# Interval-valued importance measures for business continuity management

**Conference Paper** · June 2017

DOI: 10.1201/9781315210469-193



Zhiguo Zeng
CentraleSupélec


Enrico Zio
Politecnico di Milano

*Safety and Reliability – Theory and Applications – Čepin & Briš (Eds)*


# Interval-valued importance measures for business continuity management

Zhiguo Zeng
*Chair on System Science and the Energy Challenge, Fondation Electricite de France (EDF), CentraleSupelec, Universite Paris-Saclay, Paris, France*

Enrico Zio
*Chair on System Science and the Energy Challenge, Fondation Electricite de France (EDF), CentraleSupelec, Universite Paris-Saclay, Paris, France*
*Energy Department, Politecnico di Milano, Milano, Italy*

ABSTRACT: Business Continuity Management (BCM) is a proactive approach to protect business and reduce potential losses caused by disruptive events. Various measures are involved in BCM, (e.g., protection measures, mitigation measures, emergency measures and recovery measures) and ranking their relative importance is fundamental for designing BCM plans. In this paper, we use two importance measures, i.e., business continuity improvement worth and business continuity reduction worth, to compare the importance of different business continuity measures. Confidence intervals of the two importance measures are derived to consider the influence of simulation errors. A case study of an oil tank storage farm from literature is considered.

## 1 INTRODUCTION

As modern systems grow in scales and complexities, they are more and more vulnerable to threats from various disruptive events (Zio, 2016), e.g., unexpected system failures (Hameed, et al., 2016), natural disasters (Meng, et al., 2015), terrorist attacks (Reniers and Audenaert, 2014), etc. How to keep the system in operational states under these threats is a key challenge to system designers and operators. In this context, business continuity is 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 (ISO, 2012).

Various researches have been conducted on this subject. For example, Cerullo and Cerullo (2004) proposed a comprehensive approach to business continuity management, with particular focus on internal and external information security threats. Castillo (2005) surveyed the application of business continuity management to achieve organizational disaster preparedness to various disruptive events at Boeing. Sahebjamnia (2013) proposed a framework to integrate BCM and disaster recovery planning, to ensure that the system would resume and recover its operation in an efficient and effective way. However, these works are mainly based on a qualitative analysis of the major contributors to business continuity, whereas very few works consider the quantitative modeling and analysis of business continuity. In a recent work of the authors (Zeng and Zio, 2016), an integrated model has been developed for quantitative business continuity analysis. It allows calculating the business continuity metrics given information of business continuity measures, i.e., for protection, mitigation, emergency and recovery (Zeng and Zio, 2016).

In this paper, we consider the issue of how to rank the relative importance of different business continuity measures. This is a critical problem in practice, when one wants to design an effective business continuity management plan. Various importance measures exist in risk and reliability, e.g., Birnbaum measures, differential importance measures, Risk Improvement Worth (RIW), Risk Reduction Worth (RRW), etc. (Zio, 2013). Uncertain importance measures are used to consider the uncertainty affecting the importance measures, e.g., due to epistemic uncertainty in the parameters (Baraldi et al. 2009, Modarres 2006). In this paper, we apply the uncertain importance measures on business continuity management. Confidence intervals of the importance measures are used to consider the effect of simulation errors.

The rest of this paper is organized as follows. In Sect. 2, the quantitative business continuity metrics and models are briefly reviewed. The two interval-valued importance measures are defined in Sect. 3. A case study is presented in Sect. 4. Finally, the paper is concluded in Sect. 5.

## 2 BUSINESS CONTINUITY METRICS AND MODELS

In this section, we review the quantitative metrics and models for business continuity developed in Zeng and Zio (2016), which serve as a basis for the importance measures introduced in Section 3.

Business process performance indicators, denoted by $\mathrm{PPI}_B$, are used to measure to which degree the objectives of the business process are satisfied. For example, the $\mathrm{PPI}_B$ of an electric power distribution system can be the fraction of satisfied demands. When disruptive events occur, the $\mathrm{PPI}_B$ drop to some degraded values.

In Zeng and Zio (2016), three quantitative metrics for business continuity have been defined based on the losses caused by the disruptive events, i.e., EBCV, $P_{BI}$ and $P_{BF}$.

Expected Business Continuity Value (EBCV) is defined by

$$\mathrm{EBCV} = E\left[\frac{L_{tol} - L}{L_{tol}}\right], \tag{1}$$

where $L_{tol}$ represents the maximum tolerable losses for an organization and $L$ is a random variable that describes the losses that the organization suffers due to disruptive events in [0, $T$]. Suppose the number of disruptive events in [0, $T$] is $n(T)$, $L$ can be further expressed as

$$L = \sum_{i=1}^{n(T)} \left(L_{D,i} + L_{I,i}\right), \tag{2}$$

where $L_{D,i}$ are the losses caused directly by the disruptive event; $L_{I,i}$ are the revenue losses caused by the system downtime in the recovery process. Usually, it is assumed that $L_{I,i}$ is determined by the length of the recovery time and the severity of the degradation of the $\mathrm{PPI}_B$.:

$$L_{I,k} = k \cdot t_{recv,i} \cdot \left(\mathrm{PPI}_{B,N} - \mathrm{PPI}_{B,i}\right), \tag{3}$$

where $k$ is the loss caused by the disruptive event per unit time per unit $\mathrm{PPI}_B$, $t_{recv,i}$ is the recovery time, $\mathrm{PPI}_{B,N}$ and $\mathrm{PPI}_{B,i}$ are the nominal and degraded performance indicators, respectively.

The physical meaning of EBCV is the relative difference between the average losses caused by the disruptive events and the maximum losses that an organization could stand. It is easy to verify that $\mathrm{EBCV} \in (-\infty, 1]$ and a higher value of EBCV indicates better business continuity. Also, EBCV = 0 is a borderline state: a EBCV less than zero indicates that the organization might have trouble in recovering from the disruptive events.

The second business continuity metric defined in Zeng and Zio (2016) is $\mathrm{P}_{BI}$:

$$P_{BI} = \Pr(L > 0). \tag{4}$$

The metric $\mathrm{P}_{BI}$ is the probability that at least one occurrence of Business Interruption (BI) has been caused by the disruptive event in [0, $T$]. Therefore, $\mathrm{P}_{BI}$ represents the business continuity with respect to the system resistance to the influence of the disruptive event: a lower value of $\mathrm{P}_{BI}$ indicates better business continuity.

The third business continuity metric defined in Zeng and Zio (2016) is $\mathrm{P}_{BF}$:

$$P_{BF} = \Pr(L > L_{tol}). \tag{5}$$

The metric $P_{BF}$ quantifies the probability that a Business Failure (BF) occurs in [0, $T$], i.e., the losses caused by the disruptive events are beyond tolerable. As shown in (5), $P_{BF}$ considers both resistance and recoverability of the system, and a lower value of $P_{BF}$ indicates better business continuity.

To reduce the losses caused by the disruptive events and ensure business continuity, various business continuity measures can be implemented. Generally speaking, these measures can be divided into four categories, i.e.,

- protection measures, which are used for defending the system from the disruptive events and preventing damages to the system. If protection measures succeed, the business process is not interrupted when a disruptive event occurs;
- mitigation measures, which are automatically activated when the protection measures fail and initial damage has been caused by the disruptive events. The aim of the mitigation measures is to contain the evolution of the disruptive events at the early stages of development, so that damages can be mitigated;
- emergency measures, which happen when the mitigation measures fail to contain the damage, and often require significant human intervention;
- recovery measures, which aim at re-establishing normal operation.

Business continuity of a system is, then, determined by these measures. In Zeng and Zio (2016), an integrated framework has been developed for modeling business continuity, as shown in Figure 1. The protection and mitigation measures

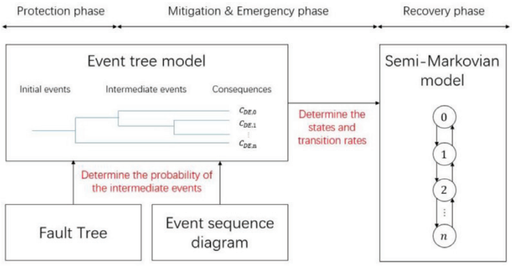



Figure 1. Integrated business continuity model (Zeng and Zio, 2016).

are modeled within a fault tree and event tree logical scheme, the emergency measures are modeled within an event sequence diagram and the recovery measures are modeled by a semi-Markovian model.

## 3 IMPORTANCE MEASURES FOR BUSINESS CONTINUITY

Conceptually, our business continuity model can be represented as

$$[\mathrm{EBCV}, P_{BI}, P_{BF}] = g\left(I_{BCM,1}, I_{BCM,2}, \cdots, I_{BCM,n}\right), \quad (6)$$

where $I_{BCM,1}, I_{BCM,2}, \cdots, I_{BCM,n}$ are the performance indicators for each business continuity measure and the business continuity metrics often need to be calculated using numerical methods, e.g., by Monte Carlo simulations.

In this paper, we apply two importance measures for business continuity management, i.e., Business Continuity Achievement Worth (BCAW) and Business Continuity Reduction Worth (BCRW). Similar to Risk Achievement Worth (Zio et al., 2006), BCAW measures the amount that the business continuity metrics would improve if a business continuity measure could reach its ideal conditions. In this paper, we use the difference between the ideal and nominal scenarios for the evaluation of BCAW:

$$\mathrm{BCAW}_i = M_{BC} \mid I_{BCM,i}^{(Ideal)} - M_{BC}^{(N)}, \quad (7)$$

where $\mathrm{BCAW}_i$ is the BCAW of the $i$th business continuity measure; $M_{BC}$ represents the business continuity metric of interest, e.g., the EBCV, $P_{BI}$ or $P_{BF}$; $M_{BC} \mid I_{BCM,i}^{(Ideal)}$ is the value of $M_{BC}$ when $I_{BCM,i}$ takes its ideal value; $M_{BC}^{(N)}$ is the value of $M_{BC}$ when all the parameters take their nominal values. The meaning of $\mathrm{BCAW}_i$ is the maximum improvement one can achieve by improving the $i$th business continuity measure.

In (7), both $M_{BC} \mid I_{BCM,i}^{(Ideal)}$ and $M_{BC}^{(N)}$ are calculated by Monte Carlo simulations of $N_S$ trials:

$$\widehat{M_{BC} \mid I_{BCM,i}^{(Ideal)}} = \frac{1}{N_S}\sum_{i=1}^{N_S} M_{BC,ideal}^{(i)}, \quad (8)$$

$$\widehat{M_{BC}^{(N)}} = \frac{1}{N_S}\sum_{i=1}^{N_S} M_{BC}^{(i)}, \quad (9)$$

where $\widehat{M_{BC} \mid I_{BCM,i}^{(Ideal)}}$ and $\widehat{M_{BC}^{(N)}}$ are the estimated values of the business continuity metrics, respectively, $N_S$ is the sample size, $M_{BC,ideal}^{(i)}$ and $M_{BC}^{(i)}, i = 1, 2, \cdots, N_S$ are the output of the Monte Carlo simulations.

To account for simulation uncertainties and errors, we use the $(1 - \alpha)$ confidence interval, rather than the point-value estimator, to measure the importance. From Central Limit Theorem (CLT) (Zio, 2013), when $N_S$ is large enough, both $\widehat{M_{BC} \mid I_{BCM,i}^{(Ideal)}}$ and $\widehat{M_{BC}^{(N)}}$ approximately follow normal distributions, whose mean values are their respective true values and the standard deviations, $\sigma_1$ and $\sigma_0$, can be calculated as

$$\sigma_1 = \frac{\sigma_{BC,ideal}}{\sqrt{N_S}}, \qquad \sigma_0 = \frac{\sigma_{BC,N}}{\sqrt{N_S}}, \quad (10)$$

where $\sigma_{BC,ideal}$ and $\sigma_{BC,N}$ are the standard deviations of $M_{BC,ideal}^{(i)}$ and $M_{BC}^{(i)}$, respectively.

When $N_S$ is large, (10) is approximated well using the sample standard deviations $S_1$ and $S_0$:

$$\sigma_1 = \frac{S_1}{\sqrt{N_S}}, \qquad \sigma_0 = \frac{S_0}{\sqrt{N_S}}, \quad (11)$$

where $S_1$ and $S_0$ are calculated by

$$S_1 = \sqrt{\frac{1}{N_S - 1}\sum_{i=1}^{N_S}\left(M_{BC,ideal}^{(i)} - \widehat{M_{BC} \mid I_{BCM,i}^{(Ideal)}}\right)^2}, \qquad S_0 = \sqrt{\frac{1}{N_S - 1}\sum_{i=1}^{N_S}\left(M_{BC}^{(i)} - \widehat{M_{BC}^{i}}\right)^2}. \quad (12)$$

From (7), when $N_S$ is large, the estimator of BCAW from Monte Carlo simulation, denoted by $\widehat{\mathrm{BCAW}_i}$, also follows a normal distribution with an expected value equal to its true value. The standard deviation of $\widehat{\mathrm{BCAW}_i}$ is

$$\sigma_{PE} = \sqrt{\sigma_1^2 + \sigma_0^2} = \sqrt{\frac{S_1^2 + S_0^2}{N_S}}, \quad (13)$$

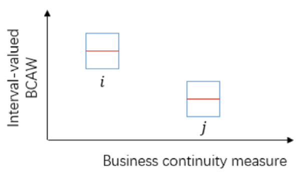
where $\sigma_1$ and $\sigma_0$ are calculated from (11).

The Interval-valued BCAW (IBCAW) is defined as the $(1 - \alpha)$ confidence interval of the Monte Carlo simulation. From (13), IBCAW can be calculated by:

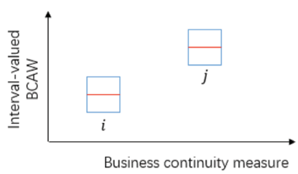
$$\mathrm{IBCAW}_i = \left[ \begin{array}{c} \widehat{\mathrm{BCAW}}_i - Z_{\alpha/2}\sqrt{\dfrac{S_1^2 + S_0^2}{N_S}}, \\ \widehat{\mathrm{BCAW}}_i + Z_{\alpha/2}\sqrt{\dfrac{S_1^2 + S_0^2}{N_S}} \end{array} \right], \tag{14}$$

where $Z_{\alpha/2}$ is the $\alpha/2$ percentile of the standard normal distribution; $S_1$ and $S_0$ are determined from (12).

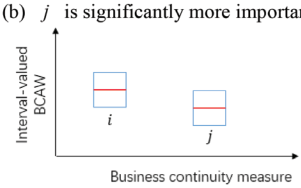
The IBCAW defined in (14) allows comparing the relative importance of business measures while considering the errors in the simulation. An illustration is given in Figure 2, where the box represents the IBCAW and the solid line inside the box indicates the point estimator of the BCAW. Suppose that we have two business continuity measures $i$ and $j$, whose IBCAW do not overlap, as shown in Figure 2 (a) or (b). This means that the improvements in the business continuity metrics are significant enough when compared to the simulation errors. Therefore, we can justifiably conclude that $i$ is more important than $j$ (Figure 2 (a)) or vice versa (Figure 2 (b)). If, on the other hand, $\mathrm{IBCAW}_i$ overlaps with $\mathrm{IBCAW}_j$, as shown in Figure 2 (c), this indicates that we do not have sufficient evidence to differentiate the importance of the two business continuity measures: a larger sample size might be needed for more convicing conclusions.




(a) $i$ is significantly more important than $j$




(b) $j$ is significantly more important than $i$




(c) We cannot fully determine the relative importance of $i$ and $j$

Figure 2. Compare the relative importance using IBCAW.

Similarly, we can define Interval-valued Business Continuity Reduction Worth (IBCRW) as

$$\mathrm{IBCRW}_i = \left[ \begin{array}{c} \widehat{\mathrm{BCRW}}_i - Z_{\alpha/2}\sqrt{\dfrac{S_1^2 + S_0^2}{N_S}}, \\ \widehat{\mathrm{BCRW}}_i + Z_{\alpha/2}\sqrt{\dfrac{S_1^2 + S_0^2}{N_S}} \end{array} \right], \tag{15}$$

where $\widehat{\mathrm{BCRW}}_i$ is the Monte Carlo point estimator of BCRW, which is defined by

$$\mathrm{BCRW}_i = M_{BC}^{(N)} - M_{BC} \mid I_{BCM,i}^{(Worst)}, \tag{16}$$

and $S_1$, $S_0$ in (15) can be determined in a similar way as (12). In (16), $M_{BC} \mid I_{BCM,i}^{(Worst)}$ is the value of $M_{BC}$ when $I_{BCM,i}$ takes its value in the worst-case scenario; $M_{BC}^{(N)}$ is the value of $M_{BC}$ when all the parameters take their nominal values.

The meaning of $\mathrm{BCAW}_i$ is the maximum reduction in business continuity one might experience due to the reduction in the $i$th business continuity measure. The IBCRW defined in (15) allows us to compare the BCRW of business measures, while considering the simulation errors in their calculations.

## 4 APPLICATION

### 4.1 *System description*

In this section, we apply the developed interval-valued importance measures on a case study from literature (Zeng and Zio, 2016). For illustrative purposes, we only present the results for IBCAW since IBCRW can be calculated in a similar way.

Zeng and Zio (2016) considers the business continuity assessment of a crude oil storage tank farm. The disruptive event considered in the analysis is lightning. The performance indicator of the tank farm is the number of available tanks. Several business continuity measures are implemented to protect the system from business disruption:

– lightning protection mast is used to protect the oil storage tank from damages caused by lightning;
– automatic rim seal fire extinguishing system can detect and automatically fight against the rim-seal fire;
– fixed foam fire extinguishing system is automatically activated if the pool fire develops to full

surface fire and aims at extinguishing full surface fires;
- fire brigade is the last defensive barrier to control the fire and prevent it from escalating to other tanks;
- restoring and/or replacing the damaged tanks can help to recover the storage capability of the tank farm.

Among them, lightning protection mast belongs to protection measures, automatic and fixed foam fire extinguishing system are mitigation measures, fire brigade is an emergency measure and restoring and/or replacing the damaged tanks belongs to recovery measures.

An integrated model is developed in Zeng and Zio (2016) to calculate the three quantitative business continuity metrics, as shown in Figure 3, in which the protection and mitigation measures are modeled by a fault tree and an event tree, the emergency measure is modeled by an event sequence diagram and the recovery measures are modeled by a semi-Markovian model. The business continuity metrics, can, then, be calculated using a simulation-based method (Zeng and Zio, 2016).

### 4.2 *Results and discussions*

We consider six performance indicators, $I_{BCM,1}, I_{BCM,2}, \cdots, I_{BCM,6}$, corresponding to different business continuity measures, as shown in Table 1.

Equation (14) is used to calculate the IBCAW for the six business continuity measures. The nominal and ideal values for $I_{BCM,1}, I_{BCM,2}, \cdots, I_{BCM,6}$ are given in Table 2. The sample size of the Monte Carlo simulation is $N_S = 10^6$. The confidence level is $\alpha = 0.1$.

The results are presented in Figure 4-Figure 6. In these Figures, the box represents the upper and lower bounds of the IBCAW, while the solid line inside the box is the point estimator of the BCAW. It can be seen from Figure 4 that if we want to

Table 1. Performance indicators for the business continuity measures.

| Notation | Meaning |
|---|---|
| $I_{BCM,1}$ | Probability that the lightning protection mast successfully defends the lightening. |
| $I_{BCM,2}$ | Failure probability of the automatic rim seal fire extinguishing system. |
| $I_{BCM,3}$ | Failure probability of the fixed foam fire extinguishing system. |
| $I_{BCM,4}$ | Probability that the fire brigade successfully controls the fire. |
| $I_{BCM,5}$ | Expected value of the recovery time for each tank. |
| $I_{BCM,6}$ | Standard deviation of the recovery time for each tank. |

Table 2. Nominal and ideal values for the performance indicators.

| Indicators | Nominal value | Ideal value |
|---|---|---|
| $I_{BCM,1}$ | 0.996 | 1 |
| $I_{BCM,2}$ | $2.38 \times 10^{-2}$ | 0 |
| $I_{BCM,3}$ | $7.03 \times 10^{-3}$ | 0 |
| $I_{BCM,4}$ | 0.693 | 1 |
| $I_{BCM,5}$ | 30 (d) | 5 (d) |
| $I_{BCM,6}$ | 5 (d) | 1 (d) |

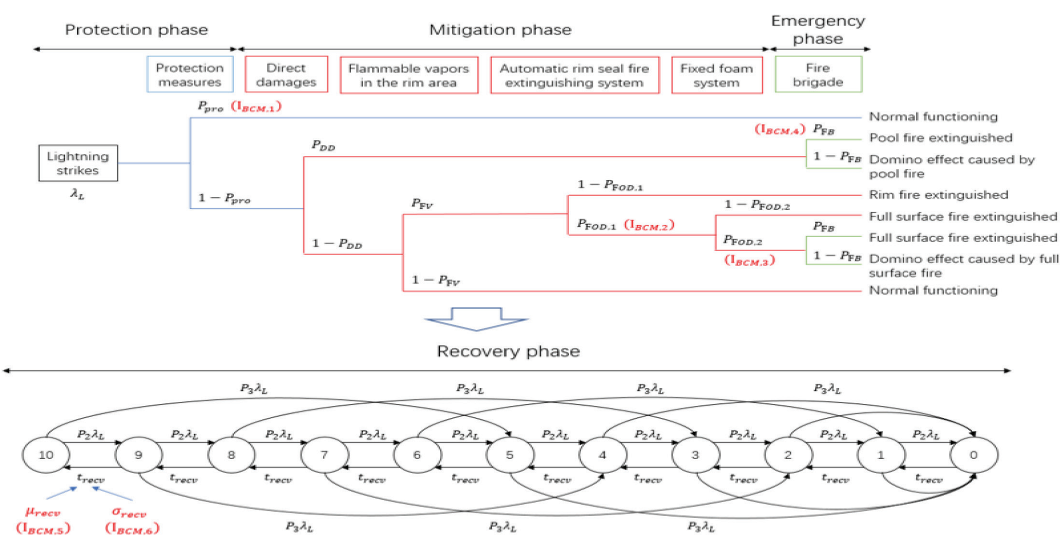



Figure 3. Business continuity model for the tank farm.

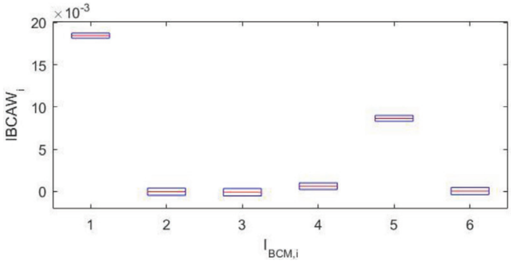



Figure 4. IBCAW of $I_{BCM,1}, I_{BCM,2}, \cdots, I_{BCM,6}$ with respect to EBCV.

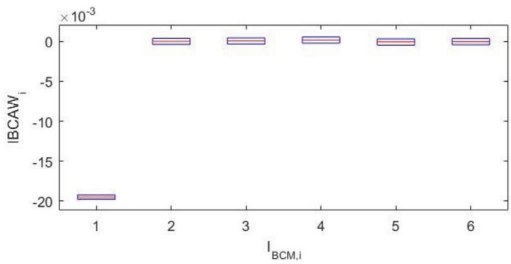



Figure 5. IBCAW of $I_{BCM,1}, I_{BCM,2}, \cdots, I_{BCM,6}$ with respect to $P_{BI}$.

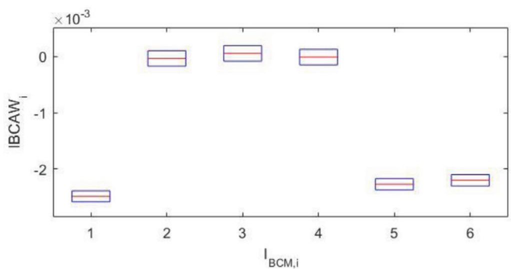



Figure 6. IBCAW of $I_{BCM,1}, I_{BCM,2}, \cdots, I_{BCM,6}$ with respect to $P_{BF}$.

enhance EBCV, the primary focus should be placed on $I_{BCM,1}$, and, then, on $I_{BCM,5}$, since the importance of these two business continuity measures are significantly larger than the others. The IBCAW of $I_{BCM,2}$, $I_{BCM,3}$, $I_{BCM,4}$ and $I_{BCM,6}$ overlap with each other, indicating that we cannot clearly differentiate their relative importance due to the presence of simulation errors. Such conclusions can also be justified from the model in Figure 3. Since $I_{BCM,1}$ relates to the first event in the event tree model, it has dominant influence on the failure of the system, which, according to (2), determines the value of the direct losses. On the other hand, the value of $I_{BCM,5}$ determines the length of the recovery process, which is the major contributor to the indirect losses in (2). Therefore, $I_{BCM,1}$ and $I_{BCM,5}$ exhibit significant importance to EBCV.

Figure 5 shows the IBCAW of different business continuity measures with respect to $P_{BI}$. It can be seen that improving the performance of $I_{BCM,1}$ can significantly improve $P_{BI}$, while the rest IBCAWs overlap with each other, making them indifferent considering the influence of simulation errors. It should be noted that for $P_{BI}$, a BCAW less than zero indicates its improvement. Also, from the definition of $P_{BI}$ in (4), we can see that $P_{BI}$ measures the system capability to resist damage caused by the disruptive events and it is closely related to the protection measures. This explains why the $I_{BCM,1}$, the only protection measure among the six business continuity measures, ranks first in terms of importance with respect to $P_{BI}$, while the other measures do not significantly affect the $P_{BI}$.

Figure 6 shows the IBCAW of different business continuity measures with respect to $P_{BF}$. Since $P_{BF}$ is the probability of business failure, a negative BCAW indicates its improvement. From Figure 6, it can be seen that $I_{BCM,1}, I_{BCM,5}$ and $I_{BCM,6}$ are significantly more important than the other three business continuity measures. This is because $P_{BF}$ is closely related to the direct and indirect losses. As shown in Figure 3, $I_{BCM,1}$ is the major contributor to the direct losses, while $I_{BCM,5}$ and $I_{BCM,6}$ determine the indirect losses. However, the relative importance of $I_{BCM,1}, I_{BCM,5}$ and $I_{BCM,6}$ cannot be differentiated considering the influence of simulation errors, since their IBCAWs overlap.

## 5 CONCLUSIONS

In this paper, we apply two interval-valued importance measures for business continuity management. The importance measures are defined based on confidence intervals of Monte Carlo simulation and allow us to compare the importance of different business continuity measures. A case study from literature is conducted to demonstrate the calculation of the proposed importance measures.

## REFERENCES


Baraldi, P., Zio, E., & Compare, M. (2009). A method for ranking components importance in presence of epistemic uncertainties. Journal of Loss Prevention in the Process Industries, 22(5), 582–592.

Castillo, C. (2005). Disaster preparedness and business continuity planning at Boeing: An integrated model. Journal of Facilities Management, 3(1), 8–26.

Cerullo, V., & Cerullo, M.J. (2004). Business continuity planning: A comprehensive approach. Information Systems Management, 21(3), 70–78.

Hameed, A., Khan, F., & Ahmed, S. (2016). A risk-based shutdown inspection and maintenance interval estimation considering human error. Process Safety and Environmental Protection, 100, 9–21.
International Organization for Standardization (ISO), Societal security – business continuity management systems, 2012.
Modarres, M. (2006). Risk analysis in engineering: techniques, tools, and trends. CRC press. Chicago.
Meng, Y., Lu, C., Yan, Y., Shi, L., & Liu, J. (2015). Method to analyze the regional life loss risk by airborne chemicals released after devastating earthquakes: A simulation approach. Process Safety and Environmental Protection, 94, 366–379.
Rabbani, M., Soufi, H.R., & Torabi, S.A. (2016). Developing a two-step fuzzy cost–benefit analysis for strategies to continuity management and disaster recovery. Safety Science, 85, 9–22.
Reniers, G.L., & Audenaert, A. (2014). Preparing for major terrorist attacks against chemical clusters: Intelligently planning protection measures wrt domino effects. Process Safety and Environmental Protection, 92(6), 583–589.
Snedaker, S. (2013). Business continuity and disaster recovery planning for IT professionals. Newnes.
Zeng, Z., & Zio, E. (2016). An integrated modeling framework for quantitative business continuity assessment. Process Safety and Environmental Protection.
Zio, E. (2016). Challenges in the vulnerability and risk analysis of critical infrastructures. Reliability Engineering & System Safety, 152, 137–150.
Zio, E. (2013). The Monte Carlo simulation method for system reliability and risk analysis. London: Springer.
Zio, E., Podofillini, L., & Zille, V. (2006). A combination of Monte Carlo simulation and cellular automata for computing the availability of complex network systems. Reliability Engineering & System Safety, 91(2), 181–190.