

On the Accident at Fukushima Daiichi Nuclear Power Plant from the Inherent Safety Points of View

Kazutoshi Hasegawa

National Research Institute of Fire and Disaster, Japan
hase-k@jcom.home.ne.jp

The Fukushima Daiichi Nuclear Power Plant, resulting from a massive earthquake, had the worst accident. Its causes are studied from safety culture and the inherent safety points of view. The matters that these fundamentals had not been embodied in the nuclear plants are as follows: priority of safety, seismic strengthening works, redundancy and diversity of subsystems, asymmetry failure mode; simplification and limitation of baneful effects on reactor cooling system, simplification of reactor building, attenuation and avoiding knock-on effect by miniaturizing reactor, tolerance toward leakage or melt-down at reactor pressure vessel, tolerance toward hydrogen gas generation, limitation of gas explosion effects, simplification of emergency countermeasures, and making status clear in emergencies. Therefore, the accident was triggered by the earthquake, but the escalation into an extremely significant accident was directly caused by a lack of safety principle and inherent safety designs. It must be more man-made than natural disaster.

1. Introduction

A massive earthquake with a magnitude of 9.0 named the Great East Japan Earthquake (GEJE) occurred on 11 March 2011. And a tsunami with the heights of more than ten meters hit a wide area of coastal Japan. At the Fukushima Daiichi Nuclear Power Plant (FDNPP) of the Tokyo Electric Power Company (TEPCO), the earthquake caused damage to the electric power supply lines to the site, and the tsunami caused extensive destruction of the operational and safety infrastructure on the site. The combined effect led to the loss of off-site and on-site electrical power. This resulted in the loss of the cooling function at the three operating reactor units as well as at the spent fuel pools. The reactor cores in Units 1-3 overheated, the nuclear fuel melted and the three reactors were damaged. Hydrogen was released from the reactor vessels, leading to explosions inside the reactor buildings in Units 1, 3 and 4 that damaged structures and equipment. Radionuclides were released from the plant to the atmosphere and were deposited on land and on the ocean. This accident was a level 7 of the international nuclear event scale of the International Atomic Energy Agency (IAEA).

Four cause investigation reports on this accident were issued by the government (ICAFNPS, 2011) (ICAFNPS, 2012), the parliament (NAIIC, 2012), the citizen organization (IICAFNPS, 2012) and the TEPCO (TEPCO, 2012) in Japan individually. Thereafter, the IAEA also issued a report on the accident (IAEA, 2015). The causes written in the four reports are discussed from the principle of safety culture and the inherent safety points of view in this paper.

2. Purposes

Safety is primarily based on safety culture and inherent safety technology in process industry. It is discussed whether these fundamentals had been adopted into the FDNPP, considering the causes made clear by the said four reports. If the TEPCO had not embodied many points on the inherent safety technologies in the plants, the accident at the FDNPP might be a man-made disaster. Therefore, the purpose is to prove from the perspective of technology if the accident was the man-made disaster or the natural disaster.

Basically this paper is not concerned with the problems relating to the human factors, the management, the governance, the legal system and the detailed safety culture which are studied by other papers (NAIIC, 2012), (Suzuki, 2014), (IAEA, 2015).

Table 1: *Inherent safety by Kletz (Kletz, 1991)*

Element nos.	Concepts
K1	Intensification
K2	Substitution
K3	Attenuation
K4	Limitation of effects
K5	Simplification
K6	Avoiding knock-on effect
K7	Making incorrect assembly impossible
K8	Making status clear
K9	Tolerance
K10	Ease of control
K11	Software

Table 2: *Inherent safety of ISO (ISO 12100, 2010)*

Element nos.	Measures
I1	General
I2	Consideration of geometrical factors and physical aspects
I3	Taking into account the general technical knowledge regarding machine design
I4	Choice of an appropriate technology
I5	Applying the principle of the positive mechanical action of a component on another component
I6	Provisions for stability
I7	Provisions for maintainability
I8	Observing ergonomic principles
I9	Preventing electrical hazard
I10	Preventing hazards from pneumatic and hydraulic equipment
I11	Applying inherently safe design measures to control system
I12	Minimizing the probability of failure of safety function
I13	Limiting exposure to hazards through reliability of equipment
I14	Limiting exposure to hazards through mechanization or automation of loading (feeding) /unloading (removal) operations
I15	Limiting exposure to hazards through location of the setting and maintenance points outside of danger zones

3. Safety culture and inherent safety techniques

The concept of safety culture was first introduced by the IAEA in 1991, as a lesson from the 1986 Chernobyl accident, and the definition is “the assembly of characteristics and attributes in organizations and individuals which establishes that as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance” (IAEA, 2002). The safety culture has been widely and highly developed for use in all industries ever since (Wikipedia, 2015).

There are both the inherent safety systematized by Kletz (Kletz, 1991), (Kletz, 2010) and the inherently safe design measures on the safety of machinery standardized in ISO 12100 (ISO 12100, 2010). The inherent safety technologies have the basic elements shown in Tables 1 and 2. Kletz expressed the elements concepts in felicitous words and phrases. The measures in Table 2 are reprinted from the headings of ISO 12100.

4. Verifications

The causes written in the four reports are discussed from the principle of safety culture and the inherent safety points of view in order to make clear if these fundamentals had been embodied in the FDNPP.

4.1 Priority of safety

The plant reactors, designed by US General Electric, were not suitable for the cultural and natural features of Japan, that is, a small, overpopulated and quake-prone country, and an atomic bombs-attacked people. Training, following a scenario of the maximum credible operating accident including a severe accident, had never been provided. The drastic technical safety measures had not been introduced since the plants were established. The TEPCO's concern was not to dedicate to the safety of the reactors following big hazards like huge earthquake and a large tsunami, but to jeopardize the confidence of the local community and general

public if the hazard was made apparent. These circumstances of risk management were peculiar to the nuclear industry in Japan. (NAIIC, 2012), (IICAFNPS, 2012), (Suzuki, 2014)

In a word, the safety culture of giving top priority to safety had not been correctly perceived and nurtured by the TEPCO. The specific matters regarding the technology are discussed as given below.

4.2 Seismic strengthening works

On 2006, "a new regulatory guide for reviewing seismic design of nuclear power reactor facilities" was formally decided upon at Nuclear Safety Commission of Japan (NSC). In actuality the revision was merely that earthquakes of up to about M6.8 were taken into consideration and the maximum acceleration became only about 450 Gal. At the time of the accident, however, the TEPCO had performed only limited seismic back-fit of the FDNPP. Despite being aware that much of the equipment and piping did not meet the requirements of the revised guide, the TEPCO had hardly implemented any seismic reinforcement works. While Nuclear and Industrial Safety Agency of Japan (NISA) recognized the need to quickly conduct seismic back-fits. Therefore, the National Diet of Japan Fukushima Nuclear Accident Independent Investigation Commission (NAIIC) did not guarantee that at the time of the GEJE the equipment and the overall piping system that were important for the safety functions of the FDNPP were in a state that could withstand the maximum acceleration of 600 Gal of the design basis earthquake ground motion approved by the NISA and the NSC at 2009. (NAIIC, 2012) The Boiling Water Reactors (BWR) of Unit 1 to 4 came online the first in 1970 and the last in 1978. The anti-earthquake procedures have been remarkably developed ever since, that is, there are earthquake resistant construction, quake-absorbing structure and damping structure. These new-developed techniques should have been introduced in the FDNPP. Therefore, it is clear that the I3 in Table 2 had been inadequate and inappropriate for keeping the FDNPP safe against any kind of earthquake.

4.3 Redundancy and diversity of subsystems

As shown in Figure 1, it was the main cause of the FDNPP accident that a station blackout occurred, that is, loss of off-site power due to the landslide caused by the earthquake and loss of the on-site power sources due to tsunami, and the seawater pumps for the cooling systems broke down simultaneously. And furthermore, the TEPCO was clearly aware of the danger of an accident. It was pointed out to them many times by the NISA since 2002 that there was a high possibility that a tsunami would be larger than had been postulated, and that such a tsunami would easily cause core damage (NAIIC, 2012), (IICAFNPS, 2012).

The electric power sources of the FDNPP, that is, the off-site power, the emergency generators and the batteries, were in sufficient redundancy against accidental failures and power loss in a regular setting. However, all safety functions were lost simultaneously due to the earthquake and the tsunami. It was fragile when faced with the simultaneous outage of multiple power sources from natural disasters, with no power supply diversity ensured among different plants, and with its fail-safe feature dependent on the switchboard and direct-current power supply (NAIIC, 2012).

These were not in diversity of design and/or technology to avoid common cause failures of submergence and common mode failures of electrical power loss. Not only redundancy but also diversity had to have been realized to ensure that the safety function remained available, as written in the details of I12 in Table 2.

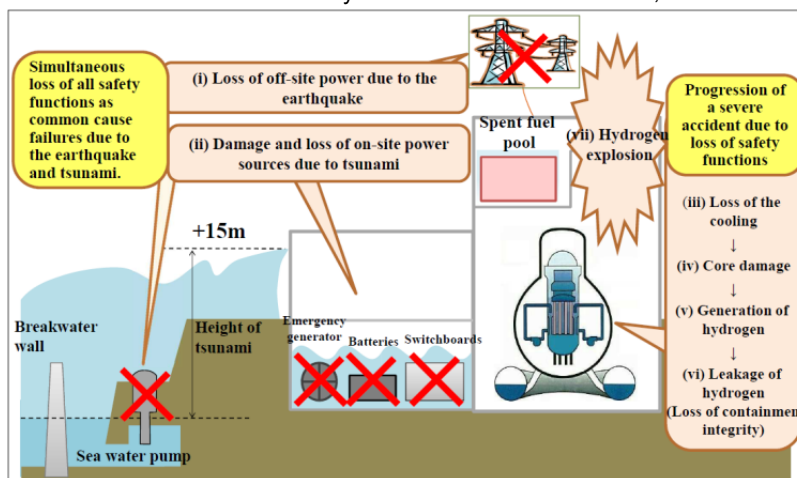


Figure 1. An overall aspect of consequence to FDNPP (NRAJ, 2013)



Figure 2. A plume of white smoke rises from around SFP of Unit 4 after the hydrogen explosion (Taken by TEPCO on 16 Mar. 2011)

4.4 Asymmetry failure mode, simplification and limitation of baneful effects on reactor cooling system

The isolation condenser (IC) system was installed in the plant reactors of Unit 1 to continue the cooling of the reactor core by repeating the cycle of condensing steam inside the reactor pressure vessel into water, using the condenser tank, and feeding that water back into the reactor. The IC was the system of asymmetry failure mode, that is, failsafe function. However, even though the IC had malfunctioned, personnel were under the impression that it had been operating normally. Thus, a great deal of time elapsed before the operations of an alternative water injection procedure using fire engines and pressure venting of the primary containment vessels were performed, and this ended up delaying efforts to cool the reactor core. Accordingly they failed to anticipate the progress of events which would have allowed them to take the necessary measures in advance. And the necessary measures were not taken in order to inject water into the reactor without interruption. Consequently, three times hydrogen explosions occurred and the accident was expanded. It is because some perfunctory education and training sessions in IC functions and operation procedures had been given and those sessions were not effective as far as the various steps taken indicated. (ICAFNPS, 2011), (ICAFNPS, 2012), (IICAFNPS, 2012)

It was extremely difficult to put the water cooling into effect as it was. For instance, if the objects for cooling were built lower than the sea level, it might be easy to supply or fill them with sea water. For the crisis management, it is vital to make the system simplification. Consequently, the FDNPP lacked an asymmetry failure mode in the details of I12 in Table 2, and the K4, the K5 and the K10 in Table 1.

4.5 Simplification of reactor building

An alternative method of water injection into the cores by fire engines which required no electricity started about twelve hours after the tsunami. On the other hand, since white smoke looked steam was confirmed to be coming from around the spent fuel pool (SFP) of each damaged reactor building as shown in Figure 2, water sprinkling by helicopters, water spraying by high-pressure water cannon trucks and water spraying by fire engines started in order to maintain water levels of the SFPs six days later (ICAFNPS, 2011). These water supplies were necessary for not only the reactors but also the SFPs.

The SFP is storage water pool for spent fuel from nuclear reactors. Not to maintain water level, melt-down of spent fuel might occur due to heat of radiolysis in the worst case. As shown in Figure 3, the SFPs were installed in the reactor buildings of the BWR containments, which made the accident complicated and the countermeasures difficult. The pool having a great hazard should be completely separated from the building. The simplification of K5 in Table 1 was not introduced into the reactor buildings.

4.6 Attenuation and avoiding knock-on effect by miniaturizing reactor

The total installed capacity of the FDNPP, including Units 1 through 6, amounted to 4,696 MW. The Units were too big to be brought under control in the crisis. A nuclear power plant in Japan is becoming increasingly bigger in recent years. The larger it is, the more difficult its control must be when an accident occurred by any possibility. A plan of the miniaturization or modularization, namely attenuation, of nuclear reactor was frustrated by the opposition of the priority to demand economic efficiency about thirty years ago.

One large single plant may usually be inherently safer than two plants each half its size, because avoiding troublesome containing such as more valves, flanges, pumps, pipes and others (Kletz, 1991). However, the nuclear reactors of the FDNPP were so large in size and in hazard that the counter measures of water cooling and the multiplied protections could hardly have any effect on avoiding knock-on effect. We should consider

the way of attenuation in which it is most likely to fail and should design smaller nuclear reactors so as to minimize the consequences, that is, the attenuation of K3 and the avoiding knock-on effect of K6 in Table 1.

4.7 Tolerance toward leakage or melt-down at reactor pressure vessel

Positioning (withdrawing or inserting) control rods, which are installed on the bottom of reactor pressure vessel as shown in Figure 4, is the normal method for controlling power in the BWR. Fortunately, it was confirmed that all control rods had been fully inserted for shutdowns after the earthquake. However, then the situation became worse and core meltdowns occurred in three reactors of Units 1, 2 and 3 at last (NAIIC, 2012). The structure of the pressure vessel with bottom holes seemed to be vulnerable to water and gases leakage due to extreme heat or contaminant pressure rise followed by the meltdown. This type of the BWR could not directly inject water into the bottom of the reactor containment vessel (pedestal). The vessel should have the tolerance of K9 in Table 1 for an accident.

4.8 Tolerance toward hydrogen gas generation

A series of hydrogen gas explosions occurred at the top spaces of reactor buildings of Units 1, 3 and 4 individually. The great amount of hydrogen was generated through a zirconium-water reaction because damage to the reactor core progressed, and leaked from the reactor pressure vessel (RPV) into the building via the reactor containment vessel (RCV) (ICAFNPS, 2012). The exploded hydrogen could have come from also the SFP due to radiolysis of hot water, but no quantitative evaluation was given at the stage (NAIIC, 2012). The RPV, the RCV and the SFP are sketched in Figure 3.

Inherent safety must tolerate hydrogen gas generation so as not to explode. For instance, a hydrogen gas should have been blanketed with an inert gas. There was no tolerance toward the hydrogen gas generation. Tolerance is K9 in Table 1.

4.9 Limitation of gas explosion effects

The hydrogen explosions caused serious damages to the reactor buildings as shown in Figure 2 and could give some damages to the RCVs including the suppression chamber, the devices and piping systems. The explosions had an effect on the escalation of the accident. On the other hand, the hydrogen explosion did not occur at the Units 2 reactor building. It is because a blowout panel (Area: Approx. 4.3 mx6.0 m, working pressure: 3520 Pa) had opened due to the impact of the vibrations or blast from the Unit 1 explosion and much of the leaked hydrogen inside the Unit 2 reactor building was released outside the structure from the blowout panel opening along with steam. Thus this served most likely to hold down the volume of hydrogen that built up inside the Unit 2 reactor building. (ICAFNPS, 2012)

By means of inherently safer ways of limiting the effects of explosions, the building should have been designed so that the explosions that do occur could not produce knock-on effects. In designing the building the TEPCO should have considered the way in which it is most likely to fail, and should have located or designed the equipment so as to minimize the consequences. To provide the building having an explosion-proof and/or the limitation of the effects, the explosion release structure and/or the installation of a rupture disc must have been introduced beforehand. These are K4 and K6 in Table 1.

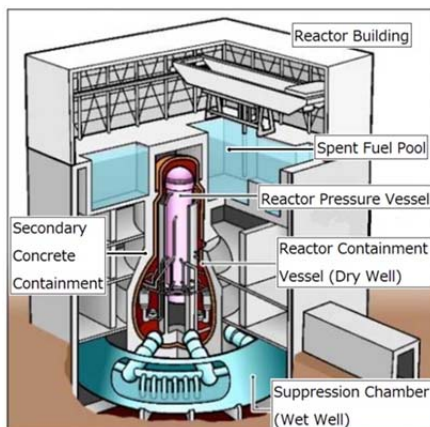


Figure 3. Cross-section sketch of Unit 1-5 reactors in FDNPP (US.NRC, 2015) (RPV height: Approx. 20 m)

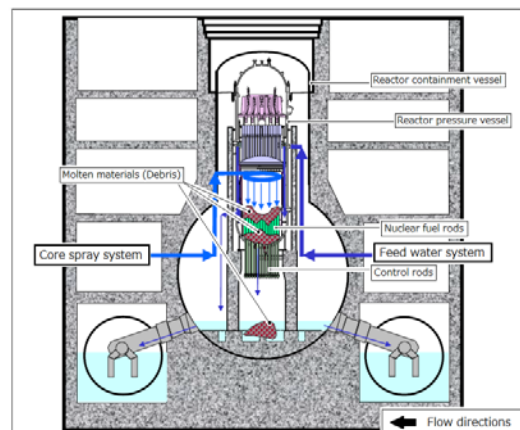


Figure 4. Presumptive state inside the reactor pressure vessel of Units 2 (TEPCO, 2013)

4.10 Simplification of emergency countermeasure

The alternative water injections, that is, using the fire protection systems to inject water into nuclear reactors and containment vessels, were mostly performed by attaching fire engines. Neither of the Units, however, showed an increase in water level corresponding to the amount of injected water and accordingly clogged piping and/or water leakage was suspected (ICAFNPS, 2011). Thereafter, bypass flows were investigated by the TEPCO. About 80% amount of the injected water is evaluated to flow into the bypass lines. If total amount of injected water had been ensured to be continuously supplied to the nuclear reactors, the reactor pressure vessels could have been flooded with water and the accidents would have converged (TEPCO, 2013).

The alternative water injection system composed of the make-up water condensate system with the fire protection system was too complicate to make sure of the direct flow line for the nuclear reactor. The final countermeasures that prevent serious damage even in the event of loss of safety functions due to common causes must be simple. The simplified safety measures can friendly function especially in case of emergency. The simplification of K5 in Table 1 was not materialized.

4.11 Making status clear in emergencies

The loss of power, the lack of information on safety parameters due to the unavailability of the necessary instruments and the loss of monitoring devices made it impossible to arrest the progression of the accident and to limit its consequences (IAEA, 2015). There was still a great deal of uncertainty associated with investigating the situation for weeks until introducing a research robot and the remote-controlled cameras.

Making status clear must be essential for preventing an expansion of the accident. A various kind of proper monitoring system having adequate independence, redundancy and diversity against internal and external hazards should have been set up in advance. This is deal with K8 in Table 1 and I11 in Table 2.

5. Conclusions and causality

The TEPCO was not in conformity with the fundamentals of safety as mentioned above. Therefore, the accident of the FDNPP was triggered by the earthquake, but the escalation into an extremely significant accident was directly caused by a lack of the technological common sense of safety principle and inherent safety designs as an inevitable consequence. The accident was not the natural disaster caused by the massive earthquake and the tsunami followed with high wave, but conclusively the man-made disaster just waiting to happen. The earthquake was a mere trigger.

References

- IAEA (International Atomic Energy Agency), 2002, Safety culture in nuclear installations, guidance for use in the enhancement of safety culture, IAEA-TECDOC-1329
- IAEA, 2015, The Fukushima Daiichi Accident, Report by the Director General, <<http://www-pub.iaea.org/books/IAEABooks/10962/The-Fukushima-Daiichi-Accident>> accessed 01.09.2015
- ICAFNPS (Investigation Committee on the Accident at Fukushima Nuclear Power Stations of Tokyo Electric Power Company), 2011; 2012, Interim Report; Final Report <<http://www.cas.go.jp/jp/seisaku/icanps/eng/>> accessed 01.09.2015
- IICAFNPS (Independent Inquiry Committee on the Accident at Fukushima Nuclear Power Stations), 2012, Inquiry Report, (in Japanese)
- ISO 12100, 2010, Safety of machinery General principles for design Risk assessment and risk reduction <http://www.iso.org/iso/catalogue_detail?csnumber=51528> accessed 01.09.2015
- Kletz, T.A., 1991, Plant Design for Safety: A User-Friendly Approach, Hemisphere Publishing Corporation.
- Kletz, T.A., Amyotte, P., 2010, Process Plants: A Handbook for Inherently Safer Design, 2nd ed. CRC Press.
- NAIIC (National Diet of Japan Fukushima Nuclear Accident Independent Investigation Commission), 2012, Main Report <<http://warp.da.ndl.go.jp/info:ndljp/pid/3856371/naaic.go.jp/en>> accessed 01.09.2015
- NRAJ (Nuclear Regulation Authority of Japan), 2013, Enforcement of the New Regulatory Requirements for Commercial Nuclear Power Reactors <<http://www.nsr.go.jp/data/000067212.pdf>> accessed 01.09.2015
- Suzuki, Atsuyuki, 2014, Managing the Fukushima Challenge. Risk Analysis, 34,1240-1256
- TEPCO (Tokyo Electric Power Company), 2012, Fukushima Nuclear Accidents Investigation Report <http://www.tepco.co.jp/en/press/corp-com/release/2012/1205638_1870.html> accessed 01.09.2015
- TEPCO, 2013, 1st Report, Press Release; 13.12.2013 (in Japanese) <http://www.tepco.co.jp/cc/press/betu13_j/images/131213j0102.pdf> accessed 01.09.2015
- US.NRC (United States Nuclear Regulatory Commission), 2015, Reactor Concepts Manual; Boiling Water Reactor Systems<<http://www.nrc.gov/reading-rm/basic-ref/teachers/03.pdf>> accessed 01.09.2015
- Wikipedia, 2015, Safety culture <https://en.wikipedia.org/wiki/Safety_culture> accessed 01.09.2015