Decoding Risk Management: The Crucial Means-End Aspect of Countermeasures and Hazards

Wu, Jing; Ren, Junru; Li, Ruixue; Zhang, Xinxin; Lind, Morten

Published in:
Proceedings of International Workshop on Functional Modeling and Safety Related Issues of Socio-Technical Systems

Publication date:
2024

Document Version
Peer reviewed version

Citation (APA):
Wu, J., Ren, J., Li, R., Zhang, X., & Lind, M. (2024). Decoding Risk Management: The Crucial Means-End Aspect of Countermeasures and Hazards. In *Proceedings of International Workshop on Functional Modeling and Safety Related Issues of Socio-Technical Systems* (pp. 13-16)

Decoding Risk Management: The Crucial Means-End Aspect of Countermeasures and Hazards

WU Jing[1)], REN Junru [1)], LI Ruixue[1)], ZHANG Xinxin[1)], LIND Morten[1)]

1) Department of Electrical and Photonics Engineering, Technical University of Denmark, Kgs. Lyngby, 2800, Denmark (jinwu; junre; ruilia; xinz; lind@dtu.dk)

Abstract— **This paper explores the relationship between countermeasures and hazards in contemporary risk management frameworks. The fundamental premise posits hazards as undesirable ends, with countermeasures serving as the means to prevent or mitigate adverse situations. Focusing on foundational principles within socio-technical systems, the paper explores the aggregation and decomposition of countermeasure-hazard relations in a means-end manner. Action theories, grounded in this dimension, offer significant potential for informed decision-making in design, operation, and maintenance tasks. Through a case study on the function-centered hazard identification approach (F-CHIA), the paper illustrates practical applications in robotics safety, deriving risk mitigation strategies within design specifications. Ultimately, it underscores the critical role of the means-end dimension in effective risk mitigation strategies, contributing to advancements in risk management.**

Keywords—functional model; risk management; countermeasures-hazards; means-end; socio-technical system

I. INTRODUCTION

The risk management framework serves as a guiding structure for mitigating risks to the As Low As Reasonably Practicable (ALARP) level, where countermeasures play a pivotal role. Countermeasures, defined as actions taken to counteract hazards, have become integral components of risk management. Extensive research over the years has focused on identifying and ensuring the effect of these countermeasures and their associated controls.

Among the recognized methodologies, the Bow Tie Model [1] stands out for its effectiveness in identifying barriers and understanding the factors influencing their performance across various industries. However, a pertinent question arises: Is the Bow Tie Model comprehensive and systematic enough? While designed to illustrate all barriers and degradation controls for effective barrier management, risk reduction analysis, and assessment of existing barriers, the method's reliance on event-based analysis poses limitations [2]. These limitations necessitate a fundamental perspective shift to address consistency and systematics in identifying barriers and degradation controls.

This paper explores the relationship between countermeasures and hazards within the context of risk management, framing it as a nuanced means-end connection. The core premise is that hazards represent undesirable ends, while countermeasures are means to mitigate or prevent adverse situations. To address this, the paper confronts three primary challenges: 1) the systematic identification of hazards, 2) the aggregation and decomposition of countermeasure-hazard relations in a means-end manner, and 3) the representation of these relations within a functional modeling framework.

The paper's primary focus is on exploring fundamental principles that address the second challenge within the realm of socio-technical systems. Central to these principles are the concepts of means-end and action theories, which play crucial roles in understanding and optimizing the relationship between countermeasures and hazards. While the paper predominantly delves into the means-end dimension of countermeasures-hazards relations, it is important to note that preliminary research[3], [4] by our group has also made acheivements in addressing the first and third challenges.

II. THEORY AND APPROACH

A. Understanding of risk management by concepts of means-end and action theories

The sustainability development of socio-technical systems introduces a broader range of hazards, reflecting the diverse interests of stakeholders. Traditional risk management frameworks often struggle to capture the dynamic and interconnected nature of these systems. To address this complexity, the means-end concept offers valuable insights into the development of countermeasures and hazard relations.

The Swiss Cheese Model[5] is a widely used framework for safety and risk analysis, illustrating levels of defense against failure as slices of Swiss cheese. While it emphasizes the importance of multiple defense layers, it falls short in explaining why the holes align. In practical applications, we need a deeper understanding of the intrinsic relations between the holes to develop more effective risk management strategies shown in Fig. 1.

In the Defense in Depth strategy, defense levels can be categorized into prevention, control, protection, and mitigation of event consequences. Actions counteracting hazards play a pivotal role in this strategy. Action theory[6] introduces four phases that an action must undergo for successful completion, with roles such as Agent and Object ensuring a means-end relation. Expanding role types[7] based on the Greimas Actant Scheme helps locate the root causes of action failures, addressing a deficiency in the Swiss Cheese Model.

Examining actions across the life cycle, from design to operation, enhances understanding. Each phase of action corresponds to one of the four holes in the Swiss Cheese Model. Failure at any phase implies the countermeasure's ineffectiveness, leading to a breakdown in hazard prevention.

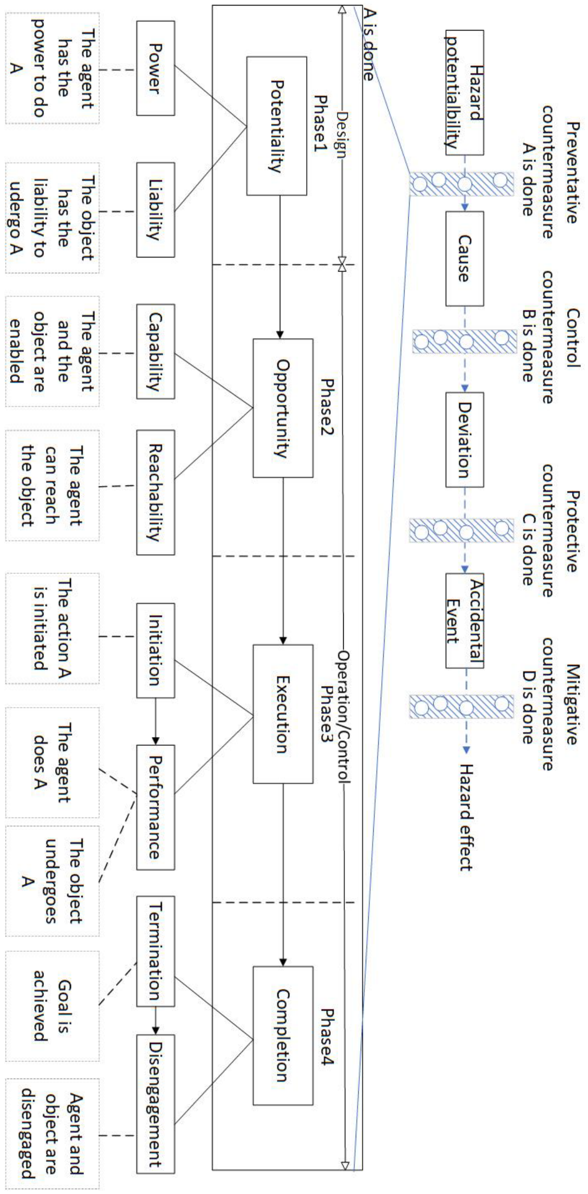


Fig.1 Understanding of risk management by concepts of means-end and action theories.

B. *Casual analysis: "To Realize" vs "To Bring About" in Countermeasure Failure*

It is, furthermore, distinguishing between the effects of "to realize" (resulting in some transformation) and "to bring about" (inducing a situation by intentionally causing something else to happen) in actions instrumental for pinpointing direct and indirect causes of countermeasure failure. Fig.2 illustrates the conceptual relations among functions, doings, means, and ends associated with "realize" and "bring about".

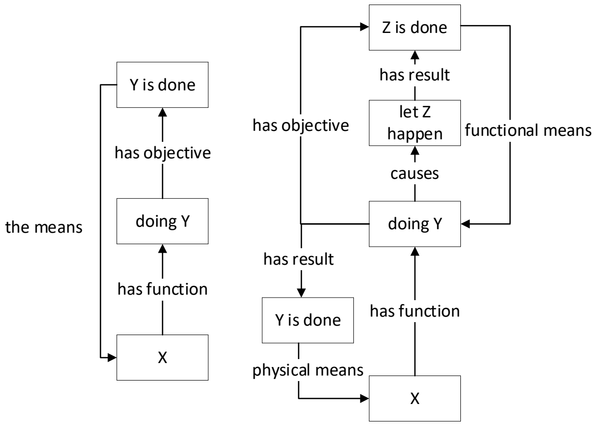


Fig.2 X's Transformation Realizing Y vs. Doing Y to Bring About Z (adapted from Lind [5]).

Consider the example of a trainer, denoted as X, whose function is to "do y," where y represents conducting training. The objective is the completion of training, and the trainer serves as a means to achieve this goal. Furthermore, training itself can be a means for another objective: ensuring safe operation. If safe operation is not guaranteed, the indirect cause can be traced to a trainer, with the direct cause attributed to ineffective training.

Identifying the root cause, which is the factor influencing the trainer, becomes crucial. This nuanced analysis significantly contributes to a more comprehensive understanding of the causal factors contributing to countermeasure failure within socio-technical systems.

III. CASE STUDY

The safety of robotics and automation technologies is a significant concern for the stakeholders. Prior research[8] introduced the function-centered hazard identification approach (F-CHIA) to systematically formulate functional requirements specifications and identify standards. This approach has been expanded to include considerations for both process and product in robotic system applications. Using the autonomous pick-place module shown in Fig.3 as a case study, we illustrated how to propose functional requirements from a safety perspective.


(a) Human involved meat pick and place process
(b) Autonomous meat pick and place experimental setup

Fig.3 The illustration of the pick and place task in a slaughterhouse. (a) is the case when humans are involved in the task in the traditional process. (b) is the robotic algorithm testing hardware in the lab at DTU[9].

The studied application involves the deployment of a robotic manipulator to take over the role of a human worker engaged in the picking and placing of meat cuts.

The envisioned task includes the robot picking variously shaped meat cuts from a conveyor belt and placing them onto a nearby "Christmas tree". This process encompasses four distinct subtasks: tracking, grasping, lifting, and hanging. The paper used the action theory for analyzing the hierarchical means-end model of the original robotic applications without the new proposed safety functions. Now we are going to examine the risk mitigation strategies in design specifications based on the proposed safety functions by applying the means-end and action theory.

For all the tasks in the robotics application examined by F-CHIA, the hazard can be the manipulator. The cause of the hazard can be that the human operator's working area overlapped with the robot manipulator's, which may lead to human injury due to an impact. The accident scenario is shown in Table 1.

Table 1 The accident scenario: human injury due to the impact of the manipulator

Hazard	Cause	Deviation
The manipulator	The human operator's working area overlapped with the robot manipulator's	The human operator is reachable by the manipulator

After examining the accident scenario by using the F-CHIA, three countermeasures for avoiding human injury due to the manipulator's impact were proposed: action A-tracking positions of human and manipulator, action B-set limit on manipulator's working space, and action C-implement emergency stop function. The pre-conditions for each action phase for the success of all the actions completion are analyzed in the Appendix. The arrows connecting the action phase boxes indicate the means-end conditions for avoiding human injury due to the manipulator's impact. If any pre-condition for the completion of one countermeasure fails, the hazard may propagate through the arrows leading to the accident effects. The layer of countermeasures can reduce the risk of accident effects.

IV. CONCLUSIONS

Building on the foundation of hazard identification, the paper focuses on the intricate relations between countermeasures and hazards. Effective risk management demands not only the identification of individual countermeasures but also an understanding of their interplay with specific hazards. To address this, the paper introduces a novel means-end analysis framework. This framework seeks to aggregate and decompose countermeasure-hazard relations, providing a structured and actionable understanding of how countermeasures function in response to identified hazards. Means-end analysis allows for a deeper understanding of the causal relationships between countermeasures and hazards, and action theories provide a framework for implementing and optimizing these relationships. The paper demonstrates the framework in robotics safety, deriving risk mitigation strategies within design specifications.

ACKNOWLEDGEMENT

The authors would like to thank DTU Offshore for supporting the presented research results.

REFERENCES

[1] CCPS, Energy Institute, Bow ties in risk management: A concept book for process safety. wiley, 2018.

[2] J. Wu, X., Zhang, M. Song, and M. Lind, Challenges in Functional Modelling for Safety and Risk Analysis. In P. Brito M, Aven T, Baraldi P, Čepin M, Zio E, editors, Proceedings of the 33rd European Safety and Reliability Conference, Research Publishing Services, Southampton, United Kingdom, pp. 1892-1899, 2023.

[3] R. Li, J. Wu, X. Zhang, and O. Ravn, Process Hazard Analysis: Proposing a Structured Procedure based on Multilevel Flow Modelling. in M P. Brito, T Aven, P Baraldi, M Čepin & E Zio (eds), Proceedings of the 33rd European Safety and Reliability Conference. Research Publishing Services, Southampton, United Kingdom, pp. 2031-2038, 2023.

[4] R. Li, J. Wu, X. Zhang, and O. Ravn, Integrating Hazard-oriented Knowledge Representation for Multilevel Flow Modelling in Process Hazard Identification. IFAC-PapersOnLine, 56(2), pp.7208–7215.

[5] J. Reason, Human Error. Cambridge University Press, 1990.

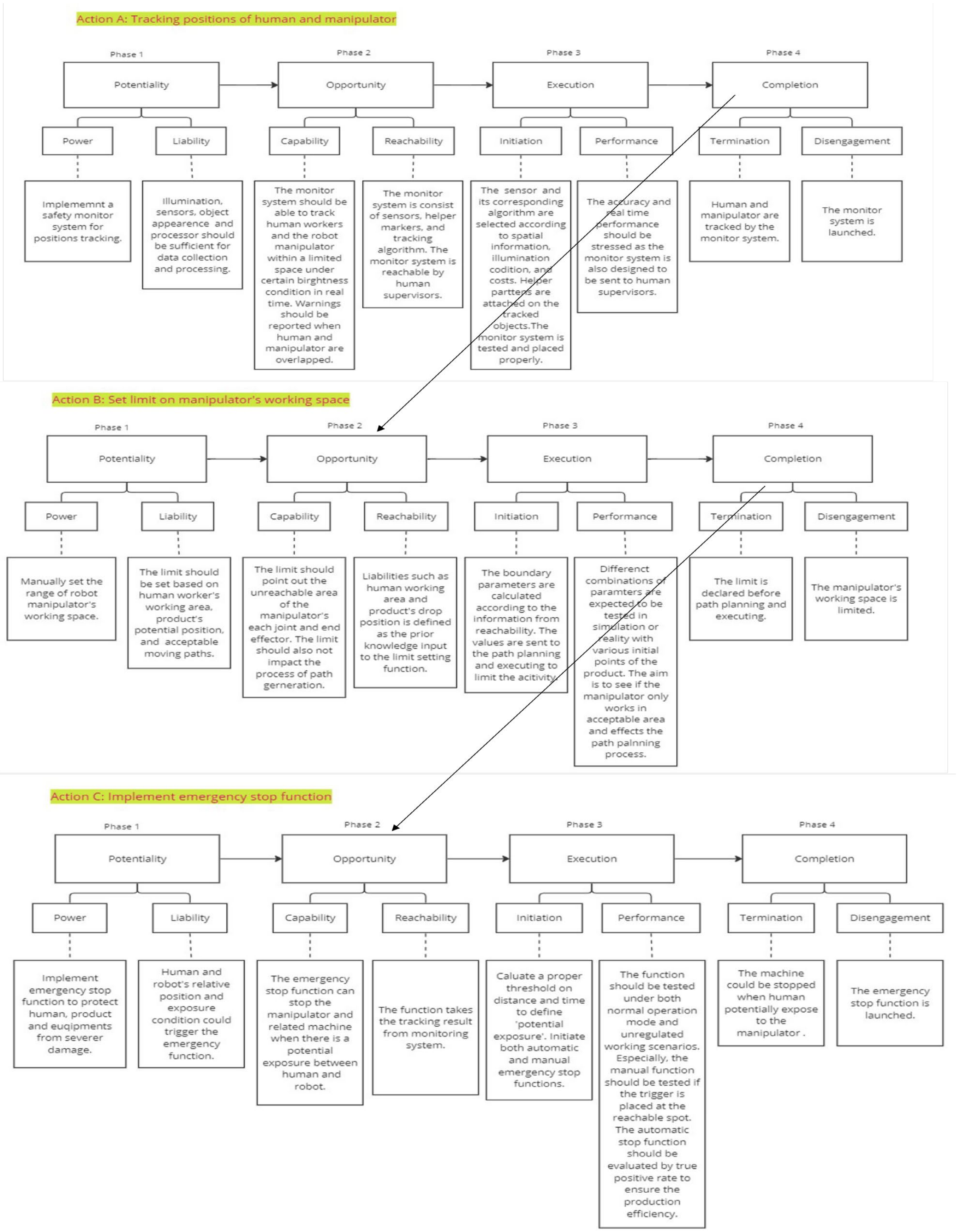
[6] M. Lind, Foundations for Functional Modeling of Technical Artefacts, M. Lind, Ed., Cham: Springer International Publishing, 2024, pp. 233–245.

[7] J. Wu, M. Lind, and I. Santos, Extending Multilevel Flow Modeling with Roles for Condition Monitoring and Preventive Maintenance, in 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Vienna, Austria, pp. 1385–1388, 2020.

[8] J. Ren, J. Wu, O. Ravn, and L. Nalpantidis, Functional requirements elicitation approach for the design and integration of robotic system for automation, in 2023 5th International Conference on System Reliability and Safety Engineering (SRSE), Beijing, China, pp. 214–219, 2023.

[9] H. Wu, T. T. Andersen, N. A. Andersen, and O. Ravn, Visual Servoing for Object Manipulation: A Case Study in Slaughterhouse, 14th International Conference on Control, Automation, Robotics and Vision (ICARCV), Phuket,Thailand,2016.

APPENDIX. MEANS-END ASPECT OF COUNTERMEASURES-HAZARDS FOR AVOIDING HUMAN INJURY DUE TO THE MANIPULATOR'S IMPACT.



Action A: Tracking positions of human and manipulator

Power: Implememnt a safety monitor system for positions tracking.

Liability: Illumination, sensors, object appearence and processor should be sufficient for data collection and processing.

Capability: The monitor system should be able to track human workers and the robot manipulator within a limited space under certain birghtness condition in real time. Warnings should be reported when human and manipulator are overlapped.

Reachability: The monitor system is consist of sensors, helper markers, and tracking algorithm. The monitor system is reachable by human supervisors.

Initiation: The sensor and its corresponding algorithm are selected according to spatial information, illumination codition, and costs. Helper partterns are attached on the tracked objects.The monitor system is tested and placed properly.

Performance: The accuracy and real time performance should be stressed as the monitor system is also designed to be sent to human supervisors.

Termination: Human and manipulator are tracked by the monitor system.

Disengagement: The monitor system is launched.

Action B: Set limit on manipulator's working space

Power: Manually set the range of robot manipulator's working space.

Liability: The limit should be set based on human worker's working area, product's potential position, and acceptable moving paths.

Capability: The limit should point out the unreachable area of the manipulator's each joint and end effector. The limit should also not impact the process of path gerneration.

Reachability: Liabilities such as human working area and product's drop position is defined as the prior knowledge input to the limit setting function.

Initiation: The boundary parameters are calculated according to the information from reachability. The values are sent to the path planning and executing to limit the acitivity.

Performance: Differenct combinations of paramters are expected to be tested in simulation or reality with various initial points of the product. The aim is to see if the manipulator only works in acceptable area and effects the path palnning process.

Termination: The limit is declared before path planning and executing.

Disengagement: The manipulator's working space is limited.

Action C: Implement emergency stop function

Power: Implement emergency stop function to protect human, product and euqipments from severer damage.

Liability: Human and robot's relative position and exposure condition could trigger the emergency function.

Capability: The emergency stop function can stop the manipulator and related machine when there is a potential exposure between human and robot.

Reachability: The function takes the tracking result from monitoring system.

Initiation: Caluate a proper threshold on distance and time to define 'potential exposure'. Initiate both automatic and manual emergency stop functions.

Performance: The function should be tested under both normal operation mode and unregulated working scenarios. Especially, the manual function should be tested if the trigger is placed at the reachable spot. The automatic stop function should be evaluated by true positive rate to ensure the production efficiency.

Termination: The machine could be stopped when human potentially expose to the manipulator .

Disengagement: The emergency stop function is launched.