Analysing the reliability of actuation elements in series and parallel configurations for high-redundancy actuation

ANALYSING THE RELIABILITY OF ACTUATION ELEMENTS IN SERIES AND PARALLEL CONFIGURATIONS FOR HIGH REDUNDANCY ACTUATION

THOMAS STEFFEN, FRANK SCHILLER, MICHAEL BLUM, AND ROGER DIXON

Abstract. A high redundancy actuator (HRA) is an actuation system composed of a high number of actuation elements, increasing both travel and force above the capability of an individual element. This approach provides inherent fault tolerance: if one of the elements fails, the capabilities of the whole actuator may be reduced, but it retains core functionality. Many different configurations are possible, with different implications for the actuator capability and reliability. This paper analyses the reliability of the HRA based on the likelihood of an unacceptable reduction in capability. The analysis of the HRA is a highly structured problem, but it does not fit into known reliability categories (such as the k-out-of-n system), and a fault tree analysis becomes prohibitively large. Instead, a multi-state systems approach is pursued here, which provides an easy, concise and efficient reliability analysis of the HRA. The resulting probability distribution can be used to find the optimal configuration of an HRA for a given set of requirements.

Keywords: redundancy, mechanical actuation, bionics, high redundancy actuator (HRA), fault-tolerance, multi-state system.

Note: this is the authors' draft - the final version is available from Taylor & Francis.

1. Introduction

1.1. **Fault Tolerance.** Fault tolerance is about dealing with faults in technical systems (Blanke et al., 2006). Its goal is to prevent a component fault from becoming a system failure (Blanke et al., 2001). So far, most theoretical considerations have focused on sensor faults. If a sensor signal is incorrect, the faulty signal can be ignored, and a redundant sensor can be used instead with minimal effect on the system. Therefore redundant sensors are very effective at reducing the probability of a fault affecting the system function (Frank, 1990).

Actuators however can fail in several different ways or fault modes, and the resulting effect on the system cannot be ignored. For instance, a valve blocked in the closed position can be tolerated by means of opening a redundant valve in parallel. However, if a valve is blocked in the open position, a parallel redundancy cannot be used to compensate, because a valve connected in series needs to be closed. Therefore, the actuator redundancy has to be studied for a network of actuators, and the expected fault modes are highly important.

Practical approaches to fault tolerant actuation ignore the different fault modes. In a typical application, 2, 3 or 4 actuators are used in parallel, very much like redundant sensors. Each actuator is strong enough to meet the performance requirements by itself, and the impact of some failed actuators on the system is considered negligible. This means in the valve example above that for instance some valves blocked in the closed position are accounted for by the parallel configuration, but valves blocked in the open position have to be prevented by additional, specific measures. If the valves are connected in series, the opposite applies: valves blocked open are ok, but valves blocked close break the system. Either way, the result is a system with a significant amount of over-engineering, because many times the required actuation power needs to be installed.

Practical approaches to fault tolerant actuation ignore the different fault modes. In a typical application, 2, 3 or 4 actuators are used in parallel, very much like redundant sensors. Each actuator is strong enough to meet the performance requirements by itself, and the impact of some failed actuators on the system is considered negligible. This means a loss of force fault is accounted for, but a solid lock-up of an actuator has to be prevented by specific structural measures. The result is a system with a significant amount of over-engineering, because many times the required actuation power needs to be installed.

The scientific literature also struggles with the distinct implications of actuator faults, with most approaches still based on an information view more suitable for the handling of sensor faults. Recent examples include the extension of the observer-based approach to cover actuator faults in the form of the virtual actuator (Steffen, 2005), and the exploitation of analytical redundancies in the form of dynamic gain scheduling and control allocation (Oppenheimer and Doman, 2006).

1.2. **High Redundancy Actuator.** The obvious way to improve reliability is to use a greater number of actuation elements. To reduce the over-dimensioning involved in this, it is possible to reduce the size and strength of elements, while retaining a reliability advantage. For example, a system with ten elements may still work with only eight of them operational, and the reliability improves because two faults can be accommodated. The overall capacity is only over-dimensioned by 25 %. This is a significant improvement over the use of two full-sized redundant actuators, which leads to 100 % over-dimensioning. The use of an optimal

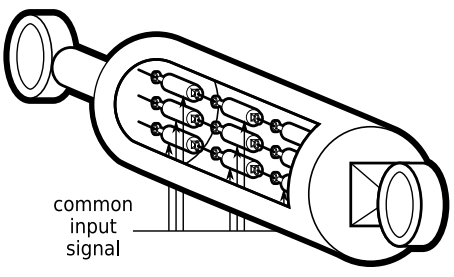


Figure 1. High Redundancy Actuator

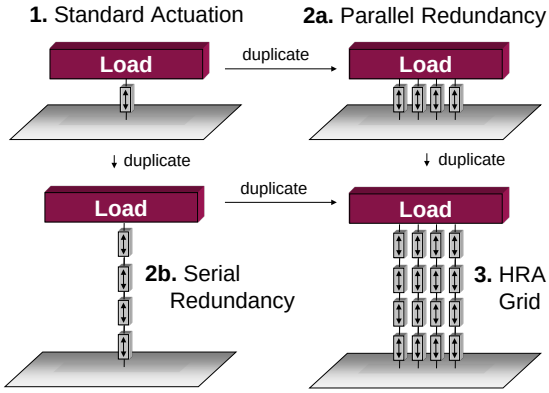


FIGURE 2. Series and Parallel Redundancy in the HRA

number and size of elements is the central idea of the high redundancy actuator (HRA).

The HRA is inspired by one of nature's answers to fault tolerant actuation: the muscle. It is composed of many individual fibres, each of which provides only a minute contribution to the force and the travel of the muscle. This allows the muscle as a whole to be highly resilient to damage of individual fibres. In this sense the HRA is a bionic system, because it is inspired by an existing biological solution.

Traditionally, only parallel aggregation is used, which makes the system resilient towards loss of force, but not with respect to lock-up faults (see Figure 2). Series aggregation could be used to address lock-up faults, but it does not help with loss of force faults. The HRA is a synthesis of both aggregations, with actuation elements being used both in parallel and in series (see Figure 1). This increases the available travel and force over the capability of an individual element, and it makes the actuator resilient to faults where an element becomes loose or locked up. These faults will reduce the overall capability, but they do not render the assembly functionless, and they do not require a change of the control structure as proposed by Jiang et al. (2010).

Initial research has focused on the modelling and control of simple configurations with four elements (Du et al., 2006, 2007). Previous studies on the reliability of electromechanical assemblies are rare: the reliability of electro-mechanical steering is discussed by Blanke and Thomsen (2006), and electrical machines and power electronics are analysed by Ribeiro et al. (2004). Neither of these consider the combination of both series and parallel structures together in a single actuator.

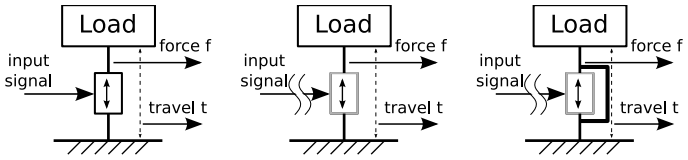
This paper presents a method to analyse the reliability of an HRA of any size, as long as it can be interpreted as a hierarchy of parallel and series configurations. The difficulty with analysing an HRA is that many faults can occur simultaneously, and the system may still be functional. Conventional methods of reliability analysis (binary fault trees, event trees, stochastic automata etc) suffer from an extreme increase of complexity. The number of cut sets increases exponentially with the system size, and this renders the analysis unmanageable even for reasonably small systems such as a configuration of 10×10 elements.

The approach presented here is loosely based on the concepts developed using graph theory in Steffen et al. (2007, 2008). It avoids the issue of complexity by using a multi-state system abstraction as used by Jenab and Dhillon (2006) that is independent of the temporal dimension of the problem. Using the principle of divide and conquer, the system is decomposed level by level, relying on simple aggregation laws of low computational complexity. The basic idea was introduced in Steffen et al. (2009), and it is presented here in a much more thorough and comprehensive treatment. The approach is applied to different 4×4 configurations for comparison, generalised results are proven about the relative advantages and disadvantages of one configuration over another of the same size, and a discussion of the computational complexity of this approach is included.

1.3. **List of Symbols.** This paper follows the notation used in the first part of Pham (2003), supplemented by the application specific interpretation of the capability c. This leads to the following symbols.

Symbol	Meaning
$P(\cdot)$	probability of an event
q	failure probability (unreliability) of an element, typically close to 0
p	reliability of an element, typically close to 1
c	generic capability, normalised (1 for a single element)
$\mathbf{c}$	vector of capabilities for several elements
c_t	travel (or velocity) capability
c_f	force capability
$n!$	factorial of n, $n! = \prod_{i=1\ldots n} i$
$\binom{i}{n}$	binomial i over n, $\binom{i}{n} = \frac{i!}{n!(n-i)!}$
x	a system configuration $x \in \{\mathrm{S},\mathrm{P}\}^k$ with size k
$r_x(c)$	probability of capability c of system x: $r_x(c) = P(c_x = c)$
$R_x(c)$	reliability of system x wrt. the requirement c, $R(c) = P(c_x \geq c)$
$R_{fx}(c_f)$	reliability of x wrt. the force requirement c_f
$R_{tx}(c_t)$	reliability of x wrt. the travel requirement c_t
$R_{ftx}(c_f, c_t)$	reliability of x wrt. force requirement c_f and travel requirement c_t

1.4. **Structure of the Paper.** Section 2 deals with the basic terms and concepts used for the reliability assessment, and it defines the behaviour of individual actuation elements. In Section 3, the effect of series or parallel arrangement of elements on reliability is investigated. In Section 4, the special cases of series-in-parallel and parallel-in-series configurations are analysed for a simple 2×2 system. In Section 6, this concept is extended to configurations with multiple layers, and an exhaustive study of 4×4 systems is presented. Section 7 contains further remarks and comparative properties of different configurations. The paper finishes with some conclusions in Section 9.



(a) nominal (b) loose fault (c) lock-up fault

FIGURE 3. A Single Actuation Element

TABLE 1. Influence of Faults on Capabilities

Fault	Force Capability	Travel Capability	Probability
None	nominal (1)	nominal (1)	$p_f p_t$
Loose	affected (0)	nominal (1)	$q_f p_t$
Lock-Up	nominal (1)	affected (0)	$p_f q_t$
Both	affected (0)	affected (0)	$q_f q_t$

2. Specification of Actuation Elements

The individual actuation elements of the HRA are specified using a number of different measures. From an abstract perspective, they can be divided into two types: physical measures and reliability measures. The first kind contains physical parameters related to the mechanical movement, such as force, speed, acceleration, or distance. The second type of parameters describes the probability of a fault.

2.1. **Specification of the Nominal Performance.** An actuation element can perform a one-dimensional mechanical movement (expansion or contraction) in response to a control input as shown in Figure 3a. To simplify the analysis, only the static case is considered in the following. So the central performance measurements of an element are the force f it can produce and the amount of travel t it can provide.

These two basic functions are called force and travel capability. It is used consistently to describe both the properties of an individual element as well as the properties of a combination of elements.

While it is entirely possible to measure the capabilities in physical units (Newton for the force and meter for the travel), this paper will use normalised values instead. The force capability c_f and travel capability c_t of a nominal element are defined to be one (without unit). This simplifies the notation significantly, and when necessary, the discrete numbers can easily be converted back into physical units.

In principle, it is possible to describe the capabilities with continuous values, and to use continuous probability distributions to describe them. However, that approach is more suitable for analysing the effect of small manufacturing deviations between elements than the effect of significant faults.

2.2. **Specification of Faults.** The two capability measures lead to two main fault modes of an element: loss of force (loose fault, see Figure 3b) and loss of travel (lock-up fault, see Figure 3c). Both faults are assumed to be total: a fault reduces the relevant capability to zero (see Table 1 and Figure 4).

For the sake of simplicity, it is assumed that both fault modes (loose and lock-up) are independent. This implies

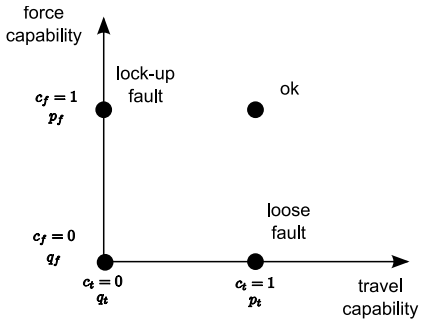


FIGURE 4. Two-Dimensional Capability Space by Fault States

TABLE 2. Two-Dimensional State Probabilities

	$c_f = 0$	$c_f = 1$
$c_t = 0$	$q_f q_t$	$p_f q_t$
$c_t = 1$	$q_f p_t$	$p_f p_t$

that they can also appear together, which may seem impossible at first. However, this analysis is concerned with the guaranteed performance of an element, and it is possible an element fails to deliver force in one situation and travel in another, so that in effect it cannot reliably provide either capability.

In applications where both fault modes are exclusive, a small error is made by these assumptions. Ways to reduce and bound this error will be discussed in Section 5.

It is also assumed that a locked-up element is fixed in its neutral position (this would be the medium length if the nominal travel is symmetric to both sides). This assumption is for convenience only and can be relaxed later.

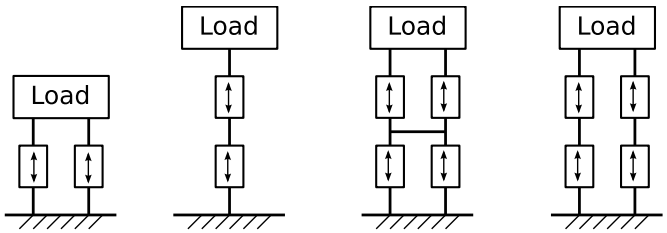
2.3. **Specification of Reliability.** In practical applications, different ways can be used to describe the reliability of an element, such as mean time to failure (MTTF), availability, failure probability over a given time, or failure probability during a specified mission. The relevant specification depends very much on the application. However, all measures are based on probabilities or probability densities over time. These functions over time can be interpreted using any of the above measures. Therefore, this paper will use fault probabilities as a generic way to measure reliability:

$$\begin{aligned} P(\text{loose}) &= P(c_f = 0) = q_f \\ P(\text{lock-up}) &= P(c_t = 0) = q_t \quad . \end{aligned}$$

2.4. **Capability Distributions.** Together with the corresponding OK-probability $P(c_f = 1) = p_f = 1 - q_f$ and $P(c_t = 1) = p_t = 1 - q_t$, these values define the two capability distributions

$$\begin{aligned} r_f(i) &= P(c_f = i) \\ r_t(j) &= P(c_t = j) \quad , \end{aligned}$$

where i and j are non-negative integer values representing the force and travel capability under consideration. Because there are two capabilities, the state space is two-dimensional as shown in Table 2. However, to avoid the complexity of two-dimensional distributions, this paper deals with one capability at a time. This separation is possible because both fault modes are assumed to be statistically independent.



(a) parallel (b) series (c) 2x2 PS (d) 2x2 SP

FIGURE 5. Basic Configurations

TABLE 3. Configurations and Capabilities

Configuration	Force Capability	Travel Capability
Parallel	increased (sum)	limited (min)
Series	limited (min)	increased (sum)
Grid	increased (times columns)	increased (times rows)

In some cases, the cumulative capability distributions

$$R_f(i) = P(c_f \geq i) = \sum_{k=i}^{c_{f,\max}} P(c_f = k) = \sum_{k=i}^{c_{f,\max}} r_f(k)$$

$$R_t(j) = P(c_t \geq j) = \sum_{k=j}^{c_{t,\max}} P(c_t = k) = \sum_{k=j}^{c_{t,\max}} r_t(k)$$

are used for determining the reliability of more complex configurations.

As more elements are used together, the capability increases, and the distributions extend to higher values. The reliability can be determined from the distribution by looking up the required performance of the system. This notion of capabilities was developed in Steffen et al. (2007), but the concept of a capability distribution is new.

3. Aggregation on a Single Level

The main reason for using several elements is that they serve to increase the capabilities (see Figure 5 and Table 1). Two elements in parallel can produce twice the force, and two elements in series can achieve twice the travel. In the following, it is assumed that n equal elements are combined, and that the capability distribution for one individual element is known.[1]

3.1. Limiting Capabilities.

Some capabilities do not increase when subsystems are combined. Instead, the capability of the resulting system is determined by the weakest part. This happens e.g. with the force capability c_f for actuation elements used in series (see Figure 5b)

$$c_{f\mathrm{S}}(\mathbf{c}_f) = \min\{c_{f1}, c_{f2}\} \quad , \tag{1}$$

where $\mathbf{c}_f$ denotes the vector $(c_{f1}\ \ c_{f2})^T$. The same equation also applies to the travel capability of elements in parallel

$$c_{t\mathrm{P}}(\mathbf{c}_t) = \min\{c_{t1}, c_{t2}\} \tag{2}$$

(see Figure 5a). These equations follow directly from the specification and physical laws, so they will be assumed as given for the reliability analysis.

In both cases, the capability of such a combined system is the minimum capability over all the subsystems or elements:

$$c_{\lim}(\mathbf{c}) = \min\{c_1, \ldots, c_n\} \quad . \tag{3}$$

This represents a classic series arrangement of multi-state subsystems (MSS), and the reliability has been well studied in the literature. Here, a new operator is introduced to calculate the new cumulative reliability distribution for the overall system.

Theorem 1. *If n elements with the cumulative reliability distributions $R_i(c)$ are connected so that the overall capability is limited by the weakest element according to Eqn. (3), the cumulative reliability distribution $R_{\lim}(c_{\lim})$ of the new system can be calculated as*

$$R_{\lim}(c) = R_1 \circledast R_2 \circledast \ldots \circledast R_n(c) \tag{4}$$

with the operator

$$(R_1 \circledast R_2)(c) = R_1(c)R_2(c) \quad . \tag{5}$$

Proof. According to the definition, the reliability $R_{\lim}(c)$ is the probability that the overall capability is at least c:

$$c_{\lim} \geq c \quad .$$

Because of Eqn. (3), this inequality holds if and only if all elements have at least this reliability:

$$\forall_i : c_{\mathrm{i}} \geq c \quad .$$

Since the capability of the elements c_i are considered to be independent, the probability of this condition can be calculated as the product of the probabilities of the individual terms:

$$P(\forall i : c_i \geq c) = \prod_i P(c_i \geq c) = \prod_i R_i(c) \quad .$$

This is exactly the result defined by the operator $\circledast$. □

Since the original Eqn. (3) is applicable in two cases, the same is true for the resulting operator $\circledast$. It can be used to describe the force of elements in series

$$R_{f\mathrm{S}} = R_{f1} \circledast R_{f2} \tag{6}$$

or the travel for elements in parallel

$$R_{t\mathrm{P}} = R_{t1} \circledast R_{t2} \quad . \tag{7}$$

Remark 1. *For a number of n identical elements $R(c) = R_i(c)$, the result can be simplified to*

$$R_{\lim}(c) = R_1 \circledast R_2 \circledast \ldots \circledast R_n(c) \tag{8}$$

$$= (R(c))^n \quad . \tag{9}$$

[1] The same basic laws of aggregating capabilities are also applicable in many other areas. Reliable rotary actuation can be achieved with velocity and torque adding gears, for example. Electrical systems deal with the dual variables of voltage and current, and series and parallel configuration are commonly used in IGBT (insulated gate bipolar transistor) high power switching devices (Shammas et al., 2006). Transportation systems and communication networks also have corresponding relations governing throughput and latency. From a reliability perspective, all these systems are essentially identical in that they use series and parallel configurations to increase two dual capabilities of primary concern.

If the elements only have the states 0 *and* 1 *(with probabilities* $r(0) = q$ *and* $r(1) = p = 1 - q$*), these results can be simplified further to the following distribution:*

$$r_{\lim}(0) = 1 - p^n \tag{10}$$

$$r_{\lim}(1) = R_{\lim}(1) = p^n \quad . \tag{11}$$

For many practical cases, it can be assumed that the probability of a fault q *is small compared to the probability of normal operation* p*. Using the assumption* $p \approx 1$*, this distribution can be (conservatively) approximated as*

$$r_{\lim}(0) \approx nq \tag{12}$$

$$r_{\lim}(1) \approx 1 - nq \quad . \tag{13}$$

3.2. **Additive Capabilities.** If several actuation elements are used together, the capability of the combined system may increase above the capability of any element. In fact, this increase is the motivation for using several elements in the first place.

In contrast to the minimum operator in Eqn. (1), the sum applies to the force capability of two elements in parallel (see Figure 5a),

$$c_{f\mathrm{P}}(\mathbf{c}_f) = c_{f1} + c_{f2} \tag{14}$$

and to the travel capability of two elements in series (see Figure 5b)

$$c_{t\mathrm{S}}(\mathbf{c}_t) = c_{t1} + c_{t2} \quad . \tag{15}$$

In both cases, the relevant capabilities of the elements add up to the capability of the overall system:

$$c_{\mathrm{add}}(\mathbf{c}) = c_1 + c_2 + \ldots + c_n \quad . \tag{16}$$

Remark 2. *This is unlike typical multi-state systems (Jenab and Dhillon, 2006), because the state space of the system* c_{add} *can be larger than the state space of any element* c_i*. So this specific case is not usually treated in the literature on multi-state systems. A similar situation is discussed for two-state systems in the k-out-of-n:G problem, but the k (which corresponds to* c_{add}*) is considered given. This is different from the situation with the HRA, where a distribution over k is sought, and therefore k is a variable.*

Again, a new operator $\oplus$ is introduced to calculate the cumulative reliability distribution of the combined system of two elements.

Theorem 2. *If* n *elements with cumulative reliability distributions* $R_i(c_i)$ *are arranged so that the capabilities add up according to Eqn. (16), the cumulative reliability distribution* $R_{\mathrm{add}}(c_{\mathrm{add}})$ *of the resulting system is defined by*

$$R_{\mathrm{add}}(c) = R_1 \oplus R_2 \oplus \ldots \oplus R_n(c) \tag{17}$$

with the operator

$$(R_1 \oplus R_2)(c) = \sum_{i=0}^{c} \left(R_1(i) - R_1(i+1)\right) R_2(c-i) \quad . \tag{18}$$

Proof. For this operator, it is easier to work with the reliability distribution r instead of the cumulative reliability distribution R. Because only integer capabilities are used, it follows from the definition of R and r that $r(i) = R(i) - R(i+1)$. Therefore, the following equation is equivalent to (18):

$$r_{\mathrm{add}}(c) = \sum_{i=0}^{c} r_1(i) r_2(c-i) \quad . \tag{19}$$

Central to this proof is the set of all capability combinations c_1 and c_2 that lead to the same overall capability $c_{\mathrm{add}} = c$. According to Eqn. (16), this set is

$$\mathcal{C}(c) = \{(c_1, c_2) \in \mathbb{N}_0^2 : c_1 + c_2 = c\} \quad .$$

The probability of the two elements to have the capabilities (c_1, c_2) is

$$P(c_1, c_2) = P(c_1)P(c_2) = r_1(c_1)r_2(c_2)$$

because both are considered to be independent. Now the probability of a given overall capability of c can be calculated as:

$$P(c_{\mathrm{add}} = c) = \sum_{(c_1,c_2)\in\mathcal{C}(c)} P(c_1)P(c_2)$$

which is equivalent to Eqn. (19). □

This operator $\oplus$, too, is applicable in two situations: the force of elements in parallel

$$R_{fP} = R_{f1} \oplus R_{f2} \tag{20}$$

and the travel for elements in series

$$R_{t\mathrm{S}} = R_{t1} \oplus R_{t2} \quad . \tag{21}$$

By using this operator $\oplus$ together with the previous operator $\circledast$ it is possible to express all possible aggregations of force and travel via parallel or serial connections.

Remark 3. *It is trivial to see that both operators satisfy several basic properties of an algebraic addition such as commutativity, associativity, and the zero and identity element. The zero element is an element that is always so strong that it never limits the overall system, while the identity element delivers no capability at all. In fact, the underlying deterministic calculations of capabilities using Eqns. (3) and (16) form a max-plus algebra.*

However, the two operators working with stochastic distributions do not satisfy the law of distributivity:

$$R_1 \oplus R_2 \circledast R_1 \oplus R_3 \neq R_1 \circledast (R_2 \oplus R_3) \quad .$$

This is caused by the initial assumption that all elements are independent, even if modelled by the same reliability distribution. So the same variable R_1 *is interpreted as referring to different elements, which are nominally identically, but subject to independent faults. This breaks the law of distributivity, so the two operators* $\circledast$ *and* $\oplus$ *do not form an algebraic ring (see Heidergott et al., 2005). Ring properties could be restored by using multidimensional distributions, but the additional complexity is not warranted in this application.*

4. Hierarchical Aggregation

An HRA contains elements in series and in parallel. Thus it is important to analyse the reliability resulting from multiple levels of aggregations. Assuming that the configuration is given, this section explains how to find the reliability distribution of the overall system by combining the operators defined above.

Any structure can be analysed using an iterative bottom-up approach. From the capability distribution of the individual elements, it is possible to calculate the distributions for the basic subsystems, which are either parallel or series arrangements of elements. Basic subsystems can be aggregated to more complex subsystems, and this can be repeated until the reliability of the overall system is found.

For a successful application of this iterative approach, it is required that the actuator configuration is described as a series-parallel network. This is possible if the HRA can be broken down into series and parallel configurations of subsystems, until the level of individual actuation elements is reached. Not all networks satisfy this condition (a detailed analysis is beyond the scope of this paper). In electrical networks, star-triangle conversion is typically used to solve this problem. This is not feasible for the stochastic analysis, because the one-to-one correspondence between faults and elements is lost. Fortunately, non series-parallel networks are rare in mechanical engineering, and an analysis of typical sample configurations has shown that they offer no advantage in terms of reliability, weight or cost.

4.1. **Notation and Formalism.** For the examples used here, it is assumed that two equal subsystems are used in series or in parallel. A series configuration of two elements is denoted with the letter S, and the parallel configuration with the letter P (cf. Section 3). A sequence of letters denotes a hierarchical configuration, from the bottom level of aggregating individual elements up to the complete system.

So two series elements, duplicated in parallel, are called SP. The dual configuration (two parallel elements, and two of these blocks arranged in series) is denoted as PS. Using two SP systems in series leads to an SPS configuration and so on. It is also possible to repeat the same aggregation type immediately, for example a PP configuration consists of 4 elements in parallel.

Several examples are shown in Figure 12. All systems defined by this notation are highly regular and symmetrical, which simplifies the analysis considerably. Following the notation from Section 3, the cumulative force capability of a configuration x is denoted with $R_{fx}(c_f)$, and the cumulative travel capability with $R_{tx}(c_t)$. This allows an easy comparison between different configurations. In the following, all elements are assumed to be identical as specified using the properties defined in Section 2.

4.2. **Iterative Reliability Calculation.** In each iterative step, two subsystems with a known reliability distribution are combined to a new system. The configuration of a subsystem is assumed to be x, and the cumulative force and travel reliability distributions are $R_{fx}(c_f)$ and $R_{tx}(c_t)$.

For a parallel configuration (xP) of two subsystems x_1 and x_2, the force increases ($c_{f1}+c_{f2}$), and the travel is limited by the weaker subsystem ($\min\{c_{t1}, c_{t2}\}$). As discussed in Section 3, the following two operators can be used to calculate the cumulative reliability distributions.

Theorem 3. *The cumulative reliability distributions for a system of two nominally identical parallel subsystems are*

$$R_{fx\mathrm{P}} = R_{fx} \oplus R_{fx} \tag{22}$$

$$R_{tx\mathrm{P}} = R_{tx} \circledast R_{tx} \quad . \tag{23}$$

Similarly, in a series configuration (xS), the force is limited by the weakest element ($\min\{c_{f1}, c_{f2}\}$), and the travel increases ($c_{t1}+c_{t2}$). So the cumulative reliability distributions are determined by the other operator, respectively.

Theorem 4. *The cumulative reliability distributions for a system of two nominally identical subsystems in series are*

$$R_{fx\mathrm{S}} = R_{fx} \circledast R_{fx} \tag{24}$$

$$R_{tx\mathrm{S}} = R_{tx} \oplus R_{tx} \quad . \tag{25}$$

Proof. The proofs for these two theorems are analogue to the proofs of Theorems 1 and 2 in Section 3. Instead of the two individual elements assumed there, two identical subsystems specified by R_{fx} and R_{tx} are used. These subsystems satisfy all the assumptions made about the elements, including the independence. □

By using these four equations iteratively, the reliability distributions of arbitrarily complex configurations can be determined in a straightforward way.

4.3. **Reliability Order.** It is obvious that some configurations are more reliable than others, even for the same overall size. The following findings will demonstrate this for the case of force reliability R_f, and the case for travel reliability is analogue but inverted.

The fundamental operation is the exchange of an SP configuration for a PS configuration. As shown in Figure 5, this means the introduction of the cross link in the centre where all four elements come together. Intuitively, this can only increase the reliability of the system.

Lemma 1. *Exchanging an SP aggregation for a PS aggregation enhances the force reliability:*

$$R_{fx\mathrm{PS}y}(c) \geq R_{fx\mathrm{SP}y}(c) \quad . \tag{26}$$

Proof. The proof is possible by looking at the reliability distributions, but it is much easier on the level of capabilities. If c_1 to c_4 are the capability of the four subsystem with configuration x, the capability of the xPS configuration

$$c_{x\mathrm{PS}} = \max(c_1 + c_2, c_3 + c_4)$$

and the capability of the xSP configuration is

$$c_{x\mathrm{SP}} = \max(c_1, c_3) + \max(c_2, c_4) \quad .$$

It follows that for all $c_i \geq 0$

$$c_{x\mathrm{SP}} \geq c_{x\mathrm{PS}} \quad .$$

Due to the monotonicity of capability aggregation, this also holds for the comparison of the full systems

$$c_{x\mathrm{SP}y} \geq c_{x\mathrm{PS}y} \quad .$$

So for every possible fault combination, the configuration xSPy is at least as strong as the configuration xPSy, and therefore the capability distribution will satisfy the relation (28). □

This lemma 1 directly leads to a more general theorem for interchanging S and P aggregation for non-adjacent layers.

Theorem 5. *Exchanging an earlier (small subsystem) S aggregation with a later (bigger subsystem) P aggregation enhances the force reliability:*

$$R_{fx\mathrm{P}y\mathrm{S}z}(c) \geq R_{fx\mathrm{S}y\mathrm{P}z}(c) \quad . \tag{27}$$

Proof. This can be shown by repeatedly applying the lemma above. For this purpose, the first S in y is moved to the front by repeatedly applying the lemma, then the next S is moved in its place etc., until the S after y can be moved into y, leaving a P in its place. In total $|y|+1$ operations are necessary, where $|y|$ is the length of y. □

The same conclusion can be found for the travel reliability, except that the effect is the opposite:

Theorem 6. *Exchanging an earlier (small subsystem) S aggregation with a later (bigger subsystem) P aggregation reduces the travel reliability:*

$$R_{tx\mathrm{P}y\mathrm{S}z}(c) \leq R_{tx\mathrm{S}y\mathrm{P}z}(c) \quad . \tag{28}$$

the proof is analogue to above. Both theorems together demonstrate that selecting the best configuration is a trade-off between robustness towards loose faults and robustness towards lock-up faults.

5. Approximation of Elements With Exclusive Error Modes

The proposed independent analysis of both fault modes is only valid under the assumption that the fault modes are independent of each other. For many practical applications, the fault modes are exclusive and therefore not independent, and it is important to consider the error introduced by this assumption of independence. The case of both fault modes being present in an element is assumed to be $q_f q_t$, but in reality it is 0. There are two principle ways to deal with this discrepancy: on the element level and on the system level.

5.1. Adjustment of Element Probabilities.

On the element level, the key problem is that the probability of the fault-free case is (see Table 1)

$$P(\text{Fault=None}) = (1-q_f)(1-q_t) = 1 - q_f - q_t + q_f q_t$$

whereas the correct (lower) value is

$$1 - q_f - q_t \quad .$$

The error $q_f q_t$ is exactly the probability of the combined fault case.

$$P(\text{Fault=Both}) = q_f q_t \quad .$$

The proposed solution to avoid this is to add the error to one of the fault probabilities. For example the force error probability can be increased to

$$q'_f = \frac{q_f}{1-q_t}$$

which leads to the correct fault-free probability

$$P(\text{Fault=None}) \quad = \quad (1-q'_f)(1-q_t) = 1 - q_f - q_t \quad .$$

The likelihood of a loose fault is overestimated by these, and this leads to a slightly inaccurate but conservative reliability result. The downside of this approach is that the size of the error on the end result is not known (unless a separate calculation is performed without the adjustment).

5.2. Adjustment of Aggregated Reliability.

Alternatively a second option can be pursued: it leaves the element fault probabilities unchanged and adjusts the reliability resulting from the aggregation instead to make it conservative. The underlying assumption in this case is that both fault modes are exclusive, both for the elements and for the aggregated system.

For the element specification, this leads to three distinct cases:

$$\begin{aligned} P(\text{Fault=None}) &= 1 - q_f - q_t \\ P(\text{Fault=Loose}) &= q_f \\ P(\text{Fault=Locked}) &= q_t \quad . \end{aligned}$$

These are exact probabilities.

For the results of the aggregated system, this assumption of exclusivity is not strictly true, because a specific combination of locked and loose elements could lower both capabilities below the requirements, even if each element exhibits only one failure mode.

While the probabilities of meeting (or not) either capability are known exactly (R_{fx} and R_{tx}), the overlap between the two cases is not known. If both fault modes were completely independent as assumed above, the probability of both being present could be calculated as $(1-R_{fx})(1-R_{tx})$. Since both fault modes are exclusive on the element level, the probability for this combined fault mode has to be lower. The exact value can only be found using a much more involving two dimensional analysis.

By using $(1-R_{fx})(1-R_{tx})$ as an upper and 0 as a lower bound, the following bounds can be found for the final system reliability:

$$\begin{aligned} R_{ftx}(c_f, c_t) &\geq 1 - (1 - R_{fx}(c_f) - (1 - R_{tx}(c_t)) \\ &= R_{fx}(c_f) + R_{tx}(c_t) - 1 \\ R_{ftx}(c_f, c_t) &\leq R_{fx}(c_f) R_{tx}(c_t) \end{aligned}$$

This is based on conservative assumptions only, and therefore the true value is known be within the bounds. The key advantage of this method is that two bounds are given, and makes it possible to quantify the error made by dealing with both fault modes independently.

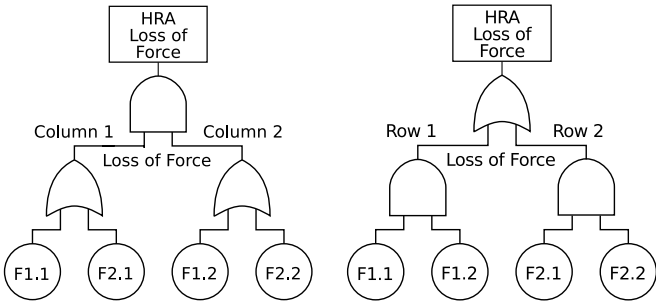
6. Example Configurations

Some representative examples of series-parallel configurations will be discussed in this section. The first two systems are two level arrangements (called series in parallel and parallel in series), as shown in Figures 5c and 5d. Later the analysis is extended to all 4×4 configurations.

6.1. Force Capability of Series in Parallel.

The first example consists of two series elements, duplicated in parallel. This configuration is called series in parallel or SP for short. It consists of two serial elements on the left (upper left 1.1 and lower left 2.1), and two corresponding serial elements on the right (upper right 1.2 and lower right 2.2). The system reliability is analysed for the capability to generate the force of a single element, and the resulting fault tree is shown in Figure 6.

Let the force capabilities or states of the left column be c_{f11} and c_{f21}, and the capabilities on the right c_{f12} and



(a) SP configuration (b) PS configuration

FIGURE 6. Fault Tree for a Force Requirement of 1

c_{f22}. All elements have the same force reliability p_f. The force capability of the system is

$$c_{f\mathrm{SP}}(\mathbf{c}_f) = c_{f\mathrm{left}} + c_{f\mathrm{right}} \tag{29}$$
$$= \min\{c_{f11}, c_{f21}\} + \min\{c_{f12}, c_{f22}\}\,. \tag{30}$$

Following the bottom up approach, the cumulative reliability distribution $R_{f\mathrm{S}}(c)$ for a single column of two elements in series needs to be determined first. According to Eqn. (6), the operator $\circledast$ is required

$$R_{f\mathrm{S}} = R_f \circledast R_f \quad ,$$

and it leads to the result

$$R_{f\mathrm{S}}(0) = 1 \tag{31}$$
$$R_{f\mathrm{S}}(1) = p_f^2 = 1 - 2q_f + q_f^2 \quad . \tag{32}$$

The computation of these reliabilities is much easier from a numerical perspective if they are expressed in terms of q. Therefore, polynomials in q_f will be used to describe them here.

This reliability distribution $R_{f\mathrm{S}}$ is used to describe the two columnar subsystems that compose the whole system. This case is particularly simple, because the subsystems are still binary (with capabilities of 0 and 1 only). Eqn. (20) can be used for the parallel arrangement of subsystems with the operator $\oplus$:

$$R_{f\mathrm{SP}} = R_{f\mathrm{S}} \oplus R_{f\mathrm{S}}$$

The resulting capability distribution is:

$$R_{f\mathrm{SP}}(c_f) = R_{f\mathrm{S}} \oplus R_{f\mathrm{S}} \tag{33}$$
$$= r_{f\mathrm{S}}(0)^{2-c_f} - r_{f\mathrm{S}}(1)^{c_f} \binom{2}{c_f} \tag{34}$$
$$= (1-p_f^2)^{2-c_f} p_f^{2c_f} \binom{2}{c_f} \tag{35}$$

or as polynomials

$$R_{f\mathrm{SP}}(0) = 1 \tag{36}$$
$$R_{f\mathrm{SP}}(1) = 1 - 4q_f^2 + 4q_f^3 - q_f^4 \tag{37}$$
$$R_{f\mathrm{SP}}(2) = 1 - 4q_f + 6q_f^2 - 4q_f^3 + q_f^4 \quad . \tag{38}$$

Under the simplifying assumption $q_f \ll p_f$, this can be approximated as

$$R_{f\mathrm{SP}}(c_f) \approx 1 - (2q_f)^{2-c_f} \binom{2}{c_f} \quad . \tag{39}$$

6.2. **Force Capability of Parallel in Series.** The second example looks at the dual assembly: two elements are used in parallel, and two of these blocks are arranged in series. The only difference to the previous assembly is the addition of the cross connection at the middle of the actuator. Now the system can be divided into a top group and a bottom group. The force adds up in each group, but the force capability of the overall system is limited by the weakest group. This leads to the capability function

$$c_{f\mathrm{SP}}(\mathbf{c}_f) = \min\{c_{f\mathrm{top}}, c_{f\mathrm{bottom}}\} \tag{40}$$
$$= \min\{c_{f11} + c_{f12}, c_{f21} + c_{f22}\}\ . \tag{41}$$

For each group of two parallel elements, the Eqn. (20) applies. It leads to

$$R_{f\mathrm{P}}(c_f) = R_f = \sum_{i=c_f}^{2} q_f^{2-i} p_f^i \binom{2}{i} \quad .$$

Expanding the resulting polynomials produces

$$R_{f\mathrm{P}}(0) = 1$$
$$R_{f\mathrm{P}}(1) = 1 - q_f^2$$
$$R_{f\mathrm{P}}(2) = 1 - 2q_f + q_f^2$$
$$R_{f\mathrm{P}}(3) = 0 \quad .$$

The second step of the analysis is more complicated, because each group is now a multi-state system with three distinct capabilities. Consequently, the simple solution from Eqns. (10) and (11) cannot be used. Eqn. (24) has to be applied, which uses the operator $\circledast$ as defined in Eqn. (5). This leads to

$$R_{f\mathrm{PS}} = R_{f\mathrm{P}} \circledast R_{f\mathrm{P}} \tag{42}$$

or

$$R_{f\mathrm{PS}}(c_f) = R_{f\mathrm{P}}^2(c_f) \tag{43}$$

This leads to the polynomial solution

$$R_{f\mathrm{PS}}(0) = 1 \tag{44}$$
$$R_{f\mathrm{PS}}(1) = 1 - 2q_f^2 + q_f^4 \tag{45}$$
$$R_{f\mathrm{PS}}(2) = 1 - 4q_f + 6q_f^2 - 4q_f^3 + q_f^4 \quad . \tag{46}$$

The resulting equation (43) can also be simplified using the assumption $q_f \ll p_f$ to the approximation

$$R_{f\mathrm{PS}}(c_f) \approx 1 - 2q_f^{2-c_f} \binom{2}{c_f - 1} \quad .$$

The difference between both structures is found by comparing Eqn. (37) with Eqn. (45), as shown in Figure 7. All other reliability values are identical, but $R_{f\mathrm{SP}}(1) \neq R_{f\mathrm{PS}}(1)$ shows a noticeable difference. The parallel in series structure is superior by nearly a factor of two for low fault probabilities q_f.

The reason becomes obvious when multiple faults are classified into fatal ones (leading to a force capability of 0) and non-fatal ones (maintaining a force capability of 1). A multiple fault is fatal if it involves several elements that are working in parallel. Assuming that one fault has already occurred, it is interesting to analyse which further fault would be fatal. In the PS structure, this is only the one element directly in parallel, while a further fault in either element of the other serial group has no effect on the force capability.

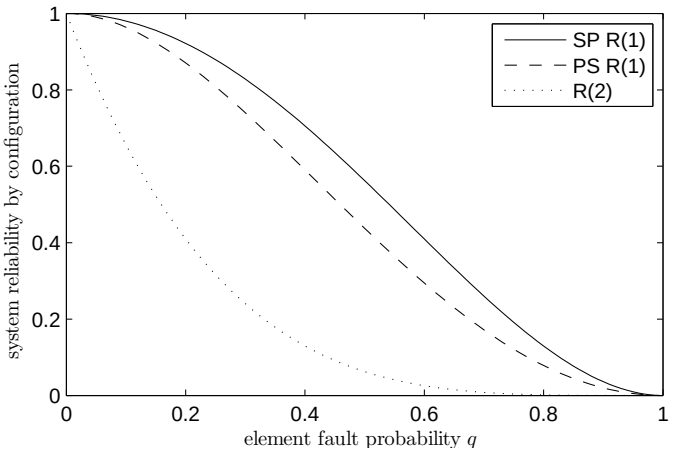


FIGURE 7. Reliability $R_{fx}(1)$ of 2×2 Configurations

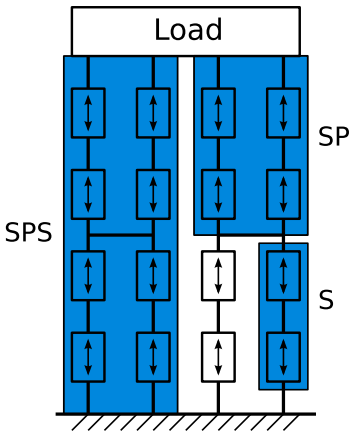


FIGURE 8. Hierarchy of the SPSP Configuration

However, in the SP structure, there are always two elements in parallel to the faulty element. A second fault in either of these reduces the force capability to 0.

6.3. **Extension to Higher Sizes.** The same considerations can be applied to any assembly that follows a series in parallel or parallel in series structure. A square system of n columns and m rows is a natural extension of the 2×2 arrangement considered above.

For the parallel in series system, the overall force capability is found to be

$$c_{f\mathrm{PS}}(\mathbf{c}_f) = \min_{i=1}^{m} \sum_{j=1}^{n} c_{f,ij} \quad . \tag{47}$$

The general form of the reliability is

$$R_{f\mathrm{PS}}(c_f) = \left(\sum_{i=c_f}^{n} (1-q_f)^{n-i} q_f^i \binom{n}{i} \right)^m \tag{48}$$

$$= \left(1 - \sum_{i=0}^{c_f-1} (1-q_f)^{n-i} q_f^i \binom{n}{i} \right)^m , \tag{49}$$

and a reasonable first order approximation is given by

$$R_{f\mathrm{PS}}(c_f) \approx 1 - m q_f^{n-c_f+1} \binom{n}{c_f - 1} \quad .$$

In a similar way, the overall force capability of a series in parallel system is

$$c_{f\mathrm{SP}}(\mathbf{c}_f) = \sum_{j=1}^{n} \min_{i=1}^{m} c_{f,ij} \quad . \tag{50}$$

This leads to a reliability function of

$$r_{f\mathrm{SP}}(c_f) = (1 - (1-q_f)^m)^{n-c_f} (1-q_f)^{m c_f} \binom{n}{c_f} ,$$

and a first order approximation of

$$R_{f\mathrm{SP}}(c_f) \approx 1 - (m q_f)^{n-c_f+1} \binom{n}{c_f - 1} \quad .$$

So the PS configuration is generally superior for when the force is relevant, and the SP configuration is superior for providing a required amount of travel or velocity. The difference between both configurations increases significantly as the requirements are reduced or the number of elements is increased.

When the travel or velocity is considered, the roles are interchanged between the SP and the PS configuration (and of course q_f is then the failure probability for lock-up faults):

$$\begin{aligned} R_{t\mathrm{PS}}(c_t) &\approx 1 - (m q_t)^{n-c_t+1} \binom{n}{c_t - 1} \\ R_{t\mathrm{SP}}(c_t) &\approx 1 - m q_f^{n-c_t+1} \binom{n}{c_t - 1} \quad . \end{aligned}$$

These equations together can also be used to find the ideal size $(n \times m)$ of an HRA. The four design parameters are the two numbers n, m representing the size as well as the required force capabilities c_f and c_t (determining the degree of redundancy). The strength required for each element can be calculated from these, as can the probability of an HRA failure due to force or travel capabilities below the requirements. Assuming that elements of any strength (force and travel) can be used, these four parameters are the main way of adjusting the reliability of the HRA, while minimising cost and weight. And even if the nominal strength is fixed, it is still possible to tune the number of essential elements required to deliver the capability (and therefore the number of redundant elements) to suit the reliability requirements.

6.4. 4×4 **Multi-Level Hierarchical Configurations.** A central aim of this paper is the analysis of hierarchical configurations with more than two levels, because they offer potentially superior overall reliability due to a better balance of fault modes. A simplifying assumption here is that each level combines two identical subsystems. Any 4×4 configuration therefore consists of four levels, two of which are series connections, while the other two parallel connections - the only difference is the order of aggregation. All six possible configurations are shown in Figure 12.

In the nominal state, all configurations are identical: both force and travel capability are four times the value of a single element. However, the response to faults differs significantly because of the existence or absence of lateral connections.

The use of fault trees for analysis an HRA leads to a number of issues. For the SSPP or PPSS configurations, it is possible to perform this analysis with a reasonably concise fault tree by introducing the (non-standard) k-out-of-n

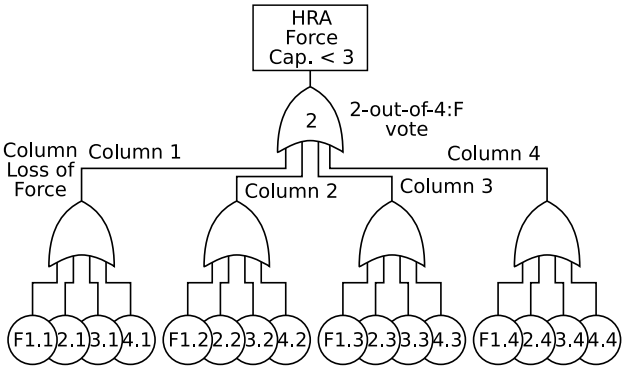


FIGURE 9. Fault Tree for the SSPP Configuration

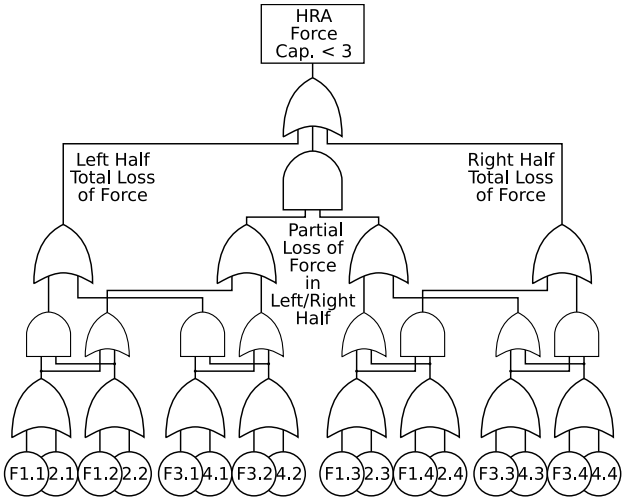


FIGURE 10. Fault Tree for the SPSP Configuration

gate as shown in Figure 9. The analysis of "mixed" configuration such as SPSP (see Figure 8) is more complicated, although it already uses shared signals subtrees to reduce the size. This means it is technically no longer a tree, and the number of cut sets can be much larger than the tree suggests. The basic problem is that most fault tree based methods cannot utilise the highly symmetrical structure to avoid repeated computation of symmetric subsystems. Our analysis also shows that two typical approximations are no longer justified: cut sets of more than the minimum size have to be considered because of their large number, and the probability of unaffected elements to be not at fault cannot be approximated as 1 without significant errors. All these issues mean that fault trees with binary signals are not a convenient way of analysing such systems.

A very simple graphical representation can be achieved by following the multi-state view of the system. The operators $\circledast$ and $\oplus$ introduced above in Eqns. (22) and (24) are used to describe the structure of the system. The resulting tree in Figure 11 could be interpreted as an extended fault tree, but it is important to realise that the connections do not represent events (binary variables), but the capability of a subsystem. Classical fault tree analysis is not able to deal with these, while a multi-state systems approach can.

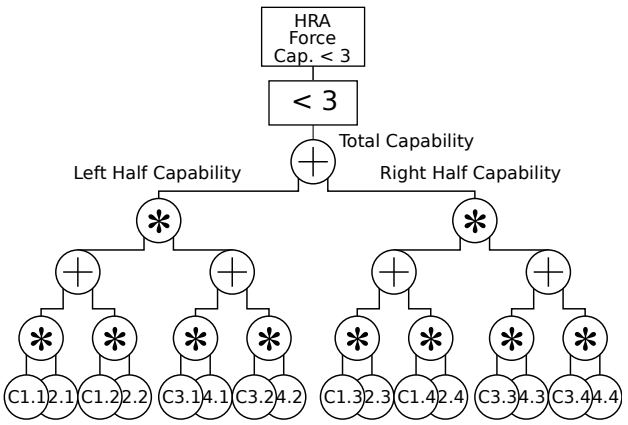


FIGURE 11. Fault Tree for the SPSP Configuration Using Multi-State Signals

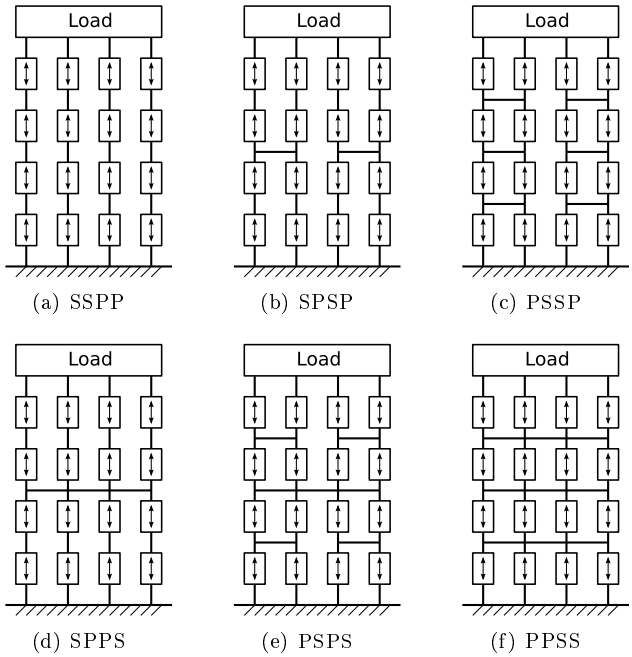


FIGURE 12. All Symmetrical Series-Parallel 4×4 Configurations

The same analysis is applied to all six configurations. Because of the textual length of the results, the two function are implemented in MATLAB using the symbolic toolbox. The reliability of a (sub)system is denoted using a vector

$$\mathbf{R}_f = (R_f(0)\ R_f(1)\ R_f(2)\ \cdots\ R_f(n))^T$$

of variable size, and the individual entries are polynomials in q_f.[2] The results are shortened by giving only the two relevant elements of this vector, and by omitting coefficients of little interest:

[2]The MATLAB symbolic toolbox has been used for the automatic manipulation of these polynomials. While MATLAB supports native functions for manipulating polynomials, these operate on vectors, and not first class polynomial objects. This makes it more difficult to represent the capability distributions.

$$
\begin{aligned}
R_{f\mathrm{SSPP}}(3) &= 1 - 24q_f^2 + 32q_f^3 + 204q_f^4 \ldots + 81q_f^{16} \\
R_{f\mathrm{SPSP}}(3) &= 1 - 40q_f^2 + 128q_f^3 + 220q_f^4 \ldots + q_f^{16} \\
R_{f\mathrm{PSSP}}(3) &= 1 - 48q_f^2 + 176q_f^3 + 276q_f^4 \ldots + 9q_f^{16} \\
R_{f\mathrm{SPPS}}(3) &= 1 - 72q_f^2 + 512q_f^3 - 1892q_f^4 \ldots + q_f^{16} \\
R_{f\mathrm{PSPS}}(3) &= 1 - 80q_f^2 + 592q_f^3 - 2228q_f^4 \ldots + q_f^{16} \\
R_{f\mathrm{PPSS}}(3) &= 1 - 96q_f^2 + 800q_f^3 - 3480q_f^4 \ldots - 3q_f^{16} \ ,
\end{aligned}
$$

and

$$
\begin{aligned}
R_{f\mathrm{SSPP}}(2) &= 1 - 16q_f^3 + 12q_f^4 + 96q_f^6 \ldots + 81q_f^{16} \\
R_{f\mathrm{SPSP}}(2) &= 1 - 32q_f^3 + 56q_f^4 - 16q_f^5 \ldots + q_f^{16} \\
R_{f\mathrm{PSSP}}(2) &= 1 - 64q_f^3 + 192q_f^4 - 240q_f^5 \ldots + 9q_f^{16} \\
R_{f\mathrm{SPPS}}(2) &= 1 - 64q_f^3 + 240q_f^4 - 352q_f^5 \ldots - q_f^{16} \\
R_{f\mathrm{PSPS}}(2) &= 1 - 128q_f^3 + 640q_f^4 - 1248q_f^5 \ldots - q_f^{16} \\
R_{f\mathrm{PPSS}}(2) &= 1 - 256q_f^3 + 1920q_f^4 - 7104q_f^5 \ldots + 3q_f^{16} \ .
\end{aligned}
$$

The results for $1 - R_f(3)$ (allowing one effective element fault) are plotted over the element fault probability q_f in Figure 13 on a linear scale. Note that the most interesting part is the area of low fault probability (close to 0) and high system reliability (close to 1), therefore the system *un*reliability $1 - R$ is shown. To highlight very small values, the same data is shown on a logarithmic scale in Figure 14. For comparison, the unreliability $1 - R_f(2)$ (up to two effective element faults) is plotted in Figure 15. A number of observations are interesting from the point of high redundancy actuation.

(1) All reliability functions have the same polynomial structure: they start at 1, the first non-constant term is a factor of q_f^2 for $R_f(2)$ and q_f^3 for $R_f(3)$, and they contain higher order terms up to q_f^{16}. This is a consequence of the basic requirements, which can be fulfilled in every configuration with zero or one faulty element.

(2) The reliabilities maintain a strict order over the configuration

$$
\begin{aligned}
&R_{f\mathrm{SSPP}}(3) > R_{f\mathrm{SPSP}}(3) > R_{f\mathrm{PSSP}}(3) \\
&> R_{f\mathrm{SPPS}}(3) > R_{f\mathrm{PSPS}}(3) > R_{f\mathrm{PPSS}}(3)
\end{aligned}
$$

for all $0 < q_f < 1$. So looking only at the force, some configurations are better than others, independent of the parameters. $R_f(2)$ only follows a partial order, because the relation between $R_{f\mathrm{PSSP}}(2)$ and $R_{f\mathrm{SPPS}}(2)$ depends on q_f.

(3) The reliability of travel ($R_t(3)$ and $R_t(2)$) follows the opposite order,

$$
\begin{aligned}
&R_{t\mathrm{SSPP}}(3) < R_{t\mathrm{SPSP}}(3) < R_{t\mathrm{PSSP}}(3) \\
&< R_{t\mathrm{SPPS}}(3) < R_{t\mathrm{PSPS}}(3) < R_{t\mathrm{PPSS}}(3)
\end{aligned}
$$

for all q_t because of the correspondence $R_{f\mathrm{SSPP}} = R_{t\mathrm{PPSS}}$ (for corresponding $q_t = q_f$) etc. So the conflict between reliable force and reliable travel is confirmed consistently.

Based on these results, it is possible to calculate the failure probability due to insufficient force and travel, and then select the best configuration for given reliability values q_t and q_f. Depending on the exact circumstances, any of the 6 configurations may be optimal.

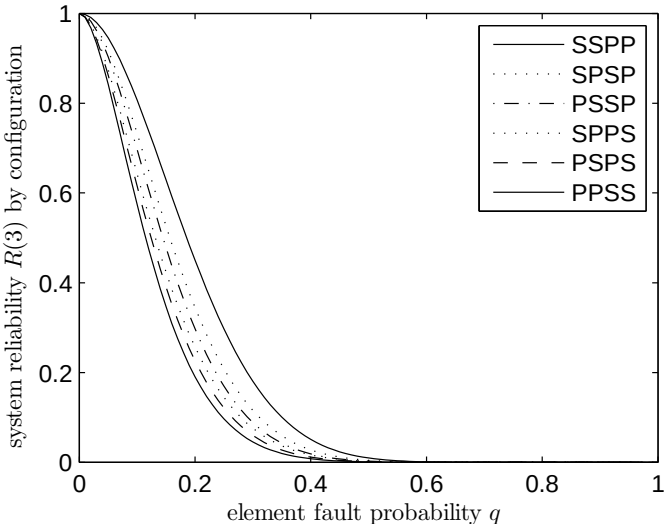


FIGURE 13. Unreliability $1 - R_{fx}(3)$ of 4×4 Configurations

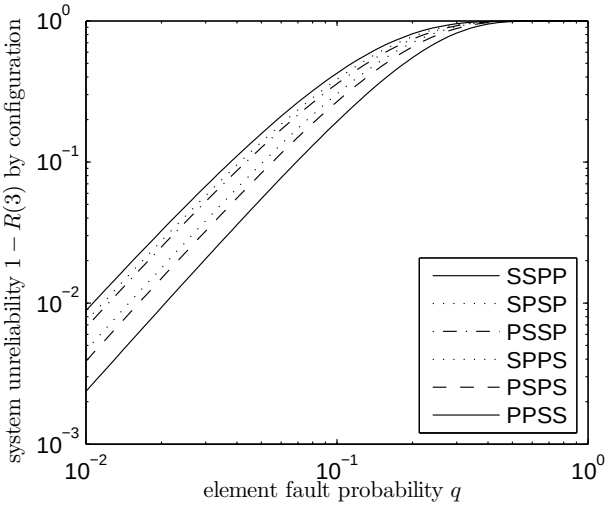


FIGURE 14. Unreliability $1 - R_{fx}(3)$ on a Logarithmic Scale

6.5. **Results Over Time.** Because the analysis so far is based on probabilities, time has not been considered. This can be changed by making the fault probability of each element time dependent. Example results are shown in Figure 16. The assumption is that each element fails with a constant rate of 1 fault every τ second (shown by the reference line), leading to $q_f(t) = 1 - e^{-t/\tau}$. Inserting this function into the polynomial $R_{fx}(3)$ leads to a combination of exponential functions describing the system reliability over time. The reliability of a single element $(1 - q_f)$ is also shown in the figure as 1×1 for comparison.

The advantage of this approach over methods working directly in the time domain (such as stochastic automatons) is the computational complexity. By calculating this result in two steps, the complexity of the time domain simulation is

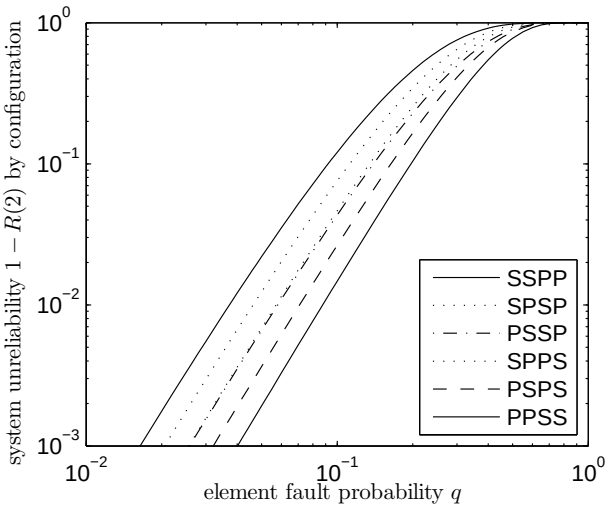


FIGURE 15. Unreliability $1 - R_{fx}(2)$ on a Logarithmic Scale

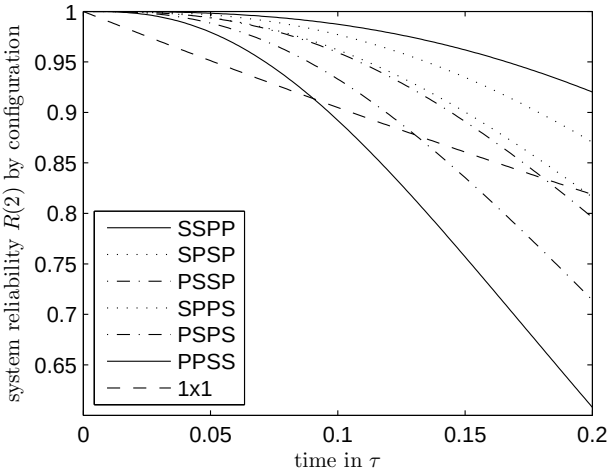


FIGURE 16. Unreliability $1 - R_{fx}(2)$ Over Time

minimal, because it only involves one element. The calculation of the system reliability is based on the approach shown above, and also bears a low computational complexity.

This separation is possible, because it is assumed that for the fault behaviour, the elements can be considered independent of each other. Even if this assumption is not exactly met, it is possible to work with a conservative approximation.

7. Selecting the Best Configuration

The original goal was to find the best configuration for a given task, and this section will show how the results can be used to compare different candidates and to identify the best one. Since there is a trade-off between robustness towards loss of force and robustness towards loss of travel, it is important to remember that both were treated separately only to simplify the analysis. Usually a system would be specified with a force requirement c_f and a travel requirement c_t. Both have to be met for a functional system. As long as both faults occur independently of each other, the

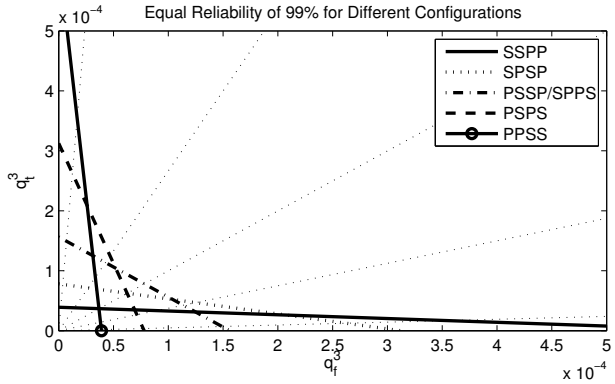


FIGURE 17. Comparison of Overall Reliability $R_x(2,2) = 0.99$

reliabilities can be multiplied to

$$R_{ftx}(c_f, c_t) = R_{fx}(c_f) R_{tx}(c_t) \quad .$$

However, since both faults are mutually exclusive in a single element, they are not completely independent. Therefore a safe (conservative) approximation is

$$R_{ftx}(c_f, c_t) \geq R_{fx}(c_f) + R_{tx}(c_t) - 1 \quad ,$$

which also has the advantage of producing less complex results.

For example the SSPP configuration leads to

$$\begin{aligned} R_{ft\mathrm{SSPP}}(2,2) &\geq R_{f\mathrm{SSPP}}(c_f) + R_{t\mathrm{SSPP}}(c_t) - 1 \\ &= 1 - 16q_f^3 + 12q_f^4 + 96q_f^6 \ldots + 81q_f^{16} \\ &\quad -256q_t^3 + 1920q_t^4 - 7104q_t^5 \ldots + 3q_t^{16} \quad . \end{aligned}$$

The dual configuration PPSS leads to a very similar result R_{PPSS}, but the places of q_f and q_t are interchanged. If only the highest order of q is considered, the following approximations are found:

$$\begin{aligned} R_{ft\mathrm{SSPP}}(2,2) &\geq 1 - 16q_f^3 - 256q_t^3 \\ R_{ft\mathrm{SPSP}}(2,2) &\geq 1 - 32q_f^3 - 128q_t^3 \\ R_{ft\mathrm{PSSP}}(2,2) &\geq 1 - 64q_f^3 - 64q_t^3 \\ R_{ft\mathrm{SPPS}}(2,2) &\geq 1 - 64q_f^3 - 64q_t^3 \\ R_{ft\mathrm{PSPS}}(2,2) &\geq 1 - 128q_f^3 - 32q_t^3 \\ R_{ft\mathrm{PPSS}}(2,2) &\geq 1 - 256q_f^3 - 16q_t^3 \quad . \end{aligned}$$

It depends on the ratio of $q_f^3 : q_t^3$ which value is the highest, and therefore which configuration provides the best reliability. This is graphically demonstrated in Figure 17. The lines denote combinations of q_f^3 and q_t^3 that lead to the same overall reliability of 99 %. The further right and up the line goes, the better the reliability of the configuration, as the system is less sensitive to the element faults. The different slopes represent different sensitivity to the two fault modes. The Pareto optimal solution contains parts of all five lines, which means that each configuration is the best choice for a certain ratio $q_f : q_t$ between the two fault modes. (This also holds for the exact reliabilities of the PSSP and SPPS configuration, although it is not obvious from the approximations used here.)

8. Computational Complexity

The main advantage of this approach is the very low computational complexity, compared to other methods that get prohibitively expensive even for moderate configuration sizes. This section will discuss the complexity in a bit more detail. Assuming a square configuration, the number of cooperating elements shall be n_1, and the number of limiting elements shall be n_2, giving a total of $n_1 n_2$ elements. The maximum capability in the system is given by n_1. It is further assumed that the structure is highly symmetric (as in the examples), and it follows that both n_1 and n_2 are powers of 2.

Each basic aggregation operation (as detailed in Theorems 6 and 7 using $\circledast$ and $\oplus$) can be performed in a linear number of basic arithmetic operations, depending on the maximum capability, so it is of complexity order $O(n_1)$. Due to the symmetric nature of the structure, each aggregation doubles the number of considered elements, so the number of required aggregations from a single element to the whole system is the dual logarithm of $n_1 n_2$ or $\log_2(n_1 n_2)$. This leads to an overall complexity of $O(n_1 \log_2 n_1 n_2)$ for determining the system reliability from a given set of fault probabilities. This complexity is so low that the computation can be performed many times to test different fault probabilities or configurations. Even systems of size 1000×1000 or more are still fast to analyse.

Structures without symmetries or broken symmetries would require further computations up to an order of $O(n_1 n_1 n_2)$. While this is still a low polynomial complexity, there is very little to gain from breaking the symmetry, and the number of configurations to analyse may explode exponentially. Hence it is not generally recommended.

Traditional methods have a much higher complexity which applied to the HRA, because a large number of faults has to be considered. Without optimisations, a fault tree analysis of the HRA involves $O(2^{n_1 n_2})$ combinations, which is prohibitive even for reasonably small systems such an 8×8 grid. Some optimisations are possible, but they do not avoid the basic problem of exponential complexity, which prevents the analysis of larger systems.

An event tree analysis would look at faults in the order of occurance. While this does increase the number of potential combinations, it also allows the elimination of significant parts of the event tree once the required capabilities are not longer met, since the order of faults is known. The resulting computational complexity is difficult to predict, because the number of faults that can be accommodated varies by fault location. It is bounded by n_1' and $n_1' n_2$, where n_1' is the number of cooperating elements required. This means the computational complexity is between $O\left(\frac{(n_1 n_2)!}{(n_1 n_2 - n_1')!}\right)$ and $O\left(\frac{(n_1 n_2)!}{((n_1 - n_1')n_2)!}\right)$, although further optimisations are possible in symmetric configurations. So this approach can be faster than the fault tree when the requirements are a significant part of the maximum capability. Again, it seems possible to study medium sized systems such as 8×8 with high capability requirements (≥ 6), but it quickly becomes prohibitively expensive above this number.

The conclusion is that the presented approach offers radically lower computational complexity than the alternatives, combined with a very simple implementation. This makes it especially suitable for the early design states, where the size of elements and their configuration is studied. Other, more accurate methods may still be useful for verification purposes.

9. Conclusions

This document has shown how to calculate the reliability of an HRA. Due to the high number of actuation elements, a new generic approach had to be developed. Using probability distributions, the problem can be solved with a low computational effort and using well understood operations. This is achieved by using a number of abstractions and approximating assumptions.

Different configurations consisting of several levels of series and parallel connections are considered and modelled using multi-state systems. Due to the approximations, the results may not represent the system in all detail, but they are still helpful for a sensible comparison between HRA designs. The results show that even with the same number of elements in the same two dimensional arrangement, the selection of the best suitable configuration (as determined by the lateral connections) has a significant influence on the reliability of the HRA. The influence is especially pronounced when high element fault rates have to be considered, as it is planned for the HRA.

The general concept of dual capabilities presented here is not restricted to actuation problems. It can be used in any domain where systems are used in parallel and serial arrangements to increase capabilities. This includes high power electronic switching devices, to transport networks and to communications systems. As long as the system can be interpreted as a hierarchy of series and parallel connections, and the independence requirements are satisfied, it is possible to analyse the reliability using the given operations on capability distributions. It would be interesting to pursue such an application to a different domain.

Acknowledgements

The HRA project is a cooperation of the Control Systems group at Loughborough University, the Systems Engineering and Innovation Centre (SEIC), and the actuator supplier SMAC Europe limited. The project was funded by the Engineering and Physical Sciences Research Council (EPSRC) of the UK under reference EP/D078350/1.

Contributors

Thomas Steffen was working on the High Redundancy Actuator project as a research associate in the control systems group of the Department of Electronic and Electrical Engineering. He has since started a lectureship in the Department of Aeronautical and Automotive Engineering, where he is a member of the Control and Reliability research group and the Loughborough Centre of Control Engineering. His research interests include fault tolerant control, model based control design,

the use of optimisation methods in control, stochastic models, and embedded programming. He is working on applications in the control of mechatronic systems, direct injection combustion engines, and aftertreatment systems.

Frank Schiller has been working as the Scientific Project Manager of the Safety and Security Division of Beckhoff Automation since March 2011. Prior to this he was professor for automation at the Technical University of Munich, Germany, where he continued his research on the field of safety and reliability started at Siemens Automation and Drives. His current special research areas comprise safety-related communication, software-based safety logic, secure fieldbus communication, and efficiently combined safety- and security approaches in automation. He holds a guest professorship at the East China University of Science and Technology, Shanghai, P.R. China.

Michael Blum has been working for exida.com GmbH as Senior Safety Engineer since May 2011, where he consults automotive companies on safety processes and concepts according to ISO 26262. His doctoral thesis about efficient safety analysis for mechatronical systems finished in 2010 was awarded by the Wittenstein prize. His current research is focused on generating Markov-models to calculate the safety characteristics of automotive and automation systems.

Roger Dixon spent several years at ALSTOM where he made significant R&D contributions in the areas of control of gasification plant, active vibration control, fault tolerant control of gas turbines and demonstration of novel electromechanical actuators for more-electric aircraft. He joined Loughborough in 2003 and is Head of the Control Systems research group in the School of Electronic Electrical and Systems Engineering. His research focuses on various aspects of control and systems engineering including: application of model-based control systems design, model-based fault detection and isolation, system condition/health monitoring and fault tolerant design of actuators and railway track switches. Roger is a Fellow of the Higher Education Academy, a registered Chartered Engineer and Fellow of the Institution of Mechanical Engineers.

References

Blanke, M., Kinnaert, M., Lunze, J., and Staroswiecki, M., *Diagnosis and fault-tolerant control*, Berlin: Springer (2006).

Blanke, M., Staroswiecki, M., and Wu, N.E. (2001), "Concepts and methods in fault-tolerant control," in *Proceedings of the American Control Conference '01*, Arlington, June, Vol. 4, pp. 2606–2620.

Blanke, M., and Thomsen, J.S. (2006), "Electrical steering of vehicles - fault-tolerant analysis and design," *Microelectronics and Reliability*, 46, 1421–1432.

Du, X., Dixon, R., Goodall, R.M., and Zolotas, A.C. (2006), "Assessment of Strategies for Control of High Redundancy Actuators," in *Proceedings of the ACTUATOR 2006*, Bremen, June.

Du, X., Dixon, R., Goodall, R.M., and Zolotas, A.C. (2007), "LQG Control for a High Redundancy Actuator," in *Proceedings of the 2007 IEEE/ASME International Conference on Advanced Intelligent Mechatronics*, Zurich, September.

Frank, P.M. (1990), "Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy- A survey and some new results," *Automatica*, 26(3), 459–474.

Heidergott, B., Olsder, G.J., and van der Woude, J., *Max Plus at Work: Modeling and Analysis of Synchronized Systems: A Course on Max-Plus Algebra and Its Applications*, Princeton University Press (2005).

Jenab, K., and Dhillon, B.S. (2006), "Assessment of reversible multi-state k-out-of-n:G/F/Load-Sharing systems with flow-graph models," *Reliability Engineering & System Safety*, 91(7), 765–771.

Jiang, B., Yang, H., and Shi, P. (2010), "Switching fault tolerant control design via global dissipativity," *International Journal of Systems Science*, 41(8), 1003–1012.

Oppenheimer, M.W., and Doman, D.B. (2006), "Control Allocation for Overactuated Systems," in *Proceedings of the 14th Mediteranean Conference on Control and Automation*, Ancona, June.

Pham, H., *Handbook Of Reliability Engineering*, Springer (2003).

Ribeiro, R.L.A., Jacobina, C.B., da Silva, E.R.C., and Lima, A.M.N. (2004), "Fault-tolerant voltage-fed PWM inverter AC motor drive systems," *IEEE Transactions on Industrial Electronics*, 51(2), 439–446.

Shammas, N.Y.A., Withanage, R., and Chamund, D. (2006), "Review of series and parallel connection of IGBTs," *IEE Proceedings Circuits, Devices and Systems*, 153, 34–39.

Steffen, T., *Control reconfiguration of dynamical systems: linear approaches and structural tests*, Lecture notes in control and information sciences (LNCIS), Berlin: Springer (2005).

Steffen, T., Davies, J., Dixon, R., Goodall, R.M., Pearson, J., and Zolotas, A.C. (2008), "Failure Modes and Probabilities of a High Redundancy Actuator," in *Proceedings of the 17th IFAC World Congress*, Seoul, July, pp. 3234–3239.

Steffen, T., Davies, J., Dixon, R., Goodall, R.M., and Zolotas, A.C. (2007), "Using a Series of Moving Coils as a High Redundancy Actuator," in *Proceedings of the 2007 IEEE/ASME International Conference on Advanced Intelligent Mechatronics*, Zurich, September.

Steffen, T., Schiller, F., Blum, M., and Dixon, R. (2009), "Increasing the Reliability of High Redundancy Actuators by Using Elements in Series and Parallel," in *Proceedings of the The 28th International Conference on Computer Safety, Reliability and Security SAFECOMP 2009*, eds. B. Buth, G. Rabe and T. Seyfarth, Hamburg, September, Springer, pp. 270–282.

Thomas Steffen, Control and Reliability Research Group, Department of Aeronautical and Automotive Engineering, Loughborough University, Loughborough, LE11 3SW, UK
URL: http://www.lboro.ac.uk/departments/aae/
E-mail address: t.steffen@lboro.ac.uk

Frank Schiller, Beckhoff Automation GmbH, Ostendstr. 196, D-90482 Nuremberg, Germany

Michael Blum, exida.com GmbH, Wildenholzener StraSSe 24, D-81671 Munich, Germany

Roger Dixon, Control Systems Group, Department of Electronic and Electrical Engineering, Loughborough University,, Loughborough, LE11 3SW, UK