Methodology for Identifying Boundaries of Systems Important to Safety in CANDU Nuclear Power Plants

Simon Therrien[1)], Dragan Komljenovic[1)]*, Philippe Therrien[1)], Carol Ruest[1)], Pierre Prévost[1)], Raynald Vaillancourt[1)]

Hydro-Québec, Nuclear Generating Station Gentilly-2, Bécancour, Québec, Canada

Abstract

This paper presents a methodology developed to identify the boundaries of the systems important to safety (SIS) at the Gentilly-2 Nuclear Power Plant (NPP), Hydro-Québec. The SIS boundaries identification considers nuclear safety only. Components that are not identified as important to safety are systematically identified as related to safety. A global assessment process such as WANO/INPO AP-913 "Equipment Reliability Process" will be needed to implement adequate changes in the management rules of those components. The paper depicts results in applying the methodology to the Shutdown Systems #1 and #2 (SDS#1, #2), and to the Emergency Core Cooling System (ECCS). This validation process enabled fine tuning the methodology, performing a better estimate of the effort required to evaluate a system, and identifying components important to safety of these systems.

***Key words*:** *reliability program, component important to safety, risk-informed decision-making*

1. Introduction

Canadian Nuclear industry has to comply with a new Regulatory standard S-98 "Reliability Programs for Nuclear Power Plants" issued by Canadian Nuclear Safety Commission (CNSC). The purpose of this standard is to help assure that licensee who constructs or operates Nuclear Power Plant (NPP) develops and implements a reliability program that assures that the systems important to safety (SIS) at the plant can and will meet their defined design and performance specifications at acceptable levels of reliability throughout the lifetime of the facility [1]. The spirit beyond this standard is to ensure that the resources are allocated for the systems significantly important to the safety.

One major requirement to the reliability program consists in identifying the SIS. The next step involves an identification of the SIS boundaries. In fact, this activity defines components that are really important in fulfilling the SIS safety functions.

2. Objective

The main objective of this paper is to depict the methodology developed for identifying boundaries of SIS at the Gentilly-2 NPP, Hydro-Québec, without using Probabilistic Safety Assessment – PSA.

*) Corresponding author: komljenovic.dragan@hydro.qc.ca

3. Scope of the work

SIS boundaries identification is realized to meet the requirements of the regulatory standard S-98 "Reliability Programs for Nuclear Power Plants". This activity takes into consideration nuclear safety only. Components that are not identified as important to safety (CIS) are systematically identified as components related to safety (CRS).

The implementation of the regulatory standard S-98 at Gentilly-2 NPP is an ongoing process. The full impact on both the management rules, and processes related to the introduction of the SIS is still under assessment. For this reason, the existing management rules for both Systems Related to Safety (SRS), and CRS cannot be modified (relaxed) until a global assessment is realized. One has to take into account other aspects such as generation, environment, other standards and legal obligations for completing this evaluation. Thus, it will be essential to use a global assessment process such as AP-913 "Equipment Reliability Process" to modify the management rules of those components [2].

Another objective related to the identification of SIS boundaries consists in an identification of a component list, which will be integrated into the station reliability database used in reliability modeling of the SIS. Since the foreseen scope of use of the CIS list is relatively large (consequences on management rules related to these components, and keeping an overall reliability of the SIS at a high level), their identification cannot be limited to the use of SIS fault trees only.

4. Assumptions

This section presents the main assumptions used in developing the CIS identification methodology.

- An initial CIS list is elaborated by means of "Universal subject index" (USI) identified in the phase of the SIS identification. A plant-wide component database is used in this stage. Insights from both the fault tree models, and system engineers give a reasonable assurance that no important component is omitted in the initial list.
- Only single failures are considered in the assessment.
- In principle, only components that have a direct impact on the safety function are considered. The limit is the first valve normally closed (cut-out point) that has to be closed and tighten during the safety function mission.
- In general, components, which state does not change while fulfilling a safety function mission, are not taken into consideration. Other processes in the plant generally govern those components such as standards related to pressure vessels, environmental qualification, seismic qualification, etc. They are not integrated into the reliability program. E.g., the list of components excluded from the reliability program includes piping, plugs, tank, junction box, pipe support, orifice, etc.

5. Bibliography survey

An exhaustive literature review has been performed to determine whether a methodology applicable for identifying critical Systems, Structures, and Components (SSC) has already been developed. The survey considered papers from both nuclear industry, and other industries potentially at risk. Numerous sources related to this topic have been identified. Despite the fact that numerous references have been investigated [2, 3, 5, 6, 7, 8, 9, 11, 12, 13, 14, 15, 16, 17, 18, 19], this survey has not allowed to notice a methodology directly applicable to the context of SIS boundaries identification at the Gentilly-2 NPP. However, this activity allowed compiling both pertinent information, and insights to develop an adequate methodology for the purpose of the SIS boundary identification. The risk-informed decision making process, and the use of insights related to importance measures factors have been particularly useful in elaborating the whole approach [4, 10, 12, 13, 20].

Some specific identifications of critical SSC have also been realized at some extend in past projects at the Gentilly-2 NPP. In fact, the environmental qualification, the preventive maintenance optimization project based on the AP-913 process, and the systems health assessment are three examples in which specific identification activities of critical SSC were performed. This work used both insights, and main results of such projects.

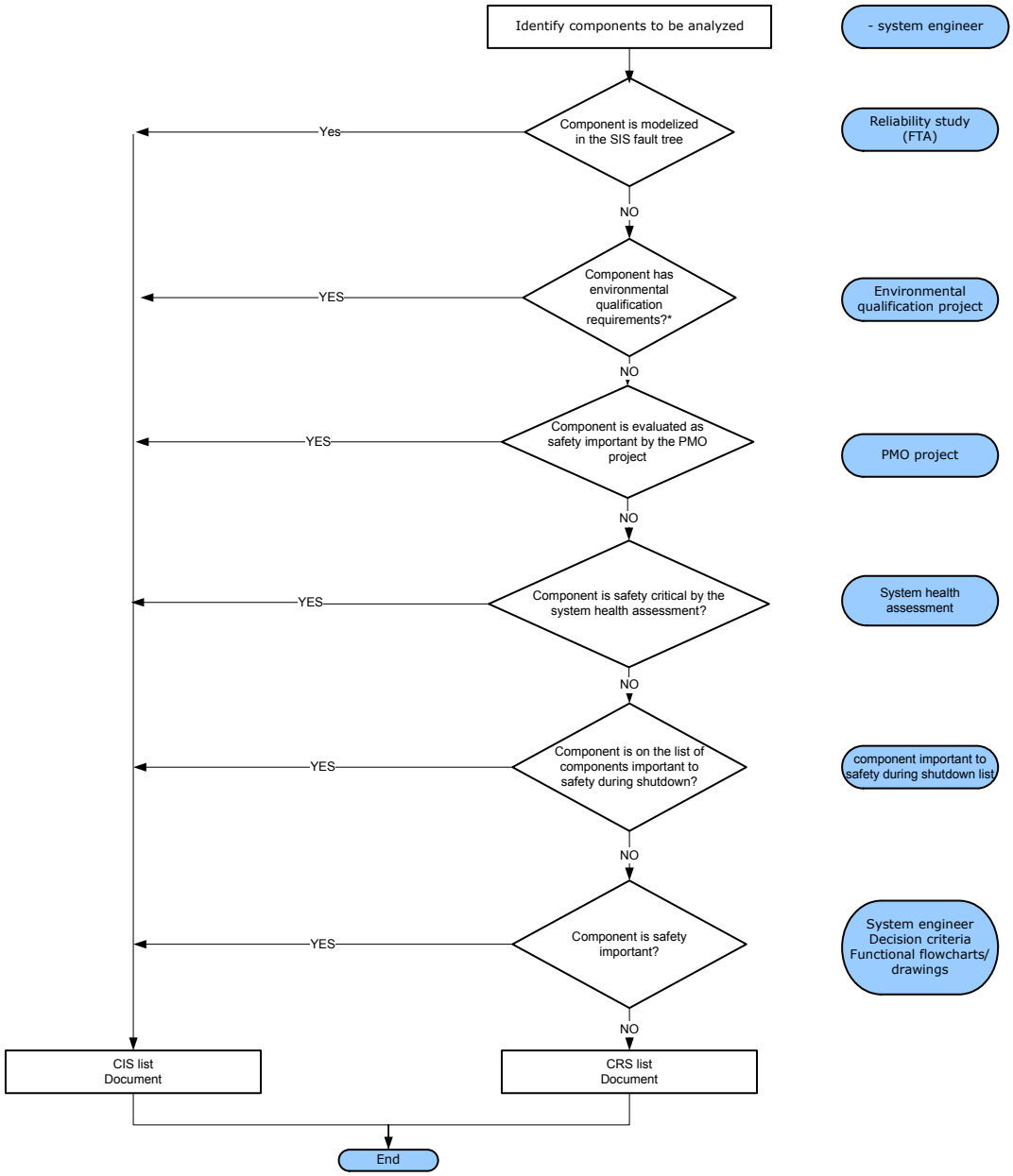
6. Methodology

The approach developed is based on risk information, and uses insights from both qualitative and quantitative assessments. The methodology also integrates, in a structured manner, the use of expert judgment. The role of the later is important in both quantifying intangible influence factors, and ensuring a coherence of obtained results. The methodology is constituted of several decision criteria based on previous assessments realized at Gentilly-2 NPP. The approach is narrowly related to the Risk-Informed Decision-Making concept, which is increasingly employed in Canadian nuclear power industry.

The main insights of the methodology are obtained from the following sources of information:

- SIS fault tree;
- Safety criticality assessment identified through the Preventive Maintenance Optimization (PMO) project based on the AP-913 “Equipment Reliability Process”;
- Safety criticality assessment in the system health report realized for the G2 refurbishment project;
- Component environmental qualification requirements;
- List of components important to safety for the shutdown state;
- System engineer evaluation (Expert judgment)

Each one of those sources provides decision criteria, which were tailored for specific assumptions and objectives related to a particular project. Thus, results from only one source of information may not be sufficient to identify CIS. However, the use of various assessments realized in specific contexts through different experts/tools provides an added value to the project, and ensures a multidisciplinary approach. It optimizes resources by avoiding re-evaluating all the components. Moreover, the methodology ensures coherence between the various evaluations realized across the plant. Figure #1 presents the developed methodology.



* See Section 6.3

Figure 1 : Methodology for SIS boundaries identification

The following section describes more in detail the main steps of the developed methodology.

6.1 SIS fault tree

Formatted: Bullets and Numbering

SIS fault tree models components required in fulfilling the SIS safety functions. Fault trees technique enables both evaluating the reliability of the systems, and calculating the importance of the basic events by using the importance measures factors. Literature review allowed determining that Risk Achievement Worth (RAW), and Fussel-Vesely (FV) are the most utilized importance measure factors. They are very helpful while using a probabilistic safety assessment (PSA). The Gentilly-2 PSA is still under development. Thus, it has been judged that a straight use of the importance measure factors from individual fault trees for a global assessment may not be quite appropriate in those circumstances. In fact, when there is no PSA, basic events are compared to a specific top event. The later does not assess the global level of risk. Consequently, it may be challenging to compare importance measures factors obtained from various individual fault trees. However, knowing that a fault tree is obtained as a result of an extensive reliability study of the system, it may be reasonably assumed that the basic events, which are significant for the system failure, are modeled in the fault tree.

Thus, all the components that are modeled in the SIS fault trees are automatically incorporated into the CIS list, since they contribute significantly to the safety function. Since all the fault trees across the station are not necessarily realized with the same level of details, it is important to consider other decision criteria. In this case, it becomes possible that a component, which is not modeled in a specific SIS fault tree, be incorporated into the CIS list. This is coherent with the risk informed approach, which considers qualitative and quantitative insights in a criticality analysis.

In the case where a component belonging to a support system is modeled in a mitigation SIS fault tree, and the same support system is categorized as a SIS, the component is integrated into the CIS list of this support system. Otherwise, those components are incorporated into the CIS list of the mitigation SIS.

6.2 Criticality safety assessment by the PMO project

The preventive maintenance optimization project at G2 is based on the WANO/INPO AP-913 “Equipment Reliability Process”. The first step of this process consists in scoping and identification of critical components. This activity is realized considering the following aspects: safety, production, costs and environment. A multidisciplinary team composed of a safety engineer, system engineers, an authorized control room operator, and a maintenance specialist performs this evaluation. The CIS identification considers the results of the safety evaluation only. If a component is evaluated important to safety by the PMO team, it is automatically incorporated into the CIS list of the SIS. The PM optimization is an ongoing practice, and the entire evaluation process is not still completed. Presently, the work is focused on the components that already have a maintenance program. It creates some inconveniences since the evaluation process is not finished. In the situation, where a component is not still evaluated through the PMO project, but is treated by the CIS identification, the obtained results of the later will be communicated to the PMO optimization team. This orientation allows both avoiding duplicate the component safety assessments, and providing a consistence between various projects including a resource optimization.

6.3 Environmental qualification project:

Environmental qualification project consists in an extensive evaluation of safety functions performed to determine component environmental qualification requirements. This activity has been done to ensure that systems are able to properly fulfill their safety functions in hostile environment conditions for LOCA events, and secondary sideline break (SSLB). An exhaustive review of the safety functions credited in both the safety report, and safety design matrices has been realized. As a result, components required to fulfill the safety functions have been identified. Components that have environmental qualification requirements, and are related to a safety function have automatically been incorporated to the CIS list of the SIS. The main inconvenient of this decision criterion is that only safety functions related to hostile environmental conditions have been analysed.

6.4 System Health Assessment

Each system of Gentilly-2 NPP has been evaluated for the refurbishment project. The objective of this assessment was to determine essential tasks for the refurbishment project. Only major components of each system were analysed, and a qualitative criticality judgment was done. The criticality assessment consisted in an evaluation by evaluating whether or not it is possible to operate for a long period of time without the component available Consequently, if a component has been identified as safety critical through the health system assessment it is automatically incorporated into the CIS list. The main inconvenient on this criterion is related to the fact that only major components have been evaluated.

6.5 Components important to safety during shutdown

A list of components important to safety in the shutdown state already exists at the Gentilly-2 NPP. This list identifies components that have to be closely monitored by the operators while the station is in a planned outage. This list allows quickly detecting component unavailability that reduces redundancy, or that compromises minimum safety requirements. Thus, if a component has been identified as shutdown safety important, it is automatically incorporated into the CIS list.

6.6 System engineer evaluation

This step consists in an evaluation of components that were not identified as CIS by one of the previous decision criteria. The system engineer is only evaluating the list of components, which are not identified as CIS. This approach helps in optimizing resources, and grants a credit to assessments previously carried out through various projects. A System Engineer assessment is qualitative, and is realized using both functional flowcharts, and conception drawings of the system. A significant number of system engineers will be involved in the SIS boundaries identification. Decision criteria have been developed for help assuring a consistence between various evaluations. If a component is qualified “CIS” by one of the listed criteria, it is incorporated to the CIS list. The criteria are as follows:

- Component has direct or indirect influence on a safety function credited in the safety envelope.
- Component has a high potential to cause an initiating event.
- Component failure requires a reactor trip, or will significantly reduce power over short term.

- Component failure affects reactor power control.
- Component failure significantly reduces redundancy of both a SIS, and defence-in-depth.
- Component is required in executing an emergency operating procedure (EOP).
- Component failure significantly reduces operator's capacity to recover an event that affects critical, and main monitoring parameters.
- Component failure significantly reduces capacity of a SIS to fulfill minimal performance requirements.
- Component failure affects more than one SIS, or may constitute a common cause failure.
- Component failure consequences are mitigated by a SSS.
- Component failure invalidates deterministic and probabilistic analysis assumptions.
- Component failure could cause an important transient that constitutes an important challenge for a safe exploitation of the plant.

As previously mentioned, these decision criteria are proposed for ensuring consistency between various system engineer assessments. This approach is consistent with the risk-informed decision making process. It highlights the importance of a structured expert judgment. Thus, it is possible to categorize a component as CIS through system engineer justifications even if it does not explicitly meet above listed decision criteria.

Components that are identified as related to the plant monitoring are automatically transferred to the monitoring category. An authorized person will evaluate those components after a complete evaluation of all the SIS. The authorized person will determine which components are essential for the safe exploitation of the plant. Further decision criteria will be defined to facilitate the evaluation of monitoring components. Components determined as important to safety by the authorized person will be integrated into the CIS list of a specific SIS. The latter includes components, which give a signal to the operators in an abnormal situation, or are required in a recovery action. Components, which belong to the SIS «Monitoring» category, will be only those ones, which contribute in keeping control room operable and habitable.

Once the whole evaluation process completed, each component will be categorized as related to safety (CRS), or important to safety (CIS). Only components that are related to monitoring are not evaluated in this stage. They will be classified, as CRS or CIS once the assessment by an authorized person is complete.

7. Case studies

This section present the results obtained through the methodology application for the Shutdown Systems #1 and #2, and the Emergency Core Cooling System (ECC).

7.1 Shutdown System #2

The methodology has been validated and improved through a pilot project on the Shutdown System #2. This system has been selected because it is a SSS, and it has been identified as the most adapted for the application of the methodology. In fact, the fault tree of the system is recently updated. Moreover, this system is closely monitored in the annual reliability report, and needed information is easily accessible. The realisation of the pilot project allowed validating the assumptions of the methodology, a better estimation of the effort required in evaluating a system. The pilot project also enabled optimizing the approach by taking into

account both lessons learned, and commentaries obtained from the system engineer. This step was necessary for optimizing further SIS evaluations, and evaluating resources required for remaining systems.

The application of the methodology on the shutdown system #2 resulted in 4 different lists: CIS, CRS, components related to monitoring, and components that are still under investigation. A thorough verification of the latter has to be realized on the field. Updates will be realized after the system engineer evaluates those components. Table 1 presents the results of the application of the methodology to the SDS#2.

Table 1: Results of SDS#2 boundaries identification

Categories	Number of components	Percentage
CIS	749	19 %
CRS	2232	58 %
Monitoring	724	19 %
To determine	163	4 %
Total	**3868**	**100 %**

The effort required to evaluate the 3868 components identified in the SDS#2 is estimated at 75 man-hours. Effort is distributed as follows: 25 hours for evaluation by the safety engineer (while working with the system engineer), 25 hours of evaluation through the system engineer (while working with the safety engineer), and 25 hours for project management, and data collection.

7.2 Shutdown System #1

Once the methodology validated through the SDS#2, SIS boundaries identification project started at the Gentilly-2 NPP. The Shutdown System #1 (SDS#1) is the second evaluated system.

Table 2 presents the results of the methodology application on the SDS#1.

Table 2: Results of SDS#1 boundaries identification

Categories	Number of components	Percentage
CIS	1256	34 %
CRS	1846	50 %
Monitoring	366	10 %
To determine	236	6 %
Total	**3704**	**100 %**

The effort required to evaluate the 3704 components identified in the SDS#1 is estimated at 55 man-hours. Effort is distributed as follows: 15 hours for evaluation by the safety engineer (while working with the system engineer), 15 hours of evaluation through the system engineer

(while working with the safety engineer), and 25 hours for project management, and data collection.

7.3 Emergency Core Cooling System

The Emergency Core Cooling system (ECC) is the third system evaluated. Table 3 presents the obtained results.

Table 3: Results of ECCS boundaries identification

Categories	Number of components	Percentage
CIS	1588	32 %
CRS	2534	51%
Monitoring	743	15 %
To determine	116	2%
Total	**4981**	**100 %**

The effort required to evaluate the 4981 components identified in the ECCS is estimated at 55 man-hours. Effort is distributed as follows: 15 hours for evaluation by the safety engineer (while working with the system engineer), 15 hours of evaluation through the system engineer (while working with the safety engineer), and 25 hours for project management, and data collection

8. Discussion

This section presents the main advantages and shortcomings related to the developed methodology:

Advantages:

- The methodology is based on previously realized assessments at the Gentilly-2 NPP. This approach optimizes resources utilization, and ensures consistency between the various plant projects.
- The presence of the system engineer in the decision-making process facilitates the implementation of the SIS categorization in the plant.
- The review of all the components allows identifying configuration management issues.
- The pilot project demonstrates that the methodology is applicable and allows obtaining results with a reasonable workload.
- The results will serve in the PMO project while evaluating the criticality of the components. They could also be used in a further AP-913 implementation.
- The obtained results define components to be integrated into the reliability database.

- The results could give insights required in improving reliability models.
- Since the methodology uses results/insights from various plant projects, it may be considered as a multidisciplinary approach.
- The methodology is consistent with risk-informed decision-making approach. It considers both deterministic, and probabilistic insights, and gives an important role to a structured expert judgment.
- The methodology allows evaluating the importance of components related to safe plant exploitation without using a PSA.

Shortcomings:

- Decision criteria are mostly qualitative.
- Several system engineers evaluate systems. Even if a set of decision criteria is defined, there might be some inconsistency in obtained results.
- It seems challenging for the system engineers to consider safety aspect only. As a result, more components could be integrated into the CIS list. This element is judged acceptable since it allows a conservative approach.
- The methodology is realised considering the S-98 regulatory standard implementation. It is not a global approach because it considers the nuclear safety aspect only. It will be challenging to change existing management rules related to CRS without performing a plant-wide evaluation of the components.

9. Conclusion

The main objective of this paper is to depict the methodology developed to identify the boundaries of the systems important to safety (SIS) at the Gentilly-2 Nuclear Power Plant (NPP), Hydro-Québec without using PSA. The SIS boundaries identification takes into consideration nuclear safety only. The work is done as a part of ongoing activities undertaken to comply with the S-98 requirements. The later standard is recently introduced into the Canadian regulatory framework.

The developed methodology integrates insights from previously realized specific projects at the station (environmental qualification, system health assessment, reliability studies, preventive maintenance optimization, outage management). Moreover, the methodology grants an important role to a structured engineering judgement. This way, one optimizes needed resources, and ensures a consistence between various plant projects, and their results. The approach used is also consistent with the Risk-informed decision-making process.

Components that are not identified as important to safety are systematically identified as related to safety. A global assessment process such as WANO/INPO AP-913 “Equipment Reliability Process” will be needed for modifying existing management rules for those components.

The methodology has been validated through Shutdown System #2 at the Gentilly-2 NPP, Hydro-Québec. The validation enabled a fine-tuning of the methodology, performing a better estimate of the effort required to evaluate a system, and identifying components important to safety of the SDS#2. The SIS boundary identification has also been completed for the Shutdown System #1 (SDS#1), and Emergency Core Cooling System (ECCS).

Tables 4 et 5 summarize both the obtained results, and effort required to complete the work.

Table 4: Summary results of three-system boundary identification

Categories	SDS#1	SDS#2	ECC
CIS	34%	19%	32 %
CRS	50%	58%	51%
Monitoring	10%	19%	15 %
To determine	6%	4%	2%

Table 5: Summary of effort needed (in man-hours) for three-system boundary identification

Categories	SDS#1	SDS#2	ECC
Safety Engineer (while working with the System Engineer)	15 h	25 h	15 h
System Engineer (while working with the Safety Engineer)	15 h	25 h	15 h
Project management, and data collection	25 h	25 h	25 h
Total:	55	75	55

Apart obtained results, the work done has allowed identifying both strong points, and shortcomings of the developed methodology. The lessons learnt will serve in further improvement of the entire approach while evaluating remaining systems important to safety.

10. References

1. CCSN, (2005), "Norme d'application de la réglementation S-98 Révision 1, Programmes de fiabilité pour les centrales nucléaires", Ottawa.
2. INPO (2001). "Equipment Reliability Process Description". AP-913, rev 1.
3. CAN/CSA, (1992). "Appendix A Guidelines for the Application of Safety-Related Systems, Overall Quality Assurance Program Requirements for Nuclear Power Plants", CSA N286.0-92
4. COG, (2005). "Risk-Informed Decision Making in the Canadian Nuclear Power Industry: Principles and Process, CANDU Owners Groups Inc. " COG-05-9010
5. EDF, (1998). "Classement des matériels importants pour la sûreté". Centre nucléaire de production d'électricité du Blayais.
6. EPRI, (1991). "Demonstration of Reliability Centered Maintenance". volume 1-3, NP-7233
7. EPRI, (1991). "Guidelines for the Safety Classification of Systems, Components, and Parts Used in Nuclear Power Plant Applications", NP-6895
8. EPRI, (1996). "The Maintenance Engineer Fundamentals Handbook", TR-106853
9. EPRI, (1997). "Property damage Risk Assessment Scoping Study", TR-108261
10. EPRI, (2002). "Reliability and risk Significance for Maintenance and Reliability Professionals at Nuclear Power Plants" 1007079
11. EPRI, (2003). "Critical Component Identification Process – Licensee Examples", TR-1007935
12. J.S; Seong, P.H. (2004). "A method for risk-informed safety significance categorization using the analytic hierarchy process and Bayesian belief networks". Reliability Engineering & System Safety 83, pp. 1 – 15.
13. Männistö, I. (2005). "Risk-Informed Classification of Systems, Structures and Components in Nuclear Power Plants", MSc Thesis, Helsinki University of Technology
14. NASA, (2000). "Reliability Centered Maintenance Guide for Facilities and Collateral Component"
15. NEI (2005). "CFR 50.69 SSC Categorization guideline", NEI-00-04 Revision 0, Washington DC.
16. Reliasoft. (2006). "Reliability Importance Measures of Components in a Complex System- Identifying the 20% in the 80/20 Rule". Reliability HotWire, Issue 66, juillet 2006
17. U.S. Department of Energy, (2003). "Guideline to Good Practices for Types of maintenance Activities at DOE Nuclear facilities", DOE-STD-1052-93
18. U.S. Department of Transportation, "Identification of Flight Critical System Components", Draft
19. Ramirez-Marques, J.E., Rocco, C. M., Gebre, B. A., Coit, D. W., Tortorella, M., (2006), "New insights on multi-state component criticality and importance", Reliability Engineering and System Safety, 91, pp. 894-904.
20. USNRC, (2005). "Integrated Risk-Informed Decision Making Process for Emergent Issues " U.S. Nuclear Regulatory Commission, LIC-504, rev. 0
21. USNRC, (2006). "Guidelines for categorizing structures, systems, and components in nuclear power plants According to their Safety Significance". U.S. Nuclear Regulatory Commission