Loughborough
University

This item was submitted to Loughborough's Institutional Repository (https://dspace.lboro.ac.uk/) by the author and is made available under the following Creative Commons Licence conditions.

For the full text of this licence, please go to:
http://creativecommons.org/licenses/by-nc-nd/2.5/

HRA - Intrinsically fault tolerant actuation through high redundancy

R. Dixon*, T. Steffen*, J. Davies*, R.M. Goodall*
A.C. Zolotas* J. Pearson** X. Du***

* 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
*** Aston University, Aston Triangle, Birmingham, B4 7ET, UK

Abstract: The aim of this paper is to summarise on-going research into a new method of providing fault tolerant actuators for high-integrity and/or safety-critical applications. The High Redundancy Actuator (HRA) project aims to exploit a large number of very small actuation elements to make up a single large actuator. This is in contrast to current technology where a relatively low level of functional redundancy is used. The HRA elements are configured and controlled in such a way that faults in individual elements are inherently accommodated without resulting in a failure of the complete actuation system. The HRA project research challenges are outlined and progress to-date is discussed.

1. INTRODUCTION

Unexpected faults can cost companies large sums of money and in extremis can lead to loss of life. In response, modern engineering applications demand high levels of availability and reliability. Fault tolerant control is about dealing with faults in technical systems (Blanke et al., 2006) and fault tolerant systems, which are capable of tolerating component malfunctions whilst still maintaining desirable and robust performance and stability properties (Patton et al., 1997), offer a solution to the availability/reliability problem.

1.1 Conventional Fault Tolerance

The majority of research to date has concentrated on sensor and system faults, with less emphasis upon the actuators. This is attributable to the fundamental differences between actuators and sensors. Sensors deal with information, and measurements may be processed or replicated analytically to provide fault tolerance. However, actuators must deal with energy conversion, and as a result actuator redundancy is essential if fault tolerance is to be achieved in the presence of actuator faults. Actuation force will always be required to keep the system in control and bring it to the desired state. No approach can avoid this fundamental requirement.

The common solution (see e.g., Pratt 2000) is to use some form of over-actuation in which the fault-free system has more control action than needed. This is usually achieved by straightforward replication of the actuators, e.g. 3 or 4 actuators are often used in parallel for aircraft flight control systems. In this approach, each actuator must be capable of performing the task alone and possibly of overriding the other faulty actuators. This over-engineering incurs penalties as cost and weight are increased and subsequently efficiency is reduced. It also cannot deal easily with lock-up (fail-fixed) faults.
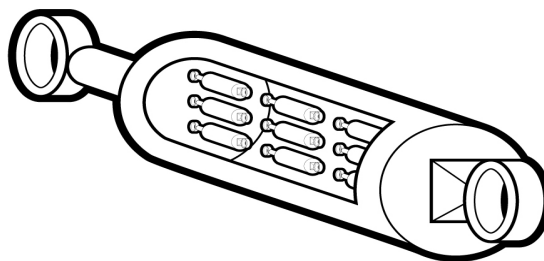

Fig. 1. The HRA concept

1.2 The High Redundancy Actuation Approach

The High Redundancy Actuator (HRA) concept is a fundamentally different approach to actuator fault tolerance, inspired by biomimetics. A muscle is composed of many individual muscle cells, each of which provides a minute contribution to the force and the travel of the muscle. These properties allow the muscle, as a whole, to be highly resilient to individual cell damage. The HRA project aims to use the same principle of cooperation to provide intrinsic fault tolerance. To achieve this, a high number of small actuator elements are assembled in parallel and in series to form one highly redundant actuator (see Figure 1). Faults within the actuator will affect the maximum capability, but through robust control full performance can be maintained without either adaptation or reconfiguration. The intention is that by careful design for specific applications it should be possible to provide actuators that gracefully degrade, and that continue to operate at the desired level of performance in the presence of multiple faults in the actuator elements. Moreover, through the appropriate integration of health monitoring methods it should be possible for the actuator to identify that it is getting close to performance limits by giving an online 'fitness' assessment (e.g., 90% capability).

1.3. Potential Benefits & Research Challenges

Three significant benefits of the HRA approach have been identified:

improved availability: it can do its job when asked and will warn maintainers when it starts to approach a critical level of faults;

improved efficiency: in terms of actuator sizing (over sizing) for fault tolerance;

graceful degradation: if fault levels exceed the critical point, system failure will not be sudden and unexpected.

However, it is not clear-cut that the high-redundancy actuation approach can provide an effective and appropriate engineering solution, principally because it involves significant complexity (in the actuator and associated control system) to provide the required redundancy. Possibly this is why the approach has not been considered seriously before, but modern control design and real-time processing capabilities now make its feasibility more likely.

The main challenges identified fall in the areas of actuator design and configuration, control, health monitoring, demonstration (case studies) and identifying suitable technologies for the HRA. All but the latter are being addressed by the current project, and progress in each area will be summarised in sections 2-6.

2. CONFIGURATIONS AND DESIGN METHODS

Compared with a conventional fault tolerant actuation approach it is clear that the HRA improves efficiency by using 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% (as compared to 100% or 200% for conventional duplex or triplex redundancy). However, for any given application, it is not immediately clear how many elements will be needed and in what configuration they should be in order to meet particular performance and reliability specifications. Weight and size constraints further complicate the design. The basic configuration variants being considered in the project are shown in Figure 2.

Two recent developments that can help the design process are: the notion of *capability* and the use of this in a probabilistic framework in order to calculate actuator *reliability*. These are discussed briefly below.

2.1 Capability & Reliability

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. Hence, the reliability of a high redundancy actuator depends on the required performance. A way to capture this connection between performance and reliability was introduced in (Steffen et al., 2008) and is further developed in (Steffen et al., 2009).
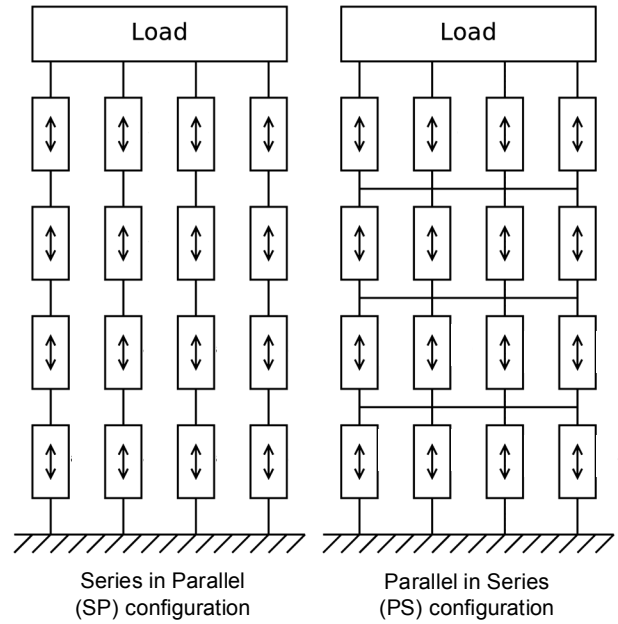
Fig. 2. Two basic 4x4 HRA configurations

The idea is to determine "capabilities" that describe the performance of the high redundancy actuator in terms of physical measures. For example, the force capability q, can be 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. 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, both elements are 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. The force and travel capabilities follow similar laws, but for different configurations and faults, as shown in Table 1. The fault modes are considered to be independent of one another, so that the capabilities can be analysed one at a time.

Table 1. The duality of force and distance

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

The actuator reliability depends on all required capabilities, and thus they need to be considered together. The function showing the reliability for a required capability is called a capability distribution. This statistical tool is able to efficiently assess different designs of HRA against a given reliability requirement. The detailed method for generation of the capability distributions is given in (Steffen et al. 2008). In sum, using probability distributions, the problem can be solved with a low computational effort, and using well understood operations.

2.2 Reliability Examples

Application of the proposed reliability to the 4x4 Series in Parallel (SP) configuration of Figure 2 yields two sets of results. for travel and force (Figure 3). Clearly, this configuration deals better with lock-up faults (loss of travel) than with loose faults. The corresponding results for a Parallel in Series (PS) configuration are identical, except that the capabilities are reversed.
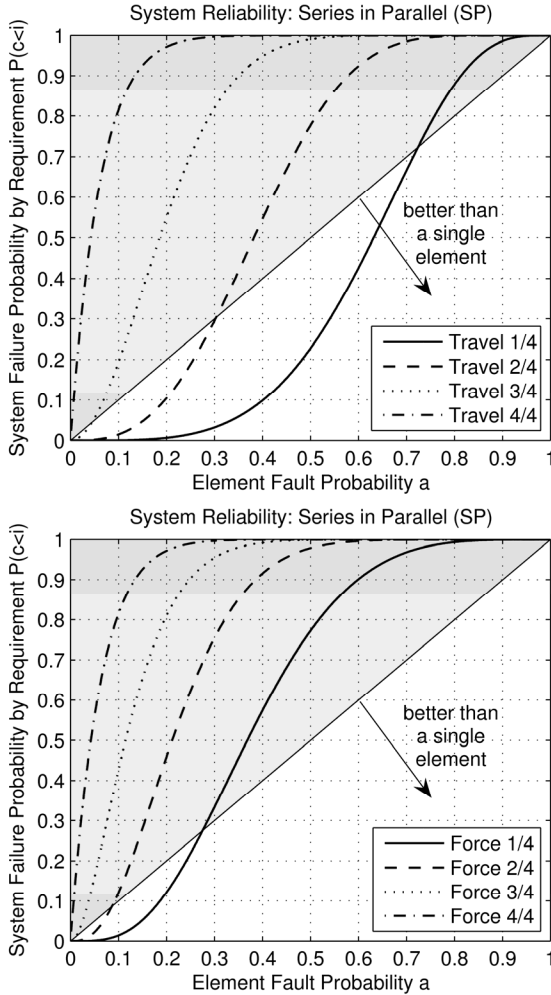

Fig. 3 Graphs showing the probability of the HRA failing to reach the desired capability level vs the probability of a single element fault (top – for distance capability, bottom – for force capability).

In the above analysis, the area of most interest is the bottom left corner (i.e. engineers generally chose reasonably reliable elements, with a low probability of fault). Figure 4 shows the results having zoomed into this area (for travel). It is clear that for requirements in terms of capability at levels of one, two or three out of four the HRA is doing better than a single equivalent large actuator. The results also show that the selection of the configuration has a significant influence on the reliability of the high redundancy actuator and that the optimal configuration for a given problem can be found by comparing the graphs. 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 up the load.

On the other hand, building on elements in series is superior in the case of loss of travel (lock-up) faults.
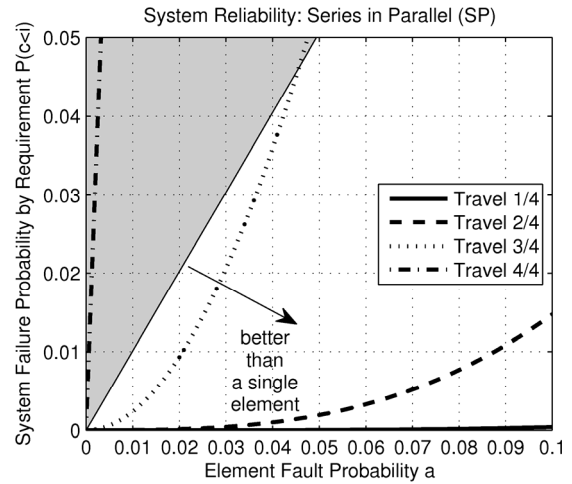

Fig. 4 Close-up of Fig. 3 (bottom), bottom left corner

3. CONTROL CHALLENGES

There are many open questions associated with control of an HRA. For example, is it possible to control such an array of actuators? If so, how? Can a robust approach be used or is reconfiguration necessary? Finally, if model-based control is to be utilised, how does the designer cope with the very high order control models concomitant with the HRA approach?

In Section 3.1, the modelling and model reduction approaches used will be summarised and recommendations made. Experimental results for control of a 2x2 electro-mechanical HRA will be presented and discussed in Section 3.2, demonstrating that classical approaches can be used successfully to control a HRA. Finally, in Section 3.3, the trade-offs between passive fault tolerance (robust control) and active fault tolerance (reconfiguration) will be discussed using results from a simulation of a 4x4 electromagnetic HRA.

3.1 HRA Model Complexity

HRA model complexity presents a real problem for model-based control approaches (see e.g., Du et al., 2007). For example a $n \times m$ HRA with 3-states for each element would have at least $3 \times n \times m$ states. Such high-order models lead to controllers that are difficult to design and implement. Moreover, due to the repeated dynamics of each sub-actuator element, there can be uncontrollable and unobservable subspaces, further complicating the controller design. There are three main ways to deal with the complexity of the system.

1. Small changes are introduced into the model parameters. This removes the repeated dynamics and resulting controllability issues but it does not change the model-complexity issue.
2. Model reduction (either using physical understanding or formal mathematical methods such as *Balanced Truncation*) addresses both the model-complexity and repeated dynamics.

3. A design method can be used that focuses on the element level, such as decentralised control design. An example would be use of a Multi-Agent System (MAS) inspired controller as will be considered in Section 3.3.

The latter two approaches have been found to work well in practice and are used in the designs discussed below.

3.2 Experimental Results for a 2x2 HRA

Experiments have been conducted to determine the effect of three types of fault on the 2x2 HRA shown in Figure 5.
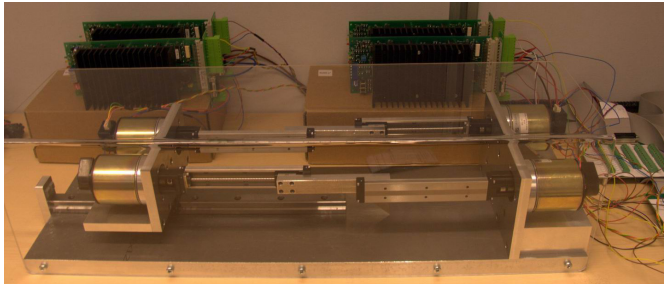

Fig. 5 Side view of the experimental HRA (at full extension)

Two different control designs were considered – in order to see how significant the control structure (classical approach) is to the degree of passive fault tolerance. Figure 6 shows the two control structures applied and figure 7 shows a typical set of step responses in the fault-free case and with three types of fault (motor open and closed circuit faults, plus lock-up).
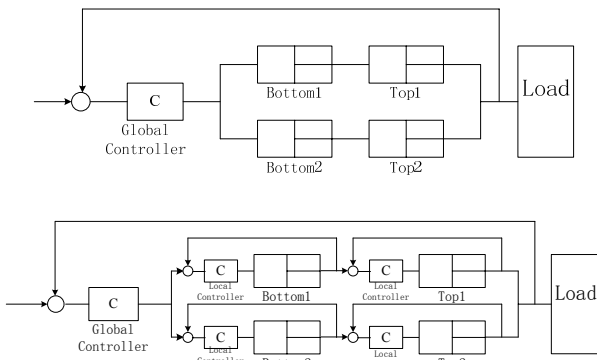

Fig. 6. Control structure of a single global position controller (top) and of both global and local current controllers (bottom)

It can be seen from Figure 7 that the control scheme results in zero tracking-error in steady-state (due to the integral action). This is the case for both schemes. It is the rise time and settling time that are most affected by the faults. Hence, the tables and figures in Figure 8 quantify the degradation in step response by analysing the change in rise time and settling time in percentage terms relative to the fault free case. This allows comparison of the two different control schemes described earlier. In both cases, it can be concluded that the lockup fault has the strongest effect on the HRA performance and it is clear that the structure with inner-loop current controllers is affected less than the simpler voltage driven system in terms of its settling time, whereas the rise time effects are similar with both control structures.
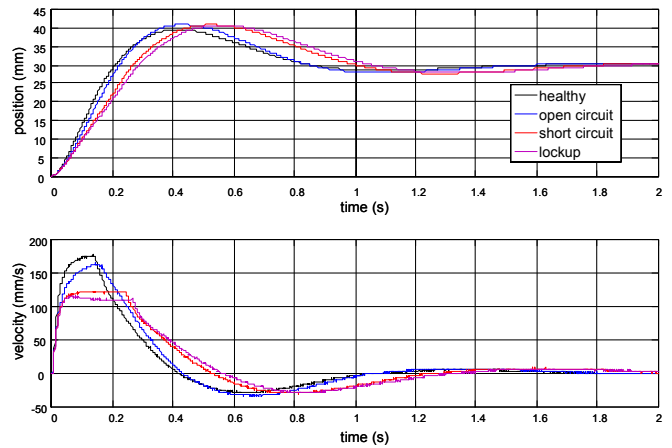

Fig. 7. Typical step responses – showing degradation due to faults

	Voltage Driven	Current Driven
Healthy	0.18	0.18
Open Circuit	0.2	0.22
Short Circuit	0.24	0.27
Lock-up	0.26	0.28

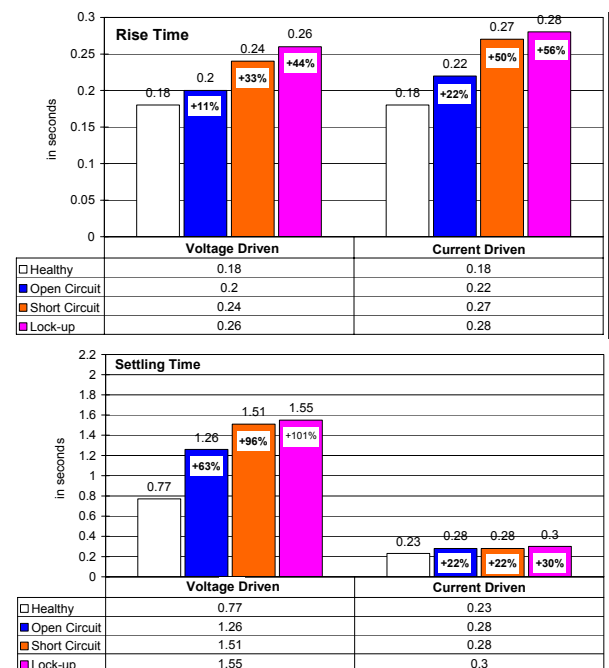|	Voltage Driven	Current Driven
Healthy	0.77	0.23
Open Circuit	1.26	0.28
Short Circuit	1.51	0.28
Lock-up	1.55	0.3

Fig. 8. Performance degradation, in terms of the rise and settling time, after three kinds of fault are injected.

The results summarised above were obtained using the controllers described in (Du et al. 2008) and, along with other results on LQG control (see Du 2008), they demonstrate the feasibility of the HRA approach for improving system fault tolerance without the need for reconfiguration.

3.3 Passive versus Active Control with Electromagnetic HRA

In this section results obtained from a simulation of an electro-magnetic HRA are presented. The aim is to obtain an indication of the possible benefits available from using reconfiguration. The HRA to be controlled, comprising 16 elements, is shown in Figure 9.

Two controllers are considered, one passive and one active. *Passive* fault tolerance is attained using a robust controller, designed using H_∞ loop shaping, which reduces the influence of element faults on the closed-loop behaviour. This approach can lead to high order controllers, but in this case it is

straightforward to reduce the controller to two states, without a significant loss in performance. The *active* approach uses a Multi-Agent System to control, detect faults and reconfigure the control laws accordingly. This Multi-Agent Control (MAC) scheme can be thought of as allowing local multiple-model control and fault detection on an individual element level. Full details of the HRA simulation model and both control approaches can be found in (Davies et al 2009a).

The structure and level of complexity in the two controllers is starkly different. The robust passive controller is simple. After the state reduction it takes the form of a single PI plus phase advance (PA) compensator acting on the global load position error, and the single control input signal, u, is fed directly to each of the 16 elements of the HRA.
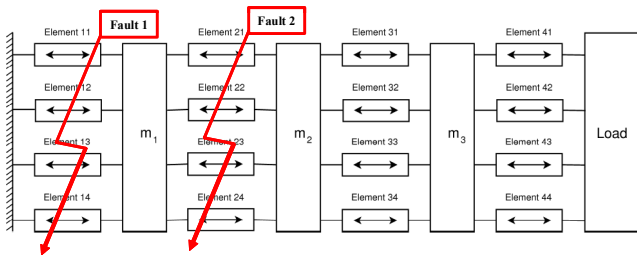

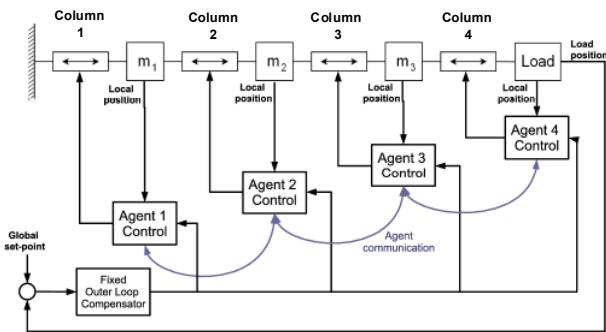Fig 9. 4x4 Parallel in Series HRA, including location of lock-up faults.

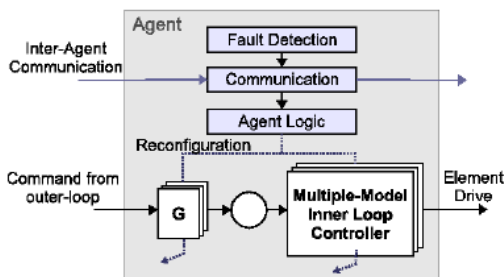Fig 10. Multi-Agent Control and monitoring scheme.

Fig 11. Agent architecture.

In contrast, the MAC scheme has four agents each of which controls and monitors one of the four parallel columns of actuators (as shown in Figure 10). These all receive their local set-points from a global PI+PA controller. As indicated by Figure 11, each agent has a set of four multiple model controllers and set-point scaling factors which are applied based on the communicated current fault status of the HRA.

The most severe fault case is known to be lock-up (see results in Section 3.2). Hence, both controllers are tested with two levels of lock-up – i.e, lock-up of the entire first parallel connection, then in the second parallel connection (as shown in Figure 9). The step response results with both controllers are compared in Figure 12.
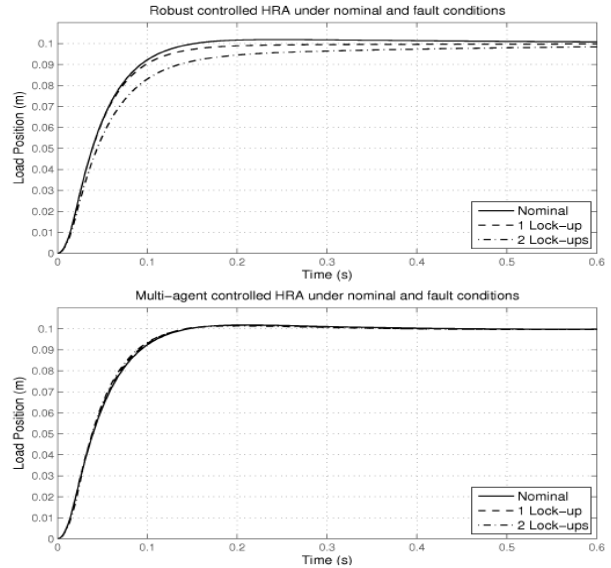

Fig 12. Step response of robust controlled and multi-agent controlled HRA in the fault free case and after one and two lock-up faults.

The results show that both the robust control and the MAC approaches provide fault tolerance to lock-up faults within a HRA. The robust control is simple to implement, however there is a slight difference in closed loop behaviour between the performance under nominal and one fault conditions. This deviation may be tolerable in a real application. However, in the case of two lock-up faults, the difference in the closed loop behaviour becomes more pronounced, and may not be acceptable. For the MAC it can be seen that nominal behaviour can be restored after faults have occurred (within the mechanical limits of the system). However, this advantage is gained in exchange for reliance on fault detection and a more complex control structure.

4. MONITORING

A key feature of the HRA concept is that failures in individual elements can be inherently accommodated without the need for explicit fault detection, isolation and reconfiguration. However, in order to ensure that a HRA can be replaced/repaired as the degraded performance gets close to a critical capability level, it is essential to have some form of health monitoring. There are two approaches being considered to provide this.

Monitoring of individual sub-actuator elements: development of detection methods for specific faults within the individual actuator elements. Within a MAC framework simple rule-based methods can be used to assess that an element is working or not, as used in the approach discussed in Section 3.3 (see also, Davies et al 2009a). Or for greater insight of the faults a multiple model approach could be used

(see Davies et al 2009b). Alternatively the outputs and inputs can be collected during experiments and system identification approaches can be used (see e.g. Dixon & Pike 2002) to detect changes in the physical parameters of the sub-actuators. Each of these areas is being explored.

Overall health monitoring: What is actually needed is a quantitative measure for the available performance capability. This can be deduced from the number of identified faults in the system (i.e. building on the approaches discussed above). Alternatively, instead of looking at the individual elements, it is also possible to observe the overall system, and directly assign a "health level". This might be based on parameter estimation for a simplified model similar to that of an individual actuator.

6. CONCLUSIONS & FUTURE WORK

6.1 Current Status – Design, Control & Monitoring

Configuration/design methods: tools for analysing the configurations in terms of *capability* and *reliability* have been developed. These were discussed and demonstrated in section 2 and provide a means to evaluate HRA configurations in order to meet specified levels of capability and reliability. These tools facilitate the outline design of HRA structures.

Control: one of the key difficulties for control is the *model complexity*. This can be dealt with by design of controllers for each element (breaking down the problem – as in the MAS approach), or by producing a reduced order model on which to base a single design. It has been demonstrated that an HRA can be controlled using *passive* approaches; that is, by relying on robustness in a fixed controller to deal with the faults in sub-actuator elements. However, it has also been shown that post-fault performance can be improved (or maintained close to nominal levels) if an *active* approach is permitted. The benefits come at the cost of increased complexity – which may be undesirable in many safety critical applications. The next steps in this area are to extend the experimental results to a 4x4 lab-scale actuator and to test in simulation at very high element levels (>100). The results will then need to be aggregated to provide design rules/processes for HRA designers.

Monitoring: work in this area is still in its early stages. Results have been found using simple rules and a MAS approach, but as in the control case the complexity and additional sensors may render this less attractive than other approaches (possibly data-based) at the HRA-level. It is clear that monitoring will be critical to the overall HRA concept.

6.2 Future – Demonstration, Case Studies & Technology

In order to demonstrate the above concepts in an experimental context the project has already developed a 2x2 electro-mechanical demonstrator (Figure 5). At the time of writing a 4x4 electromagnetic HRA is being designed using elements from SMAC – it is intended that simulated operational loads will be applied to this HRA via an electromechanical loading system. The final element of the demonstration will be a simulator that can emulate very high levels of HRA elements (>100).

Once the capability, reliability, control and monitoring approaches are all in place, it will be necessary to apply them to realistic engineering examples - in order to demonstrate the efficacy of the HRA approach. Three case studies have been identified for this: a rail-vehicle tilt actuator, a flight surface actuator and an inlet guide vane actuator (for aero gas turbines). The experimental results and the output of the case studies will be discussed in future papers.

Once the outcomes described above are in place. The authors anticipate that the viability of the HRA as a concept will have been proven. Beyond this, the main challenge will be in looking for serious applications and identifying suitable technologies from which to develop and manufacture the actuators. Of course, this will open up new technology-specific issues.

7. REFERENCES

Blanke, M., M. Kinnaert, J. Lunze, and M. Staroswiecki, (2006) Diagnosis and Fault-Tolerant Control, *Second Edition, Springer.*

Davies, J., H. Tsunashima, R. Goodall, R. Dixon, & T. Steffen, (2009a) Active Versus Passive Fault Tolerant Control of a High Redundancy Actuator, *to be published in proc. of ECC 2009.*

Davies, J., T. Steffen, R. Dixon, R. Goodall, & A.C. Zolotas, (2009b) Fault Detection in High Redundancy Actuation Using an Interacting Multiple-Model Approach, *to be published in proc. of SafeProcess 2009.*

Dixon, R. and A.W. Pike, (2002) Application of condition monitoring to an electro-mechanical actuator: a parameter estimation based approach, *Computing & Control Engineering Journal, IEE*, **132**, pp 71-81.

Du, X., (2008) High Redundancy Actuator, Ch 6., *PhD Thesis, Loughborough University, UK*

Du X.,, R. Dixon, R. M. Goodall, T. Steffen, (2008) Validation of a Two by Two High Redundancy Actuator - Experimental Results, *Proc Actuator'08, Hanseatische VeranstaLtungs-GmbH, Bremen Germany, June 2008*

Du, X., R. Dixon, R.M. Goodall, & A.C. Zolotas, (2007) LQG control for a high redundancy actuator, Proc of the 2007 IEEE/ASME Int. Conf. on Advanced Intelligent Mechatronics.

Patton, R.J., (1997) "Fault Tolerant Control: The 1997 Situation," SAFE-PROCESS'97, IFAC Symposium on fault detection, supervision and safety, Hull, U.K.

Pratt, R.W., (2000) Flight Control Systems – Practical Issues in Design and implementation, *TJ International*, ISBN 0852967667.

Steffen, T., J. Davies, R. Dixon, R.M. Goodall, J. Pearson and A.C. Zolotas, (2008) Failure modes and probabilities of a high redundancy actuator. *17th IFAC World Congress, July 6-11, Seoul, Korea*

Steffen, T., F. Schiller, M. Blum and R. Dixon, (2009) Increasing Reliability by Means of Efficient Configurations for High Redundancy Actuators. *to be published in proc. of SafeProcess 2009.*