THE REDUCTION OF MAN ACCESS INTO NUCLEAR PLANTS BY EFFECTIVE DESIGN AND THE APPLICATION OF FAULT TREE ANALYSIS

K. Branton
NIS Limited
Ackhurst Road
Chorley, Lancashire
England PR7 1NH

Dr. D. M C. Horsley
BNFL Engineering
British Nuclear Fuels PLC
Risley, Warrington,Cheshire
England WA3 6AS

ABSTRACT

The pursuit to reduce exposure and dose uptake for personnel operating and maintaining nuclear plants presents major challenges to the designer. He is generally presented with specific requirements for throughput, availability and product quality, but these are increasingly supplemented by tight restrictions on man access. These restrictions may impact on both the frequency of access and also on the degree of radiological hazard encountered on entering the active area.

On one of its latest facilities, British Nuclear Fuel's Waste Packaging & Encapsulation Plant at Sellafield (WPEP), the key design parameter was the restriction of man-access for maintenance purposes to once in five years. The starting point to develop a compliant design was to examine established nuclear engineering practice, using a combination of engineering judgement and analytical techniques.

Fault tree analysis, chosen as the most effective method of evaluating the overall system highlighted the relative merits of the various design options proposed. From this first phase of assessment, a design philosophy was established, namely to minimize complexity, impose close controls on innovation and to examine the reliability of the system and components in considerable detail Design development focused on the critical components and enabled engineering resource to concentrate on design problems of high significance. Having defined the subsystem components more accurately, the use of published failure rate data then allowed reliability to be measured against the design specification.

It was quickly established that much of the published information could only be used with caution. The majority of the statistical data related to "average" values and to operating environments far more arduous than those in the nuclear industry. The ability of the design to satisfy the specification could therefore only be assessed by a detailed interpretation of data. From this it was concluded that reliabilities in the upper ranges of the published values could reasonably be expected. In several cases the volume of information available was insufficient to form the sole basis of reliability assessment. As a result, strict manufacturing quality controls and test procedures were specified to ensure satisfactory in-service performance.

In conclusion, the design of plants such as WPEP, against rigorous design criteria places considerable onus on the verification of failure rate data. This process is likely to assume increasing importance, in the drive to reduce exposure and dose uptake. The collation of data specific to the nuclear industry offers major benefits to plant designers, operators and the industry, as a whole.

INTRODUCTION

This paper addresses the impact of design criteria which restrict man access - for maintenance purposes - to extremely low levels on in-cave equipment for an intermediate level waste solidification plant. The practical problems which arise when such criteria are imposed, and their solution, are examined by reference to a specific case study - the encapsulation caves on the British Nuclear Fuels PLC Waste Packaging and Encapsulation Plant (WPEP) at Sellafield in North West England.

PLANT DESCRIPTION

The plant is designed to package a range of active feeds: ferric hydroxide floculent (discharged from the adjacent enhanced actinide recovery plant (EARP); scrap equipment (typically ultrafilter cartridges, process valve assemblies) from a centralized effluent plant maintenance facility (EPMF) and particulate solids from the segregated effluent treatment plant (SETP).

The plant comprises two identical, handed, encapsulation caves and an integral drum store, to provide interim storage for the packaged wastes, pending the construction of a long term storage facility. (See Fig.1).

Clean empty drums are transferred from the receipt bay, via a quality assurance station, to a roller conveyor, adjacent to the encapsulation cave inlet. These drums are posted into the cave, as required, through a transfer system and double shield door arrangement.

Bulk powders, from which the cementitious encapsulant is derived, are delivered by tanker to bulk storage silos.

At the first mixing cell, metered quantities of floculent (previously transferred from EARP to a receipt/holding tank) and conditioning agent pneumatically transferred to a charge vessel located on the cave roof are introduced into the close coupled drum. The drum contents are mixed for a prescribed time, after which the drum is transferred to a flat belt conveyor to "condition".

During the conditioning period the drum is transferred to a second similar mixing cell. Metered quantities of the encapsulant media, having been previously blended by air injection, are introduced and the drum contents then mixed for a specified period. Some future feeds, such as the SETP feed may be charged into drums at the second mixing station, bypassing the first cell. After mixing, the drum is transferred to a second, similar flat belt conveyor, to cure.

After curing, the drum is introduced to a grout-capping station, where a final clean layer of grout is applied and the drum lid is finally affixed.

The external surface of each drum is then swab-monitored at a separate station for alpha, beta and gamma contamination, on completion of which, clean drums are transferred to the drum store via the cave export shaft.

Any drum which indicates levels of surface contamination higher than the permissible limits is transferred to a decontamination facility, comprising a high pressure water jet cleaning unit. The decontaminated drum is then returned for re-inspection prior to export.

Solid wastes from EPMF are processed in a specially designated area of the cave. Received via a shielded transport flask, the solids are processed in an intermediate waste container, by grout-filling, before being transferred, after curing, into a product drum compatible with the main process route.

DESIGN PARAMETERS

The development of a design to meet key criteria, in terms of availability, through-put and product quality on WPEP was largely a matter of good engineering practice and of the extent to which the parameters could be achieved. The essential skill was to recognize the degree of accuracy

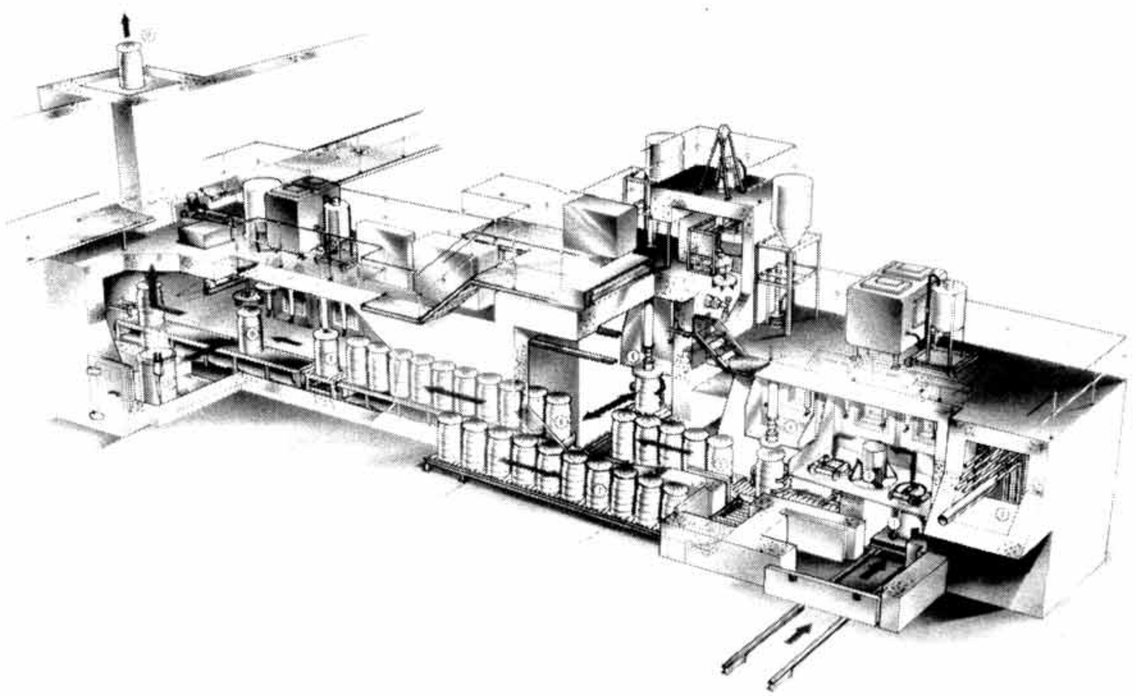

Fig. 1. Waste Packaging and Encapsulation Plant (WPEP).

required and then devise appropriate measurement techniques. Furthermore there was a need to choose and use the correct techniques for nuclear plants where the potential costs of failure generally outweigh those of prevention (and to adopt an appropriate design philosophy). WPEP provides a useful illustration of this particular skill.

The original plant specification by H&G Engineering (the principal contractor on WPEP), included process descriptions, shielding and dose uptake criteria, seismic design, battery limits decommissioning and cave maintenance requirements. This provided the design reference and established key plant criteria as follows:

- The frequency of man access to the caves for the purposes of maintenance must not exceed once in five years.
- Drums must be free from surface contamination before exit to store.
- The plant must achieve specific annual availability and production targets, in addition to the daily throughput requirement.
- The plant must ensure that the product drum contents are within allowable tolerances.
- The plant must not exceed specific limits concerning man-dose uptake assessments.
- The design life of the plant is 30 years. Individual components must have a design life of not less than 10 years.

The most significant of these parameters, in the context of this paper is the restriction on man-access. The underlying design criterion was to restrict the probability of equipment failure resulting in a plant shutdown, or break of containment for the purposes of man entry into the caves to not more than once in five years. In addition, the limits on man dose uptake and cleanliness of the exported drum necessitated a clean cave philosophy. In fact, the maximum allowable surface contamination levels for product drums on export to store are substantially less than those for C1 nuclear plant areas (where radiological or personnel monitoring is normally considered unnecessary).

The clean cave concept requires all radiation hazards and residual contamination to be removed in the event of man access. The paradox is that the plant has, at the same time, to make the event of man access extremely unlikely.

INITIAL APPROACH

The starting point to develop a compliant design for WPEP was to examine established nuclear engineering practice, by considering existing facilities of a similar type and philosophy. This was conducted in parallel with initial studies of the plant layout, within the constraints of an established process design, the available space envelope, and availability/throughput requirements.

Preliminary 1:50 and 1:20 layout drawings were produced, based on the engineering judgement of a highly experienced team. The layouts were used to prove the general design - particularly drum transportation and production throughput requirements.

With a conceptual design established, the first phase of assessment was conducted. The method chosen was a form of fault tree analysis, which was held to be the most effective technique for identifying the potential weaknesses of the system.

By constructing simple fault trees the relative merits of the various sub-systems and their significance to the overall performance, were appraised. This technique, based on engineering judgement and practical experience, enabled the design philosophy to be firmly established. It was decided to keep the complexity of the system to a minimum, to impose close controls on innovation, and to pay critical attention to reliability assessment.

Having determined the philosophy a thorough review of the earlier work, which included an iterative process of refinement, enabled a revised conceptual design to be established, to offer the best prospect of satisfying the performance criteria.

One example of the philosophy influencing the concept was the emergency drum recovery system (EDRS). This complex device was a means to transfer all drums to the product drum store in the event of equipment failure and is necessary due to the requirement for a clean cave in the event of man access. Appraisal of the design options had discounted the use of permanently installed or multiple handling systems. It was held that these options would increase the complexity and impose demands on reliability which would not apply to a single transferrable device. The design was modified to position the EDRS out-cave where it would be readily maintainable. In consequence, the EDRS did not need to be considered at all in terms of reliability assessments. The lesser ensuing problems were then those of posting in the crane without a major breach of shielding or containment, and the complexity of being able to remove all product drums to store using a single unit.

DESIGN DEVELOPMENT

Development of the design, concentrated on the practice of positioning critical equipment out-cave. Where out-cave positioning was not achievable equipment was configured for service, where possible, by master slave manipulators. This imposed on the detail design a requirement in some cases to incorporate unique design features to facilitate remote maintenance. On occasions this presented a choice between an established design which could not be maintained without man access or a novel device suitable for remote maintenance. One example was the selection of a bespoke design option on door bearings in the solids mixing cell, in preference to commercially available equipment.

It was recognized at this early stage that there would inevitably be items of equipment, which appeared to require man access. The alternative, and chosen, solution, was to configure this equipment onto removable wall plugs, which were subsequently arranged beneath the mixing cells. In order to maintain these items bagging or tenting techniques would still have to be employed but a break in containment would be prevented. (Even so, it would be necessary to remove radiological hazards from within the cave to achieve acceptable out-cave dose rates).

Sub-system fault tree analysis in the concept development phase focused attention on design elements likely to present particular problems, for example, drum positioning devices.

Drum positioning became a key issue as layout designs were developed and revealed that the spacing between drums could impose undesirable limits on throughput. In line with the design philosophy the original approach incorporated a simple positioning system which could not achieve the required degree of positioning accuracy now considered necessary. Due to the relatively large numbers of positioning devices required (some twenty pairs within each cave) the evaluation of the various alternative technical solutions and their reliability assumed considerable significance. In the final analysis photoelectric devices were chose on the basis of proven performance in a radiation environment, an ability to satisfy all the functional performance criteria and a high level of reliability.

Design development provided a comprehensive series of engineering flow diagrams (EFDs) and sequence and interlock definition documents (SIDDs) forming the basis for detailed hazard and operability studies (HAZOPs). The HAZOPs enabled a thorough review of the operation and maintenance of the plant, ensuring protection or recovery from hazards arising from any operational scenario, and decisions arising from them with respect to maintenance strategy and options had a significant effect on the ultimate design. In a typical example, it was considered necessary to provide additional or duplicate instrumentation to avoid process system or equipment faults resulting in the spillage of active material. Since this instrumentation was to be sited in-cave, the increase in components inevitably increased the probability of man access for maintenance, placing additional onus on the choice of reliable instruments.

In parallel to the HAZOP studies, the plant and equipment design was being developed to the stage of design proposal drawings (DPDs). These DPDs formed the basis of arrangement drawings, sizing and specifying critical items of equipment, identifying and locating instrumentation. At the same time, design calculations were produced to support the selection of equipment and to verify designs.

A more meaningful FTA could then be performed, to incorporate much more closely defined subsystems. This began with the acquisition of failure rate data for the critical components. The collation of this data allowed the first true measure of the design against the specification, and in particular the first measure of its ability to satisfy the once in five years man-access criterion. At the same time, this was the last opportunity to make substantial changes prior to the detail design phase within which the cost and time penalties for change would be significantly greater. It was therefore important to reach a meaningful and accurate conclusion.

USE OF FAILURE RATE DATA

At first sight, the acquisition of data appeared relatively straight forward, as many databases and reference sources exist. The problem was in identifying which data was appropriate, since many of the published sources presented "average" data which did not differentiate causes of failure. Indeed in some cases, the quoted values included human error, common mode and even secondary equipment failures. In consequence, such "average" values did not take into account the specific application and installation.

For standard components, viz bearings and couplings, where the volumes of published data was large and the practice of interpolation well established, safety factors, loadings and bearing life were calculated from manufacturers catalogue information and a sound qualitative case was established, and substantiated, to suggest that life would tend towards maximum and failure rates would be low.

For more specialized components, relevant data was less readily available and often related to very different applications and environments and its interpretation demanded considerable engineering judgement.

Generally, the extensive works testing and commissioning trials on WPEP will cater for the vast majority of early life failures, which might be caused by manufacturing defect, incorrect adjustment or 'infant mortality', and so reduce the overall likelihood of failure significantly.

In addition, potential wear out failure can be precluded in some cases by scheduled replacement. For example, each mixing cell incorporates a double seal to allow the product drum to be de-lidded and sealed against the cell. (Preventing the clean cave environment being exposed to potential contamination from the mixing cell). Research into reliability at a component level produced reliable evidence that seals could be supplied with a minimum ten year life. Investigation into specialized techniques for remote replacement of the seals in the event of failure concluded that the potential benefit was disproportionate to the increase in complexity and consequent "knock-on" effect on overall reliability. The chosen solution, was therefore, to change the seals after a five year period, irrespective of their condition.

The operating cycle of equipment also affected the assessment of reliability. In the case of the decontamination facility it is quite possible that the equipment may not be used at all. Consequently, although the calculated failure rate for the facility - which included conservative values for several novel components viz high pressure water nozzles - was initially high, when the potential usage was considered, it could legitimately be reduced to a much lower value.

In the example quoted previously, photo-electric devices had been chosen for drum positioning. The number of components involved, and their in-cave location meant that their potential contribution to the overall failure rate of the plant was very significant. The initial data acquisition program yielded statistical values spanning several orders of magnitude on this type of device from four sources including a calculated failure rate volunteered by the preferred manufacturer which was based on data for the individual components of the device derived from a further data base on electronic components. Here the designer's dilemma was clearly illustrated: adopting the worst case, the key design criteria would be jeopardized, whereas in the best case the equipment would be totally acceptable. Although experience and engineering judgement suggested that the chosen equipment would be reliable, very careful application engineering was still vital. Proximity devices to permit accurate drum positioning were selected on the basis of having no moving parts and minimal numbers of components. Furthermore, the amplifier/ transducer unit could be located out-cave. By concentrating on reducing the number of devices which would require man access for maintenance or repair, some 80 devices were sited out-cave - but still able to provide the necessary positional accuracy of in-cave equipment. A further 50 devices were arranged within the operational envelope of MSMs and 10 devices were sited on removable wall plugs. Thus, the number of components which required man-access was reduced from 145 to 5.

In some cases, failure rate analysis focused attention on design and manufacturing quality controls at a component level. An examination of electrical switch failure - using another fault tree analysis technique - indicated that the two most likely would be voltage and frequency fluctuations in the power supply or degradation due to the effects of radiation. Since the power supply for cave instrumentation is "clean" and stabilized, the most probable cause of any proximity switch failure would be degradation due to the radiation environment. As all the devices, including back-up switches, would endure the same degradation, the installation of redundant devices was discounted as an option. Having examined in detail the conditions in which the switches would operate, a much more valid assessment of its reliability could be made. In the event, the limited data available and the choice of equipment with an established track record in the radiation environment promised acceptable reliability. It was, however, decided to impose rigorous quality controls on manufacture with the object of improving the likelihood of non-failure. All the devices were tested prior to delivery and a batch sample tested to destruction at an irradiation test facility to verify the radiation tolerance. Control was extended to a level whereby even the transistors in the device were manufactured from the same semi-conductor crystal to ensure uniformity and validate the tests.

A further consideration, in this example, was that the failure of an individual switch would not produce gross contamination or breach of containment presenting a major hazard. This is important in keeping the exercise in context, and in considering the extent to which collective engineering judgement and qualitative argument may have been allowed to influence the interpretation of statistical data. That is to say that there are some situations in which it is more appropriate to take a pessimistic view than in others.

CONCLUSION

Taken overall, the application of fault tree analysis techniques, in addition to the findings of the HAZOPs studies and the initial conceptual design development, provided valuable guidelines for the detailed engineering of the plant. These collective activities enabled the critical design elements to be identified and, in consequence, the design effort to be expended on resolving the issues in proportion to their individual significance. In turn, the ground rules for these studies and analyses were established by the original design parameters which were considered, throughout, to be unalterable. The engineering judgement which was applied, both within the design team and in consultation with the client and various other specialist bodies, was focused on the achievement of a compliant design rather than challenging the specification itself. With hindsight, this was the correct approach, in that the design criteria - particularly the stringent limit on man access - was found to be ultimately achievable. It also ensured, importantly a quality of design and a level of confidence in that design which would otherwise have been difficult to achieve.

However, the function of validating system performance by reference to published failure rate databases quite clearly placed considerable onus on the engineering judgement of those involved. It can be seen from the examples cited within this paper, which offer a fair and reasonable representative cross-section, that the published data leaves much to be desired in relation to applications specific to the nuclear field, and to reprocessing plant in particular. Published reliability statistics are often derived from far more onerous environments than that encountered on

WPEP, so the use of data at the low end of the quoted ranges is justified. Major organizations in the nuclear industry, like British Nuclear Fuels often have long established databases, drawing on their own experience and providing a valuable internal reference in many instances. As the industry works towards further reductions in exposure and dose uptake these databases will become even more valuable and their benefit to plant designers will be increasingly significant.

BIBLIOGRAPHY

CHARLES O.SMITH, "Introduction to Reliability in Design".

W.GRANT IRESON, CLYDE F.COOMBS, JR "Handbook of Reliability Engineering and Management".

BALBIR S.DHILLON, "Quality Control, *Reliability, and* Engineering Design".

D.J.SMITH, "Reliability and Maintainability in Perspective".

ERNEST J.HENLEY, HIROMITSU KUMAMOTO, "Designing for Reliability and Safety Control".