.

From a discussion with regards to the components and their underlying interaction with each other with the experts in this case study, a hierarchical control structure for the humanoid robot EVE was determined, as shown in Figure 4.3.

The hierarchical control structure of the humanoid robot, EVE can be framed as a

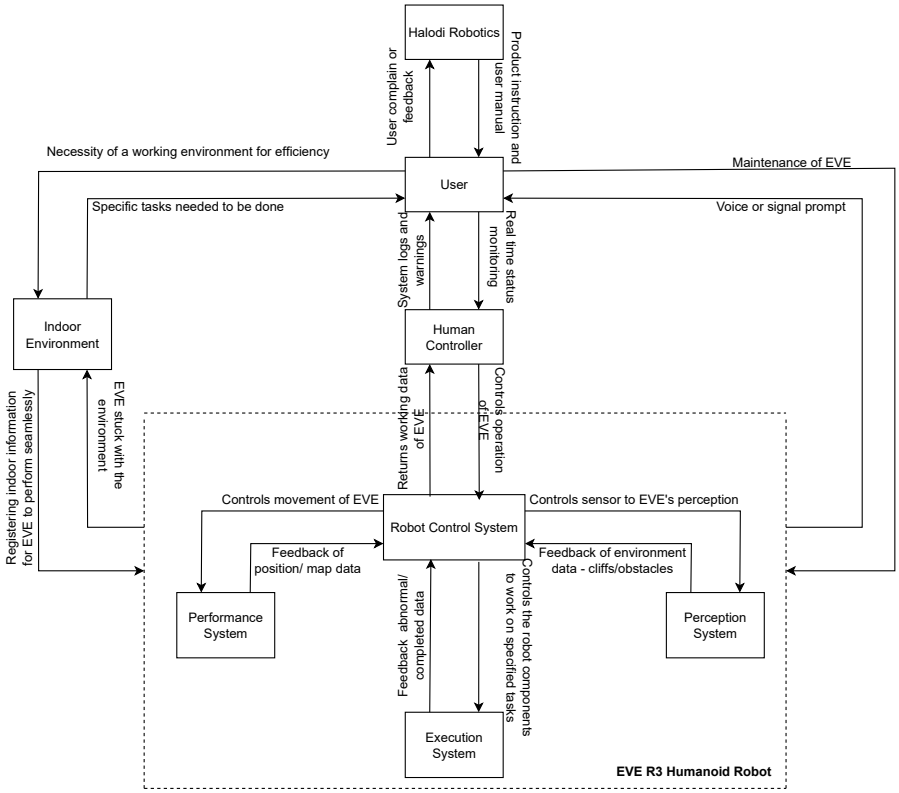


**Figure 4.3:** Hierarchical control structure

three-layered structure with sensing, decision, and execution layers.

The sensing layer has a number of data-gathering sensors, such as HD/ wide-angle cameras which is used to warn against accidental collisions and falls. The application software, and upper computer software are all parts of the decision layer, which is in charge of accepting data received by the product, analyzing the operation, and returning decision data. The drive system and task functionality system are part of the execution layer. In the context of interactions between humans and machines,

the robot can carry out any human assisting tasks in accordance with the directives provided by the decision layer.

Based on the technique described above, the interaction factor such as the relationship between people, product, and the environment must be taken into account in order to apply to scenarios that regularly occur in the human environment.

It is considered that the primary sources of risk are from interactions between person, product, and the environment. The product's structural components are regarded as secondary risk sources. In a people-product-environment system, the user and the environment is taken into account as system risk impact factors. Analyzing the hierarchical control structure of a complex product system yields risk factors from the user, product, and environmental perspectives. These risk factors served as the foundation for the suggestion, selection, and combination of approaching risk events. A short description regarding the risk factors of the person, product and the environment are mentioned as follows.

### 4.2.1 Risk characteristics - User, Product, and Environment

Users' risk factors come in many different forms. First off, individuals who are unfamiliar with the instructions are more likely to use the device improperly or inappropriately, which can cause instability and increase risk. Second, there is a chance of hazard occurring when the user interacts directly with the product, such as crush injuries from the robot collapsing on depletion of battery or the robot colliding with the user's body. Third, users differ subjectively from one another. For instance, aged users or patient may find it difficult to learn and apply new skills, and they are more likely to make mistakes as their physical capabilities and senses deteriorate. As a result, there is a higher likelihood that they won't act quickly to address robot feedback to reduce hazards. On the other hand, when the robot alarms or emits warning signals, users who do not have any idea about the robot's actions or robot's usability because of inadequate knowledge about the humanoid robot may not be able to interact properly or make decisions on their own and may respond incorrectly, putting the product in danger.

The working parameters, structural components, and defects in the current safety constraints are a few common risk factors in products. Although there is a significant likelihood that structural risks may result in mechanical and physical injuries, their impact is rather minimal and they are reasonably simple to control. Contrarily,

unusual working parameters are less likely to occur, but because the process might have been poorly managed and they have the potential to result in explosions, fires, or electrical accidents, the consequences are generally severe. Additionally, a lack of security restrictions, such as privacy protection, or a poor installation will increase risk.

Environment-related hazards typically have an indirect impact on consumers, products, and system risks. Environmental risks are comparatively simple to overlook, and once identified, they are manageable. Environmental risk is influenced by a wide range of factors, many of which are difficult to measure.

## 4.3 Identification of risk factors of EVE

From the robot's HCS, there is now an understanding of the risk characteristics such as different process layers, their control behavior, and a possible understanding on the existing safety constraints. Because a HCS enables a systematic and structured assessment of the components and interactions of a complex system, it is used to identify various risks.

In order to properly identify and assess risks, it is essential to break the system down into manageable components and understand how they are interrelated. This makes it possible to carry out a complete analysis of system elements, their interactions, emergent behaviors, and cascading effects, which leads to a deeper comprehension of potential hazards and their consequences.

Not using a HCS may lead to a lack of system understanding, inadequate risk coverage, and a lack of a standardized approach. These limitations can compromise the effectiveness and reliability of the risk identification process, potentially resulting in missed or misunderstood risks in complex systems. Thus, from the HCS, it is also possible to figure out any possible risks and risk factors based on the user, product and its environment.

With this information gathered, and considering the subject expert's experience on the product, a list of identified risk factors was extracted. The following part will include various subsections such as identifying risk sources, identifying risk events based on those sources, and identifying the causes and potential outcomes of those events.

### 4.3.1 Identification of risk sources

In order to determine the risk sources, the risk factors present in the humanoid robot system, EVE, which are the user, product, and the environment are taken into consideration. The product itself is regarded as the main risk source, and the structural elements of the product are regarded as the secondary risk sources, as was previously mentioned in the study.

From the user manual [4] of the robot EVE, the list of components of the robot are classified into multiple categories of risk sources. These are,

1. The power system – which contains the components such as the Li-ion battery, charger, battery board, BMS etc.,
2. The drive system – under which wheels, motor drivetrain technology etc., are grouped.
3. The control system – contains RGB stereo camera, sensor, etc.,
4. The task functionality system – namely the robot torso, wrist, elbow etc.,
5. The gantry system – which contains the ropes, pulleys, carabiners, tether heads, etc.,
6. The cable components of the robot.

Based on the mentioned possible risk sources, it was decided with the subject expert to condense the given list of risk sources to the components which has a comparatively higher possible use risk. The risk sources was then cut down to the power system, the drive system, the control system, and the gantry system.

### 4.3.2 Identification of risk events

The above-mentioned risk sources can lead to a variety of hazards which in turn leads to risk events affected by the product. By referring to various reports with respect to safety hazards posed by robots such as, [34], [35], [36], and the report, *"Protocol for Assessing Human- Robot Interaction Safety Risks"* from [37], while also considering the expert's opinion on the mentioned hazards occurring in a robot, a list of hazards are chosen to be the primary potential risks connected with the

humanoid robot, EVE. These risks are used to identify the risk events that could potentially occur in the humanoid robot. The identified risks are robot collapsing due to power loss, battery malfunction, overheating, electromagnetic interference, catching and dragging hazards, collision with object/people, motor lock/malfunction, software malfunction, malfunctioning control and transmission elements, hacking threat, sensitive information leak, sensor failure, dragging and twining, tensile cable issues, and low mechanical strength. A combination of 20 groups of risk events were taken into consideration for the case study's risk assessment after coupling the list of product hazards and the product components. These are,

1. Hazards from components of power system: robot collapsing due to power loss, battery malfunction, overheating, electromagnetic interference.

2. Hazards from components of driver system: overheating, catching and dragging hazards, collision with object/people, motor lock/malfunction.

3. Hazards from components of control system: electromagnetic interference, software malfunction, catching and dragging hazards, short circuit, malfunctioning control and transmission elements, hacking threat, sensitive information leak, sensor failure, collision with objects/people.

4. Hazards from components of gantry system: dragging and twining, tensile cable issues, low mechanical strength.

In a similar manner, the failure modes of all the risk events that could be produced from the product itself combined with the above extracted product hazards can be used to identify the risk events that arose from the risk sources. The components and safety constraints serve as the foundation for the STPA-FMEA technique, which is used to investigate the failure modes of products [21]. Based on this study and discussion, it was decided to proceed by categorizing the humanoid robot's failure modes into three groups.

1. Failures resulting from structural issues in the product, such as performance variations, the structure becoming loose, motor pulley wire breaks, and short circuits, are referred to as physical structure failures.

2. Failures resulting from deterioration in the performance characteristics of goods and contact issues, insulation degradation, and increased contact resistance are referred to as failures of the performance characteristics.

3. Functional failure, or the inability of the components to perform as intended under given working conditions, inability of manual or automatic devices to carry out action instructions, and issues with the system's current safety restrictions.

On adding the failure mode to the combination of product components and the product hazards, gives the following 23 different groups.

1. The components of the power system causing the collapse of the robot due to Performance characteristic failure, Battery malfunction due to Physical structure failure, Overheating due to Performance characteristic failure or Electromagnetic interference due to Performance characteristic failure.

2. The components of the Driver system causing Overheating due to Performance characteristic failure, Catching and dragging hazards due to Physical structure failure, Collision with objects/people due to Physical structure failure, Collision with objects/people due to Performance characteristic failure, Collision with objects/people due to function failure, motor lock/malfunction due to Physical structure failure, or motor lock/malfunction due to Performance characteristic failure.

3. The components of the control system causing Electromagnetic interference due to Performance characteristic failure, Software malfunction due to Performance characteristic failure, Catching and dragging hazards due to Physical structure failure, short circuit due to Physical structure failure, Malfunctioning control and transmission elements due to Performance characteristic failure, hacking threat due to Performance characteristic failure, sensitive information leak due to Performance characteristic failure, sensor failure due to function failure or collision with object/people due to function failure.

4. The components of the gantry system causing dragging and twining due to Physical structure failure, tensile cable issues due to Physical structure failure or low mechanical strength due to Physical structure failure.

### 4.3.3 Identification of causes and potential consequences of events

Whenever there occurs a risk event from the humanoid robot, EVE, there is a possibility of occurrence of an injury/accident. From the various types of injuries which were looked upon various articles and literature [21] [38] [39], 10 different types of most common injuries were selected in this study namely, electrical injury, explosion injury, burns, injuries due to environmental damage, crush injuries, smash injuries,

ground injuries, contusions, privacy leakage, and psychological damage. By combining the risk source, its potential hazards and failure modes, and the potential injury/accident, a total of 34 unique groups were identified. This is shown in the table 4.1

Thus, all of the stages for the system's STPA-FMEA technique were followed to attain the risk events. The first stage was to take into account all variables which includes the user, product, and environment; the second stage lists the four product components that were taken into consideration for this case study's risk analysis; the third stage lists the 20 potential hazards of the product; the fourth stage lists the three ways that machines can fail; and the fifth stage lists the ten different types of injuries that could result from risk events. Additionally, using the information obtained, a risk evaluation can be carried out, and all risk events can be quantified to produce a list of the most dangerous risk events and their constituent parts, respectively.

| COMPONENTS | HAZARDS | FAILURE MODE | INJURY / CONSEQUENCES | SYMBOL |
|---|---|---|---|---|
| Power system components | robot collapse due to power loss | Performance characteristic failure | Crush injury | A1 |
| | Battery malfunction | Physical structure failure | Electrical injury | A2 |
| | | | Explosion injury | A3 |
| | | | Burns (Flame) | A4 |
| | Overheating | Performance characteristic failure | Electrical injury | A5 |
| | | | Explosion injury | A6 |
| | | | Burns (Flame) | A7 |
| | Electromagnetic radiation | Performance characteristic failure | Injuries due to environmental damage | A8 |
| Driver system components | Overheating | Performance characteristic failure | Burns (flame) | B1 |
| | Catching and dragging hazards | Physical structure failure | Contusion | B2 |
| | Collision with objects/people | Physical structure failure | Ground injury | B3 |
| | | Performance characteristic failure | Ground injury | B4 |
| | | Function failure | Crush injury | B5 |
| | Motor lock/malfunction | Physical structure failure | Ground injury | B6 |
| | | Performance characteristic failure | Smash injury | B7 |
| Control system components | Electromagnetic radiation | Performance characteristic failure | Injuries due to environmental damage | C1 |
| | Software malfunction | Performance characteristic failure | Smash injury | C2 |
| | | | Privacy leakage | C3 |
| | | | Crush injury | C4 |
| | Catching and dragging hazards | Physical structure failure | Contusion | C5 |
| | Short circuit | Physical structure failure | Electrical injury | C6 |
| | | | Explosion injury | C7 |
| | | | Burns (Flame) | C8 |
| | Malfunctioning control and transmission elements | Performance characteristic failure | Ground injury | C9 |

| COMPONENTS | HAZARDS | FAILURE MODE | INJURY / CONSEQUENCES | SYMBOL |
|---|---|---|---|---|
| | Hacking threat | Performance characteristic failure | Privacy leakage | C10 |
| | | | Psychological damage | C11 |
| | Sensitive information leak | Performance characteristic failure | Privacy leakage | C12 |
| | | | Psychological damage | C13 |
| | Sensor failure | Function failure | Ground injury | C14 |
| | | | Crush injury | C15 |
| | Collision with objects/people | Function failure | Ground injury | C16 |
| Gantry system components | Dragging and twining | Physical structure failure | Smash injury | D1 |
| | Tensile cable issues | Physical structure failure | Crush injury | D2 |
| | low mechanical strength | Physical structure failure | Crush injury | D3 |

**Table 4.1:** Table of identified risks.

# Chapter 5

# Experiment and Analysis

In order to prioritize risk of the 20 identified hazard scenarios, risk quantification needs to be performed. In the following, the risk quantification considered the user and the environment along with the product factors as well.

## 5.1 Risk Evaluation

For the STPA-FMEA methodology, the RPN form of evaluation from the FMEA analysis is considered to evaluate the risk scenarios present in the EVE humanoid robot quantitatively. The RPN determines the priority levels of the risk scenarios. This means, the hazard scenario with the highest RPN value is the most hazardous and should be prioritized the most. The RPN is determined by the risk factors such as the severity of consequences (S), the probability of the occurrence of the event (O), and the detectability of the risk scenario (D) thus leading to the formulation:

$$RPN = S \times O \times D$$

Now, in order to consider the user factor and the environmental factor which associates to the human-robot interaction of the STPA methodology, two variables are added to the existing risk quantification formulation. These are the consumer factor (CF), and the environmental factor (EF). Thus, the STPA-FMEA's risk quantification formulation as stated in [21] would be as follows;

$$RPN = (S \times CFs \times EFs) \times (O \times CFo \times EFo) \times (D \times CFd \times EFd) \text{ [21]}$$

Here, the consumer depicts the user's ability to deal with the robot and the environmental factor depicts the effect on the natural environment and the social environment. Factors like temperature and humidity for robot components, light conditions

for sensors and cameras, terrain conditions such as uneven surfaces, presence of water and debris etc, influence the natural environment valuation, and factors like human training and behavior around robot, interactions with humans, ethical considerations, legal and regulatory compliance, privacy and security etc, influence the social environment valuation.

**The consumer factor.** The consumer factor valuation considers the effect of the user's capacity on a specific hazard scenario which means CF = the consumer ability evaluation X degree to which the consumer ability affects risk [21]. The consumer ability evaluation was evaluated via fuzzy comprehensive evaluation through a questionnaire. The fuzzy comprehensive evaluation is a decision-making method that makes use of fuzzy logic (representation of subjective information by assigning degrees of truth or membership to different categories or values) and multiple criteria analysis to handle uncertainty and imprecision in complex decisions. The effect of the consumer ability affecting the risk scenario was evaluated by the experts of this case study while evaluating the RPN values. For the consumer ability evaluation, the fuzzy comprehensive evaluation index was determined as the following factors - judgement ability, hands-on ability, self-protection ability, and ability to read product instructions. The evaluation set for this fuzzy comprehensive evaluation was a 5 point scale ranging between strongly disagree, disagree, neutral, agree, and strongly agree with its numerical valuations for the calculation being 5, 2, 1, 0.5, 0.2 respectively. The consumer ability evaluation is conducted with respect to determine the consumer ability of three different consumer groups namely, the healthcare workers, the elderly patients, and other stakeholders (anyone associated with the healthcare department or the patient who interacts with the robot). By evaluating the consumer ability values received from the questionnaire evaluated by the experts, the following user ability values is received; healthcare workers - 1.13333, elderly patients - 3.22917, other stakeholders - 1.39583.

**The environmental factor.** Similarly, the environmental factor valuation considers the effect of the use environment on a specific hazard scenario. This means, in formulation, EF = evaluation value for the environment X degree to which the use environment affects the hazard scenario. The environmental factor is aimed to help improve the robot adaptation to the environment and ensure that it can be used in a safe manner effectively by the healthcare professionals in different environments. The environmental evaluation value was evaluated by collecting information

from a questionnaire, whereas the effect of the use environment affecting the risk scenario was evaluated by the experts of this case study also while evaluating the RPN values. Similar to the consumer comprehensive evaluation, the environmental value evaluation was calculated with the help of a fuzzy evaluation index which were, complexity of the environment, level of control over the environment, interaction with other objects and people, and regulatory or safety standards. The evaluation set was again a 5 point scale ranging between very hard, hard, neutral, easy, and very easy and their numerical counterparts were 5, 2, 1, 0.5, 0.2 respectively. The environmental evaluation was conducted to get the valuations of three different environments namely, The nursing centre, the residential care, and the home care service. On evaluation of the environmental valuation received from the questionnaire which was evaluated by the experts, the results were as follows; Nursing centre - 2.0625, Residential care - 1.9375, Home care - 3.275.

Figure 5.1 depicts the parameters which is used for the risk assessment of the case study of the humanoid robot EVE. More details on the risk quantification evaluation, the consumer and the environmental evaluation questionnaires can be referred from Appendix A

Now with all the required data being collected, risk assessment calculation can be performed to retrieve the list of most hazardous risk scenarios. Table 5.1 indicates all the values collected for this analysis. These are in the series of, the severity or occurrence or detection score, the effect of user ability on risk event, the effect of natural environment of risk event, and the effect of social environment on risk.

| Hazard Scenario Symbol (HSS) | SEVERITY | OCCURRENCE | DETECTION | RPN (FMEA) |
|---|---|---|---|---|
| A1 | [6.5, 5.5, 5.5, 5.5] | [3, 7, 2, 3] | [9.5, 8, 1.5, 4.5] | 185.25 |
| A2 | [7, 2.5, 4, 1.5] | [2, 2, 4, 4.5] | [6, 5, 2, 4.5] | 84 |
| A3 | [8, 3.5, 5, 7.5] | [2, 4, 4.5] | [6, 5, 2, 4.5] | 96 |
| A4 | [6, 3, 5, 6] | [2, 2, 4, 4.5] | [6, 5, 2, 4.5] | 72 |
| A5 | [6.5, 4, 4, 2] | [2.5, 3.5, 2.5, 2] | [2.5, 4, 2, 3] | 40.625 |
| A6 | [7, 3.5, 4, 6.5] | [2.5, 3.5, 2.5, 2] | [2.5, 4, 2, 3] | 43.75 |
| A7 | [6.5, 3.5, 4, 5.5] | [2.5, 3.5, 2.5, 2] | [2.5, 4, 2, 3] | 40.625 |
| A8 | [4, 2, 2.5, 2.5] | [1.5, 1.5, 2, 1.5] | [5.5, 3, 2.5, 3] | 33 |
| B1 | [6, 3, 2, 2] | [3, 5, 5, 4] | [5, 7, 4.5, 6] | 90 |
| B2 | [5.5, 4.5, 5, 5.5] | [4, 5.5, 5.5, 3] | [8, 3.5, 4, 3.5] | 176 |
| B3 | [3.5, 4.5, 4, 4.5] | [2.5, 3.5, 5, 5] | [6, 3.5, 2.5, 2.5] | 52.5 |
| B4 | [2.5, 2.5, 5, 4] | [2.5, 5, 6.5, 6] | [6.5, 3, 3, 3.5] | 40.625 |
| B5 | [6.5, 4.5, 5, 5] | [3, 3.5, 5, 4] | [8.5, 4.5, 3, 3.5] | 165.75 |
| B6 | [3.5, 4.5, 5, 5] | [2, 5, 4.5, 4] | [7, 4.5, 3, 4] | 49 |
| B7 | [6, 4.5, 4.5, 5] | [2.5, 3.5, 4.5, 4.5] | [6, 5, 3, 4] | 90 |
| C1 | [4.5, 4, 4.5, 2.5] | [1.5, 2.5, 4, 2] | [2, 3, 1.5, 2.5] | 13.5 |
| C2 | [5.5, 2, 2.5, 3] | [2.5, 1.5, 1.5, 1.5] | [4.5, 4, 2, 2] | 61.875 |
| C3 | [6.5, 3.5, 2.5, 3] | [2.5, 1.5, 1.5, 1.5] | [4.5, 4, 2, 2] | 73.125 |
| C4 | [2, 2, 2, 3] | [2.5, 1.5, 1.5, 1.5] | [4.5, 4, 2, 2] | 22.5 |
| C5 | [6, 3.5, 4.5, 2.5] | [2.5, 3, 3.5, 3] | [9, 3.5, 3, 3] | 135 |
| C6 | [7.5, 3.5, 3.5, 5] | [2, 3, 4.5, 3] | [3.5, 2.5, 2.5, 2.5] | 52.5 |
| C7 | [8, 3.5 5, 6] | [2, 3, 4.5, 3] | [3.5, 2.5, 2.5, 2.5] | 56 |
| C8 | [6.5, 3, 4, 5] | [2, 3, 4.5, 3] | [3.5, 2.5, 2.5, 2.5] | 45.5 |
| C9 | [6, 3.5, 5, 4.5] | [5.5, 2.5, 2.5, 2.5] | [5, 4, 3, 4] | 165 |
| C10 | [1.5, 2, 1.5, 3] | [2.5, 2, 2, 2] | [2.5, 1.5, 1.5, 1.5] | 9.375 |
| C11 | [3, 1.5, 1.5, 2.5] | [2.5, 2, 2, 2] | [2.5, 1.5, 1.5, 1.5] | 18.75 |
| C12 | [2, 1.5, 1.5, 3] | [2.5, 2, 1, 1.5] | [1.5, 1.5, 1.5, 1.5] | 7.5 |
| C13 | [3, 1.5, 1.5, 2.5] | [2.5, 2, 1, 1.5] | [1.5, 1.5, 1.5, 1.5] | 11.25 |
| C14 | [5, 3, 5, 3] | [3, 3.5, 4, 2.5] | [5, 6, 2.5, 3.5] | 75 |
| C15 | [6.5, 2.5, 4, 3] | [3, 3.5, 4, 2.5] | [5, 6, 2.5, 3.5] | 97.5 |
| C16 | [6, 2.5, 5, 5.5] | [5.5, 4.5, 5, 5.5] | [8.5, 3.5, 2.5, 2.5] | 280.5 |
| D1 | [6, 2.5, 4, 5] | [2.5, 4.5, 4.5, 4.5] | [8, 5.5, 2.5, 3.5] | 120 |
| D2 | [6.5, 3, 3, 4.5] | [3, 5.5, 5, 3] | [6.5, 6.5, 3, 4.5] | 126.75 |
| D3 | [6.5, 2, 2, 3.5] | [2, 2.5, 1.5, 2] | [6.5, 6, 3, 4] | 84.5 |

**Table 5.1:** Results of the assessment of the Humanoid Robot EVE.

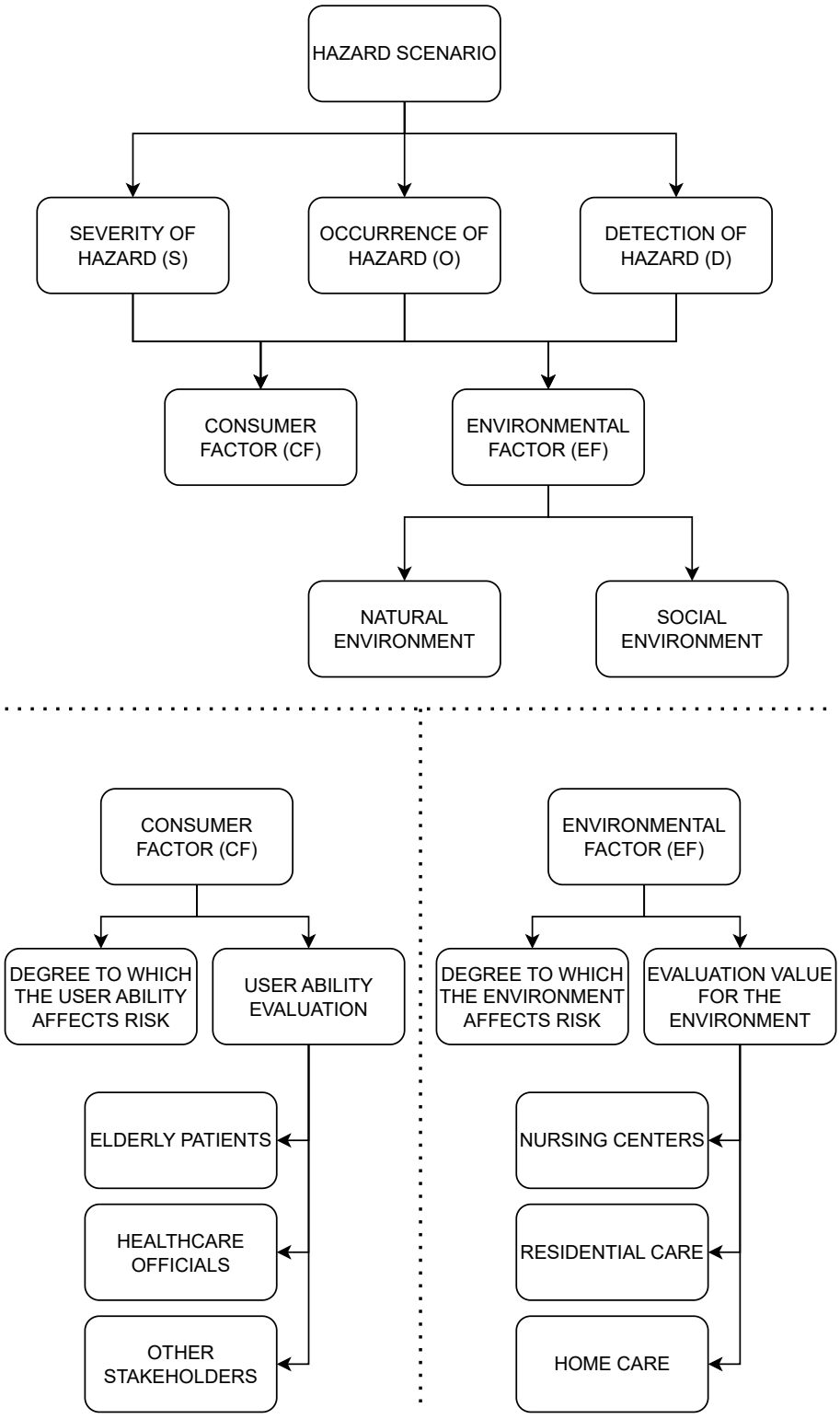


**Figure 5.1:** Factors used for the risk assessment: STPA-FMEA methodology

# Chapter 6

# Results

Based on the results obtained from the the questionnaires by the experts, The RPN values for all the identified hazard scenarios were calculated. This can be seen in figure 6.1. In terms of the evaluation of the humanoid robot EVE with the traditional FMEA, the five most hazardous scenarios out of the identified ones are as follows:

1. C16 - Collision with objects and people because of a function failure in the control system component of the humanoid robot, causing a ground injury.
2. A1 - The robot collapsing due to power loss because of a performance characteristic failure in the power system component of the robot, causing a crush injury.
3. B2 - Having catching and dragging hazards because of a physical structure failure in the driver system component of the robot, causing contusion.
4. B5 - Collision with objects and people because of a function failure in the driver system component of the humanoid robot, causing a crush injury.
5. C9 - Malfunctioning of control and transmission elements because of a performance characteristic failure in the control system component of the robot, causing a ground injury.

In order to show the effects of the user ability / competence and the effects of the two environmental factors on the identified hazards related to the humanoid robot EVE, the figures 6.2, 6.3, and 6.4 are charted.

Figure 6.2 shows the degree to which the user ability affects the identified different risk scenarios. From this graph, it can be seen that, the user competence has a noteworthy effect on the risk values of all the identified hazard scenarios out of which the most significant effect being on the scenarios - the robot collapsing due to power loss of the power system components, overheating and motor lock/malfunction of

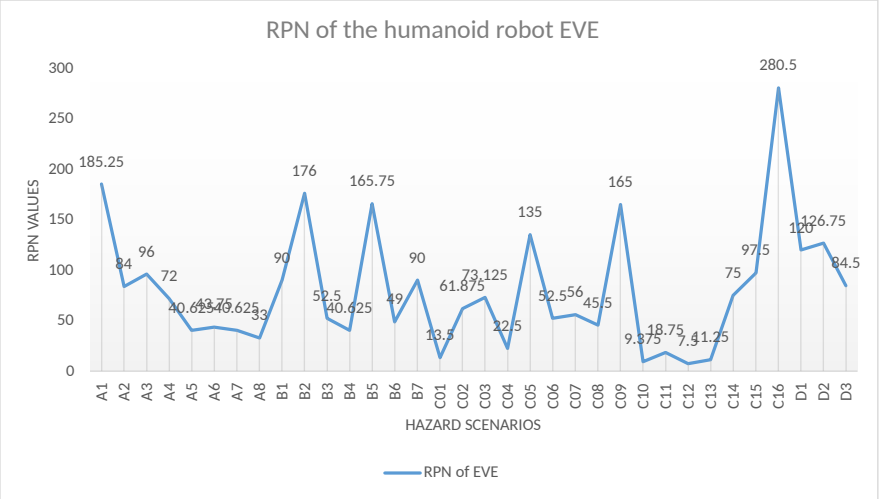


**Figure 6.1:** RPN of humanoid robot EVE

a driver system component, and tensile cable issues in the gantry system components.

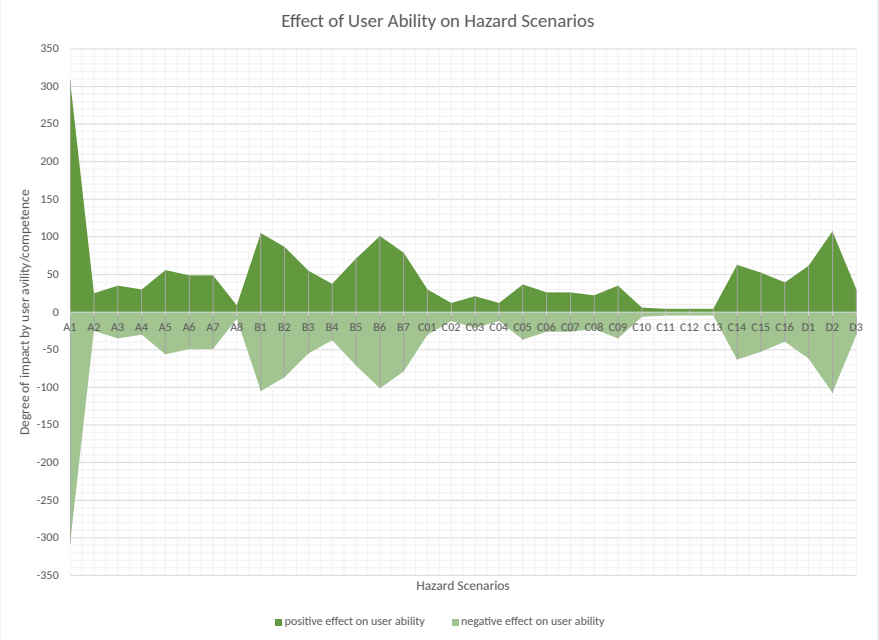


**Figure 6.2:** Effect of user ability

Meanwhile, for the environmental factors affecting the identified hazards, the figure 6.3 depicts the effect of natural environment on the hazard scenarios, whereas the figure 6.4 highlights the effect of social environment on the hazard scenarios. From figure 6.3 it is clear that the natural environment has a significant effect on the catching and dragging hazards, and collision with objects and people caused because of the driver system components. On the other hand, the figure 6.4 depicts that the

social environment has a significant effect on the battery malfunction of the power system components, and the motor lock / malfunction of the driver system components.

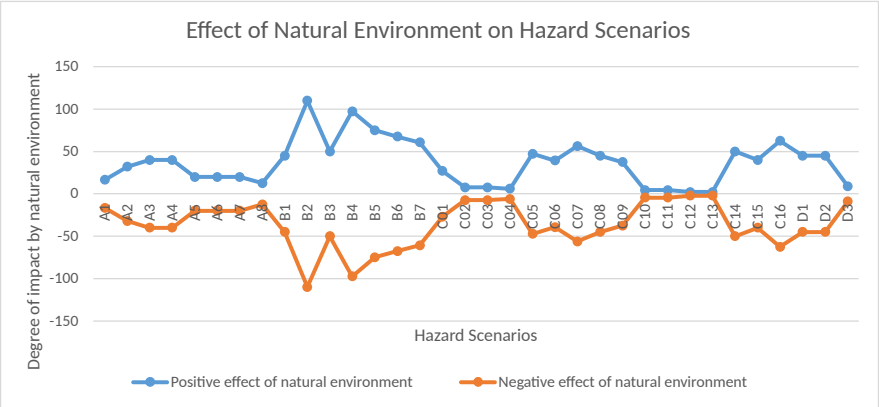


**Figure 6.3:** Effect of natural environment

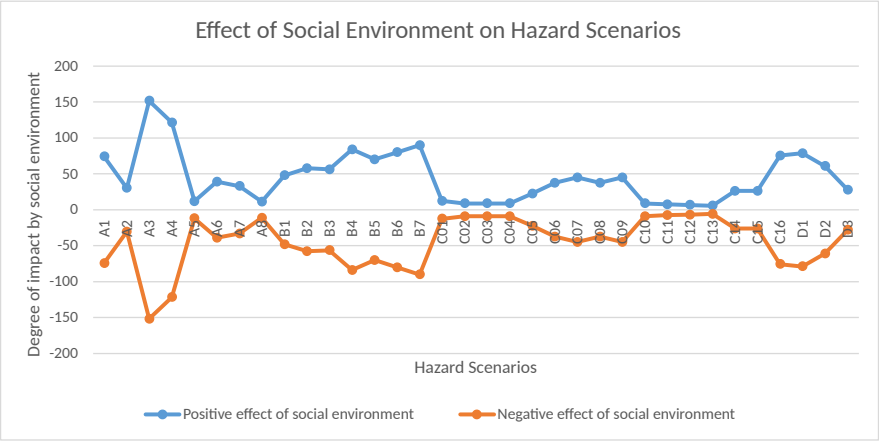


**Figure 6.4:** Effect of social environment

These external factors such as the user and the environmental factors, when combined with the classical FMEA analysis, provide a different result altogether. This means, on a worst case, the risk values of all the identified hazard scenarios may increase than the valuations being mentioned in the classical FMEA analysis. Also, this may also lead to a difference in the top most hazardous risks when compared to the classical FMEA.

Along with the additional factors affecting the risk values of all hazard scenarios, there is also a classification of different user groups, and different operating environments of humanoid robot EVE which is considered as a part of this analysis. Figure

6.5 depicts the RPN values with the external factor of the user ability being considered for four different user groups. These are the elderly patients, the healthcare workers, the other stakeholders in the healthcare/medical department, and a general user (CF = 1). From this, it can be seen that the user group consisting of elderly patients may pose a significantly higher risk when interacting with the humanoid robot compared to the trained healthcare officials who will also be interacting with the robot. Similarly, the figure 6.6 highlights the RPN values with respect to the

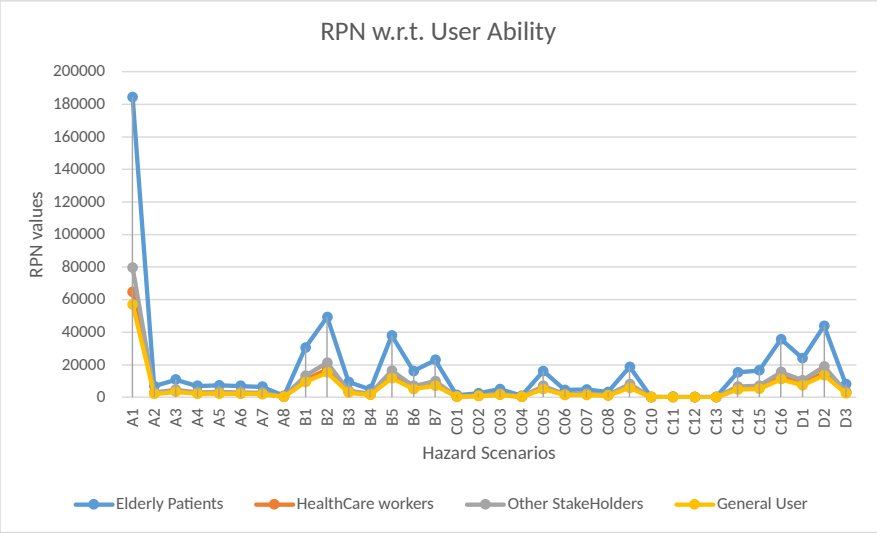


**Figure 6.5:** RPN w.r.t. user ability

natural environmental factor. The natural environmental factor consists of four different environmental settings for the analysis. These are, home-care, nursing centre, residential care, and a general natural environment (EF = 1). It can be seen from this figure that the home-care maybe the most challenging environment for the humanoid robot as it has the highest risk values across all the hazard scenarios when compared to the other environmental settings. This remains the same for the RPN values with respect to the social environment as in figure 6.7, it is clear that the the environmental setting of home-care may possess the highest possible threat when compared amongst the other environmental settings.

By combining all the above external factors to the classical FMEA analysis, the range of risk values of the STPA-FMEA analysis is retrieved. The figure 6.8 highlights the how much the range of risk values of all the identified hazard scenarios of the humanoid robot EVE changes when external factors like the user competence, natural environment and the social environment are taken into effect. The figure 6.9 considers the normalised values of the impact with the RPN values retrieved by the classical FMEA analysis (without considering the external factors) and the RPN values retrieved by the STPA-FMEA analysis (considering the external factors) to have

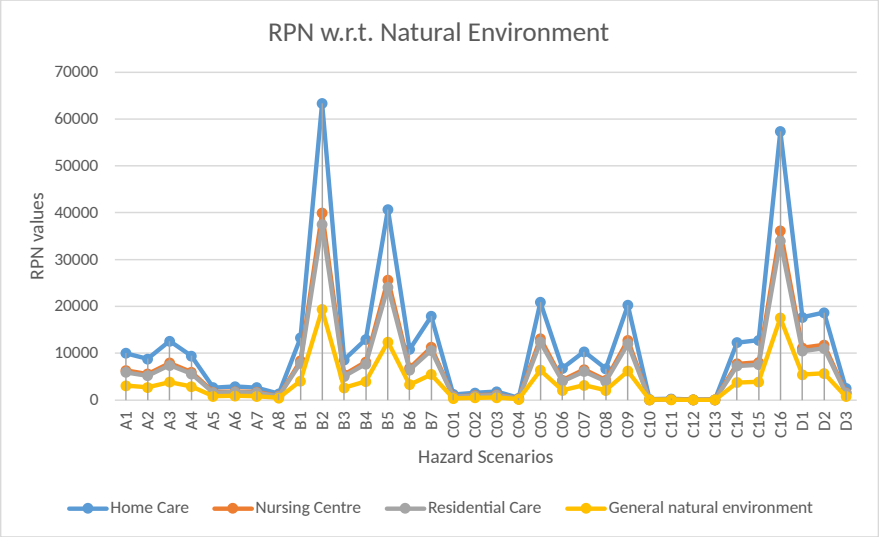


**Figure 6.6:** RPN w.r.t. natural environment

a direct comparison of each considered hazard in the analysis (difference not to be scaled). From the analysis and calculations performed to obtain this figure of the STPA-FMEA RPN valuations, the five most hazardous scenarios obtained from the STPA-FMEA analysis amongst all the identified hazard scenarios are as follows:

1. B2 - Having catching and dragging hazards because of a physical structure failure in the driver system component of the robot, causing contusion.
2. A1 - The robot collapsing due to power loss because of a performance characteristic failure in the power system component of the robot, causing a crush injury.
3. B5 - Collision with objects and people because of a function failure in the driver system component of the humanoid robot, causing a crush injury.
4. C16 - Collision with objects and people because of a function failure in the control system component of the humanoid robot, causing a ground injury.
5. B7 - Having a motor lock or malfunction because of a performance characteristic failure in the driver system component of the robot, causing smash injury.

From this ranking, it is clear that the ranking of the most hazardous risks in STPA-FMEA is different to that of the traditional FMEA analysis. The Ranking symbols in FMEA analysis were C16, A1, B2, B5, and C9 respectively. From this analysis it is certain that for the risk assessment of the humanoid robot EVE, there is a significant effect on the hazard values because of the factors like user ability, natural, and social environment.

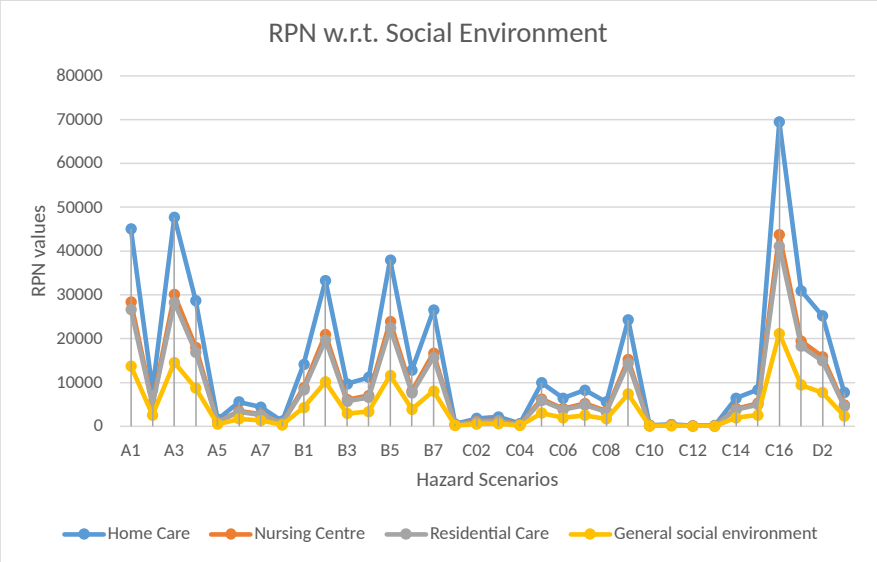


**Figure 6.7:** RPN w.r.t. social environment

For the risk assessment via quantitative methodology, the criteria of expert scoring was chosen for collecting the values such as, the severity of possible injuries caused by the identified hazards, probability of occurrence of these hazards, and the detectability of the hazards. Also, the evaluation criteria for the severity, occurrence, and detection were calculated based on the study [33]. Also, the weightage of these S, O, D values, along with the external factors considered for the valuation given by the experts who participated in this assessment was based on the study [21].

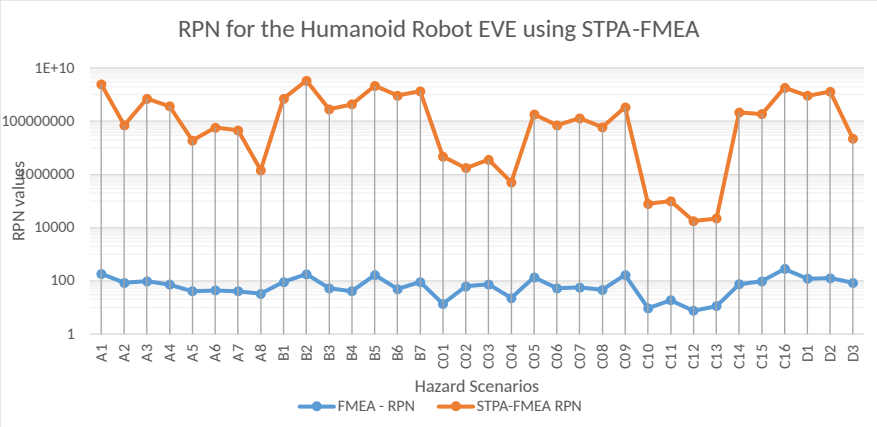


**Figure 6.8:** STPA-FMEA RPN

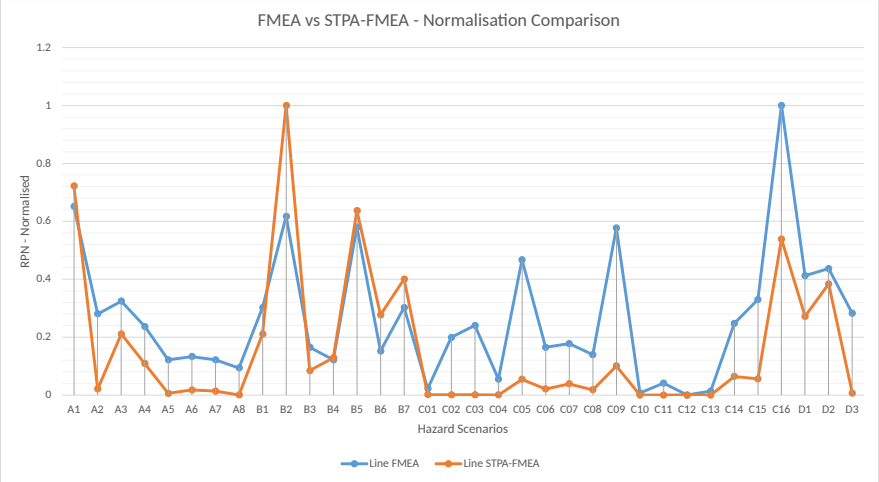


**Figure 6.9:** Normalised comparison STPA-FMEA vs Classical FMEA

# Chapter 7

# Discussion

In the previous chapters, risk assessment of the humanoid robot EVE was conducted using the STPA-FMEA methodology. The results showed a clear deviation from the output of a Classical FMEA, highlighting the importance of external factors like user ability and the environmental setting the product is in on risk assessment outcomes.The following chapter will delve into the validity of this research as to why the analysis should be considered trustworthy. The chapter will also examine the conclusions that can be made from the results of the risk assessment.

## 7.1 Validity of research

The term ”validity” in a study relates to how the findings are reliable and unaffected by the researchers' personal bias. In other words, it is a sign of the dependability and accuracy of the results. The study [40] here lists construct validity, internal validity, external validity, and reliability as the four components of validity assessment.

**Construct validity.** If the operational measures used in the study accurately reflect what the researcher meant to investigate, that is what construct validity is concerned with. There is a chance that the researcher may not be able to clearly interpret the information related to the robot and the potential hazards to the experts of this case study for the data collection to which the outputs are necessary to quantify the risks conducted in this case study. There may also be a chance where the experts of this case study may misinterpret this requested information entirely which would lead to an inaccurate risk quantification for this case study. To tackle this, an interview between the researcher and the experts was held in relation to the data collection for potential hazard scenarios to clarify the intent of the questions posed in the questionnaires and to resolve any concerns made in this respect.

**Internal validity.** The ability of a study to establish a cause-and-effect relationship between variables is referred to as internal validity. There may be a chance that a third component, which the researcher is either not aware of or does not completely comprehend, could also have an impact on a factor being researched. According to a study [41], subjectivity is present at every level of the risk and hazard analysis process. Uncertainty, a need for judgment, a significant chance for human bias, and inaccurate data are all constant risks. The likelihood that one researcher's results will differ from those of other researchers who start with the same, identical data is very high. This risk may be seen in the data collection for quantification of identified risks in this case study. This risk is addressed by setting boundaries for the hazard scenarios that are to be quantified and, completing the questionnaire simultaneously with the researcher conducting an interview to explain each hazard scenario. Additionally, the experts who contributed to the hazard analysis questionnaires typically had sufficient knowledge of humanoid robots and were able to understand the context in which the variables for the case study's examined hazard scenarios were to be asked.

**External validity.** The extent to which the results can be generalized and are relevant to those beyond the subject of the investigation is what is meant by external validity. The findings from this study may be useful and applicable in the investigation of other safety-critical systems of a similar nature. This study's findings can also be used to compare various analytical techniques with the same or a different safety-critical system.

**Reliability.** The degree to which the data and analysis depend on the particular researchers is a concern with reliability. The outcomes should be the same if the study were carried out by another researcher. By carrying out data collection in the form of both questionnaires and an interview, reliability was addressed in this study. In meetings or interviews, any ambiguities or problems with the questionnaire were resolved. The reliability, however, could be compromised if the identical questionnaire was provided to a different researcher because their perspectives might change. To reduce this possibility, one might thoroughly explain each hazard scenario in the questionnaire to clear up any misunderstandings, but doing so might make it more challenging for the expert to complete the questionnaire.

## 7.2 Inference of result

The STPA-FMEA methodology was used to complete the risk assessment for this case study. It is also evident from the study's findings that the STPA-FMEA analysis's ranking of the most hazardous risks differs from that of the conventional FMEA analysis'. This is due to the STPA-FMEA analysis's incorporation of multiple elements, such as user competence, the natural environment, and the social environment, in addition to the hazard's severity, occurrence, and detection. Additionally, this analysis includes a classification of user groups and environmental settings to demonstrate how significantly different the risk values are for various user groups and environments. The results of the analysis show that, when compared to the other user groups and environmental settings, the elderly patient user group and the home-care environmental setting had the highest RPN values. Conversely, the healthcare workers user group and the residential care environmental setting had the lowest RPN values. To conclude the risk assessment for this case study and demonstrate how this analytical range differs from the traditional FMEA analysis, a combination of all these external factors is combined altogether in the STPA-FMEA analysis to provide a comparision against the traditional FMEA analysis.

## 7.3 Product improvement via treating unsafe control behaviors

The STPA-FMEA approach can be used to help find strategies to lower hazards associated with the humanoid robot EVE after assessing the risks involved. Safety measures might be recommended to reduce or eliminate risks depending on the amount of risk and their viability. High-risk scenarios can be identified, unsafe control measures can be found, and ways to reduce the risk can be suggested after assessing the risk assessment statistics as illustrated in Chapter 6. In the end, this will make the product better and safer.

In order to improve the product by mitigating or reducing the risks identified in the hazard scenarios, certain countermeasures to avoid such risks needs to be identified. For example, consider a hazard scenario like - the motor lock or malfunction, which may occur because of something blocking the motor, leading to limited actions or no fully completed action cycle by the humanoid robot, or in the worst case, damaging or even breaking of the motor. To avoid this, there can be a mitigation strategy where a stop signal could be sent to the robot in case the robot is unable to complete a full cycle of any action smoothly. This may help reduce the risk of a fail-

ure of motor of the drive system component. The same strategy can be used if the robot causes catching and dragging hazards, so that any knock-on effects caused by this hazard scenario can be mitigated. Another hazard scenario can be the threat of hacking or stealing sensitive information which can be relatively more difficult to mitigate. This would deal with leakage of privacy of any user the robot interacts with. To try and reduce the severity of this issue, a private network can be hosted to have the interaction of the robot application software, with the machine and the server in a secure manner which could protect the transmission of data to some extent, thus avoiding information leak. Also, this robot application software can be used to send maintenance reminders to the users accessing the robot in order to avoid other possible failures which might include battery malfunction, software malfunction, or any sensor failures.

A measure called ”risk correction factor” is then introduced to account for the improvements made to increase safety after evaluating the hazard scenarios of the EVE humanoid robot. This factor is used in the following formula in order to evaluate the robot's safety whilst considering the mitigation strategies of the hazard scenarios.

$$RPN = (S \times CFs \times EFs) \times (O \times CFo \times EFo) \times (D \times CFd \times EFd) \times \alpha. \text{ [21]}$$

With the addition of this new risk correction component to the equation, the risk assessment may now be completed. Along with the addition of the correction factor $\alpha$, the assessment processes will remain the same as the risk assessment steps in the proposed technique. This could cause the risk value for some threats to decrease. When an unsafe behavior observed in the humanoid robot EVE is managed, the RPNs for the risk events impacted by the risk correction factor may decrease. In other words, the risk value of the risk events may dramatically decline and the humanoid robot may improve. Therefore, risk assessment results for various products can be acquired by following the risk identification and risk assessment process employed in this case study.

# Chapter 8

# Conclusion and future work

This thesis has presented a case study of a humanoid robot EVE for which risk assessment was performed in a healthcare setting. That is, to identify what hazards may occur if this robot is deployed in a healthcare setting assisting elderly patients. This thesis performs just that, with the combination of two risk analyses frameworks such as FMEA and STPA as its methodology. The STPA-FMEA risk assessment methodology is a new approach to guarantee the safety of the products under the risk evaluation. This combines two techniques, STPA analysis and FMEA failure mode analysis, with the aim of identifying hazards and injury brought on by the product before they can occur rather than attempting to solve them after they do. FMEA assists in identifying all the potential failure modes and root causes of a product, whereas STPA assists in identifying the risks present in a system and what can be done to prevent them. These risks are measured using the RPN approach which is used in quantification of hazards in the FMEA analysis.

In order to conduct a thorough risk assessment for this humanoid robot EVE, various external factors such as user ability, and the environmental factors interacting with the product is considered in addition to the product in hand. Thus, the results acquired from this proposed STPA-FMEA analysis is significantly different from the results obtained by traditional FMEA analysis. This shows that the external factors such as the user ability and the environmental setting has a substantial impact on the STPA-FMEA analysis. Moreover, with the STPA-FMEA analysis, hazard scenarios with high RPN can be considerably reduced by investigating and providing mitigation strategies to the unsafe control behaviours and its causes. The risk assessment for these hazard scenarios along with considering their risk correction factor can then be re-iterated to obtain a possibly reduced RPN thus, reducing the risk caused by the product.

However, there are some limitations with the case study using the STPA-FMEA

methodology. First, as this case study does not contain any supporting data for the risk analysis, the data used for this assessment is retrieved from experts through the means of interviews and questionnaires. Hence, there is some level of subjectivity involved with this kind of approach. Second, the risk analysis conducted in this case study takes all the required data from the experts who have worked only with the humanoid robot. As the robot is not deployed in the real world, there maybe a lot of unknowns with respect to identifying the risks related to robots in this particular case study which in-turn led to generalising the identified hazard scenarios for this risk assessment. Third, for the risk analysis performed in this case study, only two expert's data were utilized, this may be a limitation for the performed risk assessment on the case study.

As a part of future work, one can create a more thorough taxonomy of risks particular to humanoid robots to identify potential unique concerns and to cover every potential risk present in this case study. One can conduct an in-depth analysis of specific patient populations which the humanoid robot will be interacting with. This may involve examining the needs and vulnerabilities of different age groups, medical conditions, and cultural backgrounds of the patients to better understand the risks and potential hazards associated with the robot's actions. Also, one can address potential malfunctions of the robot's hardware, software, or communication systems by implementing the mitigation strategy for product improvement.

# Bibliography


[1] J. A. Brandsma, “IMPLEMENTATION OF SOCIAL SERVICE ROBOTS IN DUTCH HEALTHCARE.”

[2] H. Robotics, “Brochure - EVE r3 humanoid robot.”

[3] N. Gupta, J. Smith, B. Shrewsbury, and B. Bornich, “2d push recovery and balancing of the EVE r3 - a humanoid robot with wheel-base, using model predictive control and gain scheduling,” pp. 365–372.

[4] H. Robotics, “User manual halodi robotics EVE-r3.”

[5] C. Y, “Robot safety: Overview of risk assessment and reduction,” vol. 05, no. 1. [Online]. Available: http://www.omicsgroup.org/journals/robot-safety-overview-of-risk-assessment-and-reduction-2168-9695-1000139.php?aid=68463

[6] A. Zacharaki, I. Kostavelis, A. Gasteratos, and I. Dokas, “Safety bounds in human robot interaction: A survey,” vol. 127, p. 104667. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0925753520300643

[7] W. S. Lee, D. L. Grosh, F. A. Tillman, and C. H. Lie, “Fault tree analysis, methods, and applications a review,” vol. R-34, no. 3, pp. 194–203, conference Name: IEEE Transactions on Reliability.

[8] H.-C. Liu, L. Liu, and N. Liu, “Risk evaluation approaches in failure mode and effects analysis: A literature review,” vol. 40, no. 2, pp. 828–838. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0957417412009712

[9] S. Shappell and D. Wiegmann, “The human factors analysis and classification system-HFACS.”

[10] J. Dunjó, V. Fthenakis, J. A. Vílchez, and J. Arnaldos, “Hazard and operability (HAZOP) analysis. a literature review,” vol. 173, no. 1, pp. 19–32. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0304389409013727

[11] T. Ishimatsu, N. Leveson, J. Thomas, M. Katahira, Y. Miyamoto, and H. Nakao, “Modeling and hazard analysis using STPA.”

[12] D. Martin-Guillerez, J. Guiochet, D. Powell, and C. Zanon, “A UML-based method for risk analysis of human-robot interactions,” in *Proceedings of the 2nd International Workshop on Software Engineering for Resilient Systems*. ACM, pp. 32–41. [Online]. Available: https://dl.acm.org/doi/10.1145/2401736.2401740

[13] J. Guiochet, “Hazard analysis of human–robot interactions with HAZOP–UML,” vol. 84, pp. 225–237. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S092575351500346X

[14] L. Chen, J. Jiao, and T. Zhao, “A novel hazard analysis and risk assessment approach for road vehicle functional safety through integrating STPA with FMEA,” vol. 10, no. 21, p. 7400. [Online]. Available: https://www.mdpi.com/2076-3417/10/21/7400

[15] M. Shafiee, “Failure analysis of spar buoy floating offshore wind turbine systems,” vol. 8, no. 1, p. 28. [Online]. Available: https://doi.org/10.1007/s41062-022-00982-x

[16] S. Sultana, P. Okoh, S. Haugen, and J. E. Vinnem, “Hazard analysis: Application of STPA to ship-to-ship transfer of LNG,” vol. 60, pp. 241–252. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0950423018304200

[17] L. Sun, Y.-F. Li, and E. Zio, “Comparison of the HAZOP, FMEA, FRAM and STPA methods for the hazard analysis of automatic emergency brake systems,” vol. 8.

[18] P. M. Salmon, M. Cornelissen, and M. J. Trotter, “Systems-based accident analysis methods: A comparison of accimap, HFACS, and STAMP,” vol. 50, no. 4, pp. 1158–1170. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0925753511002992

[19] P. Böhm and T. Gruber, “A novel HAZOP study approach in the RAMS analysis of a therapeutic robot for disabled children,” in *Computer Safety, Reliability, and Security*, ser. Lecture Notes in Computer Science, E. Schoitsch, Ed. Springer, pp. 15–27.

[20] B. Riemersma, R. Künneke, G. Reniers, and A. Correljé, “Upholding safety in future energy systems: The need for systemic risk assessment,” vol. 13, no. 24, p. 6523, number: 24 Publisher: Multidisciplinary Digital Publishing Institute. [Online]. Available: https://www.mdpi.com/1996-1073/13/24/6523

[21] Y. Zhang and T. Liu, “Risk assessment based on a STPA–FMEA method: A case study of a sweeping robot,” vol. 43, no. 3, pp. 590–604, _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/risa.13927. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/risa.13927

[22] S. M. Sulaman, A. Beer, M. Felderer, and M. Höst, “Comparison of the FMEA and STPA safety analysis methods–a case study,” vol. 27, no. 1, pp. 349–387. [Online]. Available: http://link.springer.com/10.1007/s11219-017-9396-0

[23] J.-E. Rah, R. P. Manger, A. D. Yock, and G.-Y. Kim, “A comparison of two prospective risk analysis methods: Traditional FMEA and a modified healthcare FMEA: Comparison of FMEA and modified HFMEA,” vol. 43, no. 12, pp. 6347–6353. [Online]. Available: http://doi.wiley.com/10.1118/1.4966129

[24] Y. J. Ng, M. S. K. Yeo, Q. B. Ng, M. Budig, M. A. V. J. Muthugala, S. M. B. P. Samarakoon, and R. E. Mohan, “Application of an adapted FMEA framework for robot-inclusivity of built environments,” vol. 12, no. 1, p. 3408, number: 1 Publisher: Nature Publishing Group. [Online]. Available: https://www.nature.com/articles/s41598-022-06902-4

[25] T. Murino, M. D. Nardo, D. Pollastro, N. Berx, A. D. Francia, W. Decré, J. Philips, and L. Pintelon, “Exploring a cobot risk assessment approach combining FMEA and PRAT,” vol. 39, no. 3, pp. 706–731, _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/qre.3252. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/qre.3252

[26] C. Bensaci, Y. Zennir, D. Pomorski, F. Innal, Y. Liu, and C. Tolba, “STPA and bowtie risk analysis study for centralized and hierarchical control architectures comparison,” vol. 59, no. 5, pp. 3799–3816. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1110016820303045

[27] R. Liang, Z. Xue, and H.-Y. Chong, “Risk evaluation of logistics park projects’ lifecycle during the COVID-19 pandemic: Failure mode and effects analysis,” vol. 149, no. 1, p. 04022153, publisher: American Society of Civil Engineers. [Online]. Available: https://ascelibrary.org/doi/10.1061/%28ASCE%29CO.1943-7862.0002430

[28] L. Lipol and J. Haq, “Risk analysis method: Fmea/fmeca in the organizations,” vol. 11, pp. 74–82.

[29] M. V. Stringfellow, N. G. Leveson, and B. D. Owens, “Safety-driven design for software-intensive aerospace and automotive systems,” vol. 98, no. 4, pp. 515–525, conference Name: Proceedings of the IEEE.

[30] 14:00-17:00. ISO 31000:2018. [Online]. Available: https://www.iso.org/standard/65694.html

[31] S. N. Luko, "Risk management principles and guidelines," vol. 25, no. 4, pp. 451–454. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1080/08982112.2013.814508

[32] R. Araujo and A. de Almeida, "Learning sensor-based navigation of a real mobile robot in unknown worlds," vol. 29, no. 2, pp. 164–178, conference Name: IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics).

[33] D. Herrera, F. Roberti, R. Carelli, V. Andaluz, J. Varela Aldás, J. Ortiz, and P. Canseco, "Modeling and path-following control of a wheelchair in human-shared environments," vol. 15, p. 1850010.

[34] C. C. f. O. H. a. S. Government of Canada. CCOHS: Robots and cobots. Last Modified: 2023-06-13. [Online]. Available: https://www.ccohs.ca/oshanswers/safety_haz/robots_cobots.html

[35] Safe robot navigation in dense crowds | CROWDBOT project | fact sheet | h2020. [Online]. Available: https://cordis.europa.eu/project/id/779942

[36] P. Salvini, D. Paez Granados, and A. Billard, "Safety concerns emerging from robots navigating in crowded pedestrian areas," vol. 14.

[37] CPWR safety hazards. [Online]. Available: https://www.cpwr.com/research/published-research/cpwr-reports/safety-hazards/

[38] B. C. Jiang and C. A. Gainer, "A cause-and-effect analysis of robot accidents," vol. 9, no. 1, pp. 27–45. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/037663498790023X

[39] P. Salvini, G. Ciaravella, W. Yu, G. Ferri, A. Manzi, B. Mazzolai, C. Laschi, S. Oh, and P. Dario, "How safe are service robots in urban environments? bullying a robot," in *19th International Symposium in Robot and Human Interactive Communication*, pp. 1–7, ISSN: 1944-9437.

[40] P. Runeson, M. Höst, A. Rainer, and B. Regnell, *Case Study Research in Software Engineering: Guidelines and Examples*, 1st ed. Wiley. [Online]. Available: https://onlinelibrary.wiley.com/doi/book/10.1002/9781118181034

[41] F. Redmill, "Risk analysis - a subjective process," vol. 12, no. 2, p. 91. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/em_20020206

# Appendix A

# Questionnaires to experts to quantify the risk events

The evaluation of the risk events identified in the humanoid robot EVE is conducted via three different questionnaires to the subject experts where each questionnaire target specific details which is required for the risk quantification of the robot. These questionnaires are:

1. Consumer ability evaluation
2. Use environment evaluation
3. Risk quantification evaluation

More details regarding to the respective questionnaires are in the following sections.

## A.1 Consumer ability evaluation

In order to quantify the risk events based on user groups along with the risk quantification of the risk events of the humanoid robot EVE, the consumer ability evaluation was conducted. This was conducted to determine the consumer ability of three different consumer stakeholder groups namely, the healthcare workers, the elderly patients, and other stakeholders (anyone associated with the healthcare department or the patient who interacts with the robot). The evaluation was based on a 5-point scale ranging from strongly disagree, disagree, neutral, agree, and strongly agree with its numerical valuations for the calculation being 5, 2, 1, 0.5, 0.2 respectively. There were four different factors considered for the consumer ability evaluation as the evaluation index, of which each factor was given a weight of 25 percent of the total consumer ability evaluation in this case study. The questions posed for each of these factors are as follows.

### A.1.1 Judgement ability

1. The following stakeholders are aware of their limitations and seek professional help or advice when necessary to evaluate potential risks.

2. The following stakeholders would be knowledgeable about the different types of risks associated with the robot.

3. The following stakeholders are aware of the potential risks associated with the robot before starting to interact with it.

### A.1.2 Hands on ability

1. The following stakeholders would be able to make use of the robot up to its full potential.

2. The following stakeholders would be able to follow the safety guidelines and precautions when interacting with the robot.

3. The following stakeholders are confident in their ability to assess the risks associated with the robot.

### A.1.3 Self protection ability

1. The following stakeholders would be able to trust the manufacturers and service providers provide clear and accurate information about the risks associated with the robot.

2. The following stakeholders would be able to seek additional information about the robot if they are unsure about its safety or potential risks.

3. The following stakeholders would be able to trust that the government agencies would regulate and enforce safety standards for the robot to protect consumers from potential risks.

### A.1.4 Ability to read product instructions

1. The following stakeholders would be able to read and understand the product warnings and safety instructions before using the robot.

## A.2 Use environment evaluation

In order to quantify the risk events based on the use environments to evaluate the environment, the valuation of environmental settings was conducted. This was conducted to determine the environmental valuations of three different environments namely, the nursing centre, the residential care, and the home care service. The evaluation was based on a 5-point scale ranging from very hard, hard, neutral, easy, and very easy and their numerical counterparts were 5, 2, 1, 0.5, 0.2 respectively. There were four different factors considered for the use environment evaluation as the evaluation index, of which each factor was given a weight of 25 percent of the total use environmental evaluation in this case study. The questions posed for each of these factors are as follows.

### A.2.1 Complexity of the environment

1. Determine the ability of the humanoid robot to handle the complexity of working in the environment to provide assistance to elderly patients and the healthcare workers.

### A.2.2 Level of control over the environment

1. Determine on a scale of very poor to very good, how beneficial will it be for the humanoid robot with respect to the freedom and the level of control over the environment in order to assist the patients and healthcare workers.

### A.2.3 Interaction with other objects and people

1. How easy is it for the humanoid robot to interact with people and other objects in different environments in order to serve safely and efficiently.

### A.2.4 Regulatory or safety standards

1. How easy and viable is it for the humanoid robot to meet the regulatory and safety standards in different environments to provide assistance to the healthcare workers or patients.

## A.3 Risk quantification evaluation

The risk quantification of the humanoid robot EVE was performed by using two questionnaires in order to get all the information for the STPA-FMEA methodology. These are:

1. Risk quantification of EVE
2. Degree to which the User and the Environment affects the Hazard scenarios

**Risk quantification of EVE** This Questionnaire was used to collect relevant data with regards to the humanoid robot EVE, from which the goal was to quantify the risk of 34 unique hazard cases. This questionnaire's purpose was to collect data values like severity, occurrence and, detection with respect to each hazard, source of the hazard and, its consequences in a product component. The valuation scale considered was between 1 and 10. 1 amounting to the least risk possibility and 10 amounting to the highest possible risk value.

**Degree to which the User and the Environment affects the Hazard scenarios** The goal of this questionnaire was to collect information with regards to the degree to which the consumer ability or the use environment that would affect the hazard scenario. As the previous questionnaire was used to get information on the severity, occurrence, and detection values a specific hazard scenarios, this questionnaire was useful to gather information regarding how much would the factors like the consumer, and the use environment like the natural and the social environment would affect the severity, occurrence, and detection values of the 34 unique hazard scenarios. The valuation scale considered was between 1 and 10 where 1 indicates ”no change” and 10 indicates ”a very significant change.”.
The 34 unique hazard scenarios are split between four components. These hazard scenarios with respect to their components are as follows:

### A.3.1 Component - Power system

1. Having robot collapse due to depletion of power which is caused because of a performance characteristic failure causing a crush injury to the user.
2. Having battery malfunction which is caused because of a physical structure failure causing an electrical injury to the user.
3. Having battery malfunction which is caused because of a physical structure failure causing an explosion injury to the user.

4. Having battery malfunction which is caused because of a physical structure failure causing burn (flame) injury to the user.
5. Having overheating which is caused because of a performance characteristic failure causing an electrical injury to the user.
6. Having overheating which is caused because of a performance characteristic failure causing an explosion injury to the user.
7. Having overheating which is caused because of a performance characteristic failure causing burn (flame) injury to the user.
8. Having electromagnetic interference which is caused because of a performance characteristic failure causing injuries due to environmental damage to the user.

### A.3.2 Component - Driver system

1. Having overheating which is caused because of a performance characteristic failure causing burn (flame) injury to the user.
2. Having catching and dragging hazards which is caused because of a physical structure failure causing contusion to the user.
3. Having collision with objects/people which is caused because of a physical structure failure causing ground injury to the user.
4. Having collision with objects/people which is caused because of a performance characteristic failure causing ground injury to the user.
5. Having collision with objects/people which is caused because of a function failure causing crush injury to the user.
6. Having motor lock/malfunction which is caused because of a physical structure failure causing ground injury to the user.
7. Having motor lock/malfunction which is caused because of a performance characteristic failure causing smash injury to the user.

### A.3.3 Component - Control system

1. Having electromagnetic interference which is caused because of a performance characteristic failure causing injuries due to environmental damage to the user.

2. Having software bugs/glitches which is caused because of a performance characteristic failure causing smash injury to the user.

3. Having software bugs/glitches which is caused because of a performance characteristic failure causing crush injury to the user.

4. Having software bugs/glitches which is caused because of a performance characteristic failure causing privacy leakage to the user.

5. Having catching and dragging hazards which is caused because of a physical structure failure causing contusion to the user.

6. Having short circuit which is caused because of a physical structure failure causing an electrical injury to the user.

7. Having short circuit which is caused because of a physical structure failure causing an explosion injury to the user.

8. Having short circuit which is caused because of a physical structure failure causing burn (flame) injury to the user.

9. Having malfunctioning control and transmission elements which is caused because of a performance characteristic failure causing ground injury to the user.

10. Having hacking threat which is caused because of a performance characteristic failure causing privacy leakage to the user.

11. Having hacking threat which is caused because of a performance characteristic failure causing psychological damage to the user.

12. Having sensitive information leak which is caused because of a performance characteristic failure causing privacy leakage to the user.

13. Having sensitive information leak which is caused because of a performance characteristic failure causing psychological damage to the user.

14. Having sensor failure which is caused because of a function failure causing ground injury to the user.

15. Having sensor failure which is caused because of a function failure causing crush injury to the user.

16. Having collision with objects/people which is caused because of a function failure causing ground injury to the user.

### A.3.4 Component - Gantry system

1. Having dragging and twining which is caused because of a physical structure failure causing smash injury to the user.
2. Having tensile rope issues which is caused because of a physical structure failure causing crush injury to the user.
3. Having low mechanical strength which is caused because of a physical structure failure causing crush injury to the user.