Proceedings of the 17th World Congress
The International Federation of Automatic Control
Seoul, Korea, July 6-11, 2008

Failure Modes and Probabilities of a High Redundancy Actuator

Thomas Steffen * **Jessica Davies** * **Roger Dixon** *
Roger M Goodall * **John Pearson** ** **Argyrios Zolotas** *

* *Control Systems Group, Loughborough University, Loughborough LE11 3TU, UK, http://www.lboro.ac.uk/departments/el/research/scg/*
** *SEIC, BAE Systems, Holywell Park, Loughborough LE11 3TU, UK*
t.steffen, j.davies, r.dixon, r.m.goodall, j.t.pearson, a.c.zolotas@lboro.ac.uk

Abstract: A high redundancy actuator (HRA) is composed of a high number of actuation elements, increasing both the travel and the force over the power of an individual element. This provides inherent fault tolerance, because when an element fails, the capabilities of the actuator may be reduced, but it does not become dysfunctional. This paper analyses the likelihood of different reductions in capabilities, based on the reliability of the actuation elements used. The result is a probability distribution that quantifies the capability of the high redundancy actuator. Together with the required capabilities, this determines the fault tolerance of the actuator.

Keywords: high redundancy actuator, fault-tolerant control, fault accommodation, fault mode and effect analysis (FMEA), failure probability.

1. INTRODUCTION

1.1 Fault Tolerant Control

Fault tolerant control 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]. Whilst significant progress has been made for sensor faults, many results are not applicable to actuators. Because sensors are information systems, one sensor can be (nearly) as good as many sensors. Actuators however perform an energy conversion, and one actuation element alone may be too weak for the task.

Most existing approaches are based on the information view. For example, the observer based approach has been extended to cover actuator faults in the form of the virtual actuator [Steffen, 2005]. Likewise, the idea of analytical redundancies in sensors [Frank, 1990] has its equivalent for actuators in the form of dynamic gain scheduling and control allocation [Oppenheimer and Doman, 2006].

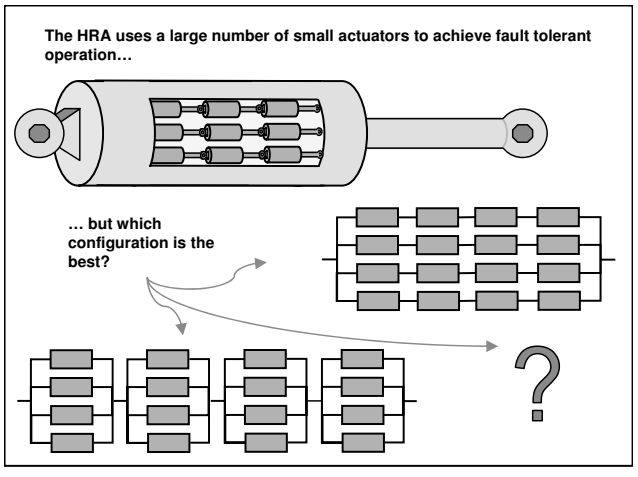

Figure 1. High Redundancy Actuator

The classical fault tolerant approach for actuation is replication: 2 or 3 actuators are used in parallel, much like redundant sensors. Each actuator is strong enough to meet the performance requirements by itself. This leads to a significant amount of over-engineering, and consequently a less efficient system (e.g. because of a higher weight).

1.2 High Redundancy Actuator

The obvious way to improve efficiency is to use a greater number of smaller actuation elements. For example, a system with ten elements may still work with only eight of them operational, and the overall capacity is only over-dimensioned by 25 %.

The idea of the High Redundancy Actuator (HRA) is to use a high number of small actuation elements 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 locks up. These faults will reduce the overall capability, but they do not render the assembly functionless. The goal is to take this into account during the design, and to maintain correct operation even if some elements are at fault.

So far, the 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 complicated 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].

This paper presents a method to analyse the reliability of a high redundancy actuator of any size, using parallel

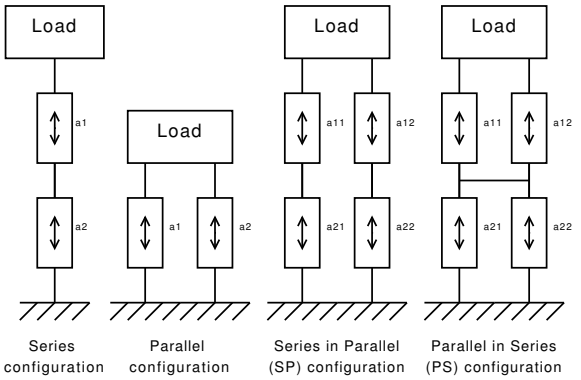

Figure 2. Basic Configuration

and series configurations. It is based on the concepts developed using graph theory in [Steffen et al., 2007a,b]. The new contribution of this paper is the determination of probabilities for the correct operation of the actuator.

2. QUANTIFYING RELIABILITY USING CAPABILITIES

2.1 Probabilities

The idea of this approach is to deduce the reliability of a high redundancy actuator from the reliability of the actuation elements used. Hence, the information on the reliability of an element is considered given. This paper assumes that the reliability of the elements is known in the form of probabilities at a certain point of time. [1]

2.2 Capabilities

A high redundancy actuator consists of many elements, and so it is possible that some of these elements are operational and some are faulty. In this situation, the actuator may still work, albeit with reduced performance. So the reliability of a high redundancy actuator depends on the required performance.

A way to capture this connection between performance and reliability was developed in [Steffen et al., 2007b]. The idea is to determine so called capabilities that describe the performance of the high redundancy actuator in terms of physical measures. For example, the force capability q can be conveniently specified in multiples of the force of an individual actuation element. Obviously using two elements in parallel creates an actuator that can produce twice the force, so the force capability is $q = 2$ (see Figure 2). And if one of the elements fail so that it cannot generate any force, the capability is reduced to $q = 1$. (If one element locks up, the whole set of element is rendered unusable, and series alternatives have to be found.)

The other important measure is the travel capability d, which states how far the actuator can move. Using several elements in series increases the travel capability. If an element gets stuck so that it cannot move, this reduces the travel capability. (It is assumed that the mass of each element is negligible compared to the load, so all elements have to provide the same force.)

[1] In practice, 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. The change of these probabilities over time can then be interpreted as any of the above measures.

Table 1. Duality of force and travel

Capability	Force	Travel	
Increased by	parallel	series	configuration
Unaffected by	series	parallel	configuration
Reduced by	loose	locked-up	element faults
Unaffected by	locked-up	loose	element faults

Force and travel capabilities follow similar laws, but for different configurations and faults. An overview of this is given in Table 1. Because of these symmetries, the force and travel capabilities can be considered to be dual.

2.3 Distributions

The reliability depends on the required capabilities, and thus both need to be considered together. The function showing the reliability over the required capability is called a capability distribution. This powerful statistical tool becomes very convenient with three simplifying assumptions:

- The capabilities are given in multiples of a single element. Therefore, the capability distribution is discrete, and not continuous.
- Only one capability is considered at a time. This is possible because the force and travel capability are independent: the loss of one does not affect the other.
- From a fault perspective, the elements are independent: the capability of one does not correlate to the capability of another. This means the one fault only affects a single element. Common mode faults cannot be analysed using this method.

After these simplifications, the distribution can be specified by calculating the probabilities for a number of discrete capability values. An example is shown in Figure 3. This distribution would be written as

	n	0	1	2
Distribution	$P(c = n)$	0.01	0.09	0.9
Cumulative values	$P(c \leq n)$	0.01	0.1	1

where c denotes a generic capability.

2.4 Specifying the Elements

Usually, the reliability of an element is specified by giving probabilities for the different fault cases. However, to be

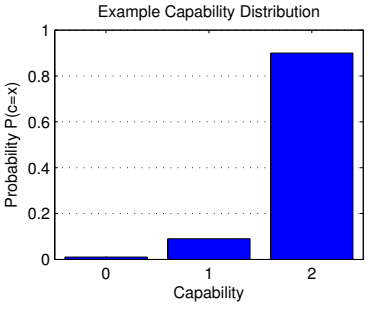

Figure 3. Example of a Capability Distribution

consistent with the further processing, this paper will assume that every element is specified by a probability distribution over the possible capabilities. For example, if an element has a 10 % chance of producing no force, the force capability distribution is

$$P(c=0)=0.1$$
$$P(c=1)=0.9 \quad .$$

3. BASIC AGGREGATION

The idea of the high redundancy actuator is that several actuation elements are used together to perform a common function or meet an overall requirement. Depending on how the elements are connected, different capabilities can result. For example, a serial connection increases the travel compared to what a single element can achieve alone, but it does not change the maximum force.

To study the influence on the connection in detail, it is assumed that n elements with the capabilities $c_1, c_2, \ldots, c_n$ are being used together. To simplify the analysis, only one capability is considered at a time (either force or travel). It is further assumed that the capability distribution is known for each element.

3.1 Additive Capabilities

When several actuation elements are used together, this increases certain capabilities above the level of an individual element. For example, two elements in parallel can produce twice the force. This means that the individual capabilities add up to the capability of the system:

$$c_{add} = c_1 + c_2 + \ldots + c_n \quad . \tag{1}$$

From a fault tolerant perspective, this is a very resilient arrangement. Because a fault only affects one element, it can reduce the capability of the system only by the amount contributed by this element. This is called graceful degradation, and it is an desirable property for many fault tolerant applications.

The probability distribution of different capabilities can be determined by summing up the joint probabilities of all the combinations leading to the same system capability. This is done with the following equation:

$$P(c_{add}=i) = \sum_{c_1,\ldots,c_n} \begin{cases} \prod_j P(c_j) & \text{if } \sum_j c_j = i \\ 0 & \text{otherwise} \end{cases} \quad . \tag{2}$$

If two elements or subsystems are combined, this operation is a convolution of the capability distributions:

$$P(c_{add}=i) = \sum_{j=0}^{i} P(c_1=j)P(c_2=i-j) \quad . \tag{3}$$

The convolution can also be used to combine more than two distributions by applying it repeatedly. This reduces the computational complexity significantly compared to the multi-dimensional sum above. Because the addition is a commutative operation, the convolutions can be applied in any order, without changing the end result.

For expressing the same convolution in terms of cumulative probabilities, the following replacement can be used:

$$P(c_{add}<i) = \sum_{j=0}^{i} P(c_2 \le i-j)P(c_1=j) \quad .$$

If all n elements are identical and have only two distinct capabilities, the resulting distribution is a binomial distribution. Assuming that each element has a probability a of no capability, and a probability b of capability 1, the distribution of an individual element is

$$P(c=0)=a \tag{4}$$
$$P(c=1)=b=1-a \quad . \tag{5}$$

The binomial distribution for the system is given by:

$$P(c_{add}=i) = a^{n-i}b^i \binom{n}{i} = a^{n-i}b^i \frac{n!}{i!(n-i)!} \quad . \tag{6}$$

For most practical cases, it can be assumed that the probability of a fault is small compared to the probability of normal operation $a \ll b \approx 1$. This leads to a binomial distribution with a strong skew, which can be approximated by neglecting the factor b:

$$P(c_{add}=i) = a^{n-i}b^i \binom{n}{i} \approx a^{n-1} \binom{n}{i} \quad . \tag{7}$$

Note that this is an over-approximation, so for the purpose of determining the failure probability is it always on the safe side. The cumulative probability for a capability below i becomes:

$$P(c_{add}<i) = \sum_{j=0}^{i-1} a^{n-j}b^j \binom{n}{j} \tag{8}$$
$$\approx \sum_{j=0}^{i-1} a^{n-j} \binom{n}{j} \approx a^{n-i+1} \binom{n}{i-1} \quad .$$

Note that the second approximation is not conservative, because it underestimates the probability of a failure. So it should be tested on a case by cases basis. If applicable, this simple result turns out to be very useful for the comparison of different configurations.

3.2 Limiting Capabilities

Some capabilities do not add up when subsystems are combined. Instead, the capability of the resulting system is determined by the capability of the weakest part. This happens for example with the force capability q when actuation elements are used in series.

The capability of such a combined system is the minimum capability over all the subsystems or elements:

$$c_{lim} = \min\{c_1, \ldots, c_n\} \quad . \tag{9}$$

So the probability of a certain system capability depends on a high number of capability combinations. All combinations are relevant where one element has exactly the

desired system capability, and all other elements have the same or higher capabilities.

$$P(c_{lim}=i)=\sum_{c_1,\ldots,c_n}\begin{cases}\prod_j P(c_j) & \text{if } \min_j c_j=i\\ 0 & \text{otherwise}\end{cases} \quad (10)$$

The calculation becomes significantly easier when cumulative probabilities are used:

$$P(c_{lim}\geq i)=\prod_j P(c_j\geq i) \quad (11)$$

$$P(c_{lim}<i)=1-\prod_j(1-P(c_j<i)) \quad . \quad (12)$$

With n elements, each having a probability a of no capability, and a probability b of capability 1, this results in the following distribution:

$$P(c_{lim}=0)=\sum_{i=0}^{n-1}a^{(n-i)}b^i\frac{n!}{i!(n-i)!} \quad (13)$$

$$=1-b^n=1-(1-a)^n \quad (14)$$

$$P(c_{lim}=1)=b^n=(1-a)^n \quad . \quad (15)$$

Using the same assumption as before ($a \ll b$), this distribution can be approximated as

$$P(c_{lim}=0)\approx na \quad (16)$$

$$P(c_{lim}=1)\approx 1-na \quad . \quad (17)$$

For more complicated distribution, the following approximation usually holds:

$$P(c_{lim}<i)=1-\prod_j(1-P(c_j<i)) \quad (18)$$

$$\approx\sum_j P(c_j=i-1) \quad . \quad (19)$$

This is based on the assumptions $P(c=i)\ll P(c=i+1)\ll 1$, which should hold for typical systems with $a \ll b$.

3.3 Multiple Levels of Aggregation

For most practical purposes, a high redundancy actuator will contain elements in series and in parallel. Thus it is important to analyse the capability distribution of these aggregations on multiple levels.

Such a system can be analysed using a bottom-up analysis. 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. By repeatedly applying this operation, the capability distributions of bigger and bigger subsystems can be constructed, until finally the distribution for the whole system is derived.

To perform this iterative approach, the actuator configuration needs to be described as a series-parallel network. This is possible if the actuator can be broken down into series and parallel configurations of subsystems, until the level of individual actuation elements is reached.

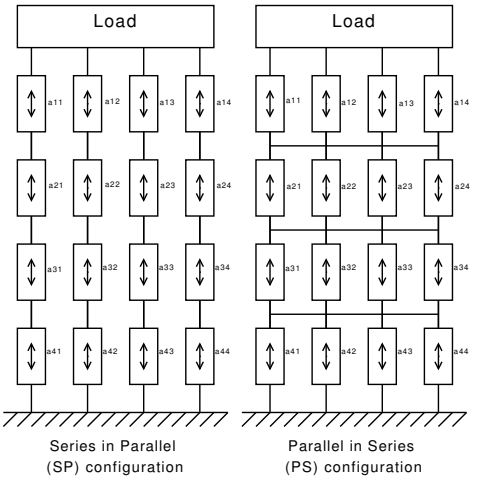

Figure 4. 4x4 Configurations: SP and PS

4. GRID CONFIGURATIONS

Two possible grid configurations are shown in Figure 4. For example, a high redundancy actuator may consist of n actuation elements in series, used m times in parallel. This is called the SP configuration, as shown on the left side of Figure 4. Let the force capabilities of the elements in the first subsystem be $q_{11},\ldots q_{n1}$, the capabilities of the second $q_{12},\ldots,q_{n2}$, up until the last subsystem $q_{1m},\ldots,q_{nm}$. In the deterministic case, the force capability of the overall system is the sum of the capabilities of the columns, which are each limited by the weakest element. This leads to:

$$q_{SP}=q_{col1}+q_{col2}+\ldots+q_{colm}=\sum_{i=1}^{m}\min_{j=1}^{n}q_{ji}\,. \quad (20)$$

The capability distribution for one column needs to be determined first (bottom-up). Applying the results of Section 3.2 to this system leads to:

$$P(q_{col}=0)=1-b^n,\ P(q_{col}=1)=b^n \quad . \quad (21)$$

In the next step, the capability of the whole actuator is deduced. This is straight forward, because the distribution of the subsystem contains only two different capabilities (0 and 1). Equation (6) can be used, if b is replaced with b^n, and a is replaced with $1-b^n$, to represent the increased probability of one of the subsystems failing. The result is:

$$P(q_{SP}=i)=(1-b^n)^{m-i}(b^n)^i\binom{m}{i} \quad . \quad (22)$$

Under the simplifying assumption $a \ll b$, this probability can be approximated as

$$P(q_{SP}=i)\approx(na)^{m-i}\binom{m}{i} \quad . \quad (23)$$

The travel can also be analysed using the same approach. In the deterministic case, the travel of the overall system is limited by the travel capabilities of each subsystem:

$$d_{SP}=\min\{d_{col1},d_{col2},\ldots,d_{colm}\}=\min_{i=1}^{m}\sum_{j=1}^{n}d_{ji}\ . \quad (24)$$

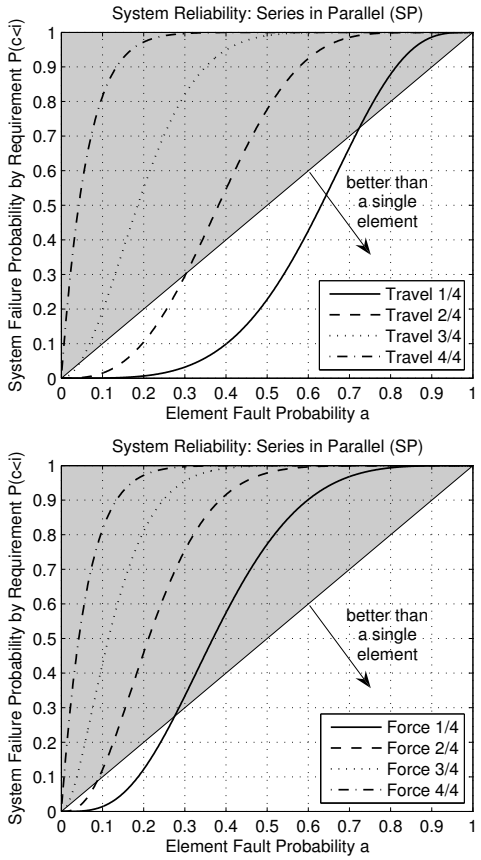

Figure 5. Reliability of the 4x4 SP configuration

The travel of the elements in each column is additive, so it follows the laws given in Section 3.1. The resulting capability distribution is given in equation (6). For reasons explained below, the cumulative form given in (8) is used.

The second step of the analysis is more complicated, because the subsystems have five distinct possible travel capabilities. Consequently, the simple solution from equations (14) and (15) cannot be used. Instead, it is necessary to perform the operation defined in equation (12). Combining (12) with (8) leads to:

$$P(d_{SP} < i) = 1 - \prod_{j=1}^{m} \left(1 - \sum_{k=0}^{i-1} a^{n-k} b^k \binom{n}{k} \right) \quad (25)$$

$$= 1 - \left(1 - \sum_{k=0}^{i-1} a^{n-k} b^k \binom{n}{k} \right)^m \quad . \quad (26)$$

The resulting equation (26) can be simplified using the assumption $a \ll b$. This leads to:

$$P(d_{SP} < i) \approx 1 - \left(1 - a^{n-i+1} \binom{n}{i-1} \right)^m$$

$$\approx m(a^{n-i+1}) \binom{n}{i-1}$$

and therefore:

$$P(d_{SP} = i) \approx m(a^{n-i}) \binom{n}{i} \quad . \quad (27)$$

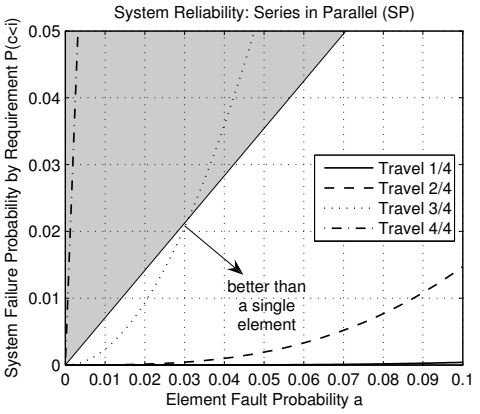

Figure 6. Reliability for low fault rates

Compared to equation (23), the only difference apart from the transposition of n and m is a factor of m^{n-i-1}. They produce identical results if the probability of a single fault in a square configuration is considered.

The same analysis can be applied to a high redundancy actuator with m parallel elements, used n times in series. In this configuration, the force is calculated as

$$q_{PS} = \min_{i=1}^{m} \sum_{j=1}^{n} q_{ij} \quad (28)$$

and the travel is determined by

$$d_{PS} = \sum_{i=1}^{m} \min_{j=1}^{n} d_{ij} \quad . \quad (29)$$

Essentially, the roles of force and travel are reversed. This is not surprising, as travel and force are dual capabilities, just as parallel and series are dual configurations. Consequently, the capability distributions are also reversed:

$$P(d_{PS} = i) \approx (ma)^{n-i} \binom{n}{i} \quad (30)$$

$$P(q_{PS} = i) \approx n(a^{m-i}) \binom{m}{i} \quad . \quad (31)$$

Comparing these equations with (23) and (27) reveals the advantages and disadvantages of both configurations. The parallel in series configuration (PS) has a low failure probability for a given force, while the series in parallel configuration (SP) is more likely to meet a certain travel requirement. The difference between both configurations increases as the requirements are reduced (or with the number of faults).

5. QUANTITATIVE EXAMPLES

The general results derived above can be used to analyse two specific high redundancy actuators in 4x4 configuration (as shown in Figure 4). One actuator uses four series elements in four parallel columns (SP), leading to the results shown in Figure 5. Since lower failure probabilities are preferable, it follows that this configuration deals better with loss of travel faults (lock-up) than with loss of force faults (loose).

Table 2. Availability with travel faults (SP)

Element	Availability in % by travel requirement			
avail.	1/4	2/4	3/4	4/4
90	99.96	98	80	20
99	99.999 996	99.998	99.8	80
99.9	99.999 999 999 6	99.999 998	99.998	98
99.99	$100 - 4\,10^{-14}$	$100 - 2\,10^{-9}$	99.999 98	99.8

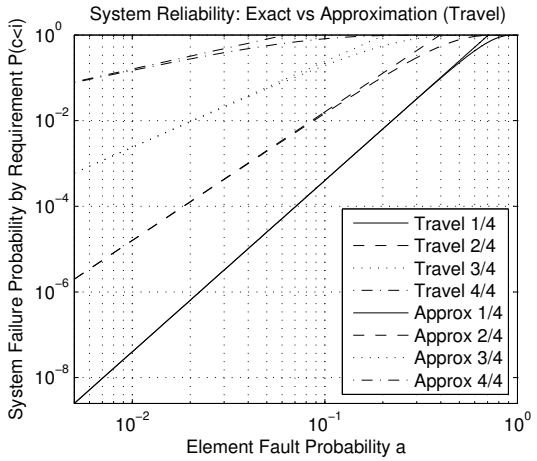

Figure 7. Approximation of travel reliability (27)

For the parallel in series configuration (PS), the results are exactly reversed: the PS configuration has the same response to loss of travel (lock-up) faults as the SP configuration has to loss of force (loose) faults, and vice versa. Just as force and travel are dual variables in relation to the energy flow, the two configurations are dual with respect to their reliability. So the PS configuration is preferable when the force capability is critical.

The improvement of the high redundancy actuator over a non-redundant configuration increases with lower fault probabilities. This is evident in Figure 6, which shows the failure probability due to loss of travel faults for the SP configuration at fault rates up to 1 %. A comparison between the exact failure probabilities and the over-approximations according to Equation (27) is shown in Figure 7 using a double logarithmic scale. For fault and failure probabilities around 1 %, the approximations (straight lines) are very accurate, but from 10 % on they become increasingly conservative.

As stated in Section 2.1, the probabilities can be interpreted in a number of ways. For example, they can be converted into the availability figures shown in Table 2 (assuming maintenance does not affect the availability).

6. CONCLUSIONS

This document has shown how to calculate the reliability of a high redundancy actuator. Due to the high number of actuation elements, a new approach needed to be developed to achieve this. Using probability distributions, the problem can be solved with a low computational effort, and using well understood operations.

The results show that the selection of the best suitable configuration has a significant influence on the reliability of the high redundancy actuator. By starting with subsystems of parallel elements, the actuator can be made more resilient against loss of force faults, as other elements can easily take over the load. On the other hand, building on elements in series is superior in the case of loss of travel (lock-up) faults.

Further studies are required to investigate more complex configurations. It is also interesting to consider the dynamical behaviour, as defined by robustness, gain margin, speed or accuracy. However, since these are not simple physical variables, but properties of a controlled system, the treatment is necessarily much more involved.

7. ACKNOWLEDGEMENTS

This 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 is funded by the Engineering and Physical Sciences Research Council (EPSRC) of the UK under reference EP/D078350/1.

REFERENCES

M. Blanke and J. S. Thomsen. Electrical steering of vehicles - fault-tolerant analysis and design. microelectronics reliability. volume 46, pages 1421–1432, 2006.

M. Blanke, M. Staroswiecki, and N. E. Wu. Concepts and methods in fault-tolerant control. In *Proceedings of the American Control Conference '01*, volume 4, 2001.

M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki. *Diagnosis and fault-tolerant control*. Springer New York, Germany, 2006.

X. Du, R. Dixon, R. M. Goodall, and A. C. Zolotas. Assessment of strategies for control of high redundancy actuators. In *Proceedings of the ACTUATOR 2006*, 2006.

X. Du, R. Dixon, R. M. Goodall, and A. C. Zolotas. Lqg control for a high redundancy actuator. In *Proceedings of the 2007 IEEE/ASME International Conference on Advanced Intelligent Mechatronics*, 2007.

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

M. W. Oppenheimer and D. B. Doman. Control allocation for overactuated systems. In *Proceedings of the 14th Mediteranean Conference on Control Automation*, June 2006.

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

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

T. Steffen, J. Davies, R. Dixon, R. M. Goodall, and A. C. Zolotas. Using a series of moving coils as a high redundancy actuator. In *Proceedings of the 2007 IEEE/ASME International Conference on Advanced Intelligent Mechatronics*, 2007a.

T. Steffen, R. Dixon, R. M. Goodall, and A. C. Zolotas. Quantifying the fault-tolerance of a high redundancy actuator assembly. *Mechatronics–The Science of Intelligent Machines*, 2007b. submitted.