New Optimal Mission Abort Policies for Coherent Systems Using Signature

Amin Karimi[*], **Mahdi Tavangar**[*,†] and **Maxim Finkelstein**[‡,§]

Abstract

For critical systems, such as satellites and aircraft, survivability can be extremely important as failures can result in irreversible economic loss and even casualties. A mission abort policy and the subsequent rescue procedure are effective tools for increasing the survivability of systems performing missions of fixed or variable duration. However, it comes at a price of decreasing the mission success probability. Therefore, a reasonable trade-off should be achieved. This problem has been studied in numerous publications, however, we are the first to discuss general multi-component coherent systems. Moreover, the new methodology based on signatures describing coherent systems is employed for description and defining a criterion of abort. Several optimization problems are formulated and discussed. The detailed numerical examples illustrate our findings and justify the developed innovative approach.

Keywords: Mission abort policy, Reliability, Signature vector, Mission success probability, System survival probability.

1 Introduction

1.1 Motivation and related literature

In practice, the survival of critical systems can have even higher priority than the completion of a mission. This happens when a failure of a system during a mission results in a substantial economic loss. Real examples of critical systems are spaceships, aircraft, drones, satellites, and data-processing computer systems. However, a mission of such systems can be aborted when a certain malfunction condition occurs or a certain number of components fail, and then a rescue procedure can be initiated to save the system

[*]Department of Statistics, Faculty of Mathematics and Statistics, University of Isfahan, Isfahan 81744, Iran.

Email addresses: M.amin.karimi@sci.ui.ac.ir (A. Karimi), M.tavangar@sci.ui.ac.ir (M. Tavangar), FinkelM@ufs.ac.za (M. Finkelstein)

[†]Corresponding author.

[‡]University of the Free State, Bloemfontein, South Africa. Department of Statistics, Faculty of Mathematics and Statistics, University of Isfahan, Isfahan 81744, Iran (e-mail: m.tavangar@sci.ui.ac.ir)

[§]Department of Management Science, University of Strathclyde, Glasgow, UK.

and prevent casualties, economic loss, and significant environmental hazards. Thus, the two metrics, i.e., mission success probability and system survivability, and their interplay are of interest (see, e.g., Peng et al. (2016) and Liu et al. (2018)).

Many critical systems are required to complete missions over a predetermined period of time. A mission abort policy is a valuable tool for maximizing the survivability of a system. Aborting a mission under certain conditions can help minimize the potential failures while increasing its chances of survival. This policy can be instrumental in reducing economic losses by increasing the system's survival probability and thereby, providing greater protection against risk. A mission abort policy can also reduce operating costs by improving efficiency and reliability. Myers (2009) in his seminal work on mission abort policies for a k-out-of-n system with exponentially distributed components lifetimes proved the efficiency of such policies in reducing the overall failure probability compared to those without abort policies. This work provided the foundation for further investigations into mission abort policies for complex systems with multiple sources of uncertainty. Recently, Zhao et al. (2023b) investigated the system structure and joint optimization of condition-based mission abort policy for the k-out-of-n: G warm standby system, which takes into account the dynamic arrival of tasks with a random amount of work. These systems have a few warm standby components that provide fault tolerance while the rest components operate in active mode initially.

Cao and Wang (2023) have extended the mission abort policy to the generalized k-out-of-n system. Levitin et al. (2017) extended this model to heterogeneous systems and adaptive abort policies. However, these models do not take into account the dynamic nature of the stochastic environment and its influence on the system's behavior and performance. To address this shortcoming, Levitin and Finkelstein (2018a) and Levitin and Finkelstein (2022) have investigated the mission abort policy for systems in a random environment modeled by shocks. Levitin and Finkelstein (2018b) have considered a threshold for mission aborting in each interval after dividing the whole mission time into numerous intervals.

In another point of view, one can also consider a case involving multiple attempts, where a mission is aborted and then repeated after successfully rescuing a system. Levitin et al. (2019) have discussed this setting when completing a mission is extremely important. Recently, Levitin et al. (2023a) proposed a new model of multiple attempts performed consecutively with a prespecified activation delay by different components. Levitin et al. (2023b) have investigated a mission abort policy in a multi-attempt scenario when the number of attempts is limited. For maximizing the aborting policy for a system that has multiple distinct tasks to complete within a predetermined mission time, Levitin et al. (2024) model and optimize the aborting policy that each task can be attempted multiple times until it is successfully completed or the system fails or the mission time expires.

Several research papers have explored the behavior of systems experiencing major and minor failures when dealing with mission abort protocols. These studies aim to understand how such systems respond to different failure scenarios and improve the effectiveness of mission abort procedures. For example, Cha et al. (2018) have considered systems that experienced both major and minor failure modes, where repairable failures were maintained through minimal repairs, and the number of minimal repairs was chosen as the decision variable of the abort strategy. Qiu et. al (2020) proposed a dynamic abort policy that takes into consideration the number of minor failures and time elapsed since the start of a mission.

Another kind of system that has been studied in the context of mission abort policies is multi-state systems. These systems, consisting of various interconnected states or modes, have been the subject of extensive research and analysis. Multi-state systems encompass a wide range of applications, including aerospace, automotive, and telecommunications industries. Levitin et al. (2020) have studied a mission abort policy for multi-state systems with variable performance. Levitin et al. (2022) developed and improved mission abort policies for multi-state systems that have product storage. These systems have the ability to store excess product in the event that system performance exceeds needed demand and to make up for any product shortages. According to Zhao et al. (2022), the joint optimization of a mission abort policy and a protective device selection policy for multi-state systems should be considered.

In addition to numerous papers addressing mission abort strategies, we would like to recommend the following papers to readers who are interested in exploring this topic further. Peng (2018) has studied the joint optimization of routine planning and termination strategies for cooperative UAVs. Zhao et al. (2019) have discussed the optimal abort policy using Markov decision processes. Qiu and Cui (2019a) developed the mission abort policy based on the two-stage degradation modeled by the increasing stochastic processes. Qiu and Cui (2019b) and Qiu et al. (2022) have considered the duration in a defective state as a decision variable for aborting a mission. Yang and Ye (2019) have investigated abort policies based on the early warning signal and have studied the analytical properties of the corresponding optimal policy. Gao et al. (2020) have investigated a mission abort policy for systems with the Weibull-distributed lifetimes. Zhao et al. (2021) have investigated a multi-criteria mission abort policy subject to a two-stage degradation process. Finkelstein et al. (2021) have studied systems exhibiting observable degradation, focusing on the decision-making process regarding mission continuation or termination during inspections. When the observed degradation exceeds a predetermined optimal threshold, the mission is aborted. Conversely, if the degradation is below this threshold, the system may either maintain its initial operational regime at full load or transition to a reduced load regime. Wu et al. (2021) have developed an optimal mission abort policy for a system consisting of m sectors and comprising of n components. Cheng et al. (2022) have discussed a mission abort policy according to a system age and degradation degree of monitored health features. Wei et al. (2023) have studied the control policy that timely aborts the mission system whose state information can not be completely monitored. Zhao et al. (2023a) have investigated the two-level rescue depot location policies and the dynamic rescue policies in mission abort policy for unmanned vehicle systems. Levitin et al. (2023c) expanded mission abort policy to include the more general and effective non-monotonic threshold function for systems that have a practical random rescue time. Yang et al. (2023) utilized incomplete health data to jointly decide whether to abort the mission and whether to carry out sampling in a dynamic manner, with the goal of minimizing the expected total costs associated with system failure, sampling, and mission failure. In their review of the mathematical models for mission abort policy, da Silva et al. (2023) focused on criteria for achieving a balance between the probability of mission success and the probability of system survival. Cheng et al. (2024) investigated a multi-component system with failure interaction to determine the optimal joint inspection and mission abort policy. They took into account the proportional hazards model to describe the impact of a single component. Liu et al. (2024) suggested the mission payload and stochastic dependence, and determine the specific mission abort policy depending on the mission's duration and component health. In order to optimize the expected cumulative reward during the mission, a Markov decision process-based dynamic mission abort decision-making model is subsequently developed.

It follows from the aforementioned literature review that the primary interest in the literature on mission abort was systems without considering their structures. It should be noted that Myers (2009) had considered the simplest k-out-of-n system with exponentially distributed lifetimes of components (see also Cao and Wang (2023)). Thus, most papers on mission abort policy deal with the black-box systems without considering their structures. However, information on internal failures of components in systems is extremely valuable as it shows the level of systems' deterioration. If a substantial number of components in the operating system have failed, this means that the probability of the system's and a mission failure is large and the possibility of mission abort should be considered. This, obviously, was not considered in the existing literature, as the structure of a multi-component system was 'out of the picture'.

In order to analyze the performance of multi-component coherent systems we employ and justify a powerful signature-based methodology that provides a structural approach for evaluating relevant reliability characteristics. There is no other way in describing the reliability functions of coherent systems allowing for expressions that are derived in this combinatorial way that can be used for our purpose. The usual structure functions as multi-linear polynomials cannot be used for this purpose. This methodology enables to consider the number of failed components as a decision variable for a mission abort. Signatures provide information on performance and reliability at the components level as well as at the system level. The development of this topic for more general coherent systems is the main objective of the current paper. This task requires the implementation of the signature-based approach to obtain mission success probability and system survivability. To our knowledge, this methodology for the probabilistic description of systems with the possibility of abort and rescue has not been considered in the literature yet. In our proposed policy, when a certain number of components fail, a mission may need to be aborted to reduce the risk of failure, thereby necessitating immediate activation of the rescue procedure.

A coherent system is a system with an increasing (in each argument) structure function, and each of the components is relevant (see, e.g., Barlow and Proschan, 1981). A well-known tool for studying the reliability of a coherent system is the *signature vector*; see for example Kochar et al. (1990) and Samaniego (2008). Let a coherent system consist of n components with lifetimes $X_1, X_2, ..., X_n$ that are independent and identically distributed following a common continuous distribution function $F(t)$. Denote by $X_{1:n}, X_{2:n}, ..., X_{n:n}$ the order statistics corresponding to X_i's. The system's signature is then defined as

$$s_i = \mathbb{P}(T = X_{i:n}), \quad i = 1, 2, ..., n, \tag{1}$$

where T denotes the system's lifetime. In fact, s_i is the probability that the component with lifetime $X_{i:n}$ causes the system to fail (i.e., the ith component failure in the system results in its failure.) The probability vector $\boldsymbol{s} = (s_1, s_2, ..., s_n)$ is then called the signature vector of a coherent system. It can be verified that $s_i = \frac{n_i}{n!}$, where n_i is the number of ways that distinct $X_1, X_2, \ldots, X_n$ can be ordered so that the ith ordered quantity corresponds to the system's failure. Under this setting, the reliability (survival) function $\bar{F}_T(t)$ of the system can be represented as

$$\bar{F}_T(t) = \mathbb{P}(T > t) = \sum_{i=1}^{n} s_i \mathbb{P}(X_{i:n} > t), \quad t \geq 0. \tag{2}$$

It is well-known that the representation (2) holds for every coherent system with components having exchangeable and absolutely continuous lifetimes of components; see, for example, Navarro et al. (2005).

1.2 Main contributions of the paper

We propose an *innovative approach* to obtaining an optimal mission abort policy for coherent systems with independent and identically distributed components (or, at least, exchangeable). It is based on describing the reliability of these systems via the corresponding signature vectors. To the best of our knowledge, this methodology has not been developed in the literature on mission abort so far. As justified by our theoretical findings and computational results, it presents an effective tool for defining and describing the advanced optimal mission abort strategies by considering relevant optimization problems and discussing the main stochastic properties of the proposed model. It also forms the basis for future generalizations in the case of heterogeneous components. The detailed numerical illustrations and the corresponding discussion justify our theoretical findings.

1.3 Organization of the paper

The remainder of the paper is organized as follows. In Section 2, we investigate the mission abort policy for a coherent system consisting of n independent components, and then we obtain the mission success probability and system survival probability for the system. Afterward, we obtain the probability of coherent system failure according to the mission abort. In Section 3, we present different methods for the proper selection of mission abort parameters. In Section 4, we investigate the mission abort policy with multiple thresholds for a coherent system. In Section 5, by presenting a numerical example and a simulation study, we examine different properties of the mission abort policy. Finally, brief concluding remarks are given in Section 6.

2 Description of the mission policy

Before introducing our strategy, we provide in the following an overview of the notations and abbreviations used throughout the paper. This will facilitate a better understanding of our strategy and its implications.

MSP	Mission success probability
SSP	System survival probability
n	Number of components in the system
$X_1, X_2, ..., X_n$	Component lifetimes
$X_{1:n}, X_{2:n}, ..., X_{n:n}$	Ordered component lifetimes
$F_{i:n}(t)$	Distribution function of $X_{i:n}$
$t_{r(L)}$	Duration of recovery or rescue period
t_M	Mission duration
$T_{f(L)}$	Random time at which an abort occurs
$Q_{L:n}$	Probability of failure for a system having an abort policy upon Lth failure
C_F	Cost of mission failure
C_L	Cost of system failure

2.1 Description of a strategy

Consider a coherent system consisting of n statistically independent and identical components that perform a mission of a fixed or variable duration t_M. In critical systems, the survival of the system is of utmost importance, and failure of such critical systems can cause substantial economic loss. To avoid the failure of a coherent system, we propose the following mission abort policy: If a predetermined number $L \in \{1, 2, ..., n-1\}$ of components fail, then, to increase the system survival and decrease the probability of a loss of the system, one should abort the mission and immediately activate the rescue or recovery procedure. Note that the parameter L is a decision variable in this approach. In section 3, we shall present two important measures that are useful in studying and evaluating the optimal mission abort strategies.

2.2 Mission success probability

The probability of mission success, which is the probability that a system will complete a specific mission within a given deadline, is an important measure of performance in the mission abort context (see, e.g., Levitin and Finkelstein (2018a), Levitin and Finkelstein (2022)). The probability of a mission success can be obtained as a joint probability of two events: the lifetime of the system is greater than t_M and the lifetime of the Lth failed component is greater than t_M, where $1 \leq L \leq n-1$. In accordance with this criterion, using the law of total probability and properties of order statistics (Kochar et al., 1999), the mission success probability can be obtained in a straightforward way as

$$
\begin{aligned}
MSP = MSP(t_M, L) &= \mathbb{P}(T > t_M, X_{L:n} > t_M) \\
&= \mathbb{P}(T > t_M, X_{L:n} > t_M, T > X_{L:n}) + \mathbb{P}(T > t_M, X_{L:n} > t_M, T \leq X_{L:n}) \\
&= \sum_{j=1}^{n} \mathbb{P}(T > t_M, X_{L:n} > t_M, X_{j:n} > X_{L:n} \mid T = X_{j:n})\mathbb{P}(T = X_{j:n}) \\
&\quad + \sum_{j=1}^{n} \mathbb{P}(T > t_M, X_{L:n} > t_M, X_{j:n} \leq X_{L:n} \mid T = X_{j:n})\mathbb{P}(T = X_{j:n}) \\
&= \sum_{j=L+1}^{n} s_j \mathbb{P}(X_{L:n} > t_M) + \sum_{j=1}^{L} s_j \mathbb{P}(X_{j:n} > t_M) \\
&= \bar{S}_L \mathbb{P}(X_{L:n} > t_M) + \sum_{j=1}^{L} s_j \mathbb{P}(X_{j:n} > t_M),
\end{aligned}
$$

where $\bar{S}_L = \sum_{j=L+1}^{n} s_j$. Thus, we have

$$
MSP = \bar{S}_L \sum_{k=0}^{L-1} \binom{n}{k} \big\{F(t_M)\big\}^k \big\{\bar{F}(t_M)\big\}^{n-k} + \sum_{j=1}^{L} \sum_{k=0}^{j-1} s_j \binom{n}{k} \big\{F(t_M)\big\}^k \big\{\bar{F}(t_M)\big\}^{n-k}.
$$

By changing the order of summations in the second term on the right-hand side of the last equation, we obtain the more compact form

$$
\begin{aligned}
MSP &= \bar{S}_L \sum_{k=0}^{L-1} \binom{n}{k} \big\{F(t_M)\big\}^k \big\{\bar{F}(t_M)\big\}^{n-k} + \sum_{k=0}^{L-1} \left(\sum_{j=k+1}^{L} s_j \right) \binom{n}{k} \big\{F(t_M)\big\}^k \big\{\bar{F}(t_M)\big\}^{n-k} \\
&= \sum_{k=0}^{L-1} \bar{S}_k \binom{n}{k} \{F(t_M)\}^k \{\bar{F}(t_M)\}^{n-k}. \qquad (3)
\end{aligned}
$$

For more details on the distribution theory of order statistics, we refer the interested reader to David and Nagaraja (2003) and Arnold et al. (1992).

Note that, the MSP is increasing in $L \in \{1, 2, ..., n-1\}$. This follows easily from (3) or from the fact that

$$
[T > t_M, X_{L:n} > t_M] \subseteq [T > t_M, X_{L+1:n} > t_M].
$$

The result is illustrated by Figure 1 where we plot the MSP for a structure consisting of two bridge systems connected in series whose common components lifetimes are Weibull-distributed with shape parameter 1 and scale parameter 10 (see the numerical example given in Section 5).

Remark 2.1. It may be an interesting problem to compare two coherent n-component systems based on their mission success probabilities. Let $\mathcal{S}_1$ and $\mathcal{S}_2$ be two coherent systems with respective signature vectors $\boldsymbol{s}_1$ and $\boldsymbol{s}_2$. Then, it can be verified that if the discrete random variables corresponding to $\boldsymbol{s}_1$ and $\boldsymbol{s}_2$ are ordered in the sense of the usual stochastic order, and the component lifetimes of $\mathcal{S}_1$ and $\mathcal{S}_2$ are also ordered in the sense of the usual stochastic order, then $MSP^{(1)} \leq MSP^{(2)}$, where $MSP^{(j)}$ is the mission success probability corresponding to system $\mathcal{S}_j$, $j = 1, 2$. We refer the reader to Shaked and Shanthikumar (2007) for definitions and basic properties of various stochastic orders.

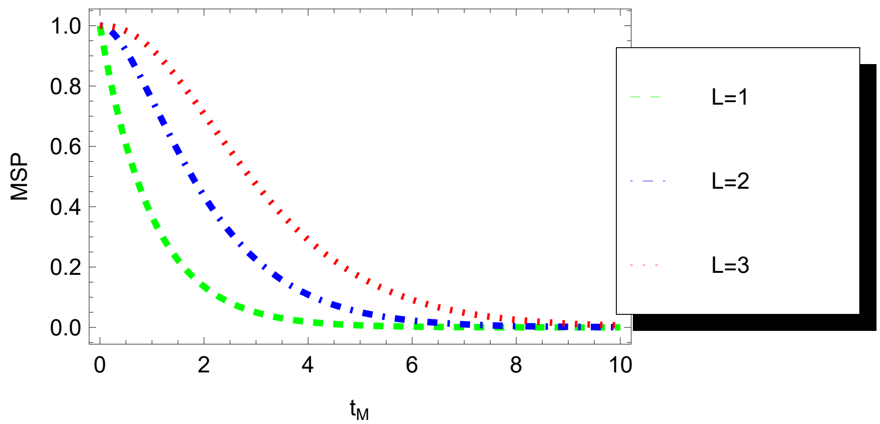

Figure 1: Mission success probability for $L = 1, 2, 3$.

Remark 2.2. The relationships between mission abort time, mission time, and mission completion probability can provide valuable insights for mission planning and decision-making. By analyzing these relationships, mission planners can identify critical variables that influence mission success and make informed decisions about mission time and aborting the mission, if necessary, to achieve the best possible outcome.

Remark 2.3. One can define the probability of the mission success probability by taking into account the variability of the mission time. In fact, one can consider the mission time T_M as a random variable depending on the external conditions: weather, air masses, currents, etc. Based on the above, we may approximately assess the probability of attaining the objectives, while the environmental conditions are variable and uncertain, which is opposite to the previous analysis where mission time was taken as fixed. This refined approach will help in building a resistant and adaptive mission plan due to which the chances of mission success would be increased irrespective of the unpredictable environmental influence. Let $f_{T_M}(t_M)$ be the probability density function of T_M. Using the total probability law, the mission success probability can then be obtained as

$$\begin{aligned} MSP = MSP(T_M, L) &= \mathbb{P}(T > T_M, X_{L:n} > T_M) \\ &= \int_0^\infty \mathbb{P}(T > T_M, X_{L:n} > T_M \mid T_M = t_M) f_{T_M}(t_M) dt_M \\ &= \int_0^\infty \sum_{k=0}^{L-1} \bar{S}_k \binom{n}{k} \{F(t_M)\}^k \{\bar{F}(t_M)\}^{n-k} f_{T_M}(t_M) dt_M. \end{aligned} \tag{4}$$

2.3 Rescue procedure (RP)

As we have mentioned at the beginning of the preceding section, in our proposed mission abort model, the rescue procedure is triggered only when the Lth component of the system fails at a random time $X_{L:n}$ preceding the mission duration time t_M. A coherent system does not fail in this period if the difference between the system lifetime and the time that mission abort starts is greater than the fixed time $t_{r(L)}$, given that the lifetime of the system is greater than the lifetime of the Lth component and the Lth order statistic is less than t_M. This can be also interpreted in terms of the corresponding remaining lifetime after aborting. In fact, the system lifetime should be greater than or equal to $X_{L:n}+t_{r(L)}$, emphasizing the fact that the initiation of the rescue procedure cannot be predetermined before a mission starts. Therefore, we define a new measure for the effectiveness of the rescue procedure as the probability

$$RP = RP(t_M, L, t_{r(L)}) = \mathbb{P}(T - X_{L:n} > t_{r(L)} \mid T > X_{L:n}, X_{L:n} < t_M).$$

In accordance with this definition, using the law of total probability, equations (1) and (2), and properties of order statistics, the following can be easily derived

$$\begin{aligned}
RP &= \mathbb{P}\left(T - X_{L:n} > t_{r(L)} \mid X_{L:n} < \min(T, t_M)\right) \\
&= \sum_{j=1}^{n} \mathbb{P}(T - X_{L:n} > t_{r(L)} \mid X_{L:n} < \min(T, t_M), T = X_{j:n}) P(T = X_{j:n}) \\
&= \sum_{j=1}^{n} s_j \mathbb{P}(X_{j:n} - X_{L:n} > t_{r(L)} \mid X_{L:n} < \min(T, t_M), T = X_{j:n}) \\
&= \sum_{j=1}^{n} s_j \int_0^{t_M} \mathbb{P}\big(X_{j:n} - X_{L:n} > t_{r(L)} \mid X_{L:n} < \min(X_{j:n}, t_M), X_{L:n} = x) f_{X_{L:n}}(x) dx \\
&= \sum_{j=L+1}^{n} s_j \int_0^{t_M} \mathbb{P}(X_{j:n} - x > t_{r(L)} \mid X_{L:n} < t_M, X_{L:n} = x) f_{X_{L:n}}(x) dx \\
&= \sum_{j=L+1}^{n} s_j \int_0^{t_M} \mathbb{P}\left(X_{j:n} > x + t_{r(L)} \mid X_{L:n} = x) f_{X_{L:n}}(x\right) dx \\
&= \sum_{j=L+1}^{n} s_j \int_0^{t_M} \int_{x+t_{r(L)}}^{\infty} f_{X_{j:n}|X_{L:n}}(t \mid x) f_{X_{L:n}}(x) dt dx \\
&= \sum_{j=L+1}^{n} \sum_{k=0}^{j-L-1} s_j \binom{n-L}{k} \\
&\qquad \times \int_0^{t_M} \left(\frac{F(x+t_{r(L)}) - F(x)}{1-F(x)}\right)^k \left(\frac{1-F(x+t_{r(L)})}{1-F(x)}\right)^{n-k} f_{X_{L:n}}(x) dx. \qquad (5)
\end{aligned}$$

Remark 2.4. Starting a rescue procedure might not be an appropriate choice of action when the Lth component fails close to the mission time (t_M). Our model can be generalized by introducing the new decision parameter ξ–the time after which abort is not executed– similar to Levitin and Finkelstein (2018a). However, we will address this in future research, where we will consider a system with heterogeneous components and derive the optimal ξ using an approach that differs from existing literature.

Example 2.5. Consider an airplane performing a mission. During the mission, it should cover a certain distance. The adversary uses electronic interference (shocks) to destroy the airplane's control systems, which consist of n components, which can cause the airplane to crash. Each subsequent interference attack is due to overheating and deterioration of the onboard interference filter, which can then fail a critical component. Attacks and then failure of critical components are detected by the sensors and the mission attempt can be aborted upon the occurrence of a predetermined number of failed components. The rescue procedure presumes to return to the original (or nearest available) airport after changing the flight altitude, which causes a reduction of the interference attack rate. After landing, the interference filters are changed and the next attempt to perform the mission starts. If, during any of the attempts, an attack succeeds in destroying the electronic equipment, the airplane is lost and the mission fails.

2.4 System survival probability

System survival probability (SSP) is another crucial indicator that is used by decision-makers to determine the possibility that a mission and any associated rescue procedure will be successful (Levitin and Finkelstein (2018a), Levitin and Finkelstein (2022)). A few of the factors taken into account are the remaining time for the mission, the possibility that the rescue procedure will be successful, and other risks or issues. There is always a potential that a system will malfunction or fail while it is in use, endangering the mission's success. To lessen these risks, a company can create a mission abort policy that details what to do in the event of a system failure. A rescue procedure to save the system and complete the mission may be launched as part of the mission abort policy. The SSP is a measure of the probability that either the mission or any associated rescue procedures will be completed successfully, without any further issues or complications. It provides decision-makers with valuable insight into the feasibility of initiating a rescue procedure and the potential outcomes. By calculating the SSP, decision-makers can determine the probability of successfully rescuing the system. This information can help them make informed decisions about whether to initiate a rescue procedure and if so, what steps to take to ensure the best possible outcome.

The SSP is a measure of the probability that the mission or its associated rescue procedure will be completed successfully. In other words, it captures the probability of success for a given mission and any related rescue procedures and is defined as

$$\begin{aligned} SSP &= S(t_M, L, t_{r(L)}) \\ &= \mathbb{P}[(T > t_M, X_{L:n} > t_M) \cup (T - X_{L:n} > t_{r(L)}, X_{L:n} < \min(T, t_M))] \\ &= MSP + RP \times \mathbb{P}[X_{L:n} < \min(T, t_M)], \end{aligned} \tag{6}$$

where the second term on the right-hand side represents the probability that the rescue procedure can successfully save the system. Also

$$\begin{aligned} \mathbb{P}[X_{L:n} < \min(T, t_M)] &= \sum_{j=1}^{n} \mathbb{P}(T > X_{L:n}, X_{L:n} < t_M \mid T = X_{j:n}) \mathbb{P}(T = X_{j:n}) \\ &= \sum_{j=1}^{n} s_j \mathbb{P}(X_{j:n} > X_{L:n}, X_{L:n} < t_M) = \sum_{j=L+1}^{n} s_j \mathbb{P}(X_{L:n} < t_M) \\ &= \bar{S}_L \sum_{k=L}^{n} \binom{n}{k} \{F(t_M)\}^k \{\bar{F}(t_M)\}^{n-k}. \end{aligned}$$

This is the probability that the system has not completed its mission and it survive until the mission is aborted. The survival probability of a system refers to the probability of successfully completing a mission and associated rescue procedures without any major failures or challenges. When the length of the mission period increases, the system survival probability obviously decreases.

Let $s_* = \min\{i : s_i > 0\}$ and $s^* = \max\{i : s_i > 0\}$. It makes sense to choose L so that $L \in \{1, 2, ..., s^*\}$. In Section 3, we shall discuss about various methods for choosing an optimal value of L. If $L < s_*$, then $MSP(t_M, L) = \mathbb{P}(X_{L:n} > t_M)$ and

$$S(t_M, L, t_{r(L)}) = \mathbb{P}(X_{L:n} > t_M) + \mathbb{P}(T - X_{L:n} > t_{r(L)}, X_{L:n} < t_M).$$

On the other hand, if $L = s_*$, the rescue procedure starts at the failure time of the first component which can cause the system failure. In this case, $MSP(t_M, L) = \mathbb{P}(X_{L:n} > t_M)$. Also, in the case where $L = s^*$, $S(t_M, L, t_{r(L)}) = MSP(t_M, L) = \mathbb{P}(T > t_M)$, meaning that it is preferable to not begin the rescue process because there is no chance that it will succeed.

This statement provides more detail and explanation of the different scenarios based on the relative lengths of mission and recovery periods and how the value of L can impact the probability of system survival.

2.5 Failure of a system

The lifetime of the system and the duration of the rescue procedure are two elements that have an impact on the probability of system failure. The system faces the risk of failure if the system's lifetime is shorter than the lifetime of the Lth component or if the system malfunctions during an attempted rescue procedure. This shows that the probability of system failure also increases as the system's lifetime shortens or when the rescue procedure becomes protracted. The system operators can reduce the probability of system failure by performing regular maintenance and testing or the rescue procedure should be shorter by recognizing these conditions and taking the necessary action. Overall, using mission abort policy and a thorough understanding of the factors that influence system failure probability can help to increase the probability of a successful mission outcome while minimizing the risk of damage to the sensitive and expensive systems involved.

The system failure probability can be defined as

$$\begin{aligned}
Q_{L:n} = Q(t_M, L, t_{r(L)}) &= \mathbb{P}(T < X_{L:n}) + \mathbb{P}(T - X_{L:n} < t_{r(L)} \mid X_{L:n} < \min(T, t_M)) \\
&= \sum_{j=1}^{n} s_j \mathbb{P}(T < X_{L:n} \mid T = X_{j:n}) + \sum_{j=1}^{n} s_j \mathbb{P}(T - X_{L:n} < t_{r(L)} \mid X_{L:n} < \min(T, t_M), T = X_{j:n}) \\
&= \sum_{j=1}^{n} s_j \mathbb{P}(X_{j:n} < X_{L:n}) + \sum_{j=1}^{n} s_j \int_0^{t_M} \mathbb{P}(X_{j:n} - x < t_{r(L)} \mid X_{j:n} > X_{L:n}, X_{L:n} = x) f_{X_{L:n}}(x)dx \\
&= \sum_{j=1}^{L} s_j + \sum_{j=L+1}^{n} s_j \int_0^{t_M} \mathbb{P}(X_{j:n} < x + t_{r(L)} \mid X_{L:n} = x) f_{X_{L:n}}(x)dx \\
&= \sum_{j=1}^{L} s_j + \sum_{j=L+1}^{n} s_j \int_0^{t_M} \int_0^{x+t_{r(L)}} f_{X_{j:n}|X_{L:n}}(t \mid x) f_{X_{L:n}}(x)dtdx \\
&= \underline{S}_L + \sum_{j=L+1}^{n} \sum_{k=j-L}^{n-L} s_j \binom{n-L}{k} \int_0^{t_M} \left(\frac{F(x + t_{r(L)}) - F(x)}{1 - F(x)} \right)^k \left(\frac{1 - F(x + t_{r(L)})}{1 - F(x)} \right)^{n-k} f_{X_{L:n}}(x)dx,
\end{aligned}$$

where $\underline{S}_L = \sum_{j=1}^{L} s_j$.

3 Choosing the optimal value of L

Choosing the optimal abort parameter is crucial in defining a mission abort policy. The abort parameter L represents the threshold for the number of component failures that can occur before the mission is aborted. To obtain an optimal value for the abort parameter, several methods can be used, including the trade-off between mission success probability and system survival probability, the trade-off between mission success probability and system loss, the mission failure cost and system loss cost, the signature vector of a coherent system, statistical analysis, simulation, and expert judgment. Statistical analysis involves analyzing data on components' failure rates and determining the optimal threshold based on statistical models and methods. Simulation involves creating a virtual model of the system and using it to simulate different scenarios to determine the optimal threshold. Expert judgment involves consulting with subject matter experts to determine the optimal threshold based on their experience and knowledge. By using these methods, the system operators can determine the optimal abort parameter that minimizes the risk of system failure while maximizing the probability of a successful mission outcome. Overall, selecting the optimal abort parameter is a critical step in defining the mission abort policy, and requires careful consideration and analysis. It should be noted that, in general, there is no universal method to choose optimal L; it is determined by the conditions and priorities of a given system. For example, if minimizing costs is a must, then the cost function will be the best method to determine L. On the other hand, if system survival is crucial, then the optimal value of L should be chosen by balancing the mission success probability against the system survival probability, such that the balance meets the requirement that the probability of system survival is above some predefined minimum value. In the following, we describe some optimization methods.

3.1 Trade-off between MSP and SSP

It is possible to obtain the optimal value of L by balancing between several items. For example, by balancing between $MSP(t_M, L)$ and $S(t_M, L, t_{r(L)})$, to maximize the MSP while providing a desired level of system survivability S^*, one can provide a solution for the restricted optimization problem (Levitin and Finkelstein, 2018a)

$$\max MSP(t_M, L) \quad \text{s.t.} \quad S(t_M, L, t_{r(L)}) \geq S^*. \tag{7}$$

Another possible approach to obtain the optimal value of L involves balancing multiple factors, such as $MSP(t_M, L)$ and $Q(t_M, L, t_{r(L)})$, to maximize the MSP while ensuring a desired level of system failure, denoted by $q*$ (Levitin et al., 2019)

$$\max MSP(t_M, L) \quad \text{s.t.} \quad Q(t_M, L, t_{r(L)}) \leq q^*. \tag{8}$$

3.2 Determining an optimal value of L based on cost

When choosing a suitable value for the mission abort parameter L, the cost of mission failure and system loss is a crucial factor. In particular, the value of L should be chosen so that the system's cost for mission failure and system loss is kept to a minimum. The system operators can perform a cost analysis that considers the potential costs of mission failure and system loss to establish the optimum value for L. The cost of maintaining or replacing damaged parts, the price of the personnel and equipment needed for the operation, and any other pertinent expenditures can all be included in this analysis. The system operators can construct a suitable decision parameter for the mission abort policy by choosing the value of L that minimizes the overall cost incurred on the system. Overall, this cost-based approach provides a practical and objective method for selecting an appropriate value for the mission abort parameter L. By taking into account the potential costs associated with mission failure and system loss, the system operators can make informed decisions that balance the risk of system failure against the cost of maintaining and operating the system. We can formulate a cost minimization problem with relation to the decision parameter L by considering the associated costs of mission failure and system loss, denoted by C_F and C_L, respectively. In particular, we can think about the probability of system loss, which is represented by $1 - S(t_M, L, t_{r(L)})$, where t_M is the mission time and $t_{r(L)}$ is the rescue time. If the system is lost, both the mission and the system would fail, resulting in a total cost of losses of C_F+C_L. Additionally, we can consider the probability of system survival but mission failure, denoted by $(S(t_M, L, t_{r(L)}) - MSP(t_M, L))$, where $MSP(t_M, L)$ is the probability of successful rescue given that a mission failure has occurred. In this case, the system would survive but the mission would fail, resulting in a cost of losses of C_F. By formulating a cost minimization problem that takes into account these probabilities and costs, we can determine an appropriate value for the decision parameter L that minimizes the expected total cost. This can be done using optimization techniques such as linear programming or dynamic programming (Levitin and Finkelstein, 2018a).

Under the aforementioned conditions, the total cost of the system can be written as

$$C(t_M, L) = (1 - S(t_M, L, t_{r(L)}))(C_F + C_L) + (S(t_M, L, t_{r(L)}) - MSP(t_M, L))C_F.$$

Our objective is to determine the optimal value of L that minimizes the total cost $C(t_M, L)$ of the system.

3.3 Using signature vectors as a basis for analysis

The signature vector of a coherent system can be utilized as a means to choose an appropriate value for the decision parameter L. Given that it offers an accurate representation of the system's reliability and failure modes, a signature vector is a helpful tool for choosing a suitable value for L. The chance of system failure for various values of L can be determined specifically using the signature vector. The system operators can construct a suitable decision parameter for the mission abort policy by choosing a value of L that yields a degree of system failure probability that is acceptable. Overall, using the signature vector to determine an appropriate value for the decision parameter L can help to ensure the reliability and safety of the system. It provides a rigorous and quantitative approach to selecting L that takes into account the system's structure and component lifetimes.

Consider a coherent system with a signature vector given by

$$\boldsymbol{s} = (0, 0, ..., 0, s_k, s_{k+1}, ..., s_\ell, 0, ..., 0),$$

where $s_j > 0$, $j = k, k+1, ..., \ell$. Many coherent systems have such a signature vector for some fixed values of k and ℓ. The value of L is chosen as the smallest value that satisfies a certain condition related to the signature vector of the system. In this approach, a fixed threshold value $q \in (0, 1)$ is chosen by the domain expert, and the value of L is selected such that the sum of the first L elements of the signature vector exceeds the threshold value q; that is,

$$L^* = \min \left\{ j : \sum_{i=1}^{j} s_i > q \right\}. \tag{9}$$

For the signature vector of the form given above, it is evident that $k \leq L^* \leq \ell$.

4 Mission abort policy with multiple thresholds

In scenarios where sensitive and expensive systems are involved, it may be beneficial to divide the mission into several intervals. By doing so, the mission abort policy can be applied separately to each interval, which can help to improve the efficiency of the overall mission (Levitin and Finkelstein (2018b), Levitin and Finkelstein (2022)). This approach can also enable the system operators to identify potential issues early on and take corrective actions before they become critical. Additionally, dividing the mission into intervals can help to reduce the impact of any failures or malfunctions that may occur, as they can be limited to a specific interval rather than affecting the entire mission. Overall, this strategy can increase the probability of a successful mission outcome while minimizing the risk of damage to the sensitive and expensive systems involved. During each interval of a mission that is divided into multiple parts, the mission may be aborted if the number of components that fail exceeds a predetermined threshold. This threshold is set for each interval and represents the maximum number of component failures that can occur before the mission becomes unfeasible or too risky to continue. By establishing such a threshold, the system operators can ensure that the mission is halted before it reaches a critical point, thus preventing further damage or loss of resources. Additionally, setting a predetermined threshold for each interval can help to identify potential issues early on, allowing the system operators to take corrective actions before they become critical. Overall, this approach can increase the probability of a successful mission outcome while minimizing the risk of damage to the sensitive and expensive systems involved.

Consider splitting the mission duration t_M into H smaller intervals $[t_{M_{h-1}}, t_{M_h})$, $h = 1, 2, ..., H$, where $t_{M_0} = 0$ and $t_{M_H} = t_M$. If the number of component failures in a given interval exceeds a predetermined threshold, denoted by L_h for $h = 1, ..., H$, then the mission is aborted and the rescue procedure is activated. This threshold is set for each interval and represents the maximum number of component failures that can occur before the mission becomes unfeasible or too risky to continue. The vector $\boldsymbol{L} = (L_1, ..., L_H)$ and $\boldsymbol{t}_M = (t_{M_1}, ..., t_{M_H})$ determine the mission abort policy. Similar to the use of a single threshold for determining mission abort, it is possible to introduce multiple thresholds for determining the probability of mission success. A mission succeeds if the system's total lifetime expectancy is greater than t_M, and whether the lifetime expectancy of the L_hth components in interval h is also greater than t_{M_h}. The MSP is defined as

$$MSP(\boldsymbol{t}_M, \boldsymbol{L}) = \mathbb{P}(T > t_M, X_{L_h:n} > t_{M_h} \quad \text{for} \quad h = 1, 2, ..., H)$$

Also, the rescue procedure for the coherent system can be written as

$$RP(\boldsymbol{t}_M, \boldsymbol{L}, t_{r(L)}) = \sum_{h=1}^{H} \mathbb{P}(T - X_{L_h:n} > t_{r(L)} \mid X_{L_h:n} < \min(T, t_{M_h})).$$

The system is considered to have survived if it successfully completes either the mission or the rescue procedure. Thus, one can define the SSP as

$$S(\boldsymbol{t}_M, \boldsymbol{L}, t_{r(L)}) = MSP(\boldsymbol{t}_M, \boldsymbol{L}) + RP \times \mathbb{P}[X_{L_h:n} < \min(T, t_{M_h}) \quad \text{for} \quad h = 1, 2, ..., H].$$

5 Sensitivity analysis and illustrative examples

5.1 Sensitivity analysis

In this section, to explain how one can utilize the models introduced in Section 2, we provide a numerical example to examine the theoretical results of the paper. All results, including figures and numerical computations, are obtained using Mathematica Program System version 10. Suppose there are two bridge systems connected in series as shown in Figure 2, and all component lifetimes follow the Weibull distribution with shape parameter $\alpha = 1$ and scale parameter $\lambda = 10$. Note that in practice, signature vectors of critical systems correspond to the higher redundancy (more zeroes before the first nonzero component of the vector). However, the considered example illustrates better and sufficiently our approach. The signature vector for this 10-component system can be calculated as follows:

$$s = (0, 4/45, 19/90, 3/10, 86/315, 34/315, 2/105, 0, 0, 0);$$

see, for example, Da et al. (2012).

Using Equation (3), we have determined the mission success probability which is plotted in Figure 3. As it is observed, if the mission abort occurs at the first order statistic (i.e., the first component failure), the probability of mission success is the lowest. This is because a mission abort at this early stage indicates a

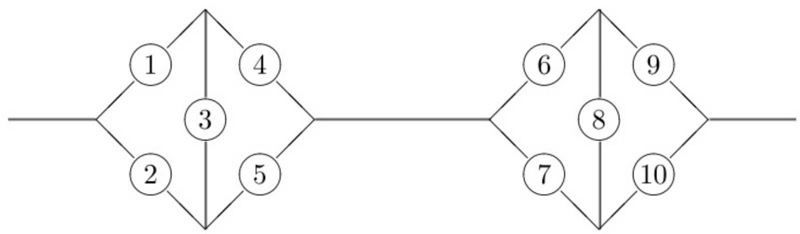

Figure 2: Reliability block diagram of a 10-component coherent system.

critical failure that may have a significant impact on the success of the mission. On the other hand, as the order statistic for mission abort increases (i.e., the mission can continue despite more components failing), the probability of completing the mission increases, too. This is because the system is still functioning despite the loss of one or more components, which indicates a higher level of redundancy and resilience in the system.

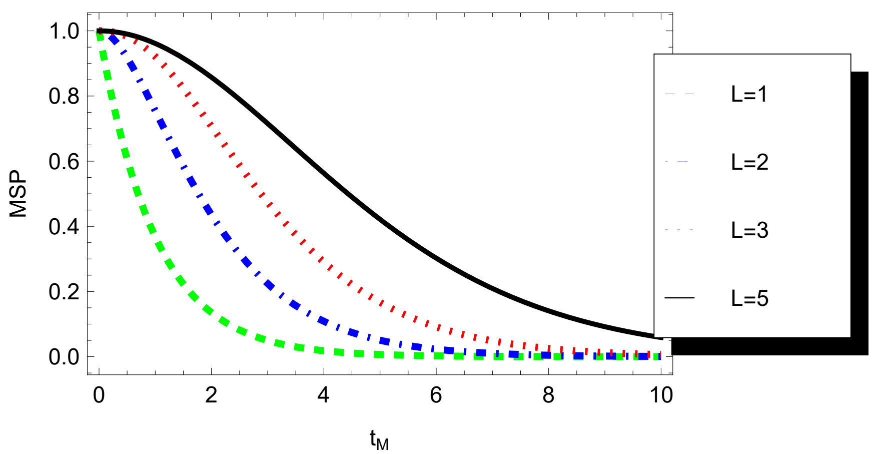

Figure 3: The mission success probability for $L = 1, 2, 3, 5$.

Some numerical values of the MSP are also summarized in Table 1. This table reflects the relationships between two variables - mission time (t_M) and mission success probability - while holding another variable (L) constant, as well as the relationships between two variables - aborting mission (L) and mission success probability - while holding another variable (t_M) constant. The results in Table 1 demonstrate that when the value of L rises, the probability of the mission succeeding increases for a certain value of t_M. This suggests a positive relationship between mission abortion and mission success probability, suggesting that, in some cases, mission abortion may increase the probability of success. The connection between the two may be explained by the fact that delaying a mission could offer more time to plan, organize, and carry it out, possibly improving the probability of success.

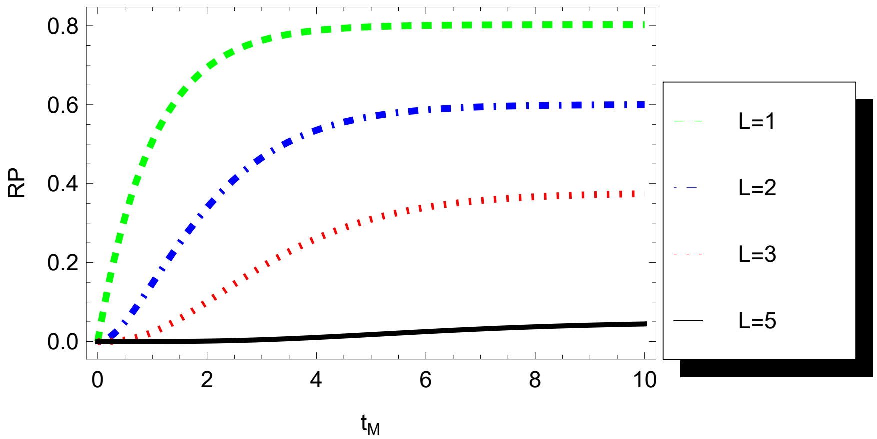

Figure 4: The rescue procedure for $L = 1, 2, 3, 5$ and $t_{r(L)} = 0.5$.

Table 1: Mission success probability for different values of L and t_M.

	$t_M = 0.5$	$t_M = 2$	$t_M = 3$	$t_M = 6$	$t_M = 7$	$t_M = 9$
$L = 1$	0.6065	0.1353	0.0497	0.0024	0.0009	0.0001
$L = 2$	0.9175	0.4349	0.2239	0.0228	0.0101	0.0019
$L = 4$	0.9603	0.8303	0.6529	0.2072	0.1283	0.0449
$L = 7$	0.9901	0.8600	0.7242	0.3352	0.2444	0.1229

On the other hand, we can see that, for any given value of L, the probability of completing the mission decreases as the mission time (t_M) increases.

Using Equation (5), we have also determined the probability of completing the rescue procedure for different scenarios where the mission abort occurs at different order statistics, as shown in Figure 4. As expected, the probability of completing the rescue procedure is higher when the mission abort occurs at the first order statistic, indicating a critical failure that has a significant impact on the rescue procedure's success. Conversely, if the mission abort occurs at a higher order statistic, the probability of completing the rescue procedure is lesser. This is because the system has experienced multiple failures, indicating a lower level of redundancy and resilience, which can increase the risk of further failures and reduce the probability of completing the rescue procedure successfully. Understanding the impact of L on the probability of completing the rescue procedure is crucial in designing reliable and robust systems for emergency situations. By determining a suitable L, one can improve the probability of mission success and ensure the safety and security of the rescue operation and its personnel.

According to Figure 4, it is clear that, for various values of L, the probability of successfully completing the rescue process gets larger with an increase in the duration of the mission. Hence, according to Table 2, for various values of L, the probability of successfully completing the rescue procedure gets larger with an increase in the duration of the rescue period.

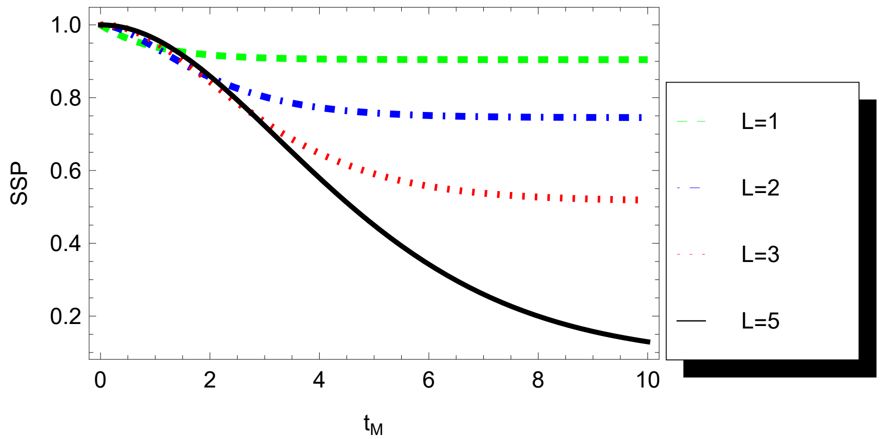

Figure 5: System survival probability for $L = 1, 2, 3, 5$ and $t_{r(L)} = 0.5$.

Overall, careful planning and preparation are necessary to ensure that the risks are minimized and the rescue procedure can be carried out successfully. This includes identifying the appropriate mission time and recovery period duration, ensuring that all necessary resources and equipment are available, and having a well-trained and experienced rescue team. By taking these measures, the probability of successfully completing a rescue procedure can be increased, even in the face of unforeseen challenges and risks.

Table 2: Probability of completing rescue procedure for components having $W(1, 10)$ distribution.

	$t_{r(L)} = 1$	$t_{r(L)} = 2$	$t_{r(L)} = 3$	$t_{r(L)} = 5$	$t_{r(L)} = 7$	$t_{r(L)} = 10$
$L = 1$	0.5074	0.6941	0.7628	0.7973	0.8020	0.8027
$L = 2$	0.1472	0.3393	0.4660	0.5702	0.5944	0.6000
$L = 3$	0.0234	0.1004	0.1891	0.3098	0.3572	0.3743
$L = 4$	0.0019	0.0160	0.0437	0.1068	0.1482	0.1716

Figure 5 depicts the graph of the probability of system survival computed by Equation (5). As we have mentioned earlier, this measure takes into account both the success of the mission and the success of any associated rescue procedure. The system survival probability decreases as the length of the mission period increases for different values of L. This is because a longer mission duration increases the probability of encountering unforeseen challenges or equipment failures during the mission, which can make it more difficult to successfully complete the mission and associated rescue procedures.

Also, it is evident from Figure 5 that the system survival probability initially decreases rapidly with increasing the mission duration and then levels off at a lower value. However, the rate of decrease in the survival probability varies for different values of L, with a higher value of L resulting in a steeper decrease in the system survival probability. Therefore, careful consideration of the appropriate values of the mission duration t_M and L is crucial during the planning and preparation stages of a mission and its associated rescue operation. By selecting appropriate values for these parameters, we can minimize the risks involved and increase the system survival probability. This may involve incorporating redundancy and backup systems into the mission design and providing comprehensive training for the crew to handle emergency situations. Moreover, it may also involve establishing protocols for communication, decision-making, and coordination between the mission control center and the crew in the field.

To determine the optimal value of L in this example, we shall examine various methodologies. For example, formula (9) can be used to derive L at an optimum value by varying predetermined values of parameter q, as illustrated in Table 3. If the system expert considers the parameter q to be 0.3, the signature vector indicates that the optimal value of parameter L is 3. On the other hand, if the expert deems q to be 0.7, the optimal value for L is 5. These results highlight the importance of selecting an appropriate value for q to determine the optimal value of L and emphasize the significance of the trade-off between mission success and system survival in this decision-making process.

Table 3: Choosing L^* according to various values of q.

q	$\sum_{l=1}^{j} s_l$	L^*
0.1	0.089	2
0.3	0.300	3
0.5	0.600	4
0.7	0.873	5

Recall that the optimization problem (7) provides an alternative approach to determine the optimal value of L by weighing a trade-off between the probability of mission success and system survival. Assume that $S^* = 0.65$. Also, suppose that the recovery period length is held constant at $t_{r(L)} = 0.2$. On the other hand, if the mission period length is extended in comparison to the recovery period, such as $t_M = 10$, the optimal value for L would be 2, indicating that the probability of system survival is significantly higher than that of mission success. In such a scenario, it is advisable to abort the mission without delay.

Table 4: The optimum values of L^* for $S^* = 0.65$ and various values of t_M.

t_M	L^*	$MSP(t_M, L^*)$	$S(t_M, L^*, 0.2)$
3.7	4	0.5250	0.6526
6	3	0.0915	0.6509
10	2	0.0063	0.8223

The probability of mission success and system survivability for various choices of L are shown in Table 5. As observed, the probability of system survival exceeds the specified value of $S^* = 0.65$ for L values of 1, 2, and 3. Notably, among all the values of L shown in the table, $L = 3$ demonstrates the best probability of mission success. It is important to note that the selected value of L affects the chances of mission success and system survivability, with different values of L leading to varied results. The significance of choosing an ideal value for L that strikes a balance between mission accomplishment and system survival is highlighted by these findings. Overall, this statement provides more detail and explanation of the methodologies and results presented, highlighting the significance of selecting an appropriate value for L based on the trade-off between mission success and system survival, recovery, and mission period lengths, and the predetermined probability of system survival

Table 5: The values of SSP and MSP for $t_M = 4$, $S^* = 0.65$, and various values of L.

L	$S(t_M, L, 0.2)$	$MSP(t_M, L)$
1	0.9636	0.0183
2	0.8594	0.1083
3	**0.7194**	**0.2900**
4	0.6196	0.4730
5	0.5848	0.5630
6	0.5811	0.5799
7	0.5810	0.5810
8	0.5810	0.5810

Figure 6 portrays the relationship between the total cost of the system and the cost of system loss for a cost of mission failure $C_F = 1$. The graph indicates that if the ratio C_L/C_F is reduced (signifying that the success probability of the mission is more significant than the system survival probability), the total cost incurred by the system decreases. Additionally, for small C_L/C_F, as the value of L increases, the overall cost imposed on the system decreases, implying that the mission's completion probability is of paramount importance. In such a scenario, it is better to abort the mission with a high value of L, and in fact, it may be preferable not to abort the mission at all. Furthermore, for large C_L/C_F, as the value of L increases, the total cost incurred by the system also increases, implying that the system's survival is of utmost importance. In such a scenario, it is better to abort the mission with a lower value of L. Overall, these findings underscore the importance of selecting an optimal value for L to balance the trade-off between mission success and system survival, as it has a significant impact on the total cost incurred by the system.

Our analysis of total system cost versus mission duration in Figure 7 reveals some key insights. For missions with a duration approaching the rescue period length, cost decreases with a higher abort component index L. This demonstrates aborting later system components is optimal when the mission timeline nears the rescue duration. In such cases, the short mission period means system survival probability remains high, even without abort. Thus, delaying aborts minimizes disruptions and costs. Conversely, for mission durations much longer than the rescue period, cost increases with larger L. Here, late abortions are suboptimal. As the mission progresses well beyond rescue length, system reliability declines. Late aborts therefore raise the probability of total system failure and associated costs. In essence, the optimal abort depends on the ratio of mission duration to rescue period. When mission time is comparable to rescue time, delaying aborts maintains system integrity while minimizing disruptions. But for long missions, timely abort is needed to avoid failure.

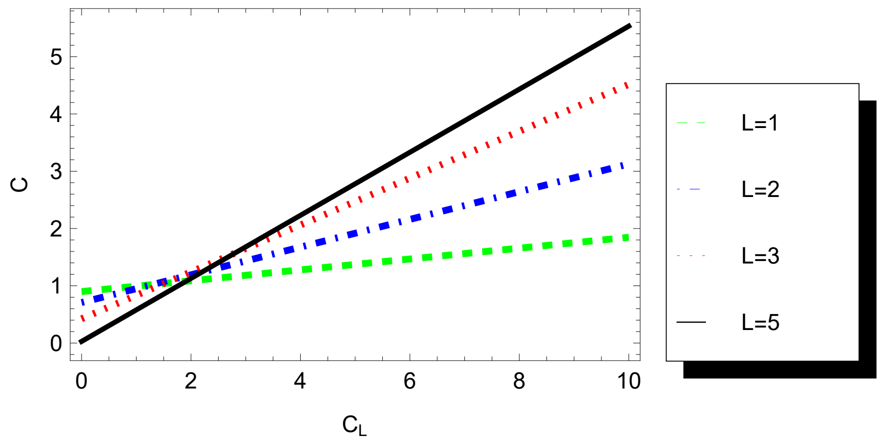

Figure 6: The total cost of the system for $L = 1, 2, 3, 5$ and $t_{r(L)} = 0.5$.

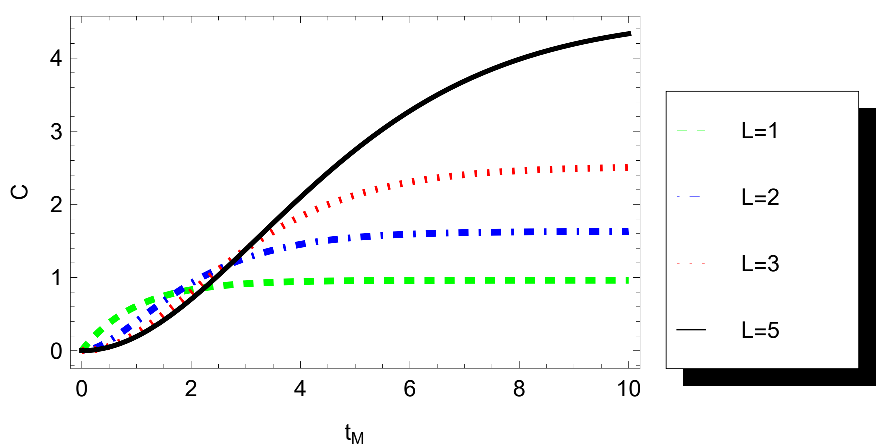

Figure 7: The total cost of the system for $L = 1, 2, 3, 5$ and $t_{r(L)} = 0.5$.

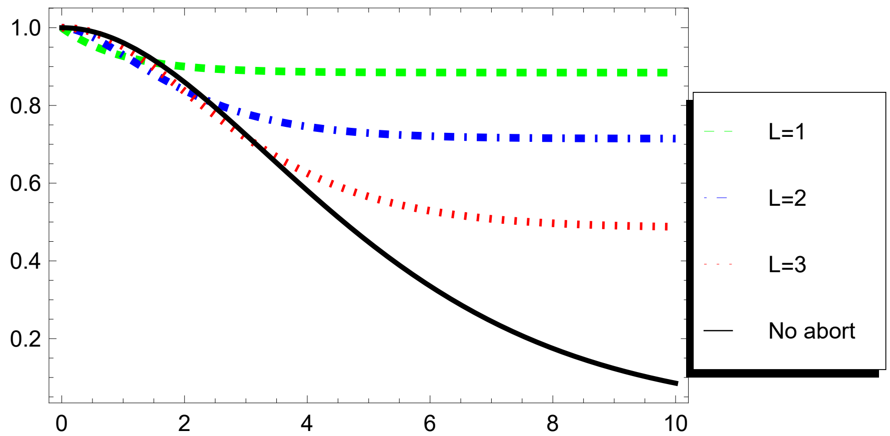

Figure 8: The system survival probability for $L = 1, 2, 3$ and $t_{r(L)} = 0.5$.

Finally, we compare the system reliability function (2), which does not consider the mission abort at all, with the system survival probability (6) which takes into account the mission abort policy described in the paper. As depicted in Figure 8, the non-abort model demonstrates a slightly higher probability for short mission durations (i.e., for small t_M). However, as t_M increases, the models incorporating mission abort, obviously, exhibit a greater probability of survival.

5.2 Simulation Study

In this section, we perform a simulation study in order to assess the MSP and RP of a network coherent system pictured in Figure 9 with an abort threshold policy and all component/vertex (or edge/link) lifetimes following the Weibull distribution with shape and scale parameters α and λ, respectively. The developed simulation results provide practical insights into how different abort thresholds, mission times and shape parameters affect the probabilities of mission success and rescue procedure. Each combination of the mission time and the abort threshold is iterated $10,000$ times. All results, including figures and numerical computations, are obtained using Mathematica Program System version 10 and R Program System version 4.3.3. Note that in practice, signature vectors of critical systems correspond to the higher redundancy (more zeroes before the first nonzero component of the vector). The signature vector for this 9-network coherent system can be calculated as follows:

$$s = (0, 0, 1/42, 1/14, 4/21, 11/28, 5/21, 1/12, 0);$$

For simulating the MSP and the RP, one can create a simulation based on the given signature vector and treat it as a discrete probability distribution. Then, as an example, to simulate the MSP, we iterate over a large number of trials to estimate the probability that both T and $X_{L:n}$ exceed t_M. The algorithm is as follows:

1. **Generate Component Lifetimes:** For each component, generate lifetimes from a distribution (e.g., exponential or Weibull), reflecting typical failure times.

2. **Determine Order Statistics:** For each trial, sort the component lifetimes and extract $X_{L:n}$, where L is the failure threshold chosen for the mission abort and $X_{L:n}$ is the Lth order statistic of the component lifetimes.

3. **Calculate System Lifetime $\boldsymbol{T}$:** Select T based on the signature vector by interpreting it as the probability of each order statistic defining the system lifetime. To be more precise,

   - Draw an index j according to the probabilities s_j from the signature vector.
   - Set $T = X_{j:n}$.

4. - Estimate MSP: For each trial, check if $T > t_M$, $X_{L:n} > t_M$ and $T - X_{L:n} > t_{r(L)}$ hold. Count the successful trials and divide by the total number of trials to estimate $\mathbb{P}(T > T_M, X_{L:n} > T_M)$.
   - Estimate RP: For each trial, check if $T > X_{L:n}$ and $X_{L:n} < t_M$. Count the successful trials and divide by the total number of trials to estimate $\mathbb{P}\left(T - X_{L:n} > t_{r(L)} \mid X_{L:n} < \min(T, t_M)\right)$.

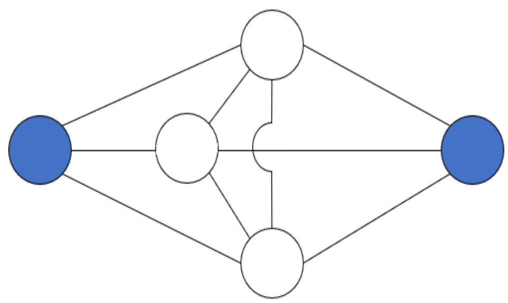

Figure 9: Reliability block diagram of a 9-network coherent system. Blue nodes are start/terminal.

Figure 10 illustrates the MSP across various values of the abort threshold parameter, L, for a Weibull distribution characterized by a shape parameter 2 and a scale parameter 10. The simulation, consisting of 10,000 repetitions, demonstrates that as the abort threshold L increases, the probability of mission success also increases. This relationship arises because larger values of L allow for the greater number of component failures. From a practical perspective, selecting a higher threshold L enables the system to tolerate additional component failures before reaching the abort criterion, effectively enhancing the probability of mission completion. Furthermore, an increase in the MSP, as represented by L, suggests that the system is better equipped to endure further degradation while still achieving its mission objectives.

Figure 11 illustrates the analysis of the MSP as a function of the Weibull shape parameter, with the threshold parameter $L = 3$ being constant. Observe that for the sufficiently small values of t_M, the larger Weibull shape parameter correlates with the increased probability of mission success (i.e., a lower probability of mission abort). This observation can be attributed to the fact that the larger shape parameter implies that components are more likely to endure the early stages of the mission, resulting in a reduction of early failures. Consequently, the larger shape parameter indicates greater reliability, suggesting that a sufficient number of components will function effectively throughout the mission duration. However, this

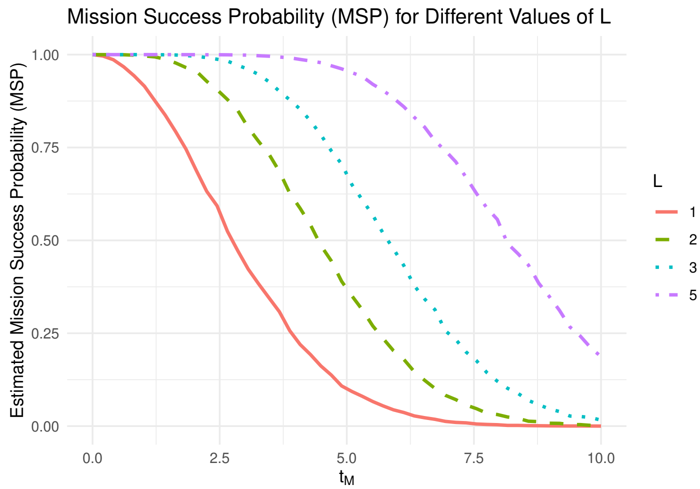

Figure 10: Estimated Mission success probability for $L = 1, 2, 3, 5$.

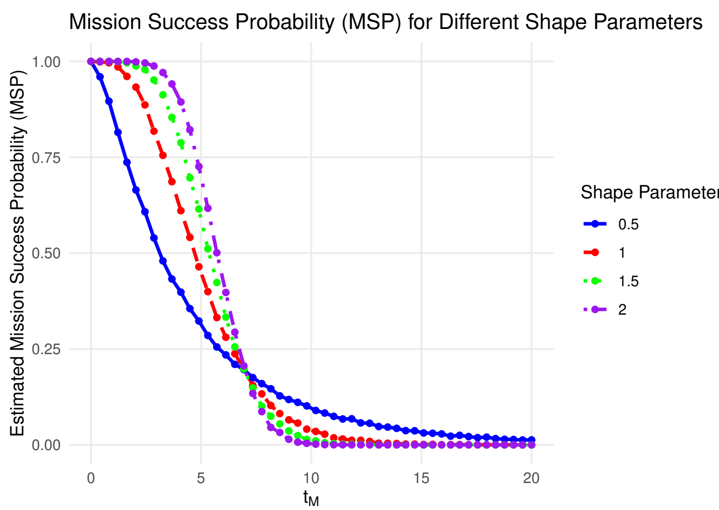

Figure 11: Estimated Mission success probability for $\alpha = 0.5, 1, 1.5, 2$.

relationship persists only until a certain time after which the larger Weibull shape parameter leads to the smaller probability of mission success.

Figure 12 illustrates the simulated rescue probability for various values of the abort threshold parameter L, utilizing the Weibull distribution with the shape parameter 2, the scale parameter 10 and $t_{r(L)} = 0.5$. This simulation, consisting in 10,000 iterations, presents the relationship between the abort threshold L and the estimated probability of completing the RP for different mission times t_M. It is evident from the figure that as the L abort threshold increases, the probability of a successful rescue decreases. This phenomenon can be attributed to the nature of the abort threshold: the larger value of L means that the system can endure more failures before commencing a rescue procedure, resulting in reduced redundancy and resilience.

Figure 13 illustrates the probability of successful completion of the RP as a function of the Weibull

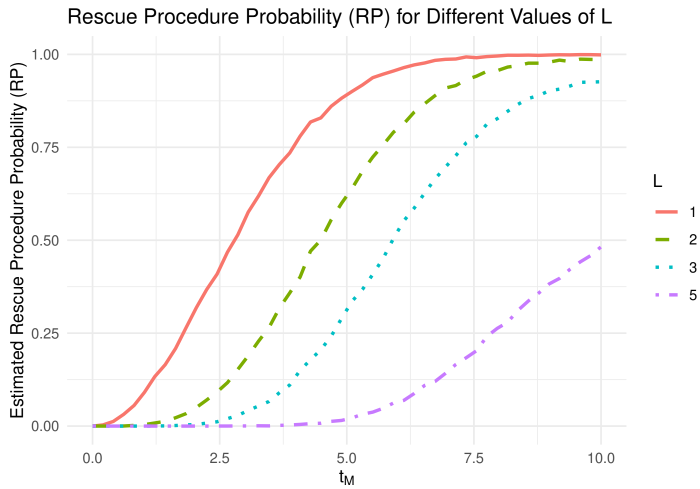

Figure 12: Estimated rescue procedure for $L = 1, 2, 3, 5$.

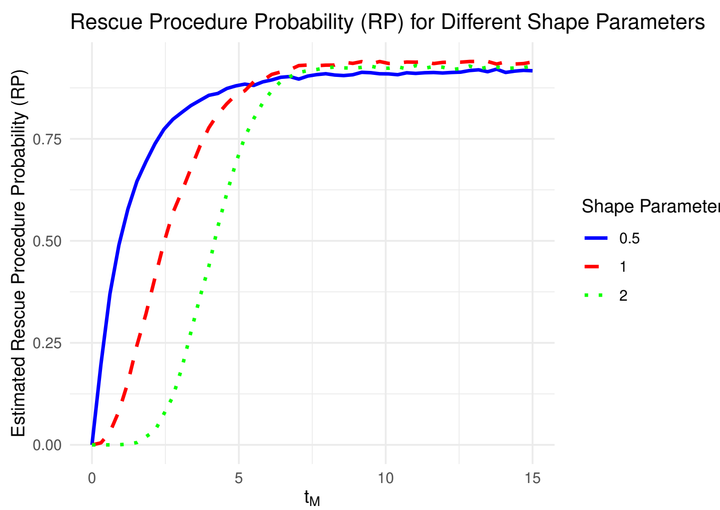

Figure 13: Estimated rescue procedure for $\alpha = 0.5, 1, 2$.

distribution shape parameter α (for a constant abort threshold $L = 3$ and a rescue time $t_{r(L)} = 0.5$). Its analysis is similar to that of the previous figure. We see an interesting phenomenon in these last two figures: the probability of a successful RP increases with t_M. This is because the proportion of successful events is calculated only for those realizations of system lifetimes that are larger than t_M, whereas the 'severity' of the restriction imposed by L and leading to aborting increases with t_M. Thus, the robustness of the operating (not aborted) system increases with t_M.

6 Conclusions

A mission abort policy and the subsequent rescue operation are effective tools for increasing the survivability of systems performing missions of fixed or variable duration. On the other hand, aborting a mission too early decreases the mission success probability, whereas aborting it too late or not aborting at all will decrease survivability. Therefore, these two aspects should be taken into account when considering the corresponding optimization procedures. This problem has been intensively studied in recent literature in various settings. A brief literature review is given in the Introduction. It is important to note that most existing publications focus on systems without detailed examinations of their underlying structures, thereby addressing primarily integrated one-component, black-box systems. Thus, valuable information on the degradation of a system manifested through the dynamic (in time) numbers of failed components is lost.

In contrast, our study is the first to explore general multi-component coherent systems proposing a novel methodology based on the corresponding signatures. It enables the consideration of the number of failed components of a system as the variable influencing the decision to abort. The corresponding optimization problems are formulated based on the traditional trade-off between mission success probability and survivability and on minimizing the cost. Furthermore, the approach that suggests the direct setting of this parameter (e.g., via expert opinions) was also discussed. Our detailed numerical illustrations with the corresponding analysis, justify theoretical findings.

There is significant potential for further expansion and development of the proposed innovative approach. It has been noted that characterization through signatures is applicable to the exchangeable lifetimes of components. Recent literature includes numerous studies aimed at generalizing the concept of signatures for non-identical and dependent components, which could serve as a foundation for future research on mission abort scenarios in multi-component systems. Additionally, integrating our methodology with system maintenance presents an intriguing avenue for exploration, further enhancing our investigations into mission abort strategies for multi-component systems.

References

[1] Arnold, B.C., Balakrishnan, N. and Nagaraja, H.N. (1992). *A First Course in Order Statistics.* Wiley, New York.

[2] Barlow, R. and Proschan, F. (1981). *Statistical Theory of Reliability and Life Testing: Probability models.* Hold, Reinhart and Wiston, Inc.

[3] Cao, S. and Wang, X. (2023). Mission abort strategy for generalized k-out-of-n: F systems considering competing failure criteria. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 1748006X231170909.

[4] Cheng, G., Li, L., Zhang, L., Yang, N., Jiang, B., Shangguan, C. and Su, Y. (2022). Optimal joint inspection and mission abort policies for degenerative systems. *IEEE Transactions on Reliability*, **72** (1), 137–150.

[5] Cheng, G., Shen, J., Wang, F., Li, L. and Yang, N. (2024). Optimal mission abort policy for a multi-component system with failure interaction.*Reliability Engineering & System Safety*, **242**, 109791.

[6] David, H. A., and Nagaraja, H. N. (2004). *Order statistics.* Wiley, New Jersey.

[7] Da, G., Zheng, B. and Hu, T. (2012). On computing signatures of coherent systems. *Journal of Multivariate Analysis*, **103** (1), 142–150.

[8] da Silva Rodrigues, A. J., Cavalcante, C. A. V., Alberti, A. R., Scarf, P., and Alotaibi, N. M. (2023). Mathematical modelling of mission-abort policies: a review. *IMA Journal of Management Mathematics*, **34** (4), 581–597.

[9] Finkelstein, M., Cha, J.H., and Ghosh, S. (2021). Optimal inspection for missions with a possibility of abortion or switching to a lighter regime. *TOP*, **29**, 722–740 .

[10] Gao, K., Xiao, H., Mi, J., Peng, R., and Zhai, Q. (2020, October). Optimal Abort Policy of a Distributed System of Computers with Weibull Failure Time. *)In 2020 Global Reliability and Prognostics and Health Management* (PHM-Shanghai) (pp. 1-5). IEEE.

[11] Kochar, S.C., Mukerjee, H. and Samaniego, F.J. (1999). The 'signature' of a coherent system and its application to comparisons among systems. *Naval Research Logistics*, **46**, 507–523.

[12] Levitin, G. and Finkelstein, M. (2018a). Optimal mission abort policy for systems in a random environment with variable shock rate. *Reliability Engineering & System Safety*, **169**, 11–17.

[13] Levitin, G. and Finkelstein, M. (2018b). Optimal mission abort policy with multiple shock number thresholds. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, **232** (6), 607–615.

[14] Levitin, G. and Finkelstein, M. (2022). Making mission abort decisions for systems operating in random environment. *In Multicriteria and Optimization Models for Risk, Reliability, and Maintenance Decision Analysis: Recent Advances* (pp. 283-304). Cham: Springer International.

[15] Levitin, G., Finkelstein, M. and Huang, H. Z. (2019). Optimal abort rules for multi-attempt missions. *Risk Analysis*, **39** (12), 2732–2743.

[16] Levitin, G., Finkelstein, M. and Huang, H. Z. (2020). Optimal mission abort policies for multistate systems. *Reliability Engineering & System Safety*, **193**, 106671.

[17] Levitin, G., Xing, L. and Dai, Y. (2017). Mission abort policy in heterogeneous nonrepairable 1-out-of-N warm standby systems. *IEEE Transactions on Reliability*, **67** (1), 342–354.

[18] Levitin, G., Xing, L. and Dai, Y. (2022). Optimal mission aborting in multistate systems with storage. *Reliability Engineering & System Safety*, **218**, 108086.

[19] Levitin, G., Xing, L. and Dai, Y. (2023a). Optimal task aborting policy and component activation delay in consecutive multi-attempt missions. *Reliability Engineering & System Safety*, **238**, 109482.

[20] Levitin, G., Xing, L.and Dai, Y. (2023b). Optimal task sequencing and aborting in multi-attempt multi-task missions with a limited number of attempts. *Reliability Engineering & System Safety*, **236**, 109309.

[21] Levitin, G., Xing, L., and Dai, Y. (2023c). Optimal aborting policy for shock exposed missions with random rescue time. *Reliability Engineering & System Safety*, **233**, 109094.

[22] Levitin, G., Xing, L. and Dai, Y. (2024). Optimal task aborting and sequencing in time constrained multi-task multi-attempt missions. *Reliability Engineering & System Safety*, **241**, 109702.

[23] Liu, Y., Chen, Y. and Jiang, T. (2018). On sequence planning for selective maintenance of multi-state systems under stochastic maintenance durations. *European Journal of Operational Research*, **268** (1), 113–127.

[24] Liu, L., Yang, J. and Yan, B. (2024). A dynamic mission abort policy for transportation systems with stochastic dependence by deep reinforcement learning. *Reliability Engineering & System Safety*, **241**, 109682.

[25] Myers, A. (2009). Probability of loss assessment of critical k-out-of-n: G systems having a mission abort policy. *IEEE Transactions on Reliability*, **58** (4), 694–701.

[26] Navarro, J., Ruiz, J.M. and Sandoval, C.J. (2005). A note on comparisons among coherent systems with dependent components using signature. *Statistics & Probability Letters*, **72**, 179–185.

[27] Peng, R. (2018). Joint routing and aborting optimization of cooperative unmanned aerial vehicles. *Reliability Engineering & System Safety*, **177** , 131–137 .

[28] Peng, R. , Zhai, Q., Xing, L. , Yang, J. (2016). Reliability analysis and optimal structure of series-parallel phased-mission systems subject to fault-level coverage. *IIE Transactions*, **48** (8), 736–746.

[29] Qiu, Q. , Cui, L. (2019a). Gamma process based optimal mission abort policy. *Reliability Engineering & System Safety*, **190** , 106496 .

[30] Qiu, Q. and Cui, L. (2019b). Optimal mission abort policy for systems subject to random shocks based on virtual age process. *Reliability Engineering & System Safety*, **189** , 11–20 .

[31] Qiu, Q. , Cui, L. and Wu, B. (2020). Dynamic mission abort policy for systems operating in a controllable environment with self-healing mechanism. *Reliability Engineering & System Safety*, **203** , 107069.

[32] Qiu, Q., Maillart, L. M., Prokopyev, O. A. and Cui, L. (2022). Optimal condition-based mission abort decisions. *IEEE Transactions on Reliability*, **72**(1), 408–425.

[33] Samaniego, F.J. and Shaked, M. (2008). Systems with weighted components. *Statistics and Probability Letters*, **78**, 815–823.

[34] Shaked, M. and Shanthikumar, J.G. (2007). *Stochastic Orders*. Springer, New York.

[35] Wei, F., Zhou, S., Ma, X. and Yang, L. (2023). Optimal mission abort planning for partially observable system. *In 9th International Symposium on System Security, Safety, and Reliability (ISSSR)* (pp. 71–76).

[36] Wu, C., Zhao, X., Qiu, Q., Sun, J. (2021). Optimal mission abort policy for k-out-of-n: F balanced systems. *Reliability Engineering & System Safety*, **208**, 107398.

[37] Yang, L. , Sun, Q. , Ye, Z.-S. (2019). Designing mission abort strategies based on early-warning information: Application to UAV. *IEEE Transactions on Industrial Informatics*, **16** (1), 277–287.

[38] Yang, L., Wei, F. and Qiu, Q. (2023). Mission risk control via joint optimization of sampling and abort decisions. *Risk Analysis.*

[39] Zhao, X., Chai, X., Sun, J. and Qiu, Q. (2022). Joint optimization of mission abort and protective device selection policies for multistate systems. *Risk Analysis*, **42** (12), 2823–2834.

[40] Zhao, X., Sun, J., Qiu, Q. and Chen, K. (2021). Optimal inspection and mission abort policies for systems subject to degradation. *European Journal of Operational Research*, **292** (2), 610–621.

[41] Zhao, X., Lv, Z., Qiu, Q. and Wu, Y. (2023a). Designing two-level rescue depot location and dynamic rescue policies for unmanned vehicles. *Reliability Engineering & System Safety*, **233**, 109119.

[42] Zhao, X., Liu, H., Wu, Y. and Qiu, Q. (2023b). Joint optimization of mission abort and system structure considering dynamic tasks.*Reliability Engineering & System Safety*, **234**, 109128.