Annals of Nuclear Energy 79 (2015) 68–77

Contents lists available at ScienceDirect

Annals of Nuclear Energy

journal homepage: www.elsevier.com/locate/anucene

Technical note

Including severe accidents in the design basis of nuclear power plants: An organizational factors perspective after the Fukushima accident

M.A.B. Alvarenga [a], P.F. Frutuoso e Melo [b,*]

[a] National Commission of Nuclear Energy, Rua General Severiano, 90, 22294-900 Rio de Janeiro, RJ, Brazil
[b] Graduate Program of Nuclear Engineering, COPPE, Federal University of Rio de Janeiro, Av. Horácio Macedo 2030, Sala G-206, 21941-914 Rio de Janeiro, RJ, Brazil

ARTICLE INFO

Article history:
Received 5 August 2014
Accepted 15 January 2015
Available online 7 February 2015

Keywords:
Severe accidents
Fukushima
Organizational factors
Design basis

ABSTRACT

The Fukushima accident was clearly an accident made by humans and not caused by natural phenomena as was initially thought. Vulnerabilities were known by both regulators and operator but they postponed measures. The emergency plan was not effective in protecting the public, because the involved parties were not sufficiently prepared to make the right decisions. The shortcomings and faults mentioned above resulted from the lack of independence and transparency of the regulatory body. Even laws and regulations, and technical standards, have not been upgraded to international standards. Regulators have not defined requirements and left for the operator to decide what would be more appropriate. In this aspect, there was clearly a lack of independence between these bodies and operator's lobby power. The above situation raised the question of urgent updating of institutions, in particular those responsible for nuclear safety. The above evidences show that several nuclear safety principles were not followed. This paper intends to highlight some existing safety criteria that were developed from the operational experience of the severe accidents that occurred at TMI and Chernobyl that should be incorporated in the design of new nuclear power plants and to provide appropriate design changes (backfittings) for reactors that belong to the previous generation prior to the occurrence of these accidents, through the study of design vulnerabilities. Furthermore, the main criteria that define an effective regulatory agency are also discussed. Although these criteria appear in IAEA guides and requirements, this paper proposes that some of these requirements should be more detailed in line with what has been learned as the most important lessons of Fukushima in order to prevent organizational failures.

1. Introduction

The three major accidents in the nuclear industry were TMI, Chernobyl and Fukushima. Regardless of the reactor design type (PWR, RBMK or BWR), these accidents have in common a partial reactor core melt. In fact, severe accidents are defined as accidents in which there is partial or total melt of nuclear fuel in the reactor core. After the TMI accident in the US (1979), it has been recognized that the occurrence of multiple faults in nuclear power plants that go beyond the concept of single failure applied to the design basis is possible (IAEA, 2000b). The combination of latent and active failures from operation and maintenance teams can lead to an accident sequence of low frequency but with high probability of leading to core meltdown. Classic examples of these sequences are: total loss of external and internal power, transients without reactor control rods drop and loss of coolant accident with violation of containment integrity. Examples of latent failures that undermine the plant safety level are failures in design, maintenance, management, training, etc. (Reason, 1990, 1997). Among these, design failures can be avoided if there is a study of plant vulnerabilities. It is necessary to identify design vulnerabilities in order to specify design changes for the prevention and mitigation of severe accidents (IAEA, 2003a, 2008, 2009b; Alvarenga and Rabello, 2011).

However, to make this happen (vulnerability studies and design changes) it is necessary to have a well-established safety culture that acts through government and private organizations (including regulatory bodies) coupled with a strong political will in this direction. Since there are well-established safety criteria for severe accidents in standards of IAEA member states, then it becomes necessary that guides and IAEA requirements be sufficiently detailed so that they can generate a consensus among nations with

* Corresponding author. Tel.: +55 21 3938 8432; fax: +55 21 3938 8444.
E-mail addresses: bayout@cnen.gov.br (M.A.B. Alvarenga), frutuoso@nuclear.ufrj.br (P.F. Frutuoso e Melo).

http://dx.doi.org/10.1016/j.anucene.2015.01.016
0306-4549/

List of acronyms

ACRS	Advisory Committee on Reactor Safeguards
ASLB	Atomic Safety and Licensing Board
BWR	boiling water reactor
CFR	Code of Federal Regulations
CNEN	Comissão Nacional de Energia Nuclear (National Commission of Nuclear Energy, Brazil)
EDO	Executive Director for Operations
EPZ	Emergency Planning Zone
ETE	evacuation time estimate
IAEA	International Atomic Energy Agency
INEEL	Idaho National Engineering and Environmental Laboratory
INSAG	International Nuclear Safety Advisory Group
IPE	Individual Plant Examination
IPEEE	Individual Plant Examination of External Events
IRSN	L'Institut de Radioprotection et de Sûreté Nucléaire (Radioprotection and Nuclear Safety Institute, France)
JNESO	Japan Nuclear Energy Safety Organization
NDJ	The National Diet of Japan
NEPA	National Environmental Policy Act
NRC	Nuclear Regulatory Commission
PAZ	Precautionary Action Zone
PL	Public Law
PSA	Probabilistic Safety Assessment
PWR	pressurized water reactor
RBMK	Reaktor Bolshoy Mochchnosty Kanalnye (high-power channel reactor)
SAMA	Severe Accident Mitigation Alternatives
SAMDA	Severe Accident Mitigation Design Alternative
SIP	shelter in place
TMI	Three Mile Island
UPZ	Urgent Protective Action Planning Zone
USGPO	United States Government Printing Office
WENRA	Western European Nuclear Regulators Association

regard to preventive and mitigative characteristics in the design of nuclear power plants in case of severe accidents, both for new and operating plants. It is worth mentioning here that the Convention on Nuclear Safety (NRC, 2010b), of which member states are signatories, endorses the principle of priority to nuclear safety and the use of updated technical standards.

However, the Fukushima accident was clearly a man-made accident and not caused by natural phenomena as the media initially released. The report of the accident investigation commission of the Japanese Parliament (NDJ, 2012) clearly states that the accident root causes were organizational and regulatory structures that sustained faulty decisions and not any issues related to the competency of any specific individual.

The above evidences show that several nuclear safety principles adopted in fundamental safety principles (IAEA, 2006) were not followed.

Since these principles have not been met in the Fukushima accident, this paper intends to highlight some existing safety criteria that were developed from the operational experience of the severe accidents that occurred at TMI and Chernobyl that should be incorporated in the design of new nuclear power plants, and to provide appropriate design changes (backfittings) for reactors that belong to the previous generation prior to the occurrence of these accidents, through the study of design vulnerabilities. Furthermore, the main criteria that define an effective regulatory agency are also discussed. Although these criteria appear in IAEA guidelines and requirements, this paper suggests that some of these requirements should be more detailed or rewritten in line with what has been learned as the most important lessons of Fukushima.

Why organizational factors were more responsible for this accident than actually technical issues? The answer to this question will be provided throughout the discussions of the next items.

This paper is organized as follows. Section 2 addresses the identification and resolution of vulnerabilities. Design criteria for the containment are the subject of Section 3. Emergency planning is focused in Section 4, while Section 5 is dedicated to the IAEA severe accident policy and also presents a discussion of the state-of-the-art in different countries, like Korea, China, and Brazil. The issue of the independence of regulatory bodies is the subject of Section 6. Conclusions of this work are presented in Section 7.

2. Identification and resolution of vulnerabilities

The Fukushima investigative committee soon discovered that safety systems such as electric power systems were not designed to withstand earthquake effects, did not meet the principles of redundancy and diversity, and systems such as vent systems may not have withstood the effects of high loads generated in the course of station blackout. Moreover, besides the earthquake loads, it may have happened the contribution of loads generated by a likely small-break loss of coolant accident that possibly occurred in Unit I. The instructions manual for severe accidents and associated training were not updated and some diagrams were lacking. These vulnerabilities were known by both regulator and operator but measures have been postponed (NDJ, 2012). This violates Safety Principle # 8 (prevention of accidents), which states that all practical efforts must be made to prevent and mitigate nuclear or radiation accidents (IAEA, 2006). This clearly shows the relevance of the defense in depth philosophy approached by many regulatory bodies for preventing and mitigating the consequences of accidents (NDJ, 2012).

This principle gives emphasis to the principle of defense in depth. The requirements of IAEA (2000b), now superseded by IAEA (2012), clearly defined that the fourth level of defense in depth was necessary to ensure that severe accidents were included in the design of nuclear power plants. The objective of this fourth level of defense is the protection of the containment function. This may be achieved by additional measures and procedures to prevent accident progression and by mitigation of the consequences of selected severe accidents, in addition to accident management procedures. The protection provided by the containment function may be demonstrated by means of best estimate methods. (D'Auria et al., 2012).

However, in the requirements of the new standard (IAEA, 2012), this is not directly related to severe accidents but instead it mentions only that the purpose of the fourth level is to mitigate the consequences of failures of the third level. This new version of the text weakens the fact that severe accidents were necessarily part of new designs or backfittings of old ones:

In the third level of defense of IAEA (2012), it is assumed that the escalation of certain anticipated operational occurrences or postulated initiating events might not be controlled at a preceding