An Adapted Risk Evaluation Methodology Applicable to both PWRs and CANDUs

Jae-Young Lee[1], Manwoong Kim[2], Jong-In Lee[2], Kyun-Joong Yoo[3]

[1]HanDong University, [2]Korea Institute of Nuclear Safety, [3]Korea Atomic Energy Research Institute

ABSTRACT

An objective of this study is to propose a methodology, which enables to evaluate the risk of the different types of nuclear power plants. The merits and demerits of various nuclear power plants put difficulties in making a consistent regulation to different types of nuclear power plants. In this regard, it is necessary to construct a common objective frame to cover all the sorts of safety characteristics of different plants such as PWRs and CANDUs. In is paper, the design risk for a nuclear power plant is defined as a function of failure frequency, the number density of incidents and the allowable dose limit. It was found that the distribution of the design risk is highly affected by the failure criteria.

To identify the effect of diversity in safety systems, the failure rate of the safety functional group is proposed. In a safety functional group, there are many alternative safety systems. By introducing the index of effectiveness of individual safety system, the natural selection rule of the safety systems in a functional group is developed. This design risk for the safety functional group could cover the single failure criteria of PWRs and multiple failure criteria of CANDUs. Furthermore, the present method could evaluate the various concepts to enhance the safety of the nuclear power plant such as the diversity design, the add-on redundancy, and the passive in a consistent way.

1. INTRODUCTION

Korea is a country having two different types of nuclear power plants such as a pressurized water reactor (PWR) and a pressurized heavy water reactor (CANDU). Since they were designed based on different criteria, i.e., the single failure criteria for PWRs and multiple failure criteria for CANDUs, it is difficult to identify which reactor is superior without developing a common objective evaluation method. In this reason, they have different manners and measures in safety evaluation and regulation. While PWR puts the evaluation and regulation method in prescriptive, CANDU has a consultative system in accordance with the designer's expertise in considering safety issues. Therefore, the regulatory body is in difficulty due to this difference in establishing consistent and comprehensive system for evaluation and regulation of those nuclear power plants.

Single failure criteria have been widely accepted in the nuclear industry because they could simplify the safety system, clearly fix the boundary of the analysis, and focus the efforts to improve reliability of a specific safety system. It is not too much to say that these criteria have stimulated the innovation of the safety system of a PWR. On the other hand, the inevitable increasement of complexity from the multiple failure criteria, i.e., diverse design of the safety systems, could not be in the limelight. However, CANDU is a good example of engineering design to show how to minimize the complexity of the diverse design as well as to improve its reliability economically. However, in terms of the positive moderator temperature coefficient, the vagueness in the license process produces overwhelmed worry on the safety of CANDUs. Whereas the negative temperature coefficient of a PWR could not provide the reactor shutdown capability, the general concerns on the positive moderator coefficient of a CANDU and its separated design of the coolant and moderator systems made CANDU equipped two independent and diverse reactor shutdown systems such as SDS1 and SDS2 [1].

The major objectives of this paper is to propose a safety measure, which could be useful for the comprehensive comparison between different types of reactors. To do this, the concepts of *design risk* and *safety functional group* are introduced. The design risk is defined in section 2 and applied to both PWRs and CANDUs aimed to assessing the adequacy of this proposed method and to investigating the effect of failure criteria.

In section 3, the concept of *the safety functional group* is introduced to know how to use the this concept for the evaluation of the safety system design. The functional group could include many alternative safety systems. For instance, the reactor shutdown functional group has temperature coefficient, shutdown rod, chemical injection, and others. If we could evaluate the reliability of the safety functional group, the failure criteria for the individual safety system plays no more roles in evaluation. In this new concepts, the selection rule should be prepared to compose the safety functional group. This selection rule plays the role of the failure criteria. If the selection rule select only one safety system among many alternatives, it acts like a single failure criteria. Also, if it selects two safety systems, then it acts like multiple failure criteria. The reactor shutdown functional group and emergency core cooling functional group are studied.

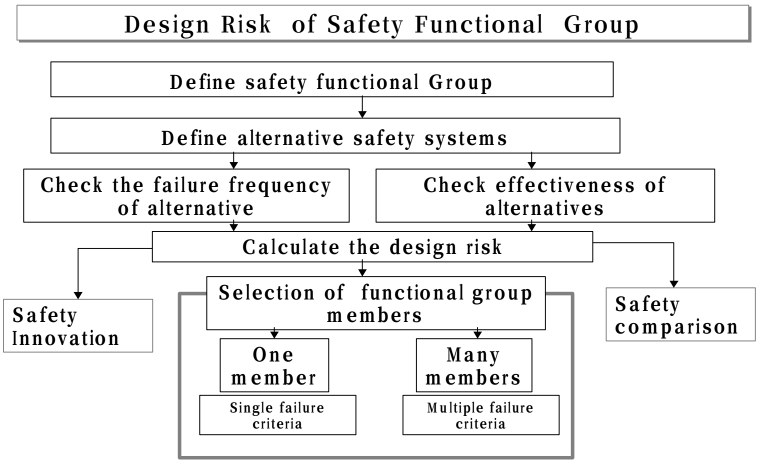
Design Risk of Safety Functional Group
Define safety functional Group
Define alternative safety systems
Check the failure frequency of alternative
Check effectiveness of alternatives
Calculate the design risk
Safety Innovation
Selection of functional group members
Safety comparison
One member
Many members
Single failure criteria
Multiple failure criteria

Fig.1. The evaluation system of design risk for safety functional groups

2. DESIGN RISK OF NUCLEAR POWER PLANT

Since the safety goal of the nuclear power plant is generally determined with an aim to limit the fuel damage frequency, the deterministic safety analyses are focused on assessment of the peak cladding temperature to determine whether it is higher than fuel melting temperature or not during the hypothetical accidents. In the meanwhile, the probabilistic safety analyses are made to evaluate the occurrence frequency of this hypothetical accident resulting the fuel damage. The design risk of a nuclear power plant could be quantified by multiplying the dose released and the frequency of the correspondent accident. Therefore, the design risk could be realized by evaluating the radioactive materials propagation to the environment which is affected by many complex factors such as the season, configuration of the ground, population etc. In this regard, the risk of nuclear power plants could be changed as the time goes on. The large uncertainty engaged in the evaluation of risk makes difficulties in comparing different reactor safety directly. Even between the same type of reactors, their different location makes difference in risks.

A. Allowable Dose Limits of PWRs and CANDUs

A deterministic safety analysis method has been established after introduction of WASH-740 by US-AEC to propose the evaluation standard for the hypothetical accidents in the nuclear power plant releasing a large amount of radioactive material. However, the probability and consequence for hypothetical accidents could be evaluated using the method of WASH-1400 reactor safety study by Rasmussen in 1975. which is now used for licensing for the complementary tool. For the public health, US NRC provided the allowable dose limit in accordance with the failure frequency which is categorized as the plant conditions.

Also, the nuclear industry in Canada has independency between the institute for the development of the reactor technology, AECL, and the institute for the regulation of the reactor safety, CNSC. The CNSC proposed the failure frequency for the safety systems and the process systems as $1.0\times10^{-3}/yr$and $1/3\times10^{0}/yr$, respectively. Each systems should be designed to satisfy the above goals through the probabilistic reliability analysis. Since they allow the failure of the safety system, the dual failure frequency is relatively high, $1/3\times10^{-3}/yr$

The allowable dose limits for PWRs and CANDUs are plotted as a function of the system failure frequency changes are shown in Fig.2. The dose limits of both reactors are very similar in the low failure frequency. But for the high failure frequency, PWR imposes more strict limit than CANDU. Apparently, in the design policy for the reactor safety, PWR has more strict criteria than those of CANDUs. However, it should be checked in consideration of the distribution of the number of failures items. By extrapolating the dose limit to the very low frequency, the allowable dose limit for the severe accident could be in the range between 100 rem and 300 rem.

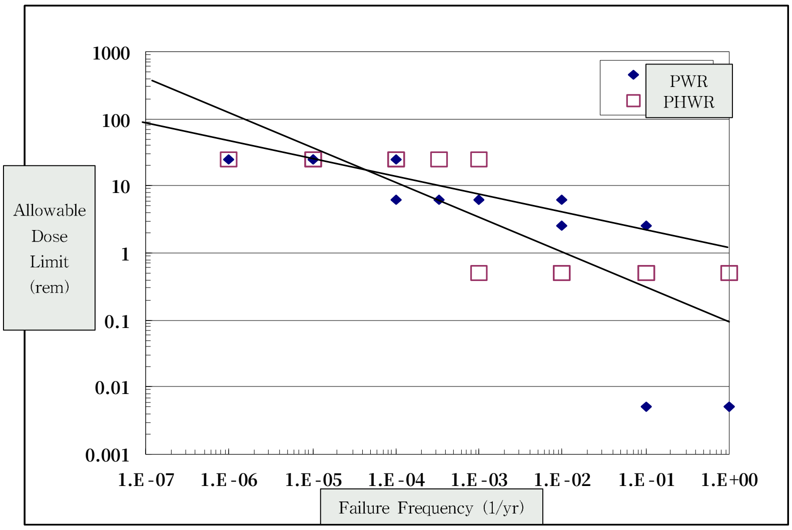

Fig.2 Allowable dose limit and failure frequency for PWR and CANDU

B. Design Risk of PWR and CANDU

The risk of the nuclear power plant is normally defined by multiplying the exposed dose to the incident frequency. This consequence analysis requires a large amount of analytical efforts. In this paper, the *design risk* is defined by multiplying the incident frequency and the allowable dose limit. If designer identifies a failure, j, the risk of j failure, $R_j(f)$, could be obtained as:

$$R_j(f) = R(f_j) = D_j(f_j) \cdot f_j \tag{1}$$

where $R(f)$ is a risk, $D(f)$ is a dose limit, and f is a failure per a reactor year.

For obtaining the total risk of each individual failure should be summed up:

$$R(f) = \sum_j R(f_j) = \sum_j D_j(f) f_j \tag{2}$$

However, if the allowable dose limit is digitalized, then the total risk of a reactor could be defined as

$$R = \int_0^\infty n(f) D(f) df \approx \int_{f_{goal}}^1 n(f) D(f) df \tag{3}$$

where f_{goal} is the cutoff failure rate for design goal(PWR $1.0\times10^{-5}/yr$) $n(f)$ is the incident number density. The number density is normalized so that $\int_0^\infty n(f)df = 1$. If not, the risk will increases as the number of failure increases. Therefore, the normalized risk could be used for the risk comparison among the different reactors.

(1) Number Density of Failures

Since the normalized number density is required to obtain the design risk of PWR and CANDU, number of failures and its failure frequency are obtained from the PSA report of Wolsong 2 nuclear power plant [2] and the representative incident for the reactor conditions for PWR. The number density profile is obtained by dividing the number of failures by the total number of failures of each reactor as shown in Fig.3.

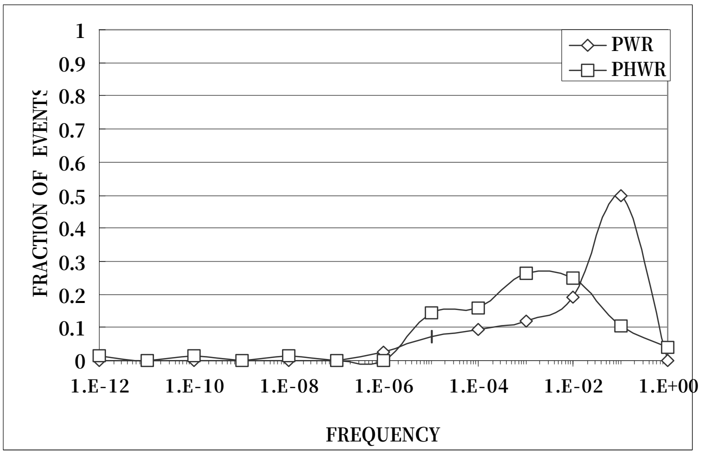

Fig.3 The distribution of incident density of the nuclear power plants for the failure frequency

There is a sharp peak at the high failure frequency for PWR. The distribution curve of CANDU has flatter distribution than PWR. As expected, PWR could reduce design risk by setting lower dose limit than CANDU in the higher failure frequency range, $10^{-1} \geq F$ since the peak in the number density of failure exists in the range. Also, it seems that the design effort of CANDU is made to reduce the number density of the failure of high frequency range. Although CANDU dose limit is larger than PWR's, CANDU could reduce the risk due to high frequency incidents compared with the PWR. In other word, in the high frequency failure rate region, reduction of number density of failure is easier than reduction of dose limit for CANDU. The opposite is for PWR. There is no clear document to support the above inference but the real design can be interpreted was made by the above reasoning, but this shows that the design limit is already working in nuclear design process implicitly.

(2) Design Risk Distribution of PWR and CANDU

As already discussed in the above, the design could be made in the way of reducing the number density in certain range of failure frequency and changing the allowable dose limit which needs socio-technical debates. The distribution of risk is more important than the numeric value of Eq. (3). The design risk of the nuclear power plants could be more realistically estimated by weighting the above distribution of the incident density.

$$R(f) = fD(f)n(f) \tag{4}$$

Since the distribution of incident density is made from data of single failure, a new definition for the dual failure is necessary for CANDUs:

$$R_d(f) = \frac{1}{2}(R_s(f) + R_s(f \times F_{shift})) \tag{5}$$

where $R_d(f)$ is the risk of the dual failure, $R_s(f)$ is the risk of single failure, F_{shift} is the failure frequency of the safety system.

The risk distribution of PWR and CANDU for both single and dual failure are presented in Fig. 4. The risk of the PWR (◆) is low in the high failure frequency and the peak of risk occurs near its safety goal: 1.0×10^{-5}/yr. In case of CANDU with single failure criteria (□), the peak risk occurs in $1.\times10^{-5} \leq F < 1.0\times10^{-4}$ /yr. CANDU has lower risk in the high failure frequency but higher risk in the low failure frequency than PWR.

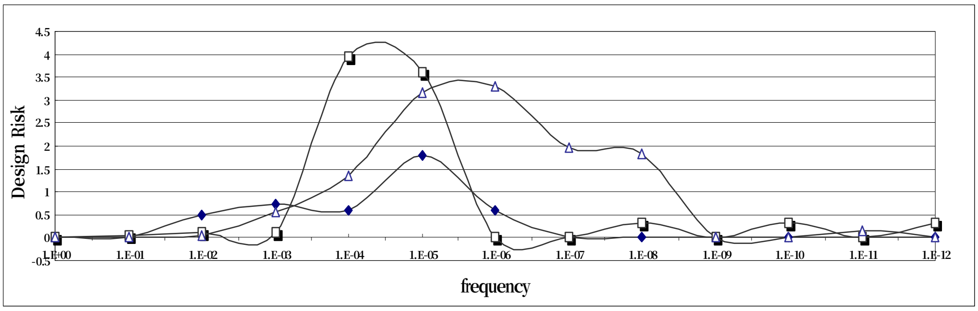

Fig. 4 Comparison of design risk of CANDU and PWR: design risk of PWR, design risk of CANDU with the single failure criteria, and the risk of CANDU with the dual fialure criteria where the failure frequency of the safety system is $1.\times10^{-3}/yr.$

But the peak in risk of CANDU according to dual failure of the safety system(△) is shifting to the left direction, $1.0\times10^{-5} < f < 1.0\times10^{-6}/yr$ Also, the risk of CANDU is lower in the high frequency region and higher in the low frequency region than that of PWR. However, the average risk of both reactors are almost in the same level.

As for the reliability of the specific safety system of a CANDU, the peak of risk occurs at $1.\times10^{-8}$/yr in Figs. 5 and 6. Without this, the risk level of CANDU is, in general, less than that of a PWR in all case. Therefore, when the nuclear industry sets the high level of safety goal such as $1.\times10^{-6}/yr$ CANDU could easily achieve it by slight improvement of the reliability of the safety system. For instance, the improvement of reliability for SDS1 in a CANDU can be easily made by adding the additional electronic channel.

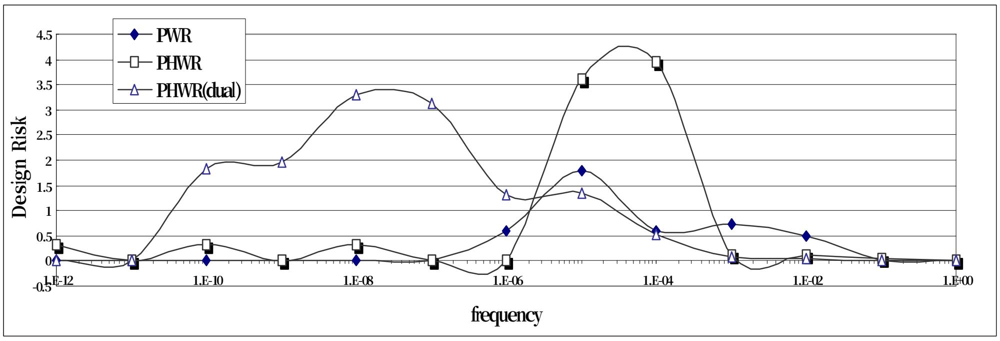

Fig. 5 The comparison of design risk of CANDU and PWR: : design risk of PWR, design risk of CANDU with the single failure criteria, and the risk of CANDU with the dual failure criteria where the failure frequency of the safety system is $1.\times10^{-4}/yr$.

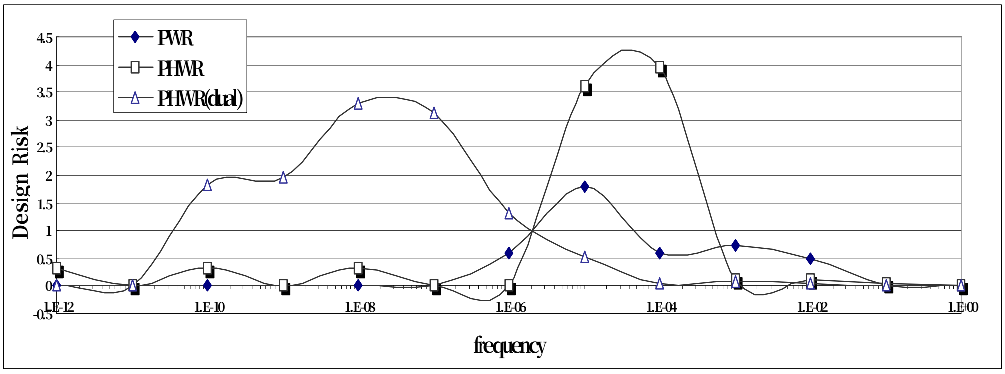

Fig. 6 Comparison of design risk of CANDU and PWR: : design risk of PWR, design risk of CANDU with the single failure criteria, and the risk of CANDU with the dual failure criteria where the failure frequency of the safety system is $1.\times10^{-5}/yr.$

3. Safety Functional Group Analyses

There are three important safety functions required for the nuclear power plant:

(1) Reactor shutdown

(2) Emergency core cooling

(3) Confinement of radiation

A lot of engineering systems have been developed and used in the nuclear power plant for the sake of safety function such as reactor shutdown system, emergency core cooling system (ECCS), containment systems were designed. In the present paper, we categorized systems into the functional group to includes many alternatives for those purposes. The conventional system is made by screening out many alternatives in compliance with the single failure criteria. Unfortunately, the current alternatives screened out produce overwhelmed worry on the safety of the total system. As for a CANDU, it also uses dual safety systems for the same safety function as a PWR. To enhance the safety through diversity and redundancy in a single frame for both CANDU and PWR, there is a need to define the safety functional group including many alternative safety systems avaliable, evaluating effectiveness of individual alternatives, and selection rule.

A. Effectiveness of Safety System

There are many alternatives in satisfying a specific safety function. For instance, the reactor shutdown function could be achieved by the temperature coefficient of reactivity, mechanical injection of poison, hydraulic injection of poison, etc. To identify the member of functional group, the selection rule for member is needed. In the present paper, for selection of members, a method to evaluate the effectiveness of the safety system is developed. For the evaluation of the effectiveness, the ideal action of the safety functional group should be determined. The ideal action could be developed through the simulation using safety code. The safety action is considers as a boundary condition normally as a function of time. The ideal action is determined from the best performance, such as the lowest peak cladding temperature, obtained by changing the safety action program, After generating ideal safety action, the real action of the safety system, which is modelled in the program, can be simulated by the safety code. In Fig.6, the time dependant difference between the ideal action and real action will be obtained:

$$\Delta E = E(t) - E_{ref}(t) \tag{6}$$

The availability of the safety system could be formulated as an entropy, S, from the information theory where the information distortion is measured in the following way using the summation of all error square [3]:

$$S = -k_b \frac{\sum \Delta E^2}{E_{ref}^2} \ln \frac{\sum \Delta E^2}{E_{ref}^2} \tag{7}$$

Assuming that the ideal safety system has a gauss error distribution centered at the average error, the normalization factor follows the ideal system in thermal equilibrium as follows:

$$E_{random} = \frac{3}{2} k_b T \tag{8}$$

Where, E is energy, T is temperature, S is entropy of safety system.

Then the availability of the safety system η_{safe} could be defined as,

$$\eta_{safe} = 1 - \frac{TS}{E_{random}} = 1 - \frac{2}{3k_b} S \tag{9}$$

Inserting Eq.(2) into Eq.(4), the effectiveness of the safety system is obtained as :

$$\eta_{safe} = 1 + \frac{2}{3}\left(\frac{\sum \Delta E^2}{E_{ref}^2} \ln \frac{\sum \Delta E^2}{E_{ref}^2} \cdot \right) \tag{10}$$

If the number of safety systems for a specific safety function is n, the total safety reliability, F_{total}, is defined by multiplying their reliability divided by their effectiveness:

$$F_{total} = \prod \frac{F_i}{\eta_i} h_i \tag{11}$$

where h_i is the heavy side function which represents the membership of safety function in the safety functional group.

$$h_i = \begin{cases} 1 & \textit{selected} \\ 0 & \textit{not selected} \end{cases} \tag{12}$$

This formulation could handle the diversity in the safety systems as well as the single failure criteria. Besides, the natural law likely inherent safety feature, could be evaluated as a kind of safety system. For instance, the negative temperature coefficient could make a reactor shutdown when fuel cooling is malfunctioned. This means that the effectiveness, η, is very low value of ε, but nor zero while the frequency of temperature coefficient failure, $F_{temperature\ coefficeint}$ is 0. Therefore, the failure frequency of safety, F_{safety}, could be;

$$F_{safety} = \frac{F_{temperature\ coefficient}}{\eta_{safety}} = \frac{0}{\varepsilon} = \textit{undefined} \tag{13}$$

Therefore, applying L'hospital's theorem to this case:

$$F_{safety} = \frac{\dfrac{dF_{temp.\ coeff.}}{dF_{temp.\ coeff.}}}{\dfrac{d\eta}{dF_{temp.\ coeff.}}} = \frac{1}{\dfrac{d\eta}{dF_{temp.\ coeff.}}} = \frac{1}{0} = \infty \tag{14}$$

Therefore, to satisfy the safety goal, the designer removes the poor natural law, i.e., negative temperature coefficient, from the safety functional group by setting $h_i = 0$

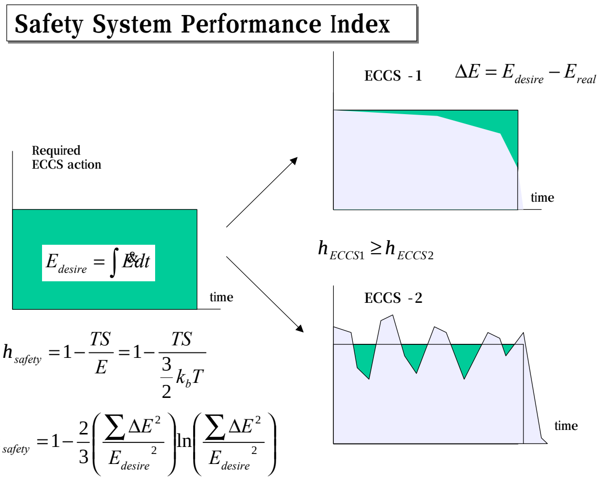
Safety System Performance Index
Required
ECCS action
$E_{desire} = \int \dot{E} dt$
time
$h_{safety} = 1 - \frac{TS}{E} = 1 - \frac{TS}{\frac{3}{2} k_b T}$
$h_{safety} = 1 - \frac{2}{3}\left(\frac{\sum \Delta E^2}{E_{desire}^{\ 2}}\right)\ln\left(\frac{\sum \Delta E^2}{E_{desire}^{\ 2}}\right)$
ECCS -1
$\Delta E = E_{desire} - E_{real}$
time
$h_{ECCS1} \geq h_{ECCS2}$
ECCS -2
time

Fig.7 The conceptual diagram to develop the safety performance index of the individual safety system.

B. Reactor Shutdown Functional Group

CANDU has two separate reactor shutdown systems, such as SDS1 and SDS2. The net positive moderator temperature coefficient of CANDU affects the shutdown system design. In case of PWR, control rod system is only adopted for the reactor shutdown due to the single failure criteria and supportive facts of negative temperature coefficient. Although PWR has the chemical and volume control system (CVCS) similar system to SDS 2 of CANDU, it has no mission of reactor shutdown. In spite of dual safety systems, there is concerns for CANDU because of the positive moderator coefficient. The temperature coefficient of reactivity is very important for the reactor dynamics but it is not enough to shutting reactor down.

Table 1 Alternative safety systems in the reactor shutdown safety functional group

Alternative	Temperature Coefficient	Control Rod	Chemical Shim	Kinetics	
				Life time of the prompt neutron	Effect of the delayed nueutron
PWR	negative	Shutdown system	CVCS	0.03 msec	N/.A
CANDU	positive	SDS1	SDS2	0.9 msec	photo-neutron by gamma ray

It is rational that the safety functional group for the reactor shutdown has temperature insertion of reactivity, mechanical insertion of reactivity, and hydraulic insertion of reactivity. The actuation time and required reactivity for the reactor shutdown could be calculated which could generate the ideal safety actions for each individual safety systems.

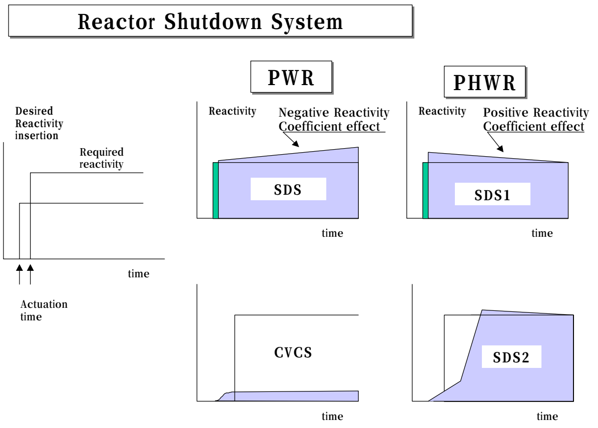

Fig.8 Conceptual drawing of the idealistic and practical actions of reactor shutdown functional group

If the required negative reactivity for reactor shutdown, $\rho_{required}$, is defined as a function of actuation time as follows :

$$\rho_{required} = \rho_r(t_{act}) \tag{15}$$

Then, the difference of reactivity between the necessary value and real value could be identified:

$$\Delta E = \rho_r(t_{act}) - \rho_{system} \tag{16}$$

Therefore, the entropy of the safety system could be determined by inserting the following relation

$$\frac{\Delta E}{E} = 1 - \frac{\rho_{system}}{\rho_r(t_{act})} \tag{17}$$

into Eq. (10). Therefore, the failure frequency of the safety system, F_{safety}, is changed into :

$$F_{safety} = \frac{1}{\eta_{safety}} F_{frequecy} \tag{18}$$

In case of the negative temperature coefficient, the effective failure frequency is undetermined because both denominator and nominator are zero:

$$F_{reactivity\ coefficeint} = \frac{1}{\eta_{safety}} F_{frequency} = \frac{1}{0} \times 0 \tag{19}$$

Applying L'hospital theorem the effective failure frequency diverges to infinite value that means this safety system is always failed.

$$F_{reactivity\ coefficeint} = \frac{1}{d\eta_{safety}} dF_{frequency} = \frac{1}{0} = \infty \tag{20}$$

Consequently, the negative temperature coefficient should be removed form the safety functional group of reactor shutdown. The reactor shutdown system of a PWR has the small effective failure rate for the improvement of reliability in the signal channel:

$$F_{shutdown,pwr} = \frac{1}{\eta_{control}} F_{shutdown} = \frac{1}{1} \times 1. \times 10^{-5} = 1. \times 10^{-5} \tag{21}$$

As summarized in Table 2, the individual safety systems could be evaluated in the same frame of the safety performance index. From this analysis, it is not rational that the CANDU safety system is waker than PWR because of positive temperature coefficient. The temperature insertion of the reactivity is not the safety system for the reactor shutdown any more for both plants.

Table 2 The individual safety systems in the frame of the safety performance index

	Shutdown Rod	Chemical Injection	Temperature Coefficient
Actuation Time	Gravity insertion: $M_{control}\frac{d^2z}{dt^2}=M_{control}g$ Actuation time: $\Delta t_{control}=\sqrt{\frac{2H}{g}}$	Hydraulic injection: $V_{\mathrm{mod}}\frac{dC}{dt}=vAC-D\nabla^2C$ Time constant $\tau_{mix}=\frac{V_{\mathrm{mod}}}{vA}=\frac{C_0}{\rho_l}\frac{M_{\mathrm{mod}}}{W_c}$	Temperature change: $M_{RCS}C_p\frac{dT_{avg}}{dt}=UA(T_{avg}-T_{sat})$ Time constant: PWR: $\tau_{\mathrm{mod}}=\frac{M_{RCS}C_p}{UA}$ CANDU $\tau_{\mathrm{mod}}=\frac{M_{\mathrm{mod}}C_p}{UA}$
PWR Single Failure	RSS : enough value $F_{PWR}=\frac{F_{shutdown}}{\eta_{control}}=\frac{1.\times10^{-5}}{1}$ (effective safety system)	CVCS : less than required value $F_{CVCS}=\frac{dF_{frequency}}{d\eta_{safety}}=\frac{1}{0}=\infty$ (inefficient safety system)	negative: less than required reactivity $F_{RC}=\frac{dF_{frequency}}{d\eta_{safety}}=\frac{1}{0}=\infty$ (inefficient safety system)
CANDU Single Failure	SDS-1 enough value $F_{SDS1}=\frac{F_{shutdown}}{\eta_{control}}=\frac{1.\times10^{-3}}{1}$ (effective safety system)	SDS2 : enough value $F_{SDS2}=\frac{F_{shutdown}}{\eta_{control}}=\frac{1.\times10^{-3}}{1}$ (effective safety system)	positive : $F_{RC}=\frac{dF_{frequency}}{d\eta_{safety}}=\frac{1}{0}=\infty$ (impossible safety system)
CANDU Multiple Failure	$\eta_{SDS1}=\eta_{control}\times\eta_{\mathrm{mod}}=1.0$ $F_{SDS}=F_{SDS1}\times F_{SDS2}=1.0\times10^{-6}/yr$		

C. Emergency Core Cooling Function

The emergency core cooling system of PWR and CANDU has almost same structures. But the reliability goal of ECCS of PWR is higher than CANDU. CANDU has another core cooling through the moderator system which is not categorized as the specific safety system.

As listed in Table 3, the ECC functional group has many alternatives. As noted, the improvement of active system can not be made efficiently in both the technical and economic point of view so that the passive safety injection system is now used in many next generation reactor. But its effectiveness should be evaluated.

The difference between the prepared ideal injection rate and the actual injection rate could produce the efficiency of the safety system as shown in Fig.9. In case of passive ECCS, the gravity injection flow rate shows more oscillation than the active injection system because of its relatively low head. The reliability of the passive safety system would be better than the active system. But the quality of action would be worse than active system.

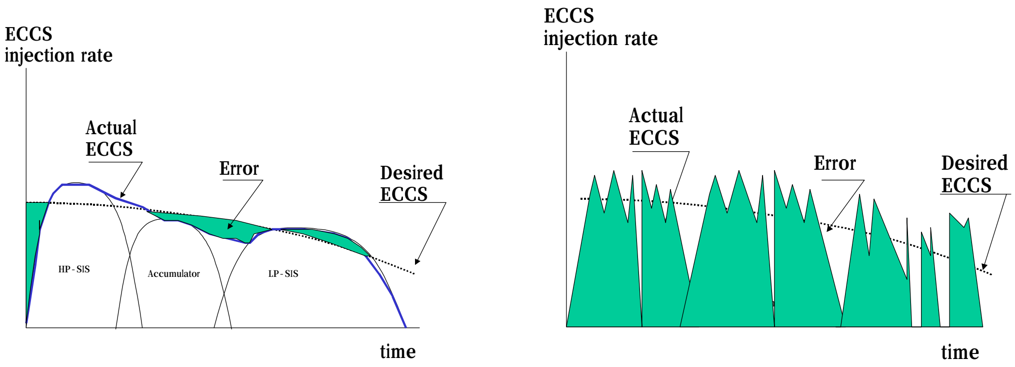

Fig. 9 The quality of injection action of both active and passive system

If the passive injection system has a failure frequency of $1.0\times10^{-6}/yr$ using multi trains and reliable valves , but its frequent oscillation produce its efficiency as 60%, the effective failure frequency of this system would be 1.6×10^{-5}/yr which is almost the same value of the active ECCS system.

As already noted in the reactor shutdown system, the duality of the CANDU core cooling system also evaluated using the same logic. If the active ECCS of CANDU has the failure frequency of $1.0\times10^{-3}/yr$ and the moderator cooling system has 1/3 1/yr. Since both system could function as the core cooling measure, the failure of the core cooling functional group would be $3.3\times10^{-4}/yr$. For CANDUs, diverse design is adopted for core cooling; ECCS for the cooling channel and moderate cooling system for the moderator system. They could improve the reliability of ECCS as the way of PWR. But it is much effective way to improve the moderator cooling system. Recently proposed idea of core catcher and density lock or other passive moderator cooling would be adopted in the moderator system which will provide many ways to improve the safety of CANDU dramatically.

Table 3. The ECC Functional Group

Safety Systems		Effective Failure Frequency	Remarks	
PWR	Active ECCS	$F_{A-PWR}=\frac{F_{A-ECCS}}{\eta_{A-ECCS}}=\frac{1.\times10^{-5}}{1}$	improve	passive
	Passive ECCS	$F_{P-PWR}=\frac{F_{P-ECCS}}{\eta_{P-ECCS}}=\frac{1.\times10^{-6}}{1.\times10^{-1}}=1.\times10^{-5}$	need its availability	
CANDU	Active ECCS	$F_{A-CANDU}=\frac{F_{A-ECCS}}{\eta_{A-ECCS}}=\frac{1.\times10^{-3}}{1}$	improve	$1.\times10^{-4,5}$ (3 line) passive
	Moderator System	$F_{A-CANDU}=\frac{F_{A-MOD}}{\eta_{A-MOD}}=\frac{\frac{1}{3}}{1}=\frac{1}{3}$	improve	reliability core catcher density lock

4. CONCLUSIONS

The present work aims to propose an integrated frame to quantify the safety of different power plants such as PWRs and CANDUs. The design risk proposed is defined to compare the safety of two different reactors. The allowable dose limit and the number density of the failure systems are used to quantify the design risk of both reactors. When the single failure criteria is applied to both plants, PWR is safer than CANDU. But when multiple failure criteria of CANDU is considered, the risk of the CANDU is almost similar to PWR. The slight improvement of the reliability of the safety systems of CANDU promises huge reduction of the design risk.

The single failure criteria of PWR and multi failure criteria of CANDU could be unified by defining the safety functional groups such as the reactor shutdown, emergency core cooling, confinement of radioactive materials. In the present work, a new way is proposed to quantify the efficiency of the individual safety system in the safety functional group, It needs the ideal safety action defined by the regulatory body. The difference between the ideal action and the real action of the specific safety system produces the entropy. The entropy is normalized to produce the efficiency of the safety system. The present method could produce the efficiency of the passive safety system based on natural laws. Also, it could be possible that the safety of the passive system is weaker than the active system. Since the present method enlarge the safety system to the safety functional group, there is no distinguish in single failure criteria and diversity in the safety system. Future works should be made in preparing the ideal safety action. Also, the test using the simulation code to quantify the safety systems efficiency.

REFERENCES

[1] “월성 가압 중수로 계통실무CANDU-PHWR SYSTEM”, 한국원자력 안전기술원(1993)

[2] Wosung NPP234, “Probalistic Safety Assessment (PSA) Report Vol.1 and II”, AECL (1995)

[3] H. Haken, “Synergetics”, Springer Verlag (1983)