On the use of analytical inequalities for improving reliability and reducing risk

Michael Todinov
Oxford Brookes University
School of Engineering, Computing and Mathematics
Oxford, Wheatley, OX33 1HX, UK
mtodinov@brookes.ac.uk

Abstract – The paper demonstrates for the first time a new domain-independent method for improving reliability and reducing risk based on two fundamental approaches of using algebraic inequalities: the forward approach, based on deriving algebraic inequalities from real systems and processes and the inverse approach, based on deriving new knowledge by meaningful interpretation of existing correct algebraic inequalities. The forward approach has been used to prove the domain-independent principle of the well-ordered systems which are characterised by the smallest possible risk of failure. In this respect, the paper answers an important question for a parallel-series system about the components that need to be subjected to condition monitoring so that the reliability of the system is maximised.
The forward approach has also been used for optimal assignment of manufacturers to products with the purpose of minimising the overall percentage of defective products.

The inverse approach has been used to generate new knowledge related to the relationship of the equivalent elastic constants of elements arranged in series and parallel and the upper and lower bounds of the percentage of faulty components in a batch of components obtained from pooling batches of components with unknown sizes.

The paper also demonstrates the principle of non-contradiction: if the variables and the different parts of a correct abstract inequality can be interpreted as a system or process, in the real world, the system or process must exhibit properties that are consistent with the abstract inequality.

Keywords: analytical inequality; meaningful interpretation; forward approach; inverse approach; principle of non-contradiction; reliability; risk; reliability improvement; risk reduction

1. Introduction

While reliability and risk assessment are truly domain-independent areas, this cannot be stated about the equally important areas of reliability improvement and risk reduction. For decades, the reliability and risk science failed to appreciate and emphasize that reliability improvement, risk and uncertainty reduction are underpinned by general principles that work in many unrelated domains.

As a consequence, *methods for measuring and assessing reliability, risk and uncertainty were developed, not domain-independent methods for improving reliability, reducing risk and uncertainty which could provide a direct input to the design process*. Indeed, in standard textbooks on mechanical engineering and design of machine components (Collins, 2003; Norton, 2006; Pahl, 2007; Childs, 2014; Budynas, 2015; Mott et al, 2018; Gullo and Dixon, 2018), for example, there is no mention of generic (domain-independent) methods for reliability improvement and risk and uncertainty reduction.

The problem is that the current approach to reliability improvement and risk reduction almost solely relies on knowledge from a specific domain and is conducted exclusively by experts in that domain. This creates the incorrect perception that effective risk reduction can be delivered solely by using methods offered by the specific domain, without resorting to a general risk reduction methods and principles.

This incorrect perception resulted in ineffective reliability improvement and risk reduction across the entire industry, the loss of valuable opportunities for reducing risk and repeated "reinvention of the wheel". Current technology changes so fast that the domain-specific knowledge related to reliability improvement and risk reduction is outdated almost as soon as it is generated. In contrast, the domain-independent methods for reliability improvement, risk and uncertainty reduction are higher-order methods that permit application in new, constantly changing situations and circumstances.

To fill a gap in the domain-independent methods for risk reduction, the paper contributes a new domain-independent method for improving reliability and reducing risk, based on algebraic inequalities.

There are a number of useful analytic inequalities such as the Arithmetic mean – Geometric mean (AM-GM) inequality, Cauchy-Schwartz inequality, the rearrangement inequality, the Chebyshev's inequality, Jensen's inequality, etc. Analytic inequalities have been discussed extensively in (Steele, 2004; Cloud et al. 1998; Engel 1998; Hardy et al.,

1999; Kazarinoff, 1961; Pachpatte 2005; Sedrakyan and Sedrakyan 2010). A comprehensive overview of the use of inequalities in mathematics has been presented in (Fink, 2000).

In probability theory (De Groot, 1989; Miller and Miller, 1999), well-known inequalities are the Tchebyshev's inequality, Markov's inequality, Boole's inequality, Bonferroni inequalities and Jensen's inequality. Some of these inequalities have been used in reliability theory to provide bounds on operational characteristics and system reliability calculated by using cut sets (Barlow and Proshan, 1965,1975; Ramakumar, 1993; Hoyland and Rausand 1994).

Applications of some of these inequalities have been considered in physics (Rastegin, 2012) and engineering (Cloud et al. 1998).

In engineering design, design inequalities have been used to express design constraints for a long time to guarantee that the design will perform its required function (Samuel and Weir, 2004). This paper shows however, that the use of algebraic inequalities in engineering is far reaching and is not restricted to specifying design constraints.

A formidable advantage of algebraic inequalities is that they *do not require knowledge related to the distributions of the variables entering the inequalities*. This makes a method based on algebraic inequalities ideal for handling deep uncertainty associated with components, properties and control parameters.

Despite the existing comprehensive introductions to analytic inequalities and the presence of applications in physics and engineering, there is a profound lack of discussion related to the applications of analytic inequalities to improve reliability and reduce risk.

There are two principal approaches of using algebraic inequalities for improving reliability and reducing risk: (i) *a forward approach*, consisting of deriving an abstract algebraic inequality from a real physical system or process which is subsequently tested and proved rigorously and (ii) *an inverse approach*, consisting of interpreting a correct abstract inequality and inferring from it unknown new properties related to a real physical system or process.

The forward approach of using algebraic inequalities for improving reliability and reducing risk is to start with the system or process, conjecture an inequality about the performance of competing alternatives and prove the conjectured inequality rigorously.

This process includes several basic steps (i) analysis of the system or process, (ii) conjecturing inequalities ranking the competing alternatives, (iii) testing the conjectured inequalities and (iv) proving the conjectured inequalities rigorously.

By following this approach, inequalities can be used to *rank reliabilities of systems with unknown reliabilities of their components.* This forward approach of exploiting algebraic inequalities has been demonstrated in (Todinov, 2016) by comparing systems with unknown reliabilities of their components. The generic strategy starts with building the functional diagram of the system, creating the reliability network for the system, deriving expressions for the system reliability of the competing alternatives, conjecturing inequalities involving the competing alternatives and finishing with a rigorous proof by using some combination of analytical techniques for proving inequalities.

In this paper, the forward approach will be applied for determining a tight upper bound for the risk of a faulty assembly and for maximising the reliability of parallel-series systems.

The inverse approach is based on the observation that useful quantitative knowledge is locked in abstract inequalities that be released by their meaningful interpretation. Furthermore, depending on the specific interpretation, knowledge, applicable to different systems from different domains can be released from the same inequality. In this sense, the inverse approach does not require or imply any forward analysis of pre-existing systems or processes. The systems or processes to which the inequality applies are solely a result of the meaningful interpretation of the variables in the inequality and its parts.

The key step of the inverse approach is creating, relevant meaning for the variables entering a correct algebraic inequality, followed by a meaningful interpretation of the different parts of the inequality

This inverse approach effectively links existing correct abstract algebraic inequalities with real physical systems or processes and not only opens opportunities for enhanced performance of systems and processes but also leads to the discovery of new fundamental properties of the systems and processes.

The inverse approach always leads to new knowledge as long as a meaningful interpretation of the algebraic inequality is provided. This is because the inverse approach is firmly rooted in the principle of non-contradiction: if the variables and the different parts of a correct abstract inequality can be interpreted as a system or process, in the real world, the system or process exhibit properties that are consistent with the abstract inequality.

In other words, the realization of the process/experiment yields results that do not contradict the algebraic inequality.

2. Equivalent elastic constants of springs in series and parallel

This example demonstrates obtaining new knowledge from the meaningful interpretation of a correct algebraic inequality, which is the essence of the inverse approach in using algebraic inequalities.

Consider the abstract inequality

$$(k_1 + k_2 + ... + k_n)\left(\frac{1}{k_1} + \frac{1}{k_2} + ... + \frac{1}{k_n}\right) \geq n^2 \tag{1}$$

where $k_i > 0$, $i = 1,...,n$ are positive real numbers and *n* is an integer number.

This inequality is correct and can be proved by expanding the left hand side of (1) which gives n^2 terms of the form k_i / k_j, $1 \leq i, j \leq n$. From these n^2 terms, *n* terms will be of the type $i = j$ and $k_i / k_j = 1$. The rest of the $n^2 - n$ terms can be paired in the sums $\frac{k_i}{k_j} + \frac{k_j}{k_i}$.

For any two numbers k_i and k_j

$$\frac{k_i}{k_j} + \frac{k_j}{k_i} \geq 2 \tag{2}$$

is fulfilled and this follows from the standard AM-GM inequality (Kazarinoff, 1961; Steele, 2004):

$$k_i + k_j \geq 2\sqrt{k_i k_j} \tag{3}$$

which follows directly from the inequality $(\sqrt{k_i} - \sqrt{k_j})^2 \geq 0$.

Indeed, squaring both sides of inequality (3) (which are non-negative numbers) and dividing by the positive number $k_i k_j$ yields inequality (2).

According to what was proved earlier, for each of the paired sums, $\frac{k_i}{k_j} + \frac{k_j}{k_i} \geq 2$ holds. The number of these sums is $(n^2 - n)/2$ and the left-hand side of inequality (1) becomes

$$(k_1 + k_2 + ... + k_n)\left(\frac{1}{k_1} + \frac{1}{k_2} + ... + \frac{1}{k_n}\right) \geq n + \frac{n^2 - n}{2} \times 2 = n^2$$

This completes the proof of inequality (1).

Now, a meaningful interpretation can be provided to inequality (1) if k_1, k_2,…, k_n stand for the stiffness values of *n* elastic elements (springs). The equivalent stiffness of springs in series is given by the well-known relationship (Samuel and Weir, 2004):

$$k_s = \frac{1}{1/k_1 + 1/k_2 + ... + 1/k_n} \tag{4}$$

For springs connected in parallel, the equivalent stiffness is

$$k_p = k_1 + k_2 + ... + k_n \tag{5}$$

Inequality (1) effectively states that the ratio k_p / k_s of the equivalent spring constant k_p of springs connected in parallel and the equivalent spring constant k_s of springs connected in series never falls below n^2 ($k_p / k_s \geq n^2$) irrespective of the individual stiffness values k_i, $i = 1,...,n$. Or, equivalently, the equivalent spring constant k_s of springs connected in series is at least n^2 times smaller than the equivalent spring constant of the springs connected in parallel, irrespective of the stiffness values k_i, $i = 1,...,n$ of the individual springs:

$$k_s \leq k_p / n^2 \tag{6}$$

The upper bound $k_s \leq k_p / n^2$ is tight and equality is attained if all stiffness values are equal $k_1 = k_2 = ... = k_n = k$.

This is an example of generating new knowledge from the meaningful interpretation of an algebraic inequality.

An application of this result can be found in the robust design of clamping devices, which often require a small variation of the spring force with the spring length.

A constant clamping force *P* can be provided by springs arranged in parallel, with a large equivalent spring constant k_1 and initial deflection x_1 ($P = k_1 x_1$) or by springs arranged in series, with a smaller equivalent spring constant $k_2 < k_1$ and larger initial deflection $x_2 > x_1$ (Figure 1). The initial spring deflection is always associated with errors (errors in cutting the springs to exact length, imperfections associated with machining the ends of the spring coil, sagging of the spring with time due to stress relaxation, variations in the length of the springs associated with the pre-setting operation, etc.).

As it can be verified from Figure 1, for the springs connected in series (with equivalent spring constant k_2), variations of magnitude Δx in the spring deflection cause much smaller variations ΔP_2 in the clamping force compared to the variations ΔP_1 in the clamping force of the stiffer springs in parallel, caused by the same variations Δx of the spring deflection. Selecting springs arranged in series results in a robust design, for which the clamping force *P* is not very sensitive to variations in the spring deflection.

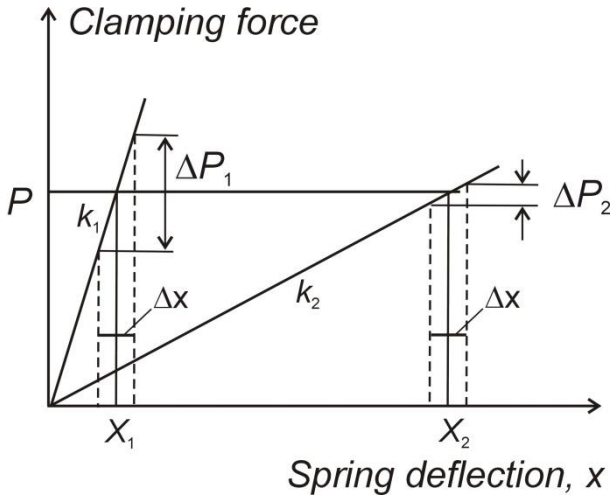

Figure 1. Clamping force variation for springs connected in parallel and for springs connected in series.

Another application of the formulated relationship can be found in the significant increase of the energy-absorbing potential of assemblies upon impact. By arranging the elastic elements in series rather than parallel, the n^2 times smaller equivalent stiffness k_s in series compared to the stiffness k_p in parallel will reduce significantly the maximum stress upon impact and with this, the risk of overstress failure will also be significantly reduced.

It is important to note that the relationship between equivalent properties of elements connected in series and parallel is not the only meaningful interpretation of inequality (1). New knowledge related to equivalent properties from various application domains can be extracted if k_1, $k_2,\ldots,k_n$ stand for electric resistance of elements arranged in series and parallel, if k_1, $k_2,\ldots,k_n$ stand for thermal resistances of elements in series and parallel and finally, if k_1, $k_2,\ldots,k_n$ stand for capacitances of capacitors arranged in parallel and series.

As a result, by using the inverse approach new knowledge related to different application domains is extracted from the same algebraic inequality.

3. Determining tight lower and upper bound for the risk of a faulty component by a meaningful interpretation of algebraic inequalities

Consider the set of ordered positive fractions $0 \le p_1 \le p_2 \le ... \le p_m \le 1$. If the fractions p_i are presented as a ratio $p_i = a_i / n_i$ of two integer numbers a_i and n_i, the following algebraic inequality holds:

$$\frac{a_1}{n_1} \le \frac{a_1 + a_2 + ... + a_m}{n_1 + n_2 + ... + n_m} \le \frac{a_m}{n_m} \tag{7}$$

where $a_1 / n_1 \le a_2 / n_2 \le ... \le a_m / n_m$.

Inequalities (7) can be proved by a mathematical induction. For the trivial case $n = 2$, it can be shown that if $0 \le p_1 \le p_2 \le 1$, $p_1 = a_1 / n_1$ and $p_2 = a_2 / n_2$ then

$$\frac{a_1}{n_1} \le \frac{a_1 + a_2}{n_1 + n_2} \le \frac{a_2}{n_2} \tag{8}$$

Indeed, from $p_1 \le p_2$ it follows that $a_1 / n_1 \le a_2 / n_2$ which is equivalent to

$$a_1 n_2 \le a_2 n_1 \tag{9}$$

Adding the quantity $a_1 n_1$ to both sides of inequality (9) results in $a_1 n_2 + a_1 n_1 \le a_2 n_1 + a_1 n_1$ which, after factoring a_1 from the left side and n_1 from the right side results in

$$a_1 (n_1 + n_2) \le n_1 (a_1 + a_2) \tag{10}$$

Dividing both sides of inequality (10) by the positive value $n_1 (n_1 + n_2)$ does not alter the direction of the inequality. The result is the inequality

$$p_1 = \frac{a_1}{n_1} \le \frac{a_1 + a_2}{n_1 + n_2} \tag{11}$$

which is the left inequality from inequalities (7), for $n = 2$.

The right inequality from inequalities (7), for $n = 2$, can be proved in a similar fashion.

Suppose now that inequalities (7) hold for the integer *k* where $k \ge 2$, $0 \le p_1 \le p_2 \le ... \le p_k \le 1$, $p_i = x_i / n_i$ (induction hypothesis):

$$\frac{a_1}{n_1} \le \frac{a_1 + a_2 + ... + a_k}{n_1 + n_2 + ... + n_k} \le \frac{a_k}{n_k} \tag{12}$$

Consider again the left inequality

$$\frac{a_1}{n_1} \le \frac{a_1 + a_2 + ... + a_k}{n_1 + n_2 + ... + n_k} \tag{13}$$

Multiplying both sides of inequality (13) by the positive quantity $n_1 (n_1 + n_2 + ... + n_k)$ does not alter its direction and the equivalent inequality

$$a_1 (n_1 + n_2 + ... + n_k) \le n_1 (a_1 + a_2 + ... + a_k) \tag{14}$$

is obtained. Without loss of generality, suppose that for the k+1st term $p_{k+1} = \frac{a_{k+1}}{n_{k+1}}$, the ranking

$$0 \le p_1 \le p_2 \le ... \le p_k \le p_{k+1} \le 1 \tag{15}$$

holds. (If this is not the case, the terms can always be renumbered so that inequality (15) is fulfilled.). Since $p_1 = \frac{a_1}{n_1} \le p_{k+1} = \frac{a_{k+1}}{n_{k+1}}$, it follows that

$$a_1 n_{k+1} \le n_1 a_{k+1} \tag{16}$$

If inequality (14) is added to inequality (16), the inequality

$$a_1(n_1 + n_2 + ... + n_k + n_{k+1}) \le n_1(a_1 + a_2 + ... + a_k + a_{k+1}) \tag{17}$$

is obtained which is equivalent to

$$a_1 / n_1 \le (a_1 + a_2 + ... + a_k + a_{k+1}) / (n_1 + n_2 + ... + n_k + n_{k+1}) \tag{18}$$

With the trivial case, corresponding to $k = 2$ and the proved induction step (18), according to the principle of the mathematical induction, the left inequality (7) holds for any $m > k$.
In a similar fashion, the right inequality (7) can also be proved.

Inequality (7) has a useful interpretation. Suppose that a_i $(i = 1,...,n)$ stands for the number of faulty components in the *i*th batch and n_i $(i = 1,...,n)$ stands for the total number of components in the *i*th batch and $p_i = a_i / n_i$ $(i = 1,...,n)$ stands for the fraction of faulty items in the *i*th batch. The number of components n_i $(i = 1,...,n)$ in the separate batches *is unknown*.

The batch with the smallest fraction of faulty components will be referred to the 'best batch' and the batch with the largest fraction of faulty components will be referred to as the 'worst batch'. Now, a meaningful interpretation of inequality (7) can be provided. The inequality effectively states that if *n* batches with defective components are pooled into a single batch, *irrespective of the number of components* n_i in the separate batches, the percentage of faulty components in the pooled batch is always smaller than the percentage of faulty components in the worst batch and larger than the percentage of faulty components in the best batch.
The fraction of faulty items in the pooled batch always remains within the tight bounds p_1 and p_m:

$$p_1 \le p \le p_m \tag{19}$$

where $p = \dfrac{a_1 + a_2 + ... + a_m}{n_1 + n_2 + ... + n_m}$.

This example demonstrates the use of the inverse approach for determining tight lower and upper bound for the percentage of faulty items in the pooled batch without any knowledge related to the sizes of the pooled batches.

4. Using inequalities for minimising the risk of a faulty assembly

The forward approach in using algebraic inequalities for risk reduction will be illustrated with an example related to minimising the probability of a faulty assembly.

Consider an assembly built with *n* types of components, each coming from a separate manufacturer. Each manufacturer can deliver any type of components, but not more than a single type of component. From past records, the fractions (percentage) of defective components characterising the separate manufacturers are $x_1, x_2, ..., x_n$, respectively. Suppose that the required numbers of components from *n* different types are $a_1, a_2, ..., a_n$, respectively. The question of interest is to determine the optimal allocation of manufacturers and types of components so that the overall percentage of defective components in the total supplied components is minimised.

The number of ways *n* manufacturers can be assigned to *n* types of components is $n!$, equal to the number of different permutations $x_{b1}, x_{b2}, ..., x_{bn}$ of *n* elements where the indices $x_{b1}, x_{b2}, ..., x_{bn}$ stand for a particular permutation of *n* consecutive numbers.

The question then reduces to determining which of the $n!$ sums $a_1x_{b1} + a_2x_{b2} + ... + a_nx_{bn}$ describing the total percentage of faulty components is the smallest. This corresponds to the optimal assignment of manufacturers which delivers the smallest percentage of faulty components.

It can be shown that the sum $a_1x_{b1} + a_2x_{b2} + ... + a_nx_{bn}$ is minimal if the two sequences $a_1, a_2, ... a_n$ and $x_1, x_2, ..., x_n$ are sorted oppositely: one is increasing and the other is decreasing.

In other words, it can be shown that the following algebraic inequality holds

$$a_1x_1 + a_2x_2 + ... + a_nx_n \le a_1x_{b1} + a_2x_{b2} + ... + a_nx_{bn} \qquad (20)$$

where $x_{b1}, x_{b2}, ..., x_{bn}$ are the assigned numbers of components to any permutation of the

manufacturers.

To prove this statement, the extreme principle will be used. Suppose that there is a sum

$$S_0 = a_1x_1 + ... + a_rx_r + ... + a_sx_s + ... + a_nx_n \quad (21)$$

where the sequence $x_1, x_2, ..., x_n$ is not monotonically decreasing and which corresponds to the smallest possible sum S_0. The sum S_0 gives the total number of faulty components from all suppliers.

If the *x*-sequence is not sorted in descending order, there will certainly be values a_r, x_r and a_s, x_s $(r < s)$ for which $x_r < x_s$ is true. If no such pair can be found, then the *x*-sequence is already decreasing.

Suppose that $a_r < a_s$ and $x_r < x_s$ is true. Now, consider the sum S_1

$$S_1 = a_1x_1 + ... + a_rx_s + ... + a_sx_r + ... + a_nx_n \quad (22)$$

which has been obtained from the sum S_0 by switching the positions of x_r and x_s only. Subtracting S_1 from S_0 gives:

$$S_0 - S_1 = a_rx_r + a_sx_s - a_rx_s - a_sx_r = a_r(x_r - x_s) - a_s(x_r - x_s) = (a_r - a_s)(x_r - x_s)$$

Because $a_r < a_s$ and $x_r < x_s$ is true, then $S_0 - S_1 = (a_r - a_s)(b_r - b_s) > 0$. Therefore, the sum S_1 is smaller than the sum S_0, which contradicts the initial assumption that S_0 is the smallest sum. Consequently, the hypothesis that the smallest sum can be attained for sequences one of which is increasing but the other is not necessarily monotonically decreasing is incorrect and this completes the proof.

5. Improving reliability and reducing risk for safety-critical systems by using inequalities

5.1 Improving reliability and reducing risk for parallel-series safety-critical systems

Often the only available information is the ranking of components in terms of their reliability, without being possible to attach any value to their failure frequencies. Such is the case where old and new components of the same type are used in the same system. Because of inevitable component wearout and deterioration, it is usually sensible to assume that the new components are more reliable than the older components.

Consider the system in Figure 2 which transports cooling liquid from three sources s1,s2 and s3 to the chemical reactor *t*.

The cooling system consists of identical pipeline sections (the arrows in Figure 2). Each pipeline section is coupled with a pump for transporting the cooling fluid through the section. Suppose that the pipeline sections and the pumps are old (sections '*a*' in Figure 2) and prone to failure due to corrosion, fatigue, wear, deteriorated seals, etc. The cooling system fulfils its mission if at least one cooling line delivers cooling fluid to the chemical reactor. Suppose, for the sake of simplicity, that all pipeline sections are in the same state of deterioration and each section is characterized by the same reliability 0.4, associated with one year of operation. Because of the deteriorated sections, the cooling system will benefit from risk-reduction, consisting of purchasing and replacing deteriorated pipeline sections with new sections (sections 'b' in Figure 2). Consequently, the replacement of any of the 9 pipeline sections is a possible risk-reduction option. Now suppose that the available budget is sufficient for purchasing and replacing exactly 3 pipeline sections 'b'. Each new pipeline section is characterised by a reliability 0.9, for one year of operation.

Because the pipeline sections work independently from one another and because all of them are identical (Figure 2a), it seems that any three pipeline sections can be replaced with new ones (Figure 2b), with the same effect.

This impression, however, is incorrect. The total removed risk of system failure is highest if the available budget is spent preferentially on replacing pipeline sections forming an entire cooling branch (Figure 2c), as opposed to replacing randomly selected sections inside the system (Figure 2b).

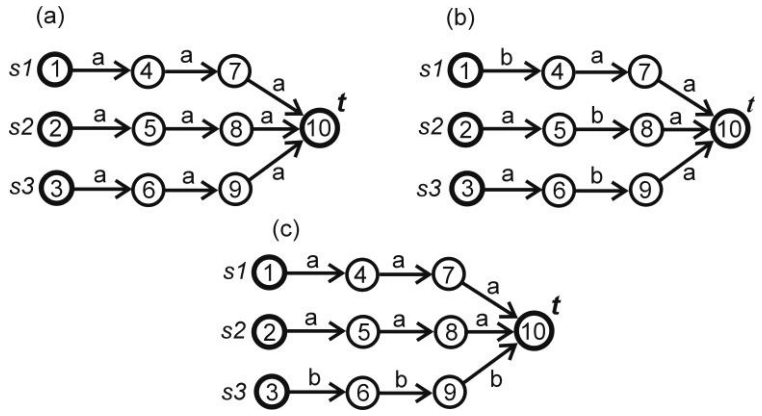

Figure 2. A safety-critical cooling system consisting of three parallel branches

Indeed, the reliability of the parallel-series arrangement in Figure 2b is:

$$R_b = 1-(1-0.4^2 \times 0.9)^3 = 0.37 \tag{23}$$

This is the probability that there will be at least a single branch carrying cooling fluid through working components from a source to the sink *t*.

The reliability of the parallel-series arrangement in Figure 2c is significantly higher:

$$R_c = 1-(1-0.4^3)^2 \times (1-0.9^3) = 0.76 \tag{24}$$

The variant presented in Figure 2c is an example of *a well-ordered parallel-series system*. A well-ordered parallel-series arrangement is obtained if the available components are used first to build the branch with the highest possible reliability; next, the remaining components are used to build the branch with the second-highest possible reliability and so on, until the entire parallel-series arrangement is built.

If there are three types of components with different age: 'new', 'medium' and 'old' components, the maximum reliability is achieved if all new components are arranged in a single branch, the medium-age components in another branch and all old-age components are grouped in a separate branch (Figure 3).

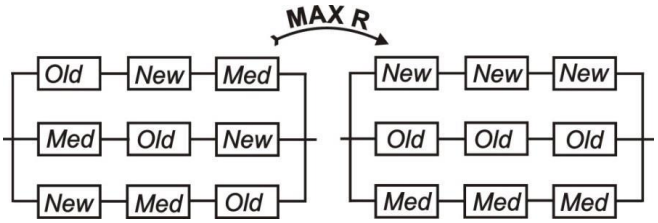

Figure 3. Minimising the risk of failure of a parallel-series system by permutation of interchangeable components

Because of the absence of a method for improving reliability and reducing risk by using inequalities, without knowledge related to the reliability values of components, the opportunity to increase reliability in parallel-series systems, at no extra cost, remained hidden despite that parallel-series arrangements are very common. Indeed, almost any safety-critical system based on detectors working in parallel, for detecting a critical event (increased pressure, temperature, concentration, displacement, toxic gas release, etc.), is a parallel-series system. The parts composing each detector are normally logically arranged in series which means that any particular detector will only work if all building elements (blocks) of the detector work. In order to detect the increase of the safety-critical factor, at least one of the

detectors must detect the increase. Consequently, with respect to detecting the increase of the safety-critical factor the detectors are logically arranged in parallel.

The domain-independent risk-reduction principle of a well-ordered system can be stated as follows: *The well-ordered parallel-series system is characterised by the smallest possible risk of failure.*

Proof. This principle will be proved by making use of an inequality. Suppose that there is a system which is not well-ordered and which possesses the highest possible reliability. The branches in a parallel-series system can always be re-arranged in such a way that for any two branches '*i*', '*j*' for which $i < j$, the branch with index '*i*' is equally reliable or more reliable than branch '*j*' ($R_i \geq R_j$), where R_i and R_j are the reliabilities of branch *i* and branch *j*, respectively. If the system is not a well-ordered system, then there will be two branches *a* and *b* ($a < b$) with reliabilities $R_a \geq R_b$, where there will be at least one component in branch *b* with a larger reliability than the reliability of the analogous interchangeable component in branch *a*. Suppose that $R_a = a_1 a_2 \times ... \times a_{na}$ and $R_b = b_1 b_2 \times ... \times b_{nb}$ are the reliabilities of branches *a* and *b* and na, nb are the number of components in branches *a* and *b*, correspondingly. Without loss of generality, suppose that the two interchangeable components are the last components in the branches *a* and *b* ($a_{na} < b_{nb}$).

The reliability of the initial system can be presented as

$$R_{sys1} = 1 - (1 - a_1 a_2 \times ... \times a_{na})(1 - b_1 b_2 \times ... \times b_{nb}) \times [1 - R_{rest}] \tag{25}$$

where R_{rest} is the reliability of the rest of the parallel-series arrangement (excluding branches *a* and *b*).

After swapping components a_{na} and b_{nb}, the reliability of the resultant system becomes

$$R_{sys2} = 1 - (1 - a_1 a_2 \times ... \times a_{na-1} b_{nb})(1 - b_1 b_2 \times ... \times b_{nb-1} a_{na}) \times [1 - R_{rest}] \tag{26}$$

Subtracting (26) from (25) yields:

$$R_{sys1} - R_{sys2} = (a_{na} - b_{nb})(a_1 a_2 \times ... \times a_{na-1} - b_1 b_2 \times ... \times b_{nb-1}) \times [1 - R_{rest}] \tag{27}$$

The inequality

$$R_a = a_1 a_2 \times ... \times a_{na} \geq R_b = b_1 b_2 \times ... \times b_{nb} \tag{28}$$

holds because of the way the branches have been arranged in descending order according to their reliability ($R_a \geq R_b$). Because $a_{na} < b_{nb}$ (by assumption), removing from the left-hand

side of (28) the positive value a_{na} and from the right-hand side of (28) the larger positive value b_{nb}, yields the stronger inequality

$$a_1 a_2 \times ... \times a_{na-1} > b_1 b_2 \times ... \times b_{nb-1} \tag{29}$$

which means that in equation (27)

$$a_1 a_2 \times ... \times a_{na-1} - b_1 b_2 \times ... \times b_{nb-1} > 0$$

holds. Since $1 - R_{rest} > 0$, and $a_{na} - b_{nb} < 0$, the right-hand side of equation (27) is negative, which means that the resultant system (after the swap of two components of the same type) has a higher reliability. This contradicts the assumption that the initial system (which is not well ordered) possesses the highest possible reliability. It was thus demonstrated that the reliability of a system which is not well-ordered, can be improved by swapping components between parallel branches. A well-ordered system is unique and there can be no two well-ordered systems. Because a parallel-series system can either be a well-ordered or not well-ordered system, the well-ordered system has the highest reliability. The domain-independent risk-reduction principle of the well-ordered systems has been proved.

The result which predicted that the reliability of the well-ordered parallel-series systems is superior to any alternative arrangement has been verified by a computer simulation. The computer simulation consisted of specifying the reliabilities of the interchangeable components in the branches and calculating the reliability of the well-ordered system. Next, a "random scrambling" of the interchangeable components in the branches is initiated, by generating random indices of components from different branches and swapping their reliability values. The swapping guarantees that any resultant system includes exactly the same set of components as the initial system. After each 'random scrambling', the reliability of the scrambled system was calculated and compared with the reliability of the well-ordered system. In all of the conducted simulations, the well-ordered systems were characterised by the largest reliability.

The principle of the well-ordered systems provides an opportunity to remove the maximum amount of system risk *by concentrating the available budget on renewing single parallel branches as opposed to randomly replacing aged components in the system.*

This result also provides the valuable opportunity to improve the reliability of common systems with parallel-series logical arrangement of their components *without the knowledge of their reliabilities and without any investment*. Unlike all traditional approaches, which invariably require resources to achieve reliability improvement and risk reduction, a system

risk reduction can also be achieved by appropriate permutation of the available interchangeable components in the parallel branches. Components of similar level of deterioration (reliability levels) should be placed in the same parallel branch (see the example from Figure 3).

The risk reduction principle based on permutation of interchangeable components has wide applications reaching far beyond its initial engineering context.

Consider a common example where three groups of people (teams) 1, 2 and 3, each of which includes three independently working team members. The teams work in parallel towards achieving the same goal (Figure 4a). The goal is achieved if at least one of the teams succeeds in achieving the goal. Within each team, the task of achieving the goal is divided into subtasks among the team members. Every single person in a team must accomplish their sub-task successfully, in order for the team to achieve the goal. The level of training of each team member is from one of the categories: Strong (S), Weak (W) and Medium (M). A person with strong level of training has a better chance of accomplishing a task successfully compared to a person with medium training or weak training. A person with medium training has a better chance of accomplishing the task successfully compared to a person with weak training.

Separating the people in groups with a similar level of training (Figure 4b) yields the highest chance of achieving the goal. Note that the risk of not achieving the goal has been reduced at no extra cost.

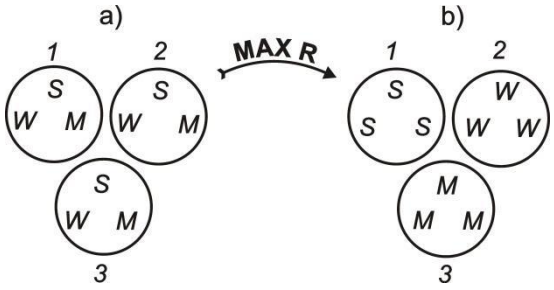

Figure 4. Three groups of people working towards achieving the same goal

5.2 Improving reliability and availability by optimal placement of the condition monitoring equipment

Monitoring provides an early warning of adverse network changes and is critical to the efficient design and operation of repairable networks and the availability of commodity supply.

Consider the system (Figure 5) which transports cooling liquid from three sources s1,s2 and s3 to the chemical reactor *t*. The cooling system consists of identical old pipeline sections (the arrows in Figure 5). Each pipeline section is coupled with a pump for transporting the cooling fluid through the section. The cooling system fulfils its mission if at least one cooling line delivers cooling fluid to the chemical reactor.

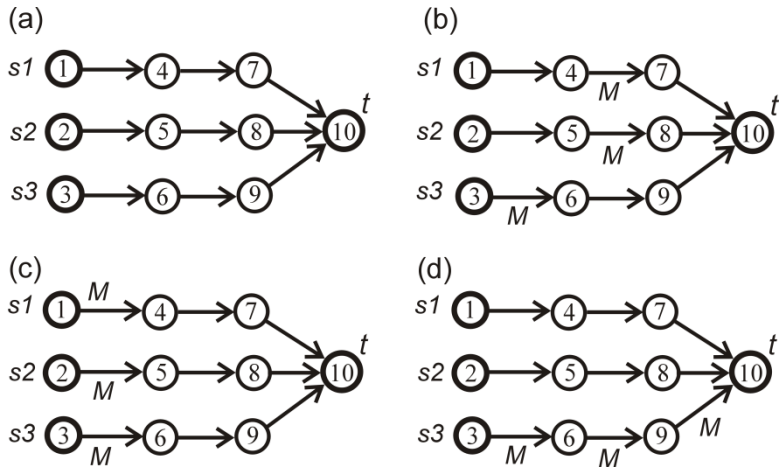

Figure 5. Monitoring the branches of a cooling system.

Introducing condition monitoring on the old cooling sections increases the reliability of the section because it permits detecting problems such as lack of proper lubrication of the pumps, deterioration of the seals and leaks, blockages of the filters, increased current in the coils of the electro-motors, etc. If a problem is registered, a maintenance action is initiated and failure is averted.

Because of cost limitations, it is not possible to install condition monitoring on all cooling sections. Suppose that, due to budget constraints, the number of condition monitoring devices is limited to three. The question of interest is the location of the condition monitoring equipment which maximises the reliability of the cooling system. For a large system including n possible locations for the condition monitoring equipment and k pieces of condition monitoring equipment, the number of possible configurations for the condition monitoring devices is equal to $C_n^k = \frac{n!}{k!(n-k)!}$ - the combinations of k distinct locations for the condition monitoring devices out of n possible locations, which is a very large number for large n and $2 < k \le [n/2]$. For large systems, testing the system reliability for each of all possible configurations of the condition monitoring equipment (Figure 5b,c) is not feasible.

Considering the previous discussion, to maximise the reliability of the system, the condition monitoring devices must all be located along a single cooling branch (Figure 5d). According to the principle of the well-ordered parallel-series systems, this is equivalent to building first a branch with the highest possible reliability.

The optimal locations of condition monitoring equipment provides the right balance between cost, risk and performance which translates into low downtimes, high network availability and small maintenance costs.

The optimal set of monitored components provides the right balance between cost, risk and performance. Optimal locations of the monitoring equipment translate into low downtimes, high network availability and smaller maintenance resources, smaller amount of consumed fossil fuels and less carbon emissions. The smaller maintenance resources also mean low operational costs and high profits.

Identifying the optimal places for system monitoring is also the key to maximising the potential of the existing infrastructure at a minimal cost. High system reliability and availability translate into a high operational availability and safety and high quality of service to customers.

Conclusions

1. The paper demonstrates a new domain-independent method for improving reliability and reducing risk based on two fundamental approaches of using algebraic inequalities: the forward approach, based on deriving algebraic inequalities from real systems and processes and the inverse approach, based on deriving new knowledge by meaningful interpretation of existing correct algebraic inequalities.

2. The forward approach has been used to prove the domain-independent risk-reduction principle of the well-ordered systems which states that the well-ordered parallel-series systems are characterised by the smallest possible risk of failure. In this respect, the paper also answers an important question for a parallel-series system about the components that need to be subjected to condition monitoring so that the reliability of the system is maximised.

3. The forward approach has also been used for optimal assignment of manufacturers to products, with the purpose of minimising the overall percentage of defective products.

4. The paper introduces the inverse approach to using algebraic inequalities based on meaningful interpretation of the variables entering the inequalities and the different parts of the inequalities. By using the inverse approach, it has been established that irrespective of the uncertainties related to the stiffness values of n springs (elastic elements), the equivalent stiffness of the springs connected in series is always at least n^2 times smaller than the equivalent stiffness of the same springs connected in parallel.

5. The inverse approach has also been used to determine tight upper and lower bounds of the percentage of faulty components in a batch of components obtained from pooling several batches of components with unknown sizes.

6. Finally, the paper demonstrates the principle of non-contradiction: if the variables and the different parts of a correct abstract inequality can be interpreted as a system or process, in the real world, the system or process must exhibit properties that are consistent with the abstract inequality.

REFERENCES

Barlow R.E. and Proschan F. (1965) Mathematical Theory of Reliability, John Wiley & Sons, Inc.

Barlow R.E. and Proschan F. (1975) Statistical Theory of Reliability and Life Testing, Rinehart and Winston, Inc.

Budynas R.G., Nisbett J.K. (2015). *Shigley's Mechanical engineering design*, 10th ed. McGraw-Hill Education.

Childs P.R.N. (2014). *Mechanical design engineering handbook*. Amsterdam: Elsevier, 2014.

Cloud M., Byron C., Lebedev, L.P., Inequalities: with applications to engineering, Springer-Verlag, New York, (1998).

Collins J.A., Mechanical design of machine elements and machines, John Wiley & Sons, Inc., New York (2003).

DeGroot M. (1989) Probability and Statistics, Addison-Wesley.

Engel A., Problem-solving strategies, Springer, New York (1998).

Fink A.M., An essay on the history of inequalities, *Journal of Mathematical Analysis and Applications*, 249**,** 118–134 (2000)

French M., Conceptual design for engineers, 3rd ed., Springer-Verlag London Ltd, London (1999).

Gullo L.G., Dixon J. (2018). *Design for safety*. Chichester: Wiley.

Hardy, G., Littlewood J.E., Pólya, G. (1999). *Inequalities*. Cambridge Mathematical Library, Cambridge University Press.

Hoyland A. and Rausand M. (1994) System Reliability Theory, John Wiley and Sons, Ltd. New York.

Kazarinoff N.D., Analytic Inequalities, Dover Publications, Inc, New York, (1961).

Lewis, E.E. (1996). Introduction to Reliability Engineering. New York: Wiley.

Miller I. and Miller M. (1999) John E. Freund's Mathematical Statistics, 6th edn, Prentice Hall International, Inc.

Mott R.L, Vavrek E.M., Wang J. (2018). *Machine Elements in Mechanical Design*, 6th ed. Pearson Education Inc.

Norton R.L., Machine design, An integrated approach, 3rd ed., Pearson International edition, 2006.

Pachpatte B.G., *Mathematical inequalities*, North Holland Mathematical Library, vol.67, Elsevier, Amsterdam, (2005).

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, September/October (4), pp.267-273 (1990).

Ramakumar R. (1993) Engineering Reliability, Fundamentals and Applications, Prentice Hall, Upper Saddle River, NJ.

Rastegin A. Convexity inequalities for estimating generalized conditional entropies from below Kybernetika, Vol. 48 (2012), No. 2, 242--253

Samuel A. and J. Weir, *Introduction to engineering design: Modelling, synthesis and problem solving strategies*, Elsevier, London 1999.

Sedrakyan H., Sedrakyan N. (2010). Algebraic Inequalities, Cham: Springer.

Shigley J.E., C.R.Mischke, *Mechanical engineering design*, 5th ed., McGraw-Hill International editions, 1989.

Steele J.M. The Cauchy-Schwarz master class: An introduction to the art of mathematical inequalities, Cambridge University Press, New York, 2004.

Thompson G., Improving maintainability and reliability through design, Professional Engineering Publishing Ltd, London (1999).

Todinov, M.T. (2016). *Reliability and Risk Models: Setting Reliability Requirements*, 2e. Wiley.