

Risk Management for Defense Systems in a Complex, Dynamic Environment

Sigal Kordova

Ariel University, Department of Industrial Engineering and Management, Ariel, Israel
sigalko@ariel.ac.il

Abstract: Identifying and assessing risk is one of the most important processes in managing complex systems and requires careful consideration. The need for an effective, efficient approach to risk management is considerably more important for defense projects based on systems of systems (SoS), because they are exposed to risk already in early stages of development. This paper uses advanced data science tools to present the complexity of the risk factors relevant to defense systems, and proposes a methodology for identifying, analyzing and monitoring the risks that they face.

Findings from an in-depth analysis of 46 classified defense projects based on SoS shows a need to focus on three main risks faced by defense projects: uncertainty, the lack of clearly defined goals, and managing a system under constrained conditions. The paper also presents some recommendations for minimizing risk factors in SoS for defense projects.

Key words: Risk management; Defense systems; System of Systems (SoS)

1. Introduction

Risk management is one of the most important areas that must be considered when managing defense projects based on systems of systems (SoS). All systems have some level of inherent risk because of the uncertainty that accompanies any new endeavor. In defense industries, the riskier the system, the higher the payoff. Thus, risk is sometimes beneficial because it has the potential to increase profits.

SoS projects for defense develop sophisticated systems to meet challenges on the battlefield. Therefore, their successful management requires functioning in a dynamic, rapidly-changing reality, in which risk assessment and prioritization may present complex challenges.

The current paper presents an ongoing study examining risks faced by classified defense projects using SoS. The findings can help project managers and systems engineers of these and similar projects minimize delays and reduce risks.

2. Literature Review

The Project Management Institute includes risk management as a key process defined in the Project Management Body of Knowledge (PMBOK). Project Risk Management includes the following processes: conducting risk management planning, identification, analysis, response planning and risk control. The objectives of project risk management are to increase the likelihood and impact of positive events, and decrease the likelihood and impact of negative events in any given project [1].

The literature includes several suggestions for describing the process of risk management. For example, Fairley [2] presents seven steps: (1) Identify risk factors; (2) Assess risk probabilities and effects; (3) Develop strategies to mitigate identified risks; (4) Monitor risk factors; (5) Invoke a contingency plan; (6) Manage the crisis; (7) Recover from the crisis.

Boehm [3] described a process with two main phases: risk assessment, which includes identification, analysis and prioritization, and risk control, which includes risk management planning, risk resolution and risk monitoring planning, tracking and corrective action. Similar to Deming's quality improvement cycle (Plan, Do, Check, Act), Kliem and Ludin [4] suggested a four-phase process (identification, analysis, control and reporting). According to ISO 31000 risk management creates and protects value [5].

Several popular risk management analysis techniques have been reported in the literature, including Monte Carlo Simulation [6], Analytical Hierarchy Process [7, 8] and Fuzzy Set Theory [8, 9]. There is much evidence in the literature that using risk management tools when managing a project creates value for its outcome and success [10-12]. On the other hand, some researchers did not find any effect [13] or found that the effect was negligible [14, 15]. Moreover, many studies are dedicated to the application of project management in specific sectors, so the practices and techniques they present are not necessarily applicable to risk management of projects in other fields [16-27].

The identification of risk factors might be influenced by the sector and area of the project. For example, the key risk factors of public-private partnership (PPP) projects are divided into two categories, the first includes risk factors that have powerful, independent influences, such as delays in government approval, government credit, and imperfect legal and regulatory systems. The second category includes risk factors that are highly variable and easily influenced, such as completion risks, insufficient revenue in the market, and fee changes [28].

Ameyaw and Chan [29] mention others risks factor such as market/revenue risks, financial risks, relationship risks and social risks. According to Lessard [30], risk management requires systematic management of risks that are generated within each link in the chain and, more

importantly, in the interfaces among links in order to limit disruptions and their propagation throughout the system. Effective management of risk, therefore, requires a systems thinking approach—understanding how systems influence one another within a whole.

According to Naaman [31], the risk management process has become an inseparable part of management procedures for defense projects, for which uncertainty management is one of the main challenges of ongoing project planning and management. Moreover, in response to dangerous events, such as plane crashes or take-off failures, safety requirements in the defense industry are strict, rigorous and demanding.



Figure 1. Impact of variables, based on project time

Figure 1 shows that, at the beginning of the project, the cost of changes is low; costs go up the more the project advances. At the same time, we can see that the effect of uncertainty and risk at the beginning of the project is higher; the more the project advances, the more these values decrease [1].

There are two types of uncertainty in defense projects:

1. Uncertainty that can be predicted in advance: It is possible to cope with this type of uncertainty by using an organized methodology, as presented in PMBOK [1]. For every stage of the project, there is an organized process that includes determining the project's leading players, and defining inputs and outputs. Risks that stem from uncertainty may be managed making a plan to minimize them.
2. Uncertainty that cannot be predicted in advance: In response to this possibility, buffers are defined in the schedule, the budget and Statement of Work (SOW), which provide leeway for dealing with unexpected changes.

According to ISO standards [5], there are certain limitations on projects managed under constraints such as timeframes for project completion, human resources, and activities that are dependent on the results of other activities. Wang [32] defined risk as a factor or action that might occur unexpectedly and, as a result, cause physical harm, damage assets or delay the timetable.

Risk is measured according to the likelihood of occurrence; the technical, programming or managerial level; and the amount of potential damage that could result from the failure to prevent its occurrence.

Engineering projects are frequently characterized by extensive scope and budget; in many cases, they include manufacturing for a specific customer according to specific needs. These characteristics intensify the importance of the risk management process, because every unplanned event that occurs, which was not considered from the outset, could potentially have significant effects on project's success and compliance with requirements [33].

According to Naaman [31], the risk management process in defense projects includes five stages:

1. Identifying risks using brainstorming
2. Analyzing the meaning and level of each risk, including assessments of severity, probability and risk level
3. Risk factor analysis and defining responses, including a contingency plan
4. Risk presentation for authorization purposes
5. Monitoring and re-measuring the risk includes ongoing risk supervision

The US Department of Defense [34] defined risk management as an interactive process, as shown in Figure 2.

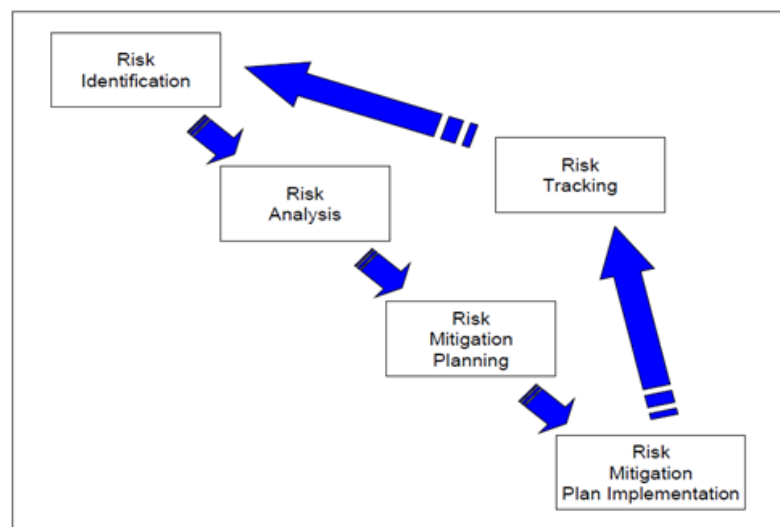


Figure 2. Risk management process according to the DoD

The PMBOK [1] presents six ways to cope with project risks, which are similar for many types of projects:

1. Risk Survey – the goal of a risk survey is to reach an agreement about the risk level and ways to cope with each risk factor
2. Preemptive Action – to be carried out in advance, usually at the earliest possible stage, with the goal of minimizing occurrence of the risk to the lowest possible level
3. Mitigation Action – an action that should be carried out immediately upon the occurrence of a risk, with the goal of minimizing the extent of the damage caused
4. Corrective Action – an action that must be carried out after the risk occurs, with the goal of returning the situation to its pre-risk state

5. Transferring the Risk – transferring responsibility for the risk and its treatment to another party
6. Accepting the Risk – taking a calculated risk, and deciding not to take any action

Chris and Stephen [35] write that for every activity in a project, it is necessary to clearly define who is responsible, create a work schedule, and make sure to integrate them into the work plan. Risk must be managed throughout the entire project's lifespan in order to reduce the effects of the risks on meeting the project's targets at all stages, including its conclusion. In engineering projects, responsibility for the risk management process is usually shared by two individuals: the systems engineer and the project manager [36-38].

Kordova, Katz and Frank [39] studied the management processes shared by project managers and systems engineers in the defense industry, and provided recommendations for joint project management that leads to project success. Figure 3 shows the division of responsibility for risk management between the systems engineer and the project manager, and how their efforts mesh.

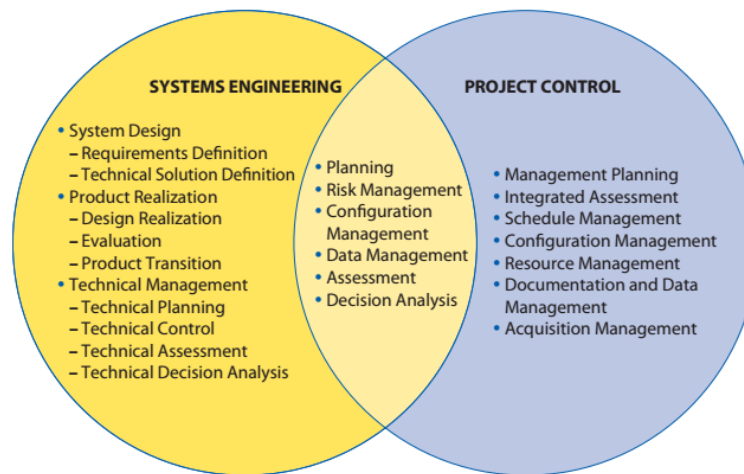


Figure 3. Overlaps between systems engineering and project management

According to Kordova, Katz and Frank [39], project risks include management-related risks (e.g., cost or organizational expenses), as well as technical/engineering risks (e.g., specifications, performance demands, and premature technology). During the project, there are joint discussions about risks, they are ranked, and a risk minimization plan is developed. Project managers usually integrate all risks, while systems engineers are generally responsible for identifying and managing only technical risks. However, technical risks often have managerial consequences, because risk minimization plans generally include the allotment of resources (schedule/budget) that are managed by the project manager.

The projects analyzed in the current paper are all defense projects that developed classified system of systems (SoS). SEBok [40] defines SoS as a set of systems or system elements that interact to provide a unique capability that none of the constituent systems could accomplish on its own. A similar definition was previously suggested by Maier [41], who defined SoS as a collection of task-oriented systems that pool their resources and capabilities to create a new, more complex system that offers additional functionality and performance beyond simply the sum of the constituent systems.

3. Methodology and Research Design

The research paradigm combines analytical, quantitative and qualitative methods, as presented in figure 4. The qualitative research started as an exploratory study. The analytical component included assessing both primary (testimony of engineers and project managers that were involved in the classified projects) and secondary (literature) sources. The quantitative component included data collection of 46 classified defense projects for developing SoS.

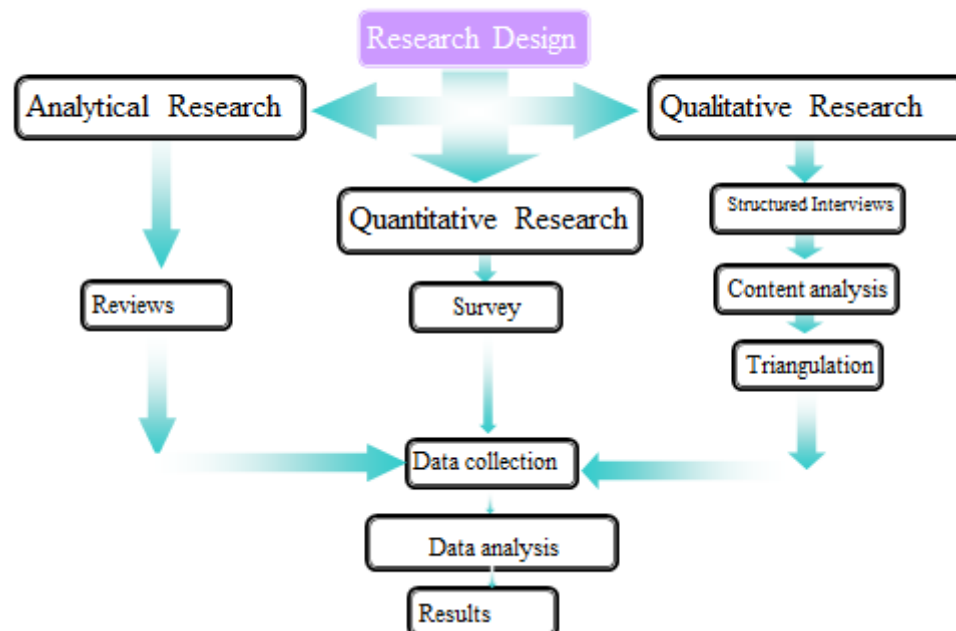


Figure 4. The research design

3.1 The exploratory stage

The qualitative research started as an exploratory study, consisting of 10 semi-structured interviews with professionals who participated in classified defense projects for developing SoS in the Air Force. The interviewees included project officers, flight-crews, pilots, project managers and systems engineers, who were asked about the projects they participated in and these projects' risk factors; the association between project budget and the extent of deviation from the planned schedule; as well as the connection between different risk factors and project scheduling delays. After recording and summarizing the interviews, a triangulation process was conducted, confirming that each finding presented in the report was mentioned by three or more interviewees, to ensure trustworthiness.

3.2 The survey

Based on results from the interviews, a survey was developed to examine the risk factors faced by SoS projects for defense purposes. Its goal was to determine the segmentation of risk factors for these projects, and examine the correlations between different risk factors and project schedule variations.

A pilot questionnaire was first distributed to 10 experts in project management, including senior systems engineers and a professor of industrial engineering, for their evaluation. Based on

their responses and comments, a final version of the survey was created and validated. The data collected by the survey included the organization's risk management methodology, the most common risk factors in defense projects and the main characteristics of organizations that manage to avoid occurrence of risks.

4. Results

4.1 Findings of the exploratory study(interviews)

The risk factors faced by defense projects, as reported by the interviewees and confirmed by the triangulation process, are:

1. The quality and quantity of human resources are critical factors in the development process; an insufficient workforce is a significant risk in the defense industry.
2. The dynamics of defense industries often makes it necessary to shorten the Time-To-Market, even though development processes are usually very time consuming.
3. Too many stakeholders are involved, influence one another, in addition to many parties from external companies working on the project and interdependent on one another.
4. Additions to the Statement of Work (SoW) and/or changes to the project's initial design.
5. The tendency to change roles/jobs once every 2-3 years in the military may create a sense of partial commitment, and an "until the end of my term" attitude towards the project. This may also cause project managers to commit to challenging SoWs and schedules.
6. The bigger the project's budget, the more the potential risks.
7. The risks that cause schedule delays can be divided into two types: insufficient planning/management and resources constraints (mainly workforce and budget-related).

4.2 Findings from the Survey

The first step in analyzing the survey was to identify the common risk factors faced by the defense projects (N = 46), which are:

1. Overly-optimistic scheduling assessment
2. Insufficient human resources
3. Changes in the original specifications
4. Lack of other (non-human) resources
5. Overlap between different project processes
6. Too many stakeholders influencing the project
7. Lack of project participants' previous experience
8. R&D required in a new field/area
9. Failure to maintain risk management processes
10. Cultural differences among project members
11. -15. Other (project manager lacks previous experience, gap in knowledge management etc.)

Figures 5 and 6 present the histogram and frequencies of the risk factors, respectively.

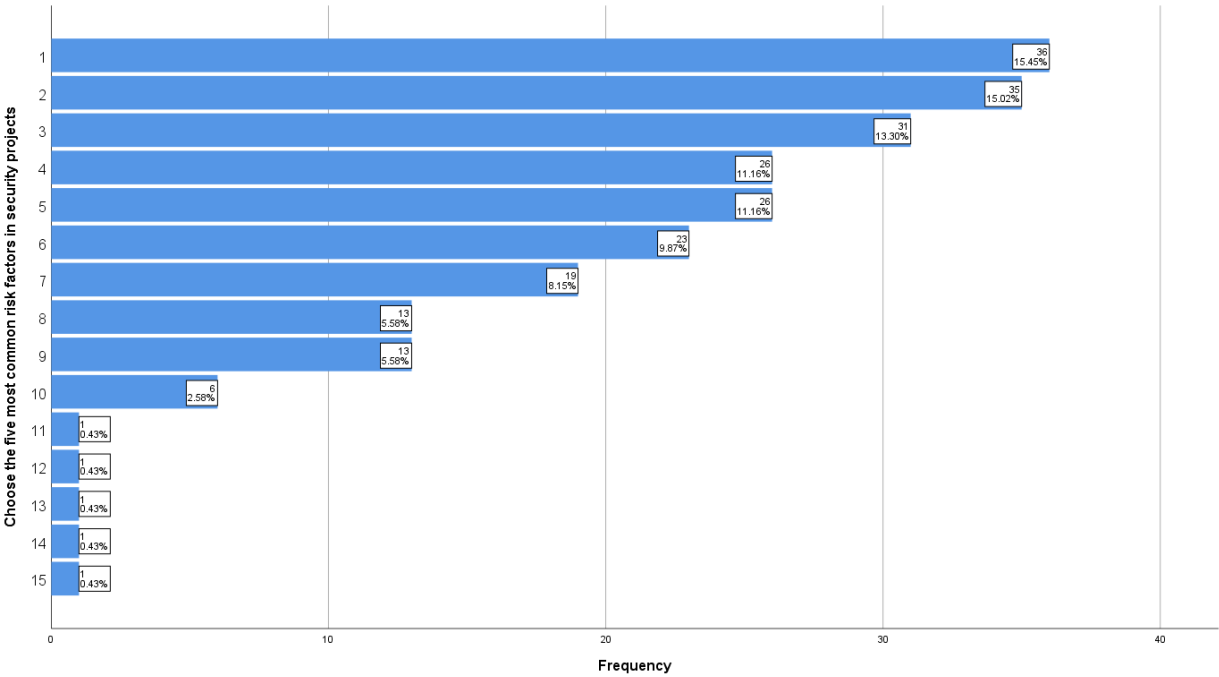


Figure 5. Histogram of risk factors faced by 46 defense projects

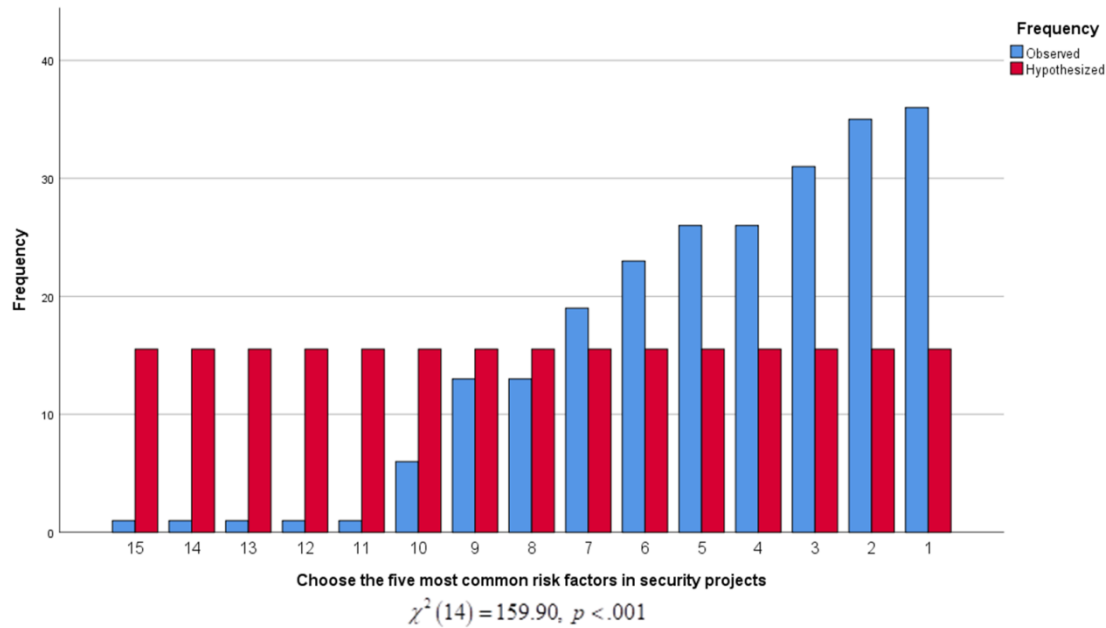


Figure 6. Frequency of risk factors faced by 46 defense projects

According to Figures 5 and 6, the five most common risk factors faced by the defense projects surveyed were: overly-optimistic scheduling assessment, insufficient human resources, changes in the original specifications, lack of other (non-human) resources, and overlap between project processes.

The second step was to use the Decision Tree procedure to create a tree-based classification model. The tree model categorizes cases into groups of predictive value of independent variables for the dependent variables (risk factors). For example, the model, shown in figure 7 below, examines the common influence of the items clusters of 19, 20, 22, 25 on item 31.

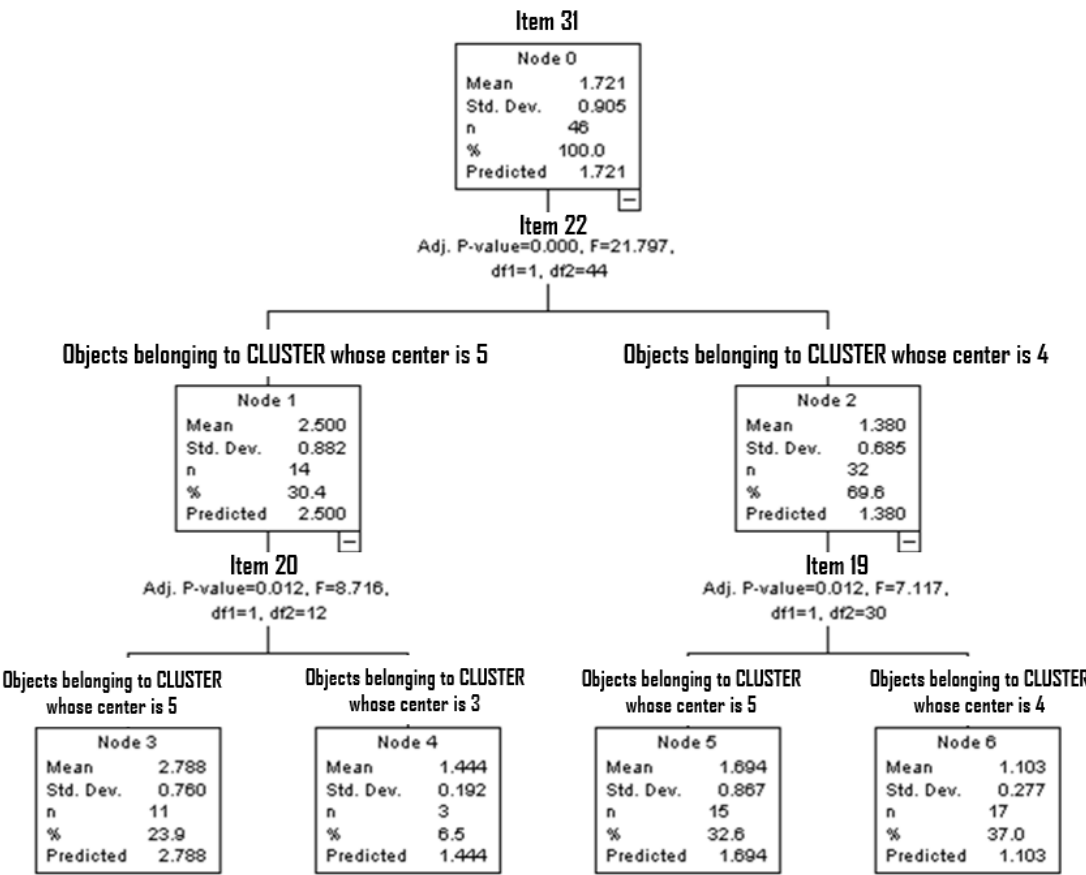


Figure 7: Tree based classification model

In this tree:

- Item 31: Schedule Variation of the project (SV)
- Item 19: The impact of insufficient human resources on risk occurrence
- Item 20: The impact of project stakeholders involvement on risk occurrence
- Item 22: The impact of overly-optimistic schedule assessment on risk occurrence
- Item 25: The impact of the project's organizational structure on risk occurrence.

According to the tree-based classification model, there is a significant difference in the influence of cluster 4 and cluster 5 on item 22 (overly-optimistic schedule assessement). The average score of overly-optimistic schedule assessement for cluster 5 is 2.5 (out of 5), while the average score of overly-optimistic schedule assessement for cluster 4 is only 1.38 (out of 5). This means that for higher clusters in item 22, schedule variation is higher, which reinforces the impact of overly-optimistic schedule assessment on risk occurrence in general and on schedule variation in particular.

The model shows a significant difference in the influence of cluster 5 and cluster 3 on item 20 (project stakeholders involvement). The average score of project stakeholders' involvement for cluster 5 is 2.78 (out of 5), while the average score of project stakeholders involvement for cluster 3 is only 1.44 (out of 5). This means that for higher clusters in item 20, schedule variation is higher, which reinforces the impact of project stakeholders' involvement on risk occurrence in general and on schedule variation in particular.

The model also shows a significant difference in the influence of cluster 5 and cluster 4 on item 19 (insufficient human resources). The average score of insufficient human resources for cluster 5 is 1.59 (out of 5), while the average score of insufficient human resources for cluster 4 is only 1.1 (out of 5). This means that for higher clusters in item 19, schedule variation is higher, which reinforces the impact of insufficient human resources on risk occurrence in general and on schedule variation in particular.

The third step in analyzing the survey was to explore the relationships between several explanatory variables and one or more response variables by using Response Surface Methodology (RSM). We used RSM in the current study primarily in order to obtain a sequence of designed experiments that could yield an optimal response. One example of how we used RSM is presented in Figures 8 and 9.

Estimated Means:		Item 19 * Item 20			
		Target: Item 31			
		Estimates			
Item 19	Item 20	Mean	Std. Error	95% Confidence Interval	
				Lower	Upper
Objects belonging to CLUSTER whose center is 5	Objects belonging to CLUSTER whose center is 5	2.190	0.153	1.880	2.501
	Objects belonging to CLUSTER whose center is 3	1.712	0.116	1.475	1.949
Objects belonging to CLUSTER whose center is 4	Objects belonging to CLUSTER whose center is 5	1.380	0.221	0.930	1.829
	Objects belonging to CLUSTER whose center is 3	1.191	0.055	1.079	1.303

		Pairwise Contrasts						
Item 20	Item 19 Pairwise Contrasts	Contrast Estimate ▼	Std. Error	t	df	Adj. Sig.	95% Confidence Interval	
							Lower	Upper
Objects belonging to CLUSTER whose center is 5	Objects belonging to CLUSTER whose center is 5 - Objects belonging to CLUSTER whose center is 4	0.811	0.276	2.939	33	0.006	0.249	1.372
	Objects belonging to CLUSTER whose center is 4 - Objects belonging to CLUSTER whose center is 5	-0.811	0.276	-2.939	33	0.006	-1.372	-0.249
Objects belonging to CLUSTER whose center is 3	Objects belonging to CLUSTER whose center is 5 - Objects belonging to CLUSTER whose center is 4	0.521	0.129	4.029	33	0.000	0.258	0.784
	Objects belonging to CLUSTER whose center is 4 - Objects belonging to CLUSTER whose center is 5	-0.521	0.129	-4.029	33	0.000	-0.784	-0.258

Significant contrasts are shaded gold. The least significant difference adjusted significance level is .05.

Overall Test Results				
Item 20	F	df1	df2	Sig.
Objects belonging to CLUSTER whose center is 5	8.637	1	33	0.006
Objects belonging to CLUSTER whose center is 3	16.234	1	33	0.000

Figure 8: Response Surface Methodology (RSM)

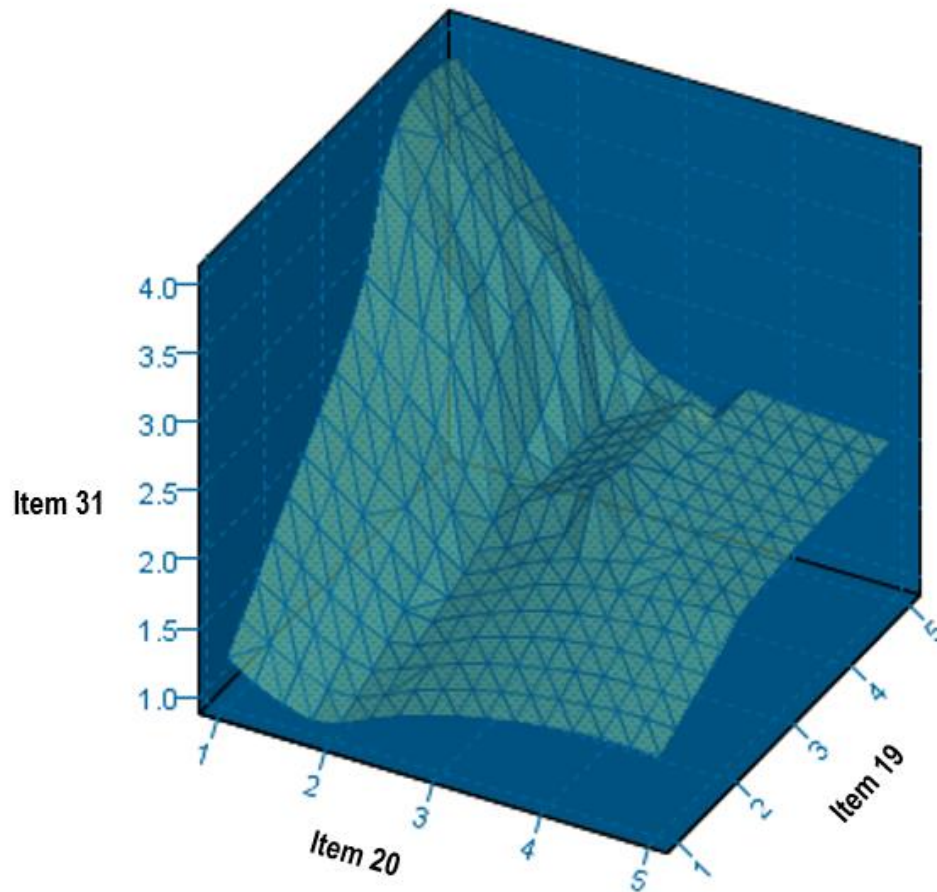


Figure 9: Interaction between items 19, 20, 31

Figures 8 and 9 show the interaction between items 19, 20 and 31. According to Figure 9, a low level of project stakeholders involvement (item 20) and a high level of human resources shortage (item 19) characterize a high level of schedule variation in a project (item 31). This finding supports the impact of a insufficient human resources, and the lower the impact of project stakeholders involvement on risk occurrence.

Step 4 of the survey analysis used advanced data science analysis tools such as Bayesian SEM Path analysis and IBM Watson Analytics analysis. The preliminary results of the data science analysis are shown in Figures 10-13.

Figures 10 and 11 rank the most common risk factors in defense projects, which are:

1. Lack of resources
2. Insufficient human resources
3. Overly-ptimistic scheduling assessment
4. Project members' lack of experience
5. Failure to maintain risk management processes
6. Too many stakeholders influencing the project
7. Coupling of separate project processes
8. Changing in the original project design
9. Requiring R&D for a new field/area
10. Cultural differences among project members

11. Other (project manager lacks previous experience, gap in knowledge management etc.)

Figure 10 presents the percentage of each risk factor; Figure 11 shows the graphical segmentation of the risk factors. The survey findings show that the most common causes of risk in defense projects are insufficient resources, changes in the initial project design, coupling of processes, overly-optimistic scheduling, and too many involved parties.

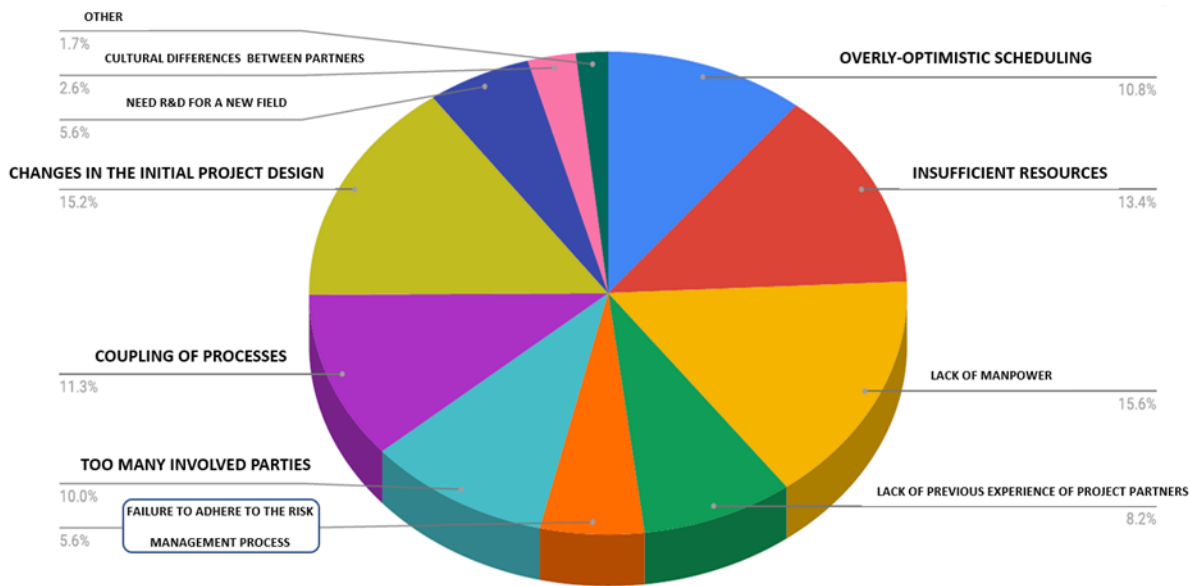


Figure 10: Segmentation of defense projects’ risk factors

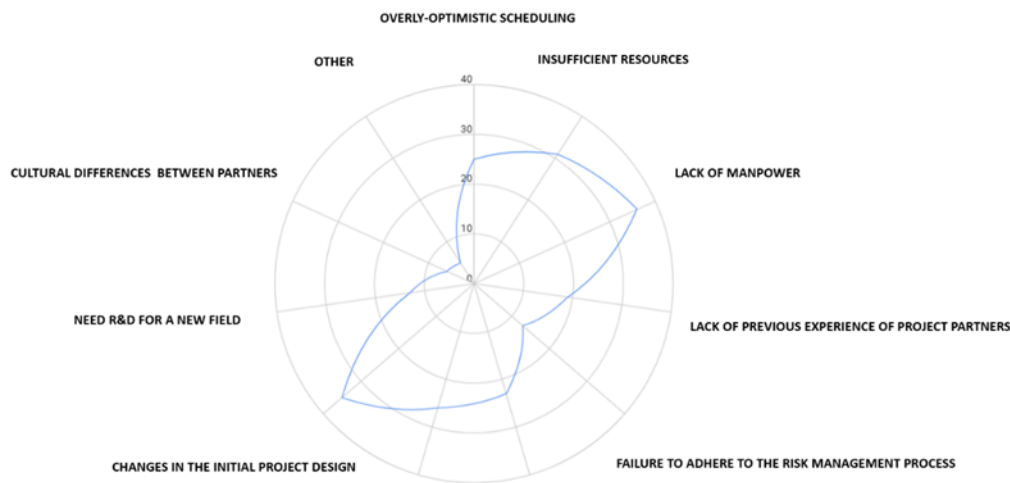


Figure 11: Graphical segmentation of risk factors

Figures 12 and 13 present the main characteristics of defense organizations that are able to avoid risks occurrence, which include:

1. Transparent risk management methodology
2. Makes a point of adhering to its risk management policy
3. Mandatory methodology for project management processes

- 4. Managers maintain control of risk management processes
- 5. Ensures the allocation of resources in order to minimize risks
- 6. Provides risk management training
- 7. The organization implements processes for managing and storing of knowledge
- 8. Synchronization between departments within the organization,
- 9. Has a culture of openness regarding problem-solving

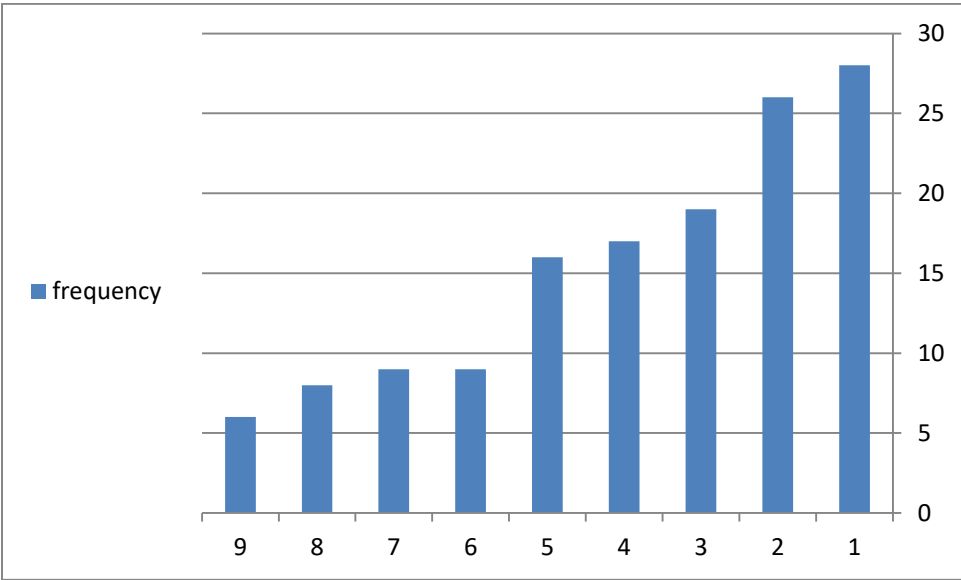


Figure 12: Frequencies of characteristics in defense organizations that are able to avoid risks

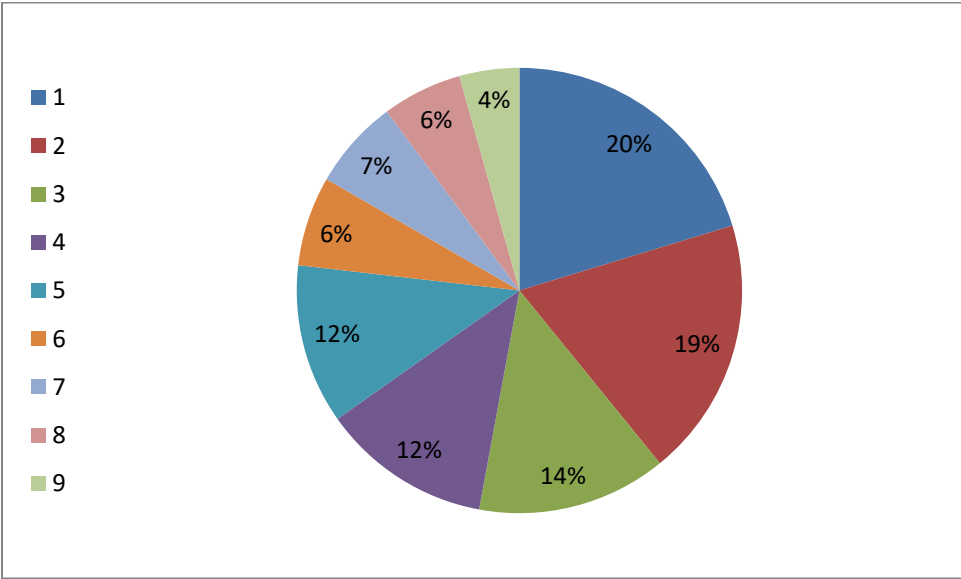


Figure 13: Percentages of characteristics in defense organizations that are able to avoid risks

5. Discussion

The risk factors faced by defense systems is the subject of increasing attention in the complex reality of the 21st century. Multifaceted battlefield challenges and evolving combat requirements

mean that defense systems must be developed rapidly, using daring innovation and technological ingenuity. Unlike others projects, the complex risk management of defense projects is rarely mentioned in the literature. The current study proposes a preliminary attempt to identify and analyze the risks in these systems.

According to the preliminary results, a strong correlation was found between the findings of the exploratory study and the survey results. These correlations are expressed in the following relationships:

1. The exploratory study found that the quality and quantity of human resources is a critical factor in development processes, but were sometimes found to be insufficient. This risk was mentioned as a significant factor in almost every interview. The survey results show that human resources was defined as the primary risk factor, ahead of all others.
2. Another risk presented in the exploratory study, reported mainly by those respondents who had a broader picture (managerial level), is the continuously changing battlefield that forces all involved parties to reduce TTM, although development processes take a substantial amount of time. This need was also mentioned in Naaman [31]. Projects' ongoing need to be remain relevant despite rapidly-changing battlefield conditions means that changes in the initial project design is a risk factor, as the survey indeed found.
3. In many defense projects, it is necessary to change the project's pre-defined goals because changing security requirements. This results in changes in the end product, which in turn delays other processes. This is why the intelligence-mission-technology analysis conducted at the beginning of the project is so critical. This analysis facilitates the prediction of possible future changes in project goals, accordingly makes it possible to introduce project changes, with a minimal influence on schedule. Thus, the robustness principle becomes stronger as a defense project advances. The ability of a product to adapt itself to changing conditions, requirements, and infrastructures is especially significant in the defense industry.
4. Defense projects suffer from too many stakeholders who mutually influence each other. This finding is in line with previous findings [5, 28-29] about the need for many partners when managing projects under constraints. Sometimes, entities from different organizations and companies are involved in a project and are mutually dependent on one another. An example of this dependence is the hiring of sub-contractors, who are required to provide services or products to the primary contractor, which are a critical part of the defense project. The interview findings show that sub-contractors have a meaningful influence on projects on several levels, from product quality to scheduling issues. This subject came up in interviews with project managers who are required to cope with complex challenges in their work with sub-contractors.

As a result of defense projects' sensitivity, project managers strive for independence, as they prefer to depend on their own skills, rather than on external sourcing, which may reduce their flexibility. Conversely, as soon as external sourcing has been decided upon, the project manager is free to deal with other parts of the project.

5. Adding to and changing the Statement of Work (SoW) for the initial project design as a consequence of needing to reduce TTM, or in light of changes in the mission's demands, it is necessary to revise, adapt, and change the initial project design. The survey findings show that in some cases, these changes may also be caused by managerial considerations. On the managerial level, a lack of thorough planning when preparing SoWs, and considering potential risks may lead to future changes that impact scheduling issues. Another aspect that leads to scheduling delays, and which was expressed in the interviews was the high frequency

of role switching within the defense industry, especially when working on classified SoS. Role switching can have numerous advantages, but it has two significant disadvantages:

- a. There is an initial learning process, during which the individual must learn to solve problems based on existing and new knowledge. At this stage, the individual may pay less attention to the project.
- b. We can assume that a project manager or officer who knows, from the beginning, that he will be managing a project from beginning to end will be more committed than one who will likely be transferred before its completion. Another related, common occurrence is the introduction of new professionals to an existing project at advanced stages. Naturally, each professional wants to make his mark on the project, even when he enters a pre-existing, stable project at a later stage. This need may generate a desire to make changes or additions that will be remembered as being initiated by specific people, but could potentially influence the project schedule.

6. Conclusions and Recommendations

The findings of the current study show the need to focus on three main challenges/risks faced by defense projects based on systems of systems (SoS):

- Uncertainty
- The lack of clearly defined goals
- Managing a project under constraint conditions

We could link each one of the risk factors presented in the study to one of these three characteristics. For example, insufficient human and general resources can be linked to managing projects under resource constraint conditions. The subject of resources could also be linked to a lack of clearly defined goals, because goals often determine the project's requirements, leaving uncertainties regarding acquisitions and accessibility. Each one of the risk factors considered might be minimized by high-quality advanced planning, to which all of the necessary resources are allocated.

The risk management process includes several advanced stages of analysis and thinking [32]. The more thoroughly the initial risk analysis process is carried out, the easier it will be to predict the risks that will affect/be affected by the budget, and provide responses to at least some cases. In addition, based on the demand to reduce development times [31], it is reasonable to assume that defense projects' SoWs will also decrease, especially in light of continuously changing battlefield-related needs, that demand rapid response times and shorter development times. Thus, the scope of defense project budgets will most likely be organized differently in the future.

6.1 Main conclusions and recommendations

1. **Organizational adaptations** will make it possible to minimize the common risk factors found in the study: the study found that *changing the project's initial design specifications* and *insufficient human resources* are the two main risk factors.

Defense projects have unique characteristics. Therefore must be a close connection between the end-user (e.g., Air Force operator), the department responsible for making the request (e.g. Development) and the accountable unit that carries out the request (e.g., Procurement Department). Generally, the party making the request is also the one who defines the technical specifications. There is a real need for organizational change that permits **transferring responsibility for SoW specifications to the party carrying out the work**. This could reduce the number of specification changes during a project. We further found that the experience accrued by

officials in the departments implement and/or making requests can also help reduce some of the above risks. One critical remark is that these organizational changes are necessary to cope with rapid developmental changes and mitigate project risks. We also found that insufficient human resources is a significant risk factor. Assuming that there are sufficient resources, **outsourcing of the SoW has the potential to reduce these risks**. However, these processes sometimes present other risks that are preferable to avoid.

To minimize potential risks, an organization should develop tools that allow for a proper, intelligent analysis of outsourcing processes based on past studies/data and valid professional knowledge.

2. **Developing generic infrastructure**, which allows for the integration of new systems, would contribute significantly in two ways:
 - a. Reduced R&D required for future integration, thereby reducing potential R&D-related risks
 - b. Decreased development times for new abilities
3. **Process automation**, with an emphasis on automated control processes. In order to reduce the risk of insufficient resources, it is necessary to automate processes as much as is possible. For example, transitioning to automated checking of new systems instead of manual checking has many advantages, including increased effectiveness, the ability to run more tests in less time, the ability to work 24/7, and a reduced need for and dependence on human resources, which reduces risk related to workforce availability as well as costs.
4. Changes in performance specifications at advanced stages is one of the main reasons for project delays. **In-depth preparation of technical and performance specifications at the beginning of the project may mitigate this risk**. A project's progress generates a great deal of stress for most of the involved parties, which may consequently create inadequate thoroughness in certain areas, including specification processes. We **recommend defining principles to regulate orderly work procedures**, which includes anchoring the time windows of all of the project partners.

A process of risk management in projects is a rational chain of practices by decision-agents in order to ensure that project implementation complies with certain conditions. The decision-makers need to identify, analyze and evaluate the risks in all stages of the project's life cycle, and use their organizational structure and administrative practices to respond to risks in way that benefits the project [23, 26, 42-43].

Proper risk management methods are crucial to implementing in defense projects involving SoS. The more managerial echelons focus on risk management, the more the attention will be paid to subject at work levels, resulting in fewer instances of risks. Moving forward on a defense project involving SoS without a proactive focus on risk management is likely to lead to more problems arising from unmanaged risks.

6.2 Study limitations and recommendations for future research

This paper presents preliminary results of a data science analysis of a concerning classified defense projects involving SoS. We expect to present the final results by January 2021. Further, we recommend that future research expand the study to other defense industries in additional countries, with different clients and suppliers.

Acknowledgments: The author would like to thank Shimon Fridkin for his contribution for the data analysis, and Sani Mazuz and Chen Dvir for their contribution for the data collection.

Conflicts of Interest: The author declares no conflict of interest.

References

1. A Guide to the Project Management Body of Knowledge (PMBOK GUIDE). Newtown Square, PA: Project Management Institute, 2018.
2. Fairley R. Risk Management for software projects. *IEEE Software* 1994; 57–67.
3. Boehm B.W. Software risk management: Principles and practices. *IEEE Software* 1991, 8: 32–41.
4. Kliem R.L.; Ludin I.S. *Reducing Project Risk*. Farnham, UK: Gower, 1997.
5. *Risk management - Principles and Guidelines*, ISO 31000:2018 <https://www.iso.org/standard/65694.html>.
6. Ye, S.; Tiong, R.L.K. NPV-at-risk method in infrastructure project investment evaluation. *J. Constr. Eng. Manag.* **2000**, 126, 227–233.
7. Hastak, M.; Shaked, A. ICRAM-1: Model for international construction risk assessment. *J. Manag. Eng.* **2000**, 16, 59–69.
8. 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. *Energy* **2018**, 165, 1089–1101.
9. Thomas, A.V.; Kalidindi, S.N.; Ganesh, L.S. Modelling and assessment of critical risks in BOT road projects. *Constr. Manag. Econ.* **2006**, 24, 407–424.
10. Mu, J.; Peng, G.; MacLachlan, D.L. Effect of risk management strategy on NPD performance. *Technovation* **2009**, <https://doi.org/10.1016/j.technovation.2008.07.006>.
11. Pimchangthong, D.; Boonjing, V. Effects of risk management practices on IT project success. *Manag. Prod. Eng. Rev.* **2017** 8, 30–37. <https://doi.org/10.1515/mper-2017-0004>.
12. Raz, T.; Shenhar, A.J.; Dvir, D. Risk management, project success, and technological uncertainty. *R&D Manag.* **2002** 32, 101–109. <https://doi.org/10.1111/1467-9310.00243>.
13. Bannerman, P.L. Risk and risk management in software projects: A reassessment. *J. Syst. Softw.* **2008**, 81, 2118–2133. <https://doi.org/10.1016/j.jss.2008.03.059>
14. Oehmen, J.; Olechowski, A.; Robert Kenley, C.; Ben-Daya, M. Analysis of the effect of risk management practices on the performance of new product development programs. *Technovation* **2014**. 34, 441–453. <https://doi.org/10.1016/j.technovation.2013.12.005>.
15. De Carvalho, M.M.; Rabechini Jr, R. Impact of risk management on project performance: The importance of soft skills. *Int. J. Prod. Res.* **2015**, 53, 321–340. <https://doi.org/10.1080/00207543.2014.919423>.
16. Jin, X-H.; Zhang G. Modelling optimal risk allocation in PPP projects using artificial neural networks. *Int. J. Proj. Manag.* **2011** 29(5): 591–603. <http://linkinghub.elsevier.com/retrieve/pii/S0263786310001158>.
17. Ojiako U.; Papadopoulos T.; Thumboristuthi C.; Yang Y.F. Perception variability for categorized risk factors. *Ind. Manag. Data Syst.* **2012**, 112(4): 600–18. <http://www.emeraldinsight.com/10.1108/02635571211225503>
18. Besner C.; Hobbs B. Contextualized project management practice: A cluster analysis of practices and best practices. *Proj. Manag. J.* **2013**, 44(1): 17–34. <http://doi.wiley.com/10.1002/pmj.21291>
19. Gil N.; Tether B.S. Project risk management and design flexibility: Analyzing a case and conditions of complementarity. *Res. Policy*, **2011**, 40(3): 415–28. <http://linkinghub.elsevier.com/retrieve/pii/S0048733310002209>
20. Baharmand H.; Zad M.; Hashemi S.H. Prioritization of effective risk factors on oil industry construction projects (by PMBOK Standard Approach). *Res. J. Appl. Sci. Eng. Technol.* **2013**, 6(3): 521–8.
21. Robinson L.A.; Levy J.I. The [r]evolving relationship between risk assessment and risk management. *Risk Anal.* **2011**, 31(9): 1334–44. <http://www.ncbi.nlm.nih.gov/pubmed/21740453>
22. Fortune J.; White D.; Jugdev K.; Walker D. Looking again at current practice in project management. *Int. J. Manag. Proj. Bus.* **2011**, 4(4): 553–72. <http://www.emeraldinsight.com/10.1108/17538371111164010>
23. Teller J.; Kock A. An empirical investigation on how portfolio risk management influences project portfolio success. *Int. J. Proj. Manag.* **2013**, 31(6): 817–29. <http://linkinghub.elsevier.com/retrieve/pii/S0263786312001688>

24. Pajares J.; López-Paredes A. An extension of the EVM analysis for project monitoring: The cost control index and the schedule control index. *Int. J. Proj. Manag.* **2011**, 29(5): 615–21. <http://linkinghub.elsevier.com/retrieve/pii/S0263786310000712>
25. Schroeder K.; Hatton M. Rethinking risk in development projects: From management to resilience. *Dev. Pract.* **2012**, 22(3): 409–416. <http://www.tandfonline.com/doi/abs/10.1080/09614524.2012.664623>
26. Petit Y. Project portfolios in dynamic environments: Organizing for uncertainty. *Int. J. Proj. Manag.* **2012**, 30(5): 539–53. <http://linkinghub.elsevier.com/retrieve/pii/S0263786311001530>
27. Kuo Y.-C.; Lu S.-T. Using fuzzy multiple criteria decision making approach to enhance risk assessment for metropolitan construction projects. *Int. J. Proj. Manag.* **2013**, 301(4): 602–14. <http://linkinghub.elsevier.com/retrieve/pii/S0263786312001342>.
28. 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; doi:10.3390/su12104152
29. Ameyaw, E.E.; Chan, A.P.C. Evaluation and ranking of risk factors in public–private partnership water supply projects in developing countries using fuzzy synthetic evaluation approach. *Expert Syst. Appl.* **2015**, 42, 5102–5116.
30. Lessard, D.R. *Uncertainty and risk in global supply chains*. MIT Sloan Research Paper No. 4991-13, 2013.
31. Naaman A. Establishment of the armed force – Research Development in Air Force, Between the Poles, Part 3, pp. 85–99, 2016.
32. Wang, J.; Lin W.; Huang Y.H. A performance-oriented risk management framework for innovative R&D projects, *Technovation*, **2010** 32: 601–611.
33. Lee E.; Park Y.; Shin J.G. Expert systems with applications. large engineering project risk management using a Bayesian Belief Network. *Expert Systems with Applications*. **2009** 36(3): 5880–5887.
34. Department of Defense. *Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs*. Washington, DC: Office of the Deputy Assistant Secretary of Defense for Systems Engineering/Department of Defense, 2015.
35. Chris C.; Stephen W. *Managing Project Risk and Uncertainty: A Constructively Simple Approach to Decision Making*. Hoboken, NJ: John Wiley & Sons, 2002.
36. Haskins C. *System Engineering Handbook*. San Diego, CA: INCOSE, 2010.
37. Sharon A.; Weck O.L.; Dori D. Project management vs. systems engineering management: A practitioners' view on integrating the project and product domains. *Syst. Eng.* **2010** 14(4): 427–440.
38. Alexander W.N.; *Systems Engineering Principles*. Hoboken, NJ: A John Wiley & Sons. 2011.
39. Koral Kordova S; Katz E; Frank M. Managing development projects – The partnership between project managers and systems engineers. *Syst. Eng.* 2018, 1-16, <https://doi.org/10.1002/sys.21474>
40. BKCASE Editorial Board. The Guide to the Systems Engineering Body of Knowledge (SEBoK). Version 1.9.1 R.D. Adcock (EIC), Hoboken, The Trustees of the Stevens Institute of Technology. 2018.
41. Maier M.W; Architecting principles for system of systems, *Syst. Eng.* **1998**, 1(4): 267–284.
42. da-Silva L.R.; Crispima J.A. The project risk management process: A preliminary study, *Proc. Technol.* 2014, 16: 943–949.
43. Besner, C.; Hobbs B; Contextualized Project Management Practice: A Cluster Analysis of Practices and Best Practices. *Proj. Manage. J.* **2013**, 44(1): 17–34.