Mechanisms for improving reliability and reducing risk by stochastic and deterministic separation

Michael Todinov
Oxford Brookes University
Department of Mechanical Engineering and Mathematical sciences,
Oxford, Wheatley, OX33 1HX, UK
mtodinov@brookes.ac.uk

ABSTRACT
The paper provides for the first time a comprehensive introduction into the mechanisms through which the method of separation achieves risk reduction and into the ways it can be implemented in engineering designs.
The concept stochastic separation of critical random events on a time interval based on guaranteeing with a specified probability a degree of distancing between them is introduced.
Efficient methods for providing stochastic separation by reducing the duration times of overlapping critical random events on a time interval are presented.
The paper also shows that the probability of overlapping of critical events, randomly appearing on a time interval, is practically insensitive to the distribution of their duration times and to the variance of the duration times as long as the mean remains the same. A rigorous proof has been presented that this statement is valid even for two random events on a time interval.
The paper also provides insight into various mechanisms through which deterministic separation improves reliability and reduces risk. It is demonstrated that the separation on properties is an efficient technique for compensating the drawbacks associated with homogeneous properties. It is demonstrated improving reliability by including redundancy, improving reliability by a segmentation and some of the deliberate weak link techniques and stress limiters techniques for reducing risk are effectively special cases of a deterministic separation.

Finally, the paper demonstrates that in a number of cases, the only way to extract benefit from the method of separation is to build and analyse a mathematical model or algorithm based on the method of separation. A comprehensive classification of the discussed methods of stochastic and deterministic separation is also presented.

Keywords: stochastic separation, deterministic separation, method of separation, mechanisms, risk reduction, reliability improvement; technical risk.

1. Introduction

A systematic classification of generic methods for reducing technical risk is crucial to safe operation, engineering designs and software, yet this very important topic has not been covered with sufficient depth in the reliability and risk literature. For many decades, the focus of reliability research has been primarily on reliability prediction rather than reliability improvement and risk reduction. A common tendency in reliability prediction is to select a statistical-based, data-driven approach. Calculating the absolute reliability built in a product is a difficult task because often, reliability-critical data (failure frequencies, strength distribution of the flaws, failure mechanisms and repair times) are unavailable, particularly for new designs, with no failure history. In addition, for highly reliable components and

systems, the amount of existing past failures is insufficient to fit a reliable and robust statistical model. The sparse available data leads to increased levels of uncertainty in the model parameters and poor predictive power of the model. In addition, past reliability data collected for a particular type of environment/duty cycle, often yield poor predictions if applied to another environment/duty cycle.

Some of these difficulties led some authors (Knowles, 1993) to question the appropriateness of a reliability prediction based on past failure rates.

The deficiencies of the data driven approach can be clearly seen on studying of the reliability of a simple system built on n identical components each characterised by reliability R, the reliability of the system becomes $R_{sys} = R^n$. Increasing the number of tests n will reduce the uncertainty associated with the unknown reliability R but will never eliminate it. An error ΔR in the reliability of a single component will then lead to a large error $\Delta R_{sys} / R_{sys} = n(\Delta R / R)$ in the predicted reliability for the system. For a system composed of 50 capacitors, from the same production batch, logically arranged in series, a mere 1% relative error in the estimated reliability of a single capacitor will result in $\Delta R_{sys} / R_{sys} = 50 \times 0.01 = 0.5$ (50%) error in the estimated system reliability, which makes the reliability prediction meaningless.

The deficiencies of the data-driven approach prompted the development of the physics-of-failure-based approach to reliability improvement (Pecht et al, 1990; Pecht, 1990) which is relatively independent of historical failure data.

According to this approach, failures and decline in performance of components and systems occur due to known underlying failure mechanisms. As a result, unlike the data-driven approach, the physics-of-failure approach addresses the underlying causes of failure. Many failure mechanisms lead to accumulation of damage. Failure is initiated when the amount of accumulated damage exceeds the endurance limit. As a result, the time to failure of components can be physically modelled.

However, the physics-of-failure approach is also associated with big difficulties which were discussed in detail in (Todinov, 2017). Acquiring the relevant knowledge and data related to failure mechanisms and quantifying all types of uncertainty, necessary for a correct physics-of-failure model of the time to failure is not always possible because of the complexity of the physical mechanisms underlying the failure modes, the complex nature of the environment and the operational stresses.

Building a physics-of-failure is a formidable task which does not need to be addressed *if a third approach is adopted to reliability improvement and risk reduction where the focus is on general methods and principles for reliability improvement and risk reduction*. As a rule, the general reliability risk reduction methods and principles do not rely on reliability data or on a detailed knowledge of physical mechanisms underlying possible failure modes. These methods derive their strength from general laws, invariants and patterns associated with increased reliability and reduced risk. As a result, these methods are particularly useful in developing new designs, with no failure history and with insufficiently researched failure mechanisms. Work on formulating general principles and methods for improving the reliability and reducing technical risk has already been done (Todinov 2007, 2015, 2016). The present paper contributes to the exiting work an important generic reliability improvement and risk reduction method referred to as '*the method of separation'*.

Harmful interaction of factors critical to reliability and risk is a major source of failures. Separating risk-critical factors to reduce this harmful interaction is therefore a major avenue for improving reliability and reducing risk. Surprisingly, the method of separation has not yet been discussed as a risk-reduction tool. Despite that a number of techniques used in

engineering are clearly instances of the method of separation, they have never been recognised as such and have never been linked with this method.

The *method of division of tasks* featured in (Pahl et al, 2007) is effectively an application of the method of separation despite that it has not been linked with this method.

Next, *deliberate weak links* and *stress limiters* have already been used for preventing the stresses from reaching dangerous levels. The deliberate weak links are consciously designed weak points that are easily replaced (Eder, 2008) and usually protect expensive devices and reduce risk by reducing the consequences from failure. Despite that this technique is effectively an instance of a separation on a parameter, it has never been recognised as such and has never been linked with the method of separation.

Another example can be given with the concept 'barrier' (Svenson, 1991; Leveson, 2011; Hollangel, 2016). Barriers have also been used as accident prevention tools and protection measure mitigating the consequences from an accident. A classification of barriers has been proposed in (Eder, 2008). Despite that barriers are also instances of separation, no link has ever been made with the method of separation. Barriers distancing triggers from hazards reduce the likelihood of an accident while barriers distancing hazards from targets reduce the consequences given that accident has occurred.

Separation has been applied in the TRIZ methodology for inventive problem solving (Altshuller 1984,1996,2007) for resolving physical contradictions in engineering of the type: 'the object must have attribute *A* during one mode of use or during one stage of a particular process and the opposite attribute (not *A*) during an alternative mode of use or an alternative process stage'. However, the separation principle in TRIZ is not oriented towards reliability improvement and risk reduction and no specific treatment has been provided in the TRIZ methodology related to the mechanisms through which the separation works in increasing reliability and reducing risk which is central to the understanding and systematic application of this method for improving the reliability of engineering designs. No specific discussion regarding the mechanisms through which the method of separation increases reliability has been presented in more recent literature related to TRIZ (Terninko et al. 1998; Savransky 2000; Orloff 2006,2012; Rantanen and Domb, 2008; Gadd 2011).

TRIZ and other frameworks where the method of separation has been used never considered *stochastic separation* for which the separation is guaranteed only with a certain probability. TRIZ also never considered logical separation, where no time, space, or separation on a condition is present yet the dangerous proximity of hazards and targets is prevented.

The research conducted on the method of separation revealed that despite some isolated applications of the method of separation for risk reduction, such as separating hazards and targets by barriers', designing 'deliberate weak links' and 'stress limiters', these techniques are not understood as manifestations of the universal method of separation.

Here, it needs to be pointed out that 'the method of separation' *is not equivalent* to 'the traditional method of barriers separating hazards from targets'. While the method of barriers between hazards and targets is a special case of the method of separation and has been widely used before, *a number of mechanisms and techniques of the method of separation are fundamentally different and virtually unknown to engineers-designers and reliability practitioners*. Here are some examples:

- The method of '*stochastic separation*' which is also a special case of the method of separation does need theoretical models to be implemented correctly and derive any benefits from it;

- *Separation based on the cost of failure* and its application aspects is still not well understood considering the large number of high-consequence failures, in different industries, where the reliability of the component was not commensurate with the cost of its failure.

- Separation to counter poor performance caused by homogeneity is not understood and rarely used in design. The list can be continued.

The existing research on the method of separation as a risk reduction tool (Todinov, 2015) is rather limited and focuses only *on the application of the separation method for blocking common cause*.

A central weakness in applying the method of separation identified in the published literature is that no coverage of the mechanisms through which the method achieves reliability improvement and risk reduction has been presented. The lack of knowledge of the mechanisms through which the method of separation works does not permit its systematic implementation for improve reliability of engineering designs.

Another weakness in applying the method of separation is that this method has never been linked with mathematical models or algorithms which in a number of cases are absolutely necessary to release its potential.

By providing a succinct description of the system, a mathematical model or algorithm based on the method of separation would deliver significant benefits:

- The system can be described by taking into consideration the complex interaction of risk-critical factors which could not be contemplated by an engineer-designer.

- A mathematical model or an algorithm based on the method of separation provides a way of tracking the impact of the risk-factors on the reliability and risk level. In this respect, the mathematical model/algorithm provides an insight into which control variables are essential and which seemingly important control variables have actually no practical impact on the reliability and risk level.

- A mathematical model or algorithm based on the method of separation provides insight into which factor need to be altered and by how much to ensure an optimal effect (for example, balance between risk and cost of investment).

The identified gaps in the existing research on the method of separation define the primary objective of this paper: a comprehensive introduction into the mechanisms through which the method of separation achieves risk reduction and into the ways this method can be implemented in engineering designs.

Another objective of the paper to demonstrate that in a number of cases, the only way to extract benefit from the method of separation is to build and analyse a mathematical model or algorithm based on the method of separation.

2. Stochastic separation of risk-critical factors/events

2.1 Real-life applications which require stochastic separation

Risk is often the result of the simultaneous presence of risk-critical factors. Reducing risk then depends on the existence of a separation between the risk-critical factors. Here are a number of real-world examples illustrating this point.

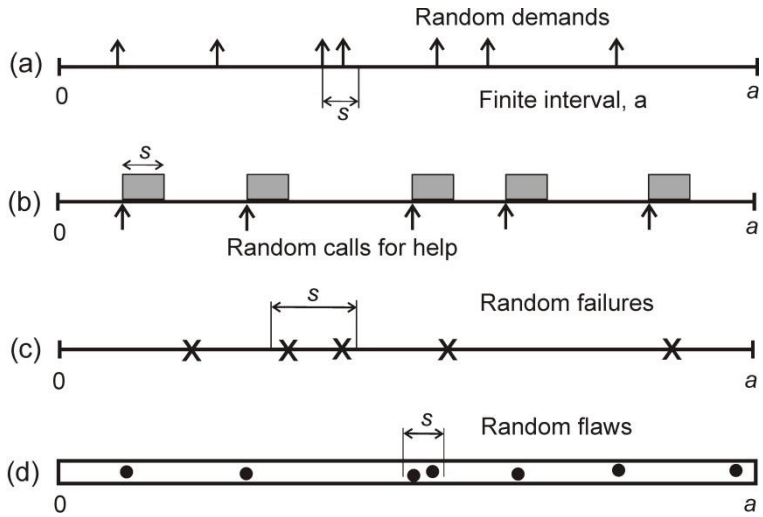

Figure 1 Common examples where risk depends on the existence of separation between risk-critical factors/events.

• A source servicing a number of randomly arriving requests (demands), where the source can only serve a single request at a time. Unsatisfied demand occurs if two or more demands cluster within a critical distance *s* (Figure 1a).

The competition of random demands for a particular resource/service on a finite time interval is a common example of risk and reliability controlled by the simultaneous presence of critical events. The appearance of a critical event engages the servicing resources and if a new critical event occurs during the service time of the first critical event, no servicing resources will be available for the second event.

Suppose that only a single repair unit is available for servicing failures on a power line. In the case of a power line failure, the repair resource will be engaged and if another failure occurs during the repair time *s* associated with the first failure (Fig.1c), no free repair resource will be available for recovering the power distribution system from the last failure. The delay in the second repair could lead to overloading of the power distribution system thereby inducing further failures.

There are cases where a very low probability of simultaneous presence (overlapping) of risk-critical critical events can be tolerated. A very low probability of a simultaneous presence of random demands can, for example, be tolerated in a situation where critically injured people demand a particular piece of life-saving equipment for a time *s* t (Fig.1b). If only a single piece of life-saving equipment is available, simultaneous demands within a time interval with length *s* cannot be satisfied and the consequences could be fatal.

• Stored spare equipment servicing the needs of customers arriving randomly during a specified time interval. After a demand from a customer, the warehouse needs a minimum time *s* to restore/return the dispatched equipment before the next demand can be serviced. In this case, the probability of unsatisfied demand equals the probability of clustering of two or more customer arrivals within the critical period needed for making the equipment available for the next customer (Figure 1a).

• Supply systems which accumulate the supplied resource before it is dispatched for consumption (compressed gaseous substances for example). Suppose that after a demand for the resource, the system needs a minimum period of specified length *s* to restore the amount of supplied resource to the level existing before the demand. In this case, the probability of unsatisfied demand equals the probability of clustering two or more demands within the critical recovery period *s* (Figure 1a).

• A related category of risk controlled by the overlapping (simultaneous presence) of

critical events is present when the appearance of one critical event (e.g. a shock) requires a particular time during which the system needs to recover. If another event appears before the system has recovered, the system's strength/capacity is exceeded by the load which results in system failure.

Such are, for example, shocks caused by failures associated with pollution to the environment (e.g. a leakage of chemicals) (Fig.1c). If such a failure is followed by another failure associated with leakage of chemicals, before a critical time interval has elapsed needed for recovery from pollution, irreparable damage to the environment could be done . For example, clustering of failures associated with a release of chemicals in the sea water could result in a dangerously high acidity which will destroy marine life.

- Forces acting on a loaded component which fails if two or more forces cluster within a critical time interval *s*.
- Clustering of two or more random flaws over a small critical distance *s* (Fig.1.d) dangerously decreases the load-carrying capacity of thin fibres and wires. As a result, a configuration where two or more flaws are closer than a critical distance cannot be tolerated during loading. Reliability in this case is governed by the probability of clustering of the random flaws.

In all of the suggested real-world examples, the overlapping of the risk-critical random events cannot be avoided therefore, risk is directly related to the probability of overlapping of risk-critical events. Reducing risk is achieved by reducing the probability of overlapping of the risk-critical events. In all these cases, it is important to guarantee with a specified probability a separation of minimum length between risk-critical events.

The probability with which the risk-critical random events should be separated varies significantly. It is directly related to the magnitude of the consequences resulting from the overlapping of two or more risk-critical events. The level of the probability of separation must be set individually by the risk experts in the respective application area.

Guaranteeing with a specified probability the existence of separation between risk-critical factors/events will be referred to as '*stochastic separation*'.

2.2 Stochastic separation of a fixed number of random events with different duration times

Consider a common case where demands for a single resource occur from a numbre of consumers, at random times during a time period, with different duration of the demand specific for the consumer. Because of the single piece of resource, a simultaneous demand from more than a single consumer cannot be satisfied.

This statement of the problem is formally presented as n random events, each with durations $d_1,...,d_n$, appearing randomly during a time interval $0,L$ ($d_1+d_2+...+d_n<L$). The objective is evaluating the probability that no overlapping of random events will be present (Fig.2a). The events start times $s_1,s_2,...,s_n$ are uniformly distributed along the interval $(0,L)$. The configuration in Fig.2a will be referred to as *X*-configuration. Note that the duration of the last event cannot possibly contribute to overlapping on the time interval $(0,L)$ and therefore can be ignored. The first $n-1$ duration intervals $d_1,...,d_{n-1}$ can then be 'cut out' of the time interval $(0,L)$ and the remaining parts of the time interval can be 'brought together' to form a shorter length $L-(d_1+d_2+...+d_{n-1})$ (Fig.2b). As a result of this operation, the points $s_1,s_2,...,s_n$ marking the start of the random events for the *X*-configuration transform into a unique *Y*-configuration where the points $s'_1,s'_2,...,s'_n$ are randomly distributed along

the length $L-(d_1+d_2+...+d_{n-1})$. As a result, for each *X*-configuration, corresponds exactly a single *Y*-configuration. Thus, for the set of all possible *X*-configurations and the set of all possible *Y*-configurations, the relationship $X \subseteq Y$ holds.

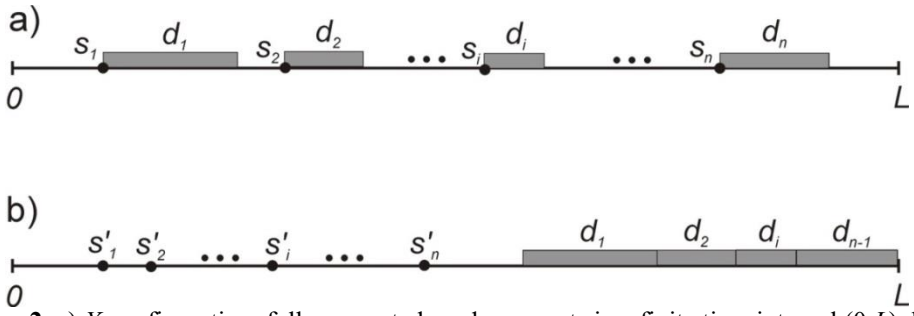

Figure 2. a) *X*-configuration: fully separated random events in a finite time interval (0,*L*); b) Y-configuration: random points generated along the interval (0,L) all falling in the interval 0, $L-(d_1+d_2+...+d_{n-1})$.

Now suppose that a set of *n* random points $s'_1, s'_2, ..., s'_n$ are randomly generated along the length *L*. If all *n* randomly generated points fall within the length $L-(d_1+d_2+...+d_{n-1})$, a *Y*-configuration is present. By inserting the corresponding demand intervals d_i ($i=1,...,n-1$) after each start time s_i, an *X*-configuration will be obtained with random non-overlapping demands along the interval 0,*L*.

Thus, from each *Y*-configuration, a unique *X*-configuration can be obtained by placing after the randomly generated points s'_i a duration intervals with lengths $d_1,...,d_{n-1}$ The start times in the *X*-configuration (Fig.2a) are therefore: $s_1 = s'_1$, $s_2 = s'_2 + d_1$, $s_3 = s'_3 + d_1 + d_2$,..., $s_n = s'_n + d_1 + d_2 + ... + d_{n-1}$. In the obtained *X*-configuration, all random events are fully separated. As a result, to each *Y*-configuration corresponds exactly a single *X*-configuration. Thus, for the set of all possible *Y*-configurations and the set of all possible *X*-configurations, the relationship $Y \subseteq X$ holds.

Since for the sets of the *X*-configurations and *Y*-configurations $Y \subseteq X$ and $X \subseteq Y$ simultaneously hold, there exists a one-to-one correspondence between the *X*-configurations, characterised by randomly located non-overlapping random events and the *Y*-configurations, characterised by randomly located random points on the smaller time interval $L-(d_1+d_2+...+d_{n-1})$. Because of the one-to-one correspondence between *X*-configurations and *Y*-configurations, the probability of an *X*-configuration can be estimated by the probability of a *Y*-configuration.

Suppose that the start times of the events are uniformly distributed along the length of the time interval (0,*L*). Let $A_1, A_2, ..., A_n$ denote the events 'the last event has a duration $d_1, d_2, ..., d_n$, correspondingly. The probability of the event *B* that there will be no overlapping of random events can be determined by the following probabilistic argument.

Initially, the conditional probability $P(B \mid A_n)$ is determined - the probability that there will be no overlapping of random events, given that the last event has a duration d_n. Because each random event has an equal chance to be the last event, the probabilities $p(A_i)$ of the events A_i are all equal to $1/n$ ($p(A_i) = 1/n$, $i = 1,...,n$).

The probability of an *Y*-configuration that *n* uniformly distributed random points $s'_1, s'_2, ..., s'_n$ along the interval (0,*L*) will fall in the interval $L-(d_1+d_2+...+d_{n-1})$ is given by $\left(\frac{L-(d_1+...+d_{n-1})}{L}\right)^n$. This is also the probability of an *X*-configuration (no overlapping events) given that the last event has a duration d_n.

$$P(B \mid A_n) = \left(1-\frac{(d_1+...+d_{n-1})}{L}\right)^n \tag{1}$$

The absence of overlapping (event *B*) however, can occur in *n* different ways. The absence of overlapping can occur given that the last event has a duration d_n, given that the last event has a duration d_{n-1},..., and so on. The probabilities $P(B \mid A_i)$, $i = 1,...,n-1$, are determined in a similar fashion. According to the total probability theorem,

$$P(B) = P(B \mid A_1)P(A_1) + ... + P(B \mid A_n)P(A_n) \tag{2}$$

As a result, the expression

$$P(B) = \frac{1}{n}\left[\left(1-\frac{d_2+d_3+...+d_n}{L}\right)^n + \left(1-\frac{d_1+d_3+...+d_n}{L}\right)^n + ... + \left(1-\frac{d_1+d_2+...+d_{n-1}}{L}\right)^n\right] \tag{3}$$

is obtained for the probability of a full separation (no overlapping) of random events with durations $d_1, ..., d_n$. Equation (3) can also be presented as

$$P(B) = \frac{1}{n}\left[\left(1-\frac{D-d_1}{L}\right)^n + \left(1-\frac{D-d_2}{L}\right)^n + ... + \left(1-\frac{D-d_n}{L}\right)^n\right] \tag{4}$$

where $D = d_1 + d_2 + ... + d_n$.

Equation (4) has been confirmed by the results from computer simulations. Thus, for four consumers demanding a particular resource for $d_1 = 5\,\text{min}$, $d_2 = 10\,\text{min}$, $d_3 = 20\,\text{min}$, and $d_4 = 35\,\text{min}$ respectively, during a time interval of 10 hours, the probability of no overlapping calculated from equation (4) is 0.7. This probability has been confirmed by the probability of 0.7 estimated from the simulation. (The details of the simulation algorithm have been omitted). For a given set of events with duration times $d_1, ..., d_n$ three principal mechanisms of stochastic separation can be implemented:

- Providing stochastic separation with a specified probability $P(B)$ by decreasing the durations of the events.
- Providing stochastic separation with a specified probability $P(B)$ by increasing the length *L* of the time interval.
- Providing stochastic separation with a specified probability $P(B)$ by decreasing the number of events.

All of these mechanisms can be implemented by solving the non-linear equation (4) with respect to *L*, or with respect to *n* or with respect to the durations of the demand times.

Suppose that three consumers are demanding a particular resource for $d_1 = 35\,\text{min}$, $d_2 = 45\,\text{min}$, and $d_3 = 60\,\text{min}$ during an interval of $L = 500$ min. The factor $0 < k < 1$ by which the demand times d_1, d_2 and d_3 need to be reduced is now sought so that the probability of no overlapping is equal to a specified level of 0.7.

To determine the factor *k*, the non-linear equation

$$f(k) \equiv \frac{1}{3}\left[\left(1-\frac{k(D-d_1)}{L}\right)^3+\left(1-\frac{k(D-d_2)}{L}\right)^3+\left(1-\frac{k(D-d_3)}{L}\right)^3\right]-0.7=0 \qquad (5)$$

can be solved with respect to *k* by a repeated bisection in the interval $k_{\min}=0.01 \le k \le k_{\max}=1$ because at the ends of this interval $f(k)$ has different signs ($f(k_{\min})>0$ and $f(k_{\max})<0$). The solution of equation (5) with respect to the parameter *k*, obtained by using a standard repeated bisection algorithm, is $k=0.6$. Thus, in order to provide the required separation probability of 0.7, the durations of the demand times need to be reduced to $d'_1=kd_1=0.6\times 35=21$; $d'_2=kd_2=0.6\times 45=27$ and $d'_3=kd_3=0.6\times 60=36$. Substituting these values in equation (4) where n=3 gives:

$$\frac{1}{3}\left[\left(1-\frac{84-21}{500}\right)^3+\left(1-\frac{84-27}{500}\right)^3+\left(1-\frac{84-36}{500}\right)^3\right]=0.7$$

Suppose that durations x_1, $x_2,...,x_{n-1},x_n$ of the first, second,...,nth random event are realisations of a random variable *X* following a statistical distribution with mean μ and standard deviation σ. According to equation (5), the probability that the random events will be separated (will not overlap) are given by

$$P(B)=\frac{1}{n}\left[\left(1-\frac{D-x_1}{L}\right)^n+\left(1-\frac{D-x_2}{L}\right)^n+...+\left(1-\frac{D-x_n}{L}\right)^n\right] \qquad (6)$$

where $D=\sum_{i=1}^{n} x_i$.

The mathematical model of stochastic separation of a fixed number of risk-critical events provides the opportunity to gain insight into the fact that the increase of the demand times x_i by a particular factor $k>1$ and the increase by the same factor $k>1$ of the length of the operational interval *L will have no impact on the probability of overlapping*. Thus, an increase of the demand times by 10% therefore can be compensated by a corresponding increase by 10% of the length of the operation interval *L*.

Even for a relatively small number of events, the sum of the event durations $\sum_{i=1}^{n} x_i - x_1$, $\sum_{i=1}^{n} x_i - x_1,...,\ \sum_{i=1}^{n} x_i - x_n$ in equation (6) can be approximated reasonably well with $(n-1)\mu$, where μ is the mean of the duration times x_i. As a result, the probability $P(B)$ of a full separation (non-overlapping) of random events becomes

$$P(B)\approx\left(1-\frac{(n-1)\mu}{L}\right)^n \qquad (7)$$

This probability is practically insensitive to the variance of the random variable *X* standing for the durations x_i of the demand times. The probability $P(B)$ depends on the expected value $\mu=E(X)$ of the demand times. The probability of event separation is practically insensitive to the variance (standard deviation σ) of the demand times *X*.

This conclusion has been verified by numerous computer simulations where the probability of overlapping has been plotted as a function of the variance of the duration times.

The simulations involved demand times following a log-normal distribution with mean 140 min, coming from 36 users over a time interval with length 60000 min (1000 hours). Each of the 36 users initiates exactly one demand, randomly located on the operational time

interval (0,60000 min). A single source for servicing the random demands is available, capable of servicing only a single random demand at a time.

The simulation results shown in Fig.3 have been obtained after incrementing the standard deviation of the demand times by a step of 5min. The calculated probabilities of unsatisfied demand of 0.95 correspond to a single source servicing the demands.

If a constant duration of the random demands is used, equal to the mean of 140 min of the log-normal distribution, the same value of 0.95 is obtained for the probability of no overlapping.

In the next simulation experiment, the log-normal distribution of the demand times was replaced by a normal distribution with the same mean (140 min). The number of users (36) and the length of the operation interval (1000 hours) were kept the same as in the previous simulation experiment. The standard deviation of the normal distribution was varied with a step of 5 min. The results were almost identical to the results in Fig.3.

The calculated probability of fully separated random demands was again 0.95.

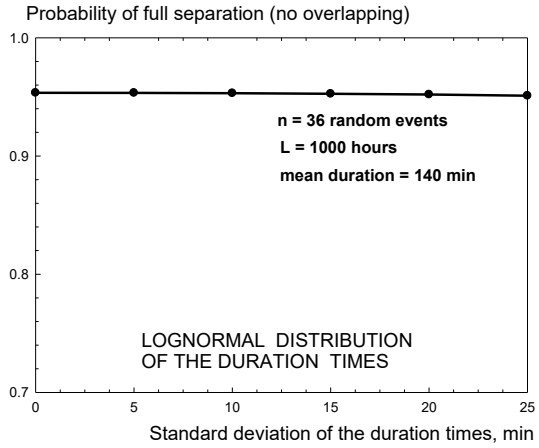

Figure 3. Probability of full separation of random events (no overlapping) as a function of the variance of the log-normal distribution modelling the duration times.

In the next simulation experiment, a uniform distribution for the duration of demand times has been selected, with a probability density function $f(t) = \frac{1}{2a}$ if $140 - a \le t \le 140 + a$ and $f(t) = 0$ if $t > 140 + a$ or $t < 140 + a$, where t is the time. The parameter a determines the spread of the uniform distribution. The uniform distribution and its parameter have been specified in such a way that its mean (140 min) coincides with the mean of the log-normal distribution and the normal distribution used in the previous simulations. Again, the random demands come from 36 users over a time interval with length 60000 min (1000 hours). Each of the 36 users initiates exactly one demand, randomly located along the operational time interval of 1000 hours. The results for the probability of unsatisfied demand, for a different spread a of the distribution, are almost identical to the ones shown in Fig.3.

In the next simulation experiment, a triangular distribution, with probability density function $f(t) = 0.004762 \times (1 - t/420)$ was used as a model of the demand times. The distribution function and the parameters of the triangular distribution have been specified in such a way that its mean (140 min) coincides with the means of the log-normal distribution, the normal distribution and the uniform distribution used in the previous simulations. Random sampling from the triangular distribution has been done by using the Von Neumann' rejection method (Ross, 1997).

The result from the simulation using demand times following a triangular distribution, were again 0.95 for the probability of a full separation, if a single source is present.

The final simulation involved a single source and only n=2 random demands during a time interval of 17 hours. The random demand times were sampled from a normal distribution with mean $\mu = 140$ minutes. The standard deviation was varied within the range (0-25min).

As can be verified from the results in Fig.4, even for the smallest possible number of random events (n=2) which could result in overlapping, the simulated probability of full separation (no overlapping) is still practically insensitive to the variance of the durations of the random demands.

Finally, the duration times were sampled from a discrete distribution with mean equal to 140 min. The discrete distribution was defined as follows: with probability 0.3 the event duration was 200.67 min and with probability 0.7, the event duration was 114 min. The mean duration time of the simulated events is therefore $\mu = 0.3 \times 200.67 + 0.7 \times 114 = 140$ min. The simulated probability of no overlapping (full separation) was 0.745 and was once again, very close to the probability of no overlapping simulated with normal distribution of the event durations with mean 140min.

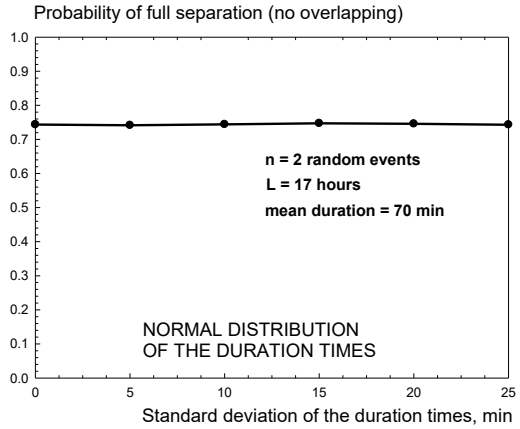

Figure 4. Probability of full separation of two random events (no overlapping) as a function of the variance of the normal distribution modelling the duration times.

The practical insensitivity of the probability of full event separation to the variance of the duration times, for a very small number of random events, can be understood from analysing the expression for the probability of no overlapping of two random events. From equation (3), this probability is:

$$P(B) = \frac{1}{2}\left[(1 - x_2 / L)^2 + (1 - x_1 / L)^2\right] \tag{8}$$

where x_1 is a random variable representing the duration time of the first event and x_2 is a random variable representing the duration times of the second random event.

Expanding expression (8) results in

$$P(B) = 0.5 \times \left(1 - 2x_2 / L + x_2^2 / L^2 + 1 - 2x_1 / L + x_1^2 / L^2\right) \tag{9}$$

Taking expectations from both sides of equation (9) results in

$$E[P(B)] = 0.5 \times \left(1 - 2E(x_2) / L + E(x_2^2 / L) + 1 - 2E(x_2) / L + E(x_1^2 / L^2)\right) \tag{10}$$

In equation (10), $E(x_1) = E(x_2) = \bar{x}$, where $\bar{x}$ is the mean of the duration times of the random events.

It is known that if X is a random variable with finite mean and y is a convex function ($\lambda y(a)+(1-\lambda)y(b) \geq y(\lambda a+(1-\lambda)b)$, $0 \leq \lambda \leq 1$; $a,b \in \mathbf{R}$) then the Jensen's inequality holds (Rosenthal, 2006):

$$E(y(x)) \geq y\big(E(x)\big) \tag{11}$$

The function $y=(x/L)^n$ is a convex function for $n \geq 1$, therefore, according to the Jensen's inequality, $E[(x/L)^n] \geq (\bar{x}/L)^n$ holds. However, for small ratios x_i/L ($i=1,2$), the terms x_i^n/L^n are very small, and the error from replacing $E(x_i^n/L^n)$ with $[E(x_i)]^n/L^n)=\bar{x}^n/L^n$ are also very small. Consequently,

$$E[P(B)]=P(B) \approx 1-2\bar{x}/L+\bar{x}^2/L^2)=\left(1-\frac{\bar{x}}{L}\right)^2 \tag{12}$$

can be used for the probability of no overlapping of the random events. As can be verified from equation (12), for small ratios $\bar{x}/L$, the probability of no overlapping of two random events is practically insensitive to the variance of their duration times.

Indeed, consider the function $f(x) \equiv (x/L)^n$, $n \geq 2$, where $x/L << 1$. Consider also the linear function $g(x)$ which is a tangent to $f(x) \equiv (x/L)^n$, at $x=\bar{x}$. Let us restrict the average demand time to $|\bar{x}| \leq (1/20)L$.

Considering that for the derivative of $f(x) \equiv (x/L)^n$ we have $f'(x) \equiv (n/L)(x/L)^{n-1}$, the slope of the tangent at $x=\bar{x}$ is $f'(\bar{x}) \equiv (n/L)(\bar{x}/L)^{n-1}$. The tangent line therefore has the equation

$$g(x)=(n/L)(\bar{x}/L)^{n-1}x+(\bar{x}/L)^n-(n/L)(\bar{x}/L)^{n-1}\bar{x} \tag{13}$$

The difference $f(x)-g(x)$ becomes

$$f(x)-g(x)=(x/L)^n-(n/L)(\bar{x}/L)^{n-1}x-(\bar{x}/L)^n+(n/L)(\bar{x}/L)^{n-1}\bar{x} \tag{14}$$

However, x can be presented as $x=\bar{x}+h$, where h is a positive or negative increment. Let us restrict its absolute value also to $|h| \leq (1/20)L$.

Substituting $x=\bar{x}+h$ in equation (14) gives

$$f(x)-g(x)=(\bar{x}+h)^n/L^n-(n/L)(\bar{x}/L)^{n-1}(\bar{x}+h)-(\bar{x}/L)^n+(n/L)(\bar{x}/L)^{n-1}\bar{x} \tag{15}$$

Expanding the right hand side of (15) gives

$$f(\bar{x}+h)-g(\bar{x}+h)=\frac{n(n-1)}{2!}\frac{\bar{x}^{n-2}}{L^{n-2}}\times\frac{h^2}{L^2}+\frac{n(n-1)(n-2)}{3!}\frac{\bar{x}^{n-3}}{L^{n-3}}\times\frac{h^3}{L^3}....+\frac{h^n}{L^n} \tag{16}$$

Without loss of generality we could assume that $h>0$. For the right hand side of (16) we have

$$f(x)-g(x) \leq \left[\frac{n(n-1)}{2!}+\frac{n(n-1)(n-2)}{3!}....+1\right]\times\frac{h^n}{L^n}$$

Considering that $n+\frac{n(n-1)}{2!}+\frac{n(n-1)(n-2)}{3!}....+1=2^n$,

$$f(x)-g(x)<2^n\times\frac{h^n}{L^n}<2^n\frac{1}{2^n\times 10^n}=\frac{1}{10^n} \tag{17}$$

As a result, the difference $f(x)-g(x)$ is very small and its expected value can be considered to be negligible

$$E[f(x)-g(x)] \approx 0 \tag{18}$$

Taking expected values from the left hand side of equation (15) results in

$$E[f(x)-g(x)]=E[(x/L)^n-(n/L)(\bar{x}/L)^{n-1}x-(\bar{x}/L)^n+(n/L)(\bar{x}/L)^{n-1}\bar{x}]$$

which is equivalent to

$$E[f(x)-g(x)]=E[(x/L)^n]-(E(x)/L)^n \tag{19}$$

Because from equation it follows that $E[f(x)-g(x)]\approx 0$, equation (19) now yields

$$E[(x/L)^n]\approx[E(x)/L]^n=\bar{x}^n/L^n \tag{20}$$

for small ratios $\bar{x}/L$.

Consequently, equation (12) can indeed be used for the probability of no overlapping of the random events. For small ratios $\bar{x}/L$, the probability of no overlapping of the two random events is practically insensitive to the variance of their duration times.

Equation (12) has also been verified by numerous computer simulations.

The simulation results and the theoretical analysis demonstrate that the probability of non-overlapping of random events is practically insensitive to the type of the distribution of the duration times, provided that the means of the distributions are not altered.

The simulation results and the theoretical analysis also demonstrate that the probability of non-overlapping of random events is practically insensitive to the variance of the duration times.

The mathematical model of stochastic separation of a fixed number of risk-critical events provided the insight that the variance of the demand times *X* practically has no impact on the level of risk as long as the mean of the demand times remains the same.

These results also provide the valuable opportunity to work with random demand times characterised by their means only and not requiring information related to the variance of the demand times.

2.3 Stochastic separation of random events following a homogeneous Poisson process

Suppose that the times of the risk-critical events follow a homogeneous Poisson process in the time interval (0,*L*) and each event has a duration equal to 's'. In other words, the number of events in the time interval is a random variable. According to an equation rigorously derived in (Todinov, 2004), the probability p_0 that there will be no clustering of two or more random events within a critical distance *s* is

$$p_0=\exp(-\lambda L)\left(1+\lambda L+\frac{\lambda^2(L-s)^2}{2!}+...+\frac{\lambda^r[L-(r-1)s]^r}{r!}\right), \tag{21}$$

where *r* denotes the maximum number of time gaps of length *s*, which can be accommodated into the finite time interval with length *L* ($r=[L/s]+1$), where $[L/s]$ is the greatest integer which does not exceed the ratio *L/s*).

Consider now the real-life problem of requests for particular unique control equipment during a 24 hour period. The requests arrive randomly (follow a homogeneous Poisson process) with density 0.2 hour^{-1} (on average 2 requests per 10 hours) and the control equipment can service only a single request at a time. Assume that initially *s=1 hour* has been allocated for servicing each request. Without using a stochastic separation model the actual probability of unsatisfied request for the control equipment could not be guessed correctly even by experts. The calculation using the model presented by equation (21) yields the highly counter-intuitive result that there is approximately 52% probability that within 24 hours there will be a case for which no control equipment will be available on demand. This counter-intuitive result is actually confirmed by the Monte Carlo simulation which also yields 52% for the probability that the equipment will be unavailable on demand.

To reduce the probability that the control equipment will be unavailable on demand to 20%, the equation

$$0.2 = 1 - \exp(-\lambda L)\left(1 + \lambda L + \frac{\lambda^2 (L-s)^2}{2!} + \ldots + \frac{\lambda^r [L-(r-1)s]^r}{r!}\right) \tag{22}$$

must be solved with respect to s. The solution yields, $s \approx 0.25$ h. In order to provide a stochastic separation that satisfies the tolerable probability of unsatisfied demand of 20%, the use of the control equipment must be restricted to 0.25hours.

This real-life example demonstrates that only by creating a mathematical model (or algorithm) based on the principle of separation, benefit can be extracted from the method of stochastic separation.

Running the model of the stochastic time separation of demand following a Poisson process reveals an interesting behaviour. While for a fixed number of random demands increasing the length of the operational time interval reduces the probability of overlapping, with random demands following a Poisson process on a time interval, increasing the length of the operational time increases the probability of overlapping.

Accordingly, Equation (21) can also be used for setting reliability requirements to provide a stochastic time separation (avoiding clustering) of duration at least s, with high probability. For any specified time of demand s and a minimum probability p_0 with which the separation intervals of length at least s must exist, solving the equations with respect to λ yields an upper bound λ^* (an envelope) for the number density of the random events. The envelope guarantees that whenever for the number density λ of events, $\lambda \le \lambda^*$ is fulfilled, the specified minimum separation of length at least s will exist between the random requests, with a minimum probability p_0. In other words, with the specified probability p_0, there will be no unsatisfied request for the required resource.

It is necessary to point out, that a stochastic time separation can be achieved not only by reducing the number density of random demands and reducing the demand times but also by increasing the number of sources servicing the random demands. This type of stochastic separation also reduces the probability that there will be a random demand for which no service will be available.

The proposed idea of stochastic time and space separation could form the core of a new methodology for reliability analysis and setting reliability requirements based on minimum separation intervals between random events on a finite interval.

3. Deterministic separation of risk-critical factors

Deterministic separation of random events on a time interval is present when, for the random events, a zero probability of overlapping is guaranteed. Full separation is important for scheduling critical random events for which any overlapping has grave consequences and, because of this, a simultaneous presence of events must be excluded completely.

Familiar examples of a deterministic separation of risk-critical factors are: (i) the time separation provided by the traffic lights, preventing collision between intersecting flows of traffic and flows of pedestrians and (ii) the space separation provided by the isolation of intersecting flows of traffic and flows of pedestrians at different levels in order to eliminate the risk of collisions and accidents.

3.1 Deterministic time separation by scheduling

3.1.1 Deterministic time separation by scheduling, with fixed starts of the events

Deterministic separation in time is required from risk-critical factors or entities whose simultaneous presence must be excluded completely.

The time separation by scheduling enforces consistent time spacing between hazardous events. The deterministic time separation is used in air traffic control, where it enforces consistent time spacing between arriving aircrafts, on the basis of real-time information about the weather, headwinds, altitude and speed. In this respect, the air-traffic control clearance is an important instrument providing the necessary separation in order to avoid collisions within controlled airspace. The separation provided by the air-traffic control clearance also guarantees a sufficient runway approach capacity which keeps the risk of accidents low.

3.1.2 Deterministic time separation with random starts of the events

The method used for deriving the equation related to the probability of overlapping of a fixed number of random events can also be used to provide a deterministic separation of events on a time interval whose start times must be random.

Suppose that n random events each with duration d, need to be scheduled over the time interval $0,L$ such that the possibility of overlapping of random events is excluded completely and, at the same time, the start times s_i of the events are truly random along the time interval $(0,L)$.

Consider the configuration for which the random start times $s'_1, s'_2, ..., s'_n$ are generated along the smaller length $L-(n-1)d$, by a random generator of uniformly distributed random numbers (Fig.5a). From this configuration, the configuration in Fig.5b can be obtained by placing after each randomly generated s'_i point, a duration interval with length d (Fig.5b). The start times in the obtained X-configuration in Fig.5b are $s_1 = s'_1$, $s_2 = s'_2+d$, $s_3 = s'_3+2d$,..., $s_n = s'_n+(n-1)d$.

As a result, the random events are scheduled over the time interval $0,L$ in such a way that no overlapping of random events is present and at the same time, the start times s_i of the events are truly random along the time interval $(0,L)$.

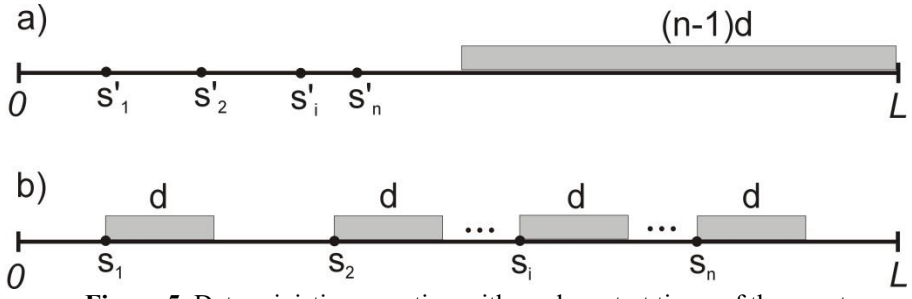

Figure 5. Deterministic separation with random start times of the events.

3.2 Deterministic time and space separation by using interlocks

Preventing the simultaneous occurrence of two events can be done by implementing a sentinel whose state is returned as 'busy' if an event is still active. The state of the sentinel

can be interpreted subjectively (separation by interpretation). The state of the sentinel is checked and a new event can be launched only if the current state of the sentinel is 'free'. Upon termination of the event, the state of the sentinel is changed to 'free'. The sentinel can also be built in an interlock which prevents the overlapping of events.

A realisation of this mechanism for deterministic time separation has been given in Fig.6 with the three buttons B1,B2 and B3 which activate corresponding electro-motors e1,e2 or e3, each of which is responsible for a motion in a particular direction. Once a button is pushed, the circuit of the corresponding electro-motor must stay latched until the stop button *S* is pressed and the circuit of the electromotor is opened. While the circuit of any particular electromotor remains energised, pushing any other button must have no effect.

Consider the circuit in Fig.6a. Pushing button B1, closes the normally open contact *k*1 and the circuit of electromotor *e*1 is latched into energized state. At the same time, the normally closed sentinel contact *F* is opened, which prevents energising the circuit of any other electro-motor (*e*2 or *e*3) (Fig.6b). Electromotor *e*1 will be running until the stop button *S* is pressed. Pressing the stop button *S* de-energizes the circuit of electro-motor *e*1 and restores the open contact *F* into its normally closed state. This is effectively a process of moving the sentinel into a 'free' state. Only now will the circuit react to pressing of any other button. Pressing button B2, for example, closes the normally open contact *k*2 and the circuit of electromotor *e*2 is latched into energised state (Fig.6d). At the same time, the normally closed sentinel contact *F* is opened and the process is repeated.

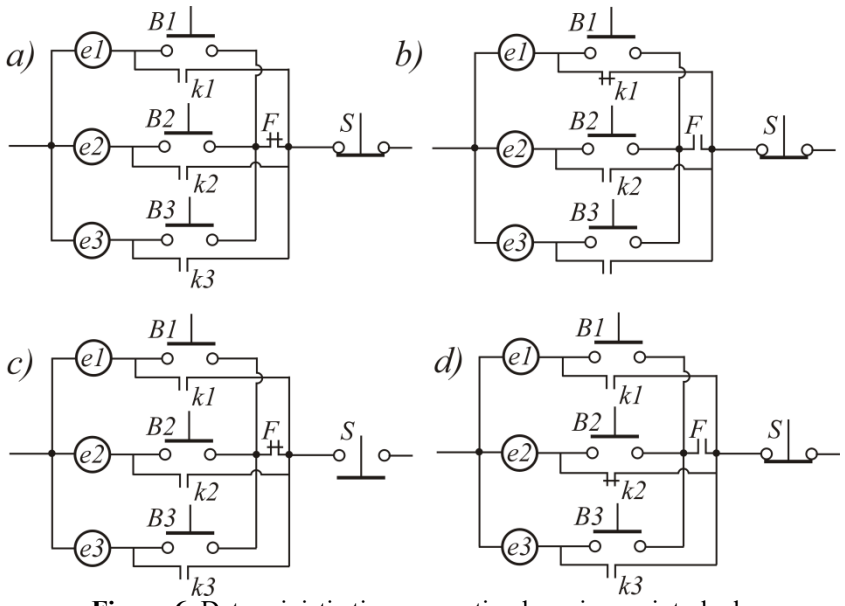

Figure 6. Deterministic time separation by using an interlock.

The dangerous simultaneous energising of two electro-motors has been excluded by the time interlock implemented through a sentinel.

The deterministic space separation can also be based on interlocks. A mechanism by which space separation can be achieved is through opening a power circuit or control circuit.

A simple implementation of this separation mechanism is the interruption of the power supply circuit from removing the protective shield of rotating machinery. As a result, it is impossible to operate the machine without positioning first the protective shield in place, which reduces the likelihood of injury.

A more sophisticated example of this type of space interlock is the presence-sensing safeguard interlocks which stop the operation of hazard equipment if a person is detected in a location where injury can occur. The presence-sensing system could be based on laser beams,

light or infra-red beams. Beams of light forming a curtain are generated and if any of the beams is blocked by a person moving towards the hazard equipment, a control circuit is opened and the power to the hazard equipment is switches off.

Another mechanism of space separation is the trapped-key interlock. In one of the possible implementations, the access for repair to the hazard equipment is through a door operated by a key which is held trapped on the door until the door is firmly closed again by operating the key. While opening the door, the key also operates a switch interrupting the power supply. The hazard equipment cannot be re-energized until the door is closed and the key released. Releasing the key essentially guarantees that the hazard equipment has been made safe.

3.4 Deterministic logical separation by using a shared unique key

Deterministic logical separation is present when it is *logically impossible* for a dangerous operation to occur at a given point in time or at a given space location. Deterministic logical separation is also in place if it is logically impossible for two or more objects to be in a dangerous proximity at a given location or at a given time.

In logical separation, no barriers of any kind are set between the different parts of the system yet separation is still present. The dangerous proximity of hazards and triggers and hazards and targets is made to be logically impossible.

Consider the safety problem related to preventing the hand of an operator from being in the cutting area of a guillotine. If the cutting action is activated only by a simultaneous pressure on two separate knobs/handles which engage both hands of the operator, it is logically impossible for the operator's hand to accidentally reside in the cutting area, at any time. The operator's hands have been separated from the cutting area through the logic of the guillotine activation. This is an example of a deterministic logical separation reducing the risk of an accident.

Logical separation avoiding dangerous simultaneous occurrence of processes can be implemented relatively easily by using the mechanism of the *shared unique key*. A unique shared key is required for activating each process in accomplishing a particular action. As a result, the dangerous action cannot occur because the unique key cannot be simultaneously present to activate more than one process. If a switch can be activated only through a specially calibrated unique key, the key will be needed for sequentially activating each process and no simultaneous occurrence of two processes could possibly occur.

The realisation of this idea can be seen on Fig.7. Suppose that a particular process requires an adjustment of a specimen before switching on X-ray beam. The dangerous simultaneous occurrence is possible if a person appears in Room *A* and switches on the *X*-ray beam while the operator is still adjusting the specimen under the *X*-ray head in room *B* (Fig.7).

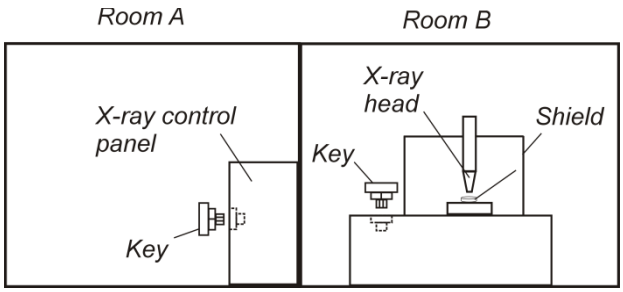

Figure 7. An example of logical separation

The dangerous action can be prevented from occurring by a logical separation implementing a shared unique key. The design of the *X*-ray equipment must be made in such a way that the switch releasing the *X*-ray shield in order to position the specimen and the

switch operating the *X*-ray beam in room *A* can only be done by using the same shared unique key. Switching on the *X*-ray beam and adjusting the specimen would then require the same object (the shared unique key) to be at two different places, at the same time, which is impossible. The safety risk has been eliminated by a logical separation based on a shared unique key.
Logical separation leads to low-cost yet very efficient designs eliminating safety risks. It is a simple yet underutilized generic tool for improving safety and reducing risk.

3.5 Deterministic separation by providing conditions for independent operation

Deterministic separation can be realised by providing conditions for independent operation of components. If failure of one component makes the failure of another component more likely, the reliability of the system can be improved by making the two devices operate independently from one another. Consider the operation of two devices where the second device is powered from the first device. Failure of the first device will cause a loss of power for the second device. The reliability of the system can be improved if the operation of the two devices is separated.

Often, in control systems, to cut the cost, the control modules share the same cables. In this case, the control channels are not independent because failure of a common cable will cause several control channels to fail. Separating (decoupling) the control channels ensures the independent operation of the control channels and improves the reliability of the system.

Separation to block a common cause is present when a component or a group of components are distanced (insulated) from the action of a common cause, simultaneously affecting the performance of the components. A common cause reduces the reliability of a number of components simultaneously. The affected components are then more likely to fail, which reduces the overall system reliability. Detailed discussion of separation mechanisms for blocking a common cause has been presented in Todinov, 2015).

4. Separation on a parameter, conditions or scale

Reducing risk by a separation assuring distinct behaviour at different values of a risk-critical parameter is present when different characteristics of an object at different values of a risk-critical parameter are ensured to reduce the likelihood of failure or the consequences given that failure has occurred.
Introducing deliberate weak links and stress limiters is an important mechanism for assuring separation from dangerous levels of risk-critical parameters.

4.1 Separation at distinct values of a risk-critical parameter through deliberate weak links and stress limiters

The deliberate weak links are deliberately created points of weakness towards which a potential failure is channelled in order to limit the magnitude of the consequences given that failure has occurred. The mechanisms through which the deliberate weak links operate can be classified into several types.

4.1.1. Deliberate weak links designed to separate a valuable part/component from excessive levels of the stress (current, voltage, temperature, pressure, force, etc.)

Effectively, this type of deliberate weak links separate from excessive levels of a particular stress. A well-known example related to this type of deliberate weak links are the

electric fuses, which protect electrical circuits against current/voltage exceeding critical tolerable levels. Another common example of this type of deliberate weak links is the shear pin in a mechanical coupling, which transmits torque up to a specified level, beyond which the shear pin fails and disconnects the driving shaft from the mechanical device. As a result, the critical torque resistance of the mechanical device cannot be reached and the mechanical device is separated from overload. Rupture discs are also examples of such deliberate weak links. They protect vessels from over-pressurisation by providing separation from excessive load.

Crash cones used in race cars separate against excessive deceleration during impact by deforming during an impact thereby increasing the time during which the deceleration force is present. Sacrificial anodes can also be considered to be deliberate weak links separating components (underground pipes, underwater installations, ship hulls) from excessive corrosion.

Deliberate weak links can also separate from excessive wear. For example, cheap rubber segments bolted on top of a conveyor act as deliberate weak links. They take all the excessive wear and their failure is followed by the replacement of a cheap rubber segment rather than by the replacement of an expensive conveyor belt.

4.1.2. Deliberate weak links designed to deflect the failure location from a region (part of the system) where the cost of failure is high.

Effectively, this mechanism provides a separation of the failure location from expensive part of the system. An efficient implementation of this type weak link is through appropriately placed pre-cracks or stress-relieve gaps around the protected valuable part of the system. The pre-cracks or gaps offer a small resistance to the propagation of the main crack. As a result, the main crack is deflected along the deliberate weak paths and damage on the valuable part of the system is prevented.

Cuts made parallel to cables buried underground act as deliberately weakened paths. In the case of very low temperatures freezing the ground, the shrinkage cracks appearing in the ground are deflected alongside the weak cuts which offer small resistance to crack propagation. As a result, the cracks in the frozen ground are deflected along the deliberate weak paths thereby preventing severing of the cables.

Consider another example related to rigid floor tiling over a concrete slab. Concrete slabs shrink as they dry out. The shrinkage is often sufficient to form cracks which propagate through the slabs. The floor tiles laid over these cracks will also crack and the result is costly damage. Deflections in suspended floors can also induce high compressive stresses in rigid floor tiling which cause delamination and cracks.

The costly damage could be avoided easily if deliberate weak links are created within the flow coverings as deliberate gaps (filled with plastic) which allow stress relieve and deflect possible cracks in the tiling caused by shrinkage.

4.1.3 Deliberate weak links designed to provide warning that the system is in a state of overload.

Effectively, this type of deliberate weak links separate from failure by providing a warning.

A mechanism through which this type of separation can be designed is to ensure that before the main failure, a secondary failure occurs that provides warning alerting the operator to decrease the load and avoid catastrophic failure.

An implementation of this separation mechanism is the retrofitable cable mechanical fuse in Fig.8 (US patent US20110027007 A1).

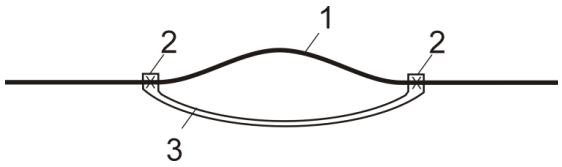

Figure 8. Retrofitable cable mechanical fuse

A cable 1 forms a slack inside the device and is attached securely to the device by the clamps 2. In normal operation conditions, the load is carried only by the weakened part 3 of the device. When the load exceeds a critical level, the weakened part first bends, then breaks and finally the load is transferred to the cable 1. This provides ample warning to the operator that the permitted operating load has been exceeded.

4.1.4 Deliberate weak links designed to trigger or activate other systems in order to reduce the consequences from failure.

An example of a weak link of this type is the alloy with low melting point which seals a reservoir with fluid under pressure (sprinkler system). In the case of fire, the deliberate weak link fails and a jet of fluid is released in the premise where fire started.

Similar to the deliberate weak links, stress limiters also separate from excessive levels of stress. A common example of a stress limiter is the anti-surge protector preventing voltage from reaching dangerous levels that could damage electrical equipment. The safety pressure valve, activated when pressure reaches a critical level, is another common example of a stress limiter separating the loading stress from the strength of the material. The friction clutches is another example of a stress limiter, that has been specifically designed to slip during a torque overload. While deliberate weak links are designed to fail and separate from excessive loading stress, stress limiters separate from excessive loading stress without necessarily suffering failure.

It is tempting to consider stress limiters as instances of deliberate weak links because they also channel failure in order to separate from excessive levels of loading stress. However, there are essential differences. Not all stress limiters are deliberate weak links just as not all deliberate weak links are stress limiters.

The retrofitable cable mechanical fuse from Fig.8, for example, is a deliberate weak link without being a stress limiter. The device only provides warning and does not limit the load.

Alternatively, the specially designed shoulder on the screw in Fig.9 which prevents over-tightening of the screw and damaging the tightened plastic component, is a stress limiter without being a deliberate weak link. The magnitude of the loading stress on the clamped part is limited without a deliberate weakness.

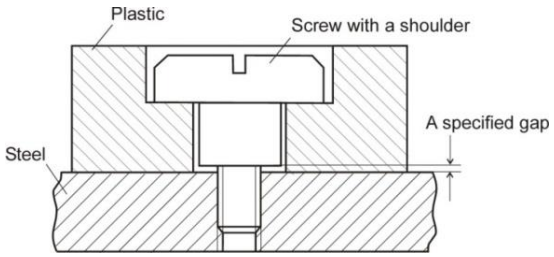

Figure 9. An example of a stress limiter: eliminating the risk of damaging the plastic part by a special design of the screw.

4.4 Separation on a parameter by using the mechanism of phase changes

Separation by using phase changes is an important mechanism to provide a separation on 'temperature' which is a common risk-critical parameter. A very reliable separation on operating temperature can be made by using the changes in the aggregate state of the material which are guaranteed with temperature. Thus, freezing volatile and flammable substance during transportation eliminates the risk of spillage and explosion during a road accident. The low melting point of special alloys can be used for highly reliable triggers for sprinkler systems in the case of fire. The reliability of complex triggers based on thermostats, sensors and electronic circuits, etc., is not very high.

Phase changes of the magnetic state of materials can also be used for separation. During induction heating for example, to prevent overheating of an object beyond a critical temperature T_{cr}, the alloy could be selected with Curie temperature equal to T_{cr}. At a temperature T_{cr}, from ferromagnetic (temperatures $T < T_{cr}$), the material will become diamagnetic (temperatures $T > T_{cr}$).

Because the magnetic properties of the material change at $T = T_{cr}$, induction heating of the material beyond $T = T_{cr}$ is no longer possible therefore overheating is not possible.

Separation based on evaporation has been used to protect the control equipment in rockets from overheating. Rockets are placed in a foam shell which evaporates after the rocket launching.

5. Separation of functions, properties or behaviour for distinct components or parts

This is an important type of deterministic separation that can be implemented through the following basic mechanisms and techniques.

5.1 Separation of functions to maximize reliability

Separation of functions consists of assigning different functions to different parts of a component or system. Separating critical functions among different parts/components improves reliability and reduces risk through several distinct mechanisms.

(i) ***Separating functions to different parts makes it easy to optimise the separate parts so that maximum reliability is achieved.*** A single component is difficult to optimise for each function. A seal, for example, carries two basic functions: sealing - isolating particular fluids and load-carrying function - resisting tensile loads or bending moments. In designing a joint, the load-carrying function cannot be assigned to the part carrying the sealing function. The reliability of the joint will be low if a single seal is required to carry the two basic functions. A common design error that has caused high-impact failures is combining the critical functions of load carrying and sealing in the design of a joint. Such was the case with the space shuttle *Challenger* booster's O-ring, which was simultaneously sealing the section of the assembly and taking the pressure of combustion (Ullman, 2003). Achieving high reliability requires separating the sealing function and the load-carrying function to distinct parts. Each of the distinct parts can be optimised for the respective function and the result is a highly reliable joint assembly.

Consider also a highly pressurized container containing corrosive fluid. It is difficult to optimise the material of the container so that high levels of strength and corrosion resistance are attained simultaneously. Low-carbon steels, for example, have high strength and low cost but their corrosion resistance in contact with the corrosive fluid is low. Conversely, plastics

have a high corrosion resistance in contact with the fluid but possess low strength. What is difficult to achieve by a single component, can be achieved by separating the functions strength and corrosion resistance into two distinct components: a steel container providing the required strength under pressure and corrosion-resistant plastic lining providing the corrosion resistance.

(ii) ***Separating functions to reduce load magnitudes***. This separation mechanism works by separating the load into several components instead of being carried by a single component. A component performing many functions is over-loaded and its strength can be easily exceeded if combined multiple demands are present. The increased resultant load increases the rate of degradation for the component. By separating the load into several components, the load on a single component is reduced.

For example, a single bearing carrying both high-magnitude radial and high-magnitude axial forces is often overloaded. Because of the high-magnitude resultant load, the rate of degradation of the bearing is elevated and its reliability is low.

By separating the functions of carrying radial and axial loads into two bearings, the load is effectively split between: a roller bearing resisting only radial loads and no axial loads and a ball bearing resisting only axial loads and no radial load. The load on each of the two bearing is reduced, the degradation rate is reduced and the reliability is increased.

(iii) Separation of a single function into multiple components

This separation mechanism is particularly relevant to separation involving a single function assigned to several identical function carriers. Separation of identical functions decreases the vulnerability of components to a single failure. Suppose that a particular function has been assigned to a component. Failure of the component will then cause a loss of the function. If the function is assigned to several identical components such that each component performs the same function, a loss of the component will not entail a loss of the function. Furthermore, the separation also relieves the stress on the overloaded component.

The traditional method of improving reliability by implementing redundancy *is effectively a special case of the method of separation* where the same function has been separated into identical components carrying the same function.

Separation of a single function of a main component to be carried by multiple smaller parts into which the main component is divided, is the essence of *the method of segmentation*, discussed in detail in (Todinov, 2017). Segmentation increases the tolerance of components to flaws causing local damage, reduces the rate of damage accumulation and damage escalation and reduces the hazard potential. Segmentation essentially replaces a sudden failure on a macro-level with gradual deterioration of the system on a micro-level through non-critical failures. Segmentation can even reduce the likelihood of a loss from opportunity bets and the likelihood of erroneous conclusion from imperfect tests (Todinov, 2017).

As a result, the method of segmentation can be considered to be a special case of the method of separation.

(iv) Separation of functions for a mutual compensation of deficiencies

The separation of functions also works through the mechanism of mutual compensation of deficiencies associated with the different components building a system. A typical example is the hybrid joint, combining an adhesive joint and mechanical fixing. There is a clear separation of functions: the adhesive part reduces the stress concentration along the joint

while the mechanical fixing increases the peel resistance of the adhesive joint and its stiffness.
Such a separation is often present in the design of complex alloys where some of the microstructural constituents provide wear resistance, while other constituents provide toughness (resistance to crack propagation).

(v) Separation of functions to prevent unwanted interactions

This separation mechanism (also known as 'separation of concerns') is well-known in the design of computer programs (Reade, 1989). A concern is a relatively simple, self-contained task, addressed by a programme section. Separation of functions in programming is achieved by encapsulating data and statements inside a section of code that has a well-defined interface. This results into a modular programme, consisting of procedures and functions. The encapsulation means that the variables defined into the encapsulated module (procedure or a function) remain only visible within the module and can be altered only within the module. Encapsulation avoids unwanted interactions between different pieces of code in the same programme. Avoiding unwanted interactions avoids the possibility of side effects and difficult to rectify bugs if a variable from one particular section of code is altered from another section of code. Furthermore, the encapsulated sections of code can be updated and tested independently, without having to alter code in the rest of the sections, which significantly decreases the possibility of introducing bugs. The encapsulated piece of code is essentially a black box with specified input and output, whose content can be independently developed and replaced without affecting the logic of the programme.

(vi) Separation of functions to improve the reliability of an estimated value

Separation of functions can even be applied to improve the reliability of an estimated value. Suppose that a probability value has been estimated from a theoretical expression. The reliability of the estimated value can be increased if the function related to estimating the particular value is separated into two or more fundamentally distinct methods. If the calculated values from the separate methods agree, not only is the confidence in the reliability of the estimated value very high, the validity of each alternative estimation method is also confirmed.
An application example can be given with equation (4) regarding the probability of no overlapping of a fixed number of random events, with different durations, on a time interval. This equation has been derived by a probabilistic argument. The probability of no overlapping of a fixed number of random events, with different durations, on a time interval has also been evaluated by a Monte Carlo simulation. Both methods yield the same result which not only confirms the validity of equation (4) but also the validity of the Monte Carlo simulation algorithm.

(vii) Separation of information

This separation mechanism prevents users from becoming overloaded, confused and disoriented with too much information, which is a commons source of costly human errors.
To mitigate the risk of human errors induced by information complexity and overload, information present in machine-human interfaces is separated into layers and only the layer of immediate relevance to the task at hand is displayed.
A common error in design of machine-human interfaces is to present to the user all available options which leads to cognitive overload and human errors. With the use of the mechanism

of information separation, the interface is designed in such a way that users who do not need particular options, never see them.

(viii) Separation of duties to reduce the risk of errors and fraud

The essence of this separation mechanism is the division of a particular key task, subject to abuse into sub-tasks assigned to different individuals.
Separation of duties among different individuals in an organization enforces accountability, eliminates conflicts of interest and errors. The result is a significantly reduced risk. Not properly following the separation of duties often entails disastrous consequences.
Thus, a person with a duty of providing a security system cannot design the security system and also test it. The separation of duties in this case, avoids the conflict of interest where a person has to report on the weaknesses of his own creation. This principle is also followed widely in the delivery of software which combines designing the software and testing it. To avoid costly bugs, the task of designing the software must be separated from the task of testing the software.
Separation of duties in handling financial transactions (e.g. authorizing the transaction, receiving the funds, depositing the funds, recording the transaction, reconciling the bank statement) reduces the possibility of fraud. No single individual has the ability to both perpetrate and conceal fraud because, due to the separation of duties, committing fraud would require the collusion between several people.
Sales transactions include conducting a sale and managing the customer delivery. Separating the duty related to conducting the sale from the duty of managing the customer delivery prevents the risk of falsifying sales records to non-existing customers and stealing funds from the company.

5.2 Separation of reliability across components according to their cost of failure

A very important separation mechanism for reducing risk is that the *allocation of reliability across components should be proportional to their cost of failure*. Components whose failure is associated with large cost of failure should have a proportionally high built-in relioability. This is the underlying principle of the risk-based design (Todinov, 2007). Components, processes and operations used in safety-critical applications should be with higher reliability compared to analogous components used in non-critical systems.

Failure of the cement used for sealing an oil production subsea well for example, causes a catastrophic pollution of the environment. Consequently, the cement seal should have a proportionately high built-in reliability. Because of the extremely high cost of failure, the reliability of the seal in a production well cannot be similar to the reliability of other cement seals not associated with such a high cost of failure. It must be significantly higher so that the probability of failure is significantly reduced which leads to a proportional reduction of the expected potential loss. Separation of reliability based on the cost of failure is therefore an important mechanism of reducing risk.

This principle can be illustrated with a production system with hierarchy (Figure 10).
In the production system from Figure 10, there are six sources of production (generators, oil and gas wells, pumps, etc.) supplying commodity (electricity, oil, gas, water) to a destination *t*. Despite that components C2 and C3 may be identical, failure of component C3 causes loss of production from source S6 only while the failure of component C2 causes loss of production from five sources (S1-S5). The reliability level of component C2 should be significantly higher than the reliability level of component C3.

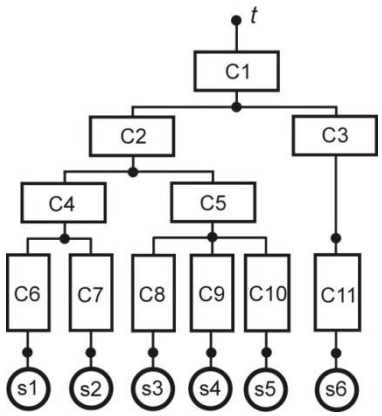

Figure 10. A production system with hierarchy based on six production sourcess.

The higher the component in the hierarchy, the more production units will be affected by its failure, the larger the reliability level for this component should be.

The separation of reliability according to the cost of failure has also a direct application in distributing a fixed budget for improving the reliability of components in order to achieve a maximum overall risk reduction. Distributing the investment uniformly (homogeneously) across all components is, as a rule, an inferior strategy. To achieve a maximum risk reduction, the available risk reduction budget should be preferentially distributed to improve the reliability of components whose failure is associated with the largest consequences and for which a unit investment yields the maximum risk reduction. A special dynamic programming algorithm recognising the intrinsic value of the available budget has been developed for this purpose in (Todinov, 2016).

5.3 Separation to counter poor performance caused by homogeneity

5.3.1 Separation of strength across components and zones according to the experienced stresses

The mechanism of separation countering the drawbacks of homogeneity is necessary in cases where the average property characterising a homogeneous state cannot provide the required reliability in terms of effective resistance against combined hazards or damage accumulation factors. This mechanism is needed in engineering design, for assuring that the different parts of a component have the appropriate properties needed to successfully resist the local loading. A homogeneous material with average value of the strength (resistance) is not optimised for any local type of loading and cannot provide sufficient resistance in all parts of the component. If the type of loading at a particular location is a cyclic loading with large amplitude, the required response from the material is high fatigue resistance. If the type of loading at a particular location is static loading and no corrosion is present, there is no need for a high fatigue resistance because the conditions responsible for the development and propagation of fatigue cracks are missing. Since the type of loading, is not homogeneous, the resistance also cannot be homogeneous.

The mechanism for implementing this type of separation requires assuring uneven distribution of the resistance against a particular stress for different components or different parts of the same component depending on the type and intensity of the local stress the component/zone experiences.

The application of this separation mechanism is illustrated with the real-life application in Fig.11. The container 1 and the cylindrical hinges 2 in Fig 11a are made of the same material, with relatively low fatigue resistance. An asymmetric lid (not shown) is rotating around the hinges 2 and loads the hinges with the pulsating force *F*. Because of the pulsating load and the small fatigue resistance of the material of the container, cracks appear at the base of the hinges and soon one of the hinges fails. Applying the mechanism of separation according to the experienced local stress, the material of the hinges must have a significantly larger fatigue resistance compared to the rest of the container. If the hinges are made of material with high fatigue resistance and inserted in the wall (as shown in Fig.11b), the fatigue resistance and the reliability of the container are increased significantly.

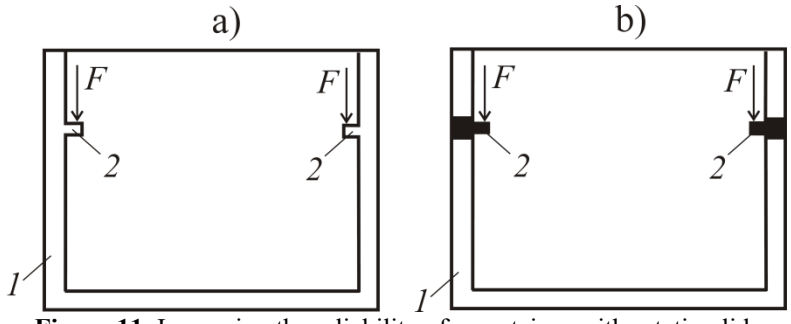

Figure 11. Improving the reliability of a container with rotating lid.

5.3.2 Separation of properties can also be used to create a component/system which, in order to be reliable, must satisfy conflicting requirements.

For example, a gear must be hard, to endure large contact stresses and intensive wear and soft, to endure impacts. These conflicting requirements require conflicting material properties: the surface of the gear must be hard while the core of the gear must be soft. In a compromise, with no separation of properties, a homogeneous material will be selected which has a satisfactory hardness to resist wear and satisfactory toughness to resist shock loading. The result is a mediocre solution which is neither optimised against wear nor against shock loading. These contradicting requirements can be simultaneously guaranteed if a separation of properties is implemented. These conflicting properties can be guaranteed by the separation of properties achieved through *case hardening* (Kalpakjian and Schmid, 2001). This consists of a local induction heating of the surface layers followed by quenching. Case hardening improves the resistance of the surface to large contact stresses and wear, while leaving the core tough which makes it resist impact loads.

5.4 Separation in geometry

Separation in geometry is present when different parts of an object or assembly have different geometry to provide optimal conditions maximizing reliability and minimizing the risk of failure. An example of separation in geometry can be given with the tapered cantilever beam in (Fig.12a). The beam can be designed to improve its load resistance for the same volume of material by tapering. The beam is made thicker at the cantilevered end where the stresses are the largest and with the smallest thickness at the free end where the stresses are the smallest.

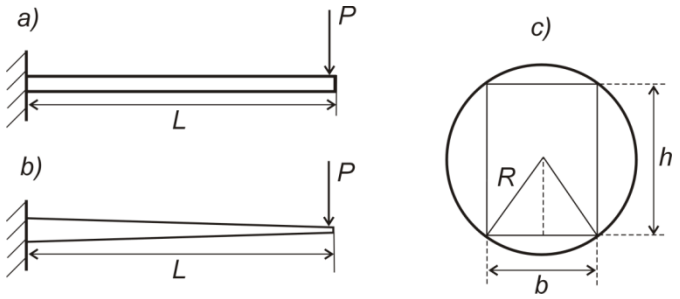

Figure 12. a,b) Separation in geometry to improve the load-carrying capacity of a cantilever beam, c) Separation in geometry to maximize the load-carrying capacity of a beam which requires building a mathematical model based on the method of separation.

In many cases, the separation in geometry can be done efficiently only after building and analysing a model based on separation. Such a case is presented in Fig.10c which features a rectangular beam cut out of a cylindrical log of radius *R=0.2m*. It is required to determine the dimensions *b* and *h* of the beam such that the beam carries the maximum possible load without failure during bending. The maximum load-carrying capacity of the beam during bending is proportional to the second moment of area $I = bh^3/12$. The larger the second moment of area the larger the load-carrying capacity of the beam.

The design parameters are the dimensions of the beam *b* and *h*. Between them there is a geometrical constraint expressed by the analytical relationship $(b/2)^2 + (h/2)^2 = R^2$, from which the design parameter *b* can be eliminated by expressing it as a function of the other design parameter *h*: $b = \sqrt{4R^2 - h^2}$. The second moment of area can now be presented as a function of a single design parameter:

$$I = \frac{1}{12} h^3 \sqrt{4R^2 - h^2} \tag{23}$$

where *h* varies in the interval $0 \le h \le 2R$.

The separation in geometry of the beam could proceed towards making the beam wider (increasing b) and shorter (decreasing h) or making the beam slender (decreasing *b* and increasing *h*). It is impossible to guess the right level of separation which delivers the largest strength.

To maximise the load-carrying capacity of the beam, the second moment of area *I* from equation (23) needs to be maximised while complying with the existing constraint $0 \le h \le 2R$.

At the end points of the interval $0 \le h \le 2R$, $I = 0$. Maximising the objective function is done in the standard way by taking the first derivative and equating it to zero. There are no points from the interval $0 \le h < 2R$ where the first derivative is not defined, therefore the local maximum will also be a global maximum. It is thus obtained that the stationary point $h = \sqrt{3}R = 0.3464$ m corresponds to the local and the global maximum of the second moment of area in the interval $0 \le h \le 2R$. The corresponding value for the parameter *b* is 0.2m. The beam with the largest load carrying capacity that can be cut from the log is with dimensions 0.2mx0.35m.

This example also demonstrates that to derive maximum risk-reduction benefit from the method of separation, in a number of cases, it is required to build and analyse a mathematical model or algorithm based on the method of separation.

A limitation of the introduced analytical model of stochastic separation is that it is applicable to a single source servicing the demands. An important continuation of future research would be to extend the presented analytical model to a case of multiple sources

servicing random demands on a time interval. Another important continuation would be a stochastic separation based on the expected overlapped time fraction by the random events.
A classification of the discussed methods of stochastic and deterministic separation is given in Fig.13.

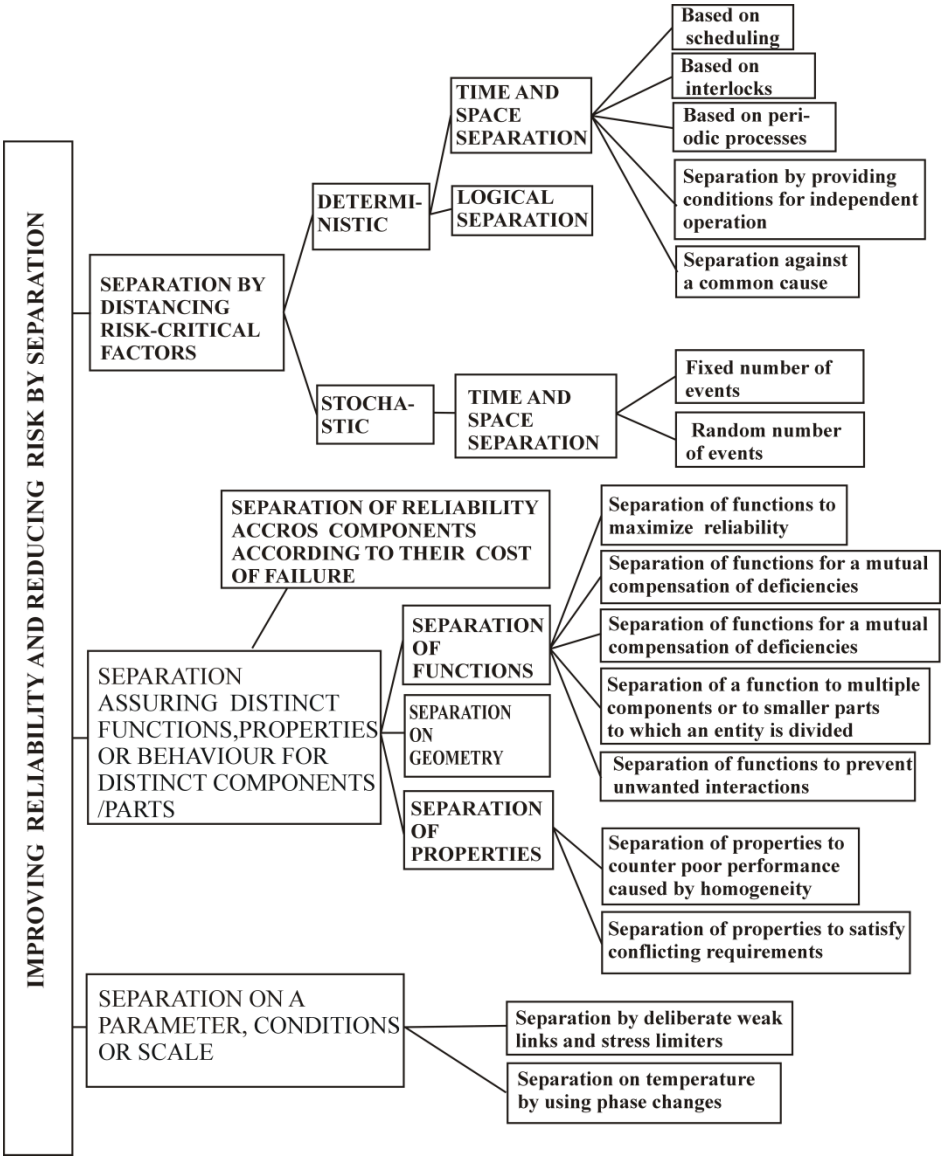

Figure 13. Classification of the discussed methods of stochastic and deterministic separation.

CONCLUSIONS

1. Various mechanisms through which the method of separation works in improving reliability and reducing risk have been introduced for the first time. A comprehensive classification of the discussed methods of stochastic and deterministic separation has also been presented.

2. The fundamental concept ‘stochastic separation of random events based on the probability of overlapping’ has been introduced for the first time.

3. Efficient methods for providing stochastic separation by reducing the duration times of overlapping critical random events on a time interval have been presented for the first time.

4. The probability of overlapping of critical events, randomly appearing on a time interval, is practically insensitive to the distribution of their durations.

5. The probability of overlapping of risk-critical events, randomly appearing on a time interval, is practically insensitive to the variance of their duration times as long as the mean remains the same. A rigorous proof has been presented that even for two random events on a time interval, if their duration fractions are small, the probability of overlapping will be practically insensitive to the variance of their duration times.

6. The independence of the probability of overlapping on the variance of the event durations provides the valuable opportunity to work with duration times characterised by their means only and not requiring data related to the variance of the duration times.

7. In a number of cases the only way to extract benefit from the method of separation, in a number of cases, it is required to build and analyse a mathematical model or algorithm based on the method of separation.

8. It is demonstrated improving reliability by including redundancy, improving reliability by a segmentation and some of the deliberate weak link techniques and stress limiters techniques for reducing risk are effectively special cases of a deterministic separation.

9. Separation on a parameter is an efficient technique for reducing risk. The separation on properties is an efficient technique for compensating the drawbacks associated with a selection based on homogeneous properties.

10. The logical separation based on the mechanism of the shared key is an efficient and low-cost separation risk reduction technique.

11. The method of separation transcends applications in mechanical engineering and is also efficient in software engineering, financial control, management and design of human-machine interfaces.

REFERENCES

Altshuller G.S. Creativity as an exact science: The theory of the solution of inventive problems, Gordon and Breach Science Publishing: New York, 1984.

Altshuller G.S. The innovation algorithm, TRIZ, systematic innovation and technical creativity, Technical Innovation Center, Inc.: Worcester, 2007.

Altshuller G.S. And suddenly the inventor appeared, TRIZ, the theory of inventive problem solving, Translation from Russian by Lev Shulyak, Technical Innovation Center, Worcester, MA, 1996.

Billinton, R., Allan, R. N. Reliability evaluation of engineering systems (2nd ed.), Plenum press, 1992.

Carter A.D.S., *Mechanical Reliability*, Macmillan Education Ltd., (1986).

Carter A.D.S., *Mechanical reliability and design*, Macmillan Press Ltd, (1997).

Eder W.E., S.Hosnedl. Design Engineering, CRC Press, 2008.

Everitt B.S. and D.J. Hand. Finite mixture distributions, Chapman and Hall, London 1981.

Gadd K. TRIZ for engineers: Enabling inventive problem solving, Wiley, 2011.

Hollangel E. Barriers and accident prevention, Routlege, 2016.

Kalpakjian S., S.Schmid. Manufacturing engineering and technology 4th ed., Prentice Hall, 2001.

Knowles I. Is it time for a new approach?. IEEE Transactions on Reliability 1993; 42(1): 2-3.

Leveson N. Engineering a safer world: systems thinking applied to safety, The MIT Press: Cambridge, Massachusetts, 2011.
Orloff M.A. Inventive thinking through TRIZ, A practical guide, 2nd ed., Springer, 2006.

Orloff M.A. Modern TRIZ A Practical Course with EASyTRIZ Technology, A practical guide, 2nd ed., Springer, 2012.

Pahl G., W. Beitz, J. Feldhusen and K.H. Grote, *Engineering design*, Springer, Berlin (2007).

Pecht M., A.Dasgupta, D.Barker, C.T.Leonard. The reliability physics approach to failure prediction modelling, Quality and Reliability Engineering International 1990, September/October (4): 267-273.

Pecht M. Why The Traditional Reliability Prediction Models Do Not Work - Is There An Alternative. Electronic Cooling 1996; 2(1): 10-12.

Rantanen K., E.Domb. Simplified TRIZ, 2nd edition, Auerbach Publications, 2008.

Reade, C. Elements of Functional Programming. Addison-Wesley Longman: Boston, MA, 1989.

Ross S., Simulation 2nd edition, Harcourt academic press, 1997.

Rosenthal J.S., 2006, *A first look at rigorous probability theory*, 2nd ed., World Scientific Publishing Co. Pte. Ltd.

Savransky S.D. Introduction to TRIZ methodology of inventive problem solving, CRC press LLC, 2000.

Svenson, O. The accident evolution and barrier function (AEB) model applied to incident analysis in the processing industries. Risk Analysis 1991; 11(3): 499-507.

Sundararajan C. (Raj). Guide to reliability engineering: Data analysis, applications, implementations and management, Van Nostrand Reinhold: New York, 1991.

Terninko J., A.Zusman, B.Zlotin. Systematic Innovation: An introduction to TRIZ, CRC Press LLC, 1998.

Todinov M.T., Risk-based reliability analysis and generic principles for risk reduction, Elsevier, 2007.

Todinov M.T. Reducing risk through segmentation, permutations, time and space exposure, inverse states, and separation, *International Journal of Risk and Contingency Management* 2015, 4(3):1-21.

Todinov M.T., Reducing risk by segmentation*, International Journal of Risk and contingency Management*, 6(3) pp.27-46, 2017.

Todinov M.T. A new reliability measure based on specified minimum distances before the locations of random variables in a finite interval, Reliability Engineering and System Safety 2004, 86: 95-103.

Todinov M.T. Distribution mixtures from sampling of inhomogeneous microstructures: Variance and probability bounds of the properties, Nuclear Engineering and Design 2002; 214: 195–204.

Ullman D.G. The Mechanical Design Process, 3rd ed., McGraw Hill, 2003.

Tunno D., Larsen S., Retrofittable cable mechanical fuse, US patent US20110027007 A1, 2011.