Torness fuel route completion

J.R. Thomson*
E. Tottman-Traynor†
W.K. Burns‡

The fuel handling plant at Torness power station has been functioning since 1989 under operational constraints due to perceived shortfalls in the as-built equipment. This has limited the achievable station load factor. This Paper describes the nature of these shortfalls, and the work to rectify them which is currently nearing completion.

Introduction

The two advanced gas-cooled reactors at Torness first generated electricity in 1988. The reactors were designed for on-load refuelling at a reactor pressure of about 40 bar, using fuel route plant which is shown schematically in Fig. 1. However, during commissioning of the fuel handling, storage and dismantling equipment in 1989, deficiencies were identified which have so far restricted the station to refuelling with the reactors shutdown and pressurized. In addition, constraints were imposed on plant, which included measures such as manual isolation of certain plant drive motors when not in use, to prevent any possibility of their operation except in the correct operating sequence. Because fuel route cycle time and the availability of the fuel handling plant are critical to station output, these restrictions have limited the achievable station load factor.

The irradiated fuel route consists of the following major items of plant.

There is the fuelling machine, which transfers hot irradiated fuel assemblies at pressure from the reactor to a decay (or buffer) store, and from the decay store to an irradiated fuel dismantling cell (IFD cell), following a period to allow fission product heating to reduce in the decay store.

There is the decay store, which consists of 32 tubes (currently upgrading to 64) which store and cool irradiated fuel assemblies (see Fig. 2) at pressure until the fission product decay heat has fallen to a level appropriate for fuel assembly dismantling at atmospheric pressure in air.

There is the IFD cell (see Fig. 3), where the irradiated fuel assemblies are dismantled into the plug unit (which is reused), fuel elements which are transferred to the storage pond, and non-fuel components which are transferred to a waste vault.

There is also the storage pond, where fuel is stored in skips for an appropriate time prior to despatch off-site.

Finally, there is the flask loading cell, in which skips containing fuel elements are loaded into flasks for despatch off-site for reprocessing or, eventually, to the new dry fuel store which is to be built at Torness.

This plant is complicated by virtue of the complex operations which it has to carry out, and because of the high standards of protection which are necessary when handling hot fuel which has recently been discharged from the reactor. By way of example, the fuelling machine protection systems consist of some 2000 input sensors and output devices. The plant is designed to carry out some 100 charge/discharge operations per year.

The Torness station was designed to probabilistic safety criteria. The complexity of its fuel route plant and the number of potential faults make the rigorous fault and hazard assessment needed for probabilistic safety assessment a major task. To satisfy these safety criteria, having summed the assessed frequency of all potential faults, requires a very high standard of engineering in the protection systems. To satisfy the safety criteria and make the plant 'user-friendly' for the operators requires good dialogue between design engineers and plant operators.

Safety-related deficiencies with the as-built plant

Restrictions were imposed to limit the station to off-load pressurized refuelling only, and to introduce a range of operator actions to isolate safety-related drives throughout the fuel route when not in use, primarily because of the remote potential for spurious out-of-sequence drive initiation by the control and protection systems. These measures were considered necessary, in spite of the fuel handling, storage and disposal equipment having in most cases four channels of control and protection equipment against the most

* Engineering Division, Scottish Nuclear Ltd, UK.
† Operations Department, Scottish Nuclear Ltd, Torness Power Station, UK.
‡ Technical Department, Torness Power Station (seconded to Projects Division), UK.

Nucl. Energy, 1993, **32**, No. 6, Dec., 349–354

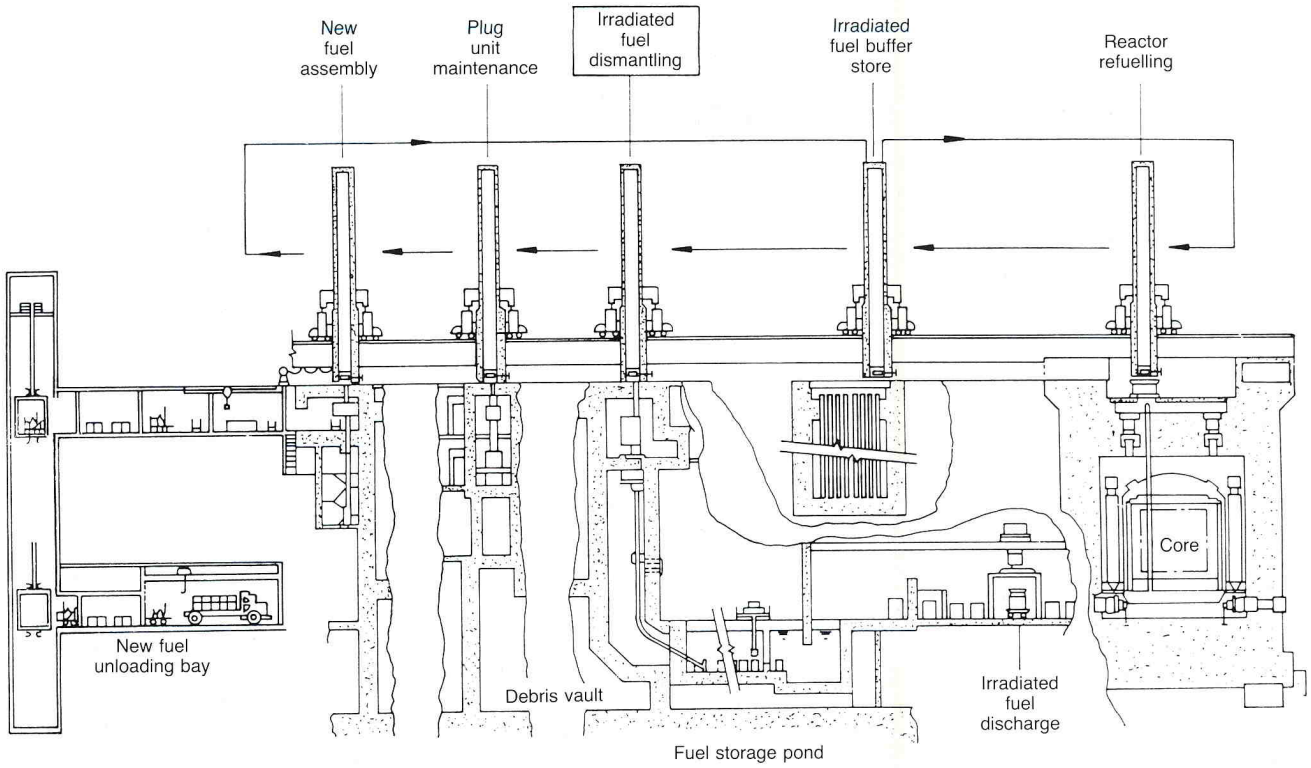

Fig. 1. Torness fuel route

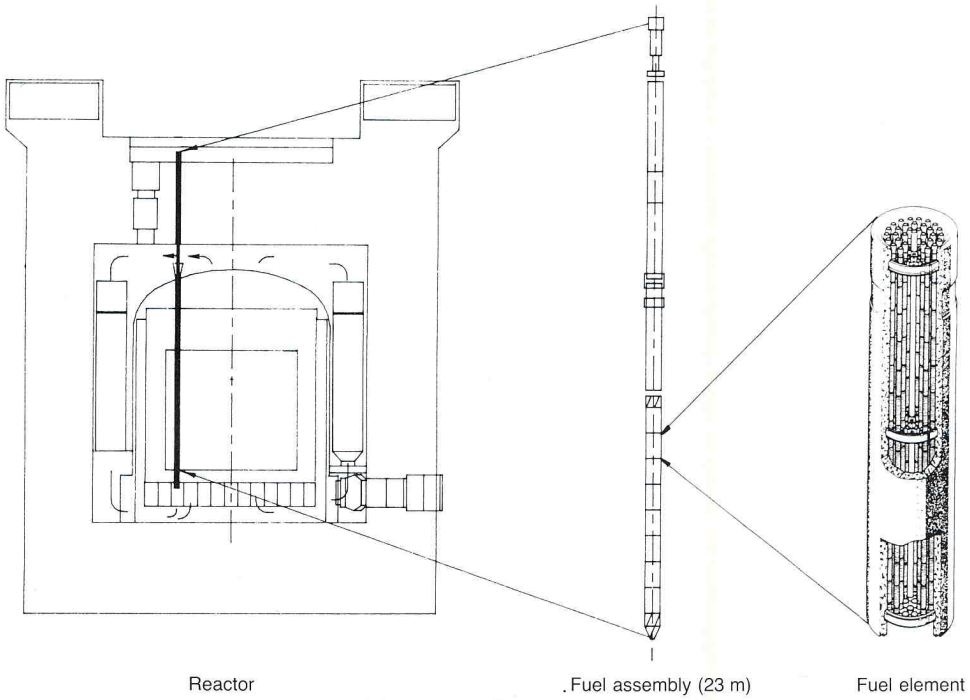

Fig. 2. Fuel assembly and reactor

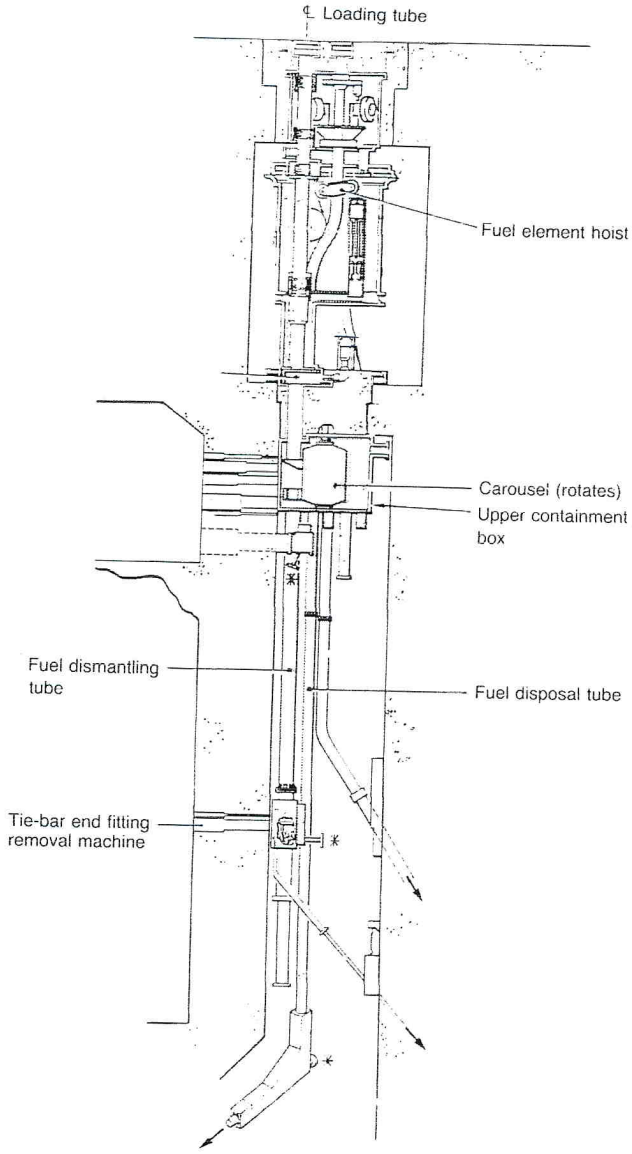

Fig. 3. Irradiated fuel dismantling cell

significant identified hazards to meet the probabilistic safety criteria set out in Table 1. This equipment consisted of two separate channels of microprocessor-based control and protection, usually backed up by two separate relay-based channels of protection. The design intent was that each twin-channel system should have an overall reliability of 10^{-4} failures on demand, and that the frequency of twin microprocessor-channel initiated faults should not exceed 10^{-3} per year.

These target reliabilities were necessary to ensure that the level of risk to the general public achieved acceptable values. The target frequencies adopted by Scottish Nuclear in the assessment of the acceptability of off-site hazards are given in Table 1, which shows that fuel route faults are 'allocated' a 50% allowance of total station risk.

The main factors which caused the claimed reliability of the equipment to be reduced related to the quality of the control and instrumentation (C & I) installed throughout the fuel route, and consisted of the following.

Quality control of the application software for the twin microprocessor channels, which was produced by two nominally independent teams to achieve diversity in specification and coding, was considered in some instances to be less rigorous than was necessary to achieve the design intent reliability.

The twin microprocessor channels used identical hardware and operating systems which were considered not to have demonstrated the required reliability.

The design had not separated control functions from protection functions in the microprocessor channels.

There was not adequate separation and segregation between relay and microprocessor channels, and in some cases electrical cross-links between channels had been engineered.

There was a lack of engineered test facilities and engineered override facilities provided for the relay-based channels. (Engineered override facilities are required for recovery from plant breakdowns. Overrides are applied only under strict administrative control.)

The as-built plant had been subjected to assessments of random failure rates using conventional reliability analysis, which in general showed that the target reliabilities were achieved. However, the plant was also subjected to a common mode failure (CMF) assessment, using a 'CMF cut-off' method, which employed reliability criteria as given in Table 2. (Other methods of CMF assessment exist, notably the Beta Factor method, but these are not normally used by Scottish Nuclear Ltd.) The CMF cut-off assessment method can be more subjective than a straightforward random failure rate assessment, since it is largely concerned with the quality of the installed plant, but it is simple to employ and does not yield answers with spuriously high accuracy. The conclusion of the CMF assessment was that the plant reliability showed a shortfall of about two orders of magnitude against the design intent.

In order to make good this shortfall, operator actions were introduced to isolate those plant drives which could

Table 1. Target frequencies adopted by Scottish Nuclear in the assessment of off-site hazards

Off-site release (ERL)*	Target 'half-station' total frequency: pry†	Target fuel route total frequency: pry
0·001–0·01	10^{-2}	5×10^{-3}
0·01–0·1	10^{-3}	5×10^{-4}
0·1–1·0	10^{-4}	5×10^{-5}
1–10	10^{-5}	5×10^{-6}
>10	10^{-6}	5×10^{-7}

* The emergency reference level (ERL) is taken as 100 mSv effective dose or 300 mSv to the critical organ.

† The term 'per reactor-year' (pry) refers to the frequency of faults associated with one reactor and half of the fuel route, i.e. half the station.

conceivably operate out-of-sequence in a fault condition and thereby lead to a radiological hazard. These operator actions enabled the plant to satisfy the safety criteria given in Table 1, but at the cost of longer refuelling cycle times and consequent reduced availability of the power plant. Operation of the refuelling plant in this mode was the subject of special safety cases referred to as 'interim' safety cases, and was only accepted as a temporary measure.

In addition to the assessed deficiencies with the C&I equipment, a further problem arose with regard to the integrity of the decay store pressure tubes. It was not possible to demonstrate with the desired degree of confidence that a dropped fuel fault at the decay store would not lead to pressure tube failure (in particular because in-service inspection of the tubes was not feasible), and the pipework supplying the cooling water jacket around each tube was not designed to withstand the high pressures that would arise in such a fault. Hence a fault scenario involving simultaneous fuel damage and containment failure had to be addressed. The conclusion of the fault analysis was that the radioactivity release from this unlikely fault could be kept at less than the emergency reference level (ERL, see Table 1) only if fuel irradiation was kept less than 12 GWd/te. This value contrasts with the design irradiation of 24 GWd/te, and it therefore was a major operational constraint for the interim safety cases. However, this constraint allowed early operation of the reactors (since the design irradiation corresponds to a dwell time for the fuel in the reactors of about five or more years, depending on the station load factor and the position of the fuel assembly within the reactor) until suitable plant modifications could be made.

A further difficult area was the IFD cell, where the complexity of the plant made development of the safety case slow. Initially the decay power levels of fuel to be dismantled in the cell were restricted to levels which impaired station output. (This arose because the cooling time for fuel in the decay store was excessively long.)

Finally, the dropped stringer reactor trip (DSRT) systems, which are essential for on-load refuelling to trip the reactor promptly in the event of a dropped fuel fault at the reactor during refuelling operations, were never fully commissioned. This arose because the other problems with the plant rendered the completion of the DSRT systems unimportant at the time the fuel route was first commissioned, since the interim safety cases restricted the reactor to off-load refuelling. Two diverse DSRT systems are installed at Torness. One system uses grab load to detect dropped fuel, and the other uses impact noise signals from the reactor diagrid.

Table 2. C&I CMF limits for fuel route protection systems

Limit	System features
10^{-5}	Extremely high integrity systems, e.g. laddic
10^{-4}	Reliable trip (or interlock) groups using fail-safe principles, or simple redundant systems, or systems with known operating experience
10^{-3}	Redundant systems, using fail-safe principles, but with non-fail-safe features
10^{-2}	Single channels with no specific fail-safe principles

Where more than one protection sub-system is claimed, products of the above CMF limits may or may not have a further CMF limit applied. The extent to which any further CMF limitation is applicable to products of the above limits is dependent upon factors such as diversity, fail-safe design, segregation/separation, testability, etc.

CMF limits are taken to be numerical (dimensionless) limits on the magnitude of the C&I protection claim in any particular fault sequence. However, the CMF limits are often quoted as 'failures per year'. A value of, say, 10^{-3} failures per year, when translated to 10^{-3} failures on demand, would be pessimistic, since testing is normally carried out more often than once per year and testing is assumed to restore the failure probability to zero immediately after the test. Nevertheless, it is generally and pessimistically assumed that the numerical CMF limit may also be quoted as 'failures on demand'.

Operational deficiencies with as-built plant

In addition to the safety issues identified above, the as-built plant was found in operation to have a number of undesirable features, in particular the following.

'Remote racks' for the fuelling machine microprocessor systems were employed at the various fuel route facilities which the fuelling machine could visit. These remote racks communicated with the main processor racks on the fuelling machine, and required connection to and disconnection from the main racks at various points in the refuelling cycle. This was frequently found to lead to sudden failures of the microprocessors and consequent loss of fuel route availability.

The control and protection software for the fuelling machine contained some residual errors which required routine application of overrides to enable normal operations to be carried out.

The IFD cell plant has four different rotary drives (the tie-bar grab (which handles the fuel stringer tie-bar during stringer dismantling), the fuel element hoist, the rotary shield plug and the carousel) which move during the fuel dismantling process and require accurate alignment. Difficulties were frequently encountered in achieving this alignment.

Plant monitoring systems and operator interfaces did not facilitate efficient fault diagnosis.

Numerous other smaller problems were identified which to a greater or lesser degree restricted fuel route cycle times or availability.

Two significant projects have been initiated as a result of concerns about future availability of the fuel route plant. First, the limited capacity of the decay store (32 storage tubes) has led to the construction of a decay store extension comprising 32 additional tubes. This work is now nearing completion. Secondly, the vulnerability of the power plant to breakdowns in IFD cell equipment, which could potentially lead to prolonged outages for that cell, has led to a contract being placed for a second IFD cell. The new cell will be constructed in a spare vault in the central block between the two reactors.

Rectification of plant deficiencies

A programme of specification, design, manufacture and installation of plant modifications, to bring the equipment reliability to its full design intent and to rectify the operational deficiencies, was begun in 1990 once interim safety cases had been accepted for the fuel route plant. This programme was lengthy, and a prime requirement was that the modification work should be done in short outages, preferably not greater than 12 weeks or so, to minimize the effect on station output.

The first outage for fuel route modifications was completed in the summer of 1991. In that outage, the fuelling machine twin relay-based protection channel logic cubicles were completely replaced, and new power supplies installed for the relay channels. The new relay channel equipment performed similar protection functions to the original channels (with some small improvements), but the new cubicles were fitted with test facilities and an engineered override capability, all cross-links with the processor channels were severed, and physical separation between the processor and relay channels was improved.

In addition, an improved package of application software was installed in the fuelling machine twin processor-based channels in the 1991 outage, which removed the need for routine application of overrides in those channels arising from logic errors in the programming. Arising from the need to service the Torness fuel route, Scottish Nuclear has developed a complete in-house capability for software specification, coding, testing, quality assurance and production of EPROMs (erasable programmable read-only memories). This work was previously undertaken by contractors. It is anticipated that there will be a continuing requirement for software improvements to optimize plant performance, and the in-house capability which Scottish Nuclear possesses gives great flexibility in producing new software packages, to the required quality assurance standards, in the shortest reasonable time.

Completion of the 1991 outage work did not remove the constraints of the 'interim' cases, in particular the need for plant drive isolations by operators, but was nevertheless an essential step along the road towards a plant state that was acceptable to both operators and safety assessors.

An additional channel of relay-based protection in the flask loading cell was installed in the second plant outage programme in the summer of 1992. Completion of this work enabled the flask loading cell to operate without any requirement for routine isolation of plant drives by the operators, a 'first' for the Torness fuel route. In several separate small outages in the IFD cell in late 1992, which were integrated into the station production programme, a range of minor modifications were completed which enabled the decay power limit for fuel entering the cell to be raised to a level which would not impair station output.

During the early part of 1993 a new decay store cooling system which employs a closed-loop secondary circuit was commissioned. This modification was carried out as a part of the project to increase the number of pressure tubes in the decay store, which was referred to above. This new cooling system enabled the fault scenario 'dropped fuel leading to containment failure' to be excluded from consideration.

The final plant outage will take place in summer 1993, and will see large-scale modifications to the fuelling machine and the IFD cell. These will comprise, amongst many other modifications, the following

(*a*) the replacement of one of the fuelling machine microprocessor-based channels with a new protection-only channel using hard-wired magnetic logic
(*b*) the installation of new software packages in the remaining fuelling machine microprocessor-based channel and in the IFD cell
(*c*) the installation of a new protection-only channel in the IFD cell, using hard-wired magnetic logic
(*d*) the completion of a diagnostic and monitoring system (DMS), covering the whole fuel route, which will facilitate fault diagnosis and will also enable a reduction in planned maintenance through condition monitoring (i.e. by monitoring plant state changes and making it possible to demonstrate proper operation of plant during normal operations)
(*e*) the repositioning of remote processor racks on the fuelling machine and associated cabling modifications
(*f*) major modifications to the IFD cell to improve plant alignment
(*g*) the completion of both dropped stringer reactor trip systems.

Following the outage for these modifications, the safety concerns relating to the perceived deficiencies of the software-based control and protection systems, and incomplete separation between nominally separate and diverse protection channels, will be laid to rest, and the requirements for routine plant drive isolations by operation staff will be removed. Significant improvements should be realized with respect to plant availability, cycle time, and reduced maintenance burden. The completion of the dropped stringer reactor trip systems should enable rapid progression from off-load pressurized to low-power on-load refuelling, to allow the full design capability of the Torness power plant to be realized.

Lessons learned

A number of important lessons have been learned or reinforced by the experience of Torness fuel route completion, but perhaps the most important are as follows

(*a*) design principles should be stated clearly and concisely, in a form that enables the design engineer to differentiate between wood and trees

(*b*) the use of processors for high-integrity applications is fraught with difficulty and demands that the greatest attention is paid to QA requirements

(*c*) the views of station operations and maintenance personnel are of great importance in helping to ensure that complex plant is nevertheless readily operable; commitment at high levels is needed to ensure that the necessary resource is allocated to this important requirement.

Acknowledgements

This Paper represents a brief summary of work which has involved many people working at Torness, Peel Park, Booths Hall and elsewhere. In particular, the efforts of the Operations and Maintenance Departments and the Fuel Route Development Group at Torness, the Fuel Route Design Section, C&I Design Section, Fuel Route Computer Group and Projects Department at Peel Park, and the SNL Booths Hall Office, deserve recognition.