Joint Optimization of Business Continuity by Designing Safety Barriers for Accident Prevention, Mitigation and Emergency Responses

Conference Paper · November 2018

DOI: 10.1109/ICSRS.2018.8688845

Zhiguo Zeng
CentraleSupélec
45 PUBLICATIONS 252 CITATIONS

Enrico Zio
Politecnico di Milano
1,014 PUBLICATIONS 14,329 CITATIONS

Joint optimization of business continuity by designing safety barriers for accident prevention, mitigation and emergency responses

Zhiguo Zeng
Chair on System Science and the Energy Challenge,
Fondation Électricité de France (EDF),
CentraleSupélec, Université Paris-Saclay,
3 Rue Joliot Curie, 91190 Gif-sur-Yvette, France
zhiguo.zeng@centralesupelec.fr

Enrico Zio
Chair on System Science and the Energy Challenge,
Fondation Électricité de France (EDF),
CentraleSupélec, Université Paris-Saclay,
3 Rue Joliot Curie, 91190 Gif-sur-Yvette, France;
Energy Department
Politecnico di Milano, 20133, Milano, Italy
enrico.zio@centralesupelec.fr, enrico.zio@polimi.it

***Abstract*—In this paper, an optimization model is developed for optimal design of the safety barriers in a nuclear power plant. By applying the developed model, safety barriers of different natures, *i.e.*, the prevention, mitigation, emergency and recovery measures, can be optimized jointly for business continuity. A hierarchical numerical optimization method based on golden search and genetic algorithm is developed to obtain the optimal solutions. A numerical case study regarding the allocation of resources among the safety barriers prevention, mitigation and emergency in a nuclear power plant is worked out to maximize business continuity against the threat of steam generator tube ruptures.**

***Index Terms*—Safety barrier, business continuity, optimization, condition-based maintenance, redundancy allocation, event tree, nuclear power plant, steam generator tube rupture**

Acronyms

EBCV	Expected Business Continuity Value.
NPP	Nuclear Power Plant.
PWR	Pressurized Water Reactor.
RCS	Reator Cooling System.
RDS	Reactor Depressurization System.
RTS	Reactor Trip System.
RWST	Refueling Water Storage Tank.
SCC	Stress Corrosion Cracking.
SG	Steam Generator.
SGTR	Steam Generator Tube Rupture.

I. Introduction

Business continuity, defined by the International Organization of Standards (ISO) as the capability of an organization to continue delivery of products or services at acceptable levels following disruptive events [1], provides an integrated way to design and manage safety barriers in a plant. In a recent work of the authors, an integrated model is developed for quantitative business continuity analysis [2], which allows calculating the business continuity metrics considering the performances of different safety barriers for accident prevention, mitigation, emergency and recovery [2].

In this paper, we use the integrated business continuity metrics defined in [2] to drive a joint optimization of the prevention, mitigation and emergency safety barriers in a Nuclear Power Plant (NPP), focusing on the Steam Generator Tube Rupture (SGTR) accident. The Steam Generator (SG) is an important system in Nuclear Power Plants, which absorbs the heat generated in the reactor core and generates steam to drive turbines and produce electricity [3]. SGTR occurs when one or more tubes in the SG breaks [3]. As SGTR can lead to accidents with severe consequences like core meltdown, a number of safety barriers are needed to protect the NPP. How to design these safety barriers, so that the normal operation of the NPP can be ensured using a limited budget, is, therefore, an important but challenging problem. Currently, this problem is mainly solved by optimizing each safety barrier individually, in terms of minimizing their failure probabilities. Depending on the different natures of the safety barriers, different optimization models might be used (*c.f.,* condition-based maintenance optimization [4], redundancy optimization [5], *etc.*). These individual optimization models, however, can only guarantee the local optimal performance on the individual safety barrier. To ensure a collectively optimal performances considering all the safety barriers, a joint optimization model needs to be developed based on the business continuity metrics that integrates the effects of all the safety barriers.

II. System description

In this paper, we consider the optimal design of the safety barriers in a NPP against the threat of SGTR. The goal is to minimize the impact of SGTR on the business continuity of the NPP. For simplicity of illustration, let us consider an assumed NPP which contains only one SG. The SG is assumed to be the same type as the one in the Zion Pressurized Water Reactor (PWR) NPP, which contains 3592 inverted U-shaped tubes used for absorbing the heat produced by the reactor core and generating steam that drives the turbines to produce electricity [6].

Since the tubes have thin walls and are operated under high pressures, they are susceptible to spontaneous rupture during operation. If tube rupture occurs in the SG, the reactor core might lose the necessary coolant for cooling it down. If not contained promptly, the SGTR event could evolve and lead to very severe consequences, such as core meltdown [7]. Therefore, safety barriers are needed to protect the NPP from the potential impact of the SGTR. Based on their purposes, these safety barriers can be divided into barriers for prevention, mitigation, emergency and recovery (Sect. II-A-II-C).

A. *Prevention barriers*

Prevention barriers aim at preventing the SGTR from occuring. As $60\% - 80\%$ SGTRs in practice are caused by Stress Corrosion Cracking (SCC) [6], the main prevention barrier against SGTR is to inspect crack lengths periodically and conduct condition-based maintenance based on the results of the inspections. An illustration of a typical SCC growth process is given in Figure 1. Normally, the periodical inspections and condition-based maintenances are conducted during the planned shutdowns of the NPP (*i.e.,* every x months), where x is usually $18 - 24$ months: Eddy current testing is used to measure the crack lengths and once the crack reaches a given threshold (denoted by y_{th}), the associated tube is plugged to prevent the tube rupture from happening [6].

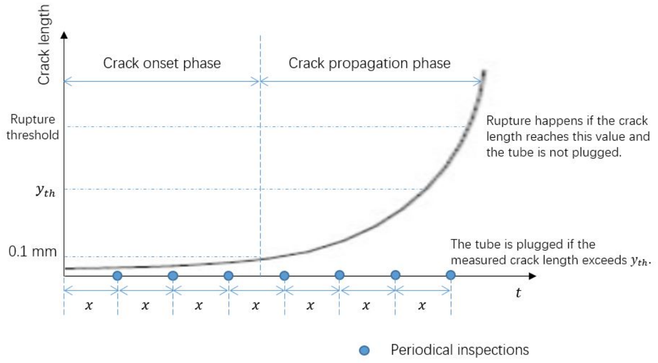

Fig. 1. An illustration of the tube crack growth process

B. *Mitigation and emergency barriers*

Mitigation and emergency barriers serve the purpose of containing the damages caused by an undesirable initiating event (in this case, the tube rupture). In this paper, without loss of generality, let us consider the following mitigation and emergency barriers, which are widely used to protect NPPs in practice:

- Reactor Trip System (RTS), which detects the pressure losses in the primary loop due to the tube rupture and shuts down the reactor within a required time [7];
- Reactor Depressurization System (RDS), which releases the increased pressure inside the reactor core due to the loss of coolant caused by the tube rupture [6];
- Refueling Water Storage Tank (RWST), which provides water to the reactor coolant system for emergency cooling of the reactor core [6];
- Reator Cooling System (RCS), which pumps water into the reactor core for emergency cooling [6].

C. *Recovery barriers*

After the SGTR is successfully contained by the safety barriers, recovery needs to be undertaken to restore normal operation of the NPP. The recovery barrier associated to the SGTR is to replace the affected SG and clear the influence of the leaked nuclear-active materials on the environment. Normally, the recovery process is modelled by a random variable T_{rec}, which represents the time needed for the NPP to get back to normal operations after the accident [2].

III. Business continuity modeling

As defined in Sect. I, business continuity is the capability of an organization to continue delivery of products or services at acceptable levels, following disruptive events [1]. It measures the system's performance under the threat of disruptive events, considering prevention, mitigation, emergency and recovery barriers. A numerical metric, called Expected Business Continuity Value (EBCV), is defined in [2] to quantify the business continuity in a given interval $[0, T]$:

$$\text{EBCV} = 1 - \frac{E\left[L([0,T])\right]}{L_{tol}}, \tag{1}$$

where $E\left[L([0,T])\right]$ is the expected value of the financial losses an organization suffers due to the impact of disruptive events; L_{tol} is the maximal tolerable losses that an organization can suffer before it goes into financial problems (*e.g.,* bankruptcy). The financial loss $L([0,T])$ comprises of the direct loss $L_D([0,T])$, which is directly caused by the disruptive event (*e.g.,* damages of the NPP), and the indirect loss $L_I([0,T])$, which refers to the revenue losses due to the unexpected shutdown of the business caused by the disruptive event. Due to the inherent stochastic nature of disruptive events, $L([0,T])$ is uncertain and is treated as a random variable. As can be seen in Eq. (1), the physical meaning of EBCV is the expected safety margin of an organization to a financially critical state, considering the potential financial losses caused by the disruptive events that could impair its business continuity.

To quantitatively evaluate the EBCV of the NPP, an event tree model is developed first, as shown in Figure 2. It can be seen from the Figure that depending on the performance of the protection, mitigation and emergency measures, three types of consequences might be resulted. Detailed explanations to the consequences are summarized in Table I.

From the event tree model in Figure 2, the occurrence probabilities of the consequences, denoted by p_{C_i}, $i = 1, 2, 3$, can be easily calculated as a function of the event probabilities along the sequences:

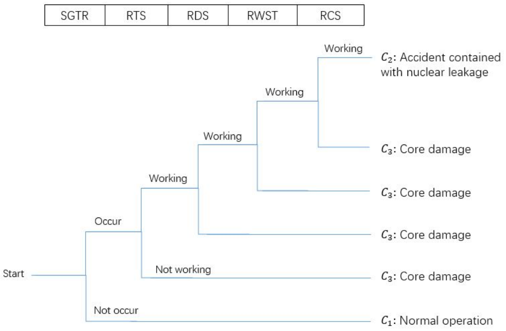

Fig. 2. Event tree model for the SGTR accident (adapted from [6])

TABLE I
CONSEQUENCES FOR THE SGTR

Consequence	Meaning
C_1	No SGTR occurs: the NPP is operating normally.
C_2	SGTR occurs, but the consequence is successfully contained by mitigation and emergency barriers: no core damage occurs, but some nuclear active materials leak to the environment.
C_3	Core damage is caused by the SGTR.

$$p_{C_i} = f_{ET}(p_{SGTR}, p_1, p_2, p_3, p_4),$$

where p_{SGTR} is the probability of rupture of a single tube; p_i, $i = 1, 2, 3, 4$ represent the failure probability of the RTS, RDS, RWST and RCS, respectively.

When consequences C_2 and C_3 occur, the NPP becomes temporarily unavailable for producing electricity, until the recovery barriers successfully restore the normal operation of the NPP. The indirect losses suffered in the recovery process can, therefore, be modelled by:

$$L_{I,C_i} = Q \cdot C \cdot T_{rec,C_i},$$

where L_{I,C_i} denotes the indirect losses in the recovery process of the ith consequence; Q is the unit price for electricity; C is the generation capacity of the NPP; T_{rec,C_i} is a random variable that represents the recovery time for the ith consequence.

Then, the $E\left[L([0,T])\right]$ in Eq. (1) becomes

$$\begin{aligned} E\left[L([0,T])\right] &= \sum_{i=1}^{3} E[L_{C_i}([0,T])] \cdot p_{C_i} \\ &= \sum_{i=1}^{3} E[L_{D,C_i} + L_{I,C_i}] \cdot p_{C_i} \\ &= p_{C_2} \cdot (L_{D,C_2} + Q \cdot C \cdot E[T_{rec,C_2}]) + \\ &\quad\; p_{C_3} \cdot (L_{D,C_3} + Q \cdot C \cdot E[T_{rec,C_3}]). \end{aligned} \tag{2}$$

Then, EBCV can be easily calculated based on Eq. (1).

IV. BUSINESS CONTINUITY GUIDED OPTIMIZATION

A. Model formulation

In this paper, we consider the joint optimization of prevention, mitigation and emergency barriers with the objective of business continuity. The purpose of the prevention measure is to reduce the probability of SGTR. As shown in Figure 1, p_{SGTR} depends on the inspection interval x and the plugging threshold y_{th}. Therefore, x and y_{th} are considered as decision variables that influence the performance of the prevention barriers. The physics-based SCC growth model developed in [6] and [8] is used to relate p_{SGTR} to x and y_{th}. We do not present this model in details due to space limitations. Interested readers can refer to [6] and [8].

The performances of the mitigation and emergency barriers, *i.e.,* the RTS, RDS, RWST and RCS in Figure 2, can be represented by their failure probabilities. Adding redundancies is a common approach used for reducing failure probabilities of mitigation and emergency barriers. In this paper, we assume that parallel redundancy using the same type of system is considered for the four mitigation and emergency safety barriers. It is easy to show that the failure probability of the ith barrier becomes:

$$p_i = (p_{i,b})^{n_i+1}, \tag{3}$$

where $p_{i,b}$ is the failure probability of the ith safety barrier system and n_i is the number of redundant systems added to the original system.

A joint optimization model is set up in Eq. (4) to maximize the business continuity of the NPP against the threat of SGTR, where x is the inspection interval for the tube crack growth process: Eddy current testing is performed every x months to measure the crack lengths for all the tubes; y_{th} is a threshold value for the crack lengths (measured in mm), above which the corresponding tube will be plugged; $n_1, n_2, \cdots, n_4$ are the number of redundant systems for the RTS, RDS, RWST, RCS, respectively.

$$\max \text{ EBCV} = g(x, y_{th}, n_1, n_2, n_3, n_4) \tag{4}$$

$$s.t. \; p_{plug} \leq p_{th}, \tag{5}$$

$$C \leq C_{th}, \tag{6}$$

$$x, n_i \in \mathbb{N}, i = 1, 2, 3, 4, y_{th} \geq 0. \tag{7}$$

The first constraint in the optimization model is the constraint on the maximal allowable number of plugged tubes in a SG. As the number of plugged tubes increases, the heat exchange efficiency of the SG decreases. According to the nuclear regulations, an SG of the type employed in Zion PWR NPP can tolerate up to 30% plugged tubes before a significant reduction in efficiency occurs [6]. Therefore, we set $p_{th} = 0.3$.

The second constraint in the optimization model regards the budget. As discussed in Sect. II, the total cost C covers the cost of improving the prevention barriers, denoted by C_P, and the cost from improving the mitigation and emergency barriers, denoted by C_M:

$$C = C_P + C_M. \tag{8}$$

The cost of the prevention barrier is determined by x and y_{th}:

$$C_P = n_{insp} \cdot C_{insp} + n_{tube} \cdot p_{plug} \cdot C_{plug} \quad (9)$$

$$= \lfloor \frac{T}{x} \rfloor \cdot C_{insp} + n_{tube} \cdot p_{plug} \cdot C_{plug}, \quad (10)$$

where $[0, T]$ is the interval considered for the business continuity analysis; C_{insp} is the price for one inspection; n_{tube} is the number of tubes in the SG; C_{plug} is the unit price for plugging one tube; and p_{plug} is the plugging rate, which further depends on x and y_{th} and needs to be calculated through simulations.

The cost for improving the mitigation and emergency barriers can, then, be calculated by

$$C_M = \sum_{i=1}^{4} C_i \cdot n_i, \quad (11)$$

where C_i is the price of adding one ith safety barrier for redundancy.

B. Model solution

The business continuity optimization model in Eq. (4) is a mixed integral programming model, which is computationally hard to solve directly. In this paper, we propose to use a hierarchical optimization framework for this problem, as shown in Algorithm 1.

```
$c = c_0$;
while current EBCV is not optimal do
    Update $c$;
    Solve the sub-optimization model in Eq. (12) for
    $p^*_{rup,SG}$ and $C^*_P$;
    Solve the sub-optimization model in Eq. (13) for
    EBCV;
end
return c;
```

Algorithm 1: Hierarchial optimization for business continuity

$$\begin{aligned} &\min\ p_{rup,SG} = f(x, y_{th}) \\ &s.t.\ p_{plug} \leq p_{th}, \\ &\qquad C_P \leq c. \end{aligned} \quad (12)$$

$$\begin{aligned} &\max\ \text{EBCV} = h(n_1, n_2, n_3, n_4; p^*_{rup,SG}) \\ &s.t.\ \sum_{i=1}^{4} C_i \cdot n_i \leq C_{th} - C^*_P \end{aligned} \quad (13)$$

By introducing a an auxiliary variable c, which represents the budget limit assigned for improving the prevention measure, the original optimization model can be divided into two sub-optimization models. The sub-optimization model in Eq. (12) corresponds to optimizing the prevention barriers under the current value of c; the sub-optimization model in Eq. (13) optimizes the mitigation (and emergency) barrier using the remaining budget. Algorithm 1 is repeated until an optimal value of c is found that maximizes the EBCV. It can be shown that solving the optimization model using Algorithm 1 is equivalent to solving the original optimization model directly.

Different methods can be used in Algorithm 1 for updating the value of c and solving the two sub-optimization models. In this paper, we use the golden search algorithm to search for the optimal value of c, while using the genetic algorithm for solving the two sub-optimization models. It should be noted that the $p_{rup,SG}$ in Eq. (12) is the probability that there is at least one tube rupture in the SG, and can be calculated from p_{SGTR}:

$$p_{SGTR} = 1 - (1 - p_{SGTR})^{n_{tube}}.$$

V. Results and discussions

In this section, we conduct a numerical case study using the NPP described in Sect. II. The event tree model in Figure 2 is used to analyze the consequences following the SGTR and EBCV is calculated using Eq. (1) and (2). Algorithm 1 is used to solve the optimization model in Eq. (4). The parameter values used in this numerical case study are summarized in Table II.

The result of the optimization is given in Table III. It can be seen from the Table that the optimal design solution requires to do a periodical inspection of the SG every 11 months and plug the tube whose crack length exceeds 18.11 (mm). At the same time, three redundant systems are added to the RDS and RCS, respectively. It can also be seen that in the optimal design plan, most of the budget is spent on the prevention barriers. This can be explained by the fact that the prevention barriers have the highest structural importance (see the event tree in Figure 2). Besides, improving the performance of the prevention barriers requires more investment than the mitigation and emergency barriers (see the comparison between C_{insp} and $C_i, i = 1, 2, 3, 4$ in Table III.)

As a comparison, an individual optimization of the prevention barrier is conducted by investing all the budget C_{th} on the it. The result is also represented in Table III. It can be seen from the comparison that although the individual optimization model can achieve lower SGTR occurrence probability for (0.0049 compared to 0.0089), its EBCV value is lower than the joint optimization model. This is because in the individual optimization model, all the resources are invested on prevention barriers. The mitigation and emergency barriers, however, are neglected and become bottlenecks to the business continuity of the NPP. Using the joint optimization model, on the other hand, can achieve a global optimal solution with higher business continuity by optimal allocation of resources across all the safety barriers.

VI. Conclusions

In this paper, a joint optimization model is developed for allocating resources among prevention, mitigation and emergency barriers to achieve optimal business continuity.

TABLE II
PARAMETER VALUES USED IN THE CASE STUDY

Parameter	Meaning	Value	Source
C	Capacity of the NPP	1100 (MW)	[6]
C_{insp}	Cost for one inspection	500 (k€)	Assumed
C_1	Cost for adding one redundant RTS	20 (k€)	Assumed
C_2	Cost for adding one redundant RDS	10 (k€)	Assumed
C_3	Cost for adding one redundant RWST	30 (k€)	Assumed
C_4	Cost for adding one redundant RCS	10 (k€)	Assumed
C_{plug}	Cost for plugging one tube	4 (k€)	Assumed
C_{th}	Total budget for improving the safe barriers	9000 (k€)	Assumed
L_{tol}	Tolerable loss	5×10^6 (€)	Assumed
L_{D,C_2}	Direct loss for the second consequence	5×10^6 (€)	The value of the SG
L_{D,C_3}	Direct loss for core damage	10^9 (€)	The value of the NPP
$p_{1,b}$	Failure probability of one RTS	0.01	Assumed
$p_{2,b}$	Failure probability of one RDS	0.018	Assumed
$p_{3,b}$	Failure probability of one RWST	2.4×10^{-3}	Assumed
$p_{4,b}$	Failure probability of one RCS	0.056	Assumed
p_{th}	Maximal tolerable plugging rate	0.3	[8]
Q	Unit price for electricity	50 (€/MWh)	[9]
T	Analysis horizon for business continuity	10 (year)	Assumed
T_{rec,C_2}	Recovery time for the second consequence	Lognormal(5.8965, 0.0821) (days)	[10]
T_{rec,C_3}	Recovery time for the core damage	Lognormal(8.2024, 0.0821) (days)	Assumed

TABLE III
OPTIMIZATION RESULTS

	Joint optimization	Prevention measures only
x^*	11 (month)	11 (month)
y^*_{th}	18.11 (mm)	16.31 (mm)
n^*_1	0	0
n^*_2	3	0
n^*_3	0	0
n^*_4	3	0
C_P	8929.5 (k€)	9000 (k€)
$p_{rup,SG}$	0.0089	0.0049
EBCV	0.5239	0.4566

A hierarchical optimization method based on golden search and genetic algorithm is developed for finding the optimal solution. The developed method was applied to design the safety barriers in a NPP against the threat of SGTR. The results of the optimization were compared to those from conventional methods that optimize the different safety barriers individually. The results show that using the joint optimization model leads to globally optimal business continuity. The conventional methods, on the other hand, often end up with local optimums of each individual safety barrier, but the global performance of business continuity is not optimal.

The proposed optimization model can be further improved from two aspects. First, how to treat the uncertainty in the optimization model deserves further investigation. Secondly, to achieve better accuracy in the optimization results, large numbers of samples are needed in the Monte Carlo simulation, which creates a challenge to the computational costs of the optimization method. Hence, more advanced methods can be developed to improve computational efficiency.

REFERENCES

[1] I. O. for Standardization, *Societal Security-business Continuity Management Systems-requirements*. International Organization for Standardization, 2012.

[2] Z. Zeng and E. Zio, “An integrated modeling framework for quantitative business continuity assessment,” *Process Safety and Environmental Protection*, vol. 106, pp. 76–88, 2017.

[3] D. Sui, D. Lu, C. Shang, Y. Wei, and X. Xu, “Investigation on response of hpr1000 under different mitigation strategies after sgtr accident,” *Annals of Nuclear Energy*, vol. 112, pp. 328–336, 2018.

[4] A. Grall, C. Bérenguer, and L. Dieulle, “A condition-based maintenance policy for stochastically deteriorating systems,” *Reliability Engineering & System Safety*, vol. 76, no. 2, pp. 167–180, 2002.

[5] D. W. Coit and A. E. Smith, “Reliability optimization of series-parallel systems using a genetic algorithm,” *IEEE Transactions on reliability*, vol. 45, no. 2, pp. 254–260, 1996.

[6] F. Di Maio, F. Antonello, and E. Zio, “Condition-based probabilistic safety assessment of a spontaneous steam generator tube rupture accident scenario,” *Nuclear Engineering and Design*, vol. 326, pp. 41–54, 2018.

[7] H. Kim, J. T. Kim, and G. Heo, “Prognostics for integrity of steam generator tubes using the general path model,” *Nuclear Engineering and Technology*, vol. 50, no. 1, pp. 88–96, 2018.

[8] R. Lewandowski, *Incorporation of Corrosion Mechanisms into a State-dependent Probabilistic Risk Assessment*. PhD thesis, The Ohio State University, 2013.

[9] S. Borovkova and M. D. Schmeck, “Electricity price modeling with stochastic time change,” *Energy Economics*, vol. 63, pp. 51–65, 2017.

[10] L. Bonavigo and M. De Salve, “Issues for nuclear power plants steam generators,” in *Steam Generator Systems: Operational Reliability and Efficiency*, InTech, 2011.