BNL--31908

DE83 002219

NUCLEAR REGULATION AND SAFETY

by

Joseph M. Hendrie
Department of Nuclear Energy
Brookhaven National Laboratory
Upton, New York 11973

BANQUET SPEECH

International Meeting on Thermal Nuclear Reactor Safety
August 29 - September 2, 1982
Americana-Congress Hotel, Chicago, Illinois
Sponsored by the American Nuclear Society and co-sponsored by the
European Nuclear Society, the Canadian Nuclear Society,
and the Japan Atomic Energy Society,
in cooperation with the U. S. Nuclear Regulatory Commission
and the International Atomic Energy Agency

Date of Speech: September 1, 1982

NUCLEAR REGULATION AND SAFETY*

Joseph M. Hendrie
Brookhaven National Laboratory
Upton, New York 11973

Good evening. It is a pleasure and an honor to be with you at this International Meeting on Thermal Nuclear Reactor Safety and to have the opportunity to speak to you this evening.

Let us enhance our after-dinner enjoyment by joining in some pleasant thoughts about nuclear regulation and safety. I suspect that some of you don't think there are any pleasant thoughts to be had about nuclear regulation. That is probably because you do not have as much experience as a regulator as I do. I am sure that all the regulators present would join me in saying that regulation can really be quite enjoyable, if it is done in the right way.

Let us shape our thoughts about nuclear regulation and safety into the form of speculations about the advice we would give to an unnamed and hypothetical country that is in the process of introducing a nuclear power industry and setting up a regulatory system. We can divide our efforts as follows: I am standing and have a microphone, so I will speculate. You are sitting down and do not have microphones. So you can listen and reflect. Napping is permitted. However, it must be done quietly and is limited to consenting adults.

Our hypothetical country has electric utilities anxious to have nuclear power plants. It has a recently-enacted national policy in favor of the use of nuclear power. Nuclear plant designers are setting to work in various industrial firms and the government has collected some engineers and has designated

---

*This work carried out under the auspices of the U. S. Department of Energy.

them as regulators. Let us provide all of these groups some guidance, based on our great experience in these matters.

First of all, let us outline the general responsibilities of these parties so that they will know what to do. The utilities are to operate the plants and are to be responsible for them in all respects. The designers are to produce designs of plants that will generate electricity economically, reliably, and safely. The regulators are to be responsible for establishing rules and standards for plant design and operation. In our hypothetical country, however, we will suggest that their mandate be extended to cover not only safety, but also the need for economical and reliable electricity, because it is the announced national policy to have the benefits of nuclear power.

We want the regulators of our hypothetical country to have some sense of responsibility for economical and reliable electricity production, as well as for safety, because we want the regulators' goals to be consistent in all respects with the national policy. We want a unity and coherence of purpose between plant design for electricity production and plant design for safety. We want the regulators to have an overall perspective of the purpose and function of the plants so that they can fully understand the effects that might be produced by regulatory requirements.

We want to avoid the possibility that, in a few years, as more details of safety issues come to attention, successive layers of regulatory requirements to cure these problems will be laid upon the plants without consideration of the possible interactions and the effects on overall plant function and safety level. We want to create from the beginning a certain tension within the regulatory body between the requirements of safety and the requirements of reliable and economical electricity production so that each factor may be fairly

balanced in internal regulatory discussions. We have some reason to suspect, from experience elsewhere, that a regulatory authority told to worry only about safety and to take no position and have no concern about whether the plants produce reliable and economical electricity, may so encumber the plants with incoherent arrays of safety measures that the national goals of our hypothetical country may not be realized.

We will have the utilities, the plant designers, and the regulators work closely together to develop the system design rules and the regulations and standards under which they will all work. The regulators will have the lead in developing these guiding documents, but the three groups will have to work closely together to understand one another's problems and to achieve a set of system design rules and regulations and standards that are workable and that will lead to the national goal of economical, reliable and safe nuclear power. Since that is the common aim of all three groups and is the expressed will of our hypothetical country, there will be no carping allowed about conflicts of interest.

The utilities, the plant designers, and the regulators of our hypothetical country are to understand that they can achieve their joint goals only with plant designs and modes of operation in which the design for reliable electricity production is fully integrated with the safety design in a coherent and economical way. All three groups must understand that they will come at the details of design and operation with some differences in emphasis, but they must resolve to work these differences out in technical discussions in which each group's views are given careful consideration and equal weight. Resolutions of differences are to be by consensus. When the utilities, the plant designers, and the regulators have worked out what they regard as a satisfactory

plant design and proposed mode of operation, we shall have them take their case before a committee of distinguished senior engineers and scientists. In public session, the plant designs and modes of operation will be explained to the senior committee and the senior committee will probe to satisfy itself that the utilities, plant designers and regulators have all done a good job and that the proposed design and method of operation fully meet the national objective of economical, reliable and safe electricity production. The discussions before the senior committee will be informal and technical in nature.

When the senior committee is satisfied that all is in order, it will so advise the appropriate government minister and a license to build the plant will be issued. It will carry with it permission to operate the plant when construction is complete, provided all three parties, the utility, the plant designers and the regulators, certify to the government minister that the construction has been carried out in full accordance with the designs and plans at the initial review stage.

We see no need for formal hearings in our hypothetical country, and so there will be none. Each utility is to be limited to one lawyer engaged in nuclear administrative law practice at any given time. The plant design groups may also each have one lawyer. The regulatory staff may have six lawyers, but only three desks will be provided.

I told you these would be pleasant thoughts about nuclear regulation.

Having framed the responsibilities of the parties and the general outline of the relations between them and of the regulatory process in our hypothetical country, let us go on to a subject we are all much interested in and offer some guidance on safety. I am sure we could offer all kinds of detailed advice about safety matters, but our time is limited this evening. Besides, we can

help fill in the assorted details on the consulting trips we hope to make to the hypothetical country.

For the present, let us stick to the essentials. The essentials of power reactor safety may be divided, like the ancient kingdom of Gaul, into three parts. So we advise our hypothetical friends and prospective clients that for safety, they must concentrate first on being able to shut down the nuclear reaction at any time, second on keeping the core covered with water, and third on being able to transfer the afterheat out of the containment.

These safety principles constitute the most generally applicable and important criteria for safety design, so we shall call them General Design Criteria and advise that they be placed in the First Appendix to the Safety Regulations (Appendix A). In fact, these three safety principles -- shut it down, keep it covered, take out the afterheat -- cover so much of reactor safety that we might well advise our hypothetical country to stop the regulations right there. However, we do not want our friends to feel inferior because their regulations are so much shorter and to the point than everybody else's, so we may as well agree at the beginning that there will have to be other regulations and criteria for design.

One of these ought to be "Thou shalt have a containment". Of course, if our friends execute the three essential safety principles with vigor and care, they will never need a containment. Nevertheless, a containment building is useful for keeping the rain off the reactor and, more to the point, a containment is essential protection in any situation where things do not work as planned and radioactive materials escape from the reactor. So let us have containments.

There will also have to be some provisions for Emergency Plans. Each plant will be required to have an emergency plan for on-site activities. There will also have to be an off-site emergency plan for each nuclear station. A suitably modified form of the American practice can be used for this purpose. Let us have the off-site emergency plan regulations require an annual notice to people in the region of a plant, saying that the utility regrets to inform them that in the event of an emergency, plant staff will be unable to attend social gatherings and community events. Since prompt notification is essential in an emergency, the utility will maintain a horse and rider at the ready at each plant. If an emergency requires notification of the public, the rider will be dispatched on orders of the county sheriff. The rider will draw the attention of the citizenry by ringing a bell as he rides. The horse will be a Quality Group A component and full quality assurance documentation will be maintained on all horses.

Some attention will have to be given to safety design features to deal with extreme natural phenomena such as earthquakes. Seismic design criteria become rather too detailed for us to discuss here this evening, but there are a couple of points we ought to see included in their seismic design regulations. The first of these is that no matter what the computer calculations say, the seismic restraint system for a piping run may not weigh more than the pipe and associated valves and fittings. The second is that any seismic restraint required after the design has reached the 100% stage for the first time shall be qualified by placing the person who requires it on a ,eismic test table and shaking him or her according to a Regulatory Guide 1.60 spectrum referenced to 0.2g--in three dimensions.

Well, there are assorted other things we might talk about, but let us go back to those three essential principles of reactor safety -- shut it down, keep it covered, take out the afterheat -- and elaborate a little bit on them.

Shutting down the nuclear reaction is probably the most reliable function of current water reactor design. The control rod systems in these reactors are very reliable. So much so, in fact, that we are unable to determine just how reliable they really are because there is a dearth of failure data. Nevertheless, some people continue to have doubts and have raised the specter of the control rod system failing to function when needed during some anticipated plant transient.

There is also the matter of the stuck rod criterion. This requires that the rest of the control rods be capable of shutting down the nuclear reaction even if one control rod is stuck in the fully withdrawn position. That criterion made a lot of sense in the days when reactors had eight control rods. But it is not so clear that it makes any sense in a reactor with 150 control rods and a core volume so large that sub-elements are capable of going critical while other sub-elements are shut down. Let us advise our hypothetical friends to consider very seriously putting in a fast-acting liquid poison system. If they build pressurized water reactors, the poison system can dump to the reactor coolant pump discharges. If they build boilers, they will want recirculation pump trips and will need to inject the poison directly to the core, probably through the core spray system. Since they are starting from scratch, although drawing upon our collective experience, there is a fair chance they will save enough by not having to argue about ATWS to pay for the installation of the fast-acting poison systems.

The second essential safety function, keeping the core covered with water, involves knowing where the water level is in the reactor vessel, as well as the ability to pump more water in when it is needed. One would think that a technologically inclined civilization capable of landing people on the moon would have no great problem in determining how much hot water there is in a large pot. That does not seem to be the case, however, or at least the practice among reactor designers does not reflect any such capability.

To be sure, the boiling water reactors have lots of water level measurement instruments. These are generally arranged to have different instrument zero points, presumably to keep the operators on their toes, and are subject to an assortment of error-causing phenomena. These range from temperature differences in the reference and variable legs and dynamic effects from the variable fluid flow velocities in different parts of the vessel, to problems in keeping the reference legs filled with water and even to having the reference legs flash to steam if the dry well temperature gets high and an attempt is made to reduce system pressure.

Nevertheless, the boilers are in good shape on water level measurement compared to pressurized water reactors, where the designers have provided water level indication only over a limited range of the pressurizer and leave us with the instruction that if we are in doubt about that, we should just pump water into the vessel until it squirts out of the top. The frailty of that approach in off-normal circumstances was demonstrated a few years ago in Pennsylvania.

The regulatory authorities are now demanding better water level indications and various efforts are underway to accomplish that. I think backfitting an improved water level measurement system to existing designs is rather harder than designing to include such improved systems in the beginning.

We ought to advise our friends in the hypothetical country to save themselves some trouble and plan on improved water level instruments from the start.

Adding water to the reactor to keep the core covered, once there is a good way of knowing when more water is needed, is a matter of having an adequate array of pumps and water sources for high and low pressure injection, with appropriate redundancy, separation, independence of supporting systems, and reliable emergency power sources. These matters are reasonably well done in current designs, so we can advise our hypotnetical friends to base their safety injection systems on present designs with attention to a few points for possible improvements.

A substantial payoff would come from improving the reliability of emergency power sources. The diesel generator sets generally used for this purpose are lovely machines once they are up and running at load, but they can be very crotchety about starting. Improvements in emergency power reliability, by whatever means, would improve the safety level all along the line.

On the plumbing side, the PWR designers in our hypothetical country ought to look at upper plenum injection and at ways to move some of the safety injection points from the cold legs down into the lower plenum of the vessel. Routing the low-pressure, high-volume safety injection into the lower plenum maximizes vessel inventory, condenses steam in the right place, and saves arguing about how much injection water is lost out the break in the event of a medium to large pipe break situation. Routing the high pressure injection into the upper plenum provides a diversity of emergency core cooling that seems very attractive.

The boilers, I should note, already are in approximately this configuration. The boilers also have the splendid feature that if there is trouble

with high pressure safety injection, the reactor can be blown down to the suppression pool. The core then simmers along at rather low pressure and any sort of portable pump that can be aligned to the vessel will do to keep the core covered.

The third great essential of reactor safety is being able to transfer the afterheat out of the containment and on to the ultimate heat sink. The three safety essentials are like the legs of a three-legged stool -- it really cannot be said that one is more important than another. They are all necessary for safety. But this third one, transferring the afterheat out of the containment in all circumstances, deserves special attention because it is vital for containment integrity. If something goes wrong with efforts to keep the core covered, there can be core damage or even core melting, but no significant offsite consequences, provided the containment heat removal systems work.

Getting the afterheat out of the reactor vessel and then out of the containment involves all sorts of pumps and valves and pipes and heat exchangers. The pumps and valves need motive power, cooling water for bearings, and perhaps lubricating oil as well as control circuits. So there are all sorts of supporting subsystems that have to function in order for the afterheat removal to work, and that complication offers many opportunities for things to go wrong. That doesn't mean that afterheat removal cannot be made highly reliable, but does suggest very careful attention to redundancy, diversity, separation, independence, and all of those good things, as well as to having a really good emergency power system.

We will forward that general caution to our friends of the hypothetical country and accompany it with one more comment about afterheat removal systems. Getting the heat out of a pressurized water reactor, once the main feedwater

system has tripped, as is its custom, depends on the auxiliary feedwater system. If the auxiliary feedwater system will not function for some reason, there is no place to go but to the draconian procedure of feed and bleed. A full pressure-rated residual heat removal system, sized to take the afterheat at the end of steam generator secondary water boiloff, would provide a place to go. It could be instrumented to come on automatically after a reactor trip and on low steam generator water level, so the operators would only have to monitor its progress as they attend to other things.

An alternative, we can tell our hypothetical friends, would be a dedicated, safety-grade secondary water supply to the steam generators. Either way, the auxiliary feedwater system could then go back to being what it ought to be, a steam plant system used for low feedwater flow conditions and not something that has to be gussied up to perform a vital safety function.

Well, I think we have now gotten our hypothetical country well started on the proper path to a successful nuclear industry. If they take our advice, their nuclear enterprise ought to be not only a successful one, but also one conducted in a reasonable and amiable climate. It should be quite a pleasant place to work.

I have been preparing to send them my resumé. If the same thought has occurred to any of you, let me know and I will see what can be done. I will not, however, reveal the address of the hypothetical country. One has to keep some trade secrets, you know.