UK Nuclear Safety Cases: Towards a Unified Approach

Chris Brookes-Mann, Director, SEABORN MONK LTD, Mottram House, 43 Greek Street, Stockport SK3 8AX

Risk assessments are familiar to virtually everyone in industry, and every risk assessment follows the same basic principles (i.e. identifying potential hazards, assessing the risks they pose, developing measures to control the risks, reviewing the measures periodically to ensure continued compliance and relevance). Some sectors and operations are covered by Approved Codes of Practice (ACOPs) published by the Health and Safety Executive (HSE) or by industry bodies, and these assist operating companies by setting out how systems should be designed, how operations should be performed, and what protective measures should be in place. This is an effective approach in instances where there are numerous plants or items of equipment all performing broadly similar functions and posing broadly similar hazards.

Nuclear licensed sites in the United Kingdom (UK) fall within the scope of the Nuclear Installations Act, and are issued with nuclear site licences by the Office for Nuclear Regulation (ONR). A nuclear site licence carries 36 Licence Conditions (LCs) which cover everything from marking the site boundary to the disposal of nuclear waste. This paper focuses on one in particular – LC14 – which covers the safety documentation that must be in place and approved by HSE before a Site Licence Company (SLC) is allowed to operate a nuclear facility. All the different pieces of safety documentation are known collectively as 'the safety case', and despite there being more than a dozen SLCs registered in the UK, there is no ACOP for nuclear safety cases meaning that there is a range of (subtly different) sets of procedures for producing a safety case to meet LC14. In respect of Nuclear Power Plants (NPPs), all existing NPPs in the UK were built either for the United Kingdom Atomic Energy Authority (UKAEA) or the Central Electricity Generating Board (CEGB), and so effectively all had the same customer: the government. This will not be the case for the new NPPs currently being designed and starting construction. Therefore the need for an ACOP would seem to be greater than ever, to ensure consistency in the application of safety standards.

Although ONR produces a specification for risk assessment and safety engineering of nuclear facilities (known as the Safety Assessment Principles or SAPs), each SLC has its own interpretation of the SAPs that informs its procedures. The aim of this paper is to strip away the differences, and by introducing the fundamental processes that underpin UK nuclear safety cases in this manner it is hoped that the paper will prompt discussion on whether there is merit in creating a safety case ACOP for the nuclear industry for the benefit of all SLCs (not just NPPs), and whether it would have the potential to centralise development of nuclear safety case processes under the auspices of HSE or potentially a body such as the Nuclear Industry Association.

Keywords: nuclear, safety case, new build, site licence company, approved code of practice

Introduction

Unlike the nineteen Nuclear Power Plants (NPPs) built in the twentieth century in the United Kingdom (UK), the ones currently being designed and starting construction in the UK will be operated by private companies from the outset. Furthermore, each private company will use a different type of reactor rather than the previous situation which – other than a small number of exceptions – involved a single design being rolled out across the country (Magnox) followed by a successor based on similar principles (Advanced Gas-cooled Reactor, AGR).

The current regulatory framework for nuclear licensed sites is based around the Nuclear Installations Act 1965 (NIA65) which was introduced to consolidate two earlier Acts as the UK's fleet of nuclear reactors expanded and switched priority from supporting atomic weapon production to the generation of electricity. NIA65 stipulates a number of Licence Conditions (LCs) which Site Licence Companies (SLCs) must observe, and one of these – LC14 – requires SLCs to produce and maintain a safety case which must demonstrate that all radiological risks associated with the licensed site are As Low As Reasonably Practicable (ALARP). An LC14 safety case is therefore a risk assessment like any other required under the Health and Safety at Work Act 1974 (HSW), but one which focuses on the radiological risk (i.e. from radioactive materials) to workers and the public. LC14 safety cases are unusual – but not unique – amongst risk assessments in that they often need to be notified to or even approved by the specialist nuclear branch of the UK Health and Safety Executive (HSE) before the facility can be built.

At the time NIA65 was introduced – and for more than thirty years afterwards – the UK nuclear industry was in public hands, and as a result there was arguably no real need to produce an Approved Code of Practice (ACOP) describing how LC14 should be met since SLCs and their regulator were both public sector organisations and therefore could be viewed as two separate but related branches of government. Having said this, the UK's nuclear regulator – currently known as the Office for Nuclear Regulation (ONR) – has been producing an extensive specification document called the Safety Assessment Principles (SAPs) since 1979, which describes in detail the regulatory expectations relating to risk assessment and safety engineering. The SAPs have always been non-prescriptive, and SLCs are required to develop their own engineering and risk assessment procedures to comply with the SAPs.

There is certainly some merit in the ONR continuing its arm's length regulatory approach from the point of view of requiring SLCs to truly understand their risk assessment and safety engineering procedures rather than just ticking boxes. This is presumably the reasoning behind a number of the Fundamental Principles (FPs) given in the SAPs, particularly SAP FP.4 which states, '*Dutyholders must demonstrate effective understanding and control of the hazards posed by a site or facility through a comprehensive and systematic process of safety assessment.*' Furthermore, any facility with the potential to exceed public dose limits in the event of a radiation accident must have its safety case approved by ONR, which effectively gives retrospective regulatory endorsement to an SLC's risk assessment and safety engineering procedures without the procedures themselves necessarily having been seen by ONR.

On the other hand, it is noticeable that the risk assessment and safety engineering procedures of established SLCs tend to be developed by reference to internal good practice that has come from having experience of submitting multiple safety cases for approval. SLCs with less mature procedures on the other hand generally carry out risk assessment and safety engineering by direct interpretation of regulatory guidance documents published by ONR and other similar bodies. It could be said that this is comparable to trying to pass one's driving test with just a copy of The Highway Code for assistance: it might be possible to do it that way, but the chances of passing first time are certainly diminished.

The Key Principles for Nuclear Safety

With this driving test analogy in mind, the SAPs give the following principles as key for nuclear safety, similar to the 'General Advice' rules in The Highway Code:

1. The underpinning safety aim for any nuclear facility should be an inherently safe design, consistent with the operational purposes of the facility.
2. The sensitivity of the facility to potential faults should be minimised.
3. Nuclear facilities should be designed and operated so that defence in depth against potentially significant faults or failures is achieved by the provision of multiple independent barriers to fault progression:
    a. Prevention of abnormal operation and failures by design;
    b. Prevention and control of abnormal operation and detection of failures;
    c. Control of faults within the design basis to protect against escalation to an accident;
    d. Control of severe plant conditions in which the design basis may be exceeded, including protecting against further fault escalation and mitigation of the consequences of severe accidents;
    e. Mitigation of radiological consequences of significant releases of radioactive material.
4. The safety function(s) to be delivered within the facility should be identified by a structured analysis.

Although it is something of a generalisation, for the purposes of this paper the first two principles are taken as being the responsibility of the SLC's engineering department, the third is shared by the engineering and safety case departments, and the fourth principle is addressed by the safety case department. Although the principles are listed in the order they appear in the SAPs, the order is more to do with strategic importance than any kind of implementation sequence.

In terms of project programming, identifying the high-level safety functions should take place virtually as soon as the concept design(s) are produced. As the design develops, so should the level of detail of the safety functions until specific parameters or performance requirements are defined for the safety measures that will be included in the design to ensure all radiological risks are ALARP. What is perhaps interesting is that not only are the SAPs non-prescriptive about how safety functions (and the wider safety case) should be developed, the International Atomic Energy Agency (IAEA) guidance document on Safety Assessments for Facilities and Activities (GSR-4) is also written at a fairly high level with only around thirty pages of technical content.

Safety Functions within the Safety Case

Safety functions are the building blocks of functional safety, which is the subject of BS EN 61508 Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems and its two subsidiary standards of relevance to the nuclear fuel cycle and nuclear power industries, BS EN 61511 Functional Safety – Safety Instrumented Systems for the Process Industry Sector and BS EN 61513 Nuclear Power Plants – Instrumentation and Control Important to Safety. The work of the different engineering disciplines in delivering safety functions is sometimes known as 'technical safety', and IAEA says this about technical safety in its Safety of Nuclear Power Plants: Design requirements document (NS-R-1):

> '*Technical Safety Objective: To take all reasonably practicable measures to prevent accidents in nuclear installations and to mitigate their consequences should they occur; to ensure with a high level of confidence that, for all possible accidents taken into account in the design of the installation, including those of very low probability, any radiological consequences would be minor and below prescribed limits; and to ensure that the likelihood of accidents with serious radiological consequences is extremely low.*'

NS-R-1 goes on to say that potential sources and levels of radiological dose to workers and the public should be identified for normal operations, fault conditions, design basis accident conditions and severe accident conditions. The need to consider both design basis accidents and severe accidents is an indication of how seriously nuclear safety is taken internationally, since Design Basis Accident Analysis (DBAA) aims to consider everything that could go wrong on a reactor or process plant as a result of control system errors or other internal or external hazards and then specify appropriate preventive, protective and/or mitigative safety measures. Severe Accident Analysis (SAA) then goes further by assuming the safety measures specified under DBAA have failed for the most serious hazards (generally involving fuel damage or loss of criticality control), and looks to identify further safety measures that could help protect the workforce and the public.

With this information, engineered safety measures can be developed through the application of technical safety, supported by procedural controls where necessary. As with GSR-4 and the SAPs, however, no particular process for doing so is put forward in NS-R-1, and so the following section considers at a high level how this is carried out in the UK.

Comparing Risk Assessment Procedures for Established and Newer SLCs in the UK

The difference between 'established' and 'newer' SLCs can be taken as those SLCs that were formerly part of the UK Atomic Energy Agency (UKAEA) and British Nuclear Fuels Ltd (BNFL) plus URENCO, versus the new and aspiring SLCs associated with the new-build NPPs plus those defence-related SLCs that are not overseen jointly by ONR and the Defence Nuclear Safety Regulator (DNSR). There is a small number of SLCs that do not fall into either category such as the former Consort research reactor at Imperial College London or the Cyclife UK Ltd radioactive waste recycling facility in Cumbria, however these facilities pose a much lower risk – particularly to the public – and so are not considered here.

With regard to the risk assessment procedures used by the two groups, they are essentially divided into internal best practice for the established SLCs and interpretation of regulatory guidance for the newer SLCs. The established SLCs are able to make use of risk assessments previously approved by ONR when defining their internal good practice, and this appears to play a large part in why established SLCs' risk assessment procedures show a fairly high degree of similarity. There is some variation in how the safety engineering requirements derived from risk assessments are implemented, however, which will be explored later.

As for newer SLCs, their approaches generally rely on interpreting regulatory guidance from ONR and IAEA, with the potential pitfall of there being no guarantee of acceptability until after the risk assessment and other documentation making up the overall safety case has been submitted. Furthermore, in some cases reliance is placed on information in the ONR's Technical Assessment Guides (TAGs) despite ONR being clear that this is not their intended purpose. The TAGs are similar to the various volumes of the Safety Report Assessment Manual published by HSE in relation to Control of Major Accident Hazards (COMAH) safety reports, and if trying to pass one's driving test by just reading the Highway Code is the analogy for carrying out risk assessments and safety engineering with only the SAPs for guidance, then an SLC using the TAGs to inform its procedures can be said to be like using a mark scheme to prepare for an examination. Doing so undoubtedly gives the SLC a feel for what ONR are expecting to see in the safety case, however placing too much reliance on the TAGs runs the risk of failing to see the wood for the trees. At the risk of labouring the point, no amount of studying The Highway Code or examination mark schemes can replace teaching and practice.

Judging by the level of convergence in established SLC's risk assessment procedures, it can be said with a fair amount of certainty that developing internal good practice iteratively by putting a safety case through regulatory approval will eventually lead to an SLC having a robust set of risk assessment procedures which will greatly improve the chances of any subsequent safety case being 'right first time'. An added complication, however, is that the risk assessment procedures of established SLC's have developed over many years, often in parallel with ONR's own expectations. Newer SLCs are therefore on an steep learning curve compared to their established counterparts; even more so considering a facility as complex as an NPP is covered by a single safety case.

It must be said that newer SLCs tend not to be starting entirely from scratch, since in the case of new-build NPPs the designs have been built and operated elsewhere in the world or are at least evolutions or existing designs. Those newer SLCs involved in defence are generally in the situation where there is existing plant that has been operated safely for some time but which requires an updated safety case. In both instances, the safety engineering tends to be present but may not necessarily be supported by suitable documentation. As can be seen from some of the Generic Design Assessment (GDA) documentation published by ONR, having a reactor design in existence elsewhere in the world does not necessarily imply regulatory acceptance in the UK, and so while none of the newer SLCs are actually starting from scratch, they still need to go through one or more cycles of review and revision of their safety cases before finally receiving regulatory approval.

Comparing Safety Engineering Procedures for Established and Newer SLCs in the UK

Even though safety engineering procedures at established SLCs are broadly the same, there is not the same level of convergence as is seen in risk assessment. In some ways, the SAPs are more prescriptive in their safety engineering requirements than they are for risk assessment since there are clear expectations laid out for reliability, redundancy and diversity in safety measures specified against higher-risk fault conditions. There is not necessarily agreement between SLCs however on details such as whether or not redundant safety measures can be seen as distinct 'primary' and 'secondary' systems (and engineered accordingly), and whether or not on-line maintenance of safety measures is considered as a matter of course or only when it crops up as a potential requirement. None of these differences should be considered as making one SLC's facilities 'safer' than another's, however there is a lack of consistency which could hamper sharing of good practice – especially with newer SLCs that do not have existing, compliant facilities to use as benchmarks.

Although it may not appear to be a major concern, there is also a lack of consistency in safety engineering nomenclature. This ought not to affect the validity of the engineering, but it is another potential barrier to the easy sharing of good practice between SLCs. It is not an issue unique to the UK in fact, as acknowledged by the World Nuclear Association (WNA) in their 2015 paper, 'Safety Classification for I&C Systems in Nuclear Power Plants - Current Status & Difficulties', and given that it is a matter that is already in hand within the nuclear industry it will not be considered further here.

The situation amongst newer SLCs is even more disjointed at this stage; certainly as far as new-build NPPs are concerned. The GDA process has highlighted fundamental philosophical differences between the approaches preferred by ONR compared to regulators in the new-build NPPs' countries of origin. For the most part, these differences can be put down to ONR employing a level of conservatism that goes beyond their counterparts elsewhere in the world – but this is not to say that ONR is unreasonably picky or other regulators are any less diligent; it is simply down to differences in the tolerability of risk in different jurisdictions and the manner in which residual risk is shown to be tolerable.

To give a couple of examples from the GDA process, one of ONR's most significant findings for the proposed EPR design was that the complexity and lack of diversity in Control and Instrumentation (C&I) did not meet their expectations despite the Probabilistic Safety Assessment (PSA) carried out on the C&I systems showing that the numerical risk of failure would meet the relevant criteria. One of ONR's most significant findings on the proposed AP1000 design was that undue credit was taken (in their opinion as UK regulator) for joints in the primary circuit failing in a Leak Before Break (LBB) mode which was considered to be only a fringe 'ALARP measure' rather than an acceptable basis for a major safety argument.

It should be reiterated for both of the examples given above that the levels of residual risk at which NPPs operate are very much lower than almost any other industry, and so for ONR to find instances of non-compliance with their own criteria does not mean that comparable NPPs being designed or operated elsewhere in the world are unsafe in any objective sense. The two examples exist at the interface between risk assessment and safety engineering insofar as the GDA findings related to engineering aspects in the design which were claimed as safety measures in the corresponding risk assessment documents. The difference between them however is that the EPR having a lack of diversity in its C&I safety engineering represents an issue with the implementation of a safety function, whereas AP1000 designers taking undue credit for LBB failure modes in the primary circuit is a safety function which ONR does not feel is justified at all. It should also be pointed out that the matters given as examples are in the process of being resolved and would not be expected to feature in the final design and/or safety case. Nevertheless, they do demonstrate the kinds of non-compliance (from the UK regulatory perspective) that can be present in a design and/or safety case which has been put together through interpretation of the SAPs and/or TAGs rather than in line with internal good practice developed iteratively with the benefit of multiple interactions with ONR addressing a number of different facilities.

This then brings the discussion back to the original point of whether an ACOP for UK nuclear safety cases would be beneficial to SLCs and indeed ONR in terms of providing the guidance for safety cases in a proactive rather than reactive fashion.

Potential Advantages and Disadvantages of an ACOP for UK Nuclear Safety Cases

From this point on, the paper will no longer make a distinction between safety engineering and risk assessment procedures, and just discuss the documentary output of both: the safety case. This is because the safety case should record all pertinent claims, arguments and evidence underpinning the safety engineering process, and should include all the decisions, assumptions and calculations that make up the risk assessment for the facility in question.

Advantages

By far the biggest beneficiary of a UK nuclear safety case ACOP would be the new and aspiring SLCs involved with new-build NPPs. They would not be required to pick up on the nuances of UK regulatory expectations as they went along, but would instead have clear guidance on how a safety case should be compiled and presented as well as being able to use the information in the SAPs and (if necessary) the TAGs to understand what a safety case should contain. The same could apply to newcomers in the nuclear supply chain, although both SLCs and suppliers would still need to demonstrate use of Suitably Qualified and Experienced Personnel (SQEP) which would prevent a complete novice picking up and using the ACOP. While an individual safety case practitioner can become SQEP through training and mentoring by a third party under current arrangements, the introduction of an ACOP would effectively extend this possibility to an entire SLC.

ONR could also potentially benefit from the introduction of an ACOP since any 'first of kind' safety cases being submitted for nuclear new-build should be written with a clearer understanding of what is required. Furthermore, an ACOP developed with input from WNA and similar industry bodies could help address inconsistencies in the approach used by established SLCs in matters such as safety classification.

Established SLCs may also see some indirect advantages since ONR should potentially be able to devote less attention to new-build safety cases, freeing more resources to decommissioning projects which will be continuing throughout the new-build period however these tend to have lower levels of risk associated with them so do not need as intense regulatory scrutiny.

Disadvantages

It would probably be naïve to assume that established SLCs would get more from an ACOP than they would contribute. Having said this, ACOPs for things like COMAH and pressure systems have been successfully developed in similar commercial environments so it is entirely possible that established SLCs would be open to sharing their intellectual property within reasonable limits. A further disadvantage for established SLCs would be that some of the debate around factors such as inconsistency in safety classification proposes the introduction of codes and standards (i.e. IEC 61513 and similar) which are relatively recent compared to the SLCs' procedures, and which may originally have been developed with input from the SLCs themselves. Since codes and standards such as IEC 61513 are based on good practice from across an industry sector, this could lead to SLCs being forced to drop their own (perfectly serviceable) procedures and naming conventions to match a standard that is notionally less well-established than their own procedures. Put this way, introduction of an ACOP might come across as change for change's sake which is not necessarily in anyone's interests. It is noted that although ACOPs have a stronger legal status than basic guidance they are not mandatory, and so an established SLC following its own mature internal good practice would certainly not be breaking any laws. This could potentially inhibit take-up of the ACOP once published, and without the 'major players' being involved the ACOP might lack credibility.

The main disadvantage for both ONR and newer SLCs however would be an erosion of the SAP FP.4 requirement for SLCs to demonstrate effective understanding and control of the hazards posed by a site or facility through a comprehensive and

systematic process of safety assessment. Newer SLCs would no longer need to go through the process of learning their way around the UK regulatory framework for themselves, and would instead have that knowledge presented to them. This would probably reduce the amount of rework required for GDA safety cases and similar first-of-kind safety cases, but would at the same time reduce the need for SLCs to take the lead in developing and maintaining their safety case processes which is not consistent with SAP FP.4. Taken to the extreme, this could lead to an SLC divesting itself of an in-house safety case capability and relying entirely on the supply chain – although there is a different LC (LC36) covering organisational capability which would limit the extent to which this could be allowed to happen. In fact, the need to countenance LC36 and the need to use SQEP resources with the third-party (if authoritative) nature of an ACOP would be likely to limit the amount of detail the guidance in a UK nuclear safety case ACOP could provide in any case.

What Might a UK Nuclear Safety Case ACOP Look Like?

Taking into account the various advantages and disadvantages discussed above, a UK nuclear safety case ACOP would need to be non-prescriptive enough to avoid prejudicing SAP FP.4 and LC36 requirements and also to avoid discouraging established SLCs from adopting it. It would need to contain sufficient clarification of ONR's expectations to help newer SLCs avoid making the incorrect assumptions or interpretational errors that have led to the GDA findings published to date, however this information is already in circulation. As such, asking aspiring SLCs to take account of previous GDA findings on different designs when developing their safety case procedures would push the SLCs to learn for themselves about what is and is not likely to receive regulatory approval. Notwithstanding the purpose of the TAGs, the information in them would provide a complementary directory of what ONR does want to see in a safety case.

It has to be said that all of this information is already available from various pages on the HSE website, in which case an ACOP would probably be little more than a digest of this information. Considering this information would be most advantageous to only a small proportion of the total number of SLCs and suppliers, it becomes a question of whether giving a limited number of organisations a helping hand in developing their safety case procedures actually adds any value to the newer SLCs and suppliers, or indeed to the industry as a whole.

An alternative to a published ACOP might be to develop an organisational mentoring scheme. To avoid conflicts with SAP FP.4 and LC36, this would need to take the form of 'guided learning' as opposed to a more passive 'being taught' format, or perhaps a requirement for new and aspiring SLCs to have their safety case procedures endorsed by ONR early in the GDA process. An SLC having its safety case procedures endorsed is unusual but not unprecedented, as BNFL had their safety case procedures endorsed by ONR's predecessor – the Nuclear Installations Inspectorate (NII) – in an official Memorandum of Understanding issued around the turn of the century when what is often referred to as the 'modern standards safety case' was being developed across the industry.

All reactors proposed to date for nuclear new-build are existing designs with modifications to suit the UK market, and this leads to a situation where the engineering for a new NPP is far more advanced than the safety case processes at the time GDA is instigated. Nevertheless, the GDA process for the EPR design took over five years from the time the initial proposals were submitted for regulatory approval to the time final approval was given to build the two units now starting to be built at Hinkley Point, and even allowing for some acceleration as ONR streamlines its GDA procedures this is potentially sufficient time for new and aspiring SLCs to develop compliant safety case procedures and have them endorsed by ONR. Of course, as indicated earlier, having a safety case approved by ONR effectively gives endorsement to the procedures that underpinned the production of the safety case. Therefore if an SLC only intends to operate a small number of NPPs all of the same design, the effort put into having its safety case procedures endorsed upfront may be nugatory as apart from site-specific details it will be possible to use much of the safety case documentation produced for the first NPP for any subsequent ones.

Conclusions

An ACOP for UK nuclear safety cases certainly seems like a good idea at first glance, however it is clear upon further investigation that anything too prescriptive runs the risk of prejudicing the (entirely valid) requirement for SLCs to 'own' their safety case procedures. Given the potential consequences of a radiation accident, short-cutting the organisational learning process behind developing a set of safety case procedures would carry risks of its own. While the amount of rework involved in the GDA process appears to make the safety case process for new and aspiring SLCs somewhat inefficient, the value to an SLC of learning ONR's expectations for itself should not be underestimated since this learning will be carried forward within the organisation's collective knowledge base as the facility or facilities commence operation.

The possibility of ONR or an industry body such as the Nuclear Industries Association (NIA) mentoring new and aspiring SLCs as they develop their safety case procedures has been explored, and while this approach would be a better fit for the organisational capability requirements of SAP FP.4 and LC36 it is not clear that the effort required to do this would be worthwhile considering an SLC hoping to build an NPP would not be building large numbers of different plants with different functions. From this point of view an ACOP could be of more use to SLCs involved in the nuclear fuel cycle rather power generation, were it not for the fact that UK fuel cycle SLCs already have well-established safety case procedures.

To summarise, therefore, the absence of an ACOP for UK nuclear safety cases would actually appear to bring some benefits for the organisational capabilities of new and aspiring SLCs. Indeed, introducing one could potentially detract from an SLC's organisational capabilities rather than boost them. An appropriate compromise could be for ONR or a body such as NIA to mentor new and aspiring SLCs as they develop their safety case processes to support their GDA submissions, or alternatively for ONR to endorse the SLC's safety case procedures separately from any design approvals. In either of these cases, however, this could potentially result in a significant amount of effort being expended to deliver limited benefits in the

short term and arguably very little benefit once the SLC has had its first safety case approved considering that any subsequent NPPs built by that SLC would be likely to be of the same design.

In conclusion, there would appear to be little actual benefit to any of the parties involved in producing an ACOP for UK nuclear safety cases. There is a marginally stronger argument for introducing some kind of mentoring for SLCs when they develop their safety case procedures or for having ONR endorse the procedures when complete, but even then it is hard to see much long-term benefit in doing so. In this instance, even though it does not follow suit with other high-hazard sectors such as COMAH and offshore oil and gas, the lack of an ACOP is not an indication of anything being broken and as such the current arrangements probably do not need to be fixed.

References

NIA65 – The Nuclear Installations Act 1965

HSW – The Health and Safety at Work Act 1974

NS-R-1 – International Atomic Energy Agency, 2000, ‘Safety of Nuclear Power Plants: Design’

SAPs – Office for Nuclear Regulation, 2014, ‘Safety Assessment Principles for Nuclear Facilities’, Revision 0

WNA 2015 – World Nuclear Association, CORDEL Digital Instrumentation & Control Task Force 2015, ‘Safety Classification for I&C Systems in Nuclear Power Plants - Current Status & Difficulties’