mathematics

MDPI

Article

The Use of Soft Logic for Risk Evaluation in Defense System of Systems

Ron S. Hirschprung and Sigal Kordova *

Department of Industrial Engineering & Management, Ariel University, Ariel 40700, Israel; ronyh@ariel.ac.il
* Correspondence: sigalko@ariel.ac.il

Abstract

Risk management is a crucial task in project management in light of the uncertainty that is almost always inherent. This phenomenon is enhanced in projects in the defense sector, due to their high complexity and their nature as system of systems (SoS). In general, traditional risk management approaches often fall short. To address this issue, this paper explores the utilization of soft logic to improve risk management methodologies in SoS. Soft logic can address the problem of representing contradictory situations. The proposed methodology, unlike the traditional one, does not collapse the variety of estimations into a single central value, thus, it is able to perform extreme evaluations as well. An empirical analysis was conducted by means of qualitative and quantitative approaches. The findings suggest that the methodology based on soft logic may enhance decision-making processes to handle risks more effectively.

Keywords: risk management; assessment; soft logic; defense system of systems (SoS)

MSC: 91G70; 91B05

1. Introduction

In today's dynamic organizational environment, diverse conditions and demands profoundly influence business operations in general, and project management in particular. Among these, risks have become a critical factor, impacting activities across nearly all sectors. To survive, grow, and remain sustainable, organizations must be prepared to address the numerous challenges arising from this complex and uncertain element [1], specifically, in risk management [2]. This is especially true in defense projects, where the development of large-scale systems or advanced military equipment highlights the acute complexities stemming from technical, organizational, and environmental dimensions.

The complexity of defense projects arises from their large scale, the interdependence of numerous systems, the integration of cutting-edge technologies, and the need for coordination across various agencies and contractors. Additionally, these projects often operate under stringent security requirements, adding another layer of complexity regarding information and communication management [3]. A notable example is the Unmanned Combat Air Vehicle (UCAV) program [4], which focuses on developing drone aircrafts capable of engaging in combat without a pilot. These systems are designed to perform tasks such as surveillance, target acquisition, and the deployment of weaponry in hostile environments. The UCAV program illustrates the integration of advanced robotics, AI, and remote sensing technologies, enhancing capabilities while minimizing risks to human life

Check for updates

Academic Editor: Rui Manuel Rodrigues Cardoso

Received: 23 January 2026
Revised: 6 February 2026
Accepted: 10 February 2026
Published: 12 February 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.

in military operations. Such projects underscore the growing emphasis on autonomy in modern defense strategies [5].

Improving risk management methodologies in such projects is crucial given the high stakes involved—financial, strategic, and operational. Traditional risk management approaches may fall short in addressing the dynamic and interconnected risks these projects face. A more sophisticated approach, such as the one proposed by Luo et al. [6], integrates fuzzy cognitive mapping and structural equation modeling to predict and mitigate risks more accurately by understanding the intricate relationships between various project elements [6]. Sharma and Chanda [7] proposed a Bayesian belief network (BBN) model to assess and estimate the risk exposure of R&D projects. The authors emphasize that managing risks effectively is crucial for project success in today's competitive and globalized business environment.

The need for enhanced risk management methodologies in defense projects is also underlined by research indicating that project complexity significantly impacts project success, necessitating a deeper understanding and proactive management of this complexity to improve outcomes [6,8].

The Project Management Body of Knowledge (PMBOK) provides a structured approach to project management that includes robust risk management practices [9]. However, the standard PMBOK methodology may face several limitations concerning complex defense projects. This research focuses on the development of System of Systems (SoS) projects in the defense industry. The U.S. Department of Defense (DoD) defines a System of Systems (SoS) as a configuration that integrates multiple independent systems into a larger system that delivers unique capabilities. These systems maintain their separate operations but collaborate to achieve a common mission, which could not be accomplished by any individual system alone [10]. The PMBOK approach might not be entirely adequate for managing risks in such projects. Defense SoS projects are characterized by their high complexity and the interdependency of their constituent systems. This complexity extends beyond what typical project management frameworks, such as PMBOK are designed to handle. As Maier [11] noted, SoS requires an architectural approach that considers both the systems' operational independence and managerial interdependence. PMBOK, primarily structured around less complex projects, might not adequately address these interdependencies. Given these challenges, an enhanced risk management strategy becomes crucial. In general, risk management, which is a critical process in most organizations, encompasses the identification, assessment, and prioritization of risks followed by coordinated efforts to minimize, monitor, and control the impact of unfortunate events [12]. However, effective risk management integrates various evaluations of risks, drawing on diverse opinions and methodologies to create a comprehensive understanding [13].

According to conservative approaches to risk management, average probability calculation methods can be utilized to assess risk probability for regular projects. This approach gathers and synthesizes risk evaluations from a panel of experts, then reconciles the varying opinions to form a consensus estimate of risk probability. This approach is designed to achieve a balanced risk assessment. However, it may lead to wrong decisions when exceptional probabilities that are suggested by some of the experts are not considered. Ignoring these assessments can be particularly problematic in defense projects, where an error in risk assessment could cause significant and sometimes irreversible damage. For example, if most experts estimate a low probability for a particular event, but one expert estimates a relatively high probability due to his specific experience or knowledge, diluting his assessment by averaging could lead to a flawed risk assessment. This phenomenon is supported by Raz, Shenhar, and Dvir [14]. who claimed that projects with high technological risk require risk management methods that address unexpected and rapid changes.

Alternative methods suggest weighing the experts' assessments not only based on the average probability but also on a range of evaluations while considering extreme values in cases where there is justification to do so. Methodologies like Monte Carlo or Bayesian [15] facilitate the modelling and analysis of risks, effectively addressing uncertainty and varying outcome distributions.

The current study focuses on evaluating risk assessment in defense projects. In fact, the proposed methodology is general, and may be adopted in any domain, however, this methodology specifically considers the above-mentioned challenges of the defense domain. Moreover, the empirical analysis is centered on classified defense SoS, while examining the unique challenges and risk probabilities associated with these complex integrations.

Based on the literature analysis and the need to improve risk management in such projects, this research aims to develop an approach that incorporates experts' extreme opinions, and not only the average ones. Additionally, thought will be given to data collection and analysis methods that allow greater flexibility in responding to background factors, such as the expert's seniority in project management or changes in the technological or military environment.

This paper introduces a novel risk management methodology that employs a soft-logic-based mathematical model. This mathematical approach can address the representation of contradictory situations (e.g., significantly different risk pass rates). In Section 3, we delve into the background of Soft Logic, explaining its principles. Section 4 details the mathematical model itself, outlining how soft logic is applied to manage risks in complex environments and its relevance to risk assessment; and Section 5 demonstrates an empirical study in the defense sector. This approach may support the decision-making process by incorporating both quantitative data and qualitative insights, offering a comprehensive framework for risk analysis. It has the potential to significantly improve the effectiveness of risk management in defense projects, where errors may incur a high cost.

2. Literature Review

This literature review surveys the complexities of risk management in defense SoS, beginning with elemental principles and their applications. It then delves into the concept of SoS, particularly their relevance and the unique challenges they pose in the defense sectors. The focus then shifts to tailored risk management strategies essential for navigating the inherent risks of defense SoS.

2.1. Risk Management

The literature provides several frameworks and approaches that describe the risk management process. For example, the ISO 31000:2018 standard offers a comprehensive framework for identifying, analyzing, evaluating, and treating risks across different areas of an organization [16]. This standard ensures that risk management is systematic, consistent, and transparent. The primary aim is to create and protect value, enhance organizational performance, foster innovation, and help achieve objectives. There are eight guiding principles outlined in this standard: risk management should be an integral part of all organizational processes, including decision-making, and not treated as a separate, standalone process; the process should be well-structured and comprehensive, covering all levels and aspects of the organization to ensure effective handling of potential risks; the risk management process should be tailored to fit the specific needs and culture of the organization, taking into account its external and internal context; stakeholder involvement is crucial, therefore, engaging stakeholders ensures that risk management remains relevant and up-to-date with diverse perspectives and fosters a culture of collective ownership in managing risk; the process should be able to recognize and respond to changes in the

external and internal environment of the organization, ensuring that risk management is proactive rather than reactive; decisions should be based on the best available information, which includes historical data, expert opinions, and feedback to anticipate future events and their impacts; these factors influence every aspect of risk management, including the way risks are identified, analyzed, and managed. Recognizing and addressing these factors can enhance the effectiveness of the risk management process. Risk management processes should evolve by learning from past activities and by improving strategy and procedures to meet the organization's objectives better.

The PMBOK emphasizes risk management as a critical process, advocating comprehensive steps that include risk identification, analysis, response planning, and control. These steps aim to increase the likelihood of positive events and decrease the possibility of adverse outcomes in projects [9]. The PMBOK guide differentiates between the concepts of risk and uncertainty within project management. Risk is an unplanned event that could impact specific project objectives if it materializes. In contrast, uncertainty is a lack of predictability about future events. The guide illustrates that at the onset of a project, the cost of making changes is relatively low, but as the project progresses, these costs increase. Concurrently, the initial stages of a project often involve higher levels of risk and uncertainty, which tend to decrease as the project moves forward. It is worth mentioning that this differentiation may sometimes lie in a gray zone, e.g., the risk of exceeding the projects' planned timeline may also be referred to as an uncertainty. The guide further categorizes uncertainty into two types: predictable uncertainty, which can be managed through structured methodologies, and unpredictable uncertainty, which is typically mitigated by incorporating buffers in the project's schedule, budget, and scope of work.

Wang's [17] definition of risk encompasses several critical elements commonly assessed in risk management practices across industries. This definition highlights risk as something potentially unexpected that can cause physical harm, damage assets, or delay schedules. It also underscores the importance of evaluating risk based on three key dimensions: likelihood of occurrence, level of impact, and potential damage. By analyzing risks through these lenses, organizations can develop more robust strategies to mitigate adverse effects and enhance their resilience against potential threats. Erfani et al. [18] propose a data-driven approach to risk identification in major transportation projects by developing a comprehensive Risk Breakdown Structure (RBS) based on U.S. state Departments of Transportation reports. Using Natural Language Processing (NLP), the RBS was shown to cover about 81% of risks across 70 projects. The study also emphasizes the value of recognizing risk interdependencies to improve the effectiveness of risk management. Dikmen & Qazi [19] critique the limitations of traditional risk matrices in construction projects and propose using risk networks as a more effective tool. By modeling the interdependencies among risks, risk networks offer a dynamic, systemic understanding of how risks influence one another. Through case study analysis, the authors demonstrate that risk networks provide richer insights into risk propagation, prioritization, and mitigation strategies. This network-based approach enables project managers to identify critical risks more accurately and make better-informed decisions under uncertainty.

Kovic and Kristiansen [20] argue that while the Gambler's Fallacy reflects irrational assumptions about independent events, not all reasoning about outcome sequences is flawed. In risk management contexts, assessing the odds of contextually relevant sequences can serve as a practical heuristic for avoiding cognitive biases in high-pressure decision-making. This approach helps reduce misclassification of rational judgments as fallacious and provides a simple, intuitive method to improve probabilistic reasoning under uncertainty.

Boehm [21] presents a model comprising two main phases: risk assessment, which includes identification, analysis, and prioritization of risks; and risk control, which encompasses planning, resolution, and monitoring of risks. This framework parallels the quality improvement cycle (plan, do, check, act) advocated by Deming [22], which is echoed in the four-phase process suggested by Kliem and Ludin [23] that further integrates identification, analysis, control, and reporting of risks. Fairley [24] outlines a systematic approach comprising the following steps: identification of risk factors, assessment of risk probabilities and impacts, development of mitigation strategies, continuous monitoring of risks, and implementing contingency plans if risks materialize. Nasteckienė [25] argues that risk management is a non-linear process deeply embedded in the daily management activities that are supported by continuous learning from past failures and successes. This practical approach allows managers to adapt risk management strategies in real-time, tailoring them to their operations' specific needs and contexts. Jat et al. [26] explore how different contextual factors, such as firm size, supply chain complexity, and industry type, affect the implementation of Supply Chain Risk Management (SCRM) practices and their impact on agility performance. Their study finds that effective SCRM enhances a firm's ability to respond quickly to disruptions, but its success depends on the firm's specific context. Notably, aligning risk management strategies with contextual characteristics is key to achieving greater agility. This underscores the importance of tailoring risk management approaches to fit organizational and environmental conditions.

Innovative analytical techniques such as the Monte Carlo simulations, the analytical hierarchy process, and fuzzy set theory are also extensively discussed in the literature for their effectiveness in risk management. These methods facilitate a more nuanced analysis of risks by providing probabilistic estimates and multi-criteria decision-making support, which are crucial in handling the complexities of large-scale projects [27–30]. Toufighi and Nugroho [31] developed a risk-based maintenance strategy for oil transfer pipelines using an intuitionistic fuzzy computational model. Their approach captures uncertainty in expert judgment to refine the evaluation of failure probabilities and consequences, thereby improving the prioritization of maintenance actions. This illustrates how advanced fuzzy logic, a closely related mathematical approach to soft logic, can strengthen risk assessment in complex, high-stakes environments such as defense projects.

Despite the advantages, the literature also indicates a variance in the effectiveness of these risk management tools. While many studies report significant benefits in terms of project outcomes, others find minimal or no impact, suggesting that the effectiveness of risk management practices may be context-dependent and influenced by the specific characteristics of a project or sector [14,32–36]. Shafqat, Oehmen, and Welo [37] examined how proactive risk management (PRM) and reactive fast learning (RFL) can mitigate unplanned design iterations in complex projects. While PRM is more established, RFL often lacks structured methods for learning and knowledge retention. Their study suggests that combining both approaches reduces unexpected iterations, a finding highly relevant for defense projects where delays and cost overruns carry critical implications.

Sector-specific risk management is highlighted in contexts such as public-private partnerships, where unique risk factors such as government approval delays and market volatility are prevalent. These sector-specific risks underscore the need for tailored risk management strategies that address the distinct challenges of different project types [38].

2.2. System of Systems (SoS)

The projects that served the empirical phase of this study are classified as defense SoS. SEBoK [39] defines SoS as a complex configuration of individual systems that interact to provide a distinctive capability that no single system could independently offer. Echoing

this, Maier [11] articulates SoS as an ensemble of specialized systems that integrate their functions and capabilities to create a composite system with enhanced functionality and superior performance, transcending its components' mere aggregation.

The SoS concept has significantly evolved from its roots in traditional system engineering to address the complexities and interdependencies characteristic of modern engineering projects. This evolution has been largely driven by the military sector, which has been at the forefront of developing and implementing SoS to enhance operational effectiveness and address multifaceted challenges [40].

The literature often discusses various initial attempts to define SoS, revealing a lack of consensus on a concrete definition [41]. The shift from considering individual systems to a collective of integrated complex systems has become pivotal. It underscores the necessity of applying complex-system principles to SoS, laying a foundational understanding for ongoing research in this field [42,43]. Notable contributions to this evolving definition include recent standards such as ISO/IEC/IEEE 21839:2019, which also discusses constituent systems [44]. The U.S. DoD's (Department of Defense) publication on Systems Engineering in a SoS environment further underscores the complexities and characteristics integral to SoS [10].

As SoS research expands, a consolidated body of knowledge or a managerial framework is still lacking in order to navigate these intricate systems effectively. Efforts like those of Gorod et al. [41] have begun to address this issue by proposing frameworks that integrate SoS characterization and their inherent network traits. There is a clear need for ongoing development of general principles applicable to SoS and practical applications of these principles, challenging the systems engineering community to redefine complex systems for contemporary needs [43].

2.3. Integrated Risk Management Approaches for Defense Systems of Systems

Defining risk management in defense SoS is vital due to their inherent complexities and their dynamic, rapidly changing environments. Defense SoS face unique challenges that require managing numerous interconnected components under fast-evolving technological and tactical conditions.

Defense SoS demand a systematic approach to risk management to prevent failures and ensure operational integrity throughout the system's development and deployment stages [45]. Defense projects operate in significantly more uncertain and dynamic environments than civilian projects. The PMBOK framework emphasizes a somewhat linear progression through project phases (initiation, planning, execution, monitoring and controlling, and closing), which may not be flexible enough to respond to the rapid changes typical in defense settings. Bennett [46] delves into the challenges and risks associated with major defense projects, specifically within the Australian Defense Force. The core of Bennett's argument is that traditional risk management practices are insufficient for the unique challenges of defense projects. He categorizes the risks into seven areas: novelty, uncertainty, complexity, interdependence, resource limitations, technological and market changes, and political constraints. Bennett advocates a shift in focus from avoiding problems to creatively and flexibly adapting in order to solve them as they arise. He also emphasizes the importance of project managers who are not just trained technicians but reflective practitioners with a deep understanding and the ability to navigate the political, strategic, and technological landscapes. An almost straightforward outcome of this insight is that the assessment of risks in such types of a complex project must provide a well representation of the full gallery of the project's partners. This last requirement of "well representation" is the main motive behind the current research. According to Bennett, successful management of defense projects relies more on the quality and preparedness of

managers and their teams than on strict adherence to predefined processes and schedules. Boehm [21] and Fairley [24] discuss how risk management in software projects (which share some characteristics with defense projects) requires iterative risk identification and management throughout the project lifecycle, suggesting a need for more dynamic methodologies. Here again, the current research aims to provide a novel methodology to address this issue by enhancing the representation of the assessments.

Recent risk management literature conceptualizes Enterprise Risk Management (ERM) as a dynamic capability that enables organizations to address uncertainty, complexity, and systemic change. By integrating formal governance structures with risk culture, artefacts, and managerial cognition, ERM supports organizational resilience beyond mere risk control. This perspective is particularly relevant for SoS, where interdependencies and emergent behavior constrain the effectiveness of static, probability-based risk assessment. Accordingly, ERM-oriented approach that emphasizes learning and adaptability provides a foundation for more robust risk evaluation in highly dynamic and uncertain environments [47,48].

Defense projects frequently involve cutting-edge technologies that evolve throughout the project lifecycle, generating high levels of technological uncertainty that are not fully addressed by standard risk management frameworks such as PMBOK [9]. As noted by Raz, Shenhar, and Dvir [14], technological risks require adaptive and flexible management strategies capable of coping with innovation-driven uncertainty. This limitation becomes even more pronounced in SoS, where technological uncertainty is compounded by interdependencies, emergent behavior, and dynamic interactions among constituent systems. Riepl, Mitter and Kuttner [49] emphasize that effective risk management under such conditions relies on integrating formal analytical tools with informal, context-sensitive mechanisms that enhance risk awareness and adaptive capacity. The complementary use of these mechanisms supports more robust risk evaluation and resilience in complex defense SoS environments characterized by technological novelty and systems uncertainty.

Recent research increasingly highlights the limitations of traditional risk matrices in representing complex causal dependencies and accumulated risk effects in large-scale systems. Burstein and Zuckerman [50] demonstrate that causal risk modeling based on directed acyclic graphs (DAGs) can reduce subjectivity and improve consistency by explicitly representing how risks propagate through interdependent system components. Complementing this perspective, Shi et al. [51] show that hybrid weighting approaches combining AHP, entropy methods, and cloud models enable richer representations of ambiguity, randomness, and fuzziness in expert evaluations while preserving the hierarchical structure of decision criteria. Together, these studies underscore the need for system-oriented risk evaluation frameworks that move beyond deterministic weights and single-point estimates toward integrated representations of causal structure and uncertainty in complex socio-technical SoS.

In summary, while PMBOK, ISO 31000:2018 standard, and other scholars provide a strong foundation for project and risk management, their standard practices may not be entirely sufficient for the specific demands of defense projects. Modifications or expansions of these methodologies can better cater to the high stakes, complexity, and dynamism of defense SoS.

3. Soft Logic Background

While some, and maybe even most phenomena in our reality can be described in deterministic means, some cannot. Leading examples can be found in soft fields that encompass human factors, such as dilemmas, paradoxes, and ambiguity. The theory of soft logic was developed in its current form by Klein & Maimon [52] in order to address these situations mathematically. For example, the privacy paradox, which is a well-known

phenomenon, describes the gap between the user's concern and behavior when dealing with privacy issues. The paradox stems from the fact that many people claim that they will protect their privacy, but do not act accordingly. This paradox is considered unexplained by most researchers, and soft logic was adopted to represent it [53].

Risk, by their nature and even according to their definitions, are ambiguous; they are based on probabilities, and its estimation is subject to the point of view, and not necessarily to a well-defined deterministic model. For example, different people may estimate the risk of a given situation in a completely different manner. Therefore, soft logic is a good candidate to represent this domain.

Soft logic has some affinity with other theories, such as Bayesian aggregation and fuzzy logic. All of these theories are "soft" by their nature and do not assume a classic logic dichotomy. Therefore, they span a values space that lies beyond a bilevel true/false space. However, while, for example, fuzzy logic assumes the existence of a singularity, i.e., a theoretical realism that does exist but cannot be accurately indicated because of the probabilistic nature of the system, soft logic is not limited to this assumption. In other words, while fuzzy logic does abandon the limitation to the [0,1] discrete set and enables the multiplication of 1 by a real number between 0 and 1, soft logic enables the existence of an unlimited number of these multiplications simultaneously. The power of soft logic lies in its ability to encapsulate contradictory situations that may coexist. Fuzzy logic, therefore, is a good tool for handling situations in which some information is missing. On the other hand, soft logic is better when there is a conflict—a common feature of risk evaluation. Bayesian aggregation recognizes the possibility of conflicts, particularly with expert opinion. It takes a step forward by avoiding averaging, a common approach in risk assessment, as discussed below. However, it combines multiple forecasts into a single distribution and therefore partially collapses the data model by reducing its dimension. Moreover, one motivation for using Bayesian aggregation is to handle noisy data, but in the risk model, we would like to focus on "noise", which may represent an unpopular opinion that, in many historical cases, was found to be true but was "socially" rejected.

Unlike classical math, where zero is a singular point, in soft logic, the zero number has an infinite number of different values and, geometrically, is no longer represented as a point but as a line. Therefore, the theorem that $\forall\, a, b \in \mathbb{R} : ab0 = b0$ is no longer necessarily true, and the zero number, which is now called 'soft zero', receives the form $b\overline{0}$ (the vinculum notation differentiates between a soft zero and a classic zero). Down the road with soft logic theory, a soft number will have two components: (a) the soft zero that was described above; and (b) a 'real' part that receives the form $a\overline{1}$, and actually represents a classical math number. Now, a soft number is defined as:

$$a\overline{1} \dot{+} b\overline{0} \quad (a, b \in \mathbb{R}) \tag{1}$$

For convenience, since $\overline{1}$ is a classic number, we will omit the vinculum, and the soft number may also be represented as $a1 \dot{+} b\overline{0}$. Note that the $\dot{+}$ operator is a unique addition that bridges between the soft and the real numbers. The soft logic theory is based on several axioms [54]. Not all axioms are required for the risk assessment model, however, since soft logic is a relatively new and unknown theory, they are introduced here to generally support the establishment of the mathematical theory and, specifically, the algebraic operations used. Understanding the implementation of soft logic can be achieved without those definitions, especially the *Multiplication of two soft numbers*, the *Inverse of a soft number*, the *n-th power of a soft number*, the *Square root of a soft number*, and the *n-th root of a soft number* axioms. The definitions are:

Axiom 1—Distinction:

if $a \neq b$ then $a\overline{0} \neq b\overline{0}$.

This axiom was mentioned above, and is the fundamental of soft logic that 'stretches' the zero from a singular point to an infinite number of values. Derived from the distinction axiom, an order can be defined between two soft zeros: If $a < b$ then $a\overline{0} < b\overline{0}$. While the order between soft zeros on their own, as well as the order between real numbers on their own is clear, the order between soft numbers is not trivial, and will be discussed later.

Axiom 2—Addition:

$$a\overline{0} + b\overline{0} = (a+b)\overline{0}.$$

The addition axiom is the equivalent of the classic algebra distributive property: $a{\cdot}(x+y) = a{\cdot}x + a{\cdot}y$ [55].

Axiom 3—Nullity:

$$a\overline{0}{\cdot}b\overline{0} = 0.$$

When the multiplication operator is applied between two soft zeros, the result collapses to a real zero. Note that this is not true for real numbers, as $a1{\cdot}b1 = ab1$ (and not necessarily $a1{\cdot}b1 = 1$). The nullity axiom is based on the dual number property: $\varepsilon^2 = 0$ [56].

Axiom 4—Bridging:

This axiom states that the soft aero and the real part can be bridged (noted as $a\overline{0}{\perp}b\overline{1}$ where $\perp$ is the bridging operator). This axiom is essential to form the soft number, and was inspired by the complex numbers system, which also extends the real number to a new form: $a + bi$ where $i = \sqrt{-1}$ [57].

Axiom 5—Non-commutativity:

$$a\overline{0}{\perp}b\overline{1} \neq b\overline{1}{\perp}a\overline{0}.$$

The non-commutativity axiom claims that the order of the soft and the real part is a significant property, and it has some equivalents in previous mathematical theories such as the one that states that certain algebraic structures are non-commutative, e.g., the non-abelian group where $a{\cdot}b \neq b{\cdot}a$ [58].

The set of all soft numbers is $\mathrm{SN} = \left\{a\overline{0} \dot{+} b : a, b \in \mathbb{R}\right\}$, and the basic operator may be defined as follows:

Addition of two soft numbers: $\left(a\overline{0} \dot{+} b\right) + \left(c\overline{0} \dot{+} d\right) = (a+c)\overline{0} \dot{+} (b+d)$
Multiplication of two soft numbers: $\left(a\overline{0} \dot{+} b\right) \times \left(c\overline{0} \dot{+} d\right) = (ad+bc)\overline{0} \dot{+} (bd)$
Inverse of a soft number: $\left(a\overline{0} \dot{+} b\right)^{-1} = \left(-\frac{a}{b^2}\overline{0} \dot{+} \frac{1}{b}\right)$ *when* $b \neq 0$,

Therefore, $(\mathrm{SN}, +, \times)$ is almost an algebraic field (if the inverse was also defined as $b = 0$, SN would also be a complete field).

***n-th* power of a soft number:**

$$\left(a\overline{0} \dot{+} b\right)^n = nab^{n-1}\overline{0} \dot{+} b^n \text{ where } n \in \mathbb{N}^+, \mathbb{N}^+ = \{0, 1, 2, 3, \ldots\}$$

Square root of a soft number:

$$\sqrt{a\overline{0} \dot{+} b} = \left(+\frac{a}{2\sqrt{b}}\overline{0}\right) \dot{+} \left(+\sqrt{b}\right), \left(-\frac{a}{2\sqrt{b}}\overline{0}\right) \dot{+} \left(-\sqrt{b}\right)$$

where $b > 0$.

***n-th* root of a soft number:**

For $b \neq 0$ and an odd n:

$$\sqrt[n]{a\overline{0} \dot{+} b} = \left(+\frac{a}{n \cdot b^{(\frac{n-1}{n})}}\overline{0}\right) \dot{+} \left(+\sqrt[n]{b}\right)$$

and

For $b > 0$ and an even n:

$$\left(+\frac{a}{n \cdot b^{(\frac{n-1}{n})}}\overline{0}\right) \dot{+} \left(+\sqrt[n]{b}\right), \left(-\frac{a}{n \cdot b^{(\frac{n-1}{n})}}\overline{0}\right) \dot{+} \left(-\sqrt[n]{b}\right)$$

Maimon and Klein further developed the theory of soft logic in the field of linear algebra to support system thinking [59]. This development is significant to the current research, because the issue of risk management is multi-dimensional and therefore requires the use of matrices. Given that SN $= \left\{a\overline{0} \dot{+} b,\ a, b \in R\right\}$, a soft vector will be: $v = (v_1, v_2, \ldots, v_n) | v_i \in SN$ when $v_i = u_i\overline{0} \dot{+} w_i$. Since a vector is a private case of a matrix, a soft matrix will be:

$$C = \left\{c_{i,j} \middle| c_{i,j} \in SN\right\} \text{when } 1 \leq i \leq n, 1 \leq j \leq m, c_{i,j} = a_{i,j}\overline{0} \dot{+} b_{i,j}$$

The soft matrix C can be represented as two sub-matrices, one with the imaginary parts and the other with the real parts in the form:

$$C = A\overline{0} \dot{+} B = \begin{Bmatrix} a_{1,1} & \cdots & a_{1,m_a} \\ \vdots & \ddots & \vdots \\ a_{n_a,1} & \cdots & a_{n_a,m_a} \end{Bmatrix}\overline{0} \dot{+} \begin{Bmatrix} b_{1,1} & \cdots & b_{1,m_b} \\ \vdots & \ddots & \vdots \\ a_{n_b,1} & \cdots & a_{n_b,m_b} \end{Bmatrix} \quad (2)$$

Note that according to this new definition, the sub-matrices A of the imaginary part ($\overline{0}$) has the dimensions ($n_a \times m_a$), while the sub-matrices B of the real part ($\overline{1}$) has the dimensions ($n_b \times m_b$), and are not necessarily the same size.

Now, the classic operators may be defined on soft matrices. Let $C_1 = A_1\overline{0} \dot{+} B_1$ and $C_2 = A_2\overline{0} \dot{+} B_2$. The additional operator is: $C_1 + C_2 = (A_1 + A_2)\overline{0} \dot{+} (B_1 + B_2)$; and the multiplication is: $C_1 \cdot C_2 = (A_1 \cdot B_1 + A_2 \cdot B_1)\overline{0} \dot{+} B_1 \cdot B_2$.

4. Risk Management with Soft Numbers

4.1. Definitions and Concepts

In the proposed model, a few officials are asked to estimate the risk level of each risk factor. Officials may be project managers from the field, members of the current project team, and so forth, and each official has background factors that rank him or her, e.g., years of seniority. An example of a risk factor is exceeding a budget, and the risk level is indexed by probability, i.e., the odds that a specific risk factor will occur. Each evaluation of the risk level of a specific risk factor may be weighted according to a given function. The risk impact is the cost of a risk factor (if it occurs), and is estimated by the project manager of the specific project or its team. The reason that the impact is not evaluated by foreign officials is that, unlike the risk level, the risk impact is unique to each project.

When a group of officials evaluates the risk level, the bottom-line risk may be the weighted average of the evaluations. While this operator is a logical action, averaging collapses detailed information and may, for example, ignore minority opinions that significantly deviate from the average. At least they should be considered (rather than suppressed by the averaging operation). Therefore, there is a justification to represent the risk with

a soft number, when the overall average risk is described by the $\overline{1}$ component, and the deviation of each participant evaluation is described by the $\overline{0}$ axis. For convenience, the notations are displayed in Table 1.

Table 1. Notations of the model.

Notation	Description
rf_j	risk factor j $(j = 1 \dots k)$
i	official index $(i = 1 \dots n)$
$rl_{i,j}$	risk level of risk factor j according to official i
bf_l	background factor l $(j = 1 \dots m)$
$bf_{i,j}$	background factor l of official i
$f_{WF}(BF_i)$	weighting function
ri_j	risk impact for risk factor j
$R^{\overline{1}}$	overall average risk index
$R^{\overline{0}}$	deviations of risk level

4.2. The Mathematical Model

The set of risk factors is defined by: $RF = \{rf_j\} = \{rf_1, rf_2, \cdots, rf_k\}$ when $(j = 1 \dots k)$. For example in this study, three risk factors are applied: exceeding schedule, exceeding budget, and changes, i.e., $RF = \{Budget, Schedule, Changes\}$. However, the model has the generality that enables the accommodation of any number of factors:

The risk level (probability) for the occurrence of risk factor j (rf_j), according to the estimation of official i $(i = 1 \dots n$, i.e., there are i officials that evaluate the risks) is defined by:

$$RL = (rl_{i,j}) = \begin{matrix} \\ \text{officials} \end{matrix} \begin{matrix} \text{risk factors} \\ \begin{pmatrix} rl_{1,1} & \dots & rl_{1,k} \\ \vdots & & \\ \vdots & rl_{i,j} & \vdots \\ \vdots & & \\ rl_{n,1} & \dots & rl_{n,k} \end{pmatrix} \end{matrix} \tag{3}$$

The officials are ranked according to m background factors, which are defined by: $BF = \{bf_l\} = \{rf_1, rf_2, \dots, rf_m\}$ when $(l = 1 \dots m)$

Thus, the entire official population background factor is given by:

$$BF_i = \{bf_{i,j}\} = \begin{matrix} \\ \text{officials} \end{matrix} \begin{matrix} \text{background factors} \\ \begin{pmatrix} bf_{1,1} & \dots & bf_{1,m} \\ \vdots & \ddots & \vdots \\ bf_{n,1} & \dots & bf_{n,m} \end{pmatrix} \end{matrix} \tag{4}$$

To provide weighting for the evaluation of each official, a weighting function that receives the background factors of an official as parameters must be defined:

$$f_{WF}(BF_i) = f\left(bf_{i,1}, bf_{i,2}, \cdots, bf_{i,m}\right) \quad \text{when}: \quad 0 \le f_{BF}(BF) \le 1 \tag{5}$$

For example, consider one background factor, seniority in project management (years). The higher the seniority is, the higher the participant's weight. This type of classification is commonly discrete, therefore, a possible function may be:

$$f_{WF}(bf_1) = \begin{cases} 0.2 & bf_1 < 5 \\ 0.6 & 5 \le bf_1 < 10 \\ 1 & 10 \le bf_1 \end{cases}$$

Note that $f_{WF}()$ is identical for all participants.

It should be emphasized that the weighting function is not an inherent component of the mathematical model, but a user-defined parameter intended to reflect project-specific judgment. The methodology, specifically the definition of Equation (5), is general enough to accommodate any range of weighting. Therefore, the seniority-based step function presented in this study serves as an illustrative example only, chosen for its simplicity and interpretability. In practice, weights may be determined by domain experts, the project management team, or the project manager, and may reflect organizational policy, contextual knowledge, or multiple background factors.

The risk impact of risk factor j (rf_j) is given by: $RI = \{ri_j\} = \{ri_1, ri_2, \ldots, ri_m\}$.

Note that in this model, the risk impact is a vector because it is set by one official. Now, the overall average risk index for each risk factor can be calculated as the weighted average of the risk level (across all officials) multiplied by the risk impact. The real component ($\overline{1}$) of the soft number describes this average risk:

$$\begin{aligned} R^{\overline{1}} &= \left\{ \overline{rl_{i,j}}_{\forall i \in n,j}(\textit{weighted by} : f_{WF}(BF_i)) \cdot ri_j \right\} = \left\{ \frac{\sum_{i=1}^{n}(rl_{i,j} \cdot f_{WF}(BF_i))}{\sum_{i=1}^{n} f_{WF}(BF_i)} \cdot ri_j \right\} \\ &= \left\{ \frac{\sum_{i=1}^{n}(rl_{i,1} \cdot f_{WF}(BF_i))}{\sum_{i=1}^{n} f_{WF}(BF_i)} \cdot ri_1, \quad \frac{\sum_{i=1}^{n}(rl_{i,2} \cdot f_{WF}(BF_i))}{\sum_{i=1}^{n} f_{WF}(BF_i)} \cdot ri_2, \cdots, \right. \\ &\qquad \left. \frac{\sum_{i=1}^{n}(rl_{i,k} \cdot f_{WF}(BF_i))}{\sum_{i=1}^{n} f_{WF}(BF_i)} \cdot ri_k \right\} \end{aligned} \tag{6}$$

And the deviations of each participant's estimation for each factor from the average risk factor are given by the absolute difference between them, when a threshold T is applied. The purpose of the threshold is to eliminate insignificant differences from the model, and it should be set subjectively in accordance with the project manager's policy. The imaginary component ($\overline{0}$) of the soft number describes the deviation of the risk, therefore, the deviation of each official i for risk factor j (rf_j) is:

$$R^{\overline{0}} = \left(\begin{cases} 0 & \left| rl_{i,j} - \frac{\sum_{i=1}^{n}(rl_{i,j} \cdot f_{WF}(BF_i))}{\sum_{i=1}^{n} f_{WF}(BF_i)} \right| < T \\ \left| rl_{i,j} - \frac{\sum_{i=1}^{n}(rl_{i,j} \cdot f_{WF}(BF_i))}{\sum_{i=1}^{n} f_{WF}(BF_i)} \right| & \textit{otherwise} \end{cases} \right) =$$

$$\begin{pmatrix} \begin{cases} 0 & \left| rl_{1,1} - \frac{\sum_{i=1}^{n}(rl_{i,1} \cdot f_{WF}(BF_i))}{\sum_{i=1}^{n} f_{WF}(BF_i)} \right| < T \\ \left| rl_{1,1} - \frac{\sum_{i=1}^{n}(rl_{i,1} \cdot f_{WF}(BF_i))}{\sum_{i=1}^{n} f_{WF}(BF_i)} \right| & \textit{otherwise} \end{cases} & \cdots & \cdots \\ \vdots & \ddots & \vdots \\ \cdots & \cdots & \begin{cases} 0 & \left| rl_{i,k} - \frac{\sum_{i=1}^{n}(rl_{i,k} \cdot f_{WF}(BF_i))}{\sum_{i=1}^{n} f_{WF}(BF_i)} \right| < T \\ \left| rl_{i,k} - \frac{\sum_{i=1}^{n}(rl_{i,k} \cdot f_{WF}(BF_i))}{\sum_{i=1}^{n} f_{WF}(BF_i)} \right| & \textit{otherwise} \end{cases} \\ . & . & . \end{pmatrix} \tag{7}$$

Note that the matrices $R^{\overline{1}}$ and $R^{\overline{0}}$ are not the same size. $R^{\overline{1}}$ represents the average risk of each risk factor, therefore, it is a vector with dimension (k). On the other hand, $R^{\overline{0}}$ represents the deviations of each participant's estimation of each factor, therefore, it is a matrix with the dimension ($n \times k$). Now, the risk is described by the soft number:

$$R = R^{\overline{1}}\overline{1} \dot{+} R^{\overline{0}}\overline{0} \tag{8}$$

Originally, the soft number was defined in the form $a\overline{0} \dot{+} b\overline{1}$, but we prefer to flip the order for considerations specific to the domain (as explained in the next chapter).

5. The Empirical Study

5.1. The Empirical Study Framework

The empirical study included two ways of assessing the risks: (a) A quantitative-based risk assessment, in which a questionnaire with preset closed questions was circulated among $n = 46$ participants. The risks were assessed based on the participants' answers; and (b) A qualitative-based risk assessment, in which six participants were interviewed. The risks were evaluated with an AI (Artificial Intelligence) automated mechanism. The research was approved by the institutional ethics committee for non-clinical research in humans.

5.2. Data Collection

The qualitative research began with an exploratory phase involving 5 semi-structured interviews with Air Force professionals engaged in classified defense SoS. The participants, including project officers, flight crews, pilots, project managers, and systems engineers, discussed their project experiences, associated risk factors, budget-project schedule relationships, and the impact of various risks on project delays. These interviews were recorded and summarized, followed by content analysis and triangulation to verify the findings. Trustworthiness was ensured by confirming any finding reported by at least three interviewees.

Following the interviews, a survey was designed to further investigate the risk factors affecting defense SoS in the Air Force, aiming to categorize these risks. Initially, a pilot questionnaire was distributed to 10 project management experts, including senior system engineers and a professor of industrial engineering, to gather their feedback. Their input helped refine the survey to its final form. A pilot group then tested this final version, which collected data on the organization's risk management methods, the prevalent risk factors in defense systems, and the characteristics of organizations that successfully mitigate risk.

The quantitative phase of the study involved a sample of $n = 46$ participants, focusing on classified defense SoS in the Air Force. The sample was obtained using a convenience-based and access-constrained strategy due to confidentiality and security restrictions in the defense SoS domain. Data were collected only from projects for which security authorities approved the release of specific non-sensitive information, with identifying details anonymized. The resulting sample reflects accessible cases rather than a random selection of defense SoS projects.

The questionnaire commenced with a consent section that provided an overview of the survey and outlined participant privacy rights. Respondents were then asked to provide demographic information, answer general questions about risk management in the defense sector, and identify the top five risk factors commonly encountered in their projects. This comprehensive approach aimed to deepen the understanding of risk factors within classified defense projects.

5.3. Quantitative-Based Risk Assessment

5.3.1. General Approach of the Quantitative Study

The population of this part of the study included $n = 46$ participants. About 20% of the participants were 20 to 29 years old, 50% 30 to 39 years old, 26% 40 to 49 years old, and 4% were above 50 years old. All participants had an academic degree, in which about 34% had a bachelor's degree, and the remaining a master's degree. The distribution of the seniority in years of the participants is depicted in Figure 1. About 22% were not currently involved in any project, 15% in one project, 15% in two projects, 17% in three projects, and 31% in four or more projects. 63% reported that they are involved in the current project from its beginning, and the remaining were not. 26% reported that they are due to accompany the project to its end, 35% reported that they are not, and 39% that they did not know. About 9% of the projects involved a budget under 50 thousand US$, 5% between 51 and 99 thousand US$, 4% between 100 and 299 thousand US$, 7% between 300 thousand and one million US$, 30% between one million and ten million US$, 30% between 10 and 100 million US$, and 15% involved 100 million US$ or above.

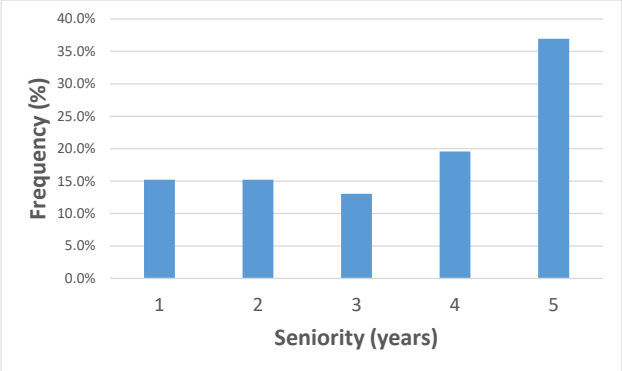


Figure 1. Seniority (years) in the field of the security projects sector.

In this study, participants were asked to rank the five most common risk factors in projects in the defense sector. We set a probability of 20% (low) if the risk factor was not ranked by a participant among the top five leading factors. Conversely, we set a probability of 40% (high) if the risk factor was rated by the participant among the top five leading factors. This method enabled us to quantify the perceived likelihood of each risk factor based on its ranking by the participants. The 20% probability reflects the lower perceived risk for factors not deemed top priorities, while the 40% probability indicates a higher perceived risk for factors considered more significant by the participants. The selection of the bilevel probability ranking is specific to the current empirical study only. However, the methodology has the generality to accommodate any discrete, and even continuous scale, a trait that is supported by the definition of the risk level (probability) for the occurrence of risk factor j (rf_j) according to the estimation of official i (Equation (3)). Naturally, the resolution of this scale will be set by the ability of the measuring means.

For demonstration purposes, we chose to focus on three risk factors: $RF = \{exceeding\ the\ schedule;\ lack\ of\ experience; unplanned\ changes\}$ when ($k = 3$). Since there were $n = 46$ participants (officials), and three risk factors in this study, the dimensions of the risk level matrix RL are (46×3). As mentioned above, the indicator was binary, and by using the transformation, each cell of RL received the values 0.2 or 0.5. The officials were ranked by the background factor of seniority in project management (years) as described in the example that appears in the methodology chapter. The weight sum was 32.4, the average was $\mu = 0.70$, and the standard deviation was $\sigma = 0.32$. The risk impacts RI were set to 25,000, 15,000, and 30,000 US$ for the risk factors exceeding the schedule, lack

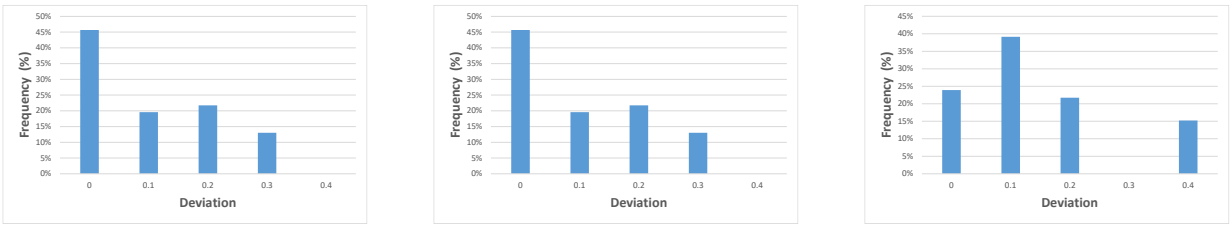
of experience, and unplanned changes, respectively. Note that these values should be set by the project manager uniquely for each project, and are provided here solely for demonstration purposes.

5.3.2. Soft Logic Representation of the Quantitative Study

Now, the overall average risk index matrix $R^{\overline{1}}$ can be calculated based on the risk levels RL and the background factors BF (which are the survey data), and f_{WF} which is set by the project manager according to preferences, and the risk impacts, RI, which are the data provided by the project manager:

$$R^{\overline{1}} = \left\{ \frac{\sum_{i=1}^{46}\left(rl_{i,1}\cdot f_{WF}(BF_i)\right)}{32.4}\cdot 25000, \quad \frac{\sum_{i=1}^{46}\left(rl_{i,2}\cdot f_{WF}(BF_i)\right)}{32.4}\cdot 15000, \quad \frac{\sum_{i=1}^{46}\left(rl_{i,3}\cdot f_{WF}(BF_i)\right)}{32.4}\cdot 30000 \right\}$$
$$= \{8843, 4833, 13056\}$$

The deviations of each participant's estimation for each factor from the average risk factor matrix $R^{\overline{0}}$ may also be calculated. Since the raw value is binary, the threshold T was applied in such a way that the value is 0, and the value of the corresponding element of $R^{\overline{0}}$ will also be set to 0. This matrix has the dimensions (46×3). Consequently, though the detailed data is difficult to visualize, it can be mathematically manipulated. As mentioned above, the importance of this component is the ability to identify "prophet of apocalypse" with a non-popular forecast. For the realization of $R^{\overline{0}}$, the distribution for each risk factor, i.e., the distribution of each column of $R^{\overline{0}}$ is depicted in Figure 2. Each subfigure represents a risk factor where the X axis is the deviation level from the weighted average and the Y axis is the frequency.



(**a**). exceeding the schedule (**b**). lack of experience (**c**). unplanned changes

Figure 2. The distribution of deviations from the average ($R^{\overline{0}}$) of the quantitative-based study.

Now, given the components $R^{\overline{1}}$ which represents the weighted risk average, and $R^{\overline{0}}$ which represents the significant deviations from the average, the comprehensive risk may be presented by the soft number $R = R^{\overline{1}}\overline{1} \dot{+} R^{\overline{0}}\overline{0}$. The risk R may be realized as depicted in Figure 3. The X-axis represents the various risk factors, and the Y-axis represents the deviation. Each bulb center is the deviation, and the bulb size is the number of officials with this deviation. The bottom bulb (glows and has the bold color) is the group of officials who had no significant deviation from the average, i.e., the $R^{\overline{1}}$, while the other bulbs deviate from the average, i.e., the $R^{\overline{0}}$. It is apparent, for example, that due to the lack of experience risk most officials agree with relatively minor deviations, which is not the case for the unplanned changes risk which naturally requires more attention and caution.

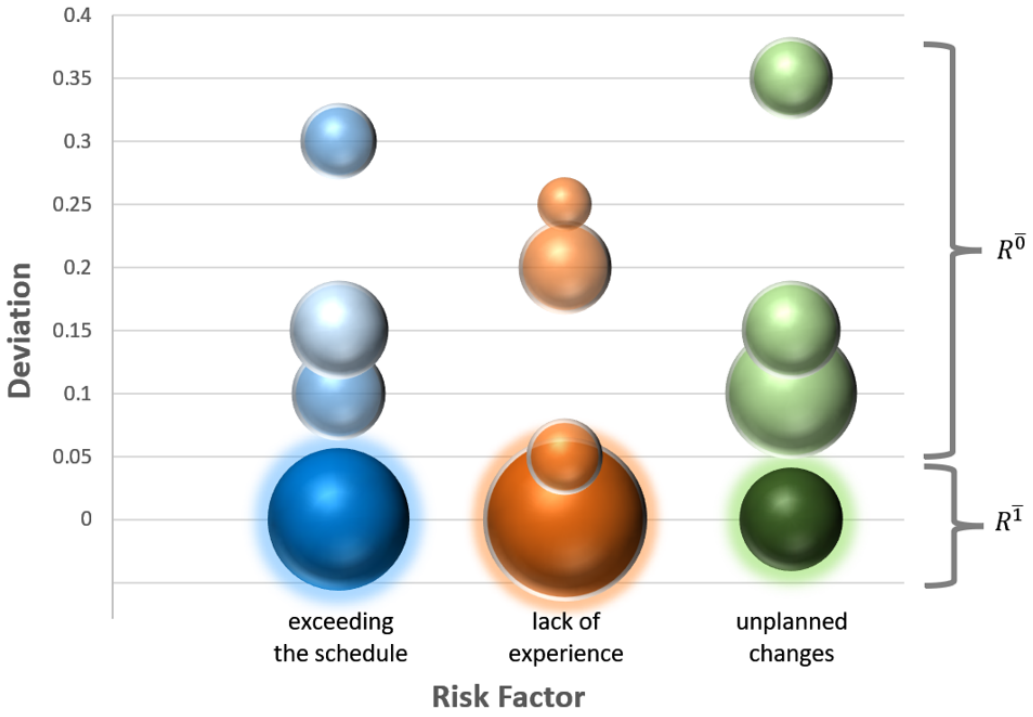


Figure 3. Realization of the soft number that represents the comprehensive risk of the quantitative-based part of the study.

5.4. Qualitative-Based Risk Level Assessment

5.4.1. General Approach of the Qualitative Study

In this study, the risk assessment was based on interviews, which are by nature qualitative measures. All the interviews were semi-structured, and they were recorded, transcribed, and summarized to establish a basis for the analysis. The purpose of these interviews was to gather information to assess risk probabilities in the context of risk management processes. To evaluate these probabilities, both quantitative and qualitative content analysis techniques were meticulously applied to extract different types of risks and to evaluate their magnitude.

Quantitative content analysis included the use of Latent Dirichlet Allocation (LDA) to uncover hidden topics in risk management [60], Latent Semantic Indexing (LSI) to reveal semantic connections among various types of risks [61,62], and the Hierarchical Dirichlet Process (HDP) for dynamic topic discovery [63]. Additionally, K-Means Clustering was used to optimize data clustering, enhancing analytical precision [64]. Term Frequency-Inverse Document Frequency (TF-IDF) measures the frequency of terms within a dataset and compares across interviews to establish their relative importance in the context of risk management and risk probabilities [65]. The Coherence Score further assisted in assessing the semantic consistency among prominent words in a topic, helping to determine the optimal number of topics for analysis [66].

On the qualitative side, content analysis identified recurring risks and themes, highlighting critical concepts and exploring insights related to risk management and risk probabilities, and also focusing on themes mentioned by three or more participants to ensure reliability in the findings. The process to determine risk probabilities involved several stages. First, individual risk probabilities for each interviewee were evaluated. In the second stage, a mind map was created to list and connect the identified risks. In the third stage, risks were grouped into larger categories, enabling a broader perspective. Finally, the last stage involved combining the risk categories into broader, unified themes. Together, these analytical strategies provided a comprehensive examination of the data,

underscoring the importance of effective risk management and demonstrating the value of combining multiple analytical techniques to achieve a holistic understanding of risk management, including the occurrence and probability of different types of risks.

5.4.2. Results

In the first stage, individual risk probabilities for each interviewee were evaluated. This involved analyzing the interviews to identify specific risks, estimating their probabilities, and summarizing the findings. The approach focused on extracting detailed information from each interviewee and assessing the probabilities of various risks based on their experiences and insights. Overall, five interviews were conducted with participants in roles including project officer, end-user, armament officer, integration engineer, and project manager.

Project officers highlighted the integration complexity risk at 70%, with coordination and communication failures posing a 60% probability. Schedule and delay risks due to project complexity and external dependencies constituted a 75% probability. Implicit risks of contractual and bureaucratic challenges had a 50% probability, with change requests potentially causing delays (55%). End-users/operators revealed that the risk of insufficient manpower was high, reaching 80%, with cultural differences contributing a 70% probability. Integration complexity in parallel projects was also at 75%, with implicit communication risks at 65%. Armament department officers indicated a 70% probability of technical surprises, with rigidity in multi-year planning at 70%, and supplier/customer identity impacting risks of 65%. Project managers found that long lead times from subcontractors carried an 80% probability of risk, with client-driven changes contributing to 65%. Budget constraints and manpower limitations had a 60% probability, while organizational flexibility posed a 70% risk. The implicit risk of communication efficacy was 65%. These findings underscore the varied risk landscape in defense and industrial project management, highlighting the need for robust risk assessment and management strategies.

The second stage involved creating a mind map to list and connect the identified risks. This step helped visualize the relationships between different risks and revealed potential patterns. The mind map provided a comprehensive view of all the risks identified throughout the interviews and demonstrated how they were interconnected, facilitating a better understanding and categorization.

The risk categories included project complexity, coordination issues, schedule delays, budget constraints, human resources shortages, supplier relationships, and technical challenges. Integration complexity posed a 75% risk probability, with technical surprises and incomplete testing by the development team contributing 70–75%. Communication failures, including delays with subcontractors, had a 65% risk, while schedule delays due to external factors and changing requirements carried 55–75% risk probabilities. Human resources issues, particularly insufficient staffing, were a significant risk at 80%, with coordination failures due to cultural differences having a 70% probability. Budget flexibility and impact on project progress, coupled with the influence of supplier and client relationships, ranged between 55–70% risk probabilities. Contractual and bureaucratic challenges presented a 50% risk, while delays in log file transfer and validation inefficiencies contributed 55–80% to the risk probabilities. Overall, the mind map highlighted the complex web of risks across defense and technology projects, underscoring the need for robust risk management strategies and proactive mitigation to navigate these challenges successfully.

In the third stage, the risks identified in the mind map were grouped into larger categories. This process aimed to organize similar risks into broader groups, allowing for a more structured analysis. Grouping risks into categories helped to understand overarching themes and the major areas of concern within the risk management process.

The categorization highlighted six major risk areas: manpower and resource allocation, coordination and communication, integration and technical complexity, organizational and cultural factors, schedule and budget risks, and supplier/customer relationship impacts. Manpower-related risks, such as insufficient staffing, held the highest average probability at 80%, indicating a critical vulnerability across various projects. Coordination and communication risks, including stakeholder coordination failures, communication delays with subcontractors, and unclear definitions of expected outcomes, averaged 64%, demonstrating the importance of clear communication channels. Integration and technical complexity, involving technical surprises, incomplete testing, and integration challenges, had the highest average at 71.17%, reflecting the inherent technical complexities of these projects. Organizational and cultural factors, encompassing organizational flexibility and project management efficiency, had a lower average of 53.75%, suggesting that these risks, while notable, might be more manageable. Schedule and budget risks, such as delays due to external factors, budget flexibility, and resource allocation, averaged 58.75%, pointing to the need for careful schedule and budget planning. Finally, supplier/customer relationship impacts, involving the influence of suppliers and bureaucratic challenges, had a 57.50% average, indicating the potential for disruptions from external sources. This structured analysis of risks provides a clearer picture of the main concerns in risk management and highlights areas that require targeted risk mitigation strategies or awareness of the potential of exceeding the project's schedule.

The final stage involved combining the risk categories into broader, unified themes. This step aimed to create a high-level view of the risks and identify common trends across all interviews. Integration complexity risks had varying probabilities among the interviewees, with the project officer and armament officer reporting a 75% risk probability. Others, like the end-user and the project manager, noted probabilities ranging from 65% to 70%. Financial risks followed a similar pattern, with probabilities ranging from 55% to 70%, indicating ongoing concerns about budget and financial stability. Human resources risks were noteworthy, with the project manager indicating a 77% probability, while the integration engineer, project officer, and end-user reported lower probabilities, ranging from 50% to 70%. The different risk probabilities in these categories highlight the varying challenges and areas of concern across defense and technology projects. Table 2 presents the three risk categories and their probabilities of occurrence.

Table 2. Probabilities of occurrence (the risk level) of key risk categories based on the qualitative study.

	Role				
Risk Category	Project Officer	End-User	Armament Officer	Integration Engineer	Project Manager
Integration Complexity	75%	70%	75%	70%	65%
Financial	55%	55%	70%	60%	60%
Human Resources	69%	64%	50%	70%	77%

5.4.3. Soft Logic Representation of the Qualitative Study

As explained above, the risk factors in the qualitative approach study are: $RF = \{Integration\ Complexity;\ Financial; Human\ Resources\}$ where $(k = 3)$. Since there were $n = 6$ participants (officials), and three risk factors in this study, the dimensions of the risk level matrix RL were (6×3) and actually is Table 2 transposed.

For the purpose of demonstration, the officials were ranked by a single factor, yielding a WF_i group (which is the private case, and the equivalent of $f_{WF}(BF_i)$ as mentioned in the

methodology). So, let $WF_i = \{0.7,\ 0.3,\ 0.3,\ 0.6,\ 0.8\}$ for the above roles correspondingly (higher rank was given for a project manager who has a broader view than an end-user, for example). The risk impacts RI were set to 15,000, 50,000, and 30,000 US$ for the integration complexity, financial, and human resources risk factors, correspondingly.

Now, the overall average risk index matrix $R^{\overline{1}}$ can be calculated based on the risk levels RL, the ranking of the participants WF_i, and the risk impacts RI, which is data that is provided by the project manager:

$$R^{\overline{1}} = \left\{ \frac{\sum_{i=1}^{6}\left(rl_{i,1}\cdot f_{WF}(BF_i)\right)}{2.7}\cdot 15000,\quad \frac{\sum_{i=1}^{6}\left(rl_{i,2}\cdot f_{WF}(BF_i)\right)}{2.7}\cdot 50000,\quad \frac{\sum_{i=1}^{6}\left(rl_{i,3}\cdot f_{WF}(BF_i)\right)}{2.7}\cdot 30000 \right\}$$
$$= \{10556, 29630, 20678\}$$

The deviations of each participant's estimation for each factor from the average risk factor matrix $R^{\overline{0}}$, with the dimensions (5×3), may also be calculated. The value of the threshold was set to $T = 0.2$, and the yielded matrix is:

$$R^{\overline{0}} = \begin{pmatrix} 0 & 0.21 & 0.21 \\ 0.49 & 0.43 & 0.5 \\ 0.48 & 0.38 & 0.54 \\ 0.28 & 0.23 & 0.27 \\ 0 & 0 & 0 \end{pmatrix}$$

Now, given the components $R^{\overline{1}}$ which represents the weighted risk average, and $R^{\overline{0}}$ which represents the significant deviations from the average, the comprehensive risk can be presented by the soft number $R = R^{\overline{1}}\overline{1} \dot{+} R^{\overline{0}}\overline{0}$. The risk R can be realized as illustrated in Figure 4, where the interpretation is identical to the one given in Figure 3.

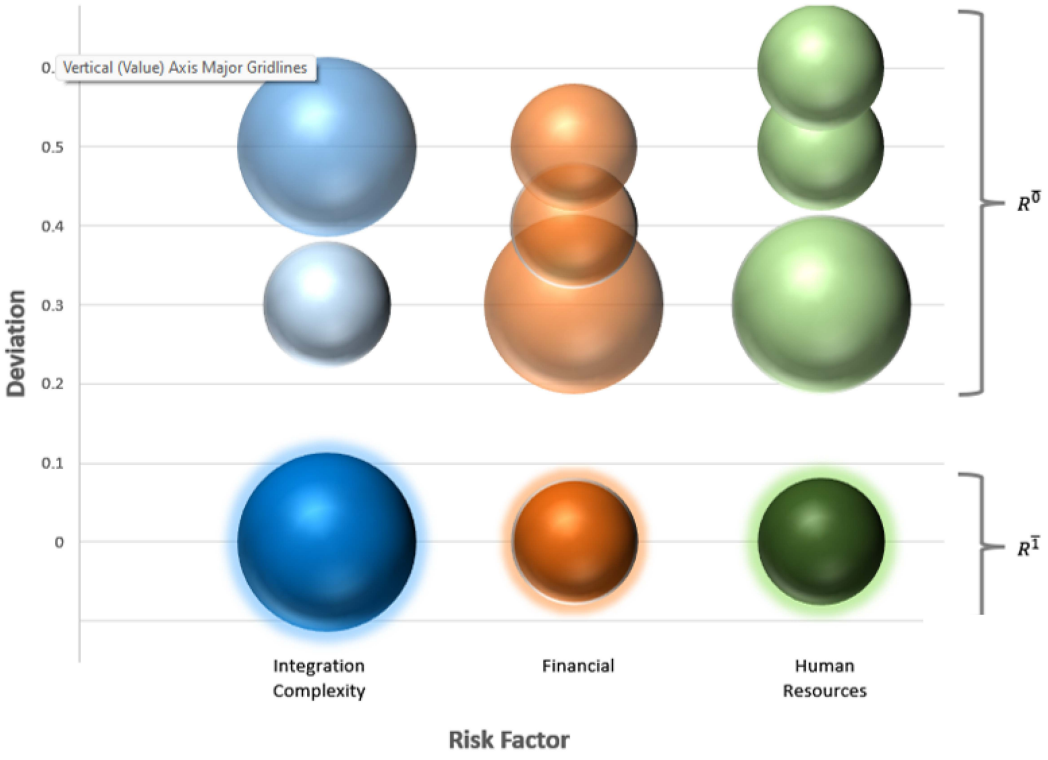


Figure 4. Realization of the soft number that represents the comprehensive risk in the qualitative study.

6. Discussion

Extreme situations such as natural disasters, wars, or pandemics pose unique challenges in project management due to their unpredictable nature and severe consequences. These scenarios require swift, effective responses under conditions of significant uncertainty and stress. Traditional project management and risk assessment methods often fall short in such contexts because they typically rely on predictable patterns and historical data, which might not be applicable or available in unprecedented scenarios [17,67]. For instance, on the day of the Titanic disaster, reports about ice fields and icebergs were indeed delivered to the ship, indicating that the captain and crew were aware of the icebergs in their path. Despite receiving several warnings from other ships that had encountered icebergs that same day, it can be inferred that the crew either did not correctly assess the risk level or decided to continue at high speed despite the warnings [68,69]. This oversight illustrates a critical gap in traditional risk management approaches, particularly in their ability to adapt to real-time, evolving dangers. The implementation of soft logic in risk management, which does not collapse the diversity of assessments into a single value, can help prevent such a disaster.

Recognizing the above-mentioned insights, our study delves into the application of soft logic to risk management in defense SoS, aiming to offer a more adaptable and comprehensive approach to handling complex, interdependent projects. In our study, we explored the application of soft logic to risk management in such projects. The study aims to address the complexity and interdependencies inherent in defense projects by introducing a novel methodology that incorporates both qualitative and quantitative data to provide a more comprehensive risk assessment. We focused on leveraging soft logic to better understand and mitigate risks, particularly those that are often overlooked by traditional risk management approaches. The proposed methodology also utilizes 'weigh experts' assessments, which also consider the seniority trait that is inherent in assorted tasks involving humans. However, while seniors are weighed accordingly, our approach ensures that minority opinions, which could be critical in certain contexts, are not ignored [6].

The literature review underscores several crucial points regarding risk management in defense SoS. While traditional risk management frameworks, such as those outlined in ISO 31000:2018 and PMBOK, offer a robust foundation, they fall short in addressing the distinctive challenges posed by defense projects [9,16]. These projects are characterized by their high complexity, interdependence, and dynamic environments, necessitating more advanced risk management approaches. The literature indicates that traditional methods may not adequately capture the intricate interrelationships among various risk factors, particularly within the context of defense SoS [8,14,45].

The gap that was identified between the existing literature and the requirements of complex SoS defense projects lies in the handling of extreme opinions and uncertainties in risk assessment. While traditional methodologies tend to average out expert opinions, potentially diluting significant insights [14], the current study emphasizes the importance of also considering extreme values and uncertainties. By incorporating soft logic, our methodology addresses this gap by providing a framework that captures a broader range of expert assessments, thereby offering a more comprehensive view of the risks. The current study employs a mixed-method approach, combining both quantitative and qualitative data collection techniques. Quantitative data were gathered by means of a questionnaire, while the qualitative insights were obtained from semi-structured interviews with experts in the field. The risk levels were assessed using a mathematical model based on soft logic, which allows handling both types of data. While the empirical study included two approaches: quantitative (based on questionnaires) and qualitative (based on interviews), by applying the proposed methodology, the results are all quantitative as required by

the risk assessment discipline. The variety of these two approaches has an impact on the applicability of the methodology. Various stakeholders can be directly asked about the evaluated probability for each risk factor, or the probability can be deduced retrospectively by reviewing many projects and analyzing the actual reality of the risks.

Moreover, recent studies highlight that traditional uncertainty analyses in risk assessment often neglect the critical component of causality [70]. This omission can lead to conceptual gaps and misinterpretations of risks, particularly in complex, interdependent projects such as defense SoS. By incorporating causal reasoning through approaches like causal Bayesian networks, risk evaluation can achieve greater transparency and robustness. This aligns with the rationale behind our proposed soft logic methodology, which, like causal approaches, aims to preserve diverse expert opinions and capture complex interrelationships among risk factors rather than collapsing them into a single probability estimate.

Another advantage of the proposed risk representation, and specifically the representation methodology, is that it can be mathematically handled. For example, when a project is a combination of several sub-projects, and each is evaluated separately, a soft number can represent a comprehensive risk model for each sub-project. Given this model, an overall risk analysis of the project can be yielded from these soft numbers. It should be noted that in this study, the risk assessment is aimed at being applied in the *conceptualization* or *planning* phases of the project [71], and thus does not consider computational effort and resources that affect response time. Even if the methodology is applied in the *execution* phase, given the typical project's timeline and task duration, this factor remains irrelevant. However, if the risk assessment is applied in real time, given the high complexity of SoS-relevant data, the response time should be considered. In this case, the issue will be addressed by: (a) providing a sufficient computational resource; and (b) optimizing the algorithm's performances.

In addition to mathematical tractability, the proposed representation addresses documented limitations of traditional risk management approaches and enables different decision-making in defense SoS. This can be attributed to the fact that traditional risk management approaches, commonly applied in defense contexts, were primarily developed for single systems and program-oriented environments. Therefore, these approaches rely on assumptions of relatively stable system boundaries, limited interaction effects, and centralized or unified control. In defense SoS those assumptions often do not hold, as risks frequently arise from interactions between independently managed subsystems, evolve over time, and reflect organizational and coordination challenges rather than isolated technical failures [11,40,45]. Moreover, in defense SoS, risk assessments are inherently heterogeneous due to extensive technological uncertainty, strong interdependencies, and asymmetric loss structures. Under such conditions, aggregation by averaging leads to dimensional collapse, suppressing extreme or minority evaluations that often correspond to rare but high-impact failure modes [14]. In addition, governance in defense SoS is typically distributed across multiple authorities, which further limits the effectiveness of program-level risk assessments [10]. As a result, conventional risk assessment practices, commonly based on static evaluations and scalar prioritization, provide limited support for reasoning about system-level vulnerability, cross-domain dependencies, and situations characterized by divergent expert judgments [70].

The contribution of the proposed soft logic framework lies in its departure from these underlying assumptions at the level of risk representation. Rather than collapsing heterogeneous assessments into a single ranking or deterministic value, the approach offers a mathematically consistent means based on the soft logic capability to represent the coexistence of agreement and disagreement within the same scenario [52]. By representing the risk map as a soft number composed of a weighted central component and an explicit deviation

structure, the model preserves both consensus and disagreement without reduction to a single scalar estimate. This non-collapsing representation enables mathematically tractable risk manipulation while preserving information about dispersion and conflict across expert assessments, addressing limitations of expectation-based risk measures in complex defense environments [13,70]. This representational flexibility is particularly relevant in defense SoS, where differing expert views often signal genuine uncertainty regarding system interactions, non-linear propagation effects, or future operational conditions [45]. By preserving this informational structure, soft logic enables a richer interpretation of risk information, supports decision-making sensitive to system fragility and precautionary considerations, and remains compatible with established risk management practices.

The proposed soft logic formulation is not intended to replace established complex-system risk modeling approaches such as Dependency Structure Matrix (DSM) analysis or system dynamics [72,73]. Instead, it provides a complementary representational layer that can be coupled with these approaches by preserving heterogeneous and potentially conflicting expert risk assessments without collapsing them into a single scalar value [45,52].

While the current study offers a novel approach to risk management, it is not without limitations. The empirical component relies on a relatively small sample, particularly for the interview data, and is therefore not intended to support statistical generalization and formal significance testing. The empirical results are presented to illustrate the applicability and interpretability of the proposed framework rather than to support population-level inference. In addition, the empirical data are based on self-reported questionnaires and interviews rather than on archival project records or historical performance datasets. As such, the findings may be affected by recall bias, subjective interpretation, and social desirability effects. These constraints also reflect practical limitations on accessing detailed historical data in defense SoS projects due to confidentiality and security restrictions. However, while this limitation appears in the current academic empirical study, it does not necessarily apply to the methodology. In real applications, relevant employees within the organization have access to the confidential data.

The reliance on expert opinions, even when using soft logic, can introduce biases based on the experts' experiences and perspectives. Additionally, the application of our methodology in a real-world setting was limited to a specific context within the defense sector, which may affect the generalizability of the findings to other sectors or types of projects. Another aspect is that in the current study, the risk factors are binary, i.e., they can occur or cannot. However, these factors can be levelled, for example, exceeding the schedule might be quantified into one week, one month, six months, etc. This may naturally affect the cost of the risk, and further research can extend the mathematical model to accommodate this aspect as well.

The complexity of soft logic and the mathematical modeling required may also pose challenges for practitioners not familiar with these concepts, and may even introduce a trust issue. While the model is grounded in mathematics, it is hard for the general project management population to grasp. This type of problems is common today in the Artificial Intelligence (AI) era, and may be addressed by means of explainability methods [74]. Exploring ways to simplify mathematical modeling and make it more accessible to practitioners could help broaden its adoption. This challenge can be achieved by constructing a user interface that shields users from mathematical complexity and provides a friendly interface.

Future research should focus on expanding the application of this methodology to domains beyond defense SoS to test its generalizability and effectiveness in different contexts. Another direction is to apply the methodology at the project planning stage and evaluate its effectiveness in light of actual events that occur during the project, i.e., risks

that materialize or do not. To enable a more complete evaluation of effectiveness relative to other established risk assessment approaches, future studies should include controlled comparisons with simpler aggregation schemes (e.g., weighted averaging) and more advanced probabilistic methods (e.g., Bayesian analysis), including the use of control groups. Additionally, exploring hybrid formulations that integrate soft logic with probabilistic inference, as well as the integration of machine learning and advanced artificial intelligence techniques, may further enhance the accuracy and robustness of risk assessments [75]. Longitudinal studies tracking the application of this methodology over project lifecycles could provide deeper insights into its impact on project outcomes.

Author Contributions: Conceptualization, R.S.H. and S.K.; Methodology, R.S.H. and S.K.; Validation, S.K.; Formal analysis, R.S.H. and S.K.; Investigation, R.S.H. and S.K.; Data curation, R.S.H. and S.K.; Writing—original draft, R.S.H. and S.K.; Writing—review & editing, R.S.H. and S.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The anonymous data presented in this study are available upon request from the corresponding author, subject to the requester's approval and a commitment to meet all ethical requirements. These conditions are due to the obligation to preserve participants' privacy and the limitations imposed by the institutional ethics committee.

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

References

1. Hardy, C.; Maguire, S.; Power, M.; Tsoukas, H. Organizing risk: Organization and management theory for the risk society. *Acad. Manag. Ann.* **2020**, *14*, 1032–1066. [CrossRef]
2. Qazi, A.; Quigley, J.; Dickson, A.; Kirytopoulos, K. Project Complexity and Risk Management (ProCRiM): Towards modelling project complexity driven risk paths in construction projects. *Int. J. Proj. Manag.* **2016**, *34*, 1183–1198. [CrossRef]
3. Azmat, Z.; Siddiqui, M. Analyzing Project Complexity, Its Dimensions and Their Impact on Project Success. *Systems* **2023**, *11*, 417. [CrossRef]
4. Gelzer, C. *X-45 Unmanned Combat Air Vehicle (UCAV)*; The Natinal Aeronautics Space Administration (NASA): Washington, DC, USA, 2023.
5. Yang, K.; Dong, W.; Cai, M.; Jia, S.; Liu, R. UCAV Air Combat Maneuver Decisions Based on a Proximal Policy Optimization Algorithm with Situation Reward Shaping. *Electronics* **2022**, *11*, 2602. [CrossRef]
6. Luo, L.; He, Q.; Xie, J.; Yang, D.; Wu, G. Investigating the Relationship between Project Complexity and Success in Complex Construction Projects. *J. Manag. Eng.* **2017**, *33*, 04016036. [CrossRef]
7. Sharma, S.K.; Chanda, U. Developing a Bayesian belief network model for prediction of R&D project success. *J. Manag. Anal.* **2017**, *4*, 321–344. [CrossRef]
8. Shenhar, A.; Dvir, D.; Levy, O. Mapping dimensions of project success. *Proj. Manag. J.* **1997**, *28*, 2–13.
9. Project Management Institute. *A Guide to the Project Management Body of Knowledge*; Project Management Institute: Newtown Square, PA, USA, 2023.
10. The Department of Defense. *Systems Engineering Guide for Systems of Systems*; Office of the Under Secretary of Defense: Washington, DC, USA, 2008.
11. Maier, M. Architecting principles for systems-of-systems. *Syst. Eng.* **1999**, *1*, 267–284. [CrossRef]
12. Hillson, D.; Murray-Webster, R. *Understanding and Managing Risk Attitude*; Taylor & Francis: London, UK, 2017.
13. Aven, T. *Risk Analysis*; John Wiley & Sons: Hoboken, NJ, USA, 2015; pp. 1–27.
14. Raz, T.; Shenhar, A.; Dvir, D. Risk Management, Project Success, and Technological Uncertainty. *RD Manag.* **2002**, *32*, 101–109. [CrossRef]
15. Loskot, P. Bayesian Methods and Monte Carlo Simulations. In *Numerical Simulation—Advanced Techniques for Science and Engineering*; IntechOpen: London, UK, 2022; pp. 57–78.
16. *ISO 31000:2018*; Risk Management—Guidelines. International Organization for Standardization: Geneva, Switzerland, 2018.
17. Wang, Y.; Wan, Y.; Wu, X.; Li, J. Exploring the risk factors of infrastructure PPP projects for sustainable delivery: A social network perspective. *Sustainability* **2020**, *12*, 4152. [CrossRef]

18. Erfani, A.; Cui, Q.; Baecher, G.; Kwak, Y.H. Data-Driven Approach to Risk Identification for Major Transportation Projects: A Common Risk Breakdown Structure. *IEEE Trans. Eng. Manag.* **2024**, *71*, 6830–6841. [CrossRef]
19. Dikmen, I.; Qazi, A. From Risk Matrices to Risk Networks in Construction Projects. *IEEE Trans. Eng. Manag.* **2021**, *68*, 1449–1460.
20. Kovic, M.; Kristiansen, S. The gambler's fallacy fallacy (fallacy). *J. Risk Res.* **2019**, *22*, 291–302. [CrossRef]
21. Boehm, B. Software Risk Management: Principles and Practices. *IEEE Softw.* **1991**, *8*, 32–41. [CrossRef]
22. Deming, W.E. *The PDSA Cycle*; The W. Edwards Deming Institute: Ketchum, ID, USA, 1986.
23. Kliem, R.; Ludin, I. *Reducing Project Risk*; Gower: Farnham, UK, 1997.
24. Fairley, R. Risk Management for software projects. *IEEE Softw.* **1994**, *11*, 57–67. [CrossRef]
25. Nasteckienė, V. Empirical investigation of risk management practices. *Management* **2021**, *26*, 79–98. [CrossRef]
26. Jat, M.; Jajja, M.S.S.; Rehman, A.U.; Farooq, S. Manufacturer's Contexts, Supply Chain Risk Management, and Agility Performance. *IEEE Trans. Eng. Manag.* **2024**, *71*, 4175–4187. [CrossRef]
27. Ye, S.; Tiong, R. NPV-at-risk method in infrastructure project investment evaluation. *J. Constr. Eng. Manag.* **2000**, *126*, 227–233. [CrossRef]
28. Hastak, M.; Shaked, A. ICRAM-1: Model for international construction risk assessment. *J. Manag. Eng.* **2000**, *16*, 59–69. [CrossRef]
29. Wu, Y.; Song, Z.; Li, L.; Xu, R. Risk management of public-private partnership charging infrastructure projects in China based on a three-dimension framework three-dimension framework. *Energy* **2018**, *165*, 1089–1101. [CrossRef]
30. Thomas, A.; Kalidindi, S.; Ganesh, L. Modelling and assessment of critical risks in BOT road projects. *Constr. Manag. Econ.* **2006**, *24*, 407–424. [CrossRef]
31. Toufighi, S.A.F.; Nugroho, Y.K. Risk-based maintenance strategy for oil transfer pipelines. *J. Eng. Des.* **2024**, *35*, 1081–1101. [CrossRef]
32. Mu, J.; Peng, G.; MacLachlan, D. Effect of risk management strategy on NPD performance. *Technovation* **2009**, *29*, 170–180. [CrossRef]
33. Pimchangthong, D.; Boonjing, V. Effects of risk management practices on IT project success. *Manag. Prod. Eng. Rev.* **2017**, *8*, 30–37. [CrossRef]
34. Bannerman, P. Risk and risk management in software projects: A reassessment. *J. Syst. Softw.* **2008**, *81*, 2118–2133. [CrossRef]
35. Oehmen, J.; Olechowski, A.; Kenley, C.R.; Ben-Daya, M. Analysis of the effect of risk management practices on the. *Technovation* **2014**, *34*, 441–453. [CrossRef]
36. De Carvalho, M.; Rabechini, R.J. Impact of risk management on project performance: The importance of soft skills. *Int. J. Prod. Res.* **2015**, *53*, 321–340. [CrossRef]
37. Shafqat, A.; Oehmen, J.; Welo, T. Planning unplanned design iterations using risk managementand learning strategies. *J. Eng. Des.* **2022**, *33*, 120–143. [CrossRef]
38. Jin, X.-H.; Zhang, G. Modelling optimal risk allocation in PPP projects using artificial neural networks. *Int. J. Proj. Manag.* **2011**, *29*, 591–603. [CrossRef]
39. SEBok. *Guide to the Systems Engineering Body of Knowledge (SEBoK), Version 2.2*; The Trustees of the Stevens Institute of Technology: Hoboken, NJ, USA, 2020.
40. Keating, C.; Rogers, R.; Unal, R.; Dryer, D.; Sousa-Poza, A.; Safford, R.; Peterson, W.; Rabaldi, G. Systems of Systems Engineering. *Eng. Manag. J.* **2003**, *15*, 36–45. [CrossRef]
41. Gorod, A.; Sauser, B.; Boardman, J. System-of-Systems Engineering Management: A Review of Modern History and a Path Forward. *IEEE Syst. J.* **2008**, *2*, 484–499. [CrossRef]
42. Shenhar, A.; Sauser, B. Systems engineering management: The multidisciplinary discipline. In *Handbook of Systems Engineering and Management*, 2nd ed.; Wiley: New York, NY, USA, 2008.
43. Agmon, N.; Kordova, S.; Shoval, S. Global Quality Management System (G-QMS) in Systems of Systems (SoS)—Aspects of Definition, Structure and Model. *Systems* **2022**, *10*, 99. [CrossRef]
44. *ISO/IEC/IEEE 21839:2019*; Systems and Systems of Software Engineering—System of Systems (SoS) Considerations in Life Cycle Stages of a System. International Organization for Standardization: Geneva, Switzerland, 2019.
45. Kordova, S.; Fridkin, S. Risk Management for Defense SoS in a Complex, Dynamic Environment. *Sustainability* **2021**, *13*, 1789. [CrossRef]
46. Bennett, F. The Seven Deadly Risks of Defence Projects. *Secur. Chall.* **2010**, *6*, 97–111.
47. Anton, S.G.; Nucu, A.E.A. Enterprise risk management: A literature review and agenda for future research. *J. Risk Financ. Manag.* **2020**, *13*, 281. [CrossRef]
48. Monazzam, A.; Crawford, J. The role of enterprise risk management in enabling organisational resilience: A case study of the Swedish mining industry. *J. Manag. Control* **2024**, *35*, 59–108. [CrossRef]
49. Riepl, J.; Mitter, C.; Kuttner, M. Risk management during the COVID-19 crisis: Insights from an exploratory case study of medium-sized family businesses. *J. Manag. Control* **2024**, *35*, 109–135. [CrossRef]

50. Burstein, G.; Zuckerman, I. A Structured Causal Framework for Operational Risk Quantification: Bridging Subjective and Objective Uncertainty in Advanced Risk Models. *Mathematics* **2025**, *13*, 2467. [CrossRef]
51. Shi, Y.; Tian, S.; Chen, Y.; Cai, C.; Guan, H.; Li, X. Assessment Method of Railway Engineering Technology Innovation in Complex Areas. *Mathematics* **2025**, *13*, 1970. [CrossRef]
52. Klein, M.; Maimon, O. Fundamentals of soft logic. *New Math. Nat. Comput.* **2021**, *17*, 703–737. [CrossRef]
53. Hirschprung, R.S.; Klein, M.; Maimon, O. Harnessing Soft Logic to Represent the Privacy Paradox. *Informatics* **2022**, *9*, 54. [CrossRef]
54. Klein, M.; Maimon, O. Axioms of Soft Logic. *p-Adic Numbers Ultrametric Anal. Appl.* **2019**, *11*, 205–215. [CrossRef]
55. Kinzer, C.J.; Stanford, T. The distributive property: The core of multiplication. *Teach. Child. Math.* **2013**, *20*, 302–309. [CrossRef]
56. Clifford, M. Preliminary Sketch of Biquaternions. *Proc. Lond. Math. Soc.* **1871**, *s1-4*, 381–395. [CrossRef]
57. Hahn, L.-S. Definition of Complex Numbers. In *Complex Numbers in Geometry*, 1st ed.; Cambridge University Press: Cambridge, UK, 1994; p. 33.
58. Herstein, I.N. Finite Abelian Groups. In *Topics in Algebra*; John Wiley & Sons: Hoboken, NJ, USA, 1991.
59. Hirschprung, R.S.; Kordova, S.; Klein, M.; Maimon, O. Representation and Assessment of Systems Thinking Competencies through Soft Logic. *IEEE Access* **2023**, *11*, 141547–141558. [CrossRef]
60. Blei, D.M.; Ng, A.Y.; Jordan, M.I. Latent dirichlet allocation. *J. Mach. Learn. Res.* **2003**, *3*, 993–1022.
61. Foltz, P.W. Using latent semantic indexing for information filtering. *ACM Sigois Bull.* **1990**, *11*, 40–47. [CrossRef]
62. Deerwester, S.; Dumais, S.T.; Furnas, G.W.; Landauer, T.K.; Harshman, R. Indexing by latent semantic analysis. *J. Am. Soc. Inf. Sci.* **1990**, *41*, 391–407.
63. Teh, Y.W.; Jordan, M.I.; Beal, M.J.; Blei, D.M. Hierarchical Dirichlet Process. *J. Am. Stat. Assoc.* **2006**, *101*, 1566–1581. [CrossRef]
64. Lloyd, S. Least squares quantization in PCM. *IEEE Trans. Inf. Theory* **1982**, *28*, 129–137. [CrossRef]
65. Jones, K.S. A statistical interpretation of term specificity and its application in retrieval. *J. Doc.* **1972**, *28*, 11–21. [CrossRef]
66. Mimno, D.; Wallach, H.M.; Talley, E.; Leenders, M.; McCallum, A. Optimizing semantic coherence in topic models. In Proceedings of the 2011 Conference on Empirical Methods in Natural Language Processing, Edinburgh, UK, 27–31 July 2011.
67. Kaplan, R.; Mikes, A. *Managing Risks: A New Framework*; Harvard Business Review: Brighton, MA, USA, 2012.
68. Bigg, G.R.; Wilton, D. Iceberg risk in the Titanic year of 1912: Was it exceptional? *Weather* **2014**, *69*, 100–104. [CrossRef]
69. Howells, D. The maiden voyage of the titanic—A meteorological perspective. *Weather* **1992**, *47*, 417–423.
70. Neil, M.; Fenton, N.; Osman, M.; Lagnado, D. Causality, the critical but often ignored component guiding us through a world of uncertainties in risk assessment. *J. Risk Res.* **2021**, *24*, 617–621.
71. Ward, S.C.; Chapman, C.B. Risk-management perspective on the project lifecycle. *Int. J. Proj. Manag.* **1995**, *13*, 145–149. [CrossRef]
72. Eppinger, S.; Browning, T. *Design Structure Matrix Methods and Applications*; The MIT Press: Cambridge, MA, USA, 2016.
73. Sterman, J. *Business Dynamics: Systems Thinking and Modeling for a Complex World*; McGraw Hill: New York, NY, USA, 2000.
74. Ferrario, A.; Loi, M. How explainability contributes to trust in AI. In Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency, Seoul, Republic of Korea, 21–24 June 2022.
75. Hegde, J.; Rokseth, B. Applications of machine learning methods for engineering risk assessment—A review. *Saf. Sci.* **2020**, *122*, 104492. [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.