AECL-9763

ATOMIC ENERGY
OF CANADA LIMITED

L'ÉNERGIE ATOMIQUE
DU CANADA LIMITÉE

ADVANCED REACTOR CONCEPTS AND SAFETY

CONCEPTS DE RÉACTEURS AVANCÉS ET SÛRETÉ

J.J. LIPSETT

Presented at IAEA Technical Committee Meeting Västeras, Sweden,
1988 May 30 – 2 June

Chalk River Nuclear Laboratories

Laboratoires nucléaires de Chalk River

Chalk River, Ontario

June 1988 juin

ATOMIC ENERGY OF CANADA LIMITED

ADVANCED REACTOR CONCEPTS AND SAFETY

by

J.J. LIPSETT

Presented at IAEA Technical Committee Meeting
Västeras, Sweden, 1988 May 30 - 2 June

Advanced CANDU Project
Chalk River Nuclear Laboratories
Chalk River, Ontario K0J 1J0

1988 June

AECL-9763

L'ÉNERGIE ATOMIQUE DU CANADA, LIMITÉE

CONCEPTS DE RÉACTEURS AVANCÉS ET SÛRETÉ

par

J.J. Lipsett

RÉSUMÉ

L'AIEA a identifié un certain besoin de cohérence de la terminologie servant à décrire l'évolution de méthodes assurant la sûreté des réacteurs nucléaires. Cela arrive à point car il semble qu'il y a danger que la précision de nombreux mots précieux soit diluée et qu'un nouveau jargon puisse apparaître et rendre confus au lieu de faciliter la communication de conceptions et concepts importants mais peut-être variés.

Parmi les difficultés auxquelles se heurte l'industrie nucléaire, il faut citer celles d'encourager et d'acquérir la connaissance étendue des risques que posent effectivement les réacteurs nucléaires. Etant donné l'importance de la communication à la fois au public et à la communauté technique en général, le point de départ quant à la définition des termes doit être les significations des dictionnaires et l'usage technique courant. La communauté du génie nucléaire devrait employer ces termes en conformité avec le monde technique entier.

Dans la présente communication, on traite d'un grand nombre des questions suggérées dans la sollicitation de réunion et on soulève certaines rôle de l'opérateur dans l'amélioration ou la détérioration de la sûreté et la façon dont la signification et l'interprétation du terme "sûreté" doit éventuellement changer au cours des prochaines décennies.

Il est avantageux de se servir de critères en fonction desquels on peut juger les techniques et le comportement en service si les critères sont génériques et non spécifiques de concepts de réacteurs particuliers. On présente certaines opinions quant au besoin de concevoir les critères avec prudence de sorte à ce qu'on encourage les solutions et concepts nouveaux au lieu de les étouffer.

Projet CANDU avancé
Laboratoires Nucléaires de Chalk River
Chalk River, Ontario K0J 1J0
1988 juin

AECL-9763

ATOMIC ENERGY OF CANADA LIMITED

ADVANCED REACTOR CONCEPTS AND SAFETY

by

J.J. Lipsett

ABSTRACT

The need for some consistency in the terms used to describe the evolution of methods for ensuring the safety of nuclear reactors has been identified by the IAEA. This is timely since there appears to be a danger that the precision of many valuable words is being diluted and that a new jargon may appear that will confuse rather than aid the communication of important but possibly diverse philosophies and concepts.

Among the difficulties faced by the nuclear industry is promoting and gaining a widespread understanding of the risks actually posed by nuclear reactors. In view of the importance of communication to both the public and to the technical community generally, the starting point for the definition of terms must be with dictionary meanings and common technical usage. The nuclear engineering community should use such words in conformance with the whole technical world.

This paper addresses many of the issues suggested in the invitation to meet and also poses some additional issues for consideration. Some examples are the role of the operator in either enhancing or degrading safety and how the meaning or interpretation of the word "safety" can be expected to change during the next few decades.

It is advantageous to use criteria against which technologies and ongoing operating performance can be judged provided that the criteria are generic and not specific to particular reactor concepts. Some thoughts are offered on the need to frame the criteria carefully so that innovative solutions and concepts are fostered, not stifled.

Advanced CANDU Project
Chalk River Nuclear Laboratories
Chalk River, Ontario, Canada K0J 1J0

1988 June

AECL-9763

TABLE OF CONTENTS

INTRODUCTION

In the spirit of the call by the International Atomic Energy Agency for the meeting, this paper attempts to address the generic aspects of reactor safety and the means used to describe the objectives and methods for accomplishing the goal.

This meeting is not intended to judge the merits of the different approaches implicit in the terms and subjects under consideration so the contents of this paper can be as unbiased as possible.

It is anticipated that this is the first step in an iterative process of defining terms and methods so some of the topics suggested for discussion have not been definitively treated and only brief comment has been offered on the subjects of criteria and appropriate physical phenomena.

PREFACE, THE FUTURE SCENE

The outcome of this technical committee's deliberations has the potential for long-lasting effects on the direction that reactor safety activities may take. It therefore seems appropriate to try to gain some appreciation of what may lie ahead.

First, however, we should remind ourselves about the fundamentals behind our discussions.

The important natural phenomena are:

- the potential of the fission-chain reaction for high power levels and for rapid rate of change of power;
- the inexorably continuing, although declining, heat generation arising from fission-product decay; and
- the radiation associated with fission-product decay.

The hazards are:

- physical damage to the plant, and
- the health, ecological, and economic consequences of the release of radioactive fission products.

The safety objectives are:

- to prevent fast reactivity excursions;
- to adequately cool the fuel under all foreseeable circumstances; and

- to prevent the release of hazardous quantities of fission products from the plant in exceptional circumstances.

Considering that:

- the nuclear power plants currently in service and being constructed must be operated safely for their design lifetime or an extended lifetime;

- there may be good reasons to adapt the existing designs so that a new generation of plants will have improved resistance or a different response to serious upsets, if only to increase the market potential;

- second- or third-generation power plants should be conceived and implemented after 2010 along with other reactor concepts aimed at different segments of the energy market;

there will be a period of several decades where different philosophies and methods for ensuring the safety of reactors will coexist.

Since it is in the best interests of the industry that all these plants be accident-free, this committee has to be careful in its assessment and definitions in order to encourage, not inhibit, innovative changes and improvements to enhance the safety or lower the risks for all three categories of power plants.

During these coming decades the public understanding of radiation hazard and the risks to health and of social disruption may improve and result in an acceptance that the real risks are generally small. Consequently, there might be a relaxation of the regulatory limits for releases and exposures. It seems more likely, however, that the trend towards a risk-free society/environment will continue and, for a potential hazard as easily measured as radiation, this will result in a tightening of restrictions and a lowering of release limits. These same trends are also affecting the alternatives to nuclear power as the deleterious effects of large-scale fossil-fuel combustion become evident in the environment. It is therefore possible that a difficult public choice will have to be made in this same time period and the nuclear power option may have a better opportunity than fossil fuels to meet any revised public view of safety. Today's standards of acceptable radioactive releases to the environment should therefore be used cautiously as absolute design criteria for future plants.

When, as we expect, the use of nuclear power expands to supply a major portion of the energy requirements for society, the issue of reliability will become increasingly important since the disruption of supply could have serious economic and social consequences and indirectly affect the health and well-being (safety) of the population. The future balance between the risk of reactor accidents and reliable plant performance (the two faces of safety) will be delicate, variable and largely unpredictable.

DEFINITION OF TERMS

Suggested Definitions

Among the difficulties faced by the nuclear industry is developing a widespread public understanding of the risks actually posed by nuclear reactors. In view of the importance of communication to both the public and to the technical community generally, the starting point for the definition of terms must be the dictionary meanings and the usage within the whole technical world, not just the nuclear engineering community. The definitions [1, 2] of some words that are important for a clear understanding of reactor safety issues are as follows:

- Inherent: an essential or natural characteristic; will always behave the same way.

- Passive: quiet, static or dormant; waiting for a call; unpowered or self-powered.

- Active: energetic, movable, in constant use; requiring outside information and/or power (usually electrical).

- Fail-safe: incorporating some feature for automatically counteracting the effect of a possible source of failure (of power, control circuits, structural components or other components).

- Foolproof: so simple, plain, or reliable as to leave no opportunity for error, misuse, or failure.

- Engineered: (from the noun engineering) the application of science and mathematics by which the properties of matter and sources of energy in nature are made useful to people in structures, machines, products, systems and processes.

- Walkaway: a word recently coined to indicate that the absence of operator attention or abandonment will not lead to serious consequences.

- Forgiving: allowing room for error or weakness.

When using these adjectives there is seldom any difficulty in applying them accurately at the component level; it is more difficult at the system level; while at the total plant level the opportunities for disagreement become apparent. For example, if an alternative cooling system consists of a self-powered, natural-convection, heat-transport path to a heat sink, but is normally isolated by electrically operated fail-safe valves, each part can be defined with some reasonable agreement, but it could be difficult to definitively classify the whole.

Of the above eight terms, most have traditional meanings that could be expanded carefully in a nuclear context, if necessary. The words "engineered" and "inherent" have, however, taken on special connotations.

Engineered versus Inherent

Although current usage is variable, the sense for these two words is to state an objective or philosophy more than a precise single meaning in the normal sense of an adjective.

"Engineered" has a very broad meaning whereas there are at least two narrow meanings or interpretations applied to the word in the context of reactor safety:

- The sense that any threat to public well-being is treated as a separate issue in that the plant is designed and built to generally accepted industrial standards for good performance and low risk of damage arising from an accident, and then surrounded or supported by additional systems to reduce the risk to the public to a very low probability.

- The assessment proposed by Rasmussen [3], that "open loop" safety is designed from analysis, separate-effects or modelled experiments and cannot be demonstrated in total without risking the destruction of the plant.

In contrast, and possibly intended as an antonym, "inherent" has been adopted to describe a process or system that incorporates all of the necessary protective features, represented by self-limiting characteristics (or "closed loop " design [3]), or a naturally triggered changeover between states that has no unsafe intermediate or alternate condition. The difficulties that this causes are:

- the presumption that no events can occur that will progress opposite to the direction that is inherently self-limiting, i.e. the divergent direction, and

- the implication that the designs that are labelled as inherently safe are not engineered whereas many that have been proposed contain significant engineering achievements and the challenge of pursuing these principles is very demanding of engineering skill.

Others [2, 3] have expressed reservations about the use of "inherent safety" when applied to a total plant, since it could raise unreasonable expectations both inside and outside the industry, and, should any plant labelled "inherently safe" experience even minor difficulties, the damage to public acceptance could be serious.

It is a laudable objective to design systems that will converge to a readily acceptable state under all circumstances. Since that is difficult to achieve, especially for large reactor sizes, hybrid designs containing systems with a mixture of appropriately active, passive and convergent characteristics should be expected and encouraged. The larger goal expressed by the "inherently safe reactor" philosophy may be only approachable and depends on the ability of the designer to foresee and forestall all eventualities.

Two aspects are of particular interest and concern since they are difficult to deal with in the generic sense:

- loss of control through unanticipated reactivity insertion;

- failure of flow ducting in natural convection systems.

ALTERNATIVE THOUGHTS

In the process of revisiting the subject of reactor safety and possible alternative design methods, I found it useful to go back to some basic principles to help define conceptual directions.

When the laws of nature are applied for technological purposes, it is necessary to understand the natural phenomena for separate and selective use, and to create a supportive, sometimes artificial environment. Therefore, the device in question will have:

- Inherent behaviour due to the physical laws and principles that are applicable to the designed arrangement.

- Engineering boundaries and conditions that isolate the device from the outside world, constrain or limit the operating range and power the systems. These would include the physical boundaries like piping, structures and mechanisms; process equipment like power sources, prime movers (pumps, etc.); values for process parameters like temperatures, flows and pressures; and reactivity mechanisms such as shim controls or adjusters.

When safety is being treated it is also necessary to be concerned with the consequences of perturbations to the engineered boundaries. An argument can be developed that failures of the engineered boundaries and conditions are the sources of major events, since the naturally occurring perturbations of large magnitude tend to be slow and therefore easily compensated while the fast ones tend to be small and statistical. It follows, therefore, that the design of the boundaries sets the accident potential for the reactor. Conversely, the accident potential can be minimized by proper boundary design, which opens up considerable scope for innovation through simplification, subdivision and redundancy, and speed of operation as in the case of limits for reactivity change.

In the event of a boundary disturbance, the consequences must be handled by either intercepting any excursion or defaulting to a different safe state or some combination of the two. Looking first at default, this means that two possible conditions or processes are always available in parallel and that the switch between them can occur easily or naturally, usually from the high-capacity, high-performance process to a low capacity, but more reliable

process. Parallel operation implies that there is an interface or boundary condition between them that changes. In cooling systems this can be a transition from forced convection to conduction, as with the HTGR or to natural convection, as with PIUS. These two examples also illustrate two distinct forms that default can take; high temperature and low temperature.

In high-temperature default, the tolerable fuel temperatures are significantly greater than normal operation so, in the event of loss of normal cooling, the system defaults naturally to heat rejection by conduction to the lower capacity alternative cooling system. Since the initial heat rejection rate is low, the core temperatures rise and the rate of heat rejection increases with the temperature. Simultaneously, the negative temperature reactivity effects drive the reactor power down and, if properly matched, the power and the heat rejection rate are in equilibrium at safe core temperatures.

In low-temperature default, there are lower limits for fuel temperatures and, since the alternative cooling has smaller natural convection heat transfer rates, the coolant temperatures must be lower. Since two coolants of different temperatures must sequentially occupy the same space, gates must be provided in the boundary that normally separates them. The principles and mechanisms that form and actuate the gates may fall into many categories; active, passive and in some cases the interaction of fluids that might be called inherent behaviour, such as in some heat pipes.

If the reactor has a negative temperature coefficient, the inherent reactivity increase accompanying the colder coolant must be compensated. In the case of PIUS and ISER this is accomplished by simultaneous poison injection that can be viewed as a pre-emptive intercept of a system excursion.

The engineering of the default and interception systems provides a wide range of opportunities for invention and the subtle use of a variety of natural laws to create the necessary gates. A series of default states might be used to provide a path to a final environmental heat sink that would give defence-in-depth.

Finally there are simple barriers, like containment, that can serve as passive interceptors for fission products.

The term interception was chosen initially to refer to reactivity effects and was to be a substitute for "SCRAM" and "TRIP", which carry a connotation of being very fast and actively triggered. In several concepts, like SLOWPOKE [6], there are passively actuated poison releases that are slow, but effective, in reactors with long time constants. The term has proved to be useful in considering a wider sense. (I should note here that I find it much easier to understand and accept passive or inherent behaviour in terms of cooling upsets rather than reactivity effects and expect to have some difficulty with definitions intended to cover the complete range of possible reactivity events.)

CRITERIA

The establishment of criteria for assessing, judging and communicating the various methods for providing safe reactor design and operation is going to be important. In the context of the iterative process envisaged for this committee, the development of these criteria is seen as a later stage following the definition of principles and terms for design and operating methods.

In particular it seems to be premature to try to compose a list of allowable laws of nature, especially for "passive" devices since it precludes some inventive minds. It might be more advantageous to first set out objectives such as the following.

> Objective 1 - The energy and forces required to operate must always be available and not able to "leak away", e.g. gravity and the mechanical or metallurgical solid state, as with the temperature triggered change from the austenitic to martensitic phases of certain nickel/tin alloys.
>
> Objective 2 - Initiating mechanisms must be reliable and repeatable, e.g. electromagnetic phenomenon like the Curie point of an electromagnet, or a physical constant like the melting point.
>
> Objective 3 - Mechanisms that are required to move must be "stick-proof", e.g. common physical effects like thermal expansion, or carefully arranged fluid interface/barriers.

Implicit with the use of words like "foolproof" and "walkaway" is the realization that human factors are an important aspect of reactor safety. This has several sides but the most obvious are design and operation. The objective is to eliminate, as far as possible, human error or oversight as factors in the initiation or exacerbation of accidents. In reactor control, automation is frequently used to reduce the role of the operator, and the designer thereby assumes a greater role in the safety equation. The same is true for a predetermined, passively activated reaction to a system upset.

It is worth considering the combination of the operator and the designer as a means of introducing redundancy and diversity into the safety process and the roles and limitations of each, for example, beneficial operator actions for safety enhancement and the operating regime in which he functions [4].

WHY CHANGE?

What is being discussed is a possible change in the direction of ensuring that reactor designs remain safe to very high standards. The reasons seem to be as follows:

- In some places and jurisdictions, there has been an ever-increasing escalation of accident scenario development and analysis and the very low probabilities of occurrence have become obscured, so that the complexity and costs of "after the fact" design changes have eventually made the plants prohibitively expensive.

- Although there has been a majority public recognition that society will require the nuclear power option in the future, there is a public distrust that must be addressed and overcome so that the option survives.

- A growing segment of reactor planners and designers believe that other philosophies and methods of ensuring reactor safety have validity and should be explored.

When specific designs are engineered and critically reviewed for implementation, the questions of relaxing defence-in-depth, redundancy and other prominent philosophic principles will have to be dealt with in detail. Establishing the validity of new methods and philosophies will not be simple because the plant and systems are man-made and will be man-operated. The best engineering tools, like probabilistic risk assessment, will still be needed, although the approach may be revised.

It would be advantageous for a system or reactor to be demonstratively safe, but even then, rare initiating events like earthquakes could not be demonstrated and would always need analysis.

SUMMARY

Most of the words being used in relation to reactor safety have traditional meanings that should be maintained and expanded carefully in a nuclear context, if necessary. The words "engineered" and "inherent" have, however, taken on special connotations that may not be easily conveyed to the public.

There is seldom any difficulty in applying these various adjectives accurately at the component level; however, when systems consist of a mixture of components and principles it could be difficult to definitively classify the whole.

The use of "inherent safety" when applied to the total power plant should be avoided since it implies an absolute that may never be achieved and unreasonable expectations should not be raised both inside and outside the industry.

It remains, however, a good thing to search for other philosophies and methods of ensuring and improving reactor safety. To design systems that will converge to a readily acceptable state under all circumstances is a laudable objective, and if achieving or approaching that objective requires hybrid designs with a mixture of appropriately active, passive and convergent characteristics, it should be expected and encouraged.

REFERENCES

[1] Webster's Ninth New Collegiate Dictionary, Merriam-Webster Inc., Springfield, MA, (1986).

[2] Parker, S.P. (Editor in Chief). McGraw-Hill Dictionary of Scientific and Technical Terms, Third Edition, McGraw-Hill Book Company, New York, NY, (1984).

[3] Rasmussen, J. Safety Control and Risk Management. Presented at the IAEC Specialists Meeting, Roskilde, Denmark, (1987 May 25-27).

[4] Meneley, D.A., University of New Brunswick, Private Communication.

[5] Rossin, A.D. Milestones and Signposts. Presented at the ANS Topical Meeting, Seattle, WA, (1988 May 2).

[6] Lynch, G.F. District Heating with Slowpoke Energy Systems. Atomic Energy of Canada Limited, Report AECL-9720, (1988 March).

ISSN 0067 - 0367

To identify individual documents in the series we have assigned an AECL- number to each.

Please refer to the AECL- number when requesting additional copies of this document

from

Scientific Document Distribution Office
Atomic Energy of Canada Limited
Chalk River, Ontario, Canada
K0J 1J0

Price: A

ISSN 0067 - 0367

Pour identifier les rapports individuels faisant partie de cette série nous avons assigné un numéro AECL- à chacun.

Veuillez faire mention du numéro AECL- si vous demandez d'autres exemplaires de ce rapport

au

Service de Distribution des Documents Officiels
L'Energie Atomique du Canada Limitée
Chalk River, Ontario, Canada
K0J 1J0

Prix: A

2480-88