WELCOME

Risk Monitoring: Past, Present & Future at Heysham 2 and Torness NPPs

Jonas Englund
EDF Energy AGR Risk Monitor Lead

UK NPP Risk Monitoring - Overview

- The Past: A review of where & how it all started
- The journey to The Present: how & why we got here
- The Present: Current ESOP risk monitor scope & function
- (Back to) The Future: Continuous Improvement Plans
- Questions?

'Definition' of a NPP Risk Monitor (1)

"A plant specific real-time analysis tool used to determine the instantaneous risk based on the actual status of the systems and components.

At any given time, the Risk Monitor reflects the current plant configuration in terms of the known status of the various systems and/ or components – for example, whether there are any components out of service for maintenance or tests.

The Risk Monitor model is based on, and is consistent with, the Living PSA. It is updated with the same frequency as the LPSA. The Risk Monitor is used by the plant staff in support of operational decisions".

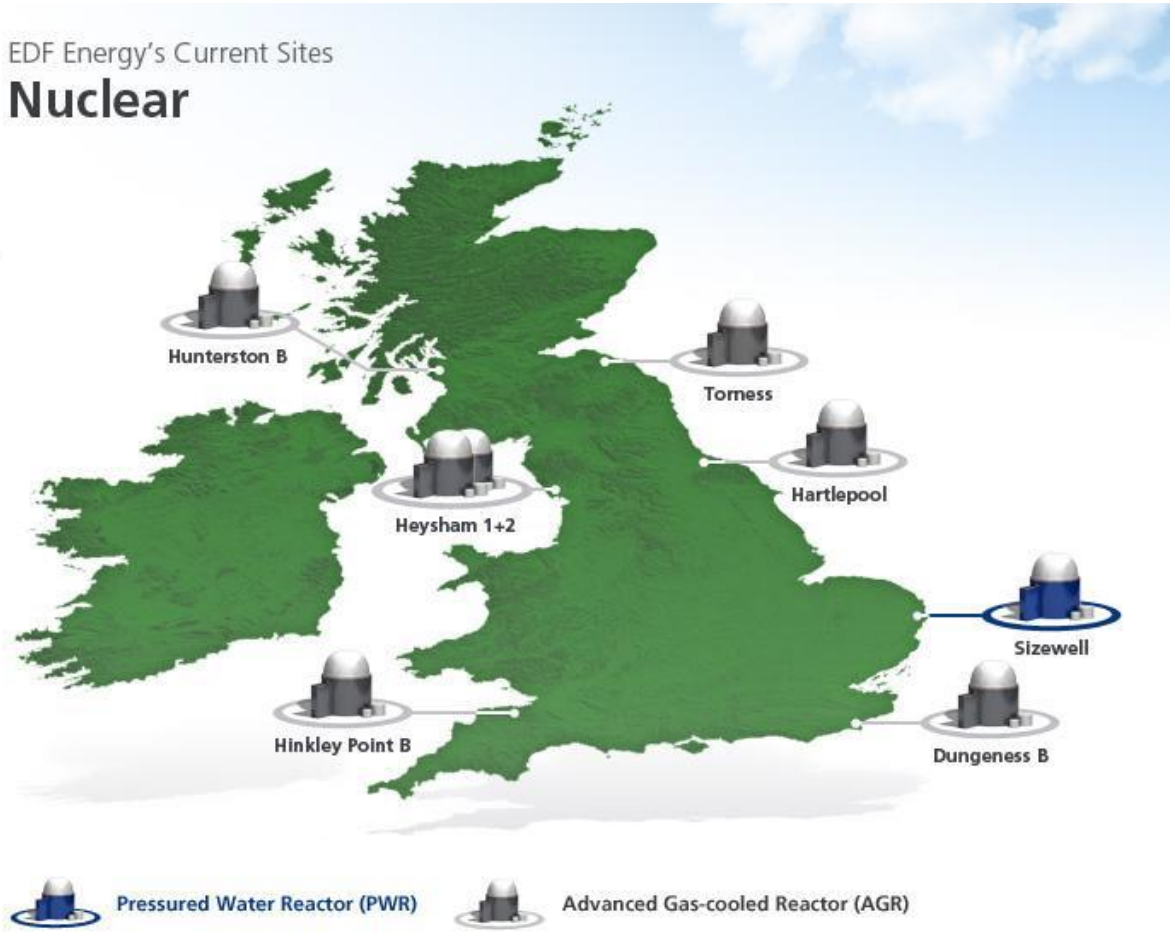
Å "Risk Informed Decisions"- not just for the Control Room!

(1) Living Probabilistic Safety Assessment (LPSA); IAEA TECDOC-1106; IAEA; August 1999

Risk Monitor – Worst Case?

Errors or inadequacies in the risk monitor (or the setting of related criteria) could mislead the operator, leading to the tolerance of elevated risk for unacceptable periods and, potentially, an actual increase in the "real" risk of a radioactive release from the plant.

Quantified Risk – underpins HY2 & TOR Design Basis



HEYSHAM 2 Safety Assessments – Design Basis

Deterministic: Technical Specifications – compliance spreadsheet

Probabilistic: Essential Systems Status Monitor (ESSM)

- The Good: Benefits / Innovations (for that time)
  - Both deterministic and probabilistic assessment of plant states were risk informing Operators in the Control Room
- The Bad: Limitations / Shortfalls
  - ESSM: Fairly limited scope PSA - Fault Tree Analysis
  - Run times: at best 10 minutes
  - Stand-alone Honeywell terminal
- The Ugly: Complications
  - ESSM: No Deterministic assessment due to coding error

TORNESS Safety Assessments – Design Basis

Deterministic: "Essential Systems Outage Program" (ESOP)

Probabilistic: LINKITT, later LINKITT2

Å The Good: Benefits / Innovations (for that time)

- ï Both deterministic and probabilistic assessment of plant states risk informing Operators in the Control Room
- ï LINKITT2: probabilistic risk assessment. When the plant availability does not comply with the Normal Operating Conditions limits, the LCO allows for the use of such a probabilistic assessment to justify an extension of the completion time.

Å The Bad: Limitations / Shortfalls

- ï Limited scope PSA
- ï Both on VAX system initially, then to PC in 1996.
- ï LINKITT2 replaced LINKITT in 1996; based on pre-solved cutsets from the early design basis PSA, i.e. limited scope & function

Early RMs: Scope, Function & Limitations

1st Periodic Safety Review (1996-98)

- PSA Development: combined separate Event Trees Fault Sequences into a single interactive model covering the whole Fault Schedule
- PSA Developed to assess discrete consequence “Dose-Bands”
- Review pushed for RM development to enable utilisation of new PSA

The Journey: A view across time

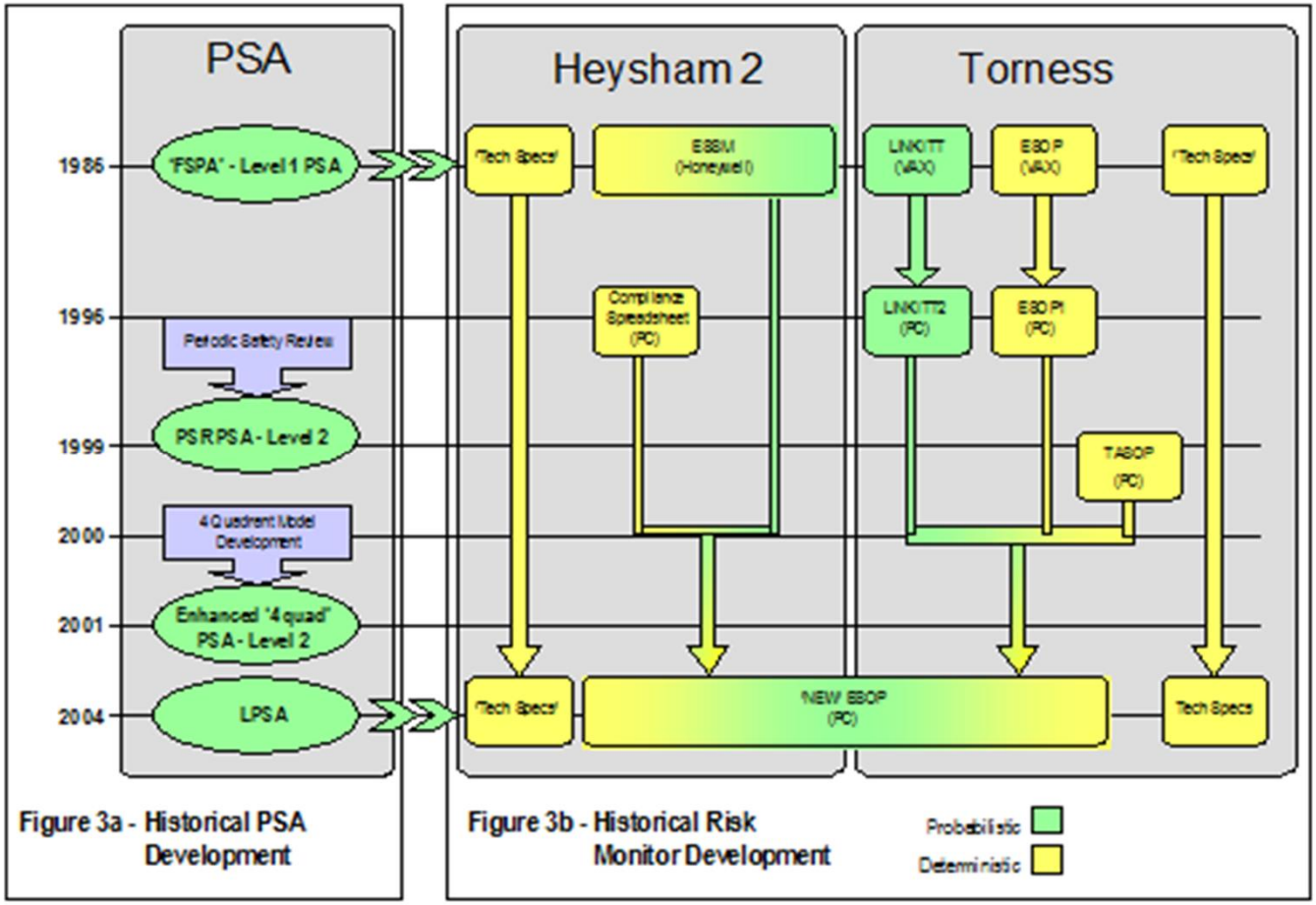


Figure 3a - Historical PSA Development

Figure 3b - Historical Risk Monitor Development

Destination: “ESOP Heysham” & “ESOP Torness”

Changes / Enhancements Made in the “Essential Systems Outage Program” (ESOP).

- Combined Deterministic & Probabilistic assessment functions in a single tool / interface (so reduced likelihood of input / output errors)
- “ESOP Torness” combined functionality of ESOP1, TASOP and LINKITT2 into a single operator aid. “ESOP Heysham” replaced ESSM & compliance spreadsheet.
- It Architecture / Platform: from VAX / Honeywell to Networked PC. Whereby all users across station now access the same ‘live’ data.
- Run PSA / risk quantification for every plant change now, even if compliant with Deterministic rules.
- Advice regarding apparent single failures or complete cutsets.

Destination: “ESOP Heysham” & “ESOP Torness”

Changes / Enhancements Made in the “Essential Systems Outage Program” (ESOP).

ï The risk values associated with “normal”, “urgent maintenance” and “unacceptable” plant states became the same at both sites. Only a change at Heysham 2, which reduced the ESSM upper limit for urgent maintenance (from 200 FPR to 100).

ï Requirement to run PSA / risk quantification for every plant change now, even if compliant with Deterministic rules.

ï Advice provided regarding apparent single failures or complete PSA cutsets (complete fault sequence).

Current ESOP Risk Monitor

Operating Rules & Quantified Risk Assessment

Control of Post-Trip Cooling (PTC) plant availability at Heysham 2 & Torness based on two main elements:

1. Deterministic assessment against pre-defined rules that permit defined combinations of plant items to be unavailable.
2. An assessment of point-in-time risk associated with the plant configuration.

Point-in-time risk quoted as factor by which risk increases above the "All Plant Available" value. This factor is termed the "Full Plant Ratio" (FPR).

$$\text{FPR} = \frac{\text{Point-in-time risk with current plant configuration}}{\text{Risk with all plant available}}$$

Current ESOP Risk Monitor

Operating Rules & Quantified Risk Assessment

- FPR<10: Normal Operation (TOR) / Normal Maintenance (HY2)
- 10<FPR<100: Restricted Operation / Urgent Maintenance
- FPR>100: Unacceptable (Controlled Reactor Shutdown).

Current ESOP Risk Monitor

Operating Rules & Quantified Risk Assessment

Deterministic rules allow combinations of plant release

- Backstop limits apply when outside of Normal Operation tables (1), e.g.
  - If satisfied, LCO 5.1.1 condition B applies (i.e. 7 hours + 1 hour to shutdown)
  - If not satisfied, LCO 5.1.1 condition C applies (i.e. 3 hours + 1 hour to shutdown)

- Deterministic & probabilistic safety assessments used in combination.
- Recognised that more detailed plant configuration assessment (PSA) underpins the probabilistic FPR compared with deterministic rules.
- If no deterministic table fits but the FPR is < 10; then Normal Operation is declared with requirement for NSG to confirm independently of CCR.

(1) Torness Terminology

Loss of RM function? – less safe & less profitable

Plant State	Current State with ESOP/Risk Monitor	State without a risk monitor	Consequence
FPR<10 + Table Fit	Normal Operation	Normal Operation	None
FPR<10 + No Table Fit	Normal Operation	3 or 7 hours operation + 1 hour to complete shutdown	Possible unnecessary Shutdown
FPR>10 + Table Fit	Restricted Operation	Normal Operation	Station is unknowingly operating in a high risk state.
FPR>10 + No Table Fit	Restricted Operation	3 or 7 hours operation + 1 hour to complete shutdown	Possible unnecessary Shutdown

ÅWithout a Risk Monitor in place there would be:

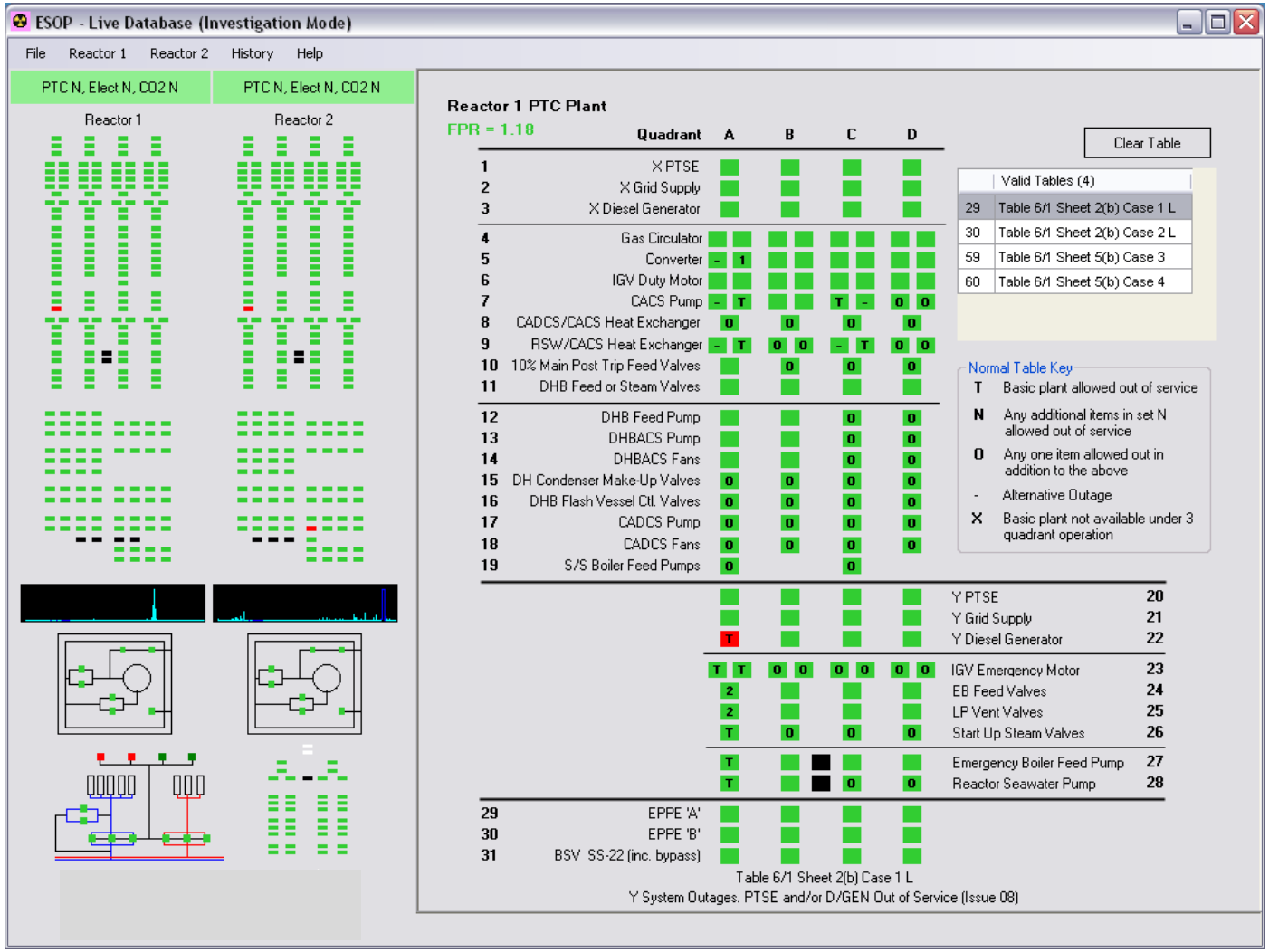
- Less information available to operations to aid Risk Informed Decision Making (RIDM)
- Increased restrictions / reduced flexibility for plant release
- Increased likelihood of a Controlled Reactor Shutdown
- Unknown risk profile

• ~ 122 periods outside of Technical Specification 'Normal Operation' tables in one year.

• ~61 were for plant states which lasted in excess of 8 hours and, using solely the deterministic rules, would either have not been permitted (if planned) or would have led to a shutdown.

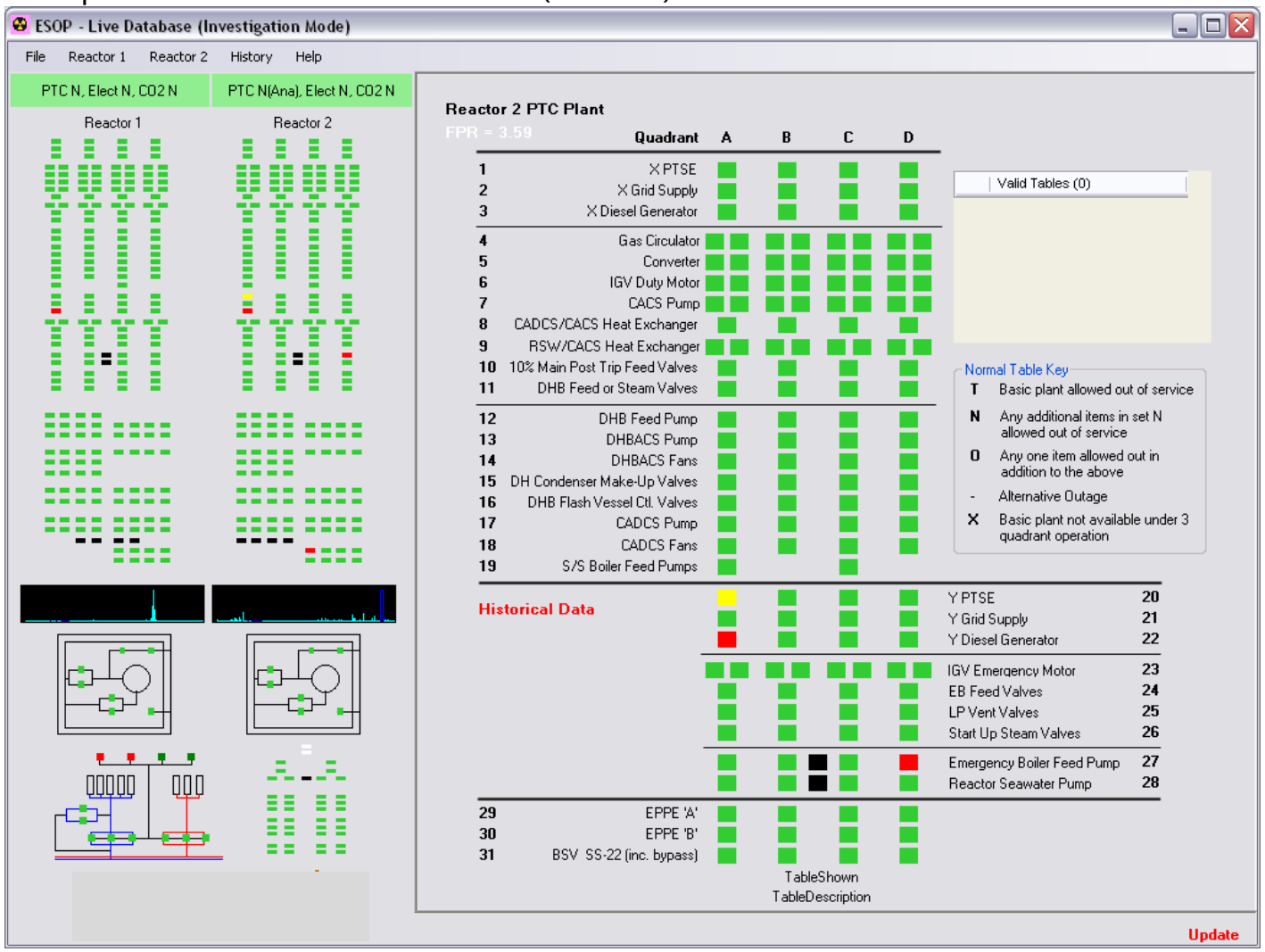
Current ESOP Risk Monitor: User Interface

- PTC plant within Normal tables (valid tables listed).



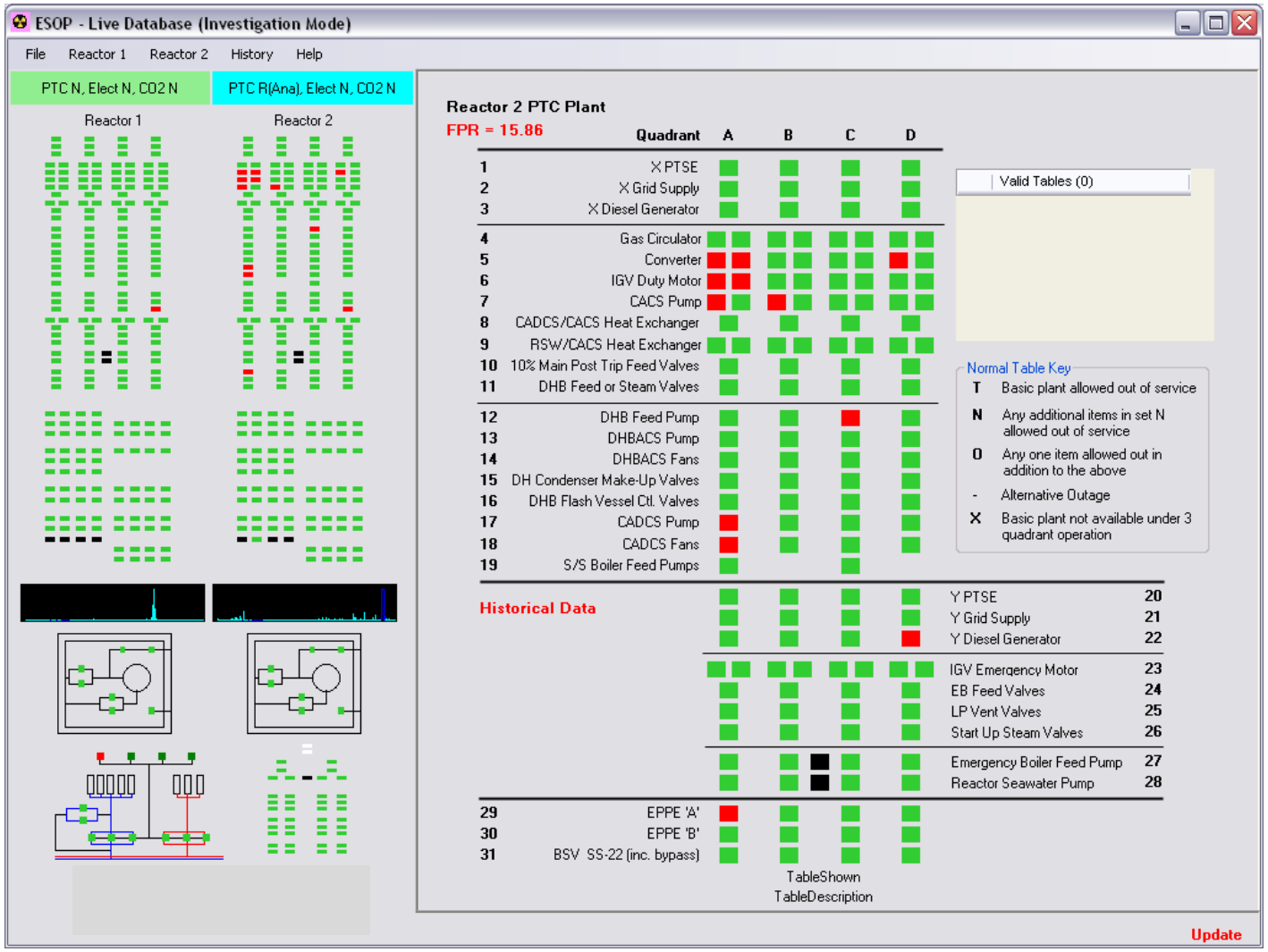
Current ESOP Risk Monitor: User Interface

- PTC plant outside of Normal Tables (FPR<10).



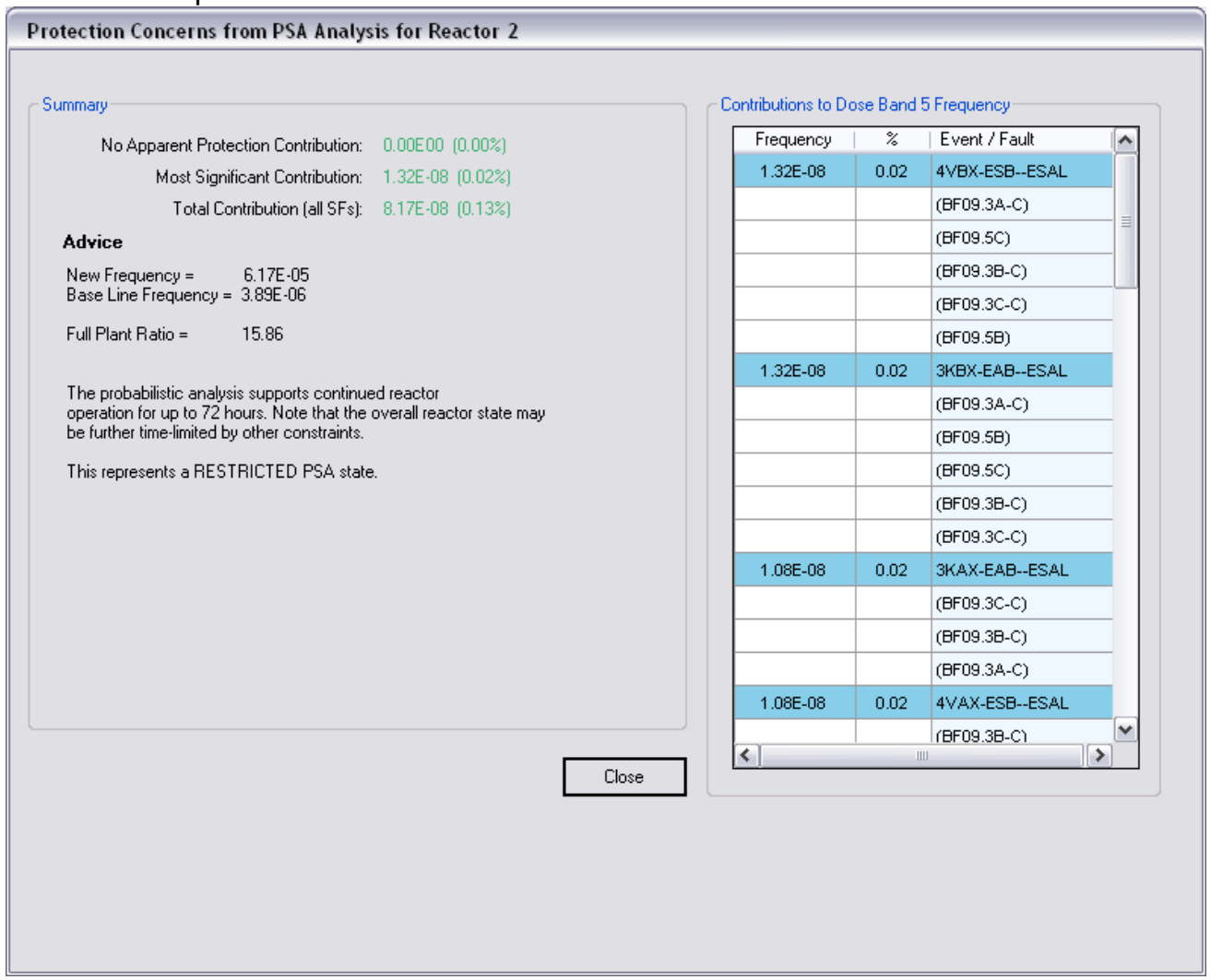
Current ESOP Risk Monitor: User Interface

- PTC plant outside of Normal Tables (FPR>10).



Current ESOP Risk Monitor: User Interface

- PSA output from ESOP



Future: Long-Term Risk Monitor Programme

- Project under way with aim of replacing ESOP with Lloyds Register RiskWatcher risk monitor as the best option
- Objective is to secure Risk Monitor sustainability to end of planned Station life
- WM planning efficiency enhancements – improved functionality
- Preservation of key ESOP attributes such as the User Interface and messaging capability
- An enhanced Risk Monitor can play a role in any future safety case for plant life extension

Summary

- Current ESOP Benefits
  - Nuclear Safety (compliance aide) & Risk Informed Decision Making (RIDM)
  - Both Deterministic & Probabilistic safety assessment
  - Continued operation – for some plant states that do not fall within established Deterministic Tech Specs
  - Provides a range of messages / warnings to user
  - Quality Assurance and scope of the PSA is key
- Risk Monitor Enhancement Project under way – key Station focus
  - Quality Assurance: Design Control and Test & Commissioning – repeat positive experience from ESOP implementation
  - Aim is to operate RiskWatcher at Heysham 2, Torness and Sizewell B
  - Vendor supported RiskWatcher User Group is growing and active

THANK YOU

EDF ENERGY