sustainability

MDPI

Article

Systems Thinking for Sustainable Early-Stage Design of Autonomous Residential Robotic Systems: A Safety-by-Design Framework Evaluated Through an Automated Window-Cleaning Robot

Maria-Alexandra Mielcioiu [1], Mihnea Cosmin Costoiu [2], Augustin Semenescu [3,4], Petruța Petcu [5,*], Dumitru Nedelcu [3,6,7], Elena-Cristina Udrea [1], Alexandru-Dorian Făină [1], Ana-Maria Nicolau [5] and Narcisa Valter [5]

[1] Doctoral School of Industrial Engineering and Robotics, Doctoral Field—Industrial Engineering, National University of Science and Technology Politehnica Bucharest, 060042 Bucharest, Romania; maria.mielcioiu@stud.aero.upb.ro (M.-A.M.); elena.faina@upb.ro (E.-C.U.); alexandru.faina@upb.ro (A.-D.F.)
[2] Faculty of Industrial Engineering and Robotics, National University of Science and Technology Politehnica Bucharest, 313 Independentei Street, 060042 Bucharest, Romania; mihnea.costoiu@upb.ro
[3] Academy of Romanian Scientists, Ilfov Street 3, 050044 Bucharest, Romania; augustin.semenescu@upb.ro (A.S.); dumitru.nedelcu@academic.tuiasi.ro (D.N.)
[4] Faculty of Materials Science and Engineering, National University of Science and Technology Politehnica Bucharest, 060042 Bucharest, Romania
[5] Faculty of Aerospace Engineering, National University of Science and Technology Politehnica Bucharest, 060042 Bucharest, Romania; ana.avramescu@upb.ro (A.-M.N.); narcisa.valter@upb.ro (N.V.)
[6] Faculty of Machine Manufacturing and Industrial Management, "Gheorghe Asachi" Technical University of Iasi, 700050 Iaşi, Romania
[7] Technical Sciences Academy of Romania, Blvd. Dacia 26, 030167 Bucharest, Romania
* Correspondence: petruta.toderasc@upb.ro

Abstract

Autonomous robotic systems operating in residential environments must maintain safe, reliable, and adaptive performance under heterogeneous conditions characterized by environmental uncertainty. Achieving this performance is difficult because such systems must simultaneously cope with variable contact states and complex subsystem interactions. Conventional component-oriented engineering approaches often fail to capture how internal faults, external disturbances, and architectural decisions interact to generate system-level instabilities and hazards. This paper proposes a Systems Thinking-based Safety-by-Design framework to support the sustainable early-stage design of autonomous residential robotic systems. The methodology formalizes the relationships among internal faults (F), environmental variability (E), system behaviour (S), architecture (A), instabilities (I), hazards (H), and safety barriers (B) through the dependencies S = f(F,E), I = g(S,A), and H = h(I,B). Environmental variability is treated as an active design driver influencing system behaviour, architectural decisions, and safety requirements. The framework is evaluated as a proof-of-concept, semi-quantitative analytical demonstration, rather than an experimentally validated result, using an autonomous window-cleaning robot: its functional subsystems are mapped to the conceptual model and fault-dominated, environment-dominated, and coupled degradation scenarios are assessed through a semi-quantitative index. The results show that risk emerges from subsystem interactions rather than isolated component failures and that adaptive architectures reduce instability propagation under uncertain operating conditions. The proposed framework supports early engineering decisions that improve robustness, resilience, safety, maintainability, and sustainability.

Check for updates

Academic Editors: In-Ju Kim and Anna Mazzi

Received: 21 July 2026
Revised: 21 August 2026
Accepted: 23 August 2026
Published: 25 August 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

Keywords: systems thinking; sustainable engineering; safety-by-design; autonomous robotic systems; early-stage design; environmental variability; resilient systems; system architecture; hazard assessment; residential robotics

1. Introduction

Autonomous residential robotic systems execute maintenance, inspection, cleaning, and monitoring tasks under high operational autonomy. Integration within smart home ecosystems transforms residential spaces into interconnected cyber–physical architectures, optimization networks for energy efficiency, and resource management frameworks [1,2]. Modern residential automation evolves from independent components toward distributed ecosystems capable of multi-sensor fusion, centralized decision-making, and coordinated autonomous operation [3], optimizing operational safety and overall environmental performance [4]. Consequently, these safety-critical systems must guarantee functional performance, reliability, and long-term robustness throughout their entire product life cycle.

Unlike industrial platforms operating in structured environments, residential robots must adapt to dynamic operating conditions. While recent developments in wall-climbing and window-cleaning systems validate the viability of autonomous locomotion, maintaining reliable adhesion, compensating for environmental disturbances, and ensuring operational safety remain fundamental design challenges [5,6]. Reconfigurable mechanical architectures are required to maintain kinematically stable locomotion across varying structural boundaries [7]. Furthermore, residential robots interface with communication networks and building management systems to support automated asset management [8]. Therefore, overall operational reliability emerges from system-level interactions rather than the isolated reliability of individual hardware components.

These challenges require sustainable engineering frameworks where the performance of autonomous robotic configurations emerges from multi-domain interactions between technical subsystems rather than isolated component dynamics [9]. The operational performance of these platforms depends simultaneously on the internal system architecture and the environmental, operational, and infrastructural boundary conditions [10]. Because autonomous robotic systems constitute complex cyber–physical architectures governed by continuous hardware-software-environment interactions, system-level analysis is mandatory; isolated component testing cannot validate or guarantee safe system-level states [11]. Furthermore, safety parameters must be embedded into the initial design stages via systematic risk assessment matrix methodologies rather than retrofitted during final validation phases [12]. Incorporating structural robustness and environmental adaptability during conceptual design directly enhances safety, reliability, maintainability, and life-cycle efficiency.

The scaling complexity of autonomous systems highlights the limitations of traditional component-oriented engineering, which fails to map how Internal Faults (F), environmental disturbances, architectural variants, control loops, and user inputs propagate failure modes through the system. Systems Thinking (ST) mitigates this by analyzing engineering systems strictly within their complete operational contexts [11]. Under this paradigm, System Behaviour (S) is defined as an emergent property of the coupled interactions between physical components, system architecture, operational bounds, and user inputs [10], while system architecture plays a central role in resilience by influencing how degradation propagates across subsystem interactions [9]. Testing alone is insufficient; robotic autonomous systems require integrated validation and verification throughout the development lifecycle [13], whereas hazardous states typically stem from subsystem interface failures rather than

single component faults [14]. Safety is thus defined as the system's capacity to maintain controlled operational states despite structural degradation and input uncertainty.

System resilience is the capacity to maintain target functional parameters under internal degradation and external disturbances. Resilience is an emergent property arising from the coupled dynamics between system architecture, environmental variability, and operational constraints. Theoretical performance computed during early design phases deviates from real-world behavior if these boundary interactions are unmodeled [10]. To eliminate this variance, hazard analysis and risk assessment must be initiated during the conceptual design phase of the autonomous system [15]. Early engineering trade-offs directly dictate life-cycle robustness, maintainability, and resource optimization [10]. Consequently, safety assurance must be integrated into the core engineering workflow from the initial concept phase rather than treated as a post-design certification requirement [16]. Resilience must be engineered systematically via model-based design, continuous monitoring, and life-cycle learning loops, transforming Safety-by-Design (SbD) into an intrinsic architectural characteristic.

Current autonomous cleaning robots prioritize trajectory planning and coverage efficiency [17]. Conventional design methods isolate component reliability, environmental adaptation, and safety analysis, limiting the capability to evaluate how architecture, control loops, and human factors collectively govern system states during conceptual design [10,14]. Safe deployment requires embedding active safety mechanisms directly into the control architecture rather than applying safety as a superficial wrapper [18]. An integrated engineering framework is therefore necessary to formally map the causal relationships between F, Environmental Variability (E), S, System Architecture (A), Instabilities (I), Hazards (H), and Safety Barriers (B) within a unified methodology.

Several systems-level hazard-analysis methods already address the limitations of purely component-based reliability engineering, including System-Theoretic Process Analysis (STPA) [19], the Functional Resonance Analysis Method (FRAM) [20], and long-established techniques such as Hazard and Operability Analysis (HAZOP) and Failure Mode and Effects Analysis (FMEA). These methods provide valuable qualitative or semi-formal representations of hazard generation but, as summarised in Table 1, none of them formalises environmental variability as an independent, quantifiable design driver acting jointly with internal faults through an explicit interaction term, and none provides a lightweight numerical index suitable for comparing candidate architectures before a detailed control structure or component list exists.

Table 1. Positioning of the proposed ST-based Safety-by-Design (SbD) framework relative to established systems-level hazard-analysis methods.

Method	Core Focus	Treatment of Environmental Variability (E)	Typical Stage of Application
STPA	Inadequate control actions within a hierarchical control structure	Environment is a contextual factor in the control structure, not an independently quantified variable	Requires a defined control structure; typically mid-to-late conceptual/ detailed design
FRAM	Performance variability arising from the resonance of everyday functions	Environment influences functions qualitatively; no explicit quantitative coupling with internal faults	Requires defined functional model; mid-to-late design or operational analysis

Table 1. *Cont.*

Method	Core Focus	Treatment of Environmental Variability (E)	Typical Stage of Application
HAZOP/FMEA	Deviations from design intent/component-level failure modes and effects	Environment is usually one of several deviation guide-words or failure causes, not a modelled driver	Requires a defined component/process list; detailed design stage
Proposed ST-based SbD framework	Joint propagation of internal faults (F) and environmental variability (E) through architecture (A) into instabilities (I) and hazards (H)	E is an explicit, quantifiable design driver coupled with F through an interaction term (Equation (5))	Early conceptual design, before a detailed control structure or component list exists

Source: authors' own creation.

The specific gap addressed by the present work is therefore the early, pre-architectural quantification of the combined effect of F and E on system instability. The proposed ST-based SbD framework is positioned as a complementary, lightweight analytical layer intended to inform and precede, rather than replace, a subsequent STPA-, HAZOP-, or FMEA-type analysis once the architecture is sufficiently defined.

The proposed framework is also complementary to prescriptive safety standards commonly applied to robotic and machinery systems, including ISO 12100 [21] (general principles of machinery risk assessment and reduction), ISO 13482 [22] (safety requirements for personal care robots), IEC 61508 [23] (functional safety of electrical/electronic/programmable safety-related systems), and ISO 13849 [24] (safety-related parts of control systems). These standards provide normative requirements, safety-integrity levels, and verification procedures for systems whose architecture and safety functions are already largely defined; they do not, however, provide a lightweight mechanism for exploring how environmental variability and internal faults jointly shape architectural robustness before that architecture exists. The F-E-S-A-I-H-B formalism is intended to occupy this earlier, pre-normative stage of design, generating comparative evidence that can subsequently be carried into a standards-compliant safety-assurance process.

This study introduces an ST-based SbD framework for the early-stage engineering design of autonomous residential robots, integrating the interactions of F, E, S, A, I, H, and B into a conceptual model to guide design decisions before fixed parameters lock the architecture. This framework uses risk assessments that simultaneously evaluate hardware, control laws, and environmental boundaries by balancing technical, operational, and environmental vectors [12]. This architecture requires safety assessment frameworks that synthesize hazards, risk indices, and structural topologies [12], supported by verification loops that solve for safety, reliability, and system behavior concurrently [11]. Finally, validating deterministic behavior under dynamic conditions requires formal verification recipes, such as model checking or runtime verification, to mathematically evaluate the system's state space [25].

The contributions of this work are: (i) an engineering framework mapping the causal interactions between F, E, S, A, I, H, and B; (ii) the integration of *E* as an active design driver shaping the architecture rather than a passive operational boundary; and (iii) validation via an autonomous window-cleaning robot case study, demonstrating early-stage optimization of resilience, maintainability, and safety [26,27]. The functional boundaries of this research are defined relative to the platform's development history: the physical mechatronic architecture, kinematics, and low-level control loops were validated from a hardware perspective in our previous work [8]. Here, the physical platform serves exclusively as an empirical

baseline to test this uncoupled systemic paradigm. The scientific contribution lies in the formulation and mathematical structure of the ST-SbD framework. This paper bypasses isolated component tuning to model emergent behaviors, abstract multi-domain degradation functions (f_{deg}), and cascading socio-technical architectural risks that govern system resilience prior to implementation [28,29].

These contributions are guided by four explicit research questions. RQ1: Can internal faults (F) and environmental variability (E) be formalised within a single early-stage conceptual framework, together with architecture (A), instabilities (I), hazards (H), and safety barriers (B)? RQ2: Does environmental variability act as an independent driver of behavioural degradation even in the absence of internal faults? RQ3: Does architectural robustness measurably influence the propagation of instability under otherwise identical fault and environmental conditions? RQ4: Can these relationships be demonstrated on a real engineering case study using a semi-quantitative, reproducible assessment? Section 3 addresses RQ1 and RQ4 through the mapping of the physical platform onto the conceptual framework (Section 3.2) and the scenario-based assessment (Section 3.3); RQ2 is addressed by the environment-dominated scenario (Section 3.3.2); and RQ3 is addressed by the comparison between rigid and adaptive architectural configurations across all three scenarios (Section 3.4).

2. Materials and Methods

The proposed methodology was developed to support the sustainable early-stage engineering design of autonomous residential robotic systems operating under heterogeneous environmental conditions. During conceptual design, architecture, operational safety, environmental adaptability, and functional robustness are strongly interdependent, making their separate evaluation insufficient for understanding overall system behaviour (S). Accordingly, the proposed approach adopts an ST perspective in which these characteristics are analysed as interacting elements of an integrated engineering system.

From this perspective, internal faults (F), environmental variability (E), architectural characteristics, and safety mechanisms are considered simultaneously throughout conceptual development. Their interactions govern degradation propagation, the formation of instabilities (I), and the effectiveness of safety measures, enabling SbD principles to influence architectural decisions before detailed engineering solutions become fixed. Consequently, the proposed methodology supports the development of robotic systems with improved robustness, resilience, maintainability, and long-term sustainability.

The methodology integrates system definition, conceptual modelling, representative degradation scenarios, and semi-quantitative assessment into a unified analytical framework. The conceptual relationships underlying the proposed methodology are illustrated in Figure 1.

Figure 1 presents the relationships among F, E, S, architecture (A), I, hazards (H), and safety barriers (B). Beyond the primary causal chain, E also acts on A and B directly, since environmental conditions influence which architectural configurations and safety barriers remain effective, and a continuous monitoring and feedback pathway links the evolution of H back into the architecture, consistent with the adaptive engineering decisions discussed in Section 2.1. These interactions provide the conceptual basis for the representative degradation scenarios and the semi-quantitative assessment presented in the following sections.

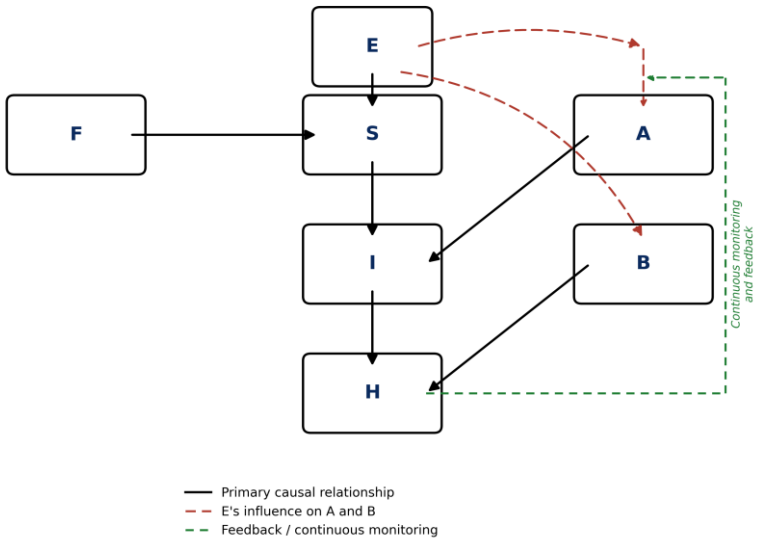


Figure 1. Conceptual ST-based SbD framework. Solid arrows denote the primary causal chain (F, E → S → I → H); dashed red arrows denote the additional influence of E on A and B; the dashed green loop denotes the continuous monitoring and feedback pathway from H back into the architecture (A). Source: authors' own creation.

2.1. Research Design and Methodological Workflow

The proposed research design follows a systems engineering approach in which the overall system behaviour (S) of an autonomous residential robotic system is analysed through the interactions among internal faults (F), environmental variability (E), architecture (A), and safety barriers (B). Rather than evaluating these elements independently, the methodology examines their combined influence on degradation propagation, the development of instabilities (I), and the generation of hazards (H), recognising that stable system behaviour depends on effective feedback mechanisms capable of compensating for disturbances and degradation processes [15]. This perspective provides the basis for integrating Safety-by-Design (SbD) principles during conceptual development, where architectural decisions have the greatest influence on subsequent system behaviour (S).

The workflow begins with the definition of the engineering system and its operational boundaries by identifying the principal functional subsystems and their interfaces with the surrounding environment. Defining these boundaries establishes a consistent reference model for analysing the mechanisms governing overall S rather than isolated component performance.

Next, the ST framework is established by introducing the variables representing internal faults (F), environmental variability (E), system behaviour (S), architecture (A), instabilities (I), hazards (H), and safety barriers (B). Their causal relationships define the analytical structure used to describe degradation propagation from its origin to its potential impact on operational safety.

Representative degradation scenarios are then formulated to investigate three operating conditions: degradation dominated by F, degradation dominated by E, and degradation resulting from their combined interaction. This classification provides a consistent basis for comparing different operating conditions under identical methodological assumptions.

Each scenario is evaluated using a semi-quantitative assessment based on measurable indicators that compare degradation propagation, the influence of A on I development, and H criticality [30]. Rather than predicting the exact S of a particular robotic platform, the assessment supports the comparative evaluation of alternative architectural solutions during conceptual design.

Finally, the results are interpreted within the SbD framework to evaluate how architectural decisions influence robustness, resilience, maintainability, service life, and adaptation to E. Continuous monitoring supported by measurable indicators and feedback mechanisms provides the information required for adaptive engineering decisions throughout system operation [15,30,31], thereby supporting sustainability-oriented engineering decisions for autonomous residential robotic systems.

The overall methodological workflow, including the continuous monitoring and feedback loop that links the interpretation of results back into the ST framework, is summarized in Figure 2.

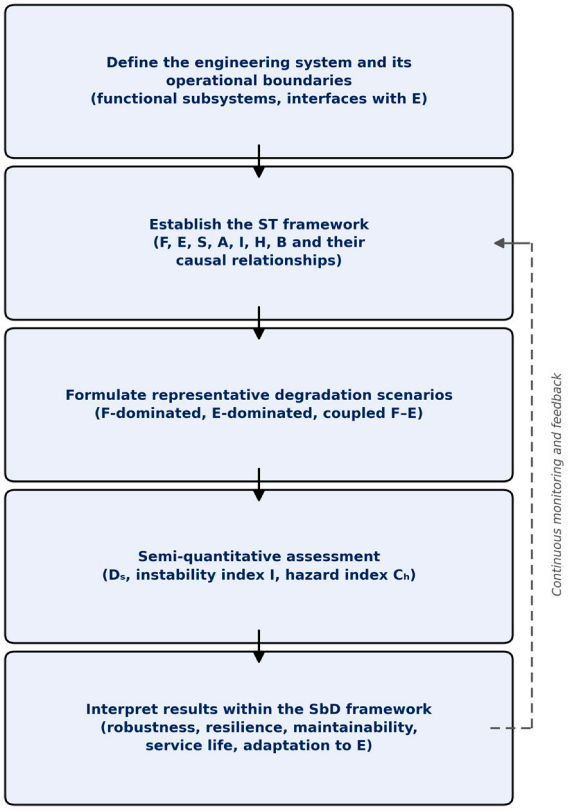


Figure 2. Methodological workflow of the proposed ST-based SbD framework, from system definition to the interpretation of results, including the continuous monitoring and feedback loop. Source: authors' own creation.

2.2. ST-Based Conceptual Framework

The proposed ST framework provides the analytical foundation for describing degradation propagation in autonomous residential robotic systems. Instead of analysing F, E, A, and B independently, the framework considers their interactions to explain how degradation evolves and ultimately influences operational safety. This systems perspective is consistent with intelligent engineering approaches recognising that the effectiveness of autonomous systems depends on integrating sensing, communication, and decision-making processes rather than evaluating individual technologies in isolation [32].

The framework is structured around seven variables (F, E, S, A, I, H, and B) that represent the principal elements governing degradation propagation. Their engineering definition and corresponding roles are summarized in Table 2.

Table 2. Definition and engineering role of the variables used in the proposed ST framework.

Variable	Meaning	Role in the Model
F	Set of internal faults (hardware, software, sensors, actuators)	Internal source of degradation
E	Operational environment variability	External source of disturbances
S	Global system state/behavior	Aggregated operational response
A	System architecture	Mode of effect propagation or damping
I	Instabilities and intermediate effects	Indicator of dynamic degradation
H	Hazards	Dangerous consequences at system/user level
B	Safety barriers	Mechanisms for prevention, detection, and mitigation

Source: authors' own creation.

Although the variables F, E, S, A, I, H, and B recur throughout Section 2, each subsequent table serves a distinct analytical purpose rather than repeating the same information: Table 2 defines the variables themselves, Table 3 (Section 2.4) characterises how they combine within each representative degradation scenario, Table 4 (Section 2.5) summarises the ordinal scales used for severity (Sev), occurrence (Occ), and exposure (Exp) in Equation (7). Table 5 (Section 3.2) then maps these variables onto the physical subsystems of the case-study platform. This progression was retained deliberately to preserve traceability from the abstract conceptual model to the concrete engineering system; the accompanying narrative has been shortened in this revision to reduce repeated explanation of the same variable set.

Table 3. Representative degradation scenarios used for the semi-quantitative assessment.

Scenario	Formal Condition	Dominant Mechanism	Effect on S	Role of A	Effect on I	Design Implication
Scenario 1 Dominant internal fault	$F \neq \emptyset, E \approx 0$	Local subsystem fault	Degradation is induced mainly by F	A may limit fault propagation	I depends on the ability of A to isolate or damp the fault	Need for redundancy and robust control
Scenario 2 Dominant environmental variability	$F = 0, E \gg 0$	Significant external disturbances	S may degrade even without F	A becomes a critical factor for absorbing environmental variations	Weak A $\rightarrow$ I $\uparrow$; Robust A $\rightarrow$ I $\downarrow$	E must be treated as an architectural design driver
Scenario 3 Combined effect	$F \neq \emptyset, E > 0$	F–E interaction	Amplified degradation with an emergent character	A determines whether effects are amplified or attenuated	Rigid A $\rightarrow$ I $\uparrow\uparrow$; Adaptive A $\rightarrow$ I $\downarrow\downarrow$	Need for modular and adaptive architecture in heterogeneous environments

Source: authors' own creation. $\uparrow$ denotes an increase, $\downarrow$ denotes a decrease, and $\uparrow\uparrow/\downarrow\downarrow$ denote a stronger increase/decrease, respectively.

Table 4. Illustrative 1–5 ordinal scale used for severity (Sev), occurrence (Occ), and exposure (Exp) in the hazard criticality index (Equation (7)). Only the anchor scores (1, 3, 5) are shown; intermediate scores (2, 4) represent intermediate conditions.

Score	Descriptor	Illustrative Criterion
1	Negligible	No injury; cosmetic or negligible property damage
3	Moderate	Minor injury or moderate localized damage requiring repair
5	Severe	Serious injury or major damage/fall of the assembly

Table 4. *Cont.*

Score	Descriptor	Illustrative Criterion
1	Rare	Not expected to occur during normal service life
3	Occasional	May occur a few times during normal service life
5	Frequent	Expected to occur repeatedly under normal operating conditions
1	Low	Robot operates while occupants are typically absent
3	Moderate	Occupants occasionally present in the operating area
5	High	Occupants frequently present near the operating robot

Source: authors' own creation.

Table 5. Functional subsystems and associated ST variables.

Functional Subsystem	Primary Engineering Function	Associated ST Variable(s)	Engineering Interpretation
LINAK LA23 linear actuator	Vertical movement of the cleaning assembly	F, S	Stroke deviations, motion delays, or actuator blockage directly influence the dynamic behaviour of the cleaning system.
MGN12 linear guide	Guidance and stabilization of the cleaning assembly	F, A	Mechanical play, increased friction, or guide blockage reduce positioning accuracy and affect structural robustness.
DC775 motor with PLG42 planetary gearbox	Brush drive system	F, S	Torque loss, speed fluctuations, or transmission faults reduce cleaning efficiency and affect dynamic performance.
Rotating brush assembly	Mechanical cleaning of the glazed surface	S	Represents the primary functional output responsible for contaminant removal.
Peristaltic pump	Controlled delivery of the cleaning solution	F, S	Overdosing or insufficient fluid delivery reduces cleaning effectiveness and alters operating conditions.
Vacuum pump	Recovery of residual cleaning liquid	F, I	Insufficient suction may leave residual liquid on the surface, increasing instability and the risk of slipping.
ESP32 DevKitC	System coordination, control, and communication	A	Central control unit coordinating subsystem interaction and autonomous operation.
L298N/A4988 motor drivers	Electrical interface for actuator control	A, F	Driver performance influences control quality and may introduce command or actuation faults.
Limit switches	Motion limiting and end-position protection	B, F	Provide protective functions while remaining potential fault sources if malfunction occurs.
Liquid-level sensor	Monitoring of cleaning-fluid availability	B, F	Detects abnormal fluid conditions and prevents unsafe operation caused by insufficient cleaning solution.
Mobile user interface	Command, monitoring, and operator intervention	A, B	Enables supervisory control and human intervention as an additional safety barrier.
Glazed surface and window frame	Physical operating environment	E	Surface geometry, material properties, and surface condition directly influence system performance.
Wind, humidity, temperature, and dust	Environmental disturbances	E	Represent the principal sources of environmental variability affecting robot operation.
Trajectory deviations, vibration, and adhesion loss	Intermediate degradation effects	I	Represent the dynamic manifestation of degradation propagating through the system.

Table 5. *Cont.*

Functional Subsystem	Primary Engineering Function	Associated ST Variable(s)	Engineering Interpretation
Fall, collision, and surface damage	Hazardous outcomes	H	Represent the final hazardous states affecting both the robotic system and the surrounding environment.
Automatic stop, sensor redundancy, and software limits	Integrated protective measures	B	Implement safety barriers that interrupt degradation propagation and reduce hazard occurrence.

Source: authors' own creation.

The interactions among these variables are formalized through three functional relationships. Accordingly, the proposed framework represents system behaviour as the result of interacting engineering functions, consistent with integrated approaches combining sensing, communication, control, and decision-support processes to capture autonomous system behaviour more realistically than analysing each function independently [28].

S is represented as a function of F and E,

$$S = f(F, E), \tag{1}$$

showing that operational performance continuously evolves under the combined influence of internal degradation and external operating conditions. The resulting S subsequently interacts with the adopted A to determine the development of I,

$$I = g(S, A), \tag{2}$$

where the architectural configuration, including the communication pathways linking functional subsystems, influences whether degradation is attenuated, redistributed, or amplified during propagation. Reliable communication infrastructures are essential for autonomous residential robotic systems operating within smart home environments [33].

H generation is then expressed as

$$H = h(I, B), \tag{3}$$

indicating that hazardous conditions depend on both the evolution of I and the effectiveness of the implemented B.

From a systems engineering perspective, Equations (1)–(3) are conceptual mapping operators rather than closed-form algebraic functions: they establish the functional dependencies and non-linear causal structures governing degradation propagation across the system architecture, without representing classical deterministic or differential relationships. In complex multi-domain cyber–physical systems, a direct deterministic formulation of f, g, and h is analytically intractable due to the qualitative nature of architectural decisions and socio-technical safety barriers. Therefore, these mapping relationships serve as the mathematical foundation for subsequent semi-quantitative and probabilistic operationalization. Specifically, the abstract behavioral function $f(F, E)$ maps the joint spaces of internal fault states and external environmental stressors onto a unified system degradation continuum. To bridge the gap between this high-level functional mapping and an evaluable engineering assessment, the abstract operator $f(F, E)$ is operationalized in Section 2.5 through a polynomial interaction model (Equation (5)). This parameterization explicitly transforms the qualitative coupling of internal mechanics and external forces into a measurable semi-quantitative degradation index (D_S).

A distinguishing feature of the proposed ST-based SbD framework is the explicit incorporation of E into the analytical model. Rather than being treated as a fixed operating condition, E actively influences S, degradation propagation, A, and the effectiveness of safety measures. This formulation provides the basis for the representative degradation scenarios and the semi-quantitative assessment presented in the following sections. Furthermore, the proposed framework can support digital engineering decision-support tools for comparing alternative conceptual solutions under multiple operating scenarios [34]. Such analytical tools are intended to complement engineering expertise by supporting the systematic evaluation of complex interactions during conceptual design rather than replacing engineering judgement [35].

2.3. Environmental Variability as an Engineering Design Driver

Conventional engineering methodologies generally treat E as an external operating condition used to verify performance under predefined scenarios. Within this perspective, environmental factors define the operating context, whereas A and safety functions are developed independently and subsequently validated against expected conditions. Although this approach supports performance evaluation under nominal operating conditions, it provides limited capability for analysing how continuously changing environments interact with degradation mechanisms and influence overall S.

For autonomous residential robotic systems, E represents a fundamentally different engineering challenge. Residential environments are inherently heterogeneous, exposing robotic platforms to changing surface characteristics, contamination, moisture, wind disturbances, geometric discontinuities, illumination conditions, and human interactions. These factors directly influence adhesion, locomotion, sensing, control performance, energy consumption, and safety functions. Consequently, degradation cannot be attributed exclusively to F because environmental conditions actively initiate, propagate, and amplify degradation throughout operation.

Within the proposed ST framework, E is incorporated as an active engineering variable interacting continuously with F. This relationship is represented conceptually as

$$(F \cup E) \rightarrow S \rightarrow I \rightarrow H, \tag{4}$$

where F and E jointly determine S, whose evolution may generate I that subsequently lead to H whenever the implemented B are unable to interrupt degradation propagation. Unlike conventional reliability-oriented approaches, this representation explicitly recognizes that H may arise not only from component failures but also from the interaction between the engineering system and its operating environment.

E influences S through two complementary mechanisms. First, it modifies the operating conditions experienced by individual subsystems, directly affecting their functional performance. Second, it alters subsystem interactions, changing the pathways through which degradation propagates across the A. Consequently, identical environmental disturbances may either be attenuated or amplified depending on the robustness of the adopted A, influencing not only operational performance but also resilience, maintainability, and overall safety.

Treating E as an engineering design driver fundamentally changes its role during conceptual development. Instead of being introduced only during verification, environmental uncertainty becomes an explicit design parameter influencing architectural decisions from the earliest stages of development. Subsystem configuration, sensing redundancy, control strategies, adhesion mechanisms, energy management, and B can therefore be evaluated according to their capability to maintain stable operation under heterogeneous conditions. Incorporating E into conceptual design consequently supports engineering decisions that

improve robustness, facilitate maintainability, extend service life, and contribute to the long-term sustainability of autonomous residential robotic systems.

This systems-level interpretation provides the basis for the representative degradation scenarios presented in the following section, where the individual and combined effects of F and E are analysed under consistent engineering assumptions.

2.4. Definition of Representative Degradation Scenarios

To evaluate the proposed ST framework under representative operating conditions, three degradation scenarios were defined to capture the principal mechanisms governing the evolution of S in autonomous residential robotic systems. The scenarios distinguish the influence of F, E, and their combined interaction, thereby providing a consistent basis for analysing degradation propagation under progressively increasing levels of system complexity. The characteristics of the representative degradation scenarios are summarized in Table 3.

The first scenario represents fault-dominated degradation, in which degradation originates primarily from F while the influence of E remains limited. Under these conditions, the evolution of S is governed predominantly by internal degradation mechanisms. This scenario reflects situations where failures affecting mechanical, electrical, sensing, or control subsystems constitute the principal source of I, allowing the intrinsic robustness of the proposed A to be evaluated independently of significant external disturbances. From an engineering perspective, this scenario supports the identification of architectural solutions capable of improving fault containment, maintainability, and service life through enhanced tolerance to internal degradation.

In this scenario, the dominant hazards (H) are typically trajectory deviation and localized collision, and the most relevant safety barriers (B) are redundant position sensing and control-level limit checks capable of isolating the fault before it propagates into the overall system state (S).

The second scenario represents environment-dominated degradation, where system components remain functionally intact while degradation is induced primarily by E. Environmental disturbances therefore become the dominant factor influencing S. Variations in surface properties, contamination, moisture, wind disturbances, or geometric discontinuities may initiate degradation even in the absence of identifiable component failures, demonstrating that H may arise directly from interaction with the operating environment. From a sustainable engineering perspective, this scenario highlights the importance of incorporating environmental adaptability during conceptual design to improve operational reliability, reduce unnecessary maintenance interventions, and increase long-term resource efficiency.

The dominant hazard (H) in this scenario is loss of adhesion under adverse environmental conditions, and the most relevant safety barriers (B) are adhesion or slip-monitoring sensors combined with an automatic stop function, since these barriers act directly on the environmentally induced degradation rather than on an internal fault.

The third scenario represents coupled degradation, in which F and E occur simultaneously. Both degradation sources contribute to the evolution of S, producing interaction effects that cannot be explained independently. This scenario reflects the operating conditions most frequently encountered in residential applications, where internal degradation and environmental variability continuously reinforce one another, increasing the propagation of I and the likelihood of H. Engineering evaluation under these conditions supports the development of modular and adaptive A capable of maintaining stable operation despite simultaneous internal and external degradation, thereby enhancing resilience, extending operational lifetime, and supporting sustainable system development.

In the coupled scenario, the dominant hazard (H) is critical instability leading to a fall of the assembly, and containing it requires the combined action of multiple safety barriers (B)—sensor redundancy, automatic stop, and software motion limits—since no single barrier is generally sufficient to interrupt propagation once both internal and environmental degradation act simultaneously.

Together, these scenarios provide a common analytical basis for evaluating degradation under progressively more complex operating conditions. Applying the same engineering variables and causal relationships throughout the analysis ensures that the observed differences result exclusively from the dominant degradation mechanisms rather than from changes in the assessment procedure. Accordingly, the proposed scenarios establish the methodological basis for the semi-quantitative assessment presented in the following section.

2.5. Semi-Quantitative Engineering Assessment

The degradation scenarios are evaluated using a semi-quantitative assessment developed to support comparative analysis during conceptual design. Rather than predicting the exact S of a specific robotic platform, the methodology provides a structured basis for evaluating how F, E, and A collectively influence degradation propagation, I development, and H generation. This approach is particularly appropriate during early-stage development, where experimental information is limited while architectural decisions have the greatest impact on subsequent S.

To operationalize the abstract conceptual mapping $S = f(F, E)$ defined in Equation (1) into a calculable metric suitable for early-stage engineering decision-making, the global system behavior is parameterized using a semi-quantitative approach. Under this formulation, the multi-domain degradation function is explicitly resolved into a first-order polynomial expansion that accounts for linear effects and non-linear interaction terms. The overall degradation affecting S is thus expressed by the degradation index (D_S):

$$D_S = w_F D_F + w_E D_E + w_{FE}(D_F D_E), \tag{5}$$

where D_F represents degradation associated with F, D_E the degradation generated by E, and w_F, w_E, and w_{FE} are weighting coefficients defining the relative contribution of each degradation source and their interaction. The coupled term $D_F D_E$ explicitly accounts for the additional effects arising when both degradation sources occur simultaneously, enabling the assessment to capture emergent S that cannot be represented by either mechanism independently. The weighting coefficients (w_F, w_E, and w_{FE}) introduced in the degradation index have a semi-quantitative nature. Their operational calibration is based on a preliminary hazard and operability analysis combined with empirical baseline data obtained from previous experimental testing of the platform's core actuators (DC775 motors) and structural guidance profiles. These weights are further constrained by experimentally observed hardware performance limits, providing a realistic representation of system degradation while reducing arbitrary parameter selection.

For transparency and reproducibility, the specific values adopted in the present assessment are disclosed explicitly (w_F = 0.5, w_E = 0.3, and w_{FE} = 0.4), reflecting the assumption that internal faults have the largest individual influence on behavioural degradation, environmental variability a moderate individual influence, and their interaction a substantial additional contribution consistent with the emergent character discussed in Section 2.3. Similarly, the architectural robustness coefficient R_A is set to 0.6 for the rigid configuration and 0.9 for the adaptive configuration, reflecting a qualitative assessment of subsystem redundancy, feedback capability, and reconfigurability rather than a measured physical property.

This degradation is related to architectural robustness through the instability index

$$I = \frac{D_S}{R_A}, \tag{6}$$

where R_A denotes the architectural robustness coefficient describing the capability of the adopted A to attenuate, redistribute, or amplify degradation during propagation across subsystem interactions. Higher values of R_A indicate architectures capable of maintaining stable operation under variable conditions, whereas lower values correspond to configurations that facilitate I development.

H criticality is evaluated using the hazard index

$$C_H = Sev \times Occ \times Exp, \tag{7}$$

where Sev denotes H severity, Occ the likelihood of occurrence, and Exp the level of exposure. Each parameter is evaluated using a predefined ordinal engineering scale, allowing all degradation scenarios to be compared under a common assessment procedure. The proposed index supports comparative analysis during conceptual design rather than replacing detailed quantitative risk assessment performed during subsequent development stages.

The ordinal scales used for Sev, Occ, and Exp in Equation (7) are summarised in Table 4.

The structure of Equations (5)–(7) follows established engineering practice rather than an arbitrary formulation. The weighted-sum-with-interaction form of Equation (5) is consistent with widely used composite degradation and sustainability indices that combine multiple contributing factors through weighted linear terms plus explicit interaction terms; the normalisation of degradation by an architectural robustness coefficient in Equation (6) follows the same logic as stress-over-capacity ratios used to compare alternative configurations in reliability engineering. Equation (7) reproduces, in structure, the classical Risk Priority Number used in Failure Mode and Effects Analysis (RPN = Severity $\times$ Occurrence $\times$ Detection) [36], with the Detection factor replaced by an Exposure factor to reflect that, for a residential robot operating around building occupants, the controlling parameter is the likelihood of human presence during a hazardous event rather than the likelihood of detecting an internal fault; this substitution mirrors the severity-probability-exposure structure already used in the ISO 12100 [21] risk-estimation model discussed in the Introduction. These parallels are intended to justify the functional form of the indices, not to claim that the specific numerical inputs used in Section 3.3 were empirically measured; as stated above, they remain semi-quantitative engineering estimates.

Together, the degradation, instability, and hazard indices establish a coherent assessment methodology that complements the proposed ST-based SbD framework. Applying the same indicators to all representative scenarios enables consistent comparison of alternative A and supports engineering decisions before detailed system implementation. The methodology is applied to the autonomous residential window-cleaning robot presented in the following section.

3. Results

The proposed ST-based SbD framework was demonstrated through its application to an autonomous residential window-cleaning robot operating under representative residential conditions. The selected platform integrates mechanical, electrical, sensing, control, and safety subsystems whose performance is continuously influenced by environmental variability (E). Its architectural complexity, safety-critical operation, and exposure to heterogeneous operating conditions make it an appropriate engineering case study for eval-

uating degradation propagation, the development of instabilities (I), and the generation of hazards (H).

Following the methodology presented in Section 2, the engineering system is first introduced and subsequently mapped onto the proposed conceptual framework, establishing the correspondence between the physical architecture (A) and the analytical variables governing degradation propagation. The representative degradation scenarios are then evaluated using the semi-quantitative assessment, allowing the influence of internal faults (F), E, and A on system behaviour (S) to be compared under consistent engineering assumptions.

The results demonstrate how the proposed methodology supports early-stage engineering decisions by identifying the mechanisms governing degradation propagation and by evaluating the influence of architectural choices on robustness, resilience, operational safety, and long-term sustainability. The individual stages of the demonstration are presented in the following subsections.

3.1. Engineering System Description

The proposed methodology was applied to an autonomous residential window-cleaning robot designed to operate on vertical glazed surfaces under heterogeneous environmental conditions. The platform was selected because its operation depends on the coordinated interaction of mechanical, electrical, sensing, control, and safety subsystems while continuously adapting to changing operating conditions, making it suitable for demonstrating the proposed engineering approach.

Unlike robotic systems operating in structured industrial environments, residential window-cleaning robots are exposed to continuously changing surface geometries, contamination levels, moisture, frame discontinuities, wind disturbances, and illumination conditions. These factors directly influence adhesion, locomotion, sensing, control performance, energy consumption, and cleaning efficiency. Consequently, operational degradation results from the combined influence of S and E rather than from isolated component failures.

The robotic platform was conceived as a modular mechatronic system that can be implemented either as an integrated solution within the upper window frame or as a retrofit installation on existing glazing systems. This dual configuration preserves the same functional objectives while increasing deployment flexibility. From a sustainability perspective, the retrofit capability extends the service life of existing residential infrastructure, minimizes structural modifications, and promotes more efficient use of engineering resources.

The engineering A comprises functional subsystems responsible for mobility and actuation, structural stabilization and guidance, cleaning with fluid delivery and recovery, sensing, control and communication, power supply, and integrated safety functions. These subsystems continuously exchange information, energy, and mechanical interactions throughout operation, while their performance is simultaneously influenced by E. As a result, degradation propagates across subsystem interfaces, making overall S dependent on the performance of the complete A rather than on individual components.

The overall configuration of the autonomous residential window-cleaning robot is presented in Figure 3, which illustrates the principal functional subsystems and their physical integration.

Figure 3 provides the physical representation of the engineering system analysed throughout the remainder of this study. The interactions established among the mechanical, electrical, sensing, control, and safety subsystems constitute the basis for the subsequent mapping onto the proposed ST framework and for the scenario-based assessment presented in the following sections.

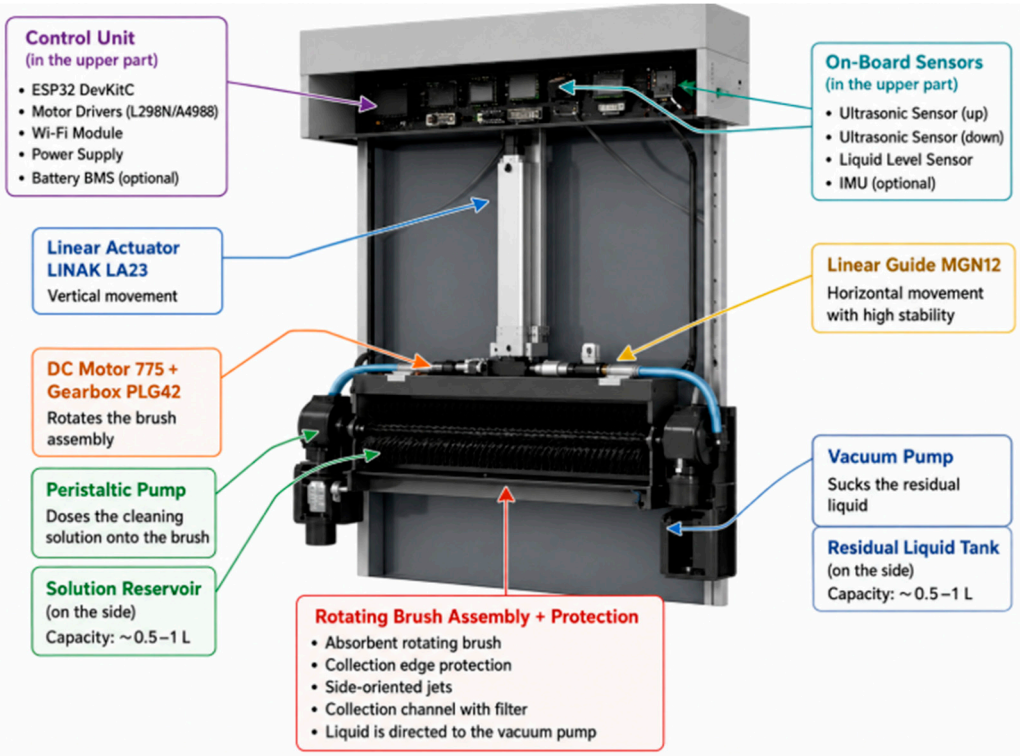


Figure 3. Overall configuration of the autonomous residential window-cleaning robot used as the engineering case study for demonstrating the proposed ST-based SbD framework. Source: authors' own creation.

3.2. Mapping the Physical System onto the ST Framework

The proposed ST-based SbD framework was applied by establishing a systematic correspondence between the physical implementation of the autonomous residential window-cleaning robot and the conceptual variables introduced in Section 2. Rather than analysing individual components in isolation, the objective of this mapping is to identify the engineering contribution of each functional subsystem to the degradation mechanisms governing the overall system. This approach enables the physical architecture to be represented within the proposed conceptual framework and provides the basis for the subsequent scenario-based assessment.

The robotic platform comprises functional subsystems responsible for mobility and actuation, adhesion and stabilization, cleaning and closed-loop fluid management, sensing, control and communication, power supply, and integrated safety. The corresponding hardware implementation includes a LINAK LA23 linear actuator with an MGN12 Linear Guide (MGN12) for controlled vertical displacement, a Direct Current 775 Motor (DC775) coupled with a PLG42 Planetary Gearbox (PLG42) for brush actuation, a peristaltic pump for controlled cleaning-fluid delivery, a vacuum pump for residual liquid recovery within the closed-loop cleaning circuit, an Espressif 32-bit Microcontroller (ESP32) for autonomous coordination, together with limit switches and liquid-level sensors for operational monitoring and protective control.

From a systems engineering perspective, the functional subsystems operate as an integrated mechatronic system whose performance depends on continuous interactions between mechanical, electrical, sensing, control, and safety functions. Consequently, degradation originating within a single subsystem may propagate through subsystem interfaces, altering S, reducing the effectiveness of A, promoting the development of I, and increasing the likelihood of H unless mitigated by the implemented safety barriers (B).

To establish the engineering correspondence between the physical system and the proposed framework, each functional subsystem was associated with one or more conceptual variables according to its dominant contribution to system operation and degradation propagation. Actuation and transmission components primarily contribute to F and S, sensing and monitoring devices support both S and B, the control subsystem governs the operational characteristics of A, while the influence of external operating conditions is represented by E. Because subsystem interactions are inherently coupled, individual components may simultaneously influence multiple conceptual variables throughout the operating cycle.

The engineering correspondence between the functional subsystems, their primary engineering functions, and the associated ST variables is summarized in Table 5.

Table 5 identifies the principal engineering function of each subsystem together with the associated ST variable(s). The proposed mapping does not establish a one-to-one relationship between physical components and conceptual variables; instead, it reflects the interconnected behaviour of the robotic platform, where multiple subsystems collectively influence degradation propagation and system resilience. This engineering representation provides the reference model for the scenario-based assessment presented in the following section.

3.3. Scenario-Based Engineering Assessment

The proposed methodology was applied to the autonomous residential window-cleaning robot using the representative degradation scenarios defined in Section 2.4. The assessment evaluates how F, E, and their combined interaction influence S, the development of I, and the occurrence of H within a common analytical framework. By applying the same engineering variables, causal relationships, and semi-quantitative assessment indicators, the relative contribution of each degradation mechanism can be consistently compared.

Three representative operating conditions were investigated. The first scenario evaluates degradation dominated by F, the second investigates degradation primarily induced by E, and the third examines the simultaneous interaction between both degradation sources. Together, these scenarios represent progressively increasing levels of system complexity and provide a consistent basis for comparative engineering assessment.

The specific D_F and D_E values used in the three scenarios below (Sections 3.3.1–3.3.3) are not drawn from an existing measurement dataset or field trial of the window-cleaning robot. They are hypothetical, representative inputs chosen by the authors to instantiate the qualitative conditions defined in Table 3 (e.g., "dominant internal fault", "dominant environmental variability") at illustrative severity levels, consistent with the semi-quantitative, proof-of-concept nature of the assessment stated in the Abstract and Section 4.3. No claim is made that these particular values are more representative of practical operating conditions than alternative values would be; the purpose of the assessment is to demonstrate how the framework differentiates between architectural configurations under a given set of inputs, not to predict the platform's actual field performance. Grounding these inputs in measured operational data, or in an existing public dataset for a comparable robotic platform, is identified as necessary future work in Section 4.3.

3.3.1. Fault-Dominated Degradation

The first scenario represents operating conditions in which degradation originates predominantly from internal faults (F), while environmental variability (E) remains limited. It reflects situations in which the autonomous residential window-cleaning robot operates under favourable environmental conditions but experiences degradation associated with sensing, actuation, control, power supply, or mechanical transmission. Representative ex-

amples include position-sensor miscalibration, actuator wear, transmission losses, reduced motor torque, and deviations in the control algorithm.

The scenario was evaluated using the semi-quantitative assessment presented in Section 2.5 by considering $D_F = 0.6$ and $D_E = 0.1$, resulting in a degradation index of $D_S = 0.354$. The corresponding instability index reached $I = 0.590$ for the rigid architectural configuration and decreased to $I = 0.393$ for the adaptive architectural configuration, while the hazard criticality index was $C_H = 36$. Using the ordinal scale defined in Table 4, this value corresponds to Sev = 3 (moderate injury or localized damage, consistent with the trajectory-deviation and localized-collision hazards identified for this scenario), Occ = 4 (frequent, reflecting the relatively high internal fault level $D_F = 0.6$), and Exp = 3 (occupants occasionally present), so that $C_H = 3 \times 4 \times 3 = 36$.

These results demonstrate that the effects of F depend not only on the severity of degradation but also on the capability of the adopted A to limit disturbance propagation. Although degradation originates locally within individual subsystems, its effects propagate through their functional interactions, influencing the overall behaviour of the robotic platform. Compared with the rigid configuration, the adaptive architecture substantially reduces instability propagation by mitigating local disturbances before they evolve into hazardous operating conditions. This finding highlights the importance of architectural robustness for improving operational resilience, even under favourable environmental conditions.

3.3.2. Environment-Dominated Degradation

The second scenario represents operating conditions in which degradation is primarily governed by E, while the internal subsystems continue to operate under nominal conditions. It reflects situations frequently encountered by autonomous residential robotic systems, where external disturbances alone are sufficient to compromise performance despite the absence of significant hardware or software faults. Representative factors include strong lateral wind, elevated surface moisture, unfavourable contact conditions, window-frame discontinuities, dust accumulation, and variations in ambient temperature or illumination.

The scenario was evaluated assuming nominal internal operation subjected to severe environmental disturbances ($D_F = 0.0$, $D_E = 0.7$), resulting in a degradation index of $D_S = 0.210$. Although this value is lower than that obtained for the fault-dominated scenario, the principal hazard is associated with the increased probability of adhesion loss under adverse operating conditions. The instability index reached $I = 0.350$ for the rigid architectural configuration and decreased to $I = 0.233$ for the adaptive architectural configuration, while the hazard criticality index increased to $C_H = 60$. Using the ordinal scale in Table 4, this corresponds to Sev = 5 (loss of adhesion may lead to a fall of the assembly), Occ = 4 (frequent, reflecting the severe environmental disturbance level $D_E = 0.7$), and Exp = 3 (occupants occasionally present), so that $C_H = 5 \times 4 \times 3 = 60$.

These results demonstrate that hazardous operating conditions may develop even in the absence of significant F when E exceeds the adaptive capability of the adopted A. Compared with the rigid configuration, the adaptive architecture reduces instability propagation by improving the system's ability to accommodate changing operating conditions. Consequently, the results confirm that E should be considered a fundamental engineering design parameter influencing architectural robustness, operational safety, and long-term resilience.

3.3.3. Coupled Degradation

The third scenario represents operating conditions in which F and E occur simultaneously. This configuration reflects the conditions most frequently encountered during

practical operation, where component degradation and environmental disturbances continuously interact throughout the service life of the robotic platform. Representative examples include reduced actuator efficiency combined with surface contamination, adhesion degradation caused by moisture together with sensor uncertainty, or control limitations under variable wind conditions.

The coupled scenario was evaluated assuming simultaneous internal degradation and significant environmental disturbances ($D_F = 0.5$, $D_E = 0.6$), resulting in the highest degradation index ($D_S = 0.550$) among the three representative scenarios. The corresponding instability index reached $I = 0.917$ for the rigid architectural configuration and decreased to $I = 0.611$ for the adaptive architectural configuration, while the hazard criticality index remained $C_H = 60$. Using the ordinal scale in Table 4, this corresponds to Sev = 5 (critical instability leading to a fall of the assembly), Occ = 3 (occasional, since the simultaneous occurrence of both degradation sources is less frequent than either source alone), and Exp = 4 (occupants frequently present, consistent with the continuous fault–environment interaction that characterises this scenario), so that $C_H = 5 \times 3 \times 4 = 60$.

The results demonstrate that the simultaneous interaction of F and E produces the most severe system response, as degradation propagates through multiple subsystem interactions rather than through a single dominant source. Although the adaptive architecture significantly reduces instability propagation compared with the rigid configuration, it cannot completely eliminate the effects of coupled degradation mechanisms. Consequently, safe operation depends on the combined contribution of an appropriate A, adaptive control strategies, and effective B.

The coupled scenario provides the strongest demonstration of the proposed ST-based SbD framework by demonstrating that degradation in autonomous residential robotic systems is governed by the interaction between internal faults, environmental variability, architectural characteristics, and safety mechanisms. This systems-level perspective supports informed engineering decisions during conceptual design and contributes to the development of robotic systems with improved robustness, resilience, operational safety, and long-term sustainability.

3.4. Comparative Analysis and Engineering Interpretation

The comparative assessment of the three representative degradation scenarios demonstrates that the behaviour of the autonomous residential window-cleaning robot is governed by the combined influence of F, E, A, and B. Although each operating condition is initiated by a different dominant degradation source, the resulting system response depends on how disturbances propagate through the functional subsystems. Consequently, degradation should be interpreted as a systems-level phenomenon rather than as the isolated consequence of individual component failures.

The numerical results obtained from the semi-quantitative engineering assessment are summarized in Table 6.

Table 6. Comparative results of the semi-quantitative engineering assessment for the representative degradation scenarios.

Scenario	D_F	D_E	D_S	$I_{(Rigid)}$	$I_{(Adaptive)}$	C_H
Scenario 1	0.6	0.1	0.354	0.590	0.393	36
Scenario 2	0	0.7	0.210	0.350	0.233	60
Scenario 3	0.5	0.6	0.550	0.917	0.611	60

Source: authors' own creation.

Table 6 highlights the distinct responses obtained under the three representative operating conditions. The fault-dominated scenario exhibits the highest degradation associated with F, whereas the environment-dominated scenario demonstrates that severe hazards may develop even under nominal internal operating conditions. The coupled scenario produces the highest instability because degradation results from the simultaneous interaction between F and E, leading to disturbance propagation across multiple subsystem interactions. These findings confirm that system response depends not only on the magnitude of individual degradation sources but also on their interaction within the adopted A.

The influence of A on instability propagation is illustrated in Figure 4. Under identical degradation conditions, the adaptive architectural configuration consistently produces lower instability indices than the corresponding rigid configuration, demonstrating a greater capability to attenuate disturbance propagation before hazardous operating conditions emerge. The largest reduction is observed in the coupled degradation scenario, where the adaptive configuration provides the greatest improvement in system stability.

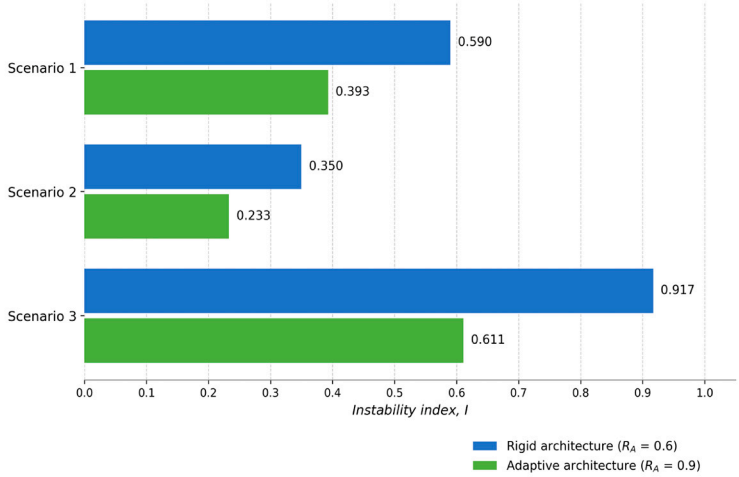


Figure 4. Comparison of the instability index for rigid and adaptive architectural configurations under the three representative degradation scenarios. Source: authors' own creation.

The assessment also demonstrates the significant influence of E on overall system performance. Rather than acting solely as an external disturbance, changing operating conditions modify subsystem interactions, degradation pathways, and the effectiveness of the implemented B. Consequently, identical levels of F may produce substantially different system responses depending on the surrounding operating conditions.

Overall, the comparative assessment demonstrates the applicability of the proposed ST-based SbD framework for analysing degradation propagation during conceptual design. By integrating F, E, A, I, H, and B within a unified analytical framework, the proposed methodology supports the comparison of alternative architectural solutions and provides a systematic basis for improving robustness, resilience, operational safety, and long-term sustainability.

4. Discussion

The results demonstrate that degradation in autonomous residential robotic systems cannot be fully explained using conventional component-oriented engineering approaches alone. Although individual subsystem failures remain important, the assessment shows that engineering performance emerges from the interaction among internal faults (F), environmental variability (E), architecture (A), and safety barriers (B) rather than from isolated component characteristics. Consequently, operational safety depends on the behaviour of the complete engineering system, while engineering failures are better

understood as consequences of interactions among multiple subsystems than isolated component failures [15].

The comparative assessment further demonstrates that identical degradation sources may produce substantially different responses depending on the adopted A. The consistently lower instability indices obtained for the adaptive configuration highlight the importance of considering architectural robustness during conceptual design rather than relying primarily on corrective safety measures introduced during later development stages. These findings further indicate that resilience should be interpreted as an emergent property of the engineering system resulting from architectural interactions rather than from the reliability of individual components [15].

The following discussion examines the engineering implications of these findings and their relevance for the conceptual design of autonomous robotic systems.

4.1. Engineering Implications of the Proposed Framework

This observation has important implications for conceptual design. Conventional development processes typically prioritize functional performance during the early design stages, while safety assessment is introduced progressively through verification and validation activities. The present results indicate that such a sequential approach may overlook degradation mechanisms emerging from subsystem interactions, which are difficult to identify using predominantly component-oriented analyses [15]. By explicitly integrating the relationships among F, system behaviour (S), A, instabilities (I), hazards (H), and B, the proposed methodology enables these interactions to be evaluated before detailed engineering solutions become fixed.

The assessment also demonstrates that A plays a fundamental role in controlling degradation propagation. Under identical degradation conditions, the adaptive configuration consistently reduced I compared with the rigid configuration, indicating a greater capability to maintain stable operation under uncertainty. From this perspective, architecture becomes more than a structural arrangement of subsystems; it actively determines how disturbances propagate throughout the engineering system. This interpretation extends the traditional role of SbD by directly linking architectural decisions with robustness, resilience, and operational safety.

Another important implication concerns the treatment of E. Rather than considering environmental conditions only during system verification, the proposed methodology incorporates E as an explicit engineering design parameter influencing subsystem interactions and degradation pathways. This approach enables uncertainty to be addressed during conceptual development, allowing sensing strategies, control architectures, adhesion mechanisms, and safety functions to be evaluated according to their ability to maintain stable operation under heterogeneous operating conditions.

Although the methodology was demonstrated using an autonomous residential window-cleaning robot, its analytical structure is not limited to this application. Because it is based on the interaction among F, E, S, A, I, H, and B, it can support the conceptual design of other autonomous robotic systems operating under uncertain environmental conditions. The principal contribution of the proposed framework therefore lies not in analysing a single robotic platform, but in providing a transferable engineering methodology that supports early architectural decisions for a broad range of safety-critical autonomous systems.

4.2. Sustainability Implications

The proposed ST-based SbD framework contributes to sustainable engineering by extending the role of safety beyond hazard prevention toward supporting robust and resource-efficient engineering solutions throughout the system life cycle. This perspective

is consistent with the view that long-term sustainability depends on engineering decisions considering the entire system life cycle rather than isolated component performance [26].

From a life-cycle perspective, explicitly considering degradation propagation supports architectural decisions that improve robustness, maintainability, and service life. By limiting the propagation of I, the proposed framework reduces the likelihood of repeated failures, unplanned maintenance, and premature component replacement, contributing to a more efficient use of engineering resources throughout system operation.

These sustainability benefits can, in principle, be linked to measurable indicators rather than treated only qualitatively: reduced instability (I) is expected to translate into fewer unplanned service interventions and a longer service life for actuation and adhesion components, while the reduction in cleaning-fluid loss associated with more stable contact conditions connects directly to the water-consumption metrics already quantified for this platform in our companion study [8]. Establishing quantitative relationships between the instability and hazard indices proposed here and service-life, maintenance-frequency, and resource-use metrics such as those reported in [8] is identified as a concrete direction for future work, rather than a claim substantiated by the present semi-quantitative analysis.

An additional sustainability benefit results from incorporating E as an explicit design parameter rather than considering it only during system verification. This approach enables sensing strategies, control architectures, adhesion mechanisms, and safety functions to be evaluated according to their capability to maintain stable operation under heterogeneous residential operating conditions, thereby improving long-term adaptability while reducing the need for subsequent architectural modifications.

The proposed methodology facilitates the simultaneous evaluation of functional performance, robustness, adaptability, maintainability, and safety during conceptual design. Such an integrated perspective is consistent with sustainability assessment approaches that consider multiple performance dimensions, including safety, robustness, adaptability, environmental impact, and operational efficiency, rather than single-performance indicators [37].

Although demonstrated using an autonomous residential window-cleaning robot, the proposed framework is applicable to a broader range of autonomous systems operating under uncertain environmental conditions. Its principal contribution therefore lies in providing a transferable engineering methodology that supports the development of robust, resilient, maintainable, resource-efficient, and sustainable autonomous systems.

4.3. Limitations and Future Research

Although the proposed ST-based SbD framework provides a structured methodology for supporting conceptual engineering design, several limitations should be acknowledged. First, the study employs a semi-quantitative assessment intended to compare degradation mechanisms and alternative architectural solutions rather than predict the exact behaviour of a specific robotic platform. Accordingly, D_S, I, and C_H should be interpreted as comparative engineering indicators supporting architectural decision-making during conceptual design.

It must be stated explicitly that this validation is purely analytical and semi-quantitative: no physical experiments were performed on the window-cleaning platform to measure D_S, I, or C_H directly, and the reported reductions in instability for the adaptive architecture are model-based projections rather than measured outcomes. Confirming that these projected reductions materialise in physical operation therefore requires dedicated experimental testing, as discussed below.

A second limitation concerns the engineering case study adopted for validation. Although the autonomous residential window-cleaning robot represents an appropriate example of a safety-critical robotic system operating under heterogeneous environmental

conditions, other autonomous platforms may exhibit additional degradation mechanisms, subsystem interactions, and operational constraints. Future work should therefore evaluate the applicability of the proposed framework to autonomous service robots, inspection platforms, collaborative robotic systems, and autonomous mobile robots operating in different environments.

In particular, future work should include a dedicated experimental campaign comparing the rigid and adaptive architectural configurations under controlled, repeatable fault and environmental conditions on the physical window-cleaning platform, and should apply the proposed framework to additional case studies with different operational profiles, such as an autonomous floor-cleaning robot or an autonomous lawnmower, to demonstrate its generalisability beyond a single platform.

The present framework also assumes predefined weighting coefficients for the semi-quantitative assessment. Although these coefficients provide a consistent basis for comparative analysis, future research should investigate calibration procedures based on experimental measurements, operational datasets, or digital twin environments capable of representing degradation propagation under realistic operating conditions. Such developments would improve the predictive capability of the methodology while preserving its applicability during conceptual design.

Another promising research direction is the integration of adaptive monitoring and intelligent decision-support techniques. Machine learning, digital twins, real-time condition monitoring, and predictive maintenance could continuously update degradation models as operational information becomes available, extending the framework from a conceptual design methodology toward a dynamic engineering decision-support tool spanning the entire system life cycle.

Finally, future research should investigate integration with broader sustainability assessment approaches, including life-cycle assessment, circular engineering strategies, and resource-efficiency evaluation. Establishing direct links between systems-level safety analysis and quantitative sustainability metrics would further strengthen the framework as a decision-support methodology for developing safer, more sustainable, and resilient autonomous engineering systems.

5. Conclusions

This study proposed an ST-based SbD framework to support the sustainable conceptual design of autonomous residential robotic systems operating under heterogeneous environmental conditions. Unlike conventional component-oriented approaches, the proposed methodology integrates internal faults (F), environmental variability (E), system behaviour (S), architecture (A), instabilities (I), hazards (H), and safety barriers (B) within a unified analytical framework, enabling degradation to be analysed as a systems-level phenomenon during the early design stages. Such an integrated perspective is consistent with sustainable engineering assessment approaches that simultaneously consider technical performance, safety, and operational robustness within a unified evaluation framework [37].

The applicability of the framework was demonstrated using an autonomous residential window-cleaning robot as an engineering case study. The physical architecture was mapped to the proposed conceptual framework, and three representative degradation scenarios were evaluated using the proposed semi-quantitative assessment methodology. The results showed that system behaviour is governed not only by individual subsystem degradation but also by the interaction among F, E, A, and B.

The comparative assessment demonstrated that A plays a fundamental role in limiting the propagation of I. Under identical degradation conditions, the adaptive architectural

configuration consistently reduced instability compared with the rigid configuration, confirming that architectural robustness is a key factor for improving operational safety and resilience. The results also highlight the importance of considering E as an explicit engineering design parameter during conceptual development rather than only during operation or system verification.

Beyond the presented case study, the proposed framework provides a transferable methodology for supporting the conceptual design of autonomous robotic systems operating under uncertain and safety-critical conditions. By integrating systems thinking with safety-oriented engineering principles, it supports informed architectural decision-making while promoting robustness, maintainability, resource efficiency, and long-term sustainability. This perspective is consistent with sustainable engineering approaches that integrate technical design with operational, environmental, and infrastructural considerations throughout the product life cycle [27].

Future research will focus on experimental validation of the proposed framework, calibration of the semi-quantitative indicators using operational data, and the integration of digital twins, real-time condition monitoring, and predictive maintenance techniques. These developments are expected to improve the predictive capability of the methodology while preserving its applicability as an engineering decision-support tool for supporting sustainable conceptual design.

Author Contributions: Conceptualization, M.-A.M., A.S., E.-C.U., A.-D.F. and A.-M.N.; methodology, A.S., M.C.C. and A.-M.N.; software, M.-A.M., P.P. and M.C.C.; validation, M.C.C., A.S., D.N., E.-C.U., A.-D.F., A.-M.N. and N.V.; formal analysis, M.C.C. and A.-M.N.; investigation, M.-A.M. and A.-M.N.; resources, M.-A.M., D.N. and N.V.; data curation, M.-A.M., M.C.C. and A.-M.N.; writing—original draft preparation, P.P., M.C.C. and A.-M.N.; writing—review and editing, M.-A.M., A.-M.N. and N.V.; visualization, P.P. and A.-M.N.; supervision, M.C.C., A.S., P.P., D.N., E.-C.U., A.-D.F., A.-M.N. and N.V.; project administration, M.-A.M.; funding acquisition, P.P., E.-C.U., A.-D.F. and A.-M.N. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Romanian Ministry of Education and National University of Science and Technology Politehnica Bucharest through the PubArt Program.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in the study are included in the article; further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

A	System Architecture
A4988	Stepper Motor Driver
AI	Artificial Intelligence
B	Safety Barriers
CH	Hazard Criticality Index
DC775	Direct Current 775 Motor
DE	Environmental Degradation Index
DF	Internal Degradation Index
DS	Overall Degradation Index
E	Environmental Variability
ESP32	Espressif 32-bit Microcontroller

F	Internal Faults
FMEA	Failure Mode and Effects Analysis
FRAM	Functional Resonance Analysis Method
H	Hazards
HAZOP	Hazard and Operability Analysis
I	Instabilities (Intermediate Effects)
IMU	Inertial Measurement Unit
L298N	Dual H-Bridge Motor Driver
LA23	LINAK LA23 Linear Actuator
MGN12	MGN12 Linear Guide Rail
PLG42	PLG42 Planetary Gearbox
RA	Architectural Robustness Coefficient
RPN	Risk Priority Number
S	System Behaviour
SbD	Safety-by-Design
ST	Systems Thinking
STPA	System-Theoretic Process Analysis
Wi-Fi	Wireless Fidelity

References

1. Sepasgozar, S.M.E.; Karimi, R.; Shirowzhan, S.; Mojtahedi, M.; Ebrahimzadeh, S.; McCarthy, D. A systematic content review of artificial intelligence and the Internet of Things applications in smart home. *Appl. Sci.* **2020**, *10*, 3074. [CrossRef]
2. Ahmed, A.A.; Belrzaeg, M.; Nassar, Y.; El-Khozondar, H.J.; Khaleel, M.; Alsharif, A. A comprehensive review towards smart homes and cities considering sustainability developments, concepts, and future trends. *World J. Adv. Res. Rev.* **2023**, *19*, 1482–1489. [CrossRef]
3. Marikyan, D.; Papagiannidis, S.; Alamanos, E. A systematic review of the smart home literature: A user perspective. *Technol. Forecast. Soc. Change* **2019**, *138*, 139–154. [CrossRef]
4. Bibri, S.E.; Krogstie, J. Smart sustainable cities of the future: An extensive interdisciplinary literature review. *Sustain. Cities Soc.* **2017**, *31*, 183–212. [CrossRef]
5. Lou, S.; Wei, Z.; Guo, J.; Ding, Y.; Liu, J.; Song, A. Current status and trends of wall-climbing robots research. *Machines* **2025**, *13*, 521. [CrossRef]
6. Parween, R.; Elara, M.R.; Saldi, Z.S.; Ng, T.; Rayguru, M.M. Modeling and analysis of a glass façade robot. *Buildings* **2021**, *11*, 225. [CrossRef]
7. Wang, B.; Zhang, W.; Luo, J.; Xu, Q. Design of a modular wall climbing robot with multi plane transition and cleaning capabilities. *Biomimetics* **2025**, *10*, 450. [CrossRef]
8. Mielcioiu, M.-A.; Petcu, P.; Nedelcu, D.; Semenescu, A.; Valter, N.; Nicolau, A.-M. Design and Implementation of a Low-Water-Consumption Robotic System for Cleaning Residential Balcony Glass Walls. *Appl. Sci.* **2026**, *16*, 945. [CrossRef]
9. Campean, F.; Kabir, S.; Dao, C.; Zhang, Q.; Eckert, C. Towards A Resilience Assurance Model for Robotic Autonomous Systems. *Proc. Des. Soc.* **2021**, *1*, 3189–3198. [CrossRef]
10. Nicolau, A.-M.; Petcu, P. A Systemic View of Biodegradable Materials: Analyzing the Environmental Performance of Compostable Coffee Capsules in Real Infrastructural Contexts. *Sustainability* **2025**, *17*, 7736. [CrossRef]
11. Luckcuck, M.; Farrell, M.; Dennis, L.A.; Dixon, C.; Fisher, M. Formal Specification and Verification of Autonomous Robotic Systems: A Survey. *ACM Comput. Surv.* **2019**, *52*, 100. [CrossRef]
12. Adesiji, A.D.; Ibitoye, S.E.; Mahamood, R.M.; Olayemi, O.A.; Omoniyi, P.O.; Jen, T.-C.; Akinlabi, E.T. Safety Considerations in Deployment of Robotic Systems—A Systematic Review. *J. Field Robot.* **2026**, *43*, 5–33. [CrossRef]
13. Araujo, H.; Mousavi, M.R.; Varshosaz, M. Testing, Validation, and Verification of Robotic and Autonomous Systems: A Systematic Review. *ACM Trans. Softw. Eng. Methodol.* **2023**, *32*, 51. [CrossRef]
14. Altieri, M.A.; Nicholls, C.I.; Henao, A.; Lana, M.A. Agroecology and the design of climate-change-resilient farming systems. *Agron. Sustain. Dev.* **2015**, *35*, 869–890. [CrossRef]
15. Nicolau, A.-M.; Semenescu, A.; Petcu, P. Assessing the Resilience of Regenerative Agricultural Systems to Climate Change: A Scenario-Based Systemic Analysis Framework. *Agriculture* **2026**, *16*, 374. [CrossRef]
16. Kurdys-Kujawska, A.; Soliwoda, M.; Grzelczak, M.; Apanel, A. Financial Innovation in Building Agricultural Sector Resilience: New Horizons and Challenges for Blended Finance in Poland. *Agriculture* **2025**, *15*, 754. [CrossRef]

17. Adam, M.; Anisi, D.A.; Ribeiro, P. A Verification Methodology for Safety Assurance of RAS. In *Annual Conference Towards Autonomous Robotic Systems*; Springer: Berlin/Heidelberg, Germany, 2025; pp. 281–294. [CrossRef]
18. Abeywickrama, D.B.; Fisher, M.; Wheeler, F.; Dennis, L. Autonomy and safety assurance in the early development of robotics and autonomous systems. *arXiv* **2025**, arXiv:2501.18448. [CrossRef]
19. Leveson, N.G. *Engineering a Safer World: Systems Thinking Applied to Safety*; MIT Press: Cambridge, MA, USA, 2011.
20. Hollnagel, E. *FRAM: The Functional Resonance Analysis Method: Modelling Complex Socio-Technical Systems*; Ashgate: Farnham, UK, 2012.
21. *ISO 12100*; Safety of Machinery—General Principles for Design—Risk Assessment and Risk Reduction. ISO: Geneva, Switzerland, 2010.
22. *ISO 13482*; Robots and Robotic Devices—Safety Requirements for Personal Care Robots. ISO: Geneva, Switzerland, 2014.
23. *IEC 61508-1*; Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems—Part 1: General Requirements. IEC: Geneva, Switzerland, 2010.
24. *ISO 13849*; Safety of Machinery—Safety-Related Parts of Control Systems—Part 1: General Principles for Design. ISO: Geneva, Switzerland, 2023.
25. Zhang, D.; Li, Y.; Jia, P.; Jiao, X.; Zheng, Y.; Wang, G.; Li, Z.; Zhang, M.; Wang, J.; Li, M. A full coverage path planning algorithm for a glass curtain wall cleaning robot driven by ropes. *Appl. Sci.* **2023**, *13*, 5052. [CrossRef]
26. Hsu, K.-C.; Hu, H.; Fisac, J.F. The Safety Filter: A Unified View of Safety-Critical Control in Autonomous Systems. *Annu. Rev. Control Robot. Auton. Syst.* **2024**, *7*, 47–72. [CrossRef]
27. Luckcuck, M. Using formal methods for autonomous systems: Five recipes for formal verification. *Proc. Inst. Mech. Eng. Part O J. Risk Reliab.* **2023**, *237*, 278–292. [CrossRef]
28. Vert, M.; Sharpanskykh, A. The Resilience of Complex Sociotechnical Systems: A Meta-Review of Conceptualisations. *Systems* **2026**, *14*, 71. [CrossRef]
29. Potts, M.W.; Sartor, P.A.; Johnson, A.; Bullock, S. A Network Perspective on Assessing System Architectures: Robustness to Cascading Failure. *Syst. Eng.* **2020**, *23*, 597–616. [CrossRef]
30. Jimenez-Ballesta, R.; Mongil-Manso, J.; Jimenez-Sanchez, A. Application of Regenerative Agriculture: A Review and Case Study in an Agrosilvopastoral Region. *Sustainability* **2025**, *17*, 9066. [CrossRef]
31. O'Donoghue, T.; Minasny, B.; McBratney, A. Digital Regenerative Agriculture. *npj Sustain. Agric.* **2024**, *2*, 5. [CrossRef]
32. Sharabati, A.-A.A.; Jreisat, E.R. Blockchain Technology Implementation in Supply Chain Management: A Literature Review. *Sustainability* **2024**, *16*, 2823. [CrossRef]
33. Orfanos, V.A.; Kaminaris, S.D.; Papageorgas, P.; Piromalis, D.; Kandris, D. A comprehensive review of IoT networking technologies for smart home automation applications. *J. Sens. Actuator Netw.* **2023**, *12*, 30. [CrossRef]
34. Zhang, L.; Chen, Z.; Laili, Y.; Ren, L.; Deen, M.J.; Cai, W.; Zhang, Y.; Zeng, Y.; Gu, P. MBSE 2.0: Toward More Integrated, Comprehensive, and Intelligent MBSE. *Systems* **2025**, *13*, 584. [CrossRef]
35. Qu, C.; Kim, E. Reviewing the Roles of AI-Integrated Technologies in Sustainable Supply Chain Management: Research Propositions and a Framework for Future Directions. *Sustainability* **2024**, *16*, 6186. [CrossRef]
36. Huang, J.; You, J.-X.; Liu, H.-C.; Song, M.-S. Failure Mode and Effect Analysis Improvement: A Systematic Literature Review and Future Research Agenda. *Reliab. Eng. Syst. Saf.* **2020**, *199*, 106885. [CrossRef]
37. Malefaki, S.; Markatos, D.; Filippatos, A.; Pantelakis, S. A Comparative Analysis of Multi-Criteria Decision-Making Methods and Normalization Techniques in Holistic Sustainability Assessment for Engineering Applications. *Aerospace* **2025**, *12*, 100. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.