

**Development of a Framework for Ethical and Cyber-Safe Robotics
in the Service Industry**

by

EMMANUEL IFIE MORDI

submitted in accordance with the requirements for
the degree of

MASTER OF SCIENCE IN COMPUTING EDUCATION

in the subject of Mathematics, Science and Technology Education

&

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: Prof. Patricia Gouws

CO-SUPERVISOR: Prof. Jeanne Kriek

February 2026

DECLARATION

Name: **Emmanuel Ifie Mordi** _____

Student number: **63277077** _____

Degree: **MSc Computing Education** _____

I declare that: (Exact wording of the title of the dissertation as appearing on the electronic copy submitted for examination)

Development of a Framework for Ethical and Cyber-Safe Robotics in the Service Industry

I declare that the dissertation is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references, and that any use of Artificial Intelligence (AI) has been fully disclosed.

I further declare that I submitted the dissertation to the appropriate originality detection system which is endorsed by Unisa and that it falls within the accepted requirements for originality.

I further declare that I have not previously submitted this work, or part of it, for examination at Unisa for another qualification or at any other higher education institution.

I further declare that where Artificial Intelligence (AI) tools have been used in the preparation of this thesis/dissertation, their use has been limited to ethical permissible support, has been fully disclosed, and does not replace my own original research, my independent critical thinking and analysis, or authorship responsibilities.

I understand that failure to disclose AI use, plagiarism and/or lack of academic integrity may constitute academic misconduct under Unisa's policies.

(The dissertation will not be examined unless this statement has been included.)



SIGNATURE

_____**27/02/2026**_____

DATE

ACKNOWLEDGEMENTS

My sincere thanks to God Almighty for His provision and the remarkable finisher's grace in completing this work. I would like to thank my supervisor, Professor Patricia Gouws, and my co-supervisor, Professor Jeanne Kriek, for their steadfast support, assistance, and encouragement throughout the preparation of this dissertation. To my wife, for her unwavering love, moral and emotional support, I am indeed grateful!

Abstract

The increased use of service robotics in sectors like hospitality, healthcare, and logistics presents opportunities but also challenges in cyber-safety, ethics, and human-robot interaction (HRI). While progress has been made, current frameworks are fragmented or focus too much on technical efficiency, neglecting ethics, social issues, and data protection. This is especially true in emerging economies where imported robots often conflict with local cultural and regulatory standards.

This study introduces a comprehensive conceptual framework called the Socio-Tactical Integrated Framework to guide ethical, cyber-safe, and contextually suitable deployment of service robotics (ACERBOTICS). A Design Science Research approach was used to develop a structured theoretical model that addresses gaps in the current research. The study includes a systematic literature review, which provides a basis for identifying and understanding existing critical gaps in the literature and design criteria for a proposed research artefact to address the gaps. Following the development of the research artefact, an expert evaluation was conducted using a questionnaire with both closed and open-ended questions to assess the relevance, clarity, applicability, and ethical robustness of the proposed framework.

Expert evaluation ($n = 47$) demonstrated high coherence, ethical robustness, and practical feasibility, while also identifying areas of improvement, including contextual adaptability and operational scalability. These insights informed the development of a refined framework that integrates ethical governance, cyber-safety resilience, socio-technical alignment, and human-centred design principles.

This study proposes a unified, theoretically grounded, and practically applicable framework for governing autonomous service robotics in diverse socio-technical environments. The proposed framework provides a basis for future empirical validation and policy development, particularly in African and other emerging-economy contexts. By integrating cyber-safety, ethics, and service robotics, this research advances scholarly understanding and promotes responsible innovation in the field of intelligent robotic systems in the service industry.

Keywords: ACERBOTICS Framework; Cyber-Safety Resilience; Ethically Aligned Design (EAD); Ethical Governance; Ethical Robotics; Human Robot Interaction (HRI); Integrated Framework; Robotics Service Industry (RSI); Socio-Technical Integration; Socio-Tactical; System Resilience; Value-Sensitive Design (VSD).

Acronyms, Abbreviations, and Symbols

- AI – Artificial intelligence
- AMR – Autonomous Mobile Robot
- EAD – Ethically Aligned Design
- HRI - Human–Robot Interaction
- IoT – Internet of Things
- ML – Machine Learning
- RSI – Robotic Service Industry
- SLR – Systematic Literature Review
- STS- Socio-Technical Systems
- VSD – Value Sensitive Design
- XAI - Explainable AI

Definitions of terminology

- **Artificial Intelligence (AI):**

This refers to the “automation of cognition,” which involves designing computational systems that mimic cognitive functions such as reasoning, knowledge representation, learning, adaptation, and metacognition. These systems can also act as “social and cognitive phenomena”, allowing machines to integrate into societies, communicate via high-level information transfer, and carry out competitive tasks that demand cognitive skills (Abbass, 2021). Technologies enabling machines to sense, learn, and act, including machine learning, natural language processing, robotics, and deep learning. (Bowen & Morosan, 2018; Jung et al., 2023; Madhan et al., 2024).

- **Autonomous Mobile Robot (AMR):**

A type of robot, utilised in hospital logistics, that operates autonomously to navigate and transport items such as food and medical supplies. These robots are integrated with IoT platforms for remote monitoring (Thamrongaphichartkul et al., 2020).

- **Conversational AI (CAI):**

AI that employs natural language processing and speech recognition for seamless human-machine interaction via voice or text (Luciano, 2023).

- **Democratised AI**

Enhancing AI accessibility and inclusivity through cost-effective, user-friendly tools (Luciano, 2023)

- **Deep Learning:**

A subset of machine learning involving artificial neural networks with multiple layers for analysing different data types. It is employed in the industry of hospitality and tourism for predictive analytics, customer behavioural analytics, and service optimisation (Essien & Chukwukelu, 2022).

- **Explainable AI (XAI):**

Seeks to enhance AI transparency and accountability through explanations of decisions and revealing underlying logic mechanisms (Luciano, 2023).

- **Human–Robot Collaboration:**

It refers to the interaction between a robot and a human, specifically, it describes how they work together in industrial robot environments such as the service industry, where robots support human workers to carry out tasks such as booking, room service and handling. This kind of cooperation makes the process more efficient and frees up a human employee to focus on a more personal service (Wu & Zhang, 2024).

- **Human–Robot Interaction:**

Interaction between robots and humans in collaboration or social environments (Foster et al., 2017; Kim et al., 2021; Kong et al., 2023; Nakanishi et al., 2020).

- Internet of Things (IoT):

A network of interconnected devices equipped with sensors, chips and software that allow them to collect, share, and act on data (M. Li et al., 2021).

- Personal Identifiable Information:

This includes information that can distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information linked or linkable to a specific individual, such as a name, address, phone number, or email address, which is unique to that individual. (Cooke, 2020; Miller et al., 2021; Urs, 2015).

- Point of Sale:

A system or place in which the transaction is carried out, such as where a customer makes a payment to the issuer of a card in exchange for goods or services. POS systems combine hardware elements (like terminals, scanners, and printers) and software applications to manage and record sales, purchase orders, customer data, and inventory. Retail and hospitality sectors commonly apply this type (Majumder et al., 2017).

- Radio Frequency:

Found in robotics systems for positioning and communication (e.g. robot waiter systems where radio frequency transmitters allow the robots to see the tables and transmit signals to access the customer devices' pagers (Cheong et al., 2015).

- Robots:

The term describes artificial beings designed to execute tasks for humans. It was popularised by Czech playwright Karel Čapek in 1920 (Liu et al., 2024).

- Self-Service Technology:

Refers to the form of technology in which customers are provided with a service where, typically, there would have been a direct service provider. These are things such as automated kiosks, check-in machines, or AI-based systems, particularly in government and hospitality. (Chen et al., 2021).

- Service robotics:

Autonomous, adaptable, networked interfaces that interact and deliver services resourcefully in industries like the service industry. Supported by artificial intelligence (AI) to adapt to their environment and independently perform tasks. (H. Kim et al., 2022; Kong et al., 2023).

- Socio-Tactical:

Socio-tactical refers to the integrated framework that combines the social, ethical, and human dimensions with tactical, systemic, and operational strategies to address real-world challenges in human-robot interaction, cyber-safe, and service robotics (author synthesised).

- **Socio-Technical:**

This refers to the integration between social and technical elements within a system, often focusing on how technology impacts social structures and vice versa (Ahlborg et al., 2019a; Bockshecker et al., 2018; Govers & van Amelsvoort, 2023a; Malatji et al., 2019a).

- **Systematic Literature Review (SLR):**

Presents an unbiased, systematic approach to the review and synthesis of all available evidence on a topic. This approach contributes to a holistic knowledge by identifying literature gaps and pointing the way for future research. This includes formulating questions, identifying studies, quality assessment, synthesis and interpretation (Li et al., 2021).

- **Technology Acceptance Model:**

A model applied to explain and predict user acceptance of technology based on the perceptions regarding the ease of use and usefulness; often used to discuss the adoption of AI systems, such as chatbots, in the hospitality industry (Pillai & Sivathanu, 2020)

- **Usability, Social Acceptance, User Experience, Societal Impact:**

A framework from the HRI to evaluate the usability, social acceptance, user experience, and societal impact of robots, especially in the hospitality industry (Tung & Au, 2018).

- **Wireless LAN:** A wireless network within a small geographical area, such as a café or a hotel (Afsheen et al., 2018).

Table of Contents

Abstract.....	iv
Acronyms, Abbreviations, and Symbols	v
Definitions of terminology	vi
Chapter 1: Introduction.....	19
1.1 Background.....	19
1.2 Problem Statement.....	20
1.2.1 Problem Statement Summary	20
1.3 Primary Objective of the Study	21
1.4 Main Research Questions	21
1.4.1 Research Sub-Question 1	21
1.4.2 Research Sub-Question 2.....	22
1.4.3 Research Sub-Question 3.....	22
1.5 Significance of the Study.....	22
1.6 Impact on Stakeholders.....	22
1.7 Encouraging Ethical Action and Social Development	23
1.8 Scope and Delimitations of Study	23
1.8.1 Scope.....	23
1.8.2 Delimitations.....	24
1.9 Structure of the Research.....	27
1.10 Summary.....	28
Chapter 2: Literature Review and Theoretical Framework	30
2.1 Introduction.....	30
2.2 Background.....	30

2.2.1	Early Automation to Robotic Systems: Historical Context and Current Trends	32
2.2.2	Trends in Robotics Driven by Recent Technology in AI.....	33
2.3	Overview of Themes.....	36
2.4	Ethics of Service Robotics.....	36
2.4.1	Privacy and Data Security	36
2.4.2	Transparency and Explainability	37
2.4.3	Bias and Fairness	37
2.4.4	Autonomy and Human Oversight.....	37
2.4.5	Economic Impact	37
2.4.6	Accountability and Liability	38
2.5	Cybersecurity Challenges	38
2.5.1	Types of Cyber Threats in RSI	38
2.5.2	Case studies of cyber incidents.....	40
2.5.3	Responding to Cybersecurity Threats.....	42
2.6	Human-Robot Interaction	42
2.6.1	Ethical Treatment of Robots	43
2.7	Ethics and Cyber-Safety Integration for Service Robotics.....	44
2.8	Theoretical Framework.....	46
2.8.1	Interdisciplinary Foundations	46
2.8.2	Cybersecurity Frameworks.....	46
2.8.3	Ethical Frameworks	46
2.8.4	Legal and Regulatory Considerations.....	47
2.8.5	Ethics and Cybersecurity Integration Framework	47
2.9	Conclusion	48
Chapter 3:	Research Methodology and Design	50

3.1	Introduction.....	50
3.2	Research Paradigm	50
3.3	Design Science Research	51
3.4	Research instrumentation.....	52
3.4.1	PRISMA Guidelines for Systematic Review	52
3.4.2	Expert Questionnaire	53
3.4.3	Evaluation Criteria.....	53
3.5	Data Collection Method.....	54
3.5.1	Expert Evaluation Questionnaire for a proposed ACERBOTICS Framework.....	54
3.5.2	Mixed-method approach.....	54
3.5.3	Purpose of Using a Mixed-Methods Approach	55
3.5.4	Qualitative data.....	55
3.5.5	Quantitative Data	58
3.6	Participants	58
3.6.1	Criteria for Participant Selection	58
3.7	Data Analysis.....	59
3.8	Ethical Considerations	59
3.9	Summary.....	60
Chapter 4:	Systematic Literature Review	61
4.1	Introduction.....	61
4.2	Critical Analysis of Existing Literature	61
4.3	Methodology Overview	63
4.3.1	Search Strategy	63
4.3.2	Inclusion and Exclusion Criteria	65
4.4	Screening and Selection Process	66

4.5	Critical Review of Literature on Ethical and Cyber-safe Service Robotic Systems	69
4.6	Geographic Distribution of Reviewed Studies	71
4.7	Socio-Technical Architectural Gap Across Methodologies	73
4.8	Cybersecurity Vulnerabilities Identified in Networked Service Robotics Systems	74
4.9	Design Criteria Identified	75
4.10	Emergent Themes from the Systematic Literature Review	77
4.11	Results and Findings.....	78
4.11.1	Contributions and Strengths of Reviewed Studies	78
4.11.2	Limitations of Reviewed Studies.....	79
4.12	Discussion.....	79
4.13	Conclusion	79
Chapter 5:	Proposed Framework Development and Presentation	81
5.1	Introduction.....	81
5.2	Theoretical Framework.....	83
5.2.1	Value Sensitive Design	84
5.2.2	Ethically Aligned Design.....	84
5.2.3	Socio-Technical Systems Theory.....	84
5.2.4	Integrative Relevance of Theoretical Frameworks to the Proposed ACERBOTICS Socio-Tactical Integration Framework for Cyber-safe and Ethical Service Robotics	84
5.2.5	Presentation of a Proposed ACERBOTICS Framework - A Socio-Tactical Integration Framework for Cyber-safe and Ethical Service Robotic Systems.....	85
5.3	Literature and SLR Foundations of the Proposed Framework Components	87
5.4	Framework Development Process	89
5.4.1	Phase 1: SLR and Extraction	89
5.4.2	Phase 2: Socio-Technical Gap Mapping.....	89

5.4.3	Phase 3: Theoretical Convergence and Adaptation	89
5.4.4	Phase 4: Visual Modelling and Feedback Loop.....	90
5.5	Socio-Technical Paradigm Shift.....	91
5.5.1	Socio-Technical Architecture Gap	91
5.6	Socio-Tactical Defined	92
5.7	Overview of Proposed ACERBOTICS Governance and Deployment Structural Layers	93
5.7.1	Evaluation of a Proposed ACERBOTICS Socio-Tactical Integration Framework for Cyber-safe and Ethical Service Robotic Systems.....	95
5.8	Framework Purpose	95
5.9	A Proposed ACERBOTICS Integrated Socio-Tactical Framework.....	97
5.10	Why The Feedback Loop Mapping Matters for Evaluation	99
5.11	Conclusion	99
Chapter 6:	Expert Evaluation and Refinement of the ACERBOTICS Socio-Tactical Integrated Framework	101
6.1	Introduction.....	101
6.2	Evaluation Methodology	102
6.2.1	Evaluation Design and Rationale.....	102
6.2.2	Criteria for Expert Selection.....	102
6.2.3	Data Collection Instrument.....	103
6.2.4	Ethical Considerations	103
6.3	Expert Evaluation Result	103
6.3.1	Quantitative Overview	103
6.3.2	Reliability of Evaluation Instrument	108
6.3.3	Comparative Analysis Across Framework Components	109
6.3.4	Identification of Strengths and Weaknesses	110

6.3.4.1	Strengths.....	110
6.3.4.2	Weakness.....	110
6.3.5	Qualitative Feedback from Expert Evaluation	111
6.3.6	Thematic Presentation of Expert Insights.....	112
6.3.6.1	Ethical Robustness and Integrity.....	112
6.3.6.2	Socio-Technical Integration and Contextual Adaptability.....	112
6.3.6.3	Clarity and Practical Usability	112
6.3.6.4	Cyber-Safety and Governance Enhancement.....	113
6.4	Thematic Analysis Procedure	113
6.4.1	Areas of Convergence.....	116
6.4.2	Areas of Divergence	117
6.4.3	Integrated Summary of Key Evaluative Outcomes	117
6.5	Summary of Key Findings.....	117
6.6	Implementations of Feedback for Framework Refinement.....	118
6.7	Refined Framework Based on Expert Feedback	118
6.7.1	Rationale for Refinement.....	118
6.7.2	Description of Modifications.....	119
6.8	Presentation of the Refined ACERBOTICS Socio-Tactical Integrated Framework.....	120
6.8.1	Comparison with the Initial ACERBOTICS Framework	122
6.8.2	Enhancement Outcomes	122
6.9	Conclusion	122
Chapter 7:	Discussion, Conclusion and Recommendations	123
7.1	Introduction.....	123
7.2	Discussion.....	124
7.2.1	Interpretation of Findings in Relation to Research Questions.....	124
7.2.2	Reflection on Research Objectives	125

7.3	Conceptual Implications	127
7.4	Methodological Implications	127
7.5	Practical and Policy Implications	128
7.6	Limitations of the Study	128
7.7	Directions for Future Research	128
7.8	Chapter Summary	129
7.9	Conclusion	129
	References.....	130
	Appendices	144
	Appendix A: SLR Extraction Matrix Informing the ACERBOTICS Socio-Tactical Framework (Synthesised by author)	145
	Appendix B: Geographic Distribution of Studies (Synthesised by author).....	146
	Appendix C: Thematic Coverage Across Studies (Synthesised by author)	147
	Appendix D: Design Criteria Identified in Reviewed Literature.....	148
	(Synthesised by author)	148
	Appendix E: Distribution of Study Relevance to Cyber-Safety, Ethical and Service Robotics Domains (Synthesised by author).....	149
	Appendix F: Study Relevance Frequency Count.....	150
	(Synthesised by author)	150
	Appendix G: Socio-Technical Architectural Gap Across Methodologies Pivotal Table (Synthesised by author)	151
	Appendix H: Thematic Coverage Gap Count (Synthesised by author).....	153
	Appendix I: Geographical Distribution Pivotal Table (Synthesised by author).....	154
	Appendix J: SLR Extraction Matrix with Identified Design Criteria (Synthesised by author).....	155
	Appendix K: Design Criteria Frequency Count (Synthesised by author)	165

Appendix L: Questionnaire for Evaluating the ACERBOTICS Framework (Synthesised by author)	166
Appendix M: Ethical Clearance Certificate (Synthesised by author).....	176
Appendix N: Critical Analysis of Literature on Cyber-Safe and Ethical Service Robotics (Synthesised by the author)	179
Appendix O: Reliability Analysis Evaluation Items (Synthesised by author)	201
Appendix P: Individual Item Reliability Statistics of Quantitative Responses (Synthesised by author).....	202
 <i>Figure 1.1 Framework Development Process for Cyber-Safe and Ethical Robotics in the RSI (Synthesised by author).....</i>	 <i>25</i>
<i>Figure 1.2 Framework Development Process Meta-Analysis (Synthesised by author)</i>	<i>26</i>
<i>Figure 2.1: Ethical and Cybersecurity Concerns in RSI- A Conceptual Overlap.....</i>	<i>156</i>
<i>Figure 2.2: Chronological Representations of Robotics in the Service Industry</i>	<i>33</i>
<i>Figure 2.3: Trends in AI Advancement that Drive Robotic Systems (Synthesised by author)</i>	<i>35</i>
<i>Figure 2.4: Integrating Cybersecurity and Ethics for Trustworthy Service Robotics</i>	<i>43</i>
<i>Figure 2.5: Understanding Risk and Promoting Safety and Ethics.....</i>	<i>45</i>
<i>Figure 4.1 Conceptual Development Cycle in SLRs (Synthesised by author).....</i>	<i>62</i>
<i>Figure 4.2 PRISMA 2020 Flow Diagram.....</i>	<i>68</i>
<i>Figure 4.3 Relevance to Key Robotic Domains (Synthesised by author)</i>	<i>70</i>
<i>Figure 4.4 Pie Chart of Geographic Distribution of Reviewed Studies (Synthesised by author)</i>	<i>72</i>
<i>Figure 4.5 Methodology Distribution of Socio-Technical Architectural Gap</i>	<i>73</i>
<i>Figure 5.1 Conceptual Underpinning Map for a Proposed ACERBOTICS framework (Synthesised by author)</i>	<i>85</i>
<i>Figure 5.2 A proposed ACERBOTICS Framework: Core Pillars (Synthesised by author).....</i>	<i>86</i>
<i>Figure 5.3 A proposed ACERBOTICS Framework Development Pipeline.....</i>	<i>90</i>

<i>Figure 5.4 Socia-Tactical Framework (Synthesised by author)</i>	<i>92</i>
<i>Figure 5.5 Iterative Governance and Deployment Cycle Architecture (Synthesised by author).....</i>	<i>93</i>
<i>Figure 5.6 ACERBOTICS Integrated Socio-Tactical Framework Architecture</i>	<i>98</i>
<i>Figure 6.1 Refined ACERBOTICS Socio-Tactical Integrated Framework.....</i>	<i>121</i>

<i>Table 2.1 Overview of Cybersecurity Incidents in Service Robotics (Synthesised by author)</i>	40
<i>Table 2.2 Overview of Cybersecurity Incidents in Service Robotics (Synthesised by author)</i>	41
<i>Table 4.1 Search Terms and Boolean Operators (Synthesised by author)</i>	64
<i>Table 4.2 Inclusion and Exclusion criteria (Synthesised by author)</i>	65
<i>Table 4.3 Summary of Design Criteria Identified</i>	75
<i>Table 5.1 SLR Foundations of the Proposed Framework Components</i>	88
<i>Table 5.2 Framework Components and Roles</i>	96
<i>Table 6.1 Descriptive Summary of Expert Ratings (n = 27)</i>	104
<i>Table 6.2 Descriptive Summary of Expert Ratings (n = 27)</i>	Error! Bookmark not defined.
<i>Table 7.1 Summary of Research Objectives Outcome (Synthesised by author)</i>	126

Chapter 1: Introduction

1.1 Background

The Robotic Service Industry (RSI) has experienced rapid and remarkable growth over the last decades, transforming manufacturing and reshaping task execution in healthcare, logistics, education, and customer service sectors. RSI involves the use of self-directed robotic systems that provide services directly to people and enhance human-centred processes (Gonzalez-Aguirre et al., 2021). These service industries have expanded considerably, powered by innovative feats in artificial intelligence (AI), machine learning (ML), and robotics. These technological advancements promise improved efficiency, accuracy, and the capacity to function independently in dynamic and hazardous environments (Wirtz et al., 2021a).

The RSI applications are diverse, ranging from autonomous delivery robots in logistics to medical robots assisting in surgeries and customer service robotics in hospitality (Xu et al., 2023). For example, the deployment of robotic concierges in hotels and automated disinfection robots during the COVID-19 pandemic demonstrated the potential to boost efficiency and decrease reliance on human labour for critical tasks (Huang et al., 2021). These innovations improve resource management and minimise the risks associated with human participation in high-risk situations.

As RSI advances, it presents intricate challenges that must be considered to guarantee its sustainability. While beneficial, RSI also presents notable challenges related to cybersecurity, human safety, and ethical concerns. The increasing interconnectivity of robotic systems with digital infrastructures, including Internet of Things (IoT) networks and cloud platforms, enlarges the attack surface, rendering RSI susceptible to cyber threats (Yaacoub et al., 2022).

Instances of cyberattacks, such as data breaches and ransomware, have already occurred in robotic applications, indicating the urgent need for stringent security measures (Fosch-Villaronga & Mahler, 2021). Additionally, safety issues stemming from malfunctions or operational mistakes in healthcare and industrial settings can result in grave outcomes, including potential harm to individuals (Quarta et al., 2017). These risks highlight the necessity for addressing vulnerabilities in human-robot interaction (HRI).

This integration of RSI also results in ethical issues regarding data privacy, bias, accountability, and job displacement. As robotic systems take on sensitive information like personal data and behavioural patterns, protecting this information is essential for upholding public trust and

ensuring operational integrity (Dwivedi et al., 2020). The demand for transparency and fairness in robotic applications underscores the need for ethical considerations in RSI's design, implementation, and regulation.

1.2 Problem Statement

RSI offers significant benefits, such as improved efficiency, precision, and automation, but also faces major cyber-safety and ethical challenges. Service robotics using AI and the IoT are vulnerable to cyber threats, including data breaches and unauthorised access (Pogliani et al., 2019; Quarta et al., 2017). These risks threaten sensitive data and human safety in critical sectors like healthcare and hospitality. Despite a growing awareness of these issues, current research often treats cyber-safety and ethics separately, leading to fragmented or insufficiently tailored approaches.

Existing cyber-safety and ethical standards fail to address the interconnected hazards posed by the complexity and autonomy of service robotics. Ethical concerns such as job displacement, algorithmic bias, and transparency remain largely untested in robotic deployments, resulting in biased AI and distrust. These issues highlight the need for a cohesive framework combining cybersecurity with ethical principles tailored to the RSI. Neglecting a holistic approach poses serious risks. Cybersecurity breaches compromise sensitive information and operational safety, endangering lives. Ignoring ethical challenges can exacerbate societal disparities and erode confidence in robotic applications, threatening the viability of RSI innovations. Existing research and governance approaches continue to address cybersecurity, ethical, and HRI challenges in a fragmented manner, with limited integration of socio-technical, contextual, and operational considerations. These gaps, which are primarily methodological and practical, highlight the need for a conceptual framework that combines cyber-safety, ethical, human-centred, and socio-technical considerations to support the responsible deployment of service robotics.

1.2.1 Problem Statement Summary

Despite advances in cybersecurity, ethical AI, robotics, and HRI, the literature indicates a limited availability of integrated governance frameworks that combine these domains to support secure, ethical, and operational service robotics (Callari et al., 2024a; IEEE, 2019a; Lu et al., 2020a). Current methods address these separately, as discussed in Sections 2.7-2.9 and synthesised in Chapter 4, resulting in fragmented guidance. As a result of these limitations, there is a need for a conceptual socio-tactical framework that integrates cyber-safety, ethical, human-centred, and

socio-technical design principles to support responsible deployment within the service robotics industry.

1.3 Primary Objective of the Study

The primary objective of this study is to develop and evaluate a conceptual socio-tactical integrated framework to support the cyber-safe, ethical, and operationally safe deployment of service robotics within the service industry.

The following secondary objectives collectively contribute to achieving this goal by identifying the cybersecurity vulnerabilities affecting networked robotic systems, examining the alignment of ethical and regulatory principles, and integrating these insights into a unified governance framework. The objectives include:

Objective 1: To investigate cybersecurity vulnerabilities in networked robotics systems.

Objective 2: To examine the alignment of existing regulatory measures with ethical principles and standards in RSI.

Objective 3: To develop a conceptual framework that mitigates cybersecurity risks, ethical considerations, and operational safety when deploying service robotics.

1.4 Main Research Questions

To what extent can a proposed unified cyber-safe and ethical framework be developed to support the secure and responsible deployment of robotic systems in the service industry?

1.4.1 Research Sub-Question 1

What cybersecurity vulnerabilities are prevalent in the RSI?

How can cybersecurity measures be deployed to safeguard sensitive data and maintain operational integrity?

Purpose: This question corresponds with Objective 1, which aims to investigate cybersecurity vulnerabilities in networked robotics systems. It also aims to uncover specific cybersecurity threats within RSI and examine strategies to reduce risks and ensure operational safety, considering the substantial dangers that robotic systems present when integrated into key service industry sectors.

1.4.2 Research Sub-Question 2

How can standardised ethical guidelines be developed to mitigate safety risks associated with algorithmic flaws in service robotics?

Purpose: This inquiry aligns with Objective 2, which focuses on identifying ethical standards and examining ethical issues associated with RSI. It also explores the ethical implications of service robotics, focusing on privacy, job displacement, robot treatment, and algorithm flaws. The question explores the creation of a framework that addresses the identified safety concerns and helps develop an ethical code for robotic deployment in HRI.

1.4.3 Research Sub-Question 3

How can a unified framework incorporating cybersecurity measures, ethical safeguards, and HRI principles be developed for service robot deployment in the service industry?

Purpose: The aim is to develop a unified framework for deploying service robotics that incorporates mitigations of cybersecurity risks, ethical considerations, and operational safety, aligning with Objective 3 of establishing ethical standards for the RSI.

1.5 Significance of the Study

The framework informs practical steps to address significant gaps in the current RSI landscape, specifically in the following areas:

Cybersecurity Practices: Offer strong encryption strategies, secure communication, and vulnerability assessments to mitigate risks such as data breaches, unauthorised access, and system manipulation.

1. Safety Guidelines: Outline safety guides that ensure humans are not harmed by the robot's evolution, especially in critical environments such as healthcare and hospitality.
2. Ethical Standards: Define standards for transparency, fairness, and accountability in deploying service robotics, covering issues such as algorithmic bias, job loss, and privacy violations.

1.6 Impact on Stakeholders

This study benefits key stakeholders: policymakers, developers, and practitioners.

- For Policymakers: Evidence-based recommendations for regulatory standards ensuring safe and ethical robotic deployments.

- For Developers: Use the framework to create robotic systems that comply with cybersecurity and ethical standards, enhancing trustworthiness and user acceptance.
- For Practitioners: Implement safety and ethical frameworks to enhance human-robot cooperation while minimising risks in service.

1.7 Encouraging Ethical Action and Social Development

This study contributes to societal welfare by addressing cybersecurity, safety, and ethics in RSI, promoting safer robotic systems, reducing user risks, maintaining operational integrity, and fostering trust in robotic systems and allaying public fears. Furthermore, it encourages inclusive use by ensuring technology benefits all population segments and by providing fair service through service robotics.

The study further contributes by addressing the identified gap between fragmented ethical and cybersecurity approaches through the development of an integrated governance framework specifically designed for service robotics environments. In conclusion, this study advances responsible technological development in RSI, leading to safe, ethical, and publicly accepted robotic systems aligned with societal norms. It is proposed that this research may contribute to the opening of new frontiers in robotics and guide stakeholders in the navigation of rapidly evolving developmental landscapes.

1.8 Scope and Delimitations of Study

1.8.1 Scope

This study seeks to develop a robust framework for cyber-safe and ethical HRI designed for the RSI. Focusing specifically on the use of robots in healthcare, hospitality, logistics and education. Three core aspects are explored:

1. Ethical Standards: Standards that incorporate fairness, transparency and accountability in robotic deployment.
2. Cybersecurity Practices: Risk identification and mitigation (data breaches, unauthorised access, and system manipulation).
3. HRI: Improve safety and build trust in spaces where humans and robots work closely together.

1.8.2 Delimitations

The following delimitations outline the boundaries within which the research is conducted:

This study explores HRI but does not analyse broader human factors such as ergonomics, cultural variation, and psychological effects. It focuses on strategies for addressing cyber threats, rather than providing detailed descriptions of advanced technologies like intrusion detection systems and overdrive scenarios. The study is designed to consider existing ethical and regulatory standards and does not include emerging regulations or country-specific variations. Furthermore, the insights garnered from the service robotics case studies may exhibit bias, as these studies were specifically chosen and do not reflect the full spectrum of robotic deployments globally.

By establishing these clear boundaries, the study ensures that it remains focused and that developing a framework for cyber-safe and ethical service robotics is realistic. These borders help inform, guide, and ground future research in areas beyond the current scope.

Figure 1.1 presents a Framework Development Process for Cyber-Safe and Ethical Robotics in the RSI as synthesised by the author.

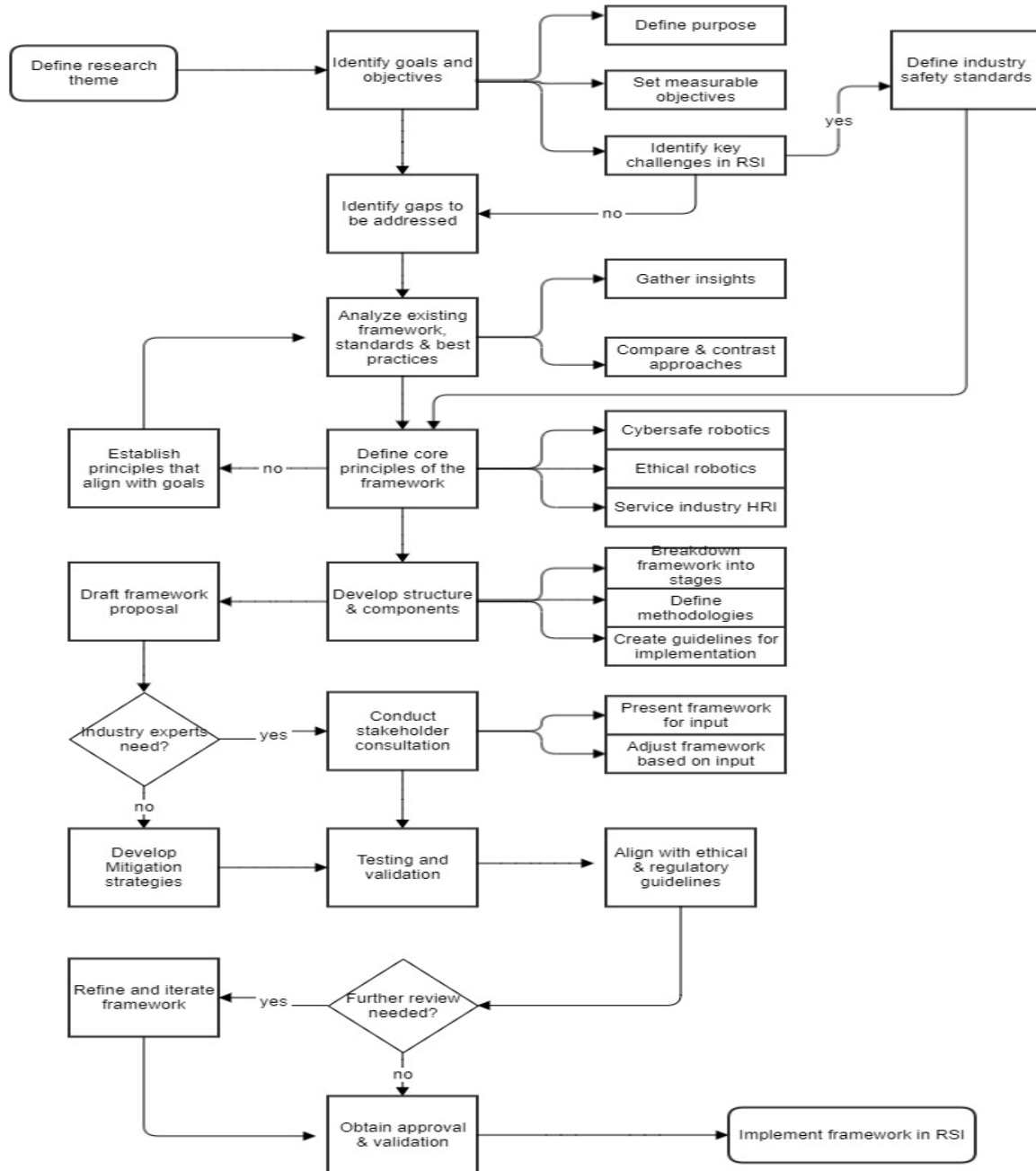


Figure 1.1 Framework Development Process for Cyber-Safe and Ethical Robotics in the RSI

(Synthesised by author)

The framework follows a structured Design Science Research approach that guides the development and validation of the framework. The process moves systematically from defining the problem and identifying gaps to designing the framework, consulting experts, refining it iteratively, and ensuring compliance with ethical and regulatory standards. The outcome is a validated implementation within robotic systems used in the service industry.

Figure 1.2 provides an overview of the research stages and framework development processes used in the study to design, evaluate, and refine the cyber-safe and ethical robotics framework for service industry contexts.

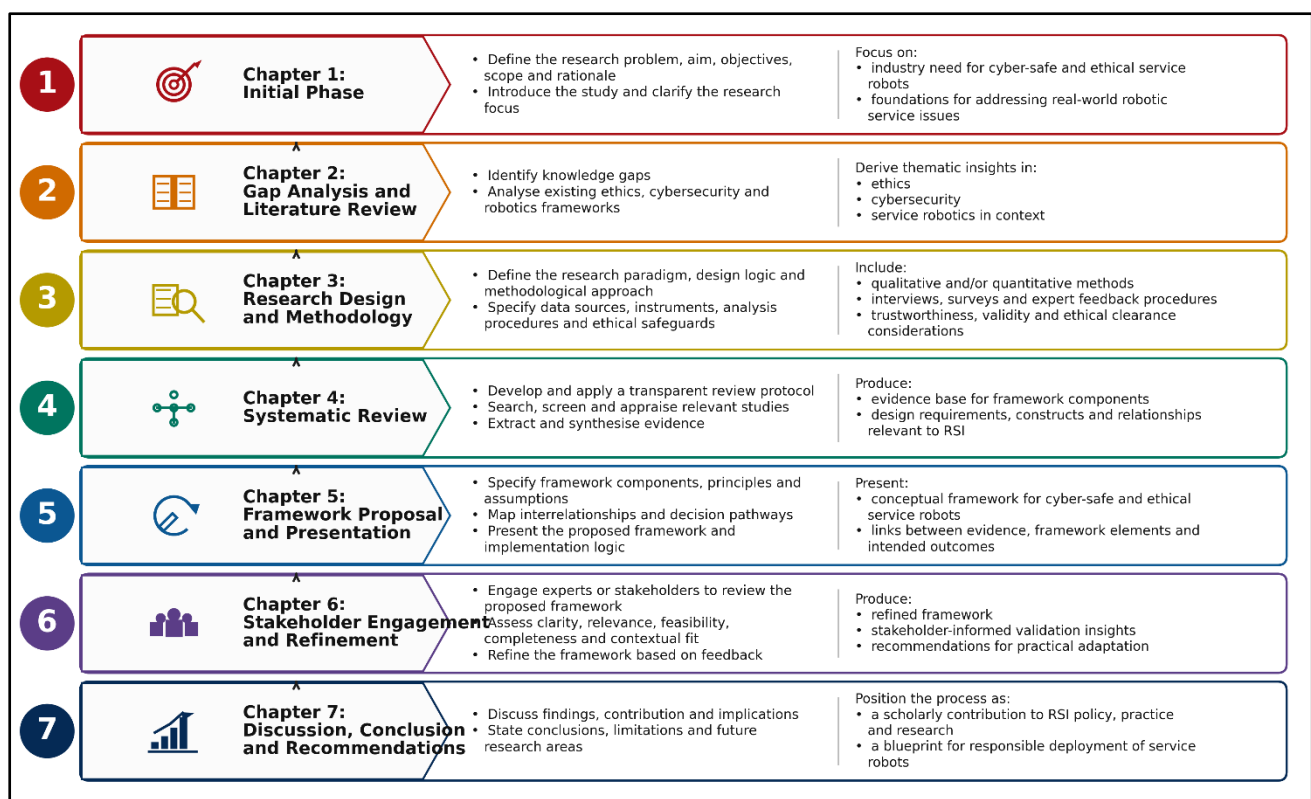


Figure 1.2 Framework Development Process Meta-Analysis (Synthesised by author)

Figure 1.2 shows the study's seven-stage progression, beginning with problem definition and theoretical foundation, followed by an SLR and gap analysis. It moves from methodological design to developing and refining the conceptual framework with experts. The final phases involve evaluation, validation, iterative improvements, and finally, synthesis, implications, and policy recommendations.

The figure highlights the logical, cumulative approach that ensures the framework's relevance both theoretically and practically. The details of each chapter are presented in Section 1.9 in relation to the research structure.

1.9 Structure of the Research

The structure of the research is presented in terms of chapters. Chapter 1 includes the introductory section, which provides the background and context of the study. Section 1 of this chapter overviews service robotics in education, healthcare, and hospitality. Section 2 identifies the current challenges, including the risks associated with cyber vulnerabilities in service robotics, ethical concerns in AI-driven automation, and gaps in existing studies, thereby establishing the problem statement. Section 3 outlines the goals and expected outcomes of the study. Section 4 poses the key questions guiding the research. Section 5 describes the significant contributions of the study. Section 6 identifies the scope and limitations of the research. Finally, Section 7 provides a brief overview of each chapter and a summary of Chapter 1.

Chapter 2: This chapter reviews the evolution of service robotics and current trends in RSI. It discusses cybersecurity concepts and frameworks relevant to robots. Ethical concerns about using robots in healthcare, retail and hospitality are explored through various ethical theories. The chapter concludes by examining the existing guidelines and frameworks for ethical robots.

Chapter 3 describes the overall research design, including qualitative and quantitative approaches. It details the methods used for collecting data, such as interviews and surveys. It also explains the technique for analysing the collected data and acknowledges any limitations or biases in the study.

Chapter 4 outlines the key components of the proposed framework for cyber-safe and ethical robots. It begins by conducting and presenting the findings of the data from literature synthesis using the model of (Lu et al., 2020b). Additionally, it details specific cybersecurity measures that should be integrated into the framework and the ethical guidelines relevant to using robots. Finally, it discusses summaries of the criteria for implementing the framework within the service industry.

Chapter 5 concentrates on developing and refining the proposed framework. It starts with a summary of the foundational research objectives and methodology, giving a detailed overview of the theoretical underpinnings that shaped the initial framework design. The chapter then moves into empirical analysis based on chosen case studies, which act as real-world examples to validate and enhance the framework. These case studies influence the framework's design and provide

insights into its relevance across different contexts within the service industry. By incorporating lessons from theoretical literature and practical applications, this chapter illustrates the iterative process of aligning the framework with practical needs and ensuring its effectiveness in addressing cybersecurity and ethical challenges related to robotics systems.

Chapter 6 evaluates the proposed framework, building on Chapter 5's foundational work where the framework was developed and its applicability outlined. While Chapter 5 focuses on designing the framework using theoretical insights and empirical case studies, Chapter 6 shifts to assessing its effectiveness and relevance. This chapter details the evaluation methodology, involving feedback and validation from a panel of multidisciplinary experts in robotics, cybersecurity and ethics. These experts assess the framework based on predefined criteria such as adaptability, reliability, and feasibility.

The evaluation also incorporates qualitative data from expert interviews and surveys to refine the framework further. Key findings highlight areas where the framework addresses cybersecurity vulnerabilities, ethical concerns, and limitations identified in the assessment. These insights inform enhancements to ensure the framework is robust and implementable. By connecting chapters 5 and 6, this chapter transitions from framework development to empirical validation, emphasising its readiness to address robotic systems challenges within the service industry. This chapter concludes by discussing the implications for policymakers, practitioners, and researchers, providing recommendations for the responsible adoption of robotic technologies, through an in-depth analysis of data gathered from a panel of experts. It outlines the feedback and insights received during the evaluation and assesses their implications for refining the framework. Additionally, the chapter explores how the framework can be applied practically in the service industry, supported by the analysis of the results.

Chapter 7 concludes by emphasising the importance of cyber-safe and ethical robots, summarising the key findings, and offering recommendations for future research to propel advancements in robotics within the service sector.

1.10 Summary

This introductory chapter sets the stage for addressing the challenges (such as cyber threats, ethical issues, and failure factors) associated with deploying service robotics. These challenges are significant for the RSI, for example, in the fields of healthcare, hospitality, logistics, and education, where human–robot interaction is the focal point.

In response to these challenges, the study outlines key research objectives and questions to address these issues through a comprehensive framework incorporating principles from ethics, cybersecurity, and HRI. This framework seeks to provide practical metrics and best practices to help close the gap between technological advancement and the associated responsibilities, ultimately promoting safer and more reliable service robotic systems.

Finally, it discusses the scope of the study, its delimitations, and outlines the research structure that informs the development of the framework.

Chapter 2: Literature Review and Theoretical Framework

2.1 Introduction

This literature review presents a foundation for discussing ethical and cybersecurity issues pertaining to service robotics. As service robotics increasingly enters homes, hospitals, and public spaces, it is crucial to understand how robotics can safely and ethically interact with humans. Ethics ensures that the actions of robots align with human values, while cybersecurity safeguards against data theft, hacking, and the misuse of sensitive information. This chapter identifies areas for integration and consolidation by examining existing literature, with a specific focus on ethics, cyber-safety issues, and service robotics. It references existing knowledge frameworks that may address aspects of the current research focus, namely the ethical and cyber-safety issues of service robotics.

This literature review focuses on the ethical and cybersecurity aspects of service robotics, particularly within the domain of HRI. Literature informs the extent to which existing approaches of service robotics, ethics and cyber-safety guidelines and standards may be adapted to or are relevant for service robotics. Service robotics has broad application areas, such as healthcare services, virtual assistance (chatbots), navigation systems and manufacturing (Mujahid et al., 2022); however, this review focuses on the relevant literature on service robotics working alongside humans in the service industry (specifically customer service and collaborative tasks).

2.2 Background

Service robotics refers to autonomous, adaptable, networked interfaces that interact and deliver services resourcefully in sectors like healthcare, travel and tourism, education, and customer service. Service robotics is supported by AI to adapt to environmental constraints and to independently perform tasks (Choi et al., 2020; Huang et al., 2021; H. Kim et al., 2022). Service robotics “enhances labour productivity and service quality” (Gonzalez-Aguirre et al., 2021), improves customer satisfaction, and addresses social issues like an ageing population and the need for a cost-efficient healthcare system (Guo et al., 2024; Huang et al., 2021).

Robotics ethics, whose key aspects include privacy, autonomy, responsibility and the impact on human jobs, governs the actions of robots according to (Belk, 2021). Service robotics raise privacy concerns as they collect sensitive information, necessitating strong data protection measures (Etemad-Sajadi et al., 2022). Autonomy and accountability are vital in scenarios affecting human

lives, such as healthcare, with advocates calling for ethical-by-design methodologies (Iphofen & Kritikos, 2021).

Cybersecurity in robotics protects against cyberattacks like hacking and data theft. As mobile robots increasingly depend on networks and cloud computing systems, they risk functional loss and safety issues (Callari et al., 2024a). Robust cybersecurity principles are vital for safety, integrating robotics, complemented by regular updates and resilience strategies (Tanimu & Abada, 2025a).

Service robotics offers revolutionary potential, but ethical and cybersecurity concerns must be addressed for safe deployment. Collaboration in engineering, law, ethics, and sociology is needed to align robotic design with societal values and safety expectations.

Figure 2.1 presents the conceptual positioning of the study with a central focus on ethics, cyber-safety, and HRI within the context of the service industry.

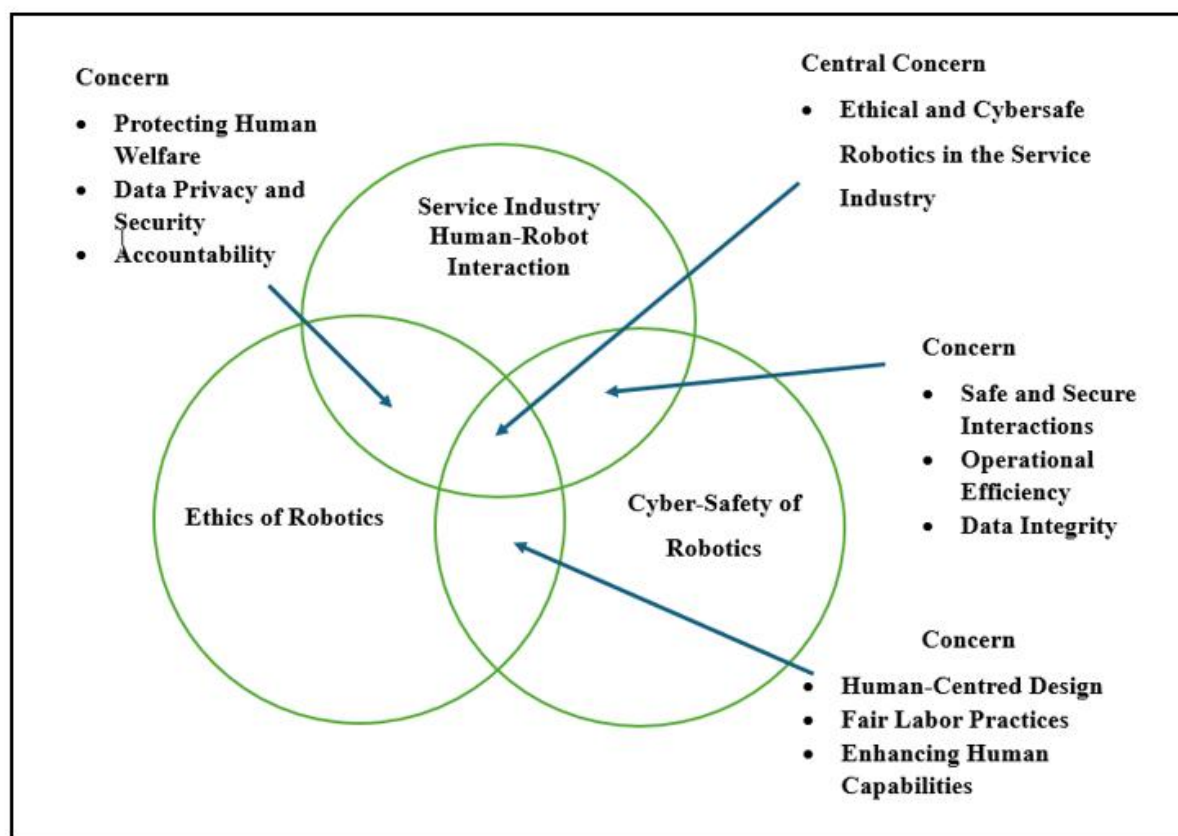


Figure 2.1: Ethical and Cybersecurity Concerns in RSI- A Conceptual Overlap

Figure 2.1 illustrates the primary research concern at the intersection of ethics of robotics, cyber-safety, and service industry HRI. The Venn diagram shows a shared need for an integrated cyber-ethical framework covering governance, transparency, and safe operational practices. It highlights

how ethical safeguards and cyber-safety are interconnected issues that must be incorporated into the socio-technical design and deployment of service robotics. Overall, the figure emphasises that ethical robustness and cyber-safety should be addressed together to promote responsible, trustworthy, and socially acceptable service robotics.

2.2.1 Early Automation to Robotic Systems: Historical Context and Current Trends

The historical development of service robotics shows a gradual yet considerable transition from early basic automation to intelligent, AI-enabled systems embedded in contemporary service environments.

While the term robot was introduced by Karel Čapek in the 1920s, large-scale technological development accelerated in the mid-twentieth century, initially within industrial manufacturing contexts before expanding into healthcare, hospitality, retail, and other high-contact service domains (Ivanov et al., 2019; Senthamarai et al., 2024). Scholarship examining this trajectory demonstrated how robotics progressively shifted from task-specific industrial machines in the 1960s to assistive and care-oriented applications between the 1970s and 1990s, and subsequently toward AI-driven, customer-facing service systems in the late and early 21st century (Essien & Chukwukelu, 2022; Wirtz et al., 2021a). The more recent developments since 202 highlighted the integration of AI-driven and HRI, including contactless service delivery, disinfection technologies, and intelligent decision support functionalities across diverse service sectors (Kim et al., 2022; Kong et al., 2023; Tung & Au, 2018; Tuomi et al., 2021). This progression shows not simply technological development, but an increasing integration of robotics with social, ethical, and cyber-safety considerations that shape contemporary service-industry deployments

Figure 2.2 presents a timeline highlighting significant milestones in the development of service robotics.

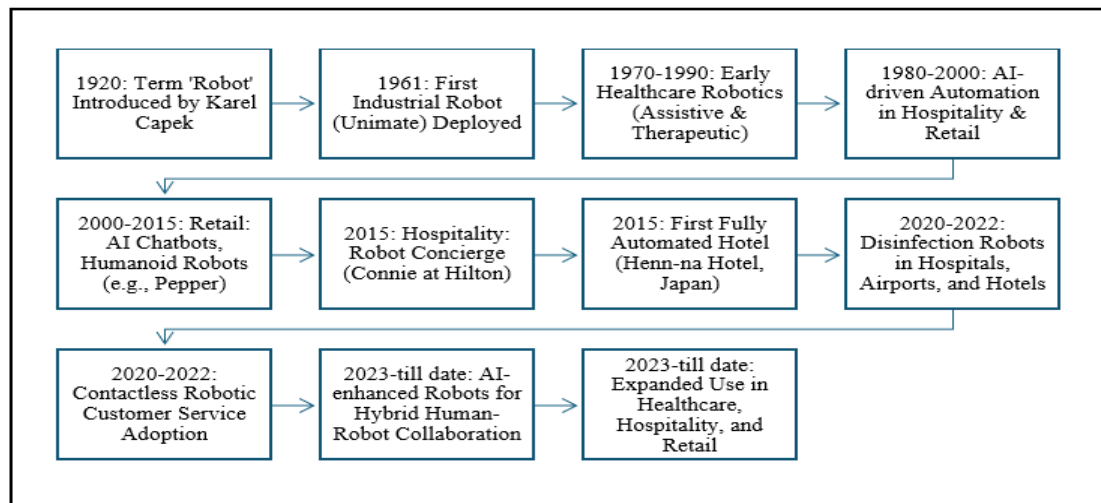


Figure 2.1: Chronological Representations of Robotics in the Service Industry

(Synthesised by author)

Figure 2.2 outlines the historical and contemporary advancements in robotics and AI. Each milestone reflects a progressive need for robust, cyber-safe and ethical frameworks, especially given the increasingly complex nature of HRI. Lee, (2021) argues that early and disinfectant robots highlight ethical challenges in sensitive environments, while AI-enhanced collaboration directly relates to hybrid systems that require trust, safety, and ethical accountability (Etemad-Sajadi et al., 2022). The deployment of the first industrial robot, Unimate, in 1961 marked a turning point in automation. This era laid the groundwork for robotics as a tool for efficiency, paving the way for ethical and cybersecurity considerations in future robotic systems (Kong et al., 2023).

2.2.2 Trends in Robotics Driven by Recent Technology in AI

Robotics has undergone significant transformations driven by advancements in AI technology. These developments enable AI-powered systems to handle intricate sequencing tasks, such as natural language processing, emotional recognition, and personalised care. AI has proved especially beneficial in scenarios requiring HRI, as with robotic concierges and customer service representatives (Huang et al., 2021).

Figure 2.2 highlights recent trends in AI that are driving the evolution of robotic systems. These include autonomous AI, which allows robots to move around without a human controlling them;

generative AI, which provides robots with enhanced abilities to create custom content; and explainable AI (also called XAI), which improves transparency by making the decision-making processes of robotic systems apparent (Luciano, 2023). These trends illustrate the blending of AI and robotics, making service robotics capable of providing greater efficiency and flexibility across industries.

The transition from innovative machines like Unimate to the modern use of AI illustrates the significant progress within the evolution spectrum. Initial automation set the stage for AI technologies (Kong et al., 2023). Philosophical perspectives on logic and reasoning laid the intellectual groundwork for these innovations. The current robotics landscape, characterised by highly autonomous systems, reflects decades of incremental improvements, interdisciplinary collaboration, and innovation. By examining the historical path of robotic systems and the philosophical context, a deeper understanding is gained of the functions the current service robotics possess or lack, and the challenging questions they pose for automation and ethics (Liang et al., 2024). The current research addresses these concerns by developing a framework to guide the safe implementation, ethical utilisation, and effective integration of robotic technology within the service industry.

Figure 2.3 presents the trends in AI advancement that drive robotic systems, as synthesised by the author.

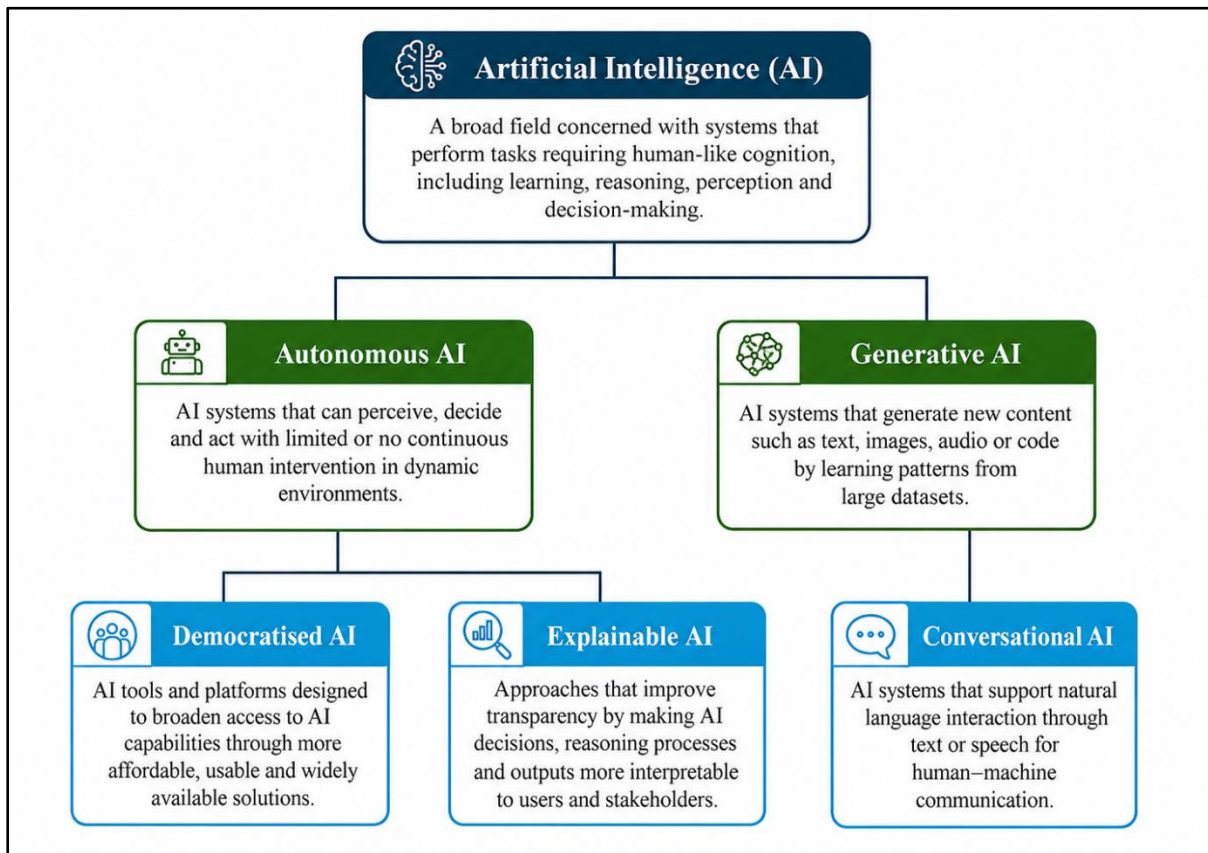


Figure 2.2: Trends in AI Advancement that Drive Robotic Systems (Synthesised by author)

From Figure 2.3, it is apparent that modern AI systems blend technical abilities with social and ethical safeguards. This is especially important in service robotics, where accountability, interpretability, and human-centered deployment are essential. Figure 2.3 presents an overview of AI paradigms consistent with (Luciano, 2023) and relevant to HRI, showing how AI capabilities diverge into autonomous and generative types, and further into specialised sub-domains such as XAI, CAI, and DAI. Overall, these categories highlight the technical foundations supporting intelligent robotic behaviour and emphasise the importance of transparency, accessibility, and human-centred interaction in service-focused AI systems.

2.3 Overview of Themes

This section covers four themes:

1. Ethics of Service Robotics, focusing on the ethical considerations of robot operations like fairness, transparency, accountability, and privacy. The theme examines ethical dilemmas in HRI and the expected contributions from current ethics frameworks.
2. Cybersecurity Challenges of Service Robotics address security concerns, such as unauthorised access, data integrity, and privacy issues. The theme surveys existing security methodologies and how they meet the challenges posed by robots.
3. Ethics and Cybersecurity Integration for Service robotics highlights the overlap between ethics and cybersecurity, ensuring that service robotics are safe and implements human values and social norms.
4. HRI concentrates on designing and assessing interaction between robots and humans in creating efficient and effective collaborative or social environments.

By exploring the four themes presented above, the review seeks to identify a research gap, offering a comprehensive perspective on current research and establishing a foundation for a novel framework of cyber ethics and security ethics in service robotics. The design criteria for a proposed framework to ensure the ethical and cyber-safe use of service robotics will be identified during the systematic literature review (SLR). These design criteria will be used to develop the proposed framework.

2.4 Ethics of Service Robotics

The introduction and use of robotic systems in service settings raise several ethical dilemmas that must be addressed for responsible deployment and operation (Belk, 2021). These considerations, as noted by (Polat et al., 2025), are vital because intelligent systems increasingly engage with humans in environments where trust, transparency, and accountability are necessary. In this section, key ethical issues such as privacy and data security, transparency and explainability, bias and fairness, autonomy and human oversight, and the broader social implications of robotic systems are explored (Aydemir & Dalpiaz, 2018; Tanimu & Abada, 2025a; Tlili et al., 2024; Wu & Zhang, 2024).

2.4.1 Privacy and Data Security

Robots dealing with privacy and data security typically handle vast amounts of sensitive data, including personal information, preferences, behaviours, and financial details (Floridi et al., 2018;

Wirtz et al., 2021). Although this data is essential for enhancing performance and user experience, it raises significant concerns regarding privacy violations and unauthorised access (IEEE, 2019). Ensuring user privacy and facilitating transparent interactions could make these robotic systems more widely utilised and accepted by users.

2.4.2 Transparency and Explainability

As more robots employ complex AI algorithms, transparency in the algorithms guiding their decision-making processes becomes increasingly critical. XAI ensures that users grasp the rationale behind robotic actions, which helps build trust and mitigate misunderstandings. If users perceive robots as untrustworthy or biased due to transparency issues, their adoption in sectors such as healthcare and hospitality will be limited, whereas they could otherwise enhance service quality (Floridi, 2023).

2.4.3 Bias and Fairness

Robotic systems powered by AI are not immune to algorithmic discrimination that may derive from training sets that mirror social inequalities. Such bias may cause discriminatory behaviour, threatening the fairness and inclusiveness of the robotic services. For example, robots used as customer service agents need to be programmed not to be biased against any user based on their demographics. It thus becomes an ethical imperative to develop and test algorithms that will mitigate bias (Floridi, 2023; Floridi et al., 2018a; Sadek et al., 2023a).

2.4.4 Autonomy and Human Oversight

This raises ethical concerns regarding the level of human oversight required for service robotics. While these devices can enhance performance on a large scale, excessive dependence on them may lead to consequences like reduced accountability or the potential for unintended actions in scenarios unforeseen by their creators. Ethical frameworks should emphasise the necessity of ‘human-in-the-loop’ measures as a supervisory and effective way to ensure these systems remain under human control, particularly in safety-critical situations or ethical challenges (Callari et al., 2024a; Weerarathna et al., 2023a).

2.4.5 Economic Impact

As service robotics become more common, fears regarding job displacement and its socioeconomic implications are understandable. While robots can enhance human productivity, they also have the potential to replace jobs that require minimal education and involve repetitive

tasks. Organisations must consider the advantages of automation alongside approaches to retrain and upskill affected workers, focusing on fostering collaboration between humans and robots instead of mere substitution (Hasan & Trianni, 2022a; Nam et al., 2021a; Wirtz et al., 2021b).

2.4.6 Accountability and Liability

Attributing responsibility for the failures or misconduct of robots presents a complex ethical challenge. For instance, when service robotics cause injury or breach ethical standards, it is crucial to clarify whether accountability lies with developers, operators, or the organisation deploying the robot. When AI fails, mechanisms should be in place to determine liability and administer suitable remedies for those affected (Benjumea, 2024a; O’Sullivan et al., 2019a).

The ethical literature consistently identifies privacy, accountability, transparency, and human dignity as foundational requirements for responsible robotic deployment. For instance, Friedman and Hendry, (2019), in Value Sensitive Design framework, emphasises the integration of human values into technology design. The IEEE’s Ethically Aligned Design Framework (IEEE, 2019a), similarly advocates for transparency, accountability, and human well-being as central governance principles. (Floridi et al., 2018a), further contend that ethical oversight should be embedded throughout the artificial intelligence lifecycle, rather than applied retrospectively. Taken together, these perspectives indicate that ethical governance should be systematically incorporated into the design and implementation of service robotic systems.

2.5 Cybersecurity Challenges

RSI has improved service delivery, but its growing dependence on interlinked services exposes the sector to various cyber threats. Integrating service robotics with service-oriented IoT networks, cloud platforms, and other digital infrastructures results in vulnerabilities that may act as potential attack vectors for malicious actors (Yaacoub et al., 2022). Robust cybersecurity measures are essential to maintain operational integrity, protect sensitive data and foster trust in robotic systems. This section discusses various cybersecurity threats to RSI, describes the most significant case studies of cybersecurity incidents, and recognises the necessity of coping with these threats to ensure the safety and secure quality of robotic operations.

2.5.1 Types of Cyber Threats in RSI

1. Data Security Risks

Service robotics usually handle and retain bulk information such as personal identifiable information, financial details, and behavioural patterns sensitive to specific organisations. Weak

encryption protocols expose this information to leaks and unauthorised access (Möller, 2023; Tanimu & Abada, 2025a). In the hospitality sector, for instance, service robotics have been exploited to gain access to guest information via robotic interfaces,² resulting in compromised privacy and the erosion of customer trust. Data breaches can lead to serious issues. Real-world examples include an incident at Henn-na Hotel in Japan, which experienced a data breach due to weak data protection. This compromise exposed sensitive customer information, causing reputational harm and financial damage (Bhimasta & Kuo, 2019). Incidents like this highlight the urgent necessity for advanced data security measures, such as encryption, access controls, and secure storage practices in robotic systems.

2. System Vulnerabilities

Another significant source of threats arises from hardware and software vulnerabilities in robotic systems (Saplacan et al., 2021; Yaacoub et al., 2022). Cybercriminals can exploit weaknesses in robotic operating systems to manipulate robot functions, deploy malicious code, or seize control of mechanical devices (Gutwirth et al., 2016). Such vulnerabilities may result in operational disruptions or safety risks, particularly in critical sectors like healthcare, where robots perform sensitive tasks such as surgeries.

For instance, outdated software or unpatched firmware can serve as an attack vector for a cyberattack, compromising robots' functionality. Regular updates, vulnerability assessments, and thorough testing can reduce these inherent risks.

3. Network-Related Threats

The use of service robotics with a connected IoT network and cloud-based platforms increases their attack surface and exposes them to network attacks. Common attacks consist of DoS (denial-of-service) attacks that overload network resources, causing disruption of service, and ransomware attacks that lock critical systems until a ransom payment is made (Tuomi et al., 2021).

In another example, ransomware incidents in the healthcare sector have locked out robotic systems, disrupting operations and risking patient safety. Likewise, DDoS attacks on the tourism and travel sectors have compromised booking systems, leading to financial losses and dissatisfaction (Bowen & Morosan, 2018). It is necessary to mitigate such attacks based on edge security protocols, secure communication protocols, and intrusion detection.

2.5.2 Case studies of cyber incidents

Table 2.1 presents significant cyber incidents that have affected service robotics across various sectors. These examples illustrate the diversity of attack types, their targets, and the consequences of insufficient security measures.

Table 2.1 Overview of Cybersecurity Incidents in Service Robotics (Synthesised by author)

Incident Name	Target Industry	Attack type	Impact
Target Corporation data breach	Hospitality and Tourism	Phishing and malware	Loss of trust, theft of personal data, disruption of operations and compromised systems (Ivanov et al., 2019; Li et al., 2021)
Privacy breach in hospitality	Hospitality	Data breach	Compromised guests' data results in reputation damage and legal implications.
Robot-assisted service	Hospitality	Data breach via service robot	Unauthorised access to guest details through robotic interface (Xu et al., 2023).

Table 2.2 Overview of Cybersecurity Incidents in Service Robotics (Synthesised by author)

Incident Name	Target Industry	Attack type	Impact
Ransomware attack	Healthcare	Ransomware	Lockout of critical service systems and halted operations pose a risk to patients' safety.
DoS attack on the booking system	Travel and Tourism	Denial-of-Service	Disruption of booking and financial losses (Bowen & Morosan, 2018; Filieri et al., 2021; Kim et al., 2021)
AI exploitation	Hospitality	Privacy breach	Sensitive data collection without consent, trust erosion (Tuomi et al., 2020).
Service robot errors and malfunctions	Hospitality	Software Code Injection	Reputational risk (Lv et al., 2022; Nam et al., 2021b).
AI failure	Hospitality	Unemphatic AI response	Lack of emotional recovery (Lv et al., 2022).
Henn-na Hotel breach	Hospitality	Data breach	Exposure of customer information. (Bhimasta & Kuo, 2019).

Table 2.1 provides a reference to the diversity of cybersecurity challenges in RSI, indicating that tailored and robust measures must be implemented to mitigate these vulnerabilities. Tailored measures will ensure defences for the specific operational environment, provide awareness of

unique threat vectors, and limit threat exposure. The robust cybersecurity architecture will foster trust, compliance, and the safe adoption of robotic systems while transforming vulnerabilities into controlled and monitored risks.

2.5.3 Responding to Cybersecurity Threats

The interconnectedness of service robotics emphasises the need for strong cybersecurity protocols (Tanimu & Abada, 2025b). Key strategies include:

- **Data Loss Prevention:** Protecting sensitive information through encryption, privileged access, and safe sharing to mitigate against breaches.
- **Updates:** Ensuring software and firmware are kept up-to-date, patching vulnerabilities, and ensuring continuous operating system security.
- **Network Protection:** Use of firewalls, intrusion detection systems, and secure communication protocols to defend against network-level threats.

The challenges of ethical governance, cyber-safety, and HRI may be systematically overcome to ensure that the RSI can build trust in robotic systems while reducing the risks of operation and enabling the market to continue to develop.

Collectively, the literature suggests that effective cyber-safety in service robotics extends beyond technical safeguards alone. While Tanimu & Abada, (2025c), emphasise the importance of encryption, system updates, and network protection, other scholars (IEEE, 2019a; Wirtz et al., 2021b), highlight the need to integrate cybersecurity measures with broader governance, ethical, and human-centred considerations to support trustworthy robotic deployments. This indicates that sustainable adoption of service robotics depends on not only mitigating technical vulnerabilities but also on promoting user trust, accountability, and operational resilience across diverse service environments.

2.6 Human-Robot Interaction

Etemad-Sajadi et al., (2022) argue that robots in the service industry must be designed to complement humans, not replace humans. The ethical HRI focuses on empathy, culture, and responsiveness in robots. Robots in healthcare, for example, should evoke compassion in responding to patients, while those in hospitality should respect and accommodate diverse expectations concerning culture, rule-abiding, and other ethical considerations. Overlooking these issues can cause user frustration, confusion and mistrust (Lv et al., 2022).

2.6.1 Ethical Treatment of Robots

The prospect of robots showing increasingly human-like traits has generated ongoing debate about their social and legal status, as well as the ethical implications of human-robot relationships (Saplacan et al., 2021). Although robots do not possess independent thought, they are designed to elicit emotional responses from people, raising important discussions about how they should be treated (Garcia-Gonzalez et al., 2022). Creating an ethical framework for AI can help guide the thoughtful development and use of robots, ensuring that human emotional responses are respected and not misused, regardless of context.

Figure 2.4 presents the conceptual integration of cyber-safety and ethics for trustworthy service robotics, as synthesised by the author, to reflect the central concerns and analytical focus of this study.

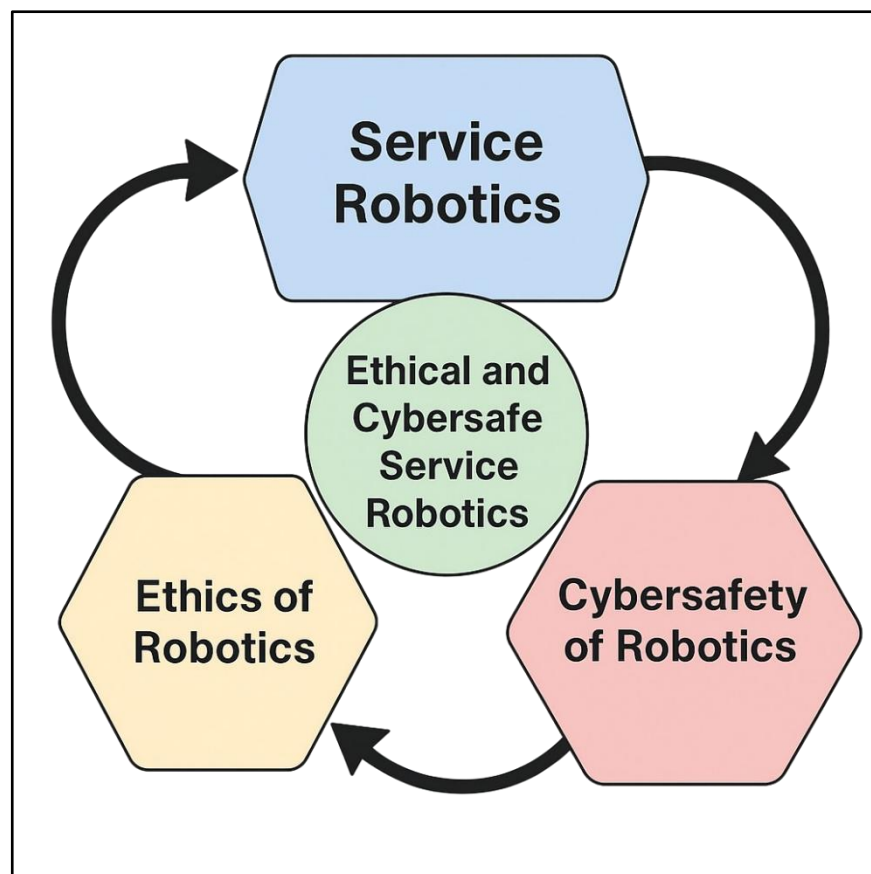


Figure 2.3: Integrating Cybersecurity and Ethics for Trustworthy Service Robotics

(Synthesised by author)

Figure 2.4 illustrates the intersection of cybersecurity vulnerabilities with ethical issues in RSI. The diagram illustrates a sequence of events wherein cybersecurity failures like data breaches, system malfunctions, or unauthorised access lead to ethical challenges such as privacy violations, reduced trust, and accountability concerns. The diagram highlights the necessity of collectively addressing these technical and ethical aspects through secure, transparent, and accountable robotic systems.

2.7 Ethics and Cyber-Safety Integration for Service Robotics

Ethics should not prohibit technological progress; it should propel technology in more socially responsible directions. Developers and policymakers must work together to establish frameworks that reconcile technological innovations with the greater good, so that robots will improve the human condition while avoiding harm and injustice (IEEE, 2019b; Lin, 2016).

Ethical and cybersecurity concerns need to be integrated into service robotics to ensure safe, secure and trustworthy deployments (Vanderelst et al. 2018). By integrating ethical guidelines and risk management into cybersecurity for HRI, these dual measures can help mitigate the risks associated with decision-making errors, personal autonomy concerns, and robot accountability. Deploying service robotics that are reliable enough to operate as intended alongside humans in collaborative settings is essential for safe and secure service robotic systems. Embracing service robotics presents both social and technical challenges, as cybersecurity breaches can seriously damage public trust (Floridi et al., 2018b).

This subsection draws from the Value Sensitive Design (VSD) framework to highlight the importance of integrating human values into both the ethical and cybersecurity dimensions of robotic systems design. VSD supports a proactive approach to integrating moral and social values, such as privacy, fairness, and safety, into technology development (Batya & David, 2019). Integration takes place through three types of investigation: conceptual, empirical, and technical. When applied to the systems that guide the behaviour of service robotics, VSD promotes a balance between technical abilities and normative considerations.

Figure 2.5 presents a cyclical, governance-oriented process for addressing risk, safety, and ethical challenges in service robotic systems by linking risk identification, best-practice formulation, and ethical promotion within the service industry.

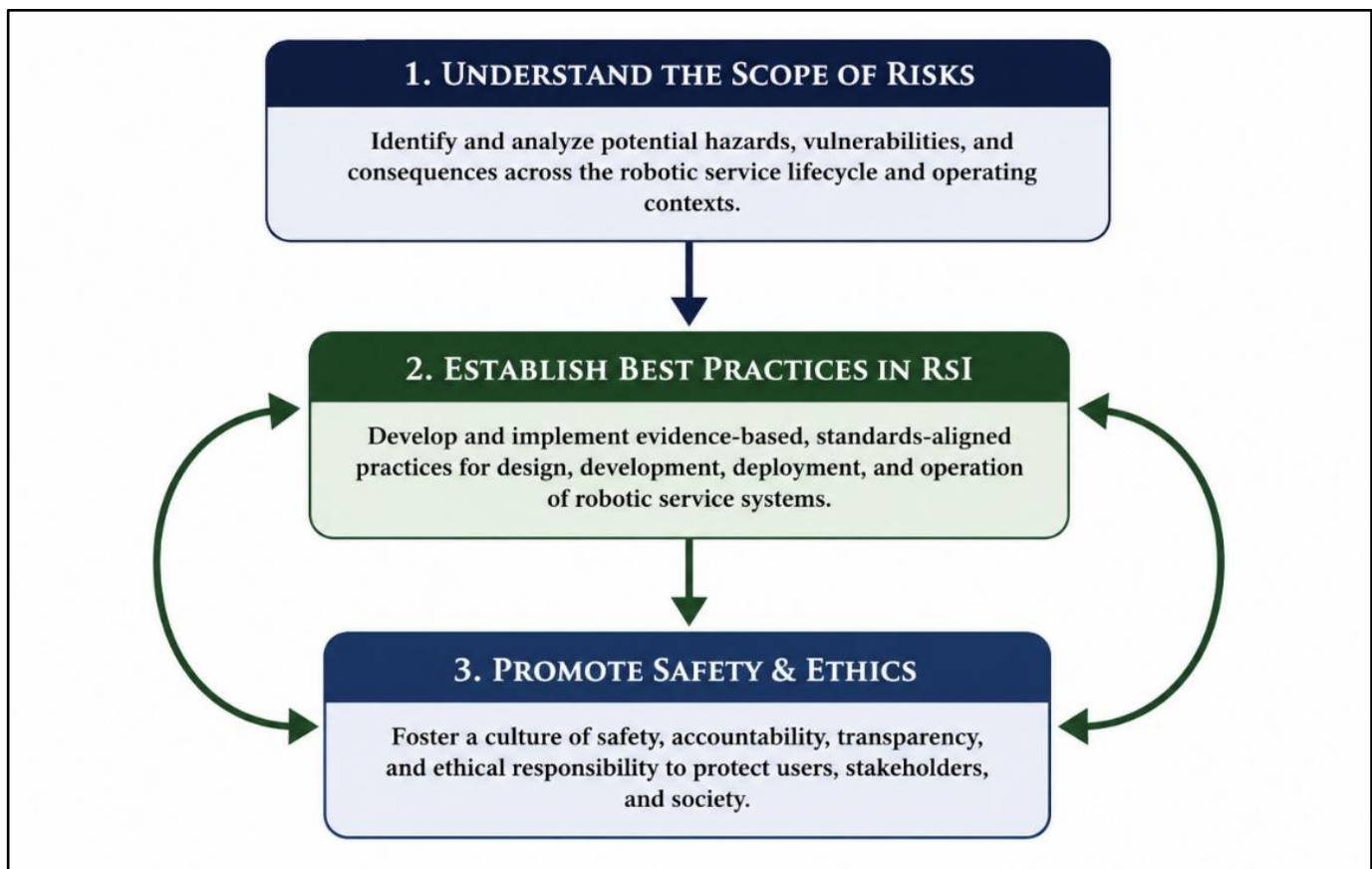


Figure 2.4: Understanding Risk and Promoting Safety and Ethics
(Synthesised by author)

Figure 2.5 illustrates an iterative, continuous process for managing risk, upholding best practices, and advancing safety and ethical outcomes. It shows a cyclical model for integrating ethics and cybersecurity into the RSI. The model begins with the foundation of risk assessment and leads to understanding the ethical and cybersecurity dimensions, defining best practices, and promoting safety and ethics. Different ethical and operational contexts may require different interpretations of best practices in RSI.

The model is deliberately cyclical. Promoting safety and ethics generates feedback that informs risk assessments and practice refinement. This iterative process reflects the VSD principle of continual evaluation, adaptation, and stakeholder engagement throughout a technology's life cycle (Batya & David, 2019). The diagram captures the incessant dynamics of threats and values in real-world robotic service environments requiring vigilance and adaptation.

By placing ethics and cybersecurity in a tight, mutually reinforcing relationship, and through the clear lens of VSD, service robotics can evolve in ways that protect human dignity, uphold societal trust, and mitigate both moral and technological risk.

2.8 Theoretical Framework

This section establishes the theoretical foundation for examining the development of cyber-safe and ethical robots in the service industry. The authors rely on well-established ethical and cybersecurity frameworks to underpin the study, while considering relevant laws and regulations to draw conclusions regarding legality. Such frameworks include: Autonomous technology and the greater human good (Omohundro, 2014), Robotic Nudges (Borenstein & Arkin, 2016), Tripartite methodology and an expanded concept of stakeholder analysis (Batya & David, 2019), ISO/IEC 21827 (2008), SSE-CMM, IT-CMF, ISM2 PRISMA, and NIST-RMF (Malatji et al., 2019a).

2.8.1 Interdisciplinary Foundations

An interdisciplinary approach is required to develop safe and ethical robots (Ahlborg et al., 2019a). Principles from engineering, computer science, ethics, and law must be integrated to achieve this goal (Vanderelst & Winfield, 2018). The objective of the study is to assume a socio-technical perspective in looking at service robotics. The study acknowledges that these robots are being designed, developed, and deployed in a context that involves technological and social factors (Skubis, 2024).

2.8.2 Cybersecurity Frameworks

To address the cybersecurity problem in robotics, a solid risk management framework needs to be in place. The NIST Cybersecurity Framework (CSF) provides a valuable model for understanding and managing contextual risks associated with robotic systems (Möller, 2023). The CSF is built around five key areas of functionality: identify, protect, detect, respond, and recover. These functions offer a structured way to assess vulnerabilities, implement security controls, and ensure resilience against cyber threats. Furthermore, standards such as ISA/IEC (Ross et al., 2018), which provide guidelines for securing industrial automation and control systems, have relevance for robotic systems.

2.8.3 Ethical Frameworks

Designing and deploying service robotics demands thoughtful consideration of ethics (IEEE, 2019b). The “Ethically Aligned Design” (EAD) study draws on several key ethical frameworks.

Firstly, deontology provides a clear structure for setting straightforward ethical guidelines for robot behaviour, as it prioritises duties and rules (IEEE, 2019b). Secondly, utilitarianism, which aims to maximise well-being, can inform service robot design to benefit the most people (Cooke, 2020). Thirdly, virtue ethics, focusing on moral character, is also relevant (IEEE, 2019b). Furthermore, recent research on care ethics may help identify principles to guide tough moral decisions in care practices involving service robotics. Transparency is also a vital complement to these frameworks and principles, as ethical service robotics should not operate in secrecy. Instead, their behaviours should be as transparent and understandable as possible, a quality essential for trustworthy robots.

2.8.4 Legal and Regulatory Considerations

Historical analysis of AI and autonomous robotic systems development indicates that technological capabilities have advanced rapidly at a pace that precedes corresponding ethical governance and regulatory framework, a concern similarly articulated in the EAD framework (IEEE, 2019). The EU's AI Act and Cyber Resilience Act mark significant steps towards strengthening governance, accountability and cyber-safety requirements within AI-driven systems and the robotic landscape (Callari et al., 2024a; Ooi & Wilkinson, 2024). These regulations delve into complex discussions about liability and data governance, such as accountability when autonomous systems cause harm or make erroneous decisions, establishing transparency requirements for AI-driven decision-making, defining responsibilities for cyber-safety vulnerabilities, and regulating the collection, processing, storage, and sharing of personal data to ensure compliance with privacy and data protection principles.

Collectively, these regulatory instruments demonstrate substantial alignment with ethical principles set out in frameworks such as the EAD, particularly in transparency, accountability, human oversight, privacy protection, and responsible innovation in autonomous systems.

2.8.5 Ethics and Cybersecurity Integration Framework

The proposed framework employs the VSD framework, a robust tool for integrating ethical and cybersecurity principles into service robotics. VSD interprets technologies as being shaped by human values and consent ((Batya & David, 2019). At its core, VSD promotes a three-fold approach – conceptual, empirical and technical – that embeds stakeholder values such as privacy, trust, autonomy, and accountability into system design and deployment.

In service robotics, the VSD approach implies developing systems for HRI that are both ethically aligned and cybersecurity aligned 20 (Dutta & Zielińska, 2021). Applying VSD principles ensures that ethical values, human rights, privacy, and safety are integrated into the system throughout its lifecycle. This approach aligns system functionality with societal and individual ethical norms. VSD helps identify these risks early by involving stakeholders in reflective, anticipatory analysis, guiding design choices toward supporting human welfare, ensuring the integrity of the data robots handle, and strengthening the robots' resilience to cybersecurity threats (Sadek et al., 2023b).

The current study on the development of ethical and cyber-safe robotic systems seeks to comprehensively grasp the problems and opportunities presented in developing cyber-safe and ethical robotics for the service industry by integrating complementary theoretical perspectives. This integrative approach stems from the fact that service robotics operates at the intersection of technical autonomy, human values, and complex socio-organisational contexts, none of which can be adequately addressed through a single theoretical lens (see Figure 2.1). VSD provides the basis for incorporating human values and ethical considerations into system design. EAD provides normative guidance on accountability, transparency, and compliance with legal and regulatory expectations, while socio-technical systems theory (STS) enables an understanding of how technological systems interact with social structures, organisational practices, and contextual constraints. Drawing on these theoretical foundations, the present study advances a holistic understanding of how service robotics can be developed to safeguard human dignity, enhance trust and robust cyber-ethical compliance across diverse operational domains.

2.9 Conclusion

This chapter reviews contributions to cyber-safety, ethics, and HRI in service robotics. The review shows that although these domains have matured individually, existing studies continue to treat them largely as separate areas of inquiry, resulting in limited integration among ethical reasoning, cyber-safety requirements, and socio-technical governance considerations.

Collectively, the reviewed literature shows broad agreement that deploying service robotics offers significant opportunities alongside complex ethical and cyber-safety challenges. While some studies emphasise technological capabilities and operational efficiencies, others highlight concerns about privacy, accountability, transparency, and human autonomy. This suggests that ethical and cyber-safe service robotics cannot be addressed by isolated technical interventions alone but require integrated governance approaches that consider social, organisational, and technological dimensions simultaneously.

The reviewed literature reveals a rich conceptual ecosystem but lacks integration between ethical reasoning and cybersecurity architectures in applied service domains. While the literature offers valuable insights and guidelines, it lacks comprehensive, empirically validated frameworks for the dynamic and high-contact nature of RSI. This review identified fragmented approaches, insufficient empirical support, overlooked socio-technical aspects, and underutilised cross-disciplinary methodologies.

Key concepts include trust, autonomy, privacy, regulatory ambiguity, and human-centred design. However, implementing these values into operational robotic systems remains a significant challenge because service robotics function within socio-technical environments where technical autonomy, data-based decision-making, and human values often intersect. The studies reviewed show that ethical intentions are frequently articulated at a conceptual level but are inadequately incorporated in system architectures and governance mechanisms (Batya & David, 2019; IEEE, 2019b; Luciano, 2023). In response, the proposed ACERBOTICS framework will inform the methodology presented in Chapter 3, which aims to create a robust framework for integrating ethical and cyber-safety considerations into the design and governance of service robotics systems.

Chapter 3: Research Methodology and Design

3.1 Introduction

In Chapter 2, the absence of a comprehensive and empirically validated framework for the dynamic and high-contact nature of service robotic systems was recognised. Chapter 3 describes the research methodology employed to achieve the objectives of the study, which aims to develop a framework using the Design Science Research (DSR) process. The proposed framework will integrate the design criteria for ethical principles and cyber-safety measures in service robotic systems. The design criteria will be identified through an SLR, utilised during the problem identification phase of the DSR process. The DSR process involves the iterative development and evaluation of the proposed framework, including assessment by a panel of experts using a questionnaire.

This chapter details the research paradigm, design, expert panel participant selection, research instruments, data collection and analysis methods, as well as the ethical considerations and limitations.

The problem identification of the DSR process is informed by the design criteria and research gaps identified during the SLR. The current literature lacks an integrated framework for ethics and cyber-safety in robotics, has limited empirical validation, and exhibits minimal stakeholder engagement (see Appendix C). The sample techniques selected, sample size, and the reasons for choosing them are discussed in the sample design and sampling methods section. Each data instrument and its selection are explained and justified in the data collection section. This chapter also discusses the overall data collection and analysis process, including limitations and ethical considerations, and concludes with a summary.

3.2 Research Paradigm

The research paradigm “governs how we ask questions and conduct the research”, reflecting a set of beliefs, values and techniques that guide a researcher’s approach (Davies & Fisher, 2018).

This study uses a pragmatist research paradigm, emphasising action, practicality, applicability, usefulness, and problem-centred (Petersen & Gencel, 2013). This approach is most suitable for achieving the study’s objective, which aims to develop a robust framework that integrates ethical principles and cyber-safety measures in service robotic systems. It is appropriate for collecting objective evidence for statistical analysis, enhancing the credibility and reproducibility of research findings on the deployment of service robotics.

(Petersen & Gencel, 2013) emphasised that a pragmatist paradigm focuses on “using all approaches available” and seeking “what is practically useful”. This endorses research that may intervene in the world to understand or solve problems, not just observe. This study relies on observable, reproducible evidence, informed by expert-based insights, to guide the development of a cyber-safe and ethical framework for service robotics. A pragmatist research paradigm emphasises action outcomes derived from real-world practice and is problem-oriented, thereby informing the fundamental framework for a mixed-methods approach of this study.

3.3 Design Science Research

The DSR methodology used in this research followed the framework proposed by Peffers et al., (2007), which outlines six steps particularly suitable for solving real-world problems, including systematic design and evaluation of artefacts to address identified organisational and technological problems. DSR is particularly appropriate for this study because the ethical and cyber-safe deployment of service robotics presents a complex socio-technical challenge that requires the development of robust governance artefacts. The relevance of such an approach is reinforced by the growing deployment of service robotics in service environments and the need for frameworks to address both operational and governance concerns (Lu et al., 2020). Consistent with Hevner et al., (2008), this study employs iterative design, evaluation, and refinement processes to develop the ACERBOTICS Socio-Tactical Integrated framework.

The research follows DSR methodology, organised into the following iterative stages:

1. Problem Identification and Motivation: The research identifies limitations in existing frameworks and highlights the need for an integrated industry-specific framework as an improved solution.
2. Objective Definition: Objectives are defined to address identified gaps, including the development and validation of the proposed framework.
3. Design and Development: Iterative development of the framework based on insights from literature and expert feedback.
4. Demonstration: Use of the framework to assess its practical application and effectiveness.
5. Evaluation: The framework’s effectiveness is thoroughly gauged through expert feedback and literature-based metrics.
6. Communication: Findings are documented and communicated in alignment with academic standards.

3.4 Research instrumentation

Two primary research instruments are employed, namely:

3.4.1 PRISMA Guidelines for Systematic Review

This study employed an SLR as its primary research methodology. The review was guided by the PRISMA framework, which provides a structured and transparent approach for identifying, screening, assessing, and reporting relevant literature (Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, 2020). This choice was made to promote methodological transparency and academic rigour in identifying strengths, weaknesses, and areas for improvement in current methods for ethical and cyber-safe service robotics.

The SLR was carried out in four distinct steps as follows:

i. Identification of relevant literature

A comprehensive search strategy was developed using Boolean operators and relevant keyword combinations tailored to the research questions. Multiple academic databases, such as Scopus, Web of Science, IEEE Xplore, and Google Scholar, were systematically searched. The initial set of results was recorded, along with other critical details, including the database name, search terms used, date, and number of results returned, to ensure the search can be replicated.

ii. Screening records

Mendeley desktop reference management software was used to eliminate duplicate records. The remaining titles and abstracts were then screened against the predefined inclusion and exclusion criteria, with a primary focus on publication type, date, language, and thematic relevance.

iii. Eligibility criteria

The full texts of potentially relevant studies were reviewed. Selection was based on both thematic relevance and methodological quality, both of which are equally important. Studies that did not meet the required quality standards were excluded. This includes some studies that were casually dismissed as not very helpful but still potentially relevant, such as those that only mentioned certain aspects. Ultimately, the reason for including a study is to ensure methodological clarity.

iv. Inclusion

The synthesis of literature included only the final and relevant studies. For the relevant studies, the necessary data were extracted using a standard coding protocol that ensured consistency and

quality in the data collection process. The protocol not only recorded basic descriptive variables, such as authorship and publication year, but also necessitated the extraction of the study design, sample size, and various other variables considered necessary for theoretical or practical reasons. Quality appraisals were conducted where applicable using the Implementation Research Logic Model (Smith et al., 2020) to guide the evaluation process, ensuring a thorough assessment of existing studies.

This systematic review focused on the following themes, providing insights that inform the design of the framework and the development of the expert questionnaire:

- Ethical Frameworks for Robotic Systems Deployment
- Cyber-safety Vulnerabilities in RSI
- HRI Principles in the Service Industry
- Legal and Regulatory Standards
- Cyber-safe and Ethical Integrated Frameworks

A flowchart based on Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines is used to illustrate the inclusion process and transparently show how studies were selected for the review. The review employed a method that ensures the study selection is conducted in a methodologically consistent manner. The PRISMA process provided a reliable method for synthesising evidence on the topic of interest.

3.4.2 Expert Questionnaire

A structured online questionnaire survey hosted on Google Forms was designed to solicit expert feedback on the proposed framework (see Appendix L). The questionnaire evaluated:

- Relevance and comprehensiveness of the framework.
- Practical applicability
- Ease of implementation.
- Alignment with contemporary challenges in robotics and automation.

3.4.3 Evaluation Criteria

The following dimensions were considered when completing the questionnaire:

1. **Relevance** - Does the framework address real and pressing challenges in RSI?
2. **Clarity** - Are the framework's concepts and structure clearly articulated?

3. **Applicability** - Can the framework be applied in real-world service domains?
4. **Completeness** - Are any important components, threats, or values missing?
5. **Ethical Soundness** - Are ethical risks and governance properly integrated?
6. **Cybersecurity Readiness** - Are data safety and system integrity effectively addressed?
7. **Socio-Technical Integration** - Does it consider human values, culture, and industry needs?
8. **Practicality** - Is the framework feasible to implement or adapt by practitioners?
9. **Coherence**: Do the components form a cohesive whole?
10. **Coverage**: Are all critical aspects (cybersecurity, ethics, socio-technical integration, local context) addressed?
11. **Usefulness**: Would this structure be actionable for designing or governing service robotics?

3.5 Data Collection Method

3.5.1 Expert Evaluation Questionnaire for a proposed ACERBOTICS Framework

A structured online questionnaire hosted on Google Forms was designed to gather expert feedback on the proposed framework (see Appendix L). These questions aim to assess the relevance, coherence, usability, and contextual sensitivity of the framework across its key dimensions, namely the ethical, cyber-safety, and socio-technical aspects. All evaluation data collected from the experts will be securely and responsibly stored on an encrypted, access-controlled institutional repository, and managed within Google Forms. Access will be restricted to the researcher and the supervisory panel, and data will be retained in accordance with the institution's ethical research policy.

The online Google Forms for data collection were sent electronically to the selected experts. This method offered both accessibility and ease of use for the invited experts. This questionnaire is anonymous (see Appendix L). The link was distributed to experts via email and social media platforms. A snowballing technique was also used in distributing the survey. Responses were captured and stored securely on Google Forms, ready for the next step in analysis.

3.5.2 Mixed-method approach

A mixed-methods approach involves the systematic integration of:

- **Quantitative methods** (e.g., experiments, surveys, statistical analysis) to measure variables, test hypotheses, and identify patterns or relationships. Quantitative data is collected using closed-ended survey questions, and responses are assessed using Likert scales, which allows for the statistical analysis of expert viewpoints.
- **Qualitative methods** (e.g., interviews, focus groups, observations) to explore participants' experiences, meanings, and perspectives in depth. Qualitative data collection elicits detailed responses from nuanced and experienced respondents, which are thematically analysed to reveal patterns of meaning and recommendations.

Mixed-methods research combines quantitative and qualitative data in a single study to provide a comprehensive understanding (Creswell and Plano Clark 2018, p. 6). Its strength lies in linking numerical patterns with context, yielding more detailed and reliable conclusions than either method alone. Insights from the literature review, guided by the PRISMA framework, inform the development of the expert questionnaire and serve as a baseline for evaluating expert responses. Expert feedback is used to validate and refine the proposed framework in an iterative process. The transparency of the methodology is ensured by thoroughly documenting the PRISMA process, including the inclusion and exclusion criteria and final study selection. The questionnaire is organised clearly to align with the research objectives and questions. All data collected is securely and responsibly stored and managed in Google Forms.

This data collection method, which is both transparent and systematic, enabled the combination of qualitative and quantitative insights with sufficient rigour and reliability, thereby producing a robust unified framework for RSI deployment.

3.5.3 Purpose of Using a Mixed-Methods Approach

- To triangulate findings: confirm or cross-validate results from different data sources.
- To complement one method with another: e.g., using qualitative data to explain surprising quantitative results.
- To develop instruments: use qualitative findings to design a questionnaire.
- To expand the breadth and depth of the study.

3.5.4 Qualitative data

The initial step in data collection involved an SLR guided by the PRISMA guidelines. These provided a clear, structured, and transparent approach to identifying studies relevant to the

research questions, ensuring a thorough exploration of cyber-safety vulnerabilities, ethical concerns, and HRI challenges in the RSI.

The SLR process involved the following steps:

1. Defining Research Questions and Objectives:

The literature review focused on addressing the key research objectives, including

- Investigate cyber-safety vulnerabilities in networked robotics systems
- Identify specific ethical standards issues associated with RSI.
- Develop a framework for deploying service robotics that integrates cyber-safety risk mitigations and ethical considerations.

2. Database Search:

The following academic databases were used to conduct searches to ensure literature credibility and reliability:

- Scopus
- ACM digital library
- IEEE Xplore
- Google Scholar

The keywords comprised various combinations of terms, including cyber-safety challenges in robotics, robot ethics, human-robot interaction, service robotics, robotics vulnerabilities, ethical standards in robotics, and cyber-safe and ethical frameworks in robotics.

3. Screening Process

This phase involved selecting studies that were highly relevant and methodologically sound, using inclusion and exclusion criteria. The initial screening was carried out by reviewing the titles and abstracts of the retrieved records, followed by a full-text assessment.

Inclusion criteria were defined to select studies that:

- Addressed ethical principles and concerns in the service industry HRI.
- Provided cyber threats, vulnerabilities, risk management, and mitigation strategies in service robotics
- Explored privacy, trust, data ethics, user acceptance and ethical concerns in HRI.

- Identified legal frameworks, governance on ethical and cyber-safe robotics in HRI, and discuss global and regional regulatory differences.
- Incorporated cyber-safety and ethical frameworks in the context of HRI.
- Were published in the English language between 2018 and 2025.
- Were conference papers, peer-reviewed journal articles, reputable case studies, and scholarly theses.
- Provided conceptual frameworks or theoretical models.

Exclusion criteria were defined to filter out studies that:

- Focused on non-service sectors or unrelated ethical frameworks
- Addressed cyber-safety issues, risk management, and design unrelated to the service industry and robotics.
- Focused on industrial robots without relating to service industry applications and limited to mechanical or technical aspects without HRI.
- Were unrelated to ethical or cyber-safe compliance
- Focused on neither HRI nor were unrelated to HRI and service domains

4. PRISMA Flowchart

To ensure the transparency and reproducibility of the literature selection process, the search results are documented in a PRISMA flow diagram. The review process, as depicted in the flow diagram, involves four stages:

- Identification - obtaining initial papers from databases with the use of search terms or a combination of terms.
- Screening - eliminating duplicates and irrelevant or unrelated studies.
- Eligibility - determination of relevant and suitable studies by a full-text review.
- Inclusion - ultimately choosing a collection of research for an in-depth qualitative analysis.

5. Data Extraction and Thematic Analysis

Data were extracted from the selected studies. The extraction process was done systematically using a structured template. The template included the following: themes, inclusion criteria, exclusion criteria, study title, authorship and publication year, paper type, country of study, study

aims/focus, key findings, relevance to cyber-safe robotics, relevance to ethical robotics, relevance to the service domain, and limitations of the study.

The data extracted were thematically analysed. This analysis informed the framework and expert questionnaire.

3.5.5 Quantitative Data

This step involved collecting data from experts using a questionnaire that yielded both quantitative and qualitative data. The data collection tool was sent electronically via Google Forms, a method that offered both accessibility and ease of use for the invited experts. This questionnaire was anonymous and in the form of a survey. The link was distributed to experts via email and social media platforms. A snowballing technique was also used in distributing the survey. Responses were captured and stored safely on Google Forms, ready for the next step in the analysis. This questionnaire ensured that both the research questions and objectives aligned with the quantitative insights gathered from the participants.

3.6 Participants

This study employed purposive sampling to select participants who are experts in the field, ensuring their qualifications and experience align with the research objectives. Experts were chosen based on their:

- Educational and professional credentials in robotics, ethics, cyber-safety or HRI.
- Experience in robotics, automation, service robotic system integration, or a related field.
- Familiarity with design frameworks and evaluation methodologies.

The participants, representing diverse backgrounds in academia, industry, and policy-making, provided critical insights to evaluate the framework's applicability, effectiveness, and relevance.

3.6.1 Criteria for Participant Selection

Participants were recruited using a purposive sampling strategy to ensure that individuals possess relevant expertise in cybersecurity, robotics, AI, ethics, governance, and service robotics (see Section 6.2.2). Recruitment was undertaken through professional organisations to ensure a multidisciplinary perspective, which included the Institute of Information Technology Professionals South Africa (IITPSA), IITPSA Special Interest Group for AI and Robotics (SIGAIR), cybersecurity, AI, and robotics communities on LinkedIn, and academic communities, including the Department of ICT, University of Mpumalanga, and IT Faculty, Eduvos. Snowball

sampling was subsequently employed to encourage eligible participants to share the questionnaire link within their professional communities, thereby broadening participation while maintaining the predefined inclusion criteria. Inclusion criteria required a significant level of professional engagement in IT, robotics, cybersecurity, AI, ethics, and governance, ensuring that responses reflected substantial domain expertise.

3.7 Data Analysis

Data analysis was conducted in three stages:

1. Quantitative Analysis:

Quantitative responses from the expert questionnaire were analysed using descriptive and inferential statistics to identify trends, patterns, and correlations. Metrics such as mean scores, frequencies, percentages and standard deviation (SD) were used.

2. Qualitative Analysis

Thematic analysis was used to analyse the qualitative data and extract nuanced insights. Common themes, patterns, and expert recommendations were identified and categorised. Thematic analysis is generally the most common qualitative method for analysing data. It involves classifying, analysing, and reporting patterns within the data (Ferri et al., 2020). The open-ended responses were analysed thematically, providing a clear description of respondents' opinions. Identifying patterns in the data was crucial for making informative findings. This analysis enriched the iterative refinement of the proposed framework.

3. Synthesis of Findings

The literature review and expert feedback results were synthesised to refine the proposed framework iteratively.

3.8 Ethical Considerations

This study followed ethical guidelines for both human and non-human subjects. It was necessary to obtain approval for research involving human subjects and to examine sensitive issues, such as beliefs. The data provided by the human participants was not only needed to answer the research questions but also could only be ethically collected after specific ethical guidelines were satisfied. The collection of data from human participants for the study required compliance. These measures ensure that the research involving human participants is conducted responsibly.

- Human Ethical Clearance:

Ethical clearance (Ref. #: 8827) was obtained from the Research Ethics Review Committee of the College of Science, Engineering and Technology (see Appendix M), Unisa. Participants were provided with informed consent forms that detail the purpose of the study, their role, and rights. Anonymity and confidentiality were ensured.

- Non-human Ethical Clearance:

Ethical considerations related to the use of robotic systems and automation were addressed. The proposed framework was developed to promote sustainable and responsible use of robotic technology. Adhering to the standards set by the Robotics and Automation Society of the Institute of Electrical and Electronics Engineers (IEEE) (Gonzalez-Aguirre et al., 2021), ensuring that the framework being developed will lead to robotic systems that operate in a responsible, sustainable, and unbiased manner.

3.9 Summary

This chapter outlines the methodological foundation for developing a cyber-safe and ethical service robotics framework. The study employed the DSR approach, which offers a structured, iterative process for creating and validating artefacts. DSR comprises six core phases, from problem identification to results communication. The qualitative exploratory approach of the study justifies the use of DSR. It describes how an SLR and expert validations, guided by PRISMA, complement each other. The iterative artefacts refinement ensures adaptability to stakeholders' needs and technological changes.

Instrumentation strategies, including coding protocols and data collection tools, were outlined to ensure replicability. The framework development was supported by qualitative analysis methods, such as thematic abstraction and conceptual modelling. Ethical safeguards, limitations, and validation strategies were also discussed to uphold integrity and trustworthiness.

In conclusion, this chapter presents a clear and structured approach to developing a robust, practical, and ethically sound framework that encourages cyber-safe and ethical decision-making in the development and deployment of service robotic systems. The next chapter details the SLR process, results, findings, and analysis based on this methodology.

Chapter 4: Systematic Literature Review

4.1 Introduction

The growing use of service robotics in sectors such as healthcare, hospitality, education, and tourism has raised concerns about ethical governance and cyber-safety. As the autonomy of service robotics increases and HRI becomes more common (Lu et al., 2020a), there is a growing need for a comprehensive framework to ensure ethical compliance and defend against cyber threats. This chapter presents an SLR to analyse current research, identify thematic gaps, and establish the design criteria for the development of the proposed research artefact, which is presented in the next chapter.

The aim of the SLR is to provide a structured, transparent, and reproducible method for synthesising existing studies focused on the specific research themes (see 4.5) and the identification of the design criteria for the proposed framework to address the research questions. This chapter also presents the results and findings of the SLR. The steps of the research methodology are outlined in Chapter 3, Sections 3.3 and 3.4. The aim of the SLR is to identify and understand relevant, high-quality, and reliable studies that can inform the research questions addressed in this study.

4.2 Critical Analysis of Existing Literature

This chapter critically reviews the relevant literature to identify the design criteria that should be included in the proposed research framework. A thematic synthesis approach was adopted, which led to the organisation of the literature around key ideas, theories, and methodologies to create a coherent narrative. This review followed the coding technique used by (Lu et al., 2020a) during their literature review.

The literature search and synthesis adopted was based on the Implementation Research Logic Model (IRLM), (Smith et al., 2020). A summary of the literature most relevant to the research question is presented, articulating the central theme, scope, and purpose. Key concepts were defined in the analysis. The differences and interpretations impact the compatibility and synthesis of research results, and the theoretical approaches, perspectives, and methods used in the literature are reviewed. This technique is centred on the principles adopted by (Lu et al., 2020a). The technique methodologically provides an overview of the extent to which the studies utilise existing frameworks or develop independent approaches, and how effectively these theoretical frameworks align with the research question and impact the findings.

The image in Figure 4.1 depicts a cyclical process for synthesising literature, emphasising the iterative evaluation, analysis, critical review, and development of an argument to justify contributions to the field. PRISMA mainly addresses the reporting requirements and methodological transparency of SLR, including search strategy, inclusion and exclusion criteria, and data extraction. Fig. 4.1 highlights the stages that follow the PRISMA process, specifically in research idea refinement, alignment with relevant theoretical frameworks such as the IRLM, and development of scholarly contributions.

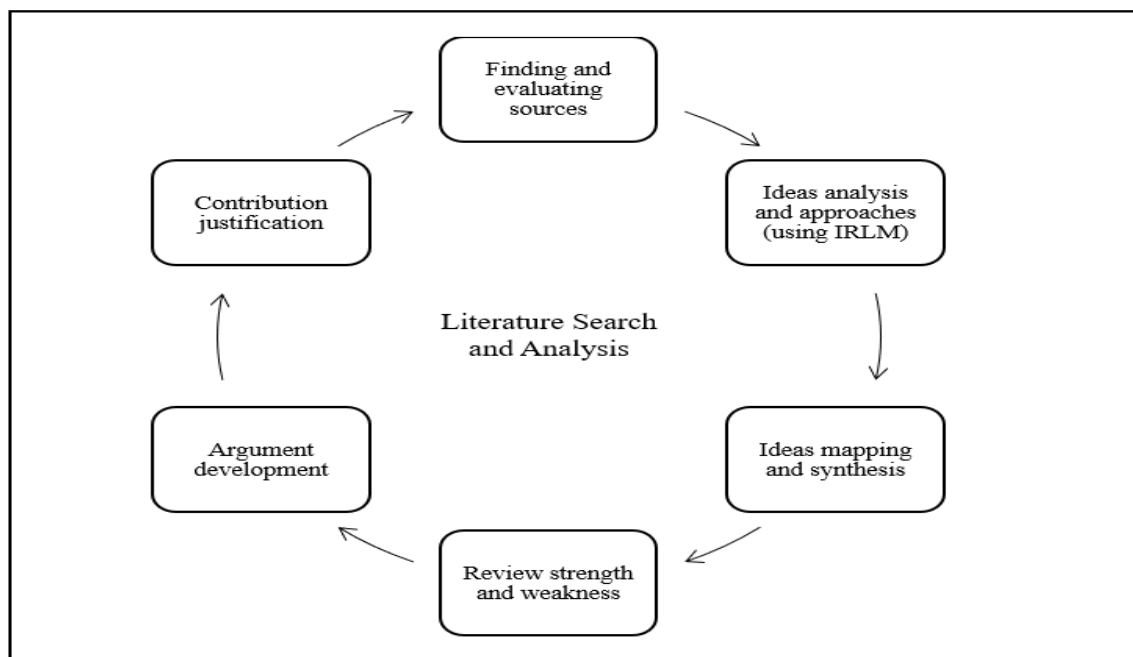


Figure 4.1 Conceptual Development Cycle in SLRs (Synthesised by author)

In Figure 4.1 a conceptual, cyclical process for synthesising literature is presented. This cycle involves iterative evaluation, analysis, critical review, and the development of an argument to justify contributions. It also highlights stages after PRISMA, such as refining research ideas, aligning with frameworks like IRLM, and advancing scholarly contributions.

The results and conclusions of each selected study were synthesised as they relate to the guiding logical structure of the SLR as presented in Chapter 4. Patterns, trends and contradictions in the literature were reviewed to determine consistent areas that may be convergent or divergent. Furthermore, the strengths and limitations of each study were critically evaluated, including the validity of the methods, the clarity of the rationale, and the logical consistency of the conclusions.

The review identified gaps in the literature, including what is missing, what remains unanswered, and what requires further research, thereby providing a foundation for the subsequent development of the proposed framework in Chapter 5.

4.3 Methodology Overview

The SLR process follows the PRISMA 2020 framework (Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, 2020) to ensure methodological rigour. Searches were performed across Google Scholar, Scopus, IEEE Xplore, and ACN databases because these databases provide high impact and comprehensive coverage of peer-reviewed studies in robotics cybersecurity, ethical design, and artificial intelligence. Publications from 2018 to 2025 were included to ensure the review captures the latest developments in service robotics and emerging governance models, keeping pace with the rapid progress of AI-driven technologies, autonomous systems, and algorithmic governance.

The total number of studies selected after applying the inclusion and exclusion criteria and full-text screening was 35. To structure the findings synthesis, the analytical approach proposed by (Lu et al., 2020a) was adopted to map the research domains, identify thematic clusters and highlight knowledge gaps in service robotics. Additionally, the IRLM provided a structured framework for planning, extracting, synthesising and aligning the results and conclusions of the reviewed studies with the underlying logic of implementation research. By combining these approaches, the SLR ensured both a domain-specific mapping of service robotics research and a systematic, logic-driven synthesis, allowing findings to be integrated coherently into the SLR extraction matrix. This demonstrates the multifaceted issues and existing gaps in the development and deployment of robotic systems in the service industry. A rigorous process involved the following:

4.3.1 Search Strategy

The review employed a systematic search strategy across multiple academic databases, including Scopus, ACM, IEEE Xplore, and Google Scholar. To ensure a comprehensive coverage of the literature, searches were conducted using Boolean operators and tailored combinations of keywords derived from the research questions, as shown in Table 4.1.

Table 4.1 Search Terms and Boolean Operators (Synthesised by author)

	Theme	Search Terms
Theme 1	Ethical Frameworks for Robotic Systems Deployment	(Ethics) OR (ethical principles) OR (ethical guidelines) OR (ethical framework) AND (service (robots) OR (service industry robotic systems))
Theme 2	Cyber-safety vulnerabilities in RSI	(Cybersecurity) OR (cybersecurity risks) OR (cyber safety) OR (cyber threats) AND (challenges) OR data protection) AND (robotic service industry) OR (service robotics)
Theme 3	Human-robot interaction (HRI) principles in the service industry	(Human-robot interaction) AND (principles) OR (framework) OR (governance) OR (Model)s AND (service robotics)
Theme 4	Legal and Regulatory Standards	(Service robotics) OR (healthcare) OR (hospitality) OR (tourism) OR (retail) OR (education) AND (legal) OR (regulatory) OR (governance) AND (models) OR (framework)
Theme 5	Cyber-Ethical Integrated Frameworks	(Cyber) AND (ethics) AND (integration) OR (cybersecurity) AND (ethical) AND (integration)AND (service) AND (robots) OR (service) AND (industry) AND (robotic) AND (systems) AND (framework) OR (guidelines) OR (principles)

Table 4.1 presents the five themes considered in the SLR. The synthesis of these themes assisted in the identification of the design criteria.

4.3.2 Inclusion and Exclusion Criteria

Studies included met the following criteria:

- Published in the English language
 - Provided theoretical or empirical contributions relevant to ethics and cyber-safety of the service robot domain
- Published in peer-reviewed academic journals, conference proceedings, and theses between 2018 and 2025.

Exclusion criteria included:

- Grey literature such as non-peer-reviewed papers, web articles, news articles, and blogs
- Studies that lack a thorough research methodology
- Studies that focus on the technical, mechanical, or design features of robotic systems without reference to ethics or HRI dimensions.
- Papers on non-service domain robotic systems or industrial robots
- Papers with no underlying objectives of ethics or cyber-safety models discussions.

Table 4.2 presents the inclusion and exclusion criteria that are considered in the SLR. These criteria guided the selection of articles within the SLR.

Table 4.2 Inclusion and Exclusion criteria (Synthesised by author)

Inclusion	Exclusion
Studies on ethical principles in robotics: autonomy, transparency, and accountability. Studies that address ethical concerns in HRI	Studies that focus on non-service sectors or unrelated ethical frameworks
Studies on cyber threats, vulnerabilities, risk management, and mitigation strategies in service robotics	Studies addressing cyber-safety issues, risk management, and design unrelated to the service industry and robotics.
Studies that explore privacy, trust, data ethics, user acceptance and ethical concerns in HRI.	Studies on industrial robots with no correlation to service industry applications

Table 4.2 Inclusion and Exclusion criteria (Synthesised by author)

Inclusion	Exclusion
	and limited to mechanical or technical aspects without HRI.
Studies on legal frameworks, governance of ethical and cyber-safe robotics in HRI, and discussing global and regional regulatory differences.	Studies unrelated to ethical or cyber-safe compliance.
Studies that incorporate cyber-safety and ethical frameworks in the context of HRI.	Studies that focus on either or are unrelated to HRI and service domains.

Table 4.2 presents the inclusion and exclusion criteria that were applied. The impact of these criteria is quantified in the PRISMA diagram (Figure 4.2).

4.4 Screening and Selection Process

Phase 1: Literature Identification and Preliminary Filtering

The initial database search yielded 118578 records across Scopus, ACM, Google Scholar, and IEEE Xplore. Following the PRISMA 2020 guidelines (Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, 2020). Duplicate records, non-peer-reviewed sources, poorly aligned studies, and records identified as ineligible through automated filtering tools were removed using Rayyan.ai and EndNote. The process eliminated 118297 records, leaving 281 records for title and abstract screening.

Phase 2: Title and Abstract Full-text assessment – conducted over 7 weeks, the remaining 281 records were manually screened for relevance to cyber-safety, ethical HRI, and socio-technical integration in the robotics service domain. After applying predefined inclusion/exclusion criteria, 35 studies met the eligibility requirements and were retained for the final review. The eligibility assessment focuses on methodological rigour, relevance to the research objectives, and contribution to the development of the proposed framework.

Phase 3: The final set of 35 studies formed the evidence base for the thematic synthesis and for deriving the design criteria used to develop the proposed framework. Screening was conducted

systematically, with detailed logs maintained to ensure traceability and transparency. The final selection comprised 35 scholarly papers. The screening process adhered to the PRISMA 2020 guidelines. The full-text eligibility assessment evaluated the methodological rigour, relevance and contextual alignment of each study with the research objectives.

In this phase, studies were excluded if:

1. The focus was not primarily on cyber-safety, ethical or service robotics domains.
2. Not the most recent work; that is, from 2018 to 2025.
3. They were duplicate or non-peer-reviewed publications.
4. They did not provide theoretical or conceptual insights applicable to the proposed development framework.

The final selected 35 studies met the inclusion criteria across the three main areas of cyber-safety, ethical, and service robotic systems, and offered a substantial methodological contribution relevant to the identification of the design criteria used in the development of the proposed framework (outlined in Chapter 5).

Figure 4.2 presents the PRISMA diagram of the phases of the SLR selection, exclusion and identification processes.

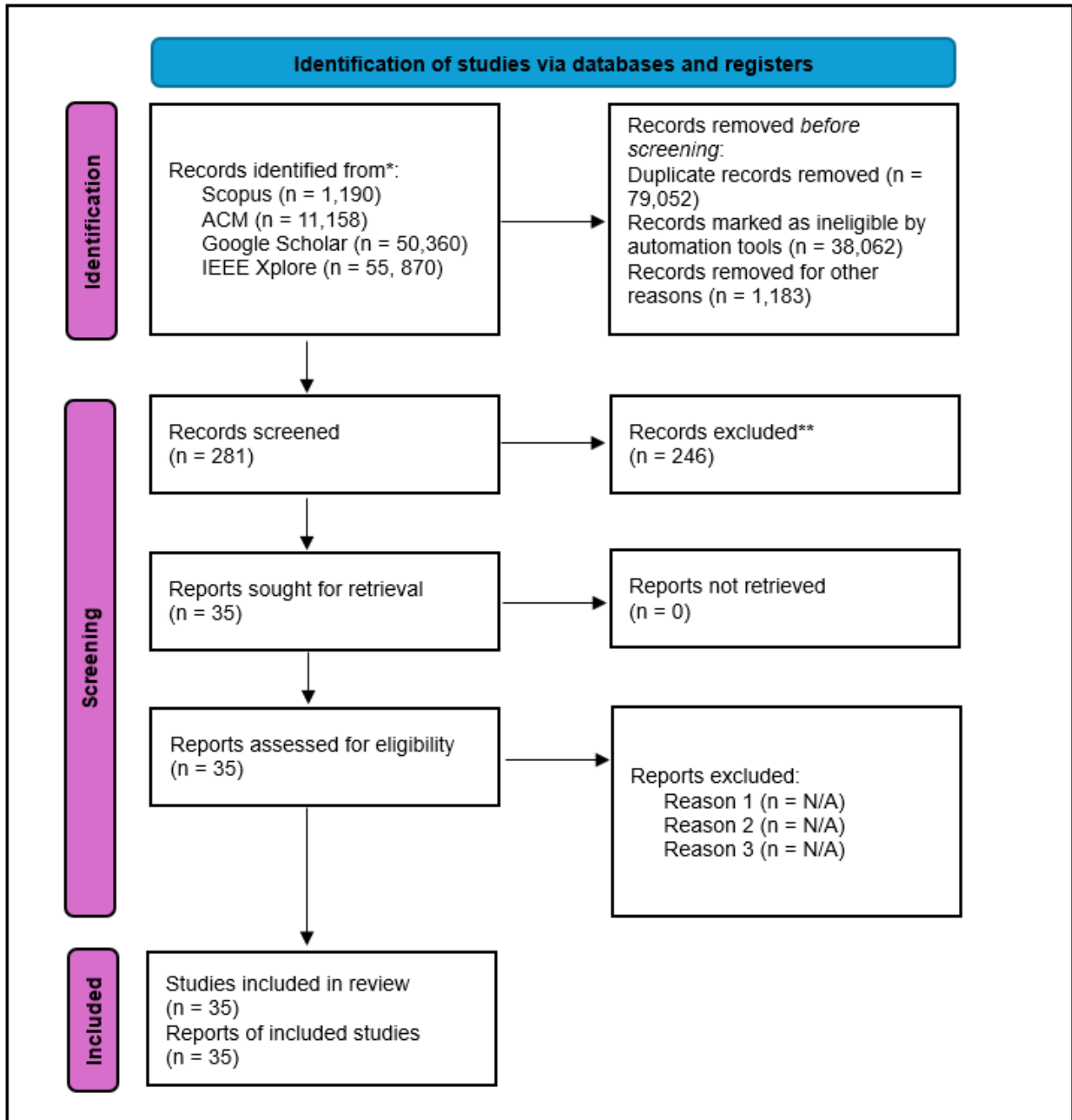


Figure 4.2 PRISMA 2020 Flow Diagram

Figure 4.2 illustrates each stage of the SLR process, namely the identification, screening, eligibility, and inclusion of the articles. The number of articles in each phase of the process is shown. The PRISMA diagram shows how records (the relevant articles) were identified across four databases (namely Scopus, ACM, IEEE Xplore, and Google Scholar), then screened and filtered. This process is based on inclusion and exclusion criteria (as presented in Table 4.2), resulting in 35 studies for final review.

Appendix N presents a summary of the articles selected, presented in terms of paper type, country of study, research aim/focus, methodology, key findings, relevance to cyber-safe robotics, relevance to ethical robotics, service industry domain, and limitations.

In Appendix N, all selected articles are presented and summarised in terms of the attributes of methodology, thematic coverage gap, geographic distribution, socio-technical architectural gap, technological bias, overlooking HRI socio-dynamics, and framework development relevance. Note that the attributes are summarised and presented graphically in the following figures.

To guide the interpretation of the selected articles, the following graphics have been collated:

- Figure 4.3 shows relevance to Key Robotic Domains
- Figure 4.4 shows the geographic distribution of the reviewed studies
- Figure 4.5 highlights the socio-technical integration gaps across different study types
- Table 4.4 presents a summary of the identified design criteria.

4.5 Critical Review of Literature on Ethical and Cyber-safe Service Robotic Systems

The reviewed literature covers five main themes: cyber-safety framework, cyber-safety challenges, ethical frameworks, HRI, legal and regulatory frameworks, and integrated cyber-ethical frameworks (see Table 4.3).

As shown in Figure 4.3, the distribution of reviewed studies across key domains demonstrates how the literature varies in its relevance to cyber-safe robotics, ethical robotics, service robotics, and overall framework development.

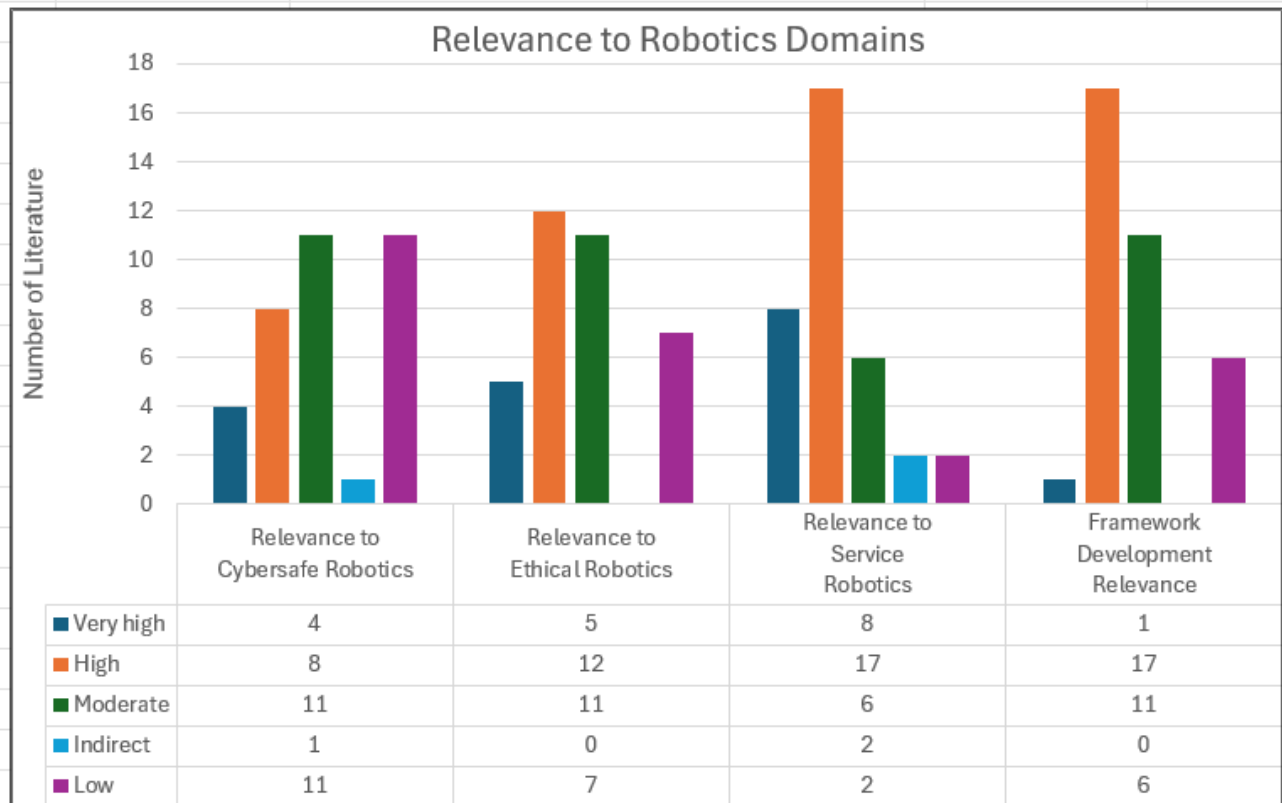


Figure 4.3 Relevance to Key Robotic Domains (Synthesised by author)

Figure 4.3 presents a bar chart summary of the selected articles (N = 35) that illustrate the four coded key areas of the robotics domain: cyber-safe robotics, ethical robotics, service, and framework development, which are categorised into five levels (very high, high, moderate, indirect, and low) of relevance.

These five levels were identified through a structured content analysis of 35 studies, using the qualitative coding technique principles adopted from (Creswell & Creswell, 2018; Saldaña, 2017) to help systematically sort the thematic relevance of the studies. The assessment was based on three main criteria: how much the study focused on the domain (cyber-safety, ethics, service robotics, framework development relevance), and how clearly the application or empirical basis was explained.

- Very High – The study covers the domain directly and thoroughly, with clear methods and theory.
- High – The domain is the focus, but the study does not fully integrate or validate it with data.
- Moderate – The study mentions the domain only in part, often as a secondary focus.

- Indirect – The study discusses the domain in general terms, without a clear focus or much detail.
- Low – The study barely mentions the domain, if at all, and only in passing.

The studies focusing on ethical (31%) and service-related robotics (29%) are more prominent, as shown in the SLR thematic analysis (see Appendix F). This predominance reflects the broader research and policy emphasis on responsible deployment, HRI ethics, and operational efficiency within service contexts, rather than on the technical underpinnings of cyber-safety. See Appendix E for the distribution of study relevance across the cyber-safety, ethical, and service robotics domains. This distribution analysis, derived from the SLR matrix, contrasts with the lesser focus on cyber-safety aspects (17%), where studies tend to address only isolated security mechanisms rather than integrated cyber-ethical safeguards. This imbalance highlights the need for a robust, integrative approach that combines ethical governance, cyber-resilience, and socio-technical adaptability to ensure holistic and context-aware deployment of service robotic systems.

In Figure 4.3 (The Relevance to Key Robotic Domains) the ratings in terms of “Very High”, “High”, “Moderate”, “Indirect”, and “Low” indicate that ethical robotics (31% of all reviewed articles) and service industry relevance (29% of all reviewed articles) account for the majority of the reviewed literature. These quantities suggest an emphasis on research domains exploring moral reasoning, trust, and user acceptance in service robotics applications. Cyber-safety concerns comprise 17% of all reviewed articles. HRI accounts for 14% of all reviewed articles, and cyber-ethical integration represents 9% of all reviewed articles (see Appendix F for detailed article classification and thematic coding process).

This distribution shows that ethical and service-relevance themes dominate, with a significant underrepresentation of integrated cyber-ethical and socio-technical frameworks, all of which are critical for the safe, ethical, and effective deployment of service robotics. These findings inform the development of a framework to integrate cybersecurity, cyber-resilience, ethical governance, and socio-tactical adaptability to guide the safe, context-aware deployment of robotics systems within the service industry. This is done by highlighting underexplored intersections, specifically cyber-ethical integration and socio-technical adaptation. These insights led to the incorporation of cyber-resilience and ethical safeguards as foundational pillars within the framework.

4.6 Geographic Distribution of Reviewed Studies

The pie chart in Figure 4.4 shows the geographic distribution of studies reviewed, highlighting contributions centred on Africa (see Appendix A).

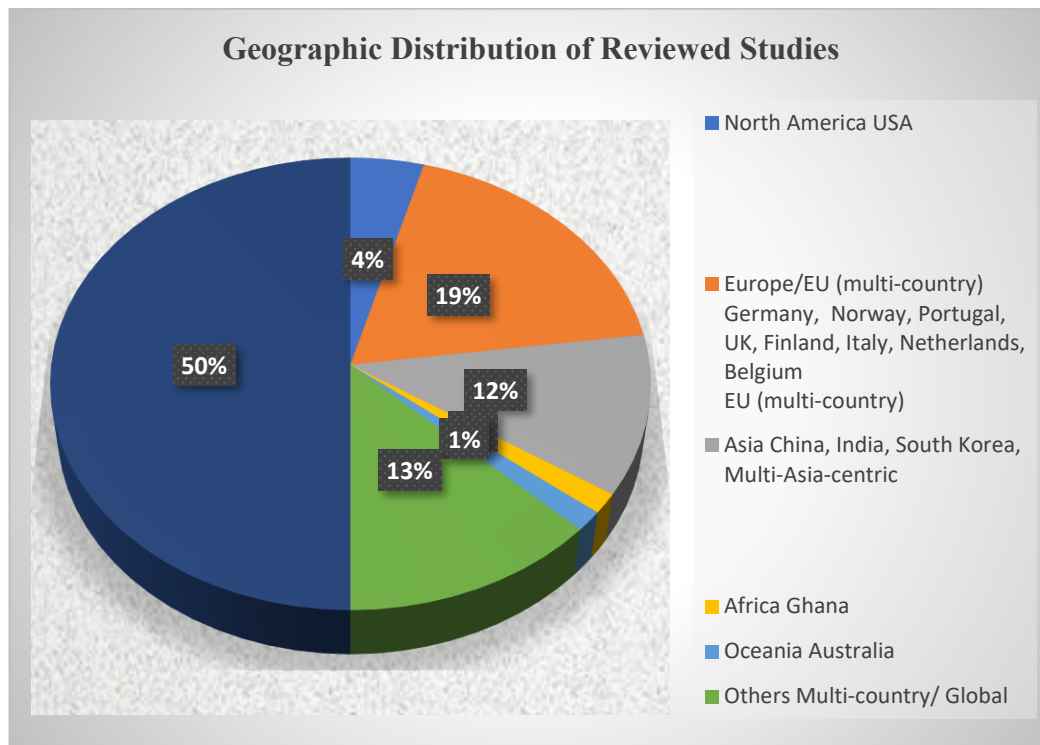


Figure 4.4 Pie Chart of Geographic Distribution of Reviewed Studies (Synthesised by author)

Figure 4.4 presents the geographic distribution of the selected articles. The chart highlights the global research imbalance, with a notable lack of Afro-centric studies, emphasising the need for contextually sound frameworks to incorporate African socio-cultural and ethical aspects into the development of service robotics.

The data reveal a clear imbalance, with North America (USA) and Eurocentric studies making up the majority, at 50% and 19% of the reviewed studies, respectively. Asian studies, including China, India, and South Korea, and broader multi-Asia-focused research, account for 13%. Importantly, only 1% of the studies are Afro-centric, originating from Ghana, pointing to a significant gap in research in African contexts.

Although the research questions do not focus on Afro-centricity, the geographic differences identified in the SLR highlight a significant gap in research on cyber-safe, ethical, service robotics in Africa. This finding does not change the design criteria but increases the relevance of the proposed framework within its context. It also emphasises the need to include socio-cultural and ethical perspectives relevant to emerging economies, such as those in Africa, making the framework potentially more useful, inclusive, and adaptable.

4.7 Socio-Technical Architectural Gap Across Methodologies

The bar chart in Figure 4.5 shows the use of methodological approaches and the types of socio-technical gaps each study addresses, which are categorised in the reviewed studies (see Appendix G).

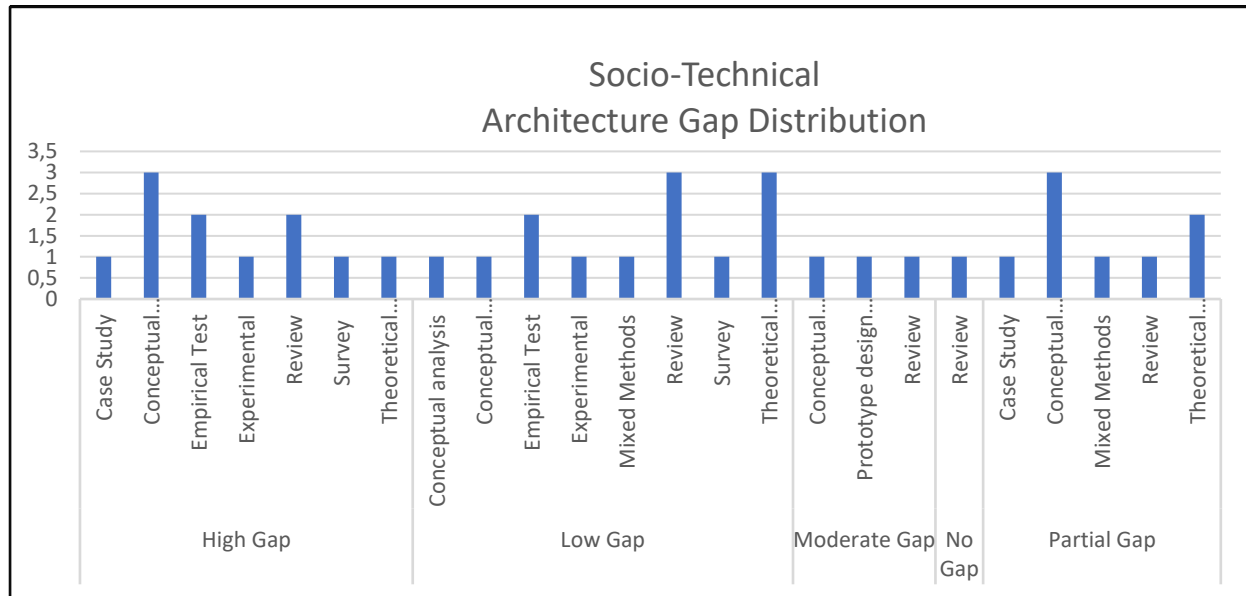


Figure 4.5 Methodology Distribution of Socio-Technical Architectural Gap

(Synthesised by author)

Figure 4.5 highlights the socio-technical integration gaps across different study types presented in the selected research articles. The conceptual and theoretical frameworks are common in studies (of the 35 articles, 37% presented such frameworks) with high or partial gaps, whereas empirical and mixed-methods studies are fewer (17% of the 35 articles) and tend to show low or moderate gaps.

The SLR based on socio-technical gap analysis arranges the reviewed studies into five levels of architectural gaps to illustrate how well existing robotic frameworks address or overlook the integration of ethical, cyber-safety, and socio-technical dimensions. This classification helps quantify methodological and conceptual deficiencies across the literature, revealing where theoretical robustness and practical applicability diverge. This includes:

- High Gap (31%)
- Low Gap (36%)
- Moderate Gap (8%)

- No Gap (3%)
- Partial Gap (22%)

These gaps are compared with their respective methods, such as conceptual, case study, experimental, and mixed methods. The High Gap studies mainly use conceptual and empirical methods, which may overlook socio-technical factors. Conceptual papers dominate both High and Partial Gap categories, showing a lack of empirical or systemic focus. Low Gap studies, on the other hand, employ diverse methods, including mixed methods, theoretical approaches, and surveys, suggesting room for better integration of technical and human analysis. Fewer studies in No Gap and Moderate Gap indicate that these areas are less well explored in terms of socio-technical dynamics.

Preliminary findings from the reviewed studies indicate that approximately 77% of the frameworks overlook the significance of cultural background and local socio-economic conditions in robot deployment, especially in Africa, where cultural norms, economic constraints, and infrastructure influence acceptance. While HRI is frequently studied, its emotional, trust, and relationship aspects are understudied, with a primary focus on technical capabilities (60%) rather than human experience and ethics (37%). Only about 52% of the studies have explored cross-industry adaptability, with 26% addressing AI manipulation and data breaches (see Appendix I).

4.8 Cybersecurity Vulnerabilities Identified in Networked Service Robotics Systems

The SLR identified several recurring cybersecurity vulnerabilities affecting networked service robotics. These vulnerabilities include:

- Unauthorised system access
- Data breaches involving sensitive personal identifiable information
- Insecure communication channels
- Software and firmware vulnerabilities
- Cloud-based security risks
- Manipulation of robotics sensing and control mechanisms

These vulnerabilities were consistently associated with risks to operational integrity, user privacy, and system reliability. The findings show that service robotics face both traditional cybersecurity threats and cyber-physical risks resulting from HRI in real-world settings. These vulnerabilities helped shape the cyber-safety design criteria integrated into the ACERBOTICS framework.

4.9 Design Criteria Identified

The findings from the 35 selected studies identified key design criteria that inform the development of the proposed framework, which focuses on ethical and cyber-safe robotics systems in the service industry domain (see Appendix J). The review reveals that although recognition of robotics potentials is increasing, most studies emphasise performance and efficiency while overlooking cyber-safety, ethical considerations, and adaptability to specific operational contexts.

Table 4.4 presents a summary of the identified design criteria.

Table 4.3 Summary of Design Criteria Identified

Design Criteria Identified	Description	Number of Studies	Proportion (%)
Ethical Integrity	Emphasises moral responsibility, fairness, transparency, and ethics.	26	74%
Cyber-Safety Resilience	Address data protection, system resilience, threat detection, and operational integrity.	23	66%
Socio-Technical Integration	address the ethical, technical and social challenges of	21	60%

Table 4.3 Summary of Design Criteria Identified

Design Criteria Identified	Description	Number of Studies	Proportion (%)
	using robotic systems		
Human-centred Design	Prioritises human needs, experience and interactions in the development and deployment of robotic systems.	18	50%
Cultural and Regional Adaptability	Focused on how robotic systems adapt to different economic and cultural settings	15	43%
Regulatory and Governance Alignment	Addresses the integration of robotics design and deployment within existing legal, ethical and policy frameworks.	13	37%
Long-Term Impact Assessment	Addresses the social, economic, and	11	31%

Table 4.3 Summary of Design Criteria Identified

Design Criteria Identified	Description	Number of Studies	Proportion (%)
	environmental factors and implications for societal well-being.		

Table 4.4 shows that Ethical Integrity and Cyber-Safety Resilience (74% and 66%, respectively) are the main themes.

The emphasis on these two areas shows a growing scholarly focus on responsible and secure robotics design, as well as prioritising safety, transparency, and ethical governance in robotic deployment. Socio-Technical integration (60%) and Human-centred aspects (50%) follow closely behind. Note that the Cultural and Regional Adaptability (43%) and Regulatory and Governance Alignment (37%) are less frequently explored, underscoring the need for an integrative framework that links ethical, cyber-safety dimensions, cultural, and context-specific frameworks. Long-Term Impact Assessment (31%) remains the least common.

4.10 Emergent Themes from the Systematic Literature Review

Analysis of reviewed studies identified seven recurring themes that inform cyber-safe and ethical service robotics. These themes, as highlighted by the frequency analysis in Table 4.4, highlight key focus areas in the literature.

1. **Ethical Integrity (74%)** was identified as the dominant theme, with research frequently highlighting accountability, transparency, fairness, privacy, and responsible decision-making as key elements of trustworthy robotic systems. This underscores the increasing impact of ethical AI and robotic governance frameworks in service settings.
2. **Cyber-Safety Resilience (66%)** emerged as the second most common theme. The literature highlighted the importance of safeguarding robotic systems against cyber threats by emphasising data protection, system resilience, threat detection, and secure operational practices. These findings suggest that cyber-safety remains a fundamental requirement for the safe deployment of robotic systems.

3. **Socio-Technical Integration (60%)** The reviewed studies emphasise the importance of considering how technological capabilities interact with social systems. They indicate that effective implementation of robotic systems depends on aligning technological design with organisational structures, human behaviour, and operational environments.
4. **Human-centred Design (50%)** emphasises users' needs, trust, usability, and HRI. The literature shows growing recognition that robotic systems must be designed around human values and experience rather than technological functionality alone.
5. **Cultural and Regional Adaptability (43%)** reflects a growing awareness that robotic deployment occurs across diverse social, cultural, and economic contexts. Studies on this theme emphasise the need for frameworks that can adapt to local conditions and stakeholders' expectations.
6. **Regulatory and Governance Alignment (37%)** focuses on the integration of robotics within the legal, ethical and policy environments. The literature highlights ongoing challenges related to accountability, liability, compliance and governance oversight.
7. **Long-Term Impact Assessment (31%)** emerged as the least representative theme. Although less frequently discussed, studies on this theme emphasise the broader societal, economic, and environmental implications of robotic deployment, indicating an area requiring further scholarly attention.

Collectively, these themes demonstrate that cyber-safe, ethical, and socio-technical considerations are highly interconnected. The findings further indicate that existing studies often address these dimensions independently, highlighting the need for an integrated framework that brings cyber-safe, ethical, and socio-technical aspects within a unified governance structure.

4.11 Results and Findings

4.11.1 Contributions and Strengths of Reviewed Studies

A diverse selection of 35 papers ($N = 35$) from the healthcare, hospitality, education, and tourism sectors demonstrates that service robotics is adaptable across various industries, particularly in healthcare and tourism ($n = 18$, which account for 51%), enhancing efficiency, improving customer experience, and reducing human labour. Studies also suggest frameworks for ethical decision-making and acceptance ($n = 13$, which accounts for 37%), focusing on privacy, autonomy, workforce displacement, and accountability. Moreover, research on AI-driven automation, cloud manufacturing, and 3D recognition ($n = 9$, which accounts for 26%) indicates potential for enhanced robot capabilities in real-time decision-making and interaction.

4.11.2 Limitations of Reviewed Studies

Findings show that, although interest in robotics is increasing, most studies originate from North America and Europe, with few exploring settings in Africa, Asia, and the Global South. This reveals a gap in Afrocentric perspectives, which are essential for creating a truly integrated robotic service framework that is inclusive. Approximately 60% of studies ($n = 21$) focus on the technical aspects of robotics, often neglecting the socio-technical integration that demonstrates how humans, culture, and technology interact. This leads to frameworks that overlook ethical and socio-cultural considerations in deploying robots in service sectors.

While 46% of studies ($n = 16$) address AI manipulations and data breaches (see Appendix I), cyber-safety safeguards in service robotics remain underexplored, leaving frameworks vulnerable to cyber threats. Furthermore, the reviewed studies ($n = 35$) employ various methods, from case studies to models, but none offer a cohesive socio-technical framework that integrates cyber-safety with ethical principles for future robotics development.

4.12 Discussion

The analysis strongly supports the need for an integrated cyber-ethical framework. The study reveals a lack of thorough integration of ethical reasoning and cyber-safety safeguards. The gaps identified in the current literature, particularly in socio-technical integration, cultural context, cyber-safety, and long-term human–robot relationships (see Appendix I), underscore the need for a robust socio-tactical framework like ACERBOTICS. This ACERBOTICS socio-tactical framework aims to integrate both ethical and technical dimensions, adapt to diverse cultural and regional contexts, and foster long-term socio-dynamics. By addressing socio-technical gaps in the existing literature, the ACERBOTICS socio-tactical framework offers a comprehensive approach that incorporates cyber-safety and ethical considerations as well as human-centred design in the development of service robotics. It seeks to prioritise region-specific issues to ensure the framework remains globally applicable while being culturally and socially sensitive to various deployment settings. Moreover, by focusing on the enduring impacts of service robotics, the framework aims to support sustainable robotics development that promotes social equity, empowers workers, and builds public trust.

4.13 Conclusion

This chapter reviews contributions to cyber-safety, ethics, and HRI in the field of service robotics. The SLR findings reveal a growing recognition of the potential of service robotics and a rich conceptual ecosystem across different sectors. However, they also highlight notable gaps,

particularly in addressing socio-technical challenges and cultural considerations, and in integrating ethical reasoning with cyber-safety safeguards in applied service domains (see Appendix C). While the literature offers valuable insights and guidelines, it lacks comprehensive, empirically validated frameworks for the dynamic and high-contact nature of service robotic systems. The SLR identified rich but fragmented approaches, insufficient empirical support, and overlooked socio-technical aspects. The analysis identified several key design criteria to address these gaps and inform the development of a comprehensive framework for ethical and cyber-safe service robotics. These criteria were selected because they represent the common themes across the theoretical and empirical studies in the SLR (see Appendix K). Derived from the literature, these criteria are essential to ensuring the safe, ethical, and effective deployment of service robotics. The next chapter will apply these criteria to structure the proposed framework. The following design criteria are derived from the literature: ethical integrity, cyber-safety resilience, socio-technical integration, human-centred design, cultural and regional adaptability, regulatory and governance alignment, and long-term impact assessment.

Chapter 5: Proposed Framework Development and Presentation

5.1 Introduction

As robotics becomes more common across global service industries, from healthcare and tourism to retail and manufacturing, the impact of deploying robotic systems is increasingly felt (Lu et al., 2020a). The gap between socio-technical integration, cultural context, cyber-safety, long-term human–robot relationships (see Appendix I), and the environment within which the technologies are used, remains significant. This was identified in the SLR, which showed that 77% of the reviewed studies primarily focus on conceptual or technical methods, with limited socio-cultural adaptation or empirical evidence (see Appendix I).

The SLR conducted (and presented in Chapter 4) reveals that existing frameworks focus primarily on technical performance and efficiency, with limited focus on the social, cultural, ethical and cyber-safety issues that emerge when in real-world HRI (Batya & David, 2019; IEEE, 2019b). This limitation underscores the need for an integrated model that bridges the technical and social dimensions of robotic system deployment in the service industry. A disconnect is particularly visible in African contexts where many robotics solutions are imported and poorly matched to local infrastructures, norms, and governance systems (Brown-Acquaye et al., 2019). The lack of locally informed design principles and ethical integration further deepens the misalignment between imported solutions and the deployment of service robotic systems.

The design criteria are derived and identified during the process of the SLR (Chapter 4). The design criteria include ethical integrity, cyber-safety resilience, socio-technical integration, human-centred design, cultural and regional adaptability, regulatory and governance alignment, and long-term impact assessment. The identified design criteria are synthesised in Section 5.4 and collectively inform the development of the proposed ACERBOTICS socio-tactical framework, discussed in this chapter. The design criteria address previously identified gaps and establish a foundation for robotic systems that are ethically responsible, cyber-secure, and culturally responsive.

The SLR of 35 relevant and selected studies revealed three key gaps in current robotic frameworks that support the design and deployment of service robotics. The identification of the gaps was derived through a structured thematic coding process applied during the extraction matrix stage (see Appendix C), where each study was analysed and categorised according to its core focus on: (1) ethical dimensions in HRI, (2) cyber-safety readiness in autonomous systems, and (3) cultural misfit, especially in Afro-centric contexts, (4) socio-technical dimensions.

In Table 4.3, qualitative thematic mapping demonstrated adequate representation of ethical consideration and service-oriented applications. In contrast, studies addressing cyber-safety and context-specific cultural alignment in service robotic systems were significantly underrepresented (see Appendix C). Qualitative synthesis supported these results, indicating that most reviewed frameworks maintained a technocentric focus and prioritised performance efficiency over a range of contextual, ethical, or human-centred concerns (see Appendix G).

The integrated thematic and interpretive analysis revealed three areas of concern:

1. Inadequate integration of ethical dimensions in HRI
2. Insufficient focus on cyber-safety readiness in autonomous systems
3. Clear cultural misalignment in imported frameworks, particularly within African developing economies.

These findings highlight the necessity for a unified socio-tactical governance framework; thus, the proposed ACERBOTICS framework is proposed to address these gaps and to support ethical, cyber-safe, and culturally relevant development and deployment of service robotics systems.

The literature reviewed is mainly composed of relevant research for this study from North America and Europe (50% and 19%, respectively), while studies based in Africa account for less than 5% of the literature considered (see Appendix B). Additionally, the research methods used in much of the work predominantly rely on conceptual modelling, with limited focus on socio-technical integration (12%) (see Appendix G). This methodological imbalance shows that conceptual and framework-based studies are the most common, whereas empirical, context-specific validations are underrepresented (see Appendix C). This gap limits the practical applicability of current robotic frameworks.

To bridge the conceptual and methodological gaps identified in the SLR (Chapter 4), this chapter presents the design criteria identified from the SLR findings and introduces the proposed ACERBOTICS socio-tactical integration framework for cyber-safe and ethical service robotic systems – an original framework for guiding the ethical, cyber-safe, and contextually responsive development of service robotics in the RSI.

The design criteria were identified through thematic synthesis as documented in Table 4.4 (see also Appendix C). Each study was systematically examined and coded for contributions to ethical reasoning, cyber-safety measures, socio-technical integration, and contextual adaptability.

The theoretical foundations of the proposed ACERBOTICS socio-tactical integration framework, specifically VSD (Batya & David, 2019) and STS Theory (Malatji et al., 2019a) were selected due to their frequent citation and high relevance to the proposed framework development in the SLR, as a paradigm informing a socio-tactical integration framework for cyber-safe and ethical service robotic systems (see Appendix J). These theories were triangulated with identified design criteria to ensure that the proposed framework is empirically grounded and conceptually coherent

The objectives of this chapter are as follows:

- To synthesise and present the design criteria derived from the SLR that underpin the proposed ACERBOTICS framework (see Appendix K).
- To explain the theoretical foundation that informs the development of the proposed framework, demonstrating the triangulation of evidence from literature (see section 5.1), design principles (see section 5.2) and contextual analysis (see section 5.5).
- To describe the architecture and operational layers of the proposed ACERBOTICS framework, indicating how each component corresponds to the identified criteria.
- To demonstrate the applicability of the proposed framework using hypothetical scenarios drawn from African service sector contexts, such as tourism.
- To outline the evaluation process, which will be conducted by a panel of industry experts focusing initially on the service sector, with potential expansion of scope in future doctoral research.

The proposed framework developed in this research does not claim that the proposed ACERBOTICS socio-tactical integration framework for cyber-safe and ethical service robotic systems achieves a definitive shift from technology-driven robotics to human-centred robotics. Rather, it proposes a conceptual pathway toward that shift, which will be empirically validated through expert evaluation and subsequent implementation (see section 5.6).

5.2 Theoretical Framework

The proposed framework is based on three related theories:

1. Value Sensitive Design (VSD)
2. Ethically Aligned Design (EAD)
3. Socio-Technical Systems Theory (STS).

These theories together offer a strong foundation for understanding and addressing the ethical, technical and social challenges of using robotic systems. VSD provides ethical grounding, EAD

offers cyber-safety and governance structure, and STS ensures contextual and socio-technical adaptability.

5.2.1 Value Sensitive Design

As described by (Batya & David, 2019), VSD is a design method that considers human values at the core of technology development stages. It involves gathering inputs from all stakeholders to ensure that systems reflect both user needs and broader social values. For robotics, VSD helps include important values like privacy, accountability, trust and respect for culture, which are sometimes overlooked in technical plans (Batya & David, 2019).

5.2.2 Ethically Aligned Design

EAD, supported by the (IEEE, 2019b), offers clear principles for making ethics a core part of autonomous and intelligent systems. EAD encourages the protection of human rights, a focus on well-being, and the inclusion of transparency and accountability. The proposed ACERBOTICS socio-tactical integration framework for cyber-safe and ethical service robotic systems utilises these ideas to ensure that ethics are integrated into its robotics systems from the outset.

5.2.3 Socio-Technical Systems Theory

STS theory implies that every technology exists within a social network, and both need to work well together for the best results (Malatji et al., 2019a). The STS emphasises how social and technical elements are interconnected, suggesting optimal system performance requires balancing both. It advocates designing systems that integrate human, social and organisational factors with technology to boost efficiency, safety, and adaptability. This view recognises that technology alone cannot achieve the best results, and understanding social dynamics, workflow, and stakeholder interactions is crucial for effective and resilient systems. In robotics, this means aligning how machines operate and interact with people's routines, culture, and social norms. The proposed ACERBOTICS socio-tactical integration framework for cyber-safe and ethical service robotic systems follows this approach to ensure its robotics can fit different contexts and adapt as needed.

5.2.4 Integrative Relevance of Theoretical Frameworks to the Proposed ACERBOTICS Socio-Tactical Integration Framework for Cyber-safe and Ethical Service Robotics

By synthesising these three frameworks (namely, VSD, EAD, and STS Theory), a proposed ACERBOTICS framework includes the design criteria (as identified during the SLR presented

in Chapter 4), a design approach that balances the following elements: ethical governance principles from EAD, human value mapping and stakeholder inclusion from VSD, and systemic human-machine-environment alignment from STS.

Figure 5.1 presents the theoretical foundations of the ACERBOTIC Socio-Tactical Integrated Framework, showing how VSD, EAD, and STS intersect to inform an integrated approach to ethical, cyber-safe, and human-centred service robotics.

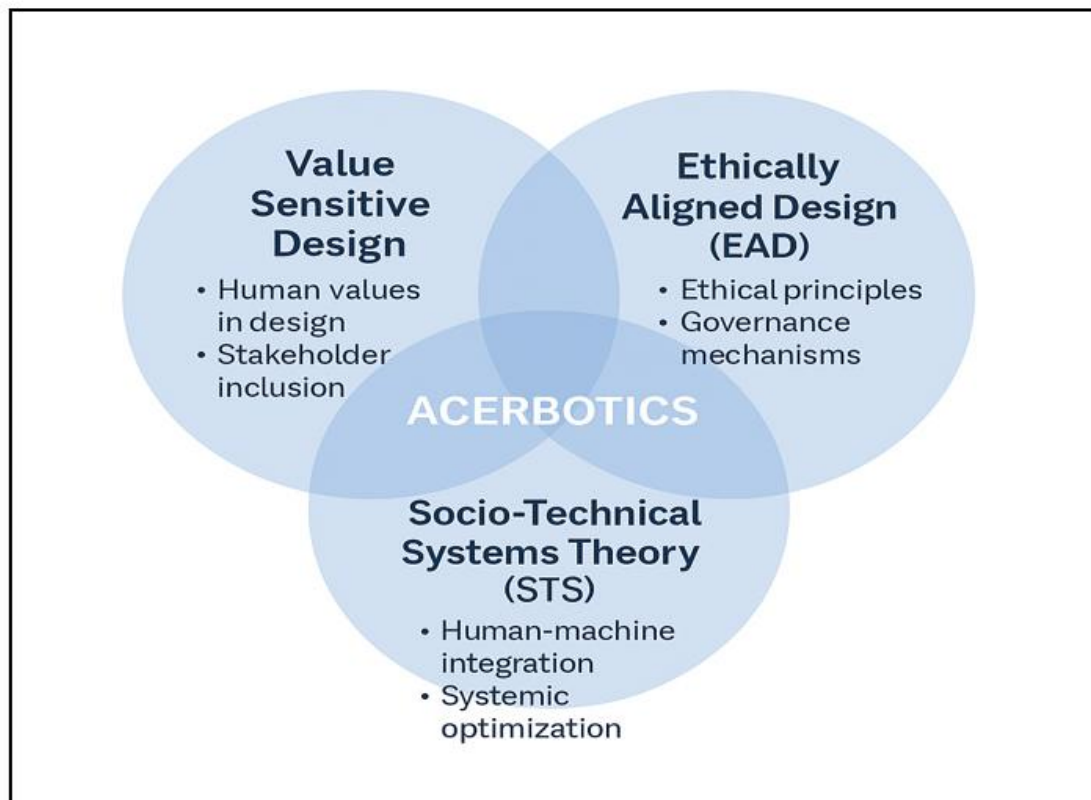


Figure 5.1 Conceptual Underpinning Map for a Proposed ACERBOTICS framework

(Synthesised by author)

Figure 5.1 shows that the integration of three interconnected design theories: VSD, EAD, and STS, provides a balanced basis for creating cyber-safe, ethically aligned, and contextually adaptable robotic systems.

5.2.5 Presentation of a Proposed ACERBOTICS Framework - A Socio-Tactical Integration Framework for Cyber-safe and Ethical Service Robotic Systems

A proposed ACERBOTICS socio-tactical integration framework for cyber-safe and ethical service robotic systems is a hybrid framework that combines STS theory, cyber-resilience architecture frameworks, and VSD principles to develop ethically aligned, cyber-safe service robotics, enabling systematic and tactical integration. It targets service sectors where robotic agents autonomously engage with humans in real-time environments.

Figure 5.2 presents the integrated structure of the ACERBOTICS framework, combining foundational governance pillars with an operational cycle for ethical and cyber-safe service robotics.

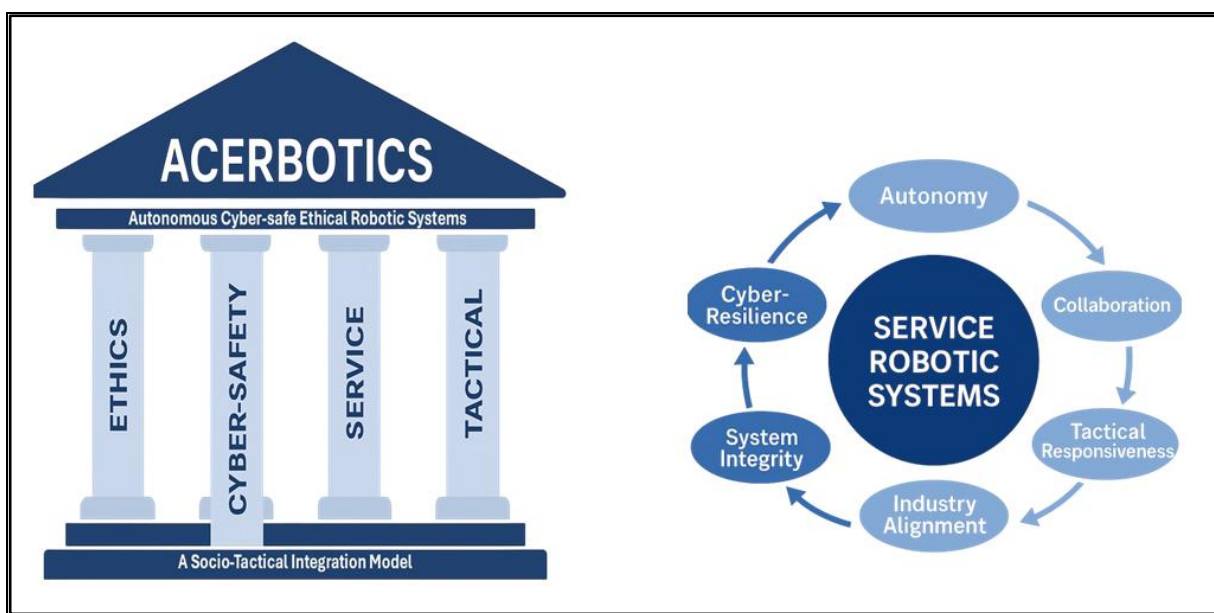


Figure 5.2 A proposed ACERBOTICS Framework: Core Pillars (Synthesised by author)

Figure 5.2 illustrates the structure and operations of the ACERBOTICS Framework. On the left, four core dimensions support the creation of cyber-safe, ethically aligned robotic systems. On the right, the operational loop shows how service robotics remain functional through interconnected elements that enable continuous interaction and adaptability across service environments.

A proposed framework, ACERBOTICS socio-tactical integration framework for cyber-safe and ethical service robotic systems, emphasises the strategic and operational aspects of incorporating robotics into human environments, focusing especially on decision-making processes, tactical deployment, and immediate interactions, rather than merely systemic or socio-technical interactions (see Section 5.4).

The four foundational pillars (Ethics, Service, Tactical, and Cyber-safety) constitute a framework that regulates robotic systems based on ethics, service domain, cyber-safety resilience, and tactical integration and responsive principles. These foundational pillars provide a socio-technical justification, aligning robotic systems with defined operational requirements and recognised ethical standards.

The circular figure comprises operational elements such as Autonomy, Cyber-Resilience, Industry Alignment, System Integrity, Collaboration, and Tactical Responsiveness. These elements define the functional dimensions of robotic systems. For instance, autonomy enables intelligent decision-making while system integrity ensures operational safety. These elements operationalise abstract pillars into practical robotic behaviours, thereby ensuring that robotic systems are both ethical and technically effective.

5.3 Literature and SLR Foundations of the Proposed Framework Components

To illustrate the theoretical foundation of the proposed framework, Table 5.1 links each component to relevant literature sources and summarises key findings from the SLR.

Table 5.1 SLR Foundations of the Proposed Framework Components

Framework Component	Theoretical/Literature Foundation	Key SLR Finding
Ethical Governance Core	VSD (Friedman & Hendry, (Friedman & Hendry, 2019); Ethically Aligned Design (Friedman & Hendry, 2019);	Need for accountability, transparency and ethical decision-making
Cyber-Safety and System Resilience	Cybersecurity governance and robotic systems literature (ENISA, 2020).	Need to address vulnerabilities, cyber threats, data protection, and resilience in networked robotic systems.
Human-Centred Design	VSD (Friedman & Hendry, 2019), and HRI literature	Need to preserve human dignity, trust, usability and user acceptance
Socio-Technical Integration	STS (Ahlborg et al., 2019b; Govers & van Amelsvoort, 2023b; Malatji et al., 2019b).	Need to align technical functionality with organisational and social contexts
Service-Sector Responsiveness	Service robotic literature	Need for domain-specific adaptation and contextual deployment
Industry Alignment	Regulatory and governance literature	Need for compliance with standards, legislation, and industry requirements.

Table 5.1 shows a clear connection between the ACERBOTICS framework components, the theoretical foundations they are based on, and the main findings of the systematic literature review (SLR). This illustrates that each component is grounded in both existing research and identified gaps in the literature, thereby enhancing the framework's overall conceptual validity.

5.4 Framework Development Process

Four phases comprise the development of the proposed ACERBOTICS socio-tactical integration framework for cyber-safe and ethical service robotic systems. These phases ensure both practical relevance and theoretical consistency and include an SLR of existing studies, identification of research gaps, and careful alignment with key values.

5.4.1 Phase 1: SLR and Extraction

The 35 academic papers that were reviewed included journal articles, conference proceedings, and relevant frameworks. Themes covered included cyber-safety frameworks, cyber-safety challenges, ethical frameworks, HRI, legal and regulatory frameworks, and integrated cyber-ethical frameworks (see Section 4.4 and Table 4.3). Several significant trends and gaps became apparent during this review process (see Sections 4.4, 4.5, & 4.6), including:

1. Over-representation of Euro-American perspectives
2. Methodological over-reliance on conceptual and simulation-based approaches
3. Neglect of Afro-centric realities and localised socio-technical factors
4. Insufficient emphasis on cyber-safety and long-term ethical implications in robotic deployments.

This gap analysis provided the empirical basis for designing an original framework that addresses these deficits.

5.4.2 Phase 2: Socio-Technical Gap Mapping

Each paper was assessed using the SLR matrix (see Appendix J) in areas such as the Afro-centric focus, socio-technical architecture gap, technological bias, overlooking of HRI socio-dynamics, and relevance to framework development. The results are striking; only about 23% of studies showed a small gap between technology and social factors, but over 50% had a large gap (see Section 4.7). These findings highlight a significant challenge in integrating technology with human and cultural needs.

5.4.3 Phase 3: Theoretical Convergence and Adaptation

The framework synthesises theoretical models from VSD to centre human and societal values, from EAD to integrate proactive ethical compliance, and from STS to ensure the system's harmonious integration across technical and social domains. These models were combined to form

a framework specifically designed for service robotics that incorporates cultural values, decentralised governance, and community-driven adaptation.

5.4.4 Phase 4: Visual Modelling and Feedback Loop

To address the requirements identified during the analysis, a layered visual model was developed. Multiple iterations refined this model to incorporate:

- Interoperability between ethical and technical subsystems
- Local deployment constraints such as low-bandwidth environments
- Alignment with human development goals such as access, equity, trust, and safety.

Figure 5.3 outlines the phased research and development process used in this study to systematically derive, synthesise, and refine the ACERBOTICS Socio-Tactical Integrated Framework.

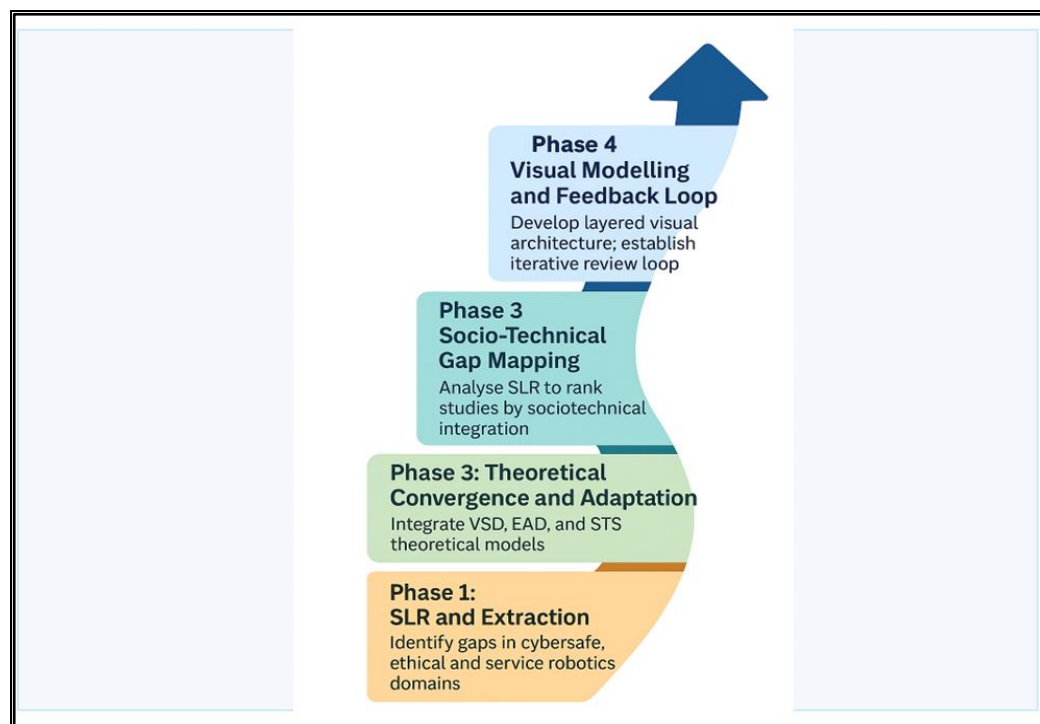


Figure 5.3 A proposed ACERBOTICS Framework Development Pipeline

(Synthesised by author)

Figure 5.3 illustrates the research design process for developing the ACERBOTICS framework, organised into four sequential phases from SLR and Extraction to Visual Modelling and Feedback Loop, which establishes an iterative review cycle for refinement of the framework

5.5 Socio-Technical Paradigm Shift

“Socio-Technical” refers to the integration of social and technical elements within a system, often focusing on how technology impacts social structures and vice-versa (Ahlborg et al., 2019a; Bockshecker et al., 2018; Govers & van Amelsvoort, 2023a; Malatji et al., 2019a).

5.5.1 Socio-Technical Architecture Gap

- **Integration issues**

Balancing competing priorities such as maintaining secure communications, ensuring patients' privacy and confidentiality, and providing timely intervention is crucial (in terms of the healthcare service domain). Well-developed frameworks often fail to align ethical considerations with security by design, resulting in ethical and operational fragmentation.

- **Operational Issues**

Some analysed papers show a strong technological bias, overlooking the socio-technical dynamics of HRI, user perceptions of robotic agents, and the ethical risks involved (see Appendix J). Cyber-safe techniques can introduce delays or complexities that impede the system's performance in time-sensitive tasks.

- **Real-Time Issues**

The extant socio-technical frameworks overlook the split-second decision-making in HRI, such as a robot's response to human actions or environmental changes.

Addressing these gaps requires a new framework that takes a “socio-tactical” approach, prioritising real-time adaptability, operational pragmatism, and integrated solutions that connect the social, ethical, and technical aspects of HRI. This framework would allow for more effective and safer integration of robotics into human environments.

Figure 5.4 presents the socio-technical integration of robotic systems within the service contexts, showing the interdependencies among social, ethical, technical, HRI, and cyber-safety aspects across various levels of implementation

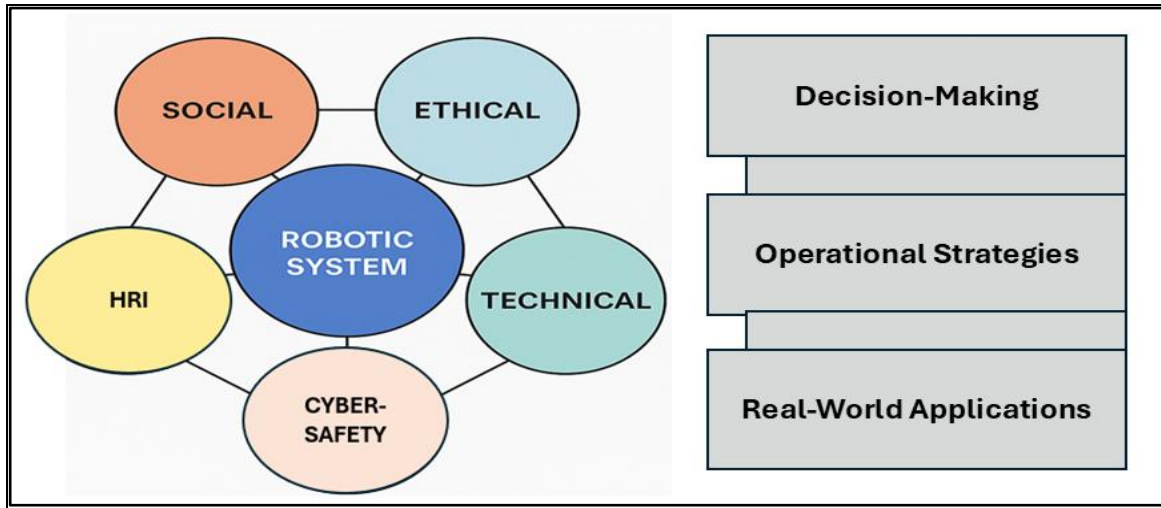


Figure 5.4 Socia-Tactical Framework (Synthesised by author)

Figure 5.4 shows how different domains interact to affect the successful deployment of service robotic systems. The five key dimensions on the left guide the design and governance, while the implementation hierarchy highlights how theoretical ideas turn into practical, safe, and ethical deployment of service robotics.

5.6 Socio-Tactical Defined

- **Socio:** Reflects the human, cultural and ethical dimension (Ahlborg et al., 2019a).
- **Tactical:** Highlights systemic, strategic, and operational readiness, differentiating it from the broader, theoretical “technical” aspects.

“Socio-tactical” implicitly refers to the integrated framework that combines the social, ethical, and human dimensions with tactical, systemic, and operational strategies to address real-world challenges in HRI, cyber-safety, and service robotics (author synthesised).

This could involve these components:

1. Ethical considerations: How robots should act ethically in various service scenarios, ensuring compliance with social values and ethical standards.
2. Cyber-safety: Ensuring that robots are secure from cyber threats, tackling how data security and privacy are operationalised in human–robot systems.
3. HRI: Understanding how humans and robots interact effectively, focusing on real-time, adaptive interactions that are both socially acceptable and tactically efficient.
4. Service Industry: Applying these principles in practical, real-world settings like healthcare, retail, travel and tourism, education, and other service-oriented use cases.

5. Tactical Deployment: Involves planning and executing robots in ways that are responsive to both short-term and long-term objectives in dynamic environments. It emphasises flexibility, adaptability, and the ability to adjust strategies based on real-world conditions.

5.7 Overview of Proposed ACERBOTICS Governance and Deployment Structural Layers

A proposed ACERBOTICS socio-tactical integration framework for cyber-safe and ethical service robotic systems uses a flexible, modular structure that integrates ethical awareness, cyber-safety resilience, and regional adaptability perspectives throughout the service robotics lifecycle. It includes five connected areas, each designed to support technical and ethical consistency and system resilience in governance and deployment processes.

Figure 5.5 presents the iterative governance architecture of the ACERBOTICS framework, showing the dynamic interaction between core governance layers that support ethical, cyber-safe, and context-aware service robotics.

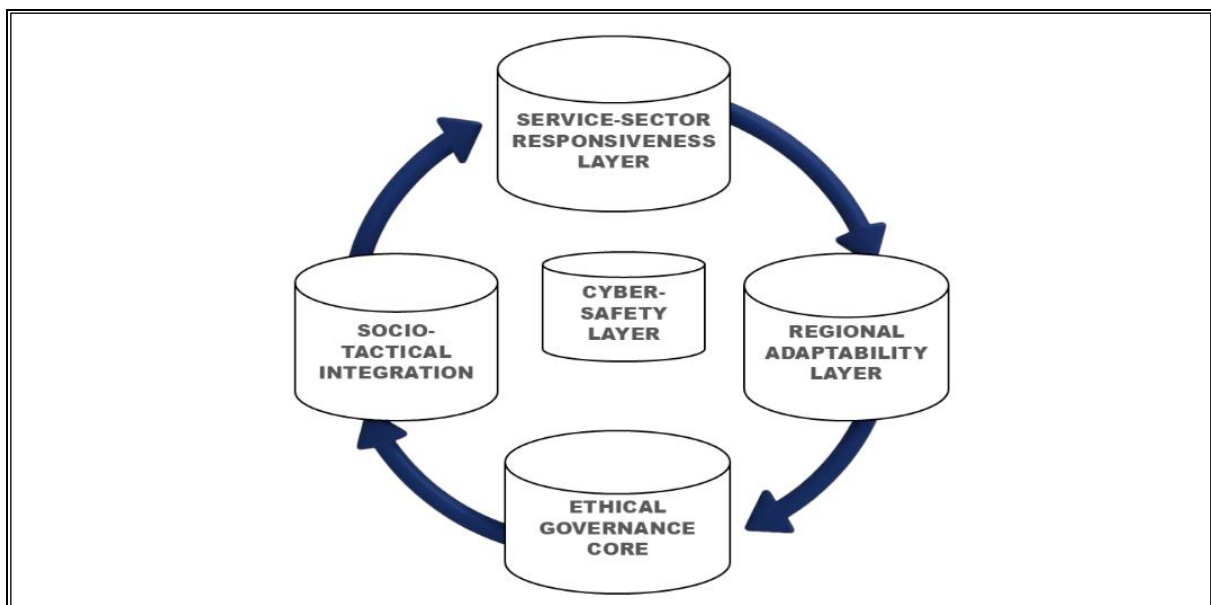


Figure 5.5 Iterative Governance and Deployment Cycle Architecture (Synthesised by author)

Figure 5.5 demonstrates how the interconnected layers work together to ensure ethical and cyber-safe robotic operations, forming a continuous loop that aligns robotic governance, maintains adaptability, and upholds ethics to achieve sustainable, context-sensitive system performance.

1. Service-Sector Responsiveness Layer

This layer focuses on applying robotic functions to specific areas, such as healthcare assistive robots and diagnostic support, tourism for customer engagement, concierge bots, and public service in queue management and multilingual translation.

2. Cyber-Safety Layer

This foundational layer safeguards robotic systems from both external and internal threats, which include risk-driven security protocols, continuous vulnerability assessment, encrypted cloud-based communication safeguards, and AI-anomaly detector systems (Rahman et al., 2024).

3. Ethical Governance Core

Informed by EAD principles (IEEE, 2019b). This core integrates transparency into the decision-making logic, embeds accountability mechanisms, includes stakeholder consultation modules, and establishes protocols for consent and data privacy.

4. Socio-Tactical Integration Layer

Based on Socio-Technical System Theory, this layer aligns robotic functionality with human needs, in line with cultural context through HRI optimisation algorithms, feedback-aware learning loops, and adaptable task modelling in public or institutional environments.

5. Regional Adaptability Layer

This layer customises robotic systems to regional social, economic, cultural, and language contexts, including culturally-aligned ethical factors, local language integration, gesture mappings, and infrastructure-sensitive design such as offline capabilities.

All layers work together to enable ongoing collaboration, continuous feedback, regulatory compliance, and adaptation as needed. For example, ethical guidelines determine how cyber-safety responses are triggered, how cyber-safety is managed for activated systems, how data is handled securely, and how users are monitored in real time. Socio-tactical insights influence how robotic systems respond to human emotions or body language. The system also learns and adapts to various user factors, such as age, literacy level, health status, and cultural differences, adjusting service delivery behaviour based on user profiles and community norms. The ethical governance core ensures informed consent before interactions and prevents biased triage behaviours. The Afro-centric layer facilitates communication in local languages and promotes cultural sensitivity during patient interactions. The service-responsiveness layer supports scheduling, queue optimisation, and user guidance. These examples demonstrate how a proposed ACERBOTICS

socio-tactical integration framework for cyber-safe and ethical service robotic systems can adapt and uphold ethical standards in African service environments.

5.7.1 Evaluation of a Proposed ACERBOTICS Socio-Tactical Integration Framework for Cyber-safe and Ethical Service Robotic Systems

The initial evaluation of the proposed framework (as set out in Section 5.4) was conducted by a panel of experts (detailed in Section 5.9) using a questionnaire (see Appendix L for the questionnaire used). The analysis of the evaluation data collected using the questionnaire is presented in Chapter 6

5.8 Framework Purpose

A proposed ACERBOTICS socio-tactical integration framework for cyber-safe, ethically aligned robotic systems in the service industry is designed to guide robotics deployment. It integrates principles of autonomy, tactical responsiveness, ethical safeguards, cyber-resilience, and socio-contextual adaptability within an operational loop, ensuring safe, responsive, and socially responsible robotic interactions in service domains such as healthcare, tourism, and customer service.

The present evaluation assesses the validity, completeness, and applicability of the framework in addressing several critical challenges, including the following:

- Cybersecurity vulnerabilities in networked service robotics
- Ethical concerns related to decision-making, bias, and safety
- Integration of HRI principles into real-world service settings

Table 5.2 outlines the core elements of the ACERBOTICS socio-tactical framework and its roles. The table demonstrates how the components interact across governance, socio-tactical, and implementation layers to support ethical reasoning, safety, and responsiveness in service robotic systems.

Table 5.2 Framework Components and Roles

Framework Component	Role in the Framework	Support for Framework's Objectives
Pillars: Ethics, Service, Tactical, System Resilience	The four foundational pillars constitute a framework that regulates robotic systems based on ethics, service domain, cyber-safety and responsive principles.	These foundational pillars provide socio-technical justification, aligning robotic systems with defined operational requirements and recognised ethical standards.
Circular Operational Elements: Autonomy, Cyber-Resilience, Industry Alignment, System Integrity, Collaboration, and Tactical Responsiveness	These elements define the functional dimensions of robotic systems. For instance, autonomy enables intelligent decision-making while system integrity ensures operational safety.	These elements operationalise abstract pillars into practical robotic behaviours, thereby ensuring that robotic systems are both ethical and technically effective.
Socio-Tactical Loop	This component represents an interlinked cyclical feedback-driven governance that includes the systemic integration of ethical, social, technical, HRI, and cyber-safety elements in service robotic systems	Facilitates ongoing feedback between ethical governance, cyber-safety mechanisms, and operational deployment, ensuring robotics are deployed adaptively, context-aware, and ethically aligned.

Table 5.2 Framework Components and Roles

Framework Component	Role in the Framework	Support for Framework's Objectives
Iterative Governance and Deployment Cycle	This architecture ensures governance guides each deployment stage, with real-world feedback refining decisions, strategies, and oversight, promoting safety, adaptability and ethics in robotics.	This governance layer provides a real-time, context-aware engine that adapts the framework to changing environments and ensures compliance with societal, cultural, and domain-specific standards.

Table 5.2 summarises the ACERBOTICS framework components and their roles in achieving the framework's goals. It shows how each component serves a specific purpose within the governance architecture, ensuring cyber-safety, ethical, human-centred, and socio-technical requirements are systematically addressed throughout deployment. This promotes logical consistency and operational integration.

5.9 A Proposed ACERBOTICS Integrated Socio-Tactical Framework

A proposed ACERBOTICS Integrated Socio-Tactical Framework, as illustrated in Figure 5.6 below, provides a unified architecture that integrates ethical governance, adaptability, and practical deployment for service robotics:

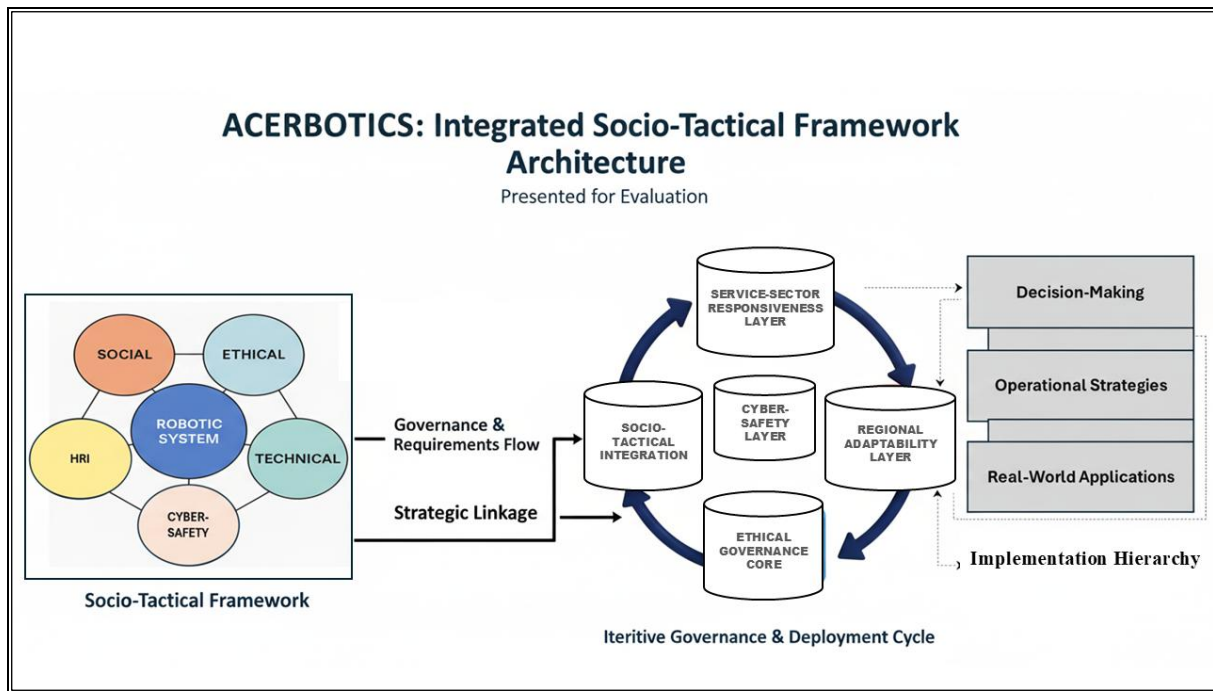


Figure 5.6 ACERBOTICS Integrated Socio-Tactical Framework Architecture

(Synthesised by author)

Figure 5.6 illustrates a combination of social, ethical, and cyber-safety dimensions in a unified framework for evaluating and guiding service robotic deployments, ensuring continuous refinement through feedback and oversight.

The socio-tactical layer of the proposed ACERBOTICS Framework provides a strategic core. The layer strategically links ethical, social, and technical factors into a continuous iterative governance and deployment cycle. This execution of the iterative governance and deployment cycle of the proposed framework ensures that governance guidelines such as ethical standards, cyber-safety protocols, and compliance procedures inform each stage of robotic system deployment, including design, testing, operation, monitoring, and post-deployment review. Real-world feedback from HRI, user evaluations, and operational analytics will contribute to refining and aligning policy decisions, adaptive control strategies, ethical practices, and oversight mechanisms such as auditing, risk assessment, and accountability structures, thereby promoting both adaptability and ethical standards in robotic deployment.

Within the implementation hierarchy of the ACERBOTICS proposed framework, decision-making (such as establishing ethical compliance benchmark and security risk thresholds) and operational strategies (such as adaptive task execution, incident response, and data governance protocols) are aligned through an adaptive feedback loop, which is executed at both the

governance and deployment layers of the framework. This alignment supports the resilience of robotic systems, sustains a human-centred focus for socio-technical collaboration, and promotes robust governance of autonomous operations across diverse robotics applications.

- **Directional Lines (Interlinkages):**

The diagram's arrows illustrate mutual influence and feedback among pillars, operational elements, and governance layers. This highlights the framework's cohesion and demonstrates how changes in one area, such as service needs, can dynamically impact others, including ethical protocols and resilience strategies.

- **Regional Adaptability Layer:**

This approach embeds local contextual awareness, especially critical for emerging and broader African economies. It helps bridge global robotic design with local socio-cultural needs, promoting equity and relevance.

- **Feedback Mechanisms (Inner-Outer Loop Interaction):**

Reflects ongoing learning, adaptation to risks, and maintenance of ethical responsibility. This approach ensures the long-term sustainability of robotics deployment, enabling continual improvement over time.

5.10 Why The Feedback Loop Mapping Matters for Evaluation

Each of these components was developed in response to specific research questions:

- Cyber-safety and data threats - addressed by System Resilience, System Integrity, and Cyber-Resilience.
- Ethical algorithmic flaws - handled through the Ethical Pillar and Governance Core.
- Service integration - reflected in Industry Alignment, Service Pillar, and Responsiveness Layer.

The results of this evaluation are intended to inform the refinement and potential standardisation of the framework for broader academic, industrial, and regulatory applications.

5.11 Conclusion

This chapter presents the ACERBOTICS Socio-Tactical Integrated Framework, designed to address ethical, cybersecurity, and socio-technical issues in service robotics, particularly in emerging economies. The framework is based on three main theories: VSD, EAD, and STS. It

highlights moral responsibility, technical resilience, and adaptability to various situations. By incorporating a socio-tactical layer, the framework links governance, design, and deployment through ongoing ethical review and safe practices. This method ensures that the design, development, and deployment of robotics align with human values, meet governance standards, and address local needs, fostering service automation that is both inclusive and sustainable.

The ACERBOTICS Socio-Tactical Integrated Framework aims to enhance robotics governance by addressing human, environmental, and technological factors. It incorporates ethical safeguards, cyber-safety, and inclusivity at every phase of robot deployment, meeting regional adaptability needs. With feedback mechanisms and phased implementation, the framework promotes transparency, trust, and accountability in service robotics. In summary, the ACERBOTICS Socio-Tactical Integrated Framework aims to establish a strong foundation for responsible robotics development and facilitates expert assessment and subsequent real-world testing, as discussed in Chapter 6.

Chapter 6: Expert Evaluation and Refinement of the ACERBOTICS Socio-Tactical Integrated Framework

6.1 Introduction

This chapter details the expert evaluation and refinement of the ACERBOTICS Socio-Tactical Integrated Framework, bringing the study to a close. The primary aim was to create a unified, contextually responsive framework that combines cyber-safety resilience, ethical safeguards, and socio-technical adaptability for service robotics systems. Building on the SLR in Chapter 4, which identified gaps in ethics, cyber-safety, socio-technical integration, and conceptual development, and on the framework development in Chapter 5 that introduced the ACERBOTICS Socio-Tactical Integrated Framework, this chapter moves from conceptual concepts to expert-based assessment and interpretive analysis. At this stage, experts assess the framework for clarity, relevance, usefulness, applicability, ethical integrity, cyber-safety readiness, socio-technical integration, coherence, coverage, completeness, and its effectiveness in addressing previously identified gaps in service robotics.

Unlike previous chapters, which focused on description and development, this chapter adopts a synthetic and interpretive approach. It combines qualitative and quantitative insights from experts' evaluations to assess the framework's robustness, applicability, and coherence. The analysis presents results and interprets implications for ethical and cyber-safe robotic design and deployment. Relying on qualitative expert evaluation rather than empirical experimentation (reserved for future research), experts in robotics, cybersecurity, ethics, AI, and service innovation responded to a structured questionnaire (see Appendix L). The feedback refines the framework, ensuring it aligns with standards and practical needs. This process helps develop the ACERBOTICS Socio-Tactical Framework as a resilient, adaptable guide for the ethical, cyber-safe, socio-tactical implementation of service robotics.

The chapter is organised into sections: 6.2 details the evaluation methodology, including design, expert criteria, and ethics; 6.3 presents results with ratings, analysis, and feedback; 6.4 describes thematic analysis and key outcomes; 6.5 introduces the refined ACERBOTICS framework with theoretical and expert modifications; 6.6 compares it to the initial version; 6.7 presents the refined framework, and section 6.8 concludes the chapter.

6.2 Evaluation Methodology

6.2.1 Evaluation Design and Rationale

A qualitative expert review was conducted to assess the conceptual validity and contextual applicability of the ACERBOTICS Socio-Tactical Integrated Framework. The questionnaire was designed to evaluate key aspects, including relevance, clarity, applicability, completeness, ethical integrity, cyber-safety readiness, socio-technical integration, usefulness, coherence, and coverage. This approach allowed for detailed feedback that extended beyond numerical scores, capturing interpretive insights essential for refining the framework.

6.2.2 Criteria for Expert Selection

Experts were selected using a purposive sampling strategy to ensure that individuals possessed relevant expertise in cybersecurity, robotics, AI, ethics, governance, and service robotics (see Section 3.6.1). Experts' contact details were obtained from directories of professional organisations to ensure a multidisciplinary perspective, including the Institute of Information Technology Professionals South Africa (IITPSA), the IITPSA Special Interest Group for AI and Robotics (SIGAIR), and LinkedIn communities dedicated to cybersecurity, AI, and robotics. In addition, permission was obtained from academic communities, including the Department of ICT at the University of Mpumalanga and the IT Faculty at Eduvos, to distribute the questionnaire to eligible staff. Snowball sampling was subsequently employed to encourage eligible participants to share the questionnaire link within their professional communities, thereby broadening participation while maintaining the predefined inclusion criteria. Inclusion criteria required a significant level of professional engagement in IT, robotics, cybersecurity, AI, ethics, and governance. To be eligible, experts were required to have demonstrated professional or research experience in one or more relevant domains, be at least 18 years of age, have experience and knowledge of service robotics, and voluntarily consent to participate in the study. These criteria ensured that the expert feedback reflected substantial domain expertise and informed perspectives on the proposed framework.

The expert evaluation employed purposive sampling to obtain informed assessments from individuals with experience in robotics, cybersecurity, governance, policy, and related disciplines. A total of 47 expert responses were obtained, providing diverse perspectives for the evaluation of a conceptual framework. Given the exploratory and evaluative nature of the study, the quantitative analysis relied primarily on descriptive statistics and internal consistency assessment rather than

on inferential statistical tests. The objective of the framework evaluation is to assess expert consensus, identify areas of convergence and divergence, and inform the framework's refinement.

6.2.3 Data Collection Instrument

The expert evaluation questionnaire (see Appendix L) was developed based on evaluation criteria (see Section 6.2.1) and incorporates both Likert-scale items and open-ended prompts. Respondents were instructed to assess each component of the framework using the requirements specified in Section 6.2.1. Open-ended questions elicited narrative responses, yielding more profound insights into the framework's strengths, gaps, and areas for improvement.

6.2.4 Ethical Considerations

Ethical approval was received from the School of Computing Ethics Committee (see Appendix M). Participation was voluntary, responses remained anonymous, and data confidentiality was upheld throughout the study. Experts were informed of their right to withdraw at any time without penalty.

6.3 Expert Evaluation Result

6.3.1 Quantitative Overview

A total of 27 valid expert responses were analysed, following the exclusion of 20 partial responses that lacked data for Q5 to Q13. The descriptive results (see Table 6.1) indicate a strong statistical consensus regarding the overall conceptual soundness, ethical robustness, operational relevance and applicability of the framework. Mean values ($M = 3.85\text{--}4.41$) across evaluation dimensions indicated broad expert agreement, with most items rated between High and Very High on the five-point Likert scale. Interpretation of expert feedback is added based on the Mean values using the Likert 1–5 evaluation scale as follows:

- 1.00–2.49 = Low
- 2.50–3.49 = Moderate
- 3.50–4.00 = High
- 4.01–5.00 = Very High

The computed mean values from 3.85 to 4.41 across the evaluated dimensions indicate that the framework effectively addresses pressing needs within the RSI while upholding ethical integrity and practical applicability.

Table 6.61 Descriptive Summary of Expert Ratings (n = 27)

Evaluation Item	Mean (M)	Standard Deviation (SD)	Interpretation
Q4. Do you think service robotics ought to adhere to a formal ethical code comparable to that of human employees?	4.96	0.19	Very High Acceptance
Q5. The ACERBOTICS Framework addresses real and pressing challenges in the Robotics Service Industry (RSI).	4.41	0.64	Very High Relevance
Q6. The framework adequately integrates multiple disciplinary perspectives (e.g., ethics, cybersecurity, HRI).	3.93	0.83	Moderate-High Integration
Q7. The framework's structure, components, and interrelationships are clearly articulated and easy to understand.	4.04	0.76	Very High Clarity
Q8. The visual representation and accompanying explanation adequately communicate the framework's purpose and scope.	4.22	0.58	Very High Comprehensibility
Q9. The framework can be practically applied in real-world service domains such as healthcare, hospitality, or logistics.	4.00	0.62	High Applicability

Table 6.62 Descriptive Summary of Expert Ratings (n = 27)

Evaluation Item	Mean (M)	Standard Deviation (SD)	Interpretation
Q10. The framework is adaptable to different organisational contexts within the service industry.	4.07	0.78	Very High Adaptability
Q11. The framework contributes significantly to the field of ethical and cybersecure robotics.	4.00	0.92	High Ethical and Cyber-Safety Contribution
Q12. There are no major omissions in the framework that could hinder its implementation or validity.	3.89	0.64	Moderate Completeness
Q13. I would recommend the use of this framework for future projects in service robotics.	4.07	0.73	Very High Endorsement
Q14. Ethical considerations such as fairness, transparency, and accountability are well-integrated within the framework.	3.96	0.81	High Integration of Ethical Principles
Q15. The framework provides a clear pathway for ensuring responsible and human-centred robotic deployment.	4.15	0.77	Very High Pathway Clarity
Q16. The framework adequately addresses data protection	3.85	0.99	High Data Protection Readiness
Q17. The framework adequately addresses threat resilience.	3.93	0.78	High Threat Resilience

Table 6.63 Descriptive Summary of Expert Ratings (n = 27)

Evaluation Item	Mean (M)	Standard Deviation (SD)	Interpretation
Q18. The framework adequately addresses system integrity.	4.19	0.68	Very High system integrity.
Q19. The cybersecurity dimension aligns with ethical and operational requirements for safe robotic deployment.	4.19	0.83	Very High Ethical-Cyber Alignment
Q20. The framework sufficiently considers human values.	3.89	0.85	High Human-centred Focus
Q21. The framework sufficiently considers cultural diversity.	4.00	0.96	High Cultural Sensitivity
Q22. The framework sufficiently considers industry-specific needs.	4.04	0.76	Very High Industry Adaptability
Q23. The socio-technical aspects are effectively integrated to enhance collaboration between humans and robots.	4.11	0.80	Very High Socio-Technical Integration
Q24. The framework is feasible for adoption by practitioners and policymakers in the service robotics field.	3.89	0.97	High Practical Feasibility
Q25. The implementation pathway described is realistic and scalable.	4.07	1.00	Very High Scalability

Table 6.1 Descriptive Summary of Expert Ratings (n = 27)

Evaluation Item	Mean (M)	Standard Deviation (SD)	Interpretation
Q26. The framework's components form a cohesive and logically structured model.	3.96	0.81	High Structural Coherence
Q27. The framework holistically addresses critical aspects such as ethics, cybersecurity, socio-technical systems, and cultural context.	4.00	0.96	Very High Holistic Coverage
Q28. The framework would be useful for guiding the ethical design, governance, and deployment of service robotics.	4.19	0.88	Very High Practical Usefulness

Table 6.1 (synthesised by author) summarises the expert evaluation results, presenting mean ratings (M) and standard deviation (SD) values for each framework dimension. The data show consistently high to very high levels of clarity, integration, and practical applicability across the framework's components. Note: Q5–Q13 were analysed, excluding 20 incomplete responses.

SD values range from 0.19 to 1.00, indicating moderate variability in expert responses and no issues affecting reliability. The lowest variability (SD = 0.54) was observed for Q11 (contribution to ethical and cybersecure robotics), indicating strong consensus on the framework's ethical and cyber-safety contributions. In contrast, the highest variability (SD = 1.00) was observed for Q25 (Realistic and scalable implementation pathway), which assessed the feasibility and scalability of the framework's implementation. This reflects differing expert perspectives on real-world implementation readiness. The divergence view is likely due to variations in industry experience or regulatory familiarity.

The consensus pattern indicates that the framework performs best in system integrity ($M = 4.19$), cyber-ethical alignment ($M = 4.19$), and practical usefulness ($M = 4.19$). This consistency suggests a common understanding of the ACERBOTICS Socio-Tactical Integrated Framework's conceptual coherence and practical potential, as well as strong professional endorsement. Moderate ratings were recorded for data protection readiness ($M = 3.85$) and practical feasibility ($M = 3.89$). This suggests that although the framework is conceptually robust, experts identified areas of further development and empirical validation might improve its implementation.

6.3.2 Reliability of Evaluation Instrument

The internal consistency of the questionnaire was assessed using Cronbach's alpha across 24 Likert-scale evaluation items (Q4-Q28). The analysis yielded a Cronbach's alpha of 0.974, indicating excellent internal consistency and high reliability among the instrument items. This result suggests that the questionnaire provided a reliable measure of expert perceptions of the conceptual robustness, ethical grounding, cyber-resilience, socio-technical integration, and applicability of the ACERBOTICS Socio-Tactical Integrated Framework.

Table 6.2 presents the reliability analysis of the expert evaluation instruments used to assess the ACERBOTICS framework, indicating the internal consistency of the Likert-scale items completed by respondents.

Table 6.662 Reliability Analysis of the Evaluation Instrument (Synthesised by author)

Coefficient	Estimate	Std. Error	95% CI	
			Lower	Upper
Cronbach's α	0.9735	0.01014	0.9536	0.9933
Mean	102.0	3.005	96.11	107.9
Variance	243.8	67.61	151.2	457.8
SD	15.61	3.136	12.30	21.40

Table 6.2 shows that the reliability analysis yielded a Cronbach's alpha coefficient of 0.974 across 25 evaluation items. The analysis was conducted using 27 complete response sets obtained from

the broader 47 expert participants. The resulting coefficient suggests excellent internal consistency, indicating that the instrument items measured related to expert perceptions regarding the framework’s conceptual robustness, ethical grounding, cyber-resilience, socio-technical integration, and applicability. The reliability coefficient substantially exceeds the common threshold of 0.70, indicating that the instrument yielded consistent, dependable responses. Detailed item-total reliability statistics, including corrected item-total correlation and Cronbach’s alpha values if individual items were deleted, are provided in Appendix P.

Table 6.3 presents a summary of the internal consistency reliability assessment of the ACERBOTICS framework evaluation instrument, based on responses obtained from expert participants.

Table 6.63 Summary of Reliability Assessment (Synthesised by author)

Measure	Value
Number of Respondents	47
Complete Responses Used for Reliability Analysis	27
Number of Evaluation Items	25
Cronbach’s Alpha (α)	0.974
Reliability Interpretation	Excellent

Table 6.3 indicates a high level of internal consistency among the expert evaluation items. The Cronbach’s alpha value of 0.974 suggests excellent reliability, supporting the robustness of the quantitative assessment results.

Appendix O contains the individual Likert-scale responses obtained from the 47 expert participants, which formed the basis for the quantitative analysis. Reliability testing was conducted on a subset of 27 complete-response records, while the broader dataset informed the descriptive statistical analysis reported in the following Section.

6.3.3 Comparative Analysis Across Framework Components

A comparative examination of the six core components, namely, Ethical Integrity, Cyber-Safety Resilience, Socio-Technical Integration, Human-centred Design, Cultural Adaptability, and Governance Alignment, showed a unique pattern (see Table 6.1). Experts rated Ethical Integrity, System Integrity, and Usefulness ($M = 4.19$) highest, indicating strong endorsement of the framework’s ethical depth and coherence. Experts perceived these components as central to the

framework's strength in integrating moral principles within autonomous system design and operational governance. Similarly, Socio-Technical Integration ($M = 4.11$) and Cultural Adaptability ($M = 4.00$) received comparatively high mean scores. This suggests that the framework effectively integrates technical automation with social and contextual variables.

However, components related to Data Protection Readiness ($M = 3.85$) and Practical Feasibility ($M = 3.89$) recorded lower means, although both remained within the High interpretation range. This showed that, although it acknowledges these dimensions, its implementational pathways, especially for contextual adaptation and cross-sector implementation, require extra refinement.

Collectively, the comparative results indicate that the ACERBOTICS showed strong internal consistency across all six pillars. Ethical and governance aspects are perceived as well developed, whereas the socio-technical and practical implementation components are perceived as promising but require further empirical refinement. These findings demonstrate the framework's contextual adaptability and coherence with minor gaps that can be addressed through industry-specific and context-specific validation.

6.3.4 Identification of Strengths and Weaknesses

6.3.4.1 Strengths

1. **Ethical and Cyber-Safety Integration:** Experts identified the framework's alignment of ethical safeguards with cyber-safety resilience as highly effective. This integration was considered a significant innovation, addressing a critical gap in service robotics research by combining moral accountability with digital safety.
2. **Conceptual Clarity and Structural Coherence:** The framework's logical organisation and visual presentation were commended for their clarity and accessibility. Experts noted that the modular structure facilitates comprehension and supports adaptability across various service sectors.
3. **Human and Context-Centric Focus:** The framework's human-centred and socio-tactical dimensions were recognised as distinctive features. The integration of cultural sensitivity and local adaptability was particularly commended for its significance for emerging economies and service-industry ecosystems.

6.3.4.2 Weakness

1. **Operational Detailing and Procedural Specification:** Although the framework is regarded as conceptually robust, experts indicated that specific components, particularly

those related to data protection and implantation feasibility, require more explicit procedural guidance, defined metrics, and monitoring tools.

2. **Socio-Technical Depth and Cross-Sector Integration:** While the framework integrates socio-technical considerations, feedback indicated that mechanisms for real-time human–robot collaboration and cross-sector transferability require further development. Experts observed that, although the framework acknowledges socio-technical dynamics, its practical mechanisms for integrating human factors, system architecture, and social context require greater specification.
3. **Empirical validation and Scalability Testing:** Experts observed that, despite the framework’s theoretical strength, empirical validation across industry contexts is necessary. Pilot testing and feedback loops were recommended to evaluate the policy’s scalability, resilience, and applicability.
4. **Cultural Adaptability:** Experts noted limited detailing of how ACERBOTICS can be contextualised within resource-constrained or culturally diverse environments, particularly in the developing economies.
5. **Operational Detailing in Cyber-Safety:** Experts suggested refining the framework’s threat modelling, risk auditing, and adaptive resilience modules to conform to current industry cybersecurity standards.

Overall, the quantitative findings confirm that the experts perceived the framework as a cohesive, conceptually robust, ethically aligned and cyber-resilient model for service robotics, with minor divergence regarding context-specific implementation. These results, supported by low variance, highlight the frameworks’ relevance and identify opportunities to improve their contextual adaptability and technical operationalisation. Such conclusions will inform the refined version of the framework presented in subsequent sections.

6.3.5 Qualitative Feedback from Expert Evaluation

Expert feedback offered valuable insights into the conceptual robustness, operational practicality, and contextual flexibility of the ACERBOTICS Socio-Tactical Integrated framework. The qualitative analysis demonstrated strong alignment with the study’s objectives, which aimed to develop a cyber-safe, ethically grounded, and socio-technically responsive framework for service robotics systems.

6.3.6 Thematic Presentation of Expert Insights

Initial analysis of open-ended responses from the expert panel identified four interrelated themes: Ethical Robustness and Integrity; Socio-Technical Integration and Contextual Adaptability; Clarity and Practical Usability; and Cyber-Safety and Governance Strengthening. Collectively, these themes capture expert perceptions of the conceptual, operational and contextual dimensions of the ACERBOTICS Socio-Tactical Integrated framework.

6.3.6.1 Ethical Robustness and Integrity

A substantial proportion of respondents consistently commended the framework's strong ethical orientation ($n = 24$), emphasising that it translates theoretical ethics into applied design principles. Respondents observed that the moral foundations, derived from VSD (Batya & David, 2019) and EAD (IEEE, 2019b), are operationalised through the autonomy and collaboration pillars. This theme demonstrates consensus regarding the framework's ethical clarity and its relevance to the responsible development of robotics.

6.3.6.2 Socio-Technical Integration and Contextual Adaptability

Respondents ($n = 21$) highlighted the framework's effectiveness in linking socio-cultural and technical systems, while a significant subset ($n = 17$) identified a need for more precise mechanisms to facilitate local adaptation in emerging economies. Several participants noted that although the framework acknowledges contextual variability, it should include a more explicit process for integrating human behavioural data and local socio-economic conditions into the deployment cycle. This feedback reflects both consensus regarding its potential and divergence concerning the depth of its operational adaptability.

6.3.6.3 Clarity and Practical Usability

A strong majority of respondents ($n = 26$) agreed that the visual and structural representations of the ACERBOTICS Socio-Tactical Integrated Framework enhance both understanding and application. One expert ($n = 1$) described it as “an effective bridge between academic theory and practical robotics governance.” A notable subset ($n = 14$), however, indicated that implementation steps would benefit from more detailed procedural guidance, particularly concerning stakeholder roles and monitoring mechanisms.

6.3.6.4 Cyber-Safety and Governance Enhancement

A significant group of experts (n = 19) emphasised the importance of further integrating risk management, data privacy, and accountability mechanisms into the framework's cyber-safety pillar. A notable subset (n = 15) recommended that more explicit specification of dynamic risk controls and integration of adaptive learning systems be implemented to enhance robustness in real-time operations.

6.4 Thematic Analysis Procedure

The expert evaluation's qualitative responses (Q29–Q32) were analysed through a thematic approach based on the six-phase model of (Braun & Clarke, 2022). Each comment was systematically reviewed, coded and categorised according to emerging meaning patterns related to the ACERBOTIC Socio-Tactical Integrated Framework. Initial analysis identified four main dimensions: Ethical Robustness and Integrity; Socio-Technical Integration and Contextual Adaptability; Cyber-Safety and Governance Strengthening; and Framework Clarity and Practical Feasibility.

Within these dimensions, eight carefully developed sub-themes were created as shown in Table 6.2, to reflect nuanced perspectives on the framework's ethical, technical, and operational robustness. These themes were then mapped to both the quantitative and qualitative findings and the theoretical foundations of the framework to ensure coherence and analytical depth.

Table 6.5 Summary of Qualitative Feedback from Expert Evaluation (n = 47) (*Synthesised by author*)

	Theme	Expert Consensus	Representative Quotation	Representative Insights	Interpretation/Implications
1	Ethical Integrity and Governance	Widespread agreement on ethical integrity and principles	“Excellent for ethical data management”	Experts commended the framework’s ethical alignment with human-focused design.	Confirms that ethical governance continues to be the fundamental basis of the framework, underpinning transparency and accountability in robotic decision-making.
2	Cyber-Safety and System Resilience	Broad agreement exists, though there is some variation in the clarity of implementation.	“Framework would benefit from more focus on post-breach recovery procedures.”	Respondents considered the cyber-safety layer to be thorough and seamlessly integrated, though some requested more explicit operational procedures and more adaptable risk controls.	Respondents viewed the cyber-safety layer as thorough and integrated, but some requested clearer operational procedures and more flexible risk controls. It demonstrates strength but requires more operational detail and more adaptable monitoring.
3	Socio-Technical Integration	Wide agreement on aligning social and technical aspects.	“The framework provides a structured, holistic approach that considers both technical and human-centred factors”	Experts highlighted that the framework links technical ability with social context, emphasising collaboration, safety, and adaptability.	Reinforces the framework's socio-technical robustness and affirms its relevance to context-aware robotic governance.
4	Human-centred and Contextual Design	Widespread agreement on human and cultural adaptability	“It allows local customisation of robot behaviour, interaction styles, and user interfaces.”	Experts observed that the framework demonstrates sensitivity to human values and cultural diversity.	Confirms that human-centred inclusion enhances framework flexibility and addresses ethical considerations across diverse sociocultural contexts.
5	Service Sector Responsiveness	Partial agreement with suggestions for domain-specific alignment.	“Adaptable, though needs customization for retail use.”	Experts highlighted the framework’s potential for cross-sector adaptability while suggesting a clearer service-specific context.	Indicates that, although the framework has broad service relevance, future empirical work should reinforce industry-specific guidance on implementation.
6	Practical Feasibility and Implementation	Varied opinions depending on sector and experience.	“The framework is promising but a bit complex for entry-level technicians.”	Many respondents described the framework as practically feasible but resource-intensive, highlighting barriers in low-infrastructure environments.	Emphasises the importance of creating pragmatic, context-specific deployment strategies for resource-limited settings.

Table 6.5 Summary of Qualitative Feedback from Expert Evaluation (n = 47) *(Synthesised by author)*

	Theme	Expert Consensus	Representative Quotation	Representative Insights	Interpretation/Implications
7	Framework Clarity and Structural Coherence	Strong agreement on the overall structural clarity	“The structure helps new professionals understand robot ethics clearly.”	Experts observed that the visual design and conceptual logic are robust, though some suggested minor refinements to the terminology to enhance technical precision.	Confirms the framework's structural strength and logical flow in its conceptual and operational design.
8	Empirical Validation and Scalability	Widespread agreement that field-based testing is necessary	“Field testing across different service environments is necessary before large-scale implementation.”	Many experts emphasised that empirical testing and long-term observation are crucial to verify applicability.	Emphasises the need for future empirical validation and scalability assessments to enhance generalisation and real-world adoption.

Table 6.2 offers a thematic synthesis of expert qualitative feedback on the ACERBOTICS Socio-Tactical Integrated Framework. The findings emphasise strong support for its ethical safeguards, socio-technical integration, and structural coherence, alongside suggestions for clearer operational details, contextual adaptations, and empirical validation. These insights contributed to the refinement and conceptual development of the framework.

Each expert's open-ended comments were reviewed to identify recurring concepts related to the framework. Standard codes included ethical clarity, practical feasibility, integration of technology and society, clarity of cyber-safety, and implementation challenges. These were grouped into initial

categories aligned with the framework's primary constructs, such as ethics, cyber-safety, socio-technical integration, and human-centred. Subsequently, the codes were clustered into broader themes reflecting underlying meaning patterns across responses, as shown:

- Comments on moral logic, responsibility, and ethics – Ethical Integrity and Governance
- References to data protection, risk management, and security – Cyber-Safety and System Resilience.
- Insights on socio-technical collaboration and adaptability – Socio-Technical Integration.
- Feedback on human values, cultural diversity, and inclusivity – Human-centred and Contextual design.
- References to service industry adaptability and domain specificity – Service Sector Responsiveness.
- Discussions on implementation challenges and feasibility – Practical Feasibility and Implementation.

Observations on clarity, structure, and terminology were cross-checked against evaluation items (Q5–Q28) and the refined framework to ensure consistency. Only comments that aligned with expert consensus and the framework dimensions were retained. Thus, the eight themes reflect both the empirical content of expert commentary and the core theoretical pillars of the ACERBOTICS framework, thereby ensuring conceptual coherence.

6.4.1 Areas of Convergence

Experts broadly agreed on three points:

- A significant majority (87.2%) affirmed that the framework demonstrates conceptual robustness, ethical grounding and relevance to contemporary challenges in service robotics.
- While (83%) identified that the integration of ethics and cyber-safety is regarded as the framework's most significant contribution to global robotics governance.

- Notably, (91.5%) endorsed the visual clarity and modular structure of the framework, rendering it suitable for cross-sector applications and academic evaluation.

6.4.2 Areas of Divergence

Key divergences were observed in:

- **Socio-cultural adaptability:** Experts from different fields expressed divergent views regarding the framework's effectiveness in accounting for contextual differences. Some experts considered it sufficient, whereas others emphasised the necessity for local calibration.
- **Operational detailing:** Opinions varied regarding whether the framework offers sufficient procedural guidance for practical adoption. Some experts viewed its flexibility as advantageous, while others perceived it as a source of ambiguity.
- **Cybersecurity implementation depth:** Although conceptually robust, several respondents recommended further development of measurable resilience metrics and data protection guidelines.

6.4.3 Integrated Summary of Key Evaluative Outcomes

A significant majority of experts (89.4%) endorsed the ethical and governance components of the framework, highlighting its capacity to integrate autonomy, moral responsibility, and cyber-resilience into a unified framework. They praised the socio-tactical loop and iterative governance model for their clear operational focus and emphasis on human–robot collaboration. However, one-third of respondents (34.0%) noted that improving implementation feasibility and empirical validation are necessary, as these areas require further procedural development to enhance scalability and better align with policies.

6.5 Summary of Key Findings

The expert evaluation identified four main points. Firstly, the ACERBOTICS framework was considered conceptually robust and ethically sound. Secondly, respondents valued the integration of cyber-safety, socio-technical, and human-centred aspects into a single governance system. Thirdly, experts noted the framework's flexibility across various service sectors and suggested more practical guidance for local use. Lastly, participants stressed the importance of ongoing empirical testing to enhance scalability and real-world applicability. These insights helped guide the refinement of the frameworks discussed in the following sections.

6.6 Implementations of Feedback for Framework Refinement

The expert evaluation aimed to assess the ACERBOTICS framework's conceptual robustness, coherence, relevance, and applicability in various service robotics contexts. It is important to note that this evaluation does not serve as empirical validation of operational performance; instead, it offers an expert-based review focusing on the framework's completeness, relevance, and applicability. The insights gained were used to refine the framework and reinforce its theoretical basis.

The qualitative feedback affirms the three central study objectives:

- **Objective 1 (Cyber-Safety):** Experts validated the inclusion of cyber-resistance and system integrity mechanisms as essential safeguards against data vulnerabilities.
- **Objective 2 (Ethical Safeguards):** Responses endorsed the ethical sensitivity and governance logic of the framework, confirming its alignment with global frameworks like the VSD and EAD.
- **Objective 3 (Unified Framework Development):** evaluators agreed that the integrated model effectively integrates ethical, cybersecurity, and socio-technical dimensions, offering a cohesive framework for robotics deployment in service industries.

Overall, evaluators expressed confidence in ACERBOTICS as a forward-looking, theoretically robust, and contextually adaptable framework that can guide the safe and ethical deployment of service robotic systems across diverse global and African settings. The qualitative evaluation demonstrates strong support for the framework's ethical and governance aspects, human-centred adaptability, and cross-sector applicability, and offers constructive suggestions to improve its cultural adaptation, cyber-safety resilience, and operational clarity, as well as empirical validation. These findings directly support the iterative improvement and future validation phases of the framework, align with the previously discussed quantitative trends, and provide a conceptual basis for refining the framework in Section 6.5.

6.7 Refined Framework Based on Expert Feedback

6.7.1 Rationale for Refinement

The Refinement of the ACERBOTICS Socio-Tactical Integrated Framework was informed by empirical evidence from expert evaluations and perspectives on ethical issues, cyber-safety governance, and socio-technical systems. While expert feedback affirmed the framework's conceptual coherence and ethical foundation, it also identified the need for more explicit

operational pathways, greater terminological precision, and improved procedural integration. These refinements are consistent with the principles of VSD (Batya & David, 2019) and EAD (IEEE, 2019b)(IEEE, 2019b)(IEEE, 2019b)(IEEE, 2019b), both of which emphasised iterative adaptation based on stakeholder engagement and context-specific feedback. Accordingly, the refinements are intended to:

- Strengthen conceptual soundness by addressing conceptual vagueness in autonomy, tactical responsiveness, and governance flow.
- Enhance practical relevance through linking high-level ethical imperatives with concrete operational processes.
- Improve empirical strength by ensuring clearer indicators for future validation and measurement.

As a result, the refinement of the framework reflects the expert consensus that an effective governance framework for service robotics must holistically integrate ethics, cyber-safety resilience, and socio-technical adaptability within a unified, context-aware structure.

6.7.2 Description of Modifications

Drawing on expert commentary and a synthesis of relevant literature, the ACERBOTICS Socio-Tactical Integrated Framework was refined along three primary dimensions:

1. Expanded and Added Components

- **System Resilience:** Added as a distinct component within the cyber-safety pillar to expand the focus beyond defensive security, encompassing proactive operational continuity and adaptive recovery.
- **Industry Alignment:** Introduced as a central pillar connecting ethical governance with practical sectoral adaptation, reflecting expert emphasis on domain-specific feasibility in areas such as healthcare, tourism, and retail.
- **Socio-Tactical Loop:** Enhanced to function as a dynamic feedback cycle among governance, human–robot collaboration, and deployment, thereby supporting real-time ethical and cyber-safety responsiveness.

2. Revised Relationships and Processes

- **Bi-directional Governance Flow:** Expert feedback led to the incorporation of reciprocal mechanisms between tactical responsiveness and ethical governance layers, ensuring continuous linkage between policy oversight and operational feedback.

- **Iterative Adaptation Process:** The relationship between autonomy and collaboration was reconceptualised as an adaptive, cyclical process rather than a linear progression, thereby capturing the iterative nature of socio-technical co-evolution.

3. Clarification of Constructs and Terminology

- Terms such as “tactical governance” and “system integrity” were revised to emphasise measurable attributes including decision-making, transparency, data resilience, and ethical accountability.
- Overlapping concepts within autonomy, collaboration, and cyber-resilience were harmonised to ensure conceptual clarity across academic and professional contexts.

6.8 Presentation of the Refined ACERBOTICS Socio-Tactical Integrated Framework

The refined ACERBOTICS Socio-Tactical Integrated Framework offers a cohesive structure organised around six interdependent pillars: Ethical Governance Core, Cyber-Safety and System Resilience, Socio-Technical Integration, Human-centred Design, Industry Alignment, and Service-Sector Responsiveness. Central to the framework is the Socio-Tactical Governance Loop, which represents the iterative interactions between ethical oversight, tactical decision-making, and feedback-driven adaptation.

Figure 6.1 presents the refined ACERBOTICS Socio-Tactical Integrated Framework, showing how ethical, cyber-safety, and human-centred principles are integrated to guide the deployment and governance of service robotic systems.

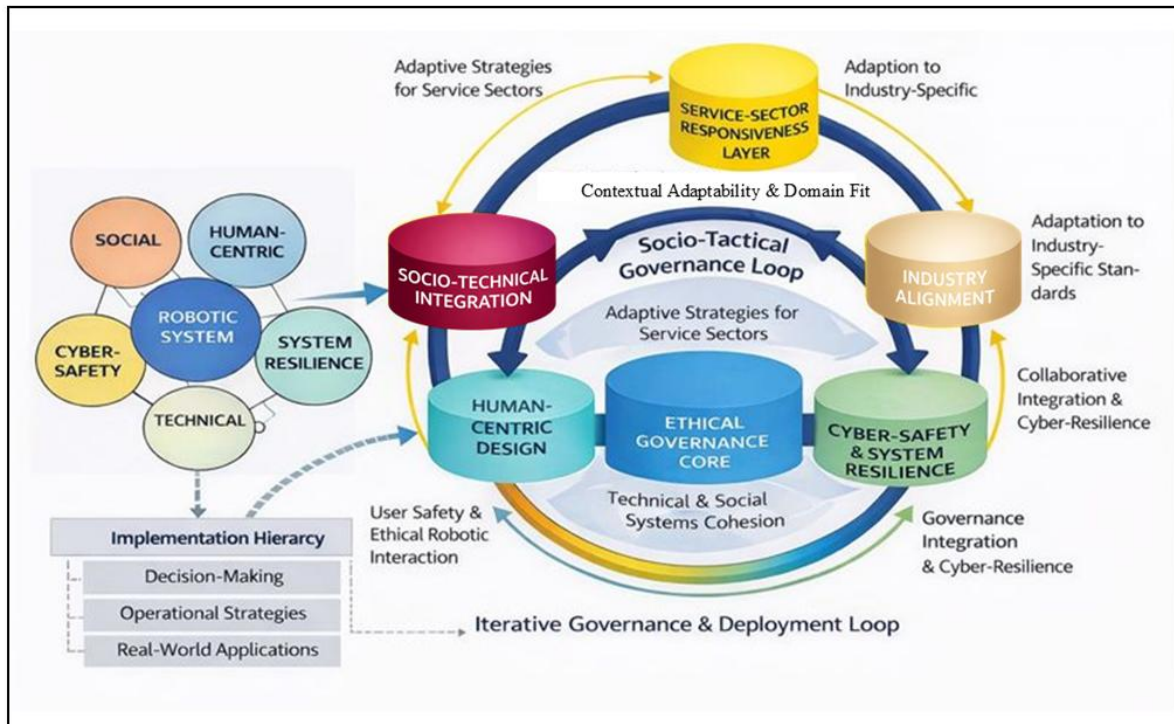


Figure 6.1 Refined ACERBOTICS Socio-Tactical Integrated Framework

(Synthesised by the author)

The ACERBOTICS Socio-Tactical Integrated Framework, based on expert feedback, comprises six interconnected pillars: Service-Sector Responsiveness, Industry Alignment, Cyber-Safety and System Resilience, Ethical Governance Core, Human-centred Design, and Socio-Technical Integration. A central Socio-Tactical Governance Loop unifies them, enabling iterative governance and adaptable deployment across sectors.

6.8.1 Comparison with the Initial ACERBOTICS Framework

The initial framework centred on static alignment among ethics, cyber-safety, and service applicability. In contrast, the refined version introduces reciprocity, ensuring that ethical considerations, cyber-safety mechanisms, and operational practices continuously inform each other through an iterative governance and learning cycle.

6.8.2 Enhancement Outcomes

- **Validity:** Enhanced by the integration of explicit constructs such as system resilience and industry alignment, both grounded in empirical feedback and conceptual rigour.
- **Applicability:** Improved by establishing more apparent operational linkages, increasing domain adaptability and expanding pathways for sector-specific implementation.
- **Conceptual robustness:** Enhanced by embedding the framework within a socio-tactical paradigm that unites human factors, cultural dimensions, and technological governance into a single architecture.

The refined ACERBOTICS Socio-Tactical Integrated Framework, therefore, constitutes a comprehensive socio-tactical governance architecture for the ethical and cyber-safe deployment of service robotic systems. By integrating theoretical principles with expert-driven refinements, it bridges the gap between conceptual vision and practical application, supporting cultural and ethical resilience and technological adaptation across diverse service industry contexts.

6.9 Conclusion

This chapter synthesised the outcomes of expert evaluation, conceptual enhancements, and practical implications related to the ACERBOTICS Socio-Tactical Integrated Framework. The evaluation confirmed that the framework demonstrates high ethical clarity, strong cyber-safety integration, and robust socio-technical adaptability. The improved design, grounded in expert consensus, demonstrates enhanced conceptual soundness, operational applicability and cross-disciplinary significance. Within the broader academic discourse, the ACERBOTICS Socio-Tactical Integrated Framework deepens understanding of how ethical governance and cyber-safety can be strategically integrated in service robotic systems to promote sustainable and integrative innovation.

Chapter 7: Discussion, Conclusion and Recommendations

7.1 Introduction

This chapter presents a critical synthesis of the findings emerging from the evaluation and refinement of the ACERBOTICS Socio-Tactical Integrated Framework. Building on critical insights from expert assessments, it interprets the results within the wider theoretical and practical contexts of ethical robotics, cyber-safety, and socio-technical governance in service industries. The chapter bridges the analytical outcomes of Chapter 6 with the overarching research objectives, offering a logical discussion of how the refined framework addresses identified gaps and advances both scholarship and professional practice.

The chapter is organised into the following sections: Section 7.2 examines the study's findings in relation to the research questions, pointing out how expert evaluation confirmed, refined, or extended the conceptual propositions from earlier chapters. Sections 7.3 to 7.5 analyse the conceptual, methodological, and real-world implications of the study with particular attention to its contribution to responsible innovation in robotic system design and deployment. Section 7.6 addresses the study's limitations, providing a fair assessment of methodological and directions for future research, identifying pathways for practical validation, contextual expansion, and long-term policy integration. Section 7.7 provides directions for future research, and section 7.8 provides the study's conclusion, summarising its significance and situating it within the wider scholarly debate.

This structure enables the chapter to integrate reflection, critique, and projection, culminating in a thorough understanding of the ACERBOTICS framework's scholarly and practical significance in advancing ethical, cyber-safety service robotics in both developing and global contexts.

7.2 Discussion

7.2.1 Interpretation of Findings in Relation to Research Questions

The expert evaluation and subsequent refinement of the ACERBOTICS Framework directly address the research questions and objectives. For research, Sub-Question 1: How can cyber-safety measures be deployed to safeguard sensitive data and maintain operational integrity? which examined cyber-safety vulnerabilities and mechanisms for ensuring system integrity. Expert feedback confirmed that the framework's Cyber-Safety and System Resilience pillar effectively integrates data protection, threat mitigation strategies and adaptive security processes. This outcome challenges the initial assumption that ethical and cyber-safety governance could function as parallel constructs, demonstrating that they must operate as interdependent layers of governance. The SLR identified recurring vulnerabilities, such as unauthorised access, data breaches, insecure communication protocols, and cyber-physical manipulation risks, thereby fulfilling Objective 1 by providing a structured understanding of cybersecurity vulnerabilities in networked robotic systems and informing the development of the framework's Cyber-Safety and System Resilience pillar. Consequently, Objective 1 was achieved by identifying, synthesising, and incorporating these vulnerabilities into the framework design process.

For the research, Sub-Question 2: How can standardised ethical guidelines be developed to mitigate safety risks associated with algorithmic flaws in service robotics? which addresses ethical guidelines and mitigation of algorithmic risks. Expert consensus validated that the Ethical Governance Core and Human-centred Design components operationalise ethical decision-making within tactical processes. This result confirms the framework's alignment with VSD principles and extends these approaches by incorporating socio-tactical responsiveness.

In response to the research, Sub-Question 3: How can a unified framework incorporating cybersecurity measures, ethical safeguards, and HRI principles be developed for service robot deployment in the service industry? which sought to unify cyber-safety, ethics, and HRI within a deployable service robotics framework, experts endorsed the Socio-Tactical Governance Loop as the integrative mechanism, and confirmed the framework's conceptual unification, while also recommending further enhancements to increase practical scalability and cultural adaptation. This extends the preliminary assumptions and acknowledges contextual limitations.

7.2.2 Reflection on Research Objectives

The results of this study show that all research objectives have been achieved through a process of SLR, the development of a framework, and expert evaluation. Objective 1 involved investigating cybersecurity vulnerabilities in networked robotic systems. The literature review identified recurring vulnerabilities, including unauthorised access, data breaches, insecure communication protocols, cyber-physical manipulation risks, software and firmware vulnerabilities, and cloud-based security risks. These insights guided the development of the Cyber-Safety and System Resilience pillar within the ACERBOTICS framework. Objective 2 examined the alignment of existing regulatory measures with ethical principles and standards in RSI. This was achieved by analysing the alignment between ethical frameworks, governance models and regulatory instruments, including the IEEE Ethically Aligned Design framework (IEEE, 2019a) and new legislative instruments such as the EU AI Act and the Cyber Resilience Act (ENISA, 2020). The analysis demonstrated that these instruments share common principles relating to transparency, accountability, human oversight, and safety, thereby informing the governance structure of the proposed framework. Objective 3 addressed the development of a conceptual framework to mitigate cybersecurity risks, address ethical considerations, and ensure operational safety in the deployment of service robotics. This objective was achieved through the design, expert evaluation, refinement, and presentation of the ACERBOTICS Socio-Tactical Integrated Framework.

Table 7.1 presents a summary of the research objectives and the achievements through evidence from the study (Synthesised by author)

Table 7.1 Summary of Research Objectives Outcome (Synthesised by author)

Research Objective	Evidence from the Study	Outcome
Objective 1: To investigate cybersecurity vulnerabilities in networked robotics systems.	SLR identified recurring vulnerabilities such as unauthorised access, data breaches, insecure communication protocols, cyber-physical manipulation risks, software and firmware vulnerabilities, and cloud-based security risks, which informed the development of the Cyber-Safety and System Resilience pillar within the ACERBOTICS framework	Achieved
Objective 2: To examine the alignment of existing regulatory measures with ethical principles and standards in RSI.	Analysis of the alignment between ethical frameworks, governance models and regulatory developments, such as EAD, VSD, the EU AI Act and the Cyber Resilience Act, identifying shared principles of transparency, accountability, safety, and human oversight	Achieved
Objective 3: To develop a unified framework that mitigates cybersecurity risks, ethical considerations, and operational safety when deploying service robotics.	Development, expert evaluation, refinement, and presentation of the ACERBOTICS Socio-Tactical Integrated Framework.	Achieved

Table 7.1 summarises the research objectives, the evidence produced by the study, and the extent to which each objective was achieved. The table demonstrates alignment among the study objectives, findings, and framework development outcomes.

7.3 Conceptual Implications

The refined ACERBOTICS Socio-Tactical Integrated Framework advances conceptual discourse in three ways:

- First, the framework bridges the gap between ethical robotics and cyber-safety governance by providing a structured architecture that aligns ethical principles with system resilience.
- Second, the framework operationalises socio-technical system theory by embedding iterative feedback and tactical adaptation, thereby extending the conceptual scope of human–robot collaboration.
- Third, the ACERBOTICS Socio-Tactical Integrated Framework enhances conceptual clarity in robotics ethics by positioning ethical governance within a dynamic, multi-pillar architecture rather than a static normative layer.

This integration diverges from existing models that isolate ethical or technical components, instead presenting an integrated socio-tactical paradigm for future robotics governance and service-based deployment.

7.4 Methodological Implications

The expert evaluation approach effectively validated conceptual models that integrate ethics, technology, and governance. Methodologically, the results show that expert-informed triangulation enhances both construct validity and practical transferability, especially within interdisciplinary frameworks. The mixed-method analysis, which combined descriptive consensus metrics with thematic insights, offered a balanced perspective that captured both conceptual strength and practical relevance. However, reliance on domain-specific experts introduces interpretive inconsistencies, suggesting that subsequent studies should complement such evaluations with empirically supported field testing.

For future studies and framework development, this approach reinforces the need of iterative co-design and stakeholder participation in refining models before empirical testing.

7.5 Practical and Policy Implications

The refined ACERBOTICS Socio-Tactical Integrated Framework is highly valuable for practitioners, policymakers, and organisations aiming to deploy service robotics ethically and securely. Essentially, the framework provides a decision-support structure that integrates ethics and cybersecurity into deployment planning, compliance auditing, and design evaluation. For organisations, it provides a scalable governance blueprint adaptable to specific sector needs, particularly in healthcare, hospitality, and logistics, where HRI is frequent. Policymakers can utilise the framework as a reference when drafting regulatory guidelines and national robotics governance strategies, aligned with international standards such as ISO/IEC 23839 (AI Risk Management), STS and EAD principles. Overall, the ACERBOTICS Socio-Tactical Integrated Framework lays a solid foundation for developing context-aware, ethically grounded robotic ecosystems in emerging economies.

7.6 Limitations of the Study

Although the expert evaluation provided valuable insights, several limitations must be considered. Methodologically, the small sample size of expert respondents and uneven sectoral representation limit the generalisability of the findings. In context, the lack of empirical evidence suggests that the framework's real-world effectiveness remains untested in operational settings. Conceptually, while the socio-tactical model captures dynamic feedback mechanisms, it needs further empirical grounding to evaluate scalability and long-term adaptability. These limitations do not diminish the framework's conceptual contributions; instead, they outline directions for iterative improvement and further research.

7.7 Directions for Future Research

Based on the current findings, several directions for future research are outlined:

1. **Empirical Validation:** Conduct field tests of the ACERBOTICS Socio-Tactical Integrated Framework in real-world service industry environments to assess its practical utility and socio-ethical effects.
2. **Cross-Cultural Application:** Examine the framework across various socio-economic contexts, especially within other emerging economies beyond Africa.
3. **Longitudinal Research:** Evaluate the framework's long-term impact on workforce adaptation, regulatory adherence, and technological trust.

4. **Integration Studies:** Broaden the framework's scope by connecting it with human-centred digital ethics, AI, and cyber-safety governance ecosystems.

These avenues will support the ongoing development of the ACERBOTICS Socio-Tactical Integrated Framework into a robust socio-tactical governance model.

7.8 Chapter Summary

Chapter 7 offered a synthesis of expert evaluations, framework refinements, and theoretical and practical insights. The findings confirmed that the ACERBOTICS Socio-Tactical Integrated Framework is conceptually robust, ethically grounded, and adaptable across various industries. The refined framework enhances government coherence, system resilience, and ethical responsiveness, providing both a theoretical contribution to robotics scholarship and a practical guide for responsible deployment. The chapter establishes the ACERBOTICS Socio-Tactical Integrated Framework as a foundational blueprint for future research, innovation, and policy development in ethical, cyber-safe, and socio-tactical robotics.

7.9 Conclusion

This study illustrated the complexity of creating governance frameworks for service robotics, especially where cyber-safety, ethics, and socio-technical factors converge. The systematic review and expert analysis found that current approaches often treat these aspects separately, leading to implementation gaps in practical service settings. Improving the ACERBOTICS Socio-Tactical Integrated Framework emphasised the importance of integrating technical safeguards within human-centred governance models. Although the framework provides a clear structure for addressing these issues, the study also highlighted the need for ongoing empirical testing across various operational contexts to enhance its practical use and scalability.

This study shows that ethical regulation and cyber-safety are now central to service robotics, not optional. The ACERBOTICS Socio-tactical Integrated Framework presents a practical blueprint for responsible innovation, system resilience, and the alignment of robotics with human dignity and accountability. Overall, the ACERBOTICS framework contributes to the sustainable, trustworthy development of service robotic systems.

References

- Abbass, H. (2021). What is Artificial Intelligence ? *IEEE Transactions on Artificial Intelligence*, 2(2), 94–95. <https://doi.org/10.1109/TAI.2021.3096243>
- Afsheen, S., Fathima, L., Khan, Z., & Elahi, M. (2018). A self-sufficient waiter robo for serving in restaurants. *International Journal for Advance Research and Development*, 3(5), 57–67.
- Ahlborg, H., Ruiz-Mercado, I., Molander, S., & Masera, O. (2019a). Bringing technology into social-ecological systems research-Motivations for a socio-technical-ecological systems approach. *Sustainability (Switzerland)*, 11(7), 1–23. <https://doi.org/10.3390/su11072009>
- Ahlborg, H., Ruiz-Mercado, I., Molander, S., & Masera, O. (2019b). Bringing technology into social-ecological systems research-Motivations for a socio-technical-ecological systems approach. *Sustainability (Switzerland)*, 11(7), 1–23. <https://doi.org/10.3390/su11072009>
- Aydemir, F. B., & Dalpiaz, F. (2018). A roadmap for ethics-aware software engineering. *Proceedings - International Conference on Software Engineering*, 15–21. <https://doi.org/10.1145/3194770.3194778S>
- Batya, F., & David, G. H. (2019). Value Sensitive Design: Shaping Technology with Moral Imagination. In *Value Sensitive Design: Shaping Technology with Moral Imagination* (pp. 1-11.).
- Belanche, D., Casalo, L. V., Flavián, C., & Schepers, J. (2020). Service robot implementation: a theoretical framework and research agenda. *Service Industries Journal*, 40(3–4), 203–225. <https://doi.org/10.1080/02642069.2019.1672666>
- Belk, R. (2021). Ethical issues in service robotics and artificial intelligence. *Service Industries Journal*, 41(13–14), 860–876. <https://doi.org/10.1080/02642069.2020.1727892>
- Benjumea, D. C. (2024a). Formalising Safety Requirements for Robotic Autonomous Systems in Highly Regulated Domains. *Proceedings of the IEEE International Conference on Requirements Engineering*, 512–516. <https://doi.org/10.1109/RE59067.2024.00066>
- Benjumea, D. C. (2024b). Formalising Safety Requirements for Robotic Autonomous Systems in Highly Regulated Domains. *Proceedings of the IEEE International Conference on Requirements Engineering*, 512–516. <https://doi.org/10.1109/RE59067.2024.00066>
- Berger, G. S., Pereira, A. I., & Costa, P. (2022). RobotAtFactory 4 . 0 : a ROS framework for the SimTwo simulator models of potential solutions to problems encountered in the. *IEEE*

International Conference on Autonomous Robot Systems and Competitions (ICARSC)
Santa Maria Da Feira, Portugal, (4), 205–210.

- Bhimasta, R. A., & Kuo, P. Y. (2019). What causes the adoption failure of service robots? A case of henn-na hotel in Japan. *Adjunct Proceedings of the 2019 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2019 ACM International Symposium on Wearable Computers*, (September), 1107–1112.
<https://doi.org/10.1145/3341162.3350843>
- Blaurock, M., Čaić, M., Okan, M., & Henkel, A. P. (2022). Robotic role theory: an integrative review of human–robot service interaction to advance role theory in the age of social robots. *Journal of Service Management*, 33(6), 27–49. <https://doi.org/10.1108/JOSM-09-2021-0345>
- Bockshecker, A., Hackstein, S., Baumöl, U., & Research Bockshecker, C. (2018). *Association for Information Systems AIS Electronic Library (AISeL) Systematization of the term digital transformation and its phenomena from a socio-technical perspective-A literature review Recommended Citation "Systematization of the term digital transf.* 11–28.
- Borenstein, J., & Arkin, R. (2016). Robotic Nudges : The Ethics of Engineering a More Socially Just Human Being. *Science and Engineering Ethics*, 31–46.
<https://doi.org/10.1007/s11948-015-9636-2>
- Bowen, J., & Morosan, C. (2018). Beware hospitality industry: the robots are coming. *Worldwide Hospitality and Tourism Themes*, 10(6), 726–733.
<https://doi.org/10.1108/WHATT-07-2018-0045>
- Braun, V., & Clarke, V. (2022). Thematic Analysis:A Practical Guide. *Canadian Journal of Program Evaluation*, 38(1), 376.
- Brown-Acquaye, W., Arthur, J. K., & Forgor, L. (2019). Developing A Framework for A Tactile Internet Enabled Robot Assisted Real-Time Interactive Medical System. *2019 International Conference on Communications, Signal Processing and Networks, ICCSPN 2019*. <https://doi.org/10.1109/ICCSPN46366.2019.9150190>
- Callari, T. C., Vecellio Segate, R., Hubbard, E. M., Daly, A., & Lohse, N. (2024a). An ethical framework for human-robot collaboration for the future people-centric manufacturing: A

collaborative endeavour with European subject-matter experts in ethics. *Technology in Society*, 78(August), 102680. <https://doi.org/10.1016/j.techsoc.2024.102680>

Callari, T. C., Vecellio Segate, R., Hubbard, E. M., Daly, A., & Lohse, N. (2024b). An ethical framework for human-robot collaboration for the future people-centric manufacturing: A collaborative endeavour with European subject-matter experts in ethics. *Technology in Society*, 78(August), 102680. <https://doi.org/10.1016/j.techsoc.2024.102680>

Chen, T., Guo, W., Gao, X., & Liang, Z. (2021). AI-based self-service technology in public service delivery: User experience and influencing factors. *Government Information Quarterly*, 38(4), 101520. <https://doi.org/10.1016/j.giq.2020.101520>

Cheong, A., Foo, E., Gan, H., Chen, J., & Lau, M. (2015). *Development of a Robotics Waiter System for the food and beverage industry*. 21–25. <https://doi.org/10.15224/978-1-63248-066-8-57>

Choi, Y., Choi, M., Oh, M., & Kim, S. (2020). Service robots in hotels: understanding the service quality perceptions of human-robot interaction. *Journal of Hospitality Marketing and Management*, 29(6), 613–635. <https://doi.org/10.1080/19368623.2020.1703871>

Cooke, L. (2020). Ethics in information technology. *ISACA Journal*, 6, 6–8. <https://doi.org/10.1017/cbo9781107445666.007>

Creswell, J. W., & Creswell, J. D. (2018). Research Design: Qualitative, Quantitative, and Mixed-Method Approaches. In *Writing Center Talk over Time*. <https://doi.org/10.4324/9780429469237-3>

Davies, Clare., & Fisher, Murray. (2018). Understanding research paradigms. *JARNA*, 21(3), 1–14.

Dutta, V., & Zielińska, T. (2021). Cybersecurity of robotic systems: Leading challenges and robotic system design methodology. *Electronics (Switzerland)*, 10(22). <https://doi.org/10.3390/electronics10222850>

Dwivedi, Y. K., Hughes, D. L., Coombs, C., Constantiou, I., Duan, Y., Edwards, J. S., Gupta, B., Lal, B., Misra, S., Prashant, P., Raman, R., Rana, N. P., Sharma, S. K., & Upadhyay, N. (2020). Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. *International Journal of Information Management*, 55(July), 102211. <https://doi.org/10.1016/j.ijinfomgt.2020.102211>

- ENISA. (2020). The EU Cybersecurity Act and European standards: an introduction to the role of European standardization. *International Cybersecurity Law Review*, 1(9), 7–12.
<https://link.springer.com/article/10.1365/s43439-020-00008-1>
- Essien, A. E., & Chukwukelu, G. (2022). Deep learning in hospitality and tourism: a research framework agenda for future research. *International Journal of Contemporary Hospitality Management*, 34(September). <https://doi.org/10.1108/IJCHM-09-2021-1176/full/html>.
- Etemad-Sajadi, R., Soussan, A., & Schöpfer, T. (2022). How Ethical Issues Raised by Human–Robot Interaction can Impact the Intention to use the Robot? *International Journal of Social Robotics*, 14(4), 1103–1115. <https://doi.org/10.1007/s12369-021-00857-8>
- Ferri, F., Grifoni, P., & Guzzo, T. (2020). Online Learning and Emergency Remote Teaching: Opportunities and Challenges in Emergency Situations. *Societies*, 10(4), 86.
<https://doi.org/10.3390/soc10040086>
- Filieri, R., D’Amico, E., Destefanis, A., Paolucci, E., & Raguseo, E. (2021). Artificial intelligence (AI) for tourism: an European-based study on successful AI tourism start-ups. *International Journal of Contemporary Hospitality Management*, 33(11), 4099–4125.
<https://doi.org/10.1108/IJCHM-02-2021-0220>
- Flavián, C., & Casaló, L. V. (2021). Artificial intelligence in services: current trends, benefits and challenges. *Service Industries Journal*, 41(13–14), 853–859.
<https://doi.org/10.1080/02642069.2021.1989177>
- Floridi, L. (2023). *The Ethics of Artificial Intelligence*.
- Floridi, L., Cows, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018a). AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. *Minds and Machines*, 28(4), 689–707.
<https://doi.org/10.1007/s11023-018-9482-5>
- Floridi, L., Cows, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018b). AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. *Minds and Machines*, 28(4), 689–707.
<https://doi.org/10.1007/s11023-018-9482-5>

- Formosa, P., Wilson, M., & Richards, D. (2021). A principlist framework for cybersecurity ethics. *Computers and Security*, 109, 102382. <https://doi.org/10.1016/j.cose.2021.102382>
- Fosch-Villaronga, E., & Mahler, T. (2021). Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots. *Computer Law & Security Review*, *Undefined*.
- Foster, M. E., Gaschler, A., & Giuliani, M. (2017). Automatically Classifying User Engagement for Dynamic Multi-party Human–Robot Interaction. *International Journal of Social Robotics*, 9(5), 659–674. <https://doi.org/10.1007/s12369-017-0414-y>
- Friedman, B., & Hendry, D. G. (2019). Value Sensitive Design: Shaping Technology with Moral Imagination. In *Value Sensitive Design: Shaping Technology with Moral Imagination* (pp. 1-11.).
- Gonzalez-Aguirre, J. A., Osorio-Oliveros, R., Rodríguez-Hernández, K. L., Lizárraga-Iturralde, J., Menendez, R. M., Ramírez-Mendoza, R. A., Ramírez-Moreno, M. A., & Lozoya-Santos, J. de J. (2021). Service robots: Trends and technology. *Applied Sciences (Switzerland)*, 11(22). <https://doi.org/10.3390/app112210702>
- Govers, M., & van Amelsvoort, P. (2023a). A theoretical essay on socio-technical systems design thinking in the era of digital transformation. *Gruppe. Interaktion. Organisation. Zeitschrift Fur Angewandte Organisationspsychologie*, 54(1), 27–40. <https://doi.org/10.1007/s11612-023-00675-8>
- Govers, M., & van Amelsvoort, P. (2023b). A theoretical essay on socio-technical systems design thinking in the era of digital transformation. *Gruppe. Interaktion. Organisation. Zeitschrift Fur Angewandte Organisationspsychologie*, 54(1), 27–40. <https://doi.org/10.1007/s11612-023-00675-8>
- Guo, L., Gong, L., Xu, Z., Wang, W., & Chen, M. H. (2024). The role of service robots in enhancing customer satisfaction in embarrassing contexts. *Journal of Hospitality and Tourism Management*, 59(October 2023), 116–126. <https://doi.org/10.1016/j.jhtm.2024.04.008>
- Gutwirth, S., Leenes, R., & De Hert, P. (2016). Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection. In S. Pompeu, Casanovas (UAB Institute of Law and Technology, Bellaterra, Barcelona & I. Sartor, Giovanni (European

University Institute, Florence (Eds.), *Law, Governance and Technology Series* (Vol. 24). Springer International Publishing.

Hasan, A. S. M. M., & Trianni, A. (2022a). Towards a Framework to Assess the Impact of Industry 4.0 Technologies & Services on Production Resources. *IEEE International Conference on Industrial Engineering and Engineering Management, 2022-Decem*, 752–756. <https://doi.org/10.1109/IEEM55944.2022.9989725>

Hasan, A. S. M. M., & Trianni, A. (2022b). Towards a Framework to Assess the Impact of Industry 4.0 Technologies & Services on Production Resources. *IEEE International Conference on Industrial Engineering and Engineering Management, 2022-Decem*, 752–756. <https://doi.org/10.1109/IEEM55944.2022.9989725>

Haskard, A., Herath, D. C., & Assaad, Z. (2022). Secure Robotics: A Definition and a Brief Review from a Cybersecurity Control and Implementation Methodology Perspective. *ArXiv, abs/2211.0*, 1–9.

Hevner, A., March, S., Park, J., & Ram, S. (n.d.). Design science in information systems research Research. *Aisel.Aisnet.Org*. Retrieved June 6, 2026, from <https://aisel.aisnet.org/misq/vol28/iss1/6/>

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2008). Design science in information systems research. *Management Information Systems Quarterly*, 28(1).

Huang, D., Chen, Q., Huang, J., Kong, S., & Li, Z. (2021). Customer-robot interactions: Understanding customer experience with service robot. *International Journal of Hospitality Management*, 99(July), 103078. <https://doi.org/10.1016/j.ijhm.2021.103078>

IEEE, F. E. (2019a). Ethically Aligned Design. *The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems*, 9–284.

IEEE, F. E. (2019b). ETHICALLY ALIGNED DESIGN. *The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems*, 9–284.

Iphofen, R., & Kritikos, M. (2021). Regulating artificial intelligence and robotics: ethics by design in a digital society. *Contemporary Social Science*, 16(2), 170–184. <https://doi.org/10.1080/21582041.2018.1563803>

- Ivanov, S., Gretzel, U., Berezina, K., Sigala, M., & Webster, C. (2019). Progress on robotics in hospitality and tourism: a review of the literature. *Journal of Hospitality and Tourism Technology*, 10(4), 489–521. <https://doi.org/10.1108/JHTT-08-2018-0087>
- Ivanov, S., & Webster, C. (2019). Conceptual framework of the use of robots, artificial intelligence and service automation in travel, tourism, and hospitality companies. In *Robots, Artificial Intelligence and Service Automation in Travel, Tourism and Hospitality* (pp. 7–37). <https://doi.org/10.1108/978-1-78756-687-320191001>
- Jean, G. (2025). *Cybersecurity Threats and Ethical Governance of AI-Driven Automation in Cloud-Based Manufacturing Systems*.
- Jung, I., Quan, W., Yu, J., & Han, H. (2023). Are you ready for robot services? Exploring robot-service adoption behaviors of hotel-goers. *International Journal of Hospitality Management*, 109(November 2022), 103404. <https://doi.org/10.1016/j.ijhm.2022.103404>
- Kim, H., So, K. K. F., & Wirtz, J. (2022). Service robots: Applying social exchange theory to better understand human–robot interactions. *Tourism Management*, 92(August 2021), 104537. <https://doi.org/10.1016/j.tourman.2022.104537>
- Kim, S. (Sam), Kim, J., Badu-Baiden, F., Giroux, M., & Choi, Y. (2021). Preference for robot service or human service in hotels? Impacts of the COVID-19 pandemic. *International Journal of Hospitality Management*, 93(July 2020), 102795. <https://doi.org/10.1016/j.ijhm.2020.102795>
- Kong, H., Wang, K., Qiu, X., Cheung, C., & Bu, N. (2023). 30 years of artificial intelligence (AI) research relating to the hospitality and tourism industry. *International Journal of Contemporary Hospitality Management*, 35(6), 2157–2177. <https://doi.org/10.1108/IJCHM-03-2022-0354>
- Kopp, T., Baumgartner, M., & Kinkel, S. (2020). Success factors for introducing industrial human-robot interaction in practice: an empirically driven framework. *International Journal of Advanced Manufacturing Technology*, 685–704. <https://doi.org/10.1007/s00170-020-06398-0>
- Lee, K. D. (2021). A Smart Network of Service Robots: Technical Challenges and Design Considerations. *IEEE Communications Magazine*, 59(8), 28–34. <https://doi.org/10.1109/MCOM.001.2100047>

- Li, K., Wu, J., Zhao, X., & Tan, M. (2019). Real-Time Human-Robot Interaction for a Service Robot Based on 3D Human Activity Recognition and Human-Mimicking Decision Mechanism. *8th Annual IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems, CYBER 2018*, 498–503. <https://doi.org/10.1109/CYBER.2018.8688272>
- Li, M., Yin, D., Qiu, H., & Bai, B. (2021). A systematic review of AI technology-based service encounters: Implications for hospitality and tourism operations. *International Journal of Hospitality Management*, 95(July 2020), 102930. <https://doi.org/10.1016/j.ijhm.2021.102930>
- Liang, C. J., Le, T. H., Ham, Y., Mantha, B. R. K., Cheng, M. H., & Lin, J. J. (2024). Ethics of artificial intelligence and robotics in the architecture, engineering, and construction industry. *Automation in Construction*, 162(October 2023), 105369. <https://doi.org/10.1016/j.autcon.2024.105369>
- Lin, P. (2016). Why Ethics Matters for autonomous cars. In M. Maurer, J. C. Gerdes, H. Winner, & B. Lenz (Eds.), *Autonomous driving: Technical, Legal and Social Aspects* (pp. 69–85). Springer Nature. <https://doi.org/10.1007/978-3-662-48847-8>
- Liu, J., Yu, Y., Chen, P., Chen, B. Y., Chen, L., & Chen, R. (2023). Facilitating urban tourism governance with crowdsourced big data: A framework based on Shenzhen and Jiangmen, China. *International Journal of Applied Earth Observation and Geoinformation*, 124(September). <https://doi.org/10.1016/j.jag.2023.103509>
- Liu, J., Zhou, L., & Li, Y. (2024). I can be myself: robots reduce social discomfort in hospitality service encounters. *International Journal of Contemporary Hospitality Management*, 36(6), 1798–1815. <https://doi.org/10.1108/IJCHM-01-2023-0004>
- Lu, V. N., Wirtz, J., Kunz, W. H., Paluch, S., Gruber, T., Martins, A., & Patterson, P. G. (2020a). Service robots, customers and service employees: what can we learn from the academic literature and where are the gaps? *Journal of Service Theory and Practice*, 30(3), 361–391. <https://doi.org/10.1108/JSTP-04-2019-0088>
- Lu, V. N., Wirtz, J., Kunz, W. H., Paluch, S., Gruber, T., Martins, A., & Patterson, P. G. (2020b). Service robots, customers and service employees: what can we learn from the academic literature and where are the gaps? *Journal of Service Theory and Practice*, 30(3), 361–391. <https://doi.org/10.1108/JSTP-04-2019-0088>

- Luciano, F. (2023). *The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities*. Oxford University Press.
<https://doi.org/10.1093/oso/9780198883098.001.0001>
- Lv, X., Yang, Y., Qin, D., Cao, X., & Xu, H. (2022). Artificial intelligence service recovery: The role of empathic response in hospitality customers' continuous usage intention. *Computers in Human Behavior*, 126(August 2021), 106993.
<https://doi.org/10.1016/j.chb.2021.106993>
- Madhan, K., Shagirbasha, S., Kumar Mishra, T., & Iqbal, J. (2024). Adoption of service robots: exploring the emerging trends through the lens of bibliometric analysis. *International Hospitality Review*, 38(2), 239–257. <https://doi.org/10.1108/ihr-12-2022-0058>
- Majumder, A., Kumar, A., Ghosh, S., Mohanty, S. P., & Bhattacharyya, K. B. (2017). Swing-Pay: One Card eets All User Paymment and Identity Needs. *IEEE Consumer Electronics Magazine*, (January), 82–92.
- Malatji, M., Von Solms, S., & Marnewick, A. (2019a). Socio-technical systems cybersecurity framework. *Information and Computer Security*, 27(2), 233–272.
<https://doi.org/10.1108/ICS-03-2018-0031>
- Malatji, M., Von Solms, S., & Marnewick, A. (2019b). Socio-technical systems cybersecurity framework. *Information and Computer Security*, 27(2), 233–272.
<https://doi.org/10.1108/ICS-03-2018-0031>
- Miller, C., Rodeghero, P., Storey, M.-A., Ford, D., & Zimmermann, T. (2021). “How Was Your Weekend?” *Software Development Teams Working From Home During COVID-19*. 624–636. <https://doi.org/10.1109/icse43902.2021.00064>
- Möller, D. P. F. (2023). Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices. In S. Jajodia, P. Samarati, J. Lopez, & J. Vaidya (Eds.), *Advances in Information Security* (Vol. 103). Springer.
https://doi.org/10.1007/978-3-031-26845-8_1
- Mujahid, A., Kalam, A., Morteza Alizadeh, S., & Fan, Y. (2022). Development of a Low-Cost Autonomous Healthcare Digital Assistant Lead RoBot (DALBOT). *Asia-Pacific Power and Energy Engineering Conference, APPEEC, 2022-Novem*, 1–6.
<https://doi.org/10.1109/APPEEC53445.2022.10072187>

- Nakanishi, J., Kuramoto, I., Baba, J., Ogawa, K., Yoshikawa, Y., & Ishiguro, H. (2020). Continuous Hospitality with Social Robots at a hotel. *SN Applied Sciences*, 2(3). <https://doi.org/10.1007/s42452-020-2192-7>
- Nam, K., Dutt, C. S., Chathoth, P., Daghfous, A., & Khan, M. S. (2021a). The adoption of artificial intelligence and robotics in the hotel industry: prospects and challenges. *Electronic Markets*, 31(3), 553–574. <https://doi.org/10.1007/S12525-020-00442-3/METRICS>
- Nam, K., Dutt, C. S., Chathoth, P., Daghfous, A., & Khan, M. S. (2021b). The adoption of artificial intelligence and robotics in the hotel industry: prospects and challenges. *Electronic Markets*, 31(3), 553–574. <https://doi.org/10.1007/S12525-020-00442-3/METRICS>
- Neupane, S., Mitra, S., Fernandez, I. A., Saha, S., Mittal, S., Chen, J., Pillai, N., & Rahimi, S. (2024). Security Considerations in AI-Robotics: A Survey of Current Methods, Challenges, and Opportunities. *IEEE Access*, 12(January), 22072–22097. <https://doi.org/10.1109/ACCESS.2024.3363657>
- Omohundro, S. (2014). *Autonomous technology and the greater human good*. 3079. <https://doi.org/10.1080/0952813X.2014.895111>
- Ooi, P. B., & Wilkinson, G. (2024). Enhancing ethical codes with artificial intelligence governance—a growing necessity for the adoption of generative AI in counselling. *British Journal of Guidance and Counselling*, 9885, 1–15. <https://doi.org/10.1080/03069885.2024.2373180>
- O’Sullivan, S., Nevejans, N., Allen, C., Blyth, A., Leonard, S., Pagallo, U., Holzinger, K., Holzinger, A., Sajid, M. I., & Ashrafian, H. (2019a). Legal, regulatory, and ethical frameworks for development of standards in artificial intelligence (AI) and autonomous robotic surgery. *International Journal of Medical Robotics and Computer Assisted Surgery*, 15(1), 1–12. <https://doi.org/10.1002/rcs.1968>
- O’Sullivan, S., Nevejans, N., Allen, C., Blyth, A., Leonard, S., Pagallo, U., Holzinger, K., Holzinger, A., Sajid, M. I., & Ashrafian, H. (2019b). Legal, regulatory, and ethical frameworks for development of standards in artificial intelligence (AI) and autonomous robotic surgery. *International Journal of Medical Robotics and Computer Assisted Surgery*, 15(1), 1–12. <https://doi.org/10.1002/rcs.1968>

- Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, M. C. (2020). *The PRISMA 2020 statement: an updated guideline for reporting systematic reviews*. The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews. <https://doi.org/10.1136/bmj.n71>
- Palaniappan, K., Lin, E. Y. T., Vogel, S., & Lim, J. C. W. (2024). Global Regulatory Frameworks for the Use of Artificial Intelligence (AI) in the Healthcare Services Sector. *Healthcare (Switzerland)*, 12(17). <https://doi.org/10.3390/healthcare12171730>
- Petersen, K., & Gencel, C. (2013). Worldviews, research methods, and their relationship to validity in empirical software engineering research. *Proceedings - Joint Conference of the 23rd International Workshop on Software Measurement and the 8th International Conference on Software Process and Product Measurement, IWSM-MENSURA 2013*, 81–89. <https://doi.org/10.1109/IWSM-Mensura.2013.22>
- Pillai, R., & Sivathanu, B. (2020). Adoption of AI-based chatbots for hospitality and tourism. *International Journal of Contemporary Hospitality Management*, 32(10), 3199–3226. <https://doi.org/10.1108/IJCHM-04-2020-0259>
- Pogliani, M., Quarta, D., Polino, M., Vittone, M., Maggi, F., Zanero, S., Pogliani, M., Quarta, D., Polino, M., Vittone, M., Maggi, F., & Zanero, S. (2019). Security of controlled manufacturing systems in the connected factory: The case of industrial robots. *Springer*, 15(3), 161–175. <https://doi.org/10.1007/s11416-019-00329-8>
- Polat, M., Karataş, İ. H., & Varol, N. (2025). Ethical Artificial Intelligence (AI) in Educational Leadership: Literature Review and Bibliometric Analysis. *Leadership and Policy in Schools*, 24(1), 46–76. <https://doi.org/10.1080/15700763.2024.2412204>
- Quarta, D., Pogliani, M., Polino, M., Maggi, F., Zanchettin, A. M., & Zanero, S. (2017). An Experimental Security Analysis of an Industrial Robot Controller. *38th IEEE Symposium on Security and Privacy*, 20(05), 22–24. <https://doi.org/10.1109/SP.2017.20>
- Rabb, N., Law, T., Chita-Tegmark, M., & Scheutz, M. (2022). An Attachment Framework for Human-Robot Interaction. *International Journal of Social Robotics*, 14(2), 539–559. <https://doi.org/10.1007/s12369-021-00802-9>

- Rahman, M. M., Khatun, F., Jahan, I., Devnath, R., & Bhuiyan, M. A. A. (2024). Cobotics: The Evolving Roles and Prospects of Next-Generation Collaborative Robots in Industry 5.0. *Journal of Robotics*, 2024. <https://doi.org/10.1155/2024/2918089>
- Ranasinghe, C. (2024). Governance and Compliance of Autonomous Systems and Robotics : Ethical and Legal Frameworks for the Future. *ANNUAL INTERNATIONAL CONFERENCE ON BUSINESS INNOVATION (ICOBI) 2024 Governance*, 468–482.
- Ross, R., Mcevilley, M., & Oren, J. C. (2018). Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. *National Institute of Standards and Technology Special Publication 800-160, 1*. <https://doi.org/https://doi.org/10.6028/NIST.SP.800-160v1>
- Sadek, M., Calvo, R. A., & Mougnot, C. (2023a). Designing value-sensitive AI: a critical review and recommendations for socio-technical design processes. *AI and Ethics*, 4(4), 949–967. <https://doi.org/10.1007/s43681-023-00373-7>
- Sadek, M., Calvo, R. A., & Mougnot, C. (2023b). Designing value-sensitive AI: a critical review and recommendations for socio-technical design processes. *AI and Ethics*, 4(4), 949–967. <https://doi.org/10.1007/s43681-023-00373-7>
- Saldaña, J. (2017). *Coding Techniques for Quantitative and Mixed Data*. <https://doi.org/10.4324/9780203729434-14>
- Salimi, S., Queralta, J. P., & Westerlund, T. (2023). Hyperledger Fabric Blockchain and ROS 2 Integration for Autonomous Mobile Robots. *2023 IEEE/SICE International Symposium on System Integration, SII 2023*. <https://doi.org/10.1109/SII55687.2023.10039326>
- Saplaçan, D., Khaksar, W., & Torresen, J. (2021). On Ethical Challenges Raised by Care Robots: A Review of the Existing Regulatory-, Theoretical-, and Research Gaps. *Proceedings of IEEE Workshop on Advanced Robotics and Its Social Impacts, ARSO, 2021-July*, 219–226. <https://doi.org/10.1109/ARSO51874.2021.9542844>
- Saxena, A., Ali, A., & Abdulsada, Z. R. (2023). Integration of PLC and Robotic Operating System for Enhanced Automation Efficiency’. *2023 2nd International Conference on Futuristic Technologies, INCOFT 2023*, 2023–2026. <https://doi.org/10.1109/INCOFT60753.2023.10425707>

- Senthamarai, M., K. R., Vikram, U., & Kathir, R. (2024). *The Role and Progression of Serving Robots in Hospitality and Service Industries*. 6(5), 1–12.
- Sharmar, A., & Guleria, K. (2021). A Framework for Hotel Inventory Control System for Online Travel Agency using Robotic Process Automation. *International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) Department of Electrical & Electronics Engineering, Galgotias College of Engineering and Technology, Gr. Noida, India*, 7, 6–10.
- Skubis, I. (2024). Exploring the Potential and Perceptions of Social Robots in Tourism and Hospitality: Insights from Industry Executives and Technology Evaluation. *International Journal of Social Robotics*, 59–72. <https://doi.org/10.1007/s12369-024-01197-z>
- Smith, D. J., Li, H. D., & Rafferty, R. M. (2020). The Implementation Research Logic Model: a method for planning, executing, reporting, and synthesizing implementation projects. *Implementation Science*, 1–12.
- Soori, M., Dastres, R., Arezoo, B., & Jough, F. K. G. (2024). Intelligent robotic systems in Industry 4.0: A review. *Journal of Advanced Manufacturing Science and Technology*, 4(3), 0–28. <https://doi.org/10.51393/j.jamst.2024007>
- Tanimu, J. A., & Abada, W. (2025a). Addressing cybersecurity challenges in robotics: A comprehensive overview. *Cyber Security and Applications*, 3, 100074. <https://doi.org/10.1016/J.CSA.2024.100074>
- Tanimu, J. A., & Abada, W. (2025b). Addressing cybersecurity challenges in robotics: A comprehensive overview. *Cyber Security and Applications*, 3, 100074. <https://doi.org/10.1016/J.CSA.2024.100074>
- Tanimu, J. A., & Abada, W. (2025c). Addressing cybersecurity challenges in robotics: A comprehensive overview. *Cyber Security and Applications*, 3, 100074. <https://doi.org/10.1016/J.CSA.2024.100074>
- Thamrongaphichartkul, K., Worrasittichai, N., Prayongrak, T., & Vongbunyong, S. (2020). A Framework of IoT Platform for Autonomous Mobile Robot in Hospital Logistics Applications. *Proceedings - 2020 15th International Joint Symposium on Artificial Intelligence and Natural Language Processing, ISAI-NLP 2020*, 1–6. <https://doi.org/10.1109/iSAI-NLP51646.2020.9376823>

- Tlili, A., Denden, M., Abed, M., & Huang, R. (2024). Artificial intelligence ethics in services: are we paying attention to that?! *Service Industries Journal*, 2069, 1093–1116.
<https://doi.org/10.1080/02642069.2024.2369322>
- Tung, V. W. S., & Au, N. (2018). Exploring customer experiences with robotics in hospitality. *International Journal of Contemporary Hospitality Management*, 30(7), 2680–2697.
<https://doi.org/10.1108/IJCHM-06-2017-0322>
- Tuomi, A., Tussyadiah, I. P., & Hanna, P. (2021). Spicing up hospitality service encounters: the case of PepperTM. *International Journal of Contemporary Hospitality Management*, 33(11), 3906–3925. <https://doi.org/10.1108/IJCHM-07-2020-0739>
- Tuomi, A., Tussyadiah, I., & Stienmetz, J. (2020). Service robots and the changing roles of employees in restaurants: A cross cultural study. In *e-Review of Tourism Research* (Vol. 17, Number 5, pp. 662–673).
- Udo, J. E., & Sallal, M. (2023). RDSF: Risk Driven Security Framework for Industrial Autonomous Robots. *Proceedings - International Conference on Distributed Computing Systems*, 2023-July(7), 1075–1076. <https://doi.org/10.1109/ICDCS57875.2023.00137>
- Urs, B.-A. (2015). Security Issues and Solutions in E-Payment Systems. *Fiat Iustitia*, 21–28.
- Vanderelst, D., & Winfield, A. (2018a). The Dark Side of Ethical Robots. *Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society*, (1), 317–322.
<https://doi.org/10.1145/3278721.3278726>
- Vanderelst, D., & Winfield, A. (2018b). The Dark Side of Ethical Robots. *Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society*, (1), 317–322.
<https://doi.org/10.1145/3278721.3278726>
- Wang, X., Wu, J., & Qu, W. (2025). A Robotic Process Automation-Based System for Intelligent Work Order Management with Active Service in Power System. *8th International Conference on Advanced Algorithms and Control Engineering (ICAACE)*, 628–631. <https://doi.org/10.1109/icaace65325.2025.11020166>
- Weerarathna, I. N., Raymond, D., & Luharia, A. (2023a). Human-Robot Collaboration for Healthcare: A Narrative Review. *Cureus*, 15(11). <https://doi.org/10.7759/cureus.49210>
- Weerarathna, I. N., Raymond, D., & Luharia, A. (2023b). Human-Robot Collaboration for Healthcare: A Narrative Review. *Cureus*, 15(11). <https://doi.org/10.7759/cureus.49210>

- Wirtz, J., Kunz, W. H., & Paluch, S. (2021a). The Service Revolution, Intelligent Automation and Service Robots. *The European Business Review*, (January), 38–44.
- Wirtz, J., Kunz, W. H., & Paluch, S. (2021b). The Service Revolution, Intelligent Automation and Service Robots. *The European Business Review*, (January), 38–44.
<https://www.researchgate.net/publication/346392669%0Awww.europeanbusinessreview.com>
- Wu, T. J., & Zhang, R. X. (2024). Exploring the impacts of intention towards human-robot collaboration on frontline hotel employees' positive behavior: An integrative model. *International Journal of Hospitality Management*, 123(December 2023).
<https://doi.org/10.1016/j.ijhm.2024.103912>
- Xu, J., Hsiao, A., Reid, S., & Ma, E. (2023). Working with service robots? A systematic literature review of hospitality employees' perspectives. *International Journal of Hospitality Management*, 113(June), 103523. <https://doi.org/10.1016/j.ijhm.2023.103523>
- Xue, Y., Wang, F., Tian, H., Zhao, M., Li, J., Pan, H., & Dong, Y. (2021). Proactive Interaction Framework for Intelligent Social Receptionist Robots. *Proceedings - IEEE International Conference on Robotics and Automation, 2021-May(Icra)*, 3403–3409.
<https://doi.org/10.1109/ICRA48506.2021.9562115>
- Yaacoub, J., Noura, H., & Salman, O. (2022). Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. *International Journal of Information Security*, 21(1), 115–158. <https://doi.org/10.1007/s10207-021-00545-8>
- Yaacoub, J. P. A., Noura, H. H. N., Salman, O., & Chehab, A. (2022). Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations. *International Journal of Information Security*, 21(1), 115–158. <https://doi.org/10.1007/s10207-021-00545-8>

Appendices

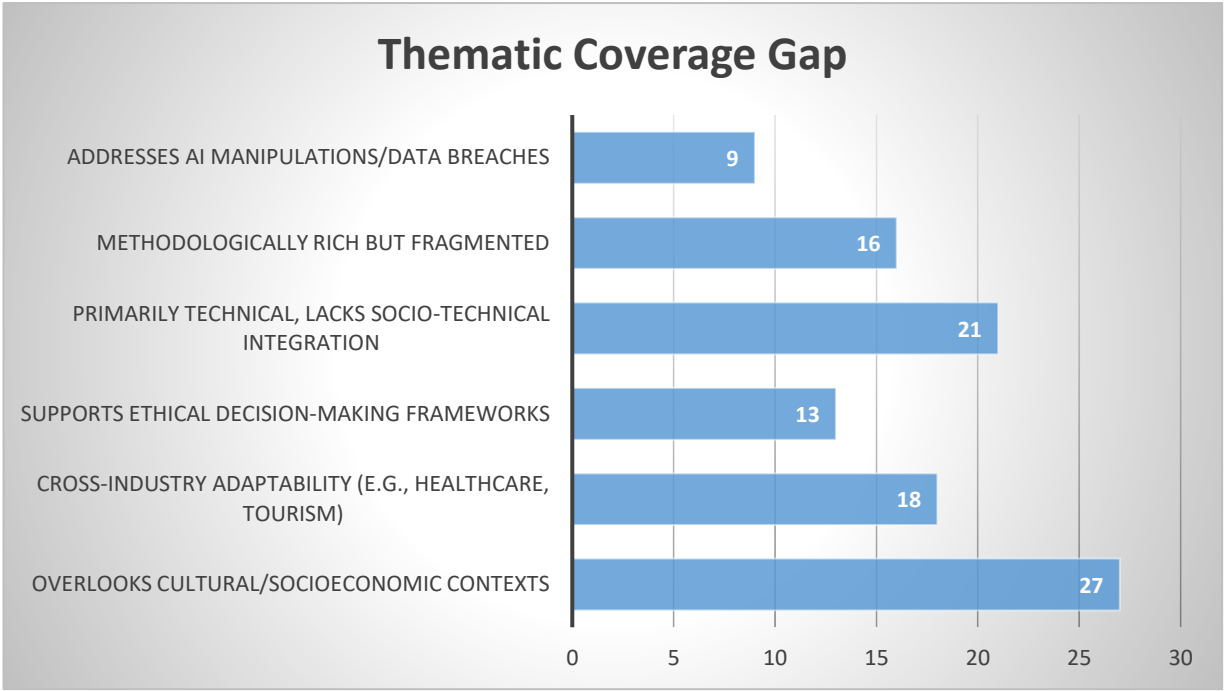
**Appendix A: SLR Extraction Matrix Informing the ACERBOTICS Socio-Tactical Framework
(Synthesised by author)**

Relevance to Cyber-safe Robotics	Relevance to Ethical Robotics	Relevance to Service Robotics	Afro-Centric Focus	Framework Development Relevance	Rating
4	5	8	1	1	Very high
8	12	17	0	17	High
12	12	7	0	12	Moderate
1	0	2	0	0	Indirect
11	7	2	0	6	Low

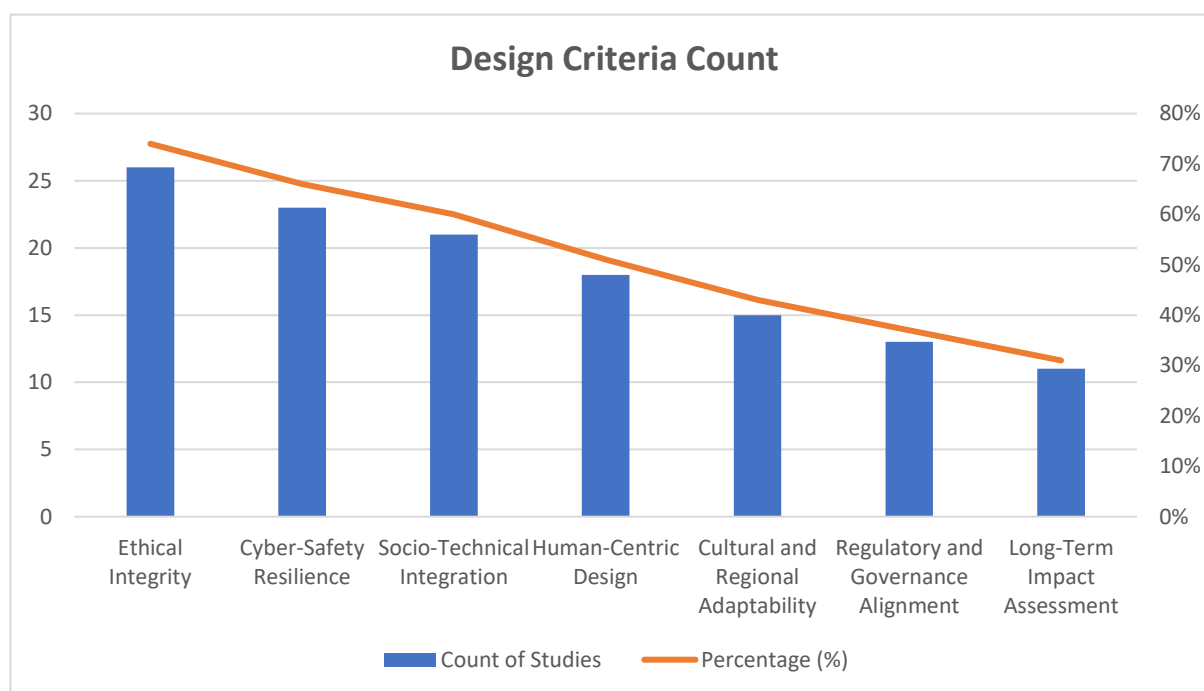
Appendix B: Geographic Distribution of Studies (Synthesised by author)

Continent	Countries	Count	Percentage
North America	USA	3	8,6%
Europe/EU (multi-country)	Germany, Norway, Portugal, UK, Finland, Italy, Netherlands, Belgium EU (multi-country)	13	37,1%
Asia	China, India, South Korea, Multi-Asia-centric	8	22,9%
Africa	Ghana	1	2,9%
Oceania	Australia	1	2,9%
Others	Multi-country/ Global	9	25,7%
SUM		35	100,0%

Appendix C: Thematic Coverage Across Studies (Synthesised by author)



Appendix D: Design Criteria Identified in Reviewed Literature (Synthesised by author)



Appendix E: Distribution of Study Relevance to Cyber-Safety, Ethical and Service Robotics Domains (Synthesised by author)

Relevance to Cyber-safe Robotics	Relevance to Ethical Robotics	Relevance to Service Robotics	Framework Development Relevance	Rating
4	5	8	1	Very high
8	12	17	17	High
12	12	7	12	Moderate
1	0	2	0	Indirect
11	7	2	6	Low

Appendix F: Study Relevance Frequency Count
(Synthesised by author)

Robotics Domain	Frequency Count	Percentage (%)
Ethical Robotics	11	31%
Service Industry Applications	10	29%
Cyber-Safety	6	17%
Human-Robot Interaction (HRI)	5	14%
Cyber-Ethical Integration	3	9%
TOTAL	35	100%

Appendix G: Socio-Technical Architectural Gap Across Methodologies Pivotal Table
(Synthesised by author)

Observable Gap	Count of Citation	Percentage
High Gap	11	31%
Case Study	1	
Conceptual framework	3	
Empirical Test	2	
Experimental	1	
Review	2	
Survey	1	
Theoretical Alignment	1	
Low Gap	13	36%
Conceptual analysis	1	
Conceptual framework	1	
Empirical Test	2	
Experimental	1	
Mixed Methods	1	
Review	3	
Survey	1	
Theoretical framework	3	
Moderate Gap	3	8%
Conceptual framework	1	

Prototype design and evaluation	1	
Review	1	
No Gap	1	3%
Review	1	
Partial Gap	7	22%
Case Study	1	
Conceptual framework	2	
Mixed Methods	1	
Review	1	
Theoretical framework	2	

Appendix H: Thematic Coverage Gap Count (Synthesised by author)

Thematic Coverage Gap		
Theme	Count of Studies	Percentage
Overlooks Cultural/Socioeconomic Contexts	27	77%
Cross-Industry Adaptability (e.g., Healthcare, Tourism)	18	51%
Supports Ethical Decision-Making Frameworks	13	37%
Primarily Technical, Lacks Socio-Technical Integration	21	60%
Methodologically Rich but Fragmented	16	46%
Addresses AI Manipulations/Data Breaches	9	26%

Appendix I: Geographical Distribution Pivotal Table (Synthesised by author)

Continent	Countries	Count	Percentage
North America	USA (3)	3	8,6%
Europe/EU (multi-country)	Germany (1), Norway (1), Portugal (3), UK (2), Finland (2), Italy (1), Netherlands (1), Belgium (1) EU (multi-country)(1)	13	37,1%
Asia	China (3), India (3), South Korea (1), Multi-Asia-centric (1)	8	22,9%
Africa	Ghana (1)	1	2,9%
Oceania	Australia (1)	1	2,9%
Others	Multi-country (4), Global (5)	9	25,7%
SUM		35	100,0%

Appendix J: SLR Extraction Matrix with Identified Design Criteria (Synthesised by author)

Citation	Paper Type	Country	Methodology	Relevance to Cyber-safe Robotics	Relevance to Ethical Robotics	Relevance to Service Industries	Affordances	Socio-Technical Architecture Gap	Technological Bias	Overlooking HRI Socio-Dynamics	Framework Development Relevance	Design criteria identified
(Rabb et al., 2022)(Rabb et al., 2022)(Rabb et al., 2022)(Rabb et al., 2022)	Conceptual	USA	Literature Review	Low	High	High	0	Low Gap	No	Minimal	High	Socio-Technical Integration; Human-centred Design; Ethical Integrity
(Kopp et al., 2020)(Kopp et al., 2020)(Kopp et al., 2020)(Kopp et al., 2020)	Empirical	Germany	Survey	Moderate	Moderate	High	0	High Gap	No	Addressed	Low	Cyber-Safety Resilience; Regulatory and Governance Alignment
(Liu et al., 2023)(Liu et al., 2023)(Liu et al., 2023)	Case Study	China	Case Study	Minimal	Minimal	High	0	High Gap	Partial		High	Socio-Technical Integration; Human-centred Design

2023)(Liu et al., 2023)

Click or tap here to enter text.
Figure 0.

SEQ
Figur(Tung & Au, 2018)(Jean, 2025)(Jean, 2025)(Jean, 2025)(Jean, 2025)
(Bowen & Morosan, 2018)(Bow en & Morosan, 2018)(Bow en & Morosan, 2018)(Bow en & Morosan, 2018)
(Saxena et al., 2023)(Saxe

													Minimal	
														Ethical Integrity; Cultural and Regional Adaptability
	Review	Multi-count	Review	High	High	Mode	0	Low Gap	No		Minimal	Moderate		
														Ethical Integrity; Long-Term Impact Assessment
	Framework	Global	Mixed Methods	Very High	High	Indirect	0	Partial Gap	Yes		Addressed	High		
														Socio-Technical Integration; Human-centred Design; Ethical Integrity
	Conceptual	Global	Conceptual	Low	High	Very High	0	Partial Gap	Partial		Addressed	High		
	Conference	India	Framework	Indirect	Low	High	0	Partial Gap	Yes		Overlooked	Moderate		Cyber-Safety Resilience; Socio-Technical Integration

na et al., 2023)(Saxe												
na et al., 2023)(Saxe												
na et al., 2023)												
Javaid & Haleem (2020)	Review	Global	Literature Review	High	Moderate	High	0	Low Gap	Yes	Overlooked	Moderate	Ethical Integrity; Cyber-Safety Resilience; Human-centred Design
Saplacan et al. (2021)	Conceptual	Norway	Review	High	Very High	High	0	High Gap	Partial	Minimal	High	Ethical Integrity; Socio-Technical Integration; Cultural and Regional Adaptability
Martins et al. (2022)	Conceptual	Portugal	Framework	Very High	Moderate	High	0	Low Gap	No	Overlooked	Moderate	Human-centred Design; Cultural and Regional Adaptability; Ethical Integrity
Braun et al. (2022)	Conceptual	Portugal	Framework	Low	Low	High	0	Low Gap	No	Addressed	Moderate	Ethical Integrity; Cyber-Safety Resilience; Regulatory and Governance Alignment
Hasan & Trianni (2022)	Conceptual	Australia	Case Study	Moderate	Moderate	Very High	0	Partial Gap	No	Overlooked	Low	Cultural and Regional Adaptability; Human-centred Design
	Conceptual											Socio-Technical Integration; Long-Term Impact Assessment
Sharma & Joshi (2021)		India	Framework	Low	Low	Very High	0	Partial Gap	Yes		Low	

Minimal												
Wang et al. (2025)	Conceptual	China	Empirical Test	Moderate	Moderate	High	0	Low Gap	Yes	Minimal	Moderate	Cyber-Safety Resilience; Cultural and Regional Adaptability
Ivanov et al. (2019)	Conceptual	Global	Conceptual	Low	High	Very High	0	High Gap	No	Limited	Moderate	Ethical Integrity; Socio-Technical Integration
(Benjumea, 2024b)(Benjumea, 2024b)(Benjumea, 2024b)(Benjumea, 2024b)												Ethical Integrity; Long-Term Impact Assessment; Cultural and Regional Adaptability
(Batya & David, 2019)(Batya & David, 2019)(Batya & David, 2019)(Batya & David, 2019)	Thesis	UK	Empirical Test	High	High	Mode rate	0	High Gap	Yes	Overlooked	Low	Ethical Integrity; Socio-Technical Integration; Human-centred Design
(IEEE, 2019b)(IEEE, 2019b)(IEEE, 2019b)	Empirical/Framework	USA/Global	Review	Very High	High	High	0	Low gap	No	Addressed	Very High	Ethical Integrity; Regulatory and Governance Alignment; Long-Term Impact Assessment
	Framework	Global	Framework	Very High	Very High	Very High	0	Low Gap	No	addressed		

2019b)(IEEE, 2019b)												
(Malatji et al., 2019a)(Malatji et al., 2019a)(Malatji et al., 2019a)(Malatji et al., 2019a)	Empirical/ Framework	Australia	Empirical Test/framework design	Very High	High	High	0	Low gap	No	Addressed	Very High	Cyber-Safety Resilience; Socio-Technical Integration; Regulatory and Governance Alignment
(Soori et al., 2024)(Soori et al., 2024)(Soori et al., 2024)(Soori et al., 2024)	Review	Global	Conceptual	Low	Low	High	0	High Gap	Yes	Overlooked	Moderate	Cyber-Safety Resilience; Regulatory and Governance Alignment
(Rahman et al., 2024)(Rahman et al., 2024)(Rahman et al., 2024)(Rahman et al., 2024)	Conceptual	Multi-Asia-centric	Conceptual analysis	Moderate	High	High	0	Low Gap	No	Limited	High	Cultural and Regional Adaptability; Socio-Technical Integration
(Salimi et al., 2023)(Salimi et al., 2023)	Conference	Finland	Empirical test	High	High	Mode rate	0	High Gap	Yes	Overlooked	Low	Ethical Integrity; Cyber-Safety Resilience

mi et al., 2023)(Sali mi et al., 2023)(Sali mi et al., 2023)												
(Shar mar & Guleria, 2021)(Shar mar & Guleria, 2021)(Shar mar & Guleria, 2021)(Shar mar & Guleria, 2021)												Socio-Technical Integration; Human-centred Design; Ethical Integrity
Guleria, 2021)	Conferenc e paper	India	Conceptual framework	Low	Low	High	0	High Gap	Yes	Overloo ked	High	
(Brown- Acquaye et al., 2019)(Bro wn- Acquaye et al., 2019)(Bro wn- Acquaye et al., 2019)(Bro wn- Acquaye et al., 2019)												Ethical Integrity; Cultural and Regional Adaptability
2019)(Bro wn- Acquaye et al., 2019)(Bro wn- Acquaye et al., 2019)	Journal paper	Ghan a	Conceptual framework	High	High	High	1	Moderat e Gap	No	Address ed	High	

Acquaye et al., 2019)												
(Belanche et al., 2020)(Belanche et al., 2020)(Belanche et al., 2020)(Belanche et al., 2020)	Journal paper	Multi-county	Theoretical framework	Low	Moderate	High	0	Low	No	Addressed	High	Cyber-Safety Resilience; Socio-Technical Integration
(Weeraratna et al., 2023b)(Weeraratna et al., 2023b)(Weeraratna et al., 2023b)(Weeraratna et al., 2023b)	Conference	Multi-county	Review	High	High	High	0	High Gap	Yes	Limited	Low	Ethical Integrity; Regulatory and Governance Alignment
(Palaniappan et al., 2024)(Palaniappan et al., 2024)(Palaniappan et al., 2024)	Journal paper	Multi-county	Review	Moderate	High	High	0	No Gap	Yes	Limited	Moderate	Cyber-Safety Resilience; Human-centred Design

niappan et al., 2024)												
(Callari et al., 2024a)(Callari et al., 2024a)(Callari et al., 2024a)(Callari et al., 2024a)	Journal paper	Vietnam	Bibliometric analysis	No	High	High	0	No Gap	No	Addressed	Moderate	Socio-Technical Integration; Long-Term Impact Assessment
(Flavián & Casalo, 2021)(Flavián & Casalo, 2021)(Flavián & Casalo, 2021)(Flavián & Casalo, 2021)												
(Flavián & Casalo, 2021)(Flavián & Casalo, 2021)	Conference	Global scope	Review/conceptual overview	Low	High	High	0	Moderate gap	No	Addressed	Low	Cultural and Regional Adaptability; Regulatory and Governance Alignment
(Ranasinghe, 2024)(Ranasinghe, 2024)												
(Ranasinghe, 2024)(Ranasinghe, 2024)	Conference	Global	Review/Survey	High	High	High	0	No Gap	No	Addressed	Low	Ethical Integrity; Cyber-Safety Resilience; Socio-Technical Integration Human-centred Design; Cultural and Regional Adaptability

singhe,
2024)

		EU										Cyber-Safety Resilience: Long-Term Impact Assessment
(Floridi et al., 2018)	Conceptual Framework	(multi-county)	Ethical theory synthesis and policy proposal	Low	Very high	Mode rate	0	Partial Gap	No	Minimal	High	
(Alves et al., 2020)	Framework/Theoretical Discussion	Portugal	Conceptual analysis and taxonomy creation	Moderate	High	Mode rate	0	Partial Gap	Yes	Addressed	High	Ethical Integrity; Regulatory and Governance Alignment
(Pagallo et al., 2022)	Security Framework Proposal	Italy	Framework design with comparative analysis of safety standards	Very high	Moderate	Low	0	Low Gap	Minimal	Overlooked	High	Socio-Technical Integration; Cyber-Safety Resilience; Cultural and Regional Adaptability
	Ethical Discussion / Literature Review	UK	Critical review of robotics in care settings	Moderate	Very high	Very high	0	Partial Gap	Yes	Addressed	Very High	Ethical Integrity; Human-centred Design; Long-Term Impact Assessment
(van de Poel, 2020)	Principlist Ethical Framework	Netherlands	Theoretical ethics application	High	Very high	Mode rate	0	Low Gap	Yes	Minimal	High	Cyber-Safety Resilience; Regulatory and Governance Alignment
(Mehta et al., 2022)	Survey / Review	USA	Survey of AI-robotics security methods	Very high	Moderate	Indirect	0	Low Gap	No	Overlooked	High	Socio-Technical Integration; Human-centred Design; Ethical Integrity

(Kim et al., 2022)	Experimental / Technical	South Korea	Prototype implementation with a real-time recognition system	Moderate	Low	High	0	High Gap	No	Addressed	Medium	Ethical Integrity; Long-Term Impact Assessment; Socio-Technical Integration
(Iphofen & Kritikos, 2021)(Iphofen & Kritikos, 2021)	Theoretical / Ethical Policy Discussion	EU	Ethical reasoning and policy alignment	High	Very high	High	0	High Gap	Yes	Partially	High	Ethical Integrity; Cyber-Safety Resilience; Socio-Technical Integration

Appendix K: Design Criteria Frequency Count (Synthesised by author)

Design Criterion	Count of Studies	Percentage (%)
Ethical Integrity	26	74%
Cyber-Safety	23	66%
Resilience		
Socio-Technical Integration	21	60%
Human-centred Design	18	51%
Cultural and Regional Adaptability	15	43%
Regulatory and Governance Alignment	13	37%
Long-Term Impact Assessment	11	31%

Appendix L: Questionnaire for Evaluating the ACERBOTICS Framework (Synthesised by author)

12/14/25, 2:26 PM

Expert Evaluation Questionnaire for the ACERBOTICS Framework: A Cybersafe and Ethical Model for Service Robotic Syste...

After section 3

Section 4 of 12

Expert Evaluation Questionnaire for ACERBOTICS Framework

These questions are designed to measure the relevance, coherence, usability, and contextual sensitivity across ethical, cybersafety, and socio-technical dimensions of the proposed framework.

Evaluation Criteria Please consider the following dimensions when completing the questionnaire:

1. **Relevance** - Does framework address real and pressing challenges in RSI?
2. **Clarity** - Are framework concepts and structure clearly articulated?
3. **Applicability** - Can framework be applied in real-world service domains?
4. **Completeness** - Are any important components, threats, or values missing?
5. **Ethical Soundness** - Are ethical risks and governance properly integrated?
6. **Cybersecurity Readiness** - Are data safety and system integrity effectively addressed?
7. **Socio-Technical Integration** - Does framework consider human values, culture, and industry needs?
8. **Practicality** - Is framework feasible to implement or adapt by practitioners?
9. **Coherence**: Do the components form a cohesive whole?
10. **Coverage**: Are all aspects (cybersecurity, ethics, socio-technical integration, local context) addressed?
11. **Usefulness**: Would this structure be actionable for designing or governing service robots?

After section 4

Section 5 of 12

Demographics (*Closed-Ended*)

To gather background information to contextualise survey responses.

Q1. What is your primary role in the service industry? *

Q2. How well do you know robotic systems used in the service industry? *

1 2 3 4 5

Not Familiar

Very Familiar

Q3. How long have you been involved with or engaged in working with robotic systems in the service sector? *

Q4. Do you think service robots ought to adhere to a formal ethical code comparable to that of human employees? *

After section 5

Section 6 of 12

Relevance and Clarity

This section evaluates how effectively the ACERBOTICS Framework addresses real and pressing challenges in robotics within the service industry, and how clearly its structure and concepts are presented. It measures whether the framework's objectives, principles, and relationships are logically articulated and understandable, ensuring its purpose aligns with current industry and research needs.

Q5. The ACERBOTICS Framework addresses real and pressing challenges in the Robotics Service Industry (RSI). *

1 2 3 4 5

Strongly Disagree

Strongly Agree

Q6. The framework adequately integrates multiple disciplinary perspectives (e.g., ethics, cybersecurity, HRI). *

1 2 3 4 5

Strongly Disagree

Strongly Agree

Q7. The framework's structure, components, and interrelationships are clearly articulated and easy to understand. *

1 2 3 4 5

Strongly Disagree

Strongly Agree

Q8. The visual representation and accompanying explanation adequately communicate the framework's purpose and scope. *

1 2 3 4 5

Strongly Disagree

Strongly Agree

After section 6

Section 7 of 12

Applicability and Completeness

This section assesses how well the ACERBOTICS Framework can be applied across real-world service robotics contexts and whether it sufficiently covers all critical dimensions - ethical, technical, and operational

Q9. The framework can be practically applied in real-world service domains such as healthcare, hospitality, or logistics. *

1 2 3 4 5

Strongly Disagree

Strongly Agree

Q10. The framework is adaptable to different organizational contexts within the service industry. *

Q11. The framework contributes significantly to the field of ethical and cybersecure robotics. *

1 2 3 4 5

Strongly Disagree

Strongly Agree

Q12. There are no major omissions in the framework that could hinder its implementation or validity. *

1 2 3 4 5

Strongly Disagree

Strongly Agree

Q13. I would recommend the use of this framework for future projects in service robotics. *

1 2 3 4 5

Strongly Disagree

Strongly Agree

After section 7

Section 8 of 12

Cybersecurity Readiness and Ethical Soundness

This section examines how effectively the ACERBOTICS Framework incorporates mechanisms to protect data, ensure system integrity, and align robotic operations with ethical principles and governance standards. It evaluates whether cybersecurity measures are proactive, resilient, and integrated with moral safeguards that promote accountability, transparency, and user trust in autonomous service robotics systems

Q14. Ethical considerations such as fairness, transparency, and accountability are well-integrated within the framework. *

1 2 3 4 5

Strongly Disagree

Strongly Agree

Q15. The framework provides a clear pathway for ensuring responsible and human-centred robotic deployment. *

1 2 3 4 5

Strongly Disagree

Strongly Agree

Q16. The framework adequately addresses data protection. *

1 2 3 4 5

Strongly Disagree

Strongly Agree

Q17. The framework adequately addresses threat resilience. *

1 2 3 4 5

Strongly Disagree

Strongly Agree

Q18. The framework adequately addresses system integrity. *

1 2 3 4 5

Strongly Disagree

Strongly Agree

Q19. The cybersecurity dimension aligns with ethical and operational requirements for safe robotic deployment. *

1 2 3 4 5

Strongly Disagree

Strongly Agree

After section 8

Section 9 of 12

Socio-Technical Integration and Practicality

This section evaluates how well the ACERBOTICS Framework integrates human, social, and technical dimensions within real-world service environments. It assesses whether the framework effectively aligns robotic functions with human values, organizational needs, and cultural contexts, while also determining its practicality - that is, how feasible, adaptable, and scalable it is for implementation by practitioners and industry stakeholders

Q20. The framework sufficiently considers human values. *

1 2 3 4 5

Strongly Disagree

Strongly Agree

Q21. The framework sufficiently considers cultural diversity. *

1 2 3 4 5

Strongly Disagree

Strongly Agree

Q22. The framework sufficiently considers industry-specific needs. *

1 2 3 4 5

Strongly Disagree

Strongly Agree

Q23. The socio-technical aspects are effectively integrated to enhance collaboration between humans and robots. *

1 2 3 4 5

Strongly Disagree

Strongly Agree

Q24. The framework is feasible for adoption by practitioners and policymakers in the service robotics field. *

1 2 3 4 5

Strongly Disagree

Strongly Agree

Q25. The implementation pathway described is realistic and scalable. *

1 2 3 4 5

Strongly Disagree

Strongly Agree

After section 9

Section 10 of 12

Coherence, Coverage and Usefulness

This section assesses the ACERBOTICS Framework's internal consistency and comprehensiveness. It checks if all components - ethical integrity, cyber-safety, socio-technical integration, and contextual adaptability - function as a cohesive unit. It also evaluates the framework's practical usefulness and application for service robots in real-world settings

Q26. The framework's components form a cohesive and logically structured model. *

1 2 3 4 5

Strongly Disagree

Strongly Agree

Q27. The framework holistically addresses critical aspects such as ethics, cybersecurity, socio-technical systems, and cultural context. *

1 2 3 4 5

Strongly Disagree

Strongly Agree

Q28. The framework would be useful for guiding the ethical design, governance, and deployment of service robots. *

1 2 3 4 5

Strongly Disagree

Strongly Agree

After section 10

Section 11 of 12

Open-Ended Feedback

This section allows expert reviewers to give detailed, reflective, and constructive feedback on the ACERBOTICS Framework, including insights, critiques, or suggestions on its soundness, applicability, clarity, and areas for improvement. It provides space for viewpoints beyond structured ratings, helping refine the framework for academic and practical use.

Q29. What key improvements would enhance the framework's clarity, usability, or impact? *

Q30. Do you consider this framework adaptable to diverse socio-economic and cultural contexts?
Please explain.

Q31. What strengths do you perceive in the ACERBOTICS framework in addressing service robotics challenges? *

Q32. Are there elements missing that would enhance real-world deployment? *

After section 11

Section 12 of 12

Thank you for your time and valuable insights! If you have any questions about this survey, please do not hesitate to contact us at 63277077@mylife.unisa.ac.za.

Description (optional)

Appendix M: Ethical Clearance Certificate (Synthesised by author)

Date: 04/08/2025

Dear: Mr Emmanuel Mordi

**Decision: Ethics Approval from
04/08/2025 to 04/08/2028**

NHREC Registration # : (if applicable)
Ref #: 8827
Name: Mr Emmanuel Mordi
Student #: 63277077
Staff #:

Researcher: Mr Emmanuel Mordi

Unisa, Mbombela

Mbombela

Email address: 63277077@mylife.unisa.ac.za

Supervisor: Dr Patricia Gouws

Email address: gouwspm@unisa.ac.za

Co-Supervisor: Professor Jeanne Kriek

Email address: kriekj@unisa.ac.za

Development of a Framework for Ethical and Cyber-Safe Robotic Systems in the Service Industry

Qualification: Msc.

Thank you for the application for research ethics approval by the College of Science, Engineering and Technology_ School of Computing_ERC for the above-mentioned research study. Ethics approval is granted for three years.

The low risk application was reviewed by the College of Science, Engineering and Technology_ School of Computing_ERC on 04/08/2025 in compliance with the Unisa Policy on Research Ethics and the Standard Operating Procedure on Research Ethics Risk Assessment.

The proposed research may now commence with the provisions that:

1. The researcher(s) will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.
2. Any adverse circumstance arising during the undertaking of the research study that may affect the ethical integrity of the study, including those involving research participants, third parties, or juristic persons, must be reported in writing to the College of Science, Engineering and Technology_ School of Computing_ERC without delay.
3. The researcher(s) will conduct the study according to the methods and procedures set out in the approved application.
4. Any changes that may affect study-related risks to research participants, juristic or third persons, must be reported in writing to the College of Science, Engineering and Technology_ School of Computing_ERC, accompanied by a progress report.

5. The researcher will ensure that the research study complies with all applicable national legislation, professional codes of conduct, institutional guidelines, and scientific standards relevant to the specific field of study. Where applicable, adherence to the following South African legislation is essential: the Protection of Personal Information Act (No. 4 of 2013), the Children's Act (No. 38 of 2005), and the National Health Act (No. 61 of 2003)
6. Future use of this research data is permitted only in de-identified form and only for secondary research with objectives similar to those of the original study. Any secondary use involving identifiable human data will require additional ethics clearance.
7. No fieldwork activities may continue beyond the stated expiry date 04/08/2028. A completed Research Ethics Progress Report must be submitted as an application for renewal and is subject to approval by the Research Ethics Committee. A Close-Out Report must be submitted upon completion of the research study.
8. The College of Science, Engineering and Technology_ School of Computing_ERC may require the submission of regular progress reports on an annual basis, in alignment with Section 7.2 of the Unisa Policy on Research Ethics (2024).

Additional Conditions

1. Disclosure of data to third parties is prohibited without explicit consent from the research participants and Unisa.
2. Research data must be stored in compliance with the university's research data management policy for a period of up to 15 years.
3. When publishing the results, the researcher must take appropriate precautions to safeguard the confidentiality and privacy of the research participants, juristic persons, third parties, and the university, in accordance with institutional policies and ethical standards.
4. Adherence to the National Statement on Ethical Research and Publication Practices, specifically Principle 7 on Social Awareness, must be ensured. This principle states: 'Researchers and institutions must be sensitive to the potential impact of their research on society, marginal groups, or individuals, and must consider these when weighing the benefits of the research against any harmful effects, with a view to minimising or avoiding the latter where possible.' The University of South Africa (Unisa) accepts no liability for any failure to comply with this principle.

Note

The reference number 8827 should be clearly indicated on all forms of communication with the intended research participants, as well as with the Committee.

Kind regards,



Prof L. Motsi
Chair of College of Science, Engineering and Technology_ School of Computing_ERC
E-mail: Dbischof@unisa.ac.za



Prof I. Naidoo
Executive Dean / By delegation from the Executive Dean of College of Science, Engineering and Technology_ School of Computing_ERC
E-mail: naidoi@unisa.ac.za

Appendix N: Critical Analysis of Literature on Cyber-Safe and Ethical Service Robotics (Synthesised by the author)

Theme	Inclusion Criteria	Exclusion Criteria	Study Title	Author (s) and Year	Paper Type	Country of Study	Research aim/focus	Methodology	Key Findings	Relevant to Cyber-safe Robotics	Relevance to Ethical Robotics	Service Industry Domain	Limitations
Ethical Frameworks	Literature on ethical principles in robotics autonomy, transparency, and accountability. Studies that address ethical concerns in HRI	Studies that focus on non-service sectors or unrelated ethical frameworks.	An ethical framework for human-robot collaboration for the future people-centric manufacturing: A collaborative endeavour with European subject-matter experts in ethics	(Callari et al., 2024a)(Callari et al., 2024a)(Callari et al., 2024a)	Journal article	Vietnam	Ethical AI in education and educational leadership	Bibliometric analysis	There is significant research on the ethics of AI in educational leadership in Western countries, as well as in China and Vietnam. However, there is a notable lack of studies from diverse cultural and socio-political contexts from underrepresented regions.	No	Covers the fundamentals of ethical robotics, including safety, Human–Robot Interaction (HRI), societal implications, and responsible design.	Directly relevant to SI since it focuses on customer experience, safety, trust and quality of service.	Focus on specific ethical dimensions, restricted geographical scope, and the reliance on bibliometric analysis.
			Artificial intelligence in services:	(Flavián & Casalo, 2021)(Flavián &	Journal article	Not specified	Analysis of research on AI ethics in	Bibliometric analysis of 286 journal articles	AI ethics in services are still developing	Low	Highly relevant	Maps current research on AI ethics in service contexts.	Relies on bibliometric methods and citation analysis that may overlook nuanced findings

Appendix N: Critical Analysis of Literature on Cyber-Safe and Ethical Service Robotics (Synthesised by the author)

Theme	Inclusion Criteria	Exclusion Criteria	Study Title	Author (s) and Year	Paper Type	Country of Study	Research aim/focus	Methodology	Key Findings	Relevant to Cyber-safe Robotics	Relevance to Ethical Robotics	Service Industry Domain	Limitations
			current trends, benefits and challenges	Casaló, 2021)(Flavián & Casaló, 2021)(Flavián & Casaló, 2021)	Conference Proceedings	UK	services , and identification of themes and trends	Bibliometric analysis of 286 journal articles	AI ethics in services are still emerging and primarily focus on trust, social cues, safety and labour implications.	Highly relevant is the ethical dimension critical to cyber-safe robotic applications.	Highly relevant is the ethical dimension of trust and safety in HRI.	Directly maps current research on AI ethics within the service industry.	and capture emerging perspectives.
			Governance and Compliance of Autonomous Systems and Robotics: Ethical and Legal Frameworks for the Future	(Ranasinghe, 2024)(Ranasinghe, 2024)(Ranasinghe, 2024)(Ranasinghe, 2024)			Systematic analysis of research on AI ethics in services						Relies on bibliometric methods and citation analysis that may overlook nuanced findings and a global perspective.
			AI4People - An Ethical Framework for a Good AI Society: Opportunities	(Floridi et al., 2018b)(Floridi et al., 2018b)(Floridi et al., 2018b)(Floridi et al., 2018b)			Analysis of research on AI ethics in services , and identification of themes						Relies on bibliometric methods that may overlook nuanced findings and qualitative details.

Appendix N: Critical Analysis of Literature on Cyber-Safe and Ethical Service Robotics (Synthesised by the author)

Theme	Inclusion Criteria	Exclusion Criteria	Study Title	Author (s) and Year	Paper Type	Country of Study	Research aim/focus	Methodology	Key Findings	Relevant to Cyber-safe Robotics	Relevance to Ethical Robotics	Service Industry Domain	Limitations
			unities, Risks, Principles, and Recommendations				and publication trends	es, and R-Software to examine patterns	and labour implications.	al for cyber-safety in robotics applications.			
			An ethical framework for human-robot collaboration for the future people-centric manufacturing: A collaborative endeavour with European subject-matter experts in ethics	(Callari et al., 2024a)(Callari et al., 2024a)(Callari et al., 2024a)(Callari et al., 2024a)	Journal article	European context	To develop a human-centred ethical framework for human-robot collaboration in manufacturing.	Empirical survey approach using a Delphi expert consensus process	The most critical ethical concern identified is “Replacement” and its implications for labour. The factors that most affect users' intention and acceptance are Social cues, Trust and Safety.	Emphasis on safety, trust and data protection aligns with cybersecurity concerns in robotics	Highlights ethical factors like safety, trust, social cues and responsibility, vital for ethical framework development in HRI	Moderate relevance. Ethical principles are applicable to service industries adopting robotics.	Limited stakeholder diversity, based on EU expert input. Basically, theoretical with less focus on practical implementation or empirical validation in real-world settings.

Appendix N: Critical Analysis of Literature on Cyber-Safe and Ethical Service Robotics (Synthesised by the author)

Theme	Inclusion Criteria	Exclusion Criteria	Study Title	Author (s) and Year	Paper Type	Country of Study	Research aim/focus	Methodology	Key Findings	Relevant to Cyber-safe Robotics	Relevance to Ethical Robotics	Service Industry Domain	Limitations
			Regulating artificial intelligence and robotics: ethics by design in a digital society	(Iphofen & Kritikos, 2021)(Iphofen & Kritikos, 2021)(Iphofen & Kritikos, 2021)(Iphofen & Kritikos, 2021)	Journal article	European context	To examine the regulatory challenges posed by AI and robotics	Literature review. Conceptual and policy analysis	Independent oversight and continuous vigilance in the design and deployment of ethical AI systems. Autonomous machines raise moral questions and pose significant challenges in policy-making	High relevance	Very high relevance	High relevance. Addresses ethical issues associated with AI applications in care, HRI and autonomous decision-making in service sectors.	Primarily conceptual and policy-oriented and lacks detailed pathways for implementing enforceable standards.
			On Ethical Challenges Raised by Care Robots : A Review of the Existing	(Saplacan et al., 2021)(Saplacan et al., 2021)(Saplacan et al., 2021)(Saplacan et al., 2021)	Conference Proceeding	Norway	To identify and analyse the ethical challenges of care robots in elderly homes and	Literature review of 20 EU care robotics projects and legal and ethical frameworks.	Identified ethical issues such as privacy, autonomy, safety, responsibility, accountability, and dignity. More so,	Highly relevant. Addresses vulnerability issues such as privacy, safety and security	Highly relevant. Addresses the ethical and regulatory issues of care robots.	Highly relevant. Focuses on caregiving and healthcare services.	Primarily conceptual and mainly centred on the EU environment.

Appendix N: Critical Analysis of Literature on Cyber-Safe and Ethical Service Robotics (Synthesised by the author)

Theme	Inclusion Criteria	Exclusion Criteria	Study Title	Author (s) and Year	Paper Type	Country of Study	Research aim/focus	Methodology	Key Findings	Relevant to Cyber-safe Robotics	Relevance to Ethical Robotics	Service Industry Domain	Limitations
			Regulatory-, Theoretical-, and Research Gaps				evaluate regulatory gaps.		there is a lack of a comprehensive legal framework in the EU.	which align with cyber-safe robotics concerns			
			Value Sensitive Design : Shaping Technology with Moral Imagination	(Batya & David, 2019)(Batya & David, 2019)(Batya & David, 2019)(Batya & David, 2019)	Book Section	USA/ Global	To analyse how AI-based systems can be designed with value sensitivity to incorporate ethics into socio-technical frameworks	SLR and critical synthesis of VSD frameworks	Highlights deficiencies in integrating ethics within socio-technical AI systems	High	Very High	High	Limited empirical validation.
			ETHICAL ALIGNMENT DESIGN	(IEEE, 2019b)(IEEE, 2019b)(IEEE, 2019b)(IEEE, 2019b)	Book Section	Global	To establish comprehensive ethical and governance standards for	Multi-stakeholder consultation and framework synthesis	Provides global reference for responsible human-aligned AI and robotic systems,	High	Very High	Very High.	Conceptual and lacks domain-specific implementation strategies.

Appendix N: Critical Analysis of Literature on Cyber-Safe and Ethical Service Robotics (Synthesised by the author)

Theme	Inclusion Criteria	Exclusion Criteria	Study Title	Author (s) and Year	Paper Type	Country of Study	Research aim/focus	Methodology	Key Findings	Relevant to Cyber-safe Robotics	Relevance to Ethical Robotics	Service Industry Domain	Limitations
Cyber-safety Issues	Studies on cyber threats, vulnerabilities, risk management, and mitigation strategies in service robotics	Studies addressing cyber-safety issues, risk management, and design unrelated to the service industry and robotics.	RDSF: Risk Driven Security Framework for Industrial Autonomous Robots	(Udo & Sallal, 2023)(Udo & Sallal, 2023)(Udo & Sallal, 2023)(Udo & Sallal, 2023)	Conference Proceedings	UK	autonomous and intelligent systems To develop a Risk-Driven Security Framework.	Review of existing risk management frameworks.	emphasising accountability, transparency and data governance. Existing risk management frameworks do not adequately address the interaction modes between humans and robots.	Directly addresses cybersecurity vulnerabilities in service robotics.	Though not directly, it supports safer robotic operations.	Primarily applicable to the service industry in HRI environments.	The study offers a conceptual framework but lacks empirical validation.
			Socio-technical systems cybersecurity framework	(Malatji et al., 2019a)(Malatji et al., 2019a)(Malatji et al., 2019a)(Malatji et al., 2019a)	Journal Paper	Australia	To develop a socio-technical model that integrates human, organisational, and technical aspects of	Empirical case analysis and conceptual model design.	Shows that integrating human, organisational and technical layers improves cyber-safety resilience and adaptive response in robotic systems	Very High	High	Very High	Limited applicability outside industrial contexts

Appendix N: Critical Analysis of Literature on Cyber-Safe and Ethical Service Robotics (Synthesised by the author)

Theme	Inclusion Criteria	Exclusion Criteria	Study Title	Author (s) and Year	Paper Type	Country of Study	Research aim/focus	Methodology	Key Findings	Relevant to Cyber-safe Robotics	Relevance to Ethical Robotics	Service Industry Domain	Limitations
Cyber-Safe Service Robotics	Literature review	Not applicable	Addressing cyber-safety challenges in robotics: A comprehensive overview	(Tanimu & Abada, 2025a)(Tanimu & Abada, 2025a)(Tanimu & Abada, 2025a)(Tanimu & Abada, 2025a)	Journal Article	Not specified	cyber-safety for complex systems.	Literature review	Identified vulnerabilities require robust authentication and encryption techniques, along with collaboration among stakeholders.	Highly relevant	Highly relevant in terms of the ethics of data protection.	Applicable to service sectors.	Not sector-specific, focuses on general strategies, and lacks empirical data.
							To explore cybersecurity challenges and mitigation strategies						
							To offer an overview of Security Considerations in AI-Robotics						
Ethical Service Robotics	Survey and taxonomy development	Not applicable	Security Considerations in AI-Robotics: A Survey of Current Methods	(Neupane et al., 2024)(Neupane et al., 2024)(Neupane et al., 2024)(Neupane et al., 2024)	Journal Article	Not specified	To introduce a framework addressing ethical and legal concerns, attack vectors, and human-robot interaction	Survey and taxonomy development	Introduced a framework addressing ethical and legal concerns, attack vectors, and human-robot interaction	Highly relevant, as it provides a comprehensive understanding of security risks in AI-	Highly relevant as it addresses the psychological impact of ethical concerns.	Applicable to service sectors that deploy AI-driven robot systems	May not cover emerging technology post 2023.

Appendix N: Critical Analysis of Literature on Cyber-Safe and Ethical Service Robotics (Synthesised by the author)

Theme	Inclusion Criteria	Exclusion Criteria	Study Title	Author (s) and Year	Paper Type	Country of Study	Research aim/focus	Methodology	Key Findings	Relevant to Cyber-safe Robotics	Relevance to Ethical Robotics	Service Industry Domain	Limitations
Cyber-Safe and Ethical Service Robotics	Inclusion Criteria: Studies focusing on the integration of cyber-safety and ethical considerations in service robotics design and implementation.	Exclusion Criteria: Studies not related to service robotics or not addressing cyber-safety or ethical aspects.	Challenges and Opportunities						interaction security while exploring vulnerabilities in navigation and control systems perception.	robotics.			
			Cyber-safety of robotic systems: Leading challenges and robotic system design methodology	(Dutta & ZIELINSKA, 2021)(Dutta & ZIELINSKA, 2021)(Dutta & ZIELINSKA, 2021)(Dutta & ZIELINSKA, 2021)	Journal Article	International	To investigate cybersecurity issues in robotic systems and suggest design improvement methodologies.	Literature review	Highlighted the necessity for user-friendly robot interfaces and the capability for multi-modal interactions in HRI within unstructured environments.	Relevant, as it highlights the need for secure design in service robotics.	Relevant, as it focuses on ethical deployment and user-friendly interfaces	Applicable to service sectors like healthcare and domestic services.	Proposed methodologies lack empirical validation.
			Developing A Framework for A Tactile Internet Enable	(Brown - Acquaye et al., 2019)(Brown-Acquaye et al., 2019)	Journal of Robotics Article	Ghana	To create a comprehensive framework and architecture for a real-	Literature Review, Theoretical Architectural Review, and	The identified enabling technologies allow the architecture to facilitate	Highly relevant. Highlights network and device-level	Highly relevant. Highlights the need for ethical and safety standard	Highly relevant. Though it focuses primarily on healthcare service delivery, principles	No details on prototype testing and implementation. It mainly concerns architecture and technological possibilities.

Appendix N: Critical Analysis of Literature on Cyber-Safe and Ethical Service Robotics (Synthesised by the author)

Theme	Inclusion Criteria	Exclusion Criteria	Study Title	Author (s) and Year	Paper Type	Country of Study	Research aim/focus	Methodology	Key Findings	Relevant to Cyber-safe Robotics	Relevance to Ethical Robotics	Service Industry Domain	Limitations
			ded Robot Assisted Real-Time Interactive Medical System	Brown-Acquaye et al., 2019)(Brown-Acquaye et al., 2019)			time, interactive medical system supported by robots, utilising tactile internet, robotics, AI, and haptics.	Conceptual Design	remote medical procedures, including diagnosis and surgery, thus addressing the shortage of skilled personnel.	requirements for maintaining cyber-safety in robotic healthcare systems	s and operator training for automation in medical procedures.	can be applied to other service sectors.	
			Integration of PLC and Robotic Operating System for Enhanced Automation Efficiency'	(Saxena et al., 2023)(Saxena et al., 2023)(Saxena et al., 2023)(Saxena et al., 2023)	Conference proceeding	India and Iraq	To evaluate the integration of Programmable Logic Controllers (PLC) with the Robotic Operating System (ROS) for industrial automation.	Literature review and conceptual analysis	Integration enhances the flexibility of automation and facilitates human-robot collaboration in industrial processes.	Potentially relevant as integration involves data exchange, communication protocols and cyber-safety considerations, which are critical.	Indirectly relevant as it emphasises on safety and reliability in automation.	Highly relevant, though it applies directly to industry automation, efficiency, and improved automation are useful for service delivery.	Limited insights into real-world application complexities. Primarily conceptual with no empirical validation.
			Intelligent	(Soori et al.,	Journal	Glob	To review	SLR of robotics	Identifies intelligent	Highly relevant	Relevant as it	Indicates a potential	Lacks empirical validation;

Appendix N: Critical Analysis of Literature on Cyber-Safe and Ethical Service Robotics (Synthesised by the author)

Theme	Inclusion Criteria	Exclusion Criteria	Study Title	Author (s) and Year	Paper Type	Country of Study	Research aim/focus	Methodology	Key Findings	Relevant to Cyber-safe Robotics	Relevance to Ethical Robotics	Service Industry Domain	Limitations
			robotic systems in Industry 4.0: A review	2024)(Soori et al., 2024)(Soori et al., 2024)(Soori et al., 2024)	Review Article	al perspective	the roles of intelligent robotic systems in Industry 4.0	and Industry 4.0 studies	t robotic applications, highlighting benefits and challenges.	t, as it addresses cyber-safety within the context of cloud-based robotic systems in Industry 4.0.	emphasises ethical considerations and promotes responsible deployment.	benefit for service sectors that adopt robotic system integration, although it mainly concentrates on industrial environments.	reviews secondary sources.
			Robot AtFactory 4.0: a ROS framework for the SimTwo simulator models of potential solutions to problems encountered in the	(Berger et al., 2022)(Berger et al., 2022)(Berger et al., 2022)(Berger et al., 2022)	Conference Proceeding	Portugal	To develop and validate a framework for integrating the SimTwo simulator with ROS.	Literature review, system development and experimental test.	The framework facilitates testing of navigation and behaviour within a realistic simulation.	Indirectly, the framework facilitates testing of navigation and behaviour within a realistic simulation. May support safer design practices.	Indirectly. Promotes the development of an autonomous system that may potentially reduce ethical concerns.	Relevant. Applicable to industrial service robotics and education in Industry 4.0	Limited to simulation and does not address ethical and cyber-safety aspects

Appendix N: Critical Analysis of Literature on Cyber-Safe and Ethical Service Robotics (Synthesised by the author)

Theme	Inclusion Criteria	Exclusion Criteria	Study Title	Author (s) and Year	Paper Type	Country of Study	Research aim/focus	Methodology	Key Findings	Relevant to Cyber-safe Robotics	Relevance to Ethical Robotics	Service Industry Domain	Limitations
Human –Robot Interaction (HRI)	Studies that explore privacy, trust, data ethics, user acceptance and ethical concerns in HRI.	Studies on industrial robots with no correlation to service industry applications and limited to mechanical or technical aspects without HRI.	Proactive Interaction Framework for Intelligent Social Receptionist Robots	(Xue et al., 2021)(Xue et al., 2021)(Xue et al., 2021)(Xue et al., 2021)	Conference Proceedings	Not specified	To propose a framework for proactive HRI in receptionist robots.	Development and testing of the framework	The proposed framework enhances the monitoring and cybersecurity management of robotic systems.	Highly relevant, as it is a cybersecurity-based control system.	Relatively relevant as it centres on data protection and integrity, which are integral components of ethics.	Applicable in social settings, such as service robotics for assistance.	Confined to receptionist contexts and may need adjustments for wider use.
			Real-Time Human-Robot Interaction for a Service Robot Based on 3D Human Activity Recognition and Human-Mimicking Decision	(K. Li et al., 2019)(K. Li et al., 2019)(K. Li et al., 2019)(K. Li et al., 2019)	Conference Proceedings	China	To develop HRI system that enables robots to recognise human activities using 3D skeletal data recognition	3-layer Long-Short-Term Memory (LSTM) neural network	The proposed system allows for natural body language interaction and intuitive decision-making in service robotics.	Relevant, focuses on safety improvement.	Highly relevant, as it enhances and supports ethical considerations in autonomous decision-making and safety.	Applicable to service domains like healthcare and area where interaction quality and operational effectiveness need improvement.	It is based on controlled experimentation and may require further testing in diverse environments.

Appendix N: Critical Analysis of Literature on Cyber-Safe and Ethical Service Robotics (Synthesised by the author)

Theme	Inclusion Criteria	Exclusion Criteria	Study Title	Author (s) and Year	Paper Type	Country of Study	Research aim/focus	Methodology	Key Findings	Relevant to Cyber-safe Robotics	Relevance to Ethical Robotics	Service Industry Domain	Limitations
			Mechanism										
			Conceptual framework for the use of robots, artificial intelligence, and service automation in travel, tourism, and hospitality industries.	(Ivanov & Webster, 2019)(Ivanov & Webster, 2019)(Ivanov & Webster, 2019)	Book Section	Multiple countries' references and a global perspective	To develop a conceptual framework for how robots, AI, and service automation (RAISA) are integrated into service sectors, analysing interaction, adoption, perception, and implications for service delivery.	SLR, analysis of empirical studies and syntheses of frameworks.	Positive attitudes towards robots are common for roles such as information provision, delivery, and domestic chores; however, resistance exists for services involving physical contact, like massages and babysitting. Customer perceptions are shaped by marketing, interactions and interface design.	Indirectly, it emphasises the adoption of technology and user experience, as well as the need for interfaces that relate to cybersecurity.	Moderately relevant, as it discusses key ethical considerations such as privacy, potential job displacement, user acceptance, transparency, and HRI concerns.	Highly relevant, provides a robust framework and review of empirical studies specific to hospitality, tourism, travel, and inform service innovation.	Aspects of ethics and cyber-safety are not discussed extensively, and differences in study contexts and cultures may affect the generalisability.

Appendix N: Critical Analysis of Literature on Cyber-Safe and Ethical Service Robotics (Synthesised by the author)

Theme	Inclusion Criteria	Exclusion Criteria	Study Title	Author (s) and Year	Paper Type	Country of Study	Research aim/focus	Methodology	Key Findings	Relevant to Cyber-safe Robotics	Relevance to Ethical Robotics	Service Industry Domain	Limitations
			An Attachment Framework for Human-Robot Interaction	(Rabb et al., 2022)(Rabb et al., 2022)(Rabb et al., 2022)(Rabb et al., 2022)	Journal Article	USA	To develop and validate the concept of attachment that differentiates its nature between humans and robots, drawing from social psychology	Literature review of attachment theory across several disciplines and analysis of existing HRI studies	Attachment in humans ranges from weak to strong, with robots responding differently depending on their capabilities and the context. Most only meet physical needs and do not serve as a secure base. The framework employs proximity-seeking to assess attachment levels, showing robots' potential to evoke various attachment responses	Indirectly relevant, understanding attachment levels can guide the development of secure robotic designs and promote safer interactions. This knowledge helps reduce the risks of unhealthy attachment and dependency.	Highly relevant as it discusses the ethical implications of human-robot attachment and helps clarify boundaries that inform ethical guidelines.	Provides insights into designing service robotics for appropriate attachment, thereby improving user acceptance and satisfaction.	The framework is a theoretical and conceptual contribution and may require empirical validation or experimentation to assess actual adoption behaviour.

Appendix N: Critical Analysis of Literature on Cyber-Safe and Ethical Service Robotics (Synthesised by the author)

Theme	Inclusion Criteria	Exclusion Criteria	Study Title	Author (s) and Year	Paper Type	Country of Study	Research aim/focus	Methodology	Key Findings	Relevant to Cyber-safe Robotics	Relevance to Ethical Robotics	Service Industry Domain	Limitations
			Success factors for introducing industrial human-robot interaction in practice: an empirically driven framework	(Kopp et al., 2020)(Kopp et al., 2020)(Kopp et al., 2020)(Kopp et al., 2020)	Journal Article on Survey-Based Empirical Study and Framework Development	Germany	To identify success factors for implementing HRI (Cobots) and to develop an empirically driven framework for human–robot collaboration.	SLR and German experts’ evaluation of identified success factors	Occupational safety, proper setup, proactive communication, and perception concerns are vital success factors. Many of these elements are independent of the application's motivation, and employees' acceptance is often ignored.	Indirectly relevant. Emphasis on safe human–robot interaction aligns with cyber-safe principles	Relevant. Highlights aspects of ethics, including transparency, job security, and trust.	Highly relevant. While it centres on manufacturing, the key success factors highlighted are also applicable to service sectors.	Highly relevant. While it centres on manufacturing, the key success factors highlighted are also applicable to service sectors.
			Cobotics: The Evolving Roles and Prospects of Next-Generation	(Rahman et al., 2024)(Rahman et al., 2024)(Rahman et al., 2024)(Rahman et al., 2024)	Journal Article	Bangladesh, Malaysia, Saudi Arabia	To explore the role of Cobotics in Industry 5.0 with an emphasis on	SLR of Cobotic studies	Cobotics plays a vital role in enhancing safety and efficiency in human–robot	Indirectly. Discusses safety, ethical considerations and data security	Relevant. Discusses ethics, including privacy and data security, as well as	Highly relevant to sectors that require human-robot collaboration. especially in healthcare and logistics	Current insights are basically theoretical and need empirical validation.

Appendix N: Critical Analysis of Literature on Cyber-Safe and Ethical Service Robotics (Synthesised by the author)

Theme	Inclusion Criteria	Exclusion Criteria	Study Title	Author (s) and Year	Paper Type	Country of Study	Research aim/focus	Methodology	Key Findings	Relevant to Cyber-safe Robotics	Relevance to Ethical Robotics	Service Industry Domain	Limitations
			Collaborative Robots in Industry 5.0	n et al., 2024)			human–robot collaboration, and future directions for Cobots-industry integration.		collaboration. Future research should focus on establishing ethical guidelines, developing user-friendly interfaces, ensuring secure data management, and conducting empirical validation through observations.	y, which are crucial for developing cyber-safe robotic systems.	guidelines for safe human-robot interaction.		
Legal and Regulatory Standards	Studies on legal frameworks, governance on ethical and cyber-safe robotics in HRI, and discussing global and regional regulatory differences.	Studies unrelated to ethical or cyber-safe compliance.	Robotic role theory: an integrative review of human–robot service interaction to advance role theory	(Blaurock et al., 2022)(Blaurock et al., 2022)(Blaurock et al., 2022)(Blaurock et al., 2022)	Journal Article	Global (syntheses studies from multiple countries)	An empirical analysis of human–robot service interaction across national differences and to develop	Systematic literature review and Conceptual framework	The development of the extent and scale of internet usage accounts for the variations in cybersecurity across regions.	Indirectly relevant, as it emphasises human–robot interaction, which can inform cybersecurity practice	Highly relevant as it emphasises ethical deployment in the area of role enactment and user perceptions.	Applicable as it offers design, management, and deployment insights in various service settings.	The proposed framework relies primarily on existing literature and lacks experimental validation.

Appendix N: Critical Analysis of Literature on Cyber-Safe and Ethical Service Robotics (Synthesised by the author)

Theme	Inclusion Criteria	Exclusion Criteria	Study Title	Author (s) and Year	Paper Type	Country of Study	Research aim/focus	Methodology	Key Findings	Relevant to Cyber-safe Robotics	Relevance to Ethical Robotics	Service Industry Domain	Limitations
			in the age of social robots				a comprehensive framework.			es of protecting robots from misuse.			
			Exploring the Potential and Perceptions of Social Robots in Tourism and Hospitality: Insights from Industry Executives and Technology Evaluation	(Skubis, 2024)(Skubis, 2024)(Skubis, 2024)	Journal Article	Europe	Exploratory qualitative study	To investigate the possibilities, acceptance, and views of social robots in the tourism and hospitality sectors.	The benefits, opportunities, and challenges of social robot integration necessitate a regulatory framework.	Indirectly relevant, as it emphasises the need to balance technology development with data privacy and security.	Highlights the ethical challenges of social robot integration.	Applicable to the service industry, such as tourism and hospitality.	Limited focus on perception and may not accurately represent the actual implementation results.
			Global Regulatory Frameworks for the Use of Artificial Intelligence	(Palanippan et al., 2024)(Palanippan et al., 2024)(Palanippan et al., 2024)	Journal Review Article	US, EU, China, Brazil, UK, Australia,	Literature analysis and policy review	To examine and analyse the existing global regulatory framework	Regulatory frameworks vary across jurisdictions with little alignment. They	Highlights the need for regulation to mitigate risks in autono	Highlights ethical concerns such as transparency, explainability, safety,	Applicable to the healthcare service sector.	Regulatory scopes differ across jurisdictions, which can influence the applicability of certain regulations. The review might not capture every

Appendix N: Critical Analysis of Literature on Cyber-Safe and Ethical Service Robotics (Synthesised by the author)

Theme	Inclusion Criteria	Exclusion Criteria	Study Title	Author (s) and Year	Paper Type	Country of Study	Research aim/focus	Methodology	Key Findings	Relevant to Cyber-safe Robotics	Relevance to Ethical Robotics	Service Industry Domain	Limitations
			ence (AI) in the Health care Services Sector	al., 2024)(Palania ppan et al., 2024)		Singapore		ork for AI in healthcare.	must be flexible and adaptable to the fast-paced evolution of AI development.	mous healthcare robotic systems, underscoring the importance of addressing cyber-safety concerns.	accountability, and data governance critical for ethical robotic systems.		nuance in the ever-changing regulatory landscape. Additionally, there is limited empirical data in healthcare on how these regulations affect the deployment of robotic systems, emphasising the need for adaptation and further research.
			Facilitating urban tourism governance with crowdsourced big data: A framework based on Shenzhen and Jiangm	(Liu et al., 2023)(Liu et al., 2023)(Liu et al., 2023)	Journal Article on Empirical Study and Framework Development	China	Literature analysis and case study	To develop a framework for leveraging crowdsourced big data to improve urban tourism governance and management.	Crowdsourced data effectively provides a scalable, data-driven governance model, and empirical testing shows the framework's potential to guide	Indirectly relevant. The framework may inspire cyber-safe protocols for big data protection in robotic systems.	Not relevant	Applicable to tourism services, guiding service providers and stakeholders on improving service delivery and management.	Limited focus on data ethics and privacy in crowdsourcing, as well as generalisability. Reliance on a single source of data may introduce bias.

Appendix N: Critical Analysis of Literature on Cyber-Safe and Ethical Service Robotics (Synthesised by the author)

Theme	Inclusion Criteria	Exclusion Criteria	Study Title	Author (s) and Year	Paper Type	Country of Study	Research aim/focus	Methodology	Key Findings	Relevant to Cyber-safe Robotics	Relevance to Ethical Robotics	Service Industry Domain	Limitations
			en, China						and enhance tourism management practices.				
			Towards a Framework to Assess the Impact of Industry 4.0 Technologies & Services on Production Resources	(Hasan & Trianni, 2022b)(Hasan & Trianni, 2022b)(Hasan & Trianni, 2022b)(Hasan & Trianni, 2022b)	Conference Paper	Australia	Propose a framework that connects Industry 4.0 technologies, services, and production resources to inform decision-making.	Literature review and theoretical framework	Industry 4.0 technologies influence resource efficiency, waste reduction, energy consumption, and productivity.	Indirectly relevant. Addresses the security implications of IoT and automation.	Indirectly relevant, as it discusses human implications and sustainability.	Highly relevant; applicable to both service and manufacturing industries.	Although there is limited empirical validation, it is an introductory framework that does not address ethical challenges.
Cyber-Ethical Integration Frameworks	Studies that incorporate cyber-safety and ethical frameworks in the context of HRI.	Studies that focus on either or unrelated to HRI and service	A Principalist framework for Cyber-safety Ethics	(Formosa et al., 2021)(Formosa et al., 2021)(Formosa et al., 2021)(Formosa et al., 2021)	Journal Article	Australia	Theoretical analysis with case studies	To develop a Principalist ethical framework for cybersecurity based on AI ethics and	Proposed mapping AI-ethics to effectively address cybersecurity challenges.	Highly relevant, as it provides a structured ethical approach to addressing cyber-safety	Highly relevant. Addresses ethical issues in cyber-safety practices relevant to robotics.	Applicable to service sectors.	The conceptual framework requires empirical validation of its effectiveness in practical settings.

Appendix N: Critical Analysis of Literature on Cyber-Safe and Ethical Service Robotics (Synthesised by the author)

Theme	Inclusion Criteria	Exclusion Criteria	Study Title	Author (s) and Year	Paper Type	Country of Study	Research aim/focus	Methodology	Key Findings	Relevant to Cyber-safe Robotics	Relevance to Ethical Robotics	Service Industry Domain	Limitations
		domains.						bioethics		issues in the robotic service industry.			
			Ethics of Artificial Intelligence and Robotics in the Architecture, Engineering, and Construction Industry	(Liang et al., 2024)(Liang et al., 2024)(Liang et al., 2024)(Liang et al., 2024)	Journal Article	US	Literature Review (PRISMA)	To investigate ethical issues related to the use of AI and robotics within AEC industry.	Identified nine ethical issues and an increasing trend on AI-Robotics ethics and proposed future research directions.	Highly relevant as it emphasises the need for robust cybersecurity measures for data protection and safety.	Highly relevant as it addresses ethical issues like job displacement, decision-making, liability and trust.	Relevant though focuses on the AEC industry, the themes' impacts apply to the service domain that deploys AI and robotics.	Focused on the AEC industry, findings may need adaptation for other service sectors.
			Secure Robotics: A Definition and a Brief Review from a Cyber-safety Control and Implementation	(Haskard et al., 2022)(Haskard et al., 2022)(Haskard et al., 2022)(Haskard et al., 2022)	Journal Article	Australia	Conceptual Analysis and Literature Review	To define secure robotics and assess cybersecurity control and implementation methodologies.	Identified five layers for implementing cybersecurity controls and the need to integrate cyber-safe measures into the robotic	Highly relevant, it provides a structured approach to implementing cybersecurity in robotics.	Highly relevant, emphasises ethical considerations in the design and deployment of secure robotics	It lacks empirical validation since it is a conceptually proposed methodology.	

Appendix N: Critical Analysis of Literature on Cyber-Safe and Ethical Service Robotics (Synthesised by the author)

Theme	Inclusion Criteria	Exclusion Criteria	Study Title	Author (s) and Year	Paper Type	Country of Study	Research aim/focus	Methodology	Key Findings	Relevant to Cyber-safe Robotics	Relevance to Ethical Robotics	Service Industry Domain	Limitations
			ion Metho dology Perspe ctive						system lifecycle.				
			Hyperl edger Fabric Blockc hain and ROS 2 Integra tion for Auton omous Mobile Robots						Integratio n promotes ethical values like transpare ncy, trust, and security. Blockcha in guarantee s data integrity and accounta bility.				
			A Frame work for Hotel Invent ory Contro l Syste m for Online Travel Agenc y using Roboti	(Sharm ar & Guleria , 2021)(Sharma r & Guleria , 2021)(Sharma r & Guleria , 2021)(Sharma	Confe rence paper	India	Develo ping a robotic process automat ion (RPA) framew ork for hotel invento ry control in online travel	Concept ual framew ork	Demonstr ates how RPA simplifies repetitive tasks in inventory managem ent, enhancin g efficiency and reducing human error.	Not relevan t, though, address automa tion securit y issues could arise.	Not relevant. Althoug h ethical consider ations, such as custome r satisfacti on and accounta bility, are mention ed.	Highly relevant. Addresses automation and hospitality.	There is a lack of empirical validation. Cybersecurity and ethical aspects have not been considered thoroughly.

Appendix N: Critical Analysis of Literature on Cyber-Safe and Ethical Service Robotics (Synthesised by the author)

Theme	Inclusion Criteria	Exclusion Criteria	Study Title	Author (s) and Year	Paper Type	Country of Study	Research aim/focus	Methodology	Key Findings	Relevant to Cyber-safe Robotics	Relevance to Ethical Robotics	Service Industry Domain	Limitations
Service Robotics	Inclusion of studies that explore the use of robots in service industries, focusing on the integration of AI and automation.	Exclusion of studies that do not focus on service robotics or do not address the integration of AI and automation.	Process Automation	r & Guleria, 2021)			agencies						
			Automatic Process Automation-Based System for Intelligent Work Order Management with Active Service in Power System	(Wang et al., 2025)(Wang et al., 2025)(Wang et al., 2025)(Wang et al., 2025)	Conference Paper	China	Validate RPA-based automated workflows for power system work order management to enhance efficiency, accuracy, and proactive governance.	Empirical test evaluation of RPA	Reduced processing time with 99.7% accuracy, manual intervention, and improved collaboration.	Not relevant, though, as addressing automation security issues could arise.	Not relevant, although ethical considerations such as customer satisfaction and accountability are implied.	Highly relevant. For utility and power services.	Limited to power service in China, with security aspects not considered.
			Conceptual framework of the use of robots, artificial intelligence and service	(Ivanov & Webster, 2019)(Ivanov & Webster, 2019)(Ivanov & Webster	Book Section	Global perspective	To develop a conceptual framework for the use of robots, AI, and service automat	Literature review and conceptual	Framework identifies gaps, barriers, drivers, and impacts of RAISA on customer experienc	Indirectly relevant. Cyber-safety is not addressed specifically.	Highly relevant. Addresses ethical issues like job loss, privacy and fairness.	Highly relevant. Focuses on service sectors and automation adoption.	Lacks empirical validation, only theoretical. Cyber-safety and ethical challenges not addressed.

Appendix N: Critical Analysis of Literature on Cyber-Safe and Ethical Service Robotics (Synthesised by the author)

Theme	Inclusion Criteria	Exclusion Criteria	Study Title	Author (s) and Year	Paper Type	Country of Study	Research aim/focus	Methodology	Key Findings	Relevant to Cyber-safe Robotics	Relevance to Ethical Robotics	Service Industry Domain	Limitations
-------	--------------------	--------------------	-------------	---------------------	------------	------------------	--------------------	-------------	--------------	---------------------------------	-------------------------------	-------------------------	-------------

			automation in travel, tourism, and hospitality companies	r, 2019)(Ivanov & Webster, 2019)			ion (RAISA) in tourism and hospitality industries.		e, operation and employment.				
--	--	--	--	----------------------------------	--	--	--	--	------------------------------	--	--	--	--

Appendix O: Reliability Analysis Evaluation Items (Synthesised by author)

S/ N	Q4. Do you think servic e roboti cs ought to adher e to a forma l ethica l code compa rable to that of huma n emplo yees?	Q5. The ACERB Frame work addres ses real and pressin g challen ges in the Roboti cs Service Industr y (RSI).	Q6. The framew ork adequa tely integra tes multipl e discipli nary perspec tives (e.g., ethics, cybers ecurity, HRI).	Q7. The framewor k's structure , compone nts, and interrelat ionships are clearly articulate d and easy to understa nd.	Q8. The visual represe ntation and accompa nyin g explana tion adequa tely commu nicate the framew ork's purpos e and scope.	Q9. The frame work can be practi cally appli ed in real- world servic e doma ins such as healt hcare , hospi tality, or logisti cs.	Q10. The framew ork is adapta ble to differe nt organiz ational context s within the service industr y.	Q11. The frame work contri butes signifi cantly to the field of ethical and cyber secur e roboti cs.	Q12. There are no major omissio ns in the framew ork that could hinder its implem entation or validity.	Q13. I would recom mend the use of this frame work for future projec ts in servic e roboti cs.	Q14. Ethical conside rations such as fairnes s, transpa rency, and account ability are well- integrat ed within the framew ork.	Q15. The frame work provid es a clear pathw ay for ensuri ng respo nsible and huma n- centre d roboti c deploy ment .	Q16. The frame work adequa tely addres ses data protec tion	Q17. The frame work adequa tely addres ses threat resili ence.	Q18. The frame work adequa tely addres ses syste m integri ty.	Q19. The cybers ecurity dimens ion aligns with ethical and operati onal require ments for safe robotic deploy ment.	Q20. The frame work suffici ently consid ers huma n value s.	Q21. The frame work suffici ently consid ers cultur al diversi ty.	Q22. The frame work suffici ently consid ers indus try- speci fic need s.	Q23. The socio- techni cal aspect s are effecti vely integra ted to enhanc e collabo ration betwe en human s and robots .	Q24. The frame work is feasibl e for adopti on by practiti oners and policy maker s in the service robotic s field.	Q25. The implem entation pathwa y describ ed is realistic and scalable .	Q26. The frame work's compone nts form a cohesi ve and logical ly structu red model .	Q27. The framew ork holistic ally addres ses critical aspect s such as ethics, cybers ecurity, socio- technic al system s, and cultural context .	Q28. The frame work would be useful for guidin g the ethical desig n, gover nance, and deploy ment of servic e roboti cs.	
1	5	5	5	4	5	5	5	4	4	4	5	5	4	4	5	5	4	4	5	5	5	4	5	5	5	5
2	5	4	3	4	4	4	3	4	4	4	3	4	3	4	4	4	3	4	4	4	3	4	4	3	4	4
3	5	5	5	5	5	4	5	5	4	4	5	5	5	5	5	4	5	5	4	4	5	5	5	5	5	4
4	5	4	4	4	5	4	5	3	4	4	5	4	4	3	4	4	4	4	5	4	4	4	3	4	4	4
5	5	5	5	4	4	4	5	5	4	5	4	5	4	4	4	5	5	5	4	4	5	4	5	4	5	4
6	5	4	4	3	4	3	3	4	4	3	4	4	3	4	3	3	3	4	3	4	3	3	3	3	3	4
7	5	5	4	5	5	4	4	5	5	5	4	4	5	4	5	5	4	5	5	4	5	4	5	5	5	5
8	5	4	4	5	4	4	4	3	5	4	4	5	3	4	4	4	5	4	5	4	5	4	5	4	5	5
9	5	5	4	5	4	4	5	4	4	5	4	5	4	4	4	4	5	5	5	5	4	5	5	4	4	5
10	5	4	3	4	4	4	3	3	4	4	3	4	3	4	4	4	4	3	3	4	4	4	4	4	4	4
11	5	5	5	4	4	5	4	5	4	4	4	5	5	4	4	4	4	4	5	4	5	4	5	4	5	4
12	5	4	3	3	4	4	3	4	3	4	3	4	4	3	4	4	4	4	4	3	4	3	3	3	3	4
13	5	5	5	5	5	4	5	5	4	4	5	4	5	4	5	4	4	4	4	5	5	5	5	5	4	5
14	5	3	3	3	4	3	3	3	4	4	3	4	3	3	4	3	3	4	4	4	3	3	4	3	3	3
15	5	5	4	5	4	4	5	5	4	5	4	4	5	4	5	5	4	5	5	4	5	5	5	4	5	5
16	5	4	4	4	4	3	4	4	3	4	3	4	3	4	4	3	4	3	3	3	3	4	3	4	3	4
17	5	5	5	4	4	5	5	5	4	5	4	5	4	4	4	5	5	4	4	5	5	4	5	4	5	5
18	5	5	5	5	5	5	4	5	4	5	5	5	5	5	4	5	5	5	4	4	4	5	4	5	5	5
19	5	4	4	4	5	4	4	3	4	4	5	5	4	4	4	5	4	5	4	5	4	4	4	4	4	4
20	5	5	4	5	4	5	5	4	5	5	4	4	5	5	4	5	5	4	5	5	4	5	5	4	5	5
21	5	4	3	4	3	3	4	3	4	3	4	3	3	4	4	4	4	3	3	3	4	3	4	3	4	4
22	5	5	4	4	5	4	4	5	4	4	5	4	5	4	5	5	4	5	4	4	5	5	4	4	4	4
23	5	4	3	3	4	4	4	3	3	4	4	3	3	4	3	4	3	4	4	3	3	3	4	4	4	3
24	5	5	4	4	4	4	4	5	4	4	4	4	4	5	5	4	4	4	4	5	4	5	4	5	5	5
25	5	4	4	3	4	4	4	3	4	4	3	4	4	4	4	4	4	3	4	4	3	3	4	3	3	4
26	5	4	3	3	4	4	3	4	3	3	4	3	3	4	3	3	3	4	3	3	3	3	3	3	4	4
27	4	3	2	3	3	3	3	2	2	2	2	2	1	1	3	2	1	1	2	2	1	1	2	1	1	1

Appendix P: Individual Item Reliability Statistics of Quantitative Responses (Synthesised by author)

Item	Cronbach's α (if item dropped)	Item-rest correlation			Mean			Variance			SD				
	Estimate	Lower 95% CI	Upper 95% CI	Estimate	Lower 95% CI	Upper 95% CI	Estimate	Lower 95% CI	Upper 95% CI	Estimate	Lower 95% CI	Upper 95% CI	Estimate	Lower 95% CI	Upper 95% CI
Q4. Do you think service robotics ought to adhere to a formal ethical code comparable to that of human employees?	0.9742	0.9545	0.9939	0.6587	0.3717	0.8307	4.963	4.890	5.036	0.03704	0.02297	0.06956	0.1925	0.1516	0.2637
Q5. The ACERBOTICS Framework addresses real and pressing challenges in the Robotics Service Industry (RSI).	0.9718	0.9505	0.9932	0.8777	0.7468	0.9432	4.407	4.167	4.647	0.4046	0.2509	0.7598	0.6360	0.5009	0.8717
Q6. The framework adequately integrates multiple disciplinary perspectives (e.g., ethics, cybersecurity, HRI).	0.9719	0.9507	0.9932	0.8215	0.6418	0.9157	3.926	3.613	4.238	0.6866	0.4258	1.290	0.8286	0.6526	1.136
Q7. The framework’s structure, components, and interrelationships are clearly articulated and easy to understand.	0.9725	0.9518	0.9933	0.7416	0.5035	0.8750	4.037	3.751	4.323	0.5755	0.3569	1.081	0.7586	0.5974	1.040
Q8. The visual representation and accompanying explanation adequately communicate the framework’s purpose and scope.	0.9733	0.9533	0.9933	0.6263	0.3233	0.8129	4.222	4.004	4.440	0.3333	0.2067	0.6260	0.5774	0.4547	0.7912
Q9. The framework can be practically applied in real-world service domains such as healthcare, hospitality, or logistics.	0.9731	0.9529	0.9933	0.6611	0.3755	0.8321	4.000	3.766	4.234	0.3846	0.2385	0.7223	0.6202	0.4884	0.8499
Q10. The framework is adaptable to different organisational contexts within the service industry.	0.9728	0.9522	0.9934	0.7074	0.4477	0.8570	4.074	3.780	4.369	0.6097	0.3781	1.145	0.7808	0.6149	1.070
Q11. The framework contributes significantly to the field of ethical and cybersecure robotics.	0.9729	0.9526	0.9932	0.7047	0.4435	0.8556	4.000	3.653	4.347	0.8462	0.5248	1.589	0.9199	0.7244	1.261

Q12. There are no major omissions in the framework that could hinder its implementation or validity.	0.9728	0.9529	0.9928	0.7067	0.4466	0.8566	3.889	3.647	4.130	0.4103	0.2544	0.7705	0.6405	0.5044	0.8778
Q13. I would recommend the use of this framework for future projects in service robotics.	0.9722	0.9515	0.9929	0.7893	0.5847	0.8995	4.074	3.799	4.349	0.5328	0.3304	1.001	0.7299	0.5748	1.000
Q14. Ethical considerations such as fairness, transparency, and accountability are well-integrated within the framework.	0.9728	0.9525	0.9930	0.7098	0.4516	0.8583	3.963	3.658	4.268	0.6524	0.4046	1.225	0.8077	0.6361	1.107
Q15. The framework provides a clear pathway for ensuring responsible and human-centred robotic deployment.	0.9724	0.9518	0.9929	0.7639	0.5409	0.8865	4.148	3.858	4.439	0.5926	0.3675	1.113	0.7698	0.6062	1.055
Q16. The framework adequately addresses data protection	0.9716	0.9501	0.9931	0.8641	0.7207	0.9366	3.852	3.479	4.225	0.9772	0.6060	1.835	0.9885	0.7785	1.355
Q17. The framework adequately addresses threat resilience.	0.9726	0.9528	0.9925	0.7244	0.4752	0.8660	3.926	3.631	4.220	0.6097	0.3781	1.145	0.7808	0.6149	1.070
Q18. The framework adequately addresses system integrity.	0.9727	0.9520	0.9934	0.7204	0.4687	0.8639	4.185	3.928	4.442	0.4644	0.2880	0.8722	0.6815	0.5367	0.9339
Q19. The cybersecurity dimension aligns with ethical and operational requirements for safe robotic deployment.	0.9719	0.9506	0.9931	0.8286	0.6548	0.9192	4.185	3.871	4.500	0.6952	0.4311	1.306	0.8338	0.6566	1.143
Q20. The framework sufficiently considers human values.	0.9722	0.9518	0.9926	0.7881	0.5826	0.8989	3.889	3.569	4.208	0.7179	0.4453	1.348	0.8473	0.6673	1.161
Q21. The framework sufficiently considers cultural diversity.	0.9724	0.9517	0.9930	0.7761	0.5617	0.8928	4.000	3.638	4.362	0.9231	0.5725	1.734	0.9608	0.7566	1.317
Q22. The framework sufficiently considers industry-specific needs.	0.9722	0.9515	0.9929	0.7907	0.5871	0.9002	4.037	3.751	4.323	0.5755	0.3569	1.081	0.7586	0.5974	1.040
Q23. The socio-technical aspects are effectively integrated to enhance collaboration between humans and robots.	0.9726	0.9521	0.9931	0.7337	0.4904	0.8709	4.111	3.809	4.413	0.6410	0.3976	1.204	0.8006	0.6305	1.097
Q24. The framework is feasible for adoption by practitioners and policymakers in the service robotics field.	0.9712	0.9493	0.9931	0.9074	0.8049	0.9573	3.889	3.521	4.256	0.9487	0.5884	1.782	0.9740	0.7671	1.335

Q25. The implementation pathway described is realistic and scalable.	0.9715	0.9499	0.9931	0.8748	0.7412	0.9417	4.074	3.698	4.450	0.9943	0.6166	1.867	0.9971	0.7853	1.367
Q26. The framework’s components form a cohesive and logically structured model.	0.9721	0.9512	0.9930	0.8024	0.6076	0.9061	3.963	3.658	4.268	0.6524	0.4046	1.225	0.8077	0.6361	1.107
Q27. The framework holistically addresses critical aspects such as ethics, cybersecurity, socio-technical systems, and cultural context.	0.9719	0.9509	0.9929	0.8329	0.6626	0.9213	4.000	3.638	4.362	0.9231	0.5725	1.734	0.9608	0.7566	1.317
Q28. The framework would be useful for guiding the ethical design, governance, and deployment of service robotics.	0.9718	0.9509	0.9926	0.8419	0.6791	0.9257	4.185	3.854	4.517	0.7721	0.4788	1.450	0.8787	0.6920	1.204