Risk-Informed Applications and Online Maintenance in France and the United States

by

Edouard Verdier

Diplôme d'Ingénieur
Ecole Polytechnique, France, 2010

Submitted to the Department of Nuclear Science and Engineering
in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Nuclear Science and Engineering

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

February 2012

Signature of Author.....
Department of Nuclear Science and Engineering
December 22, 2011

Certified by.....
Michael W. Golay
Professor of Nuclear Science and Engineering
Thesis Supervisor

Certified by.....
Neil E. Todreas
KEPCO Professor of Nuclear Science and Engineering
and Professor of Mechanical Engineering (Emeritus)
Thesis Reader

Accepted by.....
Mujid S. Kazimi
TEPCO Professor of Nuclear Engineering
Chair, Department Committee on Graduate Students

Risk-Informed Applications and Online Maintenance in France and the United States

by

Edouard Verdier

Submitted to the Department of Nuclear Science and Engineering
on December 22, 2011, in Partial Fulfillment of the
Requirements for the Degree of
Master of Science in Nuclear Science and Engineering

Abstract

During the past twenty-five years, the US Nuclear Regulatory Commission has been progressing toward a more risk-informed, performance-based regulation. This regulatory framework has effectively supported the development of online maintenance practices. In France, while the safety authority has been encouraging particular risk-informed applications, PRA (Probabilistic Risk Assessment) techniques have not penetrated the nuclear regulatory framework and industry to the same extent.

After presenting relevant differences between the French and US nuclear industries and regulatory frameworks, the development and use of risk-informed applications in both countries are reviewed. In the United States, these techniques are usually well-accepted and have brought positive results regarding operational performance, plant safety and regulatory efficiency. In France, there have been in some cases difficulties regarding the acceptability of these techniques with the safety authority, but also within the operating company. While PRA results are commonly used in the US at the operational level through the use of risk-monitors, there appear to be in France obstacles to such practices.
Online maintenance regulations and practices are then presented. US technical specifications provide much flexibility to voluntarily enter technical specifications action statements for online maintenance. As a result, following the implementation of the Maintenance Rule, online maintenance has been increasingly applied, leading to operational as well as safety improvements. In France technical specifications are more restrictive regarding these aspects, and online maintenance of safety-significant systems is often not allowed or allowed under restrictive conditions. A case study concerning the maintenance of emergency diesel generators and emergency core cooling systems is presented to illustrate and study these points in more detail. Finally, possible directions to facilitate the implementation of an online maintenance strategy in France are identified, and their implications are discussed.

This study is part of a research project sponsored by EDF at MIT.

Disclaimer: This thesis presents analyses and opinions of the author, which are not endorsed by EDF.

Thesis Supervisor: Michael W. Golay
Title: Professor of Nuclear Science and Engineering

Acknowledgements

I would like to express my gratitude to all those who made this thesis possible. I am particularly grateful to my advisor Professor Golay, for his support, advice, patience and guidance throughout this project and my graduate studies. I also wish to thank my thesis reader, Professor Todreas, for his time and his valuable comments.

I am grateful to Gerard Labadie, for his guidance and cooperation during this project, and to all the people from the R&D division at EDF who contributed to this project, in particular Pascal Brac. I would like to extend my gratitude to Kenneth Kiper, from Seabrook Station, for his expertise and his frequent help throughout this project.

Finally, I want to thank my family and my friends for their invaluable support during my graduate studies.

Contents

List of Figures

List of Tables

List of Acronyms

AOT	Allowed Outage Time
ASN	French nuclear safety authority (Autorité de Sureté Nucléaire)
BSCT	Back-Stop Completion Time
BWR	Boiling Water Reactor
CCF	Common Cause Failure
CDF	Core Damage Frequency
CFR	Code of Federal Regulations
CRMP	Configuration Risk Management Program
DG	Diesel Generator
ECCS	Emergency Core Cooling Systems
EDF	Electricité de France
EDG	Emergency Diesel Generator
EPR	European Pressurized Reactor
EPRI	Electric Power Research Institute
EPS	Probabilistic Risk Assessment (Etude Probabiliste de Sûreté)
FSCT	Front Stop Completion Time
IAEA	International Atomic Energy Agency
ICDP	Incremental Core Damage Probability
ILERP	Incremental Large Early Release Probability
INPO	Institute of Nuclear Power Operations
IPE	Individual Plant Examination
IPEEE	Individual Plant Examination of External Events
IRSN	Radioprotection and Nuclear Safety Institute (Institut de Radioprotection et de Sûreté Nucléaire)
LB	Licensing Basis
LCO	Limiting Condition for Operation
LERF	Large Early Release Frequency
LOOP	Loss of Offsite Power
MSPI	Mitigating System Performance Index
NEI	Nuclear Energy Institute
NOED	Notice of Enforcement Discretion
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
OMF	Reliability Centered Maintenance (Optimisation de la Maintenance par la Fiabilité)
PBMP	Preventive Maintenance Basic Program
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
PWR	Pressurized Water Reactor
QHO	Quantitative Health Objective
RCM	Reliability Centered Maintenance

RFO	Refueling Outage
RFS	Basic Safety Rule (Règle Fondamentale de Sûreté)
RG	Regulatory Guide
RGE	General Operating Rules (Règles Générales d'Exploitation)
RHR	Residual Heat Removal
RICT	Risk-Informed Completion Time
RMAT	Risk Management Action Time
RMTS	Risk-Managed Technical Specifications
ROP	Reactor Oversight Process
RWST	Refueling Water Storage Tank
SBO	Station Blackout
SEPS	Supplemental Emergency Power Supply
SFCP	Surveillance Frequency Control Program
SR	Surveillance Requirement
SSCs	Structures, Systems and components
STE(s)	Technical Specifications (Spécifications Techniques d'Exploitation)
STI	Surveillance Test Interval
STP	South Texas Project
STS	Standard Technical Specifications
TAC	Combustion Turbine (Turbine à Combustion)
TS, Tech Specs	Technical Specifications
TSN	Nuclear Transparency and Safety
WENRA	Western European Nuclear Regulators' Association

Chapter 1

Introduction

1.1. Thesis objective

The work presented in this thesis has been conducted as part of a larger project sponsored by EDF on Nuclear Safety Regulatory Treatments in France and the United States. This thesis focuses on the comparison and the analysis of risk-informed applications and online maintenance practices in France and the US. Specifically, the objectives of this thesis are to:

- Compare the French and US regulatory frameworks applicable to probabilistic risk assessment (PRA), understand the main differences, analyze the development of risk-informed applications, and understand the differences in the status of these techniques in the two countries
- Compare general regulations applicable to maintenance in both countries, and the role of risk-information in the formulation and the justification of maintenance programs
- Analyze and understand the main differences in the regulation of online maintenance to explain the difference in the amount of online maintenance performed in each country
- Identify the implications of an online maintenance strategy
- Understand the ongoing evolutions regarding online maintenance regulation and practices in the US
- Identify possible directions to facilitate (if needed) the development of an online maintenance strategy, if EDF were to consider such a strategy (which is not currently the case).

1.2. Background

There are significant differences in the structure of French and US nuclear industries that have consequences at many levels on the observations and analyses conducted in this thesis.

1.2.1. US nuclear industry and regulatory structure

1.2.1.1. Nuclear safety authority

In the United States, the Atomic Energy Act of 1954 is the fundamental law regarding both civilian and military uses of nuclear materials. Under this act, a single agency (the Atomic Energy Commission) had responsibility of all uses of nuclear materials. The Energy Reorganization Act of 1974 split this responsibility, creating the US Nuclear Regulatory Commission (NRC) as an independent agency in charge of regulating the use of radioactive materials for civilian purposes.

The NRC regulates commercial nuclear power plants as well as other uses of nuclear materials (e.g. nuclear medicine) through licensing, inspection and enforcement of its requirements, to ensure that people and the environment are protected. The NRC is headed by five Commissioners who are appointed by the President and confirmed by the Senate for five-year terms.

The NRC has created 4 regions, overseeing a total of 104 power-producing reactors, and 36 non-power-producing reactors. In each power-producing reactor site there are Resident Inspectors, who monitor daily operations. The NRC has a staff of approximately 3,800 persons. In 2009, the NRC received a budget of 1,046 million dollars, distributed among nuclear reactor safety (75%), nuclear materials and waste safety (24%), and inspections (1%).

NRC's regulations are found in Chapter I of Title 10, "Energy", of the Code of Federal Regulations (CFR). In addition to these rules, the NRC issues Regulatory Guides (RG), which are intended to aid licensees to implement regulations, but they do not contain regulatory requirements. The NRC issues many other types of documents that are encountered throughout this thesis, among which can already be mentioned the NUREG-Series publications, which are reports or brochures on regulatory decisions, results of research, of investigations, or on any other technical and administrative information. The NRC conducts its own research programs,

often through contractors. Its work is also complemented through research and analyses by the Electric Power Research Institute (EPRI) and by licensees. In addition, The NRC works with standards organizations to develop consensus standards/codes on systems, equipment, or materials used by the nuclear industry, for example with the ASME (American Society of Mechanical Engineers) or the ANS (American Nuclear Society).

1.2.1.2. Reactor fleet

The US is the largest producer of nuclear energy in the world, accounting for about 20 % of its total electric energy generation. There are 104 reactors in operation at 65 sites, in 31 different states, operated by some 30 different operating companies. All commercial reactors are Light Water Reactors (LWR), with about two thirds of Pressurized Water Reactors (PWR) and one third of Boiling Water Reactors (BWR). There are about 80 different designs categorized according to their vendor: Westinghouse PWRs, General Electric BWRs, Combustion Engineering PWRs, and Babcock and Wilcox PWRs.

1.2.1.3. Organizations and Institutes

In addition to NRC and individual licensees, there are several organizations and institutes that play an important role in the US nuclear industry, in particular:

- EPRI (Electric Power Research Institute), an independent, utility-funded, non-profit research institute.
- NEI (Nuclear Energy Institute), a US nuclear industry lobbying group that represents the nuclear industry before the US congress and the NRC, and which conducts public communication activities.
- INPO (Institute of Nuclear Power Operations), a non-profit organization established by the US nuclear power industry after Three Mile Island (TMI) accident to promote best practices in the operation of US nuclear power plants.

1.2.2. French nuclear industry and regulatory structure

1.2.2.1. Regulatory structure

The legal framework applicable to nuclear activities has been fundamentally recast in 2006 with the publication of the "Loi relative à la Transparence et à la Sécurité en matière

Nucléaire (TSN)" (Nuclear Transparency and Safety Act, June 13, 2006), along with the implementation decree 2007-1557 (nov. 2, 2007), which constitutes the new base for nuclear regulation. It introduces an integrated system based upon a broader conception of nuclear safety that covers accident prevention and mitigation as well as public health and environment protection. The TSN Act will soon be complemented by the "arrêté INB" (in course of finalization), which will regulate the design, construction and operation of nuclear facilities. It will also transpose the WENRA reference levels (see below) into the French regulation.

The TSN Act establishes the ASN (Autorité de Sûreté Nucléaire), the French nuclear safety authority, as an independent authority in charge of regulating nuclear safety and radiation protection and informing the public in these areas; it concerns commercial plants as well as small-scale nuclear facilities (nuclear research facilities, nuclear cycle utilities, medical installations using ionizing radiations).

In this new framework, there are three main actors in the oversight of nuclear safety: the Parliament, the Government, and the ASN. The Parliament votes laws on nuclear safety and radiation protection, while the role of the Government is to promulgate decrees on nuclear safety and radiation protection as well as to take major decisions concerning nuclear utilities. Its action is based upon recommendations from the ASN. The government also consults specialized authorities such as the High Committee on Transparency and Information on Nuclear Safety (HCTISN) or the High Council on Public Health (HCSP).

The ASN acts in many different ways:

- It advises the Government on general regulatory matters and on individual decisions,
- It prepares regulatory documents for the Government,
- It takes decisions and prescriptions that are legally binding, as per the TSN act; it may take sanctions against utilities, close a nuclear facility, or set penalties,
- It grants individual authorizations and suggests others to the Government,
- Its inspectors oversee and control nuclear activities,
- It helps to manage emergency situations,
- It informs the public (e.g. about incidents at utilities, emergency situations ...).

For technical aspects, the ASN relies upon the expertise of the IRSN (Radioprotection and Nuclear Safety Institute) and the seven Permanent Groups of Experts (GP) (e.g. for reactors (GPR), factories (GPU), ...).

The ASN is run by a board of 5 commissioners, each appointed for six years. The board defines the general strategy. Contrary to the US, there are no resident inspectors for commercial nuclear power plants. Instead, the ASN is organized in territorial divisions that are in charge of the oversight of plants in a given region (these regions being much smaller than NRC's regions). Territorial divisions deal with most licensees' requests within their territory. ASN staff is composed of about 450 people, with roughly half working in territorial divisions.

In 2010, 460 inspections were performed in French NPPs. The utility remains in any case responsible for nuclear safety, while the ASN focuses on control. For activities with an intermediary importance in terms of safety and radiation protection, the ASN allows the licensee to be responsible for it if a systematic, internal control system is set up by the licensee. The ASN controls the licensee's internal control systems through inspections and analysis of periodic reports provided by the licensee, and can at any time suspend the overall process (called "Internal Authorization Process").

In 2008, the budget of the ASN was 43 million Euros (about 60 million dollars), and the budget of the IRSN related to work in support to ASN's action was 69 million Euros (about 97 million dollars), hence a total of about 157 million dollars if ASN and IRSN are grouped together.

1.2.2.2. ASN decision and guidance

The ASN supplements laws, decrees or orders with 'technical regulatory decisions", which are legally binding once validated by the relevant Minister, takes individual decisions regarding nuclear activities, and sets forth individual requirements.

Regarding regulatory guidance, the ASN used to issue Basic Safety Rules (RFS) concerning many different technical subjects, such as the use of PRA. RFS are recommendations, not legally binding, that define safety objectives and present practices that the

ASN considers acceptable to achieve these objectives. A licensee may decide not to comply with an RFS if he can demonstrate that the safety objectives can be achieved with alternative means that he proposes to implement. In some RFS, the ASN endorsed industrial standards, such as those developed by the AFCEN, an association of industrial companies (including EDF and Areva) that has produced the RCC standards series, which concerns design, construction and operation of electrical materials (RCC-E), civil engineering (RCC-G) and mechanical materials (RCC-M). Now, since passage of the TSN Act, the ASN is in the process of issuing Guides, still not legally binding, that may supersede some RFS.

Also, since all French nuclear power plants are operated by a single company, many technical rules governing design and operation have been set in letters to EDF, usually letters accepting or amending EDF's proposal, without being formalized in regulatory documents. However, one of the objectives of the new regulatory framework initiated by the TSN Act is precisely to make this framework more formal and more adapted to the emergence of new operators and reactor designs.

1.2.2.3. WENRA

The ASN is a member of the Western European Nuclear Regulators' Association (WENRA), which was originally created on the initiative of the French safety authority to examine nuclear safety in countries of Central and Eastern Europe desiring to join the European Union (EU). Nowadays, one of the main objectives of WENRA is to harmonize to some extent nuclear safety approaches in member countries, starting from the observation that, even though nuclear safety remains a national responsibility, a nuclear incident or accident can have consequences that go beyond national borders. WENRA has established "Reactor Safety Reference Levels" (Ref. [1]), primarily based upon IAEA Safety Standards, that member safety authorities have committed to implement in the short term, including the ASN. It has consequences on ASN's regulation, in particular regarding the use of probabilistic risk assessment, as explained later in this thesis. Also, WENRA has published a document called "Safety Objectives for New Power Reactors", so that new reactors to be built in Europe may offer improved level of protection and may have high and comparable levels of safety.

1.2.2.4. Reactor fleet

With 58 reactors at 19 different sites, France is the second largest producer of nuclear energy in the world, after the United States, and the nuclear sector generates about 75 % of total electricity produced in the country, which makes France the country that relies the most on nuclear energy. Contrary to the US reactor fleet, the French one is highly standardized: all reactors are PWRs, and there are only three main designs (or series):

- 900 MWe series, with three sub-designs: CP0, CP1 and CP2 (34 units, licensed from 1972 to 1982) (CP1 and CP2 are sometimes grouped under the designation CPY)
- 1300 MWe series, with two sub-designs: P4 and P'4 (20 units, licensed from 1978 to 1985)
- 1450 MWe series, with only one design called N4 (4 units, licensed from 1984 to 1993).

All these reactors are operated by a single company, EDF (Electricité de France), owned 84% by the state.

1.2.3. Fundamental differences

There are major differences between the French and US nuclear industries and regulatory frameworks. The US industry is made up of plants of many different reactor designs, operated by many companies, while the French nuclear fleet is highly standardized and operated by a single company, EDF. A consequence of this structural difference is the relationship between the regulator and the licensee(s) in both countries:

- In the US, this relationship is based upon very formalized, generic regulatory documents, as well as individual communications with each licensee, all of these documents being made available to the public on NRC's website.
- In France, little regulation was formalized up to recently, and most of the regulations have been based upon a less formal, direct technical dialogue between the ASN and EDF. This point has been particularly evoked in the process of harmonization of nuclear safety regulation within WENRA (see Section 1.2.2.3). An advantage of this process was the possibility for the ASN to focus on this single operating company, which facilitated communication and applicability of the regulation. However, it also made the process less favorable to the entry of a new operating company or to the emergence of different reactor designs, and it made this process less transparent to the outsiders, since few

regulatory documents were formalized and made public by the ASN. However, as is explained above, these aspects are currently evolving due to the significant modifications of the regulatory framework initiated by the promulgation of the TSN Act.

As a result, safety regulation in the US is conducted largely in public, using abundant documentation that can easily become involved in public litigation. It has usually not been the case in France, where most of the regulation has been conducted outside the public view between the safety authority and the licensee. However, the TSN Act has modified this issue significantly: information regarding risks and risk reduction measures undertaken at the different NPPs must now be publicly available. In particular, for the past five years, the ASN has been publishing on its website all the letters that it sent to utilities regarding Permanent Group of Experts meetings, results of inspections...

Another important difference is the existence in France of Periodic Safety Reviews. Such safety reviews are required by the European Directive on nuclear safety (2009), with the objective of continuous improvement of safety. This requirement also appears in IAEA Fundamentals and IAEA Safety Standards, and in the TSN Act.

Also, the difference of budget between the NRC and the ASN plus IRSN taken together should be noted: the budget of the NRC is nearly seven times the budget of the combined ASN plus IRSN (considering only the part of IRSN's budget that is related to its work in support of ASN's actions), while the US reactor fleet is less than twice as large as the French one.

The status of the IRSN is also particular: while in the US the NRC pays National Laboratories and other contractors for work in support of regulatory actions, the IRSN has its own budget. The relationship between the safety authority and its research support is therefore different between France and the United States. In particular, the IRSN often performs research on its own initiative, and results can be presented to the ASN to suggest regulatory actions. In consequence, the IRSN should not be seen as a mere research support working in background of ASN's action. For many technical subjects, it works directly with EDF, and final regulatory decisions are generally primarily based upon its conclusions.

With a single operating company in France, there is no need for a lobbying group such as NEI to represent the industry before the safety authority, or for an organization such as INPO to promote best practices among utilities (at least at a national level). In France, these roles are hold by some centralized departments within EDF. Therefore, there are many fewer actors in the French nuclear industry than in the US one.

Chapter 2

Probabilistic Risk Assessment – Basic Overview

2.1. Introduction

2.1.1. Deterministic background

At the beginning of the nuclear industry, no attempt was made to quantify the risks generated by nuclear power plants, mostly because no experience was available upon which to base this quantification. In order to address underlying uncertainties, deterministic safety principles have been implemented, employing conservative design and operational policies, significant safety margins, design basis accidents (DBAs) and defense-in-depth.

A major drawback of these deterministic principles is that the implicit risk remains unquantified. Safety margins are used and redundancy is implemented without quantifying the underlying effects upon risk. In addition, it is assumed that if the plant is able to withstand serious accidents, then it will be able to withstand less serious ones, which is not necessarily obvious or true. Therefore specific defenses against smaller, but more frequent accidents are not developed. Designers may focus on serious accidents that are highly unlikely while they may neglect less challenging ones that are much more likely to occur, and that could provide a greater contribution to the plant risk. Furthermore, deterministic principles rely mostly upon expert judgments, often without a formal, technical basis of the choices they make.

2.1.2. Probabilistic Risk Assessment

PRA is defined by the NRC as "*a systematic method for assessing three questions that the NRC uses to define "risk". These questions consider (1) what can go wrong, (2) how likely it is, and (3) what its consequences might be*". PRA enables one to calculate the failure probability of systems or lines of defense, using a systematic method typically based upon the following steps:

- Identification of relevant initiating events
- Development of event trees that describe the possible sequences of events starting from the initiating events
- Evaluation at each step of the event tree, of the failure probabilities using fault trees. The final outcome (= the end state) is assumed, and possible sequences leading to this outcome are identified and quantified.

2.1.2.1. Usefulness of PRA

PRA presents many benefits, in particular to compensate for some of the weaknesses of the deterministic basis mentioned above. Without trying to provide an exhaustive list of all potential benefits of PRA, we present in this section some of the most recognized successes of this approach, based upon Ref. [4].

Benefits in design

The use of PRA can have a very beneficial effect at the design stage. It enables a designer to identify deficiencies in the design of a new reactor and to compare the effect upon safety of different design alternatives. It also enables one to quantify the risk level of the new design and thus to compare it with current or past reactor designs. PRA can be used to verify that plant risk is sufficiently "balanced" in the sense that it is not dominated by a particular kind of initiating event or accident sequence.

Benefits in operation

PRA techniques can help one identify and compare specific improvements in maintenance, testing and emergency procedures that may have a cost-beneficial effect upon safety. It can be a very powerful tool to supplement traditional, deterministic techniques in justifying hardware or procedure modifications. It can be used to assess the effect of component

or system unavailabilities and help to identify the best course of action, whether these unavailabilities are planned or unplanned.

Staff capabilities

The use of PRA results has enabled improvement of the safety cultures among engineering and operation personnel. When exposed to these techniques, they are more capable of understanding the interdependencies among different systems and their combined effect upon the plant risk level. Also, PRA insights can be incorporated into operator training programs in order to enhance the ability of operators to diagnose and respond to incidents.

Interaction with the regulator

PRA can be a powerful tool to improve communication and interaction between licensees and the regulator. It can enable utilities to respond more efficiently and effectively to regulator's concerns, and, as mentioned above, it can be particularly useful in justifying hardware and procedure modifications or in requesting changes in licensing basis.

2.1.2.2. PRA limitations

In spite of its many benefits, PRA also presents particular limitations of which one must be aware. In particular, there are three domains where further developments are still needed:

- Quantification of human reliability
- Quantification of common cause failure (CCF) probabilities. A CCF is defined as the simultaneous failure or unavailability of more than one component due to shared causes other than the dependencies already explicitly modeled in the PRA logic model [4].
- Quantification of component aging.

During the last 20 years, significant progress has been made concerning each of these difficulties, through the development of models to deal with human errors and the development of large databases to evaluate parameters in CCF models and the effects of plant aging. In addition, codes and standards have been developed to help licensees and regulators ensure that PRA models are of adequate quality, both in terms of model complexity and data accuracy.

Another major issue when using PRA insights concerns uncertainties. Quantitative results cannot be used without having some information about the underlying uncertainties, with a level

of detail that must be consistent with the role of these results in the decision-making process. Details concerning this issue can be found in Section 2.4.

2.1.3. Three PRA levels

Level 1 PRA

A Level 1 PRA analyzes how initiating events can develop into accidents that lead to core damage. The concept of "core damage" (also called "severe accident") is defined by the NRC in NUREG-1150 as the uncovering of the core by coolant, without imminent recovery. A distinction is made between PWR and BWR:

- For PWR: uncovering of the top of the active fuel (without imminent recovery)
- For BWR: water level less than 2 feet above the bottom of the active fuel (without imminent recovery).

A Level 1 PRA consists of the following activities: initiating event analysis, event tree construction, fault tree construction, accident sequence probability quantification. The main product of a Level 1 PRA is the Core Damage Frequency (CDF).

Level 2 PRA

Starting from the results of the Level 1 PRA, a Level 2 PRA consists of accident progression and source-term analysis, which yields the fractions of the inventory of radioactive materials released from the plant.

One product of a Level 2 PRA that is commonly used is the Large Early Release Frequency (LERF), defined by the NRC in RG 1.174 as "*the frequency of those accidents leading to significant, unmitigated releases from containment in a time frame prior to effective evacuation of the close-in population such that there is a potential for early health effects*".

Level 3 PRA

A Level 3 PRA (also called "consequence analysis") considers the full range of consequences caused by the dispersion of radioactive materials into the environment. It yields a set of consequence measure values for each source term group, such as early fatalities, latent cancer fatalities, population dose, land contamination... These consequences depend upon many

factors, including the population that lives in the vicinity of the plant, evacuation plans, path of the radioactive plume (impacted by wind speed and direction, rainfalls and snowfalls).

2.2. PRA basics

2.2.1. Event tree and fault tree

A Level 1 PRA is usually based upon the association of event trees and fault trees. Event trees enumerate sequences leading to an accident for a given initiating event, while fault trees are used to define how actions in the event tree can fail and to compute the frequency of such failures. A fault tree consists of a top event, basic events and logical operators.

2.2.2. Reliability, availability and failure rates

The reliability *R(t)* of a system is defined in [4] as the probability that this system will perform as required until time t, i.e.:

$$R(t) = P(T \geq t) = \int_t^{\infty} f(t')dt' \tag{2.1}$$

where *T* is the time of failure of the system and *f(t)* is the probability density function associated with *T*. The availability *A(t)* of a system is defined in [4] as the probability that this system will be operational at time t, regardless of its operability at previous times. If the system is not subject to any maintenance, the availability is defined with a formula similar to the one given for *R(t)*. In the literature, reliability and availability are sometimes used interchangeably, but one usually uses the term availability for a standby system and the term reliability for an operating system. The reliability or availability is needed for each basic event in a fault tree.

The (conditional) failure rate of the system is then defined as:

$$\lambda(t) = \lim_{dt \to 0} \frac{P(t \leq T \leq t + dt | T \geq t)}{dt} = -\frac{1}{R(t)} \frac{dR(t)}{dt} \tag{2.2}$$

(or similarly with the availability). If the failure rate is constant, the reliability is then simply given by $R(t) = e^{-\lambda t}$ (similarly for the availability).

Whether the failure rate of a component is taken as a constant or as a function of the time, some parameters need to be evaluated, which can be done based upon failure data and/or expert judgment. These parameters can be described either as fixed values (point estimates) or as random variables associated with particular probability density functions. If point estimates are used, they can be evaluated using experimental failure data and methods such as the method of moments or the method of maximum likelihood. If one wishes to describe these parameters as random variables or to combine expert judgment with experimental data, a Bayesian approach can be used.

2.2.3. Minimum cut sets and risk importance measures

In a fault tree, a minimum cut set (MCS) is a cut set that does not contain a smaller cut set, while a cut set is defined as a set of basic events in the fault tree that causes the top event to occur. MCS are highly useful tools in risk analysis. Indeed, the probability of occurrence of the top event in a fault tree is given by $P(Top\ Event) = P(\cup_i MCS_i)$.

For each component i, several risk importance measures can be computed using the PRA model. In particular:

- The Fussel-Vesely value: it is defined as the risk generated by the MCSs where the component i is involved, normalized by the nominal risk:

$$FV_i = \frac{R(MCS_{i,1} + \cdots + MCS_{i,n})}{R_{nom}} \tag{2.3}$$

  It enables one to identify the components that contribute the most to the total risk.

- The Risk Achievement Worth (RAW): it is defined as the total risk assuming that the component i is unavailable ($q_i = 1$), normalized by the nominal risk:

$$RAW_i = \frac{R_{tot|q_{i=1}}}{R_{nom}} \tag{2.4}$$

  It enables one to identify components that must be kept reliable to avoid a significant risk increase.

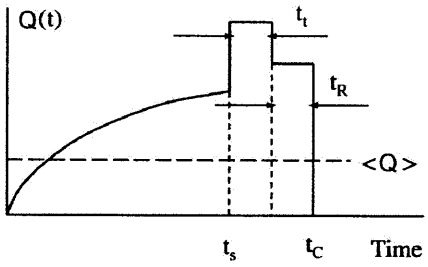
- The Risk Reduction Worth (RRW): it is defined as the nominal risk divided by the total risk where the component i is assumed to be always available ($q_i = 0$):

$$RRW_i = \frac{R_{nom}}{R_{tot|q_{i=0}}} \tag{2.5}$$

It enables one to identify which components are more valuable for improvement.

2.3. Effect of surveillance

The effect of surveillance tests on a system can be quantified, using the concept of availability, or unavailability $Q(t) = 1 - A(t)$. For a system that undergoes a single kind of test at a given period, the unavailability can be modeled as shown on Figure 2-1.



On this figure, t_s is the duration of standby, t_t is the duration of the test, and when necessary, t_R is the duration of repair, where repair is needed at a frequency f_R (i.e. f_R is the fraction of tests for which repair is needed). Then, for each interval, the unavailability is given as follows:

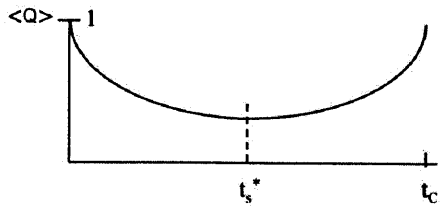
Figure 2-1 : Effect of testing on the unavailability

- For $t \in [0, t_s]$: $Q(t) = 1 - e^{-\lambda t} \approx \lambda t$ for λ taken as a constant and $t \ll 1/\lambda$
- For $t \in [t_s, t_s + t_t]$: $Q(t) = 1$
- For $t \in [t_s + t_t, t_s + t_t + t_R]$: $Q(t) = f_R$

The mean unavailability over a cycle can then be simply computed as:

$$\langle Q \rangle = \frac{1}{t_C} \cdot \left[\frac{\lambda t_s^2}{2} + t_t + f_R t_R \right] \tag{2.6}$$

By minimizing $\langle Q \rangle$, one can find an optimal value for t_s: $t_s^* = \left[\frac{2(t_t + f_R t_R)}{\lambda} \right]^2$ (see Figure 2-2).



This optimum shows well that a balance must be found between the positive effect of testing on the unavailability and the fact that, when the system is tested, it is completely unavailable ($Q = 1$).

Figure 2-2 : Optimal surveillance period

In this simple example, it was assumed that the surveillance test fully reset the unavailability of the system to zero. It is however not always the case.

2.4. Uncertainties

PRA results cannot be used without paying some attention to the underlying issue of uncertainties. The discussion presented in this section is based upon Ref. [6].

2.4.1. Aleatory and Epistemic uncertainties

Uncertainties can by classified into two different categories that have been named aleatory and epistemic uncertainties.

Aleatory uncertainty is related to events or phenomena being modeled as stochastic, or random. For example, the time of failure of a given system can be modeled as stochastic, with a probability density function that can be determined to model this "uncertainty". Of course, this is just a modeling treatment, since there is nothing intrinsically random associated with this event (we are not dealing with quantum phenomena, which are intrinsically random), as far as we know. This treatment is just a way to deal with some unknowns of the system, for example non-visible defects in the system varying from one system to another (while macroscopically speaking, these systems would be considered to be strictly identical), or small variations in the use of these systems during their lifetimes. Aleatory uncertainty is considered to be somehow "natural", and there is nothing one can do for a given system to reduce it, one can only refine the stochastic modeling of these systems (type of model, model parameters ...). It is this aspect of uncertainty that gives the term "probabilistic" in the name PRA, in which phenomena are modeled as random: failure rates, human errors, transition to one scenario or another ...

Epistemic uncertainty, however, is not intrinsic to the system, but reflects the analyst's confidence in the prediction of its PRA model, in the adequacy of the modeling of the different phenomena, and in the scope and the level of details of its PRA. For example, some random phenomenon may be modeled with a binomial or Poisson law, with some success, but the phenomenon is not strictly speaking governed by such a law, this is just a modeling treatment, more or less suitable (see "model uncertainty", Section 2.4.3). Likewise, when a mathematical model is thought to be appropriate for a given phenomenon, it is defined with some parameter(s),

for which there are also uncertainties (see "parameter uncertainties", Section 2.4.2). And so on. But contrary to Aleatory uncertainty, even though epistemic uncertainty cannot be completely eliminated, it (or at least some components of it, see below) can be reduced. Depending upon the applications of the PRA results, more or less (epistemic) uncertainty concerning the results may be acceptable, but these uncertainties have to be assessed, quantitatively or qualitatively, to the extent feasible.

What follows in this section concerns epistemic uncertainty, which can be broken down into several components, among which are Parameter Uncertainty, Model Uncertainty, and Completeness Uncertainty (which can be regarded as one aspect of model uncertainty).

2.4.2. Parameter Uncertainty

In order to develop the PRA logic structure or to represent the basic events of this structure, risk analysts use mathematical models that are defined by one or several parameters. Assuming that these models are appropriate (which is not completely true, see "model uncertainties"), the numerical values of these fundamental parameters are not perfectly known, and uncertainties will be associated with these values used in the PRA model. In order to deal with these uncertainties, analysts will typically establish probability distributions concerning the value of these parameters (this is somehow a second level of uncertainty, or an uncertainty on the uncertainty, the first level being the aleatory uncertainty of the modeled phenomenon). Once the uncertainty on each PRA model parameter has been assessed, elementary uncertainties can be propagated through the PRA structure in order to obtain the resulting probability distribution on the results of the calculation (e.g., CDF or LERF).

2.4.3. Model Uncertainty

The state of knowledge about the occurrence of some events or phenomena is often incomplete, and there may be different opinions concerning how some models should be formulated, for example to model complex matters such as common cause failures or human reliability, which gives rise to model uncertainty.

Different approaches have been suggested to address that kind of uncertainty, depending upon the specific case that is studied. In some cases where alternative models are well defined, model uncertainty can be addressed by using discrete probabilities over the alternative models that are proposed, based upon the confidence in the appropriateness of each of these models. Another approach that is used to address model uncertainty consists of modifying a defined model using an adjustment parameter to cover the different retained models. A probability distribution can then be determined for this adjustment parameter, and uncertainties can then be propagated in the exact same way as in the case of parameter uncertainty. Such approaches are however not always feasible, and different kind of sensitivity studies can be performed to assess numerically the impact on final results of some model uncertainties. Model uncertainty can also be addressed qualitatively, based upon specialists' understanding of the contributors to the results and how these results are altered by changes in assumptions or models.

2.4.4. Completeness Uncertainty

This "uncertainty" refers to the limitation in the scope of the probabilistic assessment. This limitation is sometimes chosen (e.g. to simplify the problem), sometimes imposed by the level of knowledge and understanding of particular systems or phenomena. Because it reflects an unanalyzed contribution, it appears very difficult to analyze that kind of uncertainty in a pragmatic, systematic manner. The choice of scope and level of details will often be based upon expert appreciations and experience feedbacks. One way to address some aspect of completeness uncertainty has been to build increasingly elaborate models to the point that the results become sufficiently insensitive to certain parts of the model. This practice does not guarantee adequate completeness, but it provides a procedure to indicate a minimum level of needed model development.

Chapter 3

Use of PRA in the US – Background

3.1. Historical Perspective

The first PRA study performed to assess the safety of nuclear reactors was the so called Reactor Safety Study, or WASH 1400, published in 1975, from an AEC project led by Professor Norman Rasmussen. Surprisingly, this first PRA was a Level 3 analysis, while Level 3 PRAs have not been very common until recently. The work of this report examined the events that may occur during a severe accident, as well as their radiological consequences and the probabilities of occurrence of these events, using a fault tree and event tree approach. The general conclusion of this study was that the risk to the individual posed by nuclear power stations was acceptably small, compared with other tolerated risks. In particular, it estimated the risk of core meltdown at 1/20,000 ry^{-1} (= per year and per reactor).

Prior to this study, it was usually thought that large LOCAs (Loss of Coolant Accidents) were the dominant contributors to plant risk, hence significant efforts were made to avoid or mitigate this kind of event. The CDF was also thought to be extremely low (~10^{-8} ry^{-1}). The Reactor Safety Study refuted these beliefs: it established that small break LOCAs and transients were the major contributors to the risk, while the CDF was estimated to be around 10^{-5} – 10^{-4} ry^{-1}.

Even if it was much criticized for its understatement of the uncertainties of the method, WASH 1400 established the use of PRA in the nuclear industry, in the US as in many other countries, since its methodology was considered useful and powerful.

The methods of PRA used in WASH 1400 have been greatly developed since its publication, especially after the TMI accident (1979). Indeed, this event was similar to a small

break LOCA, which the Reactor Safety Study had identified as a risk dominant class of events. Most US PRAs were developed by the licensees in the 1990s in response to NRC's Generic Letter 88-20 (ref. [14]), which required licensees to perform an Individual Plant Examination (IPE) for severe accidents associated with internal events (including internal flooding but not internal fire). Supplement 4 to the Generic Letter requested licensees to perform an Individual Plant Examination of External Events (IPEEE) for severe accidents associated with external events and internal fire events. Since the completion of the IPE and IPEEE programs, licensees have continued to update their PRAs to reflect plant modifications (many of which involved improvements identified by the IPEs and IPEEEs) and current operational experience. Five of the IPEs were the basis for the 1990 NUREG-1150 study [5] (see Section 3.3). The NRC has also developed SPAR models (Standardized Plant Analysis Risk) for each plant, which are Level 1 PRAs that the NRC uses for different applications, in particular:

- Evaluation of the significance of inspection findings, in the framework of the ROP (Reactor Oversight Process). These PRAs are also used to support inspection planning for both baseline inspections and supplementary inspections.
- Identification and prioritization of modeling issues to support NRC efforts to improve PRA quality.
- Providing support to risk-informed reviews of licensing applications.

3.2. The Safety Goals

3.2.1. Safety Goals Policy Statement

The policy statement "*Safety Goals for the Operations of Nuclear Power Plants*" [7] was published in 1986. Its objective is to "establish goals that broadly define an acceptable level of radiological risk". This policy statement resulted from the recommendations of the TMI accident commission. In this document, the NRC establishes two qualitative safety goals that are supported by two quantitative objectives, based upon the principle that "nuclear risks should not be a significant addition to other societal risks". This policy statement was also developed to lead to a "more coherent and consistent regulation of nuclear power plants, a more predictable regulatory process, a public understanding of the regulatory criteria that the NRC applies, and

public confidence in the safety of operating plants". More specifically, the two qualitative goals of the policy statement are as follows:

- "Individual members of the public should be provided a level of protection from the consequences of nuclear power plant operation such that individuals bear no significant additional risk to life and health."
- "Societal risks to life and health from nuclear power plant operation should be comparable to or less than the risks of generating electricity by viable competing technologies and should not be a significant addition to other societal risks."

In order to support these qualitative goals and to demonstrate that they are being met, the Commission has established two quantitative objectives, which are directly related to the use of PRA:

- "The risk to an average individual in the vicinity of a nuclear power plant of prompt fatalities that might result from reactor accidents should not exceed [0.1 percent] of the sum of prompt fatality risks resulting from other accidents to which members of the U.S. population are generally exposed."
- "The risk to the population in the area near a nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not exceed [0.1 percent] of the sum of cancer fatality risks resulting from all other causes."

The vicinity of the plant is described as the area within a mile from the plant site boundary.

3.2.2. Subsidiary Goals

In the document SECY 89-102, *Implementation of the safety goals* (1990) [9], the NRC endorsed subsidiary objectives concerning CDF and LERF. Such objectives are usually thought to be easier to address than the quantitative health objectives (QHOs) presented above, because they do not require a Level 3 PRA. However, they are more difficult to justify from a societal point of view than quantitative health objectives. These subsidiary objectives are:

- The CDF should be less than 10^{-4} ry^{-1}
- The LERF should be less than 10^{-5} ry^{-1}.

These goals are also called "surrogate objectives" because they may be used as alternatives to the QHOs. However, there is no strict equivalence between the two sets of

objectives, and the subsidiary objectives are generally thought to be more conservative than the original QHOs, i.e., some plants meeting the QHOs may not meet the subsidiary objectives.

The subsidiary goals do not have the status of fundamental safety goals. In 2004, the NRC explained that: "This goal [= the CDF subsidiary goal] has been determined by the staff to be a useful benchmark, but is not a Commission-approved safety goal" [12]. However, in [10], it had been stated that "the CDF of 10^{-4} is by de facto already used as a fundamental Commission goal".

3.3. NUREG-1150

The study NUREG-1150 [5], published in 1990, may be seen as an improvement of the original Reactor Safety Study (WASH-1400). It is based upon the results of five plant-specific PRA studies, serving as a basis for the IPE program started in 1988, in which the NRC requested information on the assessment of severe accidents vulnerabilities by each licensed nuclear power plant. This IPE could be done either with PRA or with other "approved means". Virtually all licensees performed their IPE with PRA.

The objectives of NUREG-1150 were to provide a "current assessment of the severe accident risks of five nuclear power plants of different designs" (2 BWRs and 3 PWRs). One major objective was to update the results of WASH 1400, including this time quantitative estimates of risk uncertainty, in response to a principal criticism of WASH 1400. Another main objective was to assess the performance of these reactors regarding the Safety Goals.

In this study, only initiating events while the reactor is at full-power operation were considered. For two of the five plants, internal and external (earthquake, fire ...) initiating events were considered, and for the remaining three, only internal events were addressed. The main results concern:

- Accident frequency estimations (Level 1 PRA): total CDF (from internal events, and external events when estimated), contribution of some plant damage states (station blackout, ATWS, LOCA ...), measure of the importance of individual events.
- Accident progression, containment loading, and structural response analysis.

- Analysis of radioactive material transport: produces an estimate of the radioactive release magnitude, with associated energy content, time, elevation, and duration of release.
- Offsite consequence analysis (Level 3 PRA): analysis of transport and dispersion of radioactive material, analysis of the radiation doses, analysis of dose mitigation by emergency response actions, calculation of health effects.

Globally, NUREG-1150 determined that the five power plants met NRC Safety Goals with some margin.

3.4. Policy Statement on the use of PRA

3.4.1. Background of the policy statement

This Policy Statement [8], entitled "*Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities*", was published in 1995. It is a major document concerning the use of PRA in the US nuclear industry, and may to some extent be compared to the French RFS [16] presented in Section 4.3. In this document, the NRC states that "a probabilistic approach to regulation enhances and extends [the] traditional, deterministic approach", in the sense that it enables the "consideration of a broader set of potential challenges to safety; [it provides] a logical means for prioritizing these challenges" on the basis of risk significance, operating experience, engineering judgment; and it allows the "consideration of a broader set of resources to defend against these challenges".

3.4.2. Content of the policy statement

In this document, the NRC emphasizes that PRA application constitutes an extension and enhancement of traditional regulation rather than a separate and different technology. Currently, the NRC uses PRA techniques as an integral part of the Design Certification review process for new reactor designs.

The two most important statements in this policy statement are as follows:

- "The commission believes that an overall policy on the use of PRA in nuclear regulatory activities should be established so that the many potential applications of PRA methodology can be implemented in a consistent and predictable manner that promotes regulatory stability and efficiency and enhances safety."
- "The use of PRA technology should be increased in all regulatory matters to the extent supported by the state-of-the-art in PRA methods and data and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy."

3.4.3. An extension and enhancement of traditional regulation

In this Policy Statement, the NRC presents some of the advantages of PRA techniques as a complement to the traditional deterministic approach. First, PRA addresses a broad spectrum of initiating events, and mitigating system reliability is then assessed, including the potential for multiple and common cause failures. Therefore, this treatment goes beyond the single failure requirements of the deterministic approach. PRA can also be used to eliminate unnecessary conservatism and to support new regulatory requirements. In addition, PRA enables one to evaluate whether nuclear facilities meet the quantitative probabilistic guidance of the Safety Goals. The PRA framework is also a powerful tool for logically and systematically evaluating the importance of uncertainties.

3.5. Use of PRA for plant-specific changes to licensing basis

3.5.1. Introduction

Regulatory Guide 1.174 [6] entitled "*An approach for using Probabilistic Risk Assessment in Risk-Informed decisions on plant-specific changes to the Licensing Basis*" (1998) is an example of the many PRA applications that have been promoted after the promulgation of the policy statement described in Section 3.4. This RG describes what the NRC considers to be an acceptable method to assess the nature and the consequences of permanent Licensing Basis (LB) changes, when the licensee is required or chooses to support this modification using risk information. It is important to note that this guidance does not preclude other approaches for requesting LB changes. It presents PRA as an efficient tool for justifying such requests that is

consistent with the Safety Goals policy statement. In this RG, the NRC presents a policy that would allow only small risk increases, consistent with the Safety Goals, and only when it is reasonably assured that sufficient defense-in-depth and sufficient margins are maintained.

The approach described in this guide supports NRC's "desire to base its decisions on the results of traditional engineering evaluations, supported by insights (derived from the use of PRA methods) about the risk significance of the proposed changes". Once again, PRA is meant to complete and support traditional engineering methods, whether it is based upon quantitative or qualitative results. Key principles of the approach are as follows:

- The proposed change is consistent with the defense-in-depth philosophy.
- The proposed change maintains sufficient safety margins.
- The risk increase (if any) is small and consistent with the Safety Goals.
- The impact of the proposed change should be monitored.

3.5.2. Use of risk information to support LB change requests

Licensee-initiated change requests that are consistent with official NRC regulations or guidance are generally not expected to be justified with risk information. However, when the request goes beyond NRC's positions (e.g. Technical Specifications changes not consistent with Standard Technical Specifications), risk information may efficiently support the request. In addition, if such risk information is not submitted, the NRC may require the licensee to complement its request with risk insights.

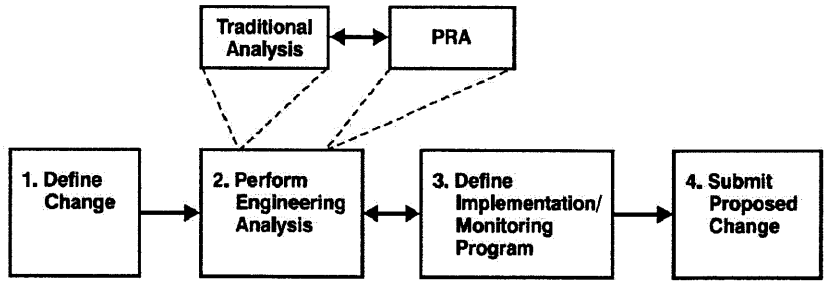


Figure 3-1 : Risk-informed request for plant-specific changes to Licensing Basis [6]

The role of risk information is to justify that proposed LB changes are consistent with the Safety Goals. However, as is explained in Section 3.2.2, the QHOs are often not easily usable, and in particular it would require a Level 3 PRA, whose uncertainties would have to be carefully studied. This is why RG 1.174 acceptance guidelines are based upon the subsidiary objectives (see Section 3.2.2) associated with CDF and LERF instead of the official Safety Goals. The main elements of a risk-informed request for plant-specific LB changes are summarized in Figure 3-1.

3.5.3. Consistency with defense-in-depth and margins

One role of the engineering analysis is to show that fundamental safety principles such as margins and defense-in-depth would not be compromised by the requested LB change, and should therefore be reevaluated to support the request.

Defense-in-depth has been an effective way to account for lack of knowledge and for uncertainties regarding materials and human reliability, and even with the advent of risk-informed techniques, defense-in-depth is still central to NRC's safety policy. In RG 1.174, the NRC gives some criteria to assess the consistency of proposed changes to the defense-in-depth philosophy:

- A reasonable balance is preserved among prevention of core damage, prevention of containment failure, and mitigation of consequences.
- Over-reliance upon programmatic activities to compensate for plant design weaknesses is avoided.
- Redundancy, independence and diversity of systems are preserved.
- Defenses against CCFs are preserved and the potential for the introduction of new ones is assessed.
- Independence of barriers is preserved.
- Defenses against human errors are preserved.

3.5.4. PRA quality

The PRA used to support the request for LB changes must have appropriate scope, level of detail and technical adequacy. This is particularly the case when the risk analysis constitutes a major piece in the justification of the request. Conversely, if traditional engineering arguments

are already convincing and sufficient by themselves to justify the request, the quality (or the justification of the quality) of the PRA could be reduced.

Different approaches may be used by the licensee to establish the technical adequacy of its PRA. RG 1.174 suggests two of them:

- Performance of a peer review of the PRA (by qualified reviewers)
- Use of industry PRA certification programs.

3.5.5. Acceptance guidelines

The quantitative guidelines are meant to be compared with full-scope PRA results (including internal and external events, full-power, low-power and shutdown operations), and the PRA should be of at least Level 2 in order to evaluate the LERF and the incremental LERF associated with the proposed changes. However, these guidelines may be adapted to deal with non full-scope, Level 1 PRA, as outlined later (see Section 3.5.6). In addition, during particular shutdown conditions when the containment function is not maintained, the LERF guidelines are not applicable. In such cases, RG 1.174 suggests that licensees use a more stringent guideline concerning the baseline CDF, e.g. by dividing numerical indications (see below, Figure 3-2) for the baseline CDF by a factor 10.

There are two sets of guidelines, one for CDF, one for LERF, and both should be met. The acceptance guidelines are summarized on Figure 3-2 and Figure 3-3. For each metric (CDF and LERF), different regions are established, with the value of the metrics prior to the realization of the proposed LB change shown along the x-axis (baseline CDF or LERF), and the increment in the corresponding metrics due to the proposed LB change shown along the y-axis (ΔCDF or ΔLERF). The NRC indicates that numerical values presented on these figures are only indicative, and these goals are intended to be compared with the actual mean values of the distributions.

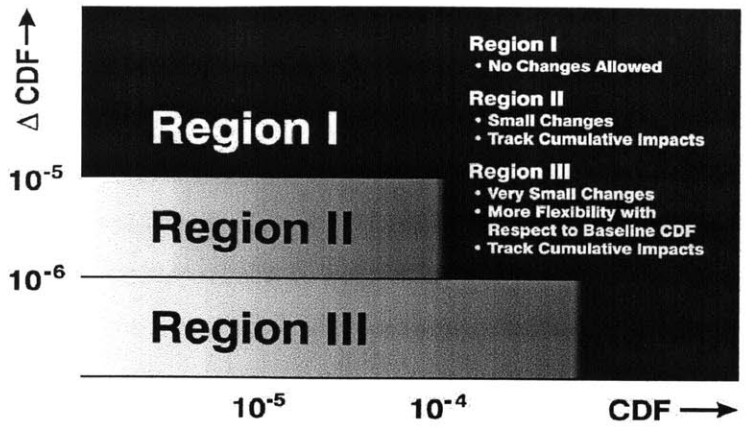


Figure 3-2 : Acceptance Guidelines for CDF [6]

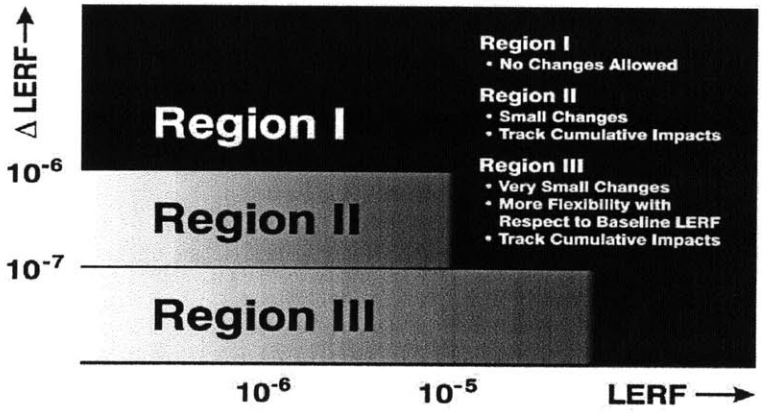


Figure 3-3 : Acceptance Guidelines for LERF [6]

In more detail, the acceptance guidelines are as follows:

1) For the CDF:

- If indications clearly show that $\Delta CDF < 0$, the proposed LB change is considered to have satisfied the principle of risk-informed regulation (for the CDF part only).
- If the calculated incremental CDF is very small ($< 10^{-6}$ ry^{-1}), the proposed change will be considered, and there is no requirement to calculate the total CDF. However, if there are indications (e.g. IPE or IPEEE result) that the CDF may be considerably higher than 10^{-4} ry^{-1}, then focus should be on finding ways to reduce it.
- If $\Delta CDF \in [10^{-6} ; 10^{-5}]$ ry^{-1}, proposed changes will be considered only if it can be shown that CDF $< 10^{-4}$ ry^{-1}.

- If $\Delta CDF > 10^{-5}$ ry^{-1}, the proposed change would *usually* not be considered.

2) For the LERF:

- If indications clearly show that $\Delta LERF < 0$, the proposed LB change is considered to have satisfied the principle of risk-informed regulation (for the LERF part only).
- If the calculated incremental LERF is very small ($< 10^{-7}$ ry^{-1}), the proposed change will be considered, and there is no requirement to calculate the total LERF. However, if there are indications that the LERF may be considerably higher than 10^{-5} ry^{-1}, the focus should be on finding ways to reduce it.
- If $\Delta LERF \in [10^{-7}; 10^{-6}]$ ry^{-1}, proposed changes will be considered only if it can be shown that $LERF < 10^{-5}$ ry^{-1}.
- If $\Delta LERF > 10^{-6}$ ry^{-1}, the proposed change would *usually* not be considered.

3.5.6. Comparison of PRA results with acceptance guidelines

The different regions of Figure 3-2 and Figure 3-3 require different levels of analysis, as explained earlier, but also inside a given region, the level of detail in the analysis of uncertainties will depend upon the calculated values of CDF and LERF. For example, in region II of Figure 3-2 and Figure 3-3, the closer the estimates of ΔCDF and ΔLERF are to the upper bounds of these regions, the more detailed the analysis must be.

As explained earlier, these Acceptance Guidelines are not meant to be used prescriptively, and even in Region I or in the upper part of region II, the request to LB changes may be considered if additional elements that would not be reflected in the quantitative risk results are provided and detailed. In addition, if compensatory measures are proposed by the licensee to counter the effect of major contributors to CDF and LERF increments, these arguments will be considered by the NRC, even when the risk impact of these compensatory measures is not quantitatively assessed [6].

As is explained in Section 3.5.5, acceptance guidelines have been developed for full scope PRAs, but adaptations are possible when the PRA is not full scope. In such cases, an assessment of the contribution of out-of-scope elements to CDF and LERF may be necessary, the level of detail of which depending on how close the calculated CDF and LERF are to the upper

bounds of the different regions (Figure 3-2 and Figure 3-3). There are also cases where such assessment would not be necessary, in particular when the non-full-scope PRA shows small CDF and LERF increments (regions III), for which the baseline CDF and LERF values are not fundamental: if it can be shown (e.g. qualitatively, or on the basis of expert judgments) that out-of-scope elements would not affect ΔCDF and ΔLERF (even though they may affect baseline CDF and LERF), then the incompleteness of the PRA would not be an issue.

Similarly, when only a Level 1 PRA is available, the LERF cannot be calculated, but alternatives exist. RG 1.174 recommends the approach presented in NUREG/CR-6595 *An Approach for Estimating the Frequencies of Various Containment Failure Modes and Bypass Events*, in which a subset of core damage accidents (that can be studied with a Level 1 PRA) can be analyzed in lieu of Large Early Releases.

3.5.7. Integrated decisionmaking: contribution of risk insights

There is no general rule for establishing the role of risk insights in the decisionmaking process, it will be application dependent. However, quantitative risk results from PRA (CDF, LERF, ΔCDF, ΔLERF...) are considered to be the most "useful and complete characterization of risk" [6], especially when proposed changes have an effect upon many SSCs (Structures, Systems and Components), and there are cases where PRA results will be "crucial" to the success of the request for LB changes [6]. But they will usefully be supplemented by qualitative risk information (including industry-wide past PRA results and experience feedback) and traditional engineering analyses. Such supplemental information can effectively support the application for LB changes and reduce NRC's reliance on the technical acceptability of the PRA.

3.6. Risk-informed changes to the Technical Specifications

Plant-specific, permanent changes to the Technical Specifications are a sub-category of plant-specific changes to licensing basis, for which guidance is provided in RG 1.174, but additional, specific guidance is provided in RG 1.177 "*An approach for plant-specific, risk-informed decisionmaking: Technical Specifications*" [11].

Since the 1980s, the NRC has been reviewing and granting many requests to change TS, and a part of them was based upon PRA insights. Typically, these requests involved relaxation of

allowed outage times (AOTs) and surveillance test intervals (STIs). Regulatory Guide 1.177 focuses mostly on these two kinds of TS changes, but other types of TS changes are possible. In this RG, the NRC identifies three categories in which most requested TS changes fall:

- Improvement in operational safety, i.e. a reduction of the plant risk or a reduction of occupational exposure of plant personnel.
- Consistency of risk basis in regulatory requirements: TS may be changed to reflect improved design features or improvements in equipment reliability that make a previous TS requirement unnecessary or ineffective.
- Reduction of unnecessary burdens: based upon the operating history of the plant and industry-wide experience feedback, some TS requirements may appear to be too stringent or inefficient.

Use of compensatory measures

Compensatory measures to reduce the risk increase may be considered in light of the acceptance guidelines provided in RG 1.174 (see Section 3.5.5). The licensee may consider compensatory measures even if these acceptance guidelines are met. RG 1.177 suggests some examples of relevant compensatory measures such as:

- Improving test and maintenance procedures to reduce risk-associated errors
- Improving operating procedures and operator training to reduce the risk and the effect of human errors
- Testing a redundant train before initiating a scheduled maintenance activity.

Acceptance Guidelines for TS changes

In addition to the acceptance guidelines provided in RG 1.174 and presented in Section 3.5.5, RG 1.77 gives additional risk acceptance guidelines for AOT change requests, in order to ensure that the risk increment is acceptably small. These guidelines are based upon the concepts of ICCDP (incremental conditional core damage probability) and ICLERP (incremental conditional large early release probability), defined as follows:

- ICCDP = [(conditional CDF with the considered equipment out-of-service) – (baseline CDF)] × (duration of the considered AOT)
- ICLERP = [(conditional LERF with the considered equipment out of service) – (baseline LERF)] × (duration of the considered AOT).

That being said, the additional acceptance criteria are (Ref. [11]): the licensee should demonstrate that the AOT change has only a small quantitative effect upon plant risk, where:

- An ICCDP smaller than 5×10^{-7} is considered to be small for a single AOT change.
- An ICLERP smaller than 5×10^{-8} is considered to be small for a single AOT change.

3.7. Implementation strategy and steady transition towards a risk-informed framework

3.7.1. NRC implementation strategy

According to [14], one of the biggest obstacles at the NRC for implementing a more risk-informed regulatory strategy was that some staff members believed that the application of risk information would be accompanied by the abandonment of the concept of safety margins. The IPEs demonstrated the benefits of the methods to help in identifying plant vulnerabilities, even though these studies were of unequal quality. The Maintenance Rule was one of the first major applications of risk-informed techniques, and even if many utilities had already RCM programs (Reliability Centered Maintenance), it made risk assessment a part of the formal regulatory framework. In order to improve the acceptance of PRA techniques among its staff, NRC's management implemented a training program focused upon risk-informed techniques and their applications. This program is considered as an important element contributing to the improvement in the acceptance of the risk-informed philosophy [12].

3.7.2. Industry implementation strategy

At first, the development of risk-informed tools was mostly driven by the NRC, especially through the IPE program. Afterwards, some utilities became particularly convinced of the usefulness of these techniques, and they improved these technologies and their applications, even though some utilities were more skeptical or even opposed to a risk-informed regulation. Indeed, many utilities first saw risk-informed regulation as an unnecessary additional burden [12]. This early reluctance was soon overcome when it appeared how efficiently these tools could help in managing risky operations. The application of the Maintenance Rule was the first major attempt of using risk information in a formal, regulatory way and it was followed by

several pilot projects regarding specific issues to develop, improve and apply risk-informed techniques. Utilities began to use risk monitors not only to obtain plant status information, but also to improve the scheduling of planned operations by improving the safety level and by making operations more efficient.

It has also proven to be an efficient way to improve the safety culture and the risk awareness among engineers and technicians through site-specific training on PRA tools and their applications. For example, in some utilities, during morning status reports senior plant management require a discussion of the risk of the current plant configuration and of the quantified changes of the risk that will occur during the day's operation (e.g. if systems were to be taken out of service for maintenance). Some utilities have even incorporated risk performance metrics into the employee evaluation and bonus programs in order to encourage them to be more aware of the risk status of the plant when performing their job (Ref. [14]).

3.7.3. Improvement of safety level and operational performance

Risk-informed regulation will likely be more widely accepted if it can be shown that plant safety level and operational performance are at least as good, if not better, as they have been in the past 40 years of deterministic regulation. Even if performing this comparison is far from being straightforward, the industry and the NRC have made attempts to develop performance metrics to make quantitative comparisons in order to assess potential improvements brought by risk-informed practices and regulations. Some of these comparisons are presented in [14]. These metrics are used to compare performance of utilities that have chosen to use risk information as a management tool with those that have not, in order to evaluate whether performances are improved by the use of risk-informed techniques.

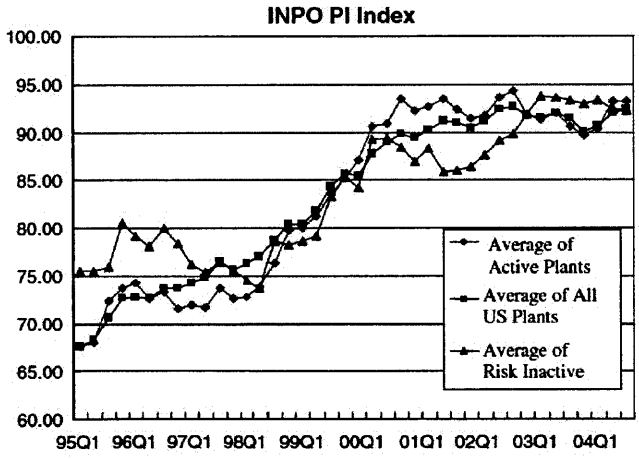
INPO performance indicator

The INPO performance indicator (PI) index is computed using a weighted combination of several INPO performance indicators ranging from 0 to 100 (the higher the indicator, the better the performance):

- Unit capability factor
- Forced loss rate
- BWR high pressure injection/heat removal system
- BWR residual heat removal system

- Unplanned automatic scrams per 7,000 hrs critical
- Safety system performance indicator
- PWR high pressure safety injection system
- PWR auxiliary feedwater system
- Emergency AC power system
- Fuel reliability
- Collective radiation exposure
- Chemistry performance indicator

Utilities are grouped into two categories: utilities that have adopted rigorous risk management practices, called "risk active" (35 plants), and utilities that have not adopted risk-informed management techniques (but have, however, implemented the risk-informed regulations such as the Maintenance Rule), called "risk inactive" (19 plants). There are also plants in neither of these two groups that will however appear in the category "all plants". Figure 3-4 presents the results for all US plants. We observe that, from 1995 to 2004, the index has increased for both categories, but it has more drastically increased for the plants in the category "risk active", because even if all plants show similar performance in 2004, the risk active ones started at a lower level. It would suggest that the use of risk-informed techniques has helped in improving performances of these plants.



	Slope (1995-2004)	Average Index (2000-2004)
Risk Active Plants	0.73	91.80
All US Plants	0.68	90.61
Risk Inactive Plants	0.52	89.74

Figure 3-4 : Standard INPO performance indicator indices for all US plants [14]

NRC accident precursor index

Since 1979, the NRC has tracked accident precursors and has ranked operating events that were most likely to lead to core damage. The ASP (Accident Sequence Precursor) index represents the total CCDP (conditional core damage probability) of all precursors during a given year divided by the total number of plants, so the smaller the ASP index, the better the performance. Figure 3-5 presents the ASP index for the different plant categories from 1994 to 2003.

The results on this figure may appear less convincing. For example, we note that there are between 1997 and 2000 very few significant precursors for risk inactive plants, while this is not the case for risk active plants. However, one can notice that between 2001 and 2003 risk active plants have performed better than risk inactive plants, and during the whole period 1994-2003, risk active plants have always been below 10^{-5} ry^{-1}, except in 1996, due to the occurrence of a LOOP event with unavailable EDG (Emergency Diesel Generator) at Catawba 2. This index is indeed very sensitive to particular events: we have just mentioned the peak of 1996 for risk active plants, but other peaks are also caused by specific events. Therefore, this index does not enable one clearly to differentiate performance of risk active and risk inactive plants. One can, however, conclude that, at least, performance of risk active plants is not degraded compared to risk inactive plants.

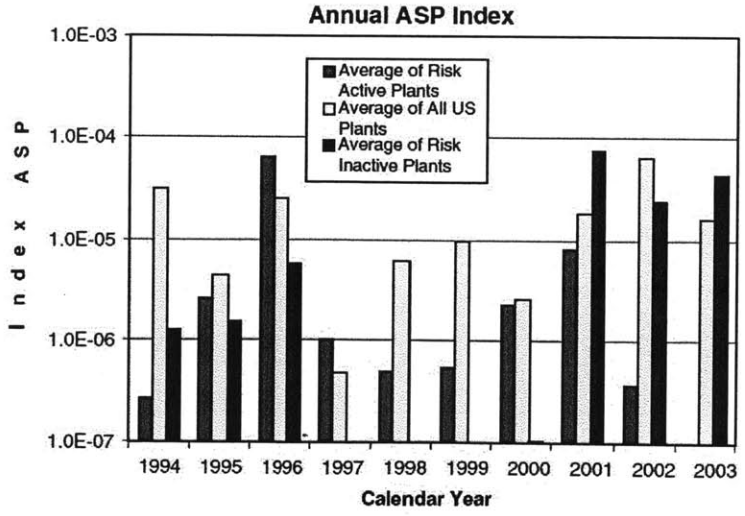


Figure 3-5 : NRC Accident Precursor Index [14]

Therefore, if risk-informed approaches enable one to improve other parameters, such as the efficiency of regulation and the competitiveness of nuclear power plants (which has been the case), the transition of the US nuclear industry toward a more risk-informed framework seems justified. It has also increased the level of risk awareness and safety culture at nuclear utilities, which is another positive element.

3.7.4. Role of defense-in-depth in risk-informed regulation

Through the process of moving towards risk-informed regulation, the issue of the role of defense-in-depth within this new framework arises. In this context, two types of concern have been expressed: on the one hand, some people fear that the benefits of risk-informed regulation could be diminished by arbitrary appeals to defense-in-depth [15] to avoid regulatory changes that seemed appropriate in the light of risk insights, as it has happened in the past. On the other hand, some people fear that risk-informed regulation could degrade the defense-in- depth philosophy. The concept of defense-in-depth is sometimes unclear, and there is no official or preferred definition of this concept. Currently, there are two main uses of this concept. The first one refers to the philosophy of maintaining high level lines of defense, such as the prevention of initiating events, the quick termination of progression of accident sequences, and the mitigation of accidents that are not quickly terminated. The second refers to the multiple barrier approach and to attributes such as redundancy, diversity and independence. In both cases there is the concept of successive and parallel levels of protection.

As seen in Section 3.4, the PRA policy statement gives PRA a subsidiary role to defense-in-depth. We have also seen in Section 3.5.3 that RG 1.174 reaffirms the importance of the defense-in-depth philosophy to account for uncertainties in system and human performance, stating also that PRAs can be used to assess the appropriate extent of defense-in-depth that should be used to achieve an acceptable safety level. It, thus, addresses the concern mentioned above of preventing the risk-informed approach from undermining the defense-in-depth concept.

In [15], the authors have identified two schools of thought concerning the scope and nature of defense-in-depth:

Structuralist Model

The structuralist model is somehow the traditional approach. It is based upon the repetition of the question "What if this barrier or safety system were to fail?" It looks for a balance between accident prevention, quick termination and mitigation, regardless of the probability of use or failure of the different systems. The implementation of this model of defense-in-depth has led in some cases to unnecessary regulatory burdens, which licensees are now trying to reduce. In addition, with this model licensees do not have an integrated view of the plant, which has resulted in the negligence of some risk-significant accident sequences (e.g. small break LOCA, see Section 3.1). In the modern version of the structuralist model (which is generally the current form of defense-in-depth, especially in France), defense-in-depth keeps a central position, while PRA is used to measure how well it has been achieved. When PRA reveals weaknesses, safety constraints will be added, and when PRA reveals unnecessary burden, constraints may be reduced. However, in most cases, there have been more regulatory reactions in cases where PRA reveals safety deficiencies than in cases where it shows that regulations or systems are superfluous [15].

Rationalist Model

The rationalist model is a more recent conception of defense-in-depth. It considers defense-in-depth as the aggregate of provisions made to account for uncertainty and lack of knowledge regarding accident initiation and evolution. It relies on two main aspects of PRA: quantified risk insights and uncertainty evaluation. Proponents of this model suggest the following process:

1) Establishing quantitative acceptance criteria, e.g. QHOs, CDF, LERF
2) Analyzing systems using PRA techniques to establish that the quantitative acceptance criteria are met
3) Evaluating the uncertainties of this analysis, and establishing what should be done to compensate for these uncertainties.

In this model, defense-in-depth is used to increase the degree of confidence in the insights of the risk analyses supporting the conclusion that the safety level is acceptable.

In [15], the authors insist on the fact that the structuralist and rationalist models are generally not in conflict. The fundamental difference between these two models is that the first presents defense-in-depth as a central value, while the second one gives defense-in-depth a subsidiary role. In order to prevent defense-in-depth from imposing unnecessary regulatory burdens, the authors recommend that the rationalist model be at least partially incorporated into the regulatory framework.

3.8. Other ongoing developments

There are numerous other ongoing activities related to PRA, among which:

- The NRC and industry are making a significant effort to develop PRA guidance documents as well as supporting technical reports.
- Both the NRC and industry continue to collect and analyze data needed to support the development and quantification of PRA models (in particular, data concerning fire risk and Human Reliability Analysis).
- In order to improve PRA quality, the NRC is also developing guidance for the treatment of uncertainties. Both traditional PRA techniques (e.g., regarding the propagation of uncertainties) and supplemental techniques (e.g., sensitivity studies, qualitative analyses, bounding analyses, screening methods) will be addressed.
- Risk-informed Technical Specification (see Chapter 7).
- Attempt to adapt current risk-informed regulation to new, safer reactor designs.

3.9. Summary

Originally considered by many licensees as an additional, unnecessary burden, risk-informed applications have found their place in the US nuclear industry and regulatory framework. Risk-informed applications are generally well accepted, even though the degree to which these tools are used and the quality/scope of the PRA models vary strongly among the licensees. Risk-informed applications were initially driven by the safety authority (IPE/IPEEE, Maintenance Rule ...); nowadays, their development is strongly influenced by a group of utilities particularly advanced in the development and the use of PRA tools. By developing (or

endorsing) detailed technical guidance for specific risk-informed applications, the NRC facilitated the implementation of these techniques by the licensees.

Indicators seem to show that risk management practices have enabled licensees to improve safety and operational performance. Undoubtedly, the use of PRA tools in licensing and operations at sites has induced an improvement in the safety culture and the risk awareness of workers. It has also enabled the NRC to improve the efficiency and the consistency of its regulatory actions.

Even though the NRC has been approving more and more ambitious risk-informed applications (such as the risk-informed Tech Specs presented in Chapter 7), it should be remembered that none of these applications is "risk-based", i.e. decisions and behaviors are never based upon risk information solely, but rather upon a blend of probabilistic and deterministic considerations, as required by the PRA Policy Statement.

Chapter 4

Use of PRA in France

4.1. Preamble

This chapter presents the regulations applicable to the use of PRA in France as well as the main risk-informed applications that have been developed, whether they have been implemented or not. Many of the observations made in this chapter cannot be proven definitively, but they are based upon observations that have been encountered within EDF. They are offered here in order to identify where there have been difficulties and to stimulate reflection on whether any changes are needed. Also, when interpretations are made, they reflect only the opinion of the author.

4.2. Historical Perspective

The safety of French nuclear reactors is based mainly on deterministic approaches. The first complete PRAs have been completed in 1990:

- Level 1 PRA for EDF 900 MWe reactors, developed by the IRSN, called EPS 900. One result: CDF = 5×10^{-5} ry^{-1} [17]. Since then, EDF has redone this PRA (which now constitutes the "Reference PRA", see below), and, reflecting PRA updates and plant modifications, the CDF has been revised to 4×10^{-6} ry^{-1}.
- Level 1 PRA for EDF 1300 MWe reactors, developed by EDF itself, called EPS 1300. One result: CDF = 10^{-5} ry^{-1}[17]. The latest value for this CDF is 4×10^{-6} ry^{-1}.

As with any PRA, many other results could be drawn from these studies (the overall CDF is only one result among many others), enabling a better understanding and ranking of SSCs in terms of their risk contribution. These PRAs considered internal initiating events and all operational modes. Internal hazards (internal flooding, fire ...) and external hazards were not considered [17]. One of the most outstanding results was the high contribution of shutdown modes to the

total CDF: 32% for the 900 MWe series, and 56% for the 1300 MWe series (latest value: 32% [26]).

Since then, there has been a substantial increase in the use of PRA in the French nuclear industry to assess the safety of operating nuclear reactors. These first two studies have had concrete consequences leading to specific measures to improve the design of the reactors as well as operational procedures. More systematically, these Level 1 PRA have been used in the framework of the Periodic Safety Reviews of the 900 and 1300 MWe reactors, also leading to specific modifications of designs and procedures. PRA results have also been used by EDF and the IRSN for different purposes: precursor analyses (analysis of the conditional risk posed by actual operational events), partial assessment of technical specifications (TS), definition of scenarios exercised on simulators for operator training, maintenance optimization ...

The EPS 1300 and 900 have been continuously updated, taking into account evolutions in designs and procedures, better knowledge of the different systems, as well as improvements in PRA methodologies. PRAs have also been developed for the 1450 MWe series and for the Flamanville 3 EPR. For this latter plant, the PRA model goes up to level 2, and a complete set of hazards PRAs has been developed.

4.3. The Basic Safety Rule (Règle fondamentale de sureté)

With the positive results of the first major PRA studies and an increase in the use of such studies, the ASN issued in 2002 a Basic Safety Rule: Règle Fondamentale de Sureté (RFS) 2002-01 [16]. The purpose of this Rule is to define acceptable methodologies for PRA and to recommend some PRA applications. The Basic Safety Rule constitutes the main official document on the use of PRA studies in the French nuclear regulatory system.

4.3.1. General doctrine of the Rule

The rule states that, even though the safety of French nuclear power plants mostly relies on deterministic methods, based upon the defense-in-depth principle, PRA studies complement these deterministic bases, thanks to their contrasting investigative approach. Therefore, the ASN reaffirms that deterministic methods (in particular the defense-in-depth principle) must remain

the fundamental basis of nuclear safety; PRAs are not supposed to supplant them or to have an equivalent role, but they are meant to complement them. More specifically, the ASN states that PRA helps to define and prioritize actions to be performed in order to reach or maintain an acceptable safety level. It enables one to have a more general view of safety, accounting for systems reliability as well as human behaviors. Indeed, PRAs consider a large number of initiating events and reveal situations covering complex associated events. Also, the Basic Safety Rule insists on the importance of uncertainties, and their effects upon the results must be analyzed, either quantitatively or qualitatively.

4.3.2. Reference PRAs

The Safety Rule requires that a Reference PRA be developed for each type of operating reactor and that it be continuously updated. For each Periodic Safety Review, a summary of the Reference PRA must be included in the safety report.

For future reactors, a Reference PRA must be developed as part of the design process, obviously iteratively. In particular, a synthesis of the PRA study must be included in the Preliminary Safety Report, presenting major contributions to the total CDF.

4.3.3. Quantitative objectives

In the Rule, the ASN strongly insists on the fact that, even though specific PRA applications may include references to quantitative objectives (e.g. CDF objectives), these objectives should be considered as guidelines and under no circumstances as strict limits. Even though it has never been made explicit, it has been mentioned that the ASN may be reluctant to define official quantitative guidelines because it does not want to fix a definitive value of acceptable safety, and it does not want operators to content themselves with a given safety objective. This situation is therefore very different from the US case, where Safety Goals and official quantitative guidelines in guidance documents associated with many different applications are used. However, quantitative objectives have been defined in consensus between EDF and the ASN, as is explained subsequently.

4.3.4. Domain covered by PRAs

Reference PRAs must be Level 1 PRAs, addressing to the extent possible all internal initiating events (except for internal hazards, e.g. internal flooding or fire) that may affect the reactor, in all reactor operational modes. In addition, Reference PRAs may be extended to address internal and external hazards as well as the frequency of radioactive release after core damage (Level 2 PRA). In the future, a new version of the Rule should be released, adding requirements concerning Level 2 PRA and hazards.

4.4. PRA applications recommended by the Rule

The Rule focuses on five main applications:

- Periodic Safety Review of operating reactors
- Precursor analysis
- Design of future reactors
- Safety assessment of materials and systems
- Technical specifications improvement.

4.4.1. Periodic Safety Review

4.4.1.1. General approach

The TSN Act requires that, every ten years, each reactor must undergo a Safety Review in order to assess the ability of the reactor to keep operating. This reassessment is accomplished in two main steps:

- First step: the Safety Review must demonstrate that the power plant meets the safety standards.
- Second step: the safety standards are reassessed, in the light of national and international experience. The safety standards may then be modified.

PRA is used during the Periodic Safety Review to estimate the CDF and its evolution since the previous Safety Review. It also helps in identifying any possible weakness involved in major contributions to the CDF.

During the first step of the safety review, the Reference PRA shall be updated to take into account most recent operating experience and new elements regarding the understanding of nuclear power plant systems. Then, in order to reveal and prioritize main contributions to the CDF, an acceptable method (according to the RFS) would be to group together elementary sequences that have analogous functional characteristics in "functional sequences". The purpose of this gathering is to constitute functional sequences whose frequencies and consequences could be reduced by implementing a single modification (or set of modifications) of the operating procedures or the design.

If modifications are decided upon after analyzing PRA results (or by other means), PRAs also help to assess advantages and drawbacks of the different available options. After the Safety Review process, the Reference PRA is updated, accounting for possible modifications decided during the review process.

4.4.1.2. EDF practice

The Level 1 analysis is comprised of three main steps [26]. First, EDF checks that the risk is balanced and identifies contributions that should be reduced, following ASN's recommendations outlined above. Then, ways to reduce these contributions are identified, and hardware and/or procedure modifications are proposed. A cost benefit approach was used for the 900 MWe third decennial review, and will be used for the 1300 MWe third decennial review.

Even though not required by the RFS, EDF has developed a methodology for a Level 2 analysis in the framework of these periodic safety reviews. This methodology will be proposed for the next periodic safety review (1300 MWe) [26].

4.4.1.3. Example

Reference PRAs have first been used during the second Periodic Safety Review of the 900 MWe reactors. As a result, several backfits have been required by the ASN, regarding in particular (Ref. [19]):

- Functional redundancy of AFWS (Auxiliary Feedwater Systems) for all modes of operation
- Improvement of the ventilation system
- Diversification of the reactor scram function

- Modifications that could mitigate the consequences of Class 1E emergency bus CCF.

4.4.2. Design of future reactors

The ASN insists that, as it was the case for past reactors, the safety of future reactors must still rely on deterministic bases. However, PRA studies will have a new role to play during the design process, and will effectively complement deterministic approaches. More precisely, some of the main contributions of PRA will be:

- Help to conceive safety-related systems, especially in terms of redundancy and diversity
- Verification that the design is "balanced" in the sense that there should not be event sequences having a large dominance in terms of CDF
- Assessment of the differences between the safety level of the new reactor concept and current reactors
- Assessment of safety improvements due to new devices designed against severe accidents
- Help to demonstrate that event sequences leading to large early releases are virtually dismissed.

Quantitative objectives will be used to assess the safety performance of the concept, but, again, these values are just guidelines, and should not be the only elements in the use of PRA results.

4.4.3. Technical specifications improvement

The role of the technical specifications is to define the limits of normal operation as well as the required actions in case of a beyond-design situation or upon the unavailability of a required system or component.

PRA can provide valuable information to help in identifying the most risk-effective course of action if a system is unavailable. PRA can also be used by the operator when asking the ASN for the authorization to perform special actions and/or to operate the reactor in a state that is not in accordance with the technical specifications, and to justify that the CDF increase remains small during such activities.

4.5. PRA quality management – Guidance

The adequacy of EDF's PRA models is managed through the use of several guides. Some of them have been internally developed, while others have been developed by other organizations such as EPRI. Information in this section is mostly based upon Ref. [26].

Level 1 PRAs

The quality of Level 1 PRAs is managed through the use of a guide developed by EDF in 2003-2004. This guide is mostly based upon EDF practice, but international standards have been used on a case-by-case basis (e.g. for the treatment of CCF). The goal of this guide is to ensure quality and consistency between the Level 1 PRAs, the Level 1 PRAs of the different reactor series being developed by different teams. This guide has not been subject to peer review, but has been transmitted to EPRI for information.

Level 2 PRAs

There is no equivalent guide used at EDF for Level 2 PRAs, even though a set of guidelines is available to the developers. Furthermore, all level 2 PRAs are developed by a single team, which reduces the risk of inconsistency between the different reactor designs and therefore reduces the need for such detailed guide.

Hazards PRAs

For the existing hazards PRAs (internal flooding, fire, seismic, see Section 4.7.1), EDF's practice is mostly based upon EPRI standards. Also, EDF has developed a detailed guide on fire PRA for the 1300 MWe Series, also usable for other designs.

IRSN review

The IRSN can request EDF to transmit their PRA models, but rarely does. More generally, the IRSN can require any information needed to evaluate EDF's PRAs. The guides mentioned above have not been reviewed by the IRSN, but these guides are for internal use only, to provide guidance on how to perform a PRA and to permit some standardization of the practices within EDF. Instead, the IRSN will review results and technical explanations included in the reports transmitted by EDF. It will pay attention to the validation of the tools, but not

particularly to the models themselves or to their maintenance. Also, the IRSN will often perform independent calculations, using its own PRA models, and will compare the results with those presented by EDF. It has been reported that these results are sometimes in conflict, reflecting the fact that IRSN's PRAs may be based upon different models or hypotheses (more frequent), or may not have the same level of detail as EDF's ones.

4.6. PRA applications to Tech Specs and Periodic Tests

In France, PRA techniques have been used to partially evaluate Technical Specifications (STEs) and Periodic Tests [21]:

- Determination of functions, systems and components availability requirements
- Choice of shutdown state
- Shutdown Initiation Time
- Treatment of simultaneous events
- TS temporary exemptions.

Risk insights can be used either to define regulatory or operational requirements or to assess the acceptability of these requirements. Concerning current reactors, STEs were defined using deterministic methods only, and were often based upon pre-existing Westinghouse Technical Specifications (because French reactors are based upon a Westinghouse design). In the 1990s, with the advent of risk-informed methods, the acceptability of STEs for most group 1 events (see Section 6.2.2 for a definition of group 1 / group 2 events, which differ according to safety importance) was assessed, using the first PRA models and simple methods [26]. In some cases, when risk insights revealed safety weaknesses, Shutdown Initiation Times have been shortened. The opposite has occurred much less frequently (Ref. [24] and [21]), even when PRA insights had revealed unnecessary regulatory burdens. Concerning Group 2 events, there has been typically no use of risk assessment. In fact, Group 2 events are often not (or not completely) modeled in PRA models. In the 2000s, more sophisticated methods have been developed to assess Tech Specs adequacy (see Section 4.6.1) on a case-by-case basis.

4.6.1. PRA applications to Shutdown Initiation Times and Repair Completion Times

STEs provide times by which shutdown should have been initiated (typically in case of a group 1 event) if the problem has not been solved, the "Shutdown Initiation Times", or by which repairs should have been completed (typically in case of a group 2 event), the "Repair Completion Times". If the licensee discovers that the problem cannot be solved before the end of the Shutdown Initiation Time (if applicable), he must initiate reactor shutdown as soon as possible. These times were originally defined using deterministic methods, but can now be assessed using PRA tools, or, for new reactors, they can be directly based upon risk insights.

In [20], two different strategies have been identified to cope with the discovery of component unavailability corresponding to an unplanned Tech Specs Group 1 event. A compromise between these two strategies is usually adopted.

4.6.1.1. Acceptable Risk Increase Strategy

The first strategy consists in defining a maximum time, T, (the shutdown initiation time or the repair completion time) during which the operator can keep the SSC in the unavailable state. This maximum time corresponds to a quantified risk increase defined by an acceptance criterion. Figure 4-1 presents this strategy, the hourly risk being the CDF.

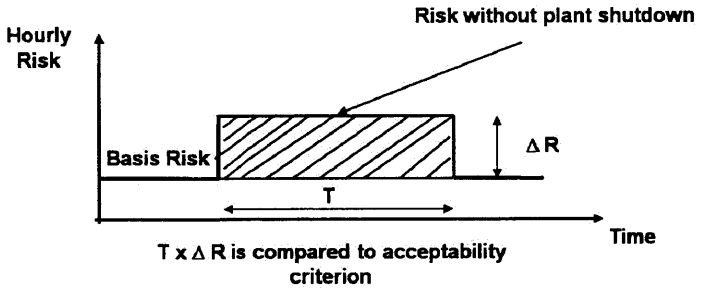


Figure 4-1 : Acceptable Risk Increase Strategy [21]

The incremental risk, $\Delta R \times T$, is then compared to an acceptance criterion. The current acceptance criterion for shutdown initiation time or repair is (Ref. [20]):

$$\Delta R \times T \leq 10^{-7}.$$

This acceptance criterion is not regulatory, but EDF and the ASN have reached a consensus to accept this numerical guidance. This value has been defined for Level 1, internal events PRA (with no hazards). This strategy of Acceptable Risk Increase is used in most cases.

4.6.1.2. Risk Minimization Strategy

In cases where the risk associated with the shutdown transient is high (i.e. greater than the consensus value, 10^{-7}), the previous strategy may not be the most appropriate. For these cases, EDF has developed a Risk Minimization Strategy that defines a shutdown initiation time T_2 such that the risk if repair is performed in the initial state is equal to the risk of the situation where the reactor is shut down to repair. These two risk profiles are plotted on Figure 4-2, on which $T_{SD} = \sum t_i$ is the total duration of the shutdown transient ($\sum t_i \cdot R_i$ is therefore the shutdown transient risk), R_a is the risk in initial state with unavailability of the system, and R_b is the risk after shutdown with unavailability of the system. The equalization of the two risks gives:

$$R_a \cdot T_2 = \sum_i t_i \cdot R_i + R_b \cdot (T_2 - T_{SD}) \tag{4.1}$$

hence the time T_2:

$$T_2 = \frac{\sum_i t_i \cdot R_i - R_b \cdot T_{SD}}{R_a - R_b} \tag{4.2}$$

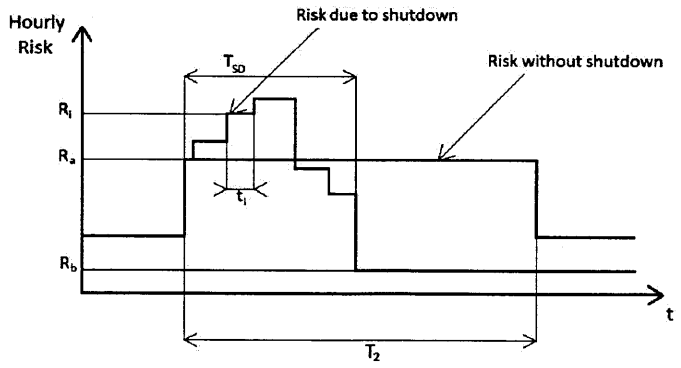


Figure 4-2 : Risk Minimization Strategy (adapted from [21])

In practice, when the shutdown transient risk is greater than 10^{-7}, a compromise between the two strategies is used, depending upon the value of the different parameters and a realistic repair time. In cases where the shutdown transient risk is particularly high (≥ 3, 4 or 5×10^{-7}), a

repair strategy without plant shutdown and based upon a realistic repair time may be considered [21].

Uncertainties are usually taken into account in two different ways, with sensitivity studies and through the use of standard shutdown initiation times (1 hr, 2 hrs, 8 hrs, 24 hrs, 3 d, 7 d, 14 d, and 1 month in case of a repair strategy): in general, the retained value is the standard value just below the value computed with the applicable strategy, even if this computed value is very close to the next standard value (e.g. if the computed value were 13.9 d, the retained value would be 7 d and not 14 d) (Ref. [24]).

It should be noted that the computation of the risk associated with a shutdown transient as performed using this method is something rather uncommon (e.g. in the United States), due to its complexity. It seems to be made possible with EDF's PRAs thanks to the fact that the number of reactor modes considered in the PRA model is greater than the number of reactor modes considered in the technical specifications. Therefore, a transient between two Tech Specs reactor modes can be "discretized" into several PRA reactor modes, and by assigning a particular time interval spent in each of these modes, the risk associated with the transient can, thus, be computed (also, point risk increases are added).

4.6.1.3. Current status

These methods have been extensively applied to assess STEs of AC power sources and Auxiliary Feedwater Systems. In particular, these applications have shown that all AOTs specified in current STEs are overly conservative, except one (that of auxiliary transformer failure). However, these studies have not led to STE modifications [26]. The safety authority has not approved these studies, and has recommended in particular that hazards and CCFs be addressed in these probabilistic studies. Even though hazards PRA are available for some reactors, there are, however, several barriers to their use. In particular, these hazards PRA are considered at EDF to be too conservative to be used in such studies. Additionally, no quantitative criterion has been defined for acceptable risk increase that takes hazards into account [26]. EDF is collecting information on the international practices regarding this issue. These matters are currently in standby status.

Concerning the development of EPR (Flamanville 3) Tech Specs, these methods should be used for studying the most important safety systems. However, at this point, it is unclear that the results of these studies will actually be used to develop the Tech Specs [26]. The difficulties mentioned above are also applicable to the EPR. In addition, as design and construction of the EPR progress, PRA models are still evolving, which means that these studies would have to be repeated (even though the methodology presents some robustness, thanks to the use of standard AOTs), which may not be feasible due to limited resources.

4.6.2. Probabilistic analysis of operational configurations

PRA insights are more and more used to analyze the risk associated with particular operational configurations. In some cases, these analyses (along with traditional deterministic approaches) may lead to TS temporary exemptions. PRA is used to assess the risk increase associated with the exemption, and to identify appropriate compensatory measures. The CDF increment is assessed and compared to an indicative acceptance criterion.

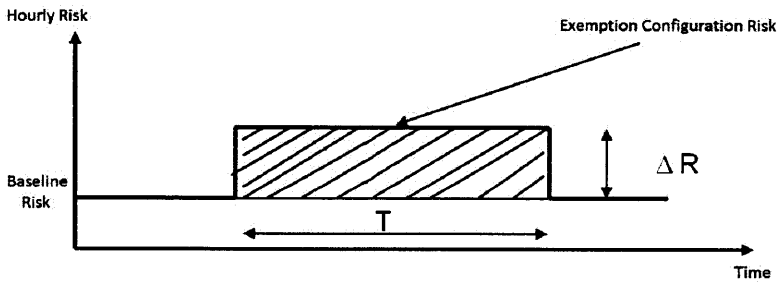


Figure 4-3 : TS Exemption Acceptance Criterion [22]

Using the notations of Figure 4-3, the product, $T \times \Delta R$, is compared to the acceptance criterion, 10^{-7} (if there has been significant conservatism in the risk assessment, values of $2\text{-}3 \times 10^{-7}$ may be acceptable) (Ref. [21] and [22]). In cases where $T \times \Delta R \geq 5 \times 10^{-8}$, PRA is used to identify compensatory measures and their effects upon plant risk.

This use of PRA appears to be one of the most accepted. Even though not mandatory, the ASN may ask for such probabilistic analysis in some cases, and it appears to have a significant importance in its decision making process.

4.6.3. Treatment of simultaneous events in the Tech Specs

For the EPR (Flamanville 3), EDF R&D is currently working on a methodology to treat the simultaneous occurrence of a planned event and an unplanned event using a blend of probabilistic and deterministic concepts. The new methodology is not meant to be used in real time, but rather in background in order to develop EPR Tech Specs (i.e. only a limited number of risk-significant configurations would be studied using this methodology). It is still at an R&D stage and it has not yet been decided whether to use it or not. One of the main difficulties would be the amount of work required to use it, given the limited available resources [26].

4.6.4. PRA application to Surveillance Test Intervals

Methodology

For current, two-train EDF reactors, STIs (Surveillance Test Intervals) have been determined using deterministic tools only. However, if these STIs were to be kept with the four-train EPR, there would be a requirement for twice as many surveillance tests, which would mean additional costs and burdens that might not be justified from a probabilistic standpoint. Therefore, for Flamanville EPR, EDF has developed a risk-informed STI determination process for safety-related systems to provide decision makers with risk insights. Proposed STI changes would then be reviewed by an expert panel that would consider quantitative results but also qualitative aspects of the proposed changes.

The maximum STI change, ΔSTI_{max}, will be associated with the maximum CDF increment, $\Delta CDF_{max} = CDF_{max} - CDF_{base}$. Acceptance guidelines (that are only indicative, not regulatory) defined for full-scope, internal events, Level 1 PRA are as follows:

- For an individual STI change: $\Delta CDF_{max,ind} = 10^{-6}$ ry^{-1}
- For all STI changes: $\Delta CDF_{max,all} = 10^{-5}$ ry^{-1}.

If the baseline CDF is smaller than 10^{-5} ry^{-1} (which is the case for the EPR), then the criteria are as follows:

- For an individual STI change: acceptable CDF increase = 10% of baseline CDF (in practice, usually less than 3% [26])
- For all STI changes: acceptable CDF increase = 100% of baseline CDF.

Current status

The methodology has been presented to the safety authority. It has raised many questions, in particular regarding the needed scope of the PRA (Level 1, no hazards). At this time, it is unclear whether this methodology will actually be used [26].

4.7. Other evolutions and prospects

4.7.1. Ongoing developments

As is mentioned earlier, the first PRAs developed in France were the Level 1, internal events EPS 900 and 1300 (1990), which did not consider internal and external hazards. Even though these PRAs were only of Level 1, they were some of the first in the world to cover all operational states of the reactor. Since then, the IRSN and EDF have been working on several developments. First, they have kept improving the quality of these Level 1 PRAs by updating them continuously, taking into account most recent experience and progress. Also, EDF's PRAs for 900 and 1300 MWe have been revised after the promulgation of the Basic Safety Rule, the reference PRAs required by this rule being now the ones made by EDF. IRSN's PRAs are used to perform independent, comparative studies. To date, EDF has for the 1300 MWe series [25]:

- Level 1 PRA, covering the reactor and the fuel pool (internal events)
- Level 2 PRA
- Hazards PRA, covering fire, internal flooding, and also seismic risk for a pilot plant (Saint-Alban).

A similar set of PRAs is being developed for the 900 MWe series, within the framework of the life extension program [25] (a Level 2 PRA for the 900 MWe series has already been developed by EDF). Concerning the 1450 MWe (N4) series, only a Level 1 PRA is available at this time.

4.7.2. Evolution of the regulatory framework

As is explained in Section 1.2.2.3, the ASN is a member of WENRA, an association of European safety authorities that is working towards a certain harmonization of nuclear safety regulation among its member countries. This association has established a list of about 300 "Reactor Safety Reference Levels" [1] that are meant to be implemented into the different national regulatory frameworks. In 2010, it was assessed (Ref. [3]) that, even though almost all of these Reference Levels were implemented by French plants, few (about one third) were actually formalized into official regulations, which is consistent with the preliminary observations made in Section 1.2.2.2 about the French regulatory system: most of the ASN's requirements have been expressed in individual letters to the sole licensee, EDF, rather than in formal regulatory documents, and EDF has also implemented safety provisions on its own initiative. The promulgation of the TSN Act in 2006 had unexpectedly disrupted ASN's original plans to transpose WENRA's Reference Levels into national regulation, but this transposition should be achieved during the coming months through the completion of certain regulatory documents [3].

In the list of Reference Levels, a small set is dedicated to PRA. This is one of the points that has been emphasized as being insufficiently implemented into French nuclear industry and regulation [2]. Indeed, these Reference Levels contain recommendations that go beyond those provided by the ASN in its Basic Safety Rule (RFS) on PRA:

- They recommend the development of Level 2 PRAs, covering all modes of operation, while the French RFS requires that reference PRA be of Level 1 only.
- They recommend that PRA models consider the following hazards: internal fire, internal flooding, severe weather conditions and seismic events. The French RFS does not require these considerations. Indeed, at the time of publication of the RFS, hazards PRAs were not well developed yet, internationally.

As explained above, EDF is anticipating these new requirements, while an updated version of the RFS (re-named "Guide" in the new regulatory framework) should be published soon.

4.8. Difficulties and barriers

Even though PRA tools have been successfully used for several applications (Tech Specs exemption requests, precursor analysis, ...), advanced, ambitious applications have sometimes failed to be widely accepted, either by the safety authority or within EDF, as shown by some examples mentioned above. There have been technical barriers, but also non-technical difficulties.

The safety authority does not seem to be opposed to risk-informed applications, but it often appears to be very demanding regarding the scope of the PRA models that are used for these applications (Level 2, hazards...), while acceptance criteria may not have been established for guiding such a scope, both in terms of level of needed detail and results, and models may be deemed to be too conservative. Also, there have regularly been debates between EDF and the IRSN regarding the PRA models and hypotheses that each uses, and in some cases, the hypotheses or studies of EDF were not accepted. Indeed, the IRSN performs independent calculations using its own PRA models or hypotheses, and its results may differ from those of EDF.

There have been also difficulties within EDF in applying some risk-informed methodologies. At the risk of caricaturing or oversimplifying, we can try to classify the reasons for these difficulties in four categories, which are obviously, to some extent, interdependent:

- Resource issues: some of the risk-informed applications that have been proposed would require significant engineering resources that may not be made available considering the priority of other needs. It has been pointed out that, generally, resources are primarily affected for the development and quality of PRA models rather than for the applications. Doing this can limit the benefits reaped from the developmental expenditures.
- Self-censorship: the difficulties encountered regarding the acceptance of some PRA applications, and the absence of methodologies for those applications or for new ones, led EDF management to think that the associated regulatory process would be long and even uncertain to succeed. Hence, it did not encourage them to propose extending some applications or to suggest new applications.[26].

- Doubts regarding operational benefits: The belief that risk-informed applications would bring operational benefits to the operator, in particular by reducing unnecessary regulatory burdens, is not unanimous at EDF: even though managers agree that PRA applications might allow some benefits, some fear that they might also induce (more) additional constraints or that the cost-benefit ratio might be too high. This reasoning led to not generalize applications or to develop new ones [26].
- Mistrust regarding PRA: PRA tools are sometimes questioned by EDF management, with many concerns existing regarding the uncertainties of these methods. Some people have expressed a feeling that risk-informed tools may allow behaviors that are not acceptable from a deterministic standpoint (e.g., use of too little conservatism or defense-in-depth). However, in the Basic Safety Rule there exist deterministic safeguards against such behaviors, as is explained in Section 4.3.1.

Due to all these reasons, the present applications such as the one for the Tech Specs will probably not be generalized, nor will new risk-informed applications be developed. No new R&D exploratory study is currently planned. As for risk-monitors, its use for the French existing plants is not considered to be appropriate, as STEs (in particular the Simultaneity Rules, see Section 6.2.2) are considered as the only basis upon which the operator should base its behavior for configuration management, for the sake of safety. Rather, EDF has developed some pedagogic tools to promote the PRA culture on-site, such as a simplified presentation of PRA results.

4.9. Summary

Since the development of the first French PRAs in 1990, much progress has been made, in the models themselves, their quality, as well as their applications. However, some of the contemplated applications were actually not implemented. For some of these applications, there have been difficulties not only with the safety authority (concerning scope, criteria, models...), but also in some cases within EDF. Also, until now, most of the resources have been allocated to the development of PRA models rather than their applications. There are however great opportunities to successfully implement risk-informed applications in French nuclear power plants. Indeed, tools and skills have reached a considerable level of maturity, and the high level

of standardization of the EDF nuclear fleet is a strength that permits a reduction in the amount of work required to implement applications in a consistent way, and that provides valuable experience feedback to improve these applications.

Even though similar benefits (and limitations) are attributed to PRA in the French and US regulatory frameworks, in France these techniques have not reached the same status as in the US. In the US, not only have risk-informed practices penetrated the regulations, but they are also more and more used on a daily basis at the operational level, as is shown in the following chapters (regarding risk-monitors, the Maintenance Rule, risk-informed Tech Specs), while in France there appears to be some reluctance towards such practices. EDF is a much larger company than any typical US operating company, and there is at EDF a clear separation between the different entities (R&D, engineering, operations). In particular, the centralization of the engineering divisions, and their separation from operations, may, to some extent, explain some of the differences from the US case, where engineering and operations are typically site-oriented and more closely coupled, hence an easier transfer of PRA technologies and expertise from the engineering staff to the operational staff. In France, ambitious risk-informed applications at the operational level are therefore unlikely to be considered in the short term. An important, but difficult step would be the decision to use risk-monitors on site, which would not necessarily involve recasting fundamentally the current configuration risk management practices (Simultaneity Rules), as will be explained in Chapter 10.

Also, in the US, for many years the NRC has stimulated the development and the use of PRA tools, e.g. through the IPE/IPEEE programs and the enforcement of the Maintenance Rule (even though, strictly speaking, the use of PRA techniques was never mandatory), to improve safety as well as regulatory efficiency. In France, the ASN has not provided similar incentives.

Chapter 5

Maintenance in France and the US - Background

5.1. Introduction

5.1.1. Role and objectives of maintenance

There are two types of maintenance: preventive maintenance, to prevent equipment failures, and corrective maintenance, to fix broken equipment. Many years of operational experience have confirmed the link between maintenance and safety: even if maintenance alone will not make a plant safer than its original design, maintenance is fundamental to ensure that the original design basis is maintained (or not unacceptably degraded). Preventive maintenance is usually well planned, using well defined procedures. Corrective maintenance procedures, however, may be lower quality, workers may be less prepared, and less time may be available to plan and perform corrective maintenance. Traditional maintenance practices focus upon individual systems and their performance, with detailed instructions and requirements. They have the advantage of being usually clear and easy to implement and regulate, even though they may sometimes lead to focusing attention upon compliance with protocols with less consideration for performance and results. Current trends in safety related maintenance take the plant into account as a whole, and focus is placed upon general safety performance rather than upon individual components and their individual performance. This is especially illustrated by the use of PRA in safety related maintenance activities (see Section 5.1.3).

In the past, equipment preventive maintenance priority ranking was based upon subjective engineering judgment. With the development of risk-based techniques, it can now be

accomplished based upon these techniques, in combination with engineering judgment and analysis of experience feedback. Online maintenance programs can also contribute to improving the quality of maintenance and the safety level, diminishing time constraints and other loads that affect personnel during outages. Indeed, outages are recognized as times of high workload, with greater risks arising due to time pressure, fatigue, and added burdens on supervisors. If workers perceive time pressure, they may make more errors and take shortcuts to complete tasks faster. In order to reduce time pressure, realistic schedules need to be justified and used in order to provide enough time to complete maintenance tasks (with sufficient time margins) while reducing the potential for maintenance errors. Increased use of online maintenance can also result in fewer forced outages.

5.1.2. Management strategy

5.1.2.1. Outage management strategy

Outage duration and quality directly influence availability and costs. Outages are periods when significant resources are expended. Past experience has shown that well-planned outages improve both safety and operational performance [27]. Comprehensive planning can enable one to reduce outage durations, avoid outage extensions, ensure reliable plant operation and reduce radiation exposures to the staff. It is recognized that an outage PRA is a good tool to provide an overview of the overall safety level obtained during the different outage operations. If an outage PRA is not used, deterministic considerations may be used, but with less coherent results being likely.

In more competitive energy markets, having emphasis on demand-dependent pricing, it appears that reliable and predictable performance during outage is often more rewarded than minimizing outage duration [28].

5.1.2.2. Human and organizational performance

There exists a weight of evidence across different industries (nuclear in particular) showing that a large proportion of equipment failures occur after maintenance and periodic tests, and that a substantial portion of those failures can be traced back to human and organizational factors arising within the tests themselves. Maintenance errors may not always be revealed by

post-maintenance tests. The proportion of maintenance errors remaining undetected may be increased by the following common trends [29]:

- Economic pressure leads to reductions in staffing, new shift schedules, and more work being performed by external contractors who may typically be less familiar with systems of the specific plants being treated.
- Many nuclear organizations worldwide are facing retirements of experienced staff, including maintenance specialists. The transfer of knowledge must be planned and managed to the extent feasible.
- The volume of maintenance activities is increased due to plant ageing.

5.1.3. Use of PRA in maintenance

5.1.3.1. An efficient tool

Current maintenance programs have been developed using mainly engineering and deterministic considerations such as defense-in-depth, functional performance based upon accident analyses, and manufacturers' recommendations. Increasing competitiveness and liberalization of electricity generation are putting emphasis upon operating plants at reduced costs. Maintenance can play a significant role in reducing costs, keeping in mind that safety must not be compromised in order to achieve cost reductions. The "risk significance" concept, arising with the advent of PRA, has opened up many possibilities to improve maintenance strategies, while improving public safety in the same time. Such methods are increasingly used to address many aspects related to maintenance, e.g.:

- Maintenance planning and scheduling
- Ranking of components according to their risk significance
- Guiding decisions related to online maintenance
- Appreciation of the risk effects during maintenance activities
- Supporting technical specification changes to accommodate maintenance needs
- Establishing use of performance indicators and criteria.

Currently, PRA based maintenance applications are often conducted using Level 1, internal event, at-power PRAs. The use of these PRAs can be more effective if the scope of available PRAs is enhanced. For example, the availability of a shutdown PRA allows the

evaluation of the effect of maintenance activities performed during shutdown periods, which can be compared to the effect of the same activities if performed online. This is a powerful tool for deciding whether some maintenance activities should be carried out online or during outages, from a purely overall safety point of view. However, other aspects must be taken into account when making any decisions of that kind: workers habits and preference, available guidance, human reliability (which may change depending upon whether maintenance is performed online or during outages). In many cases, the complexity of available plant specific PRAs may not correspond with the needs for maintenance applications (e.g., electrical components are often grouped into "macro-components" in order to simplify the models). In order to deal with this problem, the licensee can either decide to increase the level of detail of its PRA or to perform post-processing of the PRA results to achieve similar objectives.

5.1.3.2. PRA limitations for maintenance related applications

PRA is one tool among several, which has however some limitations. The risk-based ranking of systems and components can be very sensitive to PRA quality and complexity. Therefore, the use of PRA can result in a ranking that could be unrealistic, which can lead to focusing maintenance efforts where they are less required. And as mentioned above, the scope of available plant specific PRAs is in many cases not detailed enough to be effectively used in some maintenance activities.

Great attention should also be paid to uncertainties. For example, if a component ranked as "low risk" is associated with a large uncertainty, this could mean that this component may actually be risk significant. In such a case, the uncertainty should be considered in order to prevent this component from being left out of the scope of the maintenance program.

5.1.3.3. Interfaces with deterministic considerations

Traditionally, maintenance has been based upon deterministic considerations and engineering analyses such as defense-in-depth, single failure criteria, deterministic accident analysis, manufacturer's recommendations, experience feedback and industrial standards. The advent of modern PRA has opened up new opportunities to improved maintenance strategies with cost and safety benefits. Table 5-1 estimates the effect that PRA techniques could have

concerning different maintenance and testing tasks. We see that it could have a significant effect on many different aspects of maintenance programs.

Test/Inspection	Preventive Maintenance	Corrective Maintenance
- Test type (L)	- Task	- Design specification
- Scope (H)	- Scope (L)	- Scheduling (H)
- Frequency (H)	- Frequency (L)	- AOT (H but only exemptions)
- Scheduling (H)	- Scheduling (H)	
- AOT (H)	- AOT (H)	

Table 5-1: Estimated effect of PRA on maintenance programs (L=Low, H=High) [27]

It is recognized however that some dangers associated with undue reliance on PRA can arise. For example, using PRA may show that removal of all protection against a particular fault for a short period of time would be numerically acceptable, but it would remain unacceptable from a deterministic and conservative point of view, since important events, not taken into account in the PRA model, may occur and be disastrous. Therefore, the IAEA expresses the following deterministic safeguard: "For all maintenance operations, there should be protection provided for all faults at all time" [27]. The general idea to draw from such considerations is that in maintenance, but more generally in safety matters, probabilistic assessment should always be combined with deterministic, engineering considerations, because of the underlying limitations of PRA techniques (which can be reduced, but not eliminated). This is consistent with the US PRA Policy Statement and the French Basic Safety Rule.

PRA can however address some of the deterministic weaknesses regarding maintenance activities, for example [27]:

- The original basis of deterministic maintenance requirements is often not clear, and not logically developed: maintenance activities can sometimes be performed without an understanding of why they are being done and of their effect upon safety. PRA can help to rank SSCs and to show how changes in reliability can modify the public risk.
- Deterministic considerations are often binary: for example, activities are classified as either safety related or not safety related, while the reality is not always that clear. PRA enables one to use a more continuous range of judgment and to define priorities.

- Risk and reliability are not considered in a consistent and systematic way through a deterministic approach, contrary to that of PRA.
- Dependencies and CCFs are not adequately addressed by deterministic approaches, while PRA explicitly models dependencies and enables one to identify the effect of CCFs.

5.2. Maintenance in the US: the Maintenance Rule

5.2.1. The Maintenance Rule: regulatory aspects

In addition to the technical specifications that regulate most of the safety-related maintenance activities (which consumes about 80% of maintenance resources, even though it concerns only a minority of plant equipment) , the NRC has published on July 10, 1991 the Maintenance Rule, as 10 CFR 50.65 "Requirements for monitoring the effectiveness of maintenance at nuclear power plants" [30]. This Rule took effect on July 10, 1996. Before the enforcement of the Maintenance Rule, NRC inspections showed that even if licensees had adequate maintenance programs, some maintenance-related weaknesses were regularly observed, such as inadequate root cause analyses leading to repetitive failures and inadequate consideration of risk when prioritizing, planning and scheduling maintenance activities.

5.2.1.1. Performance-Based Regulation

In [31], the NRC distinguishes two kinds of rules:

Process-oriented (or programmatic, or prescriptive) rule

This is the traditional approach for most rulemaking. Such a rule includes detailed requirements and instructions. The advantage of such a rule is that it is easier to enforce: licensees have a clear idea of what they must do to implement the rule, and inspectors know exactly what to inspect. The drawback is that such rules tend to be inflexible, and may prevent licensees from using the means they judge the most efficient and effective to implement the rule.

Results-oriented (or performance-based) rule

Such a rule describes in general terms what results are expected, leaving the methods and details to achieve them up to the licensee. It has the advantage of letting the licensee decide which means are the most effective and efficient to achieve these objectives, contrary to process-

oriented rules, thus reducing regulatory burdens. It also allows the licensee to consider risk significance when designing its strategy. The drawback is that such rules are more difficult to enforce, because the requirements are less clearly defined than in process-oriented rules. It appears that licensees clearly prefer results-oriented rules to process-oriented ones. It also has the safety benefit of aligning both authority and responsibility with the operator for the results obtained.

The NRC Maintenance Rule is a results-oriented rule. It was one of the first major applications of risk insights in the US nuclear safety regulation, enabling utilities to take advantage of their IPEs to develop risk-informed programs. The positive results brought by the implementation of this Rule are widely believed to have influenced the pace of transition towards more risk-informed, performance-based regulation.

5.2.1.2. Content of the Rule

Goals and Monitoring

10 CFR 50.65 §(a)(1) requires each licensee to set goals and to monitor the performance of SSCs in a way that gives reasonable assurance that these SSCs are able to perform their functions. The Rule adds that these goals should be commensurate with safety and should take into account industry-wide operating experience. In addition, it requires licensees to take appropriate corrective actions when the performance or the condition of an SSC does not meet established goals. Being intentionally non-prescriptive, it is important to note that this paragraph requires that goals be established by the licensee, not the NRC, but with concurrence of the NRC.

Effective Preventive Maintenance

10 CFR 50.65 §(a)(2) defines an alternative strategy to the monitoring approach defined in §(a)(1). Here, the NRC states that, in some specific cases, the performance or condition of SSCs can be effectively controlled through adequate preventive maintenance rather than monitoring in terms of performance goals.

Periodic evaluation and safety assessments

10 CFR 50.65 §(a)(3) requires that performance and condition monitoring activities and associated goals (§(a)(1)) and preventive maintenance activities (§(a)(2)) be periodically evaluated, at least every refueling cycle, taking into account industry-wide experience. In addition, this paragraph requires that, when necessary, adjustments be made to ensure that the objective of preventing SSC failures through maintenance is appropriately balanced with the objective of reducing SSC unavailability due to monitoring or preventive maintenance.

Assessing and managing risk before maintenance activities

In 1999, the NRC amended the Maintenance Rule by adding a new paragraph (a)(4) that completes 10 CFR 50.65 §(a)(3). This paragraph requires that licensees perform risk assessments before maintenance activities are performed on SSCs covered by the Maintenance Rule (see below) and that they manage the increase in risk that may result from the proposed maintenance activities.

Scope of the Rule

10 CFR 50.65 §(b) defines which SSCs are within the scope of the Rule as follows:

- Safety-related SSCs
- Non-safety-related SSCs that are relied upon to mitigate accidents or are used in emergency procedures
- Non-safety-related SSCs whose failure could prevent safety-related SSCs from fulfilling their role
- Non-safety-related SSCs whose failure could cause a scram or actuate a safety system.

5.2.1.3. Industrial Guidance: Endorsement of NUMARC 93-01

Following the publication of the Maintenance Rule in 1991, the nuclear industry developed a document that provides guidance to licensees regarding the implementation of this Rule: NUMARC 93-01, "*Industry Guideline for monitoring the effectiveness of maintenance at nuclear power plants*" [34], first published in 1993. The NRC endorsed this guidance in RG 1.160 [32]. NUMARC 93-01 is the practical reference to comply with the Maintenance Rule.

5.2.2. The Maintenance Rule: industrial guidance

As a whole, NUMARC 93-01 clarifies and complements many aspects of the Maintenance Rule, while still respecting the intentionally non-prescriptive philosophy of the Rule. A simplified flowchart in Appendix A presents a summary of the Maintenance Rule process as recommended by NUMARC 93-01.

5.2.2.1. Risk Significance Determination

Once SSCs within the scope of the Maintenance Rule have been selected (see first row in flowchart of Appendix A), the licensee must establish risk significant and performance criteria.

First, risk significant criteria must be established in order to determine which of these SSCs are risk-significant, often based upon CDF calculations. Several existing guidance documents can be used, such as NUREG/CR-5695 "*A Process for Risk-Focused Maintenance*", NUREG/CR-3385 "*Measures of Risk Importance*", NUREG/CR-4550 "*Analysis of Core Damage Frequency*", or the EPRI PSA Application Guide (EPRI Report TR-105396). Utilities that have developed Reliability Centered Maintenance (RCM) programs may use studies that support such programs to find useful data to establish the risk significance of SSCs. Alternatively, NUMARC 93-01 suggests methods using the following risk importance measures to assess the risk significance of SSCs (see Section 2.2.3 for definitions of these metrics): RRW, RAW, and the CDF contribution. Specifically:

- RRW, method A: SSCs that, cumulatively, account for about 99% of the sum of RRWs related to maintenance should be considered to be candidates for risk significant SSCs.
- RRW, method B: SSCs with an RRW greater than 0.5% should be considered to be candidates for risk significant SSCs.
- CDF Contribution: Maintenance-related SSCs involved in cut sets that account for 90% of the overall CDF should be considered to be candidates for risk significant SSCs.
- RAW: SSCs with an RAW greater than 200% should be considered to be candidates for risk significant SSCs.

5.2.2.2. Establishing Performance Criteria

For SSCs that have been established as being risk-significant (see above), and for non-risk significant SSCs that are in standby mode, specific performance criteria shall be established.

Most often, the performance criteria are related to the availability, the reliability or the condition of the SSC (in particular, these criteria should be established to assure that assumptions used in plant-specific PRA or other risk-analyses are still valid). For the remaining non-risk significant SSCs, plant level performance criteria shall be established, such as:

- Unplanned automatic reactor scrams per 7000 hours critical
- Unplanned safety system actuation
- Unplanned capability loss factor.

5.2.2.3. Treatment of SSCs under §(a)(2) or §(a)(1)

The philosophy of the Maintenance Rule is to separate the treatment of SSCs into two categories:

- SSCs treated under §(a)(2) of the Rule: they are addressed through preventive maintenance programs and their performance is monitored against the performance criteria defined in Section 5.2.2.2.
- SSCs treated under §(a)(1) of the Rule: these SSCs are subject to more attention and stricter practices. It concerns SSCs that have shown performance lower than expected. For these SSCs, specific goals are established. When a goal has been met (or is no longer applicable) for a sufficient period of time, the corresponding SSC can be returned to §(a)(2) treatment.

By default, risk-significant SSCs with acceptable performance will be treated under §(a)(2) and monitored against their specific performance criteria, as well as non-risk significant SSCs that are in standby mode. Risk significant SSCs and non-risk significant SSCs in standby with unacceptable performance (even if performance criteria are being met) will be addressed under §(a)(1) and have goals established against which performance will be monitored.

Remaining non-risk significant SSCs are addressed under §(a)(2) and their performance is monitored against the established plant level performance criteria, as defined in Section 5.2.2.2. If a plant level performance criterion is not met, a root cause analysis will be conducted to determine whether this was due to failure of an SSC within the scope of the Rule, and if this failure was an MPFF (Maintenance Preventable Functional Failures). If this is the case, the licensee may decide to treat this SSC under §(a)(1) and to establish a specific goal for this SSC.

Alternatively, the licensee may continue to address this SSC under §(a)(2) after implementing adequate corrective actions. If after some time it is determined that the corrective actions have not corrected the problem, the SSC will be placed in §(a)(1) category.

5.2.2.4. Configuration Risk Management

Following the revision of the Maintenance Rule in 1999 with the addition of §(a)(4) concerning the assessment and management of risk increases resulting from maintenance activities, section 11 of NUMARC 93-01 was revised to provide guidance regarding this new paragraph, which is endorsed by the NRC in RG 1.182.

Assessment of the risk resulting from maintenance activities

The first stage in the risk-informed maintenance process is to assess the risk increment resulting from the proposed maintenance activities. NUMARC 93-01 states that this assessment should include the consideration of the following aspects:

- Technical specifications requirements
- The degree of redundancy available to perform safety functions normally served by the SSC taken out of service for maintenance
- The duration of the proposed maintenance
- The likelihood of an accident sequence that would require the out-of-service SSC
- SSCs that are affected by some dependency with the maintained SSC.

If desired, the assessment may also consider the comparison of the risk effect between the case where the SSC is maintained during outages and the case where it is performed during at-power operations. The assessment may also take into account the time necessary to restore the SSC to service if the need arises due to an emergency situation, to be compared with the time at which the SSC function would be needed.

Assessment methods for power conditions

The removal from service of a single SSC is usually covered by the Technical Specifications, therefore the assessment may be limited to the consideration of unusual external conditions (e.g. severe weather, offsite power instability ...). However, removal from service of multiple SSCs requires an assessment, performed with quantitative or qualitative (or both) considerations.

1) Quantitative considerations: this can be done using PRA insights. NUMARC 93-01 recommends that this PRA be a Level 1 PRA covering internal initiating events in at-power mode (i.e. mode 1). The use of an expanded PRA (external events, Level 2, other modes of operation) is only optional. If the PRA is not detailed enough to describe the SSC to be removed from service (for example, diesel generators may be modeled as a single component in the PRA model), the assessment should study the effect of the out-of-service component on the safety function of the component modeled in the PRA.
2) Qualitative considerations: such an approach can be performed by addressing the key safety functions affected by the SSC to be removed out of service, as well as the degree of redundancy available. In addition, the licensee may consider implementing "compensatory measures" to address the risk increase due to the maintenance activity (see below). Qualitative considerations may be especially useful to address events and SSCs not within the scope of the available plant-specific PRA.

Assessment methods for shutdown conditions

Except when a plant-specific shutdown PRA is available, the assessment will generally be performed using a qualitative approach, as described previously. However, due to decreased redundancy during outages, the licensee may consider contingencies and backup methods to achieve the key safety functions, as well as measures to reduce the probability and the consequences of potential events.

Risk management

Risk management involves using the results of the risk assessment to control the overall risk impact, through careful planning, scheduling, coordinating, monitoring, and also by taking additional actions beyond routine controls to address risk increases above particular thresholds. It can often be effectively accomplished by making use of qualitative or quantitative insights from the plant-specific PRA.

1) Action thresholds:

If the risk exceeds particular thresholds, compensatory actions would be necessary. The establishment of these thresholds can be based upon qualitative considerations: duration of out-of-service conditions, type and frequency of initiating events addressed by the out-of-service

SSC, number of remaining success paths available to mitigate these initiating events ... It can also be based upon quantitative considerations, using CDF and/or LERF criteria. The product of the incremental CDF (or LERF) and duration gives a probability (ICDP: incremental core damage probability; ILERP: incremental large early release probability). Table 5-2, from NUMARC 93-01, presents performance acceptance thresholds in terms of ICDP and ILERP: if the incremental probability is low (bottom row), no additional action is required; if it is intermediate (middle row), risk management actions shall be taken; and high incremental probabilities (top row) are not allowed in normal conditions.

ICDP	Requirement	ILERP
$> 10^{-5}$	- Configuration should not normally be entered voluntarily	$> 10^{-6}$
$10^{-6} - 10^{-5}$	- Assess non quantifiable factors - Establish risk management actions	$10^{-7} - 10^{-6}$
$< 10^{-6}$	- Normal work controls	$< 10^{-7}$

Table 5-2 : Action thresholds [34]

Alternatively, similar tables can be developed using ICDF (Incremental CDF) and ILERF (Incremental LERF) in lieu of ICDP and ILERP.

2) Risk management actions:

In NUMARC 93-01, four types of risk management actions are considered.

1. Actions to provide increased risk awareness and control:
   - Discuss planned maintenance activities with operating shift and obtain operator awareness and approval of planned evolution
   - Conduct pre-job briefing of maintenance personnel, emphasizing risk aspects
   - Request the system engineer to be present for the maintenance activity,
2. Actions to reduce duration of maintenance activity:
   - Pre-stage parts and materials
   - Preparation, training of the personnel
   - Establish contingency plan to restore out-of-service equipment quickly if needed,
3. Actions to minimize magnitude of risk increase:
   - Minimize other work in areas that could affect initiators to decrease the frequency of initiating events mitigated by the out-of-service SSC

- Minimize other work in areas that could affect redundant systems associated with the out-of-service SSC
- Establish alternate success paths for performance of the safety function of the out-of-service SSC,

4. A threshold should be establish such that risk significant configurations are not entered voluntarily.

5.2.2.5. Use of an Expert Panel

In order to implement different aspects of the Maintenance Rule, licensees typically use an Expert Panel made up of utility employees who have sufficient experience with the plant PRA and with operations and maintenance. The NRC recommends that the Expert Panel be used in particular for the following applications ([32],[35]):

- Members of the Expert Panel should use their expertise in maintenance and operation in conjunction with PRA insights (the importance measures mentioned in 5.2.2.1) to establish the final list of risk significant SSCs. This process enables one to compensate for particular limitations of PRA and risk importance measures, and it makes the process risk-informed rather than risk-based.
- The Expert Panel may be used to provide assistance in defining which SSCs should have goal established and be treated under §(a)(1), and when SSCs should be moved from §(a)(2) to §(a)(1) and vice versa.
- It may also be used to define adequate corrective actions, to define and review the effectiveness of the periodic evaluations (§(a)(3)) and to provide inputs to the configuration risk management program (§(a)(4)).

5.3. Maintenance at EDF

5.3.1. Maintenance regulation

5.3.1.1. Main Regulatory Documents

In France, there is no regulatory document similar to the US Maintenance Rule. Maintenance activities and periodic tests are regulated by the General Operating Rules (RGEs, règles générales d'exploitation), which supplement the preliminary safety report and translate

initial hypotheses and safety study results into operating rules. Among the 11 chapters of the RGEs, the following are of particular interest:

- Chapter III of the RGEs describes the technical specifications (STEs). Details about the STEs are given in Section 6.2.2.
- Chapter IX defines maintenance and testing programs for safety related systems.
- Chapter X defines testing programs regarding core physical tests.

These three RGE chapters need to be formally approved by the safety authority.

In order to improve the safety level and industrial performance, EDF regularly modifies materials and STEs. These modifications may be a consequence of periodic safety reviews or experience feedback. Modifications of the STEs may be permanent, and would then need a thorough review from the ASN. In some circumstances, EDF may temporarily need to go beyond some limits fixed by the STEs. In such cases, EDF must declare a temporary modification of the STEs to the ASN. The ASN will then review this modification, and may give its agreement. In some cases, the ASN may require additional compensatory measures if it deems that the measures proposed by EDF are not sufficient to cope with the consequences of the modification.

5.3.1.2. Operational documents

In addition to the RGEs, EDF uses more operational maintenance documents that are first written at a centralized engineering division level (e.g. for each reactor design), and these documents are then used at a plant level to write plant-specific operational documents taking into account the specificities of each individual plant. Some of these maintenance documents need ASN's approval before being used on site, while some others do not need to be formally approved as long as they respect the RGEs. More specific details about these operational documents are provided with the EDG maintenance case study (Chapter 9).

5.3.1.3. EDF general maintenance policy

In the middle of the 1990s, EDF embarked on a policy of maintenance volume reduction. This is due to several factors (Ref. [37]):

- The duration of refueling outages had significantly increased in the late 1980s (from 7 weeks in 1986 to 12 weeks in 1991 [37]) due to additional regulatory requirements.

- Before the 1990s, the production capacity was higher than the electricity demand, which is no longer the case. Then, it became a necessity to reduce the outage durations to improve the plant availability and meet the demand.
- In terms of costs, operational failures have become more expensive by a factor 3.
- In the 2000s, electricity markets were liberalized; therefore EDF needs to increase its competitiveness.

EDF's objective is to increase its competitiveness while maintaining or improving the safety level of its plants. Maintenance activities have been focused upon systems most significant to safety, radiation protection or operation effectiveness. EDF has developed a maintenance methodology called "Reliability Centered Maintenance" (OMF, Optimisation de la maintenance par la fiabilité), based upon probabilistic and deterministic considerations. Details about this method are provided in Section 5.3.2. More recently, EDF has been implementing a new maintenance strategy called AP913 (see Section 5.3.3).

EDF also takes advantage of the high level of standardization of its fleet of nuclear reactors. Beyond the possibility to standardize to some extent maintenance programs and doctrines, EDF has developed a concept of maintenance based upon "control systems" known as "sample-based maintenance" or "pilot equipment maintenance". This concept is based upon the creation of groups of similar systems or components similarly used in all plants of the fleet. EDF will then closely monitor some of the systems or components in each group, and if no fault has been detected, it reduces the need to control each of these systems or components individually.

5.3.2. Reliability Centered Maintenance

5.3.2.1. Background

Reliability Centered Maintenance (RCM) is a generic term used to describe a systematic approach to the evaluation, design and development of cost effective maintenance programs. This concept originated in the civil aviation sector in the late 1960s, when wide-body jets were being introduced into service. It was then implemented in different sectors, in particular the nuclear industry in the 1980s - 1990s. This process focuses on the functionality of equipment and the critical failure mechanisms that could lead to a loss of functionality. When used effectively,

this methodology can result in the elimination of unnecessary maintenance tasks as well as the identification and introduction of measures to address deficiencies in maintenance programs. It can also result in higher reliability at reduced costs.

Traditional maintenance programs were in the past often time-based, while RCM is often condition-based, with maintenance intervals being based upon equipment criticality and performance data. This methodology was adapted to the nuclear sector by EPRI in 1984, partly motivated by the fact that preventive maintenance programs were often based upon vendor's overly conservative recommendations and that in some cases, too little preventive maintenance was performed on some components that had not been identified as critical, leading to repetitive failures that increased costs and reduced plant availability. The RCM methodology was then adapted and developed by different operating companies around the world, leading to maintenance programs that may all be labeled "RCM" but that may actually differ significantly.

PRA can be useful for several of the typical steps of an RCM methodology, in particular for the following activities:

- System selection, based upon their safety significance (e.g. using importance measures such as RAW, RRW, CDF contribution, Fussel-Vesely, ...)
- Identification of component failure modes, evaluation of failure probabilities
- Determination of component criticality
- Assessment of the impact of proposed changes to the plant safety level.

5.3.2.2. Reliability Centered Maintenance at EDF

Methodology

In 1990, an RCM project was initiated at EDF, called OMF (Optimisation de la Maintenance par la fiabilité). This methodology was first implemented on a pilot system, and in 1991 it was decided to extend the OMF methodology to many other elementary systems. The approach was based upon four major steps:

1) **Identification of critical components**: this identification was based upon the analysis of the consequences of the different failure modes for each component. PRA results were

used to perform this analysis and to rank components and their different failure modes in terms of their contribution to the plant risk.

2) **Critical component failure analysis**: this second step consisted in a further analysis of failure modes and failure causes for components identified as critical. This analysis was performed with tools such as functional analysis, FMECA (Failure Modes Effects and Criticality Analysis), fault trees.

3) **Identification of preventive maintenance tasks**: the goal was to identify maintenance tasks in order to avoid the failures identified in the previous step.

4) **Experience feedback analysis**: the identification of significant failure modes and adequate preventive maintenance tasks requires deep understanding and knowledge of the different degradation mechanisms leading to failures, and experience feedback is essential to perform this analysis. In each EDF plant, data are collected, then centralized and analyzed by experts to evaluate and update reliability parameters.

Concerning this last step, EDF has a strong advantage since EDF plants are very standardized, especially reactors in the same series (900 MWe, 1300 MWe, 1450 MWe). Therefore, the volume of experience feedback data is larger and more valuable than in other companies, and the resulting analysis gains in precision. In addition, this standardization enabled one to perform a single OMF study for all plants within the same series, hence with reduced analytic costs.

Often, the OMF has led to increased in-service surveillance and functional testing while reducing the frequency of the most intrusive (and costly) maintenance tasks, sometimes even abandoning them. Also, the list of critical components identified in the OMF process was often shorter than the one in previous preventive maintenance programs (Ref. [40]).

Current status

From 1992 to 1995, EDF progressively applied the OMF method to develop optimized maintenance programs for 50 elementary systems classified as "high stake systems" in the 900 MWe and 1300 MWe series. From 1995, the implementation of these maintenance programs has been compulsory for all EDF plants. Due to the absence of corporate coordination, reliability-centered preventive maintenance programs were applied by the plants in a heterogeneous way [39]. Therefore, a so-called "Second Generation RCM method" was developed in 2003, which was meant to be simplified.

However, due in particular to difficulties in implementing the OMF on-sites and to low capacity factors, it was decided in 2007 to switch to a new maintenance strategy called AP913, developed by INPO, which is currently being implemented. Elements on this new methodology are given in Section 5.3.3.

Effects of the OMF

Many beneficial changes have been attributed to the use of RCM [39] at EDF:

- Maintenance has been aligned with the objectives of the production process
- Maintenance programs have been justified on a formal basis
- Experience feedback has been incorporated with better consistency
- Improvement of the culture of economic performance in the maintenance personnel
- Non-intrusive maintenance has been enhanced.

In addition to these effects, there have been economic gains directly attributable to the implementation of the RCM method. Typically, these gains were associated with reductions in the frequency of some maintenance tasks, sometimes even the elimination of particular maintenance activities, the replacement of systematic maintenance by inspections, or the use of condition-based and pilot equipment maintenance.

5.3.3. New maintenance strategy: AP913

Background

Due to difficulties in implementing the OMF on-site and to low capacity factors (compared to other countries such as the US, Finland, Switzerland...), it was decided in 2007 to implement a new maintenance strategy, AP913, an equipment reliability process that had been developed by US licensees within INPO in 2001. This implementation has several objectives ([41], [42]):

- To improve the safety level of nuclear power plants, by improving the availability of safety-related systems
- To improve the capacity factor of EDF plants
- To reduce the amount of corrective maintenance
- To standardize the monitoring of systems reliability through the use of a centralized information system
- And, indirectly, to hire new, qualified workers in order to renew the skills of the staff.

AP913 has been implemented by many US licensees. At Exelon, it resulted in a significant diminution of the forced loss rate (from 2.3% in 2003 to 1.3% in 2007) and a drastic reduction in the amount of corrective maintenance (-80% at LaSalle between 2003 and 2007) [42]. However, it is noted in ref. [43] that these benefits could also be associated to some extent with the implementation of the Maintenance Rule, especially §(a)(1) to §(a)(3) of this Rule (see Section 5.2). The Maintenance Rule strongly influenced the development of AP913, which somewhat generalized the treatment of the SSCs under the scope of the Rule to SSCs that are important for plant availability and operation. While EDF is following the example of US utilities in implementing AP913, all the aspects of the Maintenance Rule (§(a)(1) to §(a)(3)) are not necessarily part of this implementation (Ref. [43]).

Basic overview

The AP913 process consists of six basic processes, summarized on Figure 5-1. The first basic process, "scoping and identification of critical components", results in the following classification of components:

- Critical components: their failure can have an effect on plant safety, availability or operation

- Significant components: their failure can have an effect on radiation protection, the environment, the redundancy of some equipment, or can induce small losses of production
- Economic components: those for which preventive maintenance makes sense from an economic standpoint
- Run-to-failure components.

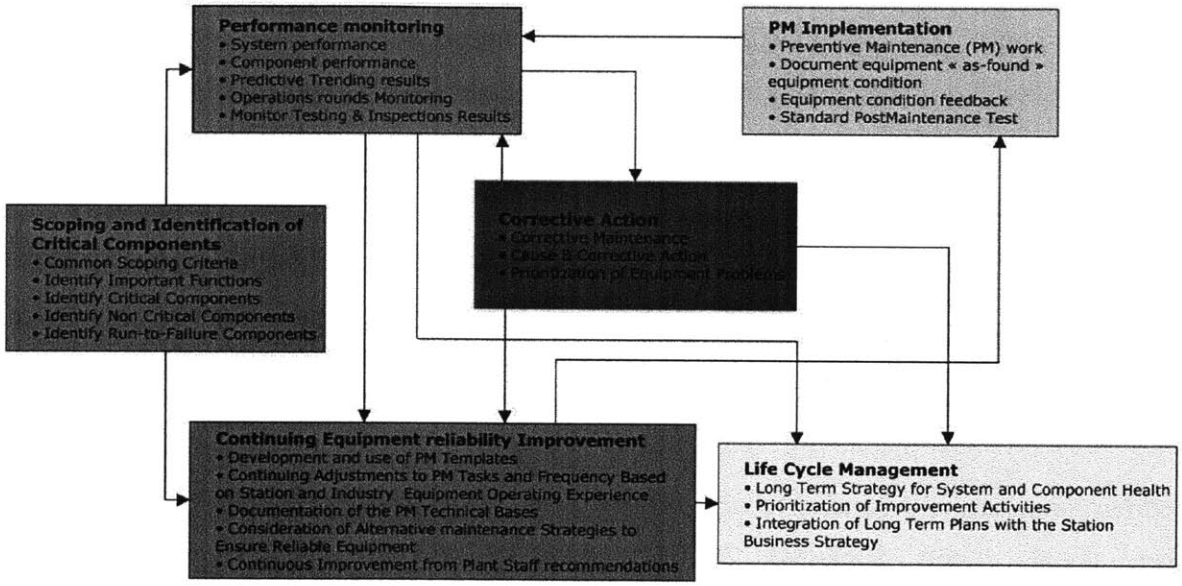


Figure 5-1 : AP913 – Basic processes (from [43])

For each component, this classification is based upon the answers to a pre-established list of questions, such as:

- Could the failure of this component cause a reactor scram?
- Could it cause the actuation of certain safeguard systems?
- Could it generate an event associated with an AOT smaller or equal to 72 hrs?

No probabilistic consideration is involved in this process. Also, based upon a list of questions, each component is further classified as:

- High/low duty cycle
- Severe/mild service condition.

Based upon this classification, maintenance templates are developed for each component, using French and US practices. These maintenance templates will then regularly evolve, taking into account experience feedback. This classification will also be used to help prioritize corrective maintenance.

Surveillance of SSCs

The surveillance of SSCs will be accomplished through the use of an integrated, centralized information system provided by IKS® (Insert Key Solutions). There are two levels of surveillance, one at the plant level and one at the national level. Based upon the use of color-coded performance indicators, surveillance will be made at the component, system and then reactor level. These results will then be integrated, locally and nationally, and maintenance programs may then be modified accordingly.

Impact and differences with the OMF

The implementation of the methodology AP913 is expected to have significant consequences, even though most maintenance programs should not be dramatically modified (current programs will be used to develop new ones), in particular safety-related systems that were already closely monitored [26]. Among the major evolutions brought by this new maintenance strategy ([26], [42]):

- More components (by a factor of 2 to 3) will be subject to maintenance.
- The amount of preventive maintenance will increase, while corrective maintenance should decrease (hence resulting in higher capacity factors). The duration of refueling outages is not expected to change.
- New workers will be hired, and the reliance on sub-contractors is expected to decrease.
- Maintenance programs should evolve more quickly, taking into account experience feedback at the local, national, but also international levels, thanks to the use of the integrated information system.

In contrast to the OMF, AP913 brings several novelties, in particular ([42],[26]):

- A significant increase in preventive maintenance
- More focus will be placed upon some non-safety related systems, such as those that have potentially high economic effects (e.g. the turbine, the alternator ...)

- AP913 is expected to be more pragmatic and easier to understand and use for those that actually perform maintenance or analyze maintenance results, in particular thanks to the IKS® software and the use of color-coded performance indicators.

While PRA insights were often used to help identify critical components within the OMF methodology, it is no longer the case with the implementation of AP913 at EDF (while it is usually the case in the US for SSCs under the scope of the Maintenance Rule).

5.4. Summary

While similar overall maintenance strategies may be used by French and US nuclear facilities (such as the methodology AP913, which is already used by many US companies and is being implemented at EDF), there are however two significant differences regarding general maintenance regulation and practices:

- The Maintenance Rule: there is no equivalent of this rule in the French system, neither in the regulations nor in EDF practices. It concerns paragraphs (a)(1) and (a)(2) of the Rule (establishment of performance criteria, at SSC or plant level), as well as paragraph (a)(4) (risk assessment and requirements for risk management actions when planning and performing maintenance activities). While there appears to be no equivalent of §(a)(1) and §(a)(2) within the French system, we will see that there is however a sort of deterministic counterpart of §(a)(4) (see "Simultaneity Rules", in Section 6.2.2).
- The use of PRA in maintenance-related matters: while PRA is commonly used by US licensees, in particular to comply with some requirements of the Maintenance Rule (risk significance determination process, maintenance planning, configuration risk management), this is not the case in the French system. PRA insights were previously used within the OMF methodology to assess the criticality of components, but this is no longer the case with the AP913 strategy.

Chapter 6

Online Maintenance – Regulation and practice

6.1. Online maintenance in the United States

6.1.1. Introduction

Online maintenance is defined by EPRI in [44] as maintenance that is performed while the main electric generator is connected to the grid. Online maintenance has always been used for some non-safety significant SSCs, but its use has been extended in the US to particular safety-significant SSCs, as well as SSCs that are important for plant availability. Nowadays, online maintenance is more used in the US than in many other countries [44]. The use of online maintenance has been increased in US nuclear facilities for operational reasons, but also for safety reasons. In particular, much attention was paid to the issue of online maintenance in the US after the 55-minute station blackout that occurred at the Vogtle nuclear power plant in 1990 while the reactor was in shutdown and one EDG was undergoing maintenance. While formerly shutdown risk had not been subject to much concern, it was then reconsidered, and performing online maintenance (not only for EDGs) appeared to make sense from a safety and operational point of view.

The benefits of online maintenance have been widely recognized (see ref. [44] (EPRI), [28] (IAEA), for example): improved equipment reliability, shorter and simpler refueling outages, better work planning, reduced stress on workers, longer fuel cycles ...

The use of online maintenance increased in the 1990s, after the introduction of mature risk-informed approaches that enabled licensees to apply online maintenance in a more

consistent way, taking into account the safety effect of multiple outages. But many US nuclear facilities began applying online maintenance more systematically after the enforcement of the Maintenance Rule [44], which was one of the first risk-informed, performance-based regulations in the US. Further, the favorable operational and safety experience of US plants has been consistent with expectations for such beneficial results.

6.1.2. Regulatory aspects

Maintenance and testing activities in US nuclear power plants are governed by the plant technical specifications (see Section 6.1.3 for details), which are part of the operating license, and by the Maintenance Rule (10 CFR 50.65) and related documents ([32], [33]), presented in Section 5.2. Licensees must comply with the AOTs and STIs prescribed by the Tech Specs and with the additional required actions that may be associated with particular Tech Specs action statements (or LCOs, Limiting Conditions for Operation).

Beyond that, in general, licensees are allowed to perform online maintenance and tests after having performed an assessment of the risk generated by the proposed maintenance configurations, providing that they manage the potential risk increase that may result from these activities (§(a)(4) of the Maintenance Rule), before and during the maintenance activities. This assessment is reviewed by resident NRC inspectors on a routine sampling basis, under the ROP, and in more depth by region-based inspectors on a periodic basis.

It should be noted that some periodic tests are required by the Tech Specs to be performed during plant shutdown. Also, licensees may apply for temporary relief from technical specifications that currently prohibit some maintenance activities during at-power operation.

Additionally, some aspects linked to the Reactor Oversight Process may limit particular online maintenance activities. Within the ROP, the NRC uses performance indicators to assess the safety level of US plants. Among these performance indicators, the MSPI (Mitigating System Performance Index) monitors the readiness of some important safety systems (emergency AC power systems, high pressure injection systems, heat removal systems, cooling water systems) to perform their safety functions in response to abnormal events. The principle of the MSPI, which consists in fact of several indicators (one for each type of monitored system), is to evaluate the CDF increase associated with each type of systems, and then, based upon particular thresholds, a

color is assigned (green, white, yellow, red). A degradation of the MSPI value may result in an increased regulatory oversight. As a result, licensees must to limit the unavailability of these safety systems, in particular when performing online maintenance on these systems.

6.1.3. Technical Specifications

6.1.3.1. Background

10 CFR 50.36 requires that each operating license contain technical specifications that are derived from the analyses and evaluations included in the safety analysis report, describing operational conditions required to provide adequate protection to public health and safety. Technical Specifications cannot be changed by licensees without NRC's approval.

As part of its regulatory standardization effort, the NRC issued in 1992 vendor-specific "improved Standard Technical Specifications" (STS) for each of the four nuclear reactor vendors. These improved STS were the result of extensive technical discussions among the NRC, owner groups, vendors and NUMARC (now NEI). While the use of these STS is not mandatory, the NRC strongly encourages licensees to update their TS (with NRC's approval still required) to be consistent with the vendor-specific STS (Ref. [46]). Their implementation is thought to improve the safety of nuclear power plants as well as the efficiency and the consistency of NRC action.

Since 1992, numerous changes have been made to the improved STS through cooperation between the NRC and the industry, represented by the owner groups and the NEI TSTF (Technical Specifications Task Force). Since 1993, a majority of US plants have converted their TS to Improved Technical Specifications (ITS) based upon the applicable vendor-specific STS [47], although some plants still use early custom technical specifications. In addition, over the past several years, most plants have requested TS changes using risk-informed approaches based upon Regulatory Guides 1.174 and 1.177 (nearly 100 such requests have been approved in the past ten years [48]), and these changes are generally not reflected in the corresponding STS.

The Tech Specs consist of:

- LCOs, such as a system unavailability, associated with specific required actions and a completion time (AOT)

- Surveillance requirements (SRs) (including periodic tests), associated with a certain frequency (or STI).

6.1.3.2. Voluntary entry into an LCO

Performing online preventive maintenance often requires intentionally entering a TS event for the affected SSC. But, contrary to the French case (see below), there is no particular requirement in the technical specifications regarding the voluntary entry into an LCO, and an intentional entry into an LCO is not a violation of the Tech Specs (except in particular cases when it is associated with a change of reactor operational mode, see Section 7.2.2) [49]. According to the NRC (ref. [50]), acceptable reasons for doing so include: performance of surveillances (including periodic tests, except in particular cases), preventive maintenance, or investigation of operational problems. Also, intentional entry into a TS event that would result in redundant systems being simultaneously inoperable should be avoided [50].

There are several reasons for which the NRC allows such behaviors, in particular (ref. [49]):

- The time needed to perform most surveillances is usually a small fraction of the AOT of the corresponding SSC
- The benefit to safety (higher reliability, verification of the operability) of the surveillance tasks is considered to more than compensate for the risk increment associated with the unavailability of the SSC.

Additionally, the NRC makes the following recommendations [49]:

- The licensee should not abuse the allowance to perform online maintenance by repeatedly entering and exiting TS events
- The licensee should have sufficient confidence in the operability of the SSC that is redundant to the out-of-service one
- When performing online maintenance, the licensee should avoid performing other maintenance activities that may increase the likelihood of a transient.

As always, when taking an SSC out of service, the licensee must:

- Comply with the corresponding TS required actions and AOT (otherwise, the licensee may have to shut the reactor down)

- Comply with the requirements of the Maintenance Rule

In practice, compliance with §(a)(4) of the Maintenance Rule ensures that the risk. associated with the planned maintenance configuration is assessed and managed, while the TS usually cover single outages only or a very limited set of combined outages (e.g. two redundant SSCs, an SSC and a support SSC, ...). However, it does not exempt the licensee from complying with the Tech Specs requirements. It can result in conflicts between the results of the Maintenance Rule risk assessment and the requirements of the Tech Specs. For example, the risk assessment may show that taking an SSC out of service for a duration longer than the AOT prescribed in the TS would be acceptable. In such cases, the licensee must either comply with the AOT provided in the Tech Specs or ask the NRC for a TS temporary exemption (via a Notice of Enforcement Discretion, NOED), which can be resource consuming for both the licensee and the NRC. This issue is being addressed through the development and the implementation of the risk-informed technical specifications (see Chapter 7).

6.1.4. Online maintenance: practice and results

Practice

As is explained in the previous section, voluntary entry into TS LCOs for online maintenance has been possible for decades. However, even if not prohibited, multiple simultaneous LCOs were considered not to be recommended, and hence of limited potential for online maintenance. With the advent of PRA and the promulgation of the Maintenance Rule, this situation changed: the intrinsic weaknesses of the technical specifications, in particular regarding multiple outages, could then be complemented by the risk assessment and management required by §(a)(4) of the Maintenance Rule, using, in particular, probabilistic tools. Closely linked to the enforcement of the Maintenance Rule is the use of software-based On-line Configuration Risk Management Tool, or risk-monitor. In 1996 (end of the Maintenance Rule implementation period), most plants were using or planning to use such tools [44].

To help licensees decide between online and offline (= during outages) maintenance, and to help them apply good online maintenance practices, guides have been developed, such as the EPRI guide *Guidance for developing and implementing an on-line maintenance strategy* [45], and forums and working groups were created so that licensees may share and discuss their

practices, such as the Configuration Risk Management Forum and the Maintenance Rule Users Group, created in the 1990s.

As shown in Table 6-1, about one half of components in an average US nuclear power plant are maintained through preventive maintenance programs (for critical and important components). In ref. [44], it is reported that all US licensees (that responded to the survey) apply some sort of online maintenance, and that more than 80% apply online maintenance to some safety-significant SSCs. As shown on Figure 6-1, overall, more than 70% of maintenance is performed online. Expectedly, this figure also shows that online maintenance is more widely applied to non-safety-significant SSCs (about 80% of them are maintained online), but nearly half of safety-significant SSCs are subject to online maintenance in a typical US plant.

Component Type	Percentage
Critical	22 %
Important	26 %
Run-to-failure	43 %
Not classified	9 %

Table 6-1 : Component classification [44]

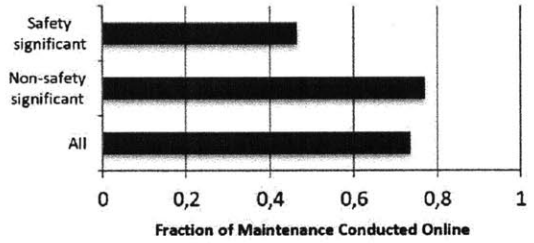


Figure 6-1 : Use of online maintenance [44]

Results

While some were concerned that industry's efforts to improve plant performance (including online maintenance) could compromise plant safety, industry data have proven otherwise, showing that operational performance and plant safety are not mutually exclusive:

- Figure 6-2 shows a significant reduction in refueling outage durations
- Between the late 1980s and today, most US plants extended the duration of their refueling cycle from 12 months to 18 or 24 months [44]
- Figure 6-4 shows a significant increase in the average capacity factor
- And, in the same time, the automatic scram rate has been reduced by a factor of five (Figure 6-3) and the US average CDF has decreased (Figure 6-4), reflecting plant safety improvement.

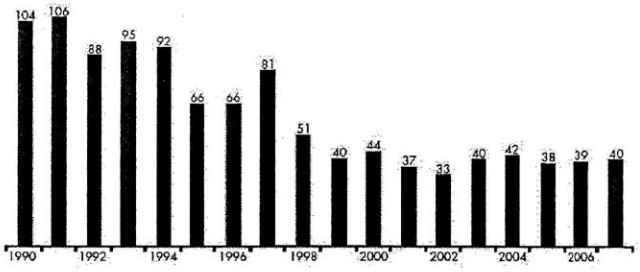


Figure 6-2 : Average refueling outage duration, in days [44]

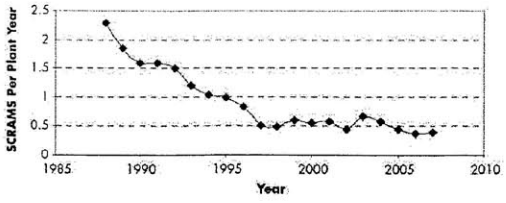


Figure 6-3 : US automatic scram rate [44]

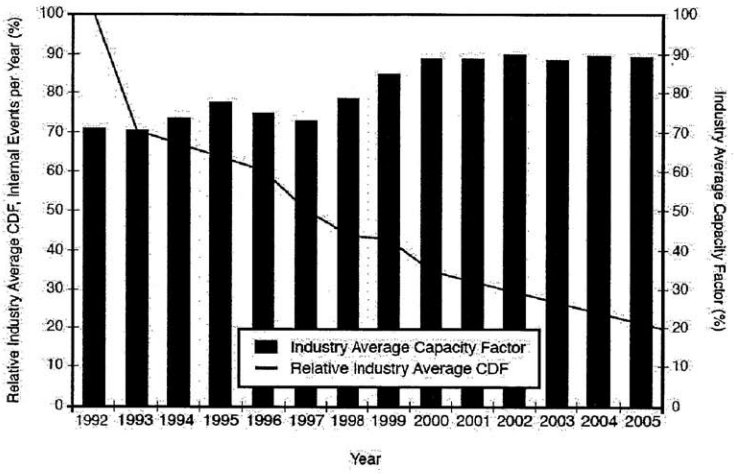


Figure 6-4 : Average capacity factor and CDF [44]

Of course, online maintenance is not the only cause of these improvements, but it is recognized as a major element, in particular regarding the reduction of refueling outage durations [44]. There are also other interesting effects that may be more difficult to quantify:

- Improvement of the safety culture, the staff being more aware of the risk importance of SSCs during at-power operations
- Less stress on workers when performing online maintenance, because of better preparation and exposure to fewer distractions than during refueling outages
- As a result, smaller risk of human errors.

6.2. Online maintenance in France

6.2.1. Regulatory aspects

In France, as in the United States, there is no specific regulation for preventive maintenance and testing of safety-related systems during operation: during outage or during operation, the licensee must comply with the technical specifications (STEs). No risk assessment is required before and during maintenance activities (even when an unexpected event occurs), contrary to the US case (Maintenance Rule §(a)(4)). However, there are significant differences in the treatment of voluntary entry into Technical Specifications and multiple outages, so that the STEs are assumed to be sufficiently conservative to avoid any configuration that would be unacceptable from a risk standpoint, hence no additional requirement. All these aspects are presented in the following section.

6.2.2. Technical Specifications (STEs)

6.2.2.1. Introduction

The Technical Specifications (STEs) constitute the third chapter of the General Operating Rules (RGEs). The STEs used on site are made up of three sections: (1) The standard document, which is valid for all reactors of the same series; (2) Site-specific complements to the standard document; and (3) generic complements to the standard document. Here, we shall focus on the standard document of the 1300 MWe series [51].

The RGEs are a direct extension of the Safety Report: they define specific rules that have to be respected in order to stay in the framework of the safety assessment presented in the Safety Report. Within the RGEs, the STEs have 3 main roles:

1) Establish boundaries for normal operating conditions in order to remain within the design limits of the systems
2) Define the essential safety functions that are necessary to maintain the integrity of the different barriers and to ensure the operability of the safety systems
3) Define required actions if these conditions are no longer met.

The standard document of the STEs has been approved by the Safety Authority and cannot be modified without its prior approval.

The STEs are organized differently from US Technical Specifications. First, they contain only TS events, with the associated allowed outage times (referred to as Shutdown Initiation

Times) and potential additional requirements. Surveillance requirements (periodic tests) are not treated in the STEs. Then, while US Technical Specifications are organized by systems or functions, French STEs are first organized by reactor states, then by systems or functions. An elementary definition of the different reactor modes is given in Table 6-2 (see [51] for more details).

Reactor Mode	Original Abbreviation	Simplified Description
At-Power Operation	RP	The reactor is critical or becoming critical
Normal Shutdown with Heat Removal by Steam Generators	AN/GV	Primary pressure between 27 and 155 bars, primary coolant mean temp. between 160 and 297.2 °C
Normal Shutdown with Heat Removal by RHR (Residual Heat Removal) System	AN/RRA	Primary pressure between 5 and 31 bars, primary temperature between 10 and 180 °C
Shutdown for Maintenance	API	Primary pressure $\leq$ 5 bars, primary temperature between 10 and 60 °C, heat removal by RHR system
Shutdown for Refueling	APR	Heat removal by RHR system
Completely Unloaded Core	RCD	

Table 6-2 : Reactor Modes

Events treated in the technical specifications are organized into two categories, group 1 and group 2 events, which are treated differently throughout the STEs. In order to determine whether an event should be labeled as group 1 or group 2 event, a probabilistic methodology has been developed, but it is still at an R&D stage [26]. Therefore, this process is still based upon a deterministic approach.

6.2.2.2. Group 1 Events

Definition

Group 1 events are TS events that involve important design hypotheses, shutdown systems and safety systems. Within this group, we find events that cause an increase in the risk of barrier deterioration (cladding, primary circuit, containment) and that can have unacceptable radiological consequences.

Required Actions

Generally, a group 1 event is associated with a Shutdown Initiation Time, which is the time by which:

- Repair has been performed, and the event has disappeared, or
- Reactor shutdown has been initiated, if required by the STE, or
- Prescribed palliative measures are effective, when no shutdown is required

If the licensee establishes that repair cannot be performed before the end of the Shutdown Initiation Time, then he must initiate the reactor shutdown as soon as possible. Once reactor shutdown has been initiated, transitions from one mode to another have to be done within maximum time durations that are prescribed in the STEs.

Planned events

1) For preventive maintenance and common operations: in general, the licensee is not allowed to enter a group 1 event voluntarily, unless when a "Borderline Condition" ("Condition Limite") has been granted, which provides some flexibility for performing preventive maintenance or common operating actions. Such Borderline Conditions are created and granted when a strong need for more flexibility regarding a specific TS event is expressed by the licensee. In particular, when no such need is expressed, no Borderline Condition is created. Even though the terms are subject to interpretation, it is mentioned in the STEs (ref. [51], section "Definitions") that these Borderline Conditions should be used only for "operational imperatives". Implicitly, this means that, originally, they are not meant to be used for online maintenance tasks when there is no technical "imperative" to carry out these tasks online. These Borderline Conditions have usually a probabilistic justification [24]. It should also be noted that even when a group 1 event is voluntarily entered, Simultaneity Rules (see below) are applicable.

2) For periodic tests: the licensee is allowed to enter group 1 events in order to perform a periodic test defined in the RGE only when these group 1 events have been explicitly identified in the associated Periodic Test Rules (Règle d'Essais), and Simultaneity Rules are still applicable. However, in the philosophy of the RGEs, it seems that such generic exemptions are defined when there is a technical need to generate a group 1 event to perform the considered periodic test, and not for operational convenience (ref. [87]).

In any of these two cases, the licensee is not allowed to voluntarily enter a group 1 event if:

- A group 1 event is already occurring
- The reactor is not in a stable state regarding neutronic and thermal-hydraulic parameters
- An incident or accident procedure is ongoing.

Simultaneity Rules

When several TS events affecting different elementary systems are simultaneously occurring, some rules have to be respected, regardless of the planned/unplanned aspect of these events. These Simultaneity Rules are defined separately for group 1 and group 2 events.

1) Simultaneous group 1 events in modes RP, AN/GV, AN/RRA

If several group 1 events occur simultaneously, the reactor has to be shut down to the mode corresponding to the lowest mode prescribed for these group 1 events (see Table 6-2 for the definition and the ranking of the different reactor modes). For example, if the reactor is in mode RP (at-power operation) and two group 1 events occur simultaneously, one being associated with a shutdown mode AN/GV, the other with a shutdown mode AN/RRA, then the reactor has to be shut down to the mode Min{AN/GV, AN/RRA}, i.e. AN/RRA, according to Table 6-2.

Then, the Shutdown Initiation Time shall be as indicated in the third row of Table 6-3.

Number of group 1 events simultaneously occurring	> 2	2		
Shortest Shutdown Initiation Time prescribed for these individual events	/	≤ 8 hrs	]8 hrs , 24 hrs]	> 24 hrs
Shutdown Initiation Time	1 hr	1 hr	8 hrs	24 hrs

Table 6-3 : Shutdown Initiation Time for multiple group 1 events

2) Simultaneous group 1 events in modes API, APR, RCD

The simultaneous occurrence of several group 1 events shall not last longer than 24 hours, and a safety analysis shall be performed to determine the best course of actions.

6.2.2.3. Group 2 Events

Definition

Group 2 events are events that could impair control, diagnostic capability, or the effectiveness of actions undertaken in case of an anomaly.

Required Actions

In general, group 2 events are associated with a Repair Completion Time and, in some cases, compensatory measures.

Planned events

The licensee is allowed to enter group 2 events voluntarily for preventive maintenance, for periodic tests or common operations as long as the required actions are performed within the prescribed Repair Completion Times and Simultaneity Rules are respected (see below). Also, the licensee is not allowed to take two redundant systems out of service voluntarily.

Simultaneity Rules

1) Simultaneous group 2 events in mode RP

If five group 2 events affecting different elementary systems are simultaneously occurring, shutdown to AN/GV mode must be initiated within 24 hours. If there are more than five group 2 events, reactor shutdown must be initiated within 1 hour.

2) Simultaneous group 2 events in modes AN/GV, AN/RRA, API, APR, RCD

The simultaneous occurrence of five group 2 events affecting different elementary systems shall not last longer than 24 hours, and no more than 1 hour for more than five group 2 events.

6.2.2.4. Transition between reactor modes

Except in cases when a reactor shutdown is explicitly required by the STEs, some simple rules have to be respected when the licensee wishes to go from one reactor mode to another:

1) The licensee is not allowed to make the reactor critical if a group 1 event is currently occurring or if more than four group 2 events affecting different elementary systems are currently occurring.

2) The licensee is not allowed to go to another reactor mode if it would generate (in the final mode or in an intermediary one) a group 1 event or more than four group 2 events affecting different elementary systems.

6.2.3. Practice and barriers

In France, while online maintenance is certainly applied for non-safety-significant systems, this is rarely the case for safety-significant SSCs. It has been reported to us in interviews that online maintenance is not in the culture of the operator, and that, on the whole, EDF's management and the safety authority are currently satisfied with the quality of maintenance being performed during refueling outages. In particular, as long as the operator complies with the STEs and the Simultaneity Rules, the configuration risk is considered to be sufficiently managed, both within EDF and the safety authority. The need to further assess the safety level, for example by performing a risk assessment as that required in the United States by the Maintenance Rule, is not widely felt. It is however true that French STEs are much more restrictive than US Tech Specs regarding the issues of voluntary entry into Tech Specs and multiple outages, through the use of prescriptive, systematic Simultaneity Rules. Hence a smaller need for such risk assessment exists. Nevertheless, a probabilistic risk analysis of planned maintenance configurations may enable the operator to assess the conservatism of these STEs, and, in some cases, to reveal possible weaknesses.

The consequence of current French STEs is that online maintenance is usually not allowed for SSCs associated with a group 1 event (i.e. safety-significant SSCs), unless when a "Borderline Condition" has been defined. But even in this case, such Borderline Conditions are often very restrictive, as is shown subsequently with the example of EDGs, hence allowing little freedom for online maintenance to occur. Also, as is mentioned in Section 6.2.2.2, Borderline Conditions were originally meant to be used for "operational imperatives", and not in order to permit on to perform online maintenance when there is no technical need to do this online (although the terms of the instructions are subject to interpretation). As for periodic tests, group 1 events can be entered only when it is technically necessary and when they have been explicitly identified in the associated Periodic Test Rules (a distinction is made between "preventive maintenance", for which Borderline Conditions apply, and "periodic tests", covered by Periodic Test Rules). There is therefore very little flexibility with current STEs to allow one to perform

online maintenance/testing. Even planning of maintenance during refueling outages is complicated due to the Simultaneity Rules [26].

In addition to these regulatory barriers, there exist other barriers to the use of online maintenance that have been reported [26]. Even though there may be an interest in online maintenance, especially for economic reasons (shorter refueling outages, higher capacity factor, better SSCs reliability...), there are other considerations that prevent going further in this direction: the need to stabilize maintenance practices and to avoid frequent changes, the feeling that questioning the STEs and the Simultaneity Rules is unacceptable, and the difficulty regarding the acceptance of these practices by the ASN.

6.3. Summary

While US technical specifications provide much flexibility for intentionally entering Tech Specs LCOs for online maintenance and periodic tests, French STEs are much more restrictive regarding this aspect and multiple outages. In the United-States, the Maintenance Rule requires licensees to assess further the risk associated with maintenance configurations, for planning but also to evaluate the impact of unplanned events when performing maintenance activities. While this requirement could have been seen as an additional burden for the operators, it actually enabled them to assess better the effect of multiple outages (during operation and refueling outages). This, coupled with the development of configuration risk management tools (risk-monitors), has effectively supported the development of online maintenance practices for risk significant SSCs (and it also supported maintenance planning and optimization during refueling outages). The consequences of an extended use of online maintenance are difficult to quantify, but studies have shown that such practices have efficiently contributed to operational as well as safety improvements. In France, the rigidity of the STEs, obstacles to the use of a risk-monitor (and more generally towards the use of risk information at the operational level) and cultural barriers all constitute difficulties in the development of online maintenance practices for safety-related systems.

Chapter 7

U.S. Risk-Informed Technical Specifications

7.1. Project description

7.1.1. Introduction

Traditionally, Technical Specifications have been addressing configuration control through specifying AOTs and actions, typically leading to plant shutdown when these AOTs are exceeded. Until very recently, US Technical Specifications were primarily based upon the deterministic design basis accidents (even though some may have been justified using PRA insights), with no consideration for the configuration-specific plant risk effect as a factor in the action requirements. In addition, Technical Specifications usually do not cover configurations involving multiple out-of-service equipment.

It has been recognized that plant configuration control can have significant temporary effects upon risk profiles, hence the addition in 1999 of §(a)(4) of the Maintenance Rule that requires a risk-informed plant configuration control. However, it has been recognized that in many instances, the deterministic TS control requirements and the risk-informed Maintenance Rule plant configuration control requirements are in conflict, while the licensee is required to comply with both. For this reason (among others), risk-informed technical specifications have been studied in order to address these incompatibilities and to provide a single, consistent treatment for plant configuration control. As appears in the following sections, these risk-informed initiatives are completely relevant to the issues of online maintenance regulation and practice in the United States.

It is important to make a clear distinction between these risk-informed TS Initiatives and "classic" TS where AOTs or STIs may have some risk-informed justification, but remain fixed, no matter what is the current plant configuration. Here, we are talking about risk-informed TS in the sense that they are based upon the current, configuration-specific risk, and not just on a fixed plant risk, as is the case when PRA is used in order to justify classic, fixed AOTs or STIs.

7.1.2. Benefits

Several benefits are expected from use of risk-informed technical specifications. A first benefit would be improved plant capacity factors and safety through the avoidance of shutdowns required by the technical specifications. Indeed, in many cases when a shutdown is required by the technical specifications, it is not the safest course of action, as a change of the plant state creates opportunities for transients and human errors. Such situations have been addressed between the licensee and the NRC on a case-by-case basis, through the use of "Notices of Enforcement Discretion" (NOEDs) that are resource consuming for both the NRC and the licensee. This process involves the use of risk-informed methods for justifying the avoidance of the shutdown required by the Tech Specs. Avoidance of this process through the use of risk-informed technical specifications would eliminate the need for exceptions to requirements, with the associated outcome uncertainty, and would provide enhanced regulatory consistency [52]. In addition, risk-informed specifications would provide more flexibility for online maintenance, hence further reduction in outage duration and better plant capacity factor. Currently, plants have often optimized their online maintenance programs to the extent feasible given their current TS, which has already enabled them to achieve shorter planned outage durations.

Initially, the risk-informed TS project was defined as eight separate initiatives intended to improve existing TS requirements through the use of risk information. In the following sections the most advanced and/or most ambitious of these risk-informed TS Initiatives are presented.

7.2. Risk-informed Initiatives 2 and 3

7.2.1. Risk-informed Initiative 2

7.2.1.1. Background

Until 2001, Technical Specifications required that, when a surveillance requirement was not performed within the prescribed surveillance test interval, the corresponding LCO (Limiting Condition for Operation) should be entered, potentially leading to a plant shutdown requirement. However, this course of action is not always the safest (Ref. [52]): indeed, there are cases where a missed surveillance cannot be performed without an operational mode change whose risk effect may actually be higher than that involved in deferring the surveillance, and shutting the reactor down may also have a higher risk than deferring the performance of this surveillance. In addition, in most cases the equipment remains capable of performing its function even though some surveillance has been missed. The goal of the proposed change was to allow that a missed surveillance may be rescheduled using the results of the configuration risk management program associated with the Maintenance Rule (§(a)(4)).

7.2.1.2. Past regulation versus proposed regulation

In the STS (e.g. Ref. [50]), Surveillance Requirement (SR) 3.0.2 specifies that a surveillance is considered to have been performed in due time if it has been performed within 1.25 times the prescribed interval, i.e. the licensee is granted 25% time in addition to the specified STI. After that, the surveillance is considered to have been missed.

Until 2001, when a surveillance requirement was missed, SR 3.0.3 allowed the licensee to delay the requirement to declare the LCO not met for up to 24 hours, or up to the limit of the specified STI, whichever was less (i.e. no more than 24 hours). After that, the LCO was considered not to have been met, and required actions had to be taken, potentially leading to a shutdown requirement if the surveillance was not successfully performed within the AOT of the system.

Risk-informed Initiative 2 was proposed to modify SR 3.0.3 in order to grant more time to perform a missed surveillance without having to declare the LCO not met. More specifically, the Initiative 2 proposed to modify SR 3.0.3 so that it would allow the licensee to delay the requirement to declare the LCO not met up to 24 hours or up to the limit of the specified STI, whichever was greater, so that the licensee could have enough time to perform this missed surveillance. In addition, modified SR 3.0.3 would require that the licensee performs a risk

evaluation for any surveillance delayed by more than 24 hours, and that the risk effects be managed (Ref. [64]).

7.2.1.3. Status of the Initiative

This initiative was approved be the NRC in 2001, and it has been incorporated into the vendor-specific STS in the framework of their last revision. In addition, this STS modification has been adopted by all except two plants [54].

7.2.1.4. Rationale of this risk-informed Initiative and implementation details

Assuming that a system or component is inoperable when a surveillance test has not been performed is deemed to be overly conservative [64]. Indeed, the vast majority of surveillances do in fact demonstrate that the systems or components are operable.

Because the AOT (which starts as soon as the LCO is entered) of some systems is too short for performing the missed surveillance before shutdown is required, it was deemed that the Technical Specifications should grant a sufficient time limit before having to enter the LCO such that the licensee could have sufficient time to perform the missed surveillance. The previous time limit before having to declare the LCO not met, *min*(24 hrs, limit of the specified STI), was often too short to perform the missed surveillance, while the proposed (and accepted) time limit, *max*(24 hrs, limit of the specified STI), was deemed acceptable [64]. Indeed, surveillances that have an STI smaller than 24 hours typically involve straightforward monitoring activities, and can therefore be performed within 24 hours when they have been missed, while other surveillances are more significant and could not be performed within 24 hours.

In addition, the Tech Specs Task Force has surveyed that between 1996 and 2001, more than 10 NOEDs regarding missed surveillances had to be issued by licensees and processed by the NRC, which is considered to be an unnecessary use of NRC and industry resources (Ref. [64]).

While *max*(24 hrs, limit of the specified STI) is provided to perform the missed surveillance, the NRC expects (STS, vol. 2) that the missed surveillance will be performed "at the first reasonable opportunity".

The risk effect should be assessed and managed through the program already in place to implement paragraph (a)(4) of the Maintenance Rule, using quantitative or qualitative methods, or both, using a degree of depth and rigor commensurate with the safety significance of the component for which a surveillance has been missed. Therefore, the implementation of this risk-informed TS initiative uses existing programs and methods only, hence it imposes no additional burden.

7.2.1.5. Situation in France

In France, the licensee has a $\pm$ 25 % margin on the Surveillance Test Intervals with respect to the periodicity specified in the French regulatory documents regarding periodic tests. However, if the periodic test has not been performed within this margin, then the surveillance requirement is considered not met, the licensee must implement compensatory measures, the associated component is considered to be inoperable and the corresponding technical specification action statement is immediately entered (possibly leading to a plant shutdown). Therefore, the situation in French nuclear power plants is even more stringent than in the two US plants where Initiative 2 has not been implemented (these two plants are granted up to 24 hrs before entering the TS event).

7.2.2. Risk-informed Initiative 3

7.2.2.1. Background

Until 2003, Technical Specifications specified that a plant could not enter a mode in which an LCO would become applicable (with some exceptions). In particular, a plant was not allowed to go to higher operational mode (e.g. full power mode) if a Tech Specs LCO was ongoing, which means that if one system required to be operable in full power mode was not operable when the reactor was still in shutdown state, the reactor was not allowed to start up, while if it had already been in the full power mode, it would have been allowed to continue operations without shutting the reactor down for the duration of the corresponding AOT. The goal of risk-informed Initiative 3 was to resolve this discrepancy, by allowing entrance into the higher operational mode while the system is inoperable, and then entering the LCO applicable to the higher mode (i.e., the system has to be made operable before the end of its AOT, otherwise the reactor must be shut down).

7.2.2.2. Past regulation versus proposed regulation

Before 2003, in the STS, LCO 3.0.4 specified that it was not allowed to enter a mode such that an LCO previously not met would become applicable (except in cases where the associated actions permitted continued operation for an unlimited period of time in this new mode). Risk-informed Initiative 3 proposed to modify LCO 3.0.4 in order to allow entry into a mode where an LCO previously not met becomes applicable if one of the following conditions is met (Ref. [50]):

a) When the associated actions that would have to be entered permit continued operation in this new mode for an unlimited period of time (i.e., same condition as before 2003),
b) After performance of a risk assessment addressing inoperable systems and components, determination of the acceptability of entering this mode where the LCO becomes applicable, and establishment of compensatory measures, if necessary,
c) In individual cases where it is specifically allowed.

The novelty brought by risk-informed Initiative 3 essentially concerns point b).

7.2.2.3. Status of the Initiative

This initiative was accepted by the NRC in 2003, and it has been incorporated into the vendor-specific STS in the framework of their last revision. In addition, this STS modification has been adopted by 85% of the utilities [66].

7.2.2.4. Rationales for this risk-informed Initiative and implementation details

As is mentioned in Section 7.2.2.1, there was earlier in LCO 3.0.4 some kind of discrepancy: when an LCO became applicable when the reactor was already in a given mode, the licensee was allowed to continue operation for the duration of the corresponding AOT, providing him with some time to repair the problem without having to shut down the reactor immediately, while if the component was already inoperable in another mode where it was not required, the licensee was in general not allowed to enter the same mode as earlier where the component is required to be operable.

This situation caused some trouble to licensees, and many systems or components were given individual LCO 3.0.4 exceptions (almost all the LCOs with AOT greater than or equal to

30 days, and many of the LCOs having AOTs greater than or equal to 7 days) (Ref. [65]). LCO 3.0.4 was thought to be overly conservative: indeed, unit startups were frequently delayed due to the restrictions imposed by LCO 3.0.4. For example, a single maintenance activity that was almost complete could cause significant delays and changes in the plans for returning the unit to service, while allowing the unit to enter the mode where the LCO becomes applicable would allow the maintenance task to be completed (without exceeding the applicable AOT, otherwise the unit would have to be shut back down) while possibly reducing the likelihood of human error caused by expediting the completion of the maintenance task before the scheduled startup.

Another rationale for this modification of LCO 3.0.4 is that when the unit goes up in mode (i.e. in power), the complement of systems available to mitigate particular events is increased. In most cases, going to higher operational mode from shutdown cooling results in lower risk due to termination of shutdown cooling and the additional mitigation capability provided by steam driven systems at higher power modes [65].

There are however cases where the risk may increase when the reactor goes to higher modes. In such cases, there are notes in the technical specifications that specifically prohibit the use of LCO 3.0.4.b when some system is inoperable. For Westinghouse PWRs, systems that were determined to be "higher risk" systems to which LCO 3.0.4.b should not be applied are presented in Table 7-1 (see Table 9-1 for a definition of the operational modes).

System	Mode(s) that cannot be entered under LCO 3.0.4.b
Diesel Generators	1, 2, 3, 4
Auxiliary Feedwater	1 (and 2, 3, 4 in some cases)
ECCS High Head Safety Injection subsystem	4
Low Temperature Overpressure Protection	4

Table 7-1: Exceptions to LCO 3.0.4.b for Westinghouse PWRs (from [50])

Concerning the risk assessment required by LCO 3.0.4.b, the NRC states in the STS that it may use quantitative or qualitative methods, or both, and that it will be conducted using the program in place to implement §(a)(4) of the Maintenance Rule. Therefore, as in the case of Initiative 2 presented above, the implementation of Initiative 3 does not constitute an additional

burden to the licensee, and no guidance in addition to the existing set regarding the implementation of the Maintenance Rule is required.

7.2.2.5. Situation in France

In the French Technical Specifications, it is specified that the licensee is not allowed to make the reactor critical if:

- A group 1 event is currently ongoing, or
- More than four group 2 events affecting different elementary systems are ongoing.

Also, the licensee is not allowed to go to another reactor state (unless when required by the TS) if it generates:

- A group 1 event, or
- More than four group 2 events affecting different elementary systems.

Therefore, no risk-assessment is involved in this process, but the distinction between group 1 and group 2 events allows the licensee to go to higher mode even though it generates up to four TS events affecting different elementary systems, as long as these events are in group 2. This requirement is not as strict as the previous US regulation (before the implementation of Initiative 3), but it does not provide the same flexibility as the risk-informed TS Initiative 3, and it does not take into account the configuration-specific risk impact of the change in reactor mode.

7.3. Risk-informed Initiative 4b

7.3.1. Background

Current TS contain equipment-specific, fixed allowed outage times: when a system is unavailable, required actions have to be completed prior to the expiration of the AOT specified in the TS. While the Tech Specs may take into account systems that directly support the considered system, usually they do not account for the combined risk impact of multiple out-of-service SSCs. The Maintenance Rule configuration risk assessment (§(a)(4)) was added in order to address this issue, but it does not exempt the operator from complying with TS requirements. This situation may lead to inconsistencies with the Maintenance Rule requirements, and it may sometimes require plant shutdown or other actions that are not the safest course of actions

regarding the specific plant configuration [52]. The main objective of Initiative 4b is to modify the TS in order to reflect an approach that would be more consistent with the approach of Maintenance Rule §(a)(4). Currently, when there is a discrepancy between TS requirements and actual risk significance, the licensee may contact the NRC and request an NOED in order to delay the shutdown requirement, using the risk assessment to support this request.

This risk-informed TS Initiative is considered to be one of the most ambitious, if not the most ambitious, while Initiatives 2 and 3 presented in the previous section are more straightforward and easy to implement by the nuclear industry. Indeed, Initiative 4b calls for the consideration of highly technical subjects such as the scope and the quality of the risk assessments (there are currently few plants with full scope PRAs), and the definition of appropriate risk management actions. However, it should be kept in mind that these topics have already been addressed to some extent by the NRC and the industry, in particular through the development and the implementation of the Maintenance Rule. But some matters may need additional consideration.

In 2006, the NEI submitted a specific proposal and guidance on this subject: NEI 06-09 *Risk-Informed Technical Specifications Initiative 4b, Risk-Managed Technical Specifications (RMTS) Guidelines*, which was approved by the NRC in May 2007 [53]. A pilot implementation project at the nuclear power plant South Texas Project (STP) was then approved in July 2007. STP is not quite representative of US nuclear power plants (in particular, it has a three-train safety system design), and its Technical Specifications are not based upon NRC Improved STS, therefore a second pilot plant has been selected, Vogtle Electric Generating Plant (VEGP), which is more representative of the units of the rest of the industry. The US nuclear industry has expressed great interest for this risk-informed Initiative, with more than 40 submittals identified in 2010 as being planned [55]. The implementation of this Initiative is expected to have safety as well as economic benefits.

7.3.2. Initiative description and industrial guidelines

Based upon Reference [56], we present here some details about the implementation of the RMTS (Risk Managed Technical Specifications) process as defined in the industrial guidance NEI 06-09 (approved by the NRC in 2007).

7.3.2.1. Technical Basis

The RMTS program is intended to apply risk insights derived from the plant-specific PRA to identify risk-informed AOTs (or CTs, Completion Times) and appropriate compensatory risk management measures associated with inoperable SSCs, using in particular configuration CDF and LERF results that are compared with acceptable risk thresholds. The Completion Time that results from this analysis is called the Risk-Informed Completion Time (RICT), which can then be used to extend the deterministic TS Completion Time (called Front-Stop Completion Time, FSCT). A major characteristic of the RMTS process is that it is fully dynamic: if some SSCs are repaired or if some new SSCs become inoperable during the process, a new RICT is calculated, taking into account the cumulative risk increment that has already occurred during this same chain of events.

In addition, an upper limit for the completion of TS actions has been defined, called the Back-Stop Completion Time (BSCT). This BSCT has been chosen to be equal to 30 days. This limit was chosen in order to provide a conservative limit to the time during which the plant can remain in a configuration that is not consistent with the design basis, and the choice of 30 days was based upon the fact that in current TS some FSCT are as long as 30 days.

The quantitative risk management threshold values that have been established for the RMTS process are consistent with those defined in previous guidance, in particular Regulatory Guide 1.174 and guidance on the Maintenance Rule (NUMARC 93-01). More specifically, these thresholds are presented in Table 7-2. In this table, RMAT refers to the Risk Management Action Time, defined below.

7.3.2.2. Details on the RMTS process

RMTS Calculations and Actions

Two different values are computed upon entry into an LCO:

- The Risk Management Action Time (RMAT): this time is defined as the time from entry into the LCO until the respective threshold value ICDP = 10^{-6} or ILERP = 10^{-7} is reached (see Table 7-2). By this time, applicable Risk Management Actions (RMA, or compensatory measures) must have been taken.
- The Risk-Informed Completion Time (RICT): this time is defined as the time from entry into the LCO until the respective threshold value ICDP = 10^{-5} or ILERP = 10^{-6} is reached (see Table 7-2), or 30 days (= the Back-Stop Completion Time, BSCT), whichever is shorter. The RICT is the time by which required actions must be completed (i.e. the RICT is simply the risk-informed AOT). If the licensee fails to complete these required actions before the end of the RICT, then he must follow TS requirements for required actions not met, including any requirement for plant shutdown (i.e., the plant is back to the "classic" TS process).

Criterion		RMTS Risk Management Guidance
CDF	LERF	
$\geq 10^{-3}$ ry^{-1}	$\geq 10^{-4}$ ry^{-1}	- Voluntary entrance into configuration prohibited. If in configuration due to emergent event, implement appropriate risk management actions.
ICDP	ILERP	
$\geq 10^{-5}$	$\geq 10^{-6}$	- Follow the Technical Specification requirements for required actions not met
$\geq 10^{-6}$	$\geq 10^{-7}$	- RMAT and RICT requirements apply - Assess non-quantifiable factors - Implement compensatory risk management actions
$<10^{-6}$	$<10^{-7}$	- Normal work controls

Table 7-2 : RMTS quantitative risk management thresholds (from [57])

The RMTS process is summarized on Figure 7-1. Another important feature of the RMTS process, as part of the industrial guidance NEI 06-09, is that the integrated risk impact of the program is tracked, and the cumulative risk associated with the use of RICT (=risk-informed AOTs) that go beyond the classic FSCTs (=classic, deterministic AOTs) is evaluated every refueling cycle. The integrated additional risk is then compared to the guidelines of Regulatory Guide 1.174 to verify that risk changes are consistent with these guidelines.

A dynamic process

As mentioned above, the RMTS is a dynamic process, i.e. it accounts for new events (e.g. an additional inoperable SSC, or, in the other direction, one of the inoperable SSCs that has been repaired during the process). In order to make it more explicit, let us consider a theoretical example.

Example of application

This example is illustrated on Figure 7-2. It should be noted that in this example, only the CDF is used, for an objective of simplicity, while in reality both CDF and LERF should be used, and the most restrictive RICT and RMAT would then be selected to govern operations.

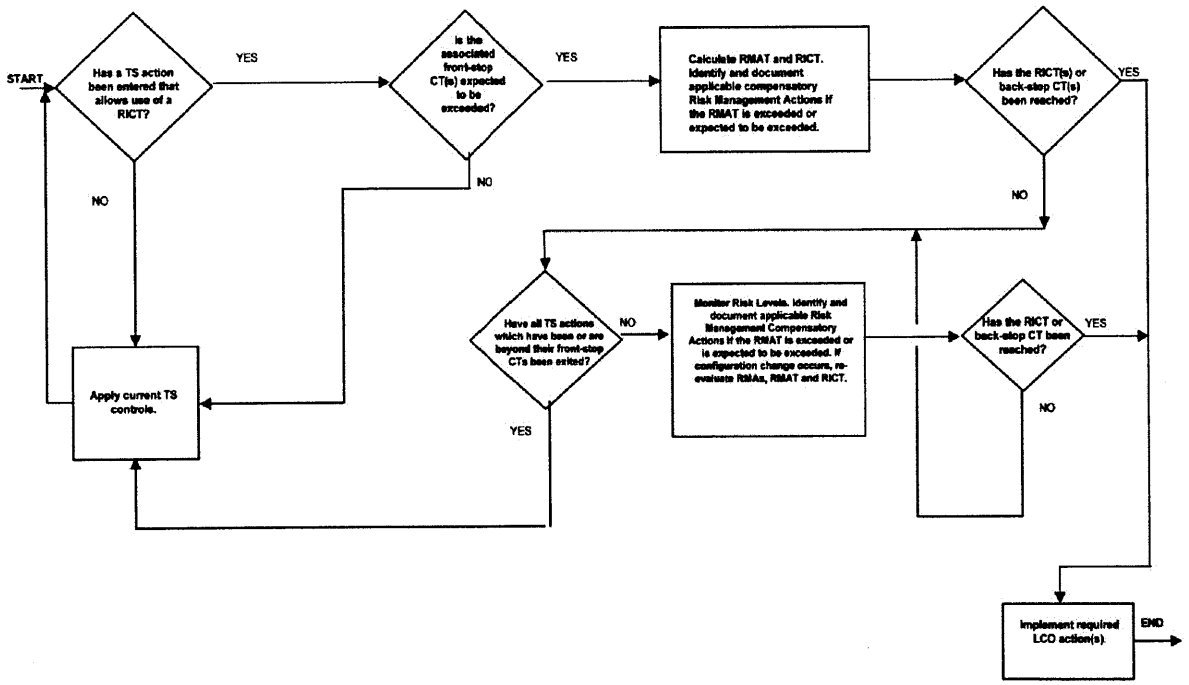


Figure 7-1 : RMTS process flowchart (from [57])

At time, t=0, component A becomes inoperable for a duration that is expected to exceed its FSCT specified in the TS, therefore the operator enters the RMTS process (Figure 7-1). The solid line on Figure 7-2 at the origin shows the evolution of the integrated incremental risk

(product of the incremental CDF and the out-of-service time). At this time, an RMAT is computed (intersection with the horizontal line corresponding to the threshold ICDP = 10^{-6}, as mentioned above), about 7 days here, and an RICT is computed (intersection with the horizontal line corresponding to the threshold ICDP = 10^{-5}). Here, the RICT would be greater than the BSCT (30 days), therefore the applicable RICT would be set to 30 days. Before reaching the RMAT (7 days), the licensee will need to develop and implement (as soon as possible) appropriate compensatory risk management actions.

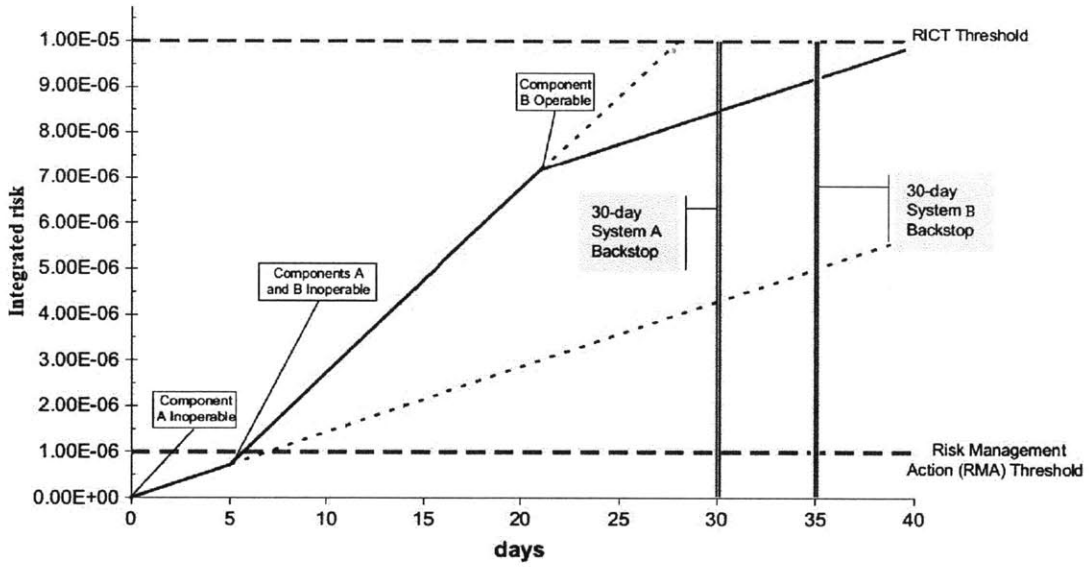


Figure 7-2 : Example of RMTS application (adapted from [57])

Then, at time, t=5 days, another component becomes unavailable, component B. Therefore, a new risk profile is established (second segment of the solid line), and new RMAT and RICT are calculated. Here, the RMAT occurs very soon after this new evolution, which required rapid evaluation, development and implementation of appropriate risk management actions. The new RICT is 28 days, now smaller than the back-stop completion time corresponding to component B (the BSCT applies separately to each inoperable component, as shown on Figure 7-2).

At t=20 days, component B is restored to service, so a new RICT is calculated. Here again, it would exceed the 30-day back-stop completion time of component A, so the applicable

RICT is reset to this BSCT value. Since at t=20 days the RMA threshold is already exceeded (ICDP = 10^{-6}), implementation of appropriate compensatory measures is still required.

7.3.2.3. PRA characteristics

The technical quality of the PRA is a critical element in implementing the RMTS process. According to Ref. [56], at a minimum, the PRA used to support the RMTS program must be a Level 1 PRA with LERF estimation capability. It must include validated modeling of internal events, including internal floods and fires. Other external events should be considered to the extent that these events could have an effect on the calculated RMAT and RICT.

As mentioned earlier, existing codes and guidance concerning PRA quality may be used for assessing the applicability of a plant PRA to the RMTS program, in particular Regulatory Guide 1.200, mentioned explicitly in [56].

7.3.3. Pilot project at South Texas Project

7.3.3.1. Background

In July 2007, the NRC approved the pilot implementation project of Initiative 4b at South Texas Project (STP) Electric Generating Station (2 × 1410 MWe, 4-loop Westinghouse PWRs) after years of collaboration between the NRC and the nuclear industry. Information presented in this section is mostly based upon References [58], [59] and [60]. STP provided key inputs to the NEI guidance document, NEI 06-09.

STP has a long history of use of PRA for performing quantitative risk assessments of online maintenance configurations under the Configuration Risk Management Program (CRMP). STP was performing such risk assessments even before the enforcement of §(a)(4) of the Maintenance Rule. In the past, as with all US plants, STP units followed prescribed AOTs established without the benefit of risk quantification. As a result, STP experienced unnecessary production loss and staff workload. The implementation of the risk-informed Initiative 4b is expected to provide greater operational flexibility for prioritizing maintenance, and lower costs while maintaining a high level of safety. It is also expected to reduce the number of plant shutdowns and the potential for initiating events during these shutdowns: it has been estimated that about one unplanned outage every four years would be avoided over the plant lifetime (Ref.

[60]), hence providing significant savings. In addition, it would remove some burden from the NRC by reducing the frequency of some special requests.

7.3.3.2. Costs saving effect

Economic effects of the implementation of the Initiative 4b at South Texas Project have been estimated in Reference [60]. First, some critical-path maintenance could be transferred from refueling outages to online maintenance, which could potentially save 12 hours of critical-path per refueling outage for half of the remaining 52 outages, which represents approximately $970,000 (at current prices) of additional revenue for each of these 26 outages, hence a total of $25.2 million.

Then, some non-critical-path maintenance could also be performed in at-power mode rather than during outages. Even though labor requirements are the same, whether these maintenance tasks are done online or during outages, performing them online would save contractor support costs during outages as well as those of associated management oversight. Savings are evaluated at $100,000 for each of the other 26 outages, i.e. a total of $2.6 million over the plant's lifespan.

As mentioned above, is has been estimated that the use of RMTS would prevent about one unplanned shutdown every four years, hence a total of 10 unplanned shutdown during the remaining life of STP nuclear power plant. Typically, an unplanned outage of a unit costs 3 days of production, for a $1.94 million loss per day currently at STP. Therefore, it would save an additional $58.32 million over the plant's lifespan.

Based upon past experience, it is expected that the RMTS program will avoid one NOED every year, which represents about $50,000 per year, as well as two non-transmitted NOEDs (not transmitted because eventually these NOEDs were not needed), which totals $20,000 annually.

All these projected savings combined constitute an average saving of $2.223 million per year, or a total saving of $88.92 million over the life of the plant.

7.3.3.3. Implementation of the RMTS program

The RMTS program has been implemented at STP using the guidance NEI 06-09 outlined in Section 7.3.2 and a software program called RICTCal (Risk Informed Completion

Time Calculator), an extension of the online maintenance tool used to comply with §(a)(4) of the Maintenance Rule, RAsCal (Risk Assessment Calculator), that has been in use for several years at STP. RICTCal is a database application that uses a graphical user interface to retrieve stored CDF and LERF values associated with a given maintenance state [58]. RICTCal then calculates RMAT and RICT using the methodology presented in Section 7.3.2.2.

Since its implementation, it appears in [59] that the RMTS has not been much used, only to replace Class 1E batteries online and another time to perform maintenance on class 1E 120V AC instrument inverters (at the date of Ref. [59], i.e. March 2010). However, there have been more cases when RMTS has "almost" been used, and even though in these cases classic TS AOTs were not exceeded, the existence of the RMTS program spared STP the need to prepare NOED that might have been needed, which avoided unnecessary costs and use of resources.

Tech Spec & Component	TS Front Stop	RMAT	RICT	Actual Inoperability Time	Actual ICDP	Actual ILERP
TS 3.8.3.1 Class 1E Instrument Inverter (Unit 1)	24 hr	> 30 days	30-day Backstop	29.1 hr	9.7×10^{-9}	7.2×10^{-10}
TS 3.8.3.1 Train C 1E Battery (Unit 1)	2 hr	2 weeks	30-day Backstop	3.6 days	2.7×10^{-7}	1.8×10^{-8}
TS 3.8.3.1 Train C 1E Battery (Unit 2)	2 hr	2 weeks	30-day Backstop	3.6 days	2.7×10^{-7}	1.8×10^{-8}
TS 3.8.3.1 Train A 1E Battery (Unit 1)	2 hr	2 weeks	30-day Backstop	6.6 days	4.4×10^{-7}	2.7×10^{-8}
TS 3.8.3.1 Train A 1E Battery (Unit 2)	2 hr	2 weeks	30-day Backstop	3.5 days	2.3×10^{-7}	1.4×10^{-8}

Table 7-3: RMTS Experience at South Texas Project [59]

The cases where the RMTS process has been used at STP from 03/2008 to 04/2009 are summarized in Table 7-3 with the associated integrated risk (ICDP and ILERP). We can notice that in all these cases, the final integrated risk are still far from the quantitative risk thresholds of

the RMTS methodology (10^{-6} and 10^{-5} for the ICDP, and 10^{-6} and 10^{-7} for the ILERP), and in none of these cases the RMAT was reached.

7.4. Risk-informed Initiative 5b – Brief overview

Current Technical Specifications provide specific surveillance requirements, associated with specific surveillance test intervals with which the licensee must comply to avoid entrance into an LCO. Initiative 2 has made the regulation more flexible regarding missed surveillances (see Section 7.2.1). However, if the licensee wishes to modify a particular STI, he must submit a detailed request to the NRC (typically using PRA insights and the methodology developed in RG 1.177) and obtain the NRC's explicit approval. This process can be lengthy and costly, both for the licensee and the NRC, and it must be repeated for each individual STI modification. The goal of Initiative 5b is to relocate STIs from the Tech Specs to a licensee-controlled program by establishing a risk-informed process (called "Surveillance Frequency Control Program", or SFCP), consistent with the philosophy of RG 1.174 and 1.177, that enables the licensee to modify individual STIs, on a case-by-case basis (and not repeatedly), without explicit agreement from the NRC for each STI modification. Only the overall process is controlled by the NRC, as part of the ROP.

The NRC has approved Initiative 5b, as well as the associated industrial guidance, NEI 04-10 Rev.1 (Ref. [63]), in September 2007. The industry has expressed a very high interest for this risk-informed technical specifications Initiative, and about 50 submittals to implement this initiative 5b have been identified as being planned [55]. A pilot implementation project at Limerick Station has been approved by the NRC in 2006, and in April 2011, the implementation of this initiative has been granted by the NRC to a dozen plants. Detailed technical information about this Initiative can be found in Ref. [63].

7.5. Summary

In the United States, while the technical specifications and the Maintenance Rule already provided some flexibility for choosing between online and offline maintenance, the risk-informed Initiatives facilitate even more the use of online maintenance, in particular the

ambitious Initiative 4b, which provides much flexibility regarding AOTs for single as well as multiple outages. The increased possibility to transfer maintenance from refueling outages to online maintenance, combined with other advantages (fewer unplanned shutdowns, fewer Tech Specs exemption requests...), is expected to allow significant savings, as explained with the example of STP. Once again, these risk-informed initiatives (aside from Initiative 5b) are based upon the use of PRA tools at the operational level, while in France there appears to be an opposition to such practices.

Also, it should be remembered that none of these risk-informed Initiatives is "risk-based", in the sense that there are always some barriers to avoid behaviors that would be unacceptable from a conservative, deterministic point of view, in particular:

- The deterministic considerations included in the official Maintenance Rule guidance (NUMARC 93-01)
- For Initiative 4b, the use of a Back-Stop Completion Time and the tracking of the integrated risk impact associated with the use of this Initiative.

Chapter 8

EDG Online Maintenance Case Study – Background

8.1. Introduction

Onsite emergency electric power sources are an essential part of the safety systems to provide sufficient power, and for a sufficient period of time upon a LOOP, to shut the reactor down and maintain it in a safe, cold shutdown. All French nuclear power plants and most US plants use EDGs as the main onsite emergency AC power sources.

Failures of EDGs are among the most important contributors to the plant CDF, which makes their reliability particularly critical. While in the past, most maintenance tasks and periodic tests were performed during refueling outages, there are usually no technical reasons preventing from performing these tasks online. As is explained in Section 6.1, the 55-minute station blackout that occurred at the Vogtle station (Unit 1) in 1990 played a particular role in the reconsideration of online maintenance practices, for EDGs, but also more generally. This LOOP, due to a truck accidentally driving into a transmission line support pole, occurred while the unit was in a refueling outage, and one EDG was out of service for maintenance. The second EDG started, but failed soon after. This event highlighted the importance of risk during refueling outages, a period of time with many different activities going on simultaneously and reduced system redundancy. Combined with the recognition that online maintenance can have operational and economic benefits (see Chapter 6), it led several utilities to consider performing EDG maintenance online, often requiring AOT extensions (for which risk-information played an important role) and sometimes the addition of an alternate AC source.

8.2. Emergency diesel generators: technical overview

8.2.1. Diesel engines: background

There are three main differences between diesel engines and gasoline engines: (1) diesel engines ignite the fuel only by the heat of compression, and have therefore no external ignition system; (2) in diesel engines, air is drawn alone into the cylinders, and there is therefore no carburetor; (3) in diesel engines, the fuel is injected into the cylinders in the form of a spray at high pressure, using a fuel-injection pump. Also, diesel engines typically use superchargers to increase the pressure of the air needed to support the combustion, in order to increase the power output of the cylinders. The supercharger can take the form of a turbocharger, which extracts mechanical energy from exhaust air through a turbine, and this energy is used to turn an air pump that compresses intake air drawn from the atmosphere and forces it into the cylinders.

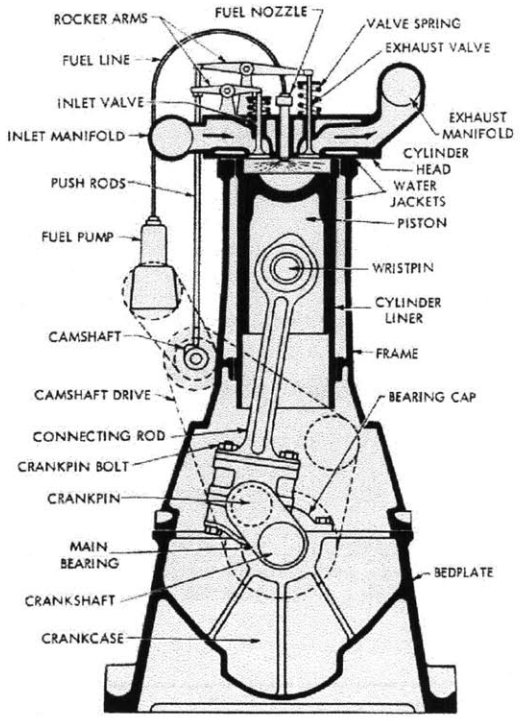


Figure 8-1 : Basic parts of a 4-cycle diesel engine

The basic parts of a typical diesel engine are presented on Figure 8-1. There are two types of cycle: 4-stroke cycle (or 4-cycle), the most common type of diesel engine, and 2-stroke cycle (or 2-cycle).

8.2.2. EDGs in Nuclear Power Plants

There are usually at least two independent EDGs per unit. EDGs used in nuclear power plants are typically small capacity (1 MW to 25 MW), medium speed, four-cycle diesel engines started by compressed air. In this study, we are especially interested in the EDGs of two types of utilities: a US utility, exemplified by Seabrook Station, and French utilities, exemplified by the EDF 1300 MWe Series.

EDGs at Seabrook Station

There are two main EDGs at Seabrook Station, plus a Supplemental Emergency Power Supply (SEPS), presented later in this thesis. These two EDGs are Colt-Pielstick PC2.3, 16-cylinder (V-arrangement), four-cycle independent diesel engines, rated at 6.083 MW. They are designed to supply 60 Hz AC power to the 4.16 kV emergency buses. Their nominal speed is 514 rpm, and an overspeed system automatically trips the engine when the speed reaches 115% of its nominal value [71].

One of the main performance criteria for these EDGs is that they must be able to reach rated speed and voltage, and achieve a "ready-to-load" condition within a maximum of 10 seconds after receiving an automatic or manual start signal.

EDGs in EDF 1300 MWe reactors

There are two EDGs per reactor, plus additional emergency power systems that is presented later in this thesis. The EDGs are Pielstick PC2.5 SEMT, 16-cylinder (V-arrangement), four-cycle diesel engines, rated at 7.65 MW. They are designed to supply 50 Hz AC power to the 6.6 kV emergency buses. Their nominal speed is 500 rpm, and an overspeed system automatically trips the engine when the speed reaches 115% of its nominal value. Like the EDGs at Seabrook, they are required to be able to reach nominal speed and voltage within a maximum of 10 seconds.

8.2.3. Auxiliary Systems

In order to run a diesel generator (DG), many auxiliary systems are needed to supply fuel and air, to remove exhaust gases, to lubricate and cool some components. These subsystems can significantly differ from one DG to another, but they all have some common characteristics. The goal here is not to describe these subsystems in detail; we present only some broad features of these auxiliary systems that will enable the reader to better comprehend the EDG maintenance case study, and we illustrate these subsystems with those in EDF 1300 MWe reactors and Seabrook Station. The description of these subsystems is based upon information available in [68],[69],[70] for the EDF 1300 MWe Series, and public documents [71],[72],[78] for Seabrook Station.

A basic, integrated representation of a DG and its subsystems as the ones in the EDF 1300 MWe Series is provided on Figure 8-2.

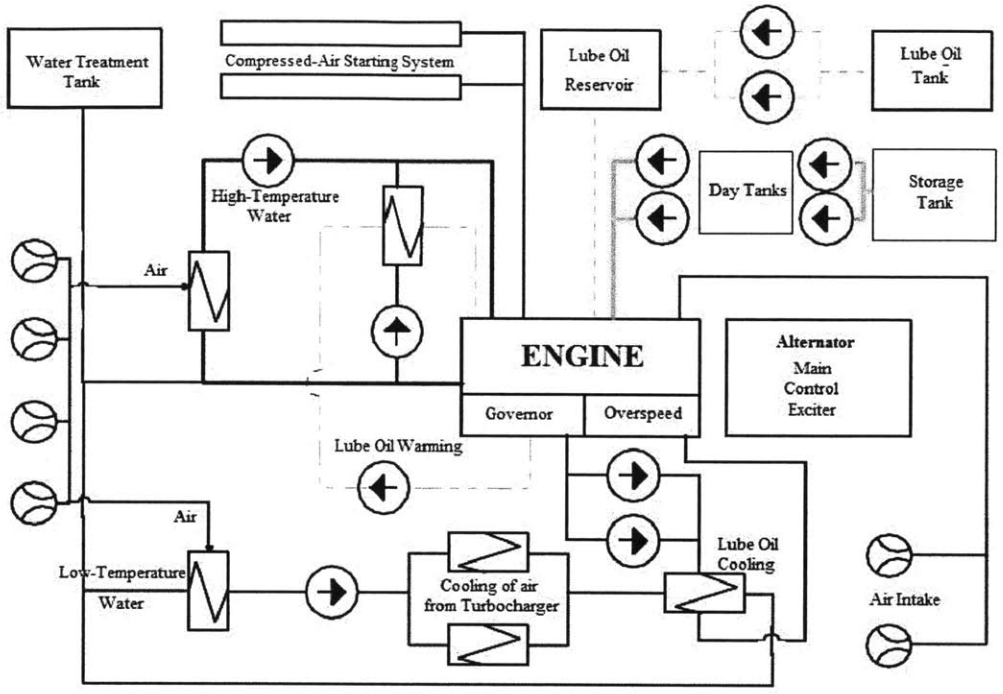


Figure 8-2 : An EDG and its auxiliary systems (adapted from [68])

Fuel oil subsystem

The role of this subsystem is to supply the DG with fuel oil. The main DGs at Seabrook Station have independent fuel oil systems, each consisting of a fuel oil storage tank, a fuel oil day tank, a fuel oil transfer pump (to transfer fuel from the storage tank to the day tank), an engine-driven fuel pump (to transfer fuel from the day tank to the engine), an auxiliary motor-driven fuel pump and the instrumentation and controls necessary for system operation. There are also cross-tie connections between the storage tanks of the two main DGs. The quantity of fuel stored on-site is sufficient to supply power to all components required to shut the reactor down and maintain it in a safe, cold shutdown for a period of 7 days. For the EDF 1300 MWe Series DGs, there are two storage tanks and one day tank for each DG, providing a quantity of fuel sufficient to supply power for a period of 200 hours (8.3 days).

Lube oil subsystem

Many parts of the diesel engine need to be properly lubricated. For the main DGs at Seabrook Station as well as the DGs in the EDF 1300 MWe reactors, the lube oil system consists of two subsystems:

- The prelube/keep-warm lube oil system: in standby, the diesel engine is pre-heated and pre-lubricated to increase the startup speed and reduce engine wear. At EDF and at Seabrook, the lube oil is pre-heated by the keep-warm heating system (see below) and is constantly circulated when the reactor is in standby status.
- The lube oil system used when the engine is running: in both types of utilities, this lube oil is cooled by the air coolant system (see below).

Coolant systems

The coolant systems installed on an EDG typically consist of the following three water subsystems:

- Keep-warm heating system: it is designed to operate when the engine is in standby status in order to maintain the engine jackets at a high enough temperature to support engine fast start and reduce wear. This jacket coolant is also used to heat the prelube/keep-warm lube oil.
- Jacket coolant system (= high temperature water system): the jacket coolant system is a water circuit designed in particular to remove heat from the cylinder liner water jackets (see Figure 8-1), the turbocharger turbines, the cylinder heads, and also to cool the governor lube oil through a heat exchanger.
- Air coolant system (= low temperature water system): the air coolant system is a water circuit designed to remove heat from the combustion air (after it exits the turbocharger and before it enters the engine), the outboard bearing and the main lube oil system.

Starting air system

Starting air is used to provide motive force to the pistons and start the diesel engine. Each DG has an independent air starting system. There are typically two 40-bar compressed air receivers per starting air system, which is sufficient to provide five successful engine starts.

Air intake and exhaust systems

Intake air is drawn from the atmosphere, compressed by the turbochargers, cooled by the air coolant system, and then delivered to the cylinder heads. Exhaust gases drive the turbocharger, go into an exhaust silencer and are discharged to the atmosphere.

Alternator

An alternator consists of a rotor and a stator, made of one or several induction coils where the alternating current is generated. While in small generators the rotor typically consists of a rotating magnet, it is replaced in large generators by a rotating coil fed with direct current that also generates a variable magnetic field. There are, therefore, in EDGs three distinct alternators on the rotating shaft:

- The main alternator: its rotor (a coil) is fed with DC, and its stator then generates the AC used be the different safety systems in the reactor. Changing the intensity of the DC (direct current) enables one to control the voltage delivered by the DG.
- The exciter: the rotor of the exciter is also a coil fed with DC. Its stator then generates AC which is rectified to obtain the DC used by the rotor of the main alternator. The DC in the rotor of the exciter is controlled by the exciter regulator.
- The pilot alternator: its rotor is made of a small magnet, its stator generates an alternative current that is then rectified to obtain the DC used to power the exciter regulator.

Speed governor

In order to control the speed (= frequency) of the engine, at least one speed governor is installed on the DG.

Alarms and fault protective devices

Numerous fault protective devices are installed on an EDG to prevent operation of a diesel in a manner that could damage it. When actuated, a protective device causes the DG to trip, i.e. turn itself off. Depending upon the mode in which the DG operates (test, safety injection, LOOP), some protective devices may be automatically bypassed: typically, when used in emergency mode, few protective devices will actually trip the generator, for safety reasons.

8.3. EDG regulation in the United States

8.3.1. Background

In the US, the regulation (10 CFR 50 Appendix A) requires that onsite electric power systems have sufficient independence, capacity and redundancy to ensure that (1) specified acceptable nuclear fuel design limits and design conditions of the reactor coolant pressure boundary are not exceeded, and (2) the core is cooled, and containment integrity and other vital functions are maintained in the event of postulated accidents, assuming a single failure.

More recently, in the light of PRA insights showing the high contribution of EDGs to the plant risk, additional requirements have been formulated. The Blackout Rule (10 CFR 50.63), outlined in the next section, requires that each US LWR be able to withstand and recover from a station blackout for a particular duration, and, given the contribution of the EDG reliability to the Blackout CDF, the NRC recommends in the associated guidance (RG 1.155) that the reliability of these EDGs be at least 0.95 or 0.975.

In order to achieve these goals, preventive maintenance is essential, so that the NRC has issued a guidance on that subject, RG 1.9 (Ref. [79]), which endorses the industrial guidance IEEE 387-1995 (Ref. [80]) with some minor modifications. As always, compliance with this guidance is not mandatory for US licensees, but it appears that most licensees do comply with it.

8.3.2. The Station Blackout Rule

8.3.2.1. Background

In the US regulatory literature, "Station Blackout" is defined as the complete loss of AC electric power to the essential and nonessential electric switchgear buses (10 CFR 50.2), i.e., a LOOP concurrent with a turbine trip and the unavailability of the emergency AC systems. It does not involve however the loss of AC power provided by batteries through inverters nor the loss of power from "alternate AC sources" (see below).

The concern about Station Blackout (SBO) arose because of accumulating experience regarding the reliability of the different AC sources. Many nuclear power plants have

experienced LOOP, with an expected increase in the frequency of such events in the coming years due to the deregulation of the electrical industry. For example, on August 14, 2003, the widespread loss of electrical power due to grid failure resulted in LOOPs at nine nuclear power plants in the United-States. In almost every case, the onsite emergency AC power sources were available immediately to supply power to the vital safety systems. However, in some cases, one of the redundant emergency AC sources was unavailable. In addition to these incidents, individual EDGs have failed to start or run in many cases, in response to periodic tests or external events.

The results of the Reactor Safety Study (WASH 1400) showed that SBO could be an important contributor to the total risk at nuclear power plants. This result has been confirmed by more advanced PRA, showing that SBO could contribute to more than 80% of the total CDF at some plants (see appendix B of ref. [84]), even though there are huge variations in this contribution from one plant to another. Appendix B, column 4, presents the contribution of SBO to CDF for some PWRs in 2000 (after the enforcement of the SBO Rule).

8.3.2.2. The rule

The Blackout Rule, 10 CFR 50.63, states that "each light-water-cooled nuclear power plant (...) must be able to withstand for a specified duration and recover from a station blackout". This duration needs to be defined for each plant, based upon (i) the redundancy of the onsite emergency AC power sources, (ii) the reliability of these sources, (iii) the expected frequency of LOOP, and (iv) the probable time required to restore offsite power after a LOOP.

The Rule adds that onsite or nearby "alternate AC power sources" would constitute acceptable capacity to cope with an SBO, provided that it has been shown that the plant is able to operate safely after the beginning of an SBO and until the alternate source(s) and required shutdown equipment are ready to operate. Alternate AC sources may serve a multiple unit site if the onsite emergency AC sources are not shared between units. Most of the time, an alternate AC power source takes the form of an additional diesel generator, or in some cases, a gas turbine.

8.3.2.3. Regulatory guidance

In order to help licensees comply with the SBO Rule, the NRC issued in 1988 RG 1.155 [82]. While the SBO Rule does not mention specific coping time or diesel generator reliability

targets, this RG addresses such issues, while other issues such as the independence of preferred power circuits and the independence between redundant diesel generators are addressed in other standards and regulatory guides.

Emergency Diesel Generators

RG 1.155 recommends an EDG minimum reliability target of 0.95 or 0.975 per demand, depending upon the configuration of the emergency AC power sources. The different groups of configuration are defined according to the number of emergency AC power sources present at the plant and the number that is required to operate decay heat removal systems.

In addition, RG 1.155 states that an adequate reliability program should be designed at each plant to ensure the reliable operation of onsite emergency AC power sources.

Ability to cope with a Station Blackout

The plant-specific minimum SBO duration capability should be based upon the factors presented in Section 8.3.2.2. RG 1.155 presents a method to calculate this duration, ranging from two hours to sixteen hours, depending upon the characteristics of each plant. The categorization of each plant is based upon (1) independence of offsite power systems, (2) reliability of EDGs (3) probability of severe weather conditions in the area of the plant, (4) severe weather recovery capability, and (5) probability of extremely severe weather.

If the plant's SBO capability is below the minimum acceptable plant-specific SBO coping duration, modifications may be necessary to increase this capability to cope with an SBO, such as the addition of an alternate AC power source.

8.3.2.4. Regulatory effectiveness

Risk reduction

The NRC expected that the implementation of the SBO Rule would result in an industry CDF reduction of 2.6×10^{-5} ry^{-1}, corresponding to a transition from a mean SBO CDF of 4.2×10^{-5} ry^{-1} before the implementation of the Rule to 1.6×10^{-5} after the implementation of the Rule. In addition, the NRC expected a significant change in the distribution of the different plant-specific SBO CDF, as detailed in Table 8-1.

After the implementation of the Rule, the industry-wide average SBO CDF was 1.0×10^{-5} ry^{-1}, hence an SBO CDF reduction of 3.2×10^{-5}, which exceeds the 2.6×10^{-5} ry^{-1} originally expected. Table 8-1 shows that the transformation of the plant-specific SBO CDF distribution was also better than expected, in the sense that more plants have low SBO CDFs and fewer plants have high SBO CDFs than expected.

Parameter	Number of Plants in SBO CDF Range ($\times10^{-5}$ ry^{-1})											
SBO CDF Range	< 0.5	0.5 0.99	1.0 1.49	1.5 1.99	2.0 2.49	2.5 2.99	3.0 3.49	3.5 3.99	4.0 4.49	4.5 4.99	5.0 9.99	10 35
Before SBO rule Implementation (estimated)	5	13	14	7	13	4	9	5	4	3	13	10
Expected After SBO rule Implementation	23	23	14	9	6	5	6	5	4	0	5	0
Actual Outcome After SBO rule Implementation	46	22	13	17	1	3	1	3	0	1	1	0

Table 8-1 : SBO CDF distribution before and after SBO Rule implementation [83]

In order to achieve these results, many plants have made some modifications. In particular, most of the plants having the highest extremely severe weather frequencies and plants having the greatest vulnerability to a plant-centered LOOP have now access to an alternate AC power supply as defined in the SBO Rule. Table 8-2 presents some examples of these modifications that have been performed to comply with the Blackout Rule and the associated CDF reductions.

The conclusion of this section is that the SBO Rule has been effective in achieving the desired SBO CDF reduction, and the plants that were most subject to SBO risk (high LOOP frequency, extremely severe weather) performed major modifications and have now relatively low SBO CDF values.

Description of Modification	Effect on Overall Risk (% Reduction of Plant CDF)
Add EDGs: - Calvert Cliffs (one safety and one non-safety EDG) - Turkey Point (two safety EDGs)	 24 20
Add safety EDG: - Diablo Canyon	 14-18
Add non-safety EDG for site: - Arkansas Nuclear 1 - Arkansas Nuclear 2	 23-36 43-47
Procedural: - Arkansas Nuclear 1: EDG service water supply valve open - Monticello: Depressurize during SBO - Monticello: Battery load shed	 7 17 17
Credit of combustion turbine generator: - Fermi	 10
Extend battery life from 2 to 4 hours: - Arkansas Nuclear 1	 16
Improve reliability of onsite gas turbine generator: - Point Beach	 13
Install AC cross-tie: - Fermi Install AC cross-connect and automatic depressurization system: - Monticello	 49 38

Table 8-2 : Modifications and their consequences on plant CDF [83]

EDG reliability

After the enforcement of the SBO Rule, we note that all licensees were strongly required by RG 1.155 to establish an EDG reliability program, and to maintain an individual EDG reliability of at least 0.95 or 0.975, depending upon some characteristics of the plant. In 2003, it has been established in ref. [83] that:

- For plants with a target of 0.95, a mean industry reliability of 0.954 has been achieved.
- For plants with a target of 0.975, a mean industry reliability of 0.967 has been achieved.

Even though the objectives of the SBO Rule concerning EDG reliability have not been completely achieved, great progress has been made. Before the Blackout Rule was issued, only

11 out of 78 plants surveyed had EDG reliability programs. Since the Rule was issued, all plants have established an EDG reliability program that has improved EDG reliability. Before issuance of the Rule, 11 of the 78 surveyed plants had a unit average EDG reliability below 0.95, and 2 below 0.90. In 2003, only 3 plants had a unit average EDF reliability below 0.95 (and above 0.90) [83].

Coping capability

In 2003, the outcome of the SBO Rule implementation was that 108 plants had selected a minimum SBO coping duration of 4 or 8 hours, completed the coping analysis, developed procedures, completed training, and 72 plants had completed modifications [83]. Therefore, the SBO expectations were mostly met. The scope and number of modifications to achieve selected coping durations even exceeded NRC's expectations, which could explain why plant risk reductions were generally greater than expected. Currently, 60 units have an alternate AC power source to reach their SBO coping time.

8.3.2.5. Conclusion and prospects

The SBO Rule has been very effective to improve the general safety level of US nuclear power plants and to increase the reliability of EDGs. Most of its objectives have been achieved. The SBO Rule has provided additional defense-in-depth to compensate for possible degradation of the offsite power supply that may result from deregulation of the electrical industry or longer than expected recovery of offsite power after extremely severe weather events.

However, as a result of the Fukushima accident, the requirements of the Rule are likely to be reconsidered [85]. One of the main issues raised by the NRC task force in charge of the 90-day review is that the SBO rule has been formulated without consideration of CCFs between onsite and offsite AC sources: these two types of sources were handled independently. In particular, widespread phenomena that could affect both types of AC sources (earthquake, flooding...) were not contemplated. Other issues identified by the NRC task force include [85]:

- Near term restoration of AC power was assumed in the formulation of the coping time requirements.

- The SBO rule focuses on preventing fuel damage, but does not consider the potential for hydrogen buildup in the containment and the potential need for power to actuate hydrogen igniters when such systems are used. Also, it does not provide any requirement regarding spent fuel cooling.
- The rule does not consider containment overpressure and the need to vent it in some designs.

In [85], the task force recommends a strategy based on three points to review the SBO Rule:

1) Licensees would need a coping capability to maintain necessary functions for at least 8 hours, with minimum reliance on operator action. During this period of time, the operator would focus on restoring AC power and implementing actions necessary for point 2).
2) Licensees would then have an "extended coping capability" to maintain necessary functions for at least 72 hours, using onsite portable equipment maintained and stored in a manner that protects it from the natural events that may call for their use.
3) Deployment of a sustainable cooling capability using preplanned and prestaged equipment from an offsite location (possibly shared by several sites).

8.3.3. EDG testing

8.3.3.1. Regulatory Guide 1.9 – Background

The guidance on EDG periodic testing is based upon several requirements regarding EDGs that are discussed in RG 1.9. The three main criteria that have to be ensured through adequate maintenance and testing are as follows [79]:

1) An EDG must be able to start and take on a specific number of large motor loads in rapid succession, while maintaining voltage and frequency within acceptable limits.
2) It must be capable of providing power quickly to engineered safety features should a LOOP and a design-basis event occur simultaneously.
3) It must be able to supply power continuously to the equipment needed to maintain the plant in a safe condition for a sufficient period of time (e.g. during 30 days, with refueling every 7 days).

Most of the emergency loads that must be powered by the EDG are those of large induction motors, and at full voltage, this type of motor draws a starting current of 5 to 8 times its rated current, which can result in significant voltage reduction in the electricity supplied by the DG. Such voltage reduction must be avoided, because they can prevent some motor from starting, can cause a running motor to stall, or damage some voltage-sensitive devices. In order to limit this voltage reduction, EDGs use a device called "load sequencer" to gradually connect the different loads to the generator. In addition, recovery from the transient caused by starting under these loads or sudden disconnection of one or several loads could cause a DG overspeed that might result in a trip (= shutdown) of the DG, due to the overspeed protective device, which must of course also be avoided.

In order to protect the EDG against major failure, RG 1.9 requires that, in the emergency mode of operation, two protective tripping devices be activated: the overspeed protection and the differential current protection system, used to detect the occurrence of internal fault. Other protective devices should be blocked from automatically tripping the DG [80] when the DG is used in emergency mode. Indeed, on many occasions in the past these protective systems have needlessly tripped the EDG because of spurious operation of a trip circuit. In test mode, however, Ref. [80] recommends that all the protective devices remain effective except during periodic tests that demonstrate the DG system response under simulated design-basis accident.

8.3.3.2. Periodic test overview

Beside the site acceptance and pre-operational tests that an EDG must undergo before it can be considered operational, the EDG is also subject to many periodic tests to ensure that its design criteria are still being met and that it is fully operational. There are three types of tests:

- Availability Tests: these tests demonstrate the continued capability of the DG to start and accept loads. It consists essentially of monthly tests (slow-start and load-run test), replaced every six months by a fast-start and load-run test.
- System operation tests: these tests demonstrate the ability of the EDG to perform its function under simulated accident conditions. They are performed every refueling outage. However, it is explicitly stated in RG 1.9 that "Certain [of these] tests may be conducted during the operating mode with NRC approval if the tests can be safely performed

without increasing the probability of plant trip, loss of power to the safety buses, or LOOP", thus giving the possibility for online maintenance. We return to this point in the next chapter.

- Independence verification test: performed every ten years or after any modification where the independence of the DGs may have been affected, this test verifies the independence of the two (or more) trains of standby electric power.

A summary of the different periodic tests recommended in RG 1.9 is presented in Table 8-3.

Tests	Monthly Testing	Six-Month Testing	Refueling Outage* Testing	Ten-year Testing
Slow-start test	X			
Fast-start test		X	X	
Load-run test	X	X		
LOOP test			X	
Combined LOOP and SIAS test			X	
Largest-load rejection test			X	
Design-load rejection test			X	
Endurance and load margin test			X	
Hot restart test			X	
Synchronizing test			X	
Protective-trip bypass test			X	
Test mode override test			X	
Independence test				X

* Some may be performed online. See quote from RG 1.9 mentioned above.

Table 8-3 : Summary of the EDG periodic tests recommended in RG 1.9

8.4. Summary

In the United States, the recognition of the importance of the SBO CDF has led the safety authority to develop regulations and detailed guidance. The Station Blackout Rule requires each

licensee to be able to withstand a blackout for a particular duration, through the definition of a regulatory "coping time". Also, this rule requires the licensees to develop an EDG reliability program to obtain an EDG reliability of at least 0.95 or 0.975. In order to obtain an acceptable EDG reliability value, the NRC issued RG 1.9 that recommends specific periodic tests with associated STIs. In particular, in RG 1.9 the NRC explicitly provides for the possibility of performing most of these tests online, even those that were originally meant to be performed during refueling outages. In order to comply with the SBO Rule, many utilities have made procedure and/or design modifications to reach the coping time, sometimes even adding an additional onsite AC power source (e.g. a DG). As a result, the industry SBO CDF has significantly decreased and the mean industry EDG reliability has increased. However, following NRC's review of the Fukushima accident, the requirements of the SBO Rule are likely to evolve.

In France, there are no similar regulatory requirements or guidance. Neither a regulatory coping time nor a regulatory EDG reliability target has been defined, and the scope and frequency of the EDG periodic tests are directly proposed by EDF and then approved by the ASN (see next Chapter).

Chapter 9

EDG and ECCS Online Maintenance Case Studies

9.1. EDG maintenance at EDF

9.1.1. Emergency AC power systems (1300 MWe Series)

Emergency Diesel Generators

There are two EDGs per nuclear reactor, designed to supply power to the Class 1E emergency buses (LHA, LHB) in case of a LOOP. A basic description of these EDGs is given in Section 8.2. These EDGs can be started in different ways:

- Manually: from the EDG local, the control room ...
- Automatically:
    - Upon a Safety Injection Signal, the EDGs are preventively started.
    - Upon LOOP: after four seconds of lack of voltage at one of the two emergency buses, the EDGs are started and connected as soon as adequate frequency and voltage are reached (i.e., in a maximum of 10 seconds after the starting signal).
    - Upon transfer of offsite power supply from the step-down transformer to the auxiliary transformer, the EDGs are started and connected to their respective Class 1E emergency busses as soon as adequate frequency and voltage are reached, should supply from the auxiliary transformer be lost.

Combustion Turbine

In addition to the EDGs, there is one combustion turbine (TAC, Turbine à Combustion) shared by all reactors of a same site. This combustion turbine, sometimes called "ultimate

emergency source", can be manually connected to either emergency bus if the corresponding EDG is unavailable. Power supplied by the TAC is usually similar to power supplied by an EDG [86], but its connection to one of the emergency buses takes some time.

Steam-driven turbo-alternator

Finally, each reactor is equipped with a turbo alternator system (LLS) that extracts steam from steam generators to drive a turbine and generate electricity when none of the offsite and onsite sources is available (Station Blackout). It is also started and used until the TAC has been connected to the emergency bus when it is needed [24]. The LLS does not have the same capability as an EDG or the TAC, and it is used only to supply power to control systems and to some systems necessary for reactor cooldown.

9.1.2. EDGs – Technical Specifications

9.1.2.1. Requirements

In full power mode, both EDGs are required to be available (as well as the TAC and the LLS system). The unavailability of one EDG constitutes a group 1 event, associated with a shutdown initiation time of 3 days, independently of the status of the TAC.

9.1.2.2. EDG Borderline Conditions – Online Maintenance

As is explained in Section 6.2.2, Group 1 events cannot be entered as often as desired, even for preventive maintenance. Group 1 events can be voluntarily entered only when a specific Borderline Condition has been granted by the ASN. For the EDGs, two Borderline Conditions have been defined for RP and AN/GV modes [51]:

1) One EDG can be taken out of service for preventive maintenance if the cumulated out-of-service duration for both EDGs remains smaller than 60 hours during one calendar year.
2) One EDG can be replaced by the TAC if, during one calendar year, the cumulated replacement duration for both EDGs remains smaller than 7 days if the TAC is rated at 7 MWe, 5 days if the TAC is rated at 4 MWe.

So, in the best case, each EDG can be taken out of service for preventive maintenance for about 5 days each year, which does not provide much flexibility to perform online maintenance.

9.1.3. EDG Periodic Testing - Background

Objectives and criteria

Periodic testing programs are defined for all systems classified as "important for safety" (IPS). These programs are prescriptive, but only some of them (EPIS systems) need to be formally approved by the ASN, among which are those for the EDGs.

For each periodic test, one or several criteria are defined in the applicable documentation. Periodic test criteria are reference values or states against which measurements or observations performed during the periodic test are compared.

Documentation

Periodic test programs are based upon four documents for each type of system [87]:

1) Exhaustiveness Analysis Note (NA, note d'analyse d'exhaustivité): NAs are written in one of EDF's centralized Engineering Division, and they must be approved by the ASN. For a given system, the NA describes all tests that need to be performed to ensure availability and operability of the system, based upon a list of all possible configurations and functions of this system.
2) Periodic Test Rules (REs, règles d'essais périodiques): derived from the corresponding NA, REs provide a more detailed description of the periodic tests identified in the NA: acceptance criteria, Group 1 events generated, STIs, ... As the NA, REs are written in one of EDF's centralized Engineering Division and must be approved by the ASN.
3) General Operating Rules (RGE), Chapter IX: this document, common to all reactors in the same series, provides in particular a list of all Group 1 events generated by periodic tests. It officially constitutes an exemption from the Technical Specifications. This document must be approved by the ASN.
4) Site-specific document (gammes d'essais périodiques): derived from the REs, this is the operational document that describes site-specific procedures to perform the periodic tests.

Periodic test acceptability

To consider a test to be satisfactory, the following conditions (among others) must be met:

- Applicable criteria must have been met
- The applicable STI must have been respected, with a margin of ± 25%.

If the periodic test is satisfactory, the system is considered to be available. If not (for example if the periodic test has not been performed within the ± 25% margin), the system is considered to be unavailable, and the corresponding Tech Specs action statement is immediately entered, possibly leading to a plant shutdown if the problem is not solved by the end of the applicable AOT [87].

9.1.4. Periodic Test Rules

Periodic Test Rules (REs) for 1300 MWe Series (Ref.[70]) are directly derived from the Exhaustiveness Analysis Note mentioned in the previous section. They provide a detailed description of periodic tests and acceptance criteria identified in the Exhaustiveness Analysis Note. Common to all 1300 MWe reactors, this document is then used on-site to write the corresponding plant-specific document, which can differ slightly from one reactor to another.

9.1.4.1. Two-month tests

Test description

For each EDG, the licensee is required to verify every other month that the DG is able to start automatically from standby conditions upon safety injection signal, and then reaches rated voltage and frequency sufficiently rapidly. After at least one hour of operation (to reach steady state), several parameters are controlled, then the EDG is shut down.

Reactor mode

Usually performed when the reactor is in power mode (RP), 2-month tests can be performed from AN/RRA to RP mode. It does not generate any EDG Tech Specs LCO.

9.1.4.2. One-cycle tests

Test description

Many tests are performed, such as:

- Testing of some command and control systems
- LOOP test and largest load rejection test
- EDG starting with only one compressed air system
- Synchronizing with offsite power and total load rejection test

Reactor mode

According to [70], 1-cycle tests must be performed during refueling outages, in mode APR or RCD. Some additional precautions are applicable.

9.1.4.3. Four-cycle test

Every four cycles, during a refueling outage (reactor in APR or RCD mode), the mechanical overspeed trip system is tested.

Also, every four or five cycles, command and control systems associated with the engine (sensors, alarms, automatic functions) are tested while the EDG is not operating.

9.1.4.4. Six-cycle test

Every six cycles, a combined safety injection signal and LOOP test is performed, followed by a largest load rejection test.

9.1.4.5. 10-year test

Every ten years, during one of the 1-cycle periodic tests at 100 %, a fuel consumption test is performed to verify that the fuel consumption remains adequate.

9.1.5. Additional controls and maintenance

In addition to these periodic tests, many other controls and maintenance tasks are performed on the EDGs. These tasks are governed by the Preventive Maintenance Basic Program (PBMP, Programme de Base de la Maintenance Préventive) applicable to the EDGs (Ref. [88]). Written in one of EDF's centralized Engineering Division, this document does not need ASN's approval before it can be used on site. However, respect of this preventive maintenance program (periodicity, satisfactory results) is a necessary condition to declare the system available. This

program has been established using results from the Reliability Centered Maintenance program (see Section 5.3.2). These surveillance tasks are categorized as follows:

- Surveillance tasks while the EDG is in standby mode: daily verifications (e.g. no leakage, no abnormal noise ...) and monthly tests (e.g. control of the color of the fuel, of the presence of solid particles in the fuel...).
- Surveillance tasks when the EDG is operating (i.e. during periodic tests): many controls are performed in parallel with the main periodic tests described above, such as: control of potential leakages, fuel and lube oil levels, visual controls, pressures, temperatures, gauges, indicators, lube oil physico-chemical analysis, lubrication...
- Surveillance tasks when the EDG is in shutdown: at more or less low frequency (intervals of a few months to 10 years or more), many maintenance and surveillance tasks are performed, some of them including partial dismantling of the EDG and replacement of some components.

All the basic maintenance and surveillance tasks that do not make the EDG inoperable can be performed online. However, the majority of the other maintenance tasks are performed during refueling outages and during decennial safety reviews, even though the Borderline Conditions provide the possibility to perform some of them online.

9.1.6. Potential for online maintenance

In France, there is a difference regarding the treatment of online preventive maintenance and online periodic tests, while from a safety point of view, it does not make any difference (whether a system is unavailable for preventive maintenance or periodic testing does not change the risk impact). Preventive maintenance involving a group 1 STE event can be performed online only through the use of applicable "Borderline Conditions", when available, while periodic tests involving a group 1 event can be performed online only when such group 1 event has been explicitly identified in Chapter IX of the RGE, which then officially constitutes an exception to the STEs.

Concerning online preventive maintenance, we have seen in Section 9.1.2.2 that two Borderline Conditions have been defined, enabling the operator to take each EDG out of service for about 5 days per year or less (in 1300 MWe reactors). It appears that this flexibility offered by the Borderline Conditions is not used systematically and in a consistent way by all EDF nuclear power plants [26], due to the absence of a general policy regarding the application of online maintenance and the use of these Borderline Conditions. Also, as is explained in Section 6.2.2.2, using the Borderline Conditions to perform online maintenance, when there is no "operational imperative" to do so, is not in accordance with the philosophy of the STEs. Additionally, even if it were decided to use these Borderline Conditions systematically to perform online maintenance, the potential for maintenance work would remain limited because significant time margins are needed. Indeed, as illustrated by the US experience, the planned duration of an online maintenance activity is usually smaller than half of the applicable AOT.

In 2004, using the PRA methodologies presented in Section 4.6, a re-assessment of the STE requirements for AC power sources was performed for the 900 MWe reactors (ref. [89]). In the 900 MWe series, the TAC is replaced by a diesel generator called GUS, shared by all units of a same site, and there is also a Borderline Condition that allows the operator to replace an EDG by the GUS for 10 days each year. The aforementioned PRA study has shown that this Borderline Condition could be extended to one month, generating an ICDP of about 1.6×10^{-8}, much smaller than the acceptance criterion of 10^{-7} defined in consensus between EDF and the safety authority (see Section 4.6). This Borderline Condition would provide much more flexibility to perform some maintenance tasks online. However, this longer Borderline Condition has never been implemented in the STEs, for some reasons already presented in Section 4.6.1.3.

Concerning the periodic tests, the EDG Periodic Test Rules outlined in Section 9.1.4 state that only the 2-month tests can be performed online (it does not generate any group 1 event), while all the other tests are to be performed in shutdown modes. As a result, the operator does not have the possibility to perform these tests during at-power operation, even though there are Borderline Conditions that allow taking one EDG out of service. If the operator wished to perform some of these tests online, EDF would have to propose a new version of the Periodic Test Rules that would then have to be approved by the ASN. But, as is explained in Section 6.2.2.2, in the philosophy of the RGE, the possibility to enter a group 1 event (when approved by

the ASN) to perform a periodic test is meant to be used when there is a technical reason for it, not for operational convenience [87]. However, it would be somewhat inconsistent if the licensee were allowed to enter a group 1 event for online preventive maintenance (in the framework of the Borderline Conditions) and not for periodic tests, the effect upon risk being the same if the out-of-service duration remains the same.

9.2. EDG Maintenance at a US facility: Seabrook Station

9.2.1. Emergency AC Power Systems

Seabrook Station is a single unit, 1245 MWe, 4-loop Westinghouse PWR. There are two kinds of AC emergency power sources at Seabrook Station: two emergency diesel generators and a Supplemental Emergency Power Supply (SEPS).

9.2.1.1. Emergency Diesel Generators

A brief technical description of the two EDGs installed at Seabrook and their support systems is given in Section 8.2. These EDGs must be capable of starting and reaching rated voltage and frequency within 10 to 12 seconds (12 seconds for a LOOP only, 10 seconds for events that require Safety Injection) [50]. The EDGs are designed to operate under three conditions:

Loss of offsite power (LOOP)

The LOOP mode of operation is initiated by the detection of an undervoltage at one of the two 4.16 kV emergency buses (E5 or E6), after some time delay before the EDGs are started in order to allow for a potential transfer of load from the unit auxiliary transformers to the reserve auxiliary transformers. If undervoltage is detected while offsite power is unavailable, the EDGs are started immediately.

Safeguard Operation

Safeguard operation is initiated by a Safety Injection (SI) signal, emitted in case of low pressurizer pressure or high containment pressure. Upon reception of the SI signal, the required safety loads are energized and the DGs are automatically started, but they run with no load.

Should offsite power fail, then the DGs would be automatically connected to their 4.16 kV emergency bus.

Test Operation

The test operation mode is manually controlled. In this mode, most of the protective trip devices of the DG are deactivated.

9.2.1.2. Supplemental Emergency Power Supply

The SEPS was added about ten years ago to enable EDG major maintenance tasks that had been traditionally performed during refueling outages to be performed online. Indeed, following the installation of the SEPS, a 14-day AOT for the two main EDGs was granted (versus a value of 72 hours previously). SEPS maintenance is performed online and the system is unavailable for about 5 days per year [74]. The addition of the SEPS was decided after the extension of a refueling outage from 33 days to 100 days due to a major EDG failure that occurred at about the fourth hour of a 24-hour run test, in November 2000.

The SEPS can be connected to both Class 1E 4.16 kV buses. It is automatically started when the bus to which it is aligned (bus E6 by default) is no longer energized by the normal sources. The SEPS consists of two individual 4.16 kV diesel generators that start and synchronize automatically upon a LOOP signal. They are always used simultaneously to energize the SEPS electrical bus [74].

9.2.2. Technical Specifications: Allowed Outage Times

The different operational modes are defined in Table 9-1.

Mode	Reactivity Condition, k_{eff}	% Rated Thermal Power*	Average Coolant Temperature
1. Power Operation	≥ 0.99	> 5%	≥ 350°F
2. Startup	≥ 0.99	≤ 5%	≥ 350°F
3. Hot Standby	< 0.99	0	≥ 350°F
4. Hot Shutdown	< 0.99	0	350°F > T_{avg} > 200°F
5. Cold Shutdown	< 0.99	0	≤ 200°F
6. Refueling**	≤ 0.95	0	≤ 140°F

* Excluding decay heat
** Fuel in the reactor vessel with the vessel head closure bolts less than fully tensioned or with the head removed

Table 9-1 : Operational Modes (from [50])

9.2.2.1. Modes 1 to 4

In modes 1 to 4, LCO 3.8.1.1 states that, at least, the following AC sources must be operable [50]:

- Two independent circuits between the offsite transmission network and the onsite Class 1E distribution system
- The two main EDGs with sufficient fuel oil and lube oil .

As is mentioned in Section 7.2.2, LCO 3.0.4.b (= risk-informed TS initiative 3) is not applicable to the DGs, i.e. the licensee is not allowed to go from shutdown modes (modes 5 and 6) to higher modes (modes 1 to 4) if an EDG is not operable.

Should one or two EDGs be inoperable, the TS prescribe the following actions.

An EDG inoperable

With an EDG inoperable, the licensee is required to [75]:

1) Demonstrate the operability of the two offsite power transmission systems within 1 hour and at least every 8 hours thereafter by verifying correct breaker alignments.
2) Demonstrate the operability of the remaining EDG within 24 hours by verifying that it starts from standby condition and reaches steady state voltage (4.16 kV ± 420 V) and frequency (60 ± 1.2 Hz) (slow-start test), unless the remaining EDG has been successfully operated in the last 24 hours or if the EDG became inoperable due to:
    - Planned preventive maintenance

- An inoperable support system with no potential common mode failure for the remaining EDG
- An independently testable component with no potential common mode failure for the remaining EDG.

3) Verify that all the systems that rely upon the remaining EDG to obtain emergency power are operable, and that the steam-driven emergency feed water pump is also operable (except in mode 4). If these conditions are not met within 4 hours, the reactor has to be at least in Hot Standby (Mode 3) within the next 6 hours and in Cold Shutdown (Mode 5) within the next 30 hours.
4) If the SEPS is available, the AOT to restore the DG to operable status is 14 days, 72 hours otherwise. This AOT was determined based upon the capacity and capability of the remaining AC sources, a reasonable time needed for diagnosis and repair, and the low probability of a design basis accident during this interval. If the end of this AOT is reached, the reactor has to be in Hot Standby (Mode 3) within the next 6 hours and in Cold Shutdown (Mode 5) within the next 30 hours.

This 14-day AOT was granted after the addition of the SEPS for both corrective and preventive maintenance, thus greatly increasing the possibility to perform online some major EDG maintenance tasks that were traditionally performed during refueling outages.

Both EDGs inoperable

With both EDGs inoperable, the licensee is required to [75]:

1) Demonstrate the operability of the two offsite power transmission systems within 1 hour and at least every 8 hours thereafter by verifying correct breaker alignments
2) The AOT to restore at least one of the EDGs to operable status is 2 hours. If the end of this AOT is reached, the reactor has to be in Hot Standby (Mode 3) within the next 6 hours and in Cold Shutdown (Mode 5) within the next 30 hours.
3) If the SEPS is available, the AOT to restore both EDGs to operable status is 14 days, 72 hours otherwise. If the end of the AOT is reached, the reactor has to be in Hot Standby (Mode 3) within the next 6 hours and in Cold Shutdown (Mode 5) within the next 30 hours.

9.2.2.2. Modes 5 and 6

In cold shutdown (Mode 5) and refueling mode (Mode 6), LCO 3.8.1.2 states that, as a minimum, the following AC sources must be operable:

- One circuit between the offsite transmission network and the onsite Class 1E system
- One EDG, with sufficient fuel oil and lube oil.

If these requirements are not met, the licensee is required to immediately suspend operations that involve the movement of fuel elements and reactivity control components within the reactor vessel, movement of irradiated fuel, crane operations with loads over the fuel storage pool; and within 8 hours, the licensee is required to depressurize and vent the Reactor Coolant System [50].

9.2.3. Surveillance Requirements

The EDG Surveillance Requirements were defined in accordance with Regulatory Guide 1.9 (Rev. 2), outlined in Section 8.3.3.

9.2.3.1. Monthly testing

Monthly testing of the EDGs at can be broken up into two categories [79]:

Basic verifications

Every month, the licensee is required to:

- Verify the inventory of fuel oil (day tank and storage tank) and lube oil
- Verify the capability of the fuel transfer pump to start and transfer fuel from the storage tank to the day tank
- Check for and remove accumulated water from the day tank and storage tanks
- Test new and stored fuel oil according to the corresponding program.

Slow-start and load-run test

Every month, the licensee must verify that the EDG starts from standby condition and reaches steady-state voltage and frequency within the prescribed margins. For this test, a slow-start procedure involving idling and gradual acceleration can be used to reduce stress and wear.

Then, the operator verifies that the EDG is capable of synchronizing with offsite power, being gradually loaded to a load comprised between 5600 kW (maximum expected accident load) and 6100 kW (continuous rating of the DG), and operating within this load band for at least 1 hour and until equilibrium temperatures are reached.

9.2.3.2. Six-month testing: fast-start and load-run test

At least every 6 months, the licensee is required to verify that the EDG is able to start from standby condition and achieve required voltage and frequency in 10 seconds [79]. This 10-second start requirement supports the assumptions in the design basis LOCA analysis. Then, the load-run test is performed as described previously. This periodic test can be performed in lieu of the monthly test.

9.2.3.3. Eighteen-month testing

These tests were originally required to be performed during reactor shutdown. However, this requirement has been relaxed in RG 1.9, as mentioned earlier, and the licensee is now allowed to perform a portion of these tests during operation, provided that an evaluation supports the safe conduct of these surveillance tests during modes other than shutdown. The extension of the at-power AOT from 72 hours to 14 days mentioned above (thanks to the addition of the SEPS) has greatly increased the possibility to perform online maintenance, and currently most of the periodic tests mentioned below are performed online (Mode 1).

Largest load and design load rejection tests

At least once per 18 months, the operator is required to verify the ability of the EDG to reject a load of at least 671 kW (largest single load) while maintaining voltage at 4160 ± 420 V and frequency at 60 ± 4 Hz. Furthermore, it must also verify the ability of the EDG to reject a full load (6083 KW) without overspeed tripping or exceeding a voltage of 4784 V.

LOOP test

In this test, the operator is required to verify that, when a LOOP signal is simulated, the emergency buses are deenergized, loads are shed from these buses, the EDG starts from standby condition and achieves steady state voltage and frequency within a maximum of 12 seconds, energizes the shutdown loads through the load sequencer, and supplies power to these loads for

at least 5 minutes. The 12-second requirement is derived from the requirements of the LOOP accident analysis.

SIAS (Safety Injection Actuation Signal) test

In this test, the operator must verify that upon an SIAS (without LOOP signal), the EDG starts from standby condition and achieves steady state voltage and frequency within a maximum of 10 seconds, then operates for at least 5 minutes.

Combined SIAS and LOOP test – Protective-trip bypass test

This test consists in the LOOP test described above, with the addition of an SIAS and a required starting time of 10 seconds. The operator must also verify that all EDG trips, except engine overspeed, low lube oil pressure, generator differential protection and emergency bus fault protection, are automatically bypassed upon the combination of an SIAS and a LOOP signal.

Endurance and load margin test

Every 18 months, the licensee is required to verify the ability of the EDG to operate at a load comprised between 5600 kW (maximum expected accident load) and 6100 kW (continuous rating of the DG) for at least 24 hours, of which 2 hours or less may be at a load between 6363 and 6700 kW.

Hot restart test

The operator must verify that, within 5 minutes of shutting down the EDG after it has operated for at least 2 hours at a load comprised between 5600 kW and 6100 kW, the EDG starts and achieves steady state voltage and frequency (within the tolerance band) within a maximum of 10 seconds after the starting signal.

Synchronizing test

The licensee must verify the EDG's capability to synchronize with offsite power upon a simulated restoration of offsite power (while the EDG is loaded with its emergency loads), transfer these loads to the offsite power, and then be restored to standby status.

Test mode override test

This test consists in verifying that, when the EDG operates in test mode and is connected to its emergency bus, a Safety Injection signal overrides the test mode by returning the EDG to standby status and automatically energizing the emergency loads with offsite power. This test is designed to ensure the availability of the EDG when being tested and connected to its bus.

9.2.3.4. Ten-year testing: independence test

At least every ten years, or after any modification that could have affected the independence of the two main EDGs, the operator must perform a fast-start test (see above) for both EDGs simultaneously, from standby conditions and during plant shutdown [79]. This test is performed to demonstrate that the EDG independence has not been compromised, which is done by comparing for each DG the evolution of the different parameters measured during this test with the same parameters measured during the usual, individual fast-start tests.

9.2.4. PRA evaluation supporting the AOT extension

As mentioned above, the 14-day AOT for one EDG when the reactor is in Mode 1 to 4 has been made possible thanks to the addition of an additional emergency AC power source, the SEPS. Previously, there was a 72-hour AOT, which was deemed too short for performing some of the 18-month surveillance tests or some maintenance tasks without risking reaching this AOT and having to shut the reactor down. Thanks to this 14-day AOT, most of the periodic tests traditionally performed during refueling outages (the 18-month periodic tests presented in Section 9.2.3.3) are now performed online. Benefits of this maintenance being performed online are examined in Section 9.2.5.

It should also be noted that Seabrook Station is not an isolated case: many other US utilities have been granted a similar AOT extension or have applied for it [48]. In order to support this AOT extension, a probabilistic risk analysis was performed to analyze the change in risk resulting from the addition of the SEPS and the AOT extension.

9.2.4.1. PRA model

The quantitative risk assessment performed to support this AOT extension is based upon a living, integrated PRA that covers all reactor modes. The power mode portions (Modes 1 to 3)

of the PRA model are full scope (internal and external events, including internal fires, seismic events, flooding...) and Level 2, while the shutdown mode portions (Modes 4 to 6) are internal events and Level 1 [77]. The Seabrook PRA has been reviewed several times in the past:

- In the 1980s: by Lawrence Livermore National Laboratory and Brookhaven National Laboratory
- In 1999: peer review, using the Westinghouse Owner's Group (WOG) methodology.

For the purpose of this PRA evaluation, the SEPS was added to the model, using conservative assumptions due to a lack of data for some of the SEPS parameter (in particular, SEPS diesels are assumed to be as reliable as the main EDGs, which is deemed conservative).

Then, the 14-day AOT had to be modeled in the PRA, which is not straightforward at all. Indeed, there is no direct link between the AOT and the risk configuration, since the maximum number of times that the corresponding LCO will be entered in one year is undetermined. Thus, assumptions have to be made regarding expected preventive and corrective maintenance practices. The duration of preventive maintenance can be predicted rather easily, thanks to industry and plant-specific experience. However, corrective maintenance cannot be easily predicted; furthermore, switching maintenance from outages to online could change the needs for corrective maintenance compared to past experience. A common assumption in this case is to assume that a tenth of AOT will be devoted to corrective maintenance each year. But one should be aware that this assumption is associated with great uncertainty.

More specifically, to model the effect on risk of the 14-day AOT at Seabrook, it was assumed in the risk assessment that all scheduled maintenance is performed in Mode 1 (full power operation), with (Ref. [74]):

- Preventive maintenance: 7 days every 18 months, which corresponds to the 18-month periodic maintenance that was performed in Mode 5 and 6 prior to the 14-day AOT extension
- Corrective maintenance (except common cause corrective maintenance): 14 days every 10 years (i.e. one tenth of AOT every year).

9.2.4.2. Risk analysis results

The addition of the SEPS combined with the 14-day AOT and online EDG maintenance provides a 30% CDF reduction, while the LERF remains virtually unchanged [77]. On the whole, this PRA study effectively supported these modifications, which were subsequently approved by the NRC

9.2.5. EDG maintenance: online versus refueling outages

Let us break up the comparison of the two strategies into several aspects:

Effect upon Refueling Outages

This is often presented as one of the main benefits of performing the maintenance of the EDGs online: it permits the operator to achieve shorter refueling outages (RFOs), hence making substantial savings. On the other side, not only does EDG maintenance during RFOs increase the duration of these RFOs, but it also increases the outage scheduling complexity. Furthermore, upon emergence of unexpected problems in the maintenance of the EDGs performed during plant outage, this practice may further increase the duration of the RFO, and it could create the need to resequence the outage schedule. Finally, we remember from Section 9.2.2.2 that, during outages, if the second EDG also becomes inoperable, the TS require that movements of fuel be immediately stopped, which would of course be a serious problem during RFOs.

Focus of Work

If EDG maintenance is done online, plant focus can be placed on that matter, while if performed during RFO, much maintenance and many different activities are performed at the same time, hence with less focus upon the maintenance of EDGs (and so the potential for human error is higher). During EDG online maintenance, measures are taken to limit the work on other systems. Even though it has not been quantified, the efficiency and quality of EDG maintenance is thought to have improved due to the online maintenance strategy.

Onsite Workers versus Contractors

Performing EDG maintenance online provides the possibility to use mostly onsite workers, which has many advantages: decreased costs, simpler from an administrative and security perspective, greater productivity and work quality as onsite workers are familiar with the

plant and its procedures, and they can prepare the EDG outage in advance and under good conditions (planning, procedures, preparation of parts and extra parts...). However, it also generates some additional costs due to workers that have to come to the plant especially for the outage of one EDG, while during RFO they would be here for the outage of both EDGs and possibly also for other tasks performed during RFO. In addition, adequate training is required to maintain skills, which has a cost too (but maintaining the skills within the plant can be beneficial for the company). Furthermore, contractors are specialist in EDG maintenance and may be more experienced and aware of EDG issues at other facilities.

EDG maintenance performed during RFO causes increased costs due to the need for EDG qualified contractors. Moreover, many plants have their RFO in the same period of the year, during which the ability of EDG vendors to support EDG outages is therefore reduced.

TS Issues

During refueling outage, no AOT is involved (only one EDG is needed), while in full power mode, there is a risk of shutdown if maintenance of the EDG is not completed by the end of the 14-day AOT. However, exceeding this AOT appears to be an unlikely event.

Nevertheless, we have seen in Section 9.2.2.1 that the inoperability of one EDG in full power modes has other consequences associated with TS requirements since the operator is required to:

- Demonstrate the operability of the systems supplied by the remaining EDG and the operability of the steam driven emergency feed water pump
- Demonstrate the operability of the two offsite circuits.

Impact on ROP Evaluation

As discussed in Section 6.1.2, one of the Performance Indicators of the Reactor Oversight Process, the risk-informed MSPI (Mitigating System Performance Index), involves the EDGs. The objective of the MSPI is to monitor the readiness of some important safety systems, including EDGs. In order to establish the color of this Performance Indicator (green, white, yellow, red), the average unavailability of the EDGs during the past three years is calculated and compared to specific threshold values that have been established according to the associated CDF increase. Planned unavailability due to online EDG maintenance contributes to this unavailability, which increases the risk for the plant to obtain a non-green MSPI color (which is

highly undesirable). This problem does not arise with EDG maintenance during RFO, because only one EDG is then required to be operational.

9.3. Online maintenance of ECCS in France and the US

9.3.1. Introduction

The role of ECCS (Emergency Core Cooling Systems) is to provide borated water to ensure core cooling and subcriticality upon one of the following postulated accidents [50]: LOCA, rod ejection, loss of secondary coolant accident, steam generator tube rupture. There are typically three phases in ECCS operation:

- Injection phase: water is taken from the refueling water storage tank (RWST) and injected into the reactor coolant system through the cold legs.
- Cold leg recirculation: once enough water has been injected, water is then taken from the containment sump and injected into the cold legs to ensure recirculation.
- Hot leg recirculation: after about 24 hours, the injection is shifted to the hot legs, providing a backflush to reduce boiling in the upper part of the core and to avoid boron precipitation.

In a typical US PWR, the ECCS are comprised of two redundant subsystems (trains), each one being composed of:

- A centrifugal charging (= high head) pump
- A safety injection (SI) (= intermediate head) pump
- A residual heat removal (RHR) (= low head) pump.

Similarly, in EDF 900 MWe (CPY) series, the ECCS are comprised of [90]:

- Three high head safety injection pumps (2 + 1) (RIS HP)
- Two redundant low head safety injection pumps (RIS BP)
- Two redundant RHR pumps (RRA).

In a PWR, there are also accumulators (vessels partially filled with borated water and pressurized with nitrogen) that are typically used during the early phase of a LOCA to rapidly inject borated water into the cold legs.

9.3.2. ECCS technical specifications in France

In the CPY series, all the ECCS pumps are required to be operational in full power mode. If one system is inoperable, the following events are treated in the Tech Specs [90]:

- If one high head pump of the train that has two such pumps is inoperable: group 2 event
- If all the high head pumps of a same train are inoperable: group 1 event
- If one low head train is inoperable: group 1 event
- If one RHR train is inoperable: group 2 event

There is no Borderline Condition applicable to the low head systems. Therefore, taking a low head pump out of service for online preventive maintenance is simply not allowed. As for the high head pumps, it is possible to maintain online a pump of the train that has two pumps, because its loss only generates a group 2 event, therefore the licensee is allowed to voluntarily generate this event (as long as the Simultaneity Rules are respected). Also, there is a Borderline Condition that allows the licensee to make this same high head train unavailable for 6 hours per year in order to perform requalification tasks when one of the two high head pumps of this train has undergone online preventive maintenance. However, the high head pump of the other train cannot be taken out of service, because it generates a group 1 event and there is no applicable Borderline Condition.

Therefore, allowed online preventive maintenance of ECCS is very limited: it is not possible for low head systems, and it is possible only for two out of three high head pumps.

9.3.3. Online maintenance of ECCS in the US

For US PWR, the two ECCS subsystems are required to be operable in full power mode (one subsystem = {a centrifugal charging pump, an SI pump, an RHR pump, an RHR heat exchanger, flow paths with the RWST and the containment sump}). The AOT for one ECCS

subsystem is typically 3 days [50], sometimes more (e.g. 7 days) when an AOT extension has been granted.

As always, voluntary entry into this tech specs LCO is not considered to be a violation of the TS, as long as (1) the AOT is respected, (2) the risk increase is assessed and managed (Maintenance Rule §(a)(4)), and (3) it is done for an acceptable reason, online preventive maintenance being considered by the NRC as an admissible reason (see Section 6.1.3.2). Concerning the periodic tests recommended in the STS (ref. [50]), no surveillance is explicitly required to be performed during plant shutdown, even though in practice, for some surveillance tasks, shutdown conditions are more appropriate.

The possibility to perform online maintenance is typically exploited in order to perform 3-month tests (in particular, concerning individual pump starting) and some minor maintenance tasks. Each time, one ECCS subsystem is taken out of service for no more than a couple of hours. The 18-month tests and major maintenance tasks (such as pump overhauls) are generally performed during RFO. There are two main reasons to this:

- AOT limitation: the duration of an online maintenance task must be short enough compared to the AOT, to have sufficient time margin to avoid an unplanned shutdown.
- Operational reasons: at-power conditions are not adequate for particular tasks, especially those that involve venting/filling the systems.

Even though the amount of ECCS maintenance performed online is small, there are however benefits in doing them online rather than during RFO. Like for EDG online maintenance, it enables the operator to place more focus upon these tasks when performed online, due to the small amount of activities ongoing at this time. Also, it enables one to slightly reduce the duration (and the scheduling complexity) of refueling outages, even though this reduction is clearly not as significant as that associated with EDG online maintenance. Nevertheless, it has been reported to us that many small maintenance tasks performed online have a cumulated effect on the reduction of RFO duration that is eventually not negligible.

Regarding the issue of ROP performance indicators, ECCS unavailability also contributes to the MSPI. However, the couple of hours of planned unavailability associated with ECCS online maintenance has only a small effect on this indicator.

9.3.4. Conclusion

While online maintenance of certain ECCS components (such as the low head safety injection pumps) is not authorized under normal circumstances by the French regulations, it is allowed in the US, under the usual conditions. But, in practice, this possibility is not heavily used, mostly for operational reasons. However, the flexibility offered by the regulation is beneficial for the operator to improve the focus upon some maintenance tasks and to somewhat reduce the number of tasks performed during RFOs.

For the ECCS, the stakes are not the same as those associated with EDGs regarding the amount and the effect of online maintenance, but these systems are probably more representative of typical safety-related systems regarding the issue of online maintenance: online maintenance is authorized, but the actual amount of maintenance performed in full power mode remains limited. It provides however an appreciable flexibility for planned periodic maintenance, and it spares the need for exemption requests when the operator occasionally needs to take a system out of service for a short period of time. Also, the cumulative effect of online maintenance practices is thought to be beneficial for operational and safety performances, as is explained in Section 6.1.4.

9.4. Summary

These case studies illustrate many of the differences between the French and US frameworks that had been identified in Chapter 6. In the US, the licensee has much flexibility to perform online maintenance, being allowed to take an SSC out of service as often as needed, as long as the risk is assessed, acceptable and managed (§(a)(4) of the Maintenance Rule) and as long as ROP performance indicators (such as the MSPI) are not unacceptably degraded. Also, in the US there is no distinction in the treatment of online maintenance and periodic tests, in the sense that AOTs and voluntary entry into TS events are considered regardless of the reason for the unavailability of the system (online maintenance or online periodic test). In France, there is

no such flexibility for online maintenance and periodic tests. In the case of EDGs, to perform online some maintenance tasks identified in the PBMP that would make an EDG inoperable, the licensee is granted a limited budget of time by the Borderline Conditions; and to perform periodic tests online, the group 1 events generated by these tests must have been explicitly identified in the applicable Periodic Test Rules when proposed to the safety authority, which was not the case for the EDGs (since it was not technically necessary).

Also, the non-prescriptive configuration risk management strategy adopted in the US (§(a)(4) of the Maintenance Rule, blend of probabilistic and deterministic considerations) provides significant flexibility for managing simultaneous outages, planned or unplanned, which is another point that facilitates the application of online maintenance. In France, configuration risk management is handled using the deterministic, prescriptive Simultaneity Rules that are more rigid, but they also have the advantage of being easier to implement.

The EDG case study also shows how PRA insights can be effectively used in the US to support Tech Specs modifications that provide more flexibility for performing online maintenance and testing of EDGs, while in France, the attempt to change the EDG STEs (and in particular the budget of time allocated by the Borderline Conditions) using PRA did not succeed, due to difficulties within EDF and with the safety authority.

Chapter 10

Conclusions and implications

10.1. Effects of online maintenance practices

In this section, we summarize generic effects of online maintenance practices encountered throughout our work. Given that online maintenance has been more applied in the US than in France (for safety systems), most of the elements below are based upon US experience.

10.1.1. Benefits of online maintenance

Online maintenance can have operational, economical, but also safety benefits. While some benefits can be quantified, others are more intangible.

- The flexibility offered in the US to the licensee to voluntarily enter one or several Tech Specs LCOs, as long as risk is assessed and managed, eliminates the need for some Tech Specs exemption requests when, exceptionally, the licensee needs to (briefly) enter a particular maintenance configuration. In France, this flexibility exists, but within the strict limits of the Simultaneity Rules and the Borderline Conditions (for group 1 events).
- Performing specific maintenance tasks during operation rather than RFO can enable one to reduce the duration of these outages, hence obtaining better capacity factors. On a case-by-case basis, this effect can be quantified, especially for particular SSCs for which major maintenance tasks are performed online (see the EDG case at Seabrook Station). For other SSCs (see the ECCS case), the effect on RFO duration may be less visible, but the cumulative effect is thought to be non-negligible. Also, performing particular tasks online can enable the operator to reduce the complexity of RFO scheduling and the potential for

RFO complication and extension. At the US industry level, online maintenance is thought to have significantly contributed to the reduction of RFO duration observed on Figure 6-2.

- The safety effect of online maintenance can be quantified, on a case-by-case basis, using PRA, as illustrated in Section 9.2.4 with the EDG case study. It enables one to verify that safety is improved or not unacceptably degraded, to assess the effect of potential hardware modifications, of some hypotheses. There are also some aspects of safety that are more intangible and difficult to quantify, but no less important, such as the improvement of the safety culture at the operational level (in particular through the use of risk monitors), a better focus of workers due to a reduced amount of activities during operation and better preparation, hence a smaller potential for human errors. Improvement of SSC reliability, when observed, can often not be linked solely to the online aspect of maintenance. At the US industry level, reductions of the scram rate and of the average CDF have been observed (see Section 6.1.4) showing that, at least, these safety parameters were not degraded during the development of online maintenance practices.
- Performing some maintenance online instead of during RFO can offer the possibility to employ onsite workers rather than contractors (see discussion in Section 9.2.5), with benefits resulting in terms of efficiency and quality.

10.1.2. Drawbacks and difficulties

Online maintenance also presents some difficulties compared to traditional RFO maintenance practices.

- Time constraints are particularly important for online maintenance: during RFO, if a maintenance activity lasts longer than planned (and belongs to the critical path), maintenance tasks may have to be shifted, but, a priori, there is no major "cliff-edge effect", while for online maintenance, if a maintenance activity lasts longer that planned and if the end of the AOT is reached, the reactor may have to be shutdown. It implies in particular that significant time margins are required (typically, the planned duration of an online maintenance activity is smaller than half of the applicable AOT). Such margins are also necessary to reduce the stress upon workers and improve the quality of maintenance.
- In order to reach an acceptable level of safety, compensatory measures and/or hardware modifications (in particular for "major" online maintenance tasks) may be needed. It may be

less necessary for very short maintenance tasks. Assessment of uncertainties and sensitivity studies are essential in risk analyses justifying Tech Specs modifications requested to facilitate the implementation of new online maintenance practices.

- If onsite workers are used instead of contractors for online maintenance, even though this may present some advantages, it also creates a need for continuous training. Onsite workers may also be less specialized than contractors and less aware of current issues encountered with the considered systems at other sites.

10.1.3. Potential candidates for online maintenance

For safety as well as operational reasons, it is clear that online maintenance cannot be indiscriminately applied to plant SSCs, in particular safety-significant SSCs. Regarding safety-significant SSCs, based upon US experience, we can identify two general classes of tasks that can be considered as candidate for online maintenance:

- Quick tasks (compared to the applicable AOT) with very low potential for complication: such maintenance tasks are usually acceptable from a safety standpoint, given their short duration, and in general they do not necessitate hardware modifications or major compensatory measures. One example encountered in this thesis is the case of the ECCS (Section 9.3.3). Such individual online maintenance tasks will typically have a small effect on the duration of RFOs but, cumulatively, they can help in shortening and simplifying these RFOs. Other advantages mentioned above may also be applicable.
- Longer, well-chosen tasks for few safety-significant SSCs: in some cases, an AOT extension may be necessary to ensure that workers have sufficient time margins to complete these tasks, and such amendment request must be strongly supported by a risk analysis. The case of EDGs at Seabrook Station (Section 9.2) is a good example of such major online maintenance task. It will often require compensatory measures and, in some cases, hardware modifications. From a deterministic standpoint, the licensee must ensure that sufficient redundancy and defense-in-depth are available, and the amount of maintenance work performed simultaneously must be limited in order to ensure sufficient staff capability and focus for the considered task, in particular to minimize the risk of outage extension. A probabilistic risk assessment is a very powerful tool, if not essential, to supplement the deterministic approach, to establish that safety is improved (or not unacceptably degraded),

and to assess the effect of potential hardware modifications. Such well-chosen tasks can bring significant benefits such as those identified in Section 10.1.1.

Each individual case would need a dedicated, plant-specific study in order to assess the implications and benefits of an online maintenance strategy. In the specific case of EDGs, the positive results observed at Seabrook Station may not be directly applicable to EDF plants without a dedicated study covering all aspects of this choice (economical, effect on RFO duration, effect on safety...). There are however elements that tend to indicate that, regardless of the regulatory difficulties (see the discussion below), an online maintenance strategy might be acceptable at least from a safety standpoint. Indeed, redundancy and diversity are available for onsite emergency AC sources, with the LLS and the TAC/GUS systems in addition to the two main EDGs (it should be noted however that, contrary to the Seabrook case, the TAC or the GUS is shared by several units), and, as is mentioned in Section 9.1.6, a PRA study had established that the budget of time allocated for the replacement of an EDG by the GUS in a CPY unit to perform online maintenance could be extended from 10 days to 1 month per year.

10.2. Online maintenance in France: possible directions and implications

As is explained in the previous chapters, the current French regulatory framework is not particularly favorable to the implementation of an online maintenance strategy for safety-significant SSCs. If EDF were to decide to switch to online maintenance and testing for some safety related systems (associated with group 1 events), changes would be needed. In this section, we identify several directions that could be considered in such a case.

10.2.1. Direction 1: no major regulatory changes

The first possible direction would not involve any major regulatory change. More specifically, the following concepts would be kept: Simultaneity Rules, distinction between group 1 and group 2 events, Borderline Conditions (for online preventive maintenance), RGE exemptions officialized in Periodic Test Rules (for online periodic tests), and no risk monitor. However, some modifications would be needed, on a case-by-case basis:

- For online preventive maintenance, Borderline Conditions may have to be created and/or extended, when acceptable from a safety standpoint.
- For online periodic tests, Periodic Test Rules would need to be modified (to include the possibility of performing online some periodic tests, thus constituting official RGE exemptions) and approved by the ASN.
- The philosophy regarding the use of Borderline Conditions and the creation of RGE exemptions in Periodic Test Rules may have to be recast to be more adapted to the issue of online maintenance, especially when there is no "technical necessity" to perform the considered maintenance task or periodic test online (see below).
- A significant cultural change would be needed, and an online maintenance policy would have to be defined at a centralized level within EDF, in order to clarify, unify, and possibly systematize the use of these two opportunities for online maintenance and testing.

For the first two items, a probabilistic approach (combined as always with more traditional approaches) would probably be the most convincing approach, since EDF would have to justify that the use of these new or extended Borderline Conditions and RGE exemptions would improve, or not unacceptably degrade the safety level.

The main advantage of this first option is that the regulatory framework would remain mostly unchanged. It presents however some drawbacks and difficulties:

- Each SSC would have to be treated on a case-by-case basis for the formulation, the justification and the approval of the necessary changes, hence creating a need for significant resources at the engineering and regulatory levels.
- Online preventive maintenance and online periodic tests would still be treated separately.
- The configuration risk management through the use of the Simultaneity Rules would still be generic (i.e. non-configuration-specific) and inflexible. In most cases, it would probably be acceptable regarding the safety level, because the Simultaneity Rules are thought to be conservative in most configurations, but there may be situations where it is not the case.
- The performance of online maintenance/testing through the use of Borderline Conditions and RGE exemptions formulated in Periodic Test Rules is actually not in complete accordance with the philosophy of these elements when there is no strong operational need for voluntary entering Group 1 events (i.e. when these maintenance tasks or periodic tests

can be performed offline without undue operational difficulties), hence the third need mentioned at the beginning of this section. Indeed, as is explained in Section 6.2.2.2, Borderline Conditions should be used for "operational imperatives", which can be interpreted as follows: if there is no imperative to perform a particular preventive maintenance task online, then the Borderline Condition should not be used for this task, and so this task should be carried out when the SSC is not needed, i.e., typically, offline. And, as is explained page 103, RGE exemptions officialized in Periodic Test Rules to perform particular periodic tests online are also typically granted only when there is a technical need for this, and usually not simply for operational convenience.

- If EDF were to decide to use a risk-informed approach to justify some of the changes mentioned above (which may not be the only possible approach, but probably the most convincing one), several questions would have to be addressed (see Section 4.8) to improve the acceptability of these methods both within the safety authority and EDF. Considering the elements presented on that matter, it appears to be a significant difficulty.

A possible adjustment to this first approach would be to standardize the treatment of online maintenance (tasks defined by the PBMP) and online periodic tests (tests defined by the Periodic Test Rules) through the system of Borderline Conditions: a budget of time would be allocated to permit voluntarily entry into a group 1 event, whether it would be to perform tasks from the PBMP or tests from the Periodic Test Rules. It would result in a more consistent treatment of the safety aspects, and would potentially reduce the amount of required work (no need to modify the Periodic Test Rules). Periodic tests for which there is a technical need to enter a group 1 event (i.e. those already identified by Periodic Test Rules) may be treated separately.

10.2.2. Direction 2: risk-informed configuration risk management

A second direction that could be considered would be to adopt a treatment similar to the risk-informed CRMP (Configuration Risk Management Program) developed by US utilities to comply with §(a)(4) of the Maintenance Rule (Section 5.2.2.4), in particular based upon the use of a risk monitor. The concepts of Borderline Conditions for online maintenance and RGE exemptions for online periodic tests would then no longer be needed. However, it could be

interesting to preserve the concept of Simultaneity Rules in order to maintain a deterministic safeguard.

The simplest solution (and probably the most conservative one, in most cases) would be to decide that, whenever the Simultaneity Rules are applicable, then they should prevail, no matter what the results of the risk-informed approach are. If this solution were to be adopted, risk information would be indicative only upon such multiple outages (but for configurations not covered by the Simultaneity Rules, it would be the main input to decide whether or not this configuration can be voluntarily entered for online maintenance/testing for the duration of the AOT). However, a more elaborate combination of the two approaches could be considered, in which there could be cases where, based upon the probabilistic risk assessment, the operator would be allowed to carry on regardless of the prescriptions of the Simultaneity Rules (the individual AOTs remaining in all cases the ultimate limits). Within this strategy, the following aspects could be considered to decide whether the operator would be allowed to go beyond the limitations imposed by the Simultaneity Rules: planned/unplanned nature of the events, margins between the results of the risk assessment and certain criteria (taking into account the uncertainties concerning these results), implementation of compensatory measures ...

Whichever solution is adopted, this second direction would call for many tasks, among which are the following:

- Development of the online configuration risk management tool, which includes in particular the choice of the scope (Level 2? Hazards? ...), the risk thresholds associated with the methodology to establish the acceptability of a given maintenance configuration (ΔCDF, ICDP, $\int \Delta CDF \cdot dt$ over a particular period, similarly with the LERF...), the treatment of uncertainties...
- Combination with the Simultaneity Rules
- Training to allow the use of this new tool on-site
- Possible AOT extensions to make feasible (with sufficient margin) the performance of particular maintenance tasks online
- Formulation of an online maintenance policy.

Compared to the first direction outlined in the previous section, this second direction presents many advantages:

- More flexibility for performing online maintenance for safety-significant SSCs (outage durations no longer restricted by Borderline Conditions).
- Depending upon the combination with the Simultaneity Rules that is adopted, the risk-informed treatment may provide the licensee with more flexibility regarding the allowed maintenance configurations (possibility to go beyond the Simultaneity Rules), for online maintenance, but also for maintenance during RFO.
- Through this option, the treatment of SSCs is more generic than with the previous one (no need to treat Borderline Conditions and RGE exemptions for online testing on a case-by-case basis). Also, online maintenance and testing would no longer be treated separately.
- The risk-informed approach enables one to address plant risk in a more systematic and consistent manner, regardless of the category of the TS events (group 1 or group 2), while currently, the Simultaneity Rules treat group 1 and group 2 events separately. Even if the choice were made to give priority to the Simultaneity Rules (when applicable), the risk monitor could still provide valuable risk information, possibly highlighting high risk situations currently allowed under the Simultaneity Rules, or conversely, situations where the Simultaneity Rules are overly conservative (and in such cases, results provided by the risk monitor could be used as a valuable input to a temporary STE exemption request, when needed).
- As explained in this thesis, the use of a risk monitor presents many other benefits, such as an improvement of the safety culture among plant workers, a better risk awareness, better risk management upon unplanned events, and better maintenance planning. The possible applications of this tool are numerous.

Use of this option would require deep cultural and regulatory changes, and the difficulties are numerous and considerable, in particular for EDF to agree with the safety authority on the scope of the risk monitor and the risk thresholds. Significant investment would therefore be needed. However, the possible applications of this new framework go far beyond the issue of online maintenance.

10.2.3. Direction 3: risk-informed AOTs

A third possible direction would be to develop a risk-informed treatment similar to that developed for the US risk-informed TS initiative 4b (see Section 7.3), where the licensee has the possibility to extend the traditional AOTs based upon a risk-informed treatment. However, in the light of elements presented throughout this thesis, there are numerous barriers to the acceptance of such a strategy in the French nuclear industry. Therefore, this option does not seem conceivable, at least in the short term.

10.3. Conclusion

In the United-States, voluntary entry into Technical Specifications for online maintenance and testing has been possible for a long time, but this possibility was not commonly exploited for safety-significant SSCs until the advent of mature risk-informed techniques that enabled licensees to quantify the effect of outages on plant risk and to compensate for some weaknesses of the deterministic technical specifications. Most licensees actually started to perform online maintenance more systematically after the promulgation of §(a)(4) of the Maintenance Rule. The implementation of this rule was often supported by the use of risk monitors, and it enabled licensees to establish a coherent framework to manage the risk associated with SSC outages, in particular during at-power operation. Online maintenance practices have appeared to be beneficial to operational, but also safety performance, even though some effects cannot be quantified or cannot be attributed solely to the use of online maintenance. More recently, the US nuclear industry has been developing and implementing ambitious risk-informed Tech Specs Initiatives that provide additional flexibility for online maintenance.

In France, the regulation is less favorable to the implementation of online maintenance practices for safety-significant SSCs. Online maintenance or testing of safety related systems is generally not allowed, or allowed under severe restrictions. Therefore, regulatory modifications would be necessary if EDF were to decide to implement an online maintenance strategy for safety-significant systems. In this chapter, we have identified three possible directions to implement such a strategy, ranging from very targeted modifications, without significantly changing the regulatory framework, to a more ambitious, risk-informed configuration risk

management. In any case, a significant culture change would be necessary, and substantial investment would be needed to solve issues regarding the acceptability of risk-informed applications with the safety authority and within EDF.

References

[1] WENRA, *Reactor Safety Reference Levels* (01/2008)

[2] ASN, O. Gupta, *Harmonization of safety approaches for Nuclear Power Plants*, WENRA Seminar (02/2006)

[3] WENRA, *Progress towards harmonization of safety for existing reactors in WENRA countries* (01/2011)

[4] H. Kumamoto and E.J. Henley, *Probabilistic Risk Assessment and Management for Engineers and Scientists* (2nd Ed., 1996)

[5] US NRC, NUREG-1150, *Severe Accident Risks: An Assessment for five US Nuclear Power Plants* (1990)

[6] US NRC, RG 1.174, *An approach for using Probabilistic Risk Assessment in risk-informed decisions on plant-specific changes to the Licensing Basis* (Rev. 1, 11/2002)

[7] US NRC, 51 FR 28044, *Safety Goals for the Operations of Nuclear Power Plants; Policy Statement* (1986)

[8] US NRC, 60 FR 42622, *Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities; Final Policy Statement* (1995)

[9] US NRC, SECY 89-102, *Implementation of the safety goals* (1990)

[10] US NRC, Memorandum from Chairman S.A. Jackson to L.J. Callan, *The Statement of Core Damage Frequency of 10-4 as a Fundamental Commission Goal* (07/1997)

[11] US NRC, RG 1.177, *An approach for plant-specific, risk-informed decisionmaking: Technical Specifications* (08/1998)

[12] US NRC, NUREG/BR-0058, *Regulatory Analysis Guidelines of the US Nuclear Regulatory Commission* (Rev. 4, 09/2004)

[13] US NRC, SECY 06-0217, *Improvement to and Update of the Risk-Informed Regulation Implementation Plan* (2006)

[14] A.C. Kadak and T. Matsuo, *The nuclear industry's transition to risk-informed regulation and operation in the United States* – Reliability Engineering and System Safety No. 92, 609-618 (2007)

[15] J.N. Sorensen, G.E. Apostolakis et al., *On the role of defense in depth in risk-informed regulation*, ANS conference PSA'99 (08/1999)

[16] ASN, Règle Fondamentale de Sureté, *Développement et Utilisation des Etudes Probabilistes de Sureté* (2002)

[17] ASN, *Les études probabilistes de sureté* – Contrôle No. 155 (12/2003)

[18] IRSN, Rapports Scientifiques et Techniques 2006, 2007, 2008

[19] IRSN, *Examples of use of risk informed applications in power reactors safety and gained results in France* (05/2005)

[20] EDF, S. Benzoni and V. Mouchard, *Méthodologie de détermination de la conduite à tenir en cas d'indisponibilité matérielle associée à un évènement de groupe 1* (05/2003)

[21] EDF, P. Brac, *PSA Applications for Technical Specifications, EDF Experience* - PWROG International Technical Workshop, May 5-6, 2010, Paris

[22] EDF, P. Brac, *Application des EPS pour les Spécifications Techniques d'Exploitation* – Module Sûreté Nucléaire, Ecole Centrale Paris (04/02/2010)

[23] NEA, CSNI/R(2007)12, *Use and Development of Probabilistic Safety Assessment* (11/2007)
[24] EDF, P. Brac, Personal Communications (12/2010, 02/2011, 12/2011)
[25] EDF, G. Labadie, Personal Communications (01/2011, 04/2011)
[26] EDF, Meetings and Interviews (06/27/2011 to 07/01/2011)
[27] IAEA, TECDOC 1138, *Advances in safety related maintenance* (03/2000)
[28] IAEA, *Management Strategies for Nuclear Power Plant Outages*, Technical Reports Series no. 449 (2006)
[29] NEA, NEA/CSNI/R(2008)12, *Better Nuclear Plant Maintenance: Improving Human and Organisational Performance* (2009)
[30] 10 CFR 50.65, *Requirements for monitoring the effectiveness of maintenance at nuclear power plants* (1991)
[31] US NRC, NUREG-1526, *Lessons Learned from Early Implementation of The Maintenance Rule at Nine Nuclear Power Plants* (1995)
[32] US NRC, RG 1.160, *Monitoring the effectiveness of maintenance at nuclear power plants* (Rev. 2, 1997)
[33] US NRC, RG 1.182, *Assessing and managing risk before maintenance activities at nuclear power plants* (2000)
[34] NEI, NUMARC 93-01, *Industry Guideline for monitoring the effectiveness of maintenance at nuclear power plants* (Rev. 2, 1996), and the Revised Section 11 (2000)
[35] US NRC, NUREG-1648, *Lessons Learned From Maintenance Rule Baseline Inspections* (1999)
[36] ASN, *Les enjeux de la maintenance* – Contrôle No. 154 (2003)
[37] N. Kerkar and P. Paulin, *Exploitation des coeurs REP* (2008)
[38] IAEA, TECDOC 1551, *Implementation Strategies and Tools for Condition Based Maintenance at Nuclear Power Plants* (05/2007)
[39] IAEA, TECDOC 1590, *Application of Reliability Centred Maintenance to optimize Operation and Maintenance in Nuclear Power Plants* (05/2007)
[40] J.P. Jacquot, A. Dubreuil-Chambardel, A. Lannoy, B. Monnier, *Développement de méthodes et d'outils pour l'optimisation de la maintenance par la fiabilité*, Journées SFEN 12/1992
[41] EDF, J. Lafouge, *AP913* (06/2008)
[42] EDF, DPI UFPI, *Formation M673 – AP913 – Module 1 – Les fondamentaux* (2008)
[43] EDF, C. Domecq, *Projet COSMA : Processus AP913, déploiement à DPN et travaux de R&D pour des axes de progrès* (08/2010)
[44] EPRI, *White Paper: On-Line Maintenance at Nuclear Power Plants: History, Implementation, and Benefits* (01/2009)
[45] EPRI, Technical Report 1009708, *Guidance for Developing and Implementing an On-Line Maintenance Strategy* (08/2004)
[46] 58 FR 39132, *Final Policy Statement on Technical Specifications Improvements for Nuclear Power Reactors* (07/1993)
[47] US NRC, NUREG-0800 §16.0, *Technical Specifications*
[48] EPRI, *White Paper: Safety and operational benefits of risk-informed initiatives* (02/2008)
[49] US NRC, Inspection Manual Part 9900: Technical Guidance, *Maintenance – Voluntary entry into limiting conditions for operation action statements to perform preventive maintenance* (01/2002)

[50] US NRC, NUREG-1431, *Standard Technical Specifications – Westinghouse Plants* (Rev. 3.0, 2004)
[51] EDF, P. Brac, *Document Standard des Spécifications Techniques d'Exploitation du palier 1300 MWe* (02/2005)
[52] NEI, *Risk-Informed Technical Specifications – Project Description* (06/2001)
[53] TSTF, TSTF Status Report – August 7, 2010
[54] G. Waig, *Status of Risk-Informed Technical Specifications Initiatives* - US NRC RIC 2010 (03/11/2010)
[55] US NRC, SECY 10-0143, *Annual update of the risk-informed and performance-based plan* (10/2010)
[56] S.M. Hess, *Risk managed technical specifications* – Progress in Nuclear Energy No. 51, 393-400 (2009)
[57] NEI, NEI 06-09, *Risk-Informed Technical Specifications Initiative 4b – Risk-Managed Technical Specifications (RMTS) Guidelines* (Rev. 0, 11/2006)
[58] E. Kee, D. Richards, C.R. Grantom and J.K. Liming, *Risk managed technical specifications implementation at South Texas Project Units 1 and 2* – Proceedings of the 16th International Conference on Nuclear Engineering (ICONE16) (05/2008)
[59] R. Grantom, *Plant Experience for Implementation of Risk-Informed Technical Specification Initiative 4b on Risk Managed Technical Specifications* - US NRC RIC 2010 (03/11/2010)
[60] E. Conaway, *Best of the Best TIP Achievement* – Nuclear Plant Journal, July-August 2008, 57-58
[61] B. Rapczynski, G. Kelly and P. Tarpinian, *Exelon's Limerick station pioneers a surveillance frequency control program* – Nuclear News, October 2007, 28-31
[62] G. Krueger, *Plant Experience for Implementation of Risk-Informed Technical Specification Initiative 5b on Surveillance Frequency Control* - US NRC RIC 2010 (03/11/2010)
[63] NEI, NEI 04-10, *Risk-Informed Technical Specifications Initiative 5b – Risk-Informed Method for Control of Surveillance Frequencies – Industry Guidance Document* (Rev. 1, 04/2007)
[64] TSTF, TSTF-358 (Rev. 6, 2001)
[65] TSTF, TSTF-359 (Rev. 9, 2003)
[66] A.J. Howe, *Risk-Informed Initiatives* - US NRC RIC 2011 (03/09/2011)
[67] E.J. Kates and W.E. Luck, *Diesel and high compression gas engines* (3rd Edition,1974)
[68] EDF, P. Brac and B. Daniel, *Etude MIT "comparaison des cadres réglementaires et des pratiques de sûreté entre France et Etats Unis" - Descriptif technique des diesels tous paliers*, H-T51-2011-00523-FR (03/2011)
[69] EDF, Y. Delauney, *Analyse d'exhaustivité des essais périodiques des groupes électrogènes de secours (LHP/Q) - 1300 MWe* (12/2009)
[70] EDF, Y. Delauney, *Règle d'essais périodiques des groupes électrogènes de secours (LHP/LHQ) – 1300 MWe* (12/2009)
[71] US NRC, ADAMS Access Number ML010650267
[72] US NRC, ADAMS Access Number ML11122A075
[73] US NRC, ADAMS Access Number ML111360432
[74] US NRC, ADAMS Access Number ML040620457
[75] US NRC, ADAMS Access Number ML042670036

[76] US NRC, ADAMS Access Number ML020240451
[77] US NRC, ADAMS Access Number ML041000405
[78] NextEra Energy, *Fact sheet on NextEra Energy Seabrook* (03/04/2011)
[79] US NRC, RG 1.9, *Application and testing of safety-related diesel generators in nuclear power plants* (Rev. 4, 03/2007)
[80] IEEE, IEEE Std 387-1995, *IEEE Standard Criteria for Diesel-Generator Units Applied as Standby Power Supplies for Nuclear Power Generating Stations* (Rev. of IEEE 387-1984, 12/1995)
[81] 10 CFR 50.63, *Loss of Alternating Current Power* (1988)
[82] US NRC, RG 1.155, *Station Blackout* (1988)
[83] US NRC, NUREG-1776, *Regulatory Effectiveness of the Station Blackout Rule* (2003)
[84] US NRC, NUREG/CR-6890, *Reevaluation of Station Blackout Risk at Nuclear Power Plants* (2005)
[85] US NRC, *The near-term task force review of insights from the Fukushima Dai-Ichi accident* (07/2011)
[86] ASN, Note Technique (02/17/2011)
[87] EDF, P. Scrivanti, *Programmes d'essais périodiques des systèmes IPS tous paliers, Généralités – Section 1* (RGE, Chap. IX, Section 1) (09/12/2001)
[88] EDF, M. Cabrol, *PBMP Systèmes élémentaires LHP/LHQ – 1300 MWe* (02/17/2005)
[89] EDF, V. Mouchard, *Réexamen des prescriptions STE relatives aux sources électriques du pallier CPY* (04/2004)
[90] EDF, V. Mouchard et al., *Document standard des spécifications techniques d'exploitation PTD n°2 CPY* (03/2008)

Appendix A Simplified Maintenance Rule flowchart

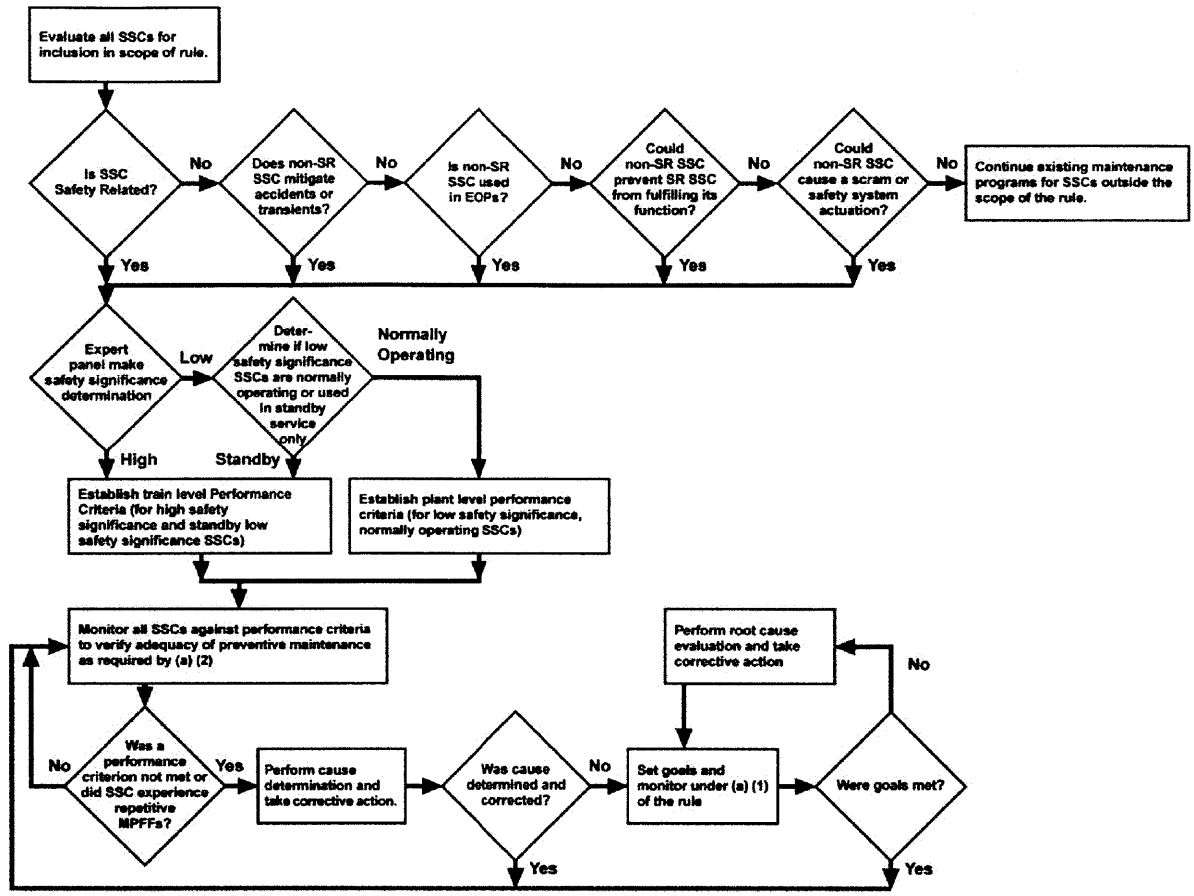


Figure A-1 : Simplified Maintenance Rule flowchart (from NRC's website)

SR = Safety-related

SSC = Structures, Systems and Components

EOP = Emergency Operating Procedures

MPFF = Maintenance Preventable Functional Failures

Appendix B Plant specific (PWR) Station Blackout information in 2000, sample

Plant	Plant CDF	SBO CDF	Percent SBO CDF of Plant CDF	Coping time in hours/EDG reliability/Aac access time in minutes/ extremely severe weather	Modification summary including dc load shed procedural modifications	SBO factors					
						PRA LOOP initiating event frequency	Number of LOOP events at power since commercial operation			LOOP event recovery times ≥ 240 minutes	
							Plant	Weather	Grid	Power	Shutdown
Crystal River Unit 3	1.53E-05	3.28E-06	21.5	4/.975/-/4	dc load shed. Added nonclass 1E battery	4.35E-01	3				
Davis-Besse	6.6E-05	3.50E-05	53	4/.95/10/2	Added 1 DG	3.50E-02	2	1		1680	
DC Cook Units 1&2	6.2E-05	1.13E-05	18.1	4/.975/-/2	dc load shed	4.0E-02	1				
Diablo Canyon Units 1&2	8.8E-05	5.0E-06	5.68	4/.95/-/1	Added 1 DG	9.1E-02	1				261 917
Farley Units 1&2	1.3E-04	1.22E-05	9.4	4/.95/10/3	Service water to Aac, auto load shedding	4.70E-02	2				
Fort Calhoun	1.36E-05	NA	–	4/.95/-/2	DC load shed	2.17E-01	2				
Ginna	8.74E-05	1.0E-06	1.14	4/.975/-/1		3.50E-03	4				
Harris	7.0E-05	1.71E-05	24.4	4/.95/-/3	Lighting in several areas, ladder to isolation valve						
Indian Point Unit 2	3.13E-05	4.47E-06	14.3	8/.95/60/2	Added a DG for gas turbine auxiliaries	6.91E-02	2		3	390	

Table B-1 : Plant-specific SBO information [83]