« ASTRID SAFETY DESIGN: PROGRESS ON PREVENTION OF SEVERE ACCIDENT »

P. Lo Pinto[1], L. Costes[1], B. Carluec[2], P. Quellien[1], S. Beils[2], L.Bourgue[3]

[1]Commissariat à l'énergie atomique (CEA), F-13108, Saint Paul lez Durance, France

[2]AREVA NP, F-69456 Lyon, France

[3] Electricité de France (EDF) SEPTEN, Villeurbanne, 69100 France

E-mail contact of main author: pierre.lo-pinto@cea.fr or laurent.costes@cea.fr

Abstract. ASTRID is the Advanced Sodium Technological Reactor for Industrial Demonstration which is intended to prepare the Generation IV reactor, with strong improvements in safety and operability. In order to meet the objectives of the Generation IV reactors and comply with the related specifications, the ASTRID project integrates innovative options.

In the earlier phase of ASTRID project, a specific safety approach was set and its main guidelines were agreed by the French Nuclear Safety Authority. This basic safety design guide is currently applied as reference for the choices of the design options. The paper presents the main applications, in terms of design provisions, to prevent any severe accident, as far as reasonably possible.
In particular, the design measures for "neutron reactivity control" are presented. These measures are based on efficient, reliable, redundant and diversified means for reactor shutdown. In addition, core features and inherent reactor behavior are enhanced and supported if needed by innovative devices. The design approach includes design criteria for assuring safe reactor shutdown states.
As concerns the "decay heat removal" safety function, its loss must be practically eliminated in order to prevent, with a very high level of confidence, a severe accident that could lead to a cliff edge effect. The method applied to reach this objective is described and the resulting heat removal systems and design means are presented.
In the frame of ASTRID safety studies, analyses presented in the paper are devoted to well define:
- A domain of accidental sequences with very low occurrence frequency for which severe accident can reasonably be prevented thanks to appropriate design provisions,
- A few hypothetical situations, consequences of which could not reasonably be mitigated, requiring robust safety demonstrations, in terms of prevention. They have to be practically eliminated.

Despite the high level of prevention of severe accident implemented in ASTRID, its safety approach postulates also a hypothetical severe accident, in order to comply with the defence-in-depth principle (fourth level) and to check that the induced potential consequences are suitably mitigated.

Key Words: severe accident - prevention - safety design

1. Introduction

ASTRID reactor is a technological demonstrator designed by CEA [1] and its industrial partners. Innovative options have been integrated to contribute to the safety and improve efficiency, reliability and operability.
Complying with WENRA (Western European Nuclear Regulators Association) recommendations, the conceptual design of ASTRID takes into account a severe accident involving whole core degradation.

The safety design approach of ASTRID [2] is based on the defence in depth principle.
The implementation of defence in depth levels includes an extension of the design basis domain whatever the low probability of the associated events sequences. The objective is to prevent further the occurrence of a severe accident (definition of SP domain). Despite this extension, mitigation provisions are integrated to cope with the consequences of a severe accident (SM domain).

This SM domain is used to check that consequences of the core degradation are acceptable and that the mitigation devices are suitable in order to reduce the off-site consequences.

As regards severe accident situations leading to unreasonably "mitigable" consequences (e.g. high energetic scenario), a robust demonstration of prevention is set for each "practically eliminated" situation.

2. Method for assessing severe accident prevention

2.1. Line of defence (LoD) method

The ASTRID project takes into account the severe accident in accordance with the fourth level of defence in depth and uses, at the stage of the design, LoD method to show that the prevention of the severe accident is sufficient.

The LoD method which implements the first three levels of the defence in depth, allows to check that any accidental evolution of the state of the plant, up to severe accident, is prevented by minimal set (in quantity and quality) of lines of defence. These LoD are conceived in order to minimize the risks of common mode failure and thus by ensuring a diversification and a functional and physical independence between them.

A LoD is described as strong (or 'a') if it corresponds physically either to passive equipment (e.g. structure) carried out and exploited like a radiological barrier, or with a safety system conceived in particular according to the single failure criterion and qualified by representative tests. The components of the LoD are designed with adapted margins with respect to the stresses corresponding to the situations in which they have to achieve their functions in accordance with relevant codes and standards. The order of magnitude of the failure probability of a strong LoD ('a'), based on the experience feedback of systems respecting such requirements, is of 10^{-3} to 10^{-4} per year or per demand.

A LoD is described as average (or 'b') if it corresponds to a system that isn't the object of the highest design requirements, in particular, if it is not designed according to the single failure criterion. An average LoD can also take the form of an operator action if it is simple and can be done within a reasonable time, if the situation is easy to identify, and if it is described in the operating procedures. The order of magnitude of the failure probability of an average LoD ('b'), starting from the experience feedback, is of 10^{-1} to 10^{-2} per year or per demand.

The favorable natural behavior of the core during the accident, supplemented if needed by dedicated provisions called "additional provisions of safety for the prevention", these Complementary Safety Devices for Prevention (DCS-P), constitute an average LoD.

The link between the LoD and the safety classification of the materials which constitute them is presented in section 3.2.

2.2. Implementation of an extended prevention domain (SP)

In the safety approach of ASTRID, the definition of the domain of the prevention situations (SP) fits first of all in the application of the principle of defence in depth, it corresponds for example to the under-level "3.b" of defence in depth as prescribed by WENRA.

Moreover, the ASTRID Project has set, as design objective (within the limits of reasonably achievable), to prevent the severe accident in case of accidental sequences (or multiple failures) of extremely low occurrence frequency. Indeed, even if the estimated frequency of the sequence is very low, in particular the sequences with failure of the reactor shutdown, the prevention of the severe accident is required. The goal is to push back as much as reasonably

achievable the limits of prevention of the severe accident. The analysis of the consequences allows in particular to seek at the stage of the design the improvement of the natural behavior of the core and if needed to define additional devices of prevention (DCS-P).

The initiating events are gathered by families according to their nature and the associated risk so as to define a limited number of operating conditions.

The selection of initiating events takes account of two requirements:

- progressiveness within the same family of events: certain events are treated as operating conditions of increasing gravity, others more severe as hypothetical situations of domain SP (situations of prevention of the severe accident), even domain SPE (practically eliminated situations);
- the operating condition of a selected category representative of a family events is envelope of the events of this family: in other words, on the one hand its consequences are envelopes of those of the family; in addition, the frequency of occurrence of an event, which can lead to consequences more severe than those of the operating condition, must be lower than the occurrence frequency of the category considered.

At this stage, the main SP situations in different families are:

- fusion in a fuel subassembly in the core,
- leaks of pipes/tanks and their double envelope (e.g., leaks of main and safety vessel),
- water-sodium-air reaction in the casemate of a Steam Generator (option SG),
- discharge of a significant amount of sodium on the roof,
- initiating events combined with failure of the reactor shutdowns systems.

The following approach concerning the unprotected control rod withdrawal (UCRW) and the local fuel melting take into account the feedback from previous projects.

UCRW: In SP situation corresponding to failure of both shutdown systems, the analysis is performed considering best-estimated values for the measured parameters (e.g., the initial linear power) but uncertainties relating to modelling are considered (e.g., the power to melt). That amounts preserve uncertainties on the linear power value (for which melting occurs) and allow to consider the linear power (Plin) in best estimate. The objective is to design the core for avoiding the propagation of a local fuel melting to the whole core. For that it is assumed that the molten fuel fraction has to be lower than 5%.

The design options considered to respect the criteria are the following ones:

- core design limiting the insertion of reactivity in case of UCRW,
- limitation of the individual neutron weight of each rod; for that all rods are used for control and safety,
- improvement of the UCRW detection :
  - first detection using the outlet temperatures of the fuel assemblies close to each rod,
  - second detection base on the measurement of the neutron flux deformation induced by UCRW.

Local fuel melting: Two kinds of situations are considered in the SP domain:

- the unprotected sub-assembly fault corresponding to the failure of both protection systems;
- Local fuel melting belonging to the SP domain for which the goal is to show that the melting volume remains sufficiently localized for maintaining the reactor shutdown capability and avoiding generalized core melting. Lastly, for the subassemblies placed

in not monitored positions (e.g. in-vessel fuel storage), the goal is to show that, in case of complete loss of flow, fuel melting in the subassembly does not occur.

2.3. Practically Eliminated Situations (SPE)

They are situations whose radiological consequences can't be reasonably controlled. They must be the object, on a case-by-case basis, of a robust demonstration of prevention. For a family or a kind of situations, only the extreme cases the consequences of which would not be controllable have to be practically eliminated. The less severe events of the family are taken into account.

The practically eliminated situations are not subject of a safety analysis to the usual direction; the safety analysis relates on the accidental sequences involving the risk to lead to such an eliminated situation and not to the consequences of the situation itself. The robust demonstration of a satisfactory prevention of SPE, require implementation of concrete provisions of prevention. The rules of analysis (e.g. consideration of uncertainties) correspond to those used for the treatment of the initiating accidental sequences.

The deterministic demonstration is supplemented, if it is relevant, by a probabilistic study (e.g. for loss of the DHR function).

The prevention provisions belong to the first three levels of defence-in-depth, just like the situations classified in SP. Compared to the SP situations whose consequences are covered by the field SM, the search for a "robust" demonstration of prevention of a SPE requires adapted specific provisions, in particular:

- the analyses aims at integrating uncertainties with a degree of confidence equivalent to the practices of category 4 in spite of a classification beyond this category 4 of the accidental sequences which precede the practical eliminated situation;
- the equipment needed in the demonstration of a, have a suitable safety classification;
- the addition of provisions, adapted to SPE considered, is also considered within the limit of reasonably feasible, to increase the number of failures necessary before appearance of SPE and to minimize the risk of common mode.

The type of safety demonstration to be brought will depend on the case of SPE to treat. The robustness of the demonstration is checked on a case-by-case analysis.

At this stage, the basic design includes a limited number of SPE situations:

TABLE I: List of SPE

Situations likely to lead to an accident of core fusion with mechanical energy releases not reasonably managed by design	*Important gas passage through the core*
	Significant core compaction
	Brutal failure of the supporting core structures
Situations likely to lead to a degradation of containment and an accident of massive release of the fission products of the fuel subassemblies	*Massive water in the primary circuit*
	Generalized hydrogen deflagration in radiological containment
	Loss of DHR function
Situations of significant degradation of the fuel assemblies whereas the provisions of containment envisaged could not be sufficient	*Handling errors leading to the fuel melting*
	Fuel melting in pool storage

3. Safety demonstration and design

3.1. Basic approach

The safety classification of the equipment (System Structures and Components - SSC) is an important stage of the design process.

The structuring requirements to design the SSC (e.g. requirements of redundancy, independence, diversification or passivity) are not deduced from the SSC classification, but rise directly from the safety analyses (e.g. application of LoD with respect to the functions of safety). These analyses, having to be used to build the safety demonstrations, make possible to identify the equipment to be envisaged as safety classified and condition their safety requirements.
The functional approach is necessary to confirm the list of the safety classified SSC but is not sufficient to classify, because the importance of the safety functions is not systematically representative of the importance, in the safety demonstrations, of the role of each SSC which take part in it.
The objective of the safety SSC classification is to reflect their importance in the safety demonstration and to apply for the same safety class (relation with the guides of design-construction) a set of coherent requirements taking into account the SSC type (e.g. civil engineering, instrumentation & control).

In a general way, for each SSC type, the requirements associated with the safety classification are formalized in guides being the subject of the broadest possible consensus on the level of the experts in the fields considered. These requirements are the fruit of R & D programmes dedicated and, as much as possible, of an experience feedback. Taking into account the innovating character of certain equipment or architectures selected to provide the safety functions on ASTRID, the use of an existing guide is not automatic and must be the subject of a study of compatibility. Adaptations of existing guides, related to specificities of ASTRID, are thus possible.

3.2. Safety classification of the equipment

For ASTRID, the method used for classification is firstly based on the role of each SCC in the safety demonstration in particular in terms of LoD (Lines of Defence) and LoM (Lines of Mitigation; i.e. equipment involved in the mitigation of severe accident).

The role of the SSC in the safety demonstrations is thus used as reference for classification as follows:

- Importance of the SSC contribution to the demonstration (e.g. effectiveness, reliability);
- Importance of the impact in case of a SSC failure (e.g. level of consequences, prevention of SPE).

For ASTRID, the main safety classes are defined as follows:

- Safety Classes of Prevention (named CSP-n):
  - CSP-1: SSC whose failure in the safety demonstration must be equivalent to the failure of more than one strong LoD.
  - CSP-2: SSC involved in a strong LoD, including confinement barrier needed to meet the objectives of category 4.
  - CSP-3:
    - SSC whose failure impacts SSC classified in CSP-1 or CSP-2;
    - barrier devoted to meet the objectives of category 2;

  - SSC monitoring SSC classified in CSP-1 or CSP-2 in order to check the availability of these materials.
- Safety Class of severe accident Mitigation (named CSM):
  - CSM: SSC involved in the accident mitigation.

4. PREVENTION OF SEVERE ACCIDENT

4.1. Reactivity control

The prevention of the severe accident is ensured by:

- Preventive measures of the initiating events likely to damage the core.
- Control of the fundamental safety functions:
  - reactivity control,
  - decay heat removal.
- Preventive measures necessary to justify “practical elimination” of particular severe accident situations whose radiological consequences cannot reasonably be limited.

The reactivity control measures are first based on efficient, reliable, redundant and diversified systems for reactor shutdown.

In addition, inherent core behavior is enhanced and supported if needed by innovative devices.

These systems are deterministically designed with stringent criteria.

An important need required for ASTRID core design is to insert sufficient negative reactivity in case of unprotected loss of cooling accident to avoid severe accident. The CFV low void core concept provides a large part of negative reactivity insertion thanks to its favourable natural behaviour [3]. At this design stage, to ensure larger margins, the natural behavior of the core is completed by additional safety devices able to insert sufficient negative reactivity (DCS-P).

4.1.1. Features of the main shutdown systems

An innovative reactivity control [4] which is studied in the frame of the ASTRID project is presented. All the rods participate to power management and shutdown. Comparatively to traditional systems, the gains of this architecture in terms of safety, are noticeable and allow reducing the overall number of control rods.

The reactivity control is ensured by a set of mobile neutron absorbents positioned in the core. The control rods are divided into two distinct and diversified families. These systems are respectively called RBC (control and shutdown device) and RBD (diverse control and shutdown device).

Two redundant and diversified automatic shutdown systems are envisaged (each system includes a mix of the both rod families).

Both control rods families, RBC and RBD, provide at the same time the functions of control (start up, adjustment of the neutronic power, compensation of the burn-up, neutronic flux adjustment) and the function of reactor shutdown. This kind of architecture, called RID (for “pilotage en RIDeau”), presents compared to a conventional system as Super Phenix type, the following advantages:

- with a larger number of control rod involved in reactor operation (as RBD are not as in previous reactor, only dedicated to shutdown needs), the RID option offers larger

margins (compared to e.g. EFR option) in case of control rod withdrawal, thus the core behaviour is enhanced;
- the possibility to improve the distribution of both rod families (RBC and RBD). At this design stage (9 RBD + 9 RBC) are implemented in ASTRID.

The control rods are composed of absorbents in B_4C enriched in ^{10}B.

RBC is a control rod element dedicated to reactor operation and shutdown. In case of gravity drop, the RBC rods drop with their driving line after decoupling the electromagnets located in gas, above the sodium level.

RBD is a diversified control element used for reactor operation and shutdown too, contrarily to past where it was only dedicated to safety function. As a major design option, disconnection in case of shutdown between the RBD rod and its drive mechanism would occur via an electromagnet located in sodium.

RBC and RBD are gathered in two independent groups connected to the shutdown systems.

The safety analysis required the detection of each initiating event by two different parameters monitored by each shutdown system.

4.1.2. Additional design provisions (DCS-P)

Within the framework of the development of additional Safety provisions aiming to severe accident Prevention (DCS-P), it is envisaged to supplement the natural behavior of the CFV core in case of total failure of both shutdown systems by the passive intervention of two types of (DCS-P) initiated by a physical phenomenon:

- one in case of loss of flow, noted (DCS-P) – H rod [5];
- the other, under development, in case of temperature increase (Curie point), noted (DCS-P) – T rod.

The insertion of negative reactivity by one of these systems (DCS-P) allows to stop the neutronic reaction and to ensure a long term safe state, compatible with the behavior of the structures.

(DCS-P)-H would constitute a provision independent of both shutdown systems. It has only a safety function.

(DCS-P)-T is carried by one family of control rods. The (DCS-P)-T includes an electromagnet in sodium.

4.2. Decay heat removal safety systems

After reactor shutdown, the core decay heat must be adequately removed in order to avoid large damage of core and primary circuit structures. This is achieved by maintaining a sufficient sodium level in the primary circuit and with capability to remove the decay heat by forced convection and by natural circulation if the normal electrical supply of the primary pumps fails as well as implementation of dedicated circuits.

The main challenge concerning the decay heat removal function is to implement very reliable systems capable to maintain the reactor in safe conditions during long time, until the decay heat decreases sufficiently to allow the decay heat removal through natural thermal losses or by a diverse heat removal system.

In case of severe accident, the long term management of molten core (corium) is mandatory. This leads to implement devices for both maintaining the corium in a sub-critical state, and removing its decay heat. The devices implemented for achieving these functions shall not be unacceptably damaged by the accident.

The architecture and the reliability of the systems involved in the decay heat removal have to allow the practical elimination of the complete loss of the DHR function.

This objective is translated in particular by:

- the search for one or several systems with important passive capacity and the less dependent possible to support systems,
- a design allowing to facilitate reparability in case of failure.

To obtain the practical elimination of the total loss of the function, the architecture is based on the implementation of three safety systems:

- two DHR systems insuring a direct cooling of the primary sodium, by heat exchangers in the vessel diving into the primary sodium, these two Direct Reactor Auxiliary Cooling Systems (DRACS) are named RRA and RRB. Each system should implement multiple trains;
- a system implemented outside of the safety vessel. It is absorbing the heat emitted by radiation and convection from the vessels. This system introduces a level of additional diversification with regard to RRA and RRB. It presents in particular the advantage not to transit by the reactor roof and not to be submitted directly to the hypothetical mechanical energy release in case of severe accident. It is well suited to manage hypothetical situations with degraded core, at long term.

The RRA is an active system located in the cold plenum.

The RRB is a passive system located in the hot plenum.

5. CONCLUSIONS

In the earlier phase of ASTRID project, a specific safety approach was set and its main orientations were agreed by the French Nuclear Safety Authority. This safety design guideline is currently applied upon the new phase of basic design for the choices of the design options.

Reactivity control function is achieved by two diverse shutdown systems with related design criteria giving sufficient safety margins for different plant states. Beyond the high reliability of these shutdown systems, inherent behavior of reactor is improved to cope with hypothetical transients without scram. This second approach by “event family” (ULOF, ULOHS…) is completed in parallel by a third “plant state” approach involving special devices acting in case of loss of flow or core heating whatever the initiating event of the accident.

Decay heat removal function is ensured by several systems with diversified thermal-hydraulic zone of implementation in order to deal each possible DHR fault situation. DHR means are composed by a system devoted to heat removal at normal shutdown states, two different safety systems connected to primary circuit, an ultimate system inside the reactor vault to manage hypothetical situations with degraded reactor, at long term. These systems are designed to favor potentials for repair at short time.

Appendix 1: References

[1] J. ROUAULT, ASTRID, The SFR GENIV Technology Demonstrator Project: Where are we Where Do We Stand For?, Proc. of ICAPP 2015, Nice, France (2015)

[2] P. Lo Pinto et al., “Safety orientations during ASTRID conceptual design phase”, Proc. of FR13, Paper CN-199-267, Paris, France (2013)

[3] C. VENARD et al., “The ASTRID core at the end of the conceptual design phase”, Proc. of FR 17, paper CN-245-288, Ekaterinburg, Russian Federation (2017)

[4] B. FONTAINE et al. “ASTRID: an innovative control rods system to manage reactivity”, Proc. of ICAPP 2016, San Francisco CA, USA, April 17-20, 2016

[5] GUÉNOT-DELAHAIE et al., “The innovative RBH additional safety device for ASTRID to address unprotected loss of flow transients: from design to qualification”, Proc. of ICAPP 2016, paper 16116, San Francisco, USA (2016)