SAFETY DESIGN IMPLEMENTATION FOR THE INTERNATIONAL THERMONUCLEAR EXPERIMENTAL REACTOR

C.W. Gordon, A.E. Poucet, G. Saji
ITER Joint Central Team
ITER San Diego Joint Work Site, 11025 North Torrey Pines Road
La Jolla, California, 92037 USA

SUMMARY

A high level of safety is being integrated into the ITER design. This paper describes some of the steps being followed in the facility, system and component design to ensure safety. The safety approach developed for ITER takes into account the moderate hazard associated with ITER, its role as an experimental facility, and draws on experience in nuclear and non-nuclear industries. A key element is a graded approach to match requirements to hazards being controlled. This is reflected in, for example, dose limits that are lower for higher frequencies, classification of components in terms of their importance to safety in order to guide the setting of requirements, and structural design. The classification system that ITER is developing for safety-relevant components is described. The implementation of this classification into the design is still very much under development, but preliminary thoughts are outlined here.

Processes are in place to determine safety functions needed to ensure public safety, to identify systems that fulfill these safety functions, to set system requirements to ensure these functions are implemented in the design, to design system components to meet requirements, and to identify design, manufacture and operations requirements needed.

At this stage of the project, it is concluded that the design and operation could meet the safety-related requirements of any of the potential host countries with only minimal modifications to accommodate the characteristics of the specific site chosen.

INTRODUCTION

The ITER Project includes a vigorous design and assessment activity to ensure the safety and environmental attractiveness of ITER. It also ensures that ITER can be sited in any of the sponsoring Parties with a minimum of site-specific redesign. In this activity, detailed safety-related design requirements have been established based on internationally recognized safety criteria and limits, and ongoing assessments have been made to evaluate the success in implementation of these in the facility, system, and component designs.

A comprehensive safety and environmental assessment has recently been completed for the ITER Detailed Design (1). This assessment has shown that the ITER design has successfully met all of the safety-related requirements that were established. This assessment further demonstrates that the safety issues involved in construction and operation of ITER are adequately known and characterized, and that design solutions are being implemented to successfully deal with these issues.

This paper describes some of the steps being followed in the facility, system and component design to ensure safety. First, the safety characteristics of ITER are described. This sets the stage for the safety requirements imposed on the design for the protection of the public. Next, the safety functions which have been identified for the protection of the public and their implementation in the design are briefly described. Safety analysis carried out during the EDA phase is one where "classical deterministic" safety analysis is complemented with probabilistic assessments (2). The results of this analysis identifies the systems and components that have a safety role and their performance requirements. The high level acceptance criteria (dose/release limits) used in this analysis are discussed next. The classification system that ITER is developing for safety-relevant components is then described. The implementation of this classification into the design is still very much under development, but preliminary thoughts are outlined here. Structural integrity plays a crucial role for machine operability, fault prevention and accident mitigation, and the integration of safety into structural design is described.

SAFETY DESIGN CHARACTERISTICS OF ITER

Fusion has built-in safety characteristics without depending on layers of "safety protection systems". Safety considerations are integrated in the design by making use of the intrinsic safety characteristics of fusion adequate to the moderate hazard inventories.

Magnetic fusion has basic favorable safety characteristics (3, 4, 5) including:

- In a fusion reactor, the reaction is self-limiting. The conditions for maintaining an ignited plasma are so stringent that off-normal events will generally terminate the reaction. The total amount of fuel in the plasma is only a few tenths of a gram and the plasma cannot remain ignited for longer than a few seconds without fueling.

- Fusion power has a moderate energy density compared with other power sources used in power plants. Radioactive decay heat densities are moderate. Fast acting emergency cooling systems are not required to maintain adequate cooling of activated structures. The time scales are such that there is ample time to intervene even in the hypothetical case that all cooling would be lost. Gross structural melting is not possible.

- The ultimate performance of confinement barriers that needs to be assured in accidents is modest; about one or two orders of magnitude reduction for tritium and mobilizable metallic dust for ITER.

- The products of the D-T reaction to be used in ITER are helium and a neutron. Radioactive activation products are produced by the interaction of the fusion neutrons with structural materials surrounding the plasma; however, the quantity and half-lives of these products are determined by the choice of materials used in the near-plasma materials and, thus, to some extent are under control of the designer.

- After about a hundred years, radiotoxicity indices (relating to ingestion and inhalation) fall to levels comparable with the ashes from coal-fired power plants for the total activated materials from a fusion power reactor with the same total electrical power generated (6).

The tokamak has a number of features that need consideration in the safety design:

- Energy sources associated with the magnetic field, decay heat, the plasma, pressurized coolants, and potential accidental chemical reactions are present.

- A low tritium burn-up fraction (approximately two percent) leads to circulating tritium inventories of the order of hundreds of grams.

- Tritium from the plasma is implanted in, or co-deposited with carbon/beryllium on the plasma facing components leading to an in-vessel tritium inventory that could potentially be released under accident conditions. Implanted tritium can also diffuse through higher temperature structures leading to contamination of heat transfer coolant.

- Neutrons produced by fusion reactions lead to activation of structures that in turn leads to: dust produced by plasma-surface interactions being radioactive, corrosion products in some heat transfer systems being radioactive, and a residual heat production after plasma termination from radioactive decay.

- The loss of charged particles from the plasma creates high heat-loads on some components (like the divertor). Because of the heat load on such components, rapid shutdown (order of seconds) is necessary to prevent damage to these components in case of anomalies in the heat removal. Shutdown may be accompanied by plasma disruptions or vertical displacement events that can induce mechanical loads on near-plasma structures.

- Hazards to site personnel, including: radiation, electro-magnetic fields, hazardous materials (e.g. beryllium), high voltages, cryogens, etc.

ITER will be a research facility. The experimental nature of ITER requires a design that permits uncertainties and flexibility of plasma operation, facilitates experimentation and accommodates changes. These needs drive the safety design to provide robust safety envelopes and to minimize the safety role and influence of plasma operations and experimental components.

ITER is also an international project designed to be siteable in any of the four participating Parties (United States, Europe, Russian Federation and Japan). This has meant developing safety design and analysis criteria and approaches which, while not matching any particular Party's approach, would permit regulatory approval without significant design changes.

SAFETY FUNCTIONS AND THEIR IMPLEMENTATION

Safety-related requirements have been integrated into the overall design requirements for the facility, systems and components. The design incorporates the well-established concepts of Defense-in-Depth and multiple lines of defense to attain high confidence in the reliability of critical safety features of the facility and ensure protection against postulated accidents. Specific safety functions (Table 1) for ensuring public safety have been integrated into the design by taking advantage of the normal systems needed for operation and the inherent safety features of fusion, with a minimum of standby engineered safety features required. Thus, the majority of components are those necessary in a tokamak; only a few components have been added only to meet safety requirements.

Limit Radioactive Inventories

Design limits are set for radioactive inventories for use in safety analyses. Control measures are provided in the design to ensure these limits can be met in operation. These include: monitoring and periodic measurements, methods to reduce inventory (such as periodic cleaning to remove dust and co-deposited tritium, or on-line coolant purification and detritiation), and isolation of inventories in the event of an accident.

Table 1
Safety Functions for Public Safety

Safety Function	Implementation
Limit radioactive inventories	-isolation to separate inventories -monitoring and procedures for periodic in-vessel inventory reduction
Provide confinement barriers	-first barrier -second barrier -exhaust drying, atmosphere detritiation, filtration, where required -ventilation + stack, where required -isolation to limit releases, where required
Ensure heat removal	-heat transfer and heat sink
Control hydrogen inventories and chemical reactions	-prevent hydrogen/air mixtures -limit inventory of chemically reactive materials -ensure heat removal to reduce reaction rates -provide off-normal fusion power shutdown -hydrogen recombination or removal
Control effects of magnetic energy	-structural support/resistance to deformations -monitoring -fast discharge of coils
Control the effects of coolant energy	-pressure suppression -containment -overpressure relief
Monitoring	-of safety functions -of effluents and releases to the environment -of radiation fields on-site
Support services to systems providing safety functions	-electrical power -instrument air -service water

Provide Confinement Barriers

There are a number of different radioactive inventories in ITER all of which require some form of confinement. A graded, multiple confinement barrier approach is used. Every radioactive inventory is contained in its vessel, process piping, component, etc. which serves as the first confinement barrier. The main function of the second confinement barrier is to prevent the spread of radioactive materials following a fault of the first confinement barrier. The two main requirements for the second confinement barriers are to:

- Meet project dose/release limits in the event of failure of the first barrier; and
- Maximize structural and spatial separation and independence from the first confinement barrier to prevent a common failure mode.

For example in the ITER tritium plant, primary vacuum pumping system and fueling systems, double-walled process piping or single-walled piping within gloveboxes or enclosures constitutes

the first and second barriers. The primary heat transfer systems' piping forms the first barrier for contained fluids, and the heat transfer systems are enclosed in vaults (the second barrier). Additional lines of defense for confinement in the vaults are a heat removal system that can reduce pressure following an accident, a dryer which can remove HTO, and filters to remove particulate.

Figure 1 illustrates the confinement barriers surrounding the tokamak. The vacuum vessel, its ducts, its penetrations and the in-vessel components' primary heat transfer systems are the first confinement barrier for the tritium and activation products inside the tokamak. The heat transfer system vaults, the cryostat and its penetrations, and heat transfer system guardpipes outside of the cryostat form the second confinement barrier. The upper and lower vaults are connected and are sized such that they can accommodate the pressurization from an ex-vessel loss of coolant accident in any one of the ex-vessel coolant loops. Both barriers are designed to be highly reliable to confine the tritium and tokamak dust inside the tokamak. Using the vacuum vessel and cryostat vessel takes advantage of the inherent magnetic fusion characteristic that high quality and high reliability vacuum vessels are needed for fusion operation; failures and leakages automatically (passively) terminate operation.

Ensure Heat Removal

During normal operation, plasma heat is removed from in-vessel components by 10 loops of the primary first wall/in-board baffle primary heat transfer system, 4 loops of the limiter/out-board baffle primary heat transfer system, and the 2 loops of the vacuum vessel primary heat transfer system.

After the plasma is shut down, decay heat from neutron activation must be removed. Decay heat is estimated to be [2] 38 MW at shutdown declining to [2] 1.9 MW after one day. There are no dedicated decay heat removal systems; instead ITER uses its many normal operation cooling systems to remove decay heat. Figure 2 shows a schematic of the ITER heat transfer systems. Since the amount of decay heat to be removed is only a small fraction of the nuclear heat load during a plasma pulse, in the current design, most loops employ an auxiliary, small pump of approximately 10% of full flow throughput, to remove decay heat from the in-vessel components. These pumps are connected to Class 3 emergency power from standby diesel generators to protect them from loss of site power. Since coolant flow stoppage of the heat rejection system leads to the loss of the heat sink, three units of small pumps, also connected to Class 3 emergency power, are included in the heat rejection system design. Most of the safety burden is on the vacuum vessel cooling system which has a natural circulation capability and is divided into two fully independent loops. Initially, the in-vessel components cool off as the plasma heat load is removed.

Control Hydrogen Inventories and Chemical Reactions

The following potential chemical reactions exist in ITER:

- Hydrogen inventories in process systems;

- Beryllium/Carbon/Tungsten - steam/air reactions inside the vacuum vessel at elevated temperatures; and
- Ozone formation in liquid/frozen air or low purity nitrogen in a radiation field.

In the case of systems containing hydrogen, the basic hydrogen safety design principles are:

- Prevent leakage of hydrogen isotopes (also required for radioactive material confinement as well);
- Eliminate the formation of hydrogen/air mixtures by use of inert or vacuum second confinement (also required for radioactive material confinement as well);
- Prevent the formation of an flammable hydrogen/air mixture in rooms by adequate ventilation; and
- Eliminate ignition sources.

Control of hydrogen generated by potential in-vessel chemical reaction consists of:

- Ensure heat removal to reduce temperatures and hence reduce reaction rates;
- Provide off-normal fusion power shutdown to terminate the heat load to in-vessel components in the event of an upset in their heat transfer systems to prevent heat up to high temperatures and subsequent in-vessel coolant leakages; and
- Limit the quantities of chemically reactive dust in vessel.

Control Effects of Magnetic Energy

The magnet system is designed, built and operated so that credible magnet system failures which could occur under normal or abnormal conditions cannot cause damage to confinement barriers that would result in a release of radioactivity exceeding the specified release limits. The primary function of the magnet system in not safety related but is to provide the toroidal and poloidal magnetic fields necessary to initiate, contain and control the plasma during the various phases of machine operation. However, the magnets use large currents and as a result they contain large amounts of electro-magnetic energy and are subjected to electromagnetic loads.

The first level of the defense in depth is at the design stage. The plant layout separates the electrical power of the coils from nuclear safety important components to the extent practical and provides robust magnet structures to limit off-normal movement, contain pressure, or act as thermal barriers. The second level in the defense in depth is to employ frequent monitoring of displacement, cryogen leaks and insulation quality while the magnets are still cold to discover any developing failure before it has the opportunity to grow to the point it could constitute an unsafe situation. In the third level, the magnet system includes active and passive protection systems to prevent damage that would impact machine availability and reduce the probability of many potential magnet faults to a very low level. These include insulation, barriers, grounding schemes, current limitation, quench detection and coil discharge systems.

Control the Effects of Coolant Energy

Confinement barriers can accommodate accident pressures. For example, the vacuum vessel and associated parts of the first confinement barrier are designed for 500 kPa (abs) internal pressure following an in-vessel coolant leakage, but the vacuum vessel structure required for electromagnetic forces requires no additional strength for this accident load. The cryostat is designed for and internal pressure of 200 kPa (abs), but the structure required for internal vacuum loads requires no additional strength for this accident load.
In the current design, the heat transfer system vaults are designed for an internal accident pressure of 240 kPa (abs). The ex-vessel primary heat transfer systems' piping is surrounded by guard pipes or within a heat transfer system vault. Water and steam released in the event of an accident are routed to the vaults away from other sources of radioactivity.

Two pressure relief systems are provided to deal with accidental overpressure:

- Vacuum vessel pressure suppression system;
- Cryostat pressure relief.

The vacuum vessel is connected to a pressure suppression system by ducts with rupture disks. There are also bleed valves that permit connection at pressures below the rupture disk setpoint. Steam from an in-vessel coolant leak would be condensed in the large tanks of water. The cryostat pressure relief system is intended to deal with potential cryogenic helium leaks in the cryostat. Since there would be no radioactivity present in such events, further confinement is not needed except to protect personnel from cryogen related hazards. In the heat transfer system vaults, coolers are provided to return the vault pressure to sub-atmospheric in the event of a steam discharge.

Monitoring

An essential aspect of the design is the provision of features to permit the monitoring of systems, providing a safety function to ensure that these systems are available and capable of fulfilling their function on demand. This is accomplished through a combination of testing, on-line monitoring and inspection. Also under consideration is a safety parameters display system for the operators.

Support Services to Systems Providing Safety Functions

Systems that provide safety functions may need support services in order for them to function (such as cooling, lubrication, electrical power, etc.). These support services need to be designed and operated such that the intended safety function will be fulfilled when required.

ITER PROJECT RELEASE LIMITS

A general project safety objective is that the ITER site personnel and the public shall be protected such that the risks to which they are exposed as a result of ITER operation shall be maintained as low as reasonably achievable (ALARA). A further general safety principle is that

the ITER design, construction, operation and decommissioning shall meet technology-independent radiation dose and radioactivity release limits for the public and site personnel. In addition, ITER project policy is to provide a conservative level of protection such that ITER can be sited by any of the Four Parties with minimum modification to accommodate site specific requirements.

Conservative release limits for tritium and activation products are based on internationally accepted dose limits from the recommendations by the International Commission on Radiological Protection (ICRP) and the International Atomic Energy Agency (IAEA). Prior to site selection, a set of radiation criteria has been adopted for the design. These criteria and their derivation are described in the General Safety and Environmental Design Criteria (7). The overall project defined safety goal for ITER is expressed in terms of dose and effluent/release limits for a set of event categories defined on the basis of their expected annual occurrence. These limits reflect the principle that accidents with higher consequences should have lower frequencies and that these consequences should be bounded. An example for tritium release limits is shown in Table 2.

ITER uses a classification of plant conditions which divides plant conditions into categories in accordance with anticipated frequency of occurrence. The categories are as follows:

Category I:	Operational events
Category II:	Likely sequences
Category III:	Unlikely sequences
Category IV:	Extremely unlikely sequences
Category V:	Hypothetical events

Category I events and plant conditions are those planned and required for normal operation, including some faults and events which can occur as a result of the experimental nature of ITER. Category II events are not planned but are likely to occur one or more times during the life of the plant but do not include Category I (normal operations) events. Category III event sequences are not likely to occur during the life of the plant (typical frequency 10^{-2}/a to 10^{-4}/a). Category IV event sequences are not likely to occur during the life of the plant with a very large margin (typical frequency 10^{-4}/a to 10^{-6}/a). Category V sequences which typically have a frequency below about 10^{-6}/a are postulated to limit the associated risk.

Table 2
Project Release Limits for Tritium (HTO)

	I	II	III	IV
EVENT SEQUENCE CATEGORY	**OPERATIONAL EVENTS**	**LIKELY SEQUENCES**	**UNLIKELY SEQUENCES**	**EXTREMELY UNLIKELY SEQUENCES**

Category Description	Events and plant conditions planned and required for ITER normal operation, including some faults and events which can occur as a result of the ITER experimental nature.	Event sequences not planned but likely to occur one or more times during the life of the plant but not including Category I events.	Event sequences not likely to occur during the life of the plant.	Event sequences not likely to occur during the life of the plant with a very large margin; limiting events for "design basis" (a)
Typical Annual Expected Frequency	list of operational events to be defined explicitly	$f > \sim 10^{-2}/a$	$10^{-2}/a > f > 10^{-4}/a$	$10^{-4}/a > f > 10^{-6}/a$
Release Limit for HTO (tritiated water)	1 g-T/a	1 g-T/event (1 g-T/a integrated over all Category II events)	50 g-T/event	100 g-T/event

Various events are postulated to ensure that sufficient means are provided to prevent unacceptable releases of hazardous materials. These postulated initiating events and sequences of subsequent failures are categorized for the purpose of assessment depending upon frequency or likelihood of occurrence, and their consequences are evaluated and compared with safety objectives set for the category.

SAFETY IMPORTANCE CLASSIFICATION: BACKGROUND AND DEFINITIONS

The ITER safety importance classification scheme implements a graded approach that gives consideration to both the magnitude of the consequences of loss of safety function and the likelihood that such safety function is required (i.e., the probability that the plant would be in a condition in which the safety function is required). It is used to indicate the importance to the overall plant safety of physical items like structures, systems or components.

The Safety Importance Classification scheme consists of four classes. The assignment of a particular class to an item is based on analysis of the safety functions assigned to the item and how the loss of the item impacts upon the performance of these functions or upon the performance of safety functions associated with other items (propagation of failure). Items that provide a safety function or that can affect the performance of a safety function are, in descending order, classified into Class 1, 2 or 3. Items that do not have any safety function and whose failure does not affect any safety function of another item are classified into Class 4 (non-safety).

Detailed rules have been formulated for the assignment of Safety Importance Classification as shown in Table 3. An item is classified into SIC 1 if its failure would "directly" lead to releases in excess of Category IV limits. It is a project position that has been met in the design that there

will be no SIC 1 components in ITER. An SIC 2 component is one that's failure would lead to releases in excess of Category IV limits only if it occurred in conjunction with some other unlikely (Category III) or extremely unlikely (Category IV) event. Those items in SIC 3 cover other items implementing safety functions or if their failure would worsen an accident condition or degrade an SIC 2 item.

SAFETY IMPORTANCE CLASSIFICATION IMPLEMENTATION

The project will have to justify to the regulator that components that have a safety function are designed and operated in such a way that this safety function is available when needed. The Safety Importance Classification system is a basis for deciding whether or not a component has a safety function and how important that function is. Requirements related to Safety Importance Classification are a means to help in the justification that the safety function can be performed as intended. As a consequence such requirements address a set of precautions that need to be taken in design, installation, testing, and operation of safety-related components that would allow us to take credit from these components in safety analysis (see for example (8)) and provide sufficient proof to the regulator that these components would perform as intended. The implementation of Safety Importance Classifications (and Quality Assurance Classifications) into the design and operation requirements is still very much under development at this stage of the ITER EDA, and the following presents some preliminary thoughts.

Table 3
Safety Importance Classification

Safety Importance Class	Classification Rules
SIC-1	Components are classified in SIC-1 if the following rule applies: **Rule 1:** The component implements a safety function that is needed in normal operation or after occurrence of Category II (Likely) events and the failure of that safety function under such conditions leads to a release that exceeds the Category IV (Extremely Unlikely) limits. (A design objective is to have no SIC-1 components in ITER.)
SIC-2	Components are classified in SIC-2 if any of the following three rules apply: **Rule 1:** The component implements a safety function that is needed after occurrence of Category III (Unlikely) or Category IV (Extremely Unlikely) events and the failure of that safety function under such conditions leads to a release that exceeds the Category IV (Extremely Unlikely) limits. If the same safety function can be accomplished by another independent system, different from the one the component belongs to, then the component may be declassified to SIC-3. **Rule 2:** • The component is needed to provide an elevated (stack) release point for releases that can exceed 1/10th of the Category IV (Extremely Unlikely) limits. **Rule 3:** • The failure of the component would degrade a safety function of a SIC-1 component..
SIC-3	Components are classified in SIC-3 if any of the following four rules apply: **Rule 1:** • The component implements a safety function whose failure could lead to a release that exceeds the Category II (Likely) limits but is lower than the Category IV (Extremely Unlikely) limits. **Rule 2:** • The failure of the component would degrade a safety function of a SIC-2 component. **Rule 3:** • The component implements a safety function needed to protect the facility personnel from radiological or toxicological hazards. **Rule 4:** • The component is needed for radiological monitoring of releases when they exceed the Category II limits (accident monitoring).
SIC-4	Not safety classified

The gradation that is built into the Safety Importance Classification system is reflected in the degree of burden of proof required: e.g. for SIC 1 components the burden of proof will be heavier than for SIC-3 components. As a general statement, and in order to provide some guidance, we might say that SIC-1 items would be expected to carry a very heavy burden of proof, e.g. as provided by nuclear design and QA codes (e.g. ASME section III class 2 or IEEE class 1E) whereas for SIC-3 items good industrial practice and positive operational experience with perhaps some additional QA would provide sufficient proof.

The concepts of "graded approach", safety classification, and related graded design and QA requirements are now being used in a number of industries, but extrapolation to ITER is not always straightforward, and it is not easy to extract general requirements to be associated with different safety classes. To investigate the consequences of safety classification, existing standards (9, 10, 11, 12, 13) have been reviewed, and some general points that seem to emerge from have been extracted and placed in an ITER context in Table 4.

Table 4
Preliminary thoughts on Implementation of Safety Importance Classification

Issue	SIC-2	SIC-3
Code	If an appropriate design code exists, the code requirements for design, construction, testing etc. need to be followed. Deviations from these requirements need to be negotiated. As a baseline for structural components it is proposed to use ASME VIII and related codes (13) for both SIC 2 and 3 items.	
QA requirements	Quality Assurance will be requested for any safety related item. The QA requirements will be graded with SIC. The ITER QA plan will address this issue. As a guideline the IAEA graded requirements (14) can be consulted.	
	IAEA Level II	IAEA Level III (maybe Level II for innovative items)
Environmental qualification	Justification must be provided that SIC 2 and SIC 3 items can withstand the abnormal environmental conditions that may arise from an accident where they are required to function. The degree of burden of proof (e.g. for testing) will vary from SIC-2 to SIC-3.	
Reliability	Reliability targets may be part of the performance specification of the safety related items. The following requirements provide proof that these targets can be met by the design.	
	Use of a systematic fault analysis method with extensive coverage (e.g. FMEA) to assess malfunctions Prove that the design can meet the reliability target using a formal method (e.g. fault tree) or can at least cope with a single active fault	Less formal methods Use of good industrial quality components may suffice as a justification
Independence, physical separation	Some justification needs to be provided that the safety functions cannot be undermined by underlying common cause failures or cascade failures.	
	In principle SIC-2 I&C should be separate and functionally isolated from normal instrumentation (separate signal channels appropriately de coupled and shielded), and with physical separation between redundant channels	No need to have separate I&C. Can use systems used in normal operation.
Inspections and tests	In-service inspections and tests may be required to demonstrate that the equipment can continue to provide its safety functions with an acceptable level of reliability. Such inspections and tests need to be commensurate with the reliability requirements. The level of administration (test records, calibration records, personnel training requirements) involved may vary from SIC-2 (more formal) to SIC-3 (less formal).	
Equipment data trail (during operation)	• Equipment "pedigree" must be established" indicating the equipment operational history • Inspection status must be indicated (tag or inspection record)	Normal maintenance logbooks may be sufficient
Equipment outage	Maintenance and other outages of both SIC-2 and 3 equipment must be covered by operating procedures and a set of "limiting conditions for operation" must be determined such that reliability requirements can be met	
Response and recovery after malfunction	Covered by a plant procedure. Principles for resuming operation need to be approved by regulator (e.g. limiting conditions for operation) No need to actually wait for green light	
Reporting of malfunctions	Malfunctions impeding safety function need to be reported to regulator	Annual logbook that may be inspected by regulator

Modification of equipment and retrofit	• Impact on safety functions needs to be analyzed • Changes need to be notified and agreed by regulator	Impact on safety functions needs to be analyzed

The requirements associated with the SIC basically address the burden of proof requested to justify that these performance and reliability requirements can be met by the design and can be maintained over the life-time of ITER.

STRUCTURAL DESIGN

Events and event combinations that need to be taken into account in the component design are identified and categorized by frequency and the Safety Importance Classification, and performance requirements determined on the basis of preliminary plant-level safety analysis. This is used by the component designer to set number of cycles for fatigue analysis and acceptable damage limits. The designer then develops the component loading conditions and selects the appropriate structural design codes and standards. Detailed design results are fed back into the design and safety analysis. This is illustrated in Figure 3.

A graded approach is applied in structural design similar to that used in ASME Section III (11) or RCC-MR (8) where less allowable damage permitted for more frequent events. Table 5 provide the damage limits at the plant and component level being applied in the ITER EDA design.
Structural design is generally performed in accordance with recognized structural codes or standards applicable to the component (e.g., ASME Section VIII). However, in some cases the conditions are outside the range of applicability of generally accepted codes. Two key cases are the in-vessel components and superconducting magnets where ITER has developed structural design criteria to be applied.

CONCLUSIONS

Processes are in place to determine safety functions needed to ensure public safety, to identify systems that fulfill these safety functions, to set system requirements to ensure these functions are implemented in the design, to design system components to meet requirements, to identify design, manufacture and operations requirements needed.

At this stage of the project, it is concluded that the design and operation could meet the safety-related requirements of any of the potential host countries with only minimal modifications to accommodate the characteristics of the specific site chosen.

Table 5
Damage Limits in Plant and Component Level

Damage Limits	Damage Limits to Component Level	Damage Limits in Plant Level and Recovery of the Plant (Plant Operational Condition)
Normal	The component should maintain specified service function.	• Within specified operational limit. • No special inspection will be required other than routine maintenance and minor adjustment.
Upset	The component must withstand these loading without significant damage requiring special inspection or repair.	• After minor adjustment, or replacement of the faulty component, the plant can be brought back to normal operation. • No effect on other components that may call for special inspection or repair.
Emergency	• Large deformations in areas of structural discontinuity, such as at nozzles, which may necessitate removal of the component from service for inspection or repair. • Insignificant general permanent deformation that may affect safety function of the component concerned. General strains should be within elastic limits. • Active components should be functional at least after transient.	• The plant may require decontamination, major replacement of damaged component or major repair work. • In addition to the damaged component, inspection may reveal localized large deformation in other components, which may call for repair of the affected components. • Nevertheless the plant maintains the specified minimum safety function during and after the events.
Faulted	• Gross general deformations with some consequent loss of dimensional stability and damage requiring repair, which may require removal of component from service. • Nevertheless deformation should not lead to structural collapse which could damage other components. • The fluid boundary maintains degraded but reasonable leak tightness and flow passage. • Active components may not be functional after transient.	• Gross damage to the affected system or component. No loss of safety function which could lead to doses in excess of the limits established for Category IV Extremely Unlikely Event. • No design consideration will be given for recovery. The recovery of the plant may be judged from severity of damage. • This level of accidental state is not expected to occur, but are postulated because their consequences would include the potential for the release of significant amounts of radioactive material.

REFERENCES

(1) "Technical Basis for the ITER Detailed Design Report", to be published, ITER EDA Documentation Series, IAEA, Vienna.

(2) POUCET, A.E., and S. J. PIET, "Safety Analysis and Design Framework in ITER", Probabilistic Safety Assessment International Topical Meeting, September 29-October 3, 1996, Park City, Utah, USA.

(3) SHIMOMURA, Y., and G. SAJI, "ITER Safety and Operational Scenario", International Symposium on Fusion Nuclear Technology, April 7-11, 1997, Tokyo, Japan.

(4) SAJI, G., et al, "Safety and Environmental Activities for ITER", 6th Technical Meeting on Developments in Fusion Safety, Naka, Japan, October 1996.

(5) SHIMOMURA, Y., et al, "Safety Characteristics of ITER", 16th IAEA Fusion Energy Conference, Montreal, Canada, 7-11 October 1996.

(6) RAEDER, J. et al. "Safety and Environmental Assessment of Fusion Power (SEAFP)", EURFUBRU - XII-217/95, June 1995.

(7) Technical Basis for the ITER Interim Design Report, Cost Review and Safety Analysis, ITER EDA Documentation Series No. 7, IAEA, Vienna, 1996.

(8) "Règles applicables aux procédés des centrales nucléaires à eau légères sous pression de 1400 MWe", EDF-FRAMATOME RCC-P 1400, rev. 1, 1991.

(9) "Design and construction rules for mechanical components of FBR nuclear islands", RCC-MR, Section 1, Subsection A: General, AFCEN June 1985.

(10) IEEE, "Standard criteria for safety systems for nuclear power generating stations", IEEE Std 603-1980, The Institute of Electrical and Electronics Engineers Inc., 1980.

(11) ASME Boiler and Pressure Vessel Code, Section III, Subsection NCA, General requirements for Division 1 and Division 2, ACI-ASME Joint Technical Committee, July 1992.

(12) IEC, "Functional Safety: Safety-related systems", IEC-1508, Draft standard of the International Electrical Committee

(13) ASME Boiler and Pressure Vessel Code, Section XI, Rules for inspection of nuclear power plant components, ACI-ASME Joint Technical Committee, July 1992.

(14) IAEA, "Grading of Quality Assurance requirements, A Manual", Technical Report Series No. 328, IAEA Vienna, 1991.

Tokamak elevation view, showing 1st & 2nd confinement barriers

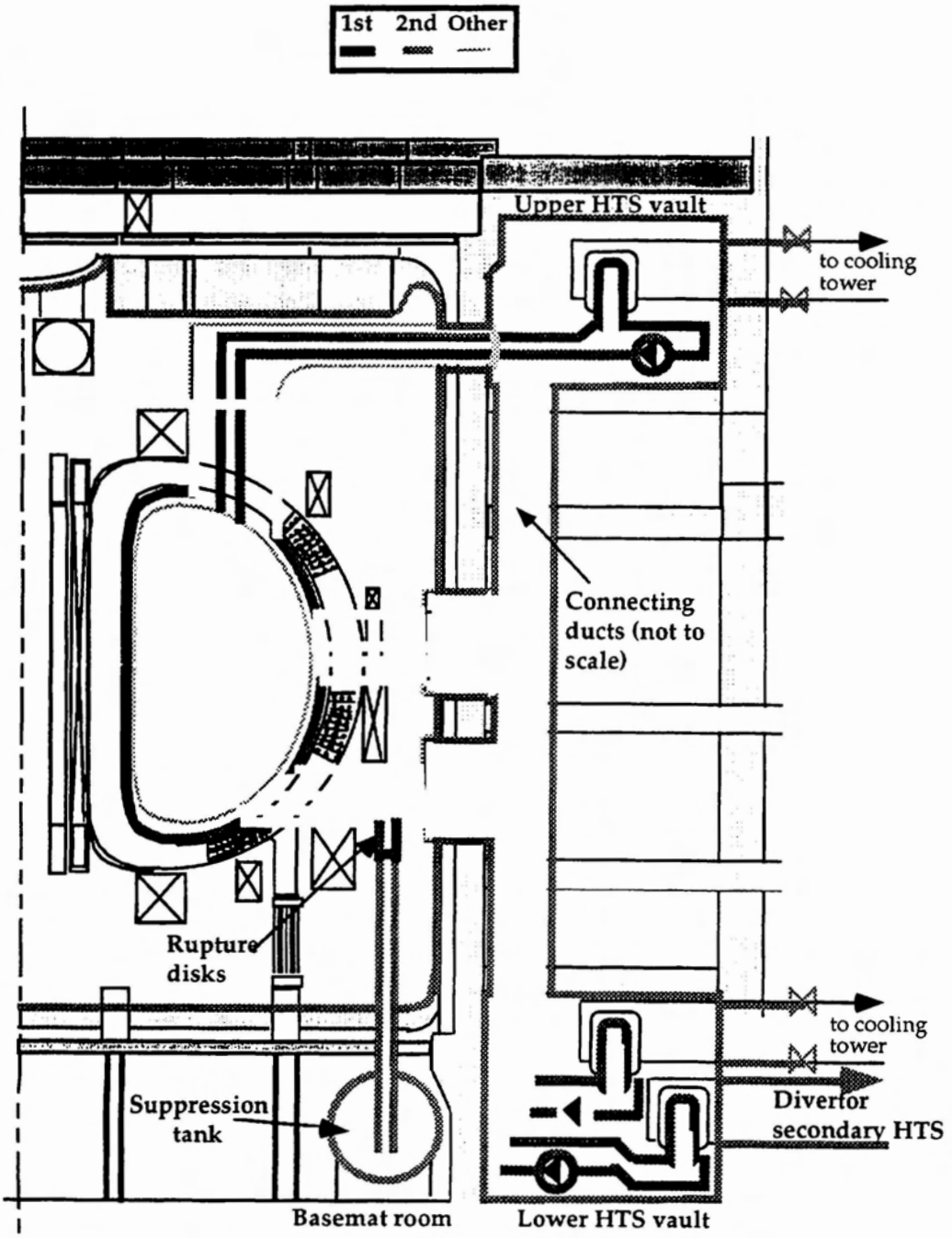

Figure 1

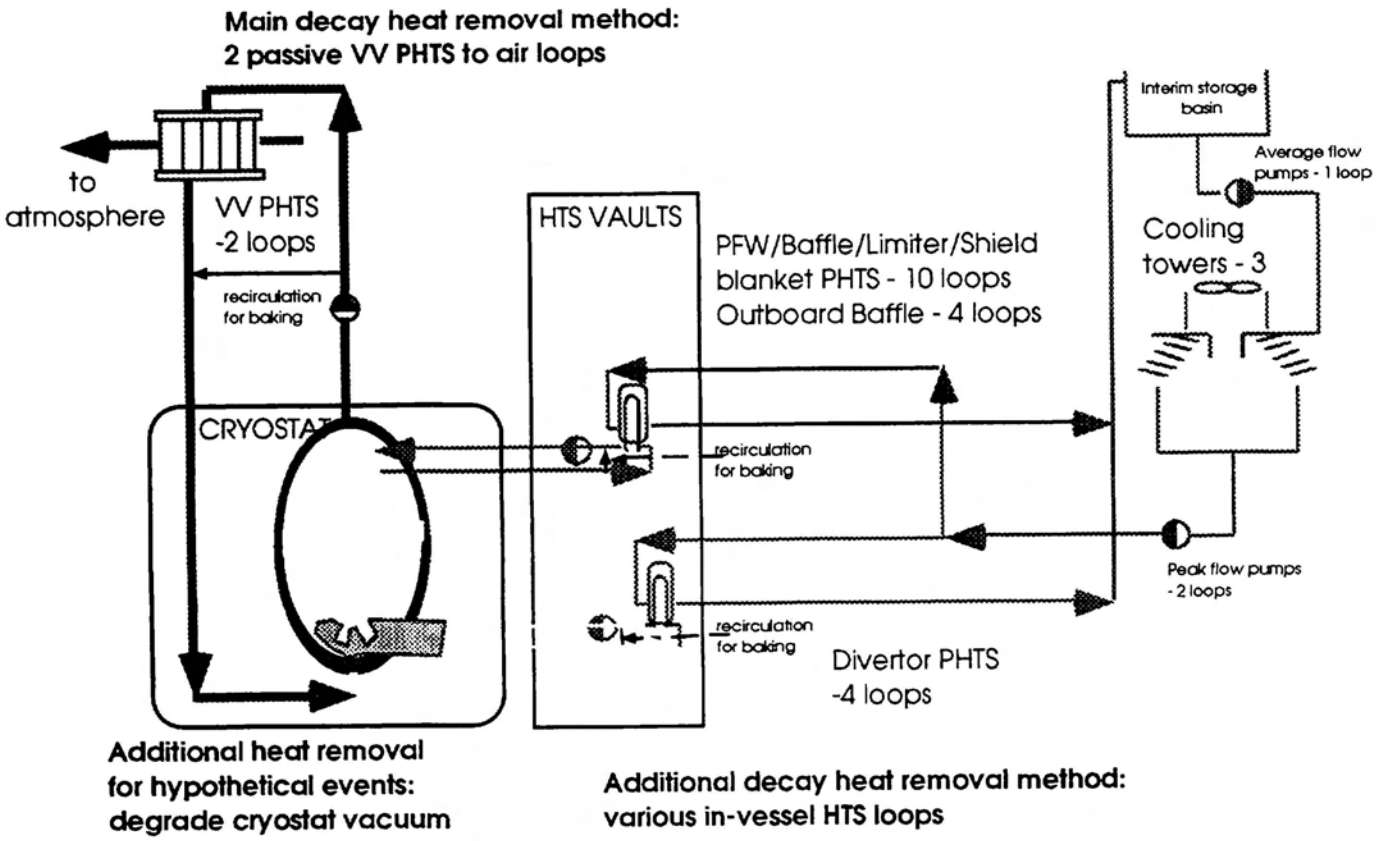

Figure 2: Heat Removal Systems

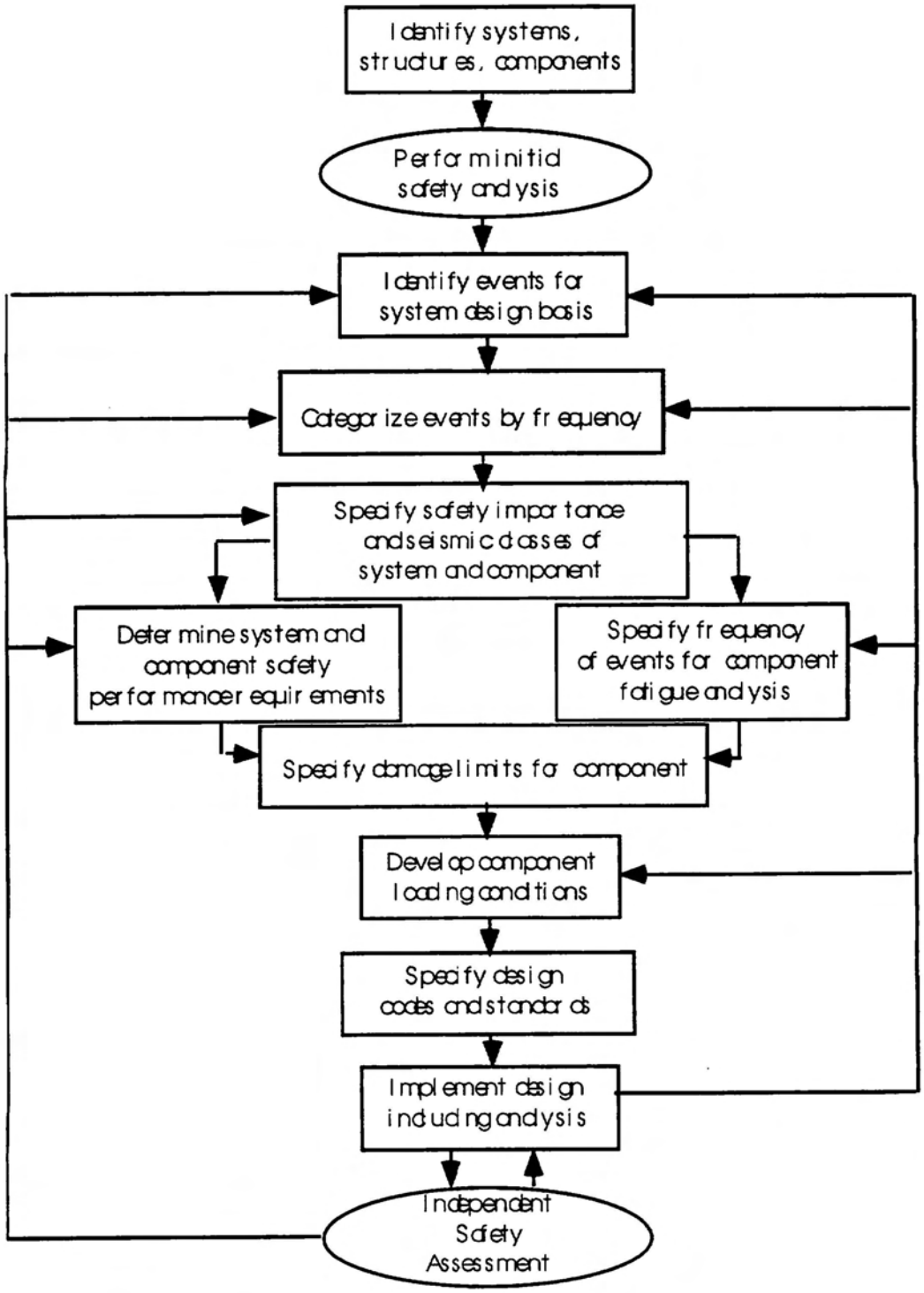

Figure 3 - Structural Design Process