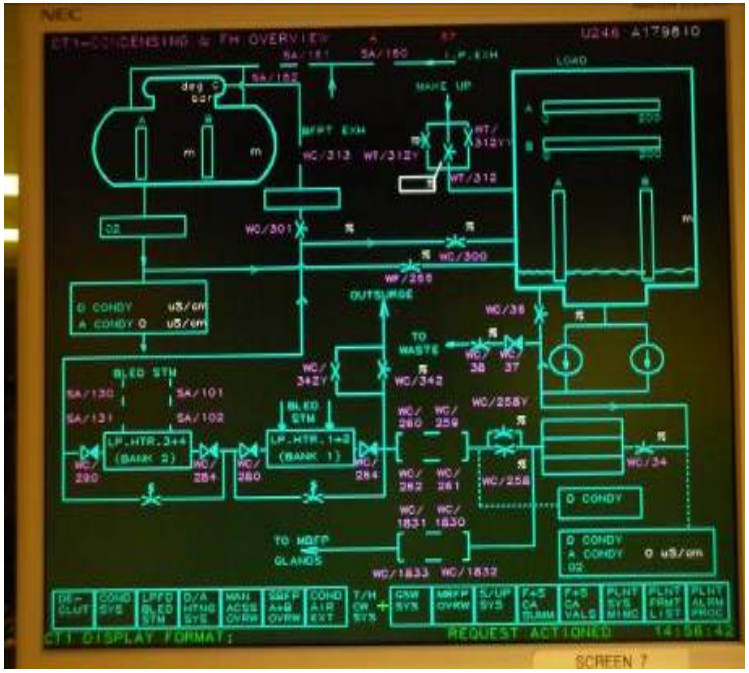
ENERGIFORSK SEMINAR October 2016

'*Management & Maintenance of a Legacy (but Critical) Data Processing & Control System*'

A. Milne (System Engineer)



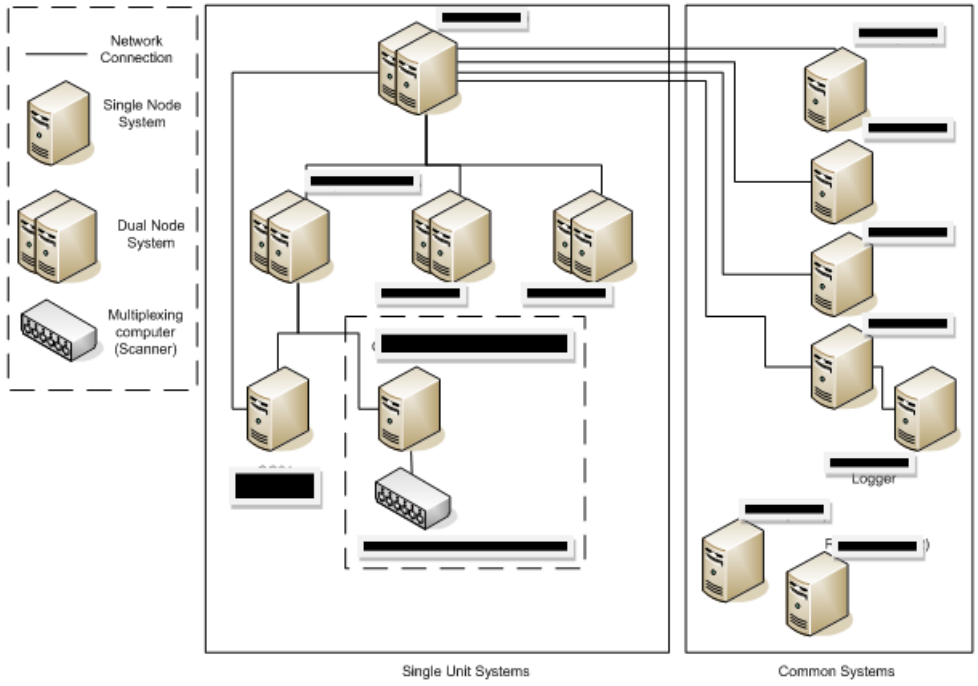
Description of system

Torness Power Station DPCS (Data Processing & Control System) provides two main areas of functionality.

The Data Processing System (DPS) presents alarms and plant information to control room engineers.

The Auto Control (AC) system operates a number of auto control loops e.g. T2 control.

Both DPS & AC play significant roles in operational safety (i.e. are safety claimed/critical) with some failure conditions potentially resulting in reactor trip (i.e. failure to comply with safety regulation).



History of system

The DPCS system (Ferranti) was designed in the 1970s/80s & is still in operation (with many original never replaced modules that now beyond MTBF). The system was initially used by the UK MOD for missile targeting/tracking but has been used in various military and industrial applications globally. Typically the hardware and operating system remained common whilst software applications have been tailored for use.

Although the underlying COTS system was used in various international locations and organisations (as far afield as India), there is now only one other known industrial user with the UK MOD having replaced their systems tens of years ago.

Replace versus Retain

With regards to Torness power station an ALARP review was carried out between 2009-2011 with the end decision to retain the existing legacy system until end of station life (2030+4). Factors in the decision making included the cost, time & risk of any potential replacement balanced against the ability to maintain performance of the existing legacy system to the end of station life.

This approach has been communicated to the UK regulator and a process of substantiation has been put in place.

The substantiation revolves around known failure rates, sufficient spares, close monitoring of failures, identification of 'outwith normal' trends and sufficient forewarning of any unforeseen age related problems to provide time to either procure more spares and/or re-engineer a solution.

Regular reviews have continually reported the DPCS as operating within original design expectations (availability & integrity) with various OPEX suggesting reliability is at a peak.

Challenges & Supporting Factors

Legacy System Challenges

Obsolete DPCS (i.e. cannot purchase replacement HW modules).

DPCS replacement estimated to be £70M+, 7+ yrs development.

Legacy software programming language and tools obsolete.

Increasing commercial drive to improve system reliability.

Increasing regulator requirements (especially in computer security).

First & Second Line maintenance 'knowledge gap' – system 'grey beards' retired/approaching retirement.

Supporting Factors

System perceived as reliable, fail rates within design expectations.

Although new modules cannot be obtained, most faults are repairable.

Although the OEM no longer exists, the core OEM team is still available.

EDF ENERGY

Support & Maintenance Strategy

"…… the ability to maintain performance … to the end of station life…"

Can our approach work ? How do we check ?

In order to validate *availability* & *reliability*, several key programs were identified:

- **Fault and Failure (F&F) Analysis**
- **Spares Analysis**
- **Obsolescence Analysis**
- **SQEP reinforcement and monitoring**
- **Supply Chain Analysis**

To continue to provide the same levels of DPCS capability it was recognised the capability to change the system should be supported. This includes both

- **Software changes**
- **Hardware changes**

Availability & Reliability (1) -

Spares, F&F and Obsolescence Analysis

Spares Analysis (SAR)

- How many do we have ?
- Which modules ?
- Are there enough (forecasting)?
- Do the spares work ? Storage?

Fault & Failure Analysis

- Failure rates per module/location – trends?
- Which components are failing ?
- Supports SAR forecasting
- MTBF/Industry OPEX

Obsolescence Analysis

- What components are used in each module (prioritisation)
- Still available/modern 'qualified' equivalent ?
- Supports Repair Loop (spares planning)

EDF ENERGY

Availability & Reliability (2) -

SQEP Reinforcement, Supply Chain Analysis

The People

- Which people ? When ?
- How many do we have ? What it the age profile ?
- What skills do they have ? gap?
- How best can knowledge be imparted ?

The Organisations

- Strategic view – 'outsourcing' v 'insourcing'
- Blue chip reputation – what is it ?
- Overall business dependency on 'our business'
- 'Insurance' versus 'flexibility'
- Contracts

EDF ENERGY

Underpinning Tools & Techniques (1)

Asset Management Tool - Asset Guardian (data visibility & accuracy)
COTS 'plain' Asset Management System – strong tailoring capability
System customised following detailed Use Case requirements phase
Replaced several previous ad-hoc & unconnected systems
Full configuration control linked with 'activity' tracking & repair loop.
'One fits all' solution used for software & auditing (e.g. computer checks)
Provides 'easy' GUI to analyse data – several KPI reports created

Culture (attitude) – Fault diagnostics, resolution & tracking
Intolerance of failure v 'it's always been like that' (focus on faults)
Closely monitor failures – ensure 'closed loop' wart repair loop understanding
Use of AMS tool to properly record & document changes

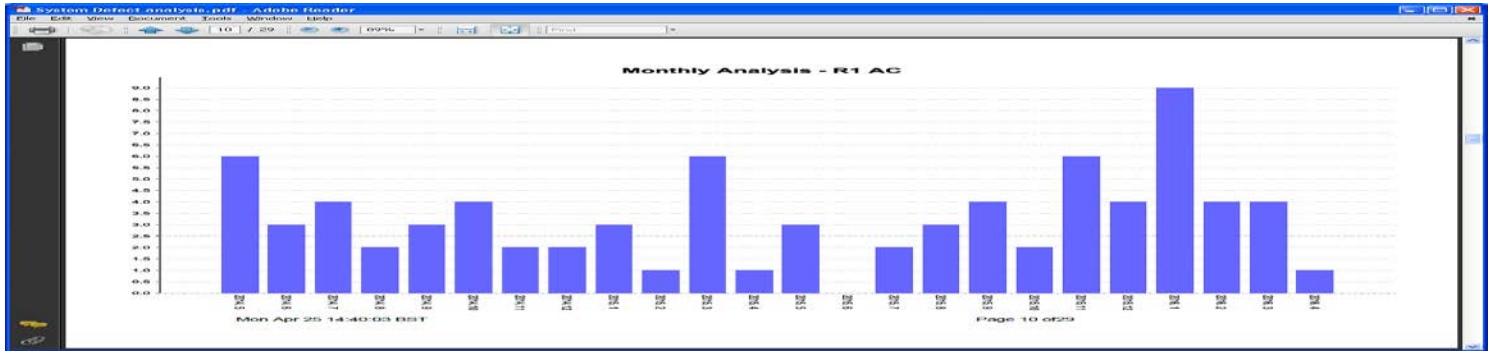
SQEP planning
What are the key local support skills ? Appetite for staff headcount changes
Retirement plans – how committed ?
SQEP 'Redundancy'
Strategic view

Documentation & review
All reports updated and reviewed by extended group involving local station 'grey beards', CTO & Vendor. Rigorous review process.
Analysis & summary carried out on annually.

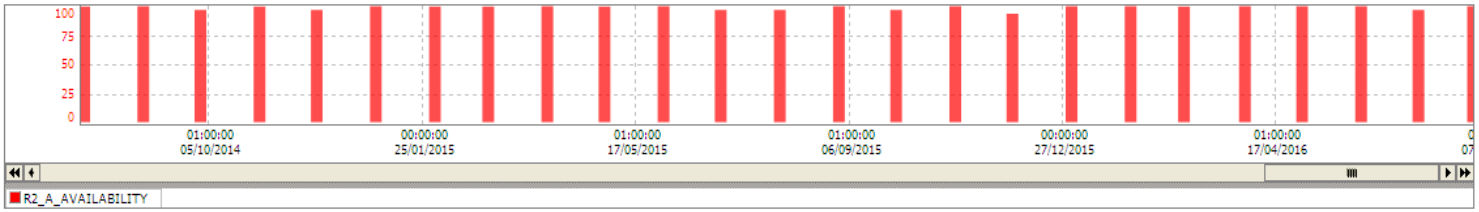
Questioning attitude at all stages

Underpinning Tools & Techniques (2)

System Availability



Statistics For R2 - A



(CSV) (CSV all)

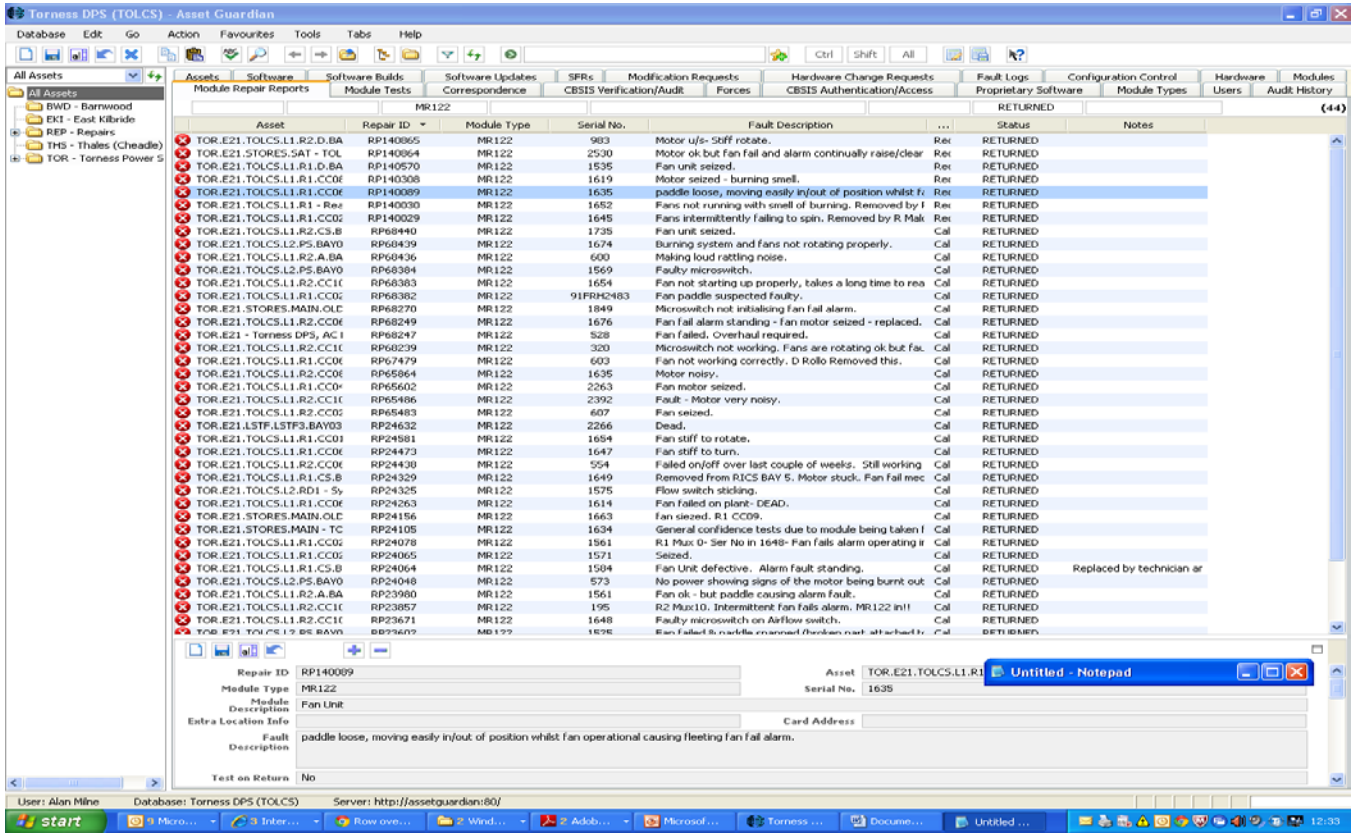
Availability

Year	January	February	March	April	May	June	July	August	September	October	November	December	Total
2016	100.00	99.97	100.00	100.00	100.00	100.00	100.00	0.00	0.00	0.00	0.00	0.00	100.00
2015	99.98	99.98	100.00	99.99	100.00	100.00	96.77	100.00	99.99	100.00	96.67	100.00	99.45
2014	100.00	99.93	100.00	99.91	100.00	100.00	99.97	100.00	100.00	99.98	100.00	100.00	99.98
2013	99.98	100.00	100.00	100.00	100.00	100.00	100.00	100.00	99.99	100.00	100.00	100.00	100.00

(reset) Show Slots

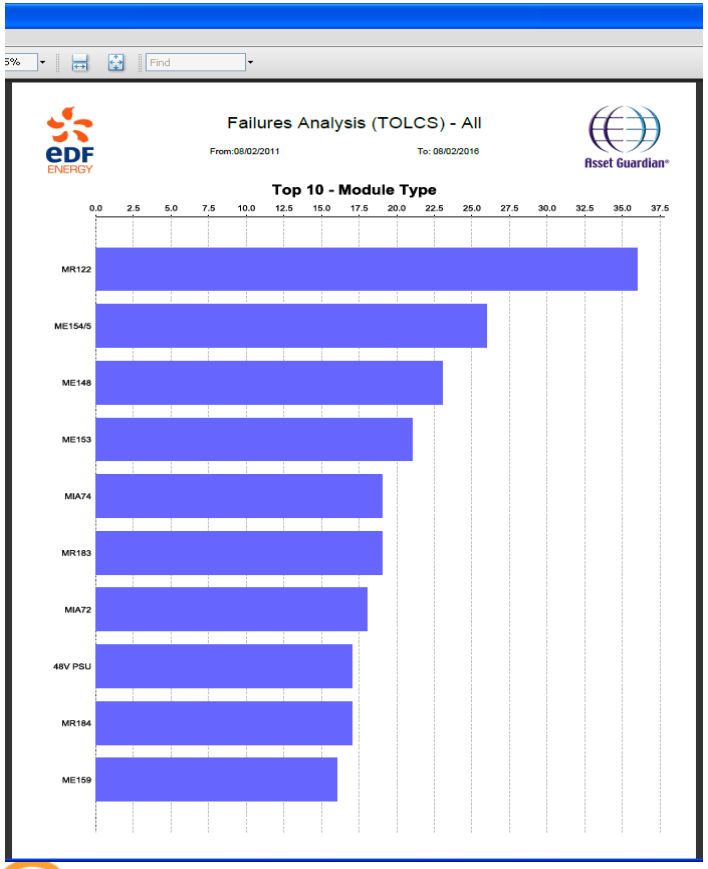
Underpinning Tools & Techniques (3)

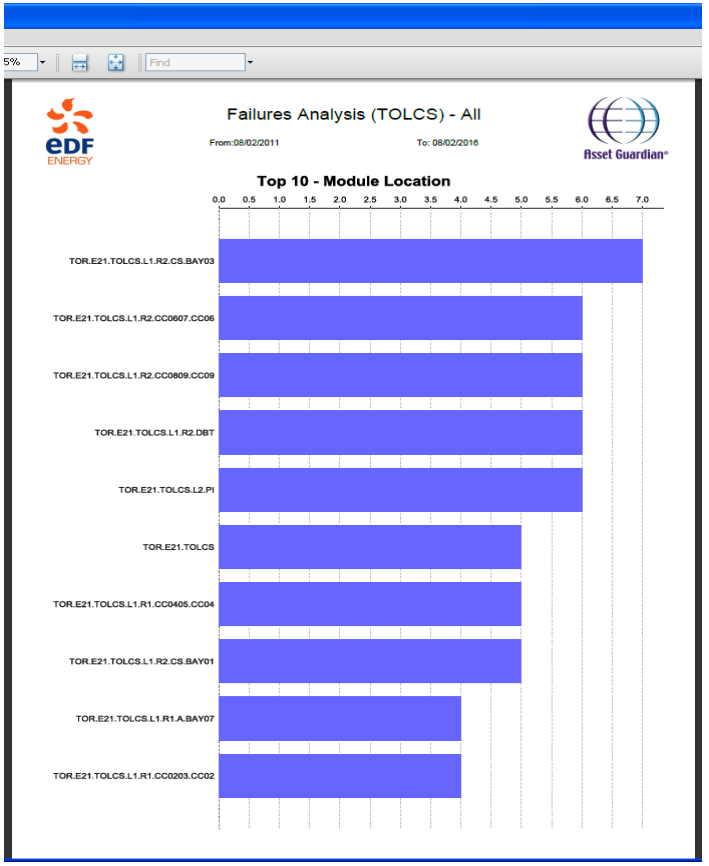
Asset Management System



Underpinning Tools & Techniques (4)

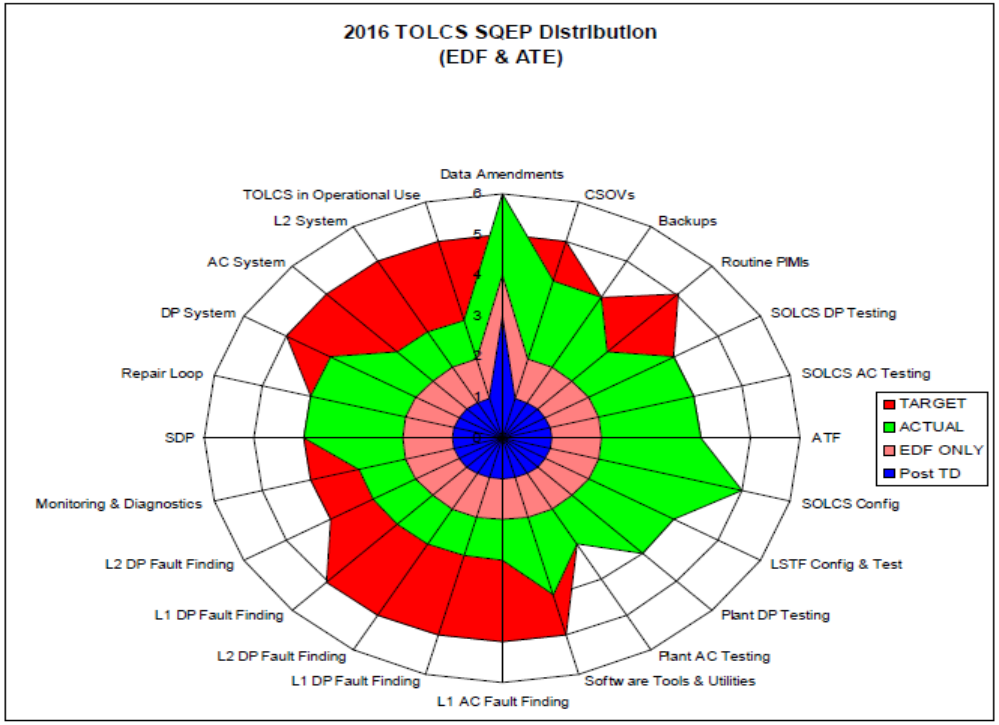
Failure Analysis





Underpinning Tools & Techniques (5)

SQEP Planning



Axis : The numerical value on the graph represents the number of people for that role.

Support for Change/Improvements (1)

The DPCS system is heavily relied upon as the main operational management system. There is a constant demand for changes and improvements to support new/changed plant and/or new/changed operational procedures.

The main stakeholder groups have traditionally included:

- Operators (improvements, automation)
- Project Teams (new signals)
- Internal (improvements)

Lately, the most significant demands have been from two main stakeholder groups:

- Station Management – reliability.
- Regulator – computer security
- Regulator – change related QA

These changes typically include BOTH hardware and/or software changes.

Although DPCS reliability & functionality have peaked, there are increasing requirements and expectations.

Support for Changes/Improvements (2)

Capability (Hardware)

- **Prioritised approach**
- **Use of AMS KPIs for 'best return on investment/effort'**
- **Element of reality i.e. PSUs are 'easy', dedicated logic chips 'hard'**
- **Equipment qualification can be very costly & time consuming.**
- **Commission Testing (practical ?).**
- **Maintenance change rather than replacement ?**

Capability (Software)

- **Several highly complex legacy issues – multi year investigations**
- **Heavy dependence on handful of 'grey beard' personnel**
- **Limited resources**
- **Succession planning coupled with development opportunity**
- **Toolchain maintenance**
- **'Insurance' versus 'flexibility'**

Cost versus Benefit

OPEX

MG20 – Annual routine now established – already paid dividends!

R2 CC09 (electrolytic caps) – All L2, R2, SOCLS & LSTF addressed – R1!

R1 CC01 – PF options switch incorrect – extent of condition addressed.

Store relay replacement – based on well known OPEX and spot checks during the year. All R2 AC store relays bulk replaced during stat outage. R1 !

PSU Replacement – TOR OPEX (&EC substantiation/testing) shared with fleet. – Ongoing program of rollout.

MR257 Replacement – TOR OPEX (&EC substantiation/testing) – Ongoing program of rollout.

Thermal Camera Walkdown – prompted by SZB PSU issue. Several issues addressed including faulty MR172 auto changeover unit, poor PSU crimping, degraded PSU power cable (PSU replaced). Routine to be established.

System Console Replacement – TOR OPEX (& EC substantiation/ testing) shared with fleet.

FUTURES

Availability & Reliability

Continue with AMS KPIs and failure trend analysis
Complete ongoing priority fault investigations
Review OPEX & amend maintenance as necessary
Maintenance - 'Grey beards knowledge capture' – training & documentation

Support for Changes/Improvements

Progress/complete ongoing hardware replacement programs
Computer Security Improvements
Continue to support stakeholder changes for DPCS integration.

Strategic

Software change support – strategic view
Outsourcing v Insourcing (burden of cost will fall to station in 2023)
SQEP reinforcement – organisational restructuring (locally)
Minimum support needed ?

EDF ENERGY

THANK YOU

EDF ENERGY