Dynamic Risk Assessment Based on Statistical Failure Data and Condition-Monitoring Degradation Data

Zhiguo Zeng, Enrico Zio

Dynamic risk assessment based on statistical failure data and condition-monitoring degradation data

Zhiguo Zeng and Enrico Zio, *Senior Member, IEEE*

***Abstract*—Traditional Quantitative Risk Assessment (QRA) methods (*e.g.*, event tree analysis) are static in nature, *i.e.*, the risk indexes are assessed before operation, which prevents capturing time-dependent variations as the components and systems operate, age, fail, are repaired and changed. To address this issue, we develop a Dynamic Risk Assessment (DRA) method that allows online estimation of risk indexes using data collected during operation. Two types of data are considered: statistical failure data, which refer to the counts of accidents or near misses from similar systems and condition-monitoring data, which come from online monitoring the degradation of the target system of interest. For this, a hierarchical Bayesian model is developed to compute the reliability of the safety barriers and a Bayesian updating algorithm, which integrates Particle Filtering (PF) with Markov Chain Monte Carlo (MCMC), is developed to update the reliability evaluations based on both the statistical and condition-monitoring data. The updated safety barriers reliabilities, are, then, used in an Event Tree (ET) for consequence analysis and the risk indexes are updated accordingly. A case study on a High-Flow Safety System (HFSS) is conducted to demonstrate the developed methods. A comparison to the DRA method which only uses statistical failure data shows that by introducing condition-monitoring data on the system degradation process, it is possible to capture the system-specific characteristics, and, therefore, provide a more complete and accurate description of the risk of the target system.**

***Index Terms*—Dynamic risk assessment, event tree analysis, hierarchical Bayesian model, condition-monitoring, Particle Filtering (PF), Markov Chain Monte Carlo (MCMC)**

I. Introduction

QUANTITATIVE Risk Assessment (QRA) has been widely applied in various areas [1–3]. Despite of the wide application, traditional QRA methods (*e.g.*, event tree analysis [4]) have been frequently criticized for being "intrinsically static", *i.e.*, the risk indexes are assessed before systems come into operation, and, so, they do not capture the time-dependent variations as components and systems operate, age, fail, are repaired and changed [5]. Dynamic Risk Assessment (DRA) is defined in [6] as a risk assessment method that updates the estimated risk of a deteriorating process according to the performance of the control system, safety barriers, inspection and maintenance activities, the human factors, and the implementation of procedures. Compared to the traditional "static" QRA, DRA is capable of capturing the time-dependent behaviors of the risk indexes and provides a more realistic description of the system risk [3, 5, 6].

Traditionally, DRA methods use only statistical failure data for risk updating, which refer to count data of accidents or near misses from similar systems [7, 8]. A drawback of using only statistical failure data is that, one has to wait for accidents or near misses (precursors) to occur before updating the estimation of the risk indexes. Besides, statistical failure data are collected from similar systems, reflecting population characteristics but not fully accounting for the individual features of the target system. A beneficial complement of statistical failure data is condition-monitoring data, which come from the online monitoring of the system's operational state and degradation process [9]. Condition-monitoring data contain information on the individual degradation process of the target system and, therefore, provide the opportunity to update the reliability values before actual failures occur. Hence, integrating condition-monitoring data with statistical failure data can significantly enhance the effectiveness of DRA.

Statistical failure data and condition-monitoring data have been used separately for DRA but the integration of the two data sources for DRA remains an open issue. To fill this gap, we develop a novel method for DRA that integrates both statistical and condition-monitoring data. The main contribution of the paper can be summarized as follows:

- A hierarchical Bayesian reliability model is developed for incorporating both statistical failure data and condition-monitoring data;
- A hybrid MH/Gibbs algorithm is developed for dynamic reliability assessment;
- A sequential Bayesian method is developed by integrating the two data sources in DRA.

The rest of this paper is organized as follows. The developed DRA method is presented in Section III and applied in Section IV to a high-flow safety alarm system. Finally, the paper is concluded in Section V with a discussion of potential future work.

II. Related works

In this section, we review existing works related to DRA. Based on the data used for DRA, we divide the existing works into two categories: in Sub-Section II-A, we discuss DRA methods using statistical failure data, while in Sub-Section II-B, we focus on DRA methods using condition-monitoring data.

Zhiguo Zeng is a postdoc researcher at Chair on System Science and the Energy Challenge, Fondation Electricite de France (EDF), CentraleSupélec, Université Paris-Saclay, Grande Voie des Vignes, 92290 Chatenay-Malabry, France. Email: zhiguo.zeng@centralesupelec.fr.

Enrico Zio is a professor at Chair on System Science and the Energy Challenge, Fondation Electricite de France (EDF), CentraleSupélec, Université Paris-Saclay, Grande Voie des Vignes, 92290 Chatenay-Malabry, France and Energy Department, Politecnico di Milano, Milano, Italy. Emails: enrico.zio@centralesupelec.fr, enrico.zio@polimi.it.

It should be noted that as [6], the DRA methods discussed in this paper only consider the time-dependent behavior of the failure probability of the safety barriers. The system failure logic, on the contrary, remains static, *i.e.*, does not change over time. For DRA with time-dependent failure logic, readers might refer to dynamic fault tree/event tree analysis (*e.g.*, see [10] and [11]).

A. DRA with statistical failure data

Statistical failure data, also known as Accident Sequence Precursor (ASP) data, refer to count data of accidents or near misses from similar systems [7, 8, 12]. Most existing DRA methods use statistical failure data to update the reliability and risk indexes. For example, an early attempt of DRA was conducted in [7, 8], where Bayes theorem was used to dynamically update the estimates of accident probabilities, using near misses and incident data collected from similar systems. Kalantarnia *et al.* developed a similar DRA method, where Bayes theorem is used for probability updating and Event Tree (ET) analysis is used for consequence modeling [12]. Roy *et al.* used ET to model the accident sequences of an ammonia storage unit and Bayes theorem for DRA [13]. Pariyani *et al.* used ET and Bayes theorem to update the risk in chemical process industries based on data from a large near-miss data base [14]. Khakzad *et al.* developed a hierarchical Bayesian model for DRA and applied it to analyze the near-accident data of offshore blowouts [15]. Yang *et al.* applied a similar hierarchical Bayesian model to dynamically assess the risk of an offshore drilling platform [16].

In [17], Bayes theorem was combined with a Bow-Tie (BT) model for DRA: failure probabilities of the primary events and safety barriers in the BT were constantly revised over time and the updated BT model was used to estimate the updated risk profile. Paltrinieri *et al.* used BT to support the DRA from metal dust accidents [18]. Abimbola *et al.* applied a similar method to update in real time the risk estimation of offshore drilling operations [19]. Khakzad *et al.* developed a DRA method using a Bayesian Network (BN) model, where the probabilities of the basic events in the BN are updated when new accident data are collected [20]. A comparison of the BT-based and BN-based methods were made in [21], and a procedure was given to map a BT into a BN. Li *et al.* considered the DRA for assessing the risk of leakage failure in submarine oil and gas pipelines using BT and BN [22]. In [23], Zarei *et al.* applied the BN in the DRA of a natural gas station.

The DRA methods reviewed above use only statistical failure data for risk updating. As mentioned in Section I, one significant drawback of statistical failure data is that they cannot give alerts prior to the occurrence of accidents, since they are collected at failure. Another issue is that statistical failure data are collected from a population of similar systems, and, therefore, do not fully account for the system-specific features of the target system.

B. DRA with condition-monitoring data

Condition-monitoring data refer to the online-monitoring data related to the system's operational state and degradation processes [9]. In practice, accident initiating events and safety barriers failures usually occur as a result of degradation mechanisms, *e.g.*, wear [24], corrosion [25], fatigue [26], crack growth [27], oxidation [28], etc. These degradation processes can be monitored and failures can be predicted and anticipated with reference to specific thresholds of the monitored variables. Condition-monitoring data contain information on the individual degradation process of the target system and provide the opportunity to update the reliability values before actual failures occur.

There are a few initial attempts of using condition-monitoring data in DRA. For example, Zadakbar *et al.* applied Kalman filtering to estimate the true degradation states from condition-monitoring data and conducted DRA based on a loss function associated with the degradation states [29]. Similar works were also conducted by the same authors using different condition-monitoring techniques, *i.e.*, Particle Filtering (PF) [30] and Principal Component Analysis (PCA) [31]. To deal with nonlinear and non-Gaussian features, Yu *et al.* developed a self-organizing map-based approach for DRA using condition-monitoring data [32]. Wang *et al.* proposed the concept of remaining time and used it to develop a DRA method for multiple condition-monitoring variables [33]. Liu and Zio [34] presented a Bayesian reliability updating method using condition-monitoring data considering the dependencies between two components. Kim *et al.* conducted a DRA by monitoring sensitive variables of a passive residual heat removal system, but without considering the possible noise in the monitored data [9].

Condition-based Fault Tree Analysis (CBFTA) is developed by Shalev and Tiran [35] for DRA, where the failure rates of the basic events are updated using condition-monitoring data, such as vibration, electrical current, etc. Hu *et al.* developed a DRA method based on Dynamic Bayesian Network (DBN), where condition-monitoring data from a process monitoring system are used to update the parameters of the DBN model [36]. Gomes *et al.* applied Kalman filter to predict the Remaining Useful Life (RUL) of the components, and then conduct DRA using a fault tree model [37]. Aizpurua et al. developed a dynamic dependability assessment framework where prognostic capability has been introduced to update the reliabilities of some minimal cut-sequence sets [38]. In [39], a dynamic Bayesian network is constructed for reliability centered maintenance planning, where the conditional probabilities of the nodes are updated based on condition-monitoring data using a Kalman filter.

The works reviewed above use only condition-monitoring data for risk updating, and do not consider statistical failure data. How to integrate condition-monitoring data with statistical failure data, then, remains a challenge for a more informed DRA. To address this issue, we develop a new DRA method. Compared to the existing methods, the developed method integrates statistical failure data and condition-monitoring data for risk model updating, and, therefore, provides a more condition-informed result from the risk assessment. It should be noted that by "integrate", we mean using both statistical failure data and condition-monitoring data to update the initial distribution of the risk index, which is derived based on

historical data. In this context, both condition-monitoring data and statistical failure data serve as evidence, i.e., they should appear in the likelihood function part of the Bayesian updating framework.

III. A NOVEL METHOD FOR DRA

In this section, we develop a new DRA method that considers both statistical and condition-monitoring data. The problem we intend to address in this paper is formally defined in Subsection III-A. A first step in the DRA is to online update the reliability of the safety barriers using the two types of data. For this, a hierarchical Bayesian reliability model is developed in Subsection III-B. Based on the model, an online assessment algorithm is developed for the reliability values of the safety barriers in Subsection III-C and III-D. Finally, a sequential Bayesian algorithm is developed in Subsection III-E to update the risk indexes using the revised reliability values of the safety barriers.

A. Problem definition

Without loss of generality, we consider an ET with n possible consequences $C_1, C_2, \cdots, C_n$, m safety barriers $B_1, B_2, \cdots, B_m$ and an initial event IE. Conceptually, the ET can be expressed as

$$\mathbf{r}_C = g_{\text{ETA}}(R_{B_1}, R_{B_2}, \cdots, R_{B_m} \mid \text{IE}), \tag{1}$$

where R_{B_i} is the reliability of the ith safety barrier and $\mathbf{r}_C = [r_{C_1}, r_{C_2}, \cdots, r_{C_n}]$ is the consequence risk index considered in this paper, which is measured by the conditional occurrence probability of the consequence given that IE has occurred:

$$r_{C_i} = Pr\{C_i \mid \text{IE has occurred}\}, i = 1, 2, \cdots, n. \tag{2}$$

In this paper, we consider the dynamic assessment of the risk indexes as defined in (1), using both statistical failure data and condition-monitoring data. Statistical data refer to the count data of the consequences of accidents that occur during the operation of similar systems, thus providing "population" information, while condition-monitoring data come from online monitoring the degradation of the specific target system of interest and describe system-specific features. More specifically, it is assumed that:

1) statistical failure data and condition-monitoring data are collected at predefined observation instants $t = t_j, j = 1, 2, \cdots, q$;
2) the collected statistical failure data are denoted by $N_{k,j}, k = 1, 2, \cdots, n$, where $N_{k,j}$ denotes the number of the kth consequences that occur in the interval $(t_{j-1}, t_j]$ and $t_0 = 0$;
3) the collected condition-monitoring data on the ith safety barrier at $t = t_j$ are denoted by $y_{i,j}$, $i = 1, 2, \cdots, m$ and $j = 1, 2, \cdots, q$;
4) the degradation threshold for the ith safety barrier is $y_{th,i}$ and failure of the ith safety barrier occurs when $y_{i,j} \leq y_{th,i}$.

The problem of DRA can, then, be defined as: at each $t = t_j, j = 1, 2, \cdots, q$, update the estimation of $\mathbf{r}_C$ in (1), based on statistical failure data $N_{k,j}$ and condition-monitoring data $y_{i,j}$.

B. Hierarchical Bayesian model for safety barrier reliability updating

In this section, a hierarchical Bayesian model is developed for evaluating the reliability of the safety barriers considering both statistical and condition-monitoring data. The model is based on the following assumptions:

1) in each interval $(t_{j-1}, t_j], j = 1, 2, \cdots, q$, the ith safety barrier in the population of similar systems has reliability $\pi_{i,j}$, where $\pi_{i,j}$ is a random variable with prior distribution $p_{0,\pi_{i,j}}$ and posterior distribution $p_{1,\pi_{i,j}}$ and $t_0 = 0$;
2) the prior distribution of $\pi_{i,1}$ is a Beta distribution with parameter α_i and β_i :
$$\pi_{i,1} \sim \text{Beta}(\alpha_i, \beta_i) \tag{3}$$
while for $j \geq 2$, $p_{0,\pi_{i,j}} = p_{1,\pi_{i,j-1}}$;
3) in each interval $(t_{j-1}, t_j], j = 1, 2, \cdots, q$, the reliability of the ith safety barrier in the target system of interest, denoted by $R_{B,i,j}$, is a random variable whose prior distribution is a Beta distribution:
$$R_{B,i,j} \sim \text{Beta}\left(K\pi_{i,j}, K(1-\pi_{i,j})\right), \tag{4}$$
where $\pi_{i,j}$ follows its posterior distribution $p_{1,\pi_{i,j}}$.
4) K is a random variable with uniform prior distribution:
$$K \sim \text{Uniform}(K_L, K_U). \tag{5}$$

From Assumption 1, the statistical count data of occurrence of accidents with given consequences in each interval can be modeled by a binomial probability model:

$$Pr\left\{N_{S,i,j}, N_{F,i,j} \mid \pi_{i,j}\right\} \propto \pi_{i,j}^{N_{S,i,j}} (1-\pi_{i,j})^{N_{F,i,j}}, \tag{6}$$

where $N_{S,i,j}$ and $N_{F,i,j}$ represent the number of successes and failures of the ith safety barrier in $(t_{j-1}, t_j]$, respectively. The detailed procedures for calculating $N_{S,i,j}$ and $N_{F,i,j}$ from the statistical failure data are given in Subsection III-C. The reason for us to choose the binomial model is that the statistical failure data on the safety barriers are of failure-on-demand type [40, 41]. Equation (6) serves as the likelihood function for the statistical failure data. It should be noted that, for simplicity, we drop the constants in the likelihood function, since they do not affect the derivation of posterior distributions in Bayes theorem [42].

According to Assumption 2, at each $t_j, j = 1, 2, \cdots, q$, the prior distribution in (3) can be updated recursively based on Bayesian theorem [41]. Since the likelihood function in (6) is conjugate to the Beta prior in (3), the posterior $p_{1,\pi_{i,j}}$ is also a Beta distribution [41]:

$$\pi_{i,j} \sim \text{Beta}\left(\alpha_i + \sum_{\tau=1}^{j} N_{S,i,\tau}, \beta_i + \sum_{\tau=1}^{j} N_{F,i,\tau}\right). \tag{7}$$

Assumption 3 relates the condition-monitoring data to the statistical failure data. To explain it, note that the mean value of the Beta distribution in (4) is calculated by [41]:

$$E\left[R_{B,i,j}\right] = \frac{K\pi_{i,j}}{K\pi_{i,j} + K(1-\pi_{i,j})} = \pi_{i,j}.$$

Therefore, it is assumed that statistical failure data from similar systems determine the mean value of the reliability of the target system under condition-monitoring. Let $M_{S,i,j}$ and $M_{F,i,j}$ denote the number of successes and failures of the ith safety barrier in $(t_{j-1}, t_j]$, respectively. Assumption 3 also indicates that $M_{S,i,j}$ and $M_{F,i,j}$ can be modeled by a binomial model:

$$Pr\left\{M_{S,i,j}, M_{F,i,j} \mid R_{B,i,j}\right\} \propto R_{B,i,j}^{M_{S,i,j}}(1-R_{B,i,j})^{M_{F,i,j}}. \tag{8}$$

Note that $M_{S,i,j}$ and $M_{F,i,j}$ have to be generated from condition-monitoring data by conducting "pseudo-tests", since in practice, we have only one sample, *i.e.*, that of the target system under condition-monitoring. Detailed procedures of generating $M_{S,i,j}$ and $M_{F,i,j}$ are discussed in details in Subsection III-C. Equation (8) is the likelihood function for the condition-monitoring data. As in (6), the constants in the likelihood function are dropped since they do not affect the derivation of the posterior distributions [41].

As discussed in [41], K can be regarded as the "prior sample size". Let $M = M_{S,i,j} + M_{F,i,j}$ denote the sample size of the pseudo-tests based on the condition-monitoring data. Roughly speaking, the ratio between K and M measures the trust on the statistical failure data compared to the condition-monitoring data: a high value of K/M indicates that one has more trust on the statistical failure data than the condition-monitoring data, and vice versa. In practice, the value of K should be determined based on the value of M to reflect the weight of trust on the two types of data. A detailed discussion on the effect of K is given in Section IV-C. Assumption 4 accounts for the uncertainty in determining the precise value of K.

Some existing works can be found in literature for DRA, e.g., [7], [20], [12], *etc.* These models, however, do not assume a hierarchical structure for the reliability and, therefore, can only be used for modeling statistical failure data. Compared to the existing models, the uniqueness of the developed model is that it proposes a hierarchical Bayesian model, which allows integrating both statistical failure data and condition-monitoring data.

C. Generating pseudo-test data

Pseudo-test data are an important concept in the developed DRA method. They are generated, based on the collected data, (either statistical failure data or condition-monitoring data), to represent the "equivalent" binomial tests and failure data on each safety barrier. In this paper, we distinguish two types of pseudo-tests:

1) Statistical data-based pseudo-tests: Statistical data $(N_{k,j}, k = 1, 2, \cdots, n, j = 1, 2, \cdots, q)$ count the number of occurrences of the consequences in each observation interval. Note that in an ET, observing a certain consequence indicates that the events associated to it have occurred. Since the events correspond to success or failure of the safety barriers, the statistical failure data can be viewed as pseudo-tests on the safety barriers. Take a simple ET in Figure 1 as an example. From Figure 1, we can see that if consequence C_2 occurs, safety barrier B_1 must be working and B_2 must be failed. Therefore, the occurrence of C_2 is equivalent to a pseudo-test on B_1 whose result is success and a pseudo-test on B_2 whose result is failure. The same reasoning applies to the other consequences and safety barriers. Let us define an indicator function $\mathbb{1}(B_i, C_k)$:

$$\mathbb{1}(B_i, C_k) = \begin{cases} 1, \text{ if the occurrence of } C_k \text{ indicates the} \\ \quad \text{success of the } i\text{th safety barrier,} \\ 0, \text{ if the occurrence of } C_k \text{ indicates the} \\ \quad \text{failure of the } i\text{th safety barrier.} \end{cases} \tag{9}$$

The pseudo-test data $N_{S,i,j}$ and $N_{F,i,j}$ can, then, be calculated from $N_{k,j}$:

$$\begin{aligned} N_{S,i,j} &= \sum_{k=1}^{n} \mathbb{1}(B_i, C_k) \cdot N_{k,j}, \\ N_{F,i,j} &= \sum_{k=1}^{n} (1 - \mathbb{1}(B_i, C_k)) \cdot N_{k,j}. \end{aligned} \tag{10}$$

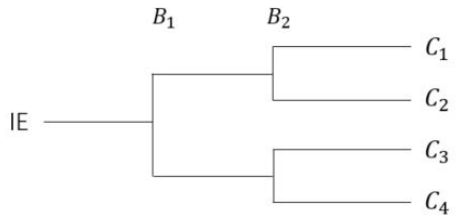


Fig. 1. An illustrative ET

2) Condition-monitoring data-based pseudo-tests: Condition-monitoring data $(y_{i,j}, j = 1, 2, \cdots, q)$ are collected by online-monitoring the degradation process of the ith safety barrier at $t = t_j, j = 1, 2, \cdots, q$. Since condition-monitoring data are often subject to process and observation noises, PF is used in this paper to estimate the true degradation states. PF is chosen for its flexibility and ability to handle complex nonlinear system dynamics and non-Gaussian noises. Although other methods, such as extended Kalman filter and unscented Kalman filter, might also be applied on nonlinear and non-Gaussian problems, they are based on Taylor approximation of a non-linear function. PF, on the other hand, does not require such approximation and fully represent the nonlinear system dynamics.

It is assumed that the degradation process of the ith safety barrier follows a state space model [43]:

$$\begin{cases} \mathbf{x}_{i,j} = g_i\left(\mathbf{x}_{i,j-1}, \epsilon_i\right) \text{ (state equation)}, \\ y_{i,j} = h_i\left(\mathbf{x}_{i,j}, \delta_i\right) \text{ (observation equation)}, \end{cases} \tag{11}$$

where $\mathbf{x}_{i,j}$ is the state variable, $y_{i,j}$ is the observation, ϵ_i is the process noise and δ_i is the observation noise. In PF, the forms of $g_i(\cdot)$ and $h_i(\cdot)$ are assumed to be known and the true system state $\mathbf{x}_{i,j}, j = 1, 2, \cdots, q$ are estimated recursively based on Bayesian theorem [43, 44] (Eq. (13)), where in (13), $p\left(\mathbf{x}_{i,j} \mid y_{i,1}, y_{i,2}, \cdots, y_{i,j}\right)$ is the posterior density for $\mathbf{x}_{i,j}$, updated at $t = t_j$; $p\left(y_{i,j} \mid \mathbf{x}_{i,j}\right)$ is determined by the

observation equation in (11) and $p\left(\mathbf{x}_{i,j} \mid y_{i,1}, y_{i,2}, \cdots, y_{i,j-1}\right)$ is determined based on the output of the PF at $t = t_{j-1}$.

In practice, (13) is evaluated using sequential Monte Carlo simulations: at each t_j, $p\left(\mathbf{x}_{i,j} \mid y_{i,1}, y_{i,2}, \cdots, y_{i,j}\right)$ is approximated by

$$p\left(\mathbf{x}_{i,j} \mid y_{i,1}, y_{i,2}, \cdots, y_{i,j}\right) \approx \sum_{k=1}^{N_P} w_{i,j}^{(k)} \delta\left(\mathbf{x}_{i,j} - \mathbf{x}_{i,j}^{(k)}\right) \quad (12)$$

where $\left\{\mathbf{x}_{i,j}^{(k)}, w_{i,j}^{(k)}\right\}, k = 1, 2, \cdots, N_P$ are the samples (referred to as "particles") and the associated weights generated by sequential importance sampling, and $\delta(\cdot)$ is the Dirac delta function.

It is shown in [43] that if at each $t = t_j$, the particles are generated by

$$\mathbf{x}_{i,j}^{(k)} \sim p(\mathbf{x}_{i,j} \mid \mathbf{x}_{i,j-1}), \quad (14)$$

where $p(\mathbf{x}_{i,j} \mid \mathbf{x}_{i,j-1})$ is the proposal density of the importance sampling and is determined by the state equation in (11), then, the weights can be updated by

$$w_{i,j}^{(k)} = \frac{w_{i,j-1}^{(k)} p\left(y_{i,j} \mid \mathbf{x}_{i,j}^{(k)}\right)}{\sum_{k=1}^{N_P} w_{i,j-1}^{(k)} p\left(y_{i,j} \mid \mathbf{x}_{i,j}^{(k)}\right)}. \quad (15)$$

Algorithm 1 [43] summarizes the major steps of the PF here employed. The purpose of resampling in Algorithm 1 is to avoid the well known problem of particle degeneracy and resampling is often conducted by sampling with replacement from $\left\{\mathbf{x}_{i,j-1}^{(k)}, w_{i,j-1}^{(k)}\right\}_{k=1}^{N_P}$ [45].

Algorithm 1 PF-based estimation of the states of the safety barriers [43]

Inputs: $\left\{\mathbf{x}_{i,j-1}^{(k)}, w_{i,j-1}^{(k)}\right\}_{k=1}^{N_P}, y_{i,j}$
Outputs: $\left\{\mathbf{x}_{i,j}^{(k)}, w_{i,j}^{(k)}\right\}_{k=1}^{N_P}$
for $k = 1 : N_P$ **do**
  Sample $\mathbf{x}_{i,j}^{(k)}$ using (14);
end for
Update $w_{i,j}^{(k)}, k = 1, 2, \cdots, N_P$, using (15);
$\hat{N_{eff}} \leftarrow \left(\sum_{k=1}^{N_P} \left(w_{i,j}^{(k)}\right)^2\right)^{-1}$;
if $\hat{N_{eff}} < N_P/2$ **then**
  Update $\mathbf{x}_{i,j}^{(k)}$ and $w_{i,j}^{(k)}$ by resampling;
end if
return $\left\{\mathbf{x}_{i,j}^{(k)}, w_{i,j}^{(k)}\right\}_{k=1}^{N_P}$.

At each $t = t_j$, the posterior density of $\mathbf{x}_{i,j}$ is approximated by the updated particles and weights from sequential importance sampling. Therefore, the particles can be viewed as pseudo-tests on the reliability of the safety barriers, based on which $M_{S,i,j}$ and $M_{F,i,j}$ can be generated (Algorithm 2).

D. Updating the reliability of the safety barriers

In this section, we discuss how to update the reliability of the safety barriers based on the pseudo-test data generated

Algorithm 2 Generating pseudo-test data based on PF

Inputs: $\left\{\mathbf{x}_{i,j}^{(k)}, w_{i,j}^{(k)}\right\}_{k=1}^{N_P}, y_{i,th}$
Outputs: $M_{S,i,j}$, $M_{F,i,j}$
$M_{S,i,j} = 0$, $M_{F,i,j} = 0$
for $k = 1 : N_P$ **do**
  $\mathbf{x}_{pseudo}^{(k)} \leftarrow$ Randomly select one element from $\left\{\mathbf{x}_{i,j}^{(k)}\right\}_{k=1}^{N_P}$, where $\mathbf{x}_{i,j}^{(k)}$ is selected with probability $w_{i,j}^{(k)}$;
  Calculate $y_{pseudo}^{(k)}$ using the observation equation in (11);
  if $y_{pseudo}^{(k)} > y_{i,th}$ **then**
    $M_{S,i,j} = M_{S,i,j} + 1$;
  else
    $M_{F,i,j} = M_{F,i,j} + 1$;
  end if
end for
return $M_{S,i,j}, M_{F,i,j}$.

in Subsection III-C. The updating is done in two stages. In the first stage, statistical failure data are used to update the reliability of similar systems ($\pi_{i,j}$). As shown in Assumption 2, the prior distribution of $\pi_{i,j}$ and the statistical failure data follow a beta-binomial model [41]. Therefore, the posterior density of $\pi_{i,j}$ can be recursively updated using (7). The updated posterior density is, then, combined with condition-monitoring data in the second stage to update the reliability of the safety barriers ($R_{B,i,j}$).

To do this, first note that $R_{B,i,j}$ is modeled by a hierarchical Bayesian model with a hyper-parameter K (see Assumptions (3) and (4) in Subsection III-B). It should be mentioned that the $\pi_{i,j}$ in (4) is not regarded as a hyper-parameter, but as a random variable with a fixed probability distribution (*i.e.*, $p_{1,\pi_{i,j}}$ yielded by the first stage updating). Based on Bayes theorem [41], the joint posterior density of $R_{B,i,j}$ and K, denoted by $p_1(R_{B,i,j}, K)$, can be expressed as

$$\begin{aligned} p_1(R_{B,i,j}, K) &\triangleq p\left(R_{B,i,j}, K \mid M_{S,i,j}, M_{F,i,j}\right) \\ &\propto p\left(M_{S,i,j}, M_{F,i,j} \mid R_{B,i,j}\right) \cdot \\ &\quad p\left(R_{B,i,j} \mid K\right) \cdot p(K), \end{aligned} \quad (16)$$

where $p\left(M_{S,i,j}, M_{F,i,j} \mid R_{B,i,j}\right)$ is the likelihood function in (8), $p\left(R_{B,i,j} \mid K\right)$ is the prior distribution of $R_{B,i,j}$ in (4), and $p(K)$ is the prior distribution of K in (5). Equation (16) can be further expressed as (20) where $B(\cdot)$ is the Beta function and Δ is a proportional constant.

Due to the complexity of (20), it is hard to derive the analytical form of $p_1(R_{B,i,j}, K)$. Therefore, we use Markov Chain Monte Carlo (MCMC) to generate samples from $p_1(R_{B,i,j}, K)$. For a detailed discussion of MCMC, readers might refer to Chapter 3 in [41]. Note that in this case, if we fix the value of K in (20), we have (21), which indicates that conditioned on K and the data, $R_{B,i,j}$ follows a Beta distribution:

$$\begin{aligned} R_{B,i,j} \mid\ & K, M_{S,i,j}, M_{F,i,j} \\ & \sim \text{Beta}(M_{S,i,j} + K\pi, M_{F,i,j} + K(1-\pi)). \end{aligned} \quad (17)$$

$$p\left(\mathbf{x}_{i,j} \mid y_{i,1}, y_{i,2}, \cdots, y_{i,j}\right) = \frac{p\left(y_{i,j} \mid \mathbf{x}_{i,j}\right) p\left(\mathbf{x}_{i,j} \mid y_{i,1}, y_{i,2}, \cdots, y_{i,j-1}\right)}{\int p\left(y_{i,j} \mid \mathbf{x}_{i,j}\right) p\left(\mathbf{x}_{i,j} \mid y_{i,1}, y_{i,2}, \cdots, y_{i,j-1}\right) d\mathbf{x}_{i,j}}, \tag{13}$$

Therefore, in the MCMC, $R_{B,i,j}$ can be updated using Gibbs sampler based on (17) [41]. On the other hand, if we condition on $R_{B,i,j}$ and the data, we have:

$$p(K \mid R_{B,i,j}, M_{S,i,j}, M_{F,i,j}) \propto R_{B,i,j}^{K\pi} \cdot (1 - R_{B,i,j})^{K(1-\pi)} \cdot \frac{1}{B(K\pi, K(1-\pi))}, \tag{18}$$

which cannot be expressed as any known probability distribution. Therefore, the Metropolis-Hastings (MH) algorithm is used to update K. In this case, we choose the proposal distribution to be a Uniform distribution over $[K_L, K_U]$, *i.e.*, the same as the prior distribution of K. Therefore, the acceptance probability p_{acc} becomes [41]:

$$\begin{aligned} p_{acc} &= \min\left(1, \frac{p(\theta^* \mid data)}{p(\theta^{(l-1)} \mid data)} \frac{f(\theta^{(l-1)} \mid \theta^*)}{f(\theta^* \mid \theta^{(l-1)})}\right) \\ &= \min\left(1, \frac{p\left(K^{(*)} \mid R_{B,i,j}, M_{S,i,j}, M_{F,i,j}\right)}{p\left(K^{(l-1)} \mid R_{B,i,j}, M_{S,i,j}, M_{F,i,j}\right)}\right), \end{aligned} \tag{19}$$

where $f(\cdot \mid \cdot)$ is the proposal density and the ratio in (19) is calculated based on (18).

A hybrid Gibbs/MH algorithm is developed to dynamically update the reliability of the safety barriers, as shown in Algorithm 3, where N_l is the number of the iterations. As l becomes large, $\left\{R^{(l)}, K^{(l)}\right\}$ converge to a random sample from the joint posterior distribution [41]. In practice, the first $N_{burn-in}$ samples are dropped to reduce the correlation between the samples [42]. Therefore, at each $t = t_j$, Algorithm 3 is used to update the reliability of the ith safety barrier and the posterior density of $R_{B,i,j}$ is approximated by $R^{(l)}, l = N_{burn-in} + 1, N_{burn-in} + 2, \cdots, N_l$.

One thing that needs special attention when applying Algorithm 3 is to check the convergence of the MCMC samples. Normally, the MCMC algorithms start from initial values that might be far away from the center of the posterior distribution. As the algorithm iterates, the MCMC samples tend to converge to samples from the posterior distribution. In this paper, we use trace plots for the convergence checks: a stable trace plot indicates good convergence, while a trace plot with significant increasing or decreasing trends means that more iterations are needed for convergence [41]. Some numerical indicators, e.g., autocorrelation coefficient, sample standard deviation of the batch means, potential scale reduction, *etc.*, can also be used to monitor the convergence of the MCMC. For more details, readers might refer to Chapter 3 of [41].

E. A sequential Bayesian updating algorithm for DRA

Once the reliability of the safety barriers are updated, DRA can be done using Algorithm 4. The resulting $\left\{\mathbf{r}_C^{(l)}\right\}_{l=1}^{N_l - N_{burn-in}}$ approximate the posterior distribution of $\mathbf{r}_C$ updated at $t = t_j$. At each $t = t_j, j = 1, 2, \cdots, q$, Algorithm 4 is recursively applied for the DRA.

Algorithm 3 A hybrid Gibbs/MH algorithm to update the reliability of the safety barriers

Inputs: $M_{S,i,j}$, $M_{F,i,j}$, $N_{S,i,j}$, $N_{F,i,j}$
Outputs: $\left\{R^{(l)}, K^{(l)}\right\}_{l=1}^{N_l}$

Set initial values for $R^{(0)}, K^{(0)}, \pi^{(0)}$;
for $l = 1 : N_l$ **do**
  $R^{(l)} \leftarrow$ Generate a random sample from (17), where $K = K^{(l-1)}, \pi = \pi^{(l-1)}$;
  $K^* \leftarrow$ Generate a random sample from the proposal density, *i.e.*, Uniform(K_L, K_U);
  $p_{acc} \leftarrow$ Calculate p_{acc} using (19), where $R_{B,i,j} = R^{(l)}, \pi = \pi^{(l-1)}$;
  $r \leftarrow$ Generate a sample from Uniform$(0, 1)$;
  if $r \leq p_{acc}$ **then**
    $K^{(l)} \leftarrow K^*$;
  else
    $K^{(l)} \leftarrow K^{(l-1)}$;
  end if
  $\pi^{(l)} \leftarrow$ Generate a random sample from (7);
end for
return $\left\{R^{(l)}, K^{(l)}\right\}_{l=1}^{N_l}$.

Algorithm 4 Sequential Bayesian updating for DRA (for $t = t_j$)

for $i = 1 : m$ **do**
  $\{N_{S,i,j}, N_{F,i,j}\} \leftarrow$ Generate pseudo-test data based on statistical failure data, using (10);
  $\left\{\mathbf{x}_{i,j}^{(k)}, w_{i,j}^{(k)}\right\}_{k=1}^{N_P} \leftarrow$ Particle filtering based on condition-monitoring data, using Algorithm 1;
  $\{M_{S,i,j}, M_{F,i,j}\} \leftarrow$ Generate pseudo-test data based on $\left\{\mathbf{x}_{i,j}^{(k)}, w_{i,j}^{(k)}\right\}_{k=1}^{N_P}$, using Algorithm 2;
  $\left\{R_{B,i,j}^{(l)}\right\}_{l=1}^{N_l - N_{burn-in}} \leftarrow$ Update $R_{B,i,j}$ using Algorithm 3;
end for
for $l = N_{burn-in} + 1 : N_l$ **do**
  $R_{B_i} \leftarrow R_{B,i,j}^{(l)}, i = 1, 2, \cdots, n$;
  $\mathbf{r}_C^{(l-N_{burn-in})} \leftarrow$ Calculate the risk indexes using (1);
end for
return $\left\{\mathbf{r}_C^{(l)}\right\}_{l=1}^{N_l - N_{burn-in}}$.

IV. Applications

In this section, we consider the High-Flow Safety System (HFSS) analyzed in [12] as a case study to demonstrate the application of the developed methods. The configuration of the HFSS is introduced first in Subsection IV-A. Then, in Subsection IV-B, pseudo-test data are generated based on statistical failure data and condition-monitoring data, respectively. The reliability of the safety barriers are updated in Subsection IV-C

$$p_1(R_{B,i,j},K)=\begin{cases}0,\ K>K_U \text{ or } K<K_L,\\ \Delta\cdot R_{B,i,j}^{M_{S,i,j}+K\pi-1}\cdot(1-R_{B,i,j})^{M_{F,i,j}+K(1-\pi)-1}\cdot\dfrac{1}{B\left(K\pi,K(1-\pi)\right)}\cdot\dfrac{1}{K_U-K_L}, \text{ otherwise.}\end{cases}\tag{20}$$

$$p\left(R_{B,i,j}\mid K,M_{S,i,j},M_{F,i,j}\right)\propto R_{B,i,j}^{M_{S,i,j}+K\pi-1}\cdot(1-R_{B,i,j})^{M_{F,i,j}+K(1-\pi)-1}.\tag{21}$$

and the results of the DRA for the HFSS are presented in Subsection IV-D.

A. Description of the HFSS

The HFSS is a system installed on a hazardous material storage tank to defend against potential accidents that might be caused by a High-Flow (HF) event, *i.e.*, the flow rate of the input pipeline becomes abnormally high for some reasons [12]. A defense-in-depth strategy is implemented by five safety barriers in the HFSS (Table I): when the HF event occurs, it is detected by the Basic Process Control (BPC) and the Bypass Line (BL) is activated by the BPC to prevent the excess flows from entering the tank. If the BPC does not work properly, the High Level Alarm (HLA) is triggered and an alarm is sent to the operator. The operator can close the Manual Valve (MV) to stop the excess flows. If, by any chance, all the above measures fail, excess flows generate high-pressure vapors in the tank. These vapors can be detected and the Pressure Safety Valve (PSV) will open automatically to reduce the pressure inside the tank.

An ET is constructed in [12] for the HFSS. Depending on the states of the safety barriers, 11 consequences, *i.e.*, $C_1,C_2,\cdots,C_{11}$ can result from an initial HF. These consequences are grouped into three categories based on their severity: normal operation (C_A), overflow of hazardous materials (C_B) and excessively high pressure inside the tank (C_C), where $C_A=C_1\cup C_2\cup C_7, C_B=C_3\cup C_5\cup C_8\cup C_{10}, C_C=C_4\cup C_6\cup C_9\cup C_{11}$. The risk of incursions in the three different consequence categories, can, then, be evaluated as

$$\begin{cases} r_{C_A}=R_1R_2+R_1(1-R_2)R_3R_4+(1-R_1)R_3R_4,\\ r_{C_B}=R_1(1-R_2)R_3(1-R_4)R_5+\\ \qquad (1-R_1)(1-R_3)R_5+\\ \qquad R_1(1-R_2)(1-R_3)R_5+\\ \qquad (1-R_1)R_3(1-R_4)R_5,\\ r_{C_C}=R_1(1-R_2)R_3(1-R_4)(1-R_5)+\\ \qquad R_1(1-R_2)(1-R_3)(1-R_5)+\\ \qquad (1-R_1)(1-R_3)(1-R_5)+\\ \qquad (1-R_1)R_3(1-R_4)(1-R_5).\end{cases}\tag{22}$$

where $R_1,R_2,\cdots,R_5$ represent the reliability of the BPC, BL, HLA, MV and PSV, respectively, and r_{C_i} is defined by (2).

B. Statistical and condition-monitoring data

Statistical data of occurrence of consequences C_A, C_B and C_C, $N_{k,j}, k=A,B,C$, are available from similar HFSS, as tabulated in Table II [12]. The data are collected annually for 10 years, *i.e.*, $t=1,2,\cdots,10$ (years). Pseudo-test data $N_{S,i,j}, N_{F,i,j}, i=1,2,\cdots,5, j=1,2,\cdots,10$ are, then, generated using (10) and listed in Table III.

TABLE II
STATISTICAL DATA FROM SIMILAR SYSTEMS [12]

Year	1	2	3	4	5	6	7	8	9	10
C_1	1	0	0	1	0	1	2	3	1	2
C_2	1	1	0	0	1	0	1	2	2	2
C_3	0	0	1	1	1	0	2	5	2	2
C_4	1	1	1	3	1	1	2	1	1	1
C_5	0	1	0	1	0	2	2	1	1	1
C_6	1	1	1	1	0	2	2	1	1	1
C_7	1	1	1	0	0	2	1	1	1	1
C_8	0	1	1	0	0	1	1	1	1	1
C_9	1	1	1	0	2	2	0	0	1	1
C_{10}	0	1	1	0	0	1	1	1	1	0
C_{11}	1	1	1	1	0	0	0	0	1	1

In this paper, we assume that the failure of the BPC and the HLA are primarily caused by the degradation of the Lithium-ion battery, which provides the needed electrical power for their operation. Typically, degradation of Lithium-ion batteries is measured by its capacity $q(t)$, which is subject to condition-monitoring. For illustrative purposes, we use the real data from CALCE (see [46] and [47] for details) as the condition-monitoring data for the BPC and the HLA. The condition-monitoring data, shown in Fig. 2, are collected in real time by measuring the current of the battery during each charging-discharging cycle. The capacities, are, then, estimated using coulomb counting method [46, 47]. The failure threshold is defined as $y_{th}=0.8$ [46, 47]. Note that to better illustrate the idea of dynamic risk assessment, we transformed the time scales of the condition-monitoring data.

As in [45], the state-space model in (23) is used to characterize the degradation behaviors of the two Lithium-ion batteries. The true degradation states (in terms of mean value and 95% credibility interval) are, then, estimated from the condition-monitoring data using PF (Algorithm 1) and presented in Fig. 2. The number of particles simulated is $N_P=5000$. It should be noted that for both safety barriers, the state variable vector $\mathbf{x}$ in Algorithm 1 contains nine elements, *i.e.*, $p_1,p_2,p_3,p_4,\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_y$, where the first four elements are updated recursively using (23) and the other elements are assumed to be constants (but unknown to us). The initial values for the state variables are drawn uniformly in the intervals of values given in Table IV.

$$\begin{cases} p_{1,t}=p_{1,t-1}+\mathcal{N}(0,\sigma_1^2),\\ p_{2,t}=p_{2,t-1}+\mathcal{N}(0,\sigma_2^2),\\ p_{3,t}=p_{3,t-1}+\mathcal{N}(0,\sigma_3^2),\\ p_{4,t}=p_{4,t-1}+\mathcal{N}(0,\sigma_4^2),\end{cases}$$

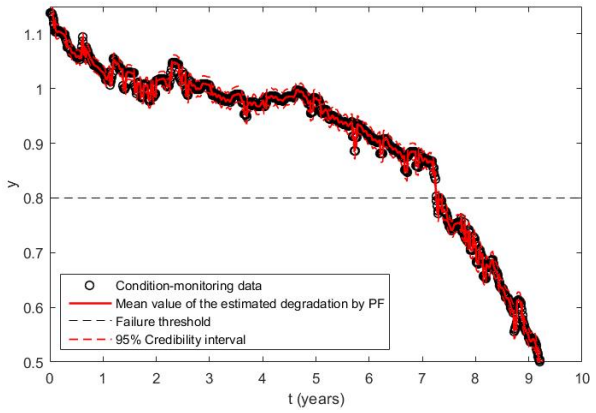
$$y_t=p_{1,t}\exp\left(p_{2,t}\cdot t\right)+p_{3,t}\exp\left(p_{4,t}\cdot t\right)+\mathcal{N}(0,\sigma_y^2).\tag{23}$$

TABLE I
SAFETY BARRIERS IN THE HFSS

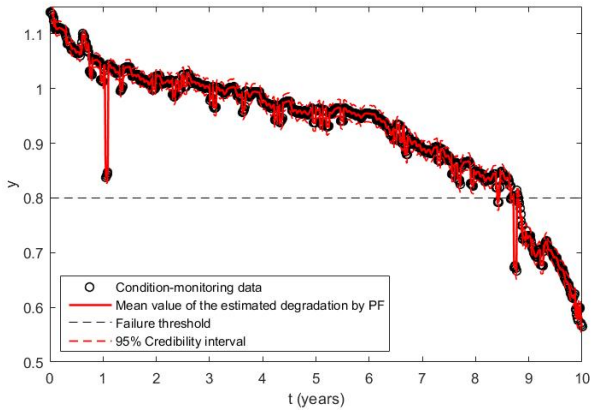
Labels	Safety barriers	Function
SB 1	Basis Process Control (BPC)	• Monitor if the HF occurs; • activate the bypass line to resolve the HF if it occurs.
SB 2	Bypass Line (BL)	Bypass the input materials and prevent them from entering the tank.
SB 3	High Level Alarm (HLA)	Trigger HF alarms to the operator.
SB 4	Manual Valve (MV)	Once closed by the operator, it stops the excessive materials from entering the tank.
SB 5	Pressure Safety Valve (PSV)	• Detect if there is high-pressure vapors in the tank; • if there is, automatically opened to release the high-pressure vapors.

TABLE III
PSEUDO-TEST DATA

Year	$N_{S,1,j}$	$N_{F,1,j}$	$N_{S,2,j}$	$N_{F,2,j}$	$N_{S,3,j}$	$N_{F,3,j}$	$N_{S,4,j}$	$N_{F,4,j}$	$N_{S,5,j}$	$N_{F,5,j}$	$M_{S,1,j}$	$M_{F,1,j}$	$M_{S,3,j}$	$M_{F,3,j}$
1	4	3	1	3	4	2	2	2	0	4	5000	0	5000	0
2	4	5	0	4	5	4	2	3	3	4	5000	0	5000	0
3	3	5	0	3	5	3	1	4	3	4	5000	0	5000	0
4	7	1	1	6	4	3	0	4	2	5	5000	0	5000	0
5	3	2	0	3	5	0	1	4	1	3	5000	0	5000	0
6	6	6	1	5	6	5	2	4	4	5	5000	0	5000	0
7	11	3	2	9	7	5	2	5	6	4	4999	1	5000	0
8	13	3	3	10	10	3	3	7	8	2	1536	3464	4998	2
9	8	5	1	7	8	4	3	5	5	4	0	5000	2036	2964
10	9	4	2	7	8	3	3	5	4	4	0	5000	0	5000



(a) Condition-monitoring data for the BPC



(b) Condition-monitoring data for the HLA

Fig. 2. Condition-monitoring data from [46, 47]

The pseudo-test data $M_{S,i,j}$ and $M_{F,j,j}, i = 1, 2, j = 1, 2, \cdots, 10$, are, then, generated using Algorithm 2, and the results are also given in Table III.

C. Dynamic reliability analysis

In this section, we demonstrate how to proceed with the dynamic reliability analysis method (Algorithm 3) of the BPC. The same procedure is applied to update the reliability of the HLA.

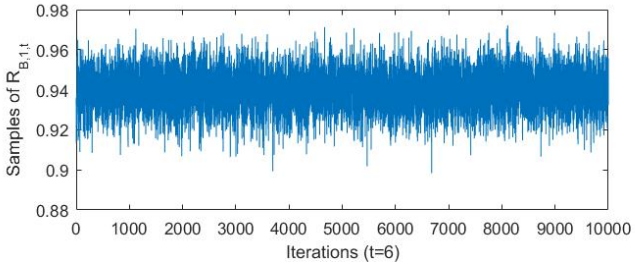
1) Parameter setting and convergence analysis: At each $t = t_j, j = 1, 2, \cdots, 10$ (years), the initial values $R^{(0)}, K^{(0)}, \pi^{(0)}$ are set as the expected values of the corresponding prior distributions:

$$\begin{aligned} R^{(0)} &\leftarrow \frac{\alpha_1 + \sum_{\tau=1}^{j} N_{S,1,\tau}}{\alpha_1 + \sum_{\tau=1}^{j} N_{S,1,\tau} + \beta_1 + \sum_{\tau=1}^{j} N_{F,1,\tau}}, \\ K^{(0)} &\leftarrow \frac{K_U + K_L}{2}, \\ \pi^{(0)} &\leftarrow \frac{\alpha_1 + \sum_{\tau=1}^{j} N_{S,1,\tau}}{\alpha_1 + \sum_{\tau=1}^{j} N_{S,1,\tau} + \beta_1 + \sum_{\tau=1}^{j} N_{F,1,\tau}}. \end{aligned} \tag{24}$$

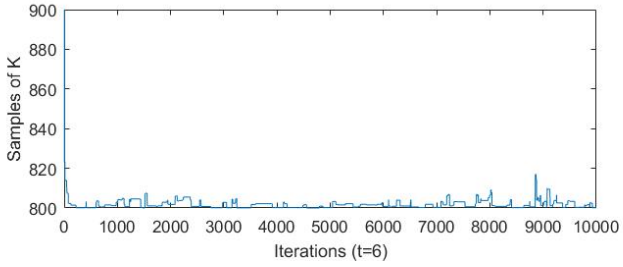
As in [12], we assume that $\alpha_1 = 2.1, \beta_1 = 0.25$. Also, we choose $K_L = 800$ and $K_U = 1000$. Posterior distributions of $R_{B,1,j}$ are generated by $N_l = 10^4$ MCMC samples, where the first $N_{burn-in} = 500$ samples are dropped for burn-in. The convergence of the MCMC is monitored using the trace plots. Normally, the MCMC algorithms are initialized with parameter values that happen to fall far from the center of the posterior distribution, updates obtained early in the chain exhibit a systematic drift toward the region of the parameter space where the posterior distribution is concentrated. Therefore, an increasing or decreasing trend in the parameter values in the trace plot indicates that the burn-in period is not over. When the trace plot stabilizes, the samples converge to the posterior distribution. Due to page limits, we only show the trace plots for $t = 6$ (years) in Fig. 3. It is seen that both $R_{B,1,j}$ and K converge well to their posterior distributions after the "burn-in" period, since both the two trace plots are stable and do not exhibit significant increasing or decreasing tendency.

TABLE IV
INITIAL INTERVALS FOR THE STATE VARIABLES

$p_{1,0}$	$p_{2,0}$	$p_{3,0}$
$[0.85, 1.2]$	$[-1 \times 10^{-3}, 0]$	$[-1 \times 10^{-3}, 0]$
$p_{4,0}$	σ_1	σ_2
$[3 \times 10^{-2}, 0.13]$	$[0.9 \times 10^{-2}, 1.1 \times 10^{-2}]$	$[0.9 \times 10^{-4}, 1.1 \times 10^{-4}]$
σ_3	σ_4	σ_y
$[0.9 \times 10^{-4}, 1.1 \times 10^{-4}]$	$[0.9 \times 10^{-2}, 1.1 \times 10^{-2}]$	$[0.9 \times 10^{-2}, 1.1 \times 10^{-2}]$



a) Trace plot for $R_{B,1,j}$



b) Trace plot for K

Fig. 3. Trace plots at $t = 6$ (years)

2) Results and discussions: The posterior distribution for the reliability of the BPC at each $t = 1, 2, \cdots, 10$ (years) is given in Fig. 4. It can be seen from Fig. 4 that, in general, the reliability degrades as time evolves. In particular, the reliability degrades slowly for $t < 7$ (years) and a dramatic decrease occurs for $7 \leq t \leq 8$ (years). The trend can be more clearly seen by computing the posterior mean of the reliability for each t_j, as shown in Fig. 5. To explain such phenomenon, first note that the posterior distribution is obtained by considering both condition-monitoring data from the target system and statistical failure data from a population of similar systems. For comparison, we compute also the posterior mean of the reliability using only statistical failure data (see [12] for details) and only the condition-monitoring data (see [45] for details), respectively. The results are also shown in Fig. 5. When $t < 7$ (years), it can be seen that the posterior estimates from both statistical failure data and condition-monitoring data are quite stable. Therefore, the estimated posterior reliability is also stable in this region. On the other hand, the estimated posterior reliability remains at relatively high values when compared to that calculated using only statistical failure data. This is because, from Fig. 2, we can see that the condition-monitoring data suggest that the BPC is highly reliable, since the safety margin (distance of the monitored variable from the failure threshold) is relatively large compared with the uncertainties in the estimation, which are represented by the 95% credibility interval in Fig. 2. When $7 \leq t \leq 8$ (years), the condition-monitoring data suggest that the degradation is approaching its threshold and the estimated posterior reliability drops coherently (see Fig. 2).

A further comparison is made in Fig. 6 by showing the posterior densities for $t = 5, 6 \cdots, 10$ (years). It can be seen from the comparison that the posterior reliability estimated by the developed method always lies between the estimates using statistical failure data and condition-monitoring data, only. This shows that the proposed method integrates information from the population of similar systems with the system-specific information contained in the condition-monitoring data. Also, it can be seen from Fig. 6 that at different times, the two data sources have different importance to the estimated reliability. Before $t = 7$ (year), the reliability estimated from condition-monitoring data is close to 1, indicating that it is highly unlikely for the safety barrier to fail due to the degradation process. The reliability estimated by integrating the two data sources, however, is much lower and determined primarily by the statistical failure data. This is because, other than the degradation process, the safety barrier can also fail due to other failure causes, *e.g.*, random shocks. Statistical failure data contain information from a population of similar systems, and, therefore, can capture well such "extra" failure causes. When $t > 7$ (year), the contribution of condition-monitoring data is higher than that of the statistical failure data. This is because, in this range, the safety barrier has already failed due to the degradation process, as suggested by the condition-monitoring data.

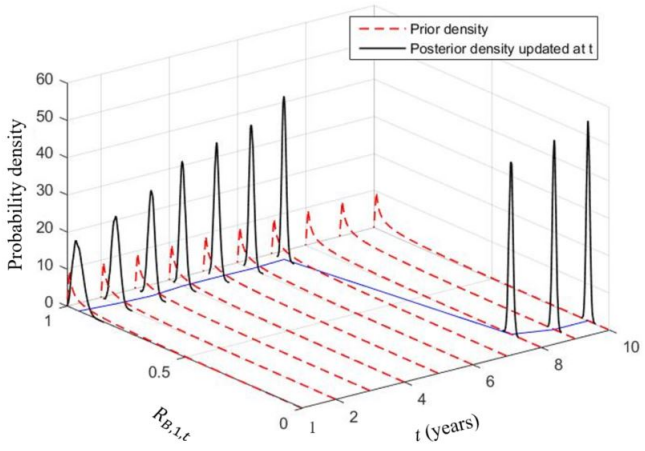


Fig. 4. Updated posterior distributions for the BPC reliability

Figure 7 shows how the initial value of K influences the

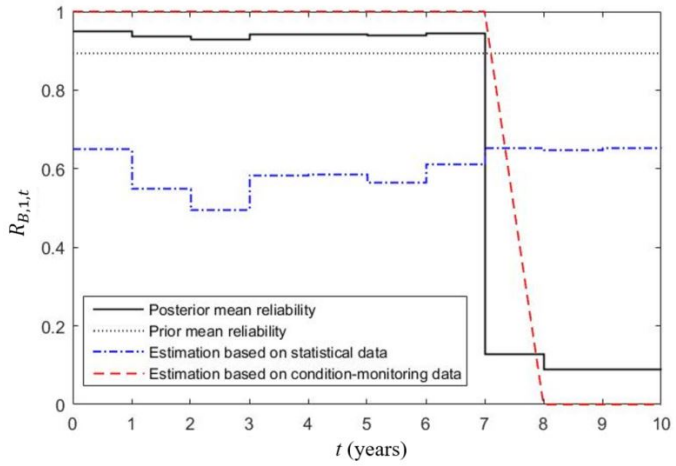


Fig. 5. Updated posterior mean of the BPC reliability

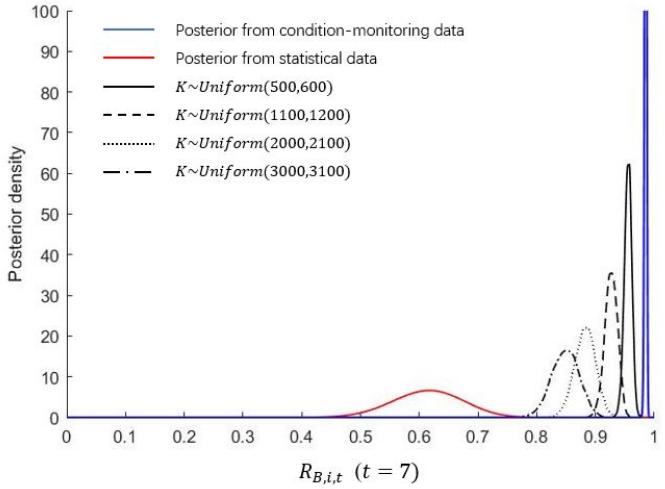


Fig. 7. Posterior distributions under different initial distributions of K

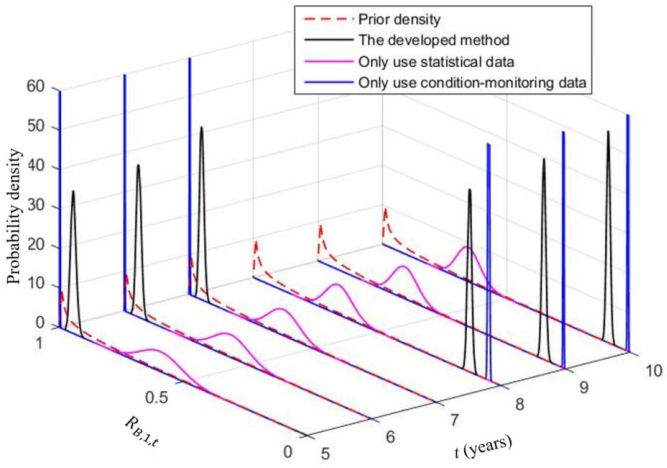


Fig. 6. Comparison of the posterior densities estimated using different data

trust on statistical failure data and condition-monitoring data. In Fig. 7, posterior distributions of the reliability are calculated at $t = 7$ (years) using different initial distributions of K. The pseudo-test sample size from statistical failure data is $N_P = 5000$. It can be seen from Fig. 7 that a larger value of K tends to shift the posterior distribution towards the one yielded by statistical failure data. Therefore, K can be viewed as the "prior sample size" of (4). In practice, the initial interval of K is set based on the assumed trust on the condition-monitoring data when compared to the statistical failure data: if we trust more the condition-monitoring data than the statistical failure data, the values of K_L and K_U should be set to be less than the pseudo-test sample size of the condition-monitoring data (N_P), and vice versa.

D. Dynamic risk assessment (DRA)

DRA of the HFSS is made using Algorithm 4. Note that for safety barriers $2, 4, 5$, we do not have condition-monitoring data. By assuming the beta-binomial model as [12], their reliability can, then, be updated using (7), based on the pseudo-test data $N_{S,i,j}$ and $N_{F,i,j}$ in Table III, $i = 2, 4, 5$. Therefore, the posterior samples for $R_{B,2,j}, R_{B,4,j}$ and $R_{B,5,j}$ can be generated directly from the corresponding posterior distributions from (7). The posterior samples for $R_{B,1,j}$ and $R_{B,3,j}$, on the other hand, are generated following the dynamic reliability analysis procedures discussed in the previous subsection. The prior distributions for $R_{B,1,j}, R_{B,2,j}, \cdots, R_{B,5,j}$ are assumed to take the same values as Table 2 of [12].

The posterior means of the risk indexes, r_{C_A}, r_{C_B} and r_{C_C} are, then, calculated based on (22) and the results are given in Fig. 8. It can be seen from Fig. 8 that, as expected, the conditional probability of C_A, which indicates the normal operation after the occurrence of the high flow event, decreases as time evolves. This is because, in general, the reliability of the five safety barriers are decreasing over time, as suggested by their posterior means in Fig. 9. The risk of accidents, therefore, becomes more severe as the safety barriers age. A closer look at Fig. 8 shows that the variation of the risk indexes can be divided into four ranges:

- A dramatic change of the risk indexes (decrease of r_{C_A} and increase of r_{C_B} and r_{C_C}) occurs in the first range, where $t \leq 5$ (years). As shown in Fig. 9, the dramatic change is caused primarily by the degradation of safety barriers 2 and 4, which affect the risk indexes according to (22).
- When $5 \leq t \leq 7$ (years), the reliability of the safety barriers are relatively stable (see Fig. 9). Therefore, the risk indexes are also stable in this range.
- The risk indexes start changing again from $t = 7$ (years) to $t = 9$ (years). This is primarily caused by, as shown in Fig. 9, the dramatic decrease of the reliability of safety barriers 1 and 3, which, as indicated in Fig. 2, is the result of the degradations reflected in the condition-monitoring data.
- Finally, in the last range when $9 \leq t \leq 10$ (years), both the reliability in Fig. 9 and the risk indexes in Fig. 8 become stable again.

Figure 8 provides a condition-informed online assessment of the risk indexes and can be used to support condition-

informed maintenance planning to reduce the risk of undesirable accident consequences along the life of the system. For example, maintenance interventions might be needed at $t = 5$ (years), since the risk of accident becomes comparable to the conditional probability of normal operation. As our previous discussions show, maintenance on safety barriers 2 and 4 can help to reduce the risk, since the change in this range is primarily caused by these two safety barriers. Also, it can be seen from the DRA that maintenance actions are needed on safety barriers 1 and 3, after $t = 7$ (years), since based on the condition-monitoring data in Fig. 2, the degradation of safety barriers 1 and 3 approaches the threshold and become critical when $t \geq 7$ (years).

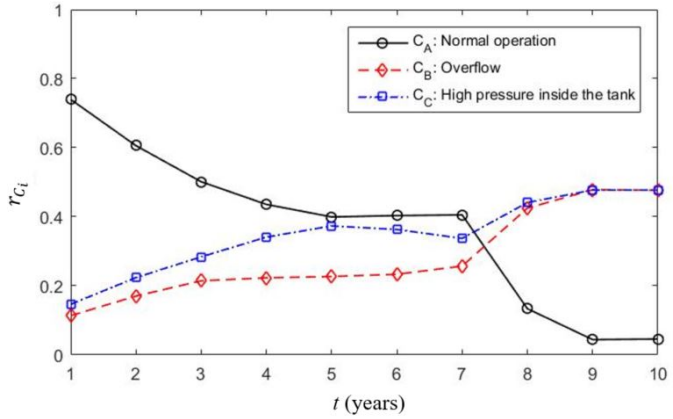


Fig. 8. Posterior means for the risk indexes

A comparison is made between the results obtained by the developed method and those of the DRA method that only considers statistical failure data [12]. By using the method in [12], the reliability of safety barriers 1 and 3 are updated using only the statistical failure data in Table II. It can be seen from Fig. 10 that before $t = 7$ (years), the risk indexes estimated by both methods show the same trend (decrease of r_{C_A} and increase of r_{C_B} and r_{C_C}) but in this region, the risks estimated by the developed method is less severe than that estimated by the method in [12]. This is because, as shown in Fig. 2, the corresponding condition-monitoring data suggest that both the BPC and the HLA have high reliability in this region, since their safety margins are large compared to the uncertainties in their estimates. Having this information, we are more confident that the HFSS can reliably work to reduce the potential risk from an accident.

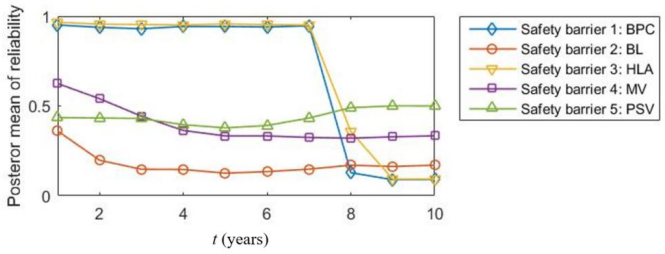
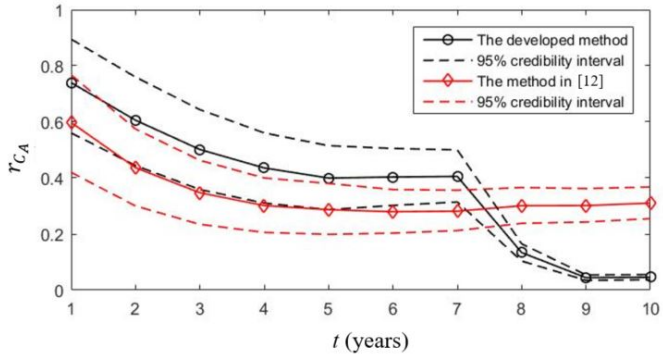
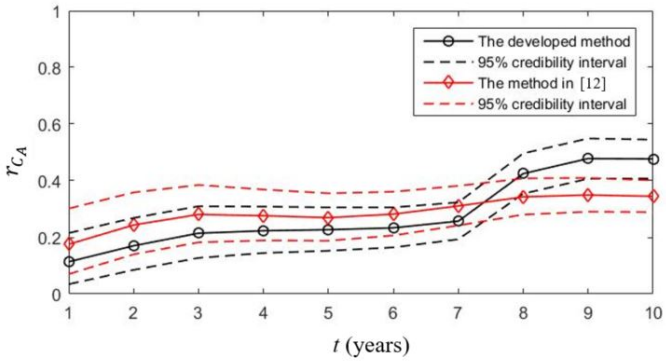


Fig. 9. The mean posterior reliability for the 5 safety barriers

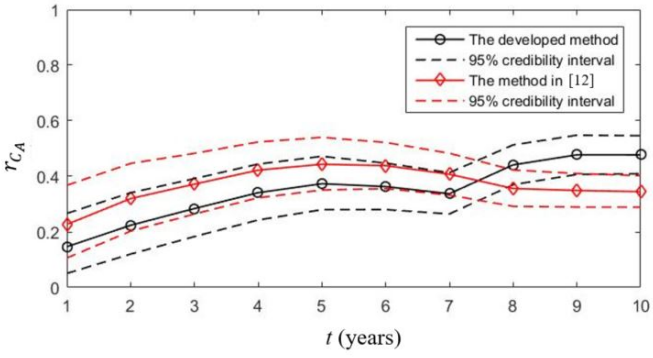
Significant differences between the two methods are observed when $t \geq 7$ (years) in Fig. 10: the developed method suggests that r_{C_A}, the conditional probability of normal operation, begins to decrease from $t > 7$ (years), while the method in [12] suggests that it remains relatively stable. Also, the credibility interval becomes significantly narrower than the one obtained from [12]. The same phenomenon is also observed in r_{C_B} and r_{C_C}. This can be explained by the differences in the posterior reliability values of safety barriers 1 and 3 given by the two methods: as shown in Fig. 5, if we only use the statistical failure data, $R_{B,1,t}$ is relatively stable over the entire range $[0, 10]$ (years); if we introduce the condition-monitoring data in Fig. 2, $R_{B,1,t}$ is stable from $t = 1$ to $t = 7$ (years), while it decreases dramatically when $t > 7$ (years). The same phenomenon can be observed on safety barrier 3, which results in the deviation of the two methods in Fig. 10.



a) Dynamic risk assessment of r_{C_A}



b) Dynamic risk assessment of r_{C_B}



c) Dynamic risk assessment of r_{C_C}

Fig. 10. Comparison to the method in [12]

V. Conclusions

In this paper, we present a newly developed sequential Bayesian algorithm to support DRA using both statistical and condition-monitoring data. The former refer to the count data of accidents or near misses from similar systems and reflect statistical population characteristic while the latter come from realtime monitoring of the degradation process of the target system of interest and reflects the system-specific conditions. In the first stage of the algorithm, condition-monitoring data are treated by a PF and integrated with statistical failure data in a MCMC-based framework to update the reliability of the safety barriers in an ETs. The updated ET is, then, used to revise the estimated risk indexes in the second stage of the algorithm. A case study on a HFSS is conducted to demonstrate the developed methods and a comparison is made to an existing DRA method based only on statistical failure data. The results show that by introducing condition-monitoring data, the developed method is able to capture the system-specific characteristics related to the degradation of the target system, and, therefore, provides a more informed description of the risk of the target system.

Note that in this paper, we have used the PF only to estimate the degradation state of the target system. On the other hand, PF can also be applied to predict the system degradation evolution in the future. Future work is, therefore, to extend the developed method from "risk updating" to "risk prognostics" by predicting the future evolution of the risk indexes using statistical and condition-monitoring data. Also, PF is a model-based method and it requires the availability of physical models to describe the degradation process. Such premise is not always held in practice. In the future, data-driven methods, *e.g.*, support vector machine, artificial neural network, etc., will also be considered for DRA. Besides, importance measures can be defined to quantify the relative importance of different data sources and to determine the required number of data in each source to support risk-informed support decision making.

Acknowledgment

The authors would like to thank Dr. Jie Liu and Miss Jinduo Xing from CentraleSupélec, Université Paris-Saclay for their help in this work. Also, the authors would like to express their deepest gratitude to the three anonymous reviewers, as well as the Associate Editor, Prof. Franz Wotawa, for their insightful comments and suggestions that greatly help us to improve the quality of this paper.

References

[1] E. Zio, *An introduction to the basics of reliability and risk analysis*, vol. 13. World scientific, 2007.

[2] E. Zio, "Some challenges and opportunities in reliability engineering," *IEEE Transactions on Reliability*, vol. 65, no. 4, pp. 1769–1782, 2016.

[3] F. Khan, S. Rathnayaka, and S. Ahmed, "Methods and models in process safety and risk management: Past, present and future," *Process Safety and Environmental Protection*, vol. 98, pp. 116–147, 2015.

[4] J. D. Andrews and S. J. Dunnett, "Event-tree analysis using binary decision diagrams," *IEEE Transactions on Reliability*, vol. 49, no. 2, pp. 230–238, 2000.

[5] V. Villa, N. Paltrinieri, F. Khan, and V. Cozzani, "Towards dynamic risk analysis: A review of the risk assessment approach and its limitations in the chemical process industry," *Safety Science*, vol. 89, pp. 77–93, 2016.

[6] F. Khan, S. J. Hashemi, N. Paltrinieri, P. Amyotte, V. Cozzani, and G. Reniers, "Dynamic risk management: a contemporary approach to process safety management," *Current Opinion in Chemical Engineering*, no. 14, pp. 9–17, 2016.

[7] A. Meel and W. D. Seider, "Real-time risk analysis of safety systems," *Computers & Chemical Engineering*, vol. 32, no. 4-5, pp. 827–840, 2008.

[8] A. Meel and W. D. Seider, "Plant-specific dynamic failure assessment using bayesian theory," *Chemical Engineering Science*, vol. 61, no. 21, pp. 7036–7056, 2006.

[9] H. Kim, S.-H. Lee, J.-S. Park, H. Kim, Y.-S. Chang, and G. Heo, "Reliability data update using condition monitoring and prognostics in probabilistic safety assessment," *Nuclear Engineering and Technology*, vol. 47, no. 2, pp. 204–211, 2015.

[10] M. Čepin and B. Mavko, "A dynamic fault tree," *Reliability Engineering & System Safety*, vol. 75, no. 1, pp. 83–91, 2002.

[11] D. Mercurio, L. Podofillini, E. Zio, and V. Dang, "Identification and classification of dynamic event tree scenarios via possibilistic clustering: application to a steam generator tube rupture event," *Accident Analysis & Prevention*, vol. 41, no. 6, pp. 1180–1191, 2009.

[12] M. Kalantarnia, F. Khan, and K. Hawboldt, "Dynamic risk assessment using failure assessment and bayesian theory," *Journal of Loss Prevention in the Process Industries*, vol. 22, no. 5, pp. 600–606, 2009.

[13] A. Roy, P. Srivastava, and S. Sinha, "Dynamic failure assessment of an ammonia storage unit: A case study," *Process Safety and Environmental Protection*, vol. 94, pp. 385–401, 2015.

[14] A. Pariyani, W. D. Seider, U. G. Oktem, and M. Soroush, "Dynamic risk analysis using alarm databases to improve process safety and product quality: Part iibayesian analysis," *AIChE Journal*, vol. 58, no. 3, pp. 826–841, 2012.

[15] N. Khakzad, F. Khan, and N. Paltrinieri, "On the application of near accident data to risk analysis of major accidents," *Reliability Engineering & System Safety*, vol. 126, pp. 116–125, 2014.

[16] M. Yang, F. I. Khan, and L. Lye, "Precursor-based hierarchical bayesian approach for rare event frequency estimation: A case of oil spill accidents," *Process Safety and Environmental Protection*, vol. 91, no. 5, pp. 333–342, 2013.

[17] N. Khakzad, F. Khan, and P. Amyotte, "Dynamic risk analysis using bow-tie approach," *Reliability Engineering & System Safety*, vol. 104, pp. 36–44, 2012.

[18] N. Paltrinieri, F. Khan, P. Amyotte, and V. Cozzani, "Dynamic approach to risk management: Application to the hoeganaes metal dust accidents," *Process Safety and*

Environmental Protection, vol. 92, no. 6, pp. 669–679, 2014.

[19] M. Abimbola, F. Khan, and N. Khakzad, "Dynamic safety risk analysis of offshore drilling," *Journal of Loss Prevention in the Process Industries*, vol. 30, pp. 74–85, 2014.

[20] N. Khakzad, F. Khan, and P. Amyotte, "Quantitative risk analysis of offshore drilling operations: A bayesian approach," *Safety Science*, vol. 57, pp. 108–117, 2013.

[21] N. Khakzad, F. Khan, and P. Amyotte, "Dynamic safety analysis of process systems by mapping bow-tie into bayesian network," *Process Safety and Environmental Protection*, vol. 91, no. 1-2, pp. 46–53, 2013.

[22] X. Li, G. Chen, and H. Zhu, "Quantitative risk analysis on leakage failure of submarine oil and gas pipelines using bayesian network," *Process Safety and Environmental Protection*, vol. 103, pp. 163–173, 2016.

[23] E. Zarei, A. Azadeh, N. Khakzad, M. M. Aliabadi, and I. Mohammadfam, "Dynamic safety assessment of natural gas stations using bayesian network," *Journal of Hazardous Materials*, vol. 321, pp. 830–840, 2017.

[24] Z. Zeng, R. Kang, and Y. Chen, "Using pof models to predict system reliability considering failure collaboration," *Chinese Journal of Aeronautics*, vol. 29, no. 5, pp. 1294–1301, 2016.

[25] Z. Zeng, Y. Chen, E. Zio, and R. Kang, "A compositional method to model dependent failure behavior based on pof models," *Chinese Journal of Aeronautics*, 2017.

[26] S. Jiang, W. Zhang, J. He, and Z. Wang, "Comparative study between crack closure model and willenborg model for fatigue prediction under overload effects," *Chinese Journal of Aeronautics*, 2016.

[27] P. Baraldi, F. Mangili, and E. Zio, "A kalman filter-based ensemble approach with application to turbine creep prognostics," *IEEE Transactions on Reliability*, vol. 61, no. 4, pp. 966–977, 2012.

[28] M. Compare, F. Martini, S. Mattafirri, F. Carlevaro, and E. Zio, "Semi-markov model for the oxidation degradation mechanism in gas turbine nozzles," *IEEE Transactions on Reliability*, vol. 65, no. 2, pp. 574–581, 2016.

[29] O. Zadakbar, S. Imtiaz, and F. Khan, "Dynamic risk assessment and fault detection using a multivariate technique," *Process Safety Progress*, vol. 32, pp. 365–375, 2013.

[30] O. Zadakbar, F. Khan, and S. Imtiaz, "Dynamic risk assessment of a nonlinear non-gaussian system using a particle filter and detailed consequence analysis," *The Canadian Journal of Chemical Engineering*, vol. 93, no. 7, pp. 1201–1211, 2015.

[31] O. Zadakbar, S. Imtiaz, and F. Khan, "Dynamic risk assessment and fault detection using principal component analysis," *Industrial & Engineering Chemistry Research*, vol. 52, no. 2, pp. 809–816, 2012.

[32] H. Yu, F. Khan, V. Garaniya, and A. Ahmad, "Self-organizing map based fault diagnosis technique for non-gaussian processes," *Industrial & Engineering Chemistry Research*, vol. 53, no. 21, pp. 8831–8843, 2014.

[33] H. Wang, F. Khan, S. Ahmed, and S. Imtiaz, "Dynamic quantitative operational risk assessment of chemical processes," *Chemical Engineering Science*, vol. 142, pp. 62–78, 2016.

[34] J. Liu and E. Zio, "System dynamic reliability assessment and failure prognostics," *Reliability Engineering & System Safety*, vol. 160, pp. 21–36, 2017.

[35] D. M. Shalev and J. Tiran, "Condition-based fault tree analysis (cbfta): A new method for improved fault tree analysis (fta), reliability and safety calculations," *Reliability Engineering & System Safety*, vol. 92, no. 9, pp. 1231–1241, 2007.

[36] J. Hu, L. Zhang, L. Ma, and W. Liang, "An integrated method for safety pre-warning of complex system," *Safety science*, vol. 48, no. 5, pp. 580–597, 2010.

[37] J. P. P. Gomes, L. R. Rodrigues, R. K. H. Galvão, and T. Yoneyama, "System level rul estimation for multiple-component systems," in *Proceedings of the 2013 Annual conference of the prognostics and health management society*, pp. 74–82, 2013.

[38] J. I. Aizpurua, V. M. Catterson, Y. Papadopoulos, F. Chiacchio, and G. Manno, "Improved dynamic dependability assessment through integration with prognostics," *IEEE Transactions on Reliability*, vol. 160, no. 3, pp. 893–913, 2017.

[39] D. Pattison, M. Segovia Garcia, W. Xie, F. Quail, M. Revie, R. Whitfield, and I. Irvine, "Intelligent integrated maintenance for wind power generation," *Wind Energy*, vol. 19, no. 3, pp. 547–562, 2016.

[40] D. L. Kelly and C. L. Smith, "Bayesian inference in probabilistic risk assessmentthe current state of the art," *Reliability Engineering & System Safety*, vol. 94, no. 2, pp. 628–643, 2009.

[41] M. S. Hamada, A. Wilson, C. S. Reese, and H. Martz, *Bayesian reliability*. Springer Science & Business Media, 2008.

[42] D. Kelly and C. Smith, *Bayesian inference for probabilistic risk assessment: a practitioner's guidebook*. Springer Science & Business Media, 2011.

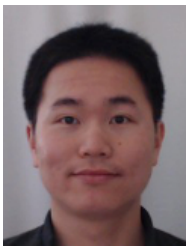
[43] M. S. Arulampalam, S. Maskell, N. Gordon, and T. Clapp, "A tutorial on particle filters for online nonlinear/non-gaussian bayesian tracking," *IEEE Transactions on Signal Processing*, vol. 50, no. 2, pp. 174–188, 2002.

[44] Z. Chen, "Bayesian filtering: From kalman filters to particle filters, and beyond," *Statistics*, vol. 182, no. 1, pp. 1–69, 2003.

[45] Y. Hu, P. Baraldi, F. Di Maio, and E. Zio, "A particle filtering and kernel smoothing-based approach for new design component prognostics," *Reliability Engineering & System Safety*, vol. 134, pp. 19–31, 2015.

[46] W. He, N. Williard, M. Osterman, and M. Pecht, "Prognostics of lithium-ion batteries based on dempster–shafer theory and the bayesian monte carlo method," *Journal of Power Sources*, vol. 196, no. 23, pp. 10314–10321, 2011.

[47] Y. Xing, E. W. Ma, K.-L. Tsui, and M. Pecht, "An ensemble model for predicting the remaining useful performance of lithium-ion batteries," *Microelectronics Reliability*, vol. 53, no. 6, pp. 811–820, 2013.



Zhiguo Zeng Zhiguo Zeng was born in 1989. He received his Bachelor's degree on Quality and Reliability Engineering on 2011 and his Ph.D. degree on Systems Engineering on 2015, both from Beihang university, China. Currently, he is a postdoc researcher at Chair on System Science and the Energy Challenge, Fondation Electricite de France (EDF), CentraleSupélec, Université Paris-Saclay. His researches focus on uncertainty quantification and analysis, belief reliability theory, dynamic risk assessment and business continuity modeling and analysis.

Enrico Zio Enrico Zio (BSc in nuclear engng., Politecnico di Milano, 1991; MSc in mechanical engng., UCLA, 1995; PhD, in nuclear engng., Politecnico di Milano, 1995; PhD, in nuclear engng., MIT, 1998) is Director of the Chair on System Science and the Energy Challenge, Fondation Electricite de France (EDF), CentraleSupélec, Université Paris-Saclay, full professor, President and Rector's delegate of the Alumni Association and past-Director of the Graduate School at Politecnico di Milano. He was the Chairman of the European Safety and Reliability Association ESRA (2010-2014), member of the scientific committee of the Accidental Risks Department of the French National Institute for Industrial Environment and Risks, member of the Korean Nuclear society and China Prognostics and Health Management society, and past-Chairman of the Italian Chapter of the IEEE Reliability Society. He was an Associate Editor of IEEE Transactions on Reliability and editorial board member in various international scientific journals, among which Reliability Engineering and System Safety, Journal of Risk and Reliability, International Journal of Performability Engineering, Environment, Systems and Engineering, International Journal of Computational Intelligence Systems. He has functioned as Scientific Chairman of three International Conferences and as Associate General Chairman of two others. His research focuses on the characterization and modeling of the failure/repair/maintenance behavior of components, complex systems and critical infrastructures for the study of their reliability, availability, maintainability, prognostics, safety, vulnerability and security, mostly using a computational approach based on advanced Monte Carlo simulation methods, soft computing techniques and optimization heuristics. He is author or co-author of five international books and more than 170 papers on international journals.

ACRONYMS

ASP	Accident Sequence Precursor
BL	Bypass Line
BN	Bayesian Network
BPC	Basic Process Control
BT	Bow-Tie
CBFTA	Condition-based Fault Tree Analysis
DBN	Dynamic Bayesian Network
DRA	Dynamic Risk Assessment
ET	Event Tree
HFSS	High-Flow Safety System
HLA	High Level Alarm
MCMC	Markov Chain Monte Carlo
MH	Metropolis-Hasting
MV	Manual Valve
PCA	Principal Component Analysis
PF	Particle Filtering
PSV	Pressure Safety Valve
QRA	Quantitative Risk Assessment
RUL	Remaining Useful Life

NOTATIONS

r_{C_i}	Conditional occurrence probability of the consequence given that IE has occurred
$N_{k,j}$	Number of the kth consequences that occur in the interval $(t_{j-1}, t_j]$
$y_{i,j}$	Condition-monitoring data on the ith safety barrier at $t = t_j$
$R_{B,i,j}$	Reliability of the ith safety barrier at $t = t_j$
$\pi_{i,j}$	Prior mean of $R_{B,i,j}$
K	Prior sample size of $R_{B,i,j}$
α_i, β_i	Parameters of the prior distribution of $\pi_{i,1}$
$N_{S,i,j}$	Number of successes in the pseudo test data generated from statistical failure data
$N_{F,i,j}$	Number of failures in the pseudo test data generated from statistical failure data
$M_{S,i,j}$	Number of successes in the pseudo test data generated from condition-monitoring data
$M_{F,i,j}$	Number of failures in the pseudo test data generated from condition-monitoring data
B_i	The ith safety barrier
N_P	Sample size of PF