NUCLEAR FUEL CYCLE ROYAL COMMISSION

SA NUCLEAR FUEL CYCLE ROYAL COMMISSION

MR KEVIN SCARCE, Presiding Commissioner
MR BEN DOYLE, Counsel Assisting

SPEAKERS:

Dr GORDON EDWARDS, President of Canadian Coalition for Nuclear Responsibility (Canada)
PROFESSOR PER PETERSON, Berkeley University of California, US
MR HEFIN GRIFFITHS and MR MARK SUMMERFIELD, Australian Nuclear Science and Technology Organisation (ANSTO)
MR PETER WILKINSON, Noetic Group

TRANSCRIPT OF PROCEEDINGS

ADELAIDE

9.00 AM, WEDNESDAY, 21 OCTOBER 2015

DAY THIRTEEN

PROCEEDINGS RECORDED BY SPARK AND CANNON

COMMISSIONER: Good morning. The public session today is on nuclear reactor safety and regulation. We have experts from Canada, the United States and southern Australia and from a local company who is expert in risk. Mr Jacobi is enjoying his second week of planned leave and I welcome Mr Ben Doyle to read the context statement for today.

MR DOYLE: Thank you, Commissioner. The terms of reference require an inquiry into the safety risks to both the environment, the community and workers as well as the general public associated with the operation of nuclear reactors. Today's session will explore these issues at a general level before the Commission focuses tomorrow on the accident at Fukushima Daiichi in 2011 and the impact it has had on the development of design principles, safety assessment procedures and regulatory oversight.

This public session aims to explore the nature of the risks associated with the process of generating electricity from nuclear fuel, and the means by which those risks are sought to be mitigated. The Commission will hear evidence concerning the risks arising from the normal operation of nuclear reactors and in the context of an accident resulting in a shut down of the reactor. These risks include not only the immediate consequences of any exposure to harmful emissions, but the broader social consequences that can follow from emergency responses.

This public session aims to explore the ways in which developments in different reactor designs have sought to address the essential safety risks involved in the operation of a reactor. There will be a focus on those reactor designs and technologies that would be most likely to be investigated as part of any future development in South Australia. The experience of the nuclear industry has demonstrated that the operation of a reactor involves the management of a low probability but high consequence risk and risks of this kind pose their own unique challenges. They require comprehensive and ongoing analysis long after the design of a reactor has been completed.

Today's session also aims to understand therefore the conditions which are necessary to create and maintain an industry which fosters a safety culture and a regulatory regime which is robust, despite the challenges that can face the regulator of an industry in which there may be few participants. This will involve consideration of the different philosophical approaches to risk management including deterministic and probabilistic safety assessments and the ALARP principles which focus on ensuring that risks are reduced to a level which are as low as reasonably practicable.

The first witness to be called by the Commission in relation to this topic is Dr Gordon Edwards. Dr Edwards is the president of the Canadian Coalition for Nuclear Responsibility, the CCNR, which he co-founded in 1975. CCNR

is a not for profit organisation dedicated to education and research on all issues related to nuclear energy, especially those pertaining to Canada. He has devoted over 40 years of research into nuclear activities in Canada and throughout this period has provided consultancy services to government and non-government bodies in relation to nuclear safety issues.

COMMISSIONER: Dr Edwards, thank you very much for joining us this morning. Can I start with a broad question, and before we address the risks associated with the operation of a nuclear reactor, can we begin to understand the two processes within the reactor which result in the generation of nuclear energy and the differences between them.

DR EDWARDS: Yes. Mr Commissioner, every nuclear reactor really is a boiler. It basically boils a lot of water to produce steam so that we can spin a turbine to generate electricity. The difference is that instead of burning a fossil fuel such as coal or oil, we obtain the energy by the splitting of uranium atoms. This is called nuclear fission, and it's this process which can be controlled by controlling the neutrons, these are little sub-atomic particles which are projectiles that cause the splitting of the uranium atoms, and by stopping the flow of those neutrons you can stop the reaction from happening, by slowing them down and reducing the number of them you can reduce the power of the reactor, or you can also have a situation where the number of neutrons increases rapidly, in which case you have what's called a power excursion, a rise in power which may or may not be planned.

So that's the fission process, and the nice thing about the fission process is that it can be shut off very rapidly. It can be shut off in emergency conditions within two seconds quite handily and, in fact, in most of the accidents that people have heard about, such as the Fukushima accident and the Three Mile Island accident, these, in fact, the reaction was stopped very, very quickly. But there is a second problem, and that second problem is radioactivity.

Radioactivity is a form of nuclear energy which cannot be stopped, there is no scientific way of stopping it, and it is a spontaneous process whereby the nucleus of a radioactive atom disintegrates suddenly and violently, giving off energy like shrapnel you might call it, sub-atomic particles that are given off with very great speed and nobody knows how to stop this process. Now, the complication is that by splitting the uranium atoms we create hundreds of new radioactive materials that were not previously present in the fuel and these hundreds of radioactive materials are very unstable, very radioactive and they generate by themselves sufficient heat to melt the core of the reactor even though the fission process may have been stopped, and that is what caused the meltdowns at Fukushima and at Three Mile Island, it was that residual radioactive heat that was unable to be stopped that caused the melting of the cores.

MR DOYLE: Dr Edwards, you have mentioned that the process of emission of radioactive particles from fission products, I want to come back to that in a little bit more detail in a moment, but are there two other sources of radioactive materials that can be created within a reactor?

DR EDWARDS: Yes, that's right. We mainly think of the fission products which are the broken pieces of uranium atoms, because they are responsible for most of the heat that is generated by - it's called the k heat. There are, however, activation products. Activation products consist of nonradioactive atoms which absorb neutrons and become destabilised and therefore radioactive. So things which were not previously radioactive, become radioactive.

For example, in the CANDU reactor which we have here in Canada, we use a moderator which is a nonradioactive form of hydrogen called heavy water. It so happens that heavy water is just like ordinary water except the hydrogen atoms are twice as heavy as usual, they're not radioactive, they're just a little heavier. Now, when a neutron is absorbed by one of these heavy hydrogen atoms, it is transformed into an atom which is three times heavier than normal and that's called tritium, it's radioactive hydrogen. That's radioactive, it has a half life of about 13 years and it is a dangerous by-product of the process, it's called an activation product.

There are many dozens of activation products created in the core of the reactor. The steel components, for example, generally have small amounts of cobalt in the steel, nonradioactive cobalt called cobalt 59. When the cobalt 59 absorbs a neutron it becomes cobalt 60 which is very dangerous because it gives off intense gamma radiation which can be quite harmful to workers or anybody else who comes into contact with them. In fact, cobalt 60 is also used as a cancer therapy device because it's very good at burning cancerous tissues that would otherwise cause the death of someone.

So the cobalt therapy is taking advantage of that damaging gamma radiation. But these are activation production and what this means is that even after the irradiated fuel has been removed from the reactors so that all the fission products have been taken out fundamentally, you still have the structures themselves being radioactive due to the activation of the materials so that even the materials inside the core of the reactor will become radioactive waste. They too will have to be buried or stored as radioactive waste for very long periods of time. Once again the fundamental factor of radioactivity is that we don't know how to shut it off, and that's why we have a radioactive waste problem.

MR DOYLE: Well, can we move now - - -

DR EDWARDS: There is - I'm sorry. There is a third process that I forgot to mention.

MR DOYLE: Yes.

DR EDWARDS: The third process is called - well, it doesn't actually have a name, but some of the uranium atoms that absorb neutrons do not split. There's one kind of uranium atom which splits. It's called uranium 235. There's another type of uranium which doesn't split when it's struck by a neutron, but it becomes heavier and transforms into a heavier than uranium element which is called plutonium. Now, not only plutonium but by absorbing more neutrons you can get other so-called transuranic elements heavier than uranium: americium, neptunium, plutonium, curium, and several others.

These substances have - they are also radioactive, but they have very, very long half-lives. They generally tend to have half-lives in the thousands or hundreds or thousands, or even millions of years, and as a result they contribute to the very long-term hazard of radioactive waste so that we can't just wash our hands of it after a few centuries. We have to actually look after it for literally hundreds of thousands, even millions of years for that reason.

MR DOYLE: Is it right they tend to be the alpha emitting materials?

DR EDWARDS: Yes, that's correct. Lighter elements generally do not give off alpha radiation. Alpha radiation is a form of radiation that most people would find peculiar. It's a non-penetrating form of radiation which is nevertheless highly damaging. You can stop alpha radiation with a piece of paper. Just put up a piece of paper in front of your face and it will stop all the alpha radiation coming off from an alpha emitter. However, if that material gets inside your body and the alpha radiation comes in direct contact with living cells, it's known to be far more damaging inside the body than gamma radiation or beta radiation, which are more penetrating. So the curious paradox is that even though it's less penetrating, it's much more harmful.

Now, there's a phrase used called a becquerel. A becquerel refers to one radioactive disintegration every second. It's a measurement of radioactivity. Each becquerel of alpha radiation is about 100 times more damaging, biologically damaging, than a becquerel of gamma or beta radiation. The reason we talk about becquerels is because radiation is actually energy coming from the core of the atom, and it's very sudden. It disintegrates. The atom disintegrates, and when it disintegrates that's when it gives off either a highly electrically charged particle, which is called an alpha particle or a beta particle, or a burst of energy called a gamma ray.

The gamma ray is what most people think about because it's analogous to x-rays, and so most people when they think of a radiation, they think of some kind of invisible ray that you've got to get away from. But in fact when you're talking about alpha radiation and beta radiation, that's an inappropriate thought. You shouldn't think about it as a form of penetrating radiation you're going to have to escape from. You think of it as a pollutant, much like a chemical pollutant, something that would get into the food or into the water or into the air so that you inhale it or ingest it, and once it's inside your body, depending upon the chemistry, it could be incorporated in different parts of your body.

For instance iodine 131 is incorporated into the thyroid gland. Strontium-90, which is also a fission product, doesn't exist in nature. This gets incorporated into the bones and the teeth and mother's milk because it's similar to calcium. Something like caesium-137 is similar to ordinary potassium, so it goes to the blood and to the soft organs, and that's why it's a danger for agricultural - people who are growing, for example - or just to give you a particular example, in Northern England even 20 years after the Chernobyl accident in the Ukraine there were sheep farmers who couldn't sell their sheep meat for fear of caesium contamination, radioactive caesium contamination from the Chernobyl accident.

Radioactive caesium is not a naturally occurring material. It only occurs because of the splitting of the uranium atom either through an atomic bomb or through a nuclear reactor. So this material has about a 30 year half-life, caesium-137, so it stays in the soil for a long time and it gets incorporated into the grass that the animals eat, and then gets incorporated into their meat, and it doesn't go to the bones, it goes to the meat, the soft organs, and that's why it poses problems for restrictions on agricultural meat products that can't be consumed safely. So they have to keep careful watch on that.

This is the fundamental problem with nuclear safety. It's not the machine that's dangerous. The machine is really not dangerous. What's dangerous is the enormous inventory of radioactive materials inside the machine, and if there's anything, whether it's a comet from outer space, or an aeroplane crashing into a nuclear reactor, or some kind of industrial accident including explosions, anything that will breach the containment and allow this radioactive material, the fission products and the other radioactive materials, to escape into the environment could have catastrophic results, and that's what makes nuclear power plants dangerous. It's not the machinery. It's the nuclear waste inside.

MR DOYLE: You've mentioned, Dr Edwards, the possibility of external events breaching containment. Can we come back to I suppose what might be a more stereotypical risk of emission of radioactive materials and the process of controlling decay heat following a shutdown. I wonder if you could explain the basic potential problem that is involved once the criticality has been

controlled but the radioactive material continues to produce decay heat.

DR EDWARDS: Yes. That's one of the fundamental problems. There are really two types of severe nuclear accidents. One involves a situation where the actual fission process gets out of hand. That can happen and that's why you need to have very rapid shutdown systems. The difficulty with the chain reaction, as it's called, of fissioning uranium atoms is that the neutron population suddenly starts exploding, then you have a real explosion. The core of the reactor could self-destruct and blow the containment - damage the containment in such a way that the radioactive inventory has a pathway to the environment, and that's why you have a serious accident of that sort.

Another type of accident, however, and one that is more likely is if you do successfully shut the reaction down, and they have very fast shutdown systems which are tested regularly and which are hopefully always going to be reliable, then you have to cope with what's called the decay heat, and that's the heat that's generated by the nuclear waste. Now, if you don't have any damage to the plant, it shouldn't be a real problem. You just keep the pumps running, and if you keep the pumps running then just like before the circulating water removes the heat as fast as it's produced, or even faster than it's produced, and everything is safe, everything is fine. However - - -

MR DOYLE: Before you go on, Dr Edwards, how does the quantity of the decay heat typically compare with the quantity of heat that's produced during fission?

DR EDWARDS: Well, during fission full power heat - for example if we had 1,000 megawatt reactor let's say, then the amount of heat that would be produced would be 3,000 megawatts. It's about three times as much as the electrical output. So two-thirds of the heat actually is waste heat. One-third of it goes to generate electricity. So you have about 3,000 megawatts of heat being generated at full power. The moment that you shut the reactor down and stop the fission process, the decay heat is about 7 per cent of full power, and that declines rapidly, so that after about four hours it has declined to about 1 per cent of full power.

However, even 1 per cent of full power is more than enough to melt the core of the reactor, and people at this point in the discussion, people have to realise there's a difference between temperature and heat. Temperature is just a measurement of how hot something is. Heat is a form of energy, and if heat is being generated, then the temperature will go up so that although the fuel is originally at a safe temperature, if that heat is not removed, the temperature will go up and up and up, and it reaches the melting point at about 2800 degrees Celsius. That's the melting point of the ceramic fuel, the ceramic fuel pellets which is, by the way, much higher than the melting point of steel so

that once the fuel melts at that temperature, it will tend to melt through anything else as well unless you can somehow prevent it from doing so. So the important thing here is to have a steady supply of cooling water that can remove that decay heat as rapidly as it's being produced. And the decay heat declines rapidly and it becomes more and more manageable as time goes on. Nevertheless, even after the fuel is removed from the reactor, it has to be put in to a pool, a spent fuel bay which still has to have circulating water in it for – in Canada here, we require it for 10 years. You have to actively cool the irradiated fuel for over 10 years just to prevent it from overheating. If you were, for example, to interrupt the cooling, even in the spent fuel bay, it wouldn't melt down but it would overheat and damage the metal cladding on the outside of the fuel and you would have a release of some of those radioactive materials, including the radioactive gases.

There are about 20 per cent of the fission products are actually radioactive gases, they're called noble gases because they don't chemically combine with anything else. There's radioactive isotopes of xenon and argon and krypton and those things are gases and so they will escape as soon as there's any defect in the fuel cladding. There's also elements such as iodine and caesium, radioactive iodine, radioactive caesium which very easily sublimate from a solid radiant to a vapour and those vapours are also given off at elevated temperatures. So although you won't have a meltdown in the spent fuel bay, you will have damage to the fuel, self-inflicted damage to the fuel and releases in to the environment. And as we've discovered in recent years, is that up until the present time, we have not really taken adequate care to have shielding around the top of the spent fuel bay. In other words, the spent fuel bay is not within the containment of the reactor. Consequently the spent fuel bay is more vulnerable to atmospheric releases.

One of the things they were concerned at, at Fukishima in unit number four was the spent fuel bay, which was open to the atmosphere and had you had a serious overheating of the fuel, then you would have had direct releases to the atmosphere which is actually not the case with the fuel in the reactor core because it is more shielded. It has various multiple containment systems. So it's not so easy to get out. Yes, so - - -

MR DOYLE: Can I come back at this point? Sorry to cut you off Dr Edwards - - -

DR EDWARDS: That's fine.

MR DOYLE: - - - to the means by which a loss of removal of decay heat within the - - -

DR EDWARDS: Right.

MR DOYLE: - - - reactor, can result in a breach of containment? Is it simply through the heat reached by the fuel that's melted and potentially leached to the bottom of the reactor vessel, or are there other pathways?

DR EDWARDS: Well, in itself the – even severe damage to the fuel does not necessarily result in a breach of containment. However, there are other mechanisms at work which can result in a breach of containment. For example, when you get the overheating of the fuel, you get – because there's water as a coolant in the reactor building, you get a lot of steam produced. And at those temperatures, we're talking here about 1,000 degrees Celsius, not up to the melting point yet, but beginning at around 1,000 degrees Celsius you get a very energetic reaction, chemical reaction between the zirconium metal, which is the cladding of the fuel and the steam. And what happens is the zirconium metal oxidises very rapidly and releases hydrogen gas. Hydrogen gas, as you know is very explosive. And again, we saw this at Fukishima, three violent explosions which were really hydrogen gas explosions caused by the interaction – the chemical interaction of the zirconium metal with the steam, resulting in any kind of little spark will – once it reaches a certain concentration can cause an explosion. That of course – and the worst circumstances could breach containment.

Interestingly enough, at Fukishima, although it damaged the outer building and resulted in some releases of radioactivity, we're lucky that it did not actually breach the main containment vessels, so that in fact most of the melted fuel at the Fukishima reactors did not get released in to the atmosphere through that. It's only the stuff that had been released, along with the steam, that's the only material that escaped. So that's why the Fukishima accident was not considered to be as disastrous as the Chernobyl accident. The Chernobyl accident you had a complete loss of containment.

MR DOYLE: Thank you.

DR EDWARDS: Now there was one thing about the Chernobyl accident, this is another mechanism. What happened at Chernobyl was that they didn't have a fancy containment system like they did at Fukishima and the roof of the building got blown off. But one of the features of the Chernobyl reactor is that when you lose the coolant, that is if there's a pipe break or anything that loses the cooling water, then at that moment, two things happen. First of all, the water is so hot in the primary coolant system, it's about 300 degrees Celsius or more and the only reason it's still water is because of enormous pressure. It's pressurised so that it cannot boil. As soon as you have a break in the pipe, all that overheated water turns in to steam, so you get a steam – flashes in to steam, which creates a great deal of steam pressure inside the building. But at the same time, you get an increase in the power level; you get a spike in the

fission process. This is called a positive void coefficient of reactivity and it only applies to certain designs of reactors, including the CANDU reactor. It turns out that any reactor which uses what are called pressure tubes instead of a pressure vessel, this is a bit technical. But basically the American design and the French design, basically they have one big boiler which is called a pressure vessel, and the fuel is inside this pressure vessel and the water circulates through that vessel. In that case, if you have a loss of coolant, it does not result in a sudden power increase. But in the CANDU design and in the Chernobyl design, you have individual tubes, pressurised tubes that are called pressure tubes, containing the fuel, and when you lose the coolant in those cases, you do get a power surge at the same time. And so this makes it particularly hazardous to make sure that that power surge is not going to overwhelm the shutdown systems.

There was another accident in Switzerland in 1969 at the Lucens reactor, a research reactor which was also a pressure tube design, which had the same type of situation where there was a loss of coolant, an immediate power surge and the reactor blew itself to kingdom come basically and destroyed itself. And that reactor was first of all sealed in a rocky cave and then eventually disposed of. But that is an unusual safety concern that caused the CANDU designers, the Canadian designers to insist upon two fully independent shutdown systems. Other reactors in the world do not have this. But the CANDU system has not one but two fast shutdown systems to mitigate against this type of situation. So that if the one shutdown system for some reason would not work, the other one would hopefully and there we have it. So there are differences in design. But the fundamental problem remains the same. How to stop the stuff from getting out? Now if the containment holds and you don't get atmospheric releases, or at least not substantial atmospheric releases, then the next problem is what if it melts down through the bottom because when it melts down, it can just keep on melting and if you get a complete core meltdown as you did at Chernobyl then the fuel just melts its way through the concrete base and in to the ground and then you have the problem of contamination of groundwater, and possible steam explosions.

Steam explosions are not fully understood as a matter of fact. It's not just due to steam pressure, it turns out that when very hot molten metal falls in to a pool of stagnant water, you get a very powerful physical explosion called a steam explosion, which is not the same as a steam pressure explosion. And that can in fact damage the containment above and lead to atmospheric releases. The worst thing of course is to get the atmospheric releases, at least in the short term. But you have that longstanding problem which they still have at Chernobyl to this day, what to do about the stuff that's all melted down in to the ground. And of course at Fukishima they haven't begun to address that.

MR DOYLE: Dr Edwards, you've mentioned a couple of aspects of the

CANDU reactor design that give rise to potential issues. I wonder if we could just take briefly, a step backwards and if you could explain the basic technological difference between a CANDU reactor and a typical light water reactor.

DR EDWARDS: Yes. Well, the main difference is the one I mentioned to you, is that the light water reactor uses a boiler, basically a large pressure vessel, very thick, very thick hold as it were, to contain all the pressurised water. Now, there really are two types of American design. So there's the pressurised water reactors which are more like the CANDU because we also have pressurised heavy water reactors, and then there's the boiling water reactors.

The boiling water reactors - and Fukushima was a boiling water reactor - there the water in the core is allowed to boil and that steam is used to turn a turbine, whereas in a pressurised water reactor they separate those two systems. They have one system which is pressurised and does not - basically it's a closed loop, it just goes around and around and delivers its heat to something called a steam generator, and there another loop of water, ordinary light water, is allowed to boil and generate the steam needed to generate electricity. So in the Canadian system we have a pressured heavy water reactor.

Now, what's the significance of the heavy water. This is again quite technical, but it turns out it was discovered long ago, way back in 1939, it was discovered that when you're using natural uranium, uranium that just comes out of the ground without going through any fancy processing other than enriching - other than refining it, you can't get a chain reaction going unless you slow down the neutrons for technical reasons. So this slowing down process is called a moderator.

Now, if you're only using natural uranium it turns out that the only moderators that really work are either very pure graphite, which is what Chernobyl used, or heavy water which is this unusual heavy form of water where the hydrogen atoms are twice as heavy as usual, they're called deuterium atoms. As a matter of fact the CANDU acronym stands for Canadian deuterium uranium reactors, so CANDU is Canadian deuterium uranium. Now, the use of heavy water means that we can use natural uranium. So we have no enrichment facilities in Canada, nor do we need it. We don't have to buy enriched uranium because we can use natural uranium as our fuel. But heavy water is very expensive but the trade-off is that we don't have to enrich the uranium.

Now, for safety reasons this doesn't make a great deal of difference. What does make the difference is the fact that we use these pressure tubes, that's what makes the difference, and the fact that we have this pressure tube design - you see, here's the difficulty, is that in a - hello.

COMMISSIONER: We just have a small problem, Dr Edwards.

DR EDWARDS: I can't see you. Can you see me?

COMMISSIONER: No, we can hear you.

DR EDWARDS: Hello again. I got interrupted there.

COMMISSIONER: We're still - we can hear you but we can't see you hear.

DR EDWARDS: You can't see me. Okay, I have got my camera turned on, so I don't know why you can't see me. How is that? Well, actually I can talk without being seen. I can be like the Ghost of Christmas Past.

COMMISSIONER: Why don't we - we'll continue to try and connect you, but let's continue with the evidence.

DR EDWARDS: Yes. Fine. So it's this pressure tube design. You see the difficulty is with a CANDU reactor, with an American reactor they enrich the fuel so that they can use ordinary light water, just ordinary like tap water, you might say, only very pure, whereas in the CANDU reactor we use natural uranium so we have to therefore use heavy water as a moderator. With the CANDU design, when you lose the coolant, you do not lose the moderator, and that means that the reaction not only continues, but actually speeds up and so you get a power spike at the very moment that you have a loss of coolant, which is like a double whammy, it's like the worst of both possible worlds.

So this requires extra fast shutdown systems and that leads to the need for the duplication. Other than that, there's no real substantial safety difference, in my view, between CANDU and American light water reactors. Of course there are differences, but how significant those differences are is a matter of debate.

MR DOYLE: Dr Edwards, have there been any advancement in the specific means of ensuring moderation in a shutdown scenario?

DR EDWARDS: I'm sorry, I don't quite understand moderation - not moderation perhaps, but cooling, is that what you mean?

MR DOYLE: Yes.

DR EDWARDS: Cooling. Fortunately in Canada we have not had any meltdowns - well, not in a power reactor. We did have one of the world's first major nuclear accidents in 1952 involving a small research reactor called the NRX reactor which is a precursor of the CANDU and it involved a power

excursion which actually destroyed the core of the reactor and blew the roof off. In a certain sense you could say it was almost like a very miniature, very, very tiny miniature version of a Chernobyl accident and that is, of course, something that gave the CANDU designers a great deal to think about when they were designing the upscale commercial sized power reactors.

But other than that, we have been very fortunate in Canada. We haven't had those types of accidents. We did have a Royal Commission inquiry in 1978, they published a report, this is the Ontario Royal Commission of Inquiry on electric power planning and they pointed out that under the most pessimistic assumptions that if we had 100 CANDU reactors operating in Canada, then again I stress under the most pessimistic assumptions, we could have a core meltdown about once in every - I believe they said four years or something like that, I may be wrong about the number, but they did say that you would be able to have meltdowns in CANDU reactors if you had a large enough number of them.

So far we have only got about 20 CANDU reactors in Canada and the population is not - that four years is wrong. I'm sorry, I misquoted that. I retract that evidence. It wasn't four years. I think it was once in 40 years. That's it, once in 40 years. That if we had 100 reactors operating in Canada at some future time, under the worst assumptions we could possibly have a meltdown once every 40 years. That's assuming, of course, that the technology remains unchanged and there aren't improvements made, et cetera, et cetera. So that puts it into a little more sobering perspective.

The difficulty with these reactor accidents is that you can't really say that for any reactor that such an accident is impossible. By its very nature it is possible, but it's highly unlikely. The difficulty with likelihood, and I'm a mathematics professor myself, the difficulty with probability is that it doesn't tell you, doesn't give you any assurance that something is not going to happen, it just tells you with what frequency you can expect it to happen, and it does not give you any way of predicting what's going to happen in a particular case. So that's why we always have to be constantly on guard and vigilant in dealing with these systems.

MR DOYLE: Dr Edwards, at that point it might convenient to move topics away from some of the inherent risks in the design considerations to the cultural and regulatory factors which in your opinion either detract from or assist in improving safety, and I wonder whether you might start with some observation about any of the particular inherent difficulties that arise in the nuclear industry because of its complexity.

DR EDWARDS: The complexity of the technology means that a lot of people are mystified by it, including decision-makers, and politicians, for example,

generally don't necessarily have a background in nuclear science. One of the only ones I know, I think, was Jimmy Carter, he was actually a nuclear engineer in the American nuclear navy. But outside of him, I don't think of any major politician who has a background in nuclear science. So that the technology is sufficiently complicated that people tend to be mystified by it and therefore feel a little bit – they find it difficult to judge, other than by trusting the experts in the industry itself. The difficulty with trusting the people in the industry itself, is that there is either consciously or unconsciously a kind of a conflict of interest there because they are devoted to the industry and they want the industry to succeed and of course they try to reassure the public that it's safe and they try their best to make it safe but there is this problem of – well, what if they weren't so devoted to the industry and had the same knowledge, would they make the same judgment? Would they perhaps see it as being unsafe? And one of the difficulties with dangerous technologies is that people who work on the technology feel conflicted and it's difficult to blow the whistle on a technology that you truly believe in. So this is an inherent problem.

Similarly when you have a regulator, although independence is the goal, it's difficult to maintain that independence. The people in the regulatory body are often drawn from the very industry that they are regulating because they are experienced in that field and consequently you need people with understanding and expertise, so how do you kind of keep regulatory independent when in fact there is this constant interaction between the people in the regulatory body and the people in the industry. They tend to come to see themselves as colleagues and if I might draw an analogy, you might think of the regulator as drifting towards being more of a coach than a referee. We are very fond of hockey here in Canada and of course the coach of the team will try and keep the players on their metal and make sure that they're doing everything properly but it's not the same thing as a referee who will blow the whistle and say, go to the penalty box, right. So this problem of independence is not an easy one to deal with.

MR DOYLE: And what are the best ways of, from a regulatory point of view, of trying to encourage that independence? Are there any particular views you have about the way in which the regulator either reports to the executive or parliament, or through different ministers that assist in preserving that independence?

DR EDWARDS: I think it's very helpful to have frequent – well, we don't have this in Canada but I think that the regulator should probably report annually to the parliamentarians so the parliamentarians can hear what kind of concerns are crossing the desk of the regulator and get some kind of insight in to the technology. Have an opportunity to ask questions and to learn more about it. There is a danger that if the regulator never interacts with the decision

makers, or the parliamentarians that it just creates a widening gap, rather than an (indistinct) Another thing that I think would be very helpful in my own opinion would be regulators, as the industry itself, they tend to be very top heavy with engineers and physical scientists, geologists and such like, chemists, the so-called hard scientists and they tend to be extremely thin on biomedical expertise. I think it's very helpful to have some biomedical expertise in the regulatory body because they have a different perspective. They have a different approach and also if and when things do go wrong, the biomedical team can be very helpful in advising the public and the workers and everybody, as to what kind of precautions to take in terms of protecting yourself. What kind of foods should be avoided? What kind of measures should be taken? I think it would be very reassuring to the public to have such people on board.

Moreover, if you had a health department, which we do not have in our regulator, if you had a health department staffed with competent and independent biomedical people, they could also help to educate workers and the public as to why we are so careful with this technology. Why we must invest in all these safety precautions because they could make it clear what the dangers are. And they could also make it clear, such basic things as informing people that if and when God forbid that there should be an accident or release of radioactivity, don't think of it as a problem of invisible rays coming from the plant, but realise that it's a problem of a multitude of pollutants going out in to the atmosphere and settling in to the food chain, so that the important thing here is not to think so much in terms of the penetrating radiation, which is the immediate risk to the workers, but to think more of the food chain and what kind of foods – for example, just to give a very simple example, it's well known that iodine 131 goes to the thyroid gland very avidly and especially in very young children can cause thyroid cancer and a multitude of other diseases.

This is why, for example, in Canada, we now distribute iodine tablets, non-radioactive iodine tablets to everybody within a certain radius of a nuclear facility, so that – the reason for these iodine tablets is that by taking the iodine tablets you can put non-radioactive iodine in to your thyroid gland which means that your body will then reject the radioactive iodine because it's already saturated. It's already got enough iodine, it doesn't want any more. So that it's a preventative measure. Now this is very important for young children, so that for example it would be beneficial to have health professionals who could tell nursing mothers and parents of young infants, perhaps for the time being to stop using fresh milk and start using powdered milk. Powdered milk that was stored before the accident occurred and this way you can cut off that milk source is one of the main ways by which the radioactive iodine gets in to the bodies of young children and nursing mothers as well.

MR DOYLE: You have been addressing the topic of making sure that there's

a proper engagement with the community about the nature of the danger presented by a potential nuclear accident. I wonder if there's also a need to ensure that there's enough transparency at a regulator and operator level to ensure that the public has an appropriate level of comfort in relation to preparedness for external events and so forth.

DR EDWARDS: Well, that is something that one has to be very careful with. In the case of nuclear technology, as opposed to the safety questions which is what we've been talking about here, there are the security questions. Now security is different from safety. Security means protecting against malicious acts, for example somebody who might want to steal radioactive material for malicious purposes, so-called dirty bomb or some kind of malicious contamination. Security is very important, not only with the theft of radioactive materials, particularly plutonium which can be used for nuclear weapons and which every nuclear reactor does produce, but also in this world, unfortunately we have to worry about such things, terrorist attacks. We've seen the planes that brought down the World Tower in New York City. We certainly don't want to see that happening at a nuclear reactor. So one does have to have extraordinary security measures in place. And in fact here in Ontario at the Bruce power plant we have a SWAT team which is very, very well trained and they have participated in competitions and have won prizes for being extremely effective at stopping any kind of intruders. So these are things that have to be thought about in the case of nuclear technology which don't readily arise in most other circumstances.

COMMISSIONER: Dr Edwards, we still can't see you but I do thank you for your evidence this morning and I wish you the best for the future.

DR EDWARDS: Well, thank you very much and the same goes to you and I – one day I hope to find myself in Australia. I've never been there but I'm looking forward to coming some day.

COMMISSIONER: Thanks Dr Edwards.

MR DOYLE: Thank you.

DR EDWARDS: Thank you.

COMMISSIONER: We will now adjourn until 12.30 when we will have Professor Peterson.

ADJOURNED **[9.48 am]**

RESUMED **[12.30 pm]**

COMMISSIONER: We resume at 12.30 and I warmly welcome Professor Peterson from Berkley University in California. Counsel assisting.

MR DOYLE: Professor Peterson teaches courses on reactor technology and reactor safety amongst other topics in a nuclear engineering faculty at Berkley. He has a particular interest in regulation and licensing of nuclear reactors and has served in many advisory roles to government bodies and organisations in the United States in relation to nuclear safety issues. He's currently a member of the Diablo Canyon Independent Safety Committee which is responsible for the periodic review of the operational safety at the Diablo Canyon nuclear power plant.

COMMISSIONER: Professor, welcome and thanks for joining us. We might just start with a bit of a general question in terms of we're trying to understand, from a safety perspective, reactor design and what's happened over the years. So perhaps if you wouldn't mind starting with, at a very general level, what are the critical safety functions and the core philosophies involved in reactor design?

PROFESSOR PETERSON: That's an excellent question. So as with other complex technologies that have hazards, such as aircraft, such as chemical facilities, such as hospitals, where you're doing something that is beneficial but you could also do harm if you didn't do it well. It's important to systematically identify potential sources of hazard and in the licensing process, design and licensing process for nuclear power stations, one has to have a systematic approach to identify all possible sources of hazard within the facility and there will be a number of different hazardous materials that one needs to review and consider. One also needs to consider all of the potential operating modes, not just when you're producing power but for example, if you were refuelling a reactor. Now that comprehensive review is necessary, the unique hazards associated with nuclear power plants really relate to the radioactive materials in the reactor core that are generated under power operation.

The fusion process that releases very, very large amounts of energy from very, very small amounts of fuel, uranium, generates in addition to the heat, radioactive products. Fission – we call them fission – the principle important hazards that needs to be considered in the design of reactors in order for them to be safe. And so most of the core philosophy and principles associated with reactor safety relate to how to make the reactor itself safe. But we don't want to minimise the fact that you need to also pay attention to how you manage spent fuel and other radioactive (indistinct) hazardous materials in the facility. But for the purpose for today, I'm going to focus most of my discussion on the safety of the reactors themselves and in particular, on the safety of reactors in operation and reactors that experience transience or accidents, to assure that there's not a release of radioactive materials. So there's, I would say perhaps,

five primary principles that one wants to think about for reactor safety and I can describe each of them briefly.

The first, as I mentioned, is that as was discovered in 1938, the fission reaction of uranium and other fissile isotopes releases multiple neutrons and in a critical reactor, on average, one of those neutrons will go on to cause another fission event, so that you can have a sustained chain reaction. The critical element in the design of a reactor from the perspective of that chain reaction is that it should be self-limiting. That is the natural response of the fuel if the fuel temperature heats up, should be to reduce the rate of the reaction. And this actually happens naturally with uranium fuel, if a reactor is designed properly because there's natural processes that will slow down the rate of reaction as fuel heats up, if a reactor is designed properly. And the light water reactors which are the current most widely deployed commercial technology and the most readily available technology, intrinsically, will shut down the chain reaction if they overheat. The types of reactors that were built in the Soviet Union that used a combination of graphite and water, do not share this characteristic. And the cause of the Chernobyl accident was actually a run away chain reaction caused by the willingness of operators to violate operating procedures and operate the reactor in ways that would make it unstable.

So this leads us to the next principle safety objective that underpins reactor safety, which is that while we know that a properly designed reactor, we can limit the rate of the chain reaction and shut down that reaction with very high reliability. Even after that reaction shuts down, the radioactive products from the chain reaction, from fission, the fission products, will continue to undergo radioactive decay and generate heat. And a critical safety function is to reliably remove that heat, preventing the fuel from rising to temperatures where damage can occur that could release radioactive materials. So because this function of removing heat reliably is of such high importance, and this was recognised very early on, in the 1950s and sixties when the first submarine reactors were being developed, very reliable systems to remove decay heat were developed. But at the time, the technology available to assure that they would have high reliability required the use of active safety systems. That is, redundant sets of pumps and power supplies and heat exchangers that could reliably inject water and remove heat.

The reason for this was much as with the Apollo programme, the fact that the mathematical models and tools were not very sophisticated and you could calculate the reliability of these active systems with high confidence. The issue with the active systems is that they can face what's called common-mode failure and this is the cause of the Fukishima accident. The flooding of the basements and the disabling of electrical power was the fundamental cause of the accident and the loss of ability to remove heat reliably, and then combined with other errors that were made during the course of the accident and a lack of

preparation to manage, was a principle cause of the large releases. Subsequently, we've developed new reactor designs, such as the AP-1000 and such as light water or small module reactors that are now in the process of being licensed in the United States and these reactors do not rely on external sources of electrical power, external heat sense in order to reliably remove under emergency conditions, heat. Because they use what we call passive safety, or gravity driven processes to perform this function.

So the next element for safety is what we call defence in depth. And that is the idea that you should not rely solely on any single mechanism or barrier to assure that you will not release any significant amount of radioactive material in to the environment, should you have an accident, either due to some type of human error, or due to some sort of external event such as earthquake or tsunami. And defence in depth for water-cooled reactors, includes having robust fuel forms but also having primary system boundary and a containment structure that is capable of containing radioactive materials, even if damage were to occur to fuel in the core. So this defence in depth also then is important to integrate in to the design in all different dimensions of how we design. So all systems should have some defence in depth elements integrated in to them.

The other critical safety function that we do provide in the design of reactors is to protect the equipment that's inside the reactor from external events. This is the reason that reactors are placed inside very, very robust engineered strong structures that can exclude the effects of external events and that are designed to withstand very severe ground motion, if you have earthquakes as well. And the Lucas Height actual reactor in Australia provides a very good example of that. If you see it actually has a very robust steel structure that surrounds the reactor building, and that is designed to make it so that objects, including aeroplanes, can't crash into the plant and cause damage that would lead to radioactive release.

And then the final element is that while was take all of these measures to assure that reactors have a very low probability of releasing radioactive materials, and there will be new designs for reactors are even more robust in this perspective, it is important for us to still also have developed emergency response capability so that we can respond if radioactive materials are released by taking appropriate measures to protect public health up to and including evacuation around a plant site.

What we have found in communities that have reactors in the United States is that the additional funding that is made available because of the fees and taxes that the power plants pay results in the emergency response capabilities in those communities being very, very robust, and that provides some societal benefit because of the fact that emergency response is something that we need

on a periodic basis when we respond to natural disasters such as fires and floods and severe weather such as hurricanes and tornadoes, and also when we need to respond to other types of industrial accidents such as chemical facility accidents.

So the core philosophy for reactor safety is to have many different mechanisms which contribute to the overall safety and which make it so that the failure of any one of those mechanisms is not going to result in any sort of substantial negative consequence. That would, I think, be a little bit long-winded, but the answer to your question.

MR DOYLE: Thank you, professor. I think you've already begun to answer the next question I had, but I wonder whether you could develop it a little further. To what extent have the nuclear accidents that have occurred since the advent of nuclear power resulted in developed thinking about some of those five safety philosophies that you've just mentioned?

PROFESSOR PETERSON: This is an outstanding question, and another really important element for any engineering systems is to have a culture which identifies problems and then makes effective corrective actions. So when we have accidents that are serious, the Chernobyl accident, Three Mile Island accident, and Fukushima accident being perhaps the most important examples, it's critical that we use the lessons that we've learned from those accidents to take actions that make it highly unlikely or impossible for that type of accident to be repeated again. So the Three Mile Island accident is an interesting - the first thing I'll do is I would treat the Chernobyl accident separately.

MR DOYLE: Yes.

PROFESSOR PETERSON: Because that really was a consequence of very different design and safety philosophy that existed in the former Soviet Union, and the design of reactors in the case of Chernobyl not only where they could have this kind of positive feedback and rapid power explosions causing severe damage to the reactor core, but also placing these reactors in buildings that did not provide any containment function so that when the accident occurred the material could be released directly into the environment. We learned a lot from the Chernobyl accident because of the fact that we were able to then observe what the consequences were over the years in terms of health effects and things of that nature.

The Three Mile Island accident was the first example of an accident that resulted from what we call internal initiating events, that is a combination of failures of equipment and human errors that led to the temporary disruption of the injection of cooling water into the core, and the set of errors that were involved are things which have subsequently actually been largely eliminated

as potential initiating events through design changes and changes to the training of reactor operators.

So the accident was initiated actually because operators had been performing maintenance on pumps that are used at low power to push water into the heat exchangers called steam generators that remove heat from that kind of reactor, and after they had finished performing the maintenance they made the mistake of not opening the valves on the pumps, which is what we call a mispositioning event in which there's been vast improvements and human reliability procedures that have greatly reduced the frequency of this type of event. That said, reactors should be designed so that no single failure, either human error or equipment failure, can cause an accident.

In the case of the Three Mile Island accident, what happened was that when the reactor was shut down because of a turbine trip, these pumps that were supposed to operate to provide cooling water did not function because they were closed off, and therefore there was no water supply to the steam generators, and the pressure and temperature in the reactor system increased rapidly and then, as designed, the emergency core cooling system activated and began injecting water and everything was perfectly fine.

But the valve opened on what's called the pressuriser in order to prevent the pressure in the primary system from exceeding design values, and what the operators didn't realise is that when they had then established cooling with the emergency core cooling system, that this valve did not completely reclose, and so they actually misinterpreted level changes that were taking place and this caused them to think that they had too much coolant in the system rather than too little. They made a huge blunder, which was to stop the injection of coolant and actually remove or let down coolant, and this allowed the core to become uncovered and overheat.

Today all these reactors have instruments that directly measure whether water is in the core or not. They're called sub-cooling margin monitors, and so this type of mistake is not one that operators would make - monitor for whether or not the core has been filled by water. So the set of corrective actions that have taken place actually have included measures that have greatly increased the reliability of plants over the years, and this is important.

Then we get to the other class of accidents, which are those which we call externally initiated accidents, and the Fukushima accident was the first example of a reactor accident, a severe reactor accident caused by external events, and as everybody knows, a once in a thousand year earthquake that should have been within the design bases because thousand year return frequency is well within the frequency for which we expect reactors to be built, but in Japan there was an unwillingness to make changes even when new

information becomes available.

So therefore correcting the vulnerability of these reactors to tsunami threat was never performed, even though the flooding caused by tsunami is particularly problematic because of its capability to do the common failure for active safety systems, and in this case to flood the basements and disable all of the emergency diesel generators as well as all of the battery supplies, and the severity of the earthquake and the tsunami had also disabled the power transmission system to bring external power to the plant site, and so they therefore entered into what we would call a station blackout.

They had still some capability to inject water into the reactors because each plant had one steam turbine driven pump, and they were taking steam from the reactor vessels and using that to drive these pumps to inject water. But that only worked on a temporary basis, and so when those steam driven pumps finally failed, and it varied from reactor to reactor how long that took, and one of the reactors used a condenser instead of a pump, the very first Daiichi unit 1.

But when those pumps failed, the Japanese had not prepared in advance to use portable equipment, as had been done in the United States after 911 when we had to think about the question of what would operators do at a plant if a large commercial aeroplane were to crash into a plant, and to disable the equipment needed for active cooling, because our plants also rely on that.

So the delays in implementing water injection and inventing of containments, the water injection ultimately they were able to establish water injection using fire trucks that were on site and they were able to inject sea water into the reactors and stop the progression, but this occurred too late from the perspective of severe damage to fuel, chemical reactions of steam with zirconium metal cladding leading to the generation of hydrogen, and then the other key issue was the fact that in these boiling water reactors, which are different from those that you would likely want to consider in Australia, but the boiling water reactors, energy building up inside the containment will cause it to pressurise and in this case by not doing controlled venting that would have filtered the release, they leak large amounts of hydrogen and fission products into the reactor buildings and this is in turn was the surplus of the explosions and the offsite release of radioactive material.

So the correct response whenever problems are detected involves a couple of things. The most important is to have a strong safety culture that rewards the recognition and reporting of problems. Here on the Independent Safety Committee we monitor the plants, Diablo Canyon's corrective action program. Of course there have been no events as serious as an accident here, but what we want to do is to make sure that we're constantly monitoring for problems at

much, much lower levels of safety significance.

For example, if a motor that is pumping water through the condensers of the turbines fails because of a failed temperature sensor monitoring the stator windings, which has happened, and this causes the plant to trip, to make sure that there is effective processes to identify the cause and then correct that problem, moreover to share that information with other plants around the country so that they can take similar corrective action, and the systematic process of whenever problems occur, of determining the cause, which can include not just the mechanical elements but also, say, deficiencies in training or deficiencies in the leadership as well, correcting those problems so that the problems are not repeated is a critical element of reactor safety and, if you think about it, safety for commercial aviation, safety in hospitals, identifying reporting problems and having them be corrected is fundamental.

What we see if you look at statistics for the United States was in 1970s and 80s nuclear plants in the United States had abysmal reliability. Any day of the week only about two-thirds of the plants would actually be operating and the rest would be shut down for a variety of different problems. It also varied a lot between utilities. Some utilities their plants were reliable, other utilities they weren't.

Systematically through the 1990s substantial improvement occurred in the United States, primarily because we deregulated electricity. That doesn't have anything directly to do with safety, but it became possible for plants that were performing very poorly and had no reliability to be sold. What was observed was when the plants were sold, uniformly within 18 months or so the capacity factors of the plants would raise from around 50 per cent up to about 85 per cent, and this was purely - it was not because the workforce had changed, instead it was because of changes in management and especially management philosophy around safety culture and encouraging the reporting of problems so that they can be corrected.

So there's a number of lessons that we have learned from these accidents which have occurred at these plants. I think one of the most important lessons is the value of how the methods for removing heat from reactor cores do not rely on external sources of electrical power and instead rely on natural or gravity driven processes to also have normal shutdown cooling which is active, uses electrical power, and the combination of those two things then contributing to safety of the new designs.

MR DOYLE: Professor, just picking up on that last aspect of the passive system and its protection against the loss of external power, are there any other aspects of a passive system which make it more safe or more reliable than an active system of cooling?

PROFESSOR PETERSON: Right. So the passive safety systems, there is a number of elements which make them attractive, and in my research group the major focus of our research has been on developing improved methods for passive safety. So through the 1990s, for example, in my research laboratory, we did most of the work studying how non-condensable gases like air can impede the condensation of steam, because in a reactor, in a light water reactor with passive safety, what you want to do is you want to supply water into the core where it can boil, removing heat, you need a mechanism to condense that water, that steam, back to water so that it can run back into the core and set up a heat removal power.

The thing that can impede the condensation is non-condensable gases. So much of the work that we did involved understanding the effects of non-condensable gases so that we could predict and prove that the passive safety systems could function with adequate heat removal capability under a wide variety of different conditions, and this was used in licensing of AP1000 and ESBWR.

So one of the major benefits that I see from having a combination of passive safety systems for emergency k heat removal and additional systems for active heat removal, as well as another layer of defence, portable equipment that can be used to restore cooling functions as well, this is called in the United States FLEX equipment, is that the passive equipment because it's located inside this robust containment building structure it's difficult to get physical access to, and because we also need to make sure that nuclear facilities are physically secure against attacks by terrorists and also against insider type of efforts, having equipment which can provide removal of heat which is physically very, very difficult to disable, because it's designed to be physically difficult to get access to, it doesn't require a pump - pumps have to be inspected once per shift generally, right - so they're located in places that operators can get to very easily.

That, of course, if you think about it, obviously makes it easier for unauthorised access to be easy as well. So in my judgment one of the benefits of going to passive safety is that it improves physical security for plants also and it reduces the size of the guard force that you're going to need for a facility because the guard force size is going to be established by time motion studies, you have a design basis threat which will be an assumption about numbers of people who are trying to attack a plant, what their weapons and capabilities are, and that will determine size of your guard force. Your guard force will be much, much smaller if your safety systems look more like a bank vault.

So these are advantages of passive safety systems. Passive safety systems also have failure mechanisms, they're more susceptible to flow blockage. So if

something unanticipated were to block flow, because the circulating forces are relatively low, you can impede heat removal, and this a principal reason why you want to have redundancy and diversity, and a part of the diversity that is good to have is some active systems that can also, with much harder driving force, drive cooling into the core. Again, perhaps a little bit like long-winded, but trying to answer the question.

COMMISSIONER: Thanks, professor. If I might continue with that theme about looking to the future. You have a lot of experience in the nuclear industry. I'd be interested in your view of what you think might be the most successful of the Generation IV technologies - and we'll ask you the million dollar question, when do you think those sorts of technologies might be commercialised and why?

PROFESSOR PETERSON: Okay. So of course. That is a very, very good question. Let me answer it sort of in two parts, because I need to divide the part which is sort of the policy framework, why we should be thinking about developing both small modular reactors which I think is an important next step, as well as why we need to be investing in the development of advanced nuclear technologies that don't use water as coolant. I cannot predict for sure, precisely which of these technical options is most likely to be successful, although I have strong opinions that drive my research programme and the things that I'm working on personally. But I think it's important to differentiate because in my judgment, the private sector has the best ability to make decisions about how to best design reactors to be more economic. So a couple of important statistics – we've been trying to study this question of what makes the construction of new nuclear plants expensive. And it's kind of shocking. I've done studies and I can forward if you'd like to see them, the simple spreadsheets, when we look at the total quantities of steel and concrete and copper, stainless steel, aluminium, the materials needed to build different types of energy infrastructure.

And so if you compare a conventional generation to advanced – generation to light water reactor, pressurised water reactor, like the Diablo Canyon plant that I'm nearby right now, two modern windmills, like the best is two megawatt, fairly large scale windmill and to a typical automobile, like say a Chevy Malibu, and if you take the prices for procuring bulk steel, bulk concrete, copper these things, the commodity prices that you can download from the internet and you multiply the quantities by these prices, to come up with the total amount that the materials cost, and then you look at how that compares to the price that you would pay today. So a typical nuclear power plant today, when you look at cost, you'll be told that you'll need to spend about $5,000 per kilowatt of capacity to get one built. And the ones we're building in the United States, the new AP-1000's are probably the – a bit more than that. The ones being built in China may be half of that but that's about $5,000 per kilowatt is the nominal number today. Of that $5,000 somewhere

between 36 and $50 pays for all the materials. That is the materials are less than one per cent of the purchase price.

So the wind turbine, those materials are currently about 11 per cent of the purchase price. For the Chevy Malibu which is a pretty sophisticated piece of equipment, you can – I mean in the reactor, this is reborn concrete. This is not that sophisticated. The automobile, the cost of the materials used to build the automobile like a Chevy Malibu is somewhere around eight per cent. So the major question is what is it that makes it so expensive to convert these materials in to reactors versus other types of energy infrastructure? And I think that one of the fundamental things that did strategic (Video link interruption) in development of nuclear technology was to assume making reactors big (Video link interruption) less expensive, and by the time we got to a 1,000 megawatt larger, I think that we were eliminating the opportunity to introduce and prove and to learn from experience. Because we were building such small numbers and because each individual reactor was so enormously expensive, the conservatism that you had to take in terms of everything that you did, because anything that would not perform perfectly would be a problem, was enormous. So this is one of the key reasons why I think that either one wants to focus on reactor technologies, which are established and we know how to build them, AP-1000 being probably the best example of a passive plant design, albeit large, we know how to build them with pretty high reliability, as well as light water reactor SMRs.

There's another technology which I think really merits serious attention in this coming decade which is the concept of floating nuclear power plants, based on the big cylindrical – currently they're used to drilling rigs in very, very robust floating structures. MIT is working on this technology; we're doing some studies as well. The key thing is that in shipyards you can fabricate steel in to large structures at much, much lower cost and much, much more rapidly than we can do when we try to build things on land at a site. Even with modularisation in the construction on land, for the construction on land, there's – it still ends up being significantly more difficult and complicated than what's routinely achieved in shipyards. So this is another area of technology that – along with smaller reactors, that I think merits looking at, or using well-established larger reactor designs.

So that takes me then to the question of what about Generation IV? And where do I think the major opportunities are? The first thing to emphasise is that among the Generation IV options, they have different advantages and disadvantages. They provide different types of products. Some of them are very, very good at delivering heat at higher temperature which is valuable from the perspective of reduced water consumption because of more efficient power conversion, of the ability to produce alternative products. Some of them are very efficient in how they would use uranium or thorium as a fuel. Some of

them have the capability to destroy waste, although all fission energy systems will generate some waste that will require geologic isolation. This is inevitable. We don't have technologies that can adequately recycle enough to completely eliminate the need for geologic disposal. And moreover, the scientific consensus that properly engineered and sited geologic disposal facilities can provide safe long term isolation for all nuclear waste is very, very high.

So then my personal interest and the major focus of my personal research has been on reactor technologies that would use molten salts as coolants and possibly even as solvents for liquid fuel. But currently the major focus on my research group is towards the use of fluoride salts as coolants. And the fluoride salts have a set of attributes that make them very interesting as coolants for reactors but these involve trade offs with other desirable features that the alternative coolants would have. The salts are chemically stable and because they have very high boiling temperatures, up above – closer to the melting temperature of steel, molten salt systems will intrinsically have very low pressure. And because they have very low pressure, they can use primary coolant (indistinct) relatively thin wall and lightweight.

In fact, this is the reason that back when people were really looking seriously at the development of reactors to power aircraft, which actually thankfully we never actually did because that would be – you don't want to put reactors in airplanes. But the performance requirements for a reactor that could be light enough to go up in an aeroplane and could deliver heat at high enough temperature to drive a gas brayton cycle; those are things that are very positive performance parameters for things that would be used on the ground as well. And the molten salts emerge as the most logical technology. So the aircraft reactor experiment that was built at Oakridge National Lab used molten fluoride salt with uranium dissolved in it as fuel. And it was a very, very compact lightweight low-pressure reactor. So at any rate, with the molten salts, they also have the chemical capability, if radioactive fission products are released from solid fuel, or if they're in the fluid fuel, the problematic fission products that Fukishima caused long term – caused the most – the largest problems, iodine and caesium, under the chemical conditions of molten salts they just get (indistinct) extremely difficult to mobilise, and so what we're concluding is that when you make this transition you can achieve your safety through more intrinsic characteristics of the reactors because of the physical and chemical processes that make it more difficult to mobilise radioactive material. Okay?

So these are some of the reasons that we have interest in studying these technologies, and in fact we've had researchers from ANSTO visit us here in the United States and some graduates students also. We have a graduate student that's currently helping us with benchmarking models for some of the

codes for the salt core reactor technologies, and ANSTO has a collaboration currently with the Chinese Academy of Sciences where they're working also to develop thorium molten salt reactor technology.

So I think that the key thing is that the Generation IV technology does remain at least a decade to two decades in the future in terms of being administrated sufficiently for commercial deployment. But I also think it's an area where any country that envisions utilising nuclear energy would want to develop its own domestic capabilities to evaluate, perform research, perhaps even generate commercial designs and deploy these reactors.

Now, the other element about reactors, when you look at the Generation IV technologies that were deployed or were developed back in the 70s and 80s into the 90s, the same basic mistake of trying to make reactors really big was committed. So, for example, the French, their Superphenix reactor was enormous and it ran into significant reliability problems. So in Gen4, I think if Gen4 reactors, the initial commercial deployment focuses on small modular configurations, then it will be far easier to innovate and to develop these technologies more rapidly, and so our major focus is on develop these technologies for deployment as multi-unit SMR configurations, and this I think is the area where we're most likely to see rapid progress towards developing the Gen4 technologies.

COMMISSIONER: Just to finish that section, and thank you for that explanation, is it your view that molten salt reactors are the most advanced in terms of the pathway to commercialisation?

PROFESSOR PETERSON: So again I need to emphasise that as a researcher at a university my focus on the molten salt technologies comes from my own judgment that they're a substantial opportunity. I do think that as we get to smaller reactors we can compress the development time scale substantially because we can build prototypes and demonstrations at sufficiently low cost that you're willing to iterate a few times before you get to the final design.

The other thing is that we've been looking at other industries to try to find examples of better practice. So a very important industry to look at is biotech where the licensing process is a phased process and you can address key fundamental questions such as basic safety characteristics very early on with go-no go type of gates. To the extent that we can develop strategies for licensing new reactor designs in a similar way, that could have a very positive impact.

A couple of additional companies where there is, I think a number of important lessons to tease out regarding innovation are the rocket company SpaceX, and the electric car company Tesla. SpaceX went through a beautiful process to

develop a small reliable rocket engine as its first step, and to test this rocket engine, what they called the Falcon 1, which was a rocket that used a single one of these Merlin engines and they had a smaller Kestrel for the second stage, and the start-up company formed by Elon Musk that successfully developed this rocket, was completely different from the approach that resulted in the Space Shuttle.

In some respects I would consider the Space Shuttle, which over its lifetime the launch costs for the Space Shuttle were $60,000 per kilogram, and the Space Shuttle had very poor reliability. Accidents with the Space Shuttle were catastrophic, and there's a number of reasons why the fundamental design of the Space Shuttle contributed to that. What Musk has done is essentially to develop a highly reliable relatively small rocket engine, and then use nine of them to power a much larger rocket that has therefore significantly higher reliability.

The Falcon 9 heavy will be three of these rockets coupled together, 27 engines, the outside tanks feeding all the engines until they're empty, then removing the first two stages and then the third one, the middle one continuing on is the second stage, which is, you know, sort of a brilliant approach that completely re-fenced the strategy for how to develop that technology.

Tesla also has a set of very good lessons that you can dig out, and so I think that - and this is a space where we'll see the most interest in innovation occurring in start-up efforts, developing smaller scale reactors. If you look at water cooled, light water, small module reactors, the company in the United States that has been the most successful and is advancing towards design certification is a start-up company called New Scale that was spun out of Oregon State University and got far enough along with a very novel reactor design where the entire - these are very small reactors that can be delivered, not just the reactor, but assembled with the containment vessel all in one unit, and just settle into place in a plant.

This is an example I think of the benefits of having innovation with smaller organisations as in biotech doing a significant amount of the initial development and then transferring these ideas to larger organisations, in this case it was Fore, which is a large, multi-billion dollar architect engineering firm that has acquired New Scale and has carrying the technology through to commercial deployment, and I think it's these sorts of strategies that will have the greatest potential to address this deficit that we've had in innovation and to find some way to arbitrage this huge difference in price for converting materials into nuclear power plants versus converting materials into wind turbines or automobiles. The companies that figure out how to narrow that gap will be highly successful.

MR DOYLE: Thank you, professor. I want to move now just briefly from the topic of design and innovation to safety and regulation. You've already mentioned I think that one of the revelations of the last 20 years was the link between reliability and safety, but I wonder with particular regard to your involvement in the safety committee that assists the Diablo Canyon facility, whether you have any insights into how safety culture and community engagement can be achieved at a local level notwithstanding that regulation might necessarily need to be federal.

PROFESSOR PETERSON: That's a very good question. So I think that there's a couple of really important points related to regulation. The first is that on the industry side it's really critical to have leadership from the board of directors on down that considers safety to actually be fundamental to the success of their business because virtually everything that a regulator wants you to do to make a plant safe also makes it more reliable and economic, and since there is such a large alignment to view regulation as being something that actually the major goals of regulation are things that you want to be competent in doing anyhow, and then of course there will still be burdens associated with regulation.

But to view it from that perspective so that you're proactive in doing the things that make sense from the perspective of making facilities reliable and economic, this is sort of a critical mindset and it contributes to the mindset of safety culture because fundamentally what you want to have is a culture and operation of these plants that incentivises the reporting of problems, so that they can get fixed. And that then has mechanisms by which you can make changes to procedures, technical specifications, licenses, where you identify things in ways that things could be done better to make them safer. So the other element around regulation is that oversight can be valuable to a business. In some ways, you can think of oversight as being quality control and validation.

So for example, in the United States it's uncommon for plants to have an independent safety committee likes ours. I'll come back to that in just a second. But of course nuclear power plants in the United States are regulated by the US Nuclear Regulatory Commission which has statutory authority to issue licences and to take licences away and to issue fines and that develops regulations and the NRC monitors the operation of the plants. When the NRC monitors, one of the ways that they judge whether or not the operator has good safety culture is to look at how many problems are being self-reported and entered in to the corrective action programme to be fixed, versus how many problems are self-revealing. That is, something breaks that shouldn't have and they have to go in and fix it. Because the evidences from safety culture is that people – that your self-reporting problems. So we have the NRC.

On top of that, in the United States, after – actually before the Three Mile Island accident – no, it was shortly after the Three Mile Island accident, the Institute for Nuclear Power Operations was formed which is an industry group that independently reviews operations, maintenance, engineering of all plants and it involves peer review. So NPO takes the best people from one plant and brings them to evaluate different plants. The NPO also is the organisation that manages the sharing of operating experience between plants. So any problem that occurs in a plant will be transmitted to all the others so that they can evaluate whether some similar problem might exist. And NPO issues rankings for plants and the interesting thing about those rankings is that the insurance companies use those rankings as the basis to set their insurance premiums, which creates an incentive for the plant management to work to do a very good job with respect to NPO, which is the reason why all of the plants in the United States have a third evaluation body which is normally called the Nuclear Safety Oversight Committee. Its job is to assess all of these different areas of the plant operation and report back to the CEO of the company how the plant is doing.

So that the CEO has an independent source of information about whether the plant is being run well and safely, that they can use to judge whether they're really prepared for the NPO and the NRC inspections and whether they are properly – whether the financial interests of the company are properly being addressed. And then the interesting thing about the independent safety committee, it was formed back in 1990 when California's public utility Commission did something very novel, which was to tell PGNE, Diablo Canyon plants were not running particularly reliably, did not have particularly high capacity factor back in the mid-eighties. And they told PGNE that rather than getting just a 100 per cent rate recovery, that they would come up with a deal where PGNE would be paid a certain amount per kilowatt-hour and if PGNE could improve the reliability of plants, they could actually recover all of their development costs. So they have an incentive to try to increase capacity factor.

The concern was that PGNE would cut corners and so part of this deal was the creation of this independent safety committee and we do not have any regulatory authority but the three members of our committee, and you can see our website dcisc.org, the three members, I'm appointed by the Governor, so Gerry Brown. We have another member who is appointed by the Attorney General and a third member who is appointed by the California Energy Commission and we serve three-year terms and so reappointments occur for one member every three years. And our job – we maintain a list of about 200 different things that we monitor at the plant. We hold public meetings three times a year, like the two-day meeting I'm at right now. And then in the intervening period we take three trips, one each month to the plant for what we call fact-findings, where a member and a consultant go to

review items on this open items list. And when we hold the meetings, public meetings in particular, we discuss what we found and we identify if new issues emerge, or if public raises concerns, we will add items to this open items list and investigate it. Then we issue a very large report, with all of our conclusions related to safety of the plant. The key thing here is that while we only make recommendations, because our recommendations go to senior state leadership, Pacific Gas and Electric has always been responsive when we make recommendations for logical reasons.

I think that there's another example where the same sort of independent technical advisory group, they have a major success and that would be the Waste Isolation Pilot Plant which was built in southern New Mexico as a geologic disposal facility for waste from US weapons programme, Transuranic Waste. In the process of designing and licensing that facility, the Department of Energy which was responsible for doing that work, had the brilliance – they already had a supportive local community in Carlsbad that had a lot of experience with mining potash and therefore were very comfortable with the idea that they could develop a mine repository in very thick bedded salts that they had there. So the Department of Energy funded an independent scientific group that the state chose to locate inside its state university system and the scientific staff of that group reviewed all of the technical issues associated with the repository design and reported back to the state government on their findings. And I think for the political leadership of the state, having the ability to have somebody independently provide a technical assessment on the technical issues was very, very helpful ultimately in being able to make the necessary political and regulatory decisions that led ultimately to this facility being successfully opened and entering in to operation.

So in my judgment, within the field of nuclear energy and nuclear reactor safety, it's really critical to set expectations for high levels of transparency and to encourage extensive questioning attitude and review because that's the mechanism by which you can have early identification of problems and effective corrective action, so that the systems can be sufficiently reliable. The safety is acceptable and then you can benefit from the fact that fission energy provides very large amounts of energy from very small amounts of material.

MR DOYLE: Thank you, professor. Just one final topic, in considering the possible establishment of a power generation industry in a new jurisdiction, there's obviously a potential issue around human resources and expertise. Do you have any particular observations about how a new participant would address that potential lack of expertise? In particular, in staffing the regulator?

PROFESSOR PETERSON: Right. Well, you know I'm a university professor, so I have a strong bias towards education and training. So I think that there's a number of different things that one needs to do. One thing that I

would advise is in strengthening your regulatory system, you already of course have the capacity to regulate nuclear reactors and the use of nuclear materials because you have a research reactor at Lucas Heights and also of course, you have extensive activities in the uranium mining as well. But to expand that capability to be sufficient to be able to regulate civil nuclear energy facilities, will require some investment. And the – one of the case studies that I would recommend looking at it is the United Arab Emirates who developed a regulatory capability so that they could import reactors from South Korea. What you will find is that that involved hiring a lot of retired Nuclear Regulatory Commission staff from the United States to come and assist in setting up that regulatory structure that they now have in the UA.

So one element will be establishing that regulatory structure. It could very easily require some legislative actions to develop or modify your statutes that create that agency. One of the things that I would consider in doing this is the value of creating an independent agency similar to the NRC. The Nuclear Regulatory Commission is not an executive branch agency of the United States. Instead it's decisions are made by a Commission that has five commissioners who serve terms of five years and who can only be removed for cause, whereas an executive branch agency, the secretary or the director serves at the will of the president and always gets removed when a new administration comes in and replaced with somebody else.

So you have, I think, more political influence over regulatory decisions with that model than with the independent agency, and the principal reason that the agency needs independence comes back to the vital importance of safety culture. In other words, you will not be able to have problems reported if the regulator does not have sufficient independence to be able to say, "We have an industry that is reporting hundreds of problems every day at their plant," which is about the number of notifications which will be filed into the corrective action program of a typical plant on any given day.

Of course, the vast majority are quite minor such as light bulbs needing to be changed and that sort of thing, but you will have hundreds and hundreds of notifications, large numbers of problems being reported, and the regulator has to be able to say the vast majority have no safety significance, because otherwise you can't get problems reported so that they can be corrected, and I think that that's one structural element that's really necessary, it's a societal contract.

For any complex technology, if you want to have safe health care, you need to create an environment where hospitals, where the staff are encouraged to report problems, even if it's embarrassing, right, and if you want to have safe commercial aeroplanes, you need to have a system where maintenance workers will report problems or if they hit a point in their procedure where you really

don't know what to do, they don't do the work around something but instead they stop work and get guidance and maybe even get the procedure modified. That's really critical.

The other element is in terms of building up the base of engineering capacity within the university system. A couple of mechanisms for doing that would be, for example, to provide scholarships to students to pursue graduates, that is, more internships at universities in the United States, for example, as well as potentially internships with industry, so that you can build up this competence and this understanding of particularly some of the modern approaches to understanding safety, and to fund some research internally so that your universities can begin to do things such as work to perform experiments and to validate models for passive safety systems using integral and separate effect tests, and to begin to contribute to technical conferences in the areas of reactor safety nuclear fuel cycles.

These would sort of be essential elements of standing up the capacity to competently regulate this technology so that you can have confidence that it will operate safely and provide the benefits of affordable, low emission electricity generation.

COMMISSIONER: Professor, that's an ideal time for us to conclude. Thank you very much for your evidence. We very much appreciate you spending the time with us.

PROFESSOR PETERSON: It's been my pleasure and I also admire the work that you're doing. I have to say that the sophistication of the questions that have been posed to me has been quite impressive, so it indicates to me that you are already well along in establishing an understanding of what the technical issues and regulatory and safety issues are associated with nuclear energy technology, and I have to say I admire your effort because of that. So I wish you the best of success in your studies and in reaching determinations about advice for policy makers.

COMMISSIONER: Thank you very much. We'll adjourn to 1430 when the Australian Nuclear Science and Technology Organisation will provide some evidence.

PROFESSOR PETERSON: Very good. Thank you so much.

COMMISSIONER: Thank you very much.

ADJOURNED **[1.36 pm]**

RESUMED **[2.30 pm]**

COMMISSIONER: We will reconvene at the time 14.30 and I welcome from the Australian Nuclear Science and Technology Organisation Mr Hefin Griffiths and Mr Mark Summerfield.

MR DOYLE: Hefin Griffiths is the Head of Nuclear Services and the Chief Nuclear Officer at ANSTO. Prior to working at ANSTO Mr Griffiths spent over 20 years working in both the civil and military fields of the nuclear industry in the United Kingdom with a focus on nuclear safety and emergency planning and is joined by Mark Summerfield, the Leader Technical Support, Nuclear Operations Division at ANSTO. Prior to moving to Australia in 1998, Mark trained in nuclear engineering at the University of Manchester and worked for many years in the nuclear industry in the United Kingdom as a systems safety engineer.

COMMISSIONER: Gentlemen, thanks for joining us. We're on the subject of nuclear reactor safety. I'm sure you're well aware. Might we start with looking at how the development of reactors since the first generation have changed and the safety implications of those various generations of reactors? Just to get a sense of how the technology has changed the safety of activity?

MR GRIFFITHS: Certainly, Commissioner. I mean if we look at the slide, the Generation I or the – actually the difference in the generations can be in some ways based on the time that they were produced but there are also some significant defining design criteria that have been incorporated through the development. So a Gen I reactor would be basically an early prototype, so an example of that would be the Magnox reactors in the UK which are natural uranium fuelled, a graphite moderated carbon dioxide cooled. They were developed through the 1950's. Actually the last one was put in to service in 1974. I happen to know that because that's the last one that's currently operating and I grew up about eight miles away from it on the Island of Anglesea in north Wales. The Generation II probably make up the majority of operating reactor systems, power reactor systems around the world and they're largely light water reactors, the pressurised water reactor or the boiling water reactor but also include the CANDU reactors that are operated in Canada.

Largely the Generation II reactors rely on active safety systems. Within the nuclear industry, as with most hazardous industries, you apply the hierarchy of controls and that will be to put in – to favour engineered systems over administrative controls. The engineered systems on Gen II systems tend to be active, so they rely upon external cooling and auxiliary systems to maintain that external cooling following any significant event or challenge. The Generation III reactors which are like the European pressurised reactor, the advanced boiling water reactors and the AP-1000 have followed on, I think from a recognition that passive engineered systems, i.e., ones that rely on the

physical characteristics of a material rather than an active intervention, represent a further step change in the safety and reliability of those reactor systems. An example of that would be instead of a reliance on external cooling to maintain the temperature of the fuel below that which – at which the cladding would fail, the modern design of reactors try to incorporate natural convection to ensure that – provide that the core is covered with a cooling media such as light water. The natural convection processes will be enough to remove the decay heat once the reactor has been safely shut down.

COMMISSIONER: Okay. And the Generation III+ is a continuation of a passive safety system?

MR GRIFFITHS: Yes.

COMMISSIONER: Yes.

MR GRIFFITHS: And moving – again with a focus on a further development of operability, maintainability, reliability, so these feed in to the – I guess the operational efficiency of the reactor systems. But generally, as with most industrial processes, the more efficient they are to operate and maintain, the more reliable they are. Serves a dual function of improving the efficiency but also the safety.

COMMISSIONER: What is the aspiration of Gen IV in terms of safety? What do we see? I know there are lots of variants - - -

MR GRIFFITHS: Yes.

COMMISSIONER: - - - out there but are there any safety principles we see being developed within that newer generation of reactor?

MR GRIFFITHS: I think as Professor Peterson was saying in the last session, it's an extension of this focus on intrinsic safety. So to looking at intrinsic features of new media for cooling for example, that would be intrinsically safe. So as he was mentioning, in terms of the molten salt reactors, the fact that they can operate them significantly lower pressures is a significant potential improvement over the current high-pressure systems. Is that fair to say Mark?

MR SUMMERFIELD: Yes. One of the things is with moving to molten salts, you don't have the phase change from a liquid to gas, as you do with water, and that makes a massive difference in how you need to address things. It's always a problem is when the water changes from water to steam is when you start getting problems with cooling and all the rest of the other safety aspects. But also operational availability and reliability of systems and simplified systems all go – are also things which are also addressed in the – as a progress

to the evolution. You see the AP-1000 here shown as a Generation III and there's a number of these figures available and others show the AP-1000 as a III+, so there's – the lines are very blurred what is II and III, what's III and III+. There's even a II+ which is, again, a very vague line.

COMMISSIONER: Yes.

MR GRIFFITHS: So again, I think they're all still basic light water systems but are evolutions of those whereas the Gen IV is reaching in to as yet undeveloped territory.

COMMISSIONER: I'll ask this question because I've asked it of all the other experts. Do you have a view on which Gen IV technology you think might be the first to be commercialised? And if so, when?

MR GRIFFITHS: I - - -

COMMISSIONER: I am quite happy for you to say - - -

MR SUMMERFIELD: I don't actually – I think the sort of time scales may be in the next decade or beyond.

MR GRIFFITHS: Obviously you're looking at 20 years and my personal preference – and this is just my opinion are towards – put the pebble beds designs where you have the beads and effectively a (indistinct) of – in the fuel and moderators all in that. Some of that work, particularly from South Africa's been very interesting but the very high temperature gas cooled reactors go back to my youth as effectively they're a very vast version of the AGRs in many respects, using helium. Which one is the optimum one? I'm afraid I have really no opinion on this.

COMMISSIONER: Okay. Well, we might move to something that I'm sure you do have an opinion on.

MR DOYLE: At this point we might just take a step back. We've addressed the inherent slipperiness in the descriptions of Generation II, III, III+ but as I understand it, there's a reasonably clear distinction between the active safety systems that you've mentioned Mr Griffiths and - - -

MR GRIFFITHS: Yes.

MR DOYLE: - - - the passive systems. And while we certainly understand that at a general level, we thought it would be useful for you to use a graphical illustration to just explain in practical terms the way the two different systems address the critical function of core cooling.

MR GRIFFITHS: Yes. As you can see on the design here, on the left hand side, you've got a Generation II pressurised water reactor of the Westinghouse type and the APR-1000 on the right hand side. Essentially the main functions of any reactor safety system are to effectively shut down the nuclear reaction by removing reactivity. Once it's shut down there is still a significant amount of decay heat that needs to be removed in order to ensure that the core and the fuel within the core remains within its integrity boundaries. As you can see on the left hand side, there's a significant amount of auxiliary equipment outside of the pressure vessel. All of which is required to maintain that heat removal capability. Each of those pumps needs to be serviced either through an external grid connection, or through diesel generators. On the right hand side, the APR-1000 has passive means of both injecting water in to the core to ensure that you've got coverage of the reactor core, but also then it allows the natural circulation which Prof Peterson was talking about where the coolant is allowed to boil off. It condenses at the top of the stainless steel pressure vessel, and then there's a heat sink to essentially the external chimney that takes that heat away. The boiled off coolant is then condensed back to go back into the system, so you get that natural circulation without reliance on external pumps. I think it's important to note, as Prof Peterson was saying, that that doesn't take away the emergency auxiliary pumps, that that is still a preferred method. The use of diesel generator back-up for those would still be incorporated, but it adds another line of defence, and defence in depth is essentially the mantra for nuclear safety.

MR DOYLE: I think the next slide shows that the difference - - -

MR GRIFFITHS: Yes.

MR DOYLE: - - - these designs can make to a plant layout arrangement.

MR GRIFFITHS: Yes.

MR DOYLE: Can you just explain what might be the advantages of the passive system in terms of plant layout?

MR GRIFFITHS: Yes. So you can see that there are a number of the buildings on the left-hand side, which is the Generation II building, are not replicated for the APR 1000, that you would still have the shielding and containment functions, but a lot of the safety related mechanisms are now incorporated in there rather than being in the auxiliary buildings. So essentially items 3 through to 10 are removed from the new design. Their functions are still provided, but they're provided in a passive manner within the containment building, but you still have the diesel generators still in place there.

What that means for a site, obviously there's economic benefits in terms of the footprint for the site, but it also removes some vulnerabilities for the items that are present in the GenII design are all outside of the building, outside of potentially the (indistinct) enclosure, and therefore more vulnerable both to external events or potential security related events.

MR DOYLE: Thank you. I wanted to come to another of a passive system, namely the OPAL reactor with which you're intimately familiar. But before we look at the safety system, I wonder if you could give the Commission a brief overview of the purpose and function of the OPAL reactor?

MR GRIFFITHS: Yes. Well, obviously we were tremendously fortunate to be allowed to build the OPAL reactor to operate it on behalf of Australia. It is an approximately 20 megawatt multipurpose reactor that is of an open pool type. It is low enriched uranium fuelled, and the purposes range from the irradiation of low enriched uranium targets for the production of (indistinct) 99 which is the precursor for technetium-99m, which is the most widely used diagnostic nuclear medicine.

We also irradiate silicon ingots for neutron transmutation doping of those ingots for applications throughout the silicon (indistinct) industry, and we supply a range of different energy neutrons to the Bragg Institute, which is adjacent to OPAL, which conducts neutron based nuclear science and technology using multiple neutron scattering instrumentation.

MR DOYLE: Thank you. I wonder if we could come now to - - -

COMMISSIONER: Just before you go there.

MR GRIFFITHS: Yes.

COMMISSIONER: You said low enriched fuel. Can you give us a - - -

MR GRIFFITHS: Yes. Many of the older types of research reactors were run on highly enriched uranium, which is equivalent I guess to weapons grade uranium. So that brings in obviously security issues and safeguarding issues in terms of nuclear non-proliferation. The OPAL reactor runs on less than 20 per cent enrichment, so it's classed as low enrichment, and also our target is low enrichment as well, so they are less than 20 per cent. So we are one of the few low enriched multipurpose reactors in the world and as such that's essentially the vanguard of where modern research reactor design is going to remove or certainly mitigate those issues around nuclear safeguards and non-proliferation issues.

MR DOYLE: Wonder if you might give us a brief outline of the reactor design, but then explain how it uses passive safety to remove decay heat in the event of a shutdown.

MR GRIFFITHS: Yes, okay. As Prof Peterson was saying that passive systems can rely on either the natural properties of the material or rely on something that's ever present, such as gravity. So in terms of first of all safely shutting down the reactor, in addition to the insertion of control rods, which is generally accepted for shutting down reactor systems, we actually rely on the reflection back of neutrons into the core from the reflector vessel which is heavy water which surrounds the main pool. So as another means of shutting down the reactor we can dump the heavy water essentially under gravity into a holding tank. That again is another mechanism of shutting down the reactor.

Once the reactor is shut down again we need to still maintain the heat removal capability to combat the decay heat. Within OPAL, although we have multiple pumping systems backed up again by diesel generators, if all those were to fail in a complete station blackout situation such as Fukushima, then the natural convention within the pool would be sufficient to maintain adequate coverage over the core until the spent fuel had reached its what's called eversafe time period. That is if it was exposed to air then although it will still get very hot, it wouldn't get hot enough to breach the (indistinct) of the fuel.

MR DOYLE: Thank you for that. We might move back very briefly to the different types of reactor designs only to mention one category that you haven't yet touched on, and that's small modular reactors. Just give us a brief overview of what defines a small modular reactor, and what are its typical features.

MR GRIFFITHS: A small modular reactor is essentially what it says on the term. It is a reactor that, unlike the very large current Gen3 and Gen3 plus reactors, it is in the range of 10 to 300 megawatt electric. Also the modular design would allow you to essentially build up that load capacity that you might need for specific purposes by just adding on further modules of a similar reactor type. That increases the flexibility of applications so that it can be used potentially as floating reactor systems to power small island nations, to be looking at supplying power to large and remote industrial applications, or for powering small townships or cities. The small size and the small power obviously have inherent safety benefits in terms of some of the - sorry, averting some of the issues with far larger and more power dense systems.

MR DOYLE: Look, turning away from the conceptual reactor designs to some lessons learnt from history, the Commission has heard some evidence already about some of the developments and lessons that have followed from accidents that have occurred over the last half century. What would be the major developments either in design or safety philosophy that you have

observed as a result of those accidents?

MR GRIFFITHS: I think, as I've discussed previously I think, the move from active systems to passive systems obviously is a potential step change in terms of the management of safety, so as you're not relying on active intervention of systems themselves that are potentially vulnerable to failure.

From a safety point of view, I think the biggest single change is the development of a robust safety culture which is a phrase that the nuclear industry claimed to have invented in the aftermath of the Chernobyl accident of 1986 and really came from work that the International Atomic Energy Agency established when they established an expert group to develop the IAEA 15 guide on safety culture, and that really has continued to be a work in progress up until I think as recently as last year, the US NRC released their most recent guidance on nuclear safety culture and how to develop and maintain that safety culture through all aspects of nuclear operations.

I think it's that integral approach to applying such standards as conservative decision-making, addressing the attitude to the full life cycle, so through the design, to look at potential fault sequences, how they can be best either safeguarded against or mitigated through operation, through maintenance, and then into the transition to safe shutdown state.

MR DOYLE: You mentioned the different fault sequences and the capacity to predict and manage them. The Commission has heard evidence, and there's wide reference in the literature to two different conceptual approaches to safety assessments.

MR GRIFFITHS: Yes.

MR DOYLE: The so-called deterministic approach and the probabilistic approach. These can be difficult concepts to grapple with in the abstract. I wonder if you could try and unpack the concept firstly to the deterministic safety approach before we then take a look at a probabilistic model that OPAL has adopted.

MR GRIFFITHS: Yes. The use of deterministic safety assessment is really the standard across the industry now and has been for some years. Essentially it involves a robust comprehensive assessment of potential initiating events using aspects such as HAZOP, hazard and operability studies, failure modes and effect analysis, operating experience, the development of fault trees, so essentially you can unpack for a particular set of events, what are the key initiating events that could lead to a particular outcome.

The evaluation of those fault sequences to look at how they would progress

from an initiating event to a defined consequence, the evaluation of the consequence both to operating staff and to members of the public over defined time periods, so for members of the public, the resulting exposure could be evaluated over a period of, for example, 70 years in terms of certain long-lived isotopes. That really will then define what the - initially through the design phase, what the number and types of safety systems that will be required, and through the evaluation of the development of the design through to the final design, how robust those safety systems actually are.

In terms of the initiating events, they would be assessed through, for example, reliability data for particular components that have been utilised. But we will also look at external events, and for that conservative assumptions are made on the events that would be selected. So there is some judgment made on the credibility of certain events but, for example, a standard would be to select a one in 10,000 year return frequency event for something like an earthquake or a tsunami. So we're really trying to select very challenging events that are then grouped within what's called the design basis. So you then work out what it is that that design is protected against.

MR DOYLE: So the basic philosophy is to start with the events that can present a hazard.

MR GRIFFITHS: Yes.

MR DOYLE: Trace through the causal pathway and ensure that the safety system has multiple controls against it.

MR GRIFFITHS: Absolutely. I mean, as I said, defensive depth is the key so that we have multiple barriers between an initiating event and a consequence. We're not reliant on one single barrier in any one case to keep us from safe and unsafe conditions.

MR DOYLE: So contrast that with the probabilistic approach, and I think we've got a slide that shows the model that is in operation with the OPAL reactor. I'll just see if I can step through it with you. I think it makes most sense, doesn't it, to begin with the step lines on the right-hand side of the graph. Could you tell the Commission what those lines represent?

MR GRIFFITHS: These lines are taken from the ARPANSA guidance but I think they're largely mirrored in the safety assessment principles that were developed by the UK Nuclear Installations Inspectorate. They relate in many ways back to earlier work that was undertaken by the Health and Safety Commission and the Health and Safety Executive while they were looking at the planning approval for the Sizewell B nuclear reactor. So they started looking at the tolerability of risk. So essentially trying to ensure that the

nuclear industry would be comparable with other similar industries both in terms of the actual risk that was presented, but also society's acceptance of that level of risk.

MR DOYLE: Can I just pause there just to make sure it's clear. On this particular graph you have got the gravity of the risk represented by a dosage rate - - -

MR GRIFFITHS: Yes.

MR DOYLE: - - - of millisieverts and the frequency probability of the event occurring on the Y axis, but the line that's represented by the safety limit reflects an underlying level of tolerable risk to society that could easily be translated in a different industry to something other than dose rates.

MR GRIFFITHS: Yes. You're right. Essentially the safety limit represents the limit of tolerability. If you are to the right-hand side or above that, then the residual risk is intolerable. The safety objective can be likened to an acceptable level of risk. If you're in between the safety objective and the safety limit, you're in what we have referred to as the polar region where you would have to demonstrate that the control measures that have been put in place will maintain the risk as low as what is reasonably achievable, social and economic factors been taken into account.

MR DOYLE: Now, with that background, if we pick one of the vertical lines on the chart which I think represent fault sequences that could occur at the OPAL reactor, I think perhaps focusing on the line RCG2FRPS, I wonder if you could try and explain in as simple terms as possible what's involved in a fault sequence and how you can go about plotting that to determine whether it's within a safe range.

MR GRIFFITHS: Yes. The simple answer is no. To start with I'll pass over to Mark to talk through the reactor based parts of that and then I'll come in with the consequence assessment.

MR SUMMERFIELD: What we did is as part of our safety analysis report which this actually - the graph comes from, we analysed a number of what we considered were beyond design basis events. This RCG2FRPS is one of those. We have in our reflective vessel 12 radiation facilities where we radiate targets for – as part of our molybdenum deduction process. These are effectively mini fuel plates. There's actually four plates per target, three targets per rig and 12 rigs in total. So we had one of the full sequences we (indistinct) events we identified was what happens if we lose the full cooling to these. So it's effectively they're mini fuel plates that would get hot. Especially with the FRPS is our first reactor protection system. If that fails to identify the fault and

fails to trip the reactor, all these targets would melt. They would melt in the reflector vessel; the reactor core would be okay. This is where it's a bit different from a power reactor because they wouldn't have this situation but we would have effectively mini-fuel plates melting, releasing their fission products. That would be released at the bottom of the core and go up.

The probabilistic safety assessment, level one of that is determining the likelihood of that and so the likelihood of that, as you can see from the vertical line up and down from that, ranges from in the region of five times to the minus three per annum, which is about once every 5,000 years, all the way down to nearly 10 to the minus six which is nearly once every million years. So the error band on the frequency is very broad and that's partly as a result of being a research reactor because unlike power reactors, we simply don't have the breadth of background of data or reliability of systems and every research reactor being unique. However, then as part of this being one of the faults we want to look, we then did the consequence assessment and looked at what would be the consequence for the most individual effective dose, which is to the individual standing on a buffer zone boundary, which is 1.6 kilometres, for 24 hours, eating any food locally, breathing the local air, just standing there getting the maximum dose they could. And as you see, the dose then comes up with slightly below point one of a millisievert, is what that person would receive, which considering that the average annual dose in the Sydney region is 1.8 to 1.9 millisievert per annum is less than five per cent of his annual dose he's going to receive anyway.

MR GRIFFITHS: So I think the key things that as you develop this, you make conservative assumptions both in terms of the initiating event, the performance of the mitigating systems that are in place, the release fraction from the target plate itself. The performance of the containment boundary, the dispersion in the atmosphere, the exposure of the person that is potentially receiving this dose and consideration of all potential exposure pathways to come up with a dose which can then be converted in to a risk by the application of the standard dose risk factors that are developed by the International Commission on Radiological Protection. But again, the key thing through this is to show how far away we are from the safety objective. That in essence, is where we want to be. Whenever you're developing a safety assessment, you want to be able to demonstrate that there is a clear safety margin between certainly where the worst-case accidents could be and the safety limit. But in this case, we're below the safety objective which gives us an ever-greater margin. Once you've developed these deterministic assessments, they will then feed in to the operating model for the reactor and form the basis of the safety case. So you set the site operators again below based on the deterministic assessments and then ensure that your actual operating below and the limiting conditions of that have a significant safety margin between where you would be in the worst case operation and the boundary which you were challenging the safety case.

MR DOYLE: Is one of the advantages of this approach, as a complement to the deterministic method, it enables you to pick which fault mechanisms pose the greatest risk relative to the tolerable risk and - - -

MR GRIFFITHS: Yes.

MR DOYLE: - - - therefore enables you to focus your energies?

MR SUMMERFIELD: Definitely. In that respect, the probabilistic safety assessment is very much used as a design tool. It's not the ultimate reliance for safety cases, it's very much identifying where is a vulnerable part, where could the most effort simple addition of a valve, or change of a minor thing can make dramatic difference overall. If you look to get – you want to have an even balance design. If you find you're risking one area that is normally about - - -

MR GRIFFITHS: And again, getting back to safety culture, again that would feed back in to things like operator training, the development of operating instructions and on the job safety assessments, so that people know where the highest potential risks are in terms of potential fault sequences and they can ensure that the work practices adequately reflect that.

MR DOYLE: To what extent are these probabilistic assessments required by regulatory regimes around the world? And if they're not required, are they routinely used nevertheless?

MR GRIFFITHS: I think for power reactors in general they are but as I say, the key aspect of safety demonstration is again – is using the deterministic method. Essentially, where you look at the worst case and ensure that you have suitable barriers embedded within that. PSA is useful I think for looking at the cumulative residual risk and as Mark said, looking at both the initial design and the design modifications that would come in the future as to where you're going to put your efforts.

MR DOYLE: All right. Well, we might leave that topic and move to the issue of emergency planning and preparedness. I wonder if you could outline what you consider to be the key phases and – that form part of emergency planning - - -

MR GRIFFITHS: Yes.

MR DOYLE: - - - and preparedness?

MR GRIFFITHS: I think essentially the starting point follows on from the

previous discussion and the starting point for emergency preparedness and response is that safety assessment. So the emergency preparedness and response procedures essentially are in place to look at beyond design basis accidents but also to support within design basis accidents to ensure that any potential exposures are as low as reasonably achievable. So the first action is the planning, which is heavily based on what the potential full sequence is and what the potential exposure pathways to either operational staff or members of the public would be. Once you've developed that emergency plan, which for nuclear organisations is not something that you do as a standalone. We would develop onsite emergency plans which would be largely under our control, but even so for significant events, we would call on support from combat agencies, such as the local fire brigade, ambulance or police. So it's vital to ensure that there's a multiagency approach to the planning to ensure that the expectations of each party is completely understood and also what the authorities and the overall command and control are going to be.

Once the plan has been prepared, approved in our case through regulatory body, ARPANSA and endorsed by all the other agencies that are called upon within the plan, preparedness is essentially the purpose of not just exercising that plan as a regulator in the UK, it should be a test. You should be testing the plan to try and find out what the weak points are. Does it rely on just having the AT? What happens if people are on holiday? What happens if a critical piece of equipment are not available? How do you work your plan to develop the – to identify the weak points and then mitigate them? If in the worst case, we have to implement the emergency plan, the key aspect is to regain control of the situations and bring the situation back into a safe state while mitigating the consequences both to staff on site, to first responders both from within the operating organisation and from outside, and to members of the public, to be aware of a transition to recovery. The phase of an event would go through an early phase where your (indistinct) would be in control.

Once you're in control, then it would tend to transition to another organisation to try and look at the transition to recovery, not just on the operating site but in any potentially affected area outside, and particularly that applies to nuclear power plants, and then the implementation of recovery, which could involve the transition of evacuated populations back into the area, the decontamination processes that would possibly have to be applied in order to make that area habitable again afterwards.

MR DOYLE: Just wanted to focus on one element of that, which was the mitigation of consequences, and this is with particular regard to lessons learned from accidents in the past and most obviously among them Fukushima. What's meant in this context by the concept of justification in relation to intervention measures, and what observations would you make about it?

MR GRIFFITHS: I think that follows on really from the basic principles of radiation protection is that any action that's undertaken that could lead to a potential exposure should be justified. In this case the actions or the interventions previously referred to as counter-measures are designed to avert radiation exposure to individuals or to population groups. Those sort of interventions include sheltering, evacuation, issuing of stable iodine tablets to saturate the thyroid to prevent further uptake of radioiodine, or the implementation of food bans, each of those actions has a detriment associated with it, whether that's a potential increase in non-radiological health and safety risks, or to risks from - to a breakdown of societal bonds.

MR DOYLE: Perhaps could we just deal with the three intervention measures you mentioned?

MR GRIFFITHS: Yes.

MR DOYLE: Sheltering. What are the sorts of previously perhaps unforeseen but now foreseeable risks involved in that?

MR GRIFFITHS: Yes. I think sheltering is probably one of the lowest risk interventions. It essentially involves going into the nearest building or going into your home, closing doors and windows, turning off airconditioning, turning on the radio or the television and looking for public information broadcasts. But there is a school of thought that if a population are advised to shelter, that a certain proportion will decide to self-evacuate, so you're having an uncontrolled evacuation which could then lead to exposure of people if they're, for example, driving into a potential radioactive plume. It can also block up escape routes that emergency services would want to use in time, or block routes that emergency services would want to use to actually get to the site.

In terms of individuals, you could have vulnerable members of society, the old and infirm, people who require access to special medicines, infants that require baby formula, for example, and even down to many locations particularly within the UK where nuclear power plants are stationed in remote and rural areas, the fact that local farmers would still feel the need to have to go out and tend to their livestock.

COMMISSIONER: So could I just interrupt for a minute?

MR GRIFFITHS: Yes.

COMMISSIONER: How do you engage the local community in your area for instance about these issues? Do you give them briefings? How do you communicate the sort of safety aspects of living close to a nuclear site?

MR GRIFFITHS: We are very open with our site. We hold many, many public tours. We have approximately 10,000 people a year come through our site from not just the local community but schools throughout New South Wales and local Probus groups, et cetera. We advertise those extensively through the local community. We engage in sponsorship at local events. Everything we can do really to try and reach out to the community and to engage with them that they can come and (a) learn more about the work that we do that we believe has a significant benefit for Australia, but also to try and allay any fears that they may have of living in proximity to Australia's only nuclear site.

MR DOYLE: Just following up that topic of making sure there's an appropriate realisation of the risks of radiation, and not an over reaction, I wonder if you might touch on what might be some of the dangers associated with evacuation where it might not be appropriate or necessary.

MR GRIFFITHS: Yes. I think we saw through the response to the Fukushima accident that evacuation was implemented fairly early in the piece which essentially it has to be done fairly early, once an accident such as that progresses then you lose your window for evacuation. I think it was a very brave decision to make that, particularly with the damage the local infrastructure caused, both by the earthquake and the tsunami, and it will undoubtedly have averted a significant collective dose to the population.

Unfortunately through the evacuation, as I was reading in a news article today I think, the cumulative total number of deaths from the evacuation has now exceeded the number of deaths that occurred in the tsunami itself, and I think that really goes to the complexity of implementing an evacuation, that there were a number of particularly vulnerable people, particularly aged residents within care facilities that unfortunately died during the evacuation, and then following on from that, as has been seen with populations that have been relocated in the Marshall Islands and following Chernobyl, there are a number of psychosocial issues that then develop associated with depression, alcoholism, with increased number of suicides, just because of, I guess, the trauma associated with being relocated from your land and the uncertainty as to when you will be allowed to return to a normal life.

I think as part of the justification process, recognises the difference between the benefits and the risks associated with each of these interventions and there are a number of guidance levels that are recommended by IAEA that are adopted by most countries. These really provide a guidance level at which you may start thinking about certain of these interventions. Obviously the greater the detriment associated with that intervention, the higher the averted dose needs to be before that becomes justified.

They are essentially guidance levels, they're not prescriptive, because it will be down to the command and control structure of that particular incident to judge whether the particular circumstances merit the imposition of a particular countermeasure, even though the averted dose may make it worthy of consideration.

COMMISSIONER: I don't think we have any more questions for you, gentlemen. Thank you very much for attending.

MR GRIFFITHS: Our pleasure.

COMMISSIONER: It has been very useful for us to put this into context, particularly with the local flavour to it.

MR GRIFFITHS: Right.

COMMISSIONER: We'll adjourn till 1600 when Mr Peter Wilkinson will provide evidence.

MR GRIFFITHS: Thank you, Commissioner.

COMMISSIONER: Thank you very much.

ADJOURNED **[3.20 pm]**

RESUMED **[4.00 pm]**

COMMISSIONER: It's 1600. We'll reconvene and I welcome Mr Peter Wilkinson from Noetic Group. Counsel.

MR DOYLE: Mr Wilkinson is the general manager of risk for Noetic, a firm providing professional advisory services across a range of industry sectors, including national security and defence, infrastructure, mining, oil and gas. Mr Wilkinson specialises in the management and corporate governance of low probability but high consequence events associated with process safety risks in the oil, gas, chemical and mining industries. Mr Wilkinson was also involved in the design of the Australian regulator for offshore petroleum and has provided many years of consultancy to government and industry in operational risk and safety management in hazardous industries.

COMMISSIONER: Thank you for joining us, Mr Wilkinson, and it's that issue of low probability, high risk activities that I want to start with today. Because of your industry knowledge, what in your view is the key to developing a safety culture at the top level of the organisation?

MR WILKINSON: Well, I think you partly answer the question in how you framed it. These are leadership issues, and the key for leaders in this area, because they are very low probability events, the sorts of disasters that we're talking about, is that they must believe that their source of disaster could happen to them. Failure to do so invariably sends a signal, maybe unintended signal, down through the organisation that the things that you have to attend to to prevent these sorts of disasters are unimportant. So it's a leadership issue and it's about maintaining what some people call chronic needs or a sense of vulnerability to these sorts of events and this is difficult to do because the events are very rare.

COMMISSIONER: So are there appropriate tools and techniques that managements typically use in these sorts of scenarios?

MR WILKINSON: Well, there are, but there's no one magic tonic for this or fantastic pill that solves all these problems, it's about hard work, consistent hard work and, in particular, when you get to the operational phase, which after all is where the serious events happen, they may have the roots in design partly, but in the operational phase there's no substitute about being absolutely clear what the, if I may call them risk barriers or risk controls - people use different terminology - what are the barriers to prevent bad things happening and who is accountable for them, and careful measurement and monitoring, and also this requires an excellent reporting culture because if people don't feel empowered and able to freely report that things aren't as they should be, well, the information can't get to a level that enables it to be dealt with, so it's a reporting culture as well.

COMMISSIONER: So if I was to, not to name companies, but to think about the characteristics of good tight leadership team managing low probability, high consequence events, what would be some of the characteristics that you have seen in your time?

MR WILKINSON: I think there's a very interesting one, and that is that if you ask senior leaders, and I was a senior executive in Caltex Australia, so I have experience of being sat at the top table, but if the leaders don't have a realistic mental model of how these things can happen, what are the causes of these disasters, it's really difficult to progress beyond that and a mistake that's been made time and time again in parts of the oil and gas industry is the focus on where you get feedback, and where you get feedback is on the higher frequency, lower consequence events, personal injuries, slips, trips and sprains.

You don't want those to happen plainly, because you're a caring organisation and caring employer, but if you put all your attention there and not on these things that are less easy to see, you make yourself much more vulnerable to

this big and rare event. So to answer your question directly, you have to be clear, absolutely clear what these controls are and how well they're working in practice.

MR DOYLE: It might be exploring a related topic, but is there a distinction between measuring injury frequencies or outages and measuring process safety, and how do you go about measuring the latter?

MR WILKINSON: Well, you have put two ideas together there. The main dichotomy that I would draw your attention to is that measuring injuries is self-evidently unlikely to offer you much of an insight into how these more complex system-type events occur, because they invariably have some component of design, some latent failures hidden in the design that only become apparent in operations when somebody makes a mistake or there's a poor process. So they will always involve this combination of engineering issues, procedural issues and frequently an individual human error.

So actually you mentioned outages. Outages of equipment or failures in reliability actually might be weak signals that there is some latent defect lurking there, and that gives you the clue as to how you have to deal and manage these low probability high consequence events. It's being alert to those signals, amongst all the other data and information that's coming to you as a middle manager or leader, being alert and knowing what to look for that is sending you a signal that something isn't working as it should, and that should require - demand investigation.

MR DOYLE: How do you go about dividing responsibility for safety issues between the different levels of management and operation within a business that's operating in this hazardous context?

MR WILKINSON: Well, I think the responsibilities should naturally fall out. But, if I may, I'll draw you to a weakness that not infrequently exists, and by that I mean it's not realistic to expect the board of a company to personally know the detail of how somebody at the front line has to construct a flange on a high pressure pipeline. But the person doing that must know that, and the immediate supervisor must know that. So there is a hierarchy really of knowledge that is expected.

So let me take this one stage further. So I've talked about the front line worker plainly must know how to do it. The supervisor must also know how to do it because how can he or she effectively supervise the work without having an insight as to how it's supposed to be done. Now, the manager of this front line worker, I wouldn't necessarily expect him or her to have the detail, but they must know that flange assembly when handling high pressure hydrocarbons in a process plant is a critical activity.

So I would expect from a leadership perspective that manager to go and talk to the supervisor and ask the supervisor, "How do you know people are doing this properly," and also make more occasional visits to the front line to find out himself. Indeed in some areas in the military that's a definition of leadership from one perspective. So does that answer your question in terms of how there is a hierarchy there from different levels of knowledge, but each successive level needs to look down not just one level but two levels at least to find out what's going on. Preferably occasionally to the front line.

MR DOYLE: Well, given that leaders at the top level can't have that detailed knowledge, what are the practical ways in which leaders can begin to instil a safety culture in an organisation that might have previously lacked it?

MR WILKINSON: The safety culture issue is one I would say I would assert is clouded by lots of complex and often academic work, however I'd suggest that there are some organisations who have got this really pretty well nailed down and know what works. I'm not saying there isn't great value in further academic research there, but I would suggest a focus on the practices that people follow is an easier way to change behaviours and get people aligned, and by that I mean if you only focus on values, and I'm not saying values are unimportant, they plainly are, but if you only focus on values, it still leaves people in doubt about practices.

So for critical controls, critical tasks, we should have those nailed down explicitly. What is the task? What is needed of that, if it is a task. It might be a piece of equipment. What is required of the critical control to ensure it does the job it's intended to do. What supporting systems, such as management systems, are needed, maintenance management systems, for example, to make this work properly, and how can we check? We have to actively monitor that critical controls are being implemented correctly, and I would suggest to you that from my experience of investigating a large number of incidents and of being involved in some globally significant ones, for example I'm still currently under contract to the US Government on the BP Macondo disaster. A common feature is that critical controls haven't been effectively monitored in the operation phase.

MR DOYLE: Well, given the importance, in your view, of ensuring that practices are adhered to and continually improved upon, where does the responsibility lie within an organisation for reviewing the adequacy of those practices? In hazardous industries that be organic changes coming from the front line itself, or is that a matter that requires a comprehensive external review?

MR WILKINSON: That's an interesting question. A key part of my answer

would be leadership but I felt I've covered that so I won't talk about leadership. But I would just like to talk about nearer the front line and I mentioned in passing the importance of engendering a culture that allows people to report things but it's not just about reporting things. As we go through that hierarchy of an organisation, the more senior one is the greater the responsibility, I think, to solve a problem as well. So if a quite senior leader goes to the board and say we've got a problem here and expects to be welcomed with that bad news, in the absence of a solution, well I think that's unrealistic. But if it's a front line worker who says look I really think there's a problem here but I don't know what to do about it. Well, that warrants reward and by reward, I don't necessarily mean money, I mean recognition that that person has taken the initiative.

I have seen at the front line, one company in the north sea in the 1990s was rewarding – give a specific example, there was a problem with a piece of water treatment plant and contrary to what most people think, big oil and gas platforms are mainly water handling plants. It's the biggest issue they have, how do they handle all those liquids. There was a problem with the water handling plant and an operator, with his colleague, designed a solution to a problem. Did their own mini hazard study, wrote it up and presented it to the production superintendent. Actually they didn't know that an engineered solution had already been decided upon on the beach, as we say, back in the office but nevertheless the production superintendent rewarded those individuals with a cheque made out to the charity of their choice. So I thought that was an act that tangibly made people at the front line feels comfortable about taking responsibility. In that case, beyond what was needed but very good behaviour.

MR DOYLE: You mentioned earlier the notion of having multiple barriers for hazardous events. Have you come across any instances of systems which have involved too many controls and how do you manage the right balance between the Swiss cheese concept of multiple layers of control but not permitting safety to become an impediment to the effective uptake of what you want the workers to do?

MR WILKINSON: Well, you're plainly familiar with reasons Swiss cheese models which I'm delighted, that saves some time. Look this is a complex area because people articulate what their controls are but it is far from uncommon to find they've articulated controls at quite a high level. So let me give an example. If you're operating an underground coalmine where there's methane explosion risks that can lead to coal dust explosion risks and we've seen these continue to happen around the world, including the developed world, in New Zealand, Pipe River and in Astoria in northern Spain in 2013 in Turkey and so on, so these aren't things that have gone away. I've been to coal mines in Australia where they've said yes we've got that nailed down, here is our

bow tie diagram, listing a 100, 80, 100, 108 controls, I think on one that I saw. And slightly flippantly I said, “Do you make coal as well?” And the point I’m making is that there’s so many apparent controls, if they were genuinely important controls how could you possibly monitor the efficacy of all of those controls. However, it’s not quite as bad as that because when you looked more closely, it was evident that many of these things were hazard management plans, it had a coal dust hazard management plan. Well, actually, buried within that hazard management plan were certain details that were really important, were genuinely critical. The whole plan wasn't critical. They needed a plan, but what was actually critical was a smaller subset.

Another example was its ventilation system. Well, plainly a ventilation is vital to maintain a concentration of methane below an explosion limit, however, only certain parts of that ventilation system are really critical. So the issue is, yes, you can have too many controls and it becomes unmanageable, but really if you focus on what's really critical you can normally, in my experience, get down to a critical few that you have to rigorously manage.

MR DOYLE: We might now move from a discussion of how one advances safety concepts within an organisation to the role of a regulator, and having particular regard to the challenges that face the establishment of a regulator and either a new application of an existing context or a new context entirely. The first thing I would suggest that the regulator needs to do is to clarify its role and the extent to which it's responsible for safety. What are the considerations or the ambiguities that arise in defining the role of the regulator?

MR WILKINSON: One of the difficulties is allied to the point I made earlier about so-called occupational health and safety incidents, slips, trips and sprains, so you get lots of feedback there, lots of incidents reported, and it's tempting from the regulatory perspective to go and investigate them, and there is a report I recently wrote for the New South Wales government that's been published that articulates the position that the regulator wasn't looking as stringently as those areas where there hadn't been an incident but, of course, just because there hadn't been an incident doesn't mean that everything is working okay. So this is back to this controls issue.

So the regulator has to be, in my view, in the high hazard industries has to be explicitly set up to say, "Look, the role here isn't just occupational health and safety, it's dealing with all those things." Whatever label you put on it, you might call it reliability, asset integrity, process safety, whatever is the right lingua franca for the particular industry, because the regulator has to appear further up the chain beyond a ladder that somebody may have fallen off, they have to look deeply into repeated software fails in a control system, they may be indicating a problem, so the regulator needs to check that the company managing these high hazard industries has actually got that under control.

So the question could arise, well, what is the regulator doing poking around looking at these points of detail in our systems that only have a marginal impact on safety, and this takes us back to the mental model of how incidents are caused, and they always generally involve these latent issues often associated with design or construction commissioning and active failures on the part of people trying to implement the system, so the regulator, I think, has to be set up explicitly to be clear what its role is.

MR DOYLE: How does the regulator define its role in relation to safety in an industry where it might be unachievable in an absolute sense?

MR WILKINSON: Well, everything has some risks, so that needs to be made clear to start with. In the high hazard industries there's generally a preference amongst regulators experienced in this area to have something approaching a safety case, a more licence based approach - I'll use the word "safety case" because it's the one I'm most familiar with and, for example, that's used in offshore oil and gas in the UK and in Australia, onshore major hazards, again UK and Australia, and in most of Europe via the Seveso Directive, but it is also used in the aviation world, satellites, air traffic control, railways and other environments, and in essence that puts the onus on the person creating the risk to demonstrate that they understand the hazards, the risks, the controls and how they are managed, and if they are articulated, the role of the regulator is usually to make a fundamental judgment on what's been articulated. Does this system, does this approach, does this case for safety stand up? Does it appear to have the capability to deliver the outcome you want, the goal you want from the regulator, and if it does when you get into the operational phase then the role of the regulator is twofold. One is to say well are they doing what they said they would do in this document but, secondly, also to check fundamentally is this still the right way of achieving that goal.

MR DOYLE: So what are the perceived advantages of approaching regulation of hazardous industries by the adoption of a safety case, as distinct from other approaches such as a prescriptive approach?

MR WILKINSON: Well, the safety case is normally associated with a so-called goal setting approach, and in the English speaking language that's most associated with the legal principle of reducing risks to as low as is reasonably practicable. The main advantage is that it allows technological evolution without having to keep changing the legislation, and the history of this comes from an organisation I worked for for 27 years, the United Kingdom's Health and Safety Executive, and Lord Robings was appointed to an inquiry to look at how safety was legislated in the UK, and made the obvious but predictable point that parliament never kept up with changes in industry, and we see that on a day-to-day basis with these so-called disruptive

technologies or different ways of ordering taxis, and the legislation follows thereafter.

So by saying, "Well, look, you're creating the risk. It's your responsibility to identify the risk, not ours, and you're the people best equipped to do it and to bear the cost and responsibility of that," that's the main advantage so it allows technological advance. An example in Australia is Australia will have the world's first ever floating liquified natural gas facility, the Shell's Prelude. No changes to the law are needed. Now, if that was going to go into the United States Gulf of Mexico, they would have to write a whole new set of prescriptive legislation to cover new technology, which they haven't done.

MR DOYLE: So what's been the resistance, if there has been resistance, to moving away from a prescriptive approach in some of those foreign regulators?

MR WILKINSON: Well, that's a difficult question for me to ask. I think there's some deep cultural issues, not to say problems in getting legislation through congress. I'm not really sure how far you want to go there.

MR DOYLE: It's not that far.

MR WILKINSON: No, I don't think I should. But it is a concept that's certainly more accepted in Anglophone type countries. There is a downside though of course. On the downside it's more complex for regulators to make a decision what does as low as is reasonably practicable mean? In practice - and there's excellent guidance on the definition of this on the UK Health and Safety Executive web site. I checked just before I came in, and it really doesn't mean much more than what's good practice. But if you've got something novel, yes we do good practice so far as we know, then we expect a greater application of those fundamental techniques that we've used, and always used, to deal with new things.

So we look for a deeper, more fundamental approach to assessing the hazards and risks, so it's more expensive, more time-consuming. However, it gives a - safety case gives a document which is more attuned - is attuned to the specific hazards and risks that can be used as the template for both the company and regulator to check. So the final advantage I've mentioned, it brings two pushing in the same direction rather than a regulator applying prescriptive rules. So it is often said that Occidentals Piper Alpha Platform largely metal prescripts it legislation but Lord Cullen said in the Public Health Piper Alpha Inquiry that that wasn't good enough to stop the disaster happening and 167 men lost their life in July 1988. So for high hazard, relatively high cost technologies, safety case type approaches are generally thought to be more effective.

MR DOYLE: And does the safety case approach, plainly it occurs at a design phase and the licensing phase of the regulatory regime but how does that translate in to the monitoring of ongoing safety procedures at a particular plant or facility?

MR WILKINSON: Well, a key part of any safety case is a – wasn't often called a formal safety assessment but I should just caution you, there is no one safety case approach. Every jurisdiction, country, industry has taken the principles I articulated at the start about hazard risk control and how they are managed, has taken those principles to apply them to the platforms, facilities, technology that they're dealing – sorry, I've forgotten the start of your question.

MR DOYLE: Just really asking about how the concept of a safety case, which tends to conjure up the idea of a static document - - -

MR WILKINSON: Yes.

MR DOYLE: - - - lives and breathes throughout the operation of a plant that - - -

MR WILKINSON: Yes.

MR DOYLE: - - - that might have been intended to have a 60-year, 80-year life?

MR WILKINSON: Well, there's two aspects to the safety case. One is often a staged approach to concept selection and design but as I say all these safety case regimes differ, so in some areas and technologies you would say here's our design safety case, or here's our concept and that allows interrogation by the regulator around the basic principles and concepts, particularly if it's something new. In the operational phase, because the safety case has to identify the hazard risk and controls, those controls are the things that we expect the company to implement and the regulator, in my view, a key role for the regulator is to go and check in practice, are they doing what they said they were doing. And maintaining those controls, actively maintaining those controls is the biggest challenge because of waxing and waning of profitability in the oil and gas industry. We see changes in personnel, company takeovers, there are all sorts of pressures but I can only speak from a – really can only speak from an oil and gas and large industry perspective.

MR DOYLE: And in monitoring compliance, what are the tools available to a regulator given that it's unlikely to have the capacity on a person to person basis to be monitoring compliance closely?

MR WILKINSON: Well, this really goes back to the role of the regulator, doesn't it? Where, what are your expectations of a regulator? We can't have 15 men on a team marking another 50 men trying to get the ball in the opposite direction. That's plainly not going to work; it would just lead to proxy. So that means we need to have a smaller group of people and it means they have to be selective. I would argue that the – what they are selective about – what they choose to do, they should be able to articulate that very clearly. The regulator should be able to say, from a transparency perspective, this is why we've chosen to look at these, but we can't look at everything. So that selection decision of what they look at, the frequency they look at, in my view should be made transparent and plainly. I think that should focus on the preventive measures but as you will have heard from earlier witnesses, things do go wrong and we have to have recovery measures in place. Some of that time must also be spent on looking as we might say in my world, the right hand side of the bow tie once the bad thing has happened, how you deal and manage that event. But it would have to be about the two and I personally would put more than 50 per cent of my activity as a regulator on the left hand side, on prevention. But we still have to look at something on the right hand side. But there's no one answer. There's no right or wrong answer to this, except my view is that mostly prevention but you also have to deal with the mitigation side.

MR DOYLE: Is there any role in these very hazardous industries for private sector involvement in monitoring or certification of operation or design of plants?

MR WILKINSON: That's an interesting question because sometimes there is a connotation of private sector bad because how can they be independent, but it's hasn't been our experience, if I talk about the North Sea or upstream offshore petroleum in Australia, and the reason for that goes back several hundred years to the ship classification societies that have provided pretty effective service typically in the area of technical efficacy of the ship's hull, the deck plates, are the engines working and are their bilge systems working and so on, so we tend to focus on the engineering issues, but in the North Sea the ship classification societies prior to Piper had a significant role, and after Piper the new regime that we've got in place explicitly required third party - or it could be second party, but normally third party verification of what were called safety critical elements.

Safety critical elements is no more than a technical word for critical control, so I use the common language "critical controls", technical language in the legislation is safety critical elements. So the company is forced to spend money on generally third party company, some are offshoots of the classification societies, but that need not be the case, to provide very well-known and established service and provide those reports to the company.

One of the things the regulator can do is to go and audit those third parties, are they doing the job properly, and when they visit facilities or go in the offices will show what the third parties are finding, because there's nothing to stop the regulator going in to check, "Is that correct?" So if the regulator finds things that aren't being found by the third party, well, that would lead to action presumably in relation to both parties.

MR DOYLE: You mentioned a moment ago "second party" regulation. Does that have any prevalence in the hazardous industries context?

MR WILKINSON: In the North Sea, the second party was permissible, they just had to demonstrate there was sufficient independence, so I know one very large global company used its well engineering team in Houston to come to the North Sea and there was sufficient separation of those management chains - obviously they all come together at the top in The Hague or London or both, but there was judged sufficient separation to permit that, however, I believe - I haven't checked prior to this hearing - that Shell have moved back to a third party, but in principle it could work.

MR DOYLE: All right. We might move now to some of the particular challenges for regulators in new industries and industries where there might be a small number of participants. Firstly, in establishing a new regulator, how does one go about populating the regulator with the relevant expertise and what are the key learnings from your experience in this area?

MR WILKINSON: Well, I've had an unusual experience of leading a group of people that developed a brand new regulator from scratch with no bums on seats before we started, we had to go and find all those people, and there are a number of factors here. I think there's some things that I won't dwell on, but it's obvious you have to have the technical skills relevant to the entity that's being regulated, so if we're regulating shipping it's inevitable we're going to have some marine engineers, naval architects and ship's masters.

However, when we set up offshore safety division after Piper in some of the teams we consciously had a more eclectic approach to recruitment. So, for example, we hired a former fast jet test observer who was an aeronautical engineer, but aeronautical engineers know a lot about light but very strong structures, known as wings. Well, these are very relevant to offshore petroleum structures. Our believe was that we needed good quality people, able to make decisions, sometimes without much support from a fundamental basis and there was no one right background. So yes, we needed all those technical expertise, so in nuclear it’s obvious what they would be, but I would strongly urge that if somebody was approaching that task and if they asked me for advice, I said yes do what you think you need to do in terms of mechanical engineers, nuclear physicists, radiation experts of course. You must have that,

however don't make yourself vulnerable to a common mode failure by not having some people who can approach these problems from a slightly different angle. And from my perspective, a large proportion of the operational incidents that I've been involved with, have very significant human organisational factors. So we've had an example where the Royal Australian Navy had some ships that weren't fit to go to sea when people thought they were, after some – what was described as hollowing out of the engineering function. So it's not – and that is a failure in leadership and management of an organisation.

People with other sorts of skills can detect problems going on in an organisation, looked at from a different perspective and the most obvious one is the human organisational factors, discipline of human factors well known to the military aviation and some other areas, less well applied in manufacturing industry, or say coalmine, partially applied in oil and gas. So there's a range of skills beyond the particular engineering skills of the industry needed.

MR DOYLE: All right. Well, a moment ago you mentioned that in the context of a goal setting based regime, rather than a prescriptive regime, that the concept of making risks as low as reasonably practicable, often devolves in to an analysis of comparison with best practice. How does a regulator judge best practice in a domestic industry that might have one or two participants?

MR WILKINSON: So I think the point you're making is a good one. And that is that regulation isn't as simple as taking a ruler to the height of the table, if it's goal setting, it's prescriptive law and this table has to be a metre, we can take a ruler and measure that. It's less easy to make those complex judgments in a goal-setting environment, particularly if you have new technology. How do you do it if you haven't seen that technology before? So that suggests strongly to me, that regulation isn't just absolute, it's also a comparative task. We have to look and be able to form a professional judgment about what good looks like. What is accepted good practice? And if you haven't got that experience locally, well you have to then get it another way and the two main ways that are used, so in offshore oil and gas we have the International Regulators Forum and regulators between a number of nations with offshore petroleum meet once or twice a year to exchange good and bad practice, lessons learnt and so on. And the other way is to explicitly have peer review of facilities. And that peer review can take place at two levels. One peer review of regulators and I believe there's an existing International Atomic Energy Authority programme for that. But also, I would suggest that – I have no first hand knowledge of what I am going to say next, but I believe it to be true, the American system involves a peer review between facilities, so if there are similar facilities of (indistinct) Australian facility, well I would suggest arrangements should be entered in to to try and facilitate a similar type of peer review with comparable facilities wherever they exist.

MR DOYLE: Now the answer to this question may involve some similar themes but it's in the nature of a low probability high consequence industry that one doesn't have a large data set to work from in terms of judging the success of a regulator and equally a failure may not necessarily be the consequence of a failing on the part of the regulator. So how do regulators in these industries go about judging their own performance? And if they don't judge them, who does?

MR WILKINSON: In a sense, that's a difficult question for me to answer because – to ask me, because I've just had to do that very task in relation to NOPSEMA and I think the operational review of NOPSEMA's involved three people, of which I was one, was tabled in the senate a month or so ago. There isn't an easy measure because the absence of an incident isn't the same as saying that neither the company nor the regulator are doing everything well. It might be chance, particularly with very low probability events, but what about the converse. If there is a serious incident does that mean the regulator's at fault. But the regulator isn't the person with their hands on the levers, press the buttons. So it's a more subtle and complex relationship. And I think it falls in to the area where there can be some hard data, so some of the hard data that we looked at in the review of NOPSEMA, the operational review, were losses of containment of hydrocarbons because if you keep the hydrocarbons, the oil and gas on the facility, in the pipe, you can't – difficult to have a fire or explosion. So we can make some judgment about data but again, this is complex. Does an increase in losses of containment mean that things are getting worse, or does it mean that people are reporting more and they're feeling comfortable?

So this is all quite a complex area. So I'm sorry to say, there isn't an easy black and white answer. I think the only way is to inquire in to those sorts of precursor type data, if it's available and you have to find that. Secondly, it's a qualitative one, you have to go and talk to the people doing the regulating, what they go about? Look for evidence of what they do? What do they look at? Are they looking at critical controls? So my report in to mining regulation in Australia, I found it difficult to find evidence that they're looking at critical controls, or how can they be offering advice, feeding back to industry as a whole, if they haven't been looking at those critical controls? So that's an area. And finally, there's a range of stakeholders. You have to take what stakeholders say with a pinch of salt of course because there are always personalities involved in here and the company that feels raked over, might have been raked over justifiably and its standards and processes and systems might've been called in to question and they might feel aggrieved about it. Doesn't mean the regulator's wrong.

So it's not an easy issue. But there is long history of doing that and published

models of doing it. As I say, there is some hard data. Have to treat it carefully. You have to go and talk to people and you make some value judgments. It's not quite – I hesitate to say this, because it's a difficult notion to persuade other people on, but these are quite expert judgments in general. Not easy to make.

MR DOYLE: Just one final topic Mr Wilkinson, we've heard in earlier evidence the concern that is constantly to be guarded against of an alignment of interest between industry and the regulator and the dangers of over familiarity - - -

MR WILKINSON: Mm.

MR DOYLE: - - - but from your experience of the front line of regulation - - -

MR WILKINSON: Yes.

MR DOYLE: - - - is there a sense in which it's necessary to strike a balance of where familiarity can breed disclosure?

MR WILKINSON: Well, I could reframe what you said completely and say there are dangers in unfamiliarity. So a personal test, that I applied with the explicit agreement of my most senior manager, when I was a regulator in these southern north sea for a time, was that if I went offshore with my – one of my staff who have accountability for those companies and those facilities and he didn't know the offshore installation manager on first name terms, it would cause me to ask why he didn't know. How often was he going? And more, I want him to know the first name teams of the key supervisors because he has to sit down with them and find out what they're doing. You cannot go in with a clipboard in front of them and writing down things because the only way you can find out what's going on, is by inferring what's going on from talking to people. Because you cannot see the molecules going down the pipe. You can't see the inside of the pipes, you have to infer what's going on on the platform from a quite subtle mix of hard evidence produced in reports of non-destructive testing of piping, dosing rates for anti-corrosion materials but crucially, what people tell you is happening and you need to find that out at all levels.

So you have to get close to people to find out what's going on. You have to be trusted because they don't tell you things if you don't. So your question is how do we guard against over familiarity and being captured, well a couple of things. One is practice with rotating people, leaving them long enough to get to know them and be productive but you need to change, different people have different views inevitably on both sides, regulated and the regulator. There are some processes you can put in. I mentioned peer review in a different context but peer review is an important tool that can be used. I mean genuine peer review, peer, not top down. But you can also have top down views. Why did

you take that judgment? Why did you make that judgment on this day in relation to that issue? And you should inquire in to those judgments on both sides. Why did you take action and say that wasn't very good? And why did you not take action on this, and why did you think that was good? And those sorts of post facto reviews are crucial part of maintaining credibility with the regulator and there's one final that some regulators have developed a quite sophisticated tool which is referred to as an enforcement management model. NOPSEMA in the past have used this. I can't recall if it's currently used. It's also used in the UK, and in essence, again, used after the event but it's a tool can say look this is the situation you found and this is what you did about it and it has a series of – it's a decision tree. A set of gates that helps to calibrate decision taking. Called the enforcement management model. It's generally used afterwards because it can never quite deal with the subtleties of individual decisions on individual issues. It would be too complex to make it a perfect decision tree, but it's very useful about honing decision taking skills, how people take decisions, why they take particular decisions and plays a role in having a more homogeneous, a more consistent approach from a regulator. So they do have to get close to people because they won't find out stuff if they don't. But you have to manage that and the knowledge that people can get too close.

MR DOYLE: Thank you.

COMMISSIONER: Mr Wilkinson, thank you very much - - -

MR WILKINSON: Thank you.

COMMISSIONER: - - - for your very practical evidence.

MR WILKINSON: Thank you.

COMMISSIONER: We will now adjourn until tomorrow morning when we will take on topic 10. Thank you very much.

MATTER ADJOURNED AT 4.48 PM UNTIL
THURSDAY, 22 OCTOBER 2015