Reactor Operation, Control and Instrumentation

1. Developing advanced control and instrumentation to improve the standards in safeguards, security and safety to maintain public confidence

As civilisation advances, society will continue to demand ever higher levels of safety for humans and protection for the environment from all industrial activity, particularly nuclear. It will also require a continual upgrading of the security against a terrorist strike and of the safeguards provided to stop the diversion of nuclear material to provide the charge for a nuclear weapon.

Providing the public with the desired reassurance on nuclear safeguards, security and safety will require the integrated, multi-disciplinary efforts of scientists, engineers and managers to give the necessary protection and provide the basis for accurate reporting by the media. It is the same informational basis that can then be used by politicians to make a truthful and valid case.

One important component in this integrated effort is the development of advanced control and instrumentation systems so that the whole nuclear process can be monitored and controlled to close tolerances. This will involve the development of new instrumentation techniques and the integration of measurements from a wide range of instruments measuring diverse parameters so as to assemble a reliable and truthful picture of what is going on in every part of the process. It will involve improved modelling and the extension of control engineering techniques to improve the detection of faults and of deliberate mal-operation such as the deliberate diversion of nuclear material. Control in whatever form can then be activitated, whether trip, building close-down, area isolation or bringing in security forces.

A key feature will be the application of ever increasing computing power so that a highly accurate, dynamic picture of every part of the nuclear fuel chain can be given in real time at every moment of the day or night. This will give transparency to the operators and managers on the grand scale.

It is fortunate that some elements of the control and instrumentation expertise that are necessary for this vision already exist in the UK, but substantial research and development are still needed nevertheless to bring the level of monitoring and control technology up to the standard needed to answer all the questions that the member of public could reasonably ask. This is the Grand Challenge.

2. Development of procedures for safety certification of embedded firmware

The majority of nuclear reactors throughout the world were conceived, designed, constructed and commissioned at a time when information and communication technologies were not sufficiently capable to have a significant role in reactor control & protection. The recent revolution in ICT ubiquity in the last 10 years has changed all of this, with the desire not only to exploit the benefits of this technology in reactor control & protection for a whole host of good reasons, but also the very real issue that OEMs now supply components that might have hidden ICT systems in them. Therefore the assessment of these systems is needed if the risk they pose to reactor control and protection is to be adequately assessed and catered for. Recent delays in the Gen 3+ construction projects associated with this

(Flamanville and Olkiluoto) and the detailed assessment and concern of the Office for Nuclear Regulation in part of the Generic Design Assessment for both EPR and the AP1000 supports this view.

Embedded firmware would 'normally' be assessed for safety certification by assessing the scale of the risk and then designing a statistical basis via which to infer the probabilistic scale of the vulnerability, experimentally. In a simple example, this might involve testing the response of a safety-critical system such as an ABS brake system by repeatedly visiting on it the full spectrum of scenarios that might realistically arise and then assessing the statistical performance. This cannot be done with a reactor since it would a) involve tests on many reactor systems that would be prohibitively expensive and b) the risk of failure cannot be countenanced. However, the tide of embedded firmware for reactor control & protection is unstoppable and offers significant benefits.

Therefore, substantial research and development activities need to be established if we are to learn how to and review the performance of techniques to assess and certify embedded firmware; we rely on its use day-to-day in high-speed transport and medical applications, and thus there's no reason which we should not be able to in the generation of nuclear power. This is the Grand Challenge.

3. Operator Training: Human-Systems Interactions

Despite the emphasis on failsafe systems and intrinsically safe designs, the operation of nuclear plant inevitably involves the actions of human operators. Decisions are made throughout normal operation according to safety guidelines, demand and an understanding of the reactor operation.

Historically, the actions of operators have also had significant ramifications in accidents. These are usually stressful situations where decisions are made under great pressure. Indeed, both Chernobyl and Fukushima demonstrated the catastrophic consequences of poor interactions between operators and plant.

The grand challenge here is to develop and refine our understanding of how operators respond to these situations in particular, and how best the systems could be adapted to take this into account. As a direct result of such understanding, operator training schemes could be improved to avoid possibly dangerous consequences.

4. Developing effective procedures for plant modification and introduction of new technologies

Nuclear power plants have an expectation of operational lifetimes of several decades. Much technology, especially (but not exclusively) that involving control and instrumentation has a very much shorter design and implementation cycle. Over the lifetime of a plant, a great deal of new technology will surely be developed, much of which could be highly beneficial to a given reactor.

The naturally risk averse approach of the regulator makes the adoption of new (and potentially safer and more effective) technology into extant designs extremely problematic. The result is that the genuine benefits that could be realised by incorporating new technology are lost. Indeed, modest concerns over implementation risk can overrule the introduction of technologies that could greatly reduce operational risk overall.

This is principally a procedural problem, which has no obvious solution. Indeed, it is very much a grand challenge. Put simply, what are the most effective procedures for the modification of plant in the light of technological advancement?