CONF-860906--20

CONF-860906--20

DE87 004977

NEW PERSPECTIVES ON REACTOR SAFETY*

R. Avery
Argonne National Laboratory
9700 South Cass Avenue
Argonne, IL 60439

Over the past few years a number of changes and new perspectives have come about in our approach to reactor safety. These changes have occured over a period of time extending from as long ago as 1975, when WASH-1400 came out representing the first major application of probablistic risk analysis (PRA) to U.S. reactor plants. The period of change has extended from that time to the present and includes new areas of focus such as safety goals, source term studies, and severe accident policy statement and approaches, including the IDCOR Program. It has also included a greatly increased interest in inherent safety. We should also include in the factors that have strongly impacted our thinking on reactor safety the key events of TMI and, now in the past several months, the Chernobyl nuclear accident. Most of all we should include the growing appreciation and realization of the very large impact of all aspects of safety considerations to reactor economics.

I wish to say something about all of the above items. Clearly, I cannot say much since each can be the subject of full conferences and more. In the few remarks that I will make, I will not address the enormous technical progress that has been made in each of the areas, but rather will focus on the perspective provided. Before proceeding further, however, one should emphasize the following two points. A dominant view has been held and continues to be held, by essentially all of those in the reactor community, that reactors pose very little risk to the public; far less than the risk one is normally exposed to and less than that posed by alternate ways of producing electricity. The record is extraordinarily good, certainly so in the United States and the Western World, and until Chernobyl one could have made the statement worldwide. It is still too early to put the Chernobyl event into any appropriate perspective. In addition to the empirical evidence, the view that reactors pose low risk is also based on an ever increasing body of research and analysis that has led to and supports this conclusion. But the second point I wish to emphasize is the other side of the coin and an aspect that we cannot ignore. And that is that directly or indirectly, safety considerations, and perhaps even more importantly, perceptions of safety held by the public, are in many ways related to most of the ills that have come to the reactor enterprise, at least in the United States.

*Work supported by the U.S. Department of Energy under Contract W-31-109-Eng-38.

DISCLAIMER

Safety Implications to Economics

The direct relationship of safety to reactor economics includes such obvious items as the direct cost of the specific safety features that have been added. Also included are delays to plant construction due to debates over safety and licensing questions or any backtracking during construction due to changing requirements. The direct aspects such as the above examples are only a part of the larger indirect impact of safety concerns to the health of the reactor enterprise. Most of the opposition to nuclear power is based on safety concerns by those opposed to the technology. This in turn leads to all of the uncertainties and delays in construction, and even uncertainty as to ultimate operation, that is inherent to the process when the technology has sharply split public acceptance and also sharply split acceptance in the government and the courts. This leads to all of the resultant adverse impacts on the economics of the plant and in its extreme form leads to the halt of all new orders. Therefore, a good case can be made, perhaps an arguable case, that essentially most of the ills of the reactor business have strong connections to safety, real or perceived. The essential question is whether this can be cured without adverse impacts on either economics or safety.

For many of the people working in the business now, a strong belief exists, perhaps as yet unproven, that optimum safety can in fact be built into a plant with no adverse economic impacts. This conclusion, if true, also depends on enlightened regulation, and of course, most people believe that we do not have this now. Although regulatory reform, whatever that is to be, may be at the heart of the question, this growing consideration of safety issues in the context of implications to economics is perhaps the major change that has evolved over the last several years.

Probablistic Risk Analysis (PRA)

The past decade has seen a great increase in the application of probablistic risk analysis techniques in safety considerations. The limitations, as well as the useful area of applications of PRA, are better understood now than when first applied. A general view is that PRA is most effective in allowing analysis of the interactions of the various components of the full system. PRA is valuable in the study of how failures in some part of the system may affect other parts and also what alternate approaches are optimum in circumventing potential difficulties. PRA is perhaps least valuable in terms of giving a reliable bottom line number as to integrated risk. It is often this latter use that receives the most focus in public interpretation of PRA results. Real questions therefore remain in the accuracy of bottom line PRA results and how to best treat the uncertainty that is inherent to the process.

Many clear benefits have come from the application of PRA techniques. A much greater appreciation exists of the key role of reliability to reactor safety. The key importance to reactor safety of some specific areas such as, for example, decay heat removal reliability have been better appreciated as a result of PRA. Also one has achieved a clearer realization that some things done in the name of safety may, in fact, reduce safety. It is thus clear that PRA has a crucial role in decision making in safety and system analysis. It is less clear how useful it is in giving a bottom line integrated risk value.

In my view, a key point about PRA is that it is the right language to think about reactor safety. Instead of making abstract generalizations, we are referring to the real features of real reactors and talking about realistic potential accidents or abnormalities as opposed to arbitrary assumptions. The fact is also true that some of the numbers entering into the PRA may have large uncertainties. It is also obvious that the PRA approach is not guaranteed to give completeness. Some aspects of design features, design characteristics, design interactions, and possible accident scenarios may be overlooked. But this in no way changes the key point that it is the right language to think about and analyze reactor safety.

Safety Goals

NRC published in 1983 a trial safety goal statement. This statement was to go through a period of several years on a trial basis. Very recently, the Commission has approved a new version of the safety goal policy statement. The subject has, of course, drawn much discussion and debate over the past few years. The essential feature of the safety goal statement is that both individual risk and societal risk due to nuclear power and including both prompt and latent fatality risk shall be very small, less than 1/10 of 1%, compared to other risks to which one is normally subjected. The statement also includes a provision that the risks from nuclear power shall be smaller than that associated with alternate means of producing electricity. The original trial safety goal statement also included several additional numerical criteria which were characterized as having lesser importance. Core disruption accidents should have a probability of less than 10^{-4} per reactor year. In cost benefit considerations to be used in deciding on design features aimed at reducing accident related exposure to the public, a value of $1000 per man rem averted is to be used. Since the original proposed statement there has been considerable debate on whether additional criteria should be inserted, for example, related to containment performance. Also the question of whether the cost benefit studies should also include averted on-site costs. All of these questions are still subjects of considerable difference of view, but the latest safety goal policy statement does not include any of the auxiliary conditions. The latest statement states as a general performance guideline that the probability of a large release in an accident be less than 10^{-6} per reactor year.

The original policy goal statement had as objectives for the statement that it was hoped that it would make clearer to the public the basis for regulatory safety decisions, also that it would make more rational such decisions. It is not at all clear that there is agreement that any of these objectives have been met or can be met by any safety goal that has yet been suggested. The value of a safety goal statement is still one that draws considerable discussion. Many people believe that no useful purpose is served by such a safety goal particularly since the nuclear industry is the only one that has articulated such a goal. What role, if any, the safety goal statement will play in licensing is not clear, but it would seem that in its present qualitative form that is is unlikely to play any significant role.

Severe Accident Considerations

Until the TMI accident there had not been much work on LWR severe accident phenomenology. It was the generally accepted position, both by the industry and by the NRC, that the probability of a severe accident, i.e., substantial core disruption or meltdown, was sufficiently low that no significant analysis of the event was merited. The connotation was left, sometimes explicitly stated, that although the probability was extraordinarily small, the consequences would indeed be horrendous. The results of the WASH-1400 report provided a quite different perspective. They showed a very low risk, but coming about from both higher probabilities and much lower consequences than previously implied. This WASH-1400 perspective and to a much larger extent, the TMI accident provided the impetus for an increased focus on severe accidents in light water reactors. It is of interest to note that the absence of work on severe accidents for light water reactors until rather recently was in rather sharp contrast to the situation relative to the fast breeder reactor where there had been over the years much severe accident work. In order to prepare for an industry position relative to likely severe accident rulemaking on light water reactors, the Industry Degraded Core Program (IDCOR) was initiated several years ago and still continues, although its work is essentially done.

The area of severe accidents continues to draw much debate with some, perhaps most, of the reactor community believing that substantial effort in this area is not necessary. This dichotomy of view is often put into a context of the relative priority of effort to be put on accident prevention as opposed to accident mitigation. In my view, much of the discussion misses the point of the importance of consideration of severe accidents. The work usually has as its objective not only the determination of the consequence of the accident, but also to find out under specific scenarios, if and how one gets into the accident and the designs or operational procedures that might prevent, interdict, or mitigate the event. The results of the severe accident studies can have important effects on the design of the system which in turn can have large impacts both on safety and economics. A very large amount of information and understanding has been obtained on LWR severe accidents from the recent studies, primarily by NRC, IDCOR, and EPRI.

As a result of severe accident policy considerations over the last few years and largely driven by the TMI accident, there has been a specific requirement relative to hydrogen control in LWR plants. NRC has also prepared a general severe accident policy statement. The essential feature of this policy statement is the view that existing plants are sufficently safe from severe accident risks that no major design retrofits are required in this area. The two major considerations and the ones that had largely triggered the IDCOR Program, had been relative to the suggestions of filtered vented containment and for core catchers. The policy statement views these or any other major retrofits as not being required for current plants. If any special requirements are identified for any plants because of some specific features, these will be considered on a case-by-case basis. The major focus of the severe accident policy statement relates to its view that primary consideration should focus on future plants, but with as yet undefined requirements relative to severe accidents.

Source Term

The source term, defined as the radioactivity inventory that would be released in the event of an accident, has been the focus of much work in the past few years. The greatly increased interest in the source term was driven by the observation at TMI, as well as other reactor events in which fission products were released from the fuel, that only a small fraction of biologically important fission products actually were released to the environment. The source term is of primary significance in relation to siting considerations as well as to emergency planning. Since no new reactor plants are being sited now, the only near term significant implications are to emergency planning. The existing source term regulation is based on the Windscale accident, and it is an important factor that no water was present in the gas cooled Windscale reactor. The existing source term regulations assume that all of the noble fission gases escape to the environment as well as 50% of the halogens, in particular I^{131}, and 1% of the nonvolatile fission products. It has been a view of many that for LWR's the release numbers are unrealistically high. In contrast to the current source term regulations, only about one part in one million of the I^{131} in the TMI accident found its way to the environment. No change has yet been made to the source term used in regulation, and it is anybody's guess if and when a charge will be made, even though a strong case can be made that the data supports a lower value.

Even though no change has been made in the regulatory sense, I believe that an extremely important philosphical change has already occurred in consideration of the source term. It is important to note that we no longer talk about a single arbitrary source term, independent of reactor and accident specifics, but rather we consider a spectrum of source terms as they are affected by the reactor under consideration and the accident scenario being analyzed. The crucial philosphical change in approach has already been accomplished. Now we are only arguing about the numbers.

The major efforts on reassessing the source term over the past few years, largely by NRC, IDCOR, and EPRI, generally confirm the view that the amount of fission products released from containment in hypothesized accidents are much lower than assumed in the regulations. There are several uncertainties in the source term still remaining. One uncertainty relates to the possible impacts of the direct heating of the containment atmosphere and the resulting possible challenge to the integrity of the containment should much finely dispersed core debris be spewed out in a failure of the primary vessel under high pressure. Another uncertainty relates to the corium concrete interaction. In this scenario the key issue is whether gas sparging from corium concrete interaction products might be sufficient to volatilize some fission products like strontium and lanthanum that have generally been considered to not be sufficiently volatile to be important fission products in the source term. Finally, of course, we must consider the possible impact of the Chernobyl nuclear accident. Until the accident is more fully understood including its fission product releases, it would appear unlikely that much will be done about source term modifications. The degree of relevence of Chernobyl to U.S. reactors is, of course, an issue that must be put into full perspective.

Inherent Safety

It is appropriate to start by defining what is meant by inherent safety. Several quite different definitions are in use. The definition I prefer does not aim at being precise in the distinction between inherent safety and other kinds of safety, but rather aims at giving the broad characteristics associated with inherent safety. Inherent safety can generally be characterized as passive safety as opposed to active safety; passive in the sense of not requiring external power. Another characteristic is that it is inherent safety as opposed to engineered safety or safety depending on add-on-devices. I would also prefer the terminology of defining the reactor as having inherent safety features or characteristics as opposed to defining the reactor to be inherently safe. Inherent safety features and characteristics would depend on, for example, thermal expansion and other thermal feedback coefficients, natural circulation, gravity, etc., as opposed to, again for example, power driven valves or control rods. Clearly any reactor will have a mixture of many characteristics related to safety, some of which will be inherent, others engineered, some passive, and others active. Finally, I do not use the term inherent safety to have a connotation necessarily of being absolutely safe. No reactor is absolutely safe. Given enough imagination one can always imagine scenarios where the reactor gets into trouble. The issue is, in a probablistic sense, of whether the probabilities and consequences are sufficiently low. However, one would both hope and expect that if a reactor's safety largely depends on inherent safety features that it would have improved safety and reliability.

In putting inherent safety into perspective, it is important to note that some object to the term, perhaps with some justification. They find the term perjorative relative to other reactors that may not have been so labeled. The term runs the risk of introducing the syndrome of "my reactor is safer than your reactor," which is not likely to be a useful position to present to the public. However, the inherent safety features and characteristics of a reactor can indeed have profound effects on its safety and its response to potential accident initiators. Several reactors in recent years have tried very successfully to exploit potential inherent safety into design. One example is the liquid metal reactor, which can be designed to have important inherent safety characteristics. The reactor will shut itself down under a wide variety of dominant risk accident initiators. EBR-II, which is in many ways characteristic of some of the proposed liquid metal fast reactor designs, recently demonstrated that it can shut itself down, with no action required of the control system, when subjected to classic core disruptive reactor accident initiators; the loss-of-flow without scram and the loss-of-heat sink without scram.

Perhaps the most valuable part of the push for inherent safety is that it keeps the concept of building safety into the plant constantly in front of the reactor designer during the entire design process. The NRC has recently put out an advanced reactor plant policy statement and in that policy statement considerable importance is attached to inherent safety. The accident at Chernobyl had given considerable impetus to the concept and it is reasonable to expect inherent safety to be a major factor in future reactor designs.

Concluding Remarks

In conclusion, the approaches and perspective that have evolved over the past several years, including much increased emphasis on PRA, safety goals, the source term, and inherent safety, are all likely to play continuing major roles in our thinking about reactor safety. In addition to these, however, many of the old concepts, such as defense in depth, continue to play key roles. All play a complementary role in the approach to the safety of reactors. Our thinking is also much affected by the major events that have occurred. Many of the changed perspectives referred to in this paper have been driven by the TMI accident. Perhaps major changes in our thinking will occur from the Chernobyl accident even though at this stage our preliminary knowledge of Chernobyl has not led to any major rethinking. Nothing has occurred to alter our basic view that properly designed and operated reactors pose very little safety risk.