CONF-800648--10

GA-A15930

THE REVISED GCFR SAFETY PROGRAM PLAN

by
A. P. KELLEY, B. E. BOYACK, and A. TORRI

MAY 1980

GENERAL ATOMIC COMPANY

GA-A15930

THE REVISED GCFR SAFETY PROGRAM PLAN

by

A. P. KELLEY*, B. E. BOYACK, and A. TORRI

This is a preprint of a paper to be presented at the Second Annual GCFR Program Technical Review Meeting, sponsored by Helium Breeder Associates, June 4-6, 1980, Rancho Bernardo, California, and to be published in the Proceedings.

Work supported by
Department of Energy
Contract DE-AT03-76SF71023

*Helium Breeder Associates, San Diego, California

GENERAL ATOMIC PROJECT 6114
MAY 1980

GENERAL ATOMIC COMPANY

THE REVISED GCFR SAFETY PROGRAM PLAN*

A. P. Kelley
Helium Breeder Associates
San Diego, California

B. E. Boyack and A. Torri
General Atomic Company
San Diego, California

ABSTRACT

This paper presents a summary of the recently revised gas-cooled fast breeder reactor (GCFR) safety program plan. The activities under this plan are organized to support six lines of protection (LOPs) for protection of the public from postulated GCFR accidents. Each LOP provides an independent, sequential, quantifiable risk barrier between the public and the radiological hazards associated with postulated GCFR accidents. To implement a quantitative risk-based approach in identifying the important technology requirements for each LOP, frequency and consequence-limiting goals are allocated to each. To ensure that all necessary tasks are covered to achieve these goals, the program plan is broken into a work breakdown structure (WBS). Finally, the means by which the plan is being implemented are discussed.

INTRODUCTION

The purpose of the safety program plan is to establish a logical framework within which the technological requirements necessary to demonstrate that the GCFR can achieve a requisite degree of safety in terms of public risk can be identified and ordered according to priority. This purpose is to be accomplished without penalizing the ability of the GCFR to

---

*This paper supported by the Department of Energy Contract DE-AT03-76SF71023.

compete successfully with alternate power generation technologies on an economic basis. By this means, the Department of Energy (DOE) and Helium Breeder Associates (HBA) can be assured of the timely and orderly execution of the safety program which they fund.

For large amounts of radioactivity to be released from the core fuel it must be severely overheated and essentially melt to present any potential hazard to the public. The yardstick for measuring this hazard potential of the plant is "risk," as measured by the probability of a given radioactivity release to the environment. Thus, the study of the plant at all levels of operation is important to ensure that a requisite level of risk is attained by reducing either accident probabilities, consequences, or both. The plan's scope must therefore include activities which address the probability of accidents which could lead to fuel melting as well as the ability of the plant to mitigate the consequences of fuel melting should it occur.

BACKGROUND

When application is made for a nuclear power plant construction license, the federal regulations specified in Title 10 of the Code of Federal Regulations (10 CFR) require that analysis be provided so that the risk to the public health and safety resulting from operation of the facility can be quantified and the margins of safety during all stages of plant operation determined. This assessment of risk has traditionally been made within the context of "multiple levels of safety design" on the basis of deterministic evaluations of conservative plant conditions. The multiple level of safety approach has been reasonably successful, judging by the absence of hazards to the public, even though 70 light water reactor (LWR) plants are in operation. Establishing such levels on the basis of deterministic analyses, however, has provided relatively little insight into the likelihood of system failures which initiate the accidents in the first place. Without such insight, it is nearly impossible to determine where safety improvements can optimally be made or where research efforts should be directed to ensure that the levels of safety are enforced. To address such issues, probabilistic analysis methods have been introduced in the past few years so that both consequence and probability information is available to assess risk.

LINES OF PROTECTION

The primary physical obstacles of the GCFR plant, as well as other nuclear plants, which prevent exposure of the public to core radioactivity are the steel cladding which encloses the core fuel, the reactor vessel which houses the core and coolant, the containment building which houses all this, and the site itself which places distance between the public and the plant. Maintenance of the first obstacle has rightfully received the traditional first priority in the plant design, such that there are three additional independent and separate means provided to protect it: the normal operating systems, the dedicated safety systems, and inherent features which ensure that cladding damage would be limited even if the above systems fail.

The goals of the safety program plan will therefore primarily be met by developing six separate and independent LOPs. The first three (operating systems, dedicated safety systems, and inherent features) maintain gross cladding integrity; the second three (primary vessel, secondary containment, and site) mitigate the consequences of accidents resulting in the release of core activity. Each provides a sequential and quantifiable risk barrier between the public and the radiological hazards associated with postulated GCFR accidents, as illustrated in Fig. 1. The six LOPs and their functions are described below.

1. LOP-1, operating systems reliability. The function of LOP-1 is to minimize the frequency of incidents requiring plant shutdown and to provide a first means of reliable shutdown and cooldown of the reactor core following all residual occurrences which require shutdown. LOP-1 employs the operational and design features in the GCFR plant to provide normal electrical power generation to

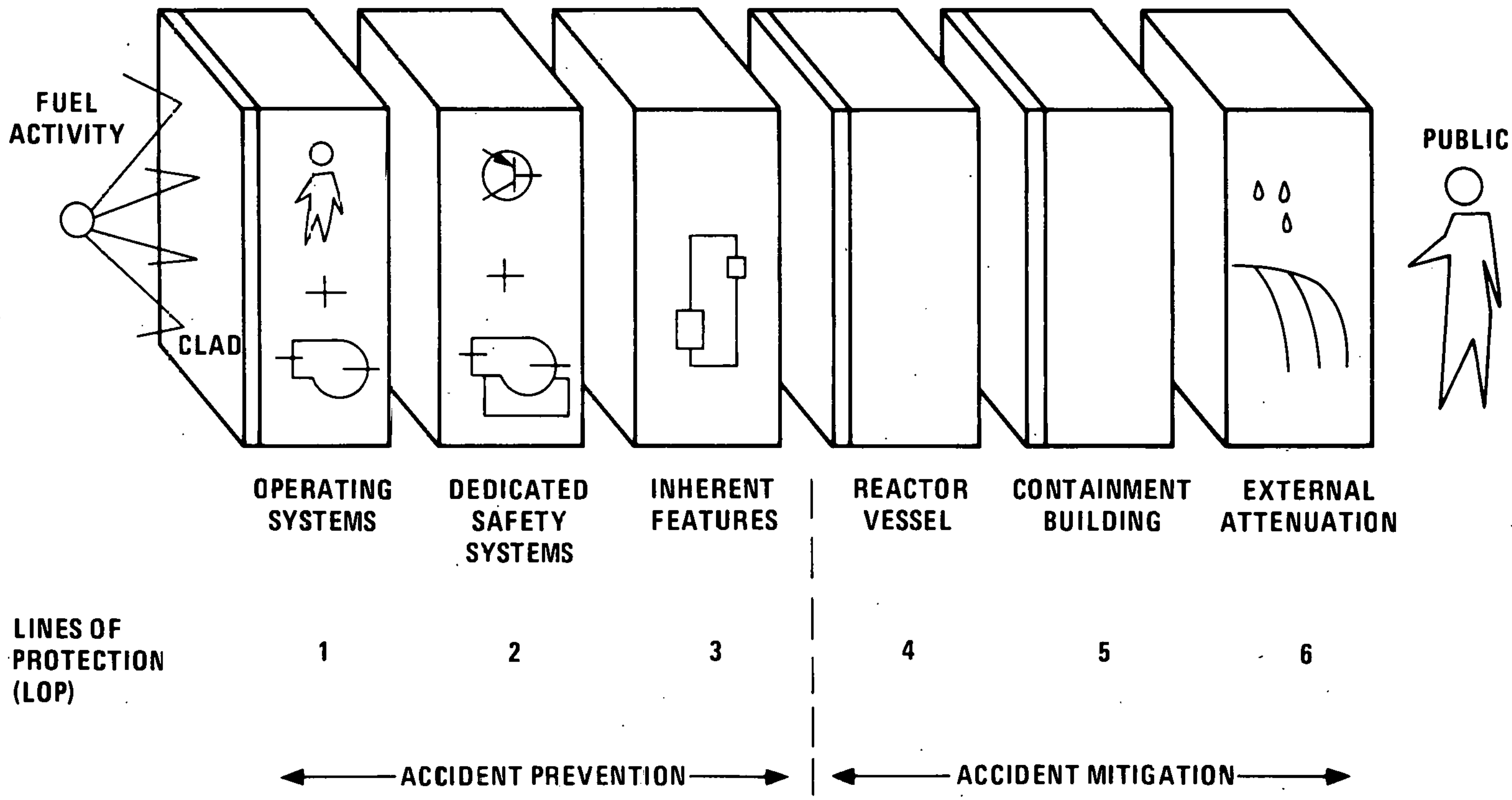

Fig. 1. Safety program barriers

accomplish this function. This includes the following systems: reactor core, reactor vessel, reactor internal components, plant control and instrumentation, main loop and shutdown cooling systems (SCS), control rod system, and related balance of plant (BOP) systems.

2. LOP-2, dedicated safety systems. The function of LOP-2 is to provide automatic, reliable shutdown and cooldown of the core in the event that the operating systems in LOP-1 fail. LOP-2 includes those systems dedicated to providing this safety function which are independent of the systems providing normal electrical power generation. This includes the following systems: core auxiliary cooling system (CACS), shutdown rod system, plant protection system and related BOP systems.

3. LOP-3, inherent accident prevention. The function of LOP-3 is to demonstrate that the inherent response of the reactor system will limit core damage even if the active systems in LOP-1 and LOP-2 fail. By providing this function with inherent features, free from human intervention, an additional level of protection is provided against common cause failure mechanisms. LOP-3 includes the following features: natural convection core cooling, inherent reactor shutdown mechanisms, and inherent local fault accommodation.

4. LOP-4, in-vessel accident containment. The function of LOP-4 is to demonstrate that the prestressed concrete reactor vessel (PCRV) structure and associated systems inherently protect the containment against consequential failure in the event of whole-core disruption resulting from the failure of LOP 1 through 3. LOP-4 deals primarily with two threats to vessel integrity: energetics and core debris.

5. LOP-5, containment integrity. The function of LOP-5 is to demonstrate that the containment building structure and associated systems can delay, control, and reduce the release of radioactivity to the environment in the event of LOP-4 failure. LOP-5 deals with missile considerations, containment pressure buildup control, containment leakage control, flammable gas control, and heat load accommodation.

6. LOP-6, radiological attentuation. The function of LOP-6 is to demonstrate that naturally occurring attenuation mechanisms limit the quantity of radioactivity which can be transported in the environment to produce significant public health effects even in the event of failure of the preceding LOPs. LOP-6 deals with aerosol depletion mechanisms, weather and siting conditions, and emergency procedure planning.

The LOPs defined above separate the core disruptive accident sequence into its major components. Each LOP independently reduces the probability and consequence, hence risk, of a given accident initiator. the failure of each successive LOP serves as the challenge to each succeeding LOP.

It should also be noted above that LOP-1 and LOP-2 deal with design features provided in the normal course of addressing the safety issues which must be addressed within the design basis, and LOPs 3 through 6 address the capability of the GCFR to accommodate and mitigate events traditionally considered beyond the design basis. The LOP approach therefore extends the traditional defense, an in-depth concept which considers the accommodation of accidents much more severe than those included within the design basis. In addition, it can be noted that it is the function of LOPs 1 through 3 to render an extremely low probability to any accident which could potentially lead to significant releases of radioactivity to the environment. It is the function of LOPs 4 through 6 to mitigate the consequences of these low-probability accidents in the unlikely event that they occur.

OVERALL GOALS

Two formidable problems are faced in implementing a quantitative risk-based approach in identifying technology requirements for each of the LOPs: (1) the overall risk acceptance criteria for the plant must be quantified, and (2) goals consistent with the overall acceptance criteria must be allocated to each of the LOPs.

In general, generic risk acceptance criteria have not been established for nuclear power plants in the U.S. However, the Nuclear Regulatory Commission (NRC) has provided some guidance in terms of risk goals for the liquid metal fast breeder reactor (LMFBR); i.e.,

1. The design should ensure minimization of the risk associated with core meltdown events to an extent comparable to that of LWR designs.

2. There must be no more than one chance in one million per year (i.e., 10^{-6} per reactor year) for potential consequences greater than 10CFR100 guidelines for an individual plant.

Until such time as risk acceptance criteria are established for nuclear power plants, the above guidance combined with other relevant NRC criteria will be assumed to present an acceptable risk objective for design and operation of the GCFR.

The problem of allocating goals to each LOP does not have a unique solution. There are innumerable combinations of weightings which might be assigned to each LOP which would be consistent with the overall acceptance criteria. The optimal allocation of LOP goals is attained by minimizing plant operating, design, or research costs. In quantifying goals early, before complete information is available, there is a danger in selecting objectives which are nonoptimal in terms of design or research costs. The alternative of having an unfocused program, however, is considered more perilous. The early identification and numerical quantification of program goals is therefore considered to be of paramount importance.

In accomplishing this allocation, it is important that realistic and demonstrable probability goals be assigned to each LOP. It is also important that the goals be optimal in terms of minimizing design or research costs. Unfortunately, the information by which trade-offs could be made to optimize these costs is not available at the present conceptual stage of the GCFR. Lacking such information, goals may be allocated on a basis consistent with that apparently achieved by commerical LWRs. This approach has the advantage of maximizing the applicability of relevant LWR operating experience.

Detailed considerations of LWR experience, including common cause failures, show that the achieved LWR system failure probability is typically in the range of 10^{-2} to 10^{-4}. Considering that for each LOP several systems must respond, a goal for LOP failure probabilities in the range of 10^{-1} to 10^{-3} appears to be realistic based upon current industry experience. Maintaining the LOP target failure probabilities within this range helps ensure that packages of work can be defined which have technically achievable probability goals, even allowing for common cause failures.

With the above in mind, as well as other considerations of maintaining some equivalence with LWR systems, Fig. 2 divides the risk envelope into individual probability and consequence targets for each LOP. The partitioning shown in this figure places a maximum reliance of 10^{-3} per demand in probability and a factor of 10^{-2} in consequence for each LOP. The combined goal of the first two LOPs, which include the systems traditionally provided to meet the design basis, is 10^{-4} per year. This target is consistent with the mean core melt frequency calculated in the LWR reactor safety study. The barriers provided in addition to the first two LOPs thus represent an accommodation of accidents traditionally beyond the design basis.

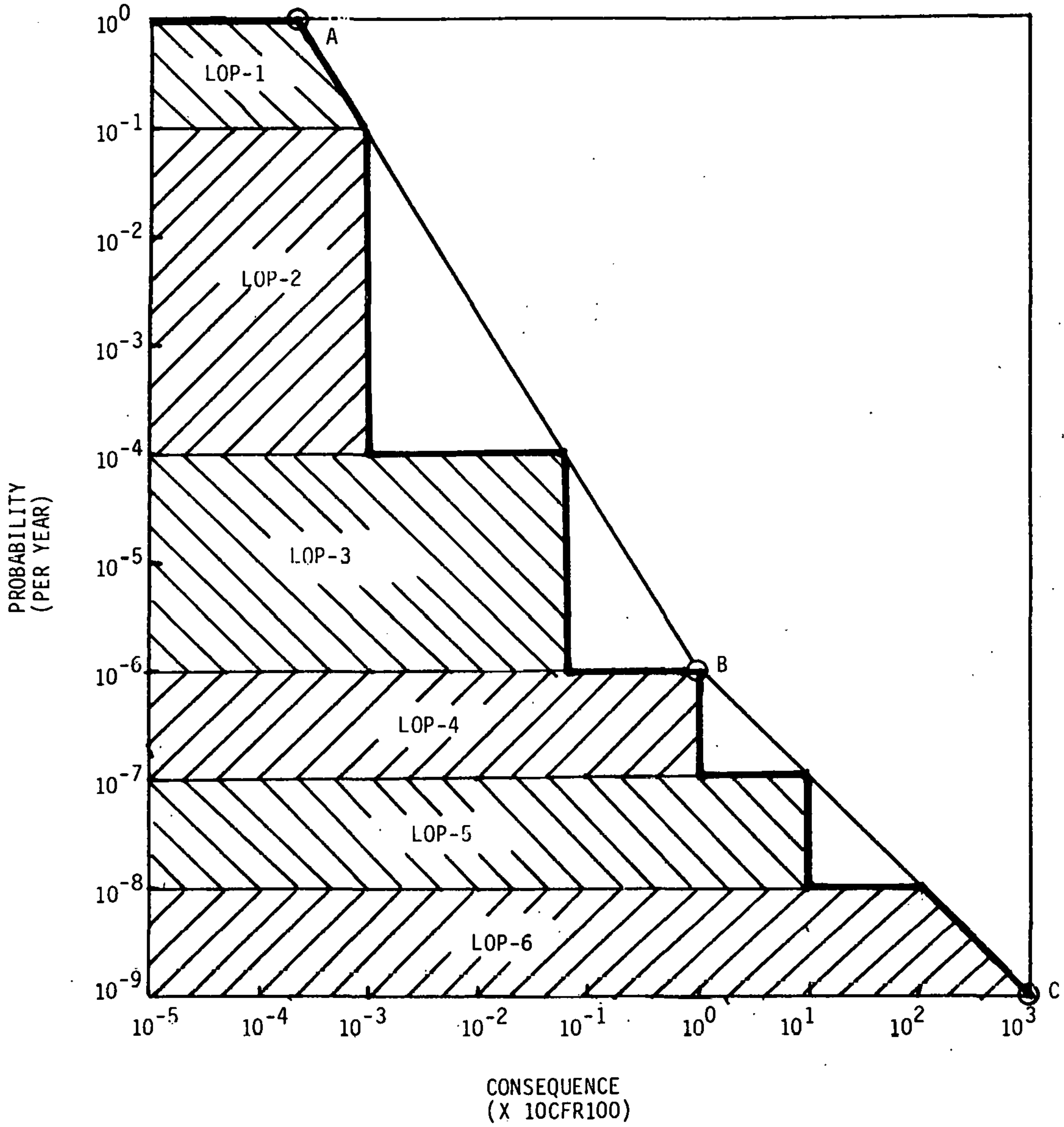

Fig. 2. LOP goal allocation

Furthermore, the consequence-aversion portion of the risk envelope is to be achieved by the LOPs for which the highest reliability can be achieved, namely LOPs 1 through 3, which include systems and features which prevent loss of coolable core geometry. Less stringent probability targets are assigned to LOPs 4 through 6, where the extreme complexity of core melt and core disassembly phenomena must be quantified.

Table 1 describes the resulting success criteria for each LOP. The public consequence criteria for each LOP are interpreted into success criteria for inherent and design features of the plant itself. At the higher frequency of events dealt with by LOPs 1 and 2, economic criteria are expected to be more limiting than the public consequence criteria; hence, the plant success criterion is concerned with limiting damage to plant equipment. Therefore, safety program emphasis in LOPs 1 and 2 will be to ensure that the reliability goals are met. At the lower LOPs, the public consequence criteria become limiting, and therefore the safety program must emphasize the attainment of both reliability and consequence goals. Notably, the success of any one of the first five barriers prevents significant harm to the public health and safety.

The success criteria defined for each LOP should not be considered unchangeable. The safety program will continue to optimize the allocation of risk criteria to the six LOPs.

STRUCTURE OF PLAN

To achieve the goals for the LOPs, the GCFR safety program plan has been organized into a WBS, of which the top two levels are shown in Fig. 3. The WBS is the hierarchial tree of products necessary for accomplishment of the program objectives. The structure is broken into three level-one products as follows:

1. Safety program integration. This task provides for the products necessary to ensure an efficient, economical, and cohesive safety

TABLE 1
LOP DEFINITIONS AND SUCCESS CRITERIA

LOP Barrier	Function	Probability	Plant Consequence	Public Consequence
1, operating systems	Shut down/cool down core following anticipated operational occurrences	$<10^{-1}$	Reoperable without extensive repair	Plant contributes less than 1% to background exposure (10CFR50, Appendix I)
2, dedicated safety systems	Shut down/cool down core in the event that the operating systems in LOP-1 fail	$<10^{-4}$	No lifetime reduction to permanent components	Exposure does not exceed a small fraction of natural background
3, inherent features	Shut down/cool down core in the event that the active systems in LOP-2 fail	$<10^{-6}$	No loss of core cooling geometry	Annual radiation worker exposure limit (10CFR20) not exceeded in any member of public
4, reactor vessel	Contain debris/energy release following core meltdown from failure of first three LOPs	$<10^{-7}$	No loss of liner or penetration integrity of vessel which could cause loss of containment integrity	No acute health effects (10CFR100); no significant latent effects
5, containment	Delay/control release of activity from LOP-4 failure	$<10^{-8}$	No unacceptable loss of containment leak-tight integrity	No acute fatalities
6, natural attenuation	Attenuate radiological consequences resulting from LOP-5 failure	$<10^{-9}$	No criteria for plant; possible site criteria	Maximum LWR consequences not exceeded

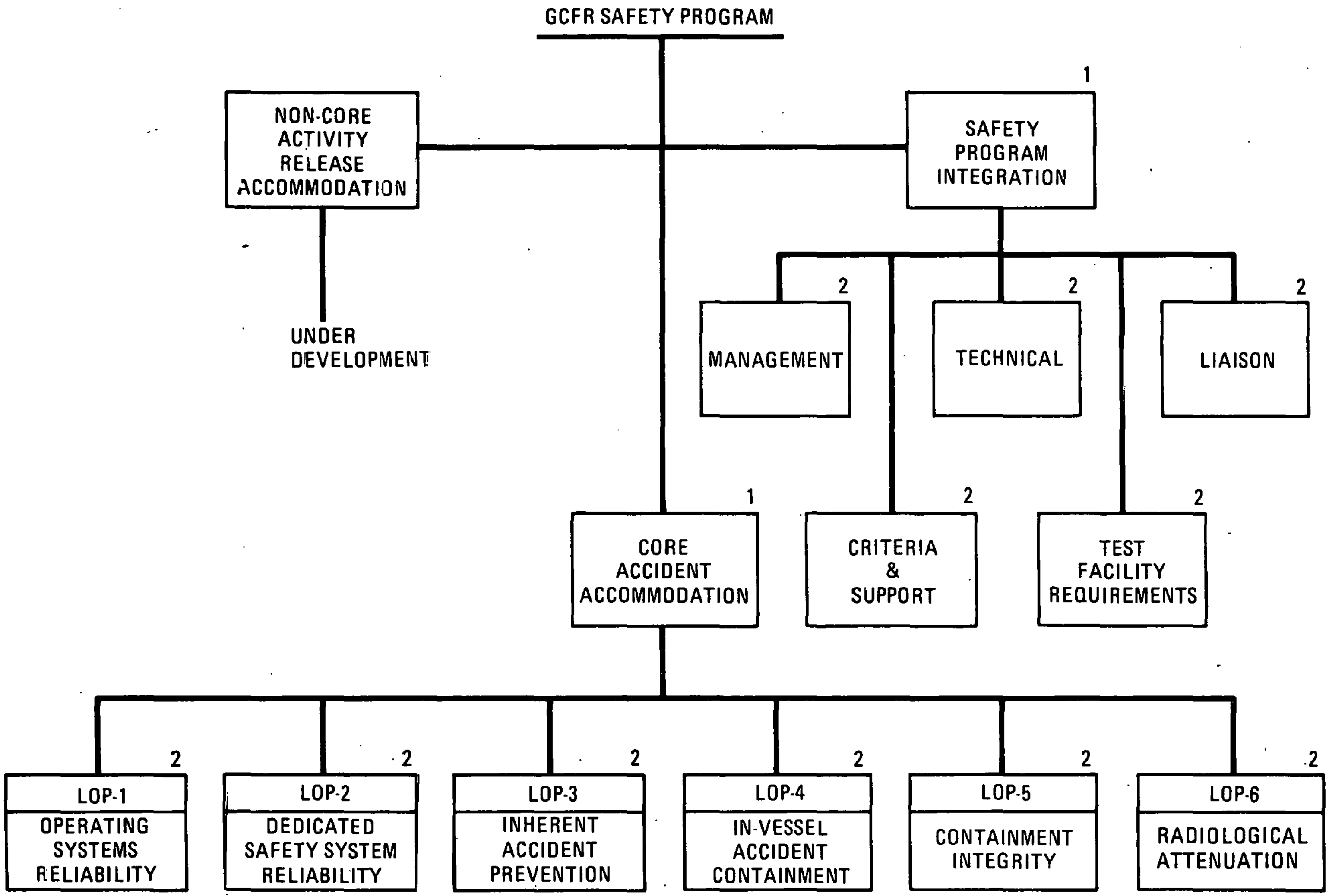

Fig. 3. GCFR work breakdown structure

program. The level two integration tasks provide for program management, criterion development, and project support functions; technical studies of reliability, risk, and accident sequences directed at defining and guiding the course of the overall safety program; preparation of integrated program test requirements and test plans; and liaison with other related nuclear safety research programs.

2. Noncore activity release accommodation. This task establishes design criteria for the nonreactor aspects of the GCFR plant to ensure that they do not pose excessive risks to the public health and safety. The nonreactor products provided by this task are exreactor fuel activity containment, pressure equalization processing system activity containment, radwaste systems activity containment, and circulating activity containment. Since the largest radioactivity inventory is within the reactor core, this paper will not discuss noncore activity release accommodation.

3. Core accident technology. This task develops the technology base necessary to ensure that each LOP provides an effective barrier against public risk. Since the goals of the safety program plan will primarily be met by developing the six LOPs, the remainder of this section will detail the WBS for each LOP.

Figure 4 presents the WBS for LOP-1, operating systems reliability. The WBS is organized to highlight the components and systems which comprise the operating systems. These include the primary cooling system, the plant control system, instrumentation systems, the reactor core, the reactor vessel and internal components, and support systems. The primary objective of the operating systems is to shut down and cool the reactor core following anticipated operational occurrences. The work packages for each level three task include the development of target reliability allocations, assessment of the reliability of design options, evaluation of the dynamic response of

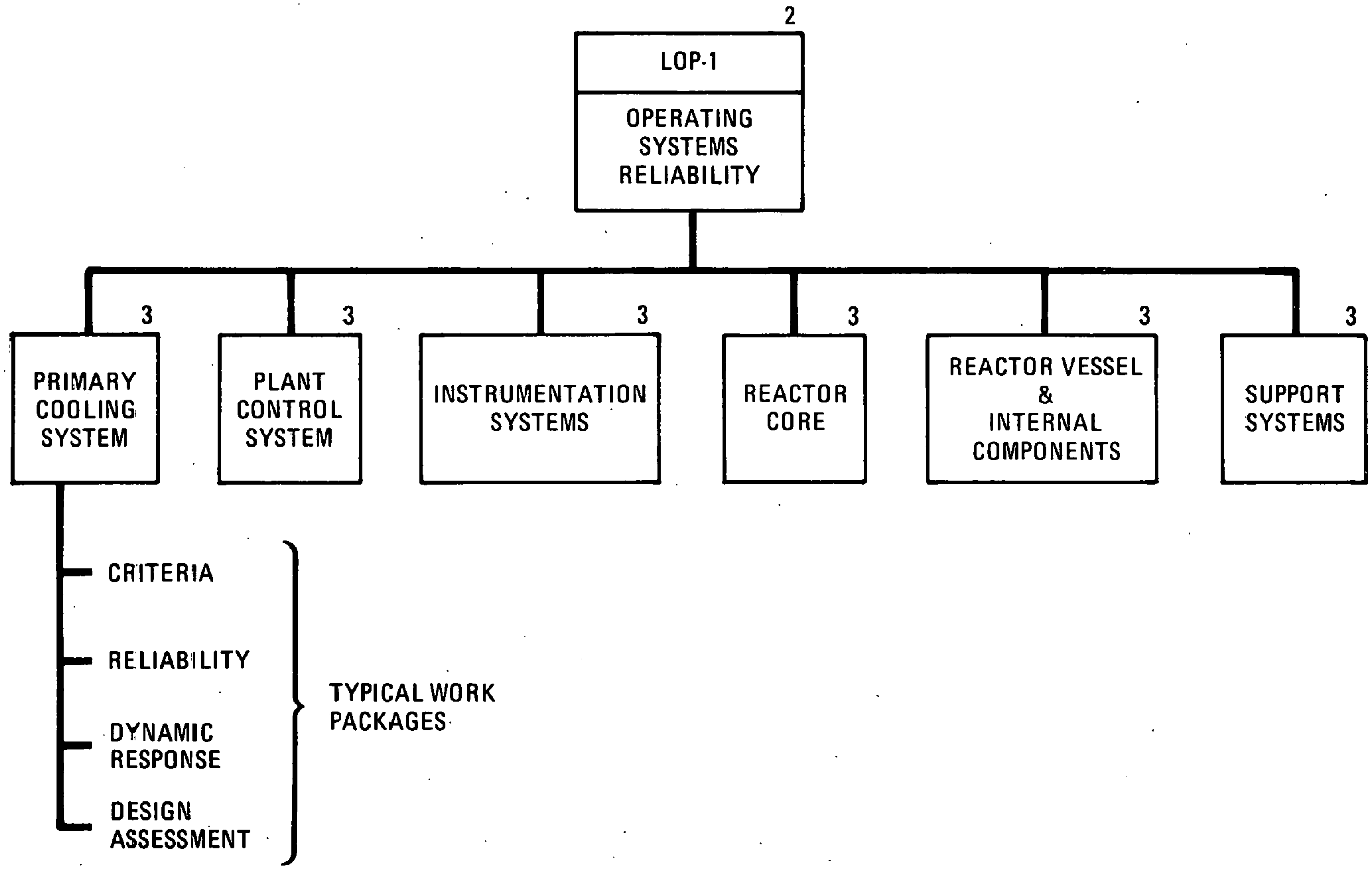

Fig. 4. Work breakdown structure for LOP-1

the system, and performance of a confirmatory design review of system reliability.

Figure 5 shows the WBS for LOP-2, dedicated safety systems reliability. The dedicated safety systems which constitute LOP-2 have historically provided a major barrier to the progression of accident sequences. For the GCFR, these systems are also assigned a major role in responding to and terminating accident sequences. The LOP-2 systems are the reactor shutdown systems, the plant protection system, and the CACS. The work packages for each level three task are similar to those described for LOP-1.

Figure 6 shows the WBS for LOP-3, inherent accident prevention. An accident prevention feature is defined as inherent if the safety-related function can be accomplished without dependence on active components and without the action of the plant protection system or the plant control system. The objective of the LOP-3 feature in concert with the LOP-2 and LOP-3 systems is to ensure that the cumulative frequency for loss of core cooling geometry is extremely low, i.e., less than 10^{-6} per reactor year. Inherent accident prevention features will be developed to protect against reactor shutdown system faults, pressurized shutdown heat removal system faults and depressurization, and local core fault propagation.

The remaining lines of protection, LOPs 4 through 6, are assigned the function of mitigating the consequences of low-probability accidents leading to loss of core cooling geometry in the unlikely event that they occur. Figure 7 presents the WBS for LOP-4, in-vessel accident containment. The level three tasks are organized to deal with the physical phenomena which may occur following a loss of core cooling geometry. These include quantifying the energetic and fuel vapor release from the core, evaluating the response of the primary vessel systems to the energetic and vapor loadings, developing means for in-vessel debris accommodation, and attenuating the activity release to the containment.

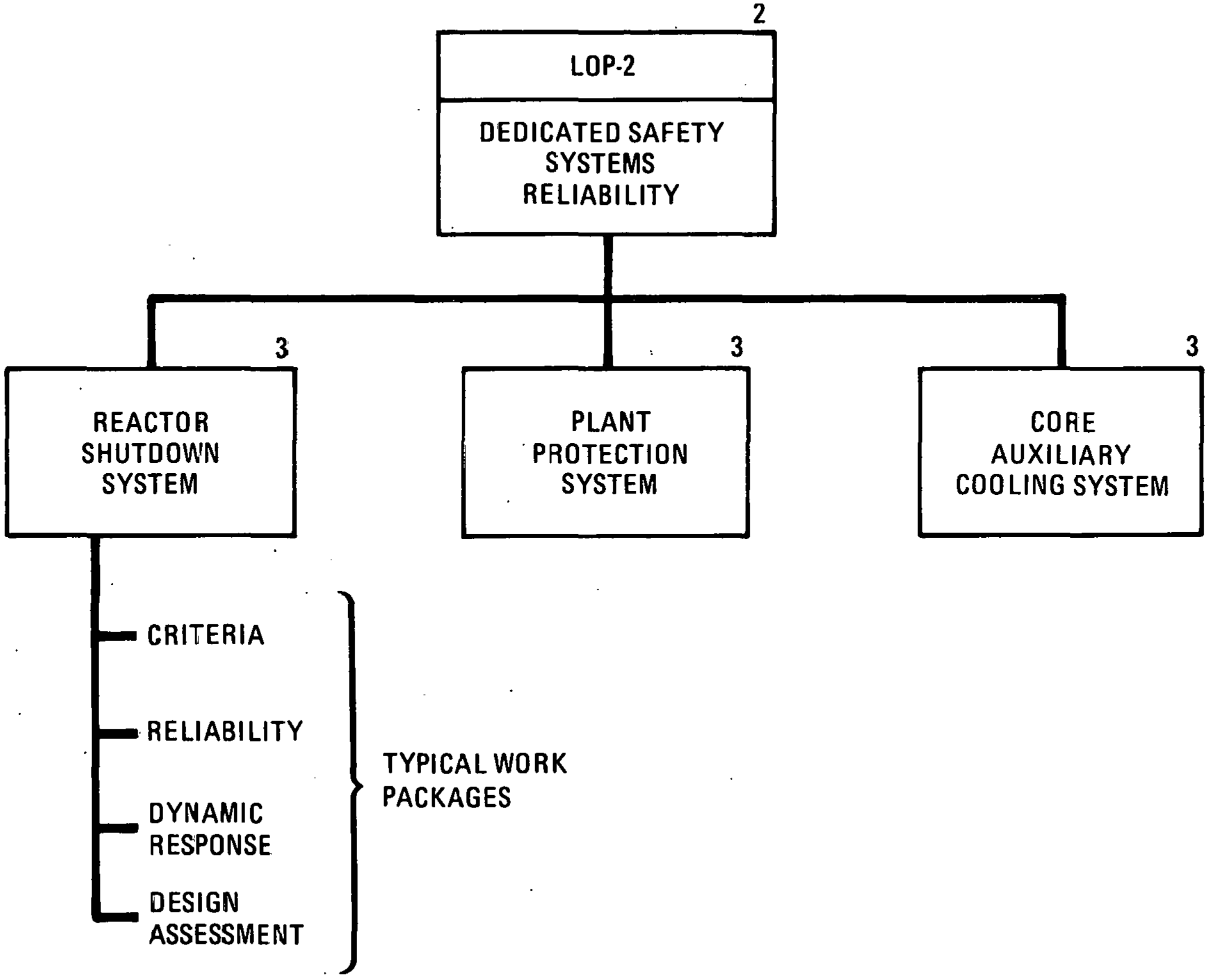

Fig. 5. Work breakdown structure for LOP-2

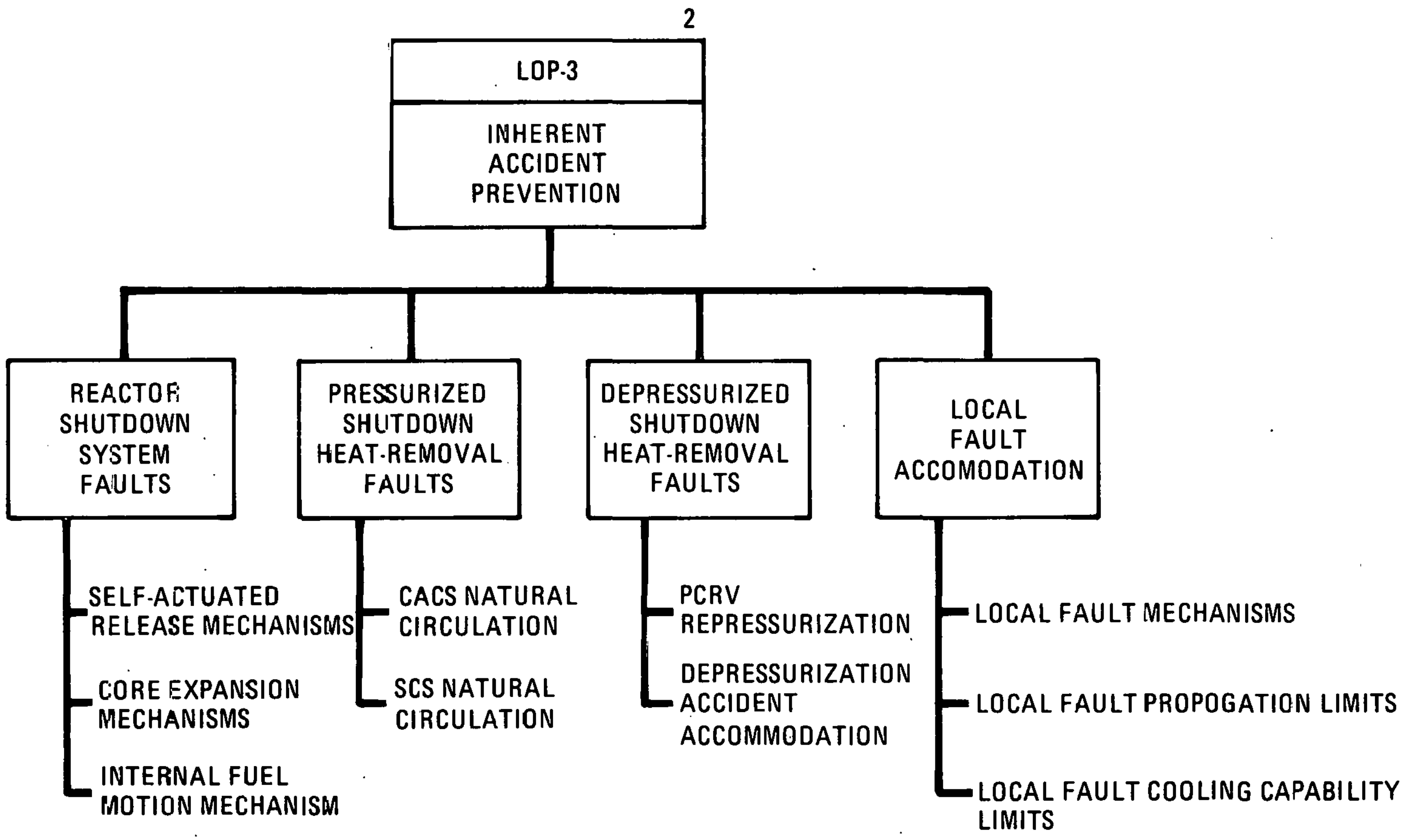

Fig. 6. Work breakdown structure for LOP-3

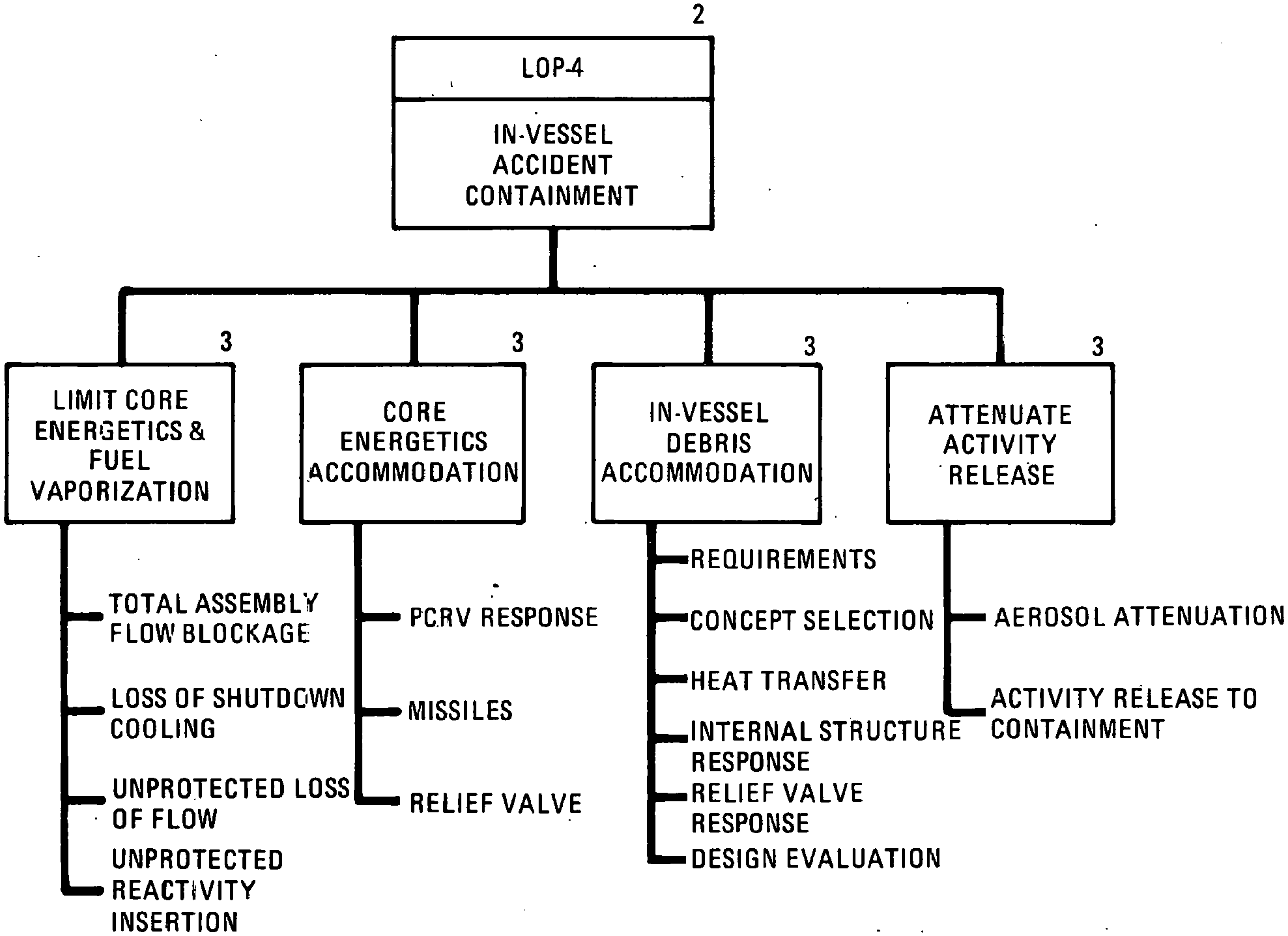

Fig. 7. Work breakdown structure for LOP-4

Figure 8 shows the WBS for LOP-5, containment integrity. Again, the level three tasks are organized to deal with the physical phenomena associated with the pressure, thermal, and missile loadings on the containment steel and base mat. The identified work packages serve to quantify the loadings, evaluate the response of the structures to these loadings, and identify optional approaches.

Figure 9 presents the WBS for LOP-6, radiological attenuation. The level three tasks identify and evaluate attenuation mechanisms for any radioactivity released from the containment and examine natural attenuation of releases as well as procedural approaches to public risk reduction.

A general cautionary note regarding the WBS is appropriate. Preparation of the revised GCFR safety program plan is still in progress. It is possible, therefore, that the structure of the plan as issued may differ somewhat from that presented here. At present, no major revisions to the WBS are envisioned.

PLAN IMPLEMENTATION

This section highlights the status of the GCFR safety program by identifying major ongoing research activities within the structure of the revised WBS. A number of GCFR activities not previously identified with the safety program will be briefly discussed. This extended list of activities is due to the inclusion of the accident prevention features of the plan (LOPs 1 through 3), which were not included in the original issue of the GCFR safety program plan.

Safety Program Implementation

The management activities which coordinate research activities within the safety program plan have been in existence since 1978. Extensive efforts have been made to ensure that safety-related criteria will be developed and licensing precedents considered. The criteria developed to

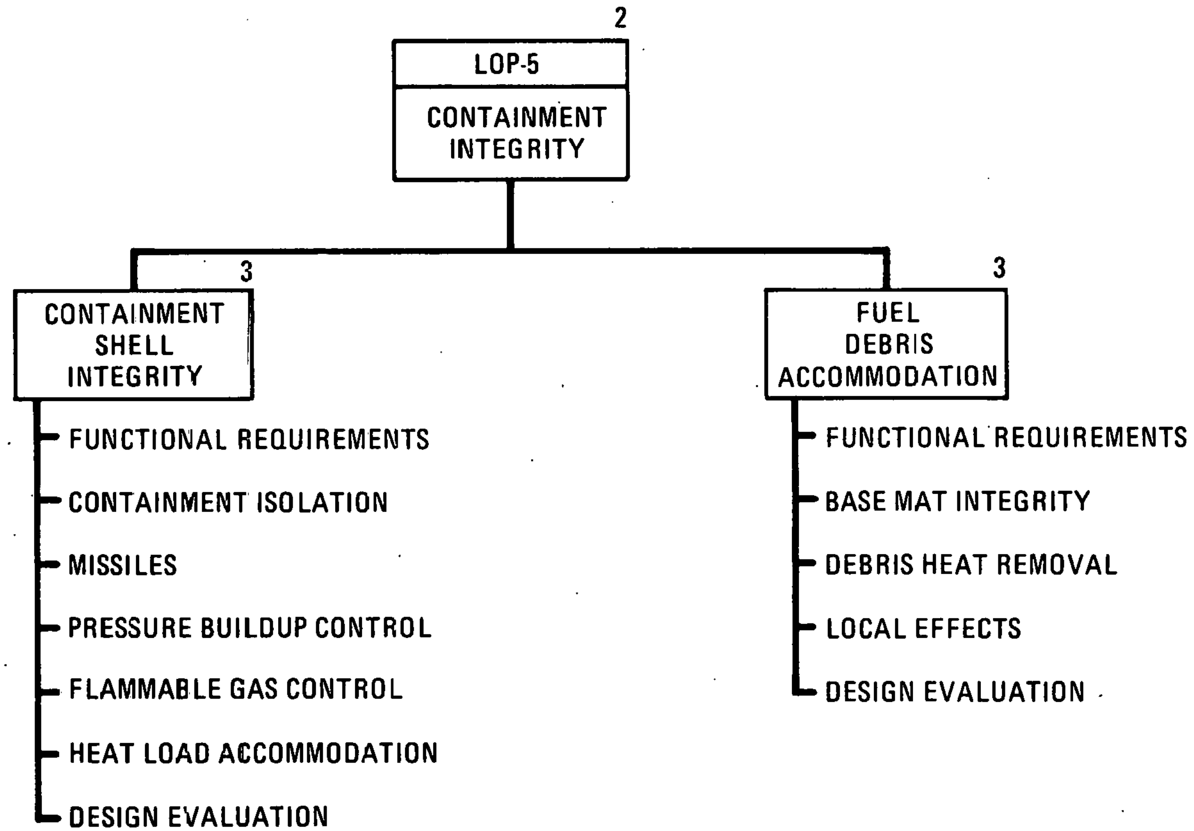

Fig. 8. Work breakdown structure for LOP-5

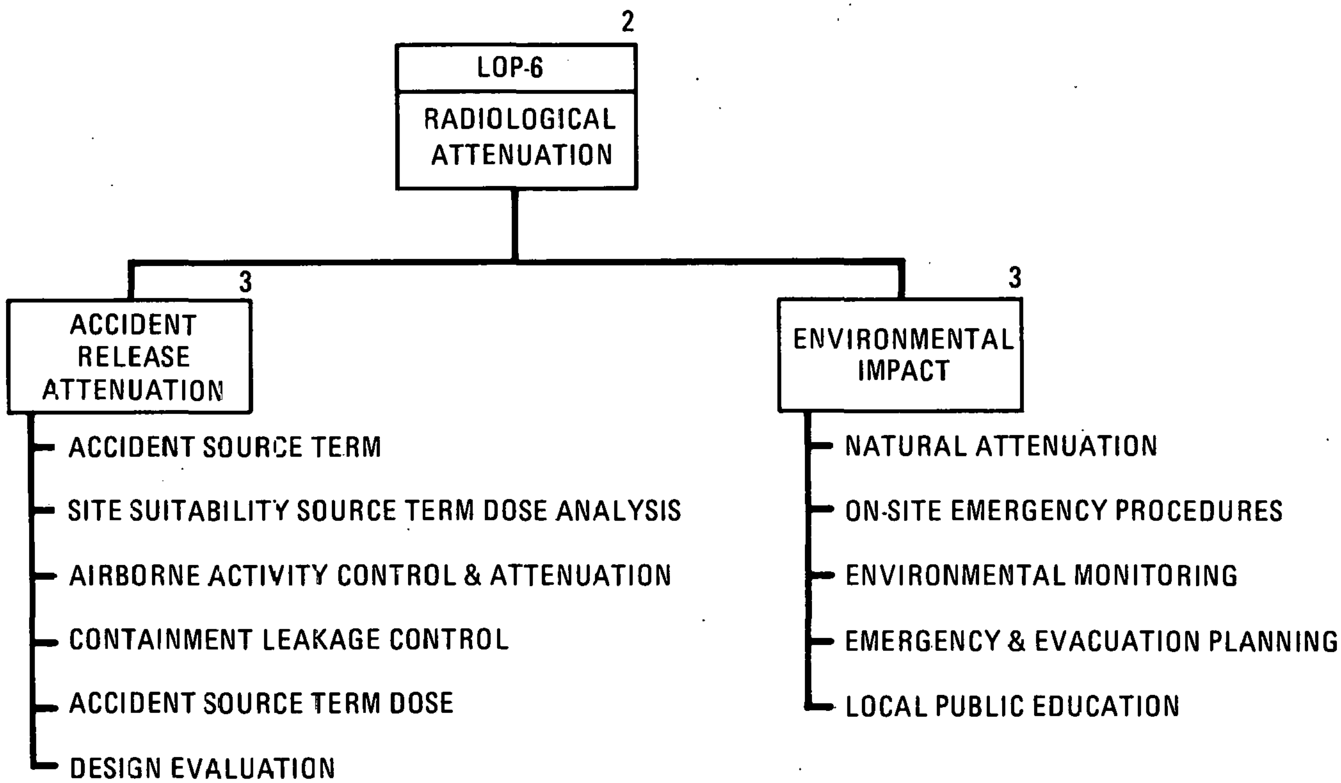

Fig. 9. Work breakdown structure for LOP-6

date include general design criteria for the GCFR, criteria for residual heat removal, shutdown system criteria, requirements for postaccident containment of a molten core, and requirements for integrating reliability considerations into the design of safety and operational systems. Test requirements have been established for a number of safety-related GCFR experiments. These include the core flow test loop (CFTL), the gas reactor in-pile safety test (GRIST-2), low-power safety experiments (LPSE), and direct electric heating (DEH) tests. Liaison activities with other reactor programs vary, with extensive high-temperature gas-cooled reactor (HTGR) interaction, moderate LMFBR liaison, and minimal LWR liaison. A major future task is the completion of risk assessment studies based on the GCFR design. The results will be used to guide the allocation of resources to the appropriate elements of the safety program.

LOP-1, Operating Systems Reliability

The tasks in this LOP generally receive a level of attention appropriate to the conceptual design phase of the program. Tentative reliability targets have been established and are being refined as needed. Design options and the reliability of the core cooling system are being assessed. Dynamic models of the systems have been developed and analysis performed as needed to support the conceptual design. Reliability assessments for the control, instrumentation, and support systems await the completion of the conceptual design.

LOP-2, Dedicated Safety Systems Reliability

The CACS is receiving a level of attention appropriate to the conceptual design phase of the program. Safety-related criteria and reliability targets have been established. CACS reliability has been evaluated, dynamic models have been developed, and analyses have been conducted as needed. An additional effort must be expended to bring the reactor shutdown and plant protection systems to the same point.

LOP-3, Inherent Accident Protection

The provision of inherent features for accident prevention is receiving additional attention. In March 1979, the program selected an upflow core option as the reference design. A major factor in this decision was the desire to provide natural circulation cooling in the CACS as an inherent feature for protection against pressurized shutdown heat removal faults. For similar reasons, a PCRV repressurization operation has been identified as protection against depressurized shutdown heat removal faults. Work has recently been initiated to examine inherent mechanisms which protect against reactor shutdown system faults. In the future, there should be an increased effort for LOP-3 activities, since each of the inherent features is recent.

LOP-4, In-Vessel Accident Containment

Two of the task areas in LOP-4 have been the primary focus of attention to date. Means of limiting core energetics and fuel vaporization have been examined for accident sequences with the potential for core disruption. A reappraisal of the work to date is under way to account for the design change to an upflow core. Several concepts for providing in-vessel debris accommodation have been identified and analyzed. The functional requirements for in-vessel debris retention have been prepared. Accommodation of the energetics resulting from a core disruptive accident will be the subject of scoping calculations during the remainder of FY-80. Little effort has been applied to attenuating activity releases to date. Activity release to the containment is currently taken as the value assigned to the Clinch River breeder reactor (CRBR) by the NRC.

LOP-5, Containment Integrity

Sufficient work has been completed to determine that the integrity of the containment shell will be maintained for at least 24 h. Among the specific phenomena considered were missile generation, pressure buildup of carbon dioxide and hydrogen, hydrogen combustion, and heat load accommodation. Work to examine fuel debris accommodation in the containment via scoping calculations is scheduled for the remainder of FY-80. The information generated from studies to date appears to be acceptable for the conceptual design phase.

LOP-6, Radiological Attenuation

Scoping calculations are in progress to examine accident release attenuation, including natural attenuation. Efforts to examine procedural approaches to public risk reduction have not been initiated.

GENERAL ATOMIC

GENERAL ATOMIC COMPANY
P. O. BOX 81608
SAN DIEGO, CALIFORNIA 92138