EUROPAIRS

Support Action

Co-funded by the European Commission under the
Euratom Research and Training Programme on Nuclear Energy
within the Seventh Framework Programme

Grant Agreement no. 232651
Start date: 01/09/2009 Duration: 21 Months

www.europairs.eu

HTRs: feedback from past projects and Analysis of Regulatory Trends

Deliverable D22

Author(s) : J. Segurado (Tractebel Engineering) , F. Roy (AVN)
Approval: C. Angulo (Tractebel Engineering)

End-User Requirements fOr industrial Process heat Applications with Innovative nuclear Reactors for Sustainable energy supply

EUROPAIRS project – Grant Agreement no. 232651

End-User Requirements fOr industrial Process heat Applications with Innovative nuclear Reactors for Sustainable energy supply

EC Scientific Officer: Panagiotis Manolatos

Document title	HTRs: feedback from Past projects and Analysis of Regulatory Trends
Author(s)	Jacobo Segurado, Francis Roy
Number of pages	41
Document type	Deliverable
Work Package	3
Document number	D22– revision 0
Date of completion	17/02/2011
Dissemination level	_ Confidential (EUROPAIRS consortium and European Commission)
Document status	Final version

Summary

The following document intends, by contrast with relevant regulatory documents and previous European Commission Projects deliverables, to document Regulators, operators associations, utilities and research and development centers points of view on Non-LWRs operation and licensing matters. The present work intends to clearly highlight the differences and provide some tools for reconciling the differences.

Revisions

Rev.	Date	Short description	First author	Work package leader	Coordinator
00	17/02/2011	Analysis of regulatory policies for coupled facilities with HTRs - VHTRs	Jacobo Segurado	Olivier Baudrand	Edgar Bogusch

Distribution list

Name	Organisation	Comments
Panagiotis MANOLATOS	*EC DG RTD*	
Partners of Europairs		

Table of contents

ABSTRACT

The following document intends, by contrast with relevant regulatory documents and previous European Commission Projects deliverables, to document Regulators, operators associations, utilities and research and development centers points of view on Non-LWRs operation and licensing matters. The present work intends to clearly highlight the differences and provide some tools for reconciling the differences.

This document is structured as follows:

A first analysis is portrayed, which investigates the past, present and future trends in the evolution of the licensing commitments for VHTGR/HTGRs. This section starts from discussions held in the US between the NRC, ACRS and DOE (or applicants) and extrapolates the highlights of the conclusions to the most likely outcome of future regulatory oversight. Overlaid on the discussion of these topics are perspectives from regulators, applicants (vendors), and international oversight organizations

An analysis of the past experience in commissioning HTR/MHTGRs world-wide.

A comparison follows amongst the different approaches available (IAEA, US, UK, South Africa, EUR).

A complementary section discusses further high level safety topics that couldn’t be systematically dealt with within the scope of the remaining sections.

CONCLUSIONS

The up to date engineering and generic licensing issues that concern Advanced Light-Water Reactors do not stipulate, in general terms, enhanced safety characteristics on future Non-LWRs designs, but to a certain extent send echoes to the applicants to suggest designs with enhanced safety characteristics and in certain topics, additional enhancements concentrate on areas of (high) uncertainty in the regulatory bodies oversight. This alternative, however, seems that will drive regulators to review each applicant design on an scenario-specific basis and generic licensing criteria and risk-metrics for Non-LWRs would be kept at the same level of prevention and protection as current criterion pertinent to LWRs and next GEN IV LWRs, which is a consistent approach.

Consequently, it is concluded that Non-LWRs safety enhancements, if any, should be directed towards (plant-specific) areas of high regulatory uncertainly: for instance, the increase in risk to the neighboring population from a coupled reactor to a process industry on a site would be likely to be small due to the enhanced safety characteristics of the new designs, but as a result of integrating PRA into the design process of Non-LWRs, design owners will be able to appraise risk sequences with the highest CDF when compelled to comprehensively quantify and itemize all initiating events and their fault sequences. This allows a more rational development of scenario specific (both for site, purpose and reactor design) licensing bases.

PRA insights during the Non-LWRs design process allow incorporation of risk information into design options such as systems, structures, and components (SSCs). PRA also allows informed-allocation of monetary and safety analysis resources (ALARP, Risk Reduction Worth, and Severe Accident Mitigation Design Alternatives analyses) to the greatest benefit to public and occupational health, safety and protection, in the main associated with (high) regulatory uncertainty.

The following options need to be carefully pondered for the future commissioning efforts:

- **Deterministic Approach.** This option uses deterministic engineering analysis and return of experience to establish the licensing basis (including selection of events) and technical requirements. This approach is in use for licensing operating LWRs and involves no use of PRA information and insights[1].

- **Risk-Informed Performance-Based Approach.** This option uses deterministic engineering judgment and analysis exploiting design specific PRA, to establish the licensing basis (including selecting licensing basis events) and technical requirements.

- **Risk-Informed Performance-Based Approach (PRA-biased). This option places greater emphasis on the use of design-specific PRA in complementing deterministic engineering judgment and analysis, to establish the licensing basis and technical requirements.**

[1] However, it is more and more customary to reconcile the plant PRA initiators with all Chapter 15 plant symptoms for new reactor applications.

- **New set of Risk-Informed and Performance-Based Regulations.** This option would use a new set of regulations to establish the licensing basis (.) and licensing requirements. The new set of regulations would exploit the risk-informed performance-based regulatory structure, and would require rulemaking to be implemented.

Given the current state of Very-High-Temperature Gas Reactors (VHTR) technology design, development and return of experience, and the quality and completeness of the associated design-specific PRA, the second option above may be preferred for licensing the prototype, which makes primary use of deterministic judgment and analysis, complemented by specific PRA (consistent with EUR requirements) to establish the licensing basis and requirements. The use of the PRA would be commensurate with the quality and completeness of the PRA presented with the application. Once the technology is demonstrated through successful operation and testing of the prototype, and a quality PRA including data becomes available, greater emphasis on design-specific PRA to establish the licensing basis and requirements will be a more viable option for licensing a commercial version of the reactor.

The research performed herein has found no impediment for the near-future licensing of a coupled VHTGR with a process industry.

1 Analysis of Regulatory Trends

1.1 Endorsement by Regulatory Bodies of higher safety levels on Non-LWRs applications.

In order to compensate for the greater uncertainties associated with (coupled applications) VHTGRs and the reduced[2] operating experience it would be anticipated that regulators would endorse higher safety (reference) levels. This practice would be intended to reduce the core damage frequency, improve accident prevention and population and exposed professionals protection (INSAG-10 guidelines).

However, for the specific VHTR case, uncertainties in the severe accident (SA) area could be compensated by enhanced accident and core damage prevention by lowering the risk from SAs sequences in the design phase, and specific VHTR technology features.

To the coupling scheme safety, valuable information can be found about PIRT (Phenomena Identification Ranking Tables) such as ‘Process Heat and Hydrogen Co-generation’, NUREG/CR-6944 Series, concluding that:

- […] hazards of a small chemical plant […] may be significantly smaller than a commercial high-temperature reactor.
- […]for many hazards, such as a hydrogen leak, the safety strategy is dilution with air to below the low inflammability limit[…]The chemical plant safety strategy implies that controlling the size of the chemical inventories, the site layout, and the separation distances between various processes facilities and storage facilities are the primary safety devices used to prevent small events becoming major accidents.
- […]accidental releases of hydrogen […] are unlikely to be a major hazard assuming some minimum separation distances.
- Heavy gases: […]Industrial experience shows that such accidents can have major off-site consequences because of the ease of the transport from the chemical plant to […] other facility. Oxygen presents a special concern.

To this regard[3], all evidence points out towards ‘business as usual’ safety policies for the industrial facility, while the nuclear plant safety goals may be subject to some or not amendments at all. Note here, however, that the safety goals invariants from coupled/not-coupled nuclear sites set in forth, such as general safety approaches allowed for the nuclear plant (notably from IAEA, NRC, INSA)[4], as to this moment, remain unmodified regardless there is a coupled facility or not (see WENRA reference safety levels). Nonetheless, there are two items to investigate further:

- External events from the facility to the nuclear site.
- Definition of the emergency preparedness, exclusion area, collective doses (for the overall application), etc.

[2] In comparison to LWRs.

[3] With exception of the intermediate loop heat exchanger failure.

[4] Based on Defense in Depth (DiD), safety design approaches (deterministic, with or without PRA), operational safety (including maintenance and incident monitoring, licensing commitments and surveillance requirements), accident control (event-oriented approach), management of severe accidents, emergency response and emergency planning (including management of emergency planning zones)

To this regard, the current safety approach is deemed complete by itself to cover the coupling (while taking properly into account specific external hazards from the non nuclear plant, specific internal hazards from the coupling circuits – intermediate heat exchanger, and both within the same safety workaround) so there is no apparent reason to postulate that the safety levels should be increased, due to the presence of a non-nuclear facility.

However, one main basis for strengthening accident prevention and DiD (namely in the confinement function (see §1.6)) is the general consensus on the safety targets of INSAG-3 for future plants[5]. No refutation up to this point (or different statement) has been made public by the IAEA to this respect and up to this moment WENRA safety goals for non-LWRs seem to be not different than those for LWRs since WENRA has yet not published any position to this respect.

Further, an increase in IAEA Safety Goals would be, however, not consistent with NEI's (May 2002) white paper (and as well with NRC's document "Policy Statement on the Regulation of Advanced Nuclear Power Plants" (51 FR 24643)), relevant equally to future LWRs as well as Non-LWRs.

Industry and stakeholders insights (such as EUR Volume 3 for instance as an example of relevant good industry practice), require an enhanced level of confidence in the performance of plant systems, structures and components, which only reflects specific requirements upon safety systems, but not in the safety goals themselves. However, to pay off for the reduced experience with Non-LWRs, improved research and development, testing and/or demonstration plant could be required to enlarge confidence in the performance of plant systems, structures and components.
Non-LWRs could make use of the same workaround to that used in the evolutionary LWR and ALWR certification to comply with any additional enhancement, including establishing improved confidence in the design and/or performance of plant systems, structures and components (SSCs).

The Electric Power Research Institute developed a "Utility Requirement Document" for ALWRs which defined the requirements that utilities desired in ALWRs. These requirements included core damage frequency (CDF) and radioactive material release objectives below those achieved by current generation LWRs as well as other plant features that EPRI considered would make future LWRs "substantially safer than existing plants''.

Regulatory Bodies such as the NRC have proposed for instance:

> …to approve implementation of enhanced safety through a process similar to that used in the evolutionary LWR and advanced light-water reactor (ALWR) design certification reviews. Endorsed enhancements could include design features, testing by the designer, or confirmatory testing in areas of large uncertainty, with the intent to achieve a level of safety and confidence similar to that achieved in the evolutionary and ALWR design certifications … [**SECY-03-0047**]

Echoes of this statement can be found in the pre-application safety evaluation of several US Non-LWRs:

- **NUREG-1338** (Draft), "Pre-application Safety Evaluation Report for the Modular High-Temperature Gas-Cooled Reactor (MHTGR)," June 1995.

[5] Namely a probability of severe core damage below 10-5 per plant operating year combined with a further reduction by a factor of at least ten in the probability of a major release requiring a short term off-site response.

- **NUREG-1368**, “Pre-application Safety Evaluation Report for the Power Reactor Innovative Small Module (PRISM) Liquid-Metal Reactor,” February 1994.
- **NUREG-1369**, “Pre-application Safety Evaluation Report for the Sodium Advanced Fast Reactor (SAFR) Liquid-Metal Reactor,” December 1991.

References:

- **SECY-93-087**, “POLICY, TECHNICAL, AND LICENSING ISSUES PERTAINING TO EVOLUTIONARY AND ADVANCED LIGHT-WATER REACTOR [ALWR] DESIGNS, APRIL 2, 1993.
- **REGULATORY GUIDE 1.174**.
- **A RISK-INFORMED, PERFORMANCE-BASED REGULATORY FRAMEWORK FOR POWER REACTORS**, NUCLEAR ENERGY INSTITUTE, MAY 2002.
- **SECY-03-0047.**
- **WENRA-TRACTEBEL ENG.**, INTERNAL COMMUNICATIONS.

1.2 Towards a (re)definition of Defence in Depth for coupled facilities

With the potential for future plant applications it would be deemed prudent developing explicit guidelines describing the VHTR DiD philosophy as it pertains to reactor specific design (VHTR) and operation (related to a downstream coupled facility).

It is to be noted that, so far, the expression defense-in-depth is used in regulations are in 10 CFR Part 50, Appendix R, *Fire Protection*, and 10 CFR Part 100.1, *Reactor Site Criteria*, the *NRC Safety Goal Policy Statement*, the *PRA Policy Statement*, and the *1999 NRC Risk-Informed, Performance-Based Regulation white paper*.

DiD principles traditionally imply that safety cannot rely dependent upon any single element of the design, construction, maintenance, operation or safety and that these elements have to be populated with layers of compensatory countermeasures to prevent, control accidents or mitigate damage (IAEA’s INSAG-10). This for instance will need to be acknowledged for the chemical attack protective function, onto external and internal systems, structures and components, which shall be included within the future DiD approaches (see NUREG/CR-6944 Vol 6 for instance, which already includes this one within the list of safety functions; DOE already recognized this function for the MHTGR application). The defence-in-depth principle is required by EUR but no statement is made about chemical attack.

So far, the following items have not been systematically endorsed by relevant safety authorities, and are yet susceptible to future changes:

- Development of a statement, description or provisions for defense-in-depth for Non-LWRs to include:
  - New Objectives,
  - New Scope,
  - New Elements.
- A policy of such characteristics, to be general, will need to be endorsed regardless of the technology ([6]).

[6] And most likely risk-informed

- This policy should be expanded through a process involving other groups review (such as utilities collectives, stakeholders, industry standards committees, etc…).

It seems that, in account for uncertainties in the technology however, for any Non-LWRs future licensing endeavors the defense-in-depth insights as derived from above, would need to be included within the technology generic design assessment (Nuclear Energy Institute statement, see below).

Seldom attempts to (re)describe the elements of DiD, examples include:

- IAEA Safety Series US-R-1, "Safety Assessment and Verification for Nuclear Power Plants," 2001.
- IAEA-TECDOC-986, "Implementation of defense in depth for next generation light water reactors," December 1997.
- Safety Series No. 75-INSAG-3, "Basic Safety Principles for Nuclear Power Plants," 1988.
- Safety Series No. 75-INSAG-3, Rev. 1,
- INSAG-12, "Basic Safety Principles for Nuclear Power Plants," 1999.
- ANS Draft 53.1, Nuclear Safety Criteria for the Design of Modular Helium Cooled Reactor Plants

Recently, the Nuclear Energy Institute, has proposed DiD to be considered a process to account for uncertainties and applied on a design-specific basis. This practice would be consistent with the difference in accident dynamics for LWRs and inherent safety for Non-LWRs, and some gain in safety margins could be exploited should the identification of uncertainties be well endorsed as well this process is started top-bottom from appropriate sources of information identifying the areas of high uncertainty (and regulatory uncertainty), such as for instances starting from PIRT-based methodologies (see NUREG/CR-6499 series).

From all above the conclusion is that for Non-LWRs, no adapted definition and workaround have been formally established at least yet but it seems reasonable to consider the following future scenarios:

- Consider DiD on a scenario-specific basis as part of the review of a specific design (i.e., w/o a newly developed prescription).
- Development of consolidated policy statements through a process involving stakeholder review, input and participation.

References :

- **REGULATORY GUIDE 1.174**
- "**A RISK-INFORMED, PERFORMANCE-BASED REGULATORY FRAMEWORK FOR POWER REACTORS**", NUCLEAR ENERGY INSTITUTE
- REGULATORY ANALYSIS GUIDELINES, **NUREG/BR-0058**, REV. 3.
- **DRAFT ANS 53.1**, NUCLEAR SAFETY CRITERIA FOR THE DESIGN OF MODULAR HELIUM COOLED REACTOR PLANTS.
- **NUREG/CR-6499**, NEXT GENERATION NUCLEAR PLANT PHENOMENA IDENTIFICATION AND RANKING TABLES (PIRTS), MARCH 2008.

1.3 International Codes and Standards

The United Kingdom operates 14 advanced gas reactors, Japan operates a 30-megawatt high-temperature, gas-cooled research reactor, and China operates the HTR-10, a 10-MWt high-temperature, gas-cooled reactor (HTGR) prototype. Both the International Atomic Energy Agency (IAEA) and the European Union have active programs on HTGR safety and development. Accordingly, other countries and organizations have developed, to varying degrees, an infrastructure supporting Non-LWR technology (including the development of standards and requirements).

The International Standards Organization (ISO) has also generated standards dealing with subjects such as quality assurance. International collaboration with other regulatory agencies and international standards organizations could be a useful way to identify the need for (new) codes, modifications to existing ones, and standards and facilitate their development.

The intended scope of the codes and standards under interest would be those associated with the safety of design, manufacture, construction, and operation.

To this point, the International Atomic Energy Agency, the Nuclear Energy Agency, and certified inspection bodies (such as TuV for instance) may be used as resources to assist in the identification of codes and standards needs, the understanding of international codes and standards.

In addition, integration/reconciliation if needed of codes such as ASME RA-S standard with Internal Fires, Low Power/Shutdown, and External Event PRAs should be consistent with regulatory safety goals expectations and requirements. The following committees are noteworthy to this regard:

- ANS 28 Subcommittee is developing **ANS 53.1** - Nuclear Safety Criteria for the Design of Modular Helium Cooled Reactor Plants.
- **ASME Section XI, Division 2** has efforts underway to develop risk-informed ISI approach for high temperature gas-cooled reactors.
- **ASME Code Case N-720** under development for Risk- Informed Safety Classification for Construction of Nuclear Facility Components, **Section III**, **Division 1.**

1.4 Risk - informed Approach for the Design Certification and Licensing Bases for (coupled) VHTR

Three approaches could be deemed appropriate for Non-LWRs within this context:

- **Probabilistic approaches in the identification of accident initiating events** assuming that there is sufficient understanding of plant and fuel performance (so that a deterministic engineering analysis can be used downstream to superbound uncertainties).
- **Allowing probabilistic approaches for the safety** classification of structures, systems, and components (including licensing commitments and extended surveillance requirements).
- **Replace the single failure criterion with a risk-informed reliability criterion**. The same applies for the predictive maintenance criterion for countries where such bylaw exists.

These recommendations are in agreement with a risk-informed approach which propagates PRA into the licensing basis, and moreover, within the design process itself of LWRs and Non-LWRs.

The second practice has been already commended by the US NRC, by granting the design certification to the US AP1000. This practice is currently in review by the UK Safety Authorities (HSE NII), and its decision to whether sanction as applicable or not this approach could be propagated downstream to other European countries. This approach has been proven to dramatically cut SSCs costs, while the designer as counterpart provides licensing commitments and strict surveillance criteria upon the SSCs. The key advantage to this option is that it is technology-free, and ensures that the design basis credits fairly both equipment and human performance. It does, however, impose tight controls over the living plant PRA documentation and plant change control (this practice is very similar to the recently developed risk informed LOCA regulations by the NRC).

However, while it is true that this approach is striking from an engineering and cost-control standpoint, it can be argued that it is unavoidable that additional licensing commitments[7] and extended quality assurance oversight[8] will be built-in within the future regulatory licensing basis.

The first practice (Probabilistic approaches in the identification of accident initiating events) was sanctioned already in SECY-93-092:

1. Events and sequences would be selected deterministically and would be complemented with insights from PRAs of the specific designs.
2. Categories of events would be defined according to their frequency. If one categorie drops below LWR design-basis accidents frequency would be analyzed without applying the conservatisms used for DBEs for instance, while for events within a category higher, would require conservative analyses.
3. Acceptance limits for core damage and onsite or offsite releases would be established for each category.
4. Methodologies and evaluation assumptions would be developed for analyzing each category of events consistent with existing LWR workaround.
5. Source terms (deterministic or performance based).
6. A set of events would be selected deterministically to assess the safety margins of the proposed designs, to determine scenarios to mechanistically determine a source term, and to identify a containment challenge scenario.
7. External events would be chosen deterministically on a basis consistent with that used for LWRs.
8. Evaluations of multi-module reactor designs would be considered as to whether specific events apply to some or all reactors on site for the given scenario for all operations permitted by proposed operating oversight.

As to the first practice, second point, if one category of events that would be examined corresponds to accident sequences of a lesser likelihood than conventional LWR design basis accidents, they would be analyzed without applying the conservatisms used for design basis accidents, while events within a category equivalent to the current design basis accident category would require conservative analyses, consistent with LWR standard oversight.

[7] Such as full diversity demonstration, which in some cases would not satisfy current standard regulations such as the use of only safety grade equipment for the safety demonstration.

[8] Such as exhaustive in-service inspection programs.

An indication of future changes in addition, is risk-informing 10 CFR 50.46, “Acceptance Criteria for Emergency Core Cooling Systems for Light-Water Nuclear Power Reactors” where the NRC and ACRS are in the process for allowing the use of risk information to replace the single-failure criterion and, in SECY-02-0176, has proposed to use risk information to modify the special treatment requirements on safety-related SSCs in 10 CFR Part 50.

However, taking as an example the UK GDA process, both first and second approaches involve:

- Public and regulatory acceptance to allow qualifying not all SSCs as safety class (traditional safety class),
- International or Local consensus in regards to the applicable of specific codes and standards (for declassified SSCs),
- Consistency between the plant PRA and the list of DBEs,
- A compromise solution between redundancy and diversity (taking into account the remarks about SSCs declassification). A full diversity is expected to be set on forth for likely events (i.e., DBC class II).

On the EUR side a first remark is that no detailed design report is available for non-LWRs. Chapter 2.1 (volume 2, chapter 1) of EUR treats the safety requirements. The revision C of the volume 2 was completed in April 2001.

- The EUR approach is based on deterministic methods, augmented by probabilistic methods (see Figure 1.4-1 below).
- The defense-in-depth principle is required by EUR.

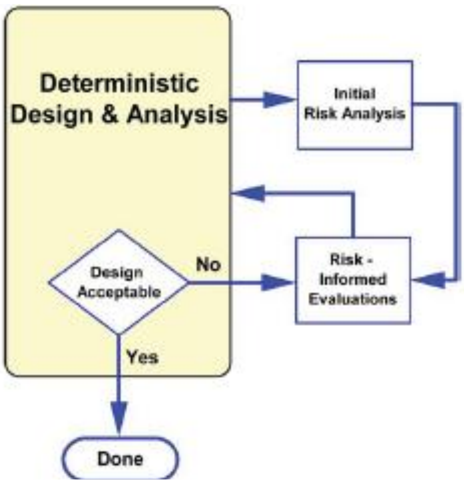


Figure 1.4-1 EUR Approach

The safety approach proposed by EUR is represented by the following diagram (Figure 1.4-2):

Definitions

Targets are values (in terms of radioactivity releases ; in terms of dose to plant personnel or to public) established by the Utilities which are more demanding than current regulatory limits.
CLI (criterion for limited impact) are non dimensional targets expressed as a maximal value to respect by a linear combination of isotope releases families.

Design determination

Normal operation (§2.1.2.2)

Deterministic (realistic) calculations (annual release and dose targets to verify)

DBC (§2.1.2.4)

Deterministic (conservative) calculations

Several CLI to verify
Fuel acceptance criteria to verify for LOCA
Containment performances to verify

DEC (§2.1.2.5)

Mandatory list of initiators
Deterministic (realistic) calculations
Several CLI to verify

Hazards (§2.1.5)
Specific approach

Design verification

3 probabilistic safety targets to verify (§2.1.2.6)
(for severe accidents, large releases sequences, and cliff edge effects sequences)

Figure 1.4-2 EUR Safety Approach

In a first step, the EUR design method is deterministic:

1. Four levels of « design basis conditions » and one level « design extension condition », as a function of initiating event frequency, and aggravating failure.
2. Specific study rules for each category.
3. Specific target in term of radiological release (in order to compare several designs independently from the site)[9]

In a second step, the verification of this design is probabilistic:

1. Frequency Targets defined for SAs, and for cliff edge effects (accidents leading to important releases)[10].
2. Calculation of dose to public requires knowing the barriers retention capability.
3. To simplify the evaluation: 1600°C as a decoupled safety criterion for most of the transients to study. Sufficient criterion for the first barrier integrity.
4. For other transients (water ingress, air ingress), more specific evaluation is required.

[9] This criteria was not used in European Commission HTR-L; European Commission HTR-L uses the dose to public as target, to be consistent with the regulation (ICRP)).

[10] In European Commission HTR-L, a residual risk category is defined to contain initiating events that are not acceptable (compressor/pump/turbine shaft failure, double ended large pipe break, large water ingress) for which the design should minimize their frequency

The EUR design method includes design bases conditions (DBC) and design extension conditions (DEC). Normal conditions and DBCs encompass a family of postulated initiating events which could challenge the safety of the plant. Those events are classified into 4 categories according to their estimated frequency of occurrence:

- Category 1: Normal operation
- Category 2 : Incident conditions (higher than 10^{-2} / y) expected to occur during the plant life
- Category 3 : Accident conditions of low frequency (between 10^{-2} and 10^{-4} / y)
- Category 4 : Accident conditions of very low frequency (between 10^{-4} and 10^{-6} / y)

If an event can only occur during a specific reactor state, the frequency of this reactor state has to be taken into account in order to introduce the event in the required category.

For each category, acceptance criteria are defined:

- Category 1 and 2 (normal conditions and incident conditions): authorized annual discharge of 10 GBq of liquid release except tritium, 50 TBq of noble gases, 1 GBq of halogens and aerosols. Those are typical values with reference to a 1500 MW plant. For units of smaller output, the limits will be pro rata the power output. The dose target to respect for the public is 0.1 mSv/y (whatever the output) and the average dose target to plant staff is 0.5 mSv/y. Those calculations are best-estimate.

- Category 3 and 4 (accidents) : specific criteria for each category. Release targets (CLI) determined on the basis of effects on emergency planning, and on food restrictions. Specific criteria for LWR fuel (% fuel experiencing DNBR, criteria for LOCA). The calculations are conservative. The basis for the determination of those EUR release targets (CLI) is a dose target of 1 mSv in category 3 and 5 mSv in category 4.

DEC (Design Extension Conditions) are SA sequences (leading to large release) or complex sequences (leading to important release). Firstly, EUR requires a mandatory list of DEC initiators (for LWR, like ATWS or station blackout) to consider in the design. Secondly, one or several additional DECs can be added to the list if the probabilistic verification of the design fails.

The final probabilistic evaluation allows verifying the deterministic design, and if enough DECs are considered in the design:

- The core damage cumulative frequency has to be less than 10^{-5} / y
- The cumulative frequency of accidents exceeding one of the CLI has to be less than 10^{-6} / y
- Sequences potentially leading to very large releases have to be well below 10^{-6} / y

However, all the precedent discussion is based upon current state-of-the art DiD definitions which not systematically include explicit guidelines for the chemical attack safety function to be included within the design basis. This point, already commented upon in Section 1.6 will require further regulatory developments and design guidelines to be implemented

References:

- The '95 NRC PRAC policy statement initiated the following activities (initiating work to risk-inform 10 CFR Part 50):

NRC REGULATORY GUIDES	1.174
	1.175
	1.176

1.177

1.178

- **EUR VOLUME III**.

1.5 Source Term Technology/Scenario-Specific in Licensing Decisions

LWR deterministic source terms are listed in NUREG-1465, and are associated with an in-vessel core melt accident in LWRs, which differs from the fission product retaining characteristics and highly unlikely meltdown at HTGRs.

Current light-water reactors use scenario-specific parameters (e.g., exclusion site area boundary) and a deterministic predetermined source term into containment to analyze the effectiveness of the containment local emplacement adequacy for licensing purposes.

The source term used in LWR (siting evaluations) is based upon an in-vessel core melt accident, a large fraction of the radionuclide inventory is released early into containment, which may very well not be applicable to HTGRs designs.

Several Non-LWRs precedents are listed as representative from regulatory oversight:

- Fort St. Vrain made use of a deterministic source term based upon TID-14844, which was made (even) more conservative by assuming additional constraints.
- The DOE sponsored a HTGR design Modular High-Temperature Gas-Cooled Reactor (MHTGR), proposing mechanistic (scenario-specific) source term was based on the characteristics of the fuel, plant, to determine the magnitude- timing and nature of fission product release from the core.
- NRC staff stated in NUREG-1338 stated that the use of a mechanistic source term yet needed extensive research and testing was needed to address the technical issues.
- In SECY-93-092 (addressing PRISM, the MHTGR, the PIUS, and the Canadian CANDU 3) mechanistic source terms should be allowed provided that:
  - Reactor and fuel performance under normal and off-normal operating conditions is sufficiently well understood to allow using a mechanistic analysis.
  - Sufficient data (should) exist on the reactor and fuel performance through the research, development, and testing programs to provide the adequate confidence in the mechanistic approach.
  - The transport of fission products can be adequately modeled for all barriers and pathways to the exterior, including specific consideration of containment design. The calculations should be as realistic as possible so that the values and limitations of any mechanism or barrier are not obscured.
  - The events considered in the analyses to develop the set of source terms for each design are selected to bound SAs and design-dependent uncertainties.
- In the very recent HTGRs pre-application US activities (US Exelon's PBMR), the designers propose an approach to mechanistic scenario-specific source terms derived from anticipated operating occurrences and design basis events as identified in the PRA for the plant, using phenomenological models of fission product transport (such mechanistic source terms accounting for uncertainties).

Using mechanistic source terms based on a selection of design basis events and a good foundation of plant-specific knowledge, such as fuel behaviour and core response under off-normal conditions, has been the trend for advanced HTGRs worldwide.

The HTR-10 in China used a source term based on a mechanistic approach in which severe core damage was not assumed but instead the radiation release was calculated specifically for the individual accidents leading to the largest release of radionuclides from the fuel elements. Although a bounding source term is used in the licensing of current LWRs, the regulations do allow for either approach. Future regulations will likely retain the flexibility of allowing the use of either a bounding or scenario-specific source terms.

Two options then, seem to be eventually accepted therefore at international wide framework:

- **Scenario-specific** (mechanistic) source terms based upon understanding fission product behavior and plant conditions and performance[11].
- **Deterministic-bounding** source term which is based on the conservative assumption of severe core damage and fission product release[12].

As a positive instance, a study by TUV Hannover (Safety Assessment of the Design of the modular HTR-2 Nuclear Power Plant, May 1990) demonstrated that for that technology in specific, the release of radioactive substances during normal operation is far below the dose limits as per §45 of the German Radiological protection ordinance (100 Bq/g is the limit for tritium concentration in the process steam, §4 Section 2), same as for §28 Section 3 under hypothetical accidental conditions.

In addition, following the concept of mutually shield activity-containing components, there are measures that might be helpful to reduce effective doses to protect the personnel against hazards of radiation exposure:

- Separation of nuclear and conventional units.
- Separation of high and low-active components.
- Separation of high-active components with respect to maintenance and repair.
- Local separation of components, valves and operating stations on one hand, and internal passages for personnel on the other.
- Modules to be erected separately in different cavities.
- Pumps of the secured intermediate loop to be arranged in different parts of the reactor building annex, and shielded.
- Containers for concentrated liquid effluents and waste erected in separate shielded room.

Taking as an example the German AVR in Juelich to exemplify the need for uncertainties to be well accounted for is for instance the correlation between (easy detectable) noble gas release and release of metallic fission products (its detection being slow and very elaborated). The fact that

[11] This option uses specifically the unique features of HTGRs designs. Understanding of plant performance, fuel behavior, and fission product release characteristics over a wide range of conditions.

[12] This option is current on LWRs and is consistent with the view (i.e., defense-in-depth) that sitting and containment decisions should be made in consideration of a severe core damage accident. For HTGRs this is likely to be highly conservative, not accurately reflecting the design attributes of HTGRs.

their release mechanisms are different, the contamination detection may be very well delayed from the release, the fact that non-LWRS cannot be instrumented regularly for temperature detection, and that a strong increase if release correlates with an increase of coolant temperatures (generally) exemplifies the need for use of uncertainty-augmented design-methodologies.

1.6 VHTR Containment

The use of a pressure-retaining containment building has been considered a key element of the basic design as a significant element of defence-in-depth for LWRs to ensure public risk acceptance.

However, certain reactor designs may have a long delay before the release of large amounts of radioactive material, or may even preclude extensive core damage altogether. In such cases it is reasonable to consider whether or not a traditional pressure-retaining containment/confinement structure is necessary at all or is the most effective way to protect public health and safety.

In addition, the physical protection of the critical plant structures from external threats does not necessarily imply pressure-retaining buildings. Moreover, coolant fluids such as Helium might not be condensable, for which the use of a pressure retaining building is negative on safety, by reducing the effectiveness of the containment heat removal systems (which in many current and future designs are to be passive), by requiring higher standards in the equipment qualification levels, and by causing buildup of non-condensable gas thus providing a driving force for any fission products that might ultimately be released from the core during the course of the accident

The licensing endeavours and forthcoming regulations should carefully ponder the next items:

- Which design feature substantially really improves safety?
- Is the reactor design such that core damage could be delayed?
- Are uncertainties better bounded by a pressure-retaining building?
- Could severe core damage (and the release of large quantities of fission products_ be screened out?

For a Non-LWR, confinement could be characterized by a negative pressure with filtered venting capabilities, but no pressure-retaining structure; postulated DBEs would make the confinement building to initially vent without filtering capabilities until the pressure was relieved (just as an instance), and resume operation once at negative pressure filtered operation thereafter[13]. In case of a loss of offsite power, slow unfiltered venting would occur, otherwise if electric power is still available negative pressure inside the building would be restored as soon as possible. The option portrayed herein would be a vented low-pressure containment design with a maximum design leak rate that meets health and safety acceptance criteria, and of course, minimizes transport mechanisms in a postulated loss of pressure accident.

[13] Temperature following a primary circuit depressurization drops sufficiently after 6 to 8 hrs to allow normal HVAC operation to resume. On resumption, the carbon filters are switched into the exhaust path to remove the most important isotopes released in the heat-up phase. Whether or not such filtered venting is to take place will depend on the need to enter the affected areas for repair to the gas pressure boundary, and the possible dose to the public from unfiltered components.

In addition to filtering, deposition in the reactor or over any other confinement structures can also retain fission products (see AVR reactor dismantling problems that confirmed effective deposition mechanisms for Cs, Sr, Ag). Currently the long core heat up time and the fission product retention capability of the fuel are considered by the designers to be sufficiently robust to make a conventional pressure-retaining containment unnecessary and possibly detrimental to the passive decay heat removal systems. It is evident that this approach puts a greater reliance on the first barrier[14] (fuel integrity).

As an example of representative relevant international practice, a confinement building was used on Fort St. Vrain and many gas-cooled reactors in other countries. SECY-93-092 addressed NRC concerns and proposed functional performance criteria to evaluate the acceptability of proposed designs, rather than prescriptive containment design, with the caveat that two criteria must be met:

- Specified onsite and offsite radionuclide release limits for the event categories within their design envelope.
- For a period of approximately 24 hours, the confinement loads result in less than the limiting leak rate used in evaluation of the event categories, mechanical stresses were to be maintained within regulatory limits (i.e., ASME level C). After, release of radioactivity must be prevented.

Air ingress is a large concern for reactors containing large quantities of graphite at elevated temperatures. In theory, a pressure-retaining containment would limit the amount of air that could enter the core, and thus limit the amount of corrosion that can occur. However, analysis shows that air ingress proceeds at a very slow rate, and by the time it is assumed that operator intervention is achieved and the leak temporarily closed, very little actual corrosion will have taken place.

As a summary, the following points need to be observed:

MITIGATION

- reducing radioactive releases to the environment
- preventing or limiting potential core damage
- removing heat to mitigate accident conditions and prevent vital equipment from exceeding design and safety limits

PREVENTION

- protecting vital equipment from internal and external events.
- protecting onsite workers from radiation.
- providing physical protection (i.e., security) for vital equipment.

However, quantification needs to be analyzed in order to provide risk and cost worth alternatives. The NRC proposed some metrics reflected hereunder:

- Does the option adequately accommodate all containment building systems?

[14] And also in the fact that fast primary depressurizations might be excluded from the design basis conditions, Juel-4275, A Safety Re-evaluation of the AVR Pebble Reactor Operation and its Consequences for future HTR Concepts, Washington, October 2008

- Would the option be expected to substantially improve plant safety by:
  - Prevents certain categories of accidents?
  - Drops fission product release?
  - Bounds known uncertainties?
- Does the option provide flexibility to the designer in meeting the events consequence acceptance criteria?
- Involves incremental costs without proportional safety benefits (i.e., equipment qualification)?

Emphasis will be made upon the fact that advanced reactor designers would need to consider the effects of a *large airplane impact* as well as other *design basis threats* (as so it has been sanctioned applicable at least by the EUR collective).

Whatever the choice would be, IAEA in the INSAG-10 document clearly states that deterministic and probabilistic approaches shall be used so that *sequences leading to early containment failure are essentially eliminated* with a high degree of confidence **(1),** severe accidents that could lead to late containment failure would be considered explicitly in the design process **(2),** for sequences without core melt, it will need to be demonstrated for advanced designs that there is no necessity for protective measures (evacuation or sheltering) for people living in the vicinity of a plant **(3)** (therefore applying to the facility).

References:

- **EUR Volume III**.
- **THE PBMR CONTAINMENT SYSTEM**, 2nd International Topical Meeting on HIGH TEMPERATURE REACTOR TECHNOLOGY, Beijing, CHINA, September 22-24, 2004 (Paper F08).
- **US NRC SECY 93-092**.
- **JUEL-4275**, A SAFETY RE-EVALUATION OF THE AVR PEBBLE REACTOR OPERATION AND ITS CONSEQUENCES FOR FUTURE HTR CONCEPTS, WASHINGTON, OCTOBER 2008.
- **INSAG-10**, DEFENCE IN DEPTH IN NUCLEAR SAFETY.
-

1.7 Reduction of the Emergency Planning Zone and Site Exclusion Area Boundary

Inspection of the literature indicates that the NRC would recommend probably no changes to emergency preparedness requirements at least immediately:

- Since provision already exists in 10 CFR 50 §47 for accommodating the unique aspects of high-temperature gas reactors,
- Since in the near term, new plants are likely to be built on an existing site which conforms to current requirements.

10 CFR 50.47 includes a provision allowing emergency preparedness zones for High Temperature Gas-Cooled Reactors (HTGRs) to be determined on a case-by-case basis, which means that the work on emergency preparedness should be coupled with accident evaluation and source term definition to eliminate over conservativisms.

The role of emergency preparedness within DiD seems to be likely endorsed by additional policies or addenda to DiD definitions as described in Section § 1.2, or either by defining event categories sampled by the frequency of their occurrence, identifying acceptance criteria for each event category and designing the plant for events down to a frequency of X-events/plant-year. Events less frequent than this would be considered only for emergency planning purposes down to Y-events/plant-year, where Y is several orders of magnitude lower than X. Structures, systems, and components would be classified “safety related” if they were necessary to enable the plant to meet acceptance criteria, but this is would have to be evaluated in a case-specific basis (see GDA UK AP1000 certification process for instance, frequent events assessment).

2 Current and Past Safety Assessments and Regulatory Criteria

2.1 NUREG-1338 “Safety evaluation report for the Modular High Temperature Gas cooled Reactor (MHTGR)”

This guide documents the development of further documentation to support future US licensing of the MHTGR concept. The NRC mentions that any licensing can only be achieved by fully complying with the 10 and 40 (“Protection of the environment”) CFR requirements.
In this document, it is important to make the distinction between the design process and safety approach-evaluation of the DOE on one side, and the review of this exercise by the NRC on the other side.

Case Study

The standard MHTGR consists of four identical reactors modules, each of them with a thermal output of 350 MWt, coupled with two steam turbine-generator sets to produce a total plant electrical output of 540 MWe. The main difference with the present European Commission HTR-L project is the presence of a steam cycle (only direct cycle considered in European Commission HTR-L). Moreover, the MHTGR is based on prismatic blocks core, but the pebble bed concept was also treated by the past European Commission European Commission HTR-L project.

DOE safety and design approach

The MHTGR licensing bases are using:

- Top level regulatory criteria,
- Licensing bases events,
- Equipment safety classification,
- Safety Related Design Conditions.

2.1.1 Top level regulatory criteria

This is a topic subject to continuing debate.
Those are quantifiable statements of acceptable consequences or risks to the public or to the environment (individual acute and latent fatality risks, annualized offsite dose guidelines, accident offsite dose, and protective action guideline dose).
Firstly, starting from the 10 CFR 50 imposing dose limits, the ANS 51.1 standard has proposed a consistent frequency-dose diagram. It is assumed that if the acceptable zone is respected, the CFR limits are also respected.
Secondly, in the frame of MHTGR, the DOE proposes a more conservative frequency-dose diagram imposing a constant design target of 1 REM for events below 2.5 10^{-2} /y (see Figure 2.1-1).

A key feature of the requirements is the need to implement protective actions for the population within a plume exposure pathway emergency planning zone (EPZ) of about 10 miles in radius. The DOE has proposed a reduced emergency-preparedness requirement for the MHTGR; on the basis that the design features (passive reactor shutdown and cooling systems with core-heatup times much longer than those for LWRs) result in a system that is safe enough to warrant a reduction in the EPZ radius to the site boundary.

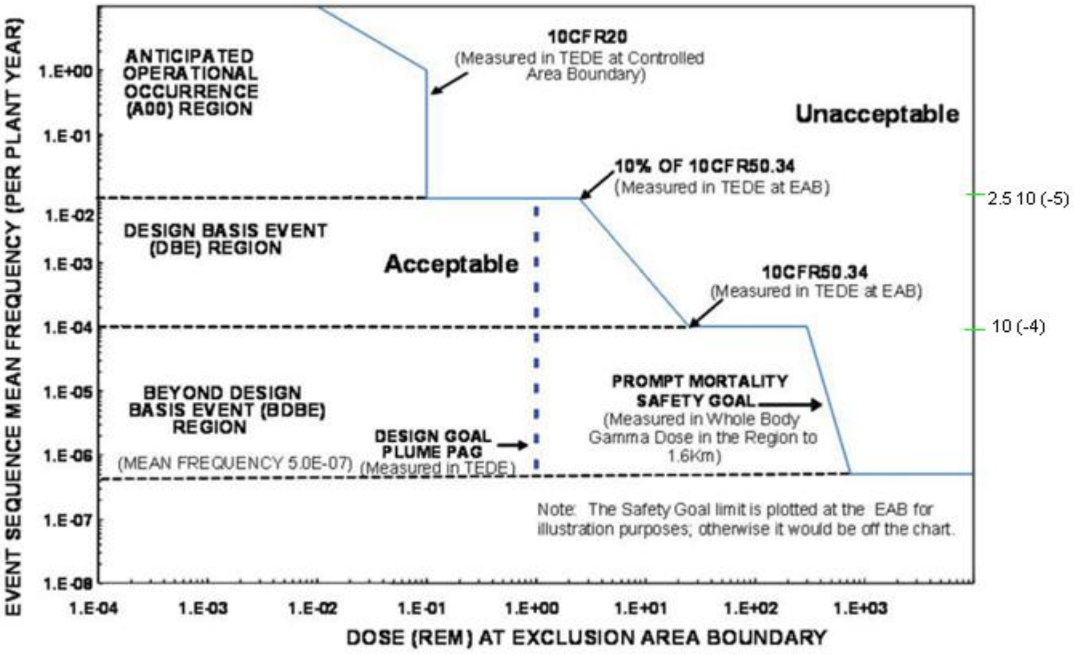


Figure 2.1.1-1 Exclusion area dose

2.1.2 Licensing basis events

Three categories have been postulated function of the event frequency:

- Anticipated Operational Occurrences (AOO) (higher than2.5 10^{-2} / y to be expected once or more in the plant lifetime ; consequences to be calculated with realistic assumptions)
- Design Basis Events (DBE) (between 2.5 10^{-2} / y and 10^{-4} / y , and not expected to occur in the lifetime of the plant ; consequences conservatively calculated)
- Emergency Planning Basis Events (EPBE) (between 10^{-4} / y and 5 10^{-7} / y not expected to occur in the lifetime of a fleet of plants, consequences realistically evaluated)

Each event is then located in the frequency-dose diagram, to verify it's situation regarding the acceptable zone.

2.1.3 Selection of safety related equipment

A two-step method is used for the identification of the MHTGR SSC (Systems, Structures and Components).

The 3 main safety functions that are to be performed by the SSC are:

- The heat generation control
- The core heat removal
- The chemical attack control

In the first step of the method, a list of DBE (for which the use of this function is critical) is established for each safety function. The list of minimal SSC "available and sufficient" can then be chosen, in order to perform the safety function for all the DBE. This is done for each of the safety functions (see Figure 2.1.3-1).

Hereafter a fictive example is given for the “core heat removal” function. All the DBE requiring this safety function are considered. Introducing one single SSC, it must be known if it is available and sufficient to perform the safety function during the DBE.

i.e., Identification of available and sufficient SSC to remove core heat during DBE						
SSC Design	**DBE 2**	**DBE 6**	**DBE 7**	**DBE 9**	**DBE 12**	**DBE 13**
SSC A	yes	yes	no	yes	no	yes
SSC B	**yes**	no	**yes**	no	no	yes
SSC D	no	no	no	yes	no	yes
SSC K	yes	no	no	no	yes	yes
SSC L	no	**yes**	no	**yes**	**yes**	**yes**

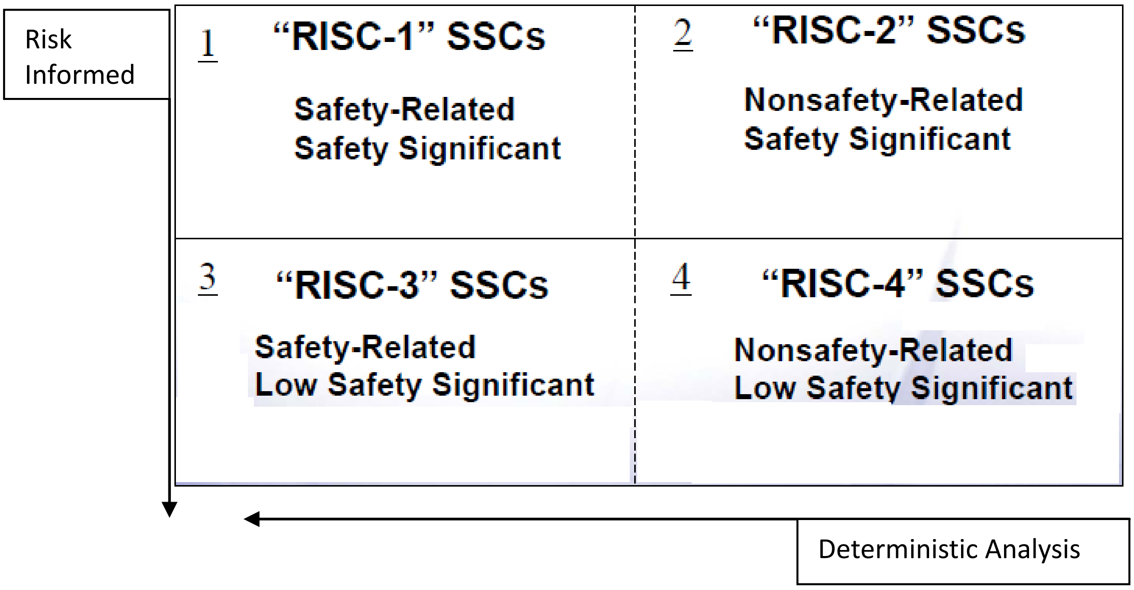
Figure 2.1.3-1 SSC identification

But a better choice would be B and L, representing the list of minimal SSC’s that are sufficient to perform the required safety function for all concerned DBE’s.

This method leads to respect the dose limits for all DBE’s and this with a minimal list of SSC that are chosen for the final MHTGR design, which increases the mitigation threshold.

In the second step, supplementary SSC can be chosen in order to lower the frequency of some events (for which consequences would be too important in DBE region) to be sure that they are outside the DBE region, which increases the prevention threshold.

Otherwise, and based upon current 10 CFR 50.69, the following leeway could be applied[15]:



2.1.4 Classification

On this basis, Regulatory Design Criteria (RDC) are written at a functional level to describe the (qualitative) requirements for SSC needed during DBE to assure compliance with 10.CFR50 §34.

[15] Not applicable to GEN IV reactors; an iterative process plus need for further development in regulations need to be observed.

Moreover, quantitative requirements are developed by stipulating that the safety-related SSC by them be sufficient for each of the DBE to meet the DBE dose criteria.
Revaluating the DBE non-mechanistically with only the safety-related SSC available leads to the Safety-Related Design Conditions (SRDC). The SRDC are used to develop the temperatures, stresses, heat loads, etc. that the SSC must meet for each of the DBE.

2.2 NRC's review of the Key Policy Safety Issues

The key safety issues identified by the NRC were:

- Selection of events that must be considered in the design,
- Sitting source-term calculation and use,
- Adequacy of the containment concept,
- Adequacy of emergency planning.

In general, the review approach used by the NRC staff paralleled that used for LWRs. It consists of an evaluation of the many factors that contribute to LWR safety (such as conservative design oversight directed toward accident prevention and the use of redundancy and diversity in accomplishing key safety functions) and ensuring that similar factors or adequate substitutes were provided for the MHTGR approach. In general, however, it can be demonstrated that the level of design detail expectancy required for Non-LWRs is higher just by quoting 10 CFR 52.47(c)(2):

> *…An application for certification of a nuclear power reactor design that differs significantly from the light-water reactor designs described in paragraph (c)(1) of this section or uses simplified, inherent, passive, or other innovative means to accomplish its safety functions must provide an essentially complete nuclear power reactor design except for site-specific elements such as the service water intake structure and the ultimate heat sink, and must meet the requirements of 10 CFR 50.43(e)…*

The NRC review approach was thusly purely deterministic, while the DOE considers PSA in its design methodology.
Defense-in-depth was considered as a basis. Inherent in the approach is the swap in emphasis in DiD from accident mitigation to accident prevention and plant protection. Therefore, the review also considered the need for a conventional containment structure and pre-planned offsite evacuation.

2.2.1 Selection of events that must be considered in the design

The NRC defined four event categories, which, in general, correspond to traditional LWR event categories (abnormal operational occurrences, design-basis accidents, SAs, emergency-planning-basis events).
In order to bound uncertainties in DOE's probabilistic analysis and to compensate for the use of non-safety-grade equipment, the NRC has imposed stringent bounding events. Following the NRC, if more information becomes available in the future about some topics (sabotage, external events), the events in each category can be revised.

2.2.2 Sitting source term calculation and use

Because of the high inherent potential to exclude core damage in the MHTGR design, a mechanistic analysis of radionuclide releases for a range of low-probability events (equivalent to severe sequences for LWRs) was proposed by the DOE as a substitute for the traditional non-

mechanistic source term that is representative of a source term from a core-melt accident utilized in LWR siting dose[16]. This approach is apparently a departure from LWR safety approach.
The NRC imposed that bounding events were used by the DOE in a mechanistic analysis as a test of the MHTGR's ability to potentially meet proposed sitting criteria (doses were calculated for each event).
The relationship between the events that must be considered in the design of the MHTGR and the use of the proposed mechanistic source term for sitting evaluations was apparently categorized to be of deep importance.
The technical features supporting the use of the mechanistic source term in computing doses at the exclusion area boundary are:

- The potential fission-product-containment capability of the coated particle type fuel.
- The potential for achievement of very few defective fuel particles at the fuel manufacturing stage (the necessary product quality specifications allows only 25 defective particles per 100000).
- The potential for the passive shutdown and heat removal systems under adverse conditions to maintain fuel-particle temperatures below about 1600°C
- The lift-off and transport phenomena pertaining to the radionuclide within the primary system.

2.2.3 Adequacy of the containment concept

DOE has suggested that the MHTGR does not require a conventional (pressure retaining) containment structure.
The basis for this proposal is that under all events, the dose guidelines of 10 CFR part 100 can be met without a conventional containment structure. However this standpoint seems questionable when challenged, for instance, by design basis threats (external events).
The containment doesn't provide a leak tight, pressurized containment function, but controlled venting function (see § 1.6). Small releases could be filtered and contained in the HVAC system as what is to be usual under normal operation conditions. For larger releases, vent pathways would as well provide overpressure protection.
It is clear that a design without a conventional containment building represents a significant departure from past practice on LWRs[17].
In any case, such designs should be sanctioned as applicable, the ultimate acceptance will require review, testing, and demonstration (see ACRS letter 3421324 on Containment related issues). The NRC proposes the following criteria to accept a design (like MHTGR) without conventional containment:

- Respecting the dose limits for each event.
- Fission product retention capability must be demonstrated via a testing program using a full-size prototype plant.

[16] This source term was calculated on the basis that no substantial fuel failure will occur even when the reactor is subjected to the bounding events. The radionuclide inventory in the primary system (plated out on primary system surfaces and to a lesser extent, circulating with the helium coolant) derived from a small amount of initially defective fuel that can be augmented to only a small degree by the occurrence of certain bounding events.

[17] And that under certain situations LWR containment buildings have been effective components of the defence-in-depth approach.

- QA, surveillance, in-service inspection, should be provided to ensure that the new and innovative systems, structures and components that contribute to performing the containment function, are built, operated and maintained over the life of the plant, in a fashion commensurate with their safety function. For example, the MHTGR fuel quality.
- Protection from sabotage and external events should be at least equivalent to that for current generation LWRs.
- No core melt accident or large release accident (as graphite fires) are present in the design events.
- An assessment would have to be made of the potential improvement in safety if a containment building were added. Judgment would then be used to determine the need for a containment building based on the changes in cost-benefit analysis.

The forth bullet above, silent nonetheless, provides some insight about what the eventual position of the NRC is as to security/safety of the containment/confinement structures when challenged by external events.

2.2.4 Offsite emergency planning

As for the containment issue, the NRC acceptance of this emergency-planning will depend on the acceptance of the proposed mechanistic source term, for which more information is needed. NRC proposes the following criteria as guidelines to accept a proposal of no traditional offsite emergency planning:

- The lower-level Protection Action Guidelines (PAG) were not predicted to be exceeded at the site boundary within the first 36 hours following any event in categories of abnormal operational occurrences (AOO), design basis accidents (DBA) and SAs (SA).
- A PRA for the plant including all events in categories AOO, DBA, SA and emergency-planning-basis events, indicates that the cumulative mean value for the frequency of exceeding the lower-level PAG at the site boundary within the firs 36 hours did not exceed approximately 10^{-6} per year.

2.3 Tthe modular HTGR (IAEA)

The IAEA TECDOC “Safety and Licensing Aspects of the Modular HTGR” is based on two IAEA workshops. The objective of the IAEA report is to provide an overview of the MHTGR technology as it relates to nuclear safety, and to make suggestions regarding the technical basis and the methodology to generate design safety requirements. The document also examines how the defence-in-depth principle is implemented/adopted by the MHTGR design and how a specific MHTGR design satisfies the three fundamental safety objectives, General Nuclear Safety, Radiation Protection and Technical Safety. The discussion of these objectives and principles provides a framework for development of future IAEA documents related to the MHTGR safety case.
The implementation of defence-in-depth for MHTGR is quite different from that of water reactors. These differences can have significant impacts on the licensing approach for Plant design, construction and operation.
The report considers only the three fundamental safety functions:

- Control of reactivity,
- Core heat removal,
- Confinement of radioactive materials.

Note that this list basically concurs with the NRC high level main safety functions except for the chemical attack, which is replaced by the confinement of radioactive by-products. Out of the scope of the present guidelines are the various shutdown modes. This report does not consider fuel storage and radioactive waste.

2.3.1 Method of the objective-provision tree

The methodology for screening the defence-in-depth of nuclear power plants is presented in the chart below. A top down approach is proposed consisting of a systematic review of the existing requirements for NPPs starting from the most general (applicable to all nuclear plants) and down to the most specific and more technology dependent ones. Since MHTGR makes extensive use of inherent design safety features, the requirements for these reactors could be less demanding than those for LWRs.
The method of the objective provisions tree represents a preliminary attempt to systematically review the implementation of the defence-in-depth. The logical framework of the objective provisions method is graphically depicted in terms of a tree (see Figure 2.3.1-1).

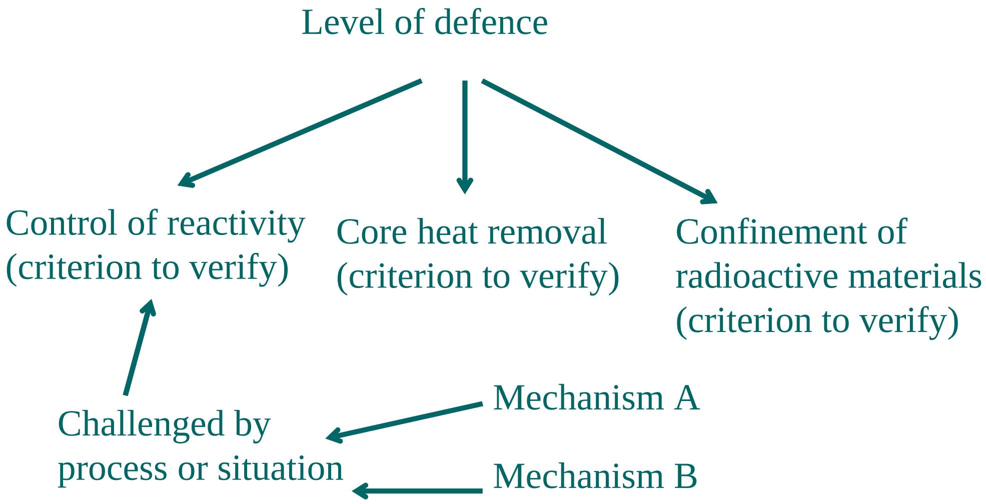


Figure 2.3.1-1 Provision tree

At the top of the tree is the level of defence (5 levels are considered) having each a specific objective:

- **Level 1** : Deviation from normal operation and prevention of failure.
- **Level 2** : Control of abnormal operation and detection of failure.
- **Level 3** : Control of accidents within the design bases.
- **Level 4** : Control of severe plant conditions, including prevention of accidents progression, and mitigation of the consequences of SAs.
- **Level 5** : Off-site measures to reduce the consequences of SAs.

For each of these levels, the 3 fundamental safety functions are checked:

- Control of reactivity;
- Core heat removal;
- Confinement of radioactivity.

For each bin “level-safety function”, an acceptance criterion is defined.

At this point the challenges of the safety functions can be identified. These challenges are general processes or situations that may prevent adequate performance of the safety functions (e.g. reactivity excursions that could damage the fuel before the shut-down). The challenges arise from a variety of mechanisms that have also to be identified. Once the mechanisms are known it is possible to determine the provisions necessary to prevent and/or control these mechanisms.

2.3.2 Result of the MHTGR IAEA review using the objective-provision tree method

The adopted top down approach shows the need for developing specific design requirements for MHTGR, for those inherent features, systems, structures or components which play important roles in the implementation of the defence-in-depth.
Stronger provisions at Level 1, reduce the requirements on monitoring and controlling at Level 2. Passive safety features at Level 3 reduce the requirements on active engineered safety features at the same level and enhance the overall safety performance. Design basis accidents are mostly dealt with inherent features and passive mechanisms. For beyond-design-basis the thermal inertia of MHTGR enhances the effectiveness of Level 4 by providing sufficient time for operator response and mitigating measures.
The MHTGR design characteristics allow the demonstration that for internal initiating events, SA scenarios can be practically excluded. Design provisions and accident management measures, however, should be considered for very unlikely external challenges, like earthquakes, floods or aircraft crashes.

2.4 Pebble bed modular reactor in the United States, Exelon Generation Company

This is the most recent and updated work to this time, and has been subject of additional review by Westinghouse Electric Corp. and Idaho National Labs.
In the same way DOE has proposed a licensing approach to the NRC for the MHTGR project in the 80s, Exelon proposes a licensing approach to the NRC for the PBMR project.
This document is rather recent (2001), and appears more than 10 years after the MHTGR licensing proposal of the DOE. At the present time, this document is not more than a proposal for a safety approach. There is no available safety evaluation of the PBMR, and no NRC review concerning this safety approach is yet available at this date concerning generic PBMR safety evaluation.
However, it has to be noted that NRC staff has recently issued:

- **In March 2002**, “Preliminary findings regarding Exelon’s proposed licensing approach for the PBMR”
- **In July 2002**, SECY-02-0139 “Plan for resolving Policy issues related to licensing Non-LWR designs”.

Although being not a complete safety evaluation, those documents are giving more information on the current ongoing NRC Risk-informed licensing framework, and are certainly useful to analyze in the frame of the EUROPAIRS project. Before that, NRC accepted only risk-informed approach in the frame of modifications on existing plants.
According to Exelon, the used approach for PBMR is close to the one developed for the MHTGR, but modified to reflect the advances that have been made since then in risk-informed regulation.

2.4.1 Safety approach and PBMR specific features

First, the approach identifies the “Top Level Regulatory Criteria” (TLRC) resulting in almost the same “frequency-dose” curve to respect as the one developed by DOE for MHTGR (see § 2.3.1). The Exelon curve is a bit more conservative in the AOO region.
A first specific feature of the PBMR is its modularity, and it requires an interpretation of the regulation for LWRs. For LWRs, the releases for normal operation are limited for the plant site, but the releases following design events are limited for each unit individually.
The proposed methodology for PMBR is more conservative, considering criteria for the site, regardless of the number of modules.
A second feature of the proposed PBMR safety approach, as it was already the case for MHTGR, is the reduction of the exclusion area from one (prompt mortality) and 10 (delayed mortality) miles, to 400 meters from the nearest module, in order to limit the emergency-preparedness requirements zone to the site boundary. The first remark is that the traditional top-down levels 1-2-3 models of an LWR PRA are grouped into a single PRA method for PBMR.
Another difference is that the fraction of time in shutdown mode for PBMR (due to online refueling) is one order of magnitude smaller than for LWR, reducing the corresponding risk exposure. The PRA model shutdown state is particular for LWR, but all states are integrated in the same model for the PBMR PRA. Moreover, the modularity principle can lead to accidents in which several modules are impacted at the same time.
For each event, the consequences are calculated (the calculation examples in the document are from MHTGR, because not yet available for PBMR) with uncertainties taken into account (for frequency and for consequences) and the results are plotted in the ‘frequency-dose” curve.

2.4.2 Structures, Systems, and Components (SSC) selection and classification

The proposed method is exactly the same as proposed by the DOE for MHTGR.

2.4.3 Consistency with current regulatory practice

After that, it is described how the PBMR licensing approach is consistent with the NRC policies on the licensing of advanced reactors. The principles of risk-informed regulation are explained, with respect to the DiD philosophy.
For PBMR, the different barriers are:

- The fuel (particle, and pebble),
- The reactor coolant pressure boundary (RCPB),
- The containment and citadel (structural barrier) and confinement boundary (to filter any release from the RCPB).

2.5 South African National Nuclear Regulator

This document is rather recent and is a list of requirements of the South-African regulator about the PBMR project which is planned to be built in South Africa.

2.5.1 NNR requirements

NNR requires that the principles of DiD and ALARA have to be adopted by the designer.
NNR defines 3 groups of events in function of both the frequency of occurrence and consequences. For each of them, safety requirements and criteria are provided.

- **Category A** having a frequency higher than 10^{-2} / y and treated as part of normal operation. The safety criteria are 20 mSv/y for the plant personnel and 250 µSv/y for the public.
- **Category B** having a frequency between 10^{-2} and 10^{-6} / y. The safety criteria are 500 mSv for the plant personnel and 50 mSv for the public, this for one single event or combination of events. This analysis shall be conservative and have to include consideration of hazards inside and outside the plant.
- **Category C** concerns all the events leading to exposure, whatever the frequency. The criteria are expressed in terms of risk to the plant personnel (10^{-5}/y) and to the public (10^{-8}/y) per site.

For category C, a PRA (probabilistic risk assessment) shall be performed in order to verify those criteria. This includes also the events or combination of events with annual frequency less than 10^{-6} /y, and all the hazards. This analysis may be carried out using best estimate methodology, but uncertainties and sensitivity studies have to be taken into account.
Moreover, a supplementary criterion (risk aversion criterion) has to be verified in order to limit the frequency of accidents leading to important fatalities. This limit reduces the contribution of the risk due to large accidents (coming from the psychological aversion of the population against SAs, whatever their frequency). However, the formulation of this criterion seems quite complicate and difficult to implement on a particular case.
In addition to those engineered safety features, an emergency response plan shall be developed: the extent of this ERP plan shall be commensurate with the radiological consequences predicted for these accident sequences.
NNR adds a glossary of terms which is very important and leads to more precise requirements (reducing the interpretation margin of the requirements for the designer). As a very important example, the single failure criterion is precisely described, concerning both active and passive components.
The single failure principle requires that the plant be capable of achieving the 3 main safety functions (reactivity control, heat removal, confinement of radioactivity) during an event even if a single failure is postulated.
Currently, the NNR is planning to impose occupational exposure limits to accidental conditions.

2.6 European Utility Requirements

The EUR organization authorizes to use the EUR document in order to develop a set of requirements documents for other nuclear designs.
In the frame of this European Commission EUROPAIRS project, aiming to set the grounds for commissioning a future HTR to VHTR in Europe, EUR is certainly a reference to be considered.
As a second remark, it has to be noted that for designs other than LWR:

- Some EUR requirements are not applicable (like fuel performance) or partially applicable or applicable with interpretation (like pressure-retaining containment requirements)
- Some requirements for HTRs don’t appear in EUR (like requirements on components)

Anyway, it is possible to already identify some key points of such a future establishment of requirements for HTR.

2.6.1 EUR safety requirements and safety approach:

This Chapter (Chapter 2.6) was already included in the discussion above in Section 1.

2.7 Past HTR Know-How Database

2.7.1 United Kingdom.

In order to be able to understand this licensing process, a brief summary of the current regulatory framework within the United Kingdom is first given. By law, all reactors within the UK require a nuclear site licence, which applies throughout the entire life cycle of the plant, from preliminary discussions over siting through to decommissioning. For all licenses there are currently 35 standard conditions that are not prescriptive in terms of detailed safety requirements but are goal setting in that they focus on the issues that are considered important to the management of safety. The Regulator’s views of the conditions that will need to be met are established in the Safety Assessment Procedures (SAPs). These are primarily intended for the assessment of new plants and are consistent with IAEA standards.

2.7.1.1 Advanced Gas Cooled Reactors (AGR)

In the case of the older AGR the initial safety cases were based on deterministic and engineering criteria. For the newer AGR, Heysham 2 and Torness, both deterministic analysis and a Level 1 PSA were performed as part of the initial safety cases. In order to demonstrate compliance with the current AGR nuclear safety standards (the Nuclear Safety Principles for the Safety Review of the AGRs), both Level 1 and Level 2 PSA have been carried out for all the AGR stations. A simple treatment of internal and external hazards amenable to probabilistic treatment has been included. The PSA are complemented by a detailed Human Factors Assessment, which has identified and underwritten the operator actions claimed in the PSA model.

2.7.2 Germany

The Safety items for the HTR Module (Siemens design of the 80s) were accepted by the TUeV Hanover (authorized body in licensing) as well as of the RSK (experts from the German Federal Government). The full recommendations of the RSK were published in Bundesanzeiger Nr. 81 (28.04.1990).
The safety concept review can be summarized as follows:

- The applicant had demonstrated successfully that the radiation exposure in the environment caused by the discharge of radioactive substances from the modular NPP during normal operation is far below the dose limits according to § 45 of the Radiological Protection Ordinance and that the measures for radiation protection of the personnel have been planned adequately.
- An important prerequisite for the assessment was to elaborate a complete and representative catalogue of design basis accidents analogously to the accident guidelines for pressurized water reactors. This task “inter alia” facilitated to distinguish between design basis accidents and accidents beyond design basis.
- Based on the design documents an extensive accident analysis was performed and design requirements were developed for all components and systems. It was verified, that the planned design of the buildings, systems and components as well as the operation modes of the plant will meet these requirements. These investigations were performed considering the conservative assumptions typical for licensing procedures of nuclear facilities.
- A further result of the accident analysis was the identification of radiologically representative accidents and a successful verification that after these accidents the dose limits given in § 28 sec. 3 of the Radiological Protection Ordinance are not exceeded and that the necessary protective measures against the hazards of nuclear technology have been planned according to the state of the art.

Based on the safety assessment it was confirmed that the design of the HTR Module meets the safety requirements to be imposed on nuclear facilities in Germany.

2.7.3 United States

2.7.3.1 Fort Saint Vrain

The safety evaluation was performed by the Commission's regulatory Staff. Despite the age of the document, the description of the licensing procedure and the used method are quite interesting for the present EUROPAIRS project. As features to mention, the effect of accidents analyses on the technical specifications, or the fact that the safety authority verified the safety studies using its own hypotheses.

The entire reactor primary system, including the steam generators and the helium circulators, is located within a steel-lined pre-stressed concrete reactor vessel (PCRV). This PCRV not only serves as a pressure vessel for the reactor, but also provides a containment function similar to that provided by the containment building for a LWR. The PCRV is housed in a conventional steel frame building (the reactor building) which is sufficiently leak-tight to assure positive flow of ventilation air through filters and to vent. While this building does not provide a containment function as such, it does serve as a confinement structure for fuel and waste handling activities in a manner analogous to that provided by the reactor building for a boiling water reactor.

The fuel consists of fissile (thorium and Uranium enriched at 93% $ThUC_2$) and fertile (thorium ThC_2) fuel particles. Both particles are provided with a three-layer coating (Triso-II) consisting of:

- An inner layer of porous pyrolytic carbon.
- An intermediate layer of silicon carbide (SiC).
- An outer layer of highly impervious, high density isotropic pyrolytic carbon.

Results from the Applicant's irradiation test program have demonstrated the fuel performances (burn up, maximal temperature). It was concluded that the fission product releases from fuel particles coating contaminant and from diffusion of fission products through intact coatings were small under normal reactor operating conditions:

- A one mile square exclusion area was defined. A low population zone (LPZ) distance of 10 miles has been selected. The nearest population center is situated 14 miles from the reactor. With such data, it has been verified that the 10 CFR Part 100 guidelines were met, calculating the potential offsite doses that might results from the postulated Design Bases Accidents.
- First of all, the response of the facility to various Anticipated Operating Transients was evaluated (turbine trip, loss of offsite power, control rod malfunction, loss of feedwater flow, etc). Those transients didn't results in release of fission products in the environment.

- A broad spectrum of accidents that might result from postulated failures of systems or components to perform their intended functions, have also been evaluated ("loss-of-forced-circulation of the coolant" and "rapid depressurization" being the 2 most representative). Different reactivity transients have also been evaluated ("control rod withdrawal being the most representative"), using a 2-dimensional heat transfer and point kinetic code. For the "rapid depressurization" accident, the method used is quite interesting. First of all, the NRC has reviewed the study performed by the utility, using sometimes more conservative hypotheses. For this accident, the source term that has been considered by the Staff is the total primary plate out activity inventory, such that the calculated dose at the exclusion boundary will reach a target value (well below the 10 CFR guidelines) being 150 rem thyroid, 75 rem bone, 7 rem whole body. As a consequence, the NRC asked to include those corresponding primary plate-out values (5000 Ci/loop for I-131 and 140 Ci/loop for Sr-90) in the Fort St. Vrain technical specification. The Applicant determined the plate-out inventory by periodic measurements with plate-out probes.
- The applicant defined a "maximum credible accident" for the Fort St Vrain reactor. It is defined as that due to failures in the seismic class I helium purification system connection to the regeneration system concurrently with the inability or failure to close the isolation valve at the discharge from the high temperature filter/absorber. The resulting accident releases primary coolant-helium and the associated radioactivity into the reactor building over a period of about 2 hours. It must be mentioned that the Staff has reviewed the study performed by the Applicant, using sometimes more conservative hypotheses (for dose calculation as an example) than those used by the Applicant. Even using the Staff most conservative hypotheses, the calculated dose at the exclusion area boundary are well below the 10 CFR 100 limits. Low population zone doses are negligible.
- The applicant also considered different initiating events ATWS (anticipated transient without scram) scenarios. For some cases, the reactor reaches an equilibrium state (without fuel failure) after 15-30 min without any operator action. For "primary system depressurization without scram", the operator will have well over 30 minutes to assess the situation and to activate a manual scram or the reserve shutdown system. For the "rod withdrawal accident without scram", about 2% of the fuel particles failed, but the PCRV integrity prevents any release.

2.8 Comparison amongst Safety approaches

A comparison between some safety approaches is performed hereafter, in order to identify the differences and the key points. No judgment is made to give more credit to one approach compared to other approaches.

2.8.1 IAEA and NUREG Regulatory Criteria.

The objective of the IAEA report is to provide an overview of the MHTGR technology as it relates to nuclear safety, and to give suggestions regarding the technical basis and the methodology to generate design safety requirements.
On the contrary to the NRC review of the MHTGR, IAEA proposes a methodology, and does not perform any safety quantitative evaluation of a given HTR project. The MHTGR described by the IAEA is the general HTR concept (with direct cycle or with steam cycle, with prismatic blocks or with pebble bed fuel product) while the MHTGR described in the NUREG is a specific project (steam cycle, prismatic block).
Moreover, the NUREG guidance refers to the licensing context applicable in the Code of Federal Regulations, while IAEA refers to INSAG3 guidelines.

The NUREG document is thus more specific and also more detailed, defining quantitative safety objectives and performing quantitative safety evaluations, while IAEA proposes a general methodology to design an HTR.
In the NUREG, the interaction between designer (DOE) and safety authorities (NRC) is closer to what could be a future HTR licensing procedure.

2.8.2 IAEA and DOE-NUREG methodologies.

IAEA approach is deterministic, based on the DiD principles.
DOE approach makes use of probabilistic quantification (but not to all extent, events are situated in a frequency-dose diagram and their consequences are calculated with best-estimate methods, except in the DBE region where the calculation is conservative and following prescriptions of 10 CFR 50 34). DOE defines quantifiable statements of acceptable consequences or risks to the public or to the environment (individual acute and latent fatality risks, annualized offsite dose guidelines, accident offsite dose and protective action guideline dose). This leads to define an acceptable zone in the frequency-dose diagram.
Moreover, in order to respect the acceptable region in the frequency-dose diagram, DOE proposes a method to select and to classify SSC (systems structure and components).
IAEA has developed a systematic methodology, called “Objective provision tree” to verify the applicability of the DiD principle.
Differences appear for the key safety functions to consider in the design:

- For DOE (MHTGR): Control of reactivity, core heat removal, and control of chemical attack
- For IAEA: Control of reactivity, core heat removal, and confinement of radioactive materials

Comparing the 2 approaches, the events to be considered in the DOE approach are to be compared with the mechanism challenging the different safety functions at a given level in the IAEA method. On both sides, the selection of events or mechanisms is fundamental to the safety evaluation.
Differences appear between criteria to be respected. IAEA uses qualitative criteria (for each pair “level-safety function”), while DOE uses quantitative dose limits to be respected for each event category.
Those approach differences can lead to much different conclusions in the final safety evaluation (next chapter).

2.8.3 IAEA and NRC Recommendations about HTR Safety.

In the NRC review of the DOE approach, the NRC follows a deterministic approach invoking PRA for the selection of events, practice extended from LWRs. The NRC defines four key safety issues to verify:

- events to consider,
- sitting source term,
- containment,
- emergency planning/preparedness.

The DOE quantitative approach shows the need for the calculation of a sitting source term, which is considered as a key point of the NRC safety evaluation. This aspect doesn’t appear in the IAEA document.
NRC doesn’t have yet a recommendation about the building type. NRC encourages the efforts of the DOE to justify that a conventional containment is not needed for the MHTGR, but NRC doesn’t exclude that, even with additional information, containment will be required. The NRC proposes

criteria to accept a design without conventional containment. Among others, the NRC asks a protection against design basis threats and external events at least equivalent to that for current generation LWRs.
According to IAEA, a conventional containment is not useful, and is possibly less safe than a filtered and vented confinement. The justification is that for LWRs, steam released from the primary can condense on the structure, resulting in a rapid decrease in pressure. This is not the case with helium, and moreover, helium leaks easily. By retaining the helium following a depressurization, the gas leaking from the containment can serve as a transport medium for radionuclides (which is not the case with a filtered confinement).
In general, IAEA recognizes the HTR concept as inherently safe. The only remark of IAEA is that <<…design provisions and accident management measures should be considered also for very unlikely external challenges, like earthquakes, floods or airplane crashes…>>. This is to be noted as a significant consistency between EUR and IAEA, but doesn't specifically prescribe that a pressure retaining building shall be hold in place.
NRC advocates that the MHTGR has the potential to make a future safety demonstration when it is deemed that the information resources are not enough, but not necessarily if new information will become available about different topics through research and prototype tests (the justification of the sitting source term being maybe the most important issue).

2.8.4 Exelon proposal for PBMR licensing approach and DOE approach for MHTGR.

In the same way DOE has proposed a licensing approach to the NRC for the MHTGR project in the 80s, Exelon proposes a licensing approach to the NRC for the PBMR project.
Following Exelon, this approach is close to the one developed for the MHTGR, but modified to reflect the advances that have been made since then in risk-informed regulation. Exelon tries to defend widely such an approach, in order to support the acceptability of deviations from current LWR licensing requirements.
The proposed method to select and to classify SSC (systems structure and components) is about the same for MHTGR and for PBMR.
The main new aspect appearing for PBMR in comparison to MHTGR is the modularity aspect requiring an interpretation of regulation for LWRs.

2.8.5 Comparison between regulators' points of view.

The review approach used by the NRC staff paralleled that used for LWRs. It consists of an evaluation of the many factors that contribute to LWR safety (such as conservative design oversight directed toward accident prevention and the use of redundancy and diversity in accomplishing key safety functions) and ensuring that similar factors or adequate substitutes were provided for the MHTGR approach.
The NRC review approach on MHTGR is purely deterministic, but this position is not recent (1989). The more recent preliminary NRC review on PBMR seems more open concerning PRA.
The NNR review is rather original, mixing deterministic calculations and complete PRA evaluations:

- Firstly, NNR defines 2 events categories (normal conditions, accidental conditions) in function of the frequency, to be deterministically treated, and having doses as criteria to respect.
- Secondly, NNR defines a third category for all the events leading to exposure, whatever the frequency. The general criterion is a risk to respect. NNR requires in fact a complete PRA of the plant.

2.8.6 EUR and other approaches

Some EUR requirements are not applicable, like the release target of a given radionuclide, or like the fuel acceptance criteria (departure from nucleate boiling ratio, criterion for loss of coolant accident) that are specific for LWR fuel.
But the safety approach and the dose targets (at the base of the release targets proposed in the document) adopted in EUR are certainly to be considered. Moreover, EUR proposes classification and qualification requirements for SSC that can be applied.
In order to strongly limit the frequencies of very large events, the “risk aversion criterion” required by the regulator NNR has the same objective than the “cliff-edge effect criterion” proposed by EUR for the design verification (the formulation being much simpler to apply as the one proposed by NNR).

2.9 Adapting LWRs Regulations to HTGRs

Given the limited regulatory experience with gas reactor technology as well as its deployment in non-traditional process heat applications, there is not an existing and complete body of regulations directly suited to the VHTR/HTR design. Consequently, derivations from the existing LWR regulations may be equally have to be proposed.

The introduction to Appendix A of 10 CFR 50 recognizes the need to adapt LWR regulations for Non-LWR applications when it states:

<<…These General Design Criteria establish minimum requirements for the principal design criteria for water-cooled nuclear power plants similar in design and location to plants for which construction permits have been issued by the Commission. **The General Design Criteria are also considered to be generally applicable to other types of nuclear power units and are intended to provide guidance in establishing the principal design criteria for such other units***…>>*

It is therefore clear that the current set of regulations and guidance should be reviewed for applicability to a high-temperature gas reactor design. Engagement with the Regulatory Bodies worldwide is needed to reach agreement on the scope and development of new regulatory policies or to change existing regulatory policies that support the high-temperature gas reactor design so that the licensing process is successful.

2.9.1. Adapting LWR Regulations: Deterministic Option

The safety approach might be rooted in deterministic engineering principles, not excluding that for determining licensing basis events (LBEs) could be risk-informed, and thusly be based on both deterministic and probabilistic elements. Other areas where a combination of deterministic and probabilistic analysis will play a role include the definition of safety functions and success criteria, the prediction of plant response to initiating events, and the development of mechanistic source terms.

2.9.2. Adapting LWR Regulations: PRA

The rationale for use of these risk-assessment techniques includes:

- Using PRA in order to aid in the screening of top events that are included in the licensing basis, maximizes the probability of establishing a comprehensive safety basis. By its nature, PRA development is a rigorous process that considers the comprehensive performance of the facility design and safety margins.
- The PRA contains deterministic in nature tools (e.g., failure modes and effects analysis and reactor system performance analyses).
- Probabilistic methods for event selection, SSC classification, special treatment identification, as well as integration and evaluation of defense-in-depth strategies will take advantage of the safety characteristics provided by gas-cooled reactor designs.
- Integrating PRA insights into the design provides a more structured means for both assessing single point vulnerabilities as required by the single failure criterion used in current LWRs and providing more robust capability for considering functional vulnerabilities and diversity for all portions of the event frequency spectrum. This is of considerable value, particularly for designs that are new or contain novel features.
- Using a PRA provides a rational method for selecting design features and resolving safety issues; hence avoiding conflicting requirements that can arise from a purely deterministic design and safety analysis approach.
- The PRA provides a rational approach for identifying, understanding, and addressing uncertainties.

3 Aspects Within the Safety Approach

From the different selected reference documents, some key points are identified in the safety approach to be developed. First of all, an efficient integration of both followings methods has to be made :

- **Deterministic approach.** The pure deterministic approach consists of putting accident initiators into categories (in function of an estimated frequency), and to fix a (dose) criterion that must be met for each category (DOE approach for MHTGR, NRC approach). The criterion to meet is fixed for one single event. In a deterministic approach, prevention and mitigation are decoupled. First of all, all the SSE are designed and classified in order to provide the required safety functions during accidents, considering single failure. This process provides strong prevention. Secondly, accident initiators are put in categories, and the objective is then only to mitigate the accident consequences.
- **Probabilistic approach.** EUR introduces a verification of the design by limiting the frequency of some groups of events (leading to core melt, leading to cliff edge effect, leading to unacceptable releases) by a bounding value. NNR introduces PRA in the design itself, requesting a complete PRA adopting as criterion the general risk of the HTR site. In such a PRA approach, prevention and mitigation aspects are coupled and have the same importance. Recent NRC safety cases have required some probabilistic analysis for PWR, and preliminary PBMR review shows that NRC is more open to this approach. Indeed, the proposed method for PBMR uses probabilistic criteria to select events for consideration in the design and, in conjunction with accident scenario specific source terms and dose limits, to demonstrate the acceptability of the plant design. The safety classification of systems, structures and components, as well as the application of the single failure criterion, are also different from conventional practice. This also affects the traditional approach to defence-in-depth by utilizing probabilistic criteria as a substitute for certain defence-in-depth attributes (e.g., single failure criterion).

In Europe, at the present time, the deterministic approach has certainly to be taken into account, and the PRA has to be considered more as a verification (confirmation) of the design, like it is done in EUR. Going one step further, a complete PRA can provide supplementary useful information in both ways:

- To demonstrate the design strength.
- To reveal some weaknesses.

The HTR safety and licensing key points are:

- The modularity concept having an impact on the release limits by module to consider (as mentioned by Exelon for PBMR). This aspect has to be treated in the safety approach.
- Conservative or best-estimate analysis, use of single failure criterion.
- Determination of one or several fuel design criteria (interface with European Commission HTR-L project).
- List of initiating events.
- Choice of safety functions to implement (Control of reactivity, core heat removal, control of chemical attack, confinement of radioactive materials).
- Method to choose and to classify SSC (structure, systems, and components).
- The prediction of the temperature in the fuel elements during operation and during accidents
- The knowledge of the radionuclide behaviour (chemically and physically) which can lead to lower the uncertainties to be considered for the source term in a licensing procedure.
- The containment or confinement choice will strongly affect the HTR investment, the release calculation, and the licensing procedure. The regulator has to be convinced about the exact containment (confinement) role of an HTR. Having in mind the role of containment for LWRs can lead to wrong requirements. Both pressure resistant containment necessity and usefulness have to be considered. Firstly, concerning necessity, the frequency of large release events is very small, and the risk reduction due to the presence of pressure resistant containment is not as significant for HTR as it is for LWR. Secondly, concerning usefulness of a pressure resistant containment, helium leaks easily and doesn't condense (as steam) to provide a pressure decrease in case of accident. For an HTR, a confinement (whatever the functions are) is thus more useful than a pressure resistant containment. The resulting vent opening pressure is also a key point to be determined.
- The approach has to be coherent for the regulator and for the public acceptance. The fact that on one side, the 5 levels of protection are systematically verified and on the other side, the HTR concept is pretended as inherently safe, could lead to a contradiction feeling.

As a summary, the following have been systematically proposed to be top safety concerns to be sanctioned as applicable regulatory oversight criteria:

- Highly reliable and less complex shutdown and decay heat removal systems. The use of inherent or passive means to accomplish this objective is encouraged (negative temperature coefficient, natural circulation, etc.).
- Longer time constants and sufficient instrumentation to allow for more diagnosis and management before reaching safety systems challenge and/or exposure of vital equipment to adverse conditions.
- Simplified safety systems that, where possible, reduce required operator actions, equipment subjected to severe environmental conditions, and components needed for maintaining safe shutdown conditions. Such simplified systems should facilitate operator comprehension, reliable system function, and more straightforward engineering analysis.

- Designs that minimize the potential for SAs and their consequences by providing sufficient inherent safety, reliability, redundancy, diversity, and independence in safety systems, with an emphasis on minimizing the potential for accidents over minimizing the consequences of such accidents.
- Designs that provide reliable equipment in the balance of plant (BOP) (or safety-system independence from BOP) to reduce the number of challenges to safety systems.
- Designs that provide easily maintainable equipment and components.
- Designs that reduce potential radiation exposures to plant personnel.
- Designs that incorporate the defense-in-depth philosophy by maintaining multiple barriers against radiation release, and by reducing the potential for, and consequences of, SAs.
- Design features that can be proven by citation of existing technology, or that can be satisfactorily established by commitment to a suitable technology development program.
- Designs that include considerations for safety and security requirements together in the design process such that security issues (e.g., newly identified threats of terrorist attacks) can be effectively resolved through facility design and engineered security features, and formulation of mitigation measures, with reduced reliance on human actions.
- Designs with features to prevent a simultaneous loss of containment integrity (including situations where the containment is by-passed), and the ability to maintain core cooling as a result of an aircraft impact, or identification of system designs that would provide inherent delay in radiological releases (if prevention of release is not possible).
- Designs with features to prevent loss of spent fuel pool integrity as a result of an aircraft impact.
- Designs with features to eliminate or reduce the potential theft of nuclear materials.
- Designs that emphasize passive barriers to potential theft of nuclear materials.

3.1 Definition of Safety Boundaries

In regards to licensing and regulatory oversight, there is a need of defining a boundary between the Nuclear Heat Supply System (NHSS) and the Balance Of Plant (BOP), which includes the Secondary Heat Transfer System (SHTS), the Process Heat Plant (PHP), the Power Conversion System (PCS). The questions herein are,

- Which parts or functions of the SHTS, PHP, PCS impact NHSS nuclear safety and classification against nuclear safety grade standards?
- Which are within the regulatory oversight of any other regulatory agencies?

Interface requirements between the safety-related and non-safety-related portions of the plant will need to be established. The objective would be to create a boundary between portions of the plant which would be subject to regulatory oversight by the respective nuclear organism and the remainder of the plant. The figure below shows a conceptual boundary between safety-related structures, systems, and components (SSCs) of primary interest and the remainder of the plant (see Figure 3.1-1).

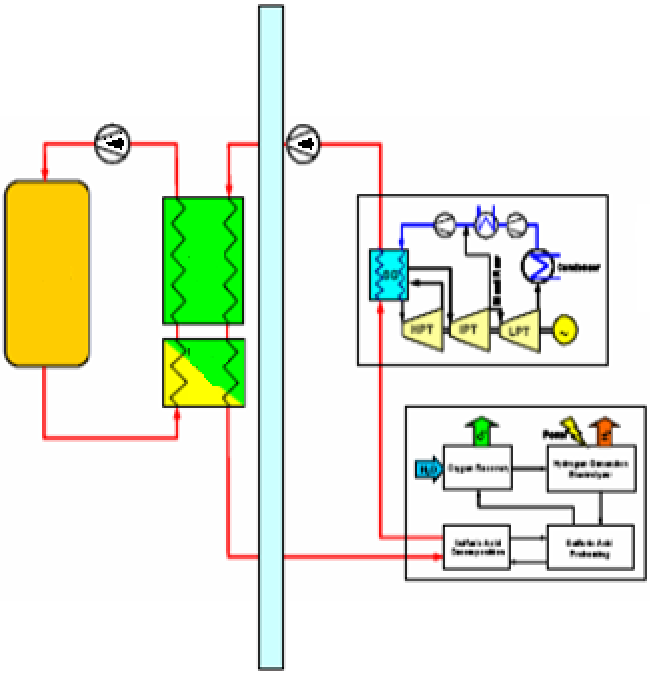


Figure 3.1-1 Regulatory Boundary

A PRA approach to the design and safety analysis process to provide assurance that safety-related SSCs and their functions are properly identified has been stressed by EUR.

SSCs are classified as either safety-related or non-safety-related, where safety-related means they have special treatment requirements to assure their accident mitigation capability and their accident prevention reliability, but not necessarily always does that correspond to a fully ASME Section III design; this in fact depends strongly on how the plant PRA is constructed, the design concept (fully passive, mixed, fully active), costs, and the degree of diversity imposed by the regulators. “Non-safety-related” traditionally means that those SSCs can be designed using non-nuclear conventional methods.

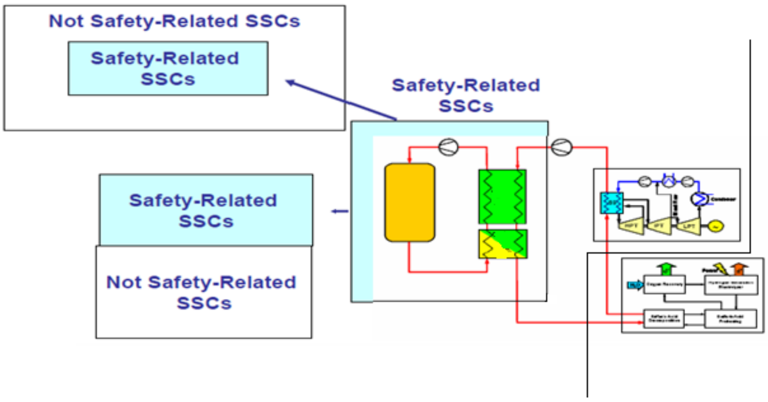


Figure 3.1-2 Classification

Examples of traditional non-safety-related designs that impact safety include, but are not limited to, fire protection, security features, Radwaste systems, and electrical power systems. The industrial portions of the plant, however, will be subject to only the standard regulatory oversight for the industrial application linked to the NHSS.

In summary, there should be a clear demarcation among:

- The safety-related SSCs,
- Non-safety-related SSCs that have a function supportive of safety or whose failure could impact safety and,
- SSCs in the non-safety-related portion of the plant.

There is another impact from coupled processes, which relies on the identification of potential “cross over” regulations related to the control of both plants from a single control room, remote shutdown capability for the non-safety-related portions of the plant, protection of nuclear plant personnel from specific external hazards coming from the non-safety-related portions of the plant, and indeed the limitations to radioactive release.