Designing of comprehensive risk analysis system for multiple layers of defense-in depth concept

YOSHIKAWA Hidekazu[1,2]

1. Symbio Community Forum, c/o Research Institute of Applied Sciences, , Tanaka-Ohi-cho, Sakyo-ku, Kyoto, 606-8202, Japan (yosikawa@kib.biglobe.ne.jp)
2. College of Nuclear Science and Technology, Harbin Engineering University, Harbin, 150001, China

Abstract: A systematic and comprehensive risk analysis system has been under development for enhancing safety of nuclear power plant throughout the whole process of design, operation and maintenance and even for nuclear emergency and post-accident management. The major subject of this paper is to correlate this risk analysis system with the defense in depth concept proposed by IAEA. The discussions are made on how all defense in depth layers are organized, with highlighting on the system configuration for both the fourth and fifth layers of the defense in depth from the learned lessons of Fukushima Daiichi accident occurred in March 2011 in Japan.
Keyword: risk analysis system; defense in depth concept; nuclear emergency response system

1 Introduction[1]

The authors of this paper have been developing a systematic and comprehensive risk monitor system for enhancing safety of nuclear power plant throughout the whole process of design, operation and maintenance and even for nuclear emergency and post-accident management. [1-3]The meaning of "risk" by the authors' study is any kinds of adverse event or happening brought by the operation and handling of nuclear power system, while the meaning of "reliability" is successful rate of a system's performance that will fulfill its expected function when it is requested. So the precondition is rather restricted and fixed for the evaluation of reliability hence objectively conducted, while it is not so for the risk evaluation, broad and more subjective nature.

In the authors' study of a systematic and comprehensive risk monitor system, the individual subsystems or components of nuclear power system are selected as the target of reliability evaluation, while the whole system which are composed by subsystems of nuclear power system are taken as the target of risk evaluation.

The whole frame of the authors' Risk Analysis System is illustrated as shown in Fig.1. It is composed by two layers: (i)Plant Defense-in-depth (Did) risk monitor for evaluating risk state for whole plant system under various plant conditions, and (ii)Reliability monitor for individual subsystems which are vital elements to sustain the plant operation both from safety and efficiency aspects.

Reliability evaluation for a sub-system is made by Reliability monitor by using a combination of FMEA and GO FLOW model. FMEA (Failure mode and effect analysis) is a useful qualitative evaluation method to screen out any conceivable failure modes and their probable consequences which may arise in the target subsystem in assumed operation conditions. GO FLOW is a quantitative evaluation methodology to reduce dynamic reliability curve of a target system for a certain expected time span with considering phased mission.[4] Application studies of the reliability monitor of the authors' risk monitor system concept have been conducted for various safety systems of conventional PWR and AP1000.[5,6]

On the other hand, the plant DiD risk monitor will identify every potential risk state caused by any conceivable event in the plant system as a whole where not only internal events but also external events arising from common cause factors and human factors should be taken into account. The basic software tool has been under development for the plant DiD risk monitor to analyze complex human-machine interaction. [7]

Received date: September 16, 2015

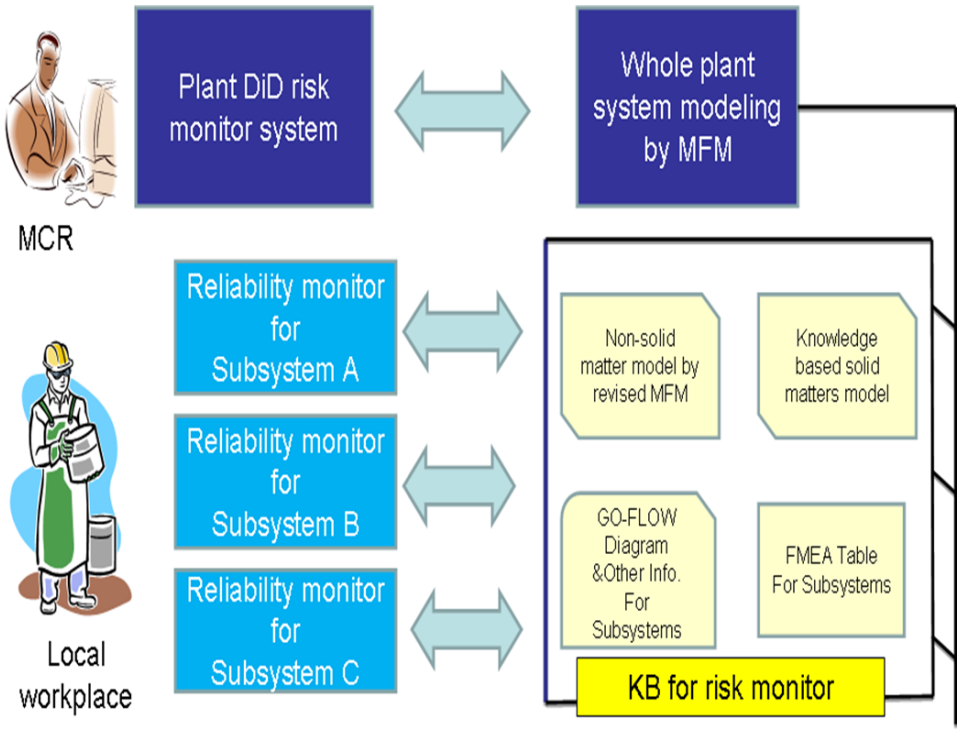

Fig. 1 Composition of authors' risk analysis system.

The author of this paper try to correlate with the authors' comprehensive risk analysis system with the defense in depth concept proposed by IAEA. The content of this paper deals with how all defense in depth layers will be realized by the authors' developed risk analysis system. As will be discussed from the succeeding sections, the most difficult application of the risk monitor will be for both the fourth and the fifth layers of the defense in depth from the real experience of Fukushima Daiichi accident occurred in March 2011 in Japan.

2 Defense in depth concept

2.1 Design principle of nuclear safety

According to a text book on nuclear safety[8], the word "defense in depth" is the central concept of design principle of nuclear safety with the multi-layered existence of four barriers (nuclear fuel, cladding, primary coolant pressure boundary including reactor pressure vessel, and containment), and the soundness of those barriers is assured by three safety functions ("stop" the nuclear reaction, "cool" the reactor and "contain" the radioactivity.) It is also said that reliability of safety functions is enhanced by principles of diversity, redundancy and physical separation.

2.2 Severe accident as the risk of nuclear power

Ultimate risk of nuclear power plant is the radioactive hazards resulting from various possible states of severe accidents. Major severe accident phenomena in light water reactors can be summarized as shown in Table 1, where many severe accident phenomenons are classified into fuel behavior, coolant behavior and violent interaction behavior with two representative accident types of transient overpower and LOCA (loss-of-coolant accident).

Those severe accident phenomena can be also classified into three stages by the progression of accident: (i) within reactor vessel, (ii) within containment vessel, and (iii) outside of containment.

Various severe accident analysis methods have been developed thus far in many nuclear developing countries, and those methods have been integrated into many severe accident analysis codes, and they can be classified into three code systems: (i)source term analysis code, (ii)integrated code, and (iii)detailed mechanistic code. Figure 2 shows the severe accident sequence and the related severe accident codes now available for the severe accident analysis of many light water reactors.

Table 1. Major severe accident phenomena in LWR

Severe accident phenomena	Transient over-power	LOCA
Fuel behavior mainly related to failure to stop the nuclear reaction	Fuel swelling Fuel failure and melting Pellet-clad interaction Fuel relocation/slumping	
Coolant behavior mainly related to failure to cool the reactor		DNB Two-phase flow Natural circulation Blowdown-refill-quench-reflood CCFL
Various violent interaction behavior mainly related to failure to contain radiological release	FCI Zr-water reaction Hydrogen explosion Steam explosion Corium-concrete reaction	

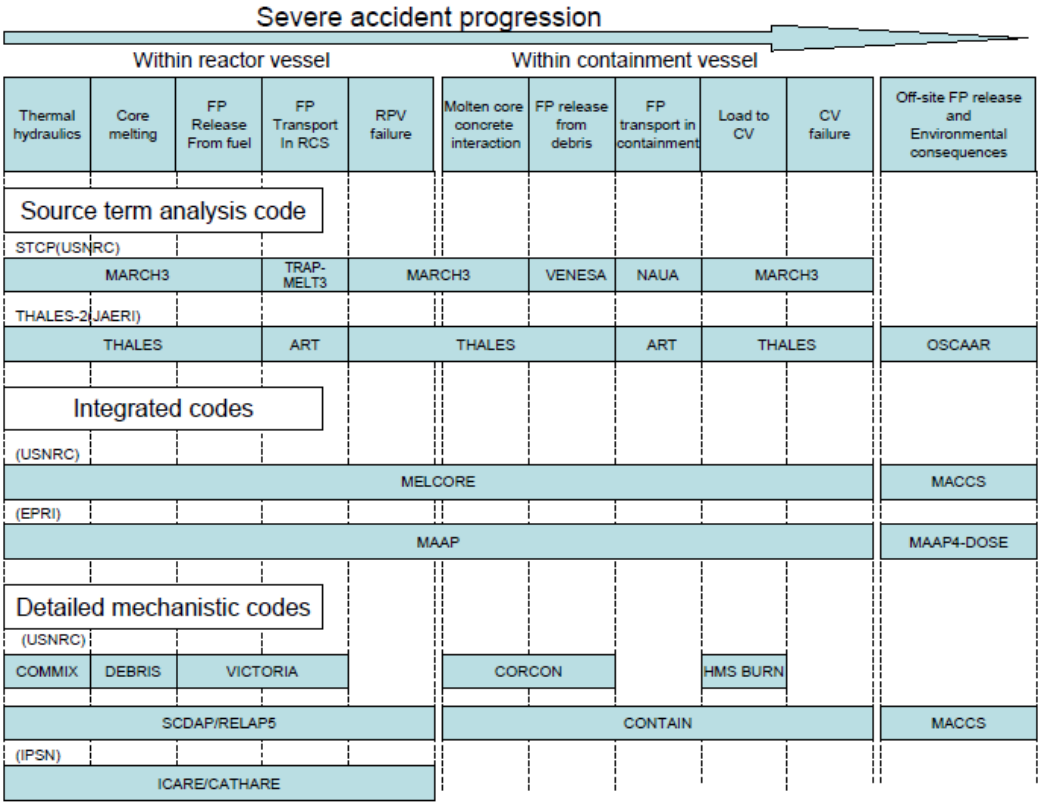

Fig. 2 Severe accident sequence and the related severe accident codes.

2.3 Defense in depth concept defined by IAEA

The concept of Defense in depth of nuclear power plant had been established by INSAG group of IAEA after Chernobyl accident. The details of the defense in depth concept are described in the report of INSAG-12 [9], and the objective and method of each layer are described as shown in Table 2.

Table 2 Defense in depth concept by IAEA INSAG-12

Layer	Objective	Method
1	Prevention of abnormal operation and failure	Conservative design and high quality in construction and operation
2	Control of abnormal operation and detection of failure	Control, limiting and protection systems and other surveillance features
3	Control of accidents within the design basis	Engineered safety features and accident procedures
4	Control of severe plant conditions including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency responses

It is also said in INSAG-12 that conservatism, quality assurance and safety culture are common requirement throughout all five layers, although conservatism is applied mainly for the layers 1 to 3 while best estimate consideration for the layers 4 and 5.

2.4 Specific characters of individual layers

The layer 1 is the initial base for protection against not only internal but also external hazards such as earthquakes, aircraft crashes, blast waves, fire, flooding. The layer 2 incorporate the inherent plant features and systems such as passive mechanism, automatic control for maintaining safety. The layer 3 employs design principles to ensure high reliability such as redundancy, avoidance of common mode failure by separation, diversity. It also employs automation to reduce human error. The measures of the first three layers will ensure maintenance of structural integrity of the reactor core and limit potential hazards for the public.

On the other hand of the those three layers, the broad aim of the fourth layer (layer 4) is to ensure the likelihood of accident entailing severe core damage and the magnitude of radioactive releases in the unlikely event are both kept as low as reasonably achievable. However the unlikely events caused by multiple failures or extremely unlikely events may bear a potential that radioactive materials could be released to the environment. The thermal inertia of the plant provides time to deal with some of these conditions by means of additional measures and procedures. The most important objective for the mitigation in this layer 4 is the protection of the confinement. Role of operator is vital to the successful management in this layer.

Lastly for the layer 5. Off-site emergency plan should cover the level of exposure expected to occur, and short and long term protective actions that constitute intervention. The responsible authorities take the corresponding actions on the advice of the operating organization and the regulatory body. Periodical exercises both the on-site and off-site organizations to ensure the readiness of the involved organization.

3 How the risk analysis system covers defense in depth layer

The discussion in the previous sections 2.3 and 2.4 will naturally indicate the clear difference of the role of the layers 1 to 3 (prevent the occurrence of core damage accident) and the layers 4 and 5 (mitigate the consequence of core damage accident). Therefore the author of this paper would like to proceed to discuss on the authors' risk analysis system by dividing the layers 1 -3 and layer 4 and 5.

3.1 What to do for the layers 1 ~3?

The authors' Did risk monitor for the layers 1~3 is basically the same as the conventional living PSA where instantaneous core melt frequency is taken as risk value. However it will not only deal with instantaneous core melt frequency alone, but also more detailed risk evaluation step by step as follows. The first step will be (i)what will be the state of three safety functions (STOP, COOL and CONTAIN). Eight different states will be conceived by judging from the two states of success (1) or failure(0) of each safety function as shown in Table 3 for risk ranking by safety function.

As you see in the column of "possibility of severe accident" in Table 3, you can qualitatively distinguish by what degree of severity of accident, but it may not be enough information for emergency management. Although it is possible to distinguish the state change in the risk ranking table by seeing whether or not individual safety function may fail or recover, it is not directly related with the damage or recovery of

the individual barriers (fuel, cladding, pressure boundary and containment). Therefore, it is necessary to measure or estimate the real accident state to judge the soundness of those barriers by other means.

Table 3 Risk ranking by safety function

Risk level	Stop	Cool	Contain	Possibility of severe accident
0	1	1	1	No risk Safely shutdown, cooled and no release
1	1	1	0	No severe accident phenomena but some problem in containment
2	1	0	1	Loss of not so serious cooling function Safely shutdown, but cooling failed but no release
3	1	0	0	Serious severe accident possible Safely shutdown, but both cooling and contain function failed
3	0	1	1	Severe accident may be suppressed by ESF function Shutdown failed but cooling and no release
3	0	1	0	Some contain function failed Shutdown failed , cooled but released
4	0	0	1	Serious though severe accident phenomena occurr because containment function succeeded Shutdown failed , cooling failed but no release
5	0	0	0	Worst severe accident because all safety functions failed

This is the step (ii) of Evaluation of time margin until core melt with confirming successful CONTAIN function by evaluating the degree of the soundness of fuel rods (fuel pellet and cladding) and reactor pressure boundary. And if you can do it by some means, you can realize the two stage visualization of dynamically changing risk as shown in Fig. 3.

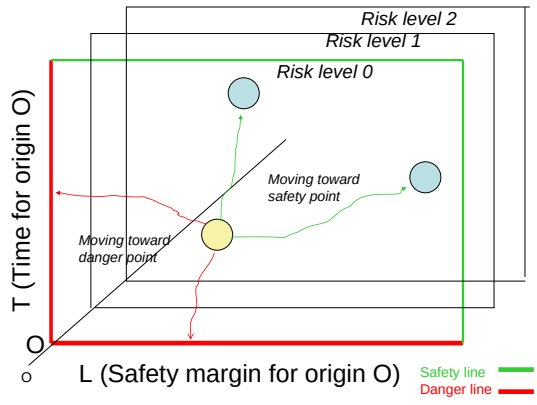

Fig. 3 Two stage visualization of dynamically changing risk.

In Fig.3, difference of risk level is shown by different plane, and quantification of risk by two factors in the same risk level: (i)Time margin to reach the point of no return, and (ii)Degree of physical damage no more to be recovered.

The image of risk monitor system for the layers 1 to 3 can be shown in Fig. 4, where a distributed HMI system will connect plant Did risk monitor in the main control room and several reliability monitors in local working places over plant intranet. In Fig. 4, proactive trouble prevention knowledge database will be mainly used for the layer 1, while online plant monitor & diagnosis tool for the layers 2 and 3. The users of Did risk monitor are operators in main control room (through operator console for online plant monitor and diagnosis tool and maintenance console for proactive trouble prevention knowledge base) while maintenance staffs with reliability monitors at local workplaces with all sharing information through online data distributing.

3.2 How about layers 4~5 ?

Then what will be for the layers 4~5 by authors' Did risk monitor? In order to consider for it, the images of the accident for the layers 4 and 5 are given by Table 4, which is taken from Table 3-2 in p.26 of Ref.[8]. Please note that for the layer 4 the consequence of the maximum DBA (Design Basis Accident) will be severer for low level safety system or partial core

melt, and that the prompt successful intervention by the layer 5 can mitigate the consequence of radioactive release caused by severe accident.

At this stage, let us first consider what can be made for the layers 4 and then by what way as the similar way of distributed HMI (Human Machine Interface) system as shown in Fig. 4. The resultant story will be as follows;

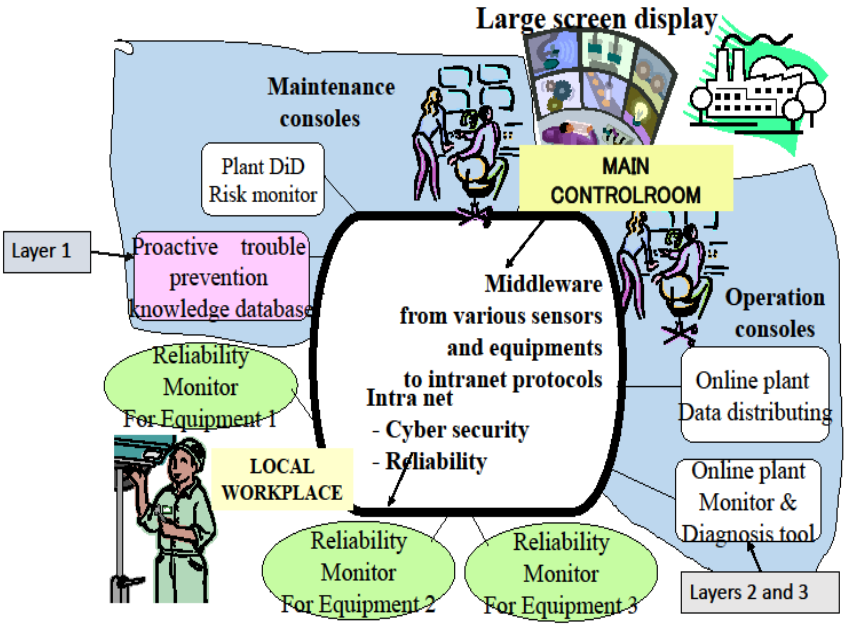

Fig. 4 Distributed HMI system for NPP.

Table 4 Different types of maximum DBA and severe accident

Type of accident	Remarks	Layer	Release rate of I-131	Order of radioactive release (TBq)	Probability /Year
A. Maximum DBA		4	10^{-7}	0.3	10^{-5}
B. Maximum DBA	Low level safety system or partial core melt	4	10^{-5}	30	10^{-5}~10^{-6}
C. Severe accident	Prompt successful intervention	5	10^{-4}	300	10^{-6}
D. Severe accident	Delayed intervention	5	10^{-3}	3,000	10^{-7}
E. Severe accident	No intervention	5	10^{-2}~10^{-1}	30,000~300,000	10^{-8}

The layer 4 evaluation start with no time margin of core melt in the layer 3 with knowing the degree of soundness of fuel rods (fuel pellet and cladding) and reactor pressure boundary.

Prompt evaluation of time margin will continue until the failure of CONTAIN function, with evaluating the core damage state and the soundness of reactor pressure boundary in order to estimate the source term to be emitted from the reactor. Therefore, the layer 4 evaluation by risk monitor should consider (i) prompt source term evaluation, (ii) prompt prognosis on what will be the future state of plant, and (iii) proposition of effective countermeasures taken by operators to recover the plant state.

However, when the plant state will aggravate so fast so that the failure of CONTAIN function may be soon anticipated, the stage of the risk monitor should go up to the layer 5 evaluation where how much radioactivity may emit from the damaged plant *(i.e.*, the estimated source term as the radioactive release to the environment). Prior to the identification of the failure of CONTAIN function, it will be also

necessary to prepare for off-site emergency action from many aspects.

The off-site emergency plan will be different from each nuclear developing countries, but the author of this paper will consider the Japanese situation based on the experience in Fukushima Daiichi accident, where the off-site nuclear emergency action is basically left for the responsibility of local government by the same way as for various natural disaster but with special administrative involvement by central government which is defined by the nuclear disaster prevention act introduced in 2000.

4 Design for the 4th and 5th risk monitor system in Japan

4.1 Japanese Nuclear Emergency Response System prior to Fukushima accident

The configuration of the nuclear emergency response system established in Japan before Fukushima accident is described in Ref. [10], and the comprehensive picture of the whole system can be illustrated as shown in Fig. 5. This is a large and fast telecommunication network system, by which all the stakeholders involved in accident management should share the accident information in common and to cope with nuclear accident management when a big accident happens at any nuclear facilities in Japan.

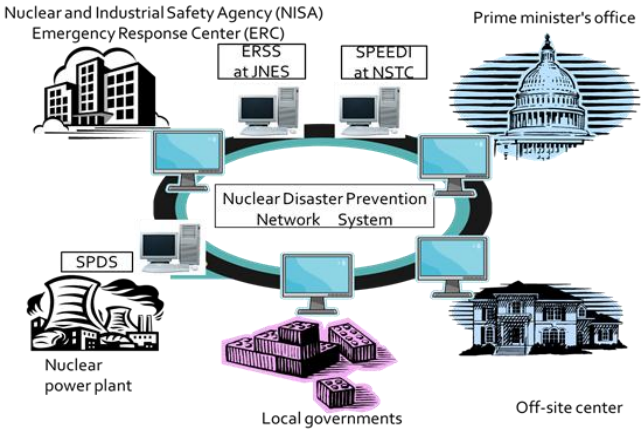

Fig.5 Nuclear Disaster Prevention Network System in Japan.

The specific feature of this Japanese nuclear emergency management system is heavy reliance on two major technical support systems: Emergency Response Support System (ERSS) and System for Prediction of Environmental Emergency Dose Information (SPEEDI). Although not go into details of the both systems, the ERSS is based on severe accident analysis code while SPEEDI analysis code for environmental radioactive dispersion from the severe accident committed nuclear power plant. There were nuclear evacuation training implemented in Japan every year after 2000, the method and range of the evacuation depend on the calculated dose rate obtained by the pair of ERSS and SPEEDI.

4.2 Lessons from Fukushima Daiichi accident

At the time of Fukushima Daiichi accident, all the roads and grounds around the plant were damaged by both earthquake and tsunami. This hindered easy transportation by the roads, and the loss of electricity with loss of all communication channels disabled the usage of ERSS and SPEEDI which were expected to work as the ace card for managing the situation in such nuclear disaster: The directions issued by the responsible body had confused many evacuees at the time.

According to the investigating report on Fukushima accident, one of the largest lessons learned from Fukushima Daiichi accident is that there was in fact no preparedness against severe accident in Japan [11]: It is ascribed to the false complacency that there will be no severe accident occurred in any nuclear power plant in Japan.

4.3 Design for 4th and 5th layer risk monitor

The author of this paper proposes to reconfigure the completely failed nuclear emergency management system during the Fukushima accident (Fig.5). The reconfiguration can be illustrated as in shown in Fig. 6, where both the layers 4 and 5 of the authors' risk monitors are also indicated. The details of the both layers 4 and 5 will be described in the subsequent sections.

4.4 The 4th Did risk monitor

In Fig.6, the emergency response support center is additionally introduced in the nuclear power station. This center is located at some distance apart from the main control room (MCR). The ERSS is implemented in the emergency response support center as the 4th Did risk monitor. In fact, this center will support the operators in MCR from the outside of the MCR in case of plant emergency. Until this layer 4 the risk monitor system concerns the plant risk within the

nuclear power station. As shown in Fig.6, the major sources of radioactive risk in the nuclear power station are not only nuclear reactor and spent fuel pool in each reactor unit but also spent fuel facility in the station.

4.5 Major point of changing ERSS

The ERSS system was originally developed and operated by JNES in Tokyo, but it should be installed in the emergency response support center of the nuclear power plant (NPP) operator in local site. The modeling capability of the ERSS should be limited to deal with the existing reactors of the corresponding NPP site.

By relocating the ERSS from Japan Nuclear Energy Safety Organization (JNES) in Tokyo to the NPP operator's emergency response support center, the communication channel between Safety Parameter Display System (SPDS) and ERSS will be shorter distance with less transmission capacity and becomes higher reliability. The analysts of NPP operator should know the plant condition better than the analysts at JNES at least for managing their own plants in severe accident condition.

4.6 The 5th Did risk monitor

In Fig.6, the off-site center will enter as the new actor for off-site emergency situation. The SPEEDI will be used as the 5th Did risk monitor. However to be compared with the scheme in Fig.5, the author of this paper changed the managing authority of ERSS from JNES in Tokyo to the emergency response support center in local nuclear power station, while that of SPEEDI from Nuclear Safety Technology Center (NSTC) in Tokyo to the off-site center in local area.

This change of the operating facilities of both ERSS and SPEEDI reflects the lessons learned at the time of Fukushima Daiichi accident. The reason is that for the off-site nuclear emergency system to work effectively, it is vital to intervene as fast as possible, in order to limit the accident consequence.

That was the problem of nuclear administration as one of the lessons of the Fukushima accident that the emergent management was not at all worked well at Fukushima by the central control that every local accident information should be concentrated to Tokyo in order to control the information disclosure before the decision making will be made in Tokyo and then the order will be given from Tokyo to local place in an emergent situation.

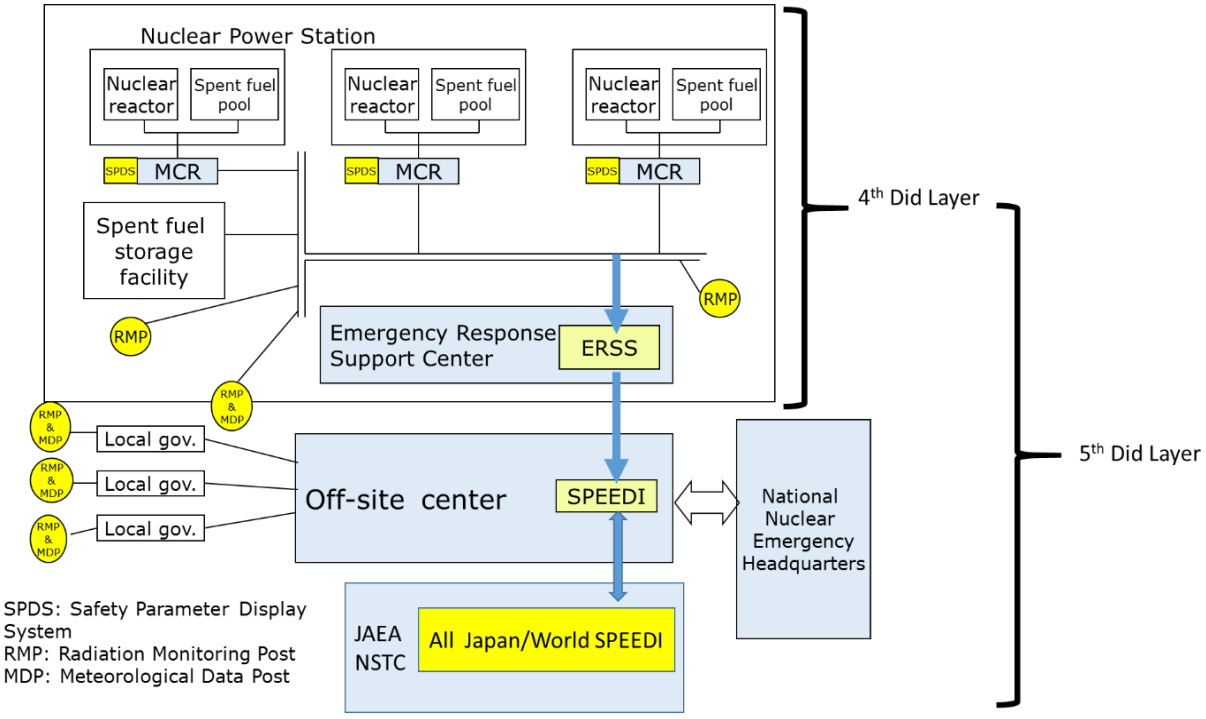

Fig.6 Design Concept for the 4th and 5th Did layers to cope with nuclear severe accident.

4.7 Major point of changing SPEEDI

The SPEEDI originally installed at NSTC in Tokyo should be also relocated to the off-site center at the local site.

The functional capability of SPEEDI should be restricted to deal with the periphery of the local site with more detailed, accurate and up-to date data on that region.

As you see in Fig.6, the source term information calculated by ERSS with various meteorological data coming from many meteorological data post (MDP) in the neighborhood of the plant will be the input data to the SPEEDI for the calculation of environmental dispersion of radioactive materials around the NPP. Also radioactive data coming from the radiation monitoring post (RMP) in many places of local area should be connected to the off-site center for daily validation of SPEEDI.

By this way, the cooperation between the emergency support center at NPP and the off-site center becomes more intimate not only in normal days but also in case of nuclear emergency. This will contribute to the success of nuclear disaster prevention activity even if serious natural disaster may cause the management of nuclear emergency to be more difficult with more complicated than by the nuclear emergency by the internal causes of NPP.

4.8 All Japan/world SPEEDI by JAEA and NSTC

For Fig. 6, it should be pointed out that the original SPEEDI system in NSTC to calculate radioactive dispersion all over Japan and that around the world by "World SPEEDI" developed by JAEA should be maintained in the respective institutions (NTSC in Tokyo while JAEA in Tokai-Mura) so that the influence of radioactive release over wide area both inside and outside of Japan can be evaluated when such a big severe accident as Fukushima Daiichi accident will occur somewhere in future.

4.9 The remaining issues

It is rather difficult to design off-site emergency response plan in the five layer as a whole to take into account of all associated social risks. This is because the nature of risk brought by off-site emergency response is versatile so that it is necessary to consider not only for avoiding short time radioactive dose for human, but also to avoid, limit and decontaminate radioactive contamination of the surrounding periphery in the long run. This issue is in fact still annoying the Fukushima area after four years and will continue for many years in future.

5 Conclusion

The nuclear emergency preparedness is the fifth layer of Defense-in depth concept for nuclear safety. In Japan, the ERSS had been developed and implemented as the ace card to the nuclear disaster prevention network system. But unfortunately it resulted in no effective use at the time of Fukushima Daiichi accident.

The root cause of the failure of ERSS is the way of organizing the whole nuclear disaster prevention network system. There was a fatal weakness in the way of constructing and maintaining disaster prevention network system. That is the over-concentration in Tokyo to manage all activities of the nuclear emergency response.

Based on the discussion mentioned, the author proposed that the ERSS should be operated and maintained by the nuclear emergency support system of the NPP operator, while the SPEEDI be relocated to the off-site center of the local site. As to the fifth layer of defense-in depth for nuclear safety, better coordination between NPP operator and local government will be crucial entity for the successful safety management during the real situation of nuclear emergency.

In this paper, the remaining problem of evacuation planning to be prepared in advance for nuclear emergency management is not discussed, because this is mainly the issue of decision making by the national nuclear safety authority and the local government for planning stage such as what will be for (i) Classify hazard, (ii) Classify emergency situation, and (iii) Deciding the range of emergency planning. However, this planning will be important for the effective designing of both the 4^{th} and 5^{th} layers of Did risk monitor system.

ACRONYMS

DBA Design Basis Accident
Did Defense-in depth
ERC Emergency Response Center
ERSS Emergency Response Support System
HMI Human Machine Interface
IAEA International Atomic Energy Agency
JAEA Japan Atomic Energy Research and Development Authority
JNES Japan Nuclear Energy Safety Organization
MCR Main Control Room
MDP Meteorological Data Post
NPP Nuclear Power Plant
NISA Nuclear and Industrial Safety Agency
NSTC Nuclear Safety Technology Center
PSA Probabilistic Safety Assessment
RMP Radiation Monitoring Post
SPDS Safety Parameter Display System
SPEEDI System for Prediction of Environmental Emergency Dose Information

References

[1] YOSHIKAWA, H., YANG, M., HASHIM, M. LIND, M., and ZHANG, Z.: "Design of Risk Monitor for Nuclear Reactor Plants, In: Progress of Nuclear Safety for Symbiosis and Sustainability, Eds: H.YOSHIKAWA and Z. ZHANG, pp.125-135, Springer, (2014).

[2] YOSHIKAWA, H., *et al.*: 2012, Nuclear Safety and Simulation, Vol. 3, No 2, pp.140~152.

[3] YOSHIKAWA, H., *et al.*: 2013, Nuclear Safety and Simulation, Vol. 4, No. 3, pp.192~202.

[4] MATSUOKA, T.: 1996, System Reliability Analysis Method GO-FLOW for probabilistic Safety Assessment, CRC Sogo Kenkyusho. (In Japanese).

[5] HASHIM, M., *et al.*: 2012, Nuclear Safety and Simulation, Vol. 3, No. 1, pp. 81~90.

[6] HASHIM, M., *et al.*: 2013, Nuclear Safety and Simulation, Vol.4, No.2, pp.147-159.

[7] YOSHIKAWA, H. and NAKAGAWA, T.: "Software System Development of NPP Plant Did Risk Monitor-Basic Design of Software Configuration-, "Proc. ICONE23,, Chiba, Japan, May 17-21,2015. (CD-ROM).

[8] PETRANGELI, G.: Nuclear Safety, 2006, Elsevier, Chapter 9 Defence in depth, 89-91.

[9] IAEA: INSAG-12 Basic safety principles for nuclear power plants 75-INSAG-3 Rev.1, Vienna, 1999.

[10] MAEKAWA, Y.: Overview of the NISA's Emergency Response Center, Journal of Atomic Energy Society of Japan, 2011, 53(4), pp. 278-282.(In Japanese).

[11] HOMMA,T.: "Towards Enhancing Preparedness and Response Arrangements and Capabilities for a Nuclear Emergency, (1); Emergency preparedness and response-Concepts in international standards and Fukushima experience", Journal of Atomic Energy Society of Japan, 56(10), pp. 661-668(2014) .(In Japanese)