

## Optimal mission abort policy for the heterogeneous two-component system with constraints on simultaneous components' rescue

Gregory Levitin<sup>a</sup> and Maxim Finkelstein<sup>b,c</sup>

<sup>a</sup>NOGA - Israel Independent System Operator, Israel

E-mail: gregory.levitin@sysmc.co.il

<sup>b</sup>University of the Free State, Bloemfontein, South Africa,

E-mail: FinkelM@ufs.ac.za

<sup>c</sup>Department of Management Science, University of Strathclyde, Glasgow, UK

**Abstract.** At many instances, mission abort in systems performing important tasks is followed by a rescue procedure that is mostly aimed at survival of costly systems. Existing mission aborting models assume that when more than one component is involved in accomplishing a mission, the rescue procedures for individual components are performed independently. However, systems often have no sufficient resources to perform the rescue procedures for several/all components simultaneously. Then the mission abort for some components can be delayed or cancelled. This paper considers the two-component system in which simultaneous rescue of both components is prohibited. It suggests algorithm for evaluating the expected mission losses for this setting. In addition, it formulates and solves the mission abort policy optimization problem and presents practical examples that show that the operational dependence between components effects the mission success metrics and the corresponding mission abort policy.

Keywords: mission abort; rescue procedure; mutual dependence

### Acronyms

NEML normalized expected mission losses

HPP homogeneous Poisson process

MAP mission abort policy

MSP mission success probability

RP rescue procedure

UAV unmanned aerial vehicle

VM virtual machine

## Notation

$\tau$	mission time
$T_{i,m}$	random arrival time of $m$ -th shock affecting $i$ -th component
$m_i$	number of shocks triggering component's $i$ mission abort (decision variable)
$\xi_i$	time from the beginning of the mission during which component $i$ is allowed to abort its mission (decision variable)
$\vartheta_i$	time from the beginning of the mission during which component is $i$ allowed to abort its mission if the abort was postponed (decision variable)
$y_i$	random time of component $i$ RP termination (completion of the RP or failure)
$\Lambda_i$	arrival rate of shocks affecting $i$ -th component during the mission
$\lambda_i$	arrival rate of shocks affecting $i$ -th component during the RP
$q_i(k)$	conditional probability that component $i$ survives $k$ -th shock given that it survived previous shocks
$Q_i(k)$	probability that component $i$ survives $k$ shocks
$F_i(k)$	probability that component $i$ fails upon experiencing $k$ -th shock
$\omega_i$	probability that component $i$ survives the first shock
$\Omega_i$	shock resistance deterioration factor for component $i$
$P(t,i,\lambda)$	occurrence probability of $i$ shocks in $[0,t)$ given that the shock rate is $\lambda$
$\varphi_i(t)$	duration of the RP started at time $t$ from the beginning of the mission
$a_i$	RP duration parameter (for $\varphi_i(t)=a_i t$ )
$\psi_i(y)$	mission abort time for which the RP completion time is $y$ for component $i$
$c_i$	cost associated with failure/loss of component $i$
$C_F$	cost associated with mission failure
$R$	MSP
$E$	NEML
$\alpha_i(x,y)$	probability that component $i$ is performing the RP during the entire time interval $[x,y)$
$\beta_i(x,y)dt$	probability that component $i$ starts the RP before time $x$ and fails during the RP in the time interval $[y,y+dt)$

$\gamma_i(x, y)dt$  probability that component  $i$  starts the RP before time  $x$  and completes the RP in time interval  $[y, y + dt)$

$1(x)$  logical function:  $1(\text{TRUE})=1, 1(\text{FALSE})=0$ .

## 1. Introduction

Starting with the seminal paper by Meyers [1], mission abort theory and its applications have developed already in a well-elaborated discipline in reliability and efficiency analyses of complex technical systems. Ensuring survival of costly, important systems can be at certain instances not less or even more crucial than completing the mission task. As systems degrade while performing a mission, probabilities of failures with substantial adverse effects increase in time. Therefore, to save a system, a mission can be aborted, and a rescue procedure (RP) can be carried out. To establish unambiguous criteria for defining the deterioration status that triggers abort, a mission abort policy (MAP) must be developed. Such policy should include decision variables reflecting the components status as well as their corresponding threshold values for triggering the abort. The recent comprehensive reviews of studies on mission abort can be found in [2], [3].

The above reasoning can be also applied to the multicomponent distributed systems performing missions or a tasks having fixed duration. Systems components can be heterogeneous and operate in different environments and different locations. Our paper describes the MAP for these systems, and the following brief literature review is mostly devoted to this case.

Various MAPs for the distributed systems with multiple components have been studied. In [4], fixed and attempt-dependent MAPs were modeled for a homogeneous multi-component multi-attempt system operating under different shock environments during PM and RP. In [5], the component-dependent MAP was co-optimized with the subtask distribution policy for a multi-component system performing a mission with multiple subtasks. In [6], a dynamic MAP was optimized for a homogeneous multi-component work-sharing system operating under a renewal process of shocks. Based on the amount of the mission work and the amount of the remaining damage, the policy determines the distribution of the remaining available components to performing the primary mission and the damage reduction procedure after each shock. In [7], a MAP was jointly optimized with

the routing and hitting policies for UAVs executing a target hitting mission. In [8], the attempt-dependent MAP was optimized for a multi-attempt multi-component system where each component may independently complete a mission and re-attempt it if being saved during the RP. In [9], the MAP was optimized for a homogeneous multi-component work-sharing system that must perform a specified amount of work. In [10], this MAP was extended to be a policy, that determines the number of components that should continue the mission whereas the rest of the operating components should abort the mission and start the RP when the triggering condition is met. In [11], MAPs for multi-component multi-state system with multiple abort criteria were analysed. In [12], MAP was co-optimized with the component activation delay for a multi-component system where multiple components may be activated consecutively with a fixed delay.

In [13], the MAP was co-designed with the inspection policy for a multi-component system with failure interactions. The abort is triggered when the system predictive reliability (updated based on degradation and age information) falls below a specified threshold. In [14], the component/attempt-dependent MAP was co-optimized with the component activation policy for a heterogeneous multi-component, multi-attempt system. In this work, the multiple attempts performed by different components may be activated according to a pre-defined schedule that allows overlaps, and the common abort command is issued upon the mission completion by any component. In [15], MAP for multi-component transportation systems with dependence between components was considered. In [16], the mission abort policy was analysed for the case of common shocks simultaneously affecting all operating components. In [17], a dynamic MAP was obtained for the swarm of components with changing states using deep reinforcement learning. In [18], a general multi-component coherent system was considered and a methodology based on signatures was employed for defining MAP criterion. In [19], it is shown that using different MAPs for groups of identical components can be beneficial in multi-attempt multi-component missions. Gao et al. [20] considered the MAP for the distributed multi-component system with random task execution times to maximize the task completion probability. Zhao et al. [21] discussed joint optimization of the mission abort rules and system's structure minimizing costs for dynamic tasks. Cha et al. [22] have studied optimal abort policy for heterogeneous systems with partially repairable components. Peng [23]

considered joint routing and performance of several unmanned arial vehicles (i.e., the distributed system of components).

To the best of our knowledge, this work is the first to consider the mission abort for the two-component system with components operational dependencies that prevent them from performing component-wise RPs simultaneously. This setting is practically important and present certain modelling and computational challenges. Indeed, in some cases when more than one component of the distributed system is involved in accomplishing a mission, a system has no ability to perform the RP of several/all components simultaneously because of the limited RP resources or the specific RP conditions. In such cases, the mission abort and the RP activation of some components can be postponed until termination (failure or completion) of the RP performed by the other components. The described dependence in the pattern of components' operation affects the overall mission success metrics that must be specifically developed to account for this scenario. The latter, along with the corresponding analysis, is the goal of this study.

The paper contributes to the state of the art by considering new specific, practically important setting when two non-identical components perform the mission operating in different environments and only one component can perform the RP at any moment. It suggests algorithm for evaluating expected mission losses for this setting. In addition, it formulates and solves the MAP optimization problem and presents practical examples illustrating the suggested methodology.

## 2. Problem statement

A system consisting of two statistically heterogeneous, but functionally identical components must accomplish a mission. Any component can complete a mission if it does not fail in operation during time  $\tau$ , thus exhibiting an important operational redundancy that increases the chance of a mission success. The components perform the mission simultaneously. During performing the mission task, each operating component  $i$  ( $i \in \{1,2\}$ ) is exposed to a specific random environment modeled by the independent homogeneous Poisson processes (HPP) of shocks with rate  $\Lambda_i$ . The random arrival times of shocks are  $T_{i,1} < T_{i,2} < \dots$ . As the number of shocks survived by a component increase, the component deteriorates and the risk of its failure/loss on each shock increases with its number.

To reduce the loss probability, any component  $i$  can abort a mission execution if it experiences and survives the  $m_i$ -th shock. Following the mission abort, the RP is carried out with duration determined by the function  $\varphi_i(t)$ , where  $t$  is the time elapsed between the start of the mission and the beginning of the RP. RP is also performed in a random environment, modeled by the HPP of shock arrivals with rate  $\lambda_i$ , where  $\lambda_i$  can be different from  $\Lambda_i$ . As  $T_{i,m_i}$  increases, the remaining time required for completing the mission decreases. This makes aborting the mission less beneficial due to the decreasing conditional probability of failure in the remaining interval of time. Therefore, component  $i$  continues the mission if  $T_{i,m_i} \geq \xi_i$  where  $\xi_i \leq \tau$  is the time threshold after which the  $m_i$ -th shock does not trigger the mission abort.

At many instances in practice, the RP resource limitation does not allow simultaneous RP of both components. Therefore, if at time  $T_{i,m_i} < \xi_i$  when component  $i$  experiences the  $m_i$ -th shock, component  $3-i$ ,  $i=1,2$  performs its RP, then component  $i$  postpones the mission abort until termination (completion or failure) of this RP. See comparison between immediate and postponed RP in Fig. 1. (Note that notation  $3-i$ , for  $i=1,2$ , is just for convenience of notation).

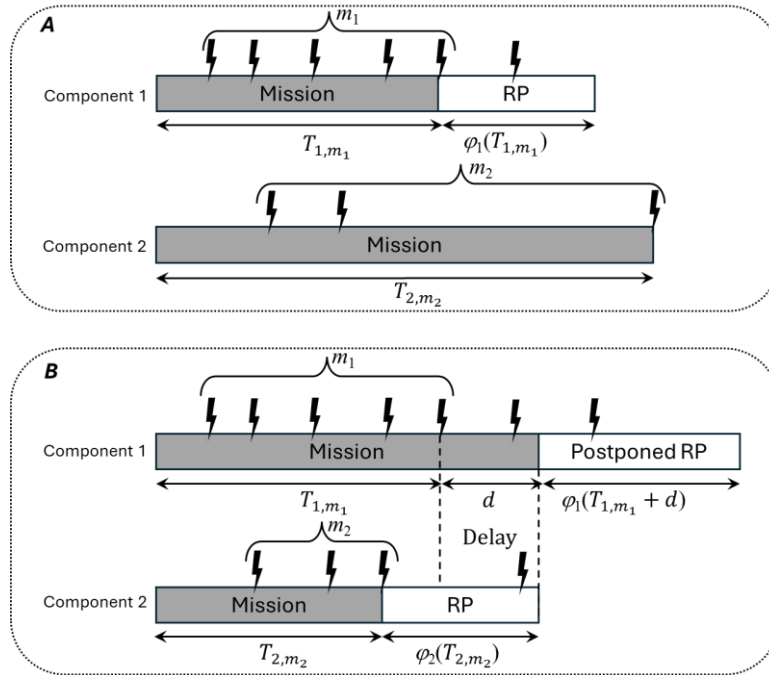


Fig. 1. Immediate RP of component 1(A) and RP of component 1 postponed till termination of RP of component 2 (B).

If after the termination of the  $(3-i)$ -th component's RP, a relatively short time remains until  $\tau$ , the component  $i$  has a good chance to complete the mission and should not abort it. Therefore, the postponed mission abort is allowed for component  $i$  only until time  $\vartheta_i$ . Fig. 2 presents the possible scenarios of successful mission accomplishment when any component  $i$  experiences at least  $m_i$  shocks during the mission and the component 1 aborts the mission first at time  $T_{1,m_1} < T_{2,m_2}$  and continues performing the RP at time  $T_{2,m_2}$  (grey and white rectangles correspond to the mission and the RP respectively). If  $T_{2,m_2} < \xi_2$  and the RP termination (completion or failure) time  $y_1 \leq \vartheta_2$ , component 2 aborts the mission and starts the RP at time  $y_1$  (see Fig. 2A). If  $T_{2,m_2} \leq \xi_2$  and  $y_1 > \vartheta_2$ , the component 2 does not abort the mission and continues operation till its completion (see Fig. 2B). If  $T_{2,m_2} \geq \xi_2$ , the component 2 never aborts the mission according to its mission abort policy (see Fig. 2C and D).

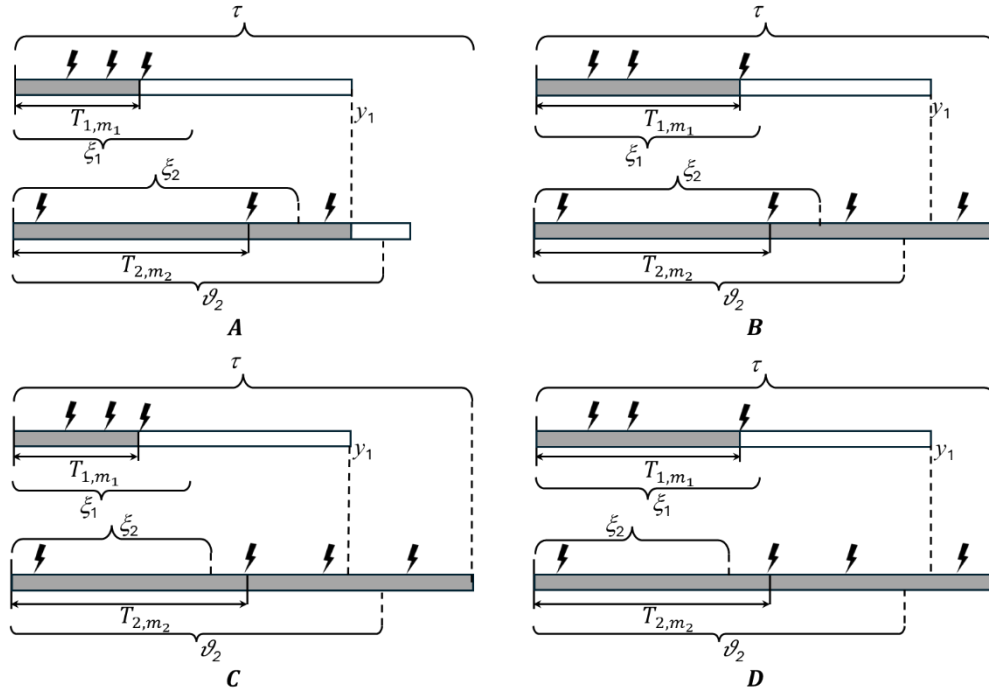


Fig. 2. Possible scenarios of mission accomplishment when any component  $i$  experiences at least  $m_i$  shocks and component 1 aborts the mission first.

In accordance with the above description, parameters  $m_i$ ,  $\xi_i$  and  $\vartheta_i$  for  $i=1,2$  define the mission abort policy (MAP), where  $\vartheta_i$  are the new parameters related to the delay in the RP that were not considered in the literature on mission abort. From the general reasoning

it follows that the too cautious MAP (low  $m_i$  and high  $\xi_i$  and  $\vartheta_i$ ) results in small MSP and components' loss probabilities. The riskier MAP (larger  $m_i$  and smaller  $\xi_i$  and  $\vartheta_i$ ) leads to the increase of both MSP and components' loss probabilities. Therefore, an optimal MAP should balance these effects. For the cost-wise setting, it can be achieved by minimizing the expected mission losses obtained in the following way

$$E(m_1, \xi_1, \vartheta_1, m_2, \xi_2, \vartheta_2) = c_1 f_1(m_1, \xi_1, \vartheta_1, m_2, \xi_2, \vartheta_2) + c_2 f_2(m_1, \xi_1, \vartheta_1, m_2, \xi_2, \vartheta_2) + C_F(1 - R(m_1, \xi_1, \vartheta_1, m_2, \xi_2, \vartheta_2)), \quad (1)$$

where  $f_i(m_1, \xi_1, \vartheta_1, m_2, \xi_2, \vartheta_2)$  and  $c_i$  are the probability of the  $i$ -th component failure/loss and the associated cost,  $R(m_1, \xi_1, \vartheta_1, m_2, \xi_2, \vartheta_2)$  is the MSP and  $C_F$  is the cost associated with the mission failure. Note that the components and mission failure events taken into account in (1) do not constitute the full group of events and reflect only the costs associated with the losses. The optimization problem can be formulated as finding  $m_1, \xi_1, \vartheta_1, m_2, \xi_2, \vartheta_2$  that minimize the normalized expected mission losses (NEML)

$$E(m_1, \xi_1, \vartheta_1, m_2, \xi_2, \vartheta_2)/C_F = f_1(m_1, \xi_1, \vartheta_1, m_2, \xi_2, \vartheta_2)c_1/C_F + f_2(m_1, \xi_1, \vartheta_1, m_2, \xi_2, \vartheta_2)c_2/C_F + 1 - R(m_1, \xi_1, \vartheta_1, m_2, \xi_2, \vartheta_2). \quad (2)$$

By minimizing the NEML, the system management either maximizes the profit achieved in the mission or minimizes expenses associated with the mission (in the non-profit case). The NEML corresponding to the optimal abort policy should be compared with 1 (which is the NEML in the case of withdrawal from the mission). If the NEML exceeds the value of 1, starting the mission has no sense as the withdrawal is more beneficial.

The following assumptions are made for the considered model:

1. Only shocks can cause components failures/losses. This assumption is relevant for the relatively short missions performed in hostile environments, where probability of internal failures is negligible compared with probability of failures due to external impacts.
2. The operation and rescue costs are negligible compared with the costs of components losses and mission failure. In many practical applications, operational costs (e.g., power or fuel consumption, communication and decision-making costs, shock detection costs) are considerably lower than the costs associated with component losses (lost equipment,

environmental damage) and those of the mission failure (financial, technical, or political consequences).

3. The shock detection mechanism is perfect, which means that all shocks are fully observable and are counted without mistakes.
4. The RP of component  $i$  can start immediately after detection of the  $m_i$ -th shock or after termination of the RP of component  $3-i$ . This assumption is relevant when no delays related to communication/decision making or RP preparation exist or the delays are negligible and no additional shocks can affect the system component between making the decision to abort the mission and activating the RP.
5. Components cannot resume the mission after completion of their RP. This assumption is relevant when the failed mission cannot be repeated because of economic, tactical, technical or time constraints.

Assumptions 1-5 are relevant for a wide range of practical situations. Two application examples are considered in this paper (below and in Section 4).

Consider two automatically guided UAVs that aim to accomplish a cargo delivery mission. The mission is completed if, at least, one of the UAVs delivers its cargo. Using two UAVs provides redundancy aimed at reducing risk of the delivery mission failure. To accomplish the delivery task, each UAV must cover a certain distance to the destination point, which takes time  $\tau$ . During the flight, each UAV  $i$  is exposed to random shocks from HPP with rate  $\lambda_i$  caused by electronic interference, which may destroy the UAV's control equipment causing the UAV's crash. The UAVs keep different altitudes, which allows to consider the shock processes affecting them as independent and different, whereas the distance to the destination point can be considered as approximately the same. As the number of experienced shocks increases, the interference filters that protect the UAVs deteriorate due to overheating, causing reduction of their resistance to shocks.

When the  $m_i$ -th shock strikes the UAV  $i$  in  $[0, \xi_i)$   $\xi_i < \tau$ , the UAV should abort the delivery task and activate the RP to reduce the UAV's failure/loss probability. To perform the RP, the UAV descends to a low altitude, where the interference rate  $\lambda_i$  is considerably smaller. At this altitude, there is a high risk of crashing into the ground obstacles. Therefore, manual control becomes necessary, and a technician needs to intervene and guide the UAV to the

closest landing position. The RP time  $\varphi_i(t)$  depends on the UAV position at time  $t$  when it aborts its mission. As only one manual override station is available to guide a UAV back, no more than one RP can be performed simultaneously. Therefore, UAV  $i$  experiencing  $m_i$ -th shock at time  $t < \zeta_i$  postpones the mission abort if UAV  $3-i$  already performs its RP at time  $t$ . The UAVs  $i$  mission can be aborted only when the technician completes the previous RP before time  $\vartheta_i$ .

Another example of a computational system performing a data processing task is presented in Section 4.

### 3. The Expected Mission Losses

#### 3.1. Components' shock resistance and shock occurrence probabilities

Let  $q_i(k)$  denote the conditional probability that component  $i$  survives the  $k$ -th shock given that it had survived all previous shocks ( $q_i(0) \equiv 1$ ). For example, according to the shock model of [24, 25],  $q_i(k)$  for  $k > 0$  can be defined as

$$q_i(k) = \omega_i \Omega_i(k), \quad i = 1, 2, \quad (3)$$

where  $\omega_i$  and  $\Omega_i(k)$  denote the survival probability under the first shock affecting the component and its shock resistance deterioration factor, respectively. Assume a specific form of this function, i.e.,  $\Omega_i(k) = \Omega_i^{k-1}$ , which is a decreasing function of argument  $k$  with  $0 < \Omega_i < 1$  modeling the decreasing survival probability at each shock as the number of survived shocks increases. Thus, the probability that the  $i$ -th component survives  $K$  shocks under this assumption is

$$Q_i(K) = \prod_{k=1}^K q_i(k) = \omega_i \Omega_i^{\frac{K(K-1)}{2}}. \quad (4)$$

The probability that component  $i$  fails upon experiencing the  $K$ -th shock after surviving all previous shocks is

$$F_i(K) = (1 - q_i(K)) \prod_{k=1}^{K-1} q_i(k) = (1 - q_i(K)) Q_i(K-1). \quad (5)$$

The probability that  $k$  shocks occur to component  $i$  from an HPP with rate  $\Lambda_i$  during time interval  $[0, t)$ , is

$$P(t, k, \Lambda_i) = e^{-\Lambda_i t} \frac{(\Lambda_i t)^k}{k!}. \quad (6)$$

Due to independence of increments of the Poisson process,  $P(x, k, \Lambda_i)P(t-x, h, \Lambda_i)$  gives

the probability that  $k$  shocks occur in  $[0, x)$  and additional  $h$  shocks from the same shock process happen in  $[x, t)$ .

The occurrence probability of a shock from the HPP with rate  $\Lambda_i$  in time interval  $[t, t+dt)$  is  $\Lambda_i dt$  for infinitesimal  $dt$ . Therefore, the probability that the  $m_i$ -th shock from this HPP occurs in  $[t, t+dt)$  is

$$P(t, m_i - 1, \Lambda_i) \Lambda_i dt. \quad (7)$$

The shock resistance parameters of the model (3) and the shock rates can be estimated either from the historical data (likelihood-based estimation [26]) or from Bayesian estimation using expert judgment [27]. For evaluating the shock resistance parameters accelerated testing or stress experiments [28] can also be applied.

### 3.2. The RP metrics

For obtaining these metrics, we will need summations with respect to the numbers of experienced shocks that should be limited for further computations in some reasonable way. To do this, note first that, as  $Q_i(k)$  are the decreasing functions, there exists a value of  $I_i(\varepsilon, \omega_i, \Omega_i)$  such that  $Q_i(k) < \varepsilon$  for any  $k > I_i(\varepsilon, \omega_i, \Omega_i)$ . Therefore, for the sufficiently small  $\varepsilon$ , one can determine the maximal number of shocks  $I = \max(I_1(\varepsilon, \omega_1, \Omega_{i1}), I_2(\varepsilon, \omega_2, \Omega_2))$  for which the survival probability of at least one of the components remains not negligible (i.e., not strictly smaller than  $\varepsilon$ ). In what follows we derive probabilities of a component survival under different scenarios. Therefore, for any scenario the number of shocks that the component experiences can be limited by the value of  $I$ .

Consider an event when the component  $i$  is performing the RP during the entire time interval  $[x, y)$  (see Fig. 3). This event can occur when four conditions are held: 1). the component aborts the mission after experiencing and surviving  $m_i$ -th shock at time  $T_{i, m_i} \leq x$ ; 2). according to the MAP the time  $T_{i, m_i}$  of the mission abort is less than  $\xi_i$ ; 3). the RP completion time exceeds  $y$  i.e.  $y \leq T_{i, m_i} + \varphi_i(T_{i, m_i})$ ; 4). the component survives any number  $h$  of RP shocks in interval  $[T_{i, m_i}, y)$ .

For any RP completion time  $y$ , the mission abort time  $\psi_i(y)$  can be obtained as a solution to the equation  $t + \varphi_i(t) = y$ . For  $T_{i, m_i} = \psi_i(y)$  the condition  $T_{i, m_i} \leq x$  is represented by the logical function  $1(\psi_i(y) < x)$  zeroed when this condition is not met.

Thus, using (5)-(7), the probability that component  $i$  is performing the RP during the entire time interval  $[x,y]$  can be obtained as the following integral

$$\alpha_i(x, y) = \Lambda_i \int_0^{\min(x, \xi_i)} 1(t + \varphi_i(t) \geq y) P(t, m_i - 1, \Lambda_i) \sum_{h=0}^{I-m_i} P(y - t, h, \lambda_i) Q_i(m_i + h) dt = 1(\psi_i(y) < \min(x, \xi_i)) \Lambda_i \int_{\psi_i(y)}^{\min(x, \xi_i)} P(t, m_i - 1, \Lambda_i) \sum_{h=0}^{I-m_i} P(y - t, h, \lambda_i) Q_i(m_i + h) dt. \quad (8)$$

In (8),  $t$  is a realization of the random mission abort time  $T_{i,m_i}$  that cannot be less than  $\psi_i(y)$  and cannot exceed  $\min(x, \xi_i)$ .

The probability that component  $i$  is performing the RP at time  $x$  can be obtained as  $\alpha_i(x, x)$ , whereas probability that at time  $x$  component  $i$  does not perform the RP is  $1 - \alpha_i(x, x)$ .

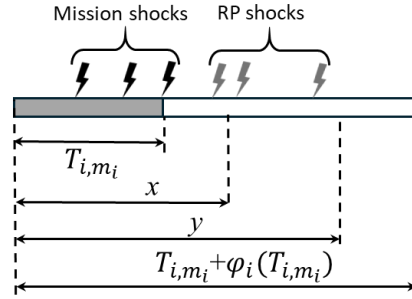


Fig. 3. RP performed during entire time interval  $[x,y]$ .

The probability that component  $i$  aborts the mission upon occurrence of the  $m_i$ -th shock before time  $x$  and fails during the RP in the time interval  $[y, y+dt)$  is

$$\beta_i(x, y) dt = 1(\psi_i(y) < x) \lambda_i \Lambda_i \left( \int_{\psi_i(y)}^x P(u, m_i - 1, \Lambda_i) \sum_{h=1}^{I-m_i} P(y - u, h - 1, \lambda_i) F_i(m_i + h) du \right) dt. \quad (9)$$

In (9)  $\Lambda_i P(u, m_i - 1, \Lambda_i) du$  is the probability that the  $m_i$ -th shock triggering the mission abort occurs in  $[u, u+du)$ .  $\lambda_i P(y - t, h - 1, \lambda_i) dt$  is the probability that the  $h$ -th RP shock causing the component failure occurs in  $[y, y+dt)$  (i.e., at time  $y - u$  since the beginning of the RP).  $F(m_i + h)$  is the probability that the component fails upon experiencing the  $m_i + h$ -th shock.

If the component  $i$  aborts the mission in time interval  $[t, t+dt)$  and survives all the RP shocks, it completes the RP in time interval

$$[t + \varphi_i(t), t + dt + \varphi_i(t + dt)) = [y, y + (1 + \varphi'_i(t)) dt), \quad (10)$$

where  $y = t + \varphi_i(t)$ . Thus, the probability that the component  $i$  completes its RP in  $[y, y + (1 + \varphi'_i(t))dt)$  is

$$\Lambda_i P(\psi_i(y), m_i - 1, \Lambda_i) \sum_{h=0}^{l-m_i} P(y - \psi_i(y), h, \lambda_i) Q_i(m_i + h) dt \quad (11)$$

and the probability that it completes the RP in  $[y, y + dt)$  is

$$\frac{1}{1 + \varphi'_i(\psi_i(y))} \Lambda_i P(\psi_i(y), m_i - 1, \Lambda_i) \sum_{h=0}^{l-m_i} P(y - \psi_i(y), h, \lambda_i) Q_i(m_i + h) dt, \quad (12)$$

where  $\psi_i(y)$  and  $y - \psi_i(y)$  are the times spent by the component during performing the mission and the RP respectively.  $Q(m_i + h)$  is the probability that the component survives  $m_i$  mission shocks and  $h$  RP shocks.

Multiplying (11) by the logical function  $1(\psi_i(y) \leq x)$  that takes the value of 0 for any mission abort time exceeding the value of  $x$ , we obtain the probability  $\gamma_i(x, y)dt$  that the component  $i$  aborts the mission before time  $x$  and completes the RP in the time interval  $[y, y + dt)$  as

$$\begin{aligned} & \gamma_i(x, y)dt \\ &= \frac{1(\psi_i(y) \leq x)}{1 + \varphi'_i(\psi_i(y))} \Lambda_i P(\psi(y), m_i - 1, \Lambda_i) \sum_{h=0}^{l-m_i} P(y - \psi(y), h, \lambda_i) Q_i(m_i + h) dt. \end{aligned} \quad (13)$$

The RP failure and completion are the mutually exclusive events. Therefore, the probability that the component  $i$  aborts the mission before time  $x$  and terminates the RP (completes the RP or fails in the RP) in time interval  $[y, y + dt)$  is  $(\beta_i(x, y) + \gamma_i(x, y))dt$ .

### 3.3. Deriving mission and RP success probabilities and NEML

Consider two scenarios when the component  $i$  can complete the mission.

1. The component  $i$  experiences fewer than  $m_i$  shocks in  $[0, \xi_i]$  and survives all shocks occurring during the entire mission time  $\tau$ . The probability of such event is

$$\tilde{r}_i = \sum_{k=0}^{m_i-1} P(\xi_i, k, \Lambda_i) \sum_{h=0}^{l-k} P(\tau - \xi_i, h, \lambda_i) Q_i(k + h). \quad (14)$$

2. The component  $i$  experiences the  $m_i$ -th shock at  $T_{m_i} < \xi_i$ , and survives all shocks during the mission time  $\tau$ , whereas component  $3-i$  is performing its RP during entire time interval  $[T_{m_i}, \vartheta_i)$ . The probability of such event is

$$\hat{r}_i = \Lambda_i \int_0^{\xi_i} P(t, m_i - 1, \Lambda_i) \alpha_{3-i}(t, \vartheta_i) \sum_{h=0}^{l-m_i} P(\tau - t, h, \lambda_i) Q_i(m_i + h) dt. \quad (15)$$

As the two considered cases of the mission completion are mutually exclusive, the probability that the component  $i$  completes the mission is  $\hat{r}_i + \tilde{r}_i$  and the overall probability that the mission is completed is

$$R=1-(1-\hat{r}_1 - \tilde{r}_1)(1 - \hat{r}_2 - \tilde{r}_2). \quad (16)$$

Consider now two mutually exclusive scenarios when component  $i$  aborts the mission and completes the RP.

1. The component  $i$  experiences the  $m_i$ -th shock in  $[t, t+dt)$  where  $t < \xi_i$  when the component  $3-i$  is not performing its RP. The component aborts the mission and survives all  $m_i$  mission shocks in  $[0, t)$  and all  $h$  RP shocks in  $[t, t + \varphi_i(t))$ . The probability of this event is

$$\tilde{s}_i = \Lambda_i \int_0^{\xi_i} P(t, m_i - 1, \Lambda_i) (1 - \alpha_{3-i}(t, t)) \sum_{h=0}^{I-m_i} P(\varphi_i(t), h, \lambda_i) Q_i(m_i + h) dt. \quad (17)$$

2. The component  $i$  experiences the  $m_i$ -th shock in  $[t, t+dt)$  where  $t < \xi_i$  when the component  $3-i$  is performing its RP, aborts the mission at time  $y < \vartheta_i$  when the RP of the component  $3-i$  is terminated and survives  $m_i$  mission shocks occurring in  $[0, t)$  and any number  $k$  of mission shocks occurring in  $[t, y)$  and any number  $h$  of RP shocks occurring in  $[y, y + \varphi_i(y))$ . The probability of this event is

$$\hat{s}_i = \Lambda_i \int_0^{\xi_i} P(t, m_i - 1, \Lambda_i) \int_t^{\vartheta_i} (\beta_{3-i}(t, y) + \gamma_{3-i}(t, y)) \sum_{k=0}^{I-m_i} P(y - t, k, \Lambda_i) \sum_{h=0}^{I-m_i-k} P(\varphi_i(y), h, \lambda_i) Q(m_i + k + h) dy dt. \quad (18)$$

For each component  $i=1,2$ , the two scenarios of the mission completion (with probabilities  $\hat{r}_i$  and  $\tilde{r}_i$ ), the two scenarios of the RP completion (with probabilities  $\tilde{s}_i$  and  $\hat{s}_i$ ) and the scenario of the component failure (with probability  $f_i$ ) constitute a complete group of mutually exclusive events. Therefore, the probability that the component  $i$  fails during the mission or RP can be obtained as

$$f_i=1-\hat{r}_i - \tilde{r}_i - \tilde{s}_i - \hat{s}_i. \quad (19)$$

Then, according to (2), the overall NEML can be defined as

$$E=f_1c_1/C_F + f_2c_2/C_F + (1-\hat{r}_1 - \tilde{r}_1)(1 - \hat{r}_2 - \tilde{r}_2). \quad (20)$$

### 3.4. Numerical algorithm for NEML evaluation

The numerical algorithm for NEML evaluation consists of two procedures. The pseudo-codes of the procedures are presented below.

Pseudo-code of numerical procedure for evaluating  $\alpha_i(x, y)$ ,  $\beta_i(x, y)$  and  $\gamma_i(x, y)$ .

```

1 For i=1,2:
2   For x=0,dt,...,ξi:
3     For y=t,t+dt,...,ϑi:
4       αi(x,y)=0; βi(x,y)=0;
5       For t=ψi(y), ψi(y)+dt,...,x:
6         A=0;
7         A=0; For h=0,..., I - mi: A=A+P(y - t, h, λi)Qi(mi + h);
8         αi(x,y) = αi(x,y) + A × P(t, mi - 1, Λi);
9         A=0; For h=0,..., I - mi: A=A+P(y - t, h - 1, λi)Fi(mi + h);
10        βi(x,y)=βi(x,y) + A × P(y, mi - 1, Λi);
11        αi(x,y) = αi(x,y)Λidt;
12        βi(x,y)=βi(x,y)λiΛidt;
13        A=0; For h=0,..., I - mi: A=A+P(y - ψ(y), h, λi)Qi(mi + h);
14        γi(x,y)=A ×  $\frac{1(\psi_i(y) \leq x)}{1+\varphi_i(\psi_i(y))}$  ΛiP(ψ(y), mi - 1, Λi)

```

Pseudo-code of numerical procedure for evaluating the NEML.

```

1 For i=1,2:
2   A=0; F=0; H=0; r̂i=0;
3   For t=0,dt,...,ξi:
4     B=0; U=0; G=0;
5     For h=0,..., I - mi: U=U+P(φi(y), h, λi)Q(mi + h);
6     For h=0,..., I - mi: G=G+P(τ - t, h, Λi)Q(mi + h);
7     For y=t,t+dt,...,ϑi:
8       C=0;
9       For k=0,..., I - mi:
10        D=0;
11        For h=0,..., I - mi - k: D=D+P(φi(y), h, λi)Q(mi + k + h);
12        C=C+D×P(y - t, k, Λi);
13        B=B+C × (β3-i(t, y) + γ3-i(t, y));
14        A=A+B×P(t, mi - 1, Λi);
15        F=F+U×P(t, mi - 1, Λi)(1 - α3-i(t, t));
16        H=H+G×P(t, mi - 1, Λi)α3-i(t, ϑi);
17        ŝi = AΛi(dt)2;
18        s̃i = FΛidt;
19        r̂i = HΛidt;
20        r̃i=0;
21        For k=0,..., mi - 1:
22          V=0;
23          For h=0,..., I - k: V=V+P(τ - ξi, h, Λi)Q(k + h);
24          r̃i=r̃i+V× P(ξi, k, Λi);
25          fi=1-r̂i - r̃i - s̃i - ŝi;
26        E=f1c1/CF + f2c2/CF + (1-r̂1 - r̃1)(1 - r̂2 - r̃2)

```

The first procedure evaluates functions  $\alpha_i(x, y)$ ,  $\beta_i(x, y)$  and  $\gamma_i(x, y)$  for  $i=1,2$ ,  $0 \leq x \leq \xi_i$  and  $t \leq y \leq \vartheta_i$ . The values of  $x$  and  $y$  vary with a predetermined step  $dt$ . Steps 4, 7, 8 and 11 of the procedure consecutively calculate  $\alpha_i(x, y)$  according to Eq. (8). Steps 4, 9, 10 and 12 calculate  $\beta_i(x, y)$  according to Eq. (9). Steps 13, 14 calculate  $\gamma_i(x, y)$  according to Eq. (13). The second procedure evaluates probabilities  $\tilde{r}_i$ ,  $\hat{r}_i$ ,  $\tilde{s}_i$  and  $\hat{s}_i$  and calculates the NEML using the obtained values of  $\alpha_i(x, y)$ ,  $\beta_i(x, y)$  and  $\gamma_i(x, y)$ . Steps 21-24 of the procedure consecutively calculate  $\tilde{r}_i$  according to Eq. (14). Steps 6, 16 and 19 calculate  $\hat{r}_i$  according to Eq. (15). Steps 5, 15 and 18 calculate  $\tilde{s}_i$  according to Eq. (17). Steps 2, 7-14 and 17 calculate  $\hat{s}_i$  according to Eq. (18). Variables  $A, B, C, D, F, G, U$  and  $V$  are used to save intermediate results. Step 25 calculates the failure probabilities  $f_i$  according to Eq. (19). Step 26 calculates the NEML according to (20).

### 3.5. Computational complexity of the NEML evaluation procedure

As can be seen from Eqs. (14), (15), (17) and (18), the most complex procedure is required for evaluating  $\hat{s}_i$ . The complexity of this procedure is  $O(I^2 dt^2)$ , where  $dt$  is the time discretization factor. Fig 4 presents the calculated values of NEML  $C$ , MSP  $R$  and component failure probability  $f=f_i$  as functions of  $dt$  for identical components with parameters  $\Omega_i = 0.86$ ,  $\omega_i = 0.7$  (for these parameters  $I=9$  provides  $Q_i(I) < 10^{-5}$ ),  $\tau=100$ ,  $\Lambda_i = 0.02$ ,  $\lambda_i = 0.01$ ,  $c_i/C_F=0.9$ ,  $\varphi_i(t) = 0.8t$ ,  $m_i=1$ ,  $\xi_i = \vartheta_i = 0.264\tau$ . The values of  $C$ ,  $R$  and  $f$  converge to constants when  $1/dt$  exceeds 800. The discrepancy between the values of the NEML for  $1/dt=500$  and  $1/dt=1000$  is 1.6%, the discrepancy between the values of the NEML for  $1/dt=800$  and  $1/dt=1000$  is 0.47%.

The running time of the procedure for the EML evaluation on 3.7 GHz PC is also presented in Fig. 4.

Having the procedure for the NEML evaluation for any MAP  $m_1, \xi_1, \vartheta_1, m_2, \xi_2, \vartheta_2$  one can find the MAP minimizing the NEML applying any available optimization software based on non-derivative methods such as simulated annealing [29], particle swarm optimization [30], cuckoo search [31], tabu search [32], immune algorithm [33], etc. In this work, we have used the genetic algorithm [34] for optimizing the MAP considering its advantages in flexible solution representation and fast convergence to near optimal solutions.

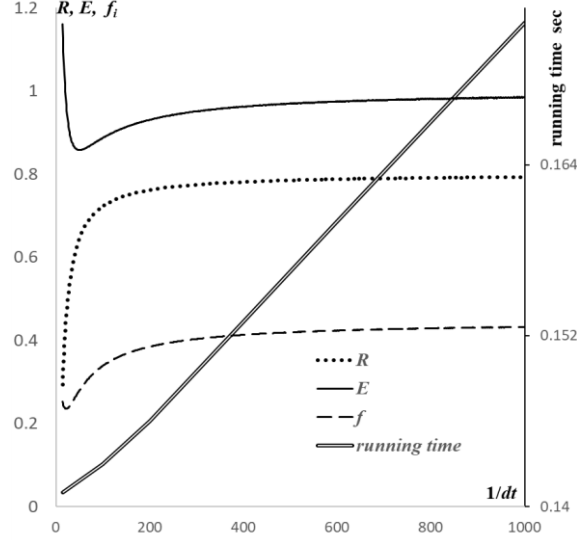


Fig. 4. System metrics and running time as functions of time discretization parameter  $dt$ .

#### 4. Illustrative example

Consider two virtual machines (data processing software versions) that must accomplish during time  $\tau=100$  h the same computational task operating with sensitive data on two different cloud servers. Each server is exposed to random hacker attacks (shocks) aimed at accessing and corrupting sensitive data. The attacks arrive in accordance with the HPP with rate  $\Lambda_i = 0.02 \text{ h}^{-1}$ . The data corruption causes immediate failure of the task performed on the server. The damage  $C_F$  is inflicted if both virtual machines (VMs) fail to complete their tasks. Each attack, even when it fails, can provide the attacker with some information about the server protection, which can be used in future attacks. Thus, the data corruption probability increases with the number of attacks. This is modelled by (4) with  $\Omega_i = 0.86$ ,  $\omega_i = 0.7$ . To reduce the data corruption probability, the computational task can be aborted if the number of attacks on the server reaches a certain threshold. After the task abort, the data and software are transferred to a safe storage (i.e., the RP is performed). During the transfer, the data can also be corrupted by hackers attacks that occur with rate  $\lambda_i = 0.01$ . The transfer time (duration of the RP) is proportional to the amount of data processed/generated on the server since the beginning of the mission, which is modelled using the function  $\varphi_i(t) = a_i t$  with  $a_i=0.8$ . If the data used/generated by VM  $i$  is corrupted during the data processing (mission) or transfer (RP), damage with cost  $c_i$  is inflicted. The single communication channel with limited capacity connects the safe storage with the

servers. Therefore, the data transmission from two servers cannot be performed simultaneously. The optimal MAP should balance the damage associated with the task failure and with the data corruption events.

#### 4.1. Identical components

Fig. 5 presents the mission metrics for a system consisting of identical VMs (components) as functions of MAP parameters  $\zeta_i$  and  $m_i$  when  $\vartheta_i = \zeta_i$  and  $c_1/C_F = c_2/C_F = 0.9$ . With increase of  $\zeta_i$  the MAP becomes more cautious, allowing mission abort during longer time. This leads to increase in probabilities  $\tilde{s}_i$  and  $\hat{s}_i$  of the components survival after the mission abort and to decrease of probabilities  $\tilde{r}_i$  that components complete the mission without aborting it. The probability  $\hat{r}_i$  that the component  $i$  that should abort the mission does not abort it (because the other component performs the RP) and completes the mission can behave non-monotonically. Indeed, on one hand the increase of  $\zeta_i$  increases the probability that component  $i$  experiences  $m_i$ -th shock at time  $T_{i,m_i} < \zeta_i$  and should abort the mission. On the other hand, the increases of  $\zeta_i$  leaves the component smaller chance to survive when it continues the mission after experiencing  $m_i$ -th shock as the other component can perform the RP latter not allowing mission abort to component  $i$ . Observe that  $\hat{r}_i$  is much smaller than  $\tilde{r}_i$  and the overall MSP  $R$  decreases with increase of  $\zeta_i$ .

The combination of increasing probabilities  $\hat{r}_i$ ,  $\tilde{s}_i$  and  $\hat{s}_i$  with decreasing probability  $\tilde{r}_i$  leads to non-monotonic behavior of the component failure probability  $f_i$ . The NEML behaves non-monotonically and has the distinct minima.

Increase of  $m_i$  makes the MAP riskier allowing the mission continuation after experiencing more shocks. Therefore, with increase of  $m_i$  both the MSP  $R$  and the components loss probabilities  $f_i$  increase. For the given cost ratios  $c_i/C_F$  the minimal NEML is achieved for  $m_i=1$  and  $\zeta_i=0.26\tau$ .

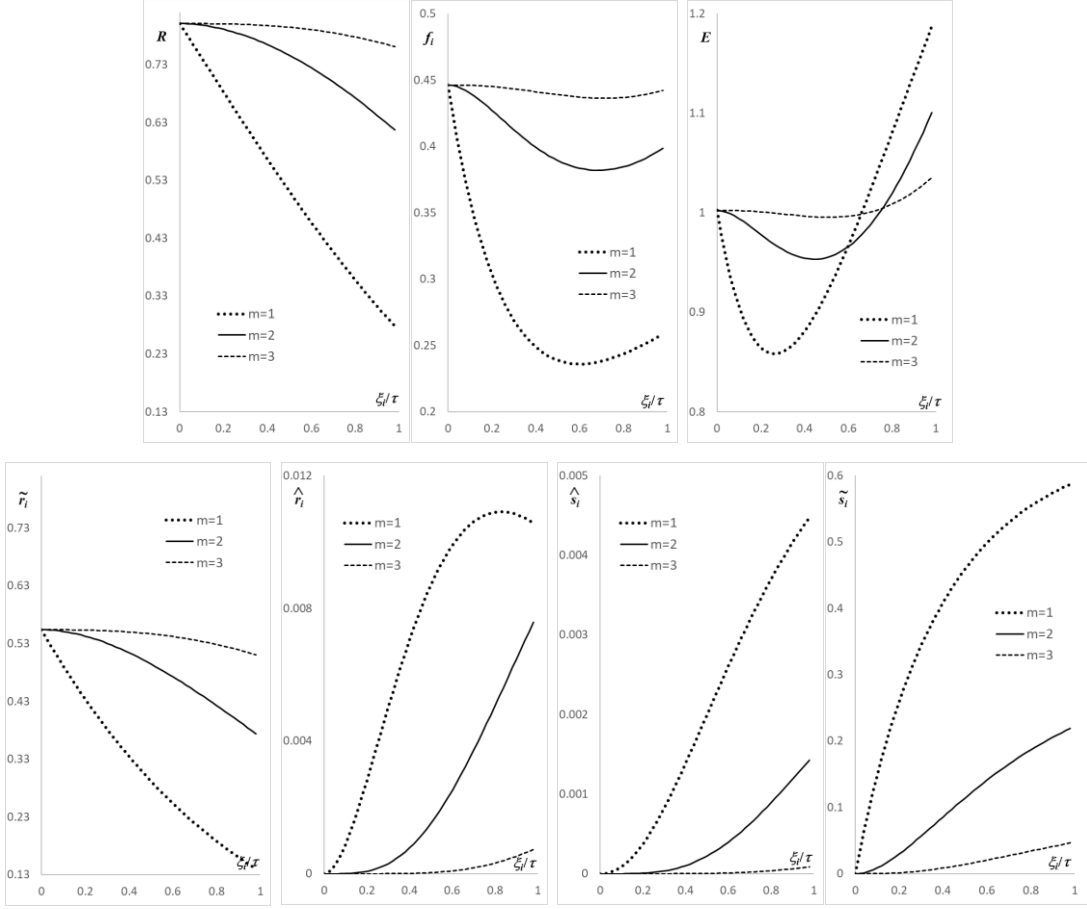


Fig. 5. Mission metrics as function of MAP parameters  $m_i$  and  $\zeta_i$

Fig. 6 presents some mission metrics as functions of MAP parameters  $\vartheta_i$  and  $m_i$  when  $\zeta_i=0.26\tau$  ( $\tilde{r}_i$  and  $\tilde{s}_i$  are not presented as they do not depend on  $\vartheta_i$ ). With increase of  $\vartheta_i$ , the probability  $\hat{r}_i$  that the component  $i$  that should abort the mission continues and completes the mission because the other component performs the RP till at least time  $\vartheta_i$  decreases. Moreover, the probability  $\hat{s}_i$  that the component  $i$  aborts the mission, performs the postponed RP and survives increases. However,  $\hat{s}_i$  is much smaller than  $\hat{r}_i$  and the effect of  $\hat{r}_i$  decrease causes the decrease of the MSP  $R$  and the increase of the component failure probability  $f_i$ . Therefore, the NEML increases with increase of  $\vartheta_i$  and the minimum value  $\vartheta_i=\zeta_i$  provides the smallest value of the NEML. With increase in  $m_i$ , the probabilities  $\hat{s}_i$  and  $\hat{r}_i$  become much smaller because the probability that component  $i$  should abort the mission decreases. The sensitivity of the NEML to the MAP parameter  $\vartheta_i$  decreases.

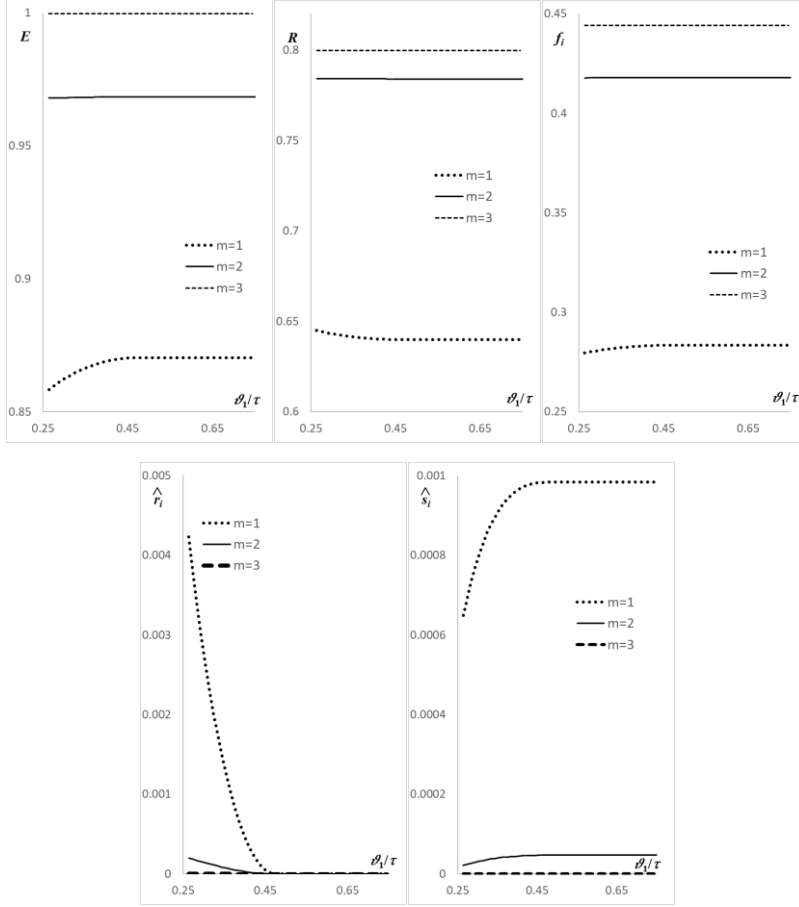


Fig. 6. Mission metrics as function of MAP parameters  $m_i$  and  $v_i$ .

Figs. 7 and 8 present the results of MOP optimization. The optimal MAP parameters and the corresponding mission metrics as functions of the cost ratios  $c_i/C_F$  are given in Fig. 7 ( $v_i=\xi_i$  always holds). When  $c_i/C_F$  are small, saving the data from corruption is much less important than completing the data processing mission. Therefore, when  $c_i/C_F \leq 0.1$  no abort MAP with  $\xi_i=0$ , which provides the greatest possible MSP  $R$  is optimal. When  $0.2 \leq c_i/C_F \leq 0.3$  the MAP is risky with  $m_i=2$  and  $\xi_i$  slowly increasing with increase of  $c_i/C_F$ . When  $c_i/C_F$  further increases, the data survival importance increases, and the MAP becomes more cautious:  $m_i$  drops to 1 (which is compensated by decreased  $\xi_i$  to avoid sharp decrease of the MSP). Further increase of  $c_i/C_F$  causes the increase of optimal values of  $\xi_i$ , which leads to decrease of both MSP  $R$  and data corruption probabilities  $f_i$ . As a result, the NEML increase with increase of the  $c_i/C_F$  ratio. Notice that NELM corresponds to  $C_F=1$ .

Therefore, the increase in the ratio  $c_i/C_F$  is achieved solely by the increase in the cost  $c_i$  and results in greater losses.

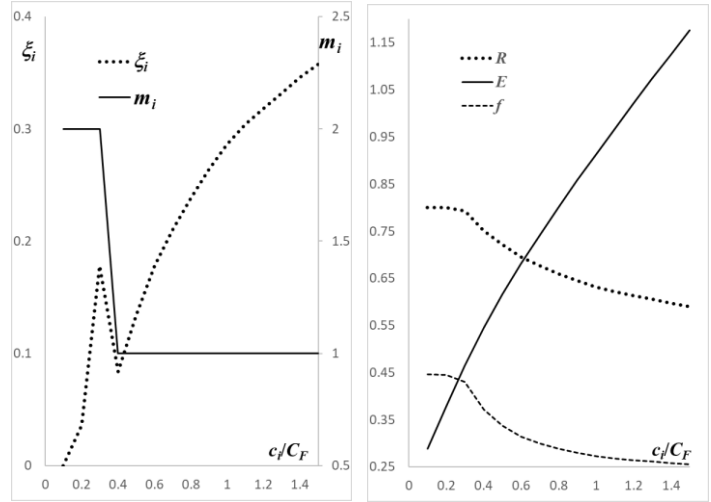


Fig. 7. Optimal MAP parameters and corresponding mission metrics as functions of  $c_i/C_F$ .

Fig. 8 presents the optimal MAP parameter  $\xi_i$  and the corresponding mission metrics as functions of the RP duration parameter  $a_i$  when  $c_i/C_F=0.9$ .

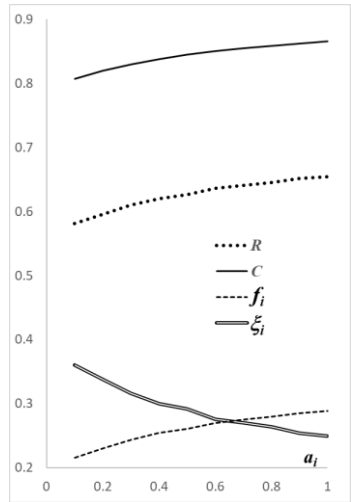


Fig. 8. Optimal MAP parameters and corresponding mission metrics as functions of the RP duration parameter  $a_i$

For any value of  $a_i$ , the optimal value of  $m_i$  is 1. When the RP becomes longer, its efficiency reduces because the data has smaller chance to remain uncorrupted during the longer transfer procedure. Moreover, longer RP of a component leaves to the other component lower chance of surviving in the case when it should but cannot abort its mission. Therefore, with increase of  $a_i$ , the MAP becomes riskier allowing the mission

abort during shorter time ( $\xi_i$  decreases). This leads to the increase of both MSP  $R$  and corruption probabilities  $f_i$  and eventually to the increase of the NEML. The decrease of  $\xi_i$  partly compensates the effect of increased RP time on the NEML.

#### 4.2. Heterogeneous components

Consider a case of different servers having different levels of protection and assume that the parameters of VM 1 operation are  $\Omega_1 = 0.8$ ,  $\omega_1 = 0.75$ ,  $\Lambda_1 = 0.01$ ,  $\lambda_1 = 0.008$ ,  $\varphi_1(t) = 0.6t$ , whereas the parameters of the second VM are as presented in the previous section.

Fig. 9 presents the optimal MAP parameters  $m_i$ ,  $\xi_i$  and the corresponding mission metrics  $R$ ,  $E$ ,  $f_i$  as functions of the cost ratios  $c_1/C_F$  and  $c_2/C_F$ . In all the best obtained MAPs  $m_2=1$  and  $\vartheta_i=\xi_i$ . When  $c_i/C_F$  increases, saving the data produced by VM  $i$  becomes more important and the MAP for this VM becomes more cautious ( $m_i$  decreases and/or  $\xi_i$  increases), which results in decrease of the data corruption probability  $f_i$  and MSP  $R$ . The increase of  $c_i/C_F$  also influences the optimal MOP for VM  $3-i$ . To compensate the more cautious MAP of VM  $i$ , the MAP of the other VM becomes riskier ( $\xi_{3-i}$  decreases), which causes the increase of the data corruption probability  $f_{3-i}$  and mildens the drop of the MSP  $R$ .

Ehen  $c_1/C_F < 1$  and  $c_2/C_F > 0.8$  the no abort policy becomes optimal for VM 1 ( $\xi_i=0$  and the MSP  $R$  and the data corruption probability  $f_1$  become independent from the cost ratios  $c_i/C_F$  anymore.

The NEML monotonically increases with increase of both  $c_1/C_F$  and  $c_2/C_F$ . For any considered combination of values of  $c_1/C_F$  and  $c_2/C_F$ , accomplishing the mission remains beneficial because the NEML is smaller than 1.

Fig. 10 presents the optimal MAP parameters  $m_i$ ,  $\xi_i$  and the corresponding mission metrics  $R$ ,  $E$ ,  $f_i$  as functions of the RP duration parameters  $a_1$  and  $a_2$  when  $c_1/C_F = 1.4$  and  $c_2/C_F = 0.9$ . In all the best obtained MAPs  $m_1=2$ ,  $m_2=1$  and  $\vartheta_i=\xi_i$ . When  $a_i$  increases, the probability that the data remains not corrupted during the longer data transfer (RP) decreases. Therefore, it becomes less beneficial to abort the computational mission, which results in reduction of the MAP parameter  $\xi_i$  (abort is allowed during shorter time from the mission beginning for which the RP is not very long). The riskier MAP causes increase of

both the MSP  $R$  and the data corruption probability  $f_i$ . The variation of RP duration parameter  $a_i$  also influences the MAP of VM 3- $i$  through the delay of activating the RP procedure.

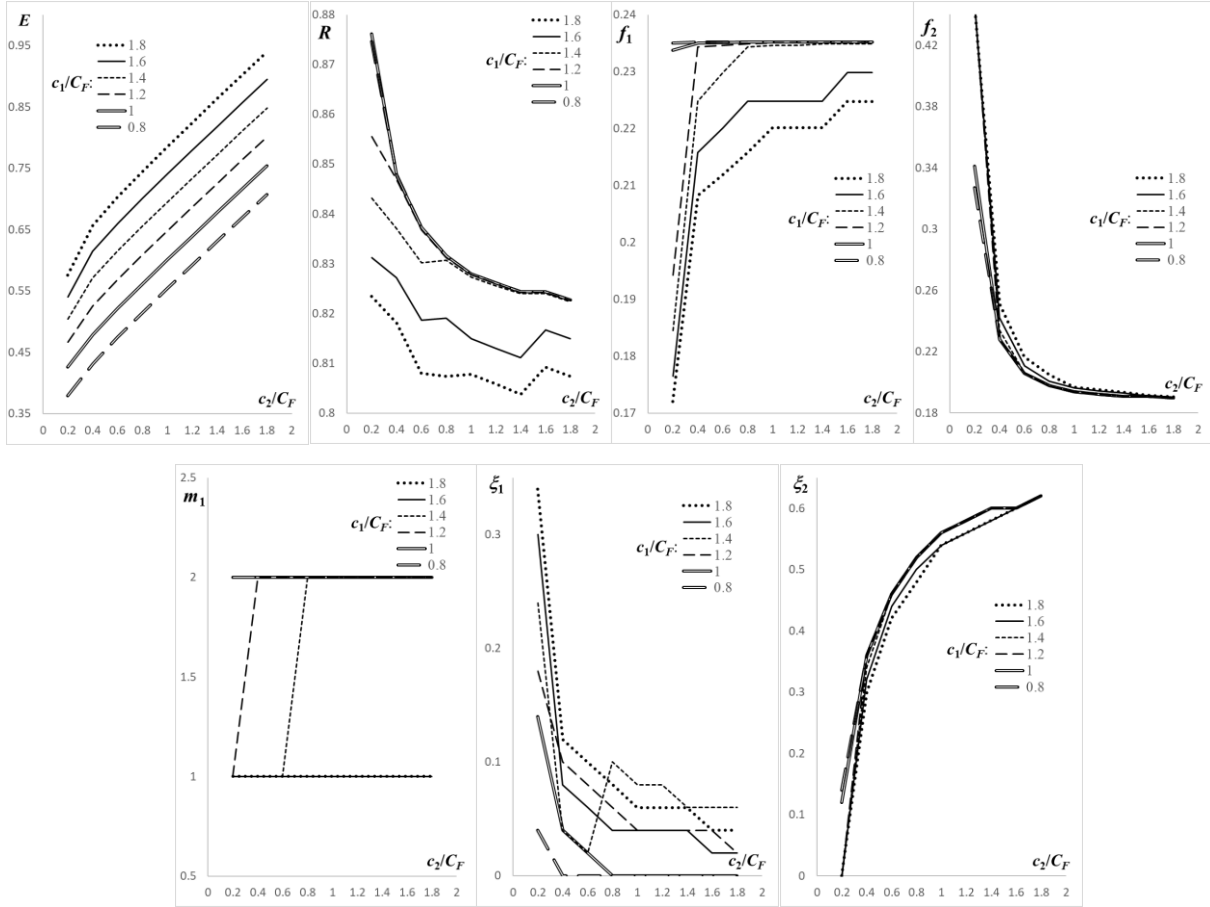


Fig. 9. Optimal MAP parameters and the corresponding mission metrics as functions of the cost ratios  $c_1/C_F$  and  $c_2/C_F$ .

The increase of  $a_2$  causes greater delay in activating the RP of VM 1, which can leave no time for the mission abort and RP activation if  $\zeta_1$  is small. To prevent the increase of the corruption probability  $f_1$  the VM 1 increases the time  $\zeta_1$  during which the mission abort is allowed. This allows the system to keep probability  $f_1$  almost constant when  $a_2$  increases. The influence of parameter  $a_1$  on the MAP of VM 2 is much smaller because  $m_1=2$  and the probability that VM 2 aborts the mission upon occurrence of the second shock (and its RP postpones the RP of VM 1) is much smaller than such probability for VM 1, which aborts the mission after the first shock.

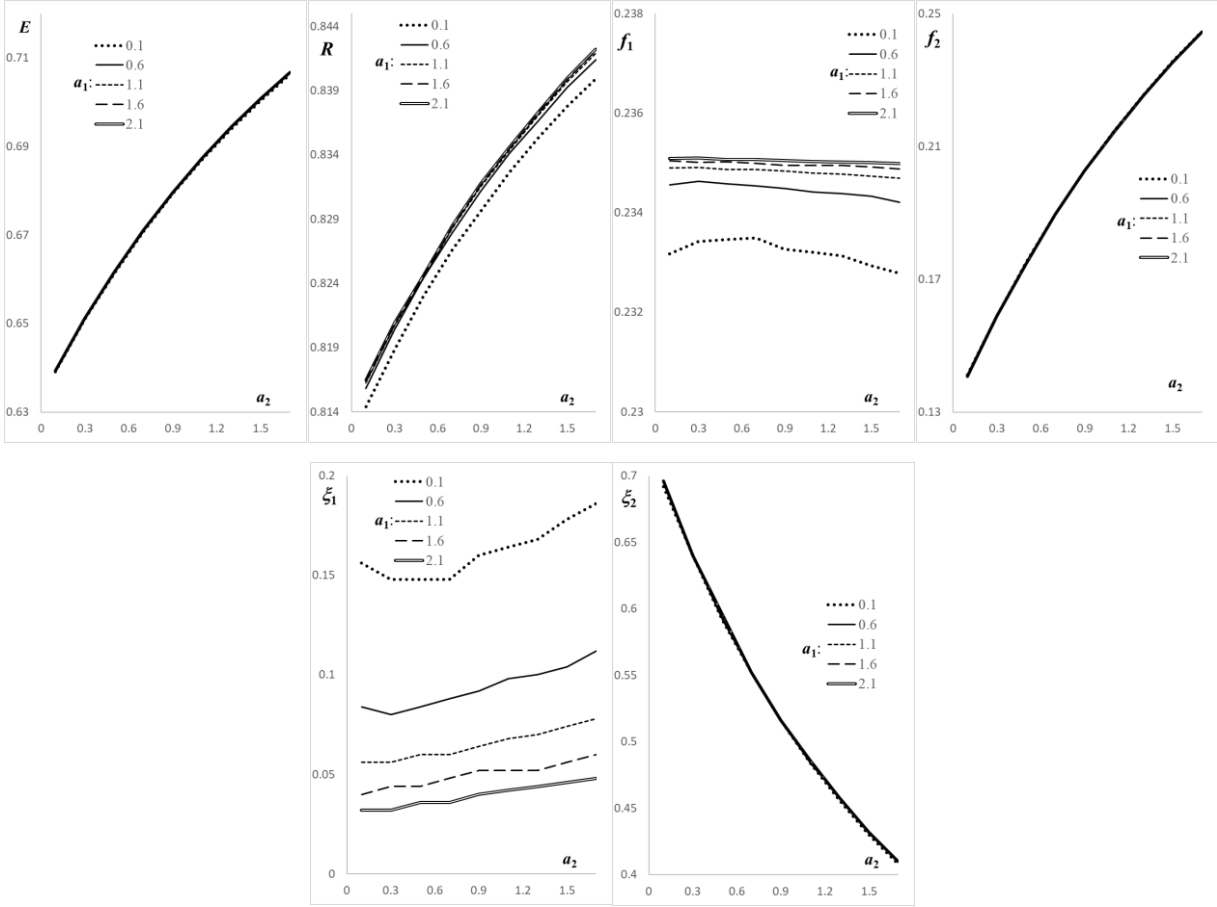


Fig. 10. Optimal MAP parameters and the corresponding mission metrics as functions of the RP duration parameters  $a_1$  and  $a_2$ .

The NEML increases with increase of  $a_2$  and is almost insensitive to the variation of  $a_1$ . When  $a_1$  increases the increase of MSP  $R$  is compensated by the increase of the data corruption probability  $f_1$ .

## 5. Conclusions and further research directions

The paper models a two-component system in which the simultaneous RP for both components is forbidden and a component cannot abort the mission when the other component performs its RP. This situation can arise in practice when there are no sufficient resources for simultaneous abort or there are other causes (logistic, management or design constraints) preventing it.

An algorithm for evaluating mission metrics for arbitrary mission and components parameters and arbitrary MAPs for the components is developed. Based on this algorithm,

the MAP optimization methodology is developed for minimizing the expected mission losses.

A detailed case study on two virtual machines that share single communication channel has been carried out, revealing the following managerial insights:

1. The mutual influence of the components' parameters on their optimal MAPs exists and should be taken into account when the operation is planned.
2. When the importance of component survival (cost ratio associated with the component's failure) increases, the MAP for the component should be more cautious, which is compensated by the riskier MAP of the other component.
3. When the RP time of the component  $i$  increases, the MAP of this component should be riskier ( $\zeta_i$  decreases, allowing mission abort during shorter time), whereas the MAP of the other component should be less risky ( $\zeta_{3-i}$  increases).
4. Before starting a mission, it is important to check the value of the NEML. If the NEML exceeds 1 for optimal MAP, it is advisable to abandon the mission.

In further research, the influence of the common shocks affecting both components on the MAP and the system metrics should be analyzed. This will bring in the dependence between components [35]. Other types of dependencies can be also considered in the future that can be modeled, e.g., via the copulas [36]. A more complex model, where  $n$  components perform a mission with no more than  $k < n$  components allowed to execute the RPs simultaneously can be also developed. This can result in components queuing for initiating the postponed RPs. Random mission [37] and the RP's times can be also of interest to consider in the follow-up studies. Whereas in relatively short missions the probability of internal component failures can be neglected, it should be considered in future research for longer mission durations. Influence of imperfect shock detection on the NEML should be also analyzed based on model [38].

## References

- [1] Myers, A. (2009). Probability of loss assessment of critical k-out-of-n: G systems having a mission abort policy, IEEE Trans. Rel., vol. 58, no. 4, pp. 694–701.
- [2] Rodrigues, A., Cavalcante, C., Alberti, A., Scarf, P., & Alotaibi, N. (2023). Mathematical modelling of mission-abort policies: a review. IMA Journal of Management Mathematics, vol. 34, no. 4, pp. 581-597.

- [3] L. Xing, G. Levitin (2025). Mission abort policies in reliability engineering: a review. *Journal of Reliability Science and Engineering*, 1, 012001.
- [4] Levitin, G., Finkelstein, M., and Xiang, Y. (2020). Optimal aborting rule in multi-attempt missions performed by multicomponent systems, *European Journal of Operational Research*, vol. 283, no. 1, pp. 244-252.
- [5] Levitin, G., Xing, L., and Xiang, Y. (2020). Optimal abort rules and subtask distribution in missions performed by multiple independent heterogeneous units. *Reliability Engineering & System Safety*, vol. 199, 106920.
- [6] Levitin, G., Xing, L., Dai, Y. (2021). Dynamic task distribution balancing primary mission work and damage reduction work in parallel systems exposed to shocks, *Reliability Engineering & System Safety*, vol. 215, 107907.
- [7] Zhu, X., Zhu, X.P., Yan, R., Peng, R. (2021). Optimal routing, aborting and hitting strategies of UAVs executing hitting the targets considering the defense range of targets, *Reliability Engineering & System Safety*, vol. 215, 107811.
- [8] Levitin, G., Finkelstein, M., Xiang, Y (2021). Optimal aborting strategy for three-phase missions performed by multiple units, *Reliability Engineering & System Safety*, vol. 208, 107408
- [9] Levitin, G., Xing, L. and Dai, Y. (2021). Mission aborting in n-unit systems with work sharing. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 52, no. 8, pp. 4875-4886.
- [10] Levitin, G., Xing, L., Xiang, Y. (2021). Partial mission aborting in work sharing systems, *Reliability Engineering & System Safety*, vol. 214, 107716.
- [11] Chai, X., Chen, B., and Zhao, X.. (2023). Optimal Mission Abort Decisions for Multi-Component Systems Considering Multiple Abort Criteria. *Mathematics*, vol. 11, no. 24, 4922.
- [12] Levitin, G., Xing, L., and Dai, Y. (2023). Optimal task aborting policy and component activation delay in consecutive multi-attempt missions. *Reliability Engineering & System Safety*, vol. 238, 109482.
- [13] Cheng, G., Shen, J., Wang, F., Li, L., Yang, N. (2024). Optimal mission abort policy for a multi-component system with failure interaction, *Reliability Engineering & System Safety*, vol. 242, 109791.
- [14] Levitin, G., Xing, L., Dai, Y. (2024). Optimal attempt scheduling and aborting in heterogenous system performing asynchronous multi-attempt mission, *Reliability Engineering & System Safety*, vol. 251, 110335.

- [15] Liu, L., Yang, J., Yan, B. (2024). A dynamic mission abort policy for transportation systems with stochastic dependence by deep reinforcement learning, *Reliability Engineering & System Safety*, vol. 241, 109682.
- [16] Levitin, G., Xing, L., Dai, Y. (2024). Optimal component activation in multi-attempt missions with common shock process, *Reliability Engineering & System Safety*, vol. 251, 110330.
- [17] Lujie Liu, L., Jun Yang, J. (2023). A dynamic mission abort policy for the swarm executing missions and its solution method by tailored deep reinforcement learning, *Reliability Engineering & System Safety*, vol. 234, 109682.
- [18] Karimi, A., Tavangar M., Finkelstein, M. (2025) New optimal mission abort policies for coherent systems using signature. To appear in *Proceedings of the Institution of Mechanical Engineering, Part O: Journal of Risk and Reliability*.
- [19] Levitin, G., Xing, L., Dai, Y. (2022). Using kamikaze components in multi-attempt missions with abort option, *Reliability Engineering & System Safety*, vol. 227, 108745.
- [20] Gao, K., Xiao, H., Mi, J., Peng, R., Zhai, Q. (2020). Optimal abort policy of a distributed system of computers with Weibull Failure times. *Global Reliability and Prognostics and Health Management Conference (PHM-Shanghai)*, 16-18 October 2020.
- [21] Zhao, X., Liu, H., Wu, Y., Qiu, Q. (2023). Joint optimization of mission abort and system structure considering dynamic tasks. *Reliability Engineering & System Safety*, vol. 234, 109128
- [22] Cha, J. H., Finkelstein, M., Levitin, G. (Optimal mission abort policy for partially repairable heterogeneous systems (2018). *European Journal of Operational Research*, vol 271, 818-825.
- [23] Peng, R. (2018). Joint routing and aborting optimization of cooperative unmanned aerial vehicles. *Reliability Engineering and System Safety*, vol.177, 131-137.
- [24] Finkelstein, M. (2008). *Failure rate modelling for reliability and risk*. Springer.
- [25] Cha, J.H. & Finkelstein, M. (2011). On new classes of extreme shock models and some generalizations. *J Appl Probab.*, vol. 48, pp. 258–270.
- [26] Hoyland, A., Rausand, M., *System Reliability Theory: Models and Statistical Methods*, John Wiley, 2009.
- [27] O'Hagan, A., Buck, C., Daneshkhah, A., Eiser, R., Garthwaite, P., David J. Jenkinson, D., Oakley, J., Rakow, T., *Uncertain Judgements: Eliciting Experts' Probabilities*. John Wiley, 2006.
- [28] Meeker, W. Q., Escobar, L. A., Pascual, F. G., *Statistical Methods for Reliability Data*, 2nd ed., John Wiley, 2022.
- [29] Chambari, A., Najafi, A., Rahmati, S., Karimi, A. An efficient simulated annealing algorithm for the redundancy allocation problem with a choice of redundancy strategies," *Reliability Engineering & System Safety*, vol. 119, pp. 158-164, 2013.

- [30] Ouyang, Z., Liu, Y., Ruan, S., Jiang, T. An improved particle swarm optimization algorithm for reliability-redundancy allocation problem with mixed redundancy strategy and heterogeneous components, *Reliability Engineering & System Safety*, vol. 181, pp. 62-74, 2019.
- [31] Mellal, M. A., Zio, E. System reliability-redundancy optimization with cold-standby strategy by an enhanced nest cuckoo optimization algorithm, *Reliability Engineering & System Safety*, vol. 201, 106973, 2020.
- [32] Ouzineb, M., Nourelfath, M., Gendreau. Tabu search for the redundancy allocation problem of homogenous series-parallel multi-state systems, *Reliability Engineering & System Safety*, vol. 93, no. 8, pp. 1257-1272, 2008.
- [33] Chen, T., You, P. Immune algorithms-based approach for redundant reliability problems with multiple component choices, *Computers in Industry*, vol. 56, no. 2, pp. 195-205, 2005.
- [34] Kramer, O. *Genetic Algorithm Essentials*, Series: Studies in Computational Intelligence, Springer Cham, 2017.
- [35] Liu, L., Yang, J., Yan, B. (2024). A dynamic mission abort policy for transportation systems with stochastic dependence by deep reinforcement learning *Reliability Engineering & System Safety*, vol 241, 109682
- [36] Nelsen, R. B. (2006). *An Introduction to Copulas*, 2nd edition, Springer
- [37] Finkelstein, M. & Cha, J.H. (2025). Is our mission profitable: the cost-effectiveness curve with the probability of a mission abort. *Reliability Engineering & System Safety*, vol 257, 110853.
- [38] Luo, L., Xing, L., Levitin, G. Optimal mission aborting under imperfect shock detection, *Reliability Engineering & System Safety*, vol. 265, 111477, (2025).