Scientific
Research
Publishing

The Fukushima Nuclear Accident: Insights on the Safety Aspects

Zieli Dutra Thomé[1], Rogério dos Santos Gomes[2], Fernando Carvalho da Silva[3], Sergio de Oliveira Vellozo[1]

[1]Department of Nuclear Engineering, Military Institute of Engineering, Rio de Janeiro, Brazil
[2]Directorate of Radiation Protection and Nuclear Safety, Brazilian National Commission for Nuclear Energy, Rio de Janeiro, Brazil
[3]Department of Nuclear Engineering, COPPE/UFRJ, Rio de Janeiro, Brazil
Email: zielithome@gmail.com, rogeriog@cnen.gov.br, fernando@con.ufrj.br, vellozo@cbpf.br

Abstract

The Fukushima nuclear accident has generated doubts and questions which need to be properly understood and addressed. This scientific attitude became necessary to allow the use of the nuclear technology for electricity generation around the world. The nuclear stakeholders are working to obtain these technical answers for the Fukushima questions. We believe that, such challenges will be, certainly, implemented in the next reactor generation, following the technological evolution. The purpose of this work is to perform a critical analysis of the Fukushima nuclear accident, focusing at the common cause failures produced by tsunami, as well as an analysis of the main redundant systems. This work also assesses the mitigative procedures and the subsequent consequences of such actions, which gave results below expectations to avoid the progression of the accident, discussing the concept of sharing of structures, systems and components at multi-unit nuclear power plants, and its eventual inappropriate use in safety-related devices which can compromise the nuclear safety, as well as its consequent impact on the Fukushima accident scenario. The lessons from Fukushima must be better learned, aiming the development of new procedures and new safety systems. Thus, the nuclear technology could reach a higher evolution level in its safety requirements. This knowledge will establish a conceptual milestone in the safety system design, becoming necessary the review of the current acceptance criteria of safety-related systems.

Keywords

Fukushima Nuclear Accident, Nuclear Safety, Safety Culture

1. Introduction

In the past, TMI and Chernobyl nuclear reactor accidents were a source of operational experiences in accident conditions, pointing out new directions for all stakeholders, bringing improvements to existing power plants. The recent accident at the Fukushima-Daiichi Nuclear Power Plant, as expected, has generated reflections about the safety of nuclear power plants operation. Thus an improvement of safety systems and operating procedures becomes necessary, representing a technological challenge for the existing reactors and for next generation of nuclear power plants as well.

The Fukushima nuclear accident has produced doubts and questions which need to be properly understood and addressed, in order to enable the continued use of nuclear power technology. Such lessons, which will come from Fukushima, will establish a conceptual milestone in the safety system design, becoming urgent the review and revaluation of the adequacy of the current acceptance criteria of safety-related systems at multi-unit stations, mainly those criteria concerning to sharing of structures, systems and components (SSC).

The accident was characterized by a progressive damage due to the loss of core cooling capability, which caused the core melting. The accident progression was characterized successively by: a) Loss of off-site power supply due to the earthquake; b) Loss of on-site power supply caused by flooding due to uncommon tsunami, producing a station blackout (SBO); c) Loss of functionality of residual heat removal systems; d) Heating reactor core and its subsequent melting; e) Generation of hydrogen due to the cladding oxidation at high temperatures and posterior hydrogen detonation, damaging the reactor buildings [1].

Several mitigation actions produced unsatisfactory results, which led to the drastic worsening of the accident, due to the existence of sharing of structures, systems and components, present in the designs of the Fukushima reactors. It is worth mentioning that this is a rather common practice in several nuclear power stations.

This paper is organized as follow: Section 2 presents the accident description, Section 3 discusses the safety culture conception, in Section 4, we discuss the design basis for flooding, Section 5 performs an approach to improve the reliability of the safety systems, in Section 6, we point out that plant-specific training is an essential safety requirement , in Sections 7 and 8, we also point out the challenge of the venting system design, Sections 9 and 10 present the concept of structures, systems and components sharing at Nuclear Power Plants (NPP) and its impact in the Fukushima accident, Section 11 presents the hydrogen explosion problem and in Section 12 we summarize some lessons learned from Fukushima accident.

2. A Brief Description about the Fukushima Nuclear Accident

On March 11, 2011 a severe earthquake occurred off the northeastern coast of Japan with the epicenter about 180 km away from the Fukushima Daiichi NPP, generating a tsunami which caused devastating damage over the whole nuclear site, composed by six BWR nuclear reactors. The electric output of these nuclear reactors are of 460 MW for Unit I, 784 MW for Units 2, 3, 4 and 5, and 1100 MW for Unit 6. The reactors 1, 2 and 3 were in operation at rated power output before the event, while the reactors 4, 5 and 6 had been in an outage.

Looking for the set of effects coming from the earthquake impact, one can conclude that the automatism of the power plants have worked quite well, scramming all operating NPPs promptly. It should be noted that was mentioned that, however, there was the occurrence possibility of a small-scale loss of coolant accident at the Unit 1 [2]. This possibility is being examined further by the Japanese Government. Considering that the external electric power sources have been lost, the emergency diesel generators automatically started, supplying power to the residual heat removal, before the tsunami arrival.

The tsunami impact, however, caused deep operational and structural damages, becoming inoperative the diesel generators and batteries. Without AC or DC power to the energy supply to the operation of decay heat removal systems, the fuel of nuclear reactors 1, 2 and 3 suffered total and partial melting respectively.

A large amount of hydrogen was released, in consequence of the reaction between zirconium and high temperature steam water, producing strong explosions, damaging the buildings of the Units 1, 3 and 4. It should be noted that the Unit 4 was shutdown and had been in a refueling outage. All of the nuclear fuel had been removed from the reactor and placed in the spent fuel pool. Because of hydrogen explosion at Unit 4, it was initially supposed that the spent fuel was uncovered, and therefore, producing hydrogen by oxidation. Despite this previous hypothesis, subsequent assessments conclude that the spent fuel stored at the pool was not damaged by the accident.

In November 2011, the Xenon-135 detection at the Unit 2 opened doubts about the evidence of nuclear recrit-

icality, however, was concluded that the spontaneous fission process of actinides, from the damaged fuel, was the unique responsible for the xenon production [3].

3. Nuclear Safety Culture

The International Nuclear Safety Advisory Group (INSAG) in its report about the Chernobyl accident assessment coined the term *safety culture* to refer to the safety regime that should prevail at a nuclear plant operation, which was introduced globally to explain how the lack of knowledge and understanding of risk and safety by the employees and organization contributed to the Chernobyl disaster [4].

Later, INSAG, under the auspices of the International Atomic Energy Agency (IAEA), enlarged the safety culture concept, considering that the development of a safety culture must be embedded in the national legislative and regulatory framework, establishing the proper chain of responsibility and authority for the required level of safety. In both operating and regulatory regimes, safety culture must be instilled in organizations through proper attitudes and practices of management [5].

A review of nuclear incidents indicates that safety culture problems affect both highly developed and developing countries [6]. Safety culture issues can arise at all stages of organizational life, and even in organizations previously recognized for their safety performance. Currently the majority of effort to improve safety culture has focused on nuclear power plants.

Looking the Fukushima accident, it seems evidenced the need of improvements in the Japanese safety culture, taking into account the lessons learned from Three Mile Island and Chernobyl accident, as well as the tools development aiming to monitor its adequate implementation. So, must be highly recommended to perform international audits programs (peer reviews) covering both operational and regulatory regimes, aiming to strengthen and enhance the effectiveness of the safety culture taking into account the IAEA safety standards and the good international practices.

4. Barrier Protection against Tsunami

Hydrological phenomena, such as flooding due to tsunamis, can cause several hazards that could affect the safety of nuclear power plants, leading to the risk of common cause failure for essentials safety systems, such as the emergency power supply systems or the electric switchyard, with the associated possibility of loss of off-site power, the decay heat removal system and other vital systems [7] [8].

IAEA presents that a conservative analysis of the tsunamis effects should be made for inclusion in the Nuclear Power Plants (NPP) design basis, taking into account the estimation of probable maximum tsunami (PMT), aiming to protect NPPs against all potential effects of external events, determined by using historical data and geological, tectonic and seismic investigations [7].

The licensing design basis for flooding generated by tsunamis of Fukushima Daiichi was initially estimated based on the effects at Japan of the tsunami generated by the magnitude 9.5 Chile earthquake in 1960. Thus, it was defined one PMT producing waves with up to 3.1 meters over mean sea level [9].

Later, new methodology to estimate tsunamis were developed by the Japan Society of Civil Engineers, in 2002, based on observations from Shioyazaky-oki earthquake (magnitude 7.9) in 1938, which resulted in a maximum water level of 5.7 meters [9] [10]. This value was not reviewed or validated by the Japanese Nuclear Regulatory Body (NISA). This assessment was undertaken by plant's operator (TEPCO) voluntarily without any instruction from NISA, and therefore, not officially recognized in the licensing documents [9].

This estimative corresponds to the tsunami height at the shoreline point in the entrance to intake structures level. The run up i.e. the water height reached at the maximum inundation point was not indicated in any presentation from TEPCO. It seems also that the calculation of the run up have not considered the specific and detailed arrangements of plant layout [9].

In the beginning of this century, geological evidences allowed to know the occurrence of the Jogan earthquake in 869 AD, with an estimated magnitude of 8.6. This earthquake caused a giant tsunami in the region of Sendai, in the province of Fukushima. According to estimates arising from the geological sediment analysis, the tsunami waves of 869 AD, similarly to the tsunami of 2011, penetrating up to 4 km from the coast, causing a great flood [11], however, the design-basis flood were not updated to take into account this new historical data.

It must be emphasized that was presents that, since 2006, NISA and TEPCO as well were aware of the possibility of a SBO at the Fukushima site if the nuclear site was reached by a tsunami and that NISA knew that

TEPCO had not prepared any measures to lessen or eliminate the risk, and failed to provide specific instructions to remedy the situation [2].

It is practically consensus that the Japanese nuclear regulatory body and the plant operator did not follow international best practices and standards concerning defenses against extreme external events. Thus, the resistance of Fukushima-Daiichi NPP to tsunamis was underestimated [2] [11].

It must noted that during the assessment for life extension of Unit I, NISA has not imposed, as requirement, the update of flood studies related to the protection of tsunamis, with the inclusion of the Jogan earthquake at its design basis.

During a meeting in London, on July 2011, the Vice-Chairman of the Japan Atomic Energy Commission noted that in recent years several warnings had been issued by the Japanese academic community about the vulnerability of nuclear power plants for the earthquakes and tsunamis occurrences. He also noted that, in 2009, some members of NISA have questioned the non-inclusion of the Jogan earthquake in studies to the design basis updating of Japanese nuclear power plants [12].

5. Diversity and Redundant Safety Systems

Among several definitions, redundancy is a common approach to improve the reliability and availability of a system, thus enabling that safety systems adequately work, even if an individual item fail to perform on demand. It should be noted that the use of redundancy increases the cost and complexity of a system design, however, it is possible to postulate an event that could produce a common cause failure (CCF) inducing failures in two or more channels of a redundant system, which can lead to its inability to function as designed.

The proper application of the concept of diversity is the way to protect redundant systems against CCF. The diversity includes the differences between the system components, considering design, manufacturers, installation, software, operation and maintenance procedures and the differences in their environment and location, in order to prevent the lost of their redundant functions [13].

The off-site power was lost when the earthquake occurred and the emergency diesel generators started up throughout the power station, as expected, however, the on-site power supply redundant systems (emergency diesel generators and batteries) were lost due to flooding caused by tsunami. Due to the lost of DC power, the instrumentation became unavailable to determine the main operational parameters of all reactors or to remotely actuate valves powered by DC power, except Unit 3 [1].

Concerning the location diversity for redundancies, is consensual that the installation of diesel generators and batteries at different levels at the Fukushima nuclear site, could reduce the vulnerability of this system to flooding, ensuring the survival of power generation system and, consequently, making feasible the operation of residual heat removal system.

It must be noted that was priority the power supply recovery, connecting batteries in series to the terminals of the control panels, in order to open valves and restore the measuring instruments, but there were no batteries stored at the Fukushima Daiichi site. However, this was improvised through the removal of batteries of the private cars of employees and TEPCO's service vehicles [14].

Concerning the design diversity for redundancies, Fukushima Daiichi NPP had nine water cooled and three air cooled diesel generators. At this point, it is important to note that the sea water pumps, used to provide cooling to the diesel generators, were installed four meters above sea level, becoming, therefore, inoperative due to the flooding.

It should be noted that some air cooled diesel generators (DG) in the Fukushima Daiichi NPP were not damaged by the tsunami, because they have been installed on an upper floor, however, their metal-clad switchgears were flooded because was installed on the lower floor, not permitting the use of these DGs.

As one of the key lessons was that, in case of CCF, equipment reserves and essential resources, such as batteries, small generators and air compressors, should be available, in real time, to safety systems operation. If these components were readily available, the Fukushima accident could have been effectively mitigated. So, the possibility for replacing such equipments should be incorporated to the redundant system.

It seems to indicate that should be recommended the immediate availability of DC power supply, through independent batteries bank placed near the control room, allowing the opening and closing of valves of essential safety systems, such as venting and safety relief valves. An independent batteries bank should power supply to others equipments of instrumentation and control.

Additionally, should be important the installation of small diesel generators in order to recharge this battery bank, extending the battery lifetime. It must be noted that the absence of electrical power supply triggered a series of human failures (including decision-making) and equipments failures that have proven unreliable when activated. It must emphasized that the equipments qualification in aggressive environments is an essential pre-requisite for the nuclear reactors design, concerning of the instrumentation and control, which would provide greater support for decision-making during the management of severe accidents.

The concept of redundant systems of nuclear power plants should be revised and expanded to incorporate the new lessons learned from this accident. New safety system technologies are under study. It is important that an international effort, by different manufacturers, be encouraged in order to use passive and active redundancies to the next generations of reactors under licensing [15].

6. Training

Nuclear safety is also closely linked with the technical and operational staff capacity and its ability to convert these experiences into operational procedures. For a proper severe accidents management, it is necessary that the personnel involved in performing the various actions during the accident conditions be adequately prepared to take effective on-site actions to prevent or to mitigate the consequences of such accident.

It is necessary that these personnel be acquainted with expected nuclear plant behavior beyond of design basis conditions, and their consequences as well. In this way, the computational simulator is an important tool for the operational training. One must be emphasized, however, that the time decision-making is closely related to familiarity with the operational characteristic of each system.

On the other hand, the management decisions are considered critical in the sense that the implementation of a decision can also include adverse effects. In such case, the potential negative consequences have to be properly assessed before an action is performed.

The Investigation Committee on the Accident at Fukushima (hereinafter referred to as the "Investigation Committee") quoted that the shift staff had not realized that all isolation condenser system (IC) valves were designed to be closed by the failsafe function when all power supplies were lost. According this reference, the shift team could not identify the operating status of the IC immediately after the tsunami [14].

Before the earthquake, no one in the shift staff, in charge of Unit 1, had knowledge about the operation characteristics of the IC, ignoring that a visual inspection of steam blow-out (and operating noise) could point out the operational status of IC [14].

As mentioned before, it becomes clear that the weak familiarity of operators with rapport the main characteristics of safety systems in emergency scenarios, inducing evaluation errors and mistaken making-decision. For example, it was inhibited the water injection in the reactor core (Unit 1) during the early moments after the tsunami, causing its melting in an unexpected short time due the mistakes about the operational status of IC.

It should be noted, that the plant-specific training is an essential requirement, since it allows a deeper knowledge of main safety subsystems behavior. This accident showed the need for a continuous and effective plant-specific training in preventive and mitigative actions on simulators, which should take into account the identification and assessment of severe accident scenarios and its progression as well. One must be emphasized, therefore, that the time decision-making is closely related to familiarity with the characteristic of each system.

7. Vent System Failures

The free volume of the BWR Mark I containment is quite small relative to the other containment types. Therefore, during an accident, the containment can be overpressurized in a relatively short period of time unless steps are taken to mitigate the pressure rise [16].

Under severe accident conditions, such as core meltdown, the pressure of the containment must be released to the atmosphere to maintain the containment integrity. However, although the venting decreases the pressure in the containment, its implementation releases radioactive material into the environment.

One of the most comprehensive studies of containment venting was performed on the Peach Bottom Atomic Power Station, a BWR with a Mark I containment. A main conclusion from that study was that the containment venting had limited potential for reducing the risk associated with the dominant severe accident sequences [17].

In 1989, the United States Nuclear Regulatory Commission (USNRC) recommended, to reduce the vulnerability of BWR Mark I containments in case of severe accidents, by the installation of a hardened wetwell vent,

improving the venting capability [18]. In general, USNRC proposed a vent modification through the installation of a direct vent path from the torus to the main stack (Direct Torus Venting System—DTVS) by-passing the SGTS.

Following the USNRC recommendation basic design, each individual plant owner designed and installed the hardened vent to meet its best plant-specific design criteria. Operators in Japan, including TEPCO, did the same [19], but there is insufficient information to know the venting system installed at Fukushima.

In the basic design, the DTVS must be isolated from the SGTS by installation of air-operated valves and a rupture disk. It should be noted that the valves of this system are normally closed and in case of loss of electrical and pneumatic power they are automatically closed. Additional filters were not considered by USNRC, because was concluded that the scrubbing at suppression pool, during the venting, was effective on reducing the source term released to the environment.

As the SBO consequence, the venting line was manually configured, through of the manual opening of vent valves, into reactor building, which required the installation of a DC power supplier and portable air compressor. It was mentioned that this manual opening is complicated due to the high radiation level that would be present following the reactor vessel failure, not allowing the access to these valves [16]. It should be noted that the venting implementation at Fukushima was interrupted sometimes by the high levels of radiation inside the reactor building [14].

As observed in Fukushima accident, the venting action did not work properly: i) In Unit 1, the venting operation produced a hydrogen explosion in the containment building; ii) In Unit 2, the recovery staff was not able to configure the venting line, thus the core depressurization, through safety relief valves (SRV), was performed, damaging the primary containment by over-pressure. The most probable over-pressure failure location in Mark I containments is the upper half of the pressure suppression pool torus. Let us comment that, on March, 15 was heard a strong sound coming from Unit 2, and its suppression pressure equalizing with atmospheric pressure, so, indicating a suppression pool rupture as expected [20]; iii) In Unit 3, the venting operation produced hydrogen explosions in the Units 3 and 4 due to backflow into the Unit 4 through the SGTS piping, since the exhaust pipe of unit 3 and 4 sharing the same main stack [21].

After the venting beginning at units 1 and 3, a strong hydrogen explosion occurred on the roof of these reactor buildings. The hydrogen transport and its accumulation in the roof are not clear, as well. One possibility was that had a leakage of hydrogen through drywell head, due to the containment pressure, exceeding its design basis. However, another possibility would be the gas migration into the reactor building through the SGTS, during the depressurization. It should be noted that with SBO occurrence, the valves of SGTS should be automatically closed.

The Investigation Committee related that the operation performed, by the recovery staff to the venting configuration, was through of the manual opening of a motor-operated valve near the stack and the opening of two air-operated valves (a larger and a smaller one) in parallel pipes [14]. As recommended by USNRC, the DTVS design provides a direct vent path from the torus to the stack bypassing the SGTS through parallel pipes [18].

According to before mentioned, we are supposing that the simultaneous opening of the parallel air-operated valves allowed the venting through two paths, via DTVS and via SGTS. The ventilation pipes and filters of SGTS were not designed to withstand large internal pressures, so these pipes would likely fail after the vent valves were opened, allowing radioactive steam, fission products and hydrogen to escape into the reactor building, with the hydrogen accumulating at the roof and likely producing an explosion [16].

Investigating the hydrogen explosion occurred in Unit4, TEPCO concludes that the containment venting from unit 3 flowed into the Unit 4 through the SGTS pipes, since the exhaust pipes of unit 4 joins the Unit 3 exhaust pipes at the main stack. It must be emphasized, however, that the Unit 4 was in outage at the moment of earthquake [21].

It is unclear why the isolation valves in the SGTS at the Unit 4 was opened, allowing the gas backflow into the reactor building and the subsequent hydrogen explosion, since this valves should be automatically closed due to loss of electric power, ruling out the hydrogen migration possibility from Unit 3 to Unit 4. Probably, this fact would point to a possible failure in the design of the DTVS installed in Fukushima or a mistake on the manual alignment of the vent valves, with the opening of SGTS valves.

8. Filtered Venting

As before mentioned, under severe nuclear accident conditions, the SGTS do not have operational capability to

perform gas filtering during the venting [16]. So, when the venting was performed through suppression pool (torus), the pool scrubbing was the only filtration mechanism. It should be noted that there are another venting path, where the gases in the containment vessel are directly released to the main stack, bypassing the beneficial effects of scrubbing through the water in the torus. Therefore, the first path is preferable due to minimization of radioactive releases [14].

It was mention that the installation of a filtered vented containment system to an existing nuclear power plant has been suggested as one approach to mitigating the effects of a severe accident, since reduces considerably the radioactive releases to environment during venting operation [21].

Several manufacturers had presented filtered venting systems designs as an update to NPP safety system. It must be emphasized that filtered venting should have, among their main requirements, the operation without electric power, monitoring of adequate performance parameters in the control room to provide status of system during operation, as well avoid potential hydrogen detonation system is initiated following a severe accident [21].

Additionally, it was commented that the Japanese were interested in install, in the 90´s, filtered venting systems for their nuclear plants, but its implementation was not done [22]. OCDE shown the filtered venting systems description selected for implementation in Germany, France and Sweden [23].

The high cost/benefit has discouraged the filtered venting system installation during the last thirty years, for almost all NPPs. However, looking for the consequences of Fukushima, we believe that the mandatory implementation of filtered venting will become, probably, a tendency by the main international nuclear regulatory bodies. The desired characteristics for the filtered venting system should be studied in depth by each regulatory body and widely discussed internationally, in order to produce a consensus in the nuclear sector.

9. Structures, Systems and Components Shared at Nuclear Power Plants

The SSC sharing aims, mainly, to reduce the construction, operation and maintenance costs. This procedure is widely used by the nuclear industry and other technologies. The SSC sharing between units at nuclear power plants translates into a reduction of overall construction time and in the respective costs for equipment, materials, and structures [24].

The reduction of these costs may have implications for sensitive items related to nuclear safety, involving risks which must be quantified. Regardless of the material benefits, safety cannot be, however, compromised, that is, the SSC sharing cannot impair the ability of the systems to perform their safety functions. Thus, an important objective of sharing systems is to reduce cost without disturbing the nuclear safety integrity.

Due to safety, operability, and license ability reasons, the choice of SSCs to be shared cannot be exclusively based on economic assessments. So, a probabilistic risk assessment must be performed taking into account the safety impact due to the SSCs sharing and its consequences at multi-units station, compared to results obtained when applied for a unique reactor site.

The existence of sharing increases the likelihood of scenarios that could impact a single unit independently, and creates a potential for scenarios that may involve several units at the site, as observed at Fukushima.

According to Oak Ridge National Laboratory, there are three different sharing strategies. The first one is a single SSC that supports both units simultaneously. In the second one there are independent SSCs for each unit. They are interconnected to attend both units. This sharing configuration increases the availability of SSCs [24]. It is important to note that these SSCs should be designed to support the demand when one unit is lost, avoiding the system shutdown due to overload. In the last type there are independent SSCs for each unit, but sharing of standby or spare equipment.

It should be noted that, before Fukushima, the simultaneous occurrence events assumption, at multi-units stations, was not considered. Thus, in this scenario, the availability of standby equipment and resources could be, eventually, not correctly estimated. The USNRC determined that, because of the low probability of a severe reactor accident, a suitable design basis for multi-unit nuclear power plants was the assumption that an accident occurs in only one of the units at a time, with all remaining units proceeding to an orderly shutdown and a maintained cooldown condition [25]. It must be emphasized, however, that such scenario did not happen at Fukushima accident, where several units were impacted simultaneously.

The USNRC had already limited the opportunities for sharing of onsite power systems at multi-unit power plant sites, because the sharing generally results in a reduction in the number and capacity of the onsite power

sources to level below those required for the same number of units located at separate sites [25]. Thus, one must question whether the SSC sharing would weaken the functionality of the redundant installed devices. This could affect the availability and proper use of these shared devices during accident mitigative actions.

As it is well known, redundancy is a common approach to improve the reliability and availability of a system, enabling safety systems performing satisfactorily its functions, even if individual systems fail when demanded. It should be noted that the use of redundant devices increases the cost and complexity of a system design. At this point, we question if the SSC sharing could be considered as in conflict to redundancy concept.

10. Impact Evaluation of the SSC Sharing in the Fukushima Accident

The Fukushima accident produced many issues that need to be answered. This knowledge needs to be incorporated in the new safety systems to be implemented in next reactor generation designs. The current safety design must also be updated to consider the new requirements that are coming from Fukushima. It should be noted that this represents a challenge for all stakeholder, including the nuclear industry and the nuclear regulatory bodies.

As explained previously, before the Fukushima, it was determined that, because of the low probability of a severe reactor accident, a suitable design basis for multi-unit nuclear power plants was the assumption that an accident would occur in only one of the units at a time. It should be noted that, in a technical analysis, events that are relatively improbable cannot be ruled out, creating the risk of not having resources for their mitigation.

During the mitigation of the Fukushima accident, it is possible to observe the influence of sharing SSCs on final outcome of the accident. Thus, in a technically complex scenario some points should be analyzed separately, such as the current SSCs sharing methodology at multi-unit stations.

In subsequent section we aim to evaluate some Fukushima SSCs shared that impacted on the ability of carrying out actions to mitigate the consequences of the nuclear accident.

10.1. Control Room Sharing

There was a main control room shared by adjacent reactors at Fukushima Daiichi NPP; one for Units 1 and 2, one for Units 3 and 4, and another for Units 5 and 6. For each control room there was only one shift supervisor with the responsibility of making decisions during the course of the accident concerning the control and operation of both units, and reporting all basic information necessary to the emergency response organization [14].

For example, there are several multi unit US nuclear power plants where there are two complete control rooms that share the same shift supervisor. In the same way, at United Kingdom the AGR reactors sites have two reactors, sharing control rooms, supervised by the same shift supervisor. Therefore, the structural arrangement designed in Fukushima Daiichi control rooms is not uncommon.

According to the Investigation Committee, communication failures between the shift staff and the on-site Emergency Response Organization (ERO) caused a misunderstanding concerning water injection in the unit 1. The ERO assumed that there was wrong evaluation of IC status. Thus, the ERO believed that the situation in Unit 2 was more dangerous than that in Unit 1. So, efforts were focused by the staff for Unit 2, instead of Unit 1, delaying the decision concerning alternative water injection into Unit 1. As a consequence of the delay in implementing of mitigative actions in Unit 1, the reactor accident at Unit 1 rapidly progressed to total fuel melting, about six hours after the tsunami arrival [14].

The control room sharing by different Units at Fukushima Daiichi impacted the accident mitigation actions. For example, the accident mitigation actions for Unit 2 had priority over the Unit 1, so, impairing the cooling of this reactor that produced a fast melting.

As observed, it must be emphasized that, according the USNRC's acceptance criteria [26], the control room should be considered a structure not subject to sharing. This situation is aggravated when the units shared, have different safety systems, as existent at Fukushima Units 1 and 2.

Due to the accident progression in the Unit 1, high radiation levels were seen inside the main control room, shared between Units 1 and 2. Because of this, it was necessary to avoid certain areas at the main control room [14]. It must be noted that, the staff access and permanency in Unit 2 control room could become prohibitive due to the high radiation levels. Thus, it is evident that the accident in one unit could impair the other unit due to the control room sharing.

It is important to remember that before Fukushima accident, the assumption of simultaneous occurrence of a severe accident at multi-units was not considered. So, the control room sharing, supposedly, would not disturb

the activities of each team individually to perform their operational functions. This was not, however, confirmed effectively.

Concerning previous USNRC sharing recommendation, we understand that it must be revised taking into account the Fukushima accident lessons. This subject must be deeply analyzed due to its operational consequences, concerning human factors engineering and human performance in order to evaluate and to improve the safety, the efficiency and the robustness of these work systems.

10.2. Main Stack Sharing

The Fukushima Units 3 and 4 shared the same main stack which caused undesirable interactions among these units due to physical interconnection between them. Similarly, the Units 1 and 2 shared another main stack.

With the accident progression the containment pressure at Unit 3 reached values above its structural design limits, necessitating venting to the main stack, aimed at gradual depressurization containment [27]. Although the venting reduces the containment pressure, maintaining its integrity, its implementation releases radioactive materials to the environment.

Since the venting pipes of Units 3 and 4 shared the same main stack, the existence of this interconnection (as a consequence of its sharing configuration) made possible hydrogen transport into the Unit 4. The hydrogen accumulated and caused an explosion in Unit 4, damaging its reactor building, despite the Unit being in outage at the moment of the earthquake [21]. It is unclear why the Unit 4 isolation vent valves were opened, in disagreement with its operational logic. Indeed, there was an operational mistake, due to the physical status of the valves (opened), allowing the hydrogen flowing into its reactor building mainly due to pressure difference among the shared venting pipelines.

The existence of an inappropriate main stack sharing in the reactor design allowed that a single failure in the venting valves to damage Unit 4, increasing the accident consequences at the Fukushima Daiichi site. Looking for the economic benefit obtained with the main stack sharing, when faced with the observed damages; it allow us to conclude about the inadequacy of this sharing design. Thus, individual vent pipes, including the main stack, without shared devices, seems to be the best design choice for multi-unit stations.

10.3. Emergency Staff Sharing

According to the IAEA report [28], the emergency staff members are composed of evaluators, decision makers and implementers, each one with their specific responsibilities. Looking for Fukushima, the ERO staff was poorly sized to cover the occurrence of simultaneous events at all units. This inadequacy of technical support staff led to misunderstanding, failures and delays in decision making, mainly as a consequence of personal stress. This situation becomes more severe in the case of the same staff is requested to perform actions at plants with different safety configuration designs, as for example, different water injection systems installed in Units 1 and 2.

Considering the technological differences of the Fukushima nuclear reactors, it is necessary to have unit-specific training for accident conditions, including all possible scenarios. The staff should be familiar with the expected nuclear plant behavior beyond of basis design conditions and the consequences as well. This could be done using simulators for the operational training. It is more evident the need for specific training of the emergency staff for each different technology of the reactors at multi-unit stations.

Emergency staff sharing compromised implementation of actions needed to minimize the consequences of the accident. Failures in accident management occurred in all the damaged Fukushima units. For this reason, it is suggested that there be a dedicated emergency staff for each unit at multi-unit stations, in order to avoid loss of focus in case of emergency.

10.4. Resources for Emergency Actions

In Fukushima, it was observed that there was not essential equipment of resources required for emergency actions, such as batteries, small AC generators and air compressors, which should be available promptly for mitigative actions. The non availability of these resources was based in the very low estimative of one event affecting simultaneously several units at the site.

It was believed that the interconnection among the various systems shared would present a robust redundancy,

thus it would not need the availability of these additional resources. It should be emphasized that accident scenarios, even improbable, cannot be discarded at a probabilistic risk assessment, otherwise they will not have adequate conditions and the resources required for mitigation if the event occurs.

Additionally, according to IAEA report [28], water is a resource that should be available between the elements necessary for severe accident mitigation after the loss of water injection capability, when the core damage became inevitable. So, it is necessary alternative water injection in order to flood the drywell in an attempt to preclude melt through of the reactor vessel [29].

As a result of the rapid accident progression, the molten fuel started to damage the reactor pressure vessel at the Unit 1 five hours after the tsunami arrival [11]. Thus, possible mitigative actions to maintain the fuel in the vessel became impossible.

It should be noted that the only alternative for water injecting at Fukushima were the pumps installed on fire engines. It should be emphasized that there was only one fire engine to attend all damaged power plants of this site, since that one was destroyed by the tsunami and another fire engine remained stopped between units 5 and 6 because of the destruction of the internal roads [14].

The existence of only three fire engines to attend six nuclear power plants at Fukushima can be understood as a resource sharing that proved to be inadequate to act in multi-unit accident scenario. It should be noted that ORNL describes the use of portable pumps provided by fire engines as a possible tool for alternative water injection into the core during mitigation actions, keeping the damaged core inside the reactor vessel and avoiding its subsequent failure and consequently the radioactivity release to the environment. It should be noted that these pumps must have adequate capacity and enough power to proper use as an alternative safety system [29].

The non-availability of these resources, in quantity and adequate capacity, disturbed the making-decision in due time, thus, implying that the performed actions have been compromised.

11. Hydrogen Explosions

It should be emphasized that until the explosion at Unit 1, no one at the Fukushima Daiichi NPP, TEPCO Head Office or the Japanese Government considered the possibility of a hydrogen gas explosion occurring in the reactor building [14]. Thus, not having been considered this possibility of explosion, no possible mitigation action, related to hydrogen concentration, was done, until the explosion in Unit 1. Later, new hydrogen explosion occurred in units 3 and 4, as mentioned before. Thus, failures occurred concerning to the identification of the accident progression sequence, although already available in the literature. It should be noted, however, that mitigation strategies of hydrogen explosions were very limited.

During the progression of the severe accident, the reactor core temperature increases, due to inoperability of the residual heat removal system, resulting on large amounts of hydrogen generation, due to zircaloy cladding oxidation reaction with steam water at high temperatures.

So, it becomes evident that an important scientific challenge for the safety use of nuclear energy (for electricity generation) should be the minimization of hydrogen generation, in the case of the occurrence of severe accidents.

The hydrogen combustion can cause explosions that may damage the containment building. Since hydrogen combustion represents a hazard to the containment integrity, mitigation strategies for hydrogen becomes one of the essential parts of any accident management program. The controlled venting, in an early stage of the accident, is assumed to prevent high hydrogen concentration in the containment [30].

In most countries, there are no strict regulatory requirements on the implementation of hydrogen mitigation strategies for existing plants. However, for the new reactors that are planned or under construction, these considerations must be included into the design [30].

Some solutions have being considered, as the passive autocatalytic recombiners (PAR) for mitigation of hydrogen generated during a severe accident (due to zircaloy oxidation at high temperature). These devices recombine hydrogen with oxygen producing steam and heat. This exothermal reaction may lead to an overheating of the catalyst elements and consequently cause an unintended ignition of the hydrogen/air-mixture. However, research is ongoing to create PARs with reduced probability of hydrogen ignition [31].

Another mitigation strategy is the deliberate ignition system to initiate combustion wherever and whenever flammable mixtures arise, removing the hydrogen by slow deflagration. It should be noted that some works have recommended the use of dual concept, using integrated recombiner-igniter system for the gas control in order to

cover a broader spectrum of accident sequences, and to provide adequate diversity [32] [33].

The search of alternative materials, for replacing the zirconium in the fuel cladding, is in progress. It is a way to prevent (or minimize) the hydrogen production. Although all metals react with steam water at high temperature, the stainless steel would be an option better than Zirconium alloys, regarding the resistance to oxidation. Another option being considered is the use of ceramics materials, such as silicon carbide aiming the hydrogen production minimization [34]. The material eventually chosen must have adequate neutronic properties for use in nuclear reactors.

In Fukushima accident, the implementation of an early venting was not possible because of the loss of electric energy and pneumatic supply. There were no other procedures or available equipment for mitigation strategy. The later completion of the venting, after the manual configuration of its path, produced strong hydrogen explosions in units 1, 3 and 4.

Additionally, it is important that the concentration of hydrogen in the containment must be permanently monitored. Some accident management procedures and making decisions may depend directly of the hydrogen concentration value. There were no gauges to hydrogen concentration measurement at the Fukushima NPP [14].

As already mentioned, the Hydrogen problem must be rethought, remaining as a challenge for the nuclear manufacturers and for the scientific community.

12. Lessons Learned

The SSCs sharing has shown that mitigation actions do not produce the expected results in order to prevent the evolution of the accident, being worsened due to low familiarity of the emergency staff with the safety systems. Thus, it is important that the periodic training program must include beyond basis design scenarios. So, the emergency staff must have full knowledge about the safety-related systems. It is evident that the possibilities of sharing at multi-units site should be carefully reanalyzed, since its applicability becomes more restrictive.

The main events that occurred during the Fukushima accident were considered, indicating the need of improvement of techniques and procedures to mitigate its consequences. So, the lessons learned from this accident are summarized below.

Lesson learned 1—A complex failures scenario occurred at Fukushima, including omissions of nuclear regulatory body, due to lack of compliance with IAEA safety standards and good international practices, allowing an underestimation probability of external events occurrence. Thus, it is highly recommended to perform international technical audits programs, aiming to strengthen and enhance the effectiveness of the safety culture.

Lesson learned 2—The concept of electrical interconnection between all power plants units, like existent at Fukushima, cannot be understood as a robust redundancy system to support common cause failure events, thus a most adequate use of diversity concept is the effective way to protect redundant systems minimizing the undesirable occurrence of SBO. Beyond this, the concept of redundant systems of nuclear power plants should be revised and expanded to incorporate the lessons from this accident. Indeed, this new redundant systems must be most complex, embedded in the concept of defense in depth.

Lesson learned 3—It seems to indicate that should be recommended the immediate availability of DC power supply, through independent battery banks, placed near the control room, allowing the opening and the closing of valves of essential safety systems, such as venting and safety relief valves, and also the power supply to others equipments of instrumentation and control. Additionally, should be important the additional installation of small diesel generators in order to recharge this battery bank, extending its lifetime.

Lesson learned 4—It must be noted that the absence of electrical power supply triggered a series of human failures (including decision-making) and equipments failures that have proven unreliable when activated. It must emphasized that the equipments qualification in aggressive environments is an essential prerequisite for the nuclear reactors design, concerning of the instrumentation and control, which would provide greater support for decision-making during the management of severe accidents.

Lesson learned 5—The severity of the Fukushima accident points to the necessity of an international consensus among all stakeholders, concerning the increase of nuclear safety conditions, thus it should be evident that after the accident in Fukushima, it becomes necessary to define new safety assessment criteria, including acceptance criteria for the use of SSCs sharing, taking into account the possibility of simultaneous accident occurrence at several reactors at multi-unit stations. The use of sharing for costs reduction may impair the nuclear safety. So, the sharing involving risks must be quantified. Regardless of the material benefits, safety must not be

compromised. Due to nuclear safety reasons, the SSCs sharing design must not be exclusively based on economic assessments.

Lesson learned 6—At Fukushima there was a main control room for adjacent units. In this way, in the first moments of the accident, efforts were focused for unit 2 instead the Unit 1, delaying the making-decision concerning to beginning of an alternative water injection into Unit 1. Thus, this work concludes that each control room should be considered a structure not subject to sharing, avoiding the hierarchical competitive relating making-decision among power plants, during the mitigative actions.

Lesson learned 7—It was identified inadequate training for emergency situations, resulting in delay in making-decisions and deterioration of the situation due to loss of time windows to apply the mitigative procedures. So, preventive and mitigative actions training can be performed on simulators, which should take into account the identification and assessment of severe accident scenarios and its progression as well.

Lesson learned 8—It should be noted that the lack of support staff, of resources and of equipments not allowed that the mitigative actions were adequately performed, take into account a simultaneous accident scenario in several Units of Fukushima-Daiichi NPP. As observed in this study, there was a high degree of improvised actions to prevent the progression of the accident, since the AMP documentation did not contained procedures to be followed in accident conditions due to external events.

Lesson learned 9—It must be emphasized that venting actions do not work properly at Fukushima, thus its design must be rethought. However, looking the accident consequences we believe that the mandatory implementation of filtered venting will become a tendency by the main international nuclear regulatory bodies.

Lesson learned 10—The Hydrogen problem must be also rethought, remaining as a challenge for the nuclear manufacturers and for the scientific community. It is in progress the search of alternative materials for replacing the zirconium in the fuel cladding as a way to minimize the hydrogen production. However, some solutions already available, as the autocatalytic recombiners and igniter systems, could be used to hydrogen concentration control in primary containment.

Lesson learned 11—Due to the main stack sharing, the hydrogen migration from unit 3 to 4 caused an explosion, destroying the Unit 4 reactor building, despite being in outage. Regarding this accident, the sharing of venting pipelines, including the main stack, should be avoided at multi-unit stations design.

Lesson learned 12—It should be emphasized that independently of the safety system improvements is essential the evolution on the personnel knowledge to actuate during a severe accident. These efforts should be focused the development of training programs, with massive use of simulators as the important tool for the operational training, in severe accident scenarios.

13. Conclusions

This work performed a critical analysis of the Fukushima nuclear accident, focusing at the common cause failures produced by tsunami, as well as an analysis of the main redundant systems. It also assessed the mitigative procedures implemented during the accident and the subsequent consequences of such actions. Our analysis shows that the accident management gave results below expectations, not avoiding the progression of the accident.

We did show that the inappropriate use of concept of SSC sharing in safety-related devices at multi-unit nuclear power plants had a negative effect on the nuclear safety, contributing to the Fukushima accident scenario.

The NPPs of the world are waiting for the technical answers for the Fukushima lessons. Such challenges will be, certainly, implemented in the next reactor generation, following the technological evolution. The technical audits could be an important mechanism to identify the main procedures to be implemented in each operational NPP and its respective priority.

It is becoming clear that the continuity of the use of nuclear energy depends on the evolution of technologies and procedures improvement that should be incorporated to the emergency systems with appropriate redundancies, ensuring the adequate safety to the public, workers and environment. The efforts to provide such a condition must be of all stakeholders, including international organizations.

Acknowledgements

References

[1]   Institute of Nuclear Power Operations (2011) Special Report on the Nuclear Accident at the Fukushima Daiichi Nuclear Power Station—INPO 011-005. INPO, Atlanta.

[2]   The National Diet of Japan (2012) The Official Report of the Fukushima Nuclear Accident Independent Investigation Commission. The National Diet of Japan, Tokyo.

[3]   Thomé, Z.D., Gomes, R.S., Silva, F.C. and Gomes, J.D.R.L. (2012) An Attempt to Confirm the Origin of ^{135}Xe Detected in the Fukushima Daiichi II Nuclear Power Plant. *Nuclear Engineering and Design*, **247**, 123-127. http://dx.doi.org/10.1016/j.nucengdes.2012.03.015

[4]   International Nuclear Safety Advisory Group (1992) The Chernobyl Accident: Updating of INSAG-1, INSAG 7. IAEA, Vienna.

[5]   International Nuclear Safety Advisory Group (1991) Safety Culture, INSAG 4. IAEA, Vienna.

[6]   International Atomic Energy Agency (2002) Self-Assessment of Safety Culture in Nuclear Installations—Highlights and Good Practices—TECDOC-1321. IAEA, Vienna.

[7]   International Atomic Energy Agency (2003) Flood Hazard for Nuclear Power Plants on Coastal and River Sites—Safety Standard Series NS-G-3.5. IAEA, Vienna.

[8]   International Atomic Energy Agency (2011) Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Installations, Specific Safety Guide SSG-18. IAEA, Vienna.

[9]   International Atomic Energy Agency (2011) International Fact Finding Expert Mission of the Fukushima Dai-ichi NPP Accident Following the Great East Japan Earthquake and Tsunami, Mission Report. IAEA, Vienna.

[10] Japan Society of Civil Engineers (2002) Tsunami Assessment Method for Nuclear Power Plants in Japan. JSCE, Tokyo.

[11] Acton, J.M. and Hibbs, M. (2011) Why the Fukushima was Preventable. Carnegie Endowment for International Peace, Washington DC.

[12] Suzuki, T. (2011) The Fukushima Nuclear Accident: Lessons Learned (So Far) and Possible Implications. *Special Seminar on the Fukushima Dai-ichi Incident*: *Implications for the UK*, *France*, *Japan and the International Community*, London, 6 July 2011.

[13] Preckshot, G.G. (1994) Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems. U.S. Nuclear Regulatory Commission, Washington DC.

[14] Hatamura, Y., Oike, K., *et al.* (2012) Investigation Committee on the Accident at Fukushima Nuclear Power Stations of Tokyo Electric Power Company. http://www.cas.go.jp/jp/seisaku/icanps/eng/final-report.html

[15] Kaufmann, A., Grouchko, D. and Groun, R. (1977) Mathematical Models for the Study of the Reliability of Systems. Academic Press, New York.

[16] Kelly, D.L. (1991) Overview of Containment Venting as an Accident Mitigation Strategy in US Light Water Reactors. *Nuclear Engineering and Design*, **131**, 253-261. http://dx.doi.org/10.1016/0029-5493(91)90283-N

[17] Dallman, R.J. and Galyean, W.J. (1988) Containment Venting as an Accident Management Strategy for BWRs with Mark I Containments. *Nuclear Engineering and Design,* **121**, 421-429. http://dx.doi.org/10.1016/0029-5493(90)90022-P

[18] United States Nuclear Regulatory (1989) Installation of a Hardened Wetwell Vent (Generic Letter 89-16). http://www.nrc.gov/reading-rm/doc-collections/gen-comm/gen-letters/1989/gl89016.html

[19] Davies, L. (2011) Beyond Fukushima: Disasters, Nuclear Energy, and Energy Law. *Brigham Young University Law Review*, **2011**, 1937-1989.

[20] Greene, S.R. (1990) The Role of BWR Secondary Containments in Severe Accident Mitigation: Issues and Insights from Recent Analyses. *Nuclear Engineering and Design,* **120**, 75-86. http://dx.doi.org/10.1016/0029-5493(90)90286-7

[21] Tokyo Electric Power Company (2012) Investigation of the Cause of Hydrogen Explosion at the Unit 4 Reactor Building. http://www.nsr.go.jp/data/000059292.pdf

[22] Schlueter, R.O. and Schmitz, R.P. (1990) Filtered Vented Containments. *Nuclear Engineering and Design*, **120**, 93-103. http://dx.doi.org/10.1016/0029-5493(90)90288-9

[23] Organization for Economic Co-Operation and Development (1988) Filtered Containment Venting Systems. *Note on the Outcome of the May* 1988 *Specialists Meeting on Filtered Containment Venting Systems*, Paris, 17-18 May 1988.

[24] Muhleim, M.D. and Wood, R.T. (2007) Design Strategies and Evaluation for Sharing Systems at Multi-Unit Plants, ORNL/LTR/INERI-BRAZIL/06-01. Oak Ridge National Laboratory, Oak Ridge.

[25] US Nuclear Regulatory Commission (1975) Shared Emergency and Shutdown Electric System for Multi-Unit Nuclear

Power Plants, Regulatory Guide 1.81. U.S. Nuclear Regulatory Commission, Washington DC.

[26] US Nuclear Regulatory Commission (2003) Control Room Habitability at Light-Water Nuclear Power Reactors, Regulatory Guide 1.196. U.S. Nuclear Regulatory Commission, Washington DC.

[27] Hirano, M., *et al.* (2012) Insights from Review and Analysis of the Fukushima Dai-Ichi Accident. *Journal of Nuclear Science and Technology*, **49**, 1-17.

[28] International Atomic Energy Agency (2009) Severe Accident Management Programmes for Nuclear Power Plants, IAEA Safety Guide NS-G-2.15. IAEA, Vienna.

[29] Cook, D.H., Greene, S.R., Harrington, R.M., Hodge, S.A. and Yue, D.D. (1981) Station Blackout at Browns Ferry Unit One—Accident Sequence Analysis, NUREG/CR-2182. Oak Ridge National Laboratory, Oak Ridge.

[30] International Atomic Energy Agency (2011) Mitigation of Hydrogen Hazards in Severe Accidents in Nuclear Power Plants, IAEA-TECDOC-1661. IAEA, Vienna.

[31] Reineck, E., Tragsdorf, I.M. and Gierling, K. (2004) Studies on Innovative Hydrogen Recombiners as Safety Devices in the Containments of Light Water Reactors. *Nuclear Engineering and Design*, **230**, 49-59.
http://dx.doi.org/10.1016/j.nucengdes.2003.10.009

[32] Heck, R., Kelber, G., Schmidt, K. and Zimmer, H.J. (1995) Hydrogen Reduction Following Severe Accidents Using the Dual Recombiner-Igniter Concept. *Nuclear Engineering and Design*, **157**, 311-319.
http://dx.doi.org/10.1016/0029-5493(95)01009-7

[33] Bröckerhoff, P., von Lensa, W. and Reinecke, E. (2000) Innovative Devices for Hydrogen Removal. *Nuclear Engineering and Design*, **196**, 307-314. http://dx.doi.org/10.1016/S0029-5493(99)00310-6

[34] Electric Power Research Institute (2011) Silicon Carbide Provides Opportunity to Enhance Nuclear Fuel Safety.
http://mydocs.epri.com/docs/CorporateDocuments/Newsletters/NUC/2011-09/09d.html