105/7/1/60/15
Dr. 1518
GA-A15697

UC-77

EVALUATION OF PROPOSED GERMAN SAFETY CRITERIA FOR HIGH-TEMPERATURE GAS-COOLED REACTORS

by
A. W. BARSELL

MASTER

Prepared under
Contract DE-AT03-76SF70046
for the San Francisco Operations Office
Department of Energy

DATE PUBLISHED: MAY 1980

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

GENERAL ATOMIC COMPANY

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency Thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

NOTICE

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use or the results of such use of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights.

Printed in the United States of America
Available from
National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Road
Springfield, Virginia 22161
Price: Printed Copy A05; Microfiche A01

**GA-A15697
UC-77**

EVALUATION OF PROPOSED GERMAN SAFETY CRITERIA FOR HIGH-TEMPERATURE GAS-COOLED REACTORS

DISCLAIMER

This book was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

**by
A. W. BARSELL**

**Prepared under
Contract DE-AT03-76SF70046
for the San Francisco Operations Office
Department of Energy**

**GENERAL ATOMIC PROJECT 6800
DATE PUBLISHED: MAY 1980**

GENERAL ATOMIC COMPANY

**THIS PAGE
WAS INTENTIONALLY
LEFT BLANK**

ABSTRACT

This report reviews proposed safety criteria prepared by the German Bundesministerium des Innern (BMI) for future licensing of gas-cooled high-temperature reactor (HTR) concepts in the Federal Republic of Germany. Comparison is made with U.S. General Design Criteria (GDCs) in 10CFR50 Appendix A and with German light water reactor (LWR) criteria. Implications for the HTR design relative to the U.S. design and safety approach are indicated. Both inherent characteristics and design features of the steam cycle, gas turbine, and process heat concepts are taken into account as well as generic design options such as a pebble bed or prismatic core. The scope and intent of the HTR criteria are consistent with those of U.S. GDCs except for several balance-of-plant criteria related to differences between U.S. and German safety philosophies. While the impact of the criteria themselves on the current U.S. HTR design approach is minimal, additional differences such as specific safety margins and degree of system redundancies may appear when HTR interpretations and regulatory standards are further developed in the two countries.

**THIS PAGE
WAS INTENTIONALLY
LEFT BLANK**

CONTENTS

ABSTRACT.	iii
1. INTRODUCTION.	1-1
References.	1-4
2. DEFINITIONS	2-1
3. CRITERIA SPECIFIC TO HTRs (GROUP III)	3-1
3.1. Testing	3-1
3.2. Reactor Coolant Boundary and PCRV	3-2
3.3. Core Design and Reactivity Control	3-4
3.4. Afterheat Removal.	3-6
3.5. Containment.	3-8
References	3-11
4. CRITERIA ANALOGOUS TO LWR (GROUP II).	4-1
4.1. Instrumentation and Control Room	4-1
4.2. Plant Protection System (PPS) and Electrical Supply.	4-2
4.3. Quality Assurance.	4-3
4.4. Health Physics and Radiation Monitoring.	4-4
4.5. Fuel Handling and Storage.	4-5
References	4-6
5. COMMON CRITERIA (GROUP I)	5-1
5.1. Plant Safety Principles.	5-1
5.2. External Influences.	5-1
5.3. Fire and Explosions.	5-2
5.4. Plant Security	5-3
5.5. Decommissioning.	5-3
5.6. Radiation Exposure	5-3
5.7. Emergency Exits and Communications	5-5
5.8. Ventilation and Air Filter Systems	5-5
References	5-6

6. SUMMARY AND IMPLICATIONS OF CRITERIA.	6-1
Reference	6-6
7. ACKNOWLEDGMENTS	7-1

APPENDICES

APPENDIX A: ENGLISH TRANSLATION OF BMI DRAFT OF FRG CRITERIA FOR HTRs	A-1
APPENDIX B: ENGLISH TRANSLATION OF BMI INTERPRETATION OF THE SINGLE FAILURE CONCEPT FOR SAFETY CRITERIA	B-1

FIGURES

1-5. Comparison of major written criteria and supporting standards in the U.S. and FRG	1-5
---	-----

TABLES

1-1. Comparison of Group III criteria for testing and primary coolant boundary	1-6
1-2. Comparison of Group III criteria for reactor core and control.	1-7
1-3. Comparison of Group III criteria for afterheat removal systems.	1-8
1-4. Comparison of Group III criteria for containment	1-9
1-5. Comparison of Group II criteria for instrumentation, control room, plant protection system, and electrical supply	1-10
1-6. Comparison of Group II criteria for quality assurance, health physics, radiation monitoring, and fuel handling and storage.	1-11
1-7. Comparison of Group I criteria for plant safety, external effects, fire, security, and decommissioning	1-12
1-8. Comparison of Group I criteria for radiation exposure, emergency plans, and ventilation systems	1-13
3-1. U.S. standards for testing	3-12
3-2. U.S. acceptance standards for pressure-bearing vessels (LWRs)	3-13
3-3. Acceptance standards for reactor core design and reactivity control.	3-14

TABLES (Continued)

3-4.	Containment acceptance standards in the U.S. and the FRG.	3-15
4-1.	U.S. and FRG acceptance standards for instrumentation and control room criteria.	4-7
4-2.	Comparison of U.S. and FRG acceptance standards for PPS and electrical power supply.	4-8
4-3.	Acceptance standards in U.S. for quality assurance	4-9
4-4.	German and U.S. acceptance standards for radiation monitoring	4-10
5-1.	Major U.S. and German acceptance standards for external events	5-8
5-2.	Fire protection standards in the FRG and U.S.	5-9
5-3.	Comparison of U.S. and German radiation exposure limits. .	5-10
5-4.	FRG and U.S. acceptance standards for radiation exposure and control.	5-11
5-5.	U.S. and German emergency planning standards	5-12
5-6.	German and U.S. acceptance standards for ventilation systems.	5-13

1. INTRODUCTION

All past licensing experience for gas-cooled high-temperature reactors (HTRs) in the U.S. (Ref. 1-1) and in the Federal Republic of Germany (FRG) has utilized existing safety criteria for light water reactors (LWRs). In the U.S., these criteria are given in 10CFR50 Appendix A, General Design Criteria, and in the FRG by the "Sicherheitskriterien für Kernkraftwerke" published by the Bundesministerium des Innern (BMI). A comparison of these two sets of safety criteria for LWRs has been made by Richardson (Ref. 1-2) and more recently in Appendix A of Ref. 1-3, although the latter focuses on the acceptance standards, that is, the licensing interpretation and implementation of the criteria, rather than on the criteria themselves. In general, the comparisons show that much less difference exists in the criteria than in the respective acceptance standards in the two countries.

A similar agreement is desired in the development of safety criteria specific to HTRs both in the U.S. and the FRG. An official draft of the German HTR safety criteria was prepared by the BMI, by supporting Technische Überwachungs Vereine (TÜV) agencies, and by the Gesellschaft für Reaktorsicherheit (GRS) for distribution to the FRG states and licensing experts in August 1979 (a description of the German licensing procedure and agencies can be found in Ref. 1-3). A licensing topical report (LTR) was issued by General Atomic Company (Ref. 1-4) in the U.S. requesting Nuclear Regulatory Commission (NRC) review of proposal changes to the General Design Criteria (GDCs) for HTR licensing criteria. The purpose of the present report is to review the German BMI draft HTR criteria, compare them with existing GDCs in the U.S., briefly describe the respective acceptance standards, and indicate implications of the new German criteria requirements for the HTR design.

An English translation of the BMI draft criteria is presented in Appendix A. Some very specific phraseology or expressions are used and are defined in the next section of this report. The criteria are reviewed in groups. Group I is for criteria independent of nuclear type. Group II is for HTR criteria analogous to LWR criteria but which may be changed in some way. Group III is for criteria specific to the HTR design and is therefore the most important group. A summary of the review is presented in Tables 1-1 through 1-8.*

The German safety criteria draft was prepared by GRS and Arbeitsgemeinschaft Kerntechnik West (ARGE) in cooperation with other state TÜVs, with some input from Hochtemperatur-Reaktorbau (HRB) and Kernforschungsanlage-Jülich (KFA). The bases of the draft were the safety evaluation report (SER) for the THTR-300, licensing experience with the HTR-1160 project, existing criteria outside of the FRG, and German LWR safety criteria published by the BMI in 1974 and updated in 1977. Insofar as possible, it was desired that the safety criteria be consistent with past HTR designs and with future concepts such as the HHT (gas turbine) and PNP (process heat) reactors and cover generic design options such as a pebble bed or prismatic core.

The BMI development of the HTR criteria has three objectives:

1. Difficulties in applying LWR criteria and Kerntechnische Ausschuss (KTA) regulations (analogous to regulatory guides in the U.S.) to HTRs should be resolved by developing specific HTR criteria.
2. The SERs for the THTR-300 and HTR-1160 and associated licensing experience should be generalized into formal regulations.

* Tables and figures appear at the end of each section.

3. Before construction of future HTRs, approved and accepted safety criteria should be developed for vendor planning and licensing standards.

It is intended that the BMI HTR criteria draft will be formalized into a final version analogous to the existing BMI criteria for LWRs (herein referred to as the German LWR criteria) after the German states and groups of nuclear experts, namely manufacturers, utilities, and consultants, have had an opportunity to express their expert opinion. While these criteria technically are not legally binding like the U.S. GDCs, they have significant force and de facto law behind them.

The structure of existing written criteria (for LWRs only) and acceptance standards (mostly for LWRs) in the U.S. and the FRG is presented in diagram form in Fig. 1-1. The criteria are general and take precedence over the acceptance standards, which consist of radiation, regulatory, and industry standards. In the FRG, the radiation protection ordinance, or Strahlenschutzverordnung (SSV), corresponds to radiation standards 10CFR50 and 10CFR100 in the U.S. Regulatory standards in the FRG consist of Reaktorsicherheits Kommission (RSK) guidelines and KTA regulations, which are analogous to U.S. regulatory guides (RGs) and standard review plans (SRPs) in that they present interpretations by licensing authorities of how the criteria and radiation ordinance can be satisfied. Often, these regulatory standards endorse or modify industry standards. Examples of such industry standards are:

FRG: AD-Merkblaetter
Unfallverhütungsvorschriften (UVV)
Deutsche Institut für Normung (DIN)

U.S.: American Society of Mechanical Engineers (ASME)
American National Standards Institute (ANSI)
Institute of Electrical and Electronics Engineers (IEEE)
American Society of Testing Materials (ASTM)

REFERENCES

- 1-1. Clark, R. A., and P. M. Williams, "Licensing Criteria for HTGRs in the United States," presented at the ANS Topical Meeting on Thermal Reactor Safety, Sun Valley, Idaho, July 31 through August 4, 1977.
- 1-2. Richardson, J. A., "Summary Comparison of West European and U.S. Licensing Regulations for LWRs," Nucl. Eng. Intern. 21, 32-41 (Feb. 1976).
- 1-3. "Gas Reactor International Cooperative Program Interim Report. United States/Federal Republic of Germany Nuclear Licensing Comparison," General Electric Report C00-4057-9, September 1978.
- 1-4. Orvis, D. D., and P. H. Raabe, "Licensing Topical Report: Interpretation of General Design Criteria for High-Temperature Gas-Cooled Reactors," DOE Report GA-A15255, General Atomic Company, January 1980.

Fig. 1-1. Comparison of major written criteria and supporting standards in the U.S. and FRG

TABLE 1-1
COMPARISON OF GROUP II CRITERIA FOR TESTING AND PRIMARY COOLANT BOUNDARY

TABLE 1-2
COMPARISON OF GROUP III CRITERIA FOR REACTOR CORE AND CONTROL

3.1 REACTOR CORE DESIGN

- DESIGN AND CONSTRUCT THE REACTOR CORE, COOLING SYSTEM, PPS AND REACTIVITY CONTROL SYSTEMS SO THAT FUEL AND PLANT SAFETY LIMITS ARE NOT EXCEEDED DURING PLANT LIFE.

3.2 COUPLING CHARACTERISTICS OF THE REACTOR CORE

- DESIGN REACTOR CORE SO THAT DAMAGE TO PRIMARY COOLANT SYSTEM DOES NOT OCCUR DUE TO REACTIVITY COUPLING PROPERTIES.

3.3 PCRV INTERNALS

- PCRV INTERNALS MUST BE SO CONSTRUCTED AND CONFIGURED THAT THEIR DESIGN VALUES ARE NOT EXCEEDED DURING PLANT OPERATION.
- THEY MUST ALSO BE SO CONSTRUCTED THAT THEIR JOB IN SHUTTING DOWN THE REACTOR AND REMOVING RESIDUAL HEAT IS NOT IMPAIRED AND DANGEROUS CONSEQUENCES SUCH AS REACTIVITY INCREASES ARE OBVIATED.

3.4 SYSTEMS FOR CONTROL AND SHUTDOWN OF THE REACTOR

- THE SYSTEMS FOR CONTROL AND SHUTDOWN OF THE REACTOR MUST BE CAPABLE OF CONTROLLING ALL REACTIVITY CHANGES SO THAT DESIGN LIMITS OF THE REACTOR ARE NOT EXCEEDED.
- EXCURSIONS MUST BE LIMITED SO THAT DESIGN LIMITS ARE MAINTAINED EVEN FOR A CONTROL FAILURE.
- ONE SHUTDOWN SYSTEM MUST BE CAPABLE OF COMPENSATING REACTIVITY CHANGES WITH MARGIN AND SHUTTING DOWN FOR A SUFFICIENT TIME EVEN WITH A SINGLE FAILURE.
- A SECOND SHUTDOWN SYSTEM MUST BE PROVIDED OF INDEPENDENT AND DIVERSE CONSTRUCTION.
- THE SECOND SHUTDOWN SYSTEM MUST BE CAPABLE OF SHUTTING DOWN AND MAINTAINING COLD SHUTDOWN WITH APPROPRIATE MARGIN.
- INHERENT CHARACTERISTICS OF THE REACTOR CORE MAY BE USED IN PLACE OF HARDWARE FOR SHUTDOWN.
- IF THE TWO SHUTDOWN SYSTEMS POSSESS COMMON COMPONENTS, IT MUST BE ASSURED THAT FAILURE IN THE FIRST SYSTEM DOES NOT IMPAIR SAFE SHUTDOWN BY SECOND SYSTEM.

GDC-10 REACTOR DESIGN

- DESIGN THE REACTOR CORE, COOLANT, CONTROL AND PPS SYSTEMS WITH APPROPRIATE MARGIN SO THAT FUEL DESIGN LIMITS ARE MAINTAINED DURING PLANT OPERATION AND OCCURRENCES.

GDC-11 REACTOR INHERENT PROTECTION

- DESIGN CORE AND COOLING SYSTEMS SO THAT PROMPT INHERENT NUCLEAR FEEDBACK TENDS TO COMPENSATE FOR RAPID REACTIVITY RISES.

NO
EQUIVALENT
GDC

GDC-26 REACTIVITY CONTROL SYSTEM REDUNDANCY AND CAPABILITY

- PROVIDE TWO INDEPENDENT REACTIVITY CONTROL SYSTEMS OF DIFFERENT DESIGN PRINCIPLES.
- ONE SYSTEM SHALL USE CONTROL RODS FOR REACTIVITY CONTROL DURING OPERATION WITH MARGIN TO ASSURE FUEL DESIGN LIMITS NOT EXCEEDED.
- SECOND SYSTEM SHALL CONTROL RATE OF REACTIVITY CHANGES FROM NORMAL POWER CHANGES TO ASSURE FUEL DESIGN LIMITS NOT EXCEEDED.
- ONE SYSTEM SHALL BE CAPABLE OF HOLDING CORE COLO SUBCRITICAL.

GDC-12 SUPPRESSION OF REACTOR POWER OSCILLATIONS

- DESIGN REACTOR SYSTEMS TO SUPPRESS POWER OSCILLATIONS WHICH CAN RESULT IN EXCEEDING FUEL DESIGN LIMITS.

GDC-28 REACTIVITY LIMITS

- DESIGN REACTIVITY CONTROL SYSTEMS TO LIMIT AMOUNT AND RATE OF REACTIVITY INCREASE TO ASSURE EFFECTS OF ACCIDENTS CAN NEITHER RESULT IN PCRV DAMAGE NOR IMPAIR CORE COOLING BY DISTURBING CORE, SUPPORT STRUCTURES, OR OTHER PCRV INTERNALS.

GDC-29 PROTECTION AGAINST OPERATIONAL OCCURRENCES

- DESIGN OF PROTECTION AND CONTROL SYSTEMS MUST ASSURE HIGH PROBABILITY OF ACCOMPLISHING SAFETY FUNCTIONS IN THE EVENT OF ANTICIPATED OPERATIONAL OCCURRENCES.

GDC-27 COMBINED REACTIVITY CONTROL SYSTEMS CAPABILITY

- DESIGN REACTIVITY CONTROL SYSTEMS WITH COMBINED CAPACITY TO CONTROL REACTIVITY CHANGES WITH MARGIN FOR STUCK RODS UNDER ACCIDENT CONDITIONS SO THAT CORE COOLING IS MAINTAINED.

TABLE 1-3
COMPARISON OF GROUP III CRITERIA FOR AFTERHEAT REMOVAL SYSTEMS

5.1 AFTERHEAT REMOVAL -
NORMAL OPERATIONS

- PROVIDE A RELIABLE AND REDUNDANT AFTERHEAT REMOVAL SYSTEM DURING NORMAL SHUTDOWNS.
- CONSTRUCT THE SYSTEM SUCH THAT FUEL DESIGN AND ACTIVITY RELEASE LIMITS ARE NOT EXCEEDED DURING PLANT LIFE.
- THE ACCIDENT AFTERHEAT REMOVAL SYSTEM CAN BE USED TO FULFILL THE REDUNDANCY REQUIREMENT.

5.2 AFTERHEAT REMOVAL SYSTEM - ACCIDENTS

- PROVIDE A RELIABLE AND REDUNDANT AFTERHEAT REMOVAL SYSTEM FOR ACCIDENTS.
- THE SYSTEM MUST BE CAPABLE OF FULFILLING ITS FUNCTION FOR SINGLE FAILURES WITHIN SPECIFICATION OF THE SINGLE FAILURE CONCEPT.
- THE N-2 FAILURE CRITERION MAY BE MODIFIED IF THE ACCEPTABILITY OF TIME DELAYS IN AFTERHEAT REMOVAL CAN BE DEMONSTRATED ON BASIS OF INHERENT DESIGN CHARACTERISTICS.
- DESIGN OF AFTERHEAT REMOVAL SYSTEM, ALONG WITH ACTIVITY BARRIERS AND SHUTDOWN SYSTEMS, MUST CONSIDER FREQUENCIES OF ACCIDENTS AND POSSIBLE INGRESS OF ALIEN SUBSTANCES AND POTENTIAL CHEMICAL REACTIONS.
- DESIGN OF AFTERHEAT REMOVAL MUST CONSIDER PRIMARY COOLANT DEPRESSURIZATION WITH EITHER ATMOSPHERIC OR WORST CASE EQUILIBRIUM CONTAINMENT BACK-PRESSURE WITH MAXIMUM CONTAINMENT LEAKAGE AND APPROPRIATE MARGIN.
- THE TWO AFTERHEAT REMOVAL SYSTEMS MAY POSSESS COMMON COMPONENTS WHEN THE OPERATION READINESS FOR ACCIDENTS IS NOT IMPAIRED AND CAN BE MONITORED AND WHEN THE COMPONENTS POSSESS THE REQUIRED RELIABILITY.
- IF INHERENT CHARACTERISTICS CAN ASSURE AFTERHEAT REMOVAL AFTER ACCIDENTS SO THAT DESIGN LIMITS ARE NOT EXCEEDED, HARDWARE REQUIREMENTS CAN BE SOFTENED.

NO EQUIVALENT
(LOSS OF COOLANT)
HTR CRITERION

GDC-34 AFTERHEAT REMOVAL

- A SYSTEM TO REMOVE RESIDUAL HEAT SHALL BE PROVIDED.
- SAFETY FUNCTION SHALL BE TO TRANSFER DECAY HEAT FROM THE CORE AT A RATE SUCH THAT FUEL DESIGN LIMITS AND RCB DESIGN CONDITIONS ARE NOT EXCEEDED.
- SUITABLE REDUNDANCY SHALL BE PROVIDED IN COMPONENTS, FEATURES, INTERCONNECTIONS, LEAK DETECTION AND ISOLATION CAPABILITIES, ASSUMING A SINGLE FAILURE AND LOSS OF EITHER ON-SITE OR OFF-SITE POWER.

GDC-35 EMERGENCY CORE COOLING SYSTEM (ECCS)

- PROVIDE A SYSTEM FOR EMERGENCY CORE COOLING AFTER ANY LOSS OF PRIMARY COOLANT SUCH THAT FUEL AND CLADDING DESIGN LIMITS NOT EXCEEDED.
- PROVIDE REDUNDANCY IN COMPONENTS, FEATURES, INTERCONNECTIONS, LEAK DETECTION, ISOLATION, AND CONTAINMENT SUCH THAT SAFETY FUNCTION CAN BE ACHIEVED, WITH A SINGLE FAILURE.

GDC-36 INSPECTION OF ECCS

- DESIGN ECCS TO PERMIT PERIODIC INSPECTION OF IMPORTANT COMPONENTS.

GDC-37 TESTING OF ECCS

- DESIGN ECCS TO PERMIT APPROPRIATE PERIODIC PRESSURE AND FUNCTIONAL TESTING.

TABLE 14
COMPARISON OF GROUP III CRITERIA FOR CONTAINMENT

TABLE 1-5
COMPARISON OF GROUP II CRITERIA FOR INSTRUMENTATION, CONTROL ROOM, PPS, AND ELECTRICAL SUPPLY

6.3 OPERATION INSTRUMENTATION

- PROVIDE EQUIPMENT FOR CONTROL, MONITORING AND SIGNALING DURING PLANT OPERATION.
- ALL SAFETY CONDITIONS MUST BE RECORDED BY THIS EQUIPMENT.
- EMERGENCY SIGNALS MUST BE PROVIDED.

6.2 ACCIDENT INSTRUMENTATION

- PROVIDE ACCIDENT EQUIPMENT WHICH RECORDS CONDITIONS AND DATA BEFORE, DURING AND AFTER AN ACCIDENT.
- DOCUMENT SAME IN TIME SEQUENCE.
- PROVIDE UNINTERRUPTABLE POWER SOURCE.
- INCLUDE INSTRUMENTS OUTSIDE THE PLANT (WEATHER DATA).
- DIVIDE INSTRUMENTS INTO "EVENT" AND "CONSEQUENCE" CATEGORIES.
- PROVIDE REDUNDANT "EVENT" INSTRUMENTS FOR CONTINUOUS RECORDING AND DOCUMENTATION DURING ACCIDENTS.
- PROVIDE "CONSEQUENCE" INSTRUMENTS FOR CONTROL ROOM DATA DISPLAY AND DOCUMENTATION (REDUNDANCY NOT REQUIRED).
- FOR EXTERNAL INFLUENCES, PROVIDE INSTRUMENTS FOR DATA RECORDING AND DISPLAY IN A PROTECTED EMERGENCY CONTROL STATION.

6.4 CONTROL ROOM AND EMERGENCY CONTROL STATION

- PROVIDE A CONTROL ROOM FOR MAINTAINING SAFETY PLANT OPERATION.
- PERSONNEL MUST BE ABLE TO ENTER AND LEAVE DURING ACCIDENTS.
- OPERATION OF SAFETY AND REACTIVITY SYSTEMS MUST STEM FROM CONTROL ROOM.
- FOR FAILURE OF CONTROL ROOM EQUIPMENT, REACTOR IS TO BE SHUT DOWN, COOLED AND CONTROLLED FROM AN EMERGENCY CONTROL STATION.
- CONTROL ROOM AND EMERGENCY STATION MUST BE SPATIALLY SEPARATE, INDEPENDENTLY SUPPLIED WITH ELECTRICITY AND PROTECTED FROM EXTERNAL EVENTS.

6.1 PLANT PROTECTION SYSTEM (PPS)

- PROVIDE A PPS WHICH CAN FULFILL ITS SAFETY FUNCTION DURING ACCIDENTS WITH MAINTENANCE PLUS SINGLE FAILURE CRITERIA.
- TWO ACTIVATION CRITERIA MUST BE AVAILABLE OR THE SINGLE ACTIVATION MUST POSSESS A HIGHER LEVEL OF SAFETY.
- IN GENERAL, THE PPS MUST BE SEPARATE FROM THE PLANT CONTROL SYSTEM (PCS).
- REDUNDANT PARTS OF PPS MUST POSSESS INDEPENDENT EQUIPMENT AND BE SPATIALLY SEPARATE.
- FAILURES WITHIN PPS MUST NOT CAUSE ANY ACTION WHICH COULD PUT REACTOR IN DANGEROUS CONDITION.
- PPS MUST ALWAYS BE IN A STATE OF READINESS WHEN FUEL OR RADIOACTIVE MATERIAL IS IN THE PLANT.

7.1 ELECTRICAL SUPPLY

- PROVIDE TWO FEEDLINE CONNECTIONS TO THE ELECTRICAL SUPPLY NETWORK, ONE TO THE MAIN GENERATOR, OTHER TO AN EMERGENCY SYSTEM.
- RELIABILITY OF ELECTRICAL SUPPLY MUST CORRESPOND TO THE RELIABILITY OF THE SYSTEM PROVIDED FOR.
- ELECTRICAL SUPPLY TO SAFETY SYSTEMS MUST HAVE INDEPENDENT, SPATIALLY SEPARATE, REDUNDANT EMERGENCY GENERATORS, SUPPLY LINES AND DISTRIBUTORS TO FULFILL SAFETY FUNCTION DURING ACCIDENTS WITH MAINTENANCE PLUS SINGLE FAILURE CRITERIA.
- REDUNDANCY OF EMERGENCY POWER MUST CORRESPOND TO THE REDUNDANCY OF THE MECHANICAL SYSTEM PROVIDED FOR.
- TIME PERIOD OF EMERGENCY POWER GENERATORS OPERATION MUST BE LONG ENOUGH TO ALLOW RESTORATION OF OTHER ELECTRICAL POWER SOURCES.

GDC-13 INSTRUMENTATION AND CONTROL

- PROVIDE INSTRUMENTATION TO MONITOR VARIABLES AND SYSTEMS IMPORTANT TO SAFETY DURING PLANT OPERATION.
- PROVIDE APPROPRIATE CONTROLS TO MAINTAIN VARIABLES AND SYSTEMS WITHIN PRESCRIBED RANGES.

GDC-19 CONTROL ROOM

- PROVIDE A CONTROL ROOM WHERE ACTIONS CAN BE TAKEN FOR OPERATION AND ACCIDENTS, INCLUDING LOC ACCIDENTS.
- PROVIDE SHIELDING FOR ACCESS AND OCCUPANCY DURING ACCIDENTS.
- PROVIDE EQUIPMENT TO SHUT DOWN REACTOR FROM CONTROL ROOM.

GDC-20 PPS FUNCTIONS

- PPS MUST INITIATE OPERATION OF SYSTEMS TO MAINTAIN FUEL DESIGN LIMITS.
- PPS MUST SENSE ACCIDENT CONDITIONS AND INITIATE SAFETY SYSTEM ACTION.

GDC-21 PPS RELIABILITY AND TESTABILITY

- PROVIDE RELIABILITY OF PPS COMPONENTS AS BEFITS THEIR SAFETY IMPORTANCE.
- REDUNDANCY AND INDEPENDENCE MUST BE SINGLE FAILURE PROOF.
- ALLOW FOR PERIODIC IN-SERVICE TESTING.

GDC-22 PPS INDEPENDENCE

- ASSURE PPS FUNCTION DURING OPERATION, TESTING, MAINTENANCE AND INTERNAL AND EXTERNAL ACCIDENTS.
- DIVERSITY OF DESIGN TO EXTENT PRACTICAL.

GDC-23 PPS FAILURE MODES

- PPS MUST BE A "FAIL SAFE" SYSTEM.

GDC-24 SEPARATION OF PPS AND PCS

- SEPARATE PPS FROM PCS SUCH THAT FAILURE IN PCS DOES NOT IMPAIR FUNCTION OF PPS.

GDC-25 REQUIREMENT FOR REACTIVITY CONTROL

- DESIGN PPS SO THAT FUEL LIMITS NOT EXCEEDED FOR SINGLE FAILURE IN REACTIVITY CONTROL SYSTEM.

GDC-17 ELECTRIC POWER SYSTEMS

- PROVIDE ON-SITE AND OFF-SITE ELECTRICAL POWER TO SYSTEMS AND COMPONENTS IMPORTANT TO SAFETY.
- ELECTRICAL SYSTEMS MUST ASSURE FUEL AND RCS LIMITS NOT EXCEEDED IN OPERATION AND CORE IS COOLED AND CONTAINMENT INTEGRITY IS MAINTAINED DURING ACCIDENTS.
- ON-SITE POWER SUPPLY MUST BE INDEPENDENT, REDUNDANT AND TESTABLE TO PERFORM FUNCTION WITH A SINGLE FAILURE.
- TRANSMISSION LINES MUST HAVE TWO INDEPENDENT CIRCUITS TO PRECLUDE SIMULTANEOUS FAILURE DURING ACCIDENTS (COMMON SWITCHYARD IS ACCEPTABLE).
- EACH OF THESE CIRCUITS MUST BE TIMELY AVAILABLE AFTER LOSS OF ON-SITE POWER TO MAINTAIN FUEL AND RCS DESIGN LIMITS.
- ONE OF THESE CIRCUITS MUST BE AVAILABLE WITHIN SECONDS AFTER LOC ACCIDENT TO ASSURE CORE COOLING, CONTAINMENT INTEGRITY AND OTHER SAFETY FUNCTIONS.
- MINIMIZE PROBABILITY OF LOSING ELECTRIC POWER FROM THE REMAINING SUPPLIES AS RESULT OF OR COINCIDENT WITH LOSS OF POWER.

GDC-18 INSPECTION AND TESTING OF ELECTRIC POWER SYSTEMS

- ALLOW FOR PERIODIC INSPECTION AND TESTING OF ELECTRIC POWER SYSTEMS IMPORTANT TO SAFETY.
- TEST OPERABILITY AND FUNCTIONABILITY OF COMPONENTS AND SYSTEMS AS A WHOLE UNDER SIMULATED DESIGN BASIS CONDITIONS.

TABLE 1-6
COMPARISON OF GROUP II CRITERIA FOR QA, HEALTH PHYSICS, RADIATION MONITORING AND FUEL HANDLING AND STORAGE

<p>2.1 QUALITY ASSURANCE</p> <ul style="list-style-type: none"> • QUALITY OF COMPONENTS AND SYSTEMS IS TO BE ASSURED AS BEFITS SAFETY IMPORTANCE. • GUIDELINES AND PROCEDURES ARE TO BE FOLLOWED IN KEEPING WITH SPECIAL REQUIREMENTS OF SAFETY OF NUCLEAR POWER PLANTS. 	<p>2.5 HEALTH PHYSICS</p> <ul style="list-style-type: none"> ○ PROVIDE WORKING CONDITIONS AND ENVIRONMENT CONDUCTIVE WITH SAFETY OF PLANT PERSONNEL. 	<p>10.1 RADIATION MONITORING</p> <ul style="list-style-type: none"> • PROVIDE MEANS OF MONITORING RADIATION DURING PLANT OPERATION AND ACCIDENTS FOR CONFORMANCE WITH FEDERAL GUIDELINES. ○ PROVIDE STATIONARY DEVICES FOR MEASURING SITE DOSES, AND ACTIVITY IN BUILDING ATMOSPHERES AND INTERNAL CIRCUITS. ○ OUTPUT OF STATIONARY DEVICES MUST BE RECORDED AND DISPLAYED IN THE CONTROL ROOM AND AT THE EXTERNAL LOCATION. ○ PROVIDE PORTABLE DEVICES FOR MEASURING SITE DOSES AND CONCENTRATION AND TYPE OF RADIOACTIVITY IN AIR AND WATER. ○ PROVIDE EQUIPMENT FOR MEASURING DOSES TO PERSONNEL AS WELL AS CONTAMINATION OF OBJECTS AND PERSONS. ○ PROVIDE SUITABLE LAB APPARATUS FOR EVALUATION OF RADIOACTIVITY PROBES. 	<p>10.2 ACTIVITY MONITORING IN EXHAUST AIR AND WATER</p> <ul style="list-style-type: none"> • PROVIDE FOR IDENTIFYING, MEASURING, RECORDING, AND IF NECESSARY LIMITING RADIOACTIVITY IN EXHAUST AIR AND WASTE WATER. • PROVIDE STATIONARY DEVICES TO MONITOR AND RECORD CONTINUOUSLY LIQUID, GASEOUS AND AEROSOL ACTIVITY RELEASE DURING PLANT OPERATION. ○ PROVIDE EQUIPMENT TO MEASURE AND RECORD LIQUID, GASEOUS AND AEROSOL RELEASE DURING ACCIDENTS FOR EVALUATION OF ENVIRONMENTAL EFFECTS. ○ MEASURED VALUES MUST BE INDICATED ON THE EQUIPMENT AND DISPLAYED AND RECORDED IN THE CONTROL ROOM. 	<p>11.1 FUEL HANDLING AND STORAGE</p> <ul style="list-style-type: none"> • PROVIDE EQUIPMENT TO ASSURE SAFE HANDLING AND STORAGE OF RADIOACTIVE MATERIAL. • DESIGN AND ARRANGE EQUIPMENT TO PRECLUDE CRITICALITY ACCIDENTS AND EXPOSURE TO PERSONNEL AND ENVIRONMENT IN EXCESS OF FEDERAL LIMITS. ○ FUEL HANDLING EQUIPMENT MUST ASSURE CORRECT POSITIONING OF FUEL IN CORE. • PRECLUDE BY SUITABLE MEASURES UNALLOWABLE RELEASE OF ACTIVITY DURING HANDLING OF IRRADIATED FUEL DURING PLANT OPERATIONS AND ACCIDENTS. • PROVIDE SUFFICIENT STORAGE CAPACITY OF IRRADIATED FUEL. • ASSURE AFTERHEAT REMOVAL IN THE STORAGE FACILITY DURING PLANT OPERATION AND DURING ACCIDENTS.
<p>GDC-1 QUALITY STANDARDS</p> <ul style="list-style-type: none"> • QUALITY OF COMPONENTS AND SYSTEMS IS TO BE ASSURED AS BEFITS SAFETY IMPORTANCE. • USE RECOGNIZED CODES AND STANDARDS, MODIFIED AS NECESSARY. • IMPLEMENT QA PROGRAM THROUGHOUT LIFE OF PLANT. 	<p>NO EQUIVALENT GDC</p>	<p>GDC-64 MONITORING RADIOACTIVITY RELEASES</p> <ul style="list-style-type: none"> • PROVIDE MEANS OF MONITORING ACTIVITY RELEASE TO CONTAINMENT ATMOSPHERE AND IN COOLANT FLUIDS AND IN THE PLANT ENVIRONS ALONG ALL DISCHARGE PATHS DURING PLANT OPERATIONS AND ACCIDENTS. 	<p>GDC-60 CONTROL OF RELEASES TO ENVIRONMENT</p> <ul style="list-style-type: none"> • DESIGN TO CONTROL RELEASE OF ACTIVITY IN GASEOUS AND LIQUID EFFLUENTS AND TO HANDLE RADIOACTIVE SOLID WASTES DURING NORMAL OPERATION AND OCCURRENCES. • PROVIDE SUFFICIENT HOLDUP CAPACITY TO RETAIN RADIOACTIVE GASEOUS AND LIQUID EFFLUENTS. 	<p>GDC-61 FUEL STORAGE AND HANDLING</p> <ul style="list-style-type: none"> • DESIGN FUEL STORAGE AND HANDLING, RADIOACTIVE WASTE AND OTHER SYSTEMS CONTAINING RADIOACTIVITY TO ASSURE SAFETY DURING OPERATIONS AND ACCIDENT CONDITIONS. ○ ALLOW FOR PERIODIC INSPECTION AND TESTING. • PROVIDE APPROPRIATE SHIELDING. • PROVIDE RESIDUAL HEAT REMOVAL. • MAINTAIN FUEL STORAGE COOLING DURING ACCIDENTS.
				<p>GDC-62 CRITICALITY IN FUEL STORAGE AND HANDLING</p> <ul style="list-style-type: none"> • PREVENT CRITICALITY BY PHYSICAL MEANS (CONFIGURATION).
				<p>GDC-63 MONITORING FUEL AND WASTE STORAGE</p> <ul style="list-style-type: none"> • PROVIDE SYSTEMS IN FUEL STORAGE AND ASSOCIATED HANDLING TO MONITOR RESIDUAL HEAT REMOVAL AND EXCESSIVE RADIATION LEVELS AND IF NECESSARY INITIATE APPROPRIATE SAFETY ACTIONS.

TABLE 1-7
COMPARISON OF GROUP 1 CRITERIA FOR PLANT SAFETY, EXTERNAL EFFECTS, FIRE, SECURITY AND DECOMMISSIONING

1.1 PLANT SAFETY PRINCIPLES

- AT ANY TIME, THE REACTOR MUST BE ABLE TO BE SHUT DOWN AND COOLED AND THE RADIATION EXPOSURE TO THE PERSONNEL AND PUBLIC HELD TO AS LOW AS POSSIBLE.
- THIS MUST FOLLOW FIRST AND FOREMOST FROM THE DESIGN AND QUALITY OF THE PLANT AS WELL AS QUALIFICATION OF THE OPERATING PERSONNEL.
- SECONDLY, THIS MUST BE ACHIEVED BY SAFETY MEASURES FOR THE CONTROL OF ACCIDENTS.

2.6 EXTERNAL INFLUENCES

- ALL PLANT PARTS REQUIRED TO SHUT DOWN AND COOL REACTOR OR PREVENT FISSION PRODUCT RELEASE MUST BE DESIGNED AGAINST NATURAL OR EXTERNAL EFFECTS.

2.7 FIRE AND EXPLOSION PREVENTION

- PROVIDE MEASURES TO OBSERVE FIRES AND EXPLOSIONS.
- DESIGN SAFETY-RELATED COMPONENTS SO THAT THEIR FUNCTION IS NOT IMPAIRED BY FIRE OR EXPLOSION.
- PROVIDE EQUIPMENT FOR EARLY DETECTION AND FIGHTING OF FIRES AND EXPLOSIONS.

2.8 PLANT SECURITY

- THE PLANT BUILDINGS AND GROUNDS MUST BE SECURED TO PREVENT ADMITTANCE OF UNAUTHORIZED PERSONNEL.
- PROVIDE A SECURE MONITORING OF PERSONNEL AND MATERIAL TRAFFIC.

2.10 DECOMMISSIONING

- THE PLANT MUST BE BUILT SO THAT IT IS ABLE TO BE RETIRED WHILE MAINTAINING FEDERAL RADIATION LIMITS.
- A CONCEPT FOR DECOMMISSIONING MUST BE AVAILABLE.

NO EQUIVALENT
HTR CRITERION

NO
EQUIVALENT
GDC

GDC-2 NATURAL PHENOMENA

- DESIGN SAFETY-RELATED STRUCTURES, COMPONENTS AND SYSTEMS TO WITHSTAND NATURAL PHENOMENA.
- USE HISTORICALLY WORST NATURAL PHENOMENA AT THE SITE AS DESIGN BASIS.
- CONSIDER APPROPRIATE COMBINATION OF PLANT CONDITIONS WITH NATURAL PHENOMENA.
- CONSIDER IMPORTANCE OF SYSTEMS TO SAFETY IN THE DESIGN FOR NATURAL PHENOMENA.

GDC-3 FIRE PROTECTION

- DESIGN AND LOCATE SAFETY-RELATED COMPONENTS AND SYSTEMS TO MINIMIZE THE PROBABILITY AND EFFECT OF FIRES AND EXPLOSIONS.
- USE NON-COMBUSTIBLE AND HEAT RESISTANT MATERIALS WHERE PRACTICAL.
- PROVIDE FIRE DETECTION AND FIRE FIGHTING SYSTEMS IN THE PLANT.

NO
EQUIVALENT
GDC

NO
EQUIVALENT
GDC

GDC-5 SHARING OF STRUCTURES, SYSTEMS AND COMPONENTS

- TO ENABLE SHARING OF STRUCTURES, COMPONENTS OR SYSTEMS IMPORTANT TO SAFETY IN DIFFERENT POWER PLANTS, IT MUST BE SHOWN THAT ACCIDENTS IN ONE UNIT DO NOT IMPAIR SHUTDOWN AND COOLDOWN OF THE OTHER UNIT(S).

GDC-4 ENVIRONMENTAL AND MISSILE DESIGN BASIS

- PROTECT STRUCTURES, SYSTEMS AND COMPONENTS AGAINST DYNAMIC EFFECTS INTERNALLY AND FROM EVENTS AND CONDITIONS OUTSIDE THE PLANT.

TABLE 1-8
COMPARISON OF GROUP I CRITERIA FOR RADIATION EXPOSURE, EMERGENCY PLANS, AND VENTILATION SYSTEMS

<p>2.3 RADIATION EXPOSURE TO THE ENVIRONMENT</p> <ul style="list-style-type: none"> ● THROUGH DESIGN AND PROCEDURES, HOLD RADIATION EXPOSURE TO THE ENVIRONMENT TO AS LOW AS POSSIBLE. 	<p>2.4 RADIATION EXPOSURE IN THE PLANT</p> <ul style="list-style-type: none"> ● ALL PLANT PARTS FOR CONTAINING RADIOACTIVE MATERIAL MUST BE FABRICATED, ARRANGED AND SHIELDED SO THAT PERSONNEL EXPOSURE, INCLUDING DURING MAINTENANCE OPERATIONS, IS HELD AS LOW AS POSSIBLE. ○ THE RADIATION PROTECTION ORDINANCE MUST BE MET DURING REPLACEMENT OPERATIONS. CONFORMANCE MEANS INCLUDE DEVICES FOR TRANSPORT, STORAGE, REGULATING, MONITORING AND SHIELDING. 	<p>2.9 EMERGENCY EXITS AND COMMUNICATIONS</p> <ul style="list-style-type: none"> ○ THE PLANT MUST HAVE DISTINCT EMERGENCY EXITS. ○ THERE MUST BE ALARMS AND MEANS OF COMMUNICATION TO PERSONNEL DURING PLANT OPERATION AND ACCIDENTS. 	<p>9.1 VENTILATION SYSTEMS</p> <ul style="list-style-type: none"> ○ PROVIDE VENTILATION FOR ROOMS WHERE THE AIRBORNE ACTIVITY CAN EXCEED FEDERAL DOSE GUIDELINES, WHERE NEEDED TO ASSURE AIR QUALITY, WHERE SAFETY-RELATED EQUIPMENT WITH AIR-COOLING REQUIREMENTS IS STORED, AND WHERE ATMOSPHERIC INERTING IS REQUIRED. ○ VENTILATION SYSTEMS MUST ASSURE DOSE LIMITS ARE NOT EXCEEDED DURING PLANT OPERATION OR ACCIDENTS. ○ PROVIDE FILTER SYSTEMS WHERE NEEDED TO MAINTAIN ACCEPTABLE AIRBORNE ACTIVITY LEVELS. 	<p>10.3 ENVIRONMENTAL MONITORING</p> <ul style="list-style-type: none"> ● MONITOR RADIATION IN THE ENVIRONMENT DURING PLANT OPERATION, ACCIDENTS AND UNFORESEEN EVENTS. ● PROVIDE DEVICES FOR MEASURING DOSE BURDENS, AIRBORNE ACTIVITY, AND SURFACE CONCENTRATIONS AS WELL AS NUCLIDE TYPE DURING PLANT OPERATION AND ACCIDENTS. ● PROVIDE DEVICES FOR MEASURING METEOROLOGICAL DATA.
<p>GDC-60 CONTROL OF RELEASE OF RADIOACTIVE MATERIALS TO THE ENVIRONMENT</p> <ul style="list-style-type: none"> ● PROVIDE MEANS TO CONTROL RELEASE OF RADIOACTIVE EFFLUENTS DURING PLANT OPERATIONS AND OCCURRENCES. ○ PROVIDE SUFFICIENT HOLDING CAPACITY FOR RETENTION OF RADIOACTIVE EFFLUENTS. 	<p>GDC-61 FUEL STORAGE AND HANDLING</p> <ul style="list-style-type: none"> ● DESIGN FUEL STORAGE AND HANDLING AND SYSTEMS CONTAINING RADIOACTIVITY TO ASSURE SAFETY DURING OPERATIONS AND ACCIDENT CONDITIONS. ● ALLOW FOR PERIODIC INSPECTION AND TESTING. ● PROVIDE APPROPRIATE SHIELDING. 	<p>NO EQUIVALENT GDC</p>	<p>NO EQUIVALENT GDC</p>	<p>GDC-64 MONITORING RADIOACTIVITY RELEASES</p> <ul style="list-style-type: none"> ● PROVIDE MEANS OF MONITORING ACTIVITY RELEASE TO CONTAINMENT ATMOSPHERE AND IN COOLANT FLUIDS AND IN THE PLANT ENVIRONS ALONG ALL DISCHARGE PATHS DURING PLANT OPERATION AND ACCIDENTS.

2. DEFINITIONS

A number of terms used in the BMI draft of HTR safety criteria have specific and narrow meanings, understood by pre-established definitions. The following definition of terms is contained in the preamble to the BMI draft. These definitions are assumed in all terminology used in this report.

1. Specified Normal Operation

- a. Operating conditions intended and suited for the plant design (power operation), assuming the able function of all systems (fault-free condition).
- b. Operating processes which occur in event of component or system malfunction (incident condition), insofar as continued operation is not disallowed on safety grounds (abnormal operation).

2. Accident

An event sequence whose occurrence (a) causes discontinued operation of the plant on safety grounds, and (b) is pre-considered in the design of the plant (design basis event).

3. Discharge of Radioactive Material

Intentional removal of fluid, aerosol, or gaseous radioactive material from the plant.

4. Release of Radioactive Material

Escape of radioactive material from barriers provided in the plant or to the environment.

5. Single Failure

Failure caused by a single event, including consequential failures resulting from the single event. For detailed application of the single failure concept in the safety criteria, see Appendix B.

6. Redundancy

Existence of more technical functional means than are necessary to fulfill the function envisaged.

7. Limiting Values (or Limits)

As used in these criteria, values specified for conditions of plant components, plant systems, or media contained therein, the adherence to which excludes a failure of safety-related equipment with appropriate safety margin.

8. Safety System

Totality of all technical equipment of a reactor plant which during accidents should protect the plant from loadings beyond those allowable and maintain consequences on operating personnel, the plant, and the environment within given limiting values.

9. Exceptional Event

Event sequence beyond the class of accidents defined above which can result in radiation exposure of one or more persons or

radioactive material release beyond regulatory limits. (Analogous to U.S. definition of class 9 events.)

10. KTA Regulations

German regulatory acceptance standards similar to RGs in the U.S.

The abbreviation:

(R) means approved regulation,

(RE) means draft regulation,

(REV) means draft regulation in preparation.

3. CRITERIA SPECIFIC TO HTRs (GROUP III)

There are five subjects considered to be distinctly HTR specific, comprising the Group III criteria. These are the criteria for testing of systems and components, for core design and reactivity control, for afterheat removal, and for the primary system and the containment fission product barriers. Since a large share of the BMI criteria draft effort was devoted to the Group III criteria, this review will begin with these.

3.1. TESTING (CRITERION 2.2)

This criterion specifically corresponds to the statement in GDC 1 that structures and systems must be tested commensurate with their safety importance. A number of alternative design measures are mentioned (Table 1-1) for the case where a component or system is not testable. The consequences of failure of such a component or system must be limited, which means the ability to shut down the reactor, cool the core, and not incur an unacceptably high fission product release must not be impaired. The provision of a separate criterion for testing obviates to some extent the need for statements requiring testing in the individual component criteria (as, for example, in GDCs 18, 21, 32, 37, and 53).

The acceptance standards for testing are represented in the U.S. by the proposed Section XI, Division 2 of the ASME Boiler and Pressure Vessel Code (Rules for Inspection and Testing of Components of Gas-Cooled Plants), 10CRF50 Appendix J for containment leak rate, and the RGs and SRPs listed in Table 3-1. Corresponding German written standards

are not as extensive. There is no equivalent of the ASME Code, although some non-nuclear industry standards exist in the UVV requirements for boilers and conventional equipment and in DIN non-safety requirements. In the RSK guidelines, testing standards are given for vessels and piping (RSK 4.1.4.4), for electrical equipment (RSK 7.2.2), and for containment pressure and leakage (RSK 5.5).

3.2. REACTOR COOLANT BOUNDARY AND PCR/V (CRITERIA 4.1-4.3)

These criteria (Table 1-1) correspond to U.S. GDCs 14 and 15 and 30 through 32 but are significantly different because of HTR design features. The HTR criteria differentiate between non-pressure-bearing and pressure-bearing components of the reactor coolant boundary. In the HTR design, the liner together with penetrations and closures forms the leak-tight boundary containing primary coolant (Ref. 3-1). According to U.S. definitions, the liner, backed by concrete, is safety class 2 rather than class 1, since it acts as a flexible membrane and is not part of the pressure boundary (Ref. 3-2). In the U.S., volumetric and visual in-service inspection of the liner is not required by either the ASME Boiler and Pressure Vessel Code, Section XI, Division 2 or the NRC, similar to British and French practice.

Criterion 4.1 gives the general definition and function of the reactor coolant boundary (RCB) and thus is similar in nature to GDC 14. The design basis of the RCB is given by Criterion 4.2, which is similar in intent to GDCs 15 and 30. Like these GDCs, Criterion 4.2 gives the general requirements to design, test, and choose materials for service and accident conditions and to monitor, but not necessarily to locate, RCB leakage. However, the HTR criterion goes further and stipulates specifically that (1) penetrations must be secured against outward forces and (2) consequences of closure failure [if a design basis accident (DBA)] must be mitigated if necessary by limiting the blowdown flow area and designing prestressed concrete reactor vessel

(PCRv) components for the blowdown forces. In past HTR licensing in the U.S., flow restrictors were provided to mitigate closure failures as DBAs.

Criterion 4.3 covers design of the pressure-bearing vessel (PCRv), corresponding to GDCs 31 and 32. As in the GDCs, the criterion contains general requirements to design for service and accident conditions and to prevent gross failure by design and material choice. The HTR criterion goes beyond the GDCs in additional specific requirements to provide, if necessary, thermal protection and monitoring of the PCRv, to withstand external influences on the outer side of the PCRv, and to maintain integrity of the prestressing cables. The first and last of these are specific to the HTR; the second is characteristic German practice which is not represented explicitly in the LWR criteria. Monitoring and periodic testing of the PCRv itself and monitoring of the functionability of the liner thermal protection system are required, as compared with GDC requirements for periodic inspection and testing and a surveillance program for LWR coolant pressure vessels. Reactor coolant makeup (GDC 33) is not addressed in the HTR criteria.

Written LWR acceptance standards for the pressure-bearing vessel are represented in the FRG by RSK guidelines 4.1, 4.2, and 21. These are relatively extensive, covering definitions (4.1.1 and 4.2.1), design and fabrication (4.1.2 and 4.2.2), construction (4.1.3 and 4.2.3), operation (4.1.4 and 4.2.4), and leakage (21.). Some KTA regulations are in preparation, but they also apply to LWRs.

Abundant corresponding acceptance standards have been written in the U.S. applicable to LWRs, for example 10CFR50, Appendix G and H; 10CFR50.55 A; ASME Code Section III, Division 2; SRPs 5.2 and 5.3; and a large number of RGs (see Table 3-2). A comparison of the respective U.S. and German LWR acceptance standards is not completely relevant because of the significant differences between the HTR and LWR

criteria for the primary coolant boundary. Instead, the application of the intent of the written acceptance standards on HTR licensed designs is summarized.

In the U.S., penetrations and closures not backed by concrete are safety class 1 pressure boundaries, subject to ASME Code, Section III design rules and 10CFR50 Appendix B (and RG 1.94) quality assurance. To meet the intent of GDC 15, overpressure protection is implemented per RG 1.67 and SRP 5.2.2 (Table 3-2). Design and fabrication acceptance standards to satisfy criteria in GDCs 30 and 31 and 10CFR50.55 A meet the intent of RGs and SRPs listed in Table 3-2, as well as 10CFR50 Appendix G. For inspection and testing of the PCR, instead of the LWR standards in Table 3-2, there is a proposed Section XI, Division 2 ASME Code for gas-cooled reactors.

In the FRG, RSK guidelines 4.1, 4.2, and 21 are not very specific standards for HTR design. In past licensing proceedings, essentially the same reactor coolant vessel design as in the U.S. was accepted, and the added criterion to consider airplane crash as an external event was not controlling.

3.3. CORE DESIGN AND REACTIVITY CONTROL (CRITERIA 3.1-3.4)

Four HTR criteria (3.1 through 3.4) were written on this subject, corresponding to GDCs 10 through 12 and 26 through 29 (Table 1-2). Criterion 3.1, Reactor Core Design, contains a general requirement to design the core, coolant, control, and plant protection systems such that radioactivity release and plant safety limits are not exceeded during plant life. It agrees almost exactly with GDC 10 and with German LWR Criterion 3.1. Similarly, Criterion 3.2 is short and general, agreeing well with German LWR Criterion 3.2 and GDCs 11 and 12 in requiring inherent core design to compensate for rapid and slow reactivity rises (the GDCs include reactor coolant as well as core design).

Criterion 3.3 deals with components internal to the PCRV. First, these components must be constructed so that their design limits are not exceeded during plant operation. Second, it must be assured that during accidents they can successfully perform any function they might have in shutting down the reactor, removing residual heat, and preventing unacceptable fission product release. No equivalent GDC exists, although a similar criterion for LWR primary vessel components can be found in the German criteria.

Criterion 3.4 is a single extensive criterion dealing with reactor control and shutdown, corresponding to GDCs 26 through 29. Despite the differences in reactor type, the criteria are written in general language, so that the requirements are comparable. In both cases, two diverse reactivity control systems are required, one of which must be capable of maintaining cold shutdown. Together, the systems must control reactivity changes not to exceed reactor safety limits, considering a single source of disturbance and stuck control rods. The HTR criterion contains a unique statement that inherent characteristics of the reactor may be used in place of shutdown system hardware when appropriate. The question of automatic versus manual activation of the second shutdown system was left open in the criterion (dependent on accident analysis).

Acceptance standards in the U.S. and the FRG for these criteria are summarized in Table 3-3. In the FRG, the listed RSK guidelines are not very explicit and do not go far beyond the criteria. The KTA regulations are definitive, and although they pertain to LWRs, one can infer from these regulations and from past HTR licensing experience that specific HTR design requirements in the FRG include:

1. Consideration of water ingress and rod injection effects on reactivity.
2. Consideration of geometry changes of pebble bed cores.

3. A 0.3% and 1% shutdown criticality margin for the first and second systems, respectively.
4. Maintaining subcriticality by the first shutdown system until time for operator action (such as 1/2 h), in case the second shutdown system is not automatic.

Some consideration was given to the possible inclusion of these specific items in the criteria themselves. Because of inherent HTR characteristics (low power density, etc.), negative reactivity insertion rates required to terminate accidents are low enough so that gravity insertion may be used for one or both shutdown systems. The combination of low power density and the more epithermal system in graphite reduces xenon oscillation potential on power spiking compared with LWRs. These and other HTR characteristics facilitate the ability of existing HTR designs to easily meet the intent of the acceptance standards given principally in the mentioned SRPs in the U.S.

3.4. AFTERHEAT REMOVAL (CRITERIA 5.1-5.2)

These criteria set the basis for the main and auxiliary core cooling systems for a shutdown HTR and so are unique and important to the HTR design. Criterion 5.1 was written to stipulate requirements for residual heat removal during normal operational shutdown. In HTR designs to date, this function is performed by the main cooling system* with reduced primary and secondary coolant flow. The criterion calls for a reliable and redundant heat removal system designed to prevent exceeding of component design and radioactivity release limits. For fulfillment of the redundancy requirements, however, the criterion explicitly allows use of the accident afterheat removal system. The purpose of this somewhat roundabout wording is to stipulate that while the normal residual heat removal system is not a safety system, it

* Only partially redundant and not designed to a specific reliability goal.

should be available for the large majority of plant shutdowns so that the demand frequency on the accident or auxiliary residual heat removal system is low. The unwritten motivation underlying this stipulation is to hold the probability of not being able to cool the core to below about 10^{-6} per reactor year (this value results from multiplying the conditional fixed low probability of total system failure times the demand frequency).

Thus, the accident afterheat removal system in Criterion 5.2 is required to be reliable, redundant, single failure proof, and designed for accumulated accident loadings. For the latter it is stipulated that the design must consider frequencies of accidents and the potential coolant gas mixture resulting from possible ingress of alien substances (air, water, etc.) and chemical reactions. A minimum pressure requirement should be derived either from the conservatively calculated containment backpressure after depressurization or from atmospheric pressure. Some common parts with the normal residual heat removal system are not precluded if reliability is maintained and if components are testable.

The important factor affecting the number of accident afterheat removal loops is the application of the single failure criterion. While the German application of the N-2 safety requirement (based on past HTR licensing in the FRG) would normally be the rule here, Criterion 5.2 allows modification of this requirement if it can be demonstrated that the loop in maintenance can be restored in time, considering the contribution of the inherent design characteristics in extending the time required for achieving sufficient afterheat removal. This is close to the U.S. practice of N-1 design with continued plant operation for some limited period for a one-loop maintenance outage of short duration. Following expiration of that time period, or for maintenance operation of longer duration, the plant would be shut down or reduced in output power to a level where the specified redundancy is restored (with attendant availability impact). Whether the impact of Criterion 5.2 will

lead to N-1 design for HTR auxiliary cooling loops in the FRG is problematical and may depend on development of the acceptance standards.

Because of the significantly different design and function requirements involved, the HTR residual heat removal system criteria are not strictly comparable to the LWR criteria*. Table 1-3 compares the GDC requirements with the HTR requirements. HTR Criteria 5.1 and 5.2 together correspond to GDC 34 in that they require a safety-related capacity for removing residual heat for all normal or accident shutdowns. However, GDC 34 is not nearly so specific or detailed in requirements. The GDC 35 through 37 ECCS criteria have no analog in HTR criteria since they deal with loss of coolant events which cannot occur in an HTR.

Acceptance standards are given in the FRG by RSK 22, Systems for Residual Heat Removal after Accidents, and in the U.S. by RG 1.139, Guidance for Residual Heat Removal, and SRP 5.4.7, Residual Heat Removal System. All of these deal with LWRs; essentially, no written standards exist on direct application to HTRs.

3.5. CONTAINMENT (CRITERIA 8.1-8.5)

Five HTR containment criteria were developed (see Table 1-4). The first four correspond approximately to GDC 16 and GDCs 50 through 57. Criterion 8.1 is similar to GDC 16 in defining the function of the containment to enclose the primary coolant and prevent fission product release to the environment. The footnote to this HTR criterion is important in that it interprets this function as including "buildings and any necessary engineered systems for retention and filtering of fission product leakage out of the containment." Thus, the option of having a controlled vented confinement rather than a high-pressure lined containment seems to be explicitly left open for the HTR. The

* Even the consequences of not having core cooling are different, so that risk is different if the probability of losing coolability is the same.

wording of GDC 16 is more ambiguous in this regard, requiring "an essentially leaktight barrier against uncontrolled release of fission products." This raises the following questions: (1) Does a controlled vented confinement meet this requirement because the barrier is leaktight except for controlled release? (2) Even if the original intent was to stipulate a high-pressure-tight containment, should this be modified in light of results of WASH-1400 and research on vented confinement concepts? Obviously, the U.S. criteria are not very clear in this regard.

The design basis of the containment is given in Criterion 8.2, which is similar to GDCs 50 and 51. Requirements to design against all accident conditions and to include margin in the design pressure are the same. GDC 51 is somewhat more specific in containment liner fracture prevention requirements. Criteria for containment atmosphere cleanup and containment heat removal systems, given for LWRs by GDCs 38 through 43, are not necessarily needed. Criterion 8.3 requires periodic pressure and leaktightness tests of the containment structure and penetrations, as do GDCs 52 and 54.

Criterion 8.4 contains detailed requirements for containment penetrations, analogous to GDCs 54 through 57. Two isolation valves, one inside and one outside the containment, are specified for each penetration in contact with the RCPB or containment atmosphere. Criterion 8.4 specifically states that these valves must be automatic or remote-controlled and sufficiently leaktight, while this is understood (but not stated) in the GDCs. Other penetrations require only one isolation valve outside the containment, as in GDC 57. Specific reliability and redundancy requirements are given in Criterion 8.4 for isolation valves, whereas GDC 54 contains only a simple general statement that they must be reliable and redundant. No corresponding requirement exists in the GDCs for the stipulation in Criterion 8.4 that the position of the isolation valves must be shown in the control room. On the

other hand, GDCs 55 through 57 stipulate that (1) external isolation valves must be as close to the containment as practical, and (2) upon loss of activating power, automatic valves must take the position of greater safety. These stipulations are not contained in Criterion 8.4.

A criterion not previously in the GDC or German LWR criteria was added to provide a barrier for liquids in the plant buildings for building and groundwater protection (Criterion 8.5). Such a barrier is to be provided on the inside of the building and should be capable of being decontaminated.

Extensive acceptance standards for LWR containments exist in both countries, as summarized in Table 3-4. Important calculated containment and subcompartment design pressure requirements in the FRG, given mostly in RSK 5.1, are as follows:

1. Blowdown of primary coolant with maximum credible accident leak rate combined with energy content of one steam generator.
2. A 2% margin increase in primary and secondary coolant volumes.
3. Inclusion of decay heat of primary coolant fission products with a 1.2 factor on the ANS 5.1 standard nominal afterheat function.
4. A 2% decrease in containment volume for building tolerance.
5. A final 15% safety margin on top of the above-calculated pressure to account for analytical uncertainties.

The U.S. standards, primarily SRP 6.2.1, stipulate either primary coolant or steam generator energy content blowdown, but not both together. Margins on the blowdown gas and containment volumes are not given

explicitly. For the construction phase license, safety margins of 10% and 40% are stipulated for the containment and subcompartment pressures, respectively. These margins are not necessarily required for the operating license stage. A further requirement, recommended by RG 1.4, is that the containment pressure be reduced below 50% of the design pressure within 24 hr after the accident because of energy exchange with the containment heat sinks.

A comparison of containment metal wall stress standards in the U.S. and the FRC, involving ASME standards and KTA rules such as in KTA 3401.3, is given in Ref. 3-3. RSK 5.2 requires that the containment have a concrete outer shell to protect against external effects as well as internal release of radiation.

REFERENCES

- 3-1. Riccardella, P. C., "Design Basis for HTGR Penetrations and Closures," General Atomic Report GA-A13832, May 7, 1976.
- 3-2. Grenier, R. M., R. J. Hsieh, and J. L. Pickering, "Leak Tightness Design Basis for HTGR Cavity Liners," DOE Report GA-A14976, General Atomic Company, May 1978.
- 3-3. Richardson, J. A., "Summary Comparison of West European and U.S. Licensing Regulations for LWRs," Nucl. Eng. Intern. 21, 32-41 (Feb. 1976).

TABLE 3-1
U.S. STANDARDS FOR TESTING

Regulatory Guides

- 1.15 Concrete rebar
- 1.18 Concrete containment structure
- 1.19 Containment liner welds (NDE)
- 1.22 Plant protection system functionability
- 1.40 Motors in containment
- 1.68 LWR test program
- 1.73 Electric valve operators
- 1.79 Emergency core cooling system
- 1.80 Instrument air systems
- 1.118 Electric power and protection systems

Standard Review Plans

- 3.9.2 Mechanical components
- 3.9.6 Pumps and valves
- 5.2.4 Reactor coolant pressure boundary

ASME Code, Section XI, Division 2 - Nuclear materials
10CFR50 Appendix J - Containment pressure and leakage

TABLE 3-2
U.S. ACCEPTANCE STANDARDS FOR PRESSURE-BEARING VESSELS (LWRs)

GDC 14 Reactor Coolant Pressure Boundary (RCPB)

SRP 5.2.1.1 Compliance with 10CFR50.55 A

GDC 15 Reactor Coolant System Design

RB 1.67 Overpressure Protection Devices

SRP 5.2.2 Overpressurization Protection

SRP 5.3.1 Materials

SRP 5.3.2 Pressure-Temperature Limits

GDC 30 Quality of RCPB

RG 1.10 Reinforcing Bar Welding

RG 1.15 Testing of Reinforcing Bars

RG 1.45 Leakage Detection of RCPB

RG 1.55 Concrete Placement

RG 1.103 Prestressing Systems

RG 1.124 Service Limits and Loads-Components

RG 1.130 Design Limits and Loading-Components

SRP 5.2.5 RCPB Leakage Detection

SRP 5.3.3 Reactor Vessel Integrity

GDC 31 Fracture Prevention of RCPB

ASME Section III Boiler and Pressure Vessel Code

10CFR50 Appendix G Fracture Toughness Requirements

RG 1.2 Thermal Shock to Pressure Vessels

RG 1.48 Design Limits and Load Combinations

RG 1.65 Materials for Closure Studs

RG 1.84 ASME Section III Design and Fabrication

RG 1.85 ASME Section III Materials

RG 1.87 Construction of ASME Class 1 Components

RG 1.99 Predicted Radiation Damage

SRP 5.2.1.3 Applicable Code Cases

SRP 5.2.3 RCPB Materials

GDC 32 Inspection of RCPB

10CFR50 Appendix H Reactor Vessel Material Surveillance

ASME Section XI Inspection and Testing of Components

RG 1.83 In-Service Inspection of Steam Generator Tubes

RG 1.94 Quality Assurance Requirements for Installation and Inspection

RC 1.133 Loose Part Detection Program

SRP 5.2.4 In-Service Inspection and Testing

TABLE 3-3
ACCEPTANCE STANDARDS FOR REACTOR CORE DESIGN AND REACTIVITY CONTROL

FRG	U.S.
<u>Criterion 3.1 Reactor Core Design</u>	<u>GDC 10 Reactor Design</u>
RSK 3.1.1 Core Design	SRP 4.2 Fuel System Design
KTA 3102.1 Helium Inventory	SRP 4.4 Thermal, Hydraulic Design
<u>Criterion 3.2 Coupling Characteristics of the Reactor Core</u>	<u>GDC 11 Reactor Inherent Protection and</u> <u>GDC 12 Power Oscillations</u>
RSK 3.2 Inherent Safety	SRP 4.3 Nuclear Design
<u>Criterion 3.3 PCR V Internals</u>	<u>No GDC</u>
RSK 3.3 Components of PCR V	RG 1.20 Vibration-Reactor Internals
KTA 3201 Components of PCR V	SRP 4.5.2 Reactor Internals Materials
<u>Criterion 3.4 Systems for Control and Shutdown of the Reactor</u>	<u>GDC 26 Reactivity Redundancy</u>
RSK 3.1.2 Shutdown Systems	SRP 4.5.1 Control Rod Material
RSK 3.1.3 Operation Transients	SRP 4.6 Design of Reactivity Control
KTA 3104 Shutdown Reactivity	<u>GDC 27 Combined Reactivity Capability</u>
RSK 20 Failure of Fast Shutdown System	SRP 7.2 Reactor Trip System
	SRP 7.4 Systems for Safe Shutdown
	<u>GDC 28 Reactivity Limits</u>
	<u>GDC 29 Protection Against Occurrences</u>
	RG 1.77 Assumptions for Control Rod Ejection
	SRP 15.4 Reactivity Anomalies

TABLE 3-4
CONTAINMENT ACCEPTANCE STANDARDS IN THE U.S. AND THE FRG

FRG	U.S.
<u>Criterion 8.2 Containment Design Basis</u> RSK 5.1 Groundrules for Design RSK 5.2 Construction Arrangements RSK 5.3 Material Requirements RSK 5.4 Fabrication KTA 3401.3 Steel Construction (RE)	<u>GDC 50 Design Basis</u> RG 1.4 LOCA Assumptions RG 1.7 Combustible Gas Control RG 1.46 Protection Against Pipe Whip RG 1.57 Design Limits for Metal Containment RG 1.107 Tendons in Concrete Containment RG 1.135 Material for Concrete Containment SRP 3.8.1 Concrete Construction SRP 3.8.2 Steel Containment SRP 3.8.3 Internal Structures SRP 6.2.1 Containment Functional Design SRP 6.2.3 Containment Design SRP 6.2.4 Containment Isolation SRP 6.2.5 Combustible Gas Control 10CFR50 Appendix K - LOCA Models
<u>Criterion 8.3 Leaktightness Tests</u> RSK 5.6 Pressure and Leak Rate Tests KTA 3405 Leakrate Tests (RE)	<u>GDC 51 Fracture Prevention</u> RG 1.18 Concrete Containment Test RG 1.19 NDE of Liner Welds RG 1.103 Concrete Prestressing RG 1.55 Concrete Placement <u>GDC 52 Leak Rate Testing</u> SRP 6.2.6 Containment Leakrate Test 10CFR50 Appendix J - Leakage Testing
<u>Criterion 8.4 Penetrations</u> RSK 5.6 Penetrations KTA 3402 Personnel Locks (R) KTA 3403 Cable Penetrations (R) KTA 3404 Isolation of Penetrations (RE) KTA 3409 Material Locks (RE)	<u>GDC 53 Testing and Inspection</u> RG 1.15 Testing of Rebar RG 1.90 ISI of Concrete Containment <u>GDC 54 Piping Penetrations</u> RG 1.96 Steam Isolation Valves <u>GDC 55 + 56 Isolation of Penetrations</u> RG 1.141 Fluid System Isolation SRP 6.2.4 Containment Isolation System ANSI-N271 <u>GDC 57 Isolation of Closed Systems</u> RG 1.11 Instrument Lines RG 1.63 Electric Penetrations

4. CRITERIA ANALOGOUS TO LWR (GROUP II)

Group II criteria are those stemming from the LWR criteria but revised to various degree for reasons of new safety developments, better applicability to HTRs and to Group III criteria, etc.

4.1. INSTRUMENTATION AND CONTROL ROOM (CRITERIA 6.2-6.4)

As previously done in the German LWR criteria, differentiation is made in the instrumentation criteria between normal and accident conditions. Criterion 6.2 deals with instrument requirements for accidents, while Criterion 6.3 pertains to instruments for normal plant operation. Together, these criteria provide more detail than the equivalent single GDC on the subject, GDC 13, as shown in Table 1-5. Likewise, Criterion 6.4 for control room requirements is somewhat more extensive than GDC 19. In both cases, the criteria call for (1) instrumentation to monitor safety-related variables during operation and accidents and (2) design for personnel access to and control of accidents from the control room. In addition, the HTR criteria require:

1. Classification of instruments into "event" and "consequence" with separate measurement requirements, including a new one to measure environmental consequences.
2. Display of data in the control room and/or emergency control station (as opposed to U.S. criteria, an emergency control station is required in German criteria as a backup to the control room).

3. An uninterruptible power source for accident instrumentation with recording redundancy for "event" but not for "consequence" instruments.
4. Allowing control actions in the long term from outside the control room.

Acceptable standards for these criteria are summarized in Table 4-1. In the U.S., the instrument requirements for earthquakes are given by ANSI N18.5 and endorsed by the NRC via RG 1.12. This includes location and number of instruments, instrument characteristics, and installation.

Variables to be measured, including the containment and reactor coolant pressure, radiation level in the containment, and radioactivity release rate during accidents, are stipulated by RG 1.97, along with measurement ranges and redundancy requirements. Compared with these U.S. standards, the German instrumentation standards are more generally worded, stipulating redundancy and reliability rather than specific instrumentation measurements. A similar situation exists for control room standards. However, both the German LWR criteria and HTR criteria draft specify an emergency control station as a backup to the control room, which is not the case in the U.S. criteria. Also, the unwritten German interpretation of the control room criterion tends to be more conservative.

4.2. PLANT PROTECTION SYSTEM (PPS) AND ELECTRICAL SUPPLY (CRITERION 6.1)

A single HTR criterion (6.1) was developed for PPS requirements analogous to GDCs 20 through 25, as shown in Table 1-5. Criterion 7.1 covers all electrical supply requirements analogous to GDCs 17 and 18 (Table 1-5).

The wording in the U.S. and German PPS criteria is basically the same; in fact, the HTR criterion for the PPS was little changed from the corresponding German LWR criterion. Requirements are that the PPS be reliable, redundant, single-failure-proof, and, in general, separate from the plant control system. For electrical supply, both GDC 17 and Criterion 7.1 require redundant on-site power sources (diesel generators) which are single-failure-proof and independent and separate supply lines. However, in the U.S., a common switchyard arrangement is allowed, while the German criterion (for both the HTR and LWR) calls for redundant and separate switchyards.

Wording in GDC 17 requiring prompt (within seconds) availability of circuits after an accident is not explicit in the HTR criteria because of the slower HTR system response. On the other hand, the HTR criteria uniquely require a period of diesel power operation which is long enough to allow restoration of other power sources.

Acceptance standards for these criteria are listed in Table 4-2. The respective standards in the two countries are basically the same, except that the German interpretation of the single failure rule leads to N-2 safety in diesel generator units, either 3 x 100% duty or 4 x 50% duty units. Also, a reliability goal of better than 10^{-4} failure of the system is practiced.

4.3. QUALITY ASSURANCE (CRITERION 2.1)

As shown in Table 1-6, the wording of HTR Criterion 2.1 on quality assurance (QA) or standards agrees well with GDC 1. Interpretation of this criterion in the FRG is represented solely by KTA regulation 1401. This document covers QA inspection, tests, monitoring and surveillance during fabrication, construction, and operation. The level of detail, however, is not as extensive as in U.S. standards for QA, which are listed in Table 4-3. The primary difference is that in the FRG the

tests and inspection are largely carried out by the independent TÜV agencies, while in the U.S. these are performed by the manufacturers themselves and documented for outside review and traceability. Some reviewers (Ref. 4-1) have attached significance to this, feeling that the German approach may place greater emphasis on in-plant inspection of construction and fabrication procedures. However, such interpretation is not clear-cut.

This criterion is not plant specific but has been placed in the Group II criteria. This is because the previous LWR wording has been considerably shortened, eliminating unneeded details and redundancies.

4.4. HEALTH PHYSICS AND RADIATION MONITORING (CRITERIA 2.4, 10.1-10.3)

This subject is covered by Criteria 2.4, 10.1, 10.2, and 10.3, as summarized in Tables 1-6 and 1-8. Criterion 2.4 is a short, general requirement to arrange the working area, conditions, and environment for plant personnel under a health physics program for their safety and protection. This has no equivalent GDC, although several U.S. regulatory and industrial standards apply, such as:

RG 1.39	Housekeeping
SRP 12.5	Health Physics
ANSI N18.7	Administrative Controls

Equivalent standards in the FRG consist of RSK 13, Working Conditions, and KTA 1301 (REV), Radiation for Plant Workers.

There are two Group II radiation monitoring criteria, 10.1 and 10.2. Criterion 10.1 covers monitoring of radiation to personnel and contamination in the plant, corresponding to GDC 64. Criterion 10.2 is concerned with monitoring of activity in radwastes and exhaust air released to the environment, corresponding to GDC 60. Both of these

HTR criteria go somewhat beyond the LWR criteria in specifying stationary radiation measuring devices with recorded output and indication in the control room with alarms, as well as portable measuring devices. The monitoring covers both normal operation and accidents.

Criterion 10.3 is a third (Group I) monitoring criterion covering measurement of meteorology and airborne activity released to the atmosphere with corresponding environmental effects (dose burdens, surface contaminations, etc.). As shown in Table 1-8, this criterion is slightly more detailed than the corresponding GDC 64.

Acceptance standards for the radiation monitoring criteria are listed in Table 4-4. Detailed RSK guidelines and KTA regulations systematically covering the radiation monitoring criteria exist in the FRG. In the U.S., detailed standards on meteorological measurement are available but radiological measurement standards are sparse.

4.5. FUEL HANDLING AND STORAGE (CRITERION 11.1)

Criterion 11.1 corresponds closely to GDCs 61 through 63, except for the additional requirement that the fuel be positioned correctly in the core (Table 1-6). Otherwise, the requirements are the same as for LWRs. Acceptance criteria are represented in the FRG by RSK 15, Fuel Handling and Storage, and KTA 3603, Handling Contaminated Water (RE), but these are not detailed standards on the subject. U.S. standards consist primarily of RG 1.13, Fuel Storage Facility Design, RG 1.25, Assumptions for Fuel Handling Accident, Standard Review Plans, RG 9.1, Fuel Handling and Storage, RGs 11.1 through 11.5, Waste Management, and industry codes ANSI N14.5, N14.10.1, and N45.2.2. Together, these comprise more detail than the German standards in that they embody seismic qualification, ALARA (as low as reasonably achievable) requirements, and criticality. One difference in practice is that low-level wastes are disposed of by the applicants themselves in the U.S. and

by the government in the FRG. More detailed acceptance standards to comply with GDCs 61 through 63 are given in Ref. 4-2, p. 40.

REFERENCES

- 4-1. "Gas Reactor International Cooperative Program Interim Report, United States/Federal Republic of Germany Nuclear Licensing Comparison," General Electric Report C00-4057-9, September 1978.
- 4-2. Richardson, J. A., "Summary Comparison of West European and U.S. Licensing Regulations for LWRs," Nucl. Eng. Intern. 21, 32-41 (Feb. 1976).

TABLE 4-1
U.S. AND FRG ACCEPTANCE STANDARDS FOR INSTRUMENTATION AND CONTROL ROOM CRITERIA

FRG	U.S.
<u>Criterion 5.2 Accident Instrumentation</u>	<u>GDC 13 Instrumentation and Control</u>
RSK 7.1 Scope of Instrumentation	RG 1.12 Instruments for Earthquakes
RSK 7.2 Requirements of Instruments	RG 1.97 Accident Instrumentation
RSK 24 Accident Instruments	RG 1.105 Instrument Set Points
KTA 3502 Accident Instrumentation (REV)	SRP 3.10 Seismic Qualification of Instrumentation
KTA 2201.5 Earthquake Instruments	SRP 3.11 Environmental Design of Instrumentation
<u>Criterion 6.3 Operation Instrumentation</u>	SRP 3.7.4 Seismic Instrumentation
RSK 6 Electrical Devices for Operation	SRP 7.5 Display Instrumentation
	SRP 7.6 Other Safety Instrumentation
	ANSI N18.5 Earthquake Instrumentation
	IEEE Standards 279 and 379
<u>Criterion 6.4 Control Room and Emergency Control Station</u>	<u>GDC 19 Control Room</u>
RSK 8 Control Room	RG 1.78 Control Room
	RG 1.95 Protection for Operators
	RG 1.114 Guidance for Operators
	SRP 9.4.1 Control Room Ventilation

TABLE 4-2
COMPARISON OF U.S. AND FRG ACCEPTANCE STANDARDS FOR PPS AND ELECTRICAL POWER SUPPLY

FRG	U.S. (a)
<u>Criterion 6.1 Plant Protection System (PPS)</u>	<u>GDC 20 PPS Functions</u>
RSK 7.3 PPS (refers only to KTA 3501)	SRP 7.3 Engineered Safety Systems
KTA 3501 PPS (R)	<u>GDC 21 Reliability and Testing of PPS</u>
	RG 1.22 Testing of Function
	<u>GDC 22-25 Independent Failure Modes, Etc.</u>
	SRP 7.3 Engineered Safety Systems
<u>Criterion 7.1 Electrical Supply</u>	<u>GDC 17 Electric Power Systems</u>
RSK 71 Scope of Electrical Devices	RG 1.6 Independence of Electrical Systems
RSK 7.2 Electrical Requirements	RG 1.9 Diesel Generator
RSK 7.4 Electrical Supply for PPS	RG 1.32 Criteria for Electrical Systems
KTA 3701.1 Electrical Supply (R)	RG 1.75 Physical Independence
	RG 1.81 Shared Electrical Systems
	RG 1.93 Availability of Electrical Systems
	RG 1.128 Design of Storage Batteries
	SRP 3.10 Seismic Qualification
	SRP 8.1 Electric Power
	SRP 8.2 Offsite Power Systems
	SRP 8.3.1 A-C Power System
	SRP 8.3.2 D-C Power System
	<u>GDC 18 Testing of Electrical Systems</u>
	RG 1.30 QA Testing of Electrical Systems
	RG 1.41 Testing of Outside Electrical Systems
	RG 1.108 Testing of Diesels
	RG 1.118 Testing of Electric Power
	RG 1.129 Testing of Storage Batteries
	RG 1.131 Tests of Electric Cables

(a) There are also numerous U.S. industry (IEEE) standards on this subject, notably IEEE 603 (Safety Systems), IEEE 308 (Electrical Supply), and IEEE 279 (PPS).

TABLE 4-3
ACCEPTANCE STANDARDS IN U.S. FOR QUALITY ASSURANCE

10CFR50	Appendix B, QA for Nuclear Plants
RG 1.26	QA Classifications
RG 1.28	QA Program Design and Construction
RG 1.30	QA Instruments
RG 1.33	QA Requirements for Operation
RG 1.37	QA Fluid Systems
RG 1.38	QA Traffic and Shipping
RG 1.54	QA Protective Coatings
RG 1.64	QA Design of Nuclear Plants
RG 1.74	QA Terms and Definitions
RG 1.88	QA Records
RG 1.94	QA Structures
RG 1.116	QA Mechanical Systems
RG 1.123	QA Procurement
SRP 17.1	QA during Design and Construction
SRP 17.2	QA during Operation
SRP 3.2.2	QA Classifications
ANSI N45.2	QA Requirements

TABLE 4-4
GERMAN AND U.S. ACCEPTANCE STANDARDS FOR RADIATION MONITORING

	<u>FRG</u>		<u>U.S.</u>
RSK 10.1	Radiation Monitoring in Plant	RG 1.21	Measuring Radioactivity Release
RSK 10.2.1	Monitoring Exhaust Water	RG 1.23	Meteorology Programs
RSK 10.2.2	Monitoring Exhaust Air	RG 1.109	Annual Doses to Man
KTA 1501	Dose Monitoring (R)	SRP 2.3.3	Meteorological Measurement
KTA 1503.1	Monitoring Exhaust Air (RE)	SRP 2.3.4-2.3.5	Diffusion Estimates
KTA 1504	Monitoring Liquid Releases (E)	RG 1.97	Accident Instruments
		ANSI N13.1	Radiological Program

5. COMMON CRITERIA (GROUP I)

The Group I criteria are the same as or only slightly reworded versions of the German LWR criteria. Therefore, for this group, comparisons with U.S. criteria should be basically the same as summarized in Refs. 5-1 and 5-2.

5.1. PLANT SAFETY PRINCIPLES (CRITERION 1.1)

This is a general introductory criterion not found in the GDCs (Table 1-7). It requires that at all times the reactor must be capable of being shut down and cooled and that the ALARA concept must be adhered to for radiation exposure during operation and accidents. This must follow from the inherent plant design and safety features as well as through personnel qualification. For satisfaction of this criterion, the remaining criteria and their acceptance standards are to be followed.

5.2. EXTERNAL INFLUENCES (CRITERION 2.6)

As shown in Table 1-7, Criterion 2.6, External Influences, corresponds to GDCs 2 and 4 but is shorter and more general. The GDCs deal in detail with natural phenomena and how they are to be considered in the design, while the German criterion requires general consideration of both natural phenomena (earthquakes, weather, etc.) and human-related external events (sabotage, aircraft, etc.). Application of these criteria can have a significant influence on the design. In fact, this is an area where significant differences have arisen in the U.S. and the FRG in licensing practice to date. Thus, close examination of the respective acceptance standards is warranted.

The major acceptance standards for external events in the U.S. and the FRG are listed in Table 5-1. A large number of standards is available in the U.S. for natural events such as floods, tornadoes, tsunamis, high winds, and earthquakes. Past nuclear plant designs in the U.S. have been affected by consideration of earthquake force and missile protection. Sabotage is considered, per RG 1.17, after the design via the control of access and surveillance. SRP 3.5 concerns aircraft crash, but only guidance in calculating whether the probability is greater than 10^{-6} per year*. By contrast, in the FRG, the standards require predetermined design against airplane crash in RSK 19.1 and in proposed KTA regulations 2202 and 2203. These standards contain detailed acceptable methods of accounting for loadings of crashing aircraft, as summarized in Ref. 5-1, pp. 33 and 34. Sabotage is not covered by the German written standards, but recommended practice, as described in Ref. 5-1, p. 34, includes anti-sabotage design features as well as administrative procedures. The German designs are little affected by storms, and no corresponding written standards are available. However, earthquake standards exist in RSK 18.1 and in KTA 2201; these are comparable to U.S. standards except that the safe shutdown earthquake probability is 10^{-5} per year instead of 10^{-6} per year as in the U.S.

5.3. FIRE AND EXPLOSIONS (CRITERION 2.7)

Criterion 2.7, Fire and Explosion Prevention, contains requirements very similar to GDC 3, namely design and procedures for fire prevention, fire detection, and fire fighting and protection of safety-related components from fire and explosion effects. Acceptance standards are now extensive in both countries, as shown in Table 5-2. The standards are very comparable and represent a fundamental concern for fire protection throughout the plant design review, construction, and operation phases.

* Above probabilities of 10^{-6} /yr, aircraft crash must be treated as a design basis event.

5.4. PLANT SECURITY (CRITERION 2.8)

This is an administrative requirement to monitor personnel traffic in and out of the plant and to prevent unauthorized admittance. No equivalent GDC exists. However, physical security requirements are given in the U.S. by 10CFR73 and SRP 13.6, Industrial Security. These correspond roughly to German perimeter monitoring and reactor building access control. However, they additionally require separate access control for vital areas of the plant.

5.5. DECOMMISSIONING (CRITERION 2.10)

Criterion 2.10 requires consideration of eventual decommissioning in the original plant design and a specific plan for decommissioning in the licensing stage. No equivalent GDC exists. However, U.S. RG 1.86 covers procedures upon termination of operating license and thus corresponds roughly to RSK 16, which briefly covers plant retirement. However, the German standards place more emphasis on provision of design features, such as component arrangement and shielding, in addition to decontamination and radioactive material disposal.

5.6. RADIATION EXPOSURE (CRITERIA 2.3-2.4)

In addition to the radiation monitoring criteria mentioned above, Criteria 2.3 and 2.4 are concerned with allowable radiation exposure to the environment and plant, respectively. They correspond only roughly to GDCs 60 and 61. Criterion 2.3 incorporates an ALARA requirement for radiation burdens to the environment around the plant during normal operation and accidents. Obviously, the exposure magnitude must also be below defined regulatory limits. Criterion 2.4 contains an ALARA requirement on personnel exposure in the plant with emphasis on maintenance operation. The criterion also specifically mentions observation of the radiation protection ordinance during component replacement

operation and the provision of devices for shielding and assuring conformance.

In contrast, the U.S. GDCs are oriented toward control of radioactive material effluents and waste. Provision of shielding to mitigate exposure during storage and handling of effluents and waste and control of release to the environment are required, except that these are not specified in the context of ALARA. Likewise, specific mention is not made of replacement operations.

Acceptance standard for limits of radiation exposure of personnel are given in the U.S. by (1) 10CFR50 Appendix I for offsite doses during plant operation, (2) 10CFR20 for occupational doses during operation, and (3) 10CFR100 for offsite doses during accidents. In the FRG, these are all given by the SSV, that is, the radiation protection ordinance. Table 5-3 presents a comparison of the respective dose limits in the FRG and the U.S. for the above three types of exposures and for the important licensing organ (whole body, thyroid, and bone) (the bone dose being a practiced rather than a formal limit in 10CFR100). The comparison shows that allowable exposure limits in German standards are higher for operational offsite doses and lower for accident releases than in U.S. standards (the U.S. limits for operational doses were lowered by a factor of 100 some years ago). Occupational dose limits are similar. There are some differences in how offsite limits are applied (e.g., site boundaries and times) that tend to make U.S. limits more flexible. Further, the dose limits are augmented by an ALARA approach in the case of operational exposure in both countries and in the German (but not U.S.) standards for accidental exposure.

The German and U.S. acceptance standards for radiation exposure limits and also for implementation of radiation material and accident analysis assumptions are presented in Table 5-4. As shown, U.S. standards are more extensively written at this time.

5.7. EMERGENCY EXITS AND COMMUNICATIONS (CRITERION 2.9)

As shown in Table 1-8, there are two requirements for Criterion 2.9, which has no equivalent GDC. One is that the plant must have distinct and marked escape exits in case of emergency. Second, there must be alarms and means of communication to personnel during emergencies. While such requirements are not covered in the U.S. by GDCs, 10CFR50 Appendix E stipulates the existence of plans for coping with emergencies and inclusion of a synopsis of such plans in the Final Safety Analysis Report (FSAR). Also, 10CFR100.3 briefly mentions emergency procedures for evacuation of the exclusion area boundary (EAB). Recently, an NRC/EPA (Environmental Protection Agency) task force proposed changes to existing federal guidance on emergency planning (EPA-520/1-75-001 and NUREG-75/111) in NUREG-0396 (EPA-520/1-78-016), a planning basis for development of state and local government emergency procedures. Further U.S. regulatory standards are given in RG 1.101 and in the SRPs listed in Table 5-5. By comparison, the written German standards are meager, as shown in Table 5-5.

5.8. VENTILATION AND AIR FILTER SYSTEMS (CRITERION 9.1)

In the U.S., the term "ventilation system" customarily refers to atmospheric control within a building during normal plant operation and certain accidents in which the building air is usually processed over filters to trap fission products before being exhausted to the atmosphere. There is no GDC stipulating such ventilation systems, although regulatory standards for such systems exist (see Table 5-6). However, for the LWR containment atmosphere, an engineered-safety-feature recirculation cleanup system designed to mitigate post-accident radiological consequences is required by GDCs 41 through 43.

Regulatory acceptance standards for ventilation systems to conform during normal operation radiological exposures with 10CFR50 Appendix I

and 10CFR20 are given by RG 1.140 and ANSI N509-1976. This RG is closely tied to the ALARA concept, with additional equipment requirements if the cost-benefit ratio is favorable. Post-accident cleanup systems, both the containment atmosphere recirculation system required as necessary by GDC 41 and ventilation systems for radwaste, fuel storage, and other areas where radioactivity is contained, are covered by RG 1.52. These are not given in the context of ALARA. Ventilation of the control room, as required by GDC 19 to maintain occupant radiation exposures below 5 rem whole body during accidents, is treated in detail by SRP 9.4.1. Ventilation systems for other areas are covered by SRP 9.4.2 through 9.4.5.

In contrast, German Criterion 9.1 is more comprehensive, covering mainly exhaust vent systems but not necessarily excluding internal circulation and filtration systems, if such are necessary to meet dose exposure criteria. However, no comparison is made between Criterion 9.1 and GDCs 41 through 43 in Table 1-8, since the emphasis of the German criterion is on ventilation systems for plant operation. Also, for HTRs a containment filter cleanup system is not needed for mitigation of design basis accidents. Past inclusion of the system in U.S. design stemmed from using conservative fission product release in the hypothetical siting event, which is not part of the FRG licensing procedure.

The German acceptance standards for ventilation systems consist of RSK 9 and a KTA 3601 draft in preparation. These are comparable to RG 1.140 and SRP 9.4 in scope and requirements.

REFERENCES

- 5-1. Richardson, J. A., "Summary Comparison of West European and U.S. Licensing Regulations for LWRs," Nucl. Eng. Intern. 21, 32-41 (Feb. 1976).

5-2. "Gas Reactor International Cooperative Program Interim Report.
United States/Federal Republic of Germany Nuclear Licensing
Comparison," General Electric Report COO-4057-9, September 1978.

TABLE 5-1
MAJOR U.S. AND GERMAN ACCEPTANCE STANDARDS FOR EXTERNAL EVENTS

	<u>FRG</u>		<u>U.S.</u>
RSK 18.1	Earthquakes	RG 1.12	Seismic
RSK 19.1	Airplane Crash	RG 1.17	Sabotage
RSK 19.4	Third Party Effects	RG 1.29	Seismic
KTA 2201.1	Seismic (R)	RG 1.59	Flood
KTA 2201.5	Seismic (R)	RG 1.60	Seismic
KTA 2202	Airplane Crash (REV)	RG 1.61	Seismic
KTA 2203	Airplane Crash (REV)	RG 1.76	Tornado
		RG 1.102	Flood
		RG 1.100	Seismic
		RG 1.117	Tornado
		SRP 2.4	Flood, Tsunami, Ice
		SRP 2.5	Seismic
		SRP 3.2	Seismic
		SRP 3.3	Wind, Tornado
		SRP 3.5	Missiles, Aircraft
		SRP 3.7	Seismic
		SRP 3.10	Seismic
		10FRC100.10	Site Evaluation
		10CFR100	Seismic and Geological
		Appendix A	
		ANSI N18.5	Seismic
		ANSI N170	Flood
		IEEE 344	Seismic

TABLE 5-2
FIRE PROTECTION STANDARDS IN THE FRG AND U.S.

<u>FRG</u>		<u>U.S.</u>	
RSK II	Fire Protection	RG 1.7	Combustible Gas
RSK 19.2	Chemical Explosions	RG 1.91	Transportation Explosions
RSK 19.3	Poison and Combustible Gas	RG 1.120	Fire Protection
KTA 2101	Fire and Explosion (REV)	SRP 9.5.1	Fire Protection

TABLE 5-3
COMPARISON OF U.S. AND GERMAN RADIATION EXPOSURE LIMITS
(CP = construction phase; OP = operation phase; SSV = Strahlenschutzverordnung)

	<u>FRG</u>	<u>U.S.</u>
<u>Normal Operation - Annual Offsite Dose Limits</u>		
Reference	SSV, para. 45	10CFR50 Appendix I
Whole body - liquid effluents	30 mrem	3 mrem
- exhaust air (gaseous release)	30 mrem	5 mrem
Thyroid - infants, food chains	90 mrem	15 mrem
Bone	180 mrem	15 mrem
<u>Normal Operation - Occupational Dose Limits</u>		
Reference	SSV, para. 49(a)	10CFR20
Whole body - quarter year	2-1/2 rem	3 rem
- year	5 rem	<12 rem ^(b)
Thyroid - quarter year	15 rem	--
- year	30 rem	30 rem
Bone - quarter year	15 rem	--
- year	30 rem	15 rem
<u>Accident Offsite Dose Limits (single occurrence)</u>		
Reference	SSV, para. 28	10CFR100
Whole body - CP	5 rem	20 rem
- OP	5 rem	25 rem
Thyroid - CP	15 rem	150 rem
- OP	15 rem	300 rem
Bone - CP	30 rem	75 rem
- OP	30 rem	150 rem

(a) In exceptional cases, annual limits may be exceeded by a factor of 2, not to exceed a factor of 5 in a lifetime.

(b) Not to exceed 5 (N-18) rem in a lifetime, where N = age of worker.

TABLE 5-4
FRG AND U.S. ACCEPTANCE STANDARDS FOR RADIATION EXPOSURE AND CONTROL
(Including Accident Assumptions)

FRG	U.S.
Strahlenschutzverordnung (SSV)	10CFR50 Appendix I
RSK 2.2 Assumptions for Radiation Exposure in the Environment	10CFR20 and 10CFR100
RSK 15 Fuel Handling and Storage	RG 1.13 Fuel Storage Design
KTA 3603 Handling Contaminated Water (RE)	RG 1.3-1.4 Assumptions for LOC
	RG 1.5 Assumptions for Steamline Break
	RG 1.21 Releases in Effluents
	RG 1.24 Assumptions of Rad Waste Tank Failure
	RG 1.25 Assumptions of Fuel Handling Accident
	RG 1.98 Assumptions of Off Gas System Failure
	RG 1.109 Annual Doses to Man
	RG 1.112 Calculation of Release of Gas and Liquid Effluents
	RG 1.113 Estimated Dispersion of Liquid Effluents
	SRP 12.1 ALARA Concept
	SRP 12.2 Radiation Sources
	SRP 12.3 Radiation Protection
	SRP 12.4 Dose Assessment
	SRP 2.4.12 Accidental Release of Liquid Effluents
	SRP 6.5.3 Fission Product Control

TABLE 5-5
U.S. AND GERMAN EMERGENCY PLANNING STANDARDS

<u>FRG</u>		<u>U.S.</u>	
RSK 12	Exits and Alarms	10CFR50 Appendix E	Emergency Plans
KTA 3901.1	Alarms and Communications (R)	10CFR100.3	Site Criteria
Proposed KTA 2101	Exits	NUREG 75/111	Emergency Response
		NUREG 0396	Emergency Plans
		EPA-520/1-75-001	Protective Actions
		RG 1.101	Emergency Planning
		SRP 2.2.1-2.2.2	Site Locations and Reports
		SRP 13.3	Emergency Planning

TABLE 5-6
GERMAN AND U.S. ACCEPTANCE STANDARDS FOR VENTILATION SYSTEMS

<u>FRG</u>		<u>U.S.</u>	
RSK 9	Ventilation Systems	RG 1.52	Ventilation Air Filter Systems
KTA 3601	Ventilation Systems (REV)	RG 1.140	Ventilation Systems
		SRP 9.4.1	Control Room Ventilation
		SRP 9.4.2	Spent Fuel Ventilation
		SRP 9.4.3	Radwaste Ventilation
		SRP 9.4.4	Turbine Ventilation
		SRP 9.4.5	Engineered Features Ventilation

6. SUMMARY AND IMPLICATIONS OF CRITERIA

The foregoing detailed evaluation of the proposed German safety criteria for HTRs has shown that these criteria take into account, where necessary, inherent and specific characteristics of the HTR concept while dovetailing congruously with the safety principles and intent of the previous German LWR criteria. For the most part, the HTR criteria are worded in general enough terms so that currently recognized HTR design options are accommodated. This applies to differences between U.S. and German design features such as pebble bed versus prismatic cores. It applies less to U.S./FRG safety philosophy differences. Significant consideration was given to assure blanket application to the different HTR concepts, such as gas turbine, steam cycle, process heat, etc.

There are a number of criteria in the BMI draft which were carried over from the previous German LWR criteria without major change but which are not found in U.S. GDCs. These are:

1. Plant Safety Principles - general overriding safety ground rules and philosophy for all the criteria.
2. Testability - a separate criterion giving in-service testing requirements and design requirements for non-testable components.
3. Reactor Internals.
4. Ventilation Systems.

5. Health Physics.
6. Plant Security.
7. Emergency Exits and Communication.
8. Decommissioning.

None of these German criteria, if implemented verbatim in U.S. safety criteria, would significantly impact current U.S. HTR design or operating practice and/or approach. In fact, the comparison has shown that many of the requirements are already specified in U.S. regulatory standards (such as RGs or SRPs) or in industry standards.

Neither the LWR nor HTR German safety criteria versions contain specific criteria on the following subjects, which are explicitly spelled out in U.S. GDCs:

1. Sharing of Structures and Systems (GDC 5).
2. Reactor Coolant Makeup (GDC 33).
3. Cooling Water (GDC 44-46).

The first of these is covered by redundancy requirements throughout the German criteria for safety systems. The second is not so important for the HTR concept because loss of primary coolant does not impair coolability. Omission of explicit cooling water criteria appears to be based on inclusion of the cooling water system as part of the afterheat removal system. However, the cooling water system can also be the link to the ultimate heat sink for such possible HTR systems as a liner cooling system, circulator bearing water system, electric motor water cooling system, etc. Probabilistic risk analysis of the HTR cooling water system redundancy (Ref. 6-1) indicates quantitatively a significant safety importance for diversity in this system, due not only to rejection of

core afterheat but also to heat loads on the components. Thus, redundancy or reliability constraints on this system should be explicit in the safety criteria.

Several safety philosophy concepts that are contained in the German LWR safety criteria and carried over to the HTR criteria draft deviate from U.S. LWR criteria and from HTR practice in the U.S. These are:

1. Site-independent design of the containment and PCRV for human-related external influences, primarily aircraft crash. The (site-dependent) flexibility in the U.S. is related to the lower probability of aircraft crash for many U.S. sites.
2. Provision of an emergency control station as a backup to the control room and permitted long-term control of accidents from this station.
3. Application of ALARA concepts to accidents as well as normal operational releases.
4. Separate and redundant electrical switchyards.

Designing for aircraft crash could add significantly, but not drastically, to HTR containment structure design costs, assuming a conventional lined containment. For a Fort St. Vrain type structure, the cost increase would be more pronounced. The second item would necessitate additional instrumentation and radiological shielding for the backup control station. The third item would not impact HTR designs significantly because of wide safety margins for design basis accidents. The fourth item is not a high-cost feature. Regarding safety philosophy, it is noted that in the BMI draft the single-failure concept, as previously defined for the German LWR criteria (see Appendix B), was retained. However, some modifications in the way the single-failure

concept is applied for some specific systems were incorporated in the HTR specific criteria summarized below. Unmodified, the German single-failure concept requires the assumption of failure of one system redundancy plus a second down for maintenance at initiation of the accident (N-2 redundancy).

The key achievement of the proposed HTR criteria is the drafting of HTR specific requirements tailored to the inherent features of the HTR design. These can be summarized as follows:

1. Differentiation between pressure-bearing (PCRVR and penetrations) and non-pressure-bearing (liner) parts of the reactor vessel. These have different inspection and testing requirements. Both warm and cold liner concepts are covered.
2. Mitigation of design basis depressurization accident (DBDA) consequences, if necessary, by restricting blowdown flow area.
3. General stipulation of minimum containment backpressure for core auxiliary cooling system afterheat removal to have "appropriate" safety margin. Differences in U.S. and German safety margin assumptions would be relegated to respective regulatory standards.
4. Modification of the criteria for LWR afterheat removal after loss of cooling to afterheat removal by an auxiliary system during accidents in the event the main afterheat removal system is unavailable. High availability and redundancy, where possible, are desired for the main afterheat removal system to reduce the demand frequency for the auxiliary system.

5. Allowance of inherent HTR design characteristics for afterheat removal design. This includes consideration of allowable time lag for startup of an active system, possible use of a passive system, and (N-1) redundancy for maintenance operations capable of restoration.
6. Allowance of manual or automatic activation of the reserve reactor shutdown system, depending on accident analysis.
7. Allowance of inherent HTR design characteristics in the design of the two reactor shutdown systems. This includes utilization of negative temperature coefficients, allowable time lags for insertion, etc.
8. More explicit definition of the containment function (than in GDC 16), allowing controlled venting and filtering of the containment after accidents if regulatory dose limits are met.
9. Elimination of explicit requirement for containment heat removal or fission product cleanup systems (German LWR Criterion 8.5 not carried over). The former system is not needed for HTRs; the latter, if needed, is implicitly covered by the ventilation system criteria.

All of these general HTR-specific requirements are consistent with or close to the current U.S. design approach. Therefore, they would not be expected to impact U.S. HTR designs by themselves. Subsequent regulatory standard interpretations in the U.S. and the FRG would likely produce differences in the design margins, redundancies, etc.

The BMI draft goes somewhat beyond formulating HTR-specific criteria. In certain cases, some changes were made which reflect improvements or additions which the BMI would like to see in the LWR criteria also. Examples of these are:

1. Addition of a separate criterion for providing a barrier for liquid contaminants in plant buildings to protect the structures and ground water.
2. Instrumentation division into "event" and "consequence" categories with separate requirements, including a new one to measure environmental consequences.
3. More detailed radiation monitoring equipment requirements.

None of these are high-cost balance-of-plant additions.

REFERENCE

- 6-1. Joksimovic, V., and K. N. Fleming, "Applications of Probabilistic Risk Assessment in the Development of HTGR Technology," General Atomic Report GA-A14289, July 1977.

7. ACKNOWLEDGMENTS

This report was made possible by the support of the U.S. Department of Energy and also by the cooperation of the FRG nuclear licensing authorities under the U.S./FRG gas-cooled reactor Umbrella Agreement. Invaluable assistance was derived from discussions with FRG HTR vendors and TÜV and BMI personnel involved in preparation of the proposed HTR criteria. In particular, the author wishes to thank Dr. Fechner of BMI, Dr. Hofmann of TÜV-Essen, and Drs. Stoelzl, Sommer, and Ledermann of HRB.

APPENDIX A

ENGLISH TRANSLATION OF BMI DRAFT OF FRG CRITERIA FOR HTRs

Contents

Section 1

- Criterion 1.1 Plant Safety Principles

Section 2

- Criterion 2.1 Quality Assurance
- Criterion 2.2 Testability
- Criterion 2.3 Radiation Exposure to the Environment
- Criterion 2.4 Radiation Exposure in the Plant
- Criterion 2.5 Working Conditions and Health Physics
- Criterion 2.6 External Influences
- Criterion 2.7 Fire and Explosions
- Criterion 2.8 Plant Security
- Criterion 2.9 Emergency Exits and Communications
- Criterion 2.10 Decommissioning of Nuclear Power Plants

Section 3

- Criterion 3.1 Reactor Core Design
- Criterion 3.2 Coupling Characteristics of the Reactor Core
- Criterion 3.3 PCRV Internals
- Criterion 3.4 Systems for Control and Shutdown of the Reactor

Section 4

- Criterion 4.1 Reactor Coolant Boundary
- Criterion 4.2 Design Basis of Reactor Coolant Boundary
- Criterion 4.3 PCRV

Section 5

- Criterion 5.1 Afterheat Removal-Specified Normal Operation
- Criterion 5.2 Afterheat Removal System for Accidents

Section 6

- Criterion 6.1 Plant Protection System
- Criterion 6.2 Accident Instrumentation
- Criterion 6.3 Operational Instrumentation
- Criterion 6.4 Control Room and Emergency Control Station

Section 7

Criterion 7.1 Electrical Supply

Section 8

Criterion 8.1 Nuclear Reactor Containment

Criterion 8.2 Containment Design Basis

Criterion 8.3 Leaktightness Tests

Criterion 8.4 Containment Penetrations

Criterion 8.5 Liquid Contaminant Barrier

Section 9

Criterion 9.1 Ventilation Systems

Section 10

Criterion 10.1 Radiation Monitoring

Criterion 10.2 Activity Monitoring in Exhaust Air and Water

Criterion 10.3 Environmental Monitoring

Section 11

Criterion 11.1 Fuel Handling and Storage

HTR SAFETY CRITERIA (DRAFT)

Section 1

Criterion 1.1 Plant Safety Principles

A nuclear power plant must be so constructed and operated that at any time during specified normal operation and accidents the plant can be safely shutdown, maintained in a shutdown condition, and the residual heat removed. Radiation exposure to personnel and the environment must be held, even below dose limits prescribed by the German atomic law, as low as possible within the state of knowledge and technology. Required safety provisions are to be based on the following groundrules.

1. The first and foremost groundrule is formed by higher requirements on the design and the quality of the plant as well as the qualification (expertise and reliability) of the personnel. These alone, without taking credit for engineered safeguards, must provide the best possible accident-free operation of the plant with minimum environmental impact. To this end, safety-related design, construction and operating groundrules are to be applied. In particular, to be achieved are:
 - o consideration of sufficient safety margins in the design of the systems and plant components;
 - o application of proven materials;
 - o ease of maintenance for systems and components under special consideration of radiation exposure of personnel;
 - o health physics and ergonomic measures for occupational locations;
 - o comprehensive quality assurance in construction, building and operation;
 - o performance of periodic tests of appropriate measure;
 - o safety surveillance of operating conditions; and
 - o recording, evaluation and safety assessment of operating experience.

From general technical experience, it is recognized that during the lifetime of a plant, malfunction of components or systems (anomalous operating conditions) will occur. For governing these anomalous conditions, systems for operating control and supervision are to be provided. These systems are to be designed such that accidents resulting from anomalous operating conditions can be avoided with sufficient reliability.

2. As a second groundrule, additional measures for the control of accidents are to be met, provided by sufficiently reliable* engineered safeguards. These safeguards are to be designed such that the personnel and the public are protected from consequences of accidents with sufficient assurance. To this end, the following design rules are to be applied:

- o redundancy, diversity, extensive use of disassociated subsystems and spatial separation of redundant subsystems;
- o safety-related system behavior during malfunction of a component or subsystem;
- o preference of passive over active safety functions.

Further, provisional organizational technical measures in appropriate measure are to be instituted within and outside the plant for determination and mitigation of exceptional events.

*Note on methodology: For assessment of the equivalent value of the safety concept, reliability analyses of systems and components important to safety are to be performed with the help of probabilistic methods, insofar as this is possible for the required accuracy within the state of knowledge and technology. This is complementary to overall judgments of safety of the plant based on deterministic methods. The required reliability of any system or component is to be determined depending on accident occurrence probabilities and consequences.

Section 2

Criterion 2.1 Quality Assurance

Planning, manufacture, maintenance and proof of quality for plant parts, systems and components are to be assured in scope and means corresponding to their safety impact. This includes both technical and organizational measures. The quality assurance shall adhere to groundrules and procedures appropriate to the special requirements of nuclear safety according to the state of knowledge and technology.

Criterion 2.2 Testability

Fundamentally, all plant parts must be so constructed and arranged that they can be tested and inspected in sufficient scope as befits their safety significance. This must be possible before plant startup and thereafter in regular time intervals. If a plant component cannot be subjected to regular periodic tests of the required scope according to the state-of-the-art for detection of potential defects, then special measures are to be taken for maintaining the fault-free condition or function of the plant component. These measures can include:

- o additional safety margin in the design;
- o special material specifications, such as purity, etc.;
- o fabrication quality;
- o constructive design, for example, redundant structures; and
- o limiting and controlling of operational parameters.

In addition, the consequences of failures still possible must be limited such that, even if those incidents which have to be considered under these circumstances would actually occur, the reactor is shutdown and held in a shutdown condition and the residual heat removed. Also, the removal or possible release of radioactive material must be held, within the limiting values established by the radiation protection ordinance, to as low as possible.

Criterion 2.3 Radiation Exposure to the Environment

For protection of the environment from radiological effects from the nuclear power plant, it must be ensured that all safety-related plant components are so designed and kept in such a condition that radiation exposure to the environment by direct radiation from the plant as well as removal and possible release of radioactive material is held,

in accordance with the state of knowledge and technology, even within the limiting values to as low as possible. For this purpose, these plant components must be so constructed and protected against consequences that they can fulfill their safety-related functions both during specified normal operation and accidents.

Criterion 2.4 Radiation Exposure in the Plant

All plant parts of a nuclear facility which contain or may contain radioactive material must be so constructed, arranged, and shielded that the radiation exposure to personnel during all activities required during normal operation is held, in accordance with the state of knowledge and technology, even within the limiting values to as low as possible. For fulfillment of this principle, plant components must be specifically constructed and arranged for ease of maintenance. Maintenance operations of replacement, repair, inspection, and periodic tests must be able to be performed throughout the plant life while fulfilling the above principle. Corresponding required measures provided for this purpose may include:

- o maintenance equipment;
- o transport equipment;
- o storage facilities;
- o handling equipment;
- o surveillance equipment; and
- o shielding and corresponding space.

Criterion 2.5 Working Conditions and Health Physics

Work tasks, working conditions and environment, work organization and work cycles are to be arranged under consideration of ergonomic principles and health physics such that requirements are met for optimally safe occupational procedures.

Criterion 2.6 External Influences

All plant components required for nuclear reactor shutdown, maintaining the shutdown condition, removing residual heat, or preventing possible release of radioactive material must be so designed and be maintained in such condition that they can fulfill their safety function during external influences, insofar as such influences logically enter into consideration. Included are natural occurrences such as earthquakes, foundation shifts, storms, tides and flood as well as

possible effects from biological organisms (i.e., swarms of birds, mussel growth in cooling water supply) or other external influences such as third party interference, airplane crash, effects of dangerous and, particularly, explosive materials and landslides. Design of these plant components is to be based on:

1. The appropriate worst natural phenomenon or other external event, within the state of knowledge and technology, which must be taken into account at the respective site location.
2. Combinations of more than one natural phenomenon or other external influence as well as combinations of these influences with accidents, insofar as the simultaneous occurrence based on probability and magnitude of consequences must be taken into consideration.

The foreseeable future development of the site characteristics must be considered.

Criterion 2.7 Fire and Explosions

Required measures for protection against fires and explosions in the plant must be met. Safety-related plant components must be so constructed and arranged that the fulfilling of their functions is not prevented through fires or explosions. Suitable equipment for early detection and fighting of fires and explosions must be provided. This equipment must be so constructed and secured that, even in the event of its own failure, damage or malfunction, the functionality of safety-related plant components is not impaired, in certain cases under consideration of the component redundancies.

Criterion 2.8 Plant Security

The whole nuclear power plant property and, in addition, plant areas within and outside of same which require special protection must be secured to prevent access of unauthorized personnel. All access to these areas must be so arranged that a complete control of personnel and freight traffic is possible.

Criterion 2.9 Emergency Exits and Communications

The nuclear power plant must have escape routes which are simple, clearly and continuously marked, and reliably lighted. Suitable alarm systems and means of communication must be available with which all persons present in the plant can be properly instructed what to do in case of an incident from at least one central location. Communication within and outside the nuclear power plant required for safety during specified normal operation, for coping with accidents, and even for unforeseeable events must be assured at all times.

Criterion 2.10 Decommissioning of Nuclear Power Plants

Nuclear power plants must be constructed such that they can be decommissioned in compliance with the radiation protection ordinance. A concept for the deposition of the plant after final decommissioning under compliance with the radiation protection ordinance must be available.

Section 3

Criterion 3.1 Reactor Core Design

The reactor core must be, with respect to its construction and power generation, so designed and manufactured that, in association with other plant systems, specified limiting values are not exceeded during accidents. In particular, this applies to activity release from the fuel elements and loads on safety-related plant components and systems, especially those for the core structure and core components connected with shutdown and cooling capability.

In the design of the reactor core and consideration of design basis events*, the most unfavorable power distributions, heat storage and transport processes, and plant power and fuel loading histories are to be assumed. Further, in the application of design data, safety margins are to be considered which sufficiently cover uncertainties in the basic data, calculational models, or measurements.

Criterion 3.2 Coupling Characteristics of the Reactor Core

The reactor core must be so designed that inherent feedback characteristics will moderate all reactivity excursions resulting from pertinent slow and rapid reactivity rises. Such moderation must be sufficient such that, in association with other inherent features and safety systems, significant damage does not occur to the reactor, to the radioactivity barriers or to the primary coolant system. To this end, precautions are to be taken in the design to assure that the prompt portion of the reactivity temperature coefficient is sufficiently negative during specified normal operation and during accidents.

Criterion 3.3 PCRV Internals

The PCRV internals must be so constructed and arranged that specified load limits are not exceeded during normal operation. In addition, the internals must be so constructed that their function for safe shutdown of the reactor and sufficient removal of residual heat is assured even for accident condition loadings so that severe consequences, for example, reactivity increases, are precluded.

Criterion 3.4 Systems for Control and Shutdown of the Reactor

The systems for control and shutdown of the reactor core must be capable of subjugating all reactivity changes during specified normal operation and accidents such that respective limiting values

*Event starting point is the steady state condition during normal operation.

of the reactor plant for these cases are not exceeded in the course of all transients which must be considered. Reactivity shifts and ramps from reactivity control equipment are to be so limited that, in association with the safety systems, specified limiting values for the reactor plant are maintained for erroneous control commands. The reactor core and the control systems must be so synchronized with each other that fluctuations of the neutron flux which could lead to exceeding specified limiting values for fuel element activity release are either not possible or are reliably foreseen and limited.

Two shutdown systems are to be provided. Both can be utilized for control of the reactor as long as by so doing the fulfilling of the following tasks is not prevented:

1. First Shutdown System

The first shutdown system must by itself be in the position to render and hold the reactor subcritical from specified normal operation or accidents, including worst control rod failure. This must be done within a time period, based on accident analysis, whereby plant safety limits are not exceeded. The reactivity introduced at the time of shutdown is to be measured in order to assure that specified limits will be maintained sufficiently long through the automatically initiated measures.

Failure of control rods most affecting the reactivity is to be considered insofar as such failure can be caused by a single disruption. At least one control rod must be assumed to be unavailable. Safety margins are to be considered in the physical design. The failure of control rods most affecting reactivity need not be considered if both shutdown systems, including the PPS signals, are equivalent with respect to shutdown characteristics, effectiveness, and timing.

2. Second Shutdown System

A second shutdown system which is independent of and of different construction than the first shutdown system is to be provided. By itself, it must be capable of rendering the nuclear reactor subcritical from any normal operating condition. It must be able to maintain subcriticality arbitrarily long for the most unfavorable reactivity balance condition possible under circumstances which come into consideration for the system. In this regard, a sufficient shutdown reactivity margin must be assured during the core lifetime under consideration of safety factors in the physical design.

If the first shutdown system is not capable by itself of maintaining the reactor core subcritical arbitrarily long in the most unfavorable reactivity balance situation, then the necessary second shutdown system must be designed to the relevant accident conditions. In this case, the requirements in the above section (1), regarding failure of control rods or elements, apply to the whole second shutdown system. Whether or not a portion of the second shutdown system is to be automatically activated must be determined from the specific accident conditions.

If it is demonstrated that inherent reactor characteristics contribute positively to the shutdown, then they can be considered in the design of the shutdown systems and replace hardware measures. The design of the shutdown systems must consider the worst fuel burnup condition.

If the shutdown systems possess common components with the system for normal control of the nuclear reactor, it must be assured that no function of the control system, not even a function produced by a fault in the control system, prevents the predesigned functioning of the shutdown system.

Section 4

Criterion 4.1 Reactor Coolant Boundary

For prevention of release of radioactive material, an enclosure (boundary) of the reactor coolant is to be provided. Fundamentally, the enclosure should encompass, depending on the design concept:

- o the leaktight membrane (liner) of the pressure-bearing vessel (see Criterion 4.3);
- o penetrations through the pressure-bearing vessel, including their closures which have a leaktightness or pressure-bearing function;
- o reactor coolant piping penetrating the liner or vessel closures, including the first isolation valves;
- o the isolation lines, including the first isolation valves; and
- o pipe lines located inside the liner interfacing with reactor coolant outside (for example, heat exchangers in the primary circuit), up to the juncture on the vessel closure or liner.

The pressure vessel does not belong to the so-defined boundary of the reactor coolant.

Criterion 4.2 Design Basis of the Reactor Coolant Boundary

The boundary of the reactor coolant must be designed with sufficient safety factors such that it withstands maximum loadings occurring during specified normal operation and accidents. All components of the enclosure must be constructively arranged such that the required initial tests during fabrication and installation are enabled. Through material selection, proper structural forming, welding and in certain cases heat treatment, a sufficiently ductile material condition must be maintained on all parts of the enclosure for the life of the plant during all operating and accident conditions. Penetrations through the pressure-bearing vessel should be secured against dislodgement. If failure of closures is within the design basis, the maximum blowdown flow area is to be limited to values suitable to the accident conditions through corresponding design measures. Components of the enclosure must not fail such that intolerable damage results to safety-related plant parts.

Criterion 4.3 PCRV

The pressure-bearing vessel (PCRV) encloses the reactor and carries the load of the inner pressure. The following requirements are placed on the PCRV:

1. The vessel is to be designed such that the pressure-bearing function is assured for specified normal operation and accidents.
2. For all loading combinations which may occur, it must be assured that the vessel can fulfill its safety function in conjunction with the enclosure of the reactor coolant.
3. The load-carrying portion of the pressure-bearing vessel is to be protected against intolerable temperature demands. If necessary, a thermal shield is to be provided whose functionability is to be monitored. If local damage to the heat shield cannot be precluded, then such local zones are to be included in the monitoring.
4. The pressure-bearing vessel is to be monitored such that safety-related deviations from nominal conditions are deleted.
5. If coolant leakage through the liner is to be reckoned with, suitable measures are to be taken to assure that the integrity of the vessel is not thereby impaired (for example, through corresponding design of the vessel or through a drainage system).
7. In the design of the pressure-bearing vessel, induced loadings from external influences (pressure waves, airplane crash, design basis and SSE earthquakes) are to be considered.
8. In order to achieve a sufficient safety margin for the stress limit of the pressure-bearing vessel, in addition to requirements (1) through (7), it must be demonstrated that failure of a prestress cable does not occur for a postulated overload or assumed disturbance, for example, failure of a single prestress wire.

Section 5

Criterion 5.1 Afterheat Removal-Specified Normal Operation

A reliable and redundant system must be provided for removal of residual heat during shutdowns in specified normal operation. It must be so constructed that specified normal operational limits are maintained for activity release from the fuel elements as well as for loadings on other safety-related plant parts (for example, primary circuit components, shutdown system, and reactor coolant boundary) during their entire lifetime. If necessary, the redundancy of the afterheat removal system for accidents can be utilized for fulfillment of the redundancy requirement for this system.

Criterion 5.2 Afterheat Removal System for Accidents

A reliable and redundant system for the removal of residual heat during accidents (afterheat removal system) must be provided. It must be so constructed that for design basis initiating events, for initial conditions coming into consideration, and for accident boundary conditions (for example, rupture sizes, rupture locations, and transients in the reactor cooling system), the following requirements are fulfilled:

- o The afterheat removal system must be able to fulfill its safety-related function even during in-operation maintenance with simultaneous occurrence of a single failure (compare with the single failure concept). If the afterheat removal can be interrupted for a time on the basis of system conditions or characteristics of the reactor, then for in-operation maintenance and inspection operations which can be concluded within this time, postulation of simultaneous occurrence of a single failure is not required.
- o Load limits for components of the activity enclosure, the afterheat removal system and the shutdown system are to be specified under consideration of the expected occurrence frequencies of accidents such that these components can always fulfill their safety-related functions.
- o For accidents with ingress of foreign media, chemical reactions and their effects are to be limited such that afterheat removal and shutdown are assured and loadings on the containment remain within specified limiting values.
- o Portions of the operational system can be incorporated in the afterheat removal system if:
 - (1) their function readiness during specified normal operation can be monitored;

- (2) the necessary subsystems possess the required reliability;
- (3) the operational readiness of the operational subsystem provided to the afterheat removal system is assured within a time period from accident initiation dictated by the special accident;
- (4) these subsystems are correspondingly designed, fabricated, and sufficiently periodically tested.

In the determination of the afterheat removal after a depressurization accident, a minimum backpressure is to be assumed which is either the site atmospheric pressure or the post-blowdown equilibrium pressure resulting from worst conditions (for example, worst-case afterheat, maximum specified leak rate from the containment, worst heat transfer to the structure) and with inclusion of a safety factor.

If the afterheat can be removed in principle, utilizing inherent characteristics (for example, heat transmission mechanisms or heat storage) or if the afterheat removal can be interrupted for a length of time without exceeding specified limiting values, then these characteristics can be considered in the design of the afterheat removal system and obviate the need for certain hardware.

Section 6

Criterion 6.1 Plant Protection System

The nuclear power plant must be equipped with a reliable⁽¹⁾ plant protection system (PPS) which initiates protective actions when predetermined limits (setpoints) are reached. The PPS must be so constructed that it can fulfill its safety-related function even during maintenance operations with the simultaneous occurrence of a single failure in the system. Neither manual actions nor commands given for operational control and regulation should be able to impair or prevent necessary protective actions. The PPS is to be so designed and built that it fulfills requirements dictated by accident analysis.

Basically, at least two criteria for initiation of protective actions must be available for any event to be controlled. Different physical parameters (for comparison with setpoints) should be incorporated in the initiating criteria. If the requirement for two initiating criteria cannot be met, then the measurement reading dependability of the single parameter used must be designed and constructed to be valued higher with regard to safety⁽²⁾ in comparison to measurement reading dependability of other parameters. Process variables which are derived

(1) Preferred methods to be applied for a "reliable" design of the PPS are:

- o redundant design of components, systems and subsystems, and spatial separation and installation corresponding to the working distance of possible failure-initiating events;
- o faults or failures should be self-alarming as far as possible;
- o application of differently constituted types of equipment (diversity principle).

(2) Preferred measures to be applied for "higher valued design or construction" are:

- o utilization of differently constituted types of equipment (diversity principle);
- o load limit tests, test cycles.

from other parameters or which only produce the initiating signal for protective action in combined working with other process variables (i.e., "and" gate) are to be considered as a single variable for safety.

Basically, the mechanical and electrical devices of PPS activation (measurement sensors up to and including the setpoint indicator) may not be used for functions in the realm of reactor control. Exceptions are allowed only if necessary due to the technical uniqueness of the PPS design or the measurement, control or operational systems, and only when in the context of accident analysis it is demonstrated that the common failure of the measurement channels for operation and for the PPS is controlled in context of an accident.

Redundant parts of the PPS fundamentally should possess devices for measurement processing and actions signaling which are independent of each other. Interfacing links may not devalue the systems redundancy and safety action initiation. Redundant parts of the PPS are to be physically separated from each other and provided with electrical power and required subsistence such that failures within one of the subsystems cannot simultaneously impair the function of other systems.

The PPS must be so designed, effected, and operated that even for any failure in the PPS itself, it does not initiate any actions which may bring the plant into a dangerous condition. The PPS is to be maintained in an operational readiness state, down to subsystems required for the plant condition, whenever fuel material or fluid, gaseous or aerosol-forming radioactive material is present within the plant.

Criterion 6.2 Accident Instrumentation

Accident instrumentation is to be provided which must fulfill the following general requirements. Before, during and after an accident or exceptional event (which could lead to radiation exposure above specified regulatory limits for accidents), a sufficient overview of the operating conditions must be enabled, all significant data describing the plant condition as well as the important weather data must be indicated, and documentation of same in the proper time sequence must be assured. In addition to the accident instrumentation inside the plant, the conduction of measurements of radiological levels and weather data outside the plant in the vicinity of the nuclear power plant must be assured in order to enable emergency protection measures to be introduced and carried out.

Classification of accident instrumentation into accident event and consequence instrumentation is to be established. A mixing of the event and consequence instrumentation is allowed. For the event instrumentation, the following requirements apply:

1. The event instrumentation is to be so designed that system and component data selected for a later elucidation of the cause and effects during the accident are clearly and continuously documented for reconstruction of the accident sequence.
2. Redundant equipment must be provided for recording the selected system and component data. The unavailability of one component of the event instrumentation may not lead to the prevention of the recording.

For the accident consequence instrumentation, the following requirements apply:

1. The accident consequence instrumentation is to be so designed that reliable and sufficiently precise indication as well as appropriate documentation is provided for data which after occurrence of an accident or exceptional event are necessary for the judgment of the plant safety, the functionality of safety systems, and decisions regarding emergency protection measures.
2. A redundant measurement reading and measurement data processing of a measurement quantity is not required if either of two conditions can be demonstrated. One is if the information content of this quantity can be conveyed by measurements of other quantities of the accident consequence instrumentation. The second is if the failure of the quantity measurement can be acceptable for a determined time period and within this time period and under the prevailing conditions the failure can be repaired or a substitute solution can be realized.
3. Indication and recording of every measurement quantity of the accident consequence instrumentation must be achieved in the power plant control room. Also, in a plant area protected against external influences (emergency control station), there must be provided indication and recording of accident consequence instrumentation which is necessary to fulfill specified instrumentation tasks after occurrence of an external event. If a measurement quantity is redundantly read, one reading can be indicated and recorded in the emergency control station and the other in the control room.

Criterion 6.3 Operational Instrumentation

The nuclear power plant must have equipment for conductance of operation (control and regulation), monitoring and alarm. At any time during specified normal operation the equipment must enable an

orderly conductance of operation and a sufficient overview on the operating conditions of the plant. All important or safety-related condition variables are to be recorded through appropriate equipment. As a rule, the usual practice of redundancy is to be continued in the equipment for operation procedures, monitoring, and alarming. Emergency alarm equipment must be available which promptly indicates changes in operating circumstances, from which a diminution in safety could result.

Criterion 6.4 Control Room and Emergency Control Station

A control room must be available from which the nuclear power plant can be operated safely during specified normal operation and from which measures can be undertaken in order to maintain or return it to safe condition. Short term control measures and switching procedures required for operation of the safety systems and for control of accidents must be able to be performed from the control room. In the long term, it is allowed that other measures may be performed outside the control room (auxiliary location).

Even for failure of equipment in the control room or adjacent rooms, as, for example, switchyard or electronic rooms, the reactor must be safely shut down and cooled and the shutdown condition and the afterheat removal must be monitored. The corresponding required control and monitoring equipment must be housed in an emergency control station.

The control room is to be so arranged and constituted, shielded, ventilated and provided with emergency power that personnel can enter, leave, and remain therein even during accidents which must be controlled and monitored from the control room. This requirement also applies to the emergency control station. The control room and emergency control station must be so physically separated from each other, independently from each other provided with power, and so protected against external influences that they cannot both simultaneously lose their functionality.

Section 7

Criterion 7.1 Electrical Supply

For the electrical power supply of safety systems, feed-in possibilities from two grid connections must be available from the main generator and, in event of its failure, from a self-sufficient, reliable and redundant emergency power system. The reliability of the electrical power supply must correspond to the reliability of the systems required to be supplied.

For the power supply of the safety systems, redundant emergency power loops which are independent and physically separated from each other must be available with emergency power generators and distributors. These must assure sufficient emergency power supply even during maintenance operations with simultaneous occurrence of a single failure (compare with the single failure concept). The redundancy of the emergency power loops with emergency power generators and distributors must correspond to the redundancy of the mechanical systems.

During external influence events the functional capability of a sufficient number of redundant emergency power loops must be assured and the emergency power supply over the long term must be secured. It must be assessed that before the uninterruptible operation time of the emergency power generators runs out, the required time of emergency power supply can be provided by other means.

Section 8

Criterion 8.1 Nuclear Reactor Containment*

The nuclear power plant must have a containment which can fulfill its safety-related function during specified normal operation and accidents. The containment, in conjunction with the reactor coolant enclosure (see Criterion 4.1) and other retention barriers for radioactive material, must assure that radiation protection law requirements are maintained for the transport and release of radioactive material to the environment during specified normal operation and accidents.

The reactor coolant enclosure (see Criterion 4.1) must be located within the containment. All other parts of the plant which contain radioactive material must likewise be located within the containment, if the requirements of the radiation protection law are not fulfilled through other appropriate measures. A reliable closure, sufficiently rapid to meet the safety protection criteria, must be provided for penetration through the containment.

Criterion 8.2 Containment Design Basis

The containment, including all penetrations and auxiliary equipment whose function is necessary for control of design basis accidents, is to be so structured and designed that it can withstand static, dynamic, and thermal loadings as required for fulfilling its safety function during specified normal operation and accidents. The containment must maintain its integrity** during external influence events.

*The containment includes the building structure and, if necessary, auxiliary systems for retention and filtering of potential leakage out of the containment.

**The requirement that the containment must maintain integrity during external influence events means that:

- o the containment remains both leaktight and structurally intact if it cannot be shown that the radiation protection ordinance is adhered to as a result of accident or operational leakage from a non-leaktight structure, or
- o the containment remains structurally intact if it can be shown that even without leaktightness the radiation protection ordinance is satisfied.

The containment design pressure is to be determined starting from the most unfavorable operating condition, considering possible accidents, and including safety margins. The formation of potentially combustible gas mixtures or the consequences of the postulated reaction of combustible gas mixtures on the containment are to be limited during potential accidents such that the fulfillment of the containment safety function is maintained. Equipment within the containment necessary for the control of accidents is to be designed to accident-specific boundary conditions and accident consequence loadings.

Criterion 8.3 Leaktightness Tests

The containment, in particular the closures and penetrations, must be so designed and structured that, during initial testing, a pressure integrity test at "test pressure" and a leaktightness test at design pressure or "test pressure" can be performed. Basically, the "test pressure" for the initial testing must be equal to the design pressure, except that for given design concepts it can be even higher. Periodic tests must be so conducted that a satisfactory conclusion on the leakrate during design basis conditions is reached. In case this does not result at the pressure of the initial tests, the leakrate during the initial tests is to be improved for the expected pressure of the periodic tests.

Criterion 8.4 Containment Penetrations

Pipelines which penetrate the containment and are connected to the reactor coolant or pipelines which are a constituent of the reactor coolant enclosure and are connected to the reactor coolant, as well as pipelines which penetrate the containment and are connected with the inner atmosphere of the containment, must basically have two isolation valves. One of these valves is to be located inside and one outside the containment. Exception from this requirement is allowed if necessary due to the technical peculiarity or the operation condition of the pipeline in question and if the safety function of the containment is not impaired.

Pipelines penetrating the containment but not falling within the above categories must have at least one isolation valve located outside the containment. The design of the isolation valves and the related piping up to the outer isolation valve must be at least equivalent to the containment design. Piping penetrations in the containment must satisfy the same design requirements which apply to the containment itself. This requirement also applies to cable penetrations. The functionality of the cable and piping penetrations important for safety must be assured even under accident loadings and accident boundary conditions.

For the leakage flow areas which are considered in the safety system protective measures, the activation signal for closure of the isolation valves must be reliably assured. The isolation valve closure must be self-activating or remote-controlled. The position of the isolation valve must be able to be monitored from the control room. Redundancy of isolation valves must carry over into their electrical supply. A sufficient physical separation is required. Each isolation valve of a redundant set must, by itself, assure the required closure of a pipeline. The isolation valves must fulfill their safety functions even under accident conditions. Containment locks, ventilation valves, and any installed seals are to be monitored for leakage; if required on the basis of radiation protection, the leakage is to be collected and controlled.

Criterion 8.5 Liquid Contaminant Barrier

Buildings in which radioactive liquid contaminants or other hazardous fluids could be present are to be provided with a liquid-tight barrier on the inside so that these fluids, which could be released from failure of containers or pipes, for example, are retained. The barrier is to be structured decontaminatable. If the failure of the interior barrier during accidents from internal or external influences cannot be excluded, and if there is no containment in the sense of Criterion 8.1, then an outside seal, for example, the groundwater seal, is to be provided such that it represents a reliable barrier relative to retention of contaminated fluids from the foundation. In this case, the outer seal is to be designed against all loadings, especially stresses and deformations, which are caused by static and dynamic forces, by settling, by expansion and by building shifts during specified normal operation and accidents from internal or external influence. To assure the continuous functionability of this barrier, additional quality assurance measures during fabrication are required for mode of construction, materials and manufacturing (compare with Criterion 2.2).

Section 9

Criterion 9.1 Ventilation Systems

The nuclear power plant must have ventilation systems available for the following compartments:

1. Compartments in which, during specified normal operation or accidents, the gasborne activity on an average yearly basis can be higher than:
 - o 1/7300 times the value of Table IV 1 and IV 2, Column 5 of the radiation protection ordinance for radionuclides or radionuclide mixes for which inhalation is controlling, or
 - o the values of Table IV 4 Column 5 for radionuclides for which submersion is controlling.

Exceptions are allowed if the prescripts of paragraphs 45 and 46, Sections 1 through 3 and 5 of the radiation protection ordinance are observed.

2. Compartments in which allowable specified values for the room air conditions cannot be otherwise maintained (without ventilation) during normal operation or in which safety-related plant parts with air cooling must function even during accidents.
3. Compartments in which the air is replaced by an inert gas or in which, on the basis of health physics, certain room air conditions must be maintained.

The ventilation systems must be so designed and constructed and be coordinated with characteristics of other plant parts that allowable specified values for the room air conditions and for the removal or possible release of radioactive material are not exceeded during specified normal operation or accidents. Recirculation systems are to be combined with exhaust systems as appropriate, so that radiation exposure to personnel inside and outside the plant is held to as low as possible, even below the regulatory limits, within the present state of knowledge and technology.

If the concentration of radioactive material in the air of specific rooms can be large enough to exceed allowable specified limits, the corresponding ventilation systems must incorporate an air filter unit. A switching of the ventilation system such that the exhaust air is conducted through filters only if needed is allowed. The air filter

units must be sufficiently reliable and so constructed that they have the required filter efficiencies under the respective demand conditions. Equipment required to monitor the condition of the filter must be available.

Section 10

Criterion 10.1 Radiation Monitoring

In the nuclear power plant, personnel, organizational, spatial, and equipment procedures must be implemented to assure radiation protection monitoring in the plant which is sufficiently precise, reliable and in the required level of detail for specified normal operation, accidents and exceptional events. In particular, there must be available:

1. stationary equipment for measurement of on-site doses;
2. stationary equipment for measurement of the concentration of radioactive material in the air of groups of rooms, or rooms in which a corresponding monitoring is necessary for personnel protection or for early detection of possible release of radioactive material;
3. stationary equipment for measurement of the concentration of radioactive material in circuits in which a corresponding monitoring is necessary for early detection of the possible release of radioactive material;
4. portable devices for determination of on-site doses as well as concentrations and type of radioactive material in the air and water;
5. equipment for measurement of personnel doses as well as the contamination of personnel and objects;
6. suitable laboratory equipment for evaluation and analysis of radioactive probes.

Measurement data from stationary equipment mentioned in items 1 through 3 are to be recorded and indicated in the control room and in an auxiliary location. The exceeding of danger alarm values and failure of the devices are to be so indicated in the control room and in the auxiliary location.

Criterion 10.2 Activity Monitoring in Exhaust Air and Water

In the nuclear power plant, personnel, organizational, and equipment procedures must be implemented to enable the amount and concentration of radioactive material discharged in exhaust air and water to be appropriately measured and recorded and, if necessary, to limit the discharge. In particular, stationary equipment must be available with which it is possible to monitor and record continuously

and separately the discharge and release of liquid, gaseous and aerosol-forming radioactive material during specified normal operation. Equipment must also be provided to measure and record the discharge or release of liquid, gaseous and aerosol-forming radioactive material during accidents to enable an evaluation of environmental consequences. All measurements should be indicated on the measuring instruments and must be indicated and recorded in the control room.

Criterion 10.3 Environmental Monitoring

Personnel, organizational, and equipment procedures must be implemented to enable radiation protection monitoring of the environment during specified normal operations, accidents, and exceptional events to be carried out sufficiently rapid, exact, reliable and in the required extent. In particular, there must be provided:

1. equipment and devices for determination of doses, dose rates, activity concentrations, surface contaminations and types of nuclides during specified normal operation;
2. equipment and devices for determination of required information on on-site doses, activity concentrations, surface contaminations and nuclide-types during possible release of radioactive material;
3. equipment for measurement of meteorological data necessary for determining the dispersion characteristics.

Section 11

Criterion 11.1 Fuel Handling and Storage

In the nuclear power plant, equipment must be provided to enable safe handling and storage of fuel material and other radioactive substances. This equipment must be so constructed, arranged and shielded that a criticality accident and unpermissible radiation exposure to personnel and the environment are precluded.

Basically, components of the helium purification system are to be designed to the design guidelines of the reactor coolant boundary. However, provisions must be available for safe handling and disposal of filters.

Through appropriate construction of handling equipment, it must be assured the fuel material can be safely and correctly positioned in the core. An unpermissible release of radioactive material from irradiated fuel material during handling as well as from handling equipment is to be prevented by suitable measures during specified normal operation and accidents. Locations where the possibility of leakage exists must be monitored.

Equipment for storage of irradiated fuel material must have adequate storage capacity. In the determination of the storage capacity, aspects such as eventual, required unloading of fuel elements from the reactor core, periodic tests, and maintenance procedures are to be considered. It is to be assured that afterheat from storage equipment will be reliably removed during specified normal operation and accidents.

APPENDIX B

ENGLISH TRANSLATION OF BMI INTERPRETATION OF THE SINGLE FAILURE CONCEPT FOR SAFETY CRITERIA

Interpretations of Safety Criteria for Nuclear Power

By BMI (Federal Ministry of the Interior) 10/26/78

The safety criteria for nuclear power plants⁽¹⁾ embody ground-rules for safety requirements on which the designs of nuclear power plants are based. In particular they assure, within the state of knowledge and technology, the required prevention of hazards in the erection and operation of plants (paragraph 7, Section 2, No. 3 of the atomic law) and the required protection against accidents or other effects of third parties (paragraph 7, Section 2, No.5).

In the course of their practical application it has been experienced that, as a result of the intentional brevity of the safety criteria, room for interpretation on some points has led to design difficulties. The Ministry of the Interior, therefore, contracted the preparation of "Interpretations of the Safety Criteria for Nuclear Power Plants". These should, as far as required, make the safety criteria more concrete to avoid design difficulties on their application. The interpretations of the safety criteria have the same meaning and are equally binding as the safety criteria themselves.

As the first product of this work, the German States' Committee for Atomic Energy published on October 26, 1978 the "Single Failure Concept-Groundrules for Application of the Single Failure Criterion". The following text of the single failure concept is hereby made known.

Interpretation of Safety Criteria for Nuclear Power Plants Single Failure Concept-Groundrules for Application of the Single Failure Criterion

(Status October 26, 1978)

In the nuclear power plant safety criteria:

- 4.2 Afterheat Removal - Specified Normal Operation,
- 4.3 Afterheat Removal System for Accidents,

- 6.1 Plant Protection System,
- 7.1 Emergency Power Supply, and
- 8.5 Heat Removal from the Containment

the assumption of a single failure⁽²⁾ is required.

- (1) A single failure consists of an accidental unforeseen failure in safety equipment in addition to but not as a consequence of the initiating event considered occurring during the specified normal operation or in an accident situation. A failure exists when a subsystem⁽³⁾ of the safety equipment cannot fulfill its function on demand. An operational possible malfunction which results in a failure in the safety equipment is equivalent to a single failure. In general, the cause of the assumed failure need not be given.
- (2) Assumption of a single failure (single failure concept) is a deterministic concept for the design of the safety equipment in nuclear power plants. It serves in addition to other procedures and measures, for example, probabilistic analyses (reliability analyses), as a means of assuring safety. Availability of the above listed safety systems required for the safe control of accidents must be assured without reliance on the redundancies which are required for satisfaction of the single failure concept, e.g., during initiating events with additional assumed single failure.
- (3) Basically, single failures are to be assumed in passive as well as active subsystems. For passive subsystems, a failure in the scope of the single failure concept need not be assumed if it is shown that:
 - o the subsystem is designed for maximum expected loadings under all design basis events, considering foreseeable changes in material characteristics in the course of plant operation with sufficient safety margins;
 - o the subsystem is fabricated from materials appropriate to the application purpose and under a comprehensive quality assurance program, and
 - o the subsystem is constructed, tested, and operated such that a sufficient reliability is assured.

The corresponding measures and safety margins are to be established as befits the safety importance of the safety equipment (oriented to the degree of consequences during design basis failures).

- (4) If, for the control of design basis events, several of the required systems in the above-mentioned criteria must fulfill their function simultaneously or sequentially, then the occurrence of a single failure is to be assumed for the summed systems according to the groundrules of the single failure concept, not for several of the systems simultaneously. An exception to this, in accident analysis with assumption of failure of the first activation signal of the Plant Protection System, is the assumption of the simultaneous occurrence of a single failure of an active subsystem. For simultaneous repair operation, however, not until after a time period of 100 hours (KTA regulation 3501) should single failure be assumed.
- (5) For each required system in the Safety Criteria 4.3, 6.1, and 7.1, the occurrence of a single failure even during maintenance operations is to be assumed. This does not apply to inspections if the function readiness of the affected subsystem can be restored promptly on required demand. Repair operations are to begin promptly after detection of damage. Maintenance work on redundant safety equipment during which the affected system is not function ready is, without special measures for replacing or making the function readiness unnecessary (for example, shutdown or power reduction), only allowed if the single failure concept is satisfied for the duration of the maintenance work and also if the allowable time of maintenance is adhered to. The inspection interval as well as the allowable assessment and replacement times (time from damage recognition to completion of replacement), in the absence of the special measures, are to be determined using reliability analyses on the above-mentioned redundant systems. This is to be done such that the reliability of these systems is not reduced below the reliability required for control of the accident. During short-time replacements the additional occurrence of a single failure of a subsystem need not be assumed if, because of the shortness of the replacement period, the reliability of the affected safety equipment is not materially reduced.
- (6) For structures and substructures and for passive parts of the containment, a failure within the scope of the single failure concept is not to be assumed if it is shown that the itemized requirements under (3) are met.
- (7) Accidents internal to the plant and those caused by external influences are basically equivalent. Thereby the single failure concept is to be applied as described. For external influences with very low occurrence probabilities (as for example aircraft crash and explosion pressure waves), the simultaneous occurrence of a single failure is not to be assumed; likewise, a simultaneous repair operation is not to be postulated. If the functioning of safety equipment for control of this kind of external influence event is required before as well as after a time of 30 minutes,

then a single failure in the active subsystems is to be assumed. In the consideration of the long-term aftercooling phase, it must be shown that if required for the necessary safety equipment for the long-term aftercooling phase, timely repair measures can be performed.

- (8) Failures to subsystems redundant to each other and design failures as a result of the same cause are not covered by the single failure concept. Failures of this kind must be avoided through appropriate measures, as for example:
- o design consideration of all design basis boundary conditions even under accident conditions;
 - o physical separation or other provisions against consequences;
 - o quality assurance; and
 - o periodic tests.

In addition, the aspects of diversity should be factored into the design.

For supplementing this single failure concept, a list of example cases is planned.

Footnotes:

1. Safety Criteria for Nuclear Power Plants dated 21/10/77, Federal Announcement No. 206, dated 9/11/77.
2. Safety Criteria for Nuclear Power Plants dated 21/10/77 (Federal Announcement No. 206, dated 9/11/77), Definitions, 5- Single Failure: "A single failure is a failure emanating from a single event, including consequential failures caused by the failure".
3. The concept "Subsystem" comprises all parts of the function entity itself as well as supply, regulating and auxiliary equipment necessary for proper safety function and in given cases also for redundancy.

GENERAL ATOMIC

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