21st Conference of the Canadian Nuclear Society
Toronto, Ontario, Canada / June 11-14, 2000

A New Approach to Determine The Environmental Qualification Requirements For The Safety Related Equipment

By

Chiheb Hasnaoui, P. Eng.
Énaq
Hasnaoui.chiheb@hydro.qc.ca

And

Gilbert Parent, P. Eng.
Hydro-Quebec, Gentilly-2
Parent.gilbert.A@hydro.qc.ca

1000, De La Gauchetière, suite 1400
Montreal, Quebec
H3B-4W5

Abstract

The objective of the environmental qualification of safety related equipment is to ensure that the plant defense-in-depth is not compromised by common mode failures following design basis accidents with a harsh environment. A new approach based on safety functions has been developed to determine what safety-related equipment is required to function during and after a design basis accident, as well as their environmental qualification requirements. The main feature of this approach is to use *auxiliary safety functions* established from safety requirements as credited in the safety analyses. This approach is undertaken in three steps:

- ✓ identification of the *auxiliary safety functions* of each *main safety function*,
- ✓ determination of the *main equipment groups* required for each *auxiliary safety function,* and
- ✓ review of the safety analyses for *design basis accidents* in order to determine the credited a*uxiliary safety functions* and their mission times for each accident scenario.

Some of the benefits of the proposed approach for the determination of the safety environmental qualification requirements are: a systematic approach for the review of safety analyses based on a safety function check list, and the insurance, with the availability of the safety functions, that Gentilly-2 defense-in-depth would not be compromised by design basis accidents with a harsh environment.

1 Introduction

The objective of the environmental qualification (EQ[1]) of safety-related equipment is to ensure that the plant defense-in-depth is not compromised by common mode failures following design basis accidents with a harsh environment. The operator should always have a reasonable assurance that the requested safety related equipment remains available when exposed to a harsh environment and will operate as credited in the safety analyses.

Safety-related equipment is required to perform its safety functions in the environments produced under all Design Basis Accident conditions (large LOCAs, small LOCAs, SSB, etc.). Environmental Qualification of equipment is required in order to eliminate "common-cause" failures (systematic, non-random, concurrent failures) due to environmental service conditions that can jeopardize the plant defense-in-depth [1].

The first step in establishing environmental qualification is to generate a list of all items of equipment to be qualified together with their qualification requirements.

A new approach based on safety functions has been developed in order to determine the safety-related equipment that is required to function during and after a design basis accident, and that requires environmental qualification. The main feature of this approach is to use *auxiliary safety functions* established from the safety requirements as credited in the safety analyses. This paper describes this approach and shows some of the results obtained.

2 Gentilly-2 background

Gentilly-2 was designed with environmental qualification requirements based on the experience and the standards available at that time. However, since Gentilly-2 commissioning in 1982, qualification standards and practices have evolved and many of the original safety analyses have been revised. Gentilly-2 environmental qualification has not been maintained up-to-date due to the lack of a preservation program. In 1997, an environmental qualification-upgrading program was initiated for Gentilly-2. This program established an integrated and comprehensive set of requirements to provide assurance that safety-related equipment can perform as required if exposed to harsh conditions and that this capability should be preserved over the rest of the life of the plant. As a part of this program, the original environmental qualification list (established by AECL) was to be reviewed to take into account the current operation and safety practices. The revised list was also required to meet the quality assurance requirements on documentation.

---

[1] The abbreviations used in this paper are given in section 7.

The original Gentilly-2 EQ list was reviewed in 1998. Based on a preliminary assessment of the EQ requirements, some equipment has been added, and others put on standby until a systematic review is performed. For each main equipment on this list, an environmental qualification priority, 1, 2 or 3 (1 is the highest priority) has been given in order to concentrate the preliminary EQ corrective actions on equipment which has the most impact on safety (*Preliminary equipment critical list*, equipment of priority 1 and 2, reference 3).

A systematic review for the determination of the required equipment, their safety-related justifications, and their EQ requirements was started in 1999. This is performed by:

- defining the scope and the parameters for this review, and
- performing a systematic review of the safety analyses.

3 Methodology of the new approach to determine the required safety-related equipment

The main feature of the new approach for determining the required safety-related equipment is to use *auxiliary safety functions* established from the safety requirements as credited in the safety analyses.

This approach is undertaken in three steps (Figure 1):

1. Identification of the *auxiliary safety functions* for each *main safety function*.
2. Determination of the *main equipment groups* required to support each *auxiliary safety function,* and
3. Review of the safety analyses in order to determine the credited a*uxiliary safety functions* and their mission times for each DBA accident scenario producing a harsh environment.

These steps are interdependent and part of an iterative process, i. e. the review of the safety analyses for credited auxiliary safety functions helps to identify missing functions.

The data collected for each step are managed with an Access® database used to update, filter and process the large amount of information collected. Figures presented hereafter are extracted from this database.

3.1 Determination of the auxiliary safety functions

This is the first identified step of the new approach. Auxiliary safety functions are required to ensure that the related *main safety function* is available; the unavailability of an auxiliary safety function does not necessarily compromise the *main safety function*.

3.1.1 Main safety functions

Safety functions are processes or conditions essential to maintain plant parameters within acceptable limits established for the design basis events [1]. They satisfy the following general safety requirements: shut down the reactor and maintain it sub-critical, maintain a heat sink for the reactor, and containment of radioactive elements inside the reactor building.

These safety requirements have been divided into six *main safety functions* [4]. These functions are credited in the analyses of design basis accidents. The environmental qualification program must demonstrate that the required safety functions are maintained for the specified mission time in the presence of harsh environmental conditions. These *main safety functions* are:

1. Reactor shutdown: shutdown systems 1 and 2 must remain effective as credited in the safety analyses.
2. Maintenance of reactor shutdown for the required mission time.
3. Establishment and maintenance of a heat sink for the reactor with the emergency core cooling system.
4. Establishment and maintenance of a heat sink for the reactor with the safety related systems. In order to ensure this function availability, three sub-functions must be available :
   - a coolant circulation means (pumps or thermosyphoning),
   - an inventory (coolant fluid) and
   - a heat sink for thermal dissipation.
5. Establishment of a containment barrier and maintenance of the reactor building structural integrity as to respect the licensing guideline dose limits.
6. Maintenance of the support systems and availability of the secondary control room to ensure the availability of the special safety systems and safety related systems safety function.

Each *main safety function* is detailed into a set of *auxiliary safety functions* for environmental qualification assessment.

3.1.2 Auxiliary safety functions

Auxiliary are established from safety requirements as credited in the safety analyses. They are classified into four families [4]:

1. Auxiliary functions for detection: measurement of a parameter and comparison to a set point for an automatic action initiation (i.e. detection of high reactor building pressure for the containment isolation).
2. Auxiliary functions related to an automatic or a manual action: equipment required to perform an action which implies a change in its status (i.e. valve opening, pump start, etc).
3. Auxiliary functions related to the maintainability of the safety functions:

- Ability of a mechanical or an instrumentation and control equipment to maintain its new status as requested by one of the previous auxiliary functions (i.e. a valve requested to open should stay open).
- Ability to maintain a passive status of mechanical and instrumentation and control equipment which is not directly requested by any of the previous auxiliary functions (i.e. no spurious opening of a normally closed valve if it could compromise the safety function).
- Safe failure of the safety system test circuits: these circuits should not impair the credited safety function.

4. Auxiliary functions related to surveillance: alarms and indications required by the operator to initiate or to confirm an automatic or a manual action and/or to ensure that a safety function is maintained (i.e. surveillance of the emergency core cooling injection flow).

Auxiliary safety functions are related to one or more *main equipment groups*. An example of an auxiliary safety function is shown in Figure 2 with its related *main equipment groups*. The use of auxiliary safety functions allows the EQ requirements for a particular group of equipment to be determined. This avoids more generic EQ requirements applied to all equipment, which could be too constraining for some equipment. It also enables the review of the safety analyses to concentrated on safety functions and not on a single piece or a group of equipment.

3.2 Determination of the main equipment groups

The second step in the new approach for the determination of environmental qualification requirements is the determination of the *main equipment groups* of each *auxiliary safety function*.

A main equipment is defined as an equipment which, by its action or its failure, directly affects the auxiliary safety function. Generally, these are the mechanical and I&C equipment specified in functional diagrams (i.e. 63432-PT3K, 3432-PV10, etc.). Only main equipment is associated with auxiliary safety functions. Auxiliary equipment is identified through the environmental qualification evaluation process. Auxiliary equipment supports a main equipment to perform its safety function; they are indirectly related to the safety function (i.e. 63432-PY3K, 3432-SV78, etc.). The objective of this discrimination between main and auxiliary equipment is to facilitate identification of the auxiliary functions attached to equipment. Figure 2 shows an example of the *main equipment groups* attached to an auxiliary safety function.

This step is actually limited, as a first iteration, to the association to auxiliary safety functions only main equipment from the *Preliminary equipment critical list* [5]. In the near future, a systematic review will be conducted to identify all the equipment required to ensure each auxiliary function.

3.3 Review of the safety analyses to determine the credited auxiliary safety functions

The third and last step of the approach is the review of the safety analyses in order to determine the auxiliary safety functions credited for each DBA accident scenario and the determination of their mission times. Figure 3 shows an example of a review for an auxiliary safety function. This process provides the EQ requirements for each auxiliary function (mission time, accident category, etc.). Consequently, it defines the EQ requirements for all the *main equipment groups* attached to each auxiliary function. For the purpose of the EQ assessment process, the EQ requirements are synthesized in order to be manageable by the users.

4 Results

An example of the EQ requirements of a main equipment group is shown in Figure 4. The EQ requirements of each main group are extracted automatically for each design basis accident category. These are:

- LOCA (including large and small)
- small LOCA
- large SSB inside the reactor building and
- large SSB outside the reactor building.

Mission times for environmental qualification are divided into four periods:

- 15 minutes
- 1 hour
- 1 day
- 3 months

These mission periods and design basis accidents categories could be changed easily inside the database (new periods, new accident categories, etc.) and new environmental qualification requirements could be assessed.

For each main equipment group, the following EQ requirements are synthesized:

- A list of the functional requirements for the main equipment group is provided to ensure the availability of the credited auxiliary functions (i.e. open, remain open, measure, etc.)
- For each functional requirement, the mission time for each accident category.

5 Conclusion

A new approach based on detailed safety functions has been developed to determine the safety related equipment required to function during and after a design basis accident and that require environmental qualification, together with their EQ requirements. The main feature of this approach is to use *auxiliary safety functions* established from safety requirements as credited in the *safety analyses*. This approach is undertaken through three steps: identification of the

a*uxiliary safety functions*, determination of the m*ain equipment groups,* and review of the safety analyses to identify the credited auxiliary safety functions.

Some of the benefits of the proposed approach for the determination of the safety EQ requirements are:

- A systematic approach for the review of the safety analyses, based on a safety function checklist.
- The insurance, with the availability of the safety functions, that Gentilly-2 defense-in-depth will not be compromised by accidents with a harsh environment.
- The current safety analyses and the changes in safety approach since Gentilly-2 commissioning are accounted for.
- Trace-ability of the justifications for any EQ requirements with the help of the database.
- Involvement of the overloaded technical support groups is minimized.
- The safety group is directly involved as opposed to the traditional approach for the determination of EQ requirements which is normally the task of technical support and environmental qualification groups.
- It is applicable to all CANDUs.

6 References

1. P. Holzman and G. Sliter, « Equipment Qualification Reference Manual », EPRI, 1992.
2. M. Garceau, "Enveloppe de qualification environnementale des équipements", Hydro-Québec, Gentilly-2, RT-98-21, December 1998.
3. G. Parent and C. Hasnaoui, "Liste préliminaire des équipements à qualifier environnementalement (QE)", Hydro-Québec, Gentilly-2, ATA-99-13, revision 1, June 1999.
4. G. Parent and C. Hasnaoui, "Fonctions de sûreté principales et auxiliaires utilisées pour déterminer les équipements à qualifier environnementalement (QE)", Hydro-Québec, Gentilly-2, ATA-99-14, revision 2, March 2000.
5. G. Parent and C. Hasnaoui, " Fonctions de sûreté rattachées aux équipements principaux de la liste QE des équipements critiques", Hydro-Québec, Gentilly-2, ATA-99-15, revision 0, March 2000.

7 Abbreviations

EQ	Environmental Qualification
DBA	Design Basis Accident
LOCA	Large Loss of Coolant
SSB	Secondary Side Break

Figure 1: G-2 approach for the determination of environmental qualification requirements flow chart

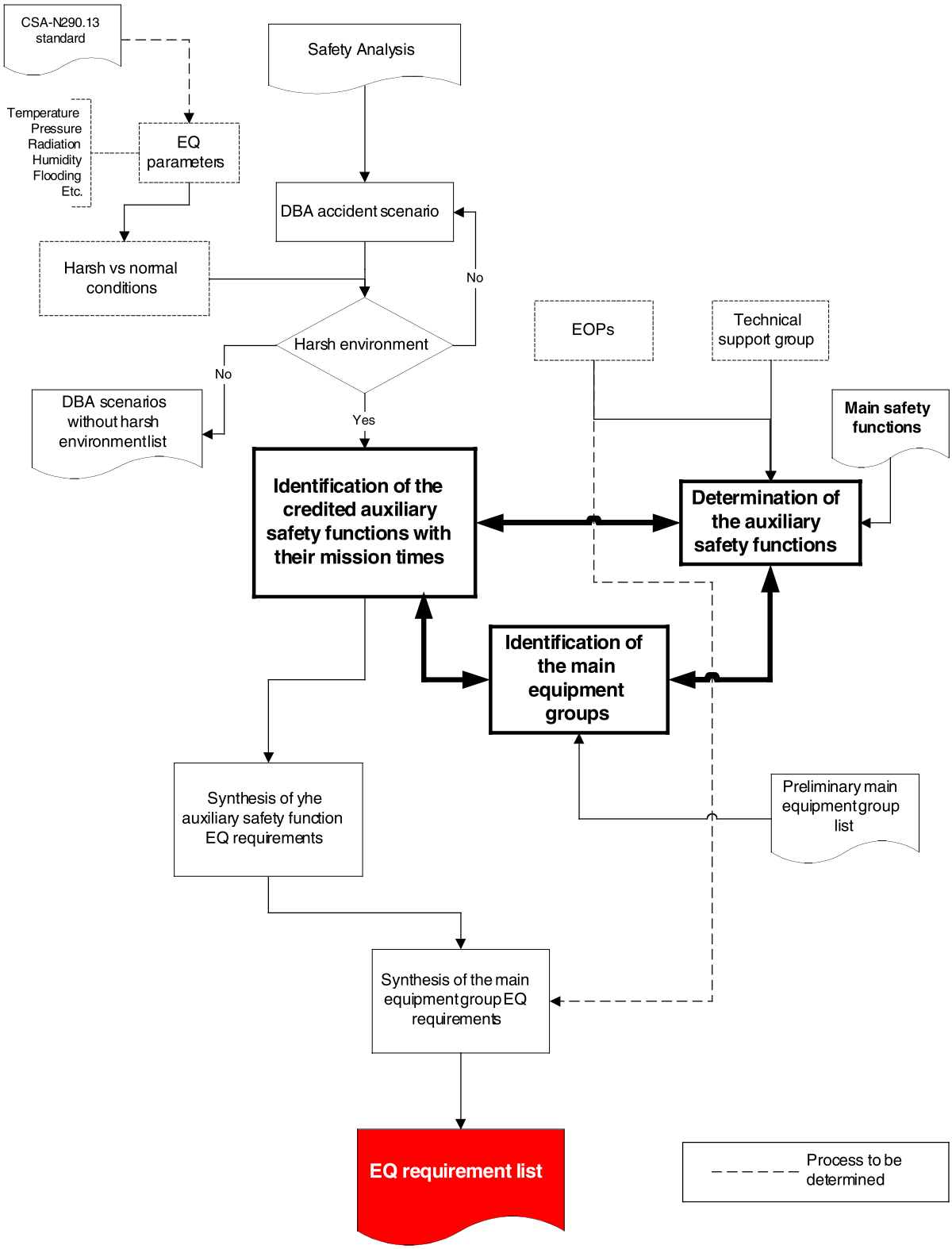

Figure 2: *Main equipment groups* associated with an auxiliary safety function

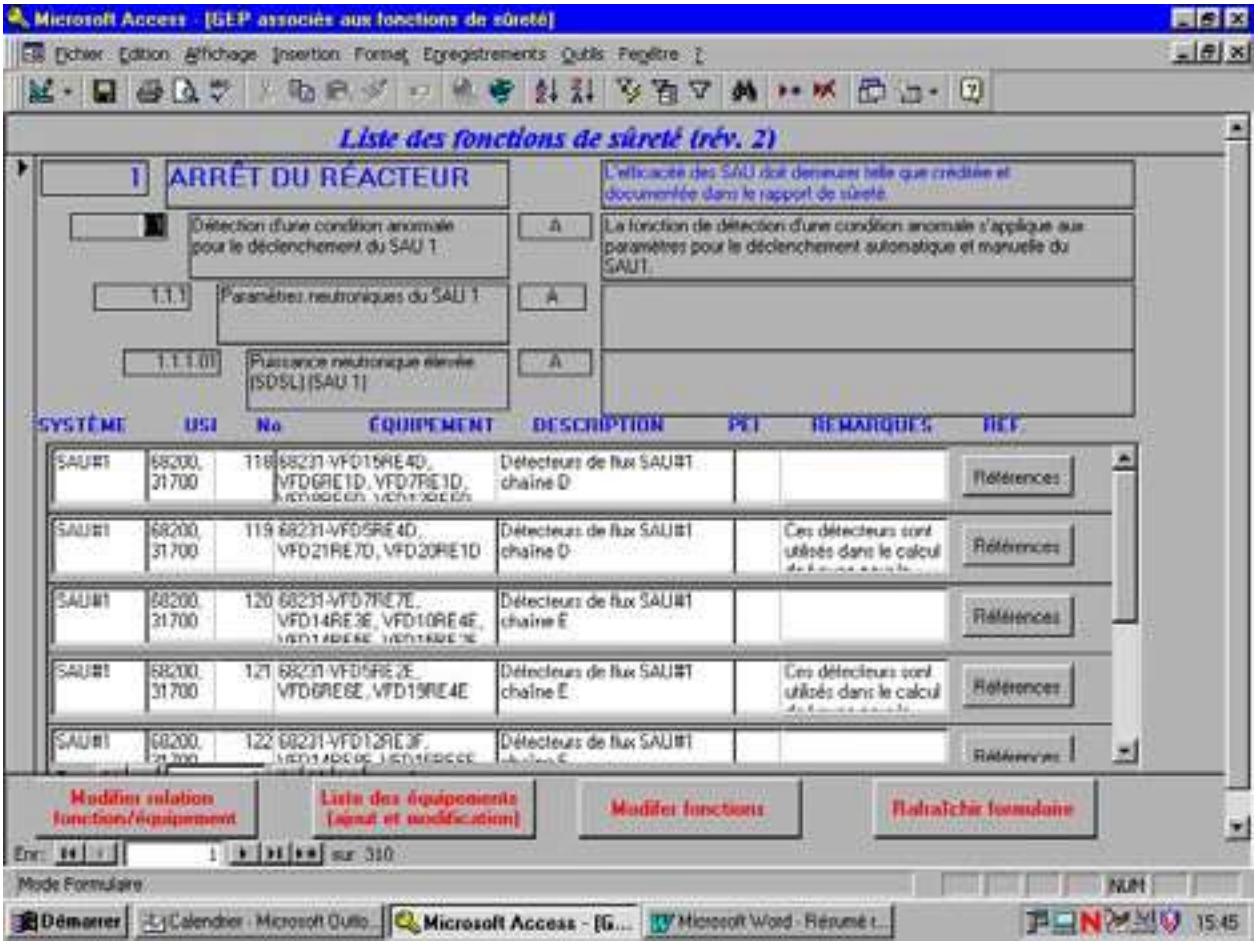

Figure 3: A safety analysis review example

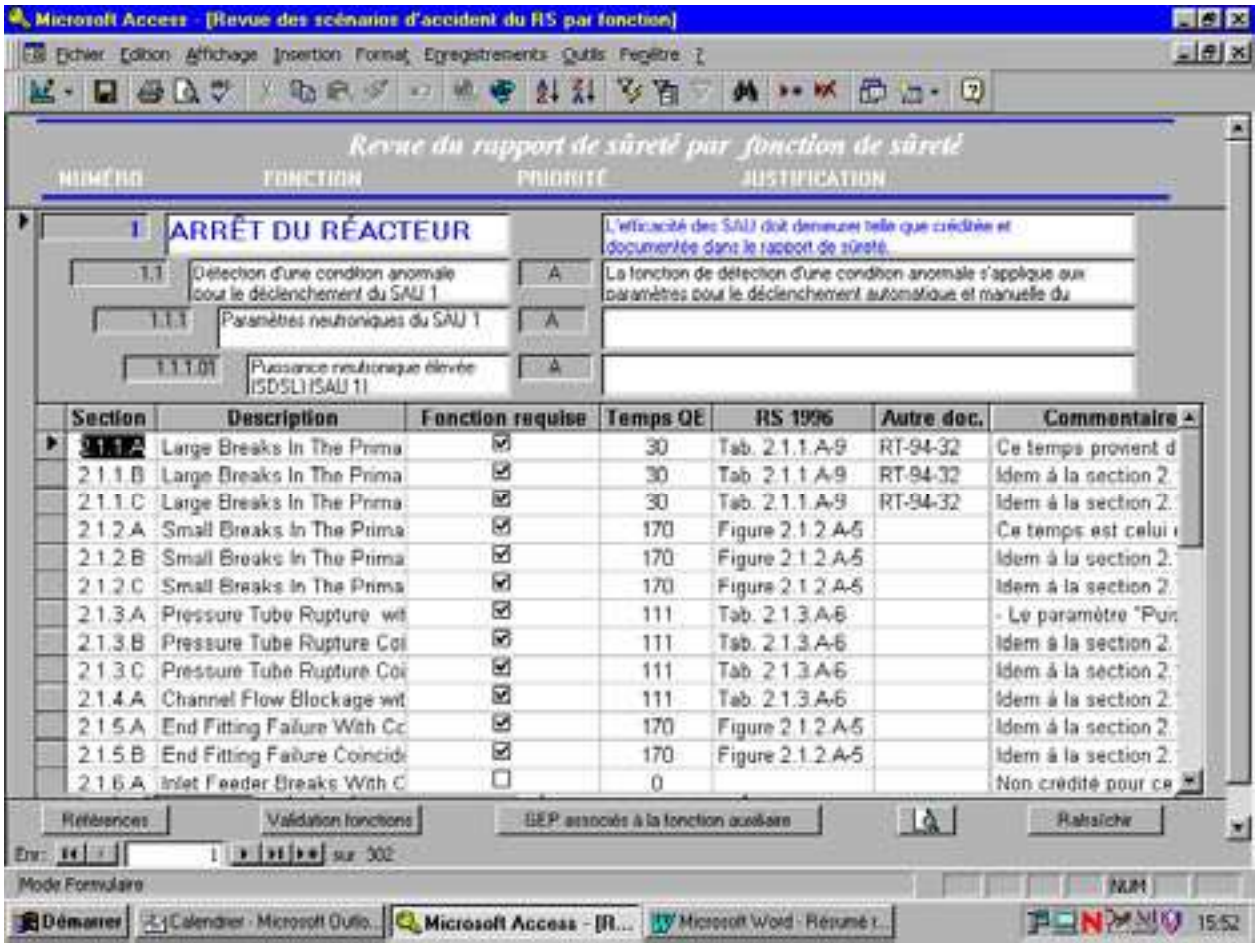

Figure 4: A main equipment group environmental qualification requirements sample