The Complex challenges of risk and hazard reduction for a Legacy Fuel Pond at Sellafield, UK – 10197

David Forsythe CEng MIMechE. Sellafield Ltd. Seascale, Cumbria, CA201PG, UK

ABSTRACT

The paper is intended to put into context the challenges associated with waste retrieval and decommissioning of the first generation MAGNOX storage Pond (FGMSP) at Sellafield in the UK. This plant is over half a century old and has a legacy inventory of nuclear material, sludge and waste stored in the main cooling pond areas and enclosed bays used for fuel operations in the past. The plant age drives the urgency to make improvements to retrieve the inventory for long term disposal.

The plant safety case does not compare to what might be expected from the output of a modern standard safety case process, and the means to demonstrate adequate protection are unusual. The plant age and the necessary form of the safety case has driven the need for new ways of thinking to make safety cases based on layers of defence and a focus on nuclear safety improvements to provide the bedrock of confidence needed to meet the challenges.

The paper sets the scene and gives examples of innovation and creativity used to meet the challenge and make progress. The technical challenges are described briefly to give an understanding of the environment in which the judgements, decisions and cases are made and to act as a vehicle to explain the innovation.

INTRODUCTION TO THE PLANT AND TECHNICAL CHALLENGE

The First Generation MAGNOX Storage Pond (FGMSP) was put into operation at Sellafield in 1959. It consists of a main pond used for underwater storage of spent reactor fuel in the form of uranium bars with a magnesium alloy (known as Magnesium Non-Oxidising or MAGNOX) outer casing. The fuel was stored within the main pond in open top containers (called skips) that were transported to the plant in shielded transport containers (called flasks). An “inlet” building facilitated transfer of the skips from the flasks to the pond. A form of overhead travelling crane supported on a gantry on either side of the pond and running its full length, was used to position the skips of fuel in the pond. This “skip handler” used a mast which extended below the water with bespoke tooling to lock onto the skips. After a cooling period the same machine was used to transfer the skips into a series of enclosed “wet bays”. These were deep enough to give adequate water shielding to operators from the fuel. They acted as extensions to the pond in that they had the same water and were linked directly to it. They were partly covered by an operating floor with a main penetration to allow operators to carry out fuel operations using long tools to manoeuvre the fuel from skips and into a machine to separate the uranium rod from its MAGNOX casing. The wet bays were used for these operations in the 1960’s but then two shielded “cells” were added in an extension to the building to allow the removal of the MAGNOX casings to be carried out above pond level with operators using remotely operated tools from outside the cells observing the process through shielded windows (see “caves 1 & 2” in fig 1).

During the 1970’s corrosion of the MAGNOX fuel cladding and the fuel itself resulted in contamination of the water and an accumulation of corrosion products in the form of sludge. The resulting loss of pond visibility led in turn to operational problems. Skips had been stacked up to three high in the pond and it was not uncommon for the skip handler to dislodge a parked skip in the poor visibility. The sludge accumulated on the pond floor also provided an unstable platform on which to park skips and some stacks subsided. These problems contributed to an accumulation of debris on the pond floor from toppled skips. Early operations were supported by improvised means to clear sludge away from operational areas resulting in accumulations of sludge and waste in the wet bays. (Shown as A to E bays and SP bay in fig 1).

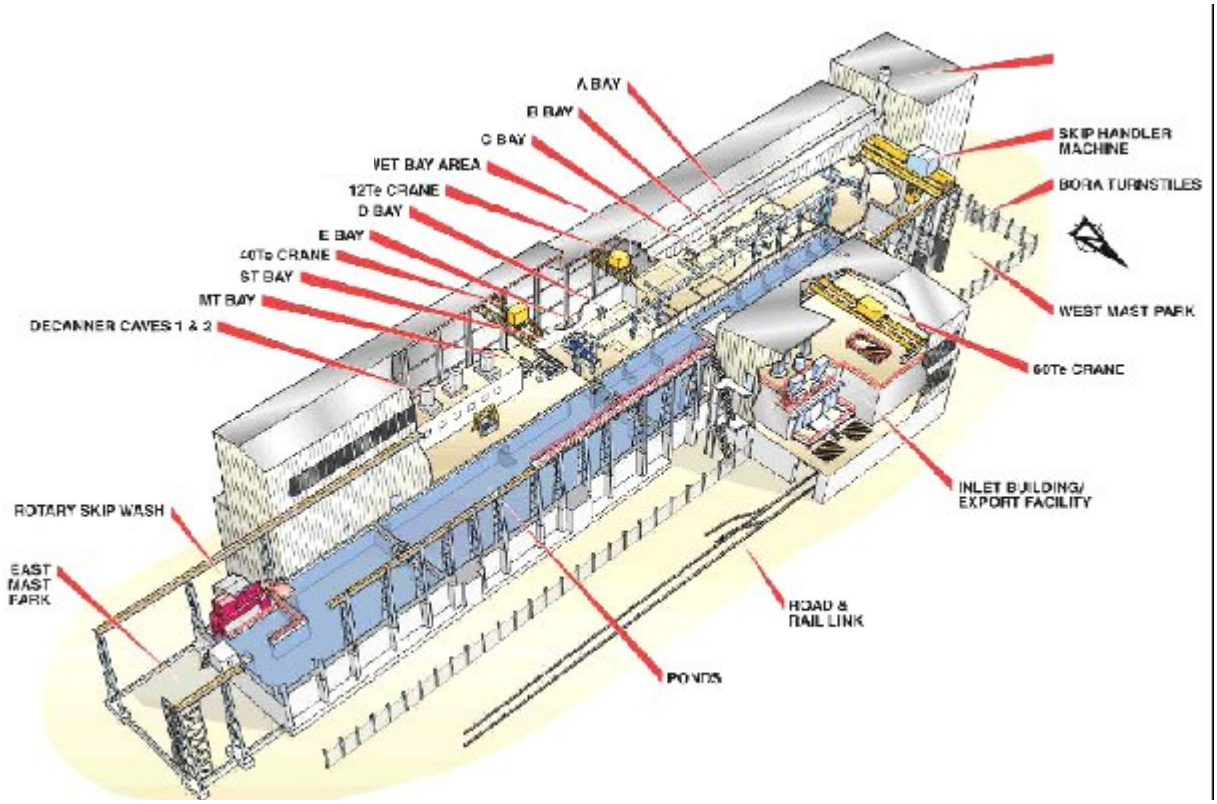

Fig.1. Schematic view of the First Generation MAGNOX storage pond.

The plant's main operations have been complete for over a decade and as much inventory has been removed as has been possible using the original plant operational systems. The remaining inventory is made up of contaminated tooling, machinery and maintenance waste, partly corroded uranium bars, and magnesium hydroxide/uranium sludge. The waste is located on the pond floor or within the wet bays. Each of the seven bays holds up to its full volume of waste (sludge, contaminated tools and other items, and uranium debris). The uranium bars are in the skips or on the pond floor mixed with other waste. The sludge coats most of the other waste and is present in very large accumulations in the pond and the bays. None of the waste can now be accessed or removed with existing systems and the radiological conditions prevent access to many areas or reduce working times to only a few minutes.

The consequences of a decline in the condition of parts of the plant's ageing containment could cause operational problems and delays. The main civil structure is at the limit of its load bearing capacity and there are space constraints as the plant and the surrounding areas are very congested. Retrieval solutions will be further restricted by the need to minimise the load on the structure. The work underway to retrieve the waste includes repairing and upgrading the basic plant infrastructure and replacement of life expired systems with new designs to perform retrieval tasks. This includes refurbishment of the main building steelwork to support deployment in the pond of new mechanical handling devices to retrieve debris and sludge from the floor and recover fuel containers which have toppled over. A new plant is under construction to store the full volume of sludge and the waste is destined for some existing (but modified) processes on the Sellafield site as well as new ones being designed.

THE CHALLENGE TO DO THINGS DIFFERENTLY

The technical and engineering expertise exists and the technology is available to tackle the challenges faced. The challenge considered here is to make robust safety cases to enable the deployment of the

required technical solutions in the facility. For the reader to understand this, a little more needs to be explained about the plant condition and the existing safety case.

The plant condition

The plant was built over half a century ago. Its inventory of nuclear material, contaminated waste and corrosion products is very significant. To put this in context, the sludge has a specific activity of 60TBqm^{-3} and that of the liquor is 5GBqm^{-3}. The civil structure itself has many construction joints. Approximately one third of the civil structure is below ground level and there is no separate secondary containment. The civil structure has many engineered penetrations in the form of a complex pipe-work system originally used in the early 1960's to provide a purge to the water covering the fuel operations. Parts of this system (henceforth referred to as the purge system) are susceptible to corrosion or damage from relatively minor impacts or seismic activity as a result of their materials of construction. Many of the pipes penetrate the structure at levels below that of the liquor surface and are therefore themselves part of the primary containment. The evidence as to whether the lines carry pond head or have some 50 year old isolation in place lies within the pond and bays beneath the sludge and waste.

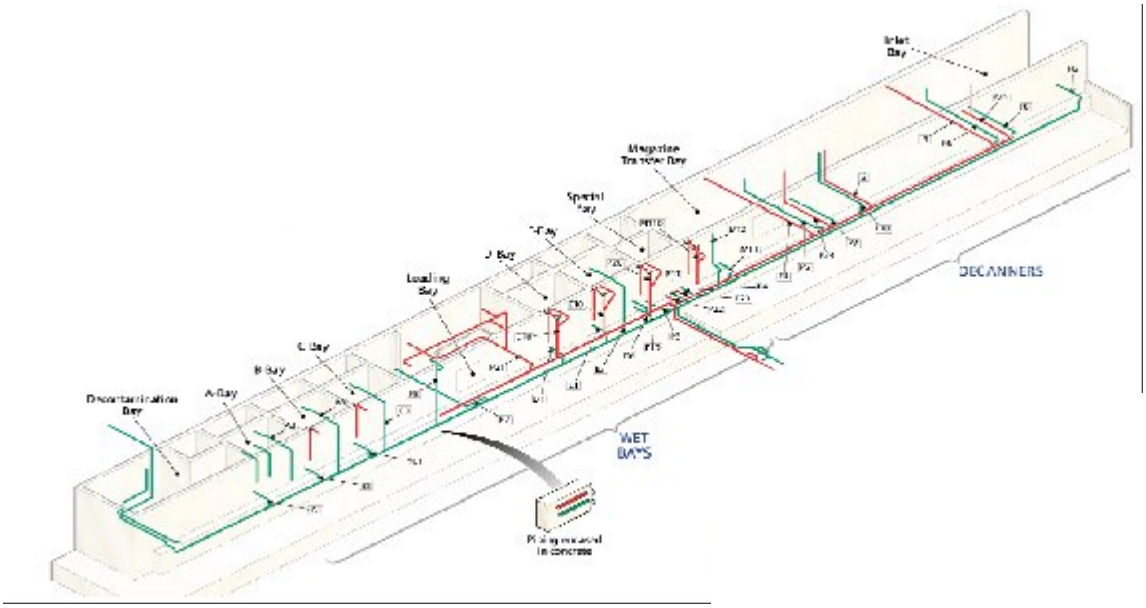

Fig. 2. Schematic of South side of the building showing an overview of the purge system. This is included to see the extent of the purge system rather than detail of the sections

At some construction joints there has been an accumulation of uranium salt deposits resulting in high dose fields in their vicinity, restricting access, working times and in some cases prohibiting access completely. The purge system also connected the pond and bays hydraulically to an adjacent "settling tank" used to remove particulates from the pond during very early operations. This is a smaller, open pond at a much lower level than the main pond

Existing Safety case

A modern standard safety case on a modern nuclear facility would define all the fault sequences which could lead to nuclear consequences. The design of the facility would have removed these faults where possible or would have built in multiple layers of defence and diversity in the safety systems. The safety case would designate the key safety systems to ensure appropriate substantiation, testing and maintenance of those systems. These principles are built into the agreement the Sellafield Site has with the key

regulatory body on the assessment methodology for modern safety cases. The agreement is known as the L99 Understandings document (Ref 1) and in it there is the expectation that in line with the nuclear safety principles outlined above, a safety case would describe a safe working envelope, with its edges defined through a series of engineered protection measures, and a set of rules and instructions defining an operating regime to remain within it.

It has not been possible to make a case on the FGMSP in the same way. It is extremely difficult to build in layers of defence by making significant improvements parts of the primary containment. It has also not been possible to provide full secondary containment for the plant, so instead of the traditional approach, the case has to call upon a second layer of measures that would, on a more modern plant, be described as emergency preparedness. Indeed, they are a form of emergency arrangements but in this case they actually form part of the safety case itself. The basis of the case is not that a failure cannot occur, it is that a failure can be rapidly detected, the potential liquor flow contained and pumped back to the pond, and repairs can be effected. In other words a case cannot be made that the risk of containment failure is very small due to a series of protective measures. A case can only be made that the risk of such a failure having an impact on operations is small because there are demonstrable means to make immediate intervention when failures occur.

Clearly, retrieval of the inventory of this plant is an extremely high priority. Ironically, the plant age and design which creates the urgency for remediation is also the limiting factor for the pace of this remediation. The safety case is restrictive to protect the structure and some of its systems from operational problems. To remove the restrictions improvements need to be made to the structure or the understanding of it. This requires engineering intervention which introduces more demands on the structure and becomes subject to the safety case restrictions. This can be a frustrating position and without some different thinking is effectively a “catch 22.”

THE APPROACH TO MAKING THE CHANGE

The challenge then has been the management of the risks to as low as reasonably practicable while making interventions to improve the plant or remove inventory from it within the constraints of the safety case. It has been necessary to think differently and become very innovative in the approach. It has also been necessary to overcome initial resistance to new approaches by those who manage the safety case processes that are the company’s very cornerstones of nuclear safety and those who regulate the industry. While there have been continued efforts to engineer means to retrieve the material, remove some of the fault initiators and improve the structure there has also been progress to innovate and to break the “catch 22”. This plan has included steps to:

- Develop additional emergency arrangements that can be built into the safety case to provide a second layer of defensive measures
- Implement and sustain a programme of conduct of work and nuclear safety culture improvements to create a robust and confidence building foundation to bring along key stakeholders
- Find means to structure and formalise balance of risk arguments and engineering judgements to use them in lieu of engineering substantiation in our safety cases in a way that is usable by our operators and project managers and is acceptable to our regulators.
- Build on regulatory confidence to develop new ways of staging the regulatory permissions by completely restructuring the safety cases and the methodologies used in their construction.

The plan sets out a long journey that that has already been partly travelled. It allows an absolutely uncompromising position on nuclear safety to be maintained while removing many of the traditional constraints. There’s a long way to go yet but the following sections describe the successes that have been achieved to date in delivering this ambitious and innovative vision. This is done through a series of case studies describing what was achieved and relating the details back to the elements of the plan described above.

CASE STUDY OF EMERGENCY PUMP INSTALLATION

Summary of the Problem

As described earlier, parts of the contingency arrangements for the plant need to become an integral part of the safety case. One example is the provision of a capability to contain liquor and return it to the pond should the pond water purge system pipes which penetrate the structure below water level, fail. The safety case identifies a number of failure mechanisms:

- Failure of the pipe material through frost damage or corrosion
- Failure of the pipe material in a seismic event.
- Failure of the pipe material due to impact.
- Work within the pond or bays as part of risk reduction work or retrieval work causing an internal failure then inducing a flow in the system and overflow of pond liquor at the settling tanks.

Key elements of the work completed

Where access has been possible many of the pipes have been isolated using mechanical means or encapsulated in a foaming concrete. Accessible pipes have been protected from frost in the form of lagging and, where they are not accessible due to high radiation fields, remote heating banks have been installed and are used in winter months. Vehicle movements are restricted and crash barriers and extensive concrete shield walls prevent collisions. The settling tanks have been cleared of bulk sludge (close to 200m^3 now in modern containment) and remote access gained to the hydraulic links to the pond. The pipes there have been sealed using remote resin bag injection techniques which have been substantiated in off-site testing. This is a significant improvement in that the isolation can have a level of substantiation which does not rely on potentially unreliable historic data about the condition of valves in the line.

The remaining issues

The next step was to improve the contingency arrangements to support essential decommissioning work. An engineered trench acts as a sump for operational liquor arisings outside the wet bays and this was served by a pumping system. However, the necessary decommissioning work would create potential arisings beyond the capacity of the pumping system and any damage to the purge system would delay the essential work. It was very important therefore that the pumping capacity was increased and the reliability of the pumping system improved over a much broader range of possible demands. This work was essential to allow decommissioning work to progress elsewhere within the FGMSP against a very tight programme. The opportunity was taken to increase the system performance to provide adequate contingency during the future decommissioning work. The new system was significantly larger and would need a higher seismic withstand capability including its own diverse generator supply. Such a large and substantial system would prove difficult to install in a constrained area and the safety case would have to consider the interactions with the FGMSP and the transient risks associated with doing the work

Innovation in Making the Case for Installation of New Pumps

To avoid too much technical detail, the work is related back to the overall plan. The safety case for installing and operating the pumps is extremely complex as close access is needed to the pipe-work and service lines bringing the risk of initiating a failure; a classic “catch 22”. It was considered whether it would be better to produce a large safety case to cover all the work before starting with significant time penalties in preparation, approval and regulatory permissioning or to stage the safety case with a significant increase in workload for approval and regulatory permissioning.

The best of both options was achieved. An overall large case was commenced which quickly identified the main risks and optioneering showed the least risk method of approaching the tasks. By working with the regulators and presenting a proposal to them it was shown that although the risks of pipe failure exists and the consequences are significant, the protective measures could all be condensed down to two main areas, control of the installation (mobile crane operations close to the building) and provision of contingency measures to allow liquor to be contained and returned to the pond and the pipes repaired should the worst happen.

Rather than wait for time consuming detailed assessment of high volumes of detailed hazard analysis by the Regulator and rather than try to devise and substantiate engineered protection, a different case was made. It was based on the premise that it could be demonstrated to the Regulator through emergency exercises that the emergency preparedness was extremely robust and could be considered as a layer of defence. It was also based on the premise that on- site inspection of the mobile crane lifting arrangements prior to committing the plant to any risk from those arrangements could show robustness of those arrangements to the extent that they, too, could be considered as a layer of defence. Given the urgency of the work, we were able to make a compelling balance of risk argument that the level of assessment normally expected for the level of risk would add only time to the work for no value.

To achieve the goal, a hold –point logic was created in the form of a safety case phased implementation plan. Regulators attended emergency exercises over a number of months where capability to recover was well demonstrated. At the specific hold points, they sent appropriate experts to inspect trials of the lifting arrangements using a mobile crane off site. They also sent the same people to inspect the arrangements prior to the real crane lifts. This included an inspection of the controls, the training and the equipment itself. It proved to be a very effective confidence building exercise and what would normally have expected to be between 3 to 6 months of assessment was turned into two, 3 hour site inspections, and the safety case approval and regulatory permissioning effectively never ventured onto the project critical path.

Since the successful installation work of the new pumping system, it has been possible to apply the same model in a number of ways on subsequent work (with similar risks and potential consequences). The receipt tanks for the pond sludge when it is retrieved are under construction close to the plant. That work is effectively under self-regulation in recognition by the regulators that the safety case is based around control of lifting on the site and the crane collapse risks close to the pond (and other nuclear facilities close by). Other key work has been carried out by other parts of the site which has put the purge pipe-work at risk due to significant vibration effects (very large crane lifts in an adjacent plant and demolition of facilities near by). The case has been made based on enhanced emergency preparedness which has been demonstrated through inspection and exercise rather than purely through a traditional hazard analysis case.

A very similar case was later made for a lift of a new machine onto the gantry supporting the pond skip handler, a travelling overhead crane spanning the pond carrying a mast used historically to move containers of nuclear material to grid locations in the pond. The new machine was designed to refurbish the gantry system and was to be lifted on to the gantry rails in a single lift using a 1000Te mobile crane. This carried the highest category of safety case we have. Typically a case of this magnitude would require over 6 months of regulatory attention before receiving permission. Some benefit from early regulator engagement was expected but permission was received within 10 days, a record for the Sellafield site, by using the on site inspection approach and enhanced emergency preparedness.

In addition, the hold point strategy employed on the pump installation has now been developed into an overall strategy for all of the plant's project safety cases. In early days at the moment, the concept of "inspection windows" at key parts of the projects where the fault conditions lend themselves to this approach, has been accepted by the regulators and many high safety category safety cases, usually expected to take up 3 to 6 months of regulatory engagement time, have been narrowed down to a few days of inspection opportunity. While the detailed assessment work is still needed to prepare the work, it can be more easily kept away from the critical path.

CASE STUDY FOR RAPID INTERVENTIONS SAFETY CASE

Background to the Need for this Case

As described earlier in the paper the purge pipe work system forms part of the pond's primary containment. These service lines were part of the original 1959 installation and are in poor condition. Before the new emergency pumping system was installed there was reliance on a much lower capacity pumping system. While that system was still operational, there were two key events on the plant that gave some good learning themselves but together drove the need for a new type of safety case to suit the needs of the plant programme.

Fig 3 showing the service lines above the purge pipes and a close up of an example of a corroded section. of the purge pipes

The first such event was a failure of one of the redundant service lines. Not all of the line runs above the purge system and a section of this particular 200mm diameter water main failed where it crossed the street adjacent to the plant. The failure mode was corrosion of the pipe hangers in an area where adjacent steam pipe lagging had held up rain water. A number of hangers failed following the transfer of load after the first failure and the pipe sagged and cracked. There were immediate lessons on care of redundant services but also for potential for failed, redundant services fall onto key safety equipment (emergency pumping system in this case). It was also obvious that the sections of pipe over the purge system might also fail.

The second such event was the partial failure of a small vent section of the purge system which lay above the pond liquor level. The failure mode was again corrosion of a mild steel section. In this case, there was a high potential to delay other important work. The pipe did not fail completely but lost sufficient section to crack and start to lean. The vent pipe was directly above the most corroded part of the purge system which was also in the highest radiation field making direct access very difficult (up to $9Svh^{-1}$). There was an immediate risk of the vent pipe failing completely and falling onto the purge line below.

This was treated as a plant abnormality and an incident control centre was set up to manage the recovery. In such cases there is a requirement of the Sellafield Site Licence to plan and risk assess the recovery operations quickly, not wait until a formal safety case has been produced. That is produced retrospectively for the information of the regulators. A command and control approach is taken to working up recovery options and making appropriate option choices through a risk assessment process to ensure that the recovery does not worsen the situation but recovers from the situation as quickly as is safe to do so. In this case a successful intervention was made after evaluating a number of options. There were only a few hours of daylight left and the winds were forecast to increase. The option to restrain the failed vent pipe from

above and then to cut it free and withdraw it into the building was chosen to prevent the situation worsening. During the operation, another repair team was also on standby in case the worst were to happen.

The following day the urgency of the situation was over but there were further recovery operations needed. It was likely that the remainder of the vent line had limited life before it too would fail. There were also similar vent lines on other parts of the system. It was clear that further interventions would be needed to prevent further failures arising. The arrangements under the site licence are focussed on either an emergency or business as usual. There is no middle ground which considers an urgent situation which may develop further in hours or days. It was clear that some judgement was needed to follow the safety case route as closely as possible while allowing a plant intervention as early as possible. Without any in-depth thought it was also clear that the risk of damaging the primary containment would exist for the intervention and this would mean the safety category of the "plant modification" would be such that Independent Nuclear Safety Assessment would be needed and also regulator permission. Plant modifications are also categorised for environmental impact potential and this would be the highest category requiring internal approval by the site Nuclear Safety Committee chaired by the head of the site.

The first Intervention Safety Case

To produce a full safety case for a plant modification of this category would normally take months with 3 months of approvals. We needed to deal with our problem within a few days. For the answer, consideration was given to what had just been achieved in recovery from the emergency situation. The appropriate people had been used to quickly identify what could go wrong and what the worst consequences would be. Options were identified for the completion of the work which would remove or control the risks. As a back up, preparations were made to recover from the worst case event which could occur if the work went wrong. From one perspective this is no different to the basic steps of producing a full safety case. The work is technically simple enough that the bounding risks are already known or simple to identify without a complex hazard identification process. The hazard analysis phase is reduced to a single step by assuming all faults cause a complete failure of the primary containment. The measures to control the risk and provide mitigation had already been identified during the emergency.

Consultation was made with the regulators, representatives of the Independent Nuclear Safety Assessment, those who run the processes for the Sellafield site, safety case authors familiar with this area of the plant and some complete independents to act as a peer check. The output after a day around the table together was a detailed method statement which identified all the protective measures needed to do the work. These were designated as Required Operating Instructions and Safety Features in the same way as would have been designated through a safety case written through the usual processes. From this it was then possible to produce a very simple and fit for purpose modification proposal to take through the approval route.

The situation was also discussed with the regulators who agreed that the work was urgent and supported the position that given the level of urgency they were comfortable that the appropriate level of risk assessment had been demonstrated and the risks associated with doing the work were manageable. The methodology had identified and designated appropriate safety measures and there had been both peer checking and agreement by Independent Nuclear Safety Assessment. The latter would normally issue a certificate to indicate full compliance with the assessment process. This was not possible given the different approach. However they were able to advise the Sellafield site and the regulator that the process that had been followed was robust and fit for purpose and we were able to proceed and remove the remaining vent line safely.

Development of the Rapid Intervention Safety Case.

Having delivered the above work safely, it was clear that given the condition of the purge lines and the services and other ancillary equipment, the situation was likely to arise again. Now that the situation was foreseeable, such a reactive approach would not be acceptable. However, it had now been proven that the work could be done safely and there were elements of the production of the "safety case" that could be used again. The immediate safety driver to do things differently to the normal safety case was no longer a key factor so support within the organisation and from the regulators would prove to be a much tougher battle.

The figure 4 shows on the left hand side, a summary of what had been achieved procedurally after removing the remaining vent line. To the right is what was proposed for a future case. A "PMP" is a Plant Modification Proposal which is the summary document to implement the safety case for a modification to the plant. Under the Sellafield Site Licence, PMP's must be categorised according to the potential nuclear and environmental consequences of the change introduced, either by virtue of the nature of the change itself or the work going wrong. A category D would have little nuclear safety impact, A category C would have minor consequences on the site, a category B would have significant consequences on the Sellafield Site and trivial off-site consequences. A category A would have significant consequences to the public. The first PMP was a retrospective one produced for the emergency. The second was the one produced to carry out the very urgent work. An OSM is an Operational Safety Memo and is a form of safety case we use to support plant modifications.

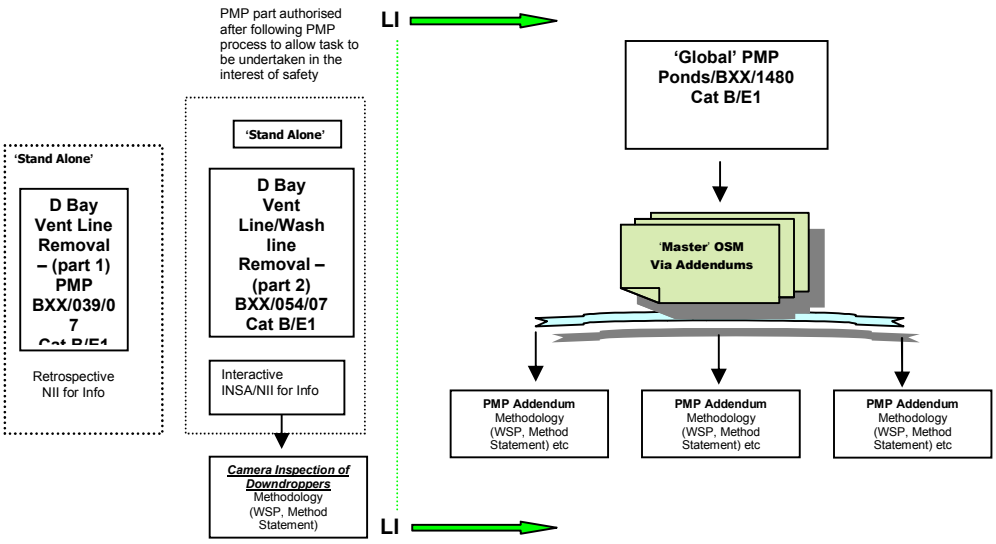

Fig. 4. Overview of the Rapid Innovation safety case

The basis of the proposal was to validate the earlier work by underpinning it with a safety case produced through the normal route and approved in the normal way. However, in this case it was not yet known what interventions were needed; it was only known what the bounding risks were, i.e. collision with the purge system or dropping things on it. Both were assumed to have the potential to cause a breach and hence needed safety features and the back up of emergency preparedness to be proven. The concept then of being unable to fully define the scope of work but demonstrating that it can be done safely (and recover if it goes wrong) was a tough one to introduce. To the regulators this might seem like a licence to do anything without seeking further permission and it would be potentially seen internally as a system "work around".

It was neither of these things, but to justify the approach, additional controls were needed. What is seen in the figure 4 is effectively a process to produce a simple safety case to show how the engineering methods, to make a particular intervention, meet the safety function requirements which are identified generically

based on the previous experience. The Operational Safety Memo identified the safety function requirements of whatever would be used to prevent collision with, or dropped loads onto, the purge system. Each intervention would have its own simple case demonstrating how the safety functions are met for the particular engineering involved to the standard expected of any safety case where the consequences have such high potential. A Plant Modification Proposal for each intervention would be extremely repetitive in that the process would force it to describe all the work, hazards and risks whether they were generic or not and as it would have to "stand alone" it would have to introduce the reader to the overall concept and describe the plant and the conditions each time. The FGMSP had already been piloting a new approach to making changes "in flight" to Plant Modification Proposals through the use of an addendum to highlight all the changes separately while leaving the original intact and unchanged. This allowed the approval bodies to track the changes very easily and the scope and impact of the change was far more evident than a full re-issue of the document with the changes buried in the detail. This concept was adopted for the new safety case. The Operational safety Memo would be implemented through a single Plant Modification Proposal. This effectively introduced a new local process whereby addenda to the Plant Modification Proposal would be used to substantiate the engineering and methodology used for individual interventions. In this way the regulators and internal approval bodies would only have to approve one Plant Modification Proposal and the safety case (The Operational Safety Memo) that it implemented.

Within the process, to improve the level of control in lieu of the very formal process of seeking regulator permission for each intervention, it was made a requirement that each intervention proposal (an addendum to the Plant Modification Proposal) should be approved by the department Management Safety Committee, a committee one step higher up the safety management hierarchy than the Plant Modification Committee which would usually approve these cases. This offered protection against the process being used outside of its original intent (i.e. for urgent intervention work). Each addendum would also be sent to the regulator for information prior to the intervention taking place. This allowed any concerns or issues to be raised without the need for any further formal assessment leading to permission.

Implementation of the rapid Interventions safety Case

The case was taken through a very protracted approval route due to its novel nature and high consequences if things went wrong. This included the departmental Management Safety Committee, the Operating unit Management Safety Committee and then the site Nuclear Safety Committee. The latter has a large contingent of external (to the company) membership and is effectively the ultimate peer challenge. This committee wanted the endorsement of the site process owner for safety cases to agree that this was a legitimate way forward and not a "work around". They did and after a long challenge and after some considerable time spent with the chairman (the company Managing Director) "off-line" there was agreement to proceed.

The process has since been used for twelve separate interventions which could be argued to have saved more than 3 months each in progressing the remediation of the pond. These have included:

- Deployment of a wheeled remotely operated vehicle to venture into otherwise prohibitive radiation fields and inaccessible areas to inspect parts of the purge system where there were particular concerns over imminent failure. The safety case called for the substantiation of the tethering system so that any failure of the controls would not lead to a collision with the purge system.
- Removal of redundant equipment causing potential obstructions to flow of liquor to the pumping system should the purge system fail and leak. In this case it was control of access and tethering of tooling which carried the key safety function.
- Deployment of endoscopic cameras into parts of the liquor and waste filled bays themselves to gather information on isolation requirements and to identify a potential leak path. The substantiation of the deployment rig was key in this case.

One final control that was put in place on the case was that it would self expire or time out and needed regulator approval to revalidate it. That time is nearing now and the regulator who was so sceptical and

challenging last year, now is encouraging expedition of the approach to have it revalidated as the benefits have become very clear and the robustness of the safety controls have been self evident in each case.

CASE STUDY FOR RETURN TO SERVICE OF THE GANTRY REFURBISHMENT SYSTEM

This case study considers how a case was made to re-start operations using the gantry refurbishment system following suspension of operations after problems in early operation identified weaknesses in the safety case. That made this one of the most challenging cases to make. It required a very strong foundation of regulator confidence and another novel approach formalising management controls in a way which made them as acceptable as engineered means of protection.

Background to the Need for the Case

The gantry refurbishment system is a large double bridge structure spanning the pond. It is able to run the length of the pond using the pond skip handling machine to act as a pushing and towing vehicle. Its purpose was to provide safe access and lifting capability to allow the gantry itself and the skip handler rails it supports, to be refurbished. The whole of the rails and gantry are fundamental to the remediation of the pond as the skip handler is needed to deploy the retrievals equipments and to move the containers of fuel around the pond. Its condition had degraded due to 50 years exposure to a wet coastal atmosphere and corrosion had made it unsafe to use.

Fig. 5. The Gantry refurbishment system over the pond (the central yellow structure). To the right is the skip handler (also yellow)

There had been a safety case made to operate the gantry refurbishment system which relied on a lot of management controls where engineering of safety mechanisms and safety features was either impractical or the working dose fields made it almost prohibitive. The focus of the safety case had been to prevent the combined machines advancing further than intended along the pond. There was to be a strict regime of rail inspections and small advances to allow the rails to be refurbished without any significant weight from the

combined machines being transmitted through them. In the worst case scenario, if the machines were to travel onto unrefurbished rails, the structure could collapse.

The safety case was challenged after some problems during early operations and a means needed to be found to strengthen the case without introducing delays for major engineering work. More importantly, the gantry refurbishment system had been lifted onto the rails as described earlier in a single 1000Te mobile crane lift. This had been difficult to justify due to the transient risks but a balance of risk argument had been made successfully. A case to remove the GRS from the rails to modify it to include better engineered safeguards would be a last-resort option. Therefore, the safety case needed to be strengthened through management controls which needed to be made more robust and acceptable as viable options to engineered measures.

Regulator Confidence

The case to continue operating the GRS would have been too difficult to make had it not been for existing high regulator confidence in the teams. The view of the regulators had been transformed over the previous 12 months by an aggressive sustainable programme of improvements to the management of nuclear safety and the nuclear safety culture. There was a risk that the degraded plant conditions could be all too easily lead to a decline in the nuclear safety culture. The very successful delivery of the first year of the improvement programme was key to ensuring that this was not the case and earning the confidence of the Regulator. The programme was too extensive and complex to discuss at length in this paper but some aspects were crucial to the case in question:

- Many physical improvements to the plants containment and systems for early detection of problems. This included replacing many old and degraded sump and collection vessel level systems with modern ones and cleaning out of redundant equipment and decontamination of areas to allow access for inspection.
- The strengthening of “human performance” by the introduction and embedding of specific human performance tools. These included tools to improve the questioning attitude at all levels of the organisation, tools to strengthen critical communications during important safety operations, and improved training for those with key safety accountabilities.
- Significant physical and cultural improvements to the operation of the plant control room based on the WANO guidance. Much of this was supported by field engineering work on the plant to remove “standing alarms” from the control room. These are plant indicators which have been in continuous alarm due to historic configuration changes or equipment becoming redundant. The “alarms” had been a distraction so the improvements made were very significant. Combined with the installation of improved plant monitoring systems, this laid the foundations to introduce big cultural changes to the control room. There is now in place a control room charter, an improved set of instructions and procedures and an operator focus on key nuclear safety parameters. These improvements have received extremely positive feedback from many of the Sellafield Site’s key stakeholders.
- The use of learning from the Texas City refinery disaster of 2005 to create nuclear safety focus boards and nuclear safety “dashboards” using a process called “Process Safety Indicators” or PSI.
- The introduction of daily nuclear safety focus meetings at both plant supervisor level and management level giving strength and support to a solid and growing nuclear safety culture. The meetings ensure that the plant condition and emerging problems are appropriately prioritised along with the remediation work as part of scheduling for the day.

The parts of the PSI process used result in fault sequence identification and identification of “layers of defence” against those fault sequences. There are some similarities to a safety case production process but unlike the safety case process, the PSI process does not dismiss faults based on probability or frequency grounds. It simply asks what disaster looks like for the plant, what are the routes to reach it and what stops disaster being reached. The nuclear safety dashboard is a visual representation of the layers of defence

identified by the process. It does not replace the safety case as a means to justify operation; it merely makes visible how many layers of defence there are and what is their condition or status at any given time. It can be used as a live operational tool to drive decisions and to alert the operators and management if the integrity of individual barriers become degraded or the number of layers of defence becomes reduced. The use of the dashboards and the focus meetings to discuss them daily has been a great success and the main confidence builder with the regulators.

Making the Re-Start Case

There were two key elements of innovation used to make the case in the difficult circumstances already described. The first was the adoption of a process to justify operating with a safety case with known gaps or shortfalls. There have been some forms of this approach used outside of the site but this was the first such approach for an application like this. It was decided to adopt this process in its infancy and adapt it for use on a decommissioning building like the FGMSP. It was used to justify proceeding with urgent refurbishment work to support waste retrieval from the pond with a safety case that had shortfalls against modern standards and the potential consequences of failure were very high.

The original case was restructured to remove the parts of the operations with the shortfalls from the scope where practical to do so. For example there were many fault sequences involving the combined machines driving onto unrefurbished rail. The scope was reduced to allow only manual movement using a "hand wind" procedure until the engineering protection against these faults had been substantiated, an extremely lengthy process. The justification prevented schedule delays due to the substantiation of the safety features but placed greater onus on the management controls.

That leads to the second area of innovation. The challenge was to improve the integrity of the management controls to justify their use in lieu of substantiated engineered measures. The use of the PSI process in producing a nuclear safety dashboard for the plant was the source of an idea to apply the process uniquely to the gantry refurbishment work. For this there was no template to follow and no guidance on how to apply the process in this way. It is very important to realise that the process does not replace the safety case process on the project. Instead it allows better use of all of the layers of defence, including those designated by the safety case, but also those which could not stand alone in a safety case for lack of adequate substantiation and those which exist by virtue of the management controls in place. The visualisation of the defensive layers on a dashboard bring a formality and structure to the controls which was missing from the original case.

The modified safety case and the justification for continuing with the shortfalls were submitted to the regulator for permission to re-start after internal approval. The regulators were invited to inspect the management controls and the use of the dashboard as the key management and operational tool and they recognised that many months of assessment and substantiation work were saved with no detriment to the nuclear safety of the work

CONCLUSION AND A LOOK TO THE FUTURE

By taking a journey through three case studies, the paper has put into context the challenges associated with waste retrieval and decommissioning of the FGMSP at Sellafield in the UK. It has given examples of innovation and creativity used to meet the challenge and make progress. It is not just about the technical challenges although some of these have been described to allow the reader to understand the environment in which the judgements, decisions and cases have been made and to act as a vehicle to explain the innovation that has been applied. Within the 3 studies it has been shown that:

- The plant safety case is very unusual and uses contingency arrangements to demonstrate that primary containment failures, though predicted, will not result in significant environmental release

- The safety case requires more and more the use of judgement and management controls. New tools have been developed and existing ones adapted to make judgements and management controls usable and demonstrable in a modern safety case.
- Improvements in nuclear safety have boosted regulator confidence and the innovative use of Process Safety Indicators has allowed the construction of more fit for purpose safety cases and strengthened the management of nuclear safety.
- Lessons have been learned from how we assess risks in an emergency to make parts of this approach applicable and usable in a safety case.
- Safety cases can be constructed to facilitate on-site inspection to minimise the programme implications of detailed assessment of the hazard analysis allowing regulators to give permission against hold point programmes rather than initial full assessment.

The work that has been done in driving innovation into difficult safety cases is only the start. There is more to come but there are now have the foundations to develop flexible permissioning with our regulators (and this is already bearing fruit), to develop generic safety cases where the risks can be bounded (we are building this philosophy into our main retrieval project safety cases now), to use the PSI process to expand and simplify the plant safety case with a direct link to the daily control tools, and to better formalise other parts of our emergency arrangements to expand the case further. This enables us to maintain an uncompromising approach to nuclear safety but find the right balance to progress the remediation of the First Generation Magnox Storage Pond with an innovative, flexible but very robust safety case to meet the challenges we face.

REFERENCES

1. L99 BNFL[(note 1)]/NII Understandings, Issue4, November 2004

Note 1
BNFL is British Nuclear Fuels plc, the parent company for the Sellafield site before 2008. NII are the Nuclear Installations Inspectorate, a division of the UK's regulatory body, The Health and Safety Executive. The "Understandings" are the output of discussions between BNFL and NII on the methodologies and standards to be used for safety cases on the Sellafield site, now adopted by Sellafield Ltd the current licensee.