 doi:10.20944/preprints202012.0389.v1

Risk Management for Defense SoS in a Complex, Dynamic Environment

Sigal Kordova

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

Shimon Fridkin
HIT – Holon Institute of Technology, Faculty of Management of Technology
52 Golomb St., Holon, Israel, 50810201
shimon.fridkin@gmail.com

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 industries, because they are exposed to risk already in early stages of development. This paper uses Heterogeneity and Homogeneity analysis between risk factors with Cochran's Q test and Multidimensional scaling in order to present the complexity of the risk factors relevant to defense SoS, and proposes a methodology for identifying, analyzing and monitoring the risks that they face. Findings from an in-depth analysis of 46 classified defense SoS shows a need to focus on three main risks faced by defense projects: insufficient human resources, changes in the original specifications, and lack of other (non-human) resources. The paper also presents some recommendations for minimizing risk factors in defense SoS.

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

1. Introduction

Defense Systems of Systems (SoS) can be defined as a collection of systems that exchange information and interact synergistically. Defense SoS are characterized by the unique challenges facing the complexity of their systems, which must be developed rapidly using daring innovation and technological ingenuity. Moreover, in the defense arena, SoS must meet sophisticated challenges on the battlefield.

Defense SoS require systematic management of risks that limits risk disruptions and their propagation throughout the systems. Therefore, risk management is one of the most important areas that must be considered when managing defense 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.

Successful management of defense SoS 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 SoS. The findings can help project managers and systems engineers of these and similar SoS 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

 doi:10.20944/preprints202012.0389.v1

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.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 December 2020 doi:10.20944/preprints202012.0389.v1

Figure 1. Impact of variables, based on project time [1]

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].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 December 2020 doi:10.20944/preprints202012.0389.v1

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.

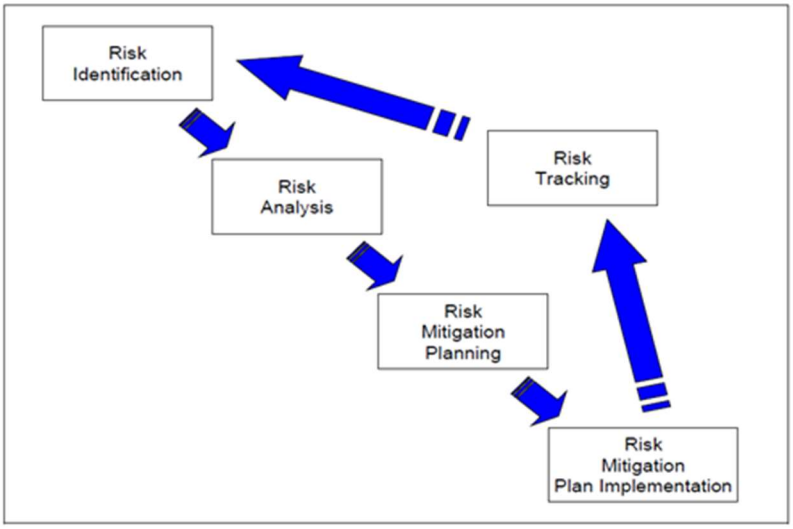

Figure 2. Risk management process according to the DoD

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,

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 December 2020 doi:10.20944/preprints202012.0389.v1

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.

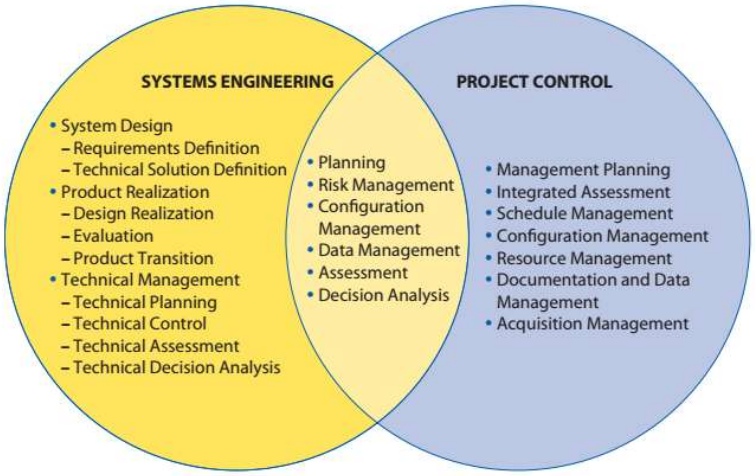

Figure 3. Overlaps between systems engineering and project management

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 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 from 46 classified defense SoS in the Air Force. Figure 4 represents the research design.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 December 2020 doi:10.20944/preprints202012.0389.v1

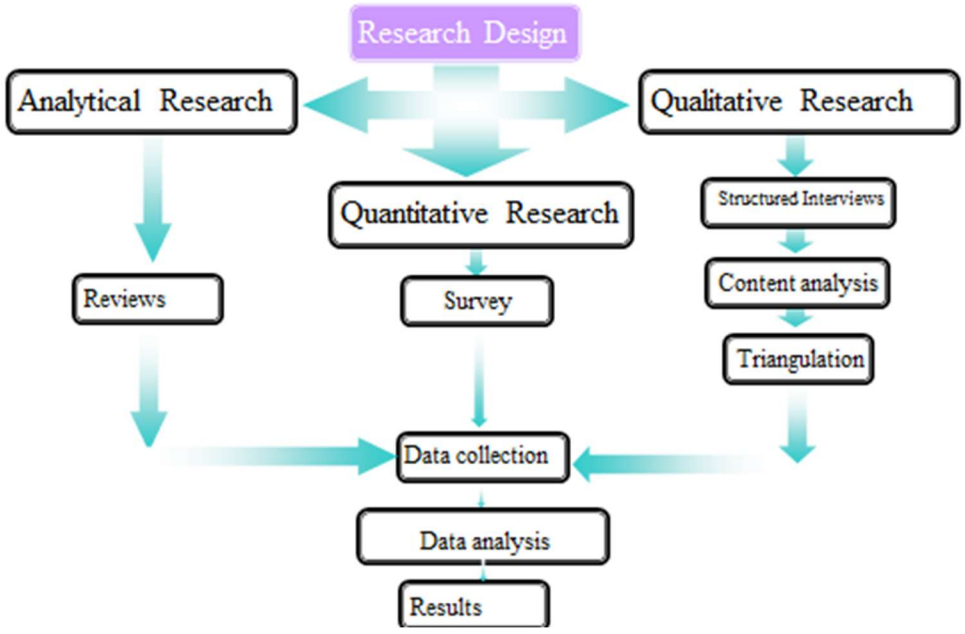

Figure 4. The research design

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 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, content analysis was performed and triangulation process was conducted in order to confirm each finding presented in the report which 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 defense SoS in the Air Force. Its goal was to determine the segmentation of risk factors for these systems.

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. In order to validate the final version of the survey a pilot group was selected to complete the questionnaire. The data thus collected included the organization's risk management methodology, the most common risk factors in defense systems, and the main characteristics of organizations that manage to avoid the occurrence of risks. The data collected by the survey included the most common risk factors in

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 December 2020 doi:10.20944/preprints202012.0389.v1

defense systems. During the survey, each respondent was asked to select the five most common risk factors in defense systems from the following list:

- Risk factor 1: Failure to maintain risk management processes
- Risk factor 2: Delays in supporting infrastructure
- Risk factor 3: Cultural differences among system members
- Risk factor 4: Overly-optimistic scheduling assessment
- Risk factor 5: Insufficient human resources
- Risk factor 6: Lack of other (non-human) resources
- Risk factor 7: Lack of system team' previous experience
- Risk factor 8: Lack of system stakeholders' previous experience
- Risk factor 9: Too many stakeholders influencing the system
- Risk factor 10: Complexity of the military operation
- Risk factor 11: R&D required in a new field/area
- Risk factor 12: Overlap between different system processes
- Risk factor 13: Changes in the original specifications
- Risk factor 14: Gap in knowledge management
- Risk factor 15: Dependence on other factors

In the first stage statistical analysis, frequencies of the risk factors faced by 46 defense systems were counted. In the second stage, Heterogeneity and Homogeneity between the risk factors was calculated using Cochran's Q test and I^2 statistic. In third stage, Multidimensional scaling was performed.

4. Results

4.1 Findings of the exploratory study(interviews)

The risk factors faced by defense SoS, 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 system and interdependent on one another.
4. Additions to the Statement of Work (SoW) and/or changes to the system'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 system. This may also cause project managers to commit to challenging SoWs and schedules.
6. The bigger the system'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

In the first stage, frequencies of the risk factors faced by 46 defense SoS were presented. Figure 5 present the bar chart (frequencies) of the risk factors faced these defense SoS.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 December 2020 doi:10.20944/preprints202012.0389.v1

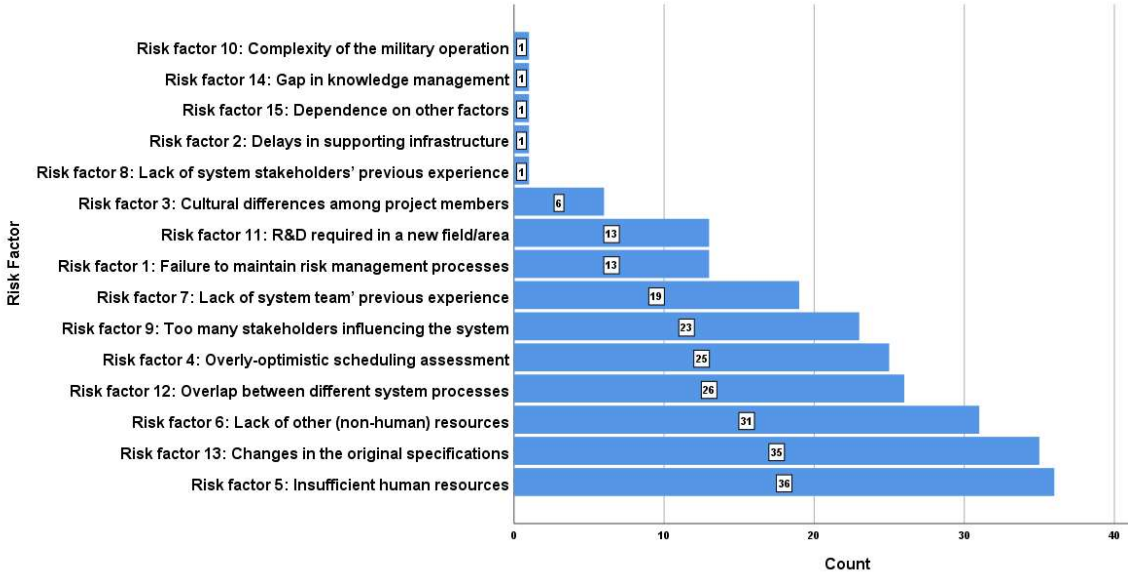

Figure 5. Bar chart of Risk factors faced by 46 defense SoS

According to Figure 5, the seven most common risk factors faced by the defense SoS surveyed were: Risk factor 5 (Insufficient human resources), Risk factor 13 (Changes in the original specifications), Risk factor 6 (Lack of other (non-human) resources), Risk factor 12 (Overlap between different system processes), Risk factor 4 (Overly-optimistic scheduling assessment), Risk factor 9 (Too many stakeholders influencing the system), and Risk factor 7 (Lack of system team' previous experience)

In the second stage, Heterogeneity and Homogeneity between the risk factors was evaluated using Cochran's Q test and I^2 statistic. Table 1 lists (in descending order) the proportion of each of the 10 Risk factors (Risk factors 2 (Delays in supporting infrastructure), 8 (Lack of system stakeholders' previous experience), 10 (Complexity of the military operation), 14 (Gap in knowledge management) and 15 (Dependence on other factors) were not included in the analysis because respondents mentioned them only once).

Table 1. The proportion of each of the 10 Risk factors (N=46)

Risk Factor	Proportion
Risk factor 5: Insufficient human resources	.78
Risk factor 13: Changes in the original specifications	.76
Risk factor 6: Lack of other (non-human) resources	.67
Risk factor 12: Overlap between different project processes	.57
Risk factor 4: Overly-optimistic scheduling assessment	.54
Risk factor 9: Too many stakeholders influencing the system	.50
Risk factor 7: Lack of system team' previous experience	.41
Risk factor 1: Failure to maintain risk management processes	.28
Risk factor 11: Research & development required in a new field/area	.28
Risk factor 3: Cultural differences among project members	.13

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 December 2020 doi:10.20944/preprints202012.0389.v1

Next, in the framework of Heterogeneity, we conducted a Cochran's Q test and I^2 statistic (Risk factors 2, 8, 10, 14 and 15 were not included in the analysis because respondents mentioned them only once). As part of Cochran's Q test, Pairwise Comparisons were conducted with a Bonferroni-adjusted alpha level of 0.005 (0.05/10), in order to detect Heterogeneity. The findings of Cochran's Q test can be seen in Figure 6, which shows the Pairwise Comparisons in an explicit configuration. All of the blue lines represent significant difference between one risk factor's frequency to another that have been adjusted by the Bonferroni correction for multiple tests. All of the red lines represent significant difference between one risk factor's frequency to another that have been not adjusted by the Bonferroni correction for multiple tests.

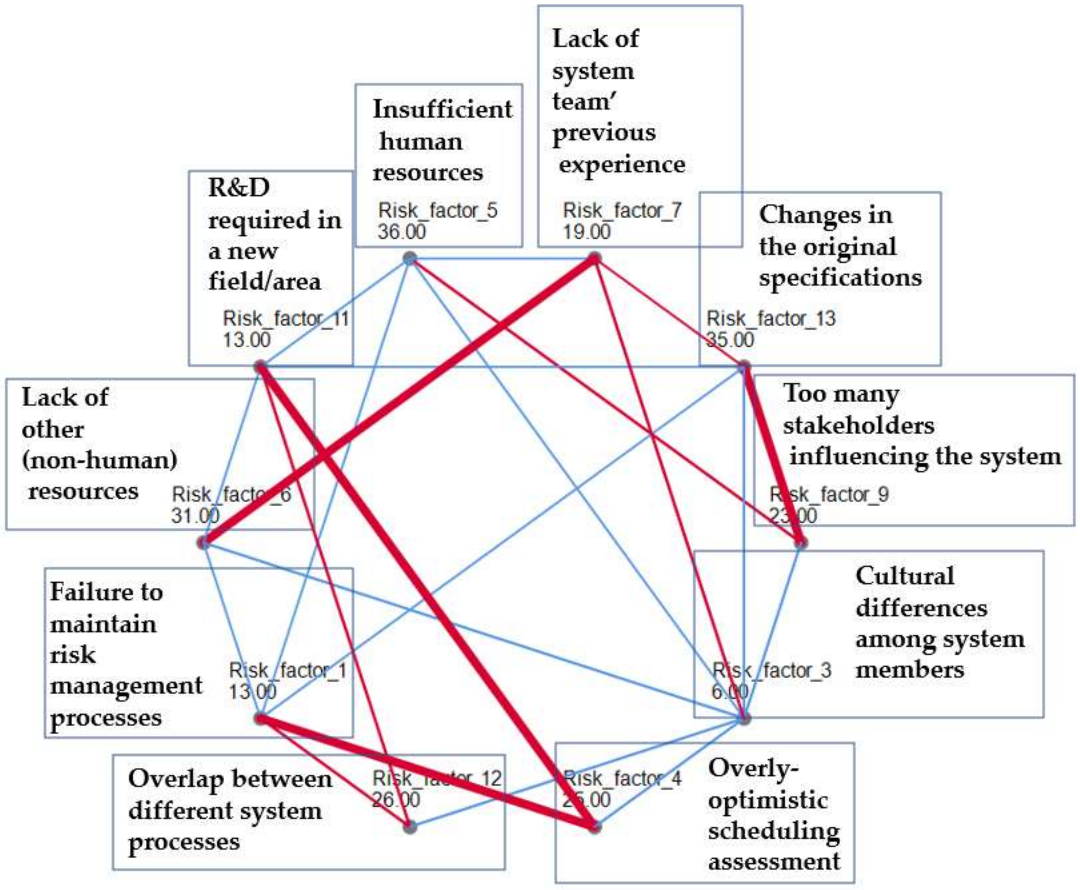

Figure 6. Cochran's Q test and Pairwise Comparisons with a Bonferroni-adjusted alpha level of 0.005 (*Total N = 46; Related-Samples Cochran's Q Test Statistic = 70.156; df = 9; Asymptotic Sig.(2-sided test) = .000; I^2=75.99*)

The Pairwise Comparisons show that Risk Factor 5 was noted significantly more by the respondents than Risk factor 7 (Lack of system team's previous experience; Frequency=19), Risk factor 11 (R&D required in a new field/area; Frequency=13), Risk factor 1 (Failure to maintain risk management processes; Frequency=13) and Risk factor 3 (Cultural differences among system members; Frequency=6). Therefore, we propose that it is the most crucial Risk factor. Similarly, Risk factor 13 (Changes in the original specifications; Frequency=35) and Risk factor 6 (Lack of other (non-human) resources; Frequency=31) where noted significantly higher by the respondents than Risk factor 1 (Failure to maintain risk management processes; Frequency=13),

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 December 2020 doi:10.20944/preprints202012.0389.v1

Risk factor 11 (R&D required in a new field/area; Frequency=13) and Risk factor 3 (Cultural differences among system members; Frequency=6), making Risk factor 13 and Risk factor 6 second in importance. In addition, Risk factor 12 (Overlap between different system processes; Frequency=26) was noted significantly higher by the respondents than Risk factor 3 (Cultural differences among system members; Frequency=6), making Risk factor 12 third in importance.

Additionally, as part of Cochran's Q test, in order to detect Homogeneity, Stepwise step-down analysis was conducted based on asymptotic significances. Table 2 presents the findings of the Stepwise step-down analysis.

Table 2. Homogeneous Subsets of Risk Factors

Sample[a]	Subset	
	1	2
Risk factor 3: Cultural differences among system members	.130	
Risk factor 1: Failure to maintain risk management processes	.283	
Risk factor 11: Research & development required in a new field/area	.283	
Risk factor 7: Lack of system team' previous experience	.413	
Risk factor 9: Too many stakeholders influencing the system	.500	.500
Risk factor 4: Overly-optimistic scheduling assessment	.543	.543
Risk factor 12: Overlap between different project processes	.565	.565
Risk factor 6: Lack of other (non-human) resources		.674
Risk factor 13: Changes in the original specifications		.761
Risk factor 5: Insufficient human resources		.783
Test Statistic	10.096	-64.96
Sig. (2-sided test)	.121	1.000
Adjusted Sig. (2-sided test)	.168	1.000

Note: Homogeneous subsets are based on asymptotic significances. The significance level is .05.
a. Each cell shows the sample number of successes.

The Stepwise step-down analysis shows that there are two subsets of Risk factors. Subset 1 characterized by Risk factors 7 (Lack of system team' previous experience), 11 (Research & development required in a new field/area), 1 (Failure to maintain risk management processes) and 3 (Cultural differences among project members). The proportions of these risk factors range from 0.13 to 0.413 which converge to a group of risk factors whose proportions are significantly smaller than the proportions of the group of risk factors belonging to Subset 2. The group of these risk factors is called "Risk Factors with Low Impact Intensity".

Subset 1 is characterized by Risk factors 5 (Insufficient human resources), 13 (Changes in the original specifications) and 6 (Lack of other (non-human) resources). The proportions of these risk factors range from 0.674 to 0.783 which converge to a group of risk factors whose proportions are significantly higher than the proportions of the group of risk factors belonging to Subset 1. The group of these risk factors is called "Risk Factors with High Impact Intensity".

Risk factors (Risk factor 9: Too many stakeholders influencing the system, Risk factor 4: Overly-optimistic scheduling assessment and Risk factor 12: Overlap between different project processes) whose proportions range from 0.5 to 0.565 adjoin two groups "Risk Factors with High Impact Intensity" and "Risk Factors with High Impact Intensity". This group of risk factors is called "Risk Factors with Moderated Impact Intensity".

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 December 2020 doi:10.20944/preprints202012.0389.v1

To validate the findings, which were based on of Cochran's Q test, Multidimensional scaling was performed. First, it had to be decided how many dimensions the solution should have. The follow scree plot (Figure 7) helped make this decision.

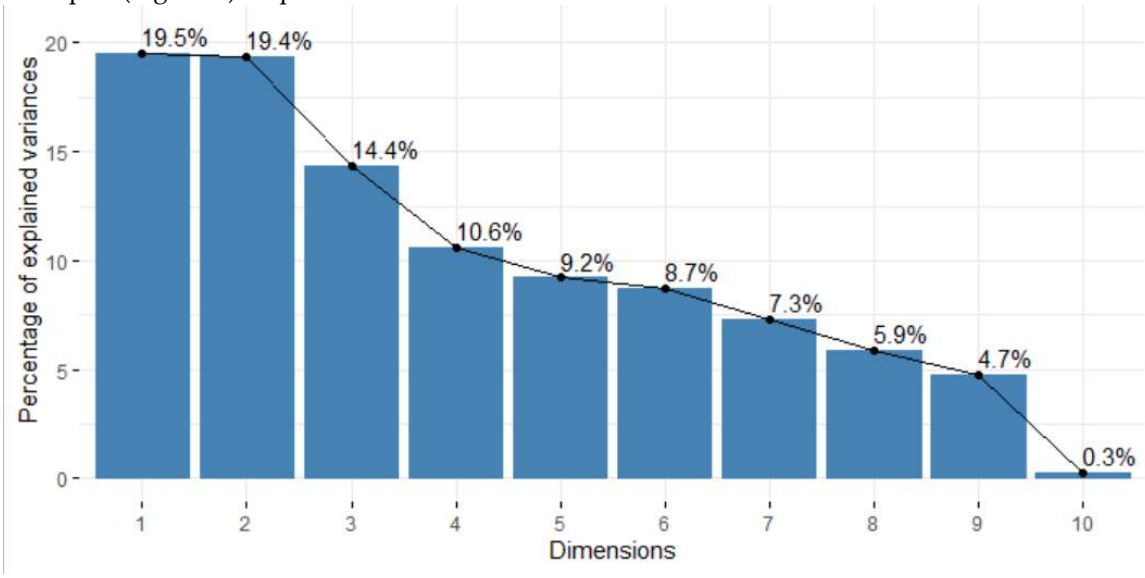

Figure 7. Scree plot

The procedure begins with a 10-dimensional solution and works down to a 2-dimensional solution. The scree plot shows the normalized raw stress of the solution at each dimension. It can be seen from the plot that increasing the dimensionality from 2 to 3 and from 3 to 4 offers large improvements in the stress. After dimension 4, the improvements are rather small. Therefore, it was decided to analyze the data by using a 2-dimensional solution, because the results are easier to interpret.

The common space plot (Figure 8) gives a visual representation of the relationships between the objects.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 December 2020 doi:10.20944/preprints202012.0389.v1

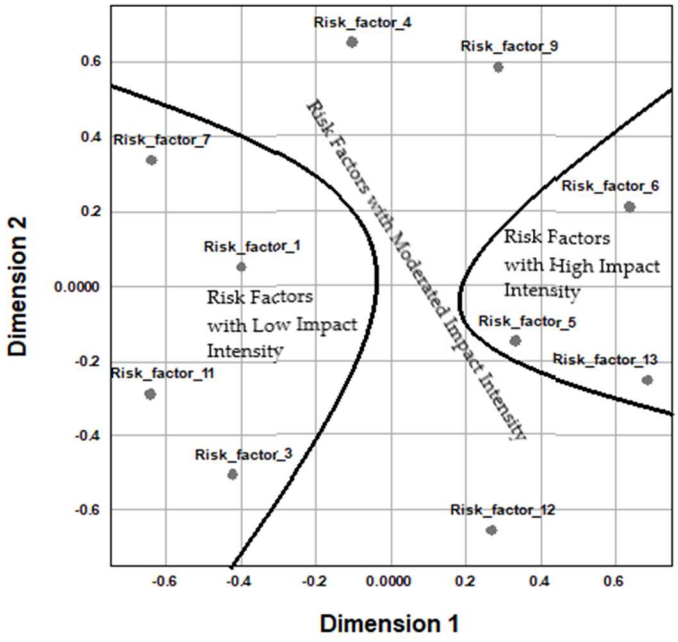

Figure 8. Common space coordinates (Stress and Fit Measures: Normalized Raw Stress = 0.072; Stress-I[a] = .270; Stress-II[a] = .798; S-Stress[b] = .175; Dispersion Accounted For (D.A.F.) = .927; Tucker's Coefficient of Congruence = .962; a. Optimal scaling factor = 1.078; b. Optimal scaling factor = 1.078.)

Figure 8 shows that dimension 1 (on the x axis) strong correlated with Risk factors with High Impact Intensity: Risk factor 6 (Lack of other (non-human) resources), 13 (Changes in the original specifications) and 5 (Insufficient human resources). Dimension 2 is in diverse relationships with Risk factors with Low Impact Intensity (Risk factor 3: Cultural differences among system members, Risk factor 1: Failure to maintain risk management processes and Risk factor 11: Research & development required in a new field/area) and with Risk factors with Moderate Impact Intensity (Risk factor 9: Too many stakeholders influencing the system, Risk factor 4: Overly-optimistic scheduling assessment and Risk factor 12: Overlap between different system processes).

In order to validate the findings produced by Cochran's Q test (including Heterogeneity and Homogeneity analyzes) and Multidimensional scaling (which yielded similar results) it was decided to conduct another analysis: Hierarchical Cluster Analysis. Figure 9 shows the Dendrogram for single linkage solution of the analysis.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 December 2020 doi:10.20944/preprints202012.0389.v1

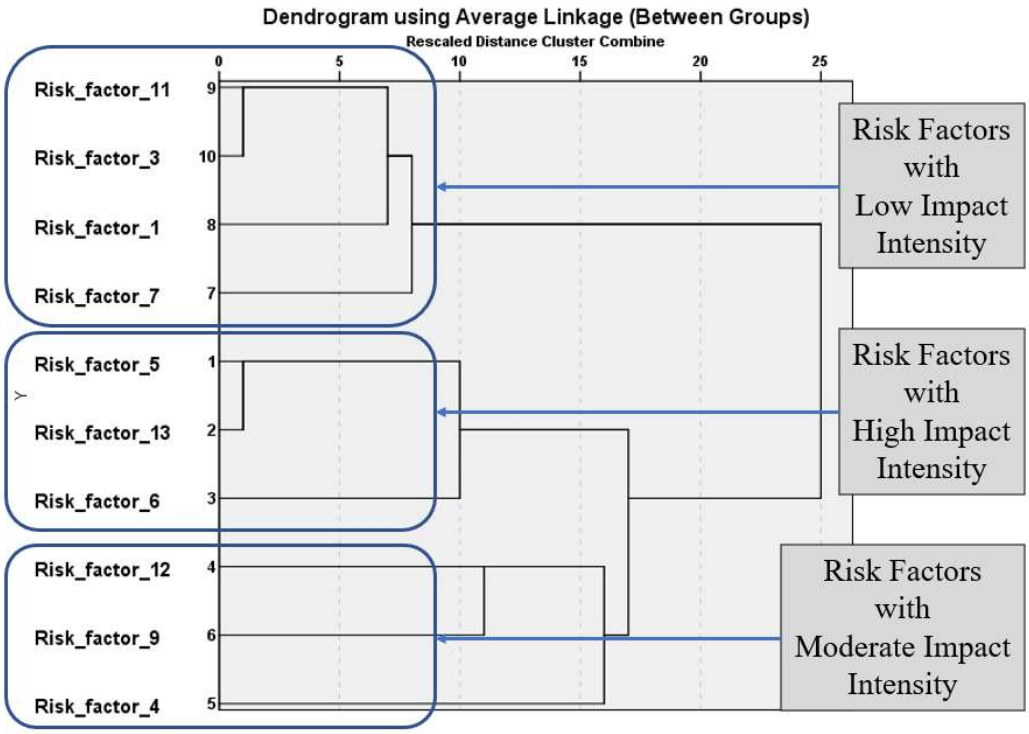

Figure 9. Dendrogram for single linkage solution (Cluster method: Between group-linkage; Measure: Binary: Simple matching)

From Hierarchical Cluster Analysis it can be clearly seen that Risk factors with High Impact Intensity (5, 13 and 6) are the first in the hierarchy of influence. Followed in second place in terms of impact are Risk factors with Moderate Impact Intensity (12, 4 and 9) and last - Risk factors with Low Impact Intensity (7, 11, 1 and 3).

5. Discussion

The risk factors faced by defense SoS is the subject of increasing attention in the complex reality of the 21st century. Multifaceted battlefield challenges and evolving combat requirements mean that defense SoS must be developed rapidly, using daring innovation and technological ingenuity. Unlike others systems, the complex risk management of defense SoS is rarely mentioned in the literature. The current study proposes a preliminary attempt to identify and analyze the risks in these systems.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 December 2020 doi:10.20944/preprints202012.0389.v1

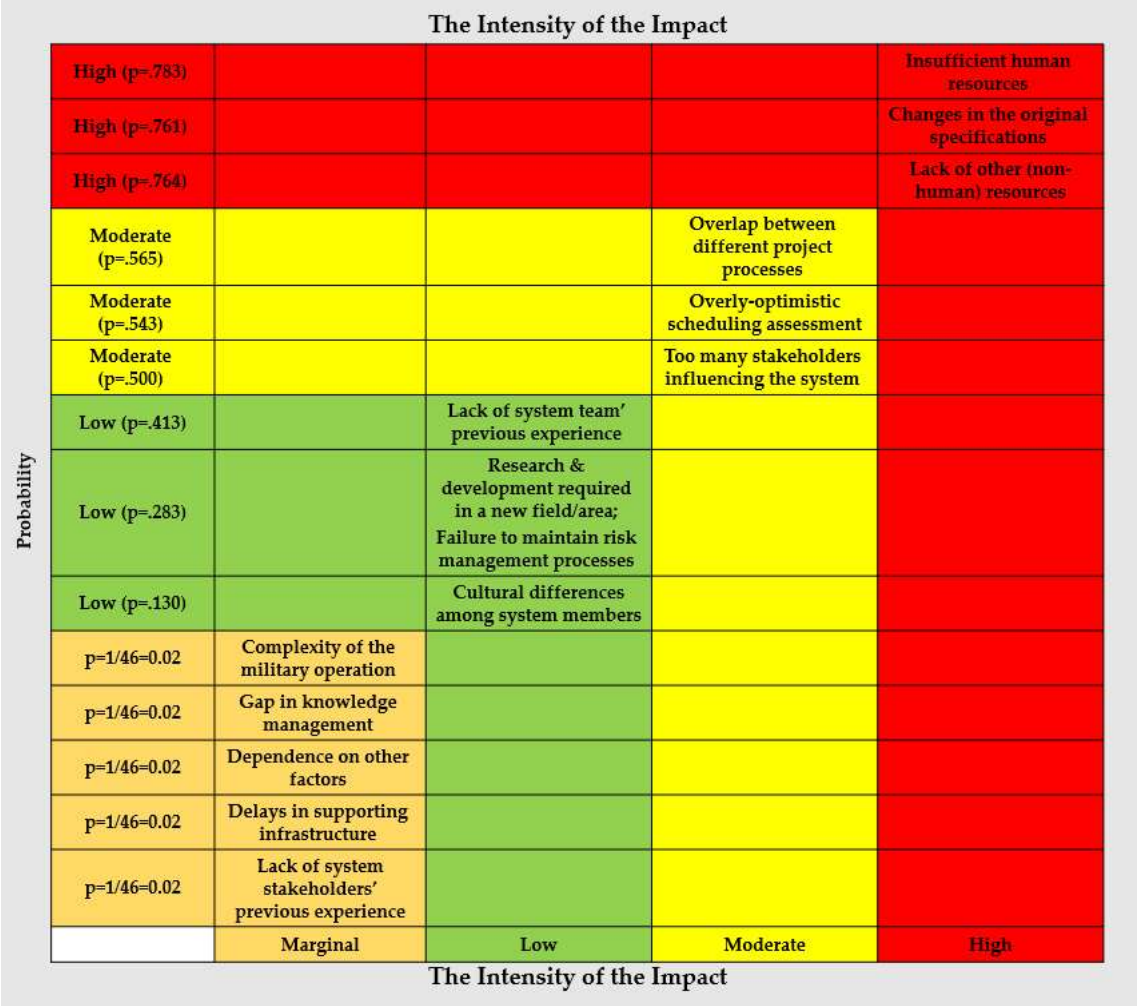

Figure 10: The risk map of 46 defense SoS

Figure 10 presents the risk map that was built according to the survey results. The risk map shows the connection between the intensity of each risk factor and the probability of the risk. Risk factor 13 (changes in the original specifications) was rated as the most influential risk factor that associates it with a group of high-impact risk factors, along with Risk factors 5 (Insufficient human resources) and 6 (Lack of other (non-human) resources).

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 insufficient human resources (Risk factor 5) 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 the time of IOC, although development processes take a

substantial amount of time. This need was also mentioned in Naaman [31]. Systems' ongoing need to be remain relevant despite rapidly-changing battlefield conditions means that changes in the original specifications (Risk factor 13) is a significant risk factor, as the survey indeed found.

3. In many defense systems, it is necessary to change the system'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 process is so critical. This analysis facilitates the prediction of possible future changes in system goals, accordingly makes it possible to introduce system changes, with a minimal influence on schedule. Thus, the robustness principle becomes stronger as a defense SoS advances. The ability of a product to adapt itself to changing conditions, requirements, and infrastructures is especially significant in the defense industry.
4. Defense SoS 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 SoS. The interview findings show that sub-contractors have a meaningful influence on SoS 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.

Because defense SoS have high 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 system.

5. The survey findings show a linkage between risk factor 13: changes in the original specifications and some others factors (risk factors 4, 5, 6, 9, 12) that may in some instances be caused by managerial considerations. All these potential risks might lead to future changes that impact scheduling delays.
6. 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.

 doi:10.20944/preprints202012.0389.v1

6. Conclusions and Recommendations

The findings of the current study show the need to focus on some main challenges/risks faced by defense SoS:

Risk factor 5: Insufficient human resources
Risk factor 6: Lack of other (non-human) resources
Risk factor 13: Changes in the original specifications

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 systems' 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 systems 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*, *insufficient human resources and lack of other (non-human) resources* are the three main risk factors.

Defense systems 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 system 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 system partners.

A process of risk management in defense SoS is a rational chain of practices by decision-agents in order to ensure that system 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 SoS. The more managerial echelons focus on risk management, the more the attention will paid to subject at work levels, resulting in fewer instances of risks. Moving forward on a defense 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 results of a data science analysis of 46 classified defense SoS.. 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 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.; Thumborisuthi 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-Silvaa 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.