Powerful knowledge

EDF believes the key to nuclear safety is peer review, a strong safety culture and continual oversight. Nick Kochan visits EDF and asks what op risk managers could learn from the example set by the UK's leading nuclear operator

At the Gloucester facility of EDF Energy, the UK subsidiary, one particular wall hanging attracts attention. It's a large timeline chart, perhaps fifteen feet long, detailing every key date in the crisis at the Fukushima nuclear facility in Japan. It continues to be updated as new material is published about the spread of radiation, about the technical and design issues that gave rise to the tsunami-related event, and about the operating company, Tokyo Electric Power (Tepco).

Nuclear power is forever in the spotlight. The Fukushima crisis has continuing implications for the people and economy of Japan. It has also precipitated decisions by the German and Italian governments to reverse policies to adopt nuclear energy. In the UK, Fukushima has posed particular concerns since Parliament voted on July 19 to select nuclear power as a key long-term energy source. It has entrusted the operation of eight existing nuclear power stations to EDF, which also operates 58 power stations in its home country of France and five in the US – eight more will be constructed over the next 15 years.

Fukushima was a wake-up call for the company, says Roger Ecob, the EDF manager in charge of ensuring the company complies with UK nuclear safety regulations. "What happened in Japan in March does not make our plant less safe to operate. But there are some lessons for us there about what we assume in the event of one of these unthinkable disasters, so that we would be in a better position to manage it," he says. Ecob and the other engineers and safety officers at EDF are receiving large quantities of information about the Fukushima crisis. They have concluded that the causes of the crisis related more to the design of the plant than to operational or human error. Ecob says: "The question for me is: was the design right for the types of hazards they were going to experience? The indications are that they could have reasonably expected to get a seismic event of the size that they got, and they could have expected that they would get a tsunami at the height that they got. So why didn't the design recognise that? We are required to make our designs robust against certain seismic events. We make assumptions on the type of tsunami or surge waves or wind loading or fire – there are a whole load of hazards that you can consider" (*www.risk.net/2086815*).

This puts Fukushima in a minority. Technical functioning and design management are critical factors in the successful operation of a plant, but

Sizewell B apprentices

David Barber, the head of safety and regulation at EDF's nuclear business, cites a report by the Institute of Nuclear Power Operations in Atlanta that looked at the causes of failures. This concluded that problems were more likely to occur as a result of human error than mechanical or design problems. He says, "You might have your plant design right, but it also depends on what people do with that, and how it is managed. You have to ask yourself, when something goes wrong, is it the fault of the individual on the frontline, the culture or the environment in which they are operating. The major factor in about 75% of less severe cases is organisation and culture."

Operational risk in the nuclear environment takes two forms. The first relates to safety; the second to running the company's commercial activities. The challenge for management is to decide when conditions have reached the point where the threat to safety is such that they close the plant down, ending its output and thus its revenue stream. Barber says that point would come when the plant's managers feel they are out of control. "You know when you are in control. One of the phrases in the control room is: you are either in control, or out of control. The moment you feel you are out of control you shut the thing down, and that is before the reactor hits the critical barrier. If you don't shut it down, there are automatic plant shutdown limits you will hit. But you want to give yourself the margin."

"You don't wait for the [automatic] protection to operate. Operational risk management is maximising your margin at all times"

David Barber, EDF

Maintaining the safety margin is critical to the management of the nuclear plant, Barber says. "You don't wait for the [automatic] protection to operate. Operational risk management is maximising your margin at all times. So in this case you are in a dynamic situation in the control room." In a situation where managers can see their safety margins reducing, Barber explains, they have the option of acting sooner and "conserving their margin" to protect themselves against further slippage, and risk of uncontrolled activity, or of allowing the worrying activity to continue, and pushing their margin closer to the point where it becomes dangerous. Barber says the company aims to "maximise its margins and so minimise its risk. We adopt conservative principles".

Failures occur when individuals are under pressure to take shortcuts at the expense of safety, Barber says. "If all we say is that we want this plant back on by a particular time and I don't care how you do it, then the operator will be thinking, 'I will take shortcuts'. If, on the other hand, you enforce the view that you do the right things, that you have a personal as well as a legal responsibility to act in a careful way, then outcomes will be better. We also tell people that if there is any challenge to them doing the job as they should do, safely, then they should let us know and we will do everything we can to sort it out. And they need to believe you. So you are fostering that culture." Cultural and organisational failings account for a number of recent industrial crises, he says.

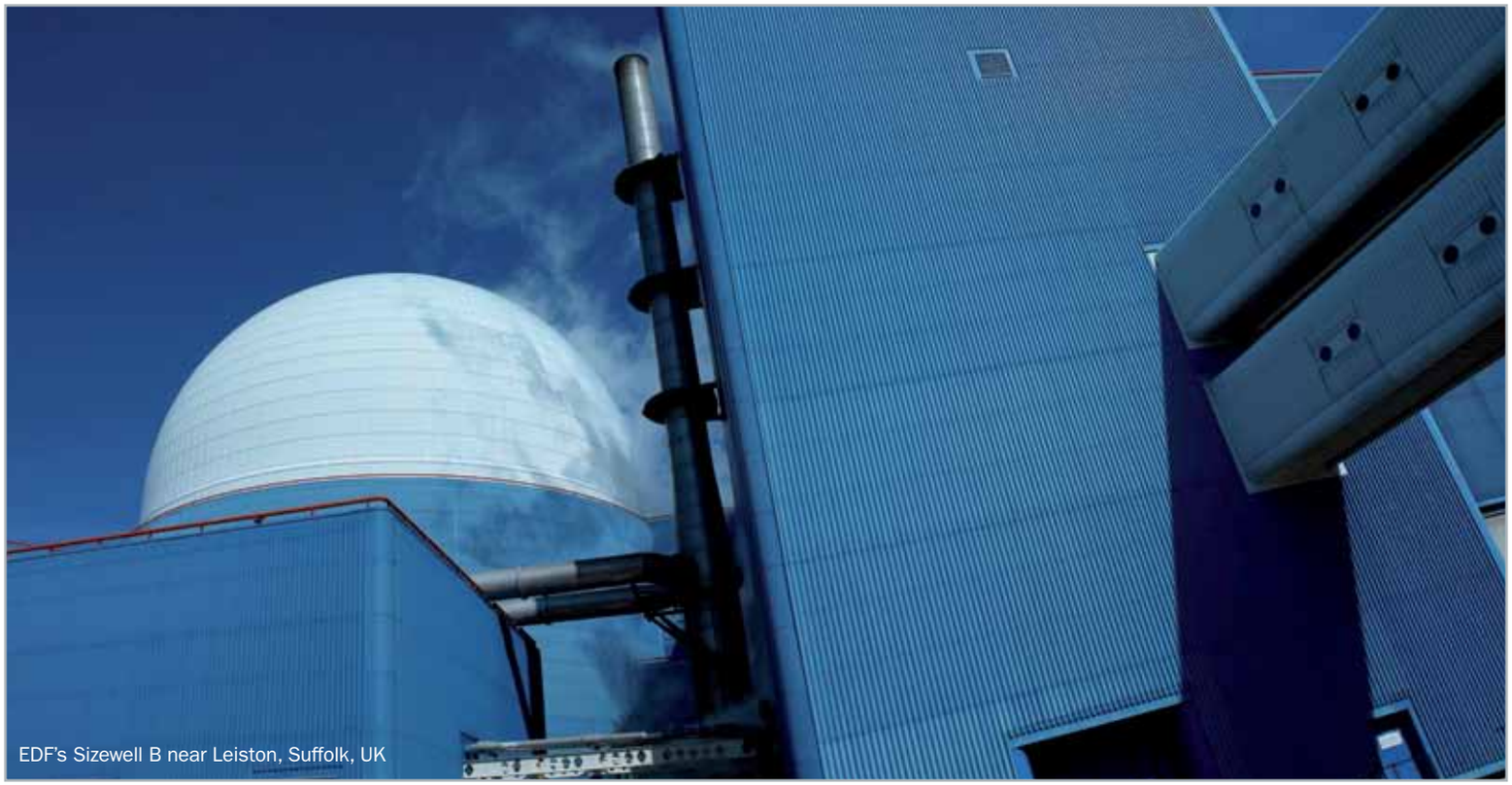
Barber continues: "Operational excellence as a goal [must mean that] everyone has this mindset of minimising risk in everything they do. For example, do I pick that piece of paper up because if someone else drops one there it could cause a fire? It is how far down that line we go. Ultimately you have to say: What is the common factor? The leadership and management of the organisation must provide the right environment for safety to succeed."

In addition to human and cultural factors, operators have to consider a statistical concept of risk. This is based around the concept of 'as low as reasonably practicable' – a term derived from the UK Health and Safety at Work Act, which covers the nuclear industry, among others. The Act says organisations have to reduce the risk to their employees and to the public to "as low as is reasonably practicable".

Ecob comments: "So if you are operating in this area, the question is: What could you do that is reasonably practicable to reduce risk?"

EDF applies a three-tiered system. "We have a top-level figure," says Ecob. "If the assessed risk from the power plants is bigger than that number, then it is unacceptable to operate. We call that 'intolerable'. At a much lower level we say, 'that risk is so low it is not going to do any harm to the public', so we call that 'broadly acceptable'. In this circumstance, we can stop focusing on measures to reduce risk in that region." In between the two thresholds are risks that are small enough not to halt operations but still large enough to merit attention and risk-reduction efforts.

These thresholds are calculated in numerical terms. "They might say something is allowed if the



EDF's Sizewell B near Leiston, Suffolk, UK

risk to the public in [terms of] killing somebody is 10^{-4} – that is, it might happen once in every 10,000 years," he says. "If you are above that you should not really be operating. If it is less than one in a million years, then we are broadly happy. So those are the numerical values of risk within which we charge ourselves to work."

Operational risk management at a nuclear power plant starts at the design stage; the floor plan is subject to a number of principles, whose underlying ethos is to minimise risk. EDF describes this as 'defence in depth'.

Ecob says: "We achieve defence in depth by providing redundancy, diversity, separation and segregation." Redundancy means the design includes back-ups for critical equipment such as pumps. Diversity requires the company to have as many different elements as possible – individual components should be made by a number of manufacturers to protect against all failing at the same time, or in the same way, because of a common flaw in design or manufacture. Separation simply means keeping items physically apart, and segregation requires an additional barrier between components to prevent the spread of an uncontrolled failure such as a fire, flood or explosion from damaging back-up equipment as well.

"Those four elements constitute defence in depth, and that is the whole ethos of the design. If something might fail, it doesn't matter because I've got another one. If that fails, I have a different one over there, and so on. In that way you can be confident that the overall probability or frequency of all those things failing, thus putting me in a difficult position, is small. And that comes back to the principle of 'as low as reasonably practicable'."

"We have a top-level figure. If the assessed risk from the power plants is bigger than that number, then it is unacceptable to operate in. We call that 'intolerable'"

Roger Ecob, EDF

All equipment and processes are subject to scrutiny and risk weighting by industry regulators. Nuclear operators work to safety standards policed by the Office for Nuclear Regulation, and are covered by the Nuclear Installations Act. "There need to be checks and barriers, frameworks to operate in, challenges both inside and outside the company, degrees of oversight – all of that needs to be built into a framework to give us more confidence and assurance of the operational risk," says Barber. "We then manage it to as low a level as reasonable. So as a board of the company you can assure yourself your operations continue to be safe.'

Regulation of the nuclear industry is rigorous and complex. The law governing nuclear safety requires each power station to have a nuclear site licence that governs any activities involving nuclear engineering on the site. An operator can expect to have regular discussions with the government regulator on subjects such as the nature of the nuclear matter that can be on the site, how nuclear matter can be carried offsite, and the records, documentation and certification that must be maintained. The objective is to make it unambiguously clear what activities would constitute a breach of the licence. The licence also specifies the qualifications required for operators of the stations, and for other responsible members of the company.

The industry is also overseen by global authorities, which serve to pass round industry best practice standards and topical information. Operators' safety procedures are regularly subject to peer review by representatives of other companies. The competitive issues of secrecy and privacy do not apply in the nuclear industry – setting it apart from other complex engineering sectors such as oil and gas. Members of the World Association of Nuclear Operators (Wano) subject themselves to peer reviews, whereby they agree to give the reviewer complete access to their operations. The company is given the reviewer's findings and is expected to act on them. Barber says reviews inevitably focus on issues raised in a previous report to ensure they have been covered. Operators are kept informed about problems occurring in nuclear plants round the world, which are communicated to Wano. "We receive significant operating experience reports," says Barber. "Each of the utilities then has to respond to this and say 'this is what we are doing'. It is a way of continuously learning from each other, so the standards are continuously improving. That means striving for operational excellence – or minimising operational risk."

TURBINE DISINTEGRATION: PREPARING FOR THE WORST

Turbine disintegration failure is probably the most dangerous event that can hit a nuclear plant. It is one for which the operators plan, they constantly assess the consequences of such a crisis and build up models for their levels of protection if such a catastrophe did occur. They must also assess whether these risk levels overstep the mark set by the Office for Nuclear Regulation.

Nuclear power stations generally operate in four stages. Heat is generated by nuclear fission in fuel rods in the reactor, at a rate controlled by inserting or removing control rods, which absorb neutrons and slow the reaction. The reactor is cooled by a circulating primary coolant – which can be water, carbon dioxide gas or even liquid sodium. The primary coolant passes out of the reactor vessel and through a boiler where it turns the secondary coolant – water – into steam. This superheated steam is then piped to turn large turbines, which spin generators to produce electricity.

EDF has a model that assumes a catastrophic turbine failure will happen once in every 100,000 years of operation. This number is derived from the frequency at which turbine disintegrations have occurred around the world. Roger Ecob, the EDF manager in charge of ensuring the company complies with UK nuclear safety regulations, says: "If [disintegration] happens, this big million horsepower machine, going around 3,000 times a minute, starts shedding the turbine blades. They have huge amounts of energy so they will go a long, long way. They will penetrate structures and buildings. Those missiles might hit the condenser, which sits under the turbine and is what turns the steam back into water for recycling round the feed system, back into the kettle [the reactor and heat exchanger]. That tends to give you the problem of a local flood, because there is lots of water being pumped into it."

Another consequence of turbine failure is a fire, because the generators attached to the turbines themselves are cooled by hydrogen, a highly flammable gas. Ecob says: "That will cause a very nasty accident. We have to think through what the missiles might do, we must think what the flood might do to the equipment we need, and we have to think of what the fire might do."

Reactor hall in the EDF Hunterston B power station in North Ayrshire, Scotland

The issue of turbine failure is made more critical because the reactor in a nuclear power station cannot be turned off immediately. In this sense it differs from any other form of power generation. When the reactor is shut down in an emergency, the control rods drop into the core of the reactor and the nuclear fission chain reaction stops instantly. However, the radioactive products of the fission reaction remain in the core, and continue to decay, producing more heat. "You end up with 'decay heat', so the reactor carries on generating, initially at about 10% of the power it had at full power levels," says Ecob. "And that decays quite quickly down to 1% or 2% of that power over a few hours."

This means that when the operators shut the reactor down, the process goes through several stages. The first, the shutdown itself, is described as 'tripping' the reactor, and can be done manually or automatically. "We have a whole pile of protection systems that say: 'Something has gone wrong so I am going to generate a trip signal'," says Ecob. "That would be things like temperature sensors, pressure sensors – all things that say: 'We are not at equilibrium here. We don't want to carry on operating.'"

The trip signal feeds into a logic processing system, which then tells the control rods to drop into the core – or, to be more accurate, it deactivates the mechanism holding the rods out. "So the rods drop in, which now shuts it down, but we still have to get rid of that residual heat that the reactor will be generating. We call that 'post-trip cooling'," Ecob says.

Post-trip cooling is provided by pumping water through the boilers to extract the heat from the primary coolant, which flows through the core. To cool the reactor as fast as possible, the steam produced can be dumped rather than being piped to the turbines and recirculated, as would happen during normal operations.

Ecob says the engineers also have to keep forcing the primary coolant gas round its circuit through the reactor. "We need gas circulators to circulate the gas through the core, and then water pumps to pump the water through the boilers so the heat can come out of the gas and into the boilers and away. If we can achieve that, then we have a reactor that is shut down safely, and cooled, so that it does not then start to overheat. And we have to have that post-trip cooling equipment available to use after an accident, if we are going to keep the reactor safe."

Ecob takes a robust view of EDF's competence to handle the failure. "Even in the event of a turbine disintegration – almost the worst thing that can happen – we still need to make sure we have got equipment that is not going to get damaged by missiles, or flood or fire. This enables the operators to continue to carry out those essential post-recall functions."

The company achieves this by good design: keeping critical equipment in places where it will not be affected by flying turbine fragments, fire or flood. It protects them against fire by fireproofing them, and will position them in places high enough above the condenser level to be unaffected by a flood. "These are the fundamentals of basically how we keep our nuclear reactors safe," says Ecob. "It is all about fault conditions. It is only when we get things wrong that we get into this automatic trip, post-shutdown and post-trip cooling. That is the way we demonstrate we are working within this tolerable or broadly risk-acceptable basis." ■