CONF-8805138--1

DE88 011014

IMPLICATIONS OF PASSIVE SAFETY BASED ON HISTORICAL INDUSTRIAL EXPERIENCE

C. W. Forsberg*
Chemical Technology Division

Oak Ridge National Laboratory
Post Office Box 2008
Oak Ridge, Tennessee 37831
U.S.A.

for
International Atomic Energy Agency (IAEA)
Technical Committee Meeting

on
Definitions and Understanding of Engineered Safety; Passive Safety
and Related Terms

in
Västerås, Sweden
May 30 - June 2, 1988

---

*Research sponsored by the Office of Nuclear Energy, U.S. Department of Energy, under contract DE-AC05-84OR21400 with Martin Marietta Energy Systems, Inc.

IMPLICATIONS OF PASSIVE SAFETY BASED ON HISTORICAL INDUSTRIAL EXPERIENCE

C. W. Forsberg

Abstract

In the past decade, there have been multiple proposals for applying different technologies to achieve passively safe light water reactors (LWRs). A key question for all such concepts is, "What are the gains in safety, costs, and reliability for passive safety systems?" Using several types of historical data, estimates have been made of gains from passive safety and operating systems, which are independent of technology.

Proposals for passive safety in reactors usually have three characteristics: (1) Passive systems with no moving mechanical parts, (2) systems with far fewer components and (3) more stringent design criteria for safety-related and process systems. Each characteristic reduces the potential for an accident and may increase plant reliability. This paper addresses gains from items (1) and (2). Passive systems often allow adoption of more rigorous design criteria which would be either impossible or economically unfeasible for active systems. This important characteristic of passive safety systems cannot be easily addressed using historical industrial experience.

I. INTRODUCTION

In the past decade, many proposals have been made for development of passive safety systems for some or all of the safety needs of water cooled reactors (Duncan, Forsberg, Hannerz, Vijuk). The key question for such concepts is, "What are the gains if passively safe reactors are developed?" This article examines potential gains in safety, reliability, and economics from adoption of passive systems. The emphasis is on identifying and quantifying gains independent of particular technological solutions. While the primary incentive has been passive safety, potential gains from passive technologies apply equally to non-safety-related passive operating systems.

In this report, passive safety is first defined. Then studies are reviewed which examine gains from adopting passive technology from several different perspectives. No single study or analysis can quantify these gains, but together, multiple studies can quantify the range of potential advantages.

II. DEFINITIONS OF SAFETY

There are no agreed upon definitions of safety terms for reactors or other hazardous facilities, although some definitions have been studied [Kletz]. Terms such as passive, inherent, failsafe, transparent, and others are used. In the United States, safety goals for developmental light water reactors [PIUS type reactors (Forsberg, Hannerz)] are being defined by the term PRIME (Passive, Resilient, Inherent, Malevolence resistance, and Extended protection for long-time periods). Defining and explaining PRIME safety goals provides a mechanism to understand what is and is not passive safety and some of the implications thereof. From the definition of passive safety, key characteristics are identified which can be used to compare passive and active systems.

A. Definition of PRIME Safety Goals

Passive

Passive safety is defined to be the use of safety systems without moving parts. Moving parts include, but are not limited to, mechanical valves, mechanical check valves, motors, pumps, and electrical equipment.

Resilient

Resilient safety systems operate when needed but are not activated by normal plant operating transients or other anticipated common events. There should be no temptations for operating or engineering crews to bypass or alter safety-related systems. Safety systems should facilitate the return to normal process operations and thus facilitate the resiliency of normal operations.

Inherent

Inherent safety means selecting materials or structural configurations to totally eliminate certain classes of accidents. For example, water is inherently safe against fire; so no safety system is needed to prevent water from burning. Inherent safety is the ultimate form of safety since it eliminates the possibility of an accident.

Malevolence Resistance

Malevolence resistance is the ability to passively withstand, without major radionuclide release to the environment, operator error or inaction, maintenance errors, internal sabotage, short-term terrorist plant takeover, or military assault with off-the-shelf weapons. In some cases, the consequences of operator/maintenance error and sabotage are identical; only the intent is differs. (The ability to withstand military assault is for normal battlefield weapons and excludes both nuclear weapons and specially designed non-nuclear weapons.)

High resistance to malevolence requires, as a prerequisite, both passive safety systems with no moving parts (including elimination of such items as maintenance shutoff valves which could stop operation of safety systems if improperly configured) and inherent safety features. In both the Three Mile Island (TMI) and the Chernobyl power plant accidents, operating crews shut down key safety systems for what were thought to be valid reasons at the time. In both cases, the safety systems would have prevented the accidents if they had been allowed to operate. Malevolence resistance requires more than passive safety since a passive safety system can be fragile.

Extended Protection

Extended safety refers to providing safety for extended periods of time after an accident or after abandonment of facilities for any reason. Nominally, this is taken to include passive long-term heat removal (years) in the case of plant abandonment and shorter-term heat removal (one week) in the case of major plant damage.

Like malevolence resistance, extended protection may require passive and inherent safety as prerequisites because of the long-term performance limitations of active systems.

B. Characteristics of Passive Safety

With an understanding of PRIME safety, a better understanding of passive safety is possible. Passive systems usually have three characteristics: (1) no moving parts (classical definition), (2) systems with far fewer components and structures , and (3) more stringent design criteria in terms of safety and plant availability. Many of the gains from passive safety systems are not the direct result of no moving parts but rather are the consequence of system simplifications or tighter design criteria that are only possible by elimination of moving parts.

Each of the subsequent sections explores one of the three characteristics of passive safety. Through industrial studies, the effects of each characteristic can be evaluated independently of the other characteristics.

III. ADVANTAGES OF PASSIVE SAFETY BY ELIMINATION OF ACTIVE ELECTROMECHANICAL EQUIPMENT

The potential gains from passive safety by elimination of active electromechanical equipment in LWR systems can be derived from operating records <u>if it is assumed that:</u>

1. A passive system is as complex as an active system.

2. The design criteria (reliability, repair difficulty) for passive systems are <u>identical</u> to those of active systems.

These assumptions are unrealistic; however, by sorting out the effects of different characteristics of passive systems, an understanding of passive systems is gained.

In the United States, the nuclear power plant operators are required to file with the U.S. Nuclear Regulatory Commission (NRC) Licensee Event Reports (LERs) for events which have the potential for impacting safety. These LERs are evaluated by the Nuclear Operations Analysis Center at Oak Ridge National Laboratory for the NRC. Data on equipment or system faults, personnel errors, and the unit and environmental effects described in LERs are entered into the Sequence Coding and Search System (SCSS) data base [NRC, LER]. Using information from the entire LER, each individual occurrence (e.g., component failure, system failure, personnel error, etc.) is coded as a separate step in the overall sequence of events at a particular reactor. Specific information encoded for each step includes the cause, system identification, component identification, component vendor, effect, personnel activity, and more. The individual steps are linked together in chronological order to construct an overall event sequence. The relationships between steps, such as predecessor and successor relationships, can be searched as well as the detailed information of individual steps.

With the SCSS data base, problems in or failures of primary, auxiliary or safety, secondary, and support systems can be analyzed. The eleven categories of failures are administration, construction, design, fabrication, installation, maintenance, operations, radiation protection, testing, others, and unknown. By definition, a passive system does not require an operator to operate it; hence, operations errors cannot occur. Other types of failures such as construction, design, fabrication, and installation will occur for both passive and active systems. Some types of errors–administrative, maintenance, radiation protection, testing, and unknowns–can occur for both passive and active systems but are much less likely to occur in passive systems. For example, a passive system may require application of paint to prevent corrosion; however, the level of maintenance would be less than for an active system which has pumps, valves, and motors.

Using the data (Table 1) from LERs of U.S. light water reactors, a first-level screening analysis indicates passive systems could eliminate 20% (operating errors) to 75% (operating plus other errors) of all safety-related system failures assuming: (1) passive systems are as complex as active systems and (2) design criteria are identical. The SCSS data base only includes safety-related events; however, it is reasonable to assume that if passive systems could be adopted for both safety and process systems, equivalent reductions in unplanned plant downtime would occur.

Table 1 also summarizes the error links between various causes of failure and the various reactor systems. The definitions of reactor systems are given in Table 2. Analysis of this data identifies failures by category and system and provides a basis to identify where the greatest gains are possible by adoption of passive systems to power reactor safety.

To fully understand this data, several characteristics of system failures need to be understood. A system can fail due to multiple causes. For example, if a design error combined with a maintenance error caused a primary reactor system failure, this would be recorded as 1 of the 124 errors linking system design mistakes with primary reactor system failures and as 1 of the 246 errors linking maintenance errors with primary reactor system failures. Similarly, a single failure can cause failures in multiple systems. For example, a design failure of a structural support member could affect both the electrical system and the feedwater system. Last, non-safety systems can fail, such as the main generator. If such a failure were then followed by a failure in a safety system–such as failure of a diesel generator to start – the main generator failure would be included because it was in the sequence of events which showed a safety system failure.

Table 1. Categories of errors versus system faults and failures[a]

			Error link by system												
Cause of failure or fault	Total error links	Percentage error link	Primary reactor	Essential reactor auxiliary	Essential services	Essential auxiliary	Electrical	Feed-water	Heat and ventilation	Instrument and control	Service auxiliary	Structural	Waste management
Operations													
1. Operation	2275	20	505	203	61	133	248	328	72	534	63	53	75
Building errors													
2. Construction	235	2	14	10	12	12	38	11	13	56	55	13	1
3. Design	1360	12	124	131	45	68	158	106	62	512	71	35	48
4. Fabrication	516	5	69	52	15	46	66	42	14	188	10	3	11
5. Installation	725	6	49	50	24	40	106	47	22	250	97	28	12
Subtotal	2836	25	256	243	96	166	368	206	111	1006	233	79	72
Other errors													
6. Administration	362	3	25	30	20	30	43	20	16	129	26	17	6
7. Maintenance	2516	22	246	189	76	139	402	224	106	911	99	68	56
8. Rad. Protection	103	1	0	1	2	6	0	0	7	49	21	11	6
9. Testing	2381	21	204	217	64	120	291	142	77	1122	79	26	39
10. Other/unknown	876	8	93	79	24	73	81	80	27	309	61	35	14
Subtotal	6238	55	568	516	186	368	817	466	233	2520	286	157	121
Total	11,349	100	1329	962	343	667	1433	1000	416	4060	582	289	268

---

[a] Includes License Event Reports (LERs) between 1984 and 1988; earlier LERs were reported under a different set of requirements and are not directly comparable.

Table 2. System categories in Licensing Event Reports

System category	Example of subsystems
1. Primary reactor systems	Reactor core, control rod drive, reactor vessel, pressurizer, steam generator, recirculating water
2. Essential reactor auxiliary systems	Auxiliary feedwater, emergency boration, residual heat removal, emergency core cooling, pressure relief
3. Essential service systems	Component cooling water, essential compressed air, emergency generator lube oil/fuel/starting/cooling subsystems
4. Essential auxiliary systems	Containment isolation, containment cooling, containment pressure control, containment combustible gas control
5. Electrical systems	High/medium/low voltage AC, instrument/control/computer AC, and DC, emergency power generation
6. Feedwater, steam, and power conversion systems	Main stream, turbogenerator, main condenser, condensate and feedwater
7. Heating, ventilation, and air conditioning systems	Reactor building HVAC, primary containment vacuum relief
8. Instrumentation & control systems	Alarm/annunciator, computer, fire detection, in-core/ex-core neutron monitoring, reactor power control
9. Service auxiliary systems	Sampling, control and service air, demineralizer water, raw cooling water
10. Structural systems	Containment, primary reactor containment, reactor drywell, reactor auxiliary building
11. Waste management systems	Liquid radwaste, solid radwaste, gaseous radwaste

LERs as a data source have several technical limitations. Over the years, the reporting requirements for LERs have changed, so, for consistency, only LERs generated since 1984 have been included in this analysis.

Another constraint is that the nuclear industry is a relatively young industry. It would be expected that LERs describing design, construction, and fabrication errors would decrease for any reactor from time of initial startup. As plants age, most of these errors would be identified and corrected. In an industry with relatively young plants, a disproportionate number of errors are to be expected in these categories. As the average plant age increases, a larger proportion of errors would be expected to result from operation and maintenance. Analysis of this phenomenon is, however, complex because there is also a learning curve which reduces operating and maintenance errors with time. The operating experience as reflected in the data bases today is insufficient to accurately quantify these effects. In four or five years, there should be sufficient data for analysis of learning curves.

IV. CONSEQUENCES OF REDUCTION OF PLANT COMPLEXITY BY USE OF PASSIVE SYSTEMS

A. Introduction

Experience shows that a second characteristic of passive systems is that they are less complex than active systems. Research has begun to quantify: (1) how to measure plant complexity and (2) the cost, safety, and plant availability impacts of plant complexity. The average (typical) differences in plant complexity between active and passive systems has not been studied because until very recently there were no reliable ways to measure plant complexity. This section reviews recent research findings on measuring complexity and quantifying its cost. Such research is a starting point to quantify gains of passive safety through simplicity.

Two sets of adverse consequences occur because of complexity. First are the obvious linear effects–the increased capital and repair cost with increasing quantities of equipment. Second, there are the increased capital costs (especially engineering indirect costs), lower plant availability, and longer repair times due to system interactions between components. Some examples from everyday experience can clarify what these system costs are.

Consider the operation and maintenance of a farm wagon versus that of a color television set. The wagon is a simple machine. If it fails, it is easy to diagnose what went wrong. In fixing such machines, the mechanic spends most of his time making repairs. In contrast, consider a television for which someone has randomly adjusted all the dials. To make it work properly (have high availability), it takes considerable time to adjust it to the proper settings. The many dials (controls) make adjustment time consuming. If the television must be repaired, its interaction complexity becomes more obvious. The repairman spends most of his time diagnosing what is wrong and relatively little time actually repairing the television. This additional cost for diagnosing (understanding) problems is an additional cost of complexity.

An alternative example is an automobile from the 1960s and one from the 1980s. The former was quite sophisticated, but still retained first-order connections between failures and malfunctions and the causes of failure. This is no longer true for many new automobiles with computerized components, multiple feedback loops, and multiple interactions between engine operating systems, emission control systems, fuel utilization systems, and other systems. The diagnostic problem grows with system complexity.

In terms of a complex power plant, the same effects occur. During operations, it takes time to diagnose a problem. Sometimes this results in the plant being shut down. If an operator can quickly diagnose a problem, changing plant operations can often allow a plant to continue to operate. Sometimes, as a result of plant interaction complexity, the operator is confused. The accident at the TMI Nuclear Power Station would have been avoided if the operators had successfully diagnosed the problem. In all of these cases, there are additional penalties caused by system complexity beyond the additional equipment.

Both generic studies (Perrow) and studies specific to nuclear power (Trauger) have examined plant complexity in a qualitative manner. More recent studies are attempting to quantify the cost, safety, and availability effects of plant complexity. Two of these studies are described below. Both studies are early attempts to quantify complexity; hence, the results are not final.

B. Complexity and Light Water Reactors

In the United States, researchers at the Massachusetts Institute of Technology (MIT) have been investigating theories of complexity for application to nuclear power plant design [Golay 1]. In particular, this work at MIT has, as one technical goal, to relate plant complexity to plant availability [Golay 2]. This is part of a larger effort to better factor into the design process the cost of reactor downtime and repair.

The work by Golay is based on the following observations: as system complexity increases, the downtime or plant unavailability is larger than would be predicted by addition of the times needed to fix individual pieces of equipment. This is because "the source of lost availability for a power station are the machines of the plant <u>and</u> the humans who operate and repair them." Humans cannot instantly diagnose plant problems, and the time necessary to diagnose problems increases monotonically with system complexity.

The MIT work indicates that the average number of steps, n, necessary by an operator to identify the status of a system for repair or change in plant operations can be represented by

$$n = 1/2\,(2)^{H},$$

where

$$H = \sum_{i=1}^{Ns} P_i \ln_2 (P_i),$$

where

H = informational entropy of the system,
Ns = number of independent system states,
P_i = probability that a system is in the i^{th} state.

An example can show the implications of this equation. Consider a piping system with multiple valves in series and the positions of the valves unknown. The valves are located in a radioactive area with no access. Each valve can be closed or opened, but the initial valve positions are unknown. With each attempt, one can observe if water flows through the set of valves. Table 3 shows the average number of such tests (change one valve position, observe if water flows through pipe) needed to define the initial setting of all of the valves as a function of the number of valves in the system. Figure 1 shows possible valve positions for the one, two, and three valve cases.

Now compare this system with a nuclear power plant system, such as a motor-driven feedwater system, when the start button is pushed in the control room but nothing happens. The plant operator must diagnose what went wrong. The failure could be anything from a defective start button to a broken feedwater pump casing. One obvious solution is to add instrumentation. For the earlier valve example, this could be a set of valve position indicators. For the feedwater system, it might be a motor voltage indicator that would indicate whether the motor was receiving power. Instrumentation would reduce the time needed to diagnose a problem but would not eliminate it. Furthermore, instrumentation can give false readings. Analysis shows that the time required to diagnose system status for repair, start of operation, or stopping an accident continually increases with system complexities.

Current research has related loss of plant availability to complexity for certain reactor subsystems but has not been generalized for application to the entire power plant. With additional research and data, direct correlations between complexity and loss of plant availability should be possible.

C. New Pioneer Chemical Process Plant Experience with Complexity

During the 1960s and 1970s, the chemical industry in the United States built a number of chemical process plants using new processes. The cumulative experience was that capital costs were considerably higher than expected. The RAND Corporation [Merrow] conducted a study of 44 pioneer chemical process plants built by private industry to identify the causes of unexpected cost growth. The complexity of some of these plans is equivalent to a nuclear power plant. Because the level of complexity varies between chemical plants, they provide a source of data to evaluate plant complexity versus cost.

The "normal" causes of unexpected cost overruns (unexpected inflation, unanticipated regulatory standards, labor strikes, and bad weather) accounted for only 26% of the unexpected costs.

Table 3. Number of diagnostic tests to define system status number of components for valve system

Number of valves	Number of tests to define position of each valve
1	1
2	2
3	4
4	8
5	16
6	32

Assume each valve has a 50% probability of being open or closed. This simple case is actually the upper bound case. In most systems, probabilities are not 50% for each possibie state. With nonuniform probabilities, diagnostic time to find equipment failures can be reduced by checking equipment with high failure rates first.

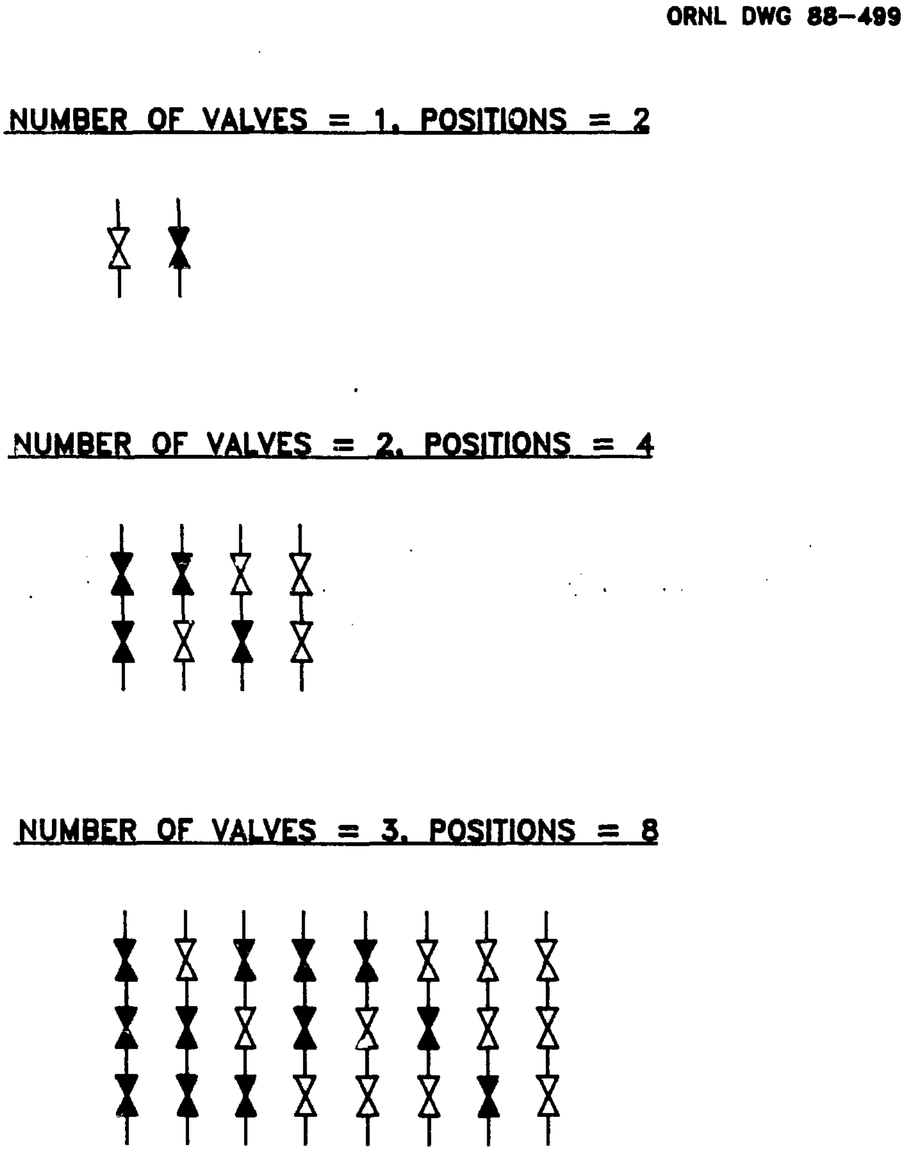

Fig. 1. Possible valve positions for systems with different levels of complexity.

The primary causes of unexpected cost growth were

(1) the number of unproven process steps,
(2) how well the project was defined before start of construction, and
(3) the complexity of the plant.

Table 4 summarizes the results of the analysis. Most noteworthy, the unexpected cost growth equaled 0.01137 times the number of process steps in the plant. In other words, on the average, each additional process step added to a chemical plant increased total plant costs by 1% beyond what was originally estimated.

This experimental evidence suggests that as plant complexity increases, additional unexpected integration costs between plant components occur in addition to normal costs. If the plant complexity doubles, costs will more than double if all other characteristics are held constant.

V. IMPACT OF PASSIVE SAFETY ON DESIGN CRITERIA

The third characteristic of passive systems compared to active systems is that such systems usually meet more stringent or more readily achieved design criteria. This is due to two factors.

First, in the normal design process, design criteria and requirements are specified in advance. If a passive system is chosen rather than an active system, the passive system will often meet much more stringent criteria in terms of safety and plant reliability than specified. For example, gravity flow of water is much more reliable than pumping water.

Second, the existence of passive systems often leads to consideration of higher design criteria including criteria that could not be met with electromechanical systems. Design criteria and requirements are in part determined by what is possible. For example, the proposed consideration of PRIME safety criteria is partly based on the existence of passive safety systems. The PRIME criteria include malevolence resistance and reactor safety for extended times after an accident. These types of criteria may require passive safety as a prerequisite requirement.

Table 4. Cost Growth Model for Pioneer Chemical Plant

Cost growth = 1.12196 - 0.00297 [PCTNEW]
- 0.02125 [IMPURITIES] - 0.01137 [COMPLEXITY]
+ 0.00111 [INCLUSIVENESS] - 0.0401 [PROJ. DEF]

Cost growth = Ratio estimated to actual cost
PCTNEW = Percentage of unproven technology
IMPURITIES = Difficulties with impurities in process (range 0-5)
COMPLEXITY = Block count of all process steps in plant
INCLUSIVENESS = Completeness of cost estimate (% of items included)
PROJECT DEF. = Level of site-specific and engineering information (range 2-8)

The mean ratio of estimated to actual costs for the cost estimates that were studied was 0.78.

VI. CONCLUSIONS

Passive safety and passive operating systems are systems without moving mechanical components (valves, motors, pumps) or electrical components. Experience with passive safety systems show major improvements in safety and reliability compared to active systems. In part this is a consequence of eliminating active components; in part this is a consequence of simpler systems with fewer components. Passive systems make possible the adoption of higher design criteria including improved malevolence resistance and maintenance of safe conditions for long time periods after an accident.

ACKNOWLEDGMENT

I would like to thank W. P. Poore of the Nuclear Operations Analysis Center at Oak Ridge National Laboratory for computer searches of the Sequence Coding and Search System Data Base. I would also like to thank M. Golay of the Department of Nuclear Engineering at the Massachusetts Institute of Technology for helpful discussions on the issues of plant complexity.

REFERENCES

[Duncan] J. D. Duncan, "Preliminary Conceptual Design Study for a Small LWR," EPRI NP-5150M (June 1987).

[Forsberg] C. W. Forsberg, "A Process Inherent Ultimate Safety Boiling Water Reactor," Nuclear Technology, Vol. 72, p. 121 (February 1986).

[Golay-1] M. W. Golay, P. H. Seong, and V. P. Manno, "A Measure of System Complexity and Its Relation to Diagnosis," International Journal of General Systems (in press).

[Golay-2] M. W. Golay, V. P. Manno, and P. H. Seong, "Simplificaton in Advanced Reactor Designs," American Nuclear Society Topical Meeting on Safety of Next Generation Power Reactors, Seattle, Washington (May 1-5,1988).

[Hannerz] K. Hannerz, "Adapting the LWR to Future Needs: Secure -P(PIUS)," Power Engineering, p. 54 (September 1985).

[Kletz] T. A. Kletz, Cheaper, Safer Plants or Wealth and Safety at Work: Notes on Inherently Safer and Simpler Plants, The Institution of Chemical Engineers, Rugby, Warwickshire, England.

[LER] U.S. Nuclear Regulatory Commission, Licensee Event Report (LER) Compilation, NUREG/CR-2000, ORNL/NSIC-200, Vol. X, No. Y (issued monthly).

[Merrow] E. W. Merrow, K. E. Phillips, and C. W. Myers, Understanding Cost Growth and Performance Shortfalls in Pioneer Process Plants, RAND Corporation, R-2569-DOE (September 1981).

[NRC] U.S. Nuclear Regulatory Commission, Sequence Coding and Search System for Licensee Event Reports: User's Guide, NUREG/CR-3905 (April 1985).

[Perrow] C. Perrow, Normal Accidents, Basic Books, Inc; New York (1984).

[Trauger] D. B. Trauger et al., Nuclear Power Options Viability Study: Vol. III, Nuclear Discipline Topics, ORNL/TM-9780/3 (Sept. 1985).

[Vijuk] R. P. Vijuk and T. L. Schutz, "Passive Safety Approach for the Advanced (W) 600 MWe PWR," International Energy Conversion Engineering Conference, Philadelphia (Aug. 1987).