DNSR/22/11/2

4 Nov 09

SUCCESSOR SSBN

SAFETY REGULATORS' ADVICE ON THE SELECTION OF THE PROPULSION PLANT IN SUPPORT OF THE FUTURE DETERRENT REVIEW NOTE

Issue

1. Safety Regulators' advice to support decisions to be made impacting the design and progress of the successor SSBN.

Background

2. In response to a request from the SRO, this advice has been prepared by Cdre Andrew McFarlane (the Defence Nuclear Safety Regulator - DNSR), with a ship safety contribution from Mr Gavin Rudgley (the Naval Authority). It has been reviewed with Mr Howard Mathers (the Chairman of both the Defence Nuclear and the Ship Environment and Safety Boards), with the independent Defence Nuclear Safety Committee[1] and with Dr Mike Weightman (HM Chief Inspector of Nuclear Installations)[2].

3. The aim is to set out the legal and policy framework within which the project must propose and the Department must in due course decide on the appropriate propulsion plant for the successor SSBN, and against which both the statutory and internal MOD regulators will review the safety of the acquisition, operation and support of the deterrent, to inform their permissioning of specific activities. It is informed by the analysis and emerging evidence provided by the project of the options under consideration, and the formal review of this undertaken by the Reactor Plant Safety Committee and the Project's Platform Safety Committee.

The Legal and Defence Policy Position

4. The most significant legislation is the Health and Safety at Work Act (HSWA). Among the many provisions of the Act, two are fundamental.

- There is a duty on employers to ensure, so far as is reasonably practical, the safety of employees, and of others who may be affected by their undertaking.

- There is a duty on employers to ensure, so far as is reasonably practical, the safety of employees, and of others who may be affected by their undertaking.

These provisions are underpinned by a large body of case law. In summary it is always a legal requirement to reduce risks to people so far as is reasonably practical which is commonly expressed as reducing risk as low as is reasonably practical (ALARP).

5. Among the many regulations made under the HSWA, two are particularly significant. The Ionising Radiations Regulations set out the basis on which the radiation risk to employees must be reduced ALARP, and the Radiation Emergencies (Preparedness and Public Information) Regulations set out the basis on which the potential consequences from a radiation emergency are to be managed, in order to protect both employees and members of the public.

6. The Nuclear Installations Act (NIA) (which is a statutory provision of the HSWA) defines the process to be followed to demonstrate that the risks to people from nuclear plant are reduced ALARP. The Environment

1 This will be reviewed by DNSC members at their meeting on 10 Nov 09.
2 This was undertaken at the Senior Operational Liaison Meeting on 3 Nov 09.

Act and the Radioactive Substances Act (RSA) require that the environmental impact of nuclear plant is minimised to the best practicable environmental option using best available techniques – this is synonymous with reducing the effect on the environment ALARP.

7. There are defence exemptions from some aspects of this legislation (notably from the licensing requirements of the NIA when the submarine reactor plant is intact or under direct crown control, and from the RSA when under direct crown control), but there is no general exemption from the HSWA. Thus the statutory regulators, the Nuclear Installations Inspectorate (currently part of the HSE), the Environment Agency (EA) and Scottish Environment Protection Agency (SEPA) have statutory responsibilities with accountability to the UK or Scottish Ministers and Parliament. Where there are exemptions, the SofS policy is that arrangements will be adopted which are, so far as is reasonably practicable, at least as good as the requirements of the legislation: these are regulated by the internal MOD regulators with accountability through 2nd PUS to SofS. The MOD regulators work closely with their statutory counterparts to achieve coherent regulation. In summary, the legal requirement is unequivocally to reduce the risks to all people and to the environment ALARP.

8. The legal interpretation on what is expected of an employer to reduce risk ALARP is contained in case law, but the HSE has published guidance based on this. The 2001 document "Reducing Risks Protecting People" (R2P2) sets out the strategic position and the basis of HSE's decision making process. There are particular societal concerns relating to nuclear hazards, as recognised in a number of public enquiries, notably the Sizewell B public enquiry which completed in 1988. This led to the publication of "The Tolerability of Risk from Nuclear Power Stations" (TOR) last revised in 1992. This guidance was updated in the publication of revised "Safety Assessment Principles for Nuclear Facilities" (SAPs) in 2006. DNSR worked closely with HSE in this revision and subsequently adopted them so that SAPs now provide formal guidance to both the HSE/NII and to DNSR on their regulatory decision making. In line with UK practice they are non-prescriptive in nature, and leave the onus on the duty-holder to demonstrate ALARP[3]. But from this guidance some key principles can be drawn.

ALARP – What is it? How is it assessed?

9. The starting point in assessing whether risk has been reduced ALARP is to compare the practice with others undertaking similar activities. From this it is possible to identify "best practice" in any particular field. But while best practice is likely to be delivered by only one or a few leading organisations, it is also possible to identify "relevant good practice" – the practice that is recognised by those in the field as an expectation. Sometimes this will be published by an industry association or by the HSE in an Approved Code of Practice (ACOP). There is, however, no ACOP on nuclear safety in submarines. The regulators' clear expectation is that any new plant must conform to relevant good practice, or demonstrate a comparable level of risk, without any reference to cost benefit analysis[4]. There are, however, societal expectations which change over time and standards are likely to increase. Thus in the future relevant good practice may well improve to include today's best practice. The requirement therefore is to conform to relevant good practice, but also to examine best practice and where reasonably practicable, to adopt it.

10. Having adopted relevant good practice, it is also essential to test whether this has reduced risk ALARP. **To do this it is necessary to consider a wide range of possible options to further reduce risk. For each option, the risk that would be averted by its implementation must be balanced against the sacrifice (in money time & trouble) incurred in implementing the option.** The case law position is that unless the

---

3 It is the dutyholder (who may be a nuclear Licensee or Authorisee), who must decide whether an activity is ALARP. Regulators may review this decision, and may agree or otherwise that the activity should proceed, and accordingly may seek to influence the decision from an early stage, but the decision is the dutyholder's.
4 HSE advice, based on case law, is clear on this point, that this requirement is not influenced by cost. This point was emphasised by Dr Weightman.

sacrifice can be shown to be grossly disproportionate to the risk averted, then the improvement must be implemented[5].

11. SAPs also contain a large number of engineering principles[6]. Among them is the guidance that safety should be secured by measures as near as possible to the top of the following hierarchy:

- Conservative design and passive safety measures that do not rely on control systems or human intervention;
- Active engineered safety measures that are initiated automatically;
- Active engineered safety measures that must be initiated manually;
- Administrative safety measures and procedures;
- Mitigation measures to minimise the consequence of failure.

And What is "Relevant Good Practice" in Nuclear Submarine Design and Operation?

12. For the last 50 years UK submarine design and operation has developed its own "relevant good practice" largely in isolation from peers. In recent years the opportunity for greater technology interchange with the US, and greater benchmarking with the UK civil nuclear power generation industry has allowed more comparison. Some aspects of the UK submarine programme represent best practice, for example submarine pressure hull structural design, and the protection against fire. But in a number of areas it is clear that the UK programme currently falls short of current relevant good practice. The FSM team have conducted a limited benchmarking exercise to identify relevant good practice and best practice in nuclear submarine operation, which has been reviewed by the project safety committee.

13. From this, there are two major areas of discrimination where current UK practice falls significantly short of benchmarked relevant good practice.

Control of submarine depth. For all submarine operations, depth is controlled by a combination of hydrostatic lift (by adjusting the ballast of the submarine) and dynamic lift (using speed through the water and control surfaces). US established practice is to deliver a high reliability of propulsion, from the main propulsion system, even under reactor fault conditions. UK practice in current class submarines is to accept a much lower reliability from the main propulsion system, and to back this up with a very low power (but high reliability) emergency propulsion system. This system will not provide sufficient dynamic lift, so safety is achieved by procedural controls constraining the combinations of speed and depth, backed up by use of ballast systems (but this may not be effective under all circumstances).

Loss of (reactor) Coolant Accident (LOCA). All pressurised water reactors are potentially vulnerable to a structural failure in the primary circuit, causing a rapid depressurisation and boiling off of most of the cooling water. This results in failure of the fuel cladding, and a release of highly radioactive fission products outside the reactor core. While the further containment provided by the submarine's pressure hull may contain the majority of this material inside the submarine, some leakage is likely to occur and in any event the radioactive "shine" from the submarine poses a significant risk to life to those in close proximity, and a public safety hazard out to 1.5km from the submarine. Current designs of UK and global civil power plants have systems for safety injection of coolant into the reactor pressure vessel head and passive core cooling systems. US nuclear submarines have similar systems suitably engineered for the submarine environment. UK submarines

---

5 This is discussed further later at para 20

6 The SAPs provide advice to regulators on expectations for relevant good practice. But they are not mandatory, nor are they intended to be used as design or operational standards – this is for the dutyholder to define.

compare poorly with these benchmarks, with the ability to tolerate only a structural failure equivalent to a 15mm diameter hole, and an assessed higher likelihood of this occurring due to the materials used, the complexity of systems and the number of welds. It is assessed that in the current UK PWR2 plant the initiating structural failure causing a LOCA is twice as likely to occur as in equivalent civil and submarine reactor good practice.

Furthermore the current PWR2 emergency core cooling system does not inject coolant to the reactor pressure vessel head, and is highly dependent on manual procedural control.

Implications for Current UK Submarines

14. For current classes of submarine, including the ASTUTE Class under construction, there is a limit to what improvements are reasonably practicable to implement, although the regulators will continue to press for incremental improvements where these are practicable, and the associated increase in cost or schedule risk is not grossly disproportionate. The regulators will review continued operation of these classes of submarine on this basis.

Implications for the Successor SSBN

15. For the successor SSBN, it is clearly reasonably practicable to implement more significant improvements, and it is therefore a legal responsibility to do so. These improvements must both demonstrate conformity to relevant good practice (and where not grossly disproportionate, best practice, recognising that the SSBN Successor will be in service until the 2060s), and must demonstrate that risk has been reduced ALARP.

16. The options available to improve the safety performance for the successor SSBN will be set out by the project. For these options, Project Safety Reports have been issued by the FSM team and reviewed by the Platform Safety Committee, focussing on the differences between the Adapt Astute and Derived Submarine options. A Preliminary Safety Report (PSR) has been published for PWR3, reviewed by the Reactor Plant Safety Committee (RPSC) and presented by the Naval Reactor Plant Authorisee (NRPA) to DNSR, giving DNSR clear evidence of the likely safety performance of this plant. The RPSC have also advised the NRPA that without improvement PWR2 is not an ALARP solution: DNSR agrees with this position based on assessment of the ASTUTE safety case. Work is understood to have been completed by the Project Team to articulate the changes that might be made to the existing PWR2 plant to address some of the key safety improvements offered by PWR3 without a fundamental redesign; this is the PWR2b design concept, which the project team advise is technically feasible. The delivery/schedule risk and associated cost are the subject of current work This analysis must be published, reviewed by the RPSC and presented to DNSR, in support of the Initial Gate Business Case.

Current Assessment

17. While the full range of options remains to be fully articulated, it is possible to make some preliminary assessments.

• Control of submarine depth. The FSM team have postulated 3 options for improving the control of depth: the high reliability main propulsion system through continuity of steam power delivered by PWR3; a much higher power emergency propulsion motor powered by a high energy submarine battery; and an emergency rapid de-ballasting system; or a combination of these. Of these, the emerging analysis is that the best protection is delivered by the high reliability main propulsion system delivered by PWR3, although as this is still vulnerable to a failure along the single shaft line, some further defence in depth should be considered. But the emerging analysis is suggesting that the safety performance delivered by installing both a high power emergency propulsion motor, and a rapid deballasting system might provide a safety performance not far short of that from the PWR3 Derived

Submarine, although these fall lower down the safety hierarchy outlined earlier. The risk of development and integration of these options must also be further understood.

• Loss of Coolant Accident. A number of proposals have been made for implementation of improvements to the PWR2 reactor plant. Those that are reasonably practicable to implement should be implemented in the later ASTUTE Class submarines. More significant changes are included in the PWR2b option, which would improve a number of facets of reactor safety, and which certainly would improve overall compliance with the guidance in SAPs. But for the dominant fault sequence of a LOCA, the ability to protect against reasonably foreseeable leaks can only be achieved by injection of emergency core cooling through the reactor pressure vessel (RPV) head directly into the core (direct head injection). This is very complex to analyse and implement for the PWR2 plant, and would require significant technical demonstration, whereas it is far more straightforward in the PWR3 design. While PWR2b has yet to be reviewed and formally presented, it nonetheless seems likely that the only option that will deliver relevant good practice in this important facet of safety is the PWR3 Derived Submarine.

18. It would appear therefore that while a PWR2 Adapt Astute submarine may demonstrate relevant good practice for control of depth, in response to the vulnerability to a LOCA an unmodified PWR2 is unacceptable and only the PWR3 Derived Submarine is likely to demonstrate relevant good practice.

19. As stated at para 9 above, to demonstrate ALARP the starting point is to demonstrate adoption of relevant good practice without reference to a cost/benefit argument. But even if a suitable adaptation of PWR2 was considered to represent relevant good practice, then it would still be necessary to consider further available improvements, and assess whether the associated sacrifice of implementing them would be grossly disproportionate. For this it is necessary to make a judgement by balancing the safety benefit provided by PWR3 with the associated sacrifice (money time or trouble), and assessing whether the sacrifice is disproportionate to the benefit.

20. It appears that while there may be some very limited capability sacrifices, overall the PWR3 Derived Submarine will not only deliver a safer, but also overall a more capable submarine than the PWR2 Adapt Astute. The dominant sacrifices between the options are therefore in cost and in schedule risk. The emerging analysis of these from the concept validation programme will be presented in the Review Note. The safety regulators will not review these figures for themselves, but will take note of the outcome of independent verification (including head office scrutiny) of the cost and schedule models. In due course the Department may need to make a judgement of whether this cost and schedule sacrifice is grossly disproportionate to the very significant safety benefit in the improved LOCA performance and the smaller improvement in control of depth, either in the standalone context of the SSBN successor, or in conjunction with consideration of the Maritime Future Underwater Capability. (An extract of HSE advice on the assessment of gross disproportion is included at Annex B.)

Risk Probability Targets – a Cautionary Note

21. Excessive attention is often paid to probabilistic risk targets. Both R2P2 and SAPs set out targets in terms of the acceptability of the risk of individual or gross fatalities, and probabilistic safety analysis can be used to compare against these targets. A brief summary of the targets is provided at Annex A. This is useful for illustration to compare, within a hazard area, the probability of different events which may result in fatalities. But, to re-iterate, there is no legal requirement to meet these targets – the legal requirement is to reduce risk ALARP, primarily by use of sound engineering and conservative design. And although illustrations of risk probability may suggest that the risk of multiple fatalities resulting from loss of depth control may be orders of magnitude greater than the risk of fatalities from a LOCA, this does not obviate the legal requirement to reduce the nuclear risk ALARP.

Conclusion

22. he legal requirement on both MOD as the operator and on industry as the suppliers is to reduce the risk to people[7] and the environment as low as is reasonably practicable (ALARP). To achieve this it is necessary to demonstrate compliance with relevant good practice, and to implement additional safety improvements until it is judged that the sacrifice associated with making any further safety improvements is disproportionate to the safety benefit. At present the case has not yet been made to the safety regulators to agree whether this is achievable through significant improvements to a PWR2 powered submarine (ie PWR2b) or whether this can only be achieved through PWR3. And to inform the ALARP assessment, greater confidence is also required in the associated cost and schedule implications. The two most significant discriminators are control of depth and response to a loss of coolant accident (LOCA). On the emerging analysis, it appears that it may be possible to demonstrate that adequate control of depth can be achieved by improvements to a PWR2 submarine, but the necessary safety performance in response to a LOCA is likely to be delivered only through a PWR3 submarine.

22. To remove the uncertainty in this regulatory position, two key activities are required. Firstly there must be a formal presentation of the safety analysis and arguments for PWR2b, and of the associated cost and schedule risk. And secondly there must be greater confidence in the cost and schedule risk delta between the options.

Andrew McFarlane
Cdre RN
Head of the Defence Nuclear Safety Regulator
Annexes:
A. Probabilistic Safety Targets.
B. Assessment of Gross Disproportion

7 Throughout this document, the risk to people refers to the ship's company, the local nuclear site workforce, and to members of the public, except where these are separately identified.