Safety Assessment of Human-Robot Collaborations Using Failure Mode and Effects Analysis and Bow-Tie Analysis

Abdelrhman Haggy, Abel K. Philip, Sneha Rose Priya Jacob, Juliane Schneider, Mohammed Marwan Anchukandan, Philipp Kranz[a] and Marian Daun[b]

Center for Robotics, Technical University of Applied Sciences Würzburg-Schweinfurt, Schweinfurt, Germany

Keywords: Human Robot Collaboration, Safety Analysis, Risk Analysis, Bow-Tie, Hazard Analysis, Failure Modes and Effects Analysis.

Abstract: Human-Robot collaboration is seen as chance to flexibilize modern production processes. The close interaction of humans and robots allows for fast semi-automation of process steps that cannot be fully automated or only at high cost. However, due to the close vicinity and complex interactions between human and robot establishing safety is challenging. Robotic safety is largely centered on machine safety and does not consider effects stemming from the runtime application. This paper investigates the use of failure mode and effects analysis and Bow-Tie Analysis for assessing the safety of human-robot collaborations. We applied the combined safety assessment approach to an industrial case example of a collaborative assembly process. Results show that safety analyses are applicable and particularly, the combination of top-down bow-tie and bottom-up failure mode and effects analysis is promising for the thorough assessment of dynamic human-robot collaboration applications.

1 INTRODUCTION

Human-robot collaboration (HRC) systems differ from conventional industrial robots in the type of interaction between humans and robots. Collaborative robots (i.e. cobots) can be designed to work in close vicinity to humans and share a common workspace. This involves a variety of potential hazards that need to be identified, analyzed and mitigated in a structured approach. However, currently safety assessment for robotic systems mostly relies on the assessment of the machine, not considering the dynamic interaction with the human (Berx et al., 2022).

In practice, safety and risk assessments for HRC systems are primarily based on ISO 12100, ISO 10218 and ISO 31000, which provide comprehensive guidelines for identifying, assessing and mitigating risks. In addition, safety standards of other domains often demand thorough safety assessment already at the conceptual state of development, but are not used in the robotics field. Corresponding methods such as Failure Mode and Effects Analysis (FMEA) and Fault Tree Analysis (FTA) are widely used and for safety and risk assessment (Cristea and Constantinescu, 2017). Other safety analysis methods, such as Hazard and Operability Analysis (HAZOP) and Hazard and Risk Assessment (HARA), have already been applied in the field of HRC. Although HAZOP may not fully address systemic flaws or human errors, while HARA evaluates risks but may not fully recognize associated failures.

In this paper, we investigate whether a combination of Bow-Tie Analysis and FMEA is useful to assess the safety of HRC systems, and can adequately consider the human component, as well as the interaction between human and robot. Thereby, Bow-Tie Analysis shall provide a comprehensive visualization of risk paths, while calculation of the RPN (risk priority number) from the FMEA enables a detailed bottom-up assessment of specific failure modes. The combination is employed in the context of a collaborative assembly application.

The paper is outlined as follows: Section 2 discusses the related work. Based on this, the approach is introduced to integrate FMEA and Bow-Tie Analysis for evaluating the safety of human-robot collaborations in Section 3. The approach is evaluated through its application to an industrial case study in Section 4. To this end, Section 5 concludes the paper.

[a] https://orcid.org/0000-0002-1057-4273
[b] https://orcid.org/0000-0002-9156-9731

Haggy, A., Philip, A., Jacob, S., Schneider, J., Anchukandan, M., Kranz, P. and Daun, M.
Safety Assessment of Human-Robot Collaborations Using Failure Mode and Effects Analysis and Bow-Tie Analysis.
DOI: 10.5220/0013017500003822

In *Proceedings of the 21st International Conference on Informatics in Control, Automation and Robotics (ICINCO 2024) - Volume 1*, pages 432-439
ISBN: 978-989-758-717-7; ISSN: 2184-2809

2 RELATED WORK

2.1 Safety and Risk Assessment

There are various standards that serve as guidelines for safety assessment and risk reduction.

ISO 12100 contains comprehensive guidelines for the risk assessment and risk reduction of machines and industrial robots (iso, 2010). The standard focuses on the identification of potential hazards, the assessment and evaluation of risks and the implementation of suitable risk reduction measures.

Another relevant standard is ISO 10218, which deals with the safety of industrial robots and robot systems (iso, 2011). It defines specific requirements for the design, integration and implementation of robotic systems to ensure safe operations in industrial environments. It also contains special guidelines for risk assessment in human-robot interaction.

ISO 31000 describes principles and guidelines for risk management in various industries (iso, 2018). Although the standard does not refer specifically to robotics, it provides guidance on identifying, assessing and mitigating risks in complex industrial processes. It also describes a comprehensive approach to risk management that is applicable to different organizational contexts.

2.2 Safety and Risk Assessment Methods

In industrial safety and risk assessment, various methods are used to ensure the safety and reliability of systems. These methods can be classified into two principal categories: bottom-up and top-down approaches. In contrast to the bottom-up approach, which initially identifies safety risks at the most granular level and subsequently aggregates these risks, the top-down method initiates the process at the system level and progressively breaks down the risks into more specific categories. The approaches can be used individually or in combination to analyze potential risks.

Probably the most frequently used bottom-up method is FMEA, which guarantees that potential faults within a system are found and the impact of those faults on the overall performance of the system is analyzed. FMEA improves the robustness of the system by highlighting important elements and procedures which need tighter control. (Liu et al., 2019).

Another well-known technique is Hazard and Operability Analysis (HAZOP). The method deals systematically with process deviations and their possible consequences for identifying and assessing potential hazards that exist within the industrial process. HAZOP makes sure all possible risks are accounted for and managed accordingly. (Reddy, 2015)

Aside from the bottom-up methods, there are also well-known methods such as Fault Tree Analysis (FTA), which follows a top-down approach to estimate the probability of certain failures in the system. It makes logical interconnections between the possible causes that might lead to system-wide failure and calculates their probability of occurrence, a structured way of understanding and mitigating risks. (Ruijters and Stoelinga, 2015).

One method that uses both bottom-up and top-down is the Bow-Tie Analysis, which brings together FTA and Event Tree Analysis in a flexible way. It represents a multimedia approach, where the routes from possible causes of a hazard to its potential consequences are diagrammed out through preventive and mitigative barriers. The technique identifies the cause-and-effect relationship, hence indicating the intervention points on which effective prevention or mitigation of risk can take place. (Tait and Edwards, 2021).

2.3 Safety and Risk Assessment in Human-Robot Collaboration

In their study, Lee and Yamada focus on the integration of FTA and FMEA for the design of safety functions in robots that collaborate with humans (Lee and Yamada, 2012). With their method, they determine the safety integrity level required for the system, perform risk assessments to identify potential failures, and show the design of safety functions that comply with the determined safety integrity level. This approach is illustrated by the case study of the skill assist system, an assistive device used in manufacturing and social settings. The proposed methodology is limited to the design of the safety function for system failures and cannot be directly applied to other safety functions that can prevent dangerous events caused by human factors.

Zacharaki et al. give an overview of safety boundaries in human-robot interaction. They focus on the aspects related to safe interactions between humans and robots (Zacharaki et al., 2020). The overview highlights various safety techniques, such as safety zones, real-time monitoring or dynamic safety boundaries. These methods help to prevent accidents in collaborative workspaces and strengthen trust between humans and collaborative robots. In their work, existing safety analysis techniques were examined and compared but not actively applied.

In their paper, Huck et al. mention that the risk assessment of industrial robots in practice is often based on experience, expert knowledge and checklists. However, with the growth of HRC, complexity increases, making risk assessment more difficult. Scientific developments offer new tools and methods to support these assessments, but these are rarely used in industry. Their paper analyzes the literature on innovative risk assessment approaches for HRC and evaluates interviews with experts to understand the needs of the industry. They discuss the challenges that need to be addressed to implement these new approaches in practice. Many of the approaches proposed in the literature are too complex and are difficult or impossible to transfer to individual use cases and lack proper validation (Huck et al., 2021).

A further field towards safety assessment of human-robot collaborations is the use of model-based techniques. In previous work, it has been shown that goal models adapted for the needs of collaborative systems (Daun et al., 2021), can be a good means to support safety assessment of human-robot collaborations (Daun et al., 2023). Particularly, a dedicated goal modeling profile (Manjunath et al., 2024) allows documenting safety hazards, mitigation strategies, and dependencies between these in early stages. However, this does not replace a structured safety assessment process.

3 APPROACH UNDER INVESTIGATION

In this paper, we investigate the use of Bow-Tie Analysis in combination with FMEA to support safety assessment of HRC. The goal behind this combination is to achieve a thorough risk assessment framework that encompasses both top-down, system-level hazard identification and bottom-up, component-level failure analysis.

3.1 Rationale for Integrating Bow-Tie Analysis and FMEA

Through the integration of Bow-Tie Analysis and FMEA two complementary approaches are combined. Bow-Tie Analysis is a top-down approach which visualizes the potential hazards and their respective consequences leading to a clear overview of the risk landscape. Overall, Bow-Tie helps in understanding the broad context of risks and is used for the identification of critical control measures. On the other hand, the FMEA with its RPN ranking provides the possibility of clearly presenting the level of risks. The integration of these two methods enables a comprehensive approach to safety analysis that incorporates the broad identification and visualization of risks through the Bow-Tie Analysis and the risk analysis using the RPN score from the FMEA. This hybrid method improves both the range and detail of risk assessment, leading to better safety management.

In the aerospace industry, for example, Bow-Tie Analysis first identifies a hazardous risk such as an in-flight engine failure. It examines possible causes such as bird strikes and considers potential consequences such as an emergency landing. FMEA is then utilized to focus on specific components of the engine to identify failure modes and suggest mitigation strategies, such as using more resilient materials. (Sharma and Srivastava, 2018)

3.2 Methodology

For the combination of Bow-Tie Analysis and FMEA, two artifacts are essential: The hazard evaluation template and the bow-tie diagram.

The hazard evaluation template is a structured template to address and evaluate each hazard. This template includes an introduction that provides an overview and context for the hazard within the system.

Bow-tie diagrams visually map the hazard and its associated risk factors. This involves identifying threats, escalation factors that could worsen the situation, and possible consequences if the hazard occurs. Additionally, preventive and mitigating controls currently in place are documented. The bow-tie diagram as can be seen in Figure 1 visually represents the relationships among the hazard, threats, controls, and consequences, enhancing understanding and communication of risk pathways and control measures. Note, that various different graphical representations of bow-tie diagrams have been proposed (cf. (de Ruijter and Guldenmund, 2016)). In this paper, we focus on the basic form of bow-tie diagrams to avoid increasing complexity on the diagram-level and to investigate the fitting of Bow-Tie Analysis to support safety assessment of HRC in general.

After completing the Bow-Tie Analysis, FMEA is applied for a detailed risk assessment. The Risk Priority Number (RPN) is obtained as combination of Severity, Occurence, and Undetectability (Afefy, 2015):

- Severity (S): The potential impact or seriousness of a failure on the system is evaluated. Higher severity means more significant consequences.
- Occurrence (O): This assesses how likely it is for a particular failure to happen. A higher occurrence

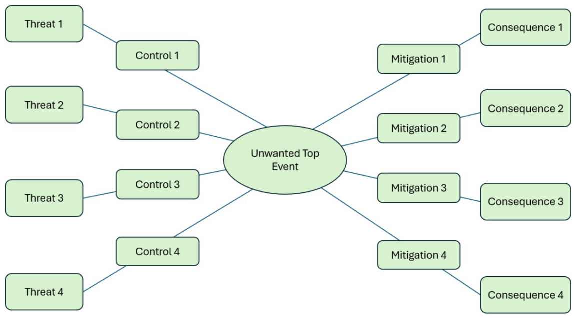

Figure 1: Bow-tie diagram for hazard analysis.

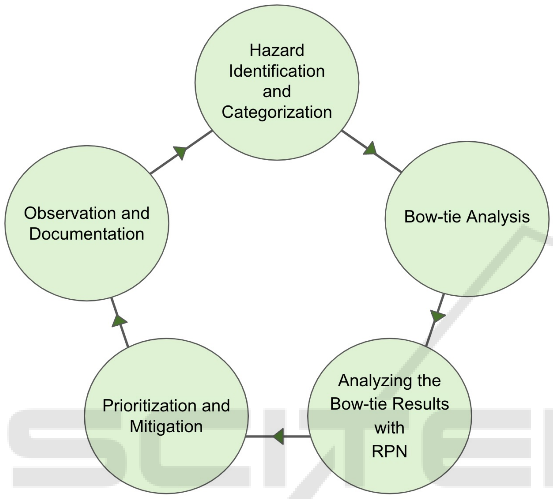

Figure 2: Safety assessment process.

rate indicates that the failure is more frequent.

- Detectability (D): This measure the ability to identify or detect a potential failure before it occurs. Lower detectability rating signifies a higher difficulty of detecting the failure in advance.[1]

3.3 Safety Assessment Process

The proposed safety assessment process consists of five steps, which are depicted in Figure 2. The following section provides a detailed explanation of each of the aforementioned steps.

- *Step 1: Hazard Identification and Categorization*
  The process starts with a thorough review of the operational workflow. To organize the efforts, a framework is employed that categorizes hazards into three main categories - Human-related, Cobot-related, and Collaborative workspace-related. These categories are adapted from (Berx et al., 2022), excluding the 'External' and 'Enterprise' categories as they are not the focus of this research. These chosen categories, informed by on-site observations, allow to systematically collect and address potential hazards.
- *Step 2: Bow-Tie Analysis*
  Once the hazards are identified, Bow-Tie Analysis is used to map the potential causes and their respective consequences arising from a central undesired event. A common hazard in HRC that could be identified as such an event is: "Trapping and Crushing between Robot and Fixed Structures." The elements of the Bow-Tie Analysis would then be the following:
  - Top Event: "Trapping and Crushing between Robot and Fixed Structures" which could considerably impact the safety of the workspace.
  - Threats and Consequences: Map out the primary threats leading to the top event, such as unexpected robot movements and failure of safety mechanisms. The consequences in this case are human injury and loss of trust in technology.
  - Control Measures and Mitigation: Documented existing preventive controls (measures to prevent threats from causing the top event) and mitigative controls (measures to reduce the impact if the top event occurs). For example, installing safety sensors and emergency stop buttons, implementing safety zones and barriers, and conducting regular safety audits and maintenance.
- *Step 3: Analyzing the Bow-tie Results with RPN*
  This step involves quantifying the risks associated with each identified threat by evaluating their Severity, Occurrence, and Undetectability. Using these ratings, the RPN for each threat is calculated. The RPN helps prioritize the identified hazards based on their potential impact on the assembly process.
- *Step 4: Prioritization and Mitigation*
  High-priority risks are addressed first by implementing additional control measures or improving existing ones. For example, to address the threat of 'Unexpected human entry into the robot's path,' more robust access control measures are implemented, such as 'Setting up safety zones using physical barriers' and 'Installation and regular testing of emergency stop switches'.

[1]Note that for Severity and Occurrence, the higher the probability, the higher the value; conversely, for Detectability, the higher the probability, the lower the value. In this work, therefore, the term Undetectability (the probability of the failure being undetected before it causes harm) is used instead of Detectability to avoid confusion and hence maintain a consistent order in the evaluation.

- *Step 5: Observation and Documentation*
  All findings from Bow-Tie Analysis and FMEA are documented in comprehensive templates, detailing the threats, consequences, control measures, and RPN calculations.

4 EVALUATION

4.1 Case Study

As case study for evaluating the applicability of the approach, a collaborative toy truck assembly was chosen. The system has a virtual separation of workspaces, dividing the area into distinct zones for human operators, collaborative tasks, and robotic operations. Step-by-step assembly instructions are projected onto the human workspace to provide real-time guidance.

A control interface starts the assembly process, tracks the completion of each step, and moves on to the next. The system also ensures precise component placement during each assembly step. Additionally, quality control is maintained through an overhead camera system that continuously monitors the assembly process.

The assembly procedure begins with the human operator initiating the process by pressing a start button. In the component placement phase (Coexistence Mode), the robot places the truck parts load carrier, cabin, and chassis in an assembly bracket while the human operator simultaneously prepares the axle holders. During the collaborative assembly phase (Collaboration Mode), the robot assists by positioning each axle on the base of the truck and holding it in place. Finally, once the truck is fully assembled, it is removed from the collaborative workspace and placed in a designated area for completed assemblies.

4.2 Results

In this section, examples from the application results are shown. This section is structured according to the identified three main categories of safety hazards for human robot collaboration: 'Human', 'Robot', and 'Collaborative Workspace'.

4.2.1 Human-Related Hazards

Examples of Identified Hazards:

- Hazard 1: Human Error - Human error can lead to mistakes in decision-making and task execution.
- Hazard 2: Inadequate Communication - Inadequate communication can cause misunderstandings and misinterpretations.
- Hazard 3: Non-Compliance with Safety Procedures - Non-compliance with safety procedures can increase the risk of accidents and injuries.

Bow-Tie Analysis for Human-Related Hazards: In this example, the hazard of '*Human error*' is analyzed. The Bow-tie diagram in figure 3 shows the key hazard and the main contributing factors and their respective controls. On the left side of the diagram, various causes of human error are identified, each paired with appropriate control measures to minimize their occurrence. These include inadequate training, high stress levels, fatigue, and poor communication, which are controlled through comprehensive training programs, stress management initiatives, shift rotations and breaks, and clear communication protocols, respectively. On the right side of the diagram, the potential consequences of human error are detailed along with their mitigations. These consequences, such as increased risk of accidents, decreased productivity, higher error rates, and decreased employee morale, are addressed through regular safety drills, monitoring and feedback systems, error-proofing measures, and a supportive work environment.
Identified causes and controls:

- Cause 1: Inadequate Training - controlled by Comprehensive Training Programs
- Cause 2: High stress levels - controlled by Stress Management Programs
- Cause 3: Fatigue - controlled by Shift Rotations and Breaks
- Cause 4: Poor communication - controlled by Clear Communication Protocols

Identified consequences and mitigations:

- Consequence 1: Increased Risk of Accidents - mitigated by Regular Safety Drills
- Consequence 2: Decreased Productivity - mitigated by Monitoring and Feedback Systems
- Consequence 3: Higher Error Rates - mitigated by Error-Proofing Measures
- Consequence 4: Decreased Employee Morale - mitigated by supportive Work Environment

4.2.2 Robot-Related Hazards

Examples of Identified Hazards:

- Hazard 1: Mechanical Failure - Breakdowns or malfunctions of robotic components, such as motors or actuators, which can lead to unintended movements or complete stoppages.

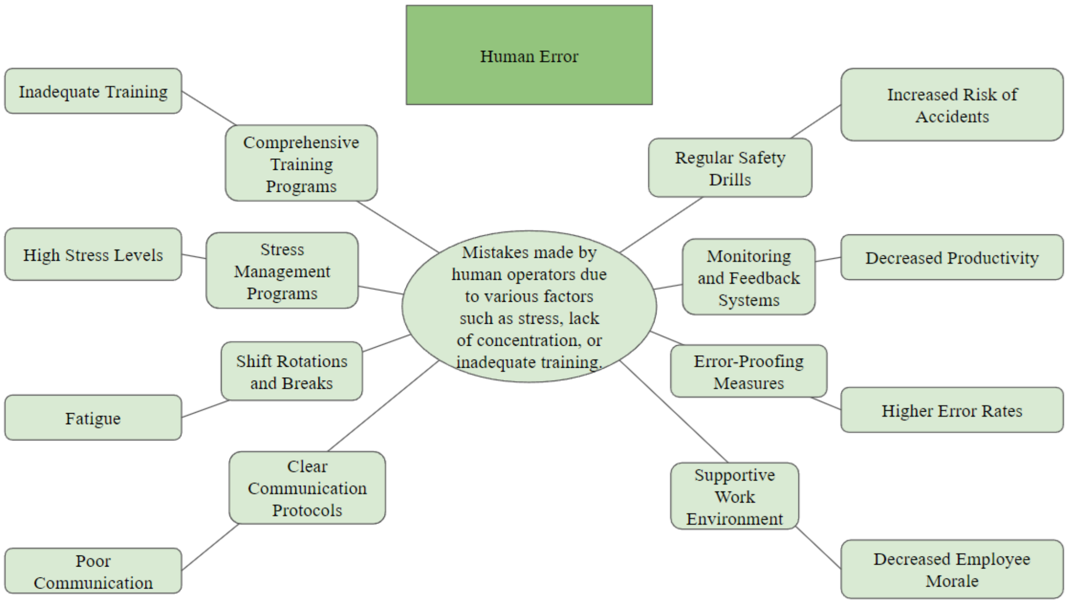

Figure 3: Bow-tie diagram for human-related hazard.

- Hazard 2: Software Bugs - Errors in the robot's software that could cause the robot to perform unintended actions, potentially leading to unsafe situations.
- Hazard 3: Inadequate Maintenance - Lack of regular maintenance and inspections, which can result in deteriorating performance and increased likelihood of failures or malfunctions.

Bow-Tie Analysis for Robot-Related Hazards: In this example, the focus is on mechanical failure. The diagram in figure 4 highlights the various causes, such as wear and tear, lack of maintenance, overloading, and manufacturing defects, and the corresponding controls like condition monitoring systems, regular maintenance schedules, load sensors, and quality control in manufacturing. The consequences of mechanical failure include unintended robot movements, interruption of the work process, damage to workpieces, and injury to personnel. These are mitigated by emergency stop mechanisms, redundant systems, safety barriers, and operator training.
Identified causes and controls:

- Cause 1: Wear and Tear - controlled by Condition Monitoring Systems
- Cause 2: Lack of Maintenance - controlled by Regular Maintenance Schedules
- Cause 3: Overloading - controlled by Load Sensors
- Cause 4: Manufacturing Defects - controlled by Quality Control in Manufacturing

Identified consequences and mitigations:

- Consequence 1: Unintended Robot Movements - mitigated by Emergency Stop Mechanisms
- Consequence 2: Interruption of the work process - mitigated by Redundant Systems
- Consequence 3: Damage to Workpieces - mitigated by Safety Barriers
- Consequence 4: Injury to Personnel - mitigated by Operator Training

4.2.3 Collaborative Workspace Hazards

Examples of Identified Hazards:

- Hazard 1: Sudden stops in movement - Unexpected halts in the robot's motion can lead to collisions or injuries.
- Hazard 2: Unpredictable movements - Robots performing unplanned actions can create hazardous situations for nearby workers.
- Hazard 3: Trapping and crushing between robot and fixed structures - Limited space can lead to workers getting trapped or crushed between the robot and fixed structures, causing severe injuries.

To better understand and manage these hazards, a Bow-Tie Analysis was conducted for each category. This method provides a visual representation of the pathways from causes to a central hazard and then to consequences, along with associated controls and mitigations.

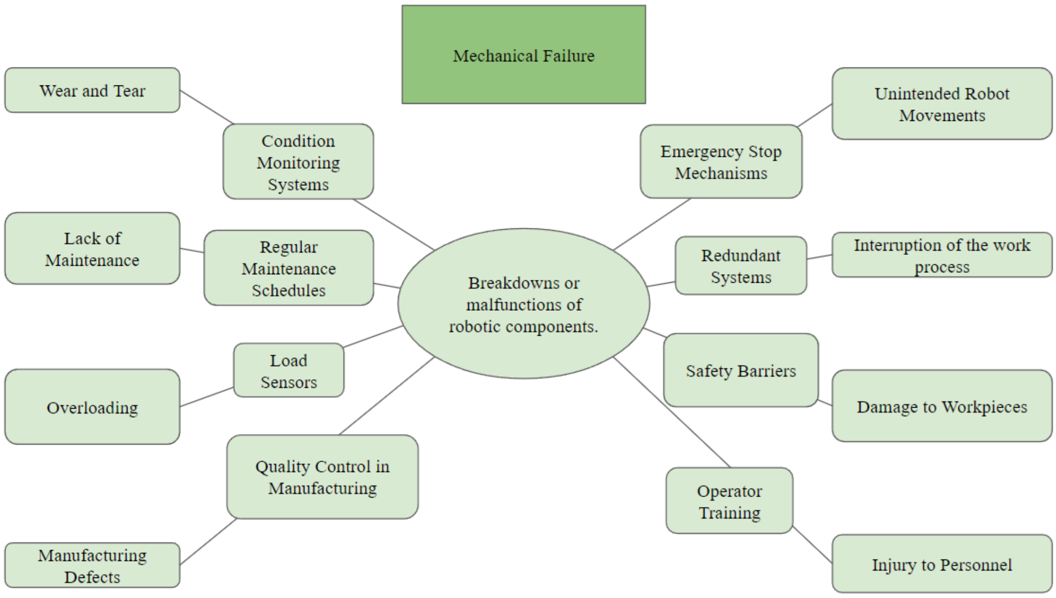

Figure 4: Bow-tie diagram for robot-related hazard.

Bow-Tie Analysis for Collaborative Workspace Hazards: In this example, the hazard of 'Trapping and Crushing' is examined. The Bow-tie in figure 5 shows the causes including unexpected robot movements, missing or incorrect safety zones, unexpected human entry into the safety zone, and failure of safety mechanisms. Controls such as regular maintenance and calibration, setting up and checking safety zones, employee training, and installation and testing of safety mechanisms are identified. Consequences of trapping and crushing include blood loss, interruption of the work process, loss of trust in workplace safety, and legal and financial consequences. These are mitigated through first aid and medical care, repair and maintenance, communication and safety analysis, and accident investigation.
Identified causes and controls:

- Cause 1: Unexpected robot movements - controlled by Regular maintenance and calibration
- Cause 2: Missing or incorrect safety zones - controlled by Setting up and regularly checking safety zones
- Cause 3: Unexpected human entry into the safety zone - controlled by Employee training
- Cause 4: Failure of safety mechanisms - controlled by Installation and regular testing of Safety mechanisms

Identified consequences and mitigations:

- Consequence 1: Blood loss: Potentially more serious if larger blood vessels are affected - mitigated by First aid kit, First responder, Medical care
- Consequence 2: Interruption of the work process - mitigated by Repair and maintenance
- Consequence 3: Loss of trust: loss of employee trust in the safety of the workplace - mitigated by Communication, Statement, Safety analysis
- Consequence 4: Legal and financial consequences - mitigated by Accident investigation

5 CONCLUSION

For human-robot collaborations safety is a vital concern. Due to the close proximity of operation and the overlapping working spaces, multiple safety hazards arise. Therefore, thorough safety assessment is inevitable. However, in literature only few approaches for safety assessment of human-robot collaborations do exist. In addition, reports of application of traditional safety analysis are also only published sparsely. Therefore, in this paper, we report on the application of a combination of FMEA and Bow-Tie analysis for early safety assessment of human-robot collaborations using an industrial case example from the manufacturing domain.

Our study shows that the integration of the Bow-Tie Analysis with the RPN calculation from FMEA provides a detailed safety and risk assessment in HRC environments. By combining the top-down visualization and detail of the Bow-Tie Analysis with bottom-

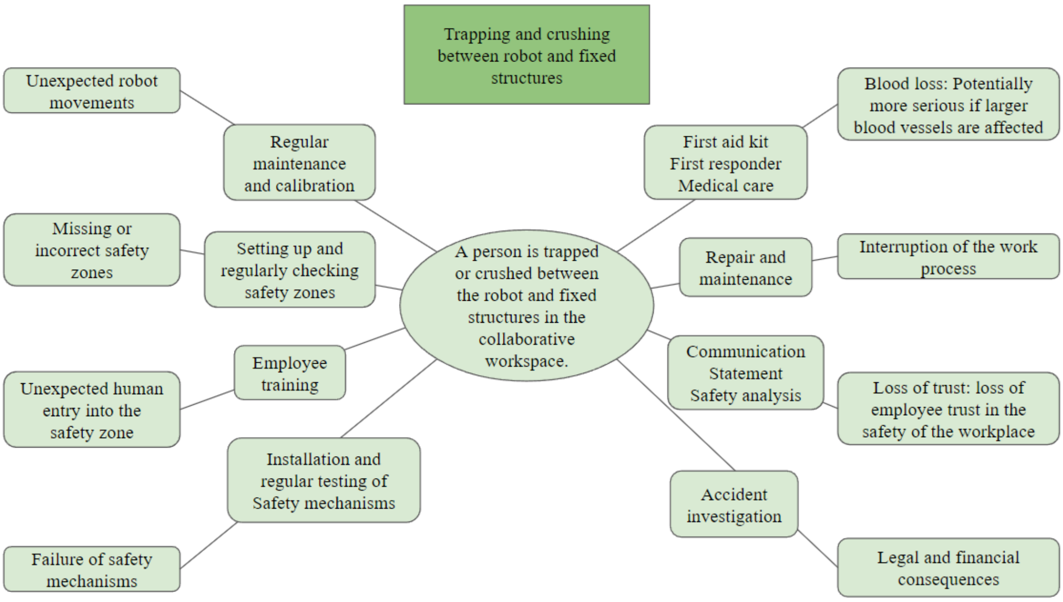

Figure 5: Bow-tie diagram for collaborative workspace hazard.

up classification of the risk level by the RPN calculation, it is possible to systematically identify, analyze and address potential hazards in a collaborative assembly process.

REFERENCES

(2010). *ISO 12100: Safety of machinery — General principles for design — Risk assessment and risk reduction*. International Organization for Standardization.

(2011). *ISO 10218-1: Robots and robotic devices — Safety requirements for industrial robots — Part 1: Robots*. International Organization for Standardization.

(2018). *ISO 31000: Risk management — Guidelines*. International Organization for Standardization.

Afefy, I. H. (2015). Hazard analysis and risk assessments for industrial processes using fmea and bow-tie methodologies. *Industrial Engineering and Management Systems*, 14(4):379–391.

Berx, N., Decré, W., Morag, I., Chemweno, P., and Pintelon, L. (2022). Identification and classification of risk factors for human-robot collaboration from a system-wide perspective. *Computers & Industrial Engineering*, 163:107827.

Cristea, G. and Constantinescu, D. (2017). A comparative critical study between fmea and fta risk analysis methods. *IOP Conference Series: Materials Science and Engineering*, 252(1):012046.

Daun, M., Brings, J., Krajinski, L., Stenkova, V., and Bandyszak, T. (2021). A grl-compliant istar extension for collaborative cyber-physical systems. *Requirements Engineering*, 26(3):325–370.

Daun, M., Manjunath, M., and Jesus Raja, J. (2023). Safety analysis of human robot collaborations with grl goal models. In *International Conference on Conceptual Modeling*, pages 317–333. Springer.

de Ruijter, A. and Guldenmund, F. (2016). The bowtie method: A review. *Safety science*, 88:211–218.

Huck, T. P., Münch, N., Hornung, L., Ledermann, C., and Wurll, C. (2021). Risk assessment tools for industrial human-robot collaboration: Novel approaches and practical needs. *Safety Science*, 141:105288.

Lee, S. and Yamada, Y. (2012). Risk assessment and functional safety analysis to design safety function of a human-cooperative robot. In *Human Machine Interaction-Getting Closer*. Citeseer.

Liu, P., Liu, S., and Xie, M. (2019). Failure mode and effects analysis for proactive healthcare risk management: A systematic literature review. *Quality and Reliability Engineering International*, 35(5):1279–1291.

Manjunath, M., Raja, J. J., and Daun, M. (2024). Early model-based safety analysis for collaborative robotic systems. *IEEE Transactions on Automation Science and Engineering*.

Reddy, K. (2015). *Hazard identification and risk assessment*. CBS Publishers & Distributors Pvt Ltd.

Ruijters, E. and Stoelinga, M. (2015). Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools. *Computer Science Review*, 15:29–62.

Sharma, K. D. and Srivastava, S. (2018). Failure mode and effect analysis (fmea) implementation: a literature review. *J Adv Res Aeronaut Space Sci*, 5(1-2):1–17.

Tait, R. and Edwards, D. (2021). Bow-tie analysis: A modern method for risk assessment. *Journal of Safety Research*.

Zacharaki, A., Kostavelis, I., Gasteratos, A., and Dokas, I. (2020). Safety bounds in human robot interaction: A survey. *Safety science*, 127:104667.