ELSEVIER

0951-8320(95)00030-5

Reliability Engineering and System Safety **49** (1995) 59–73

0951-8320/95/$9.50

Marked point process framework for living probabilistic safety assessment and risk follow-up

Elja Arjas

Department of Mathematical Sciences, University of Oulu, FIN-90570 Oulu, Finland

&

Jan Holmberg*

VTT Automation, Industrial Automation, P.O. Box 1301, FIN-02044 VTT, Finland

(Received 5 October 1994; accepted 19 March 1995)

We construct a model for living probabilistic safety assessment (PSA) by applying the general framework of marked point processes. The framework provides a theoretically rigorous approach for considering risk follow-up of posterior hazards. In risk follow-up, the hazard of core damage is evaluated synthetically at time points in the past, by using some observed events as logged history and combining it with re-evaluated potential hazards. There are several alternatives for doing this, of which we consider three here, calling them initiating event approach, hazard rate approach, and safety system approach. In addition, for a comparison, we consider a core damage hazard arising in risk monitoring. Each of these four definitions draws attention to a particular aspect in risk assessment, and this is reflected in the behaviour of the consequent risk importance measures. Several alternative measures are again considered. The concepts and definitions are illustrated by a numerical example.

1 INTRODUCTION

Probabilistic safety assessment (PSA) is the main methodology in assessing the risks of operation of nuclear power plants. In order to arrive at a credible and useful PSA model of the plant, system knowledge, deterministic safety analyses, engineering judgements and operating experience should be utilized in a sound manner. In a nuclear power plant, operating experience is used to assess the reliability parameters of the model as well as to verify the adequacy of the assumptions used in the system models. When this procedure is continuously updated PSA becomes a continuous safety evaluation method called *living PSA*.[1]

In living PSA, category y core damage hazard rate $\lambda_t(y)$ is regarded as an instantaneous quantity dependent on the conditions of the plant. In general, the hazard rate is decomposed into the hazard rate of an initiating event and the probability that the safety systems fail to respond to the initiating event, i.e.,

$$\lambda_t(y) = \sum_{x \in E^0} \lambda_t(x) c_t(x, y), \tag{1}$$

where $x \in E^0$ indexes the initiating event categories, $\lambda_t(x)$ is the hazard rate of initiating event of category x, and $c_t(x, y)$ is the conditional probability that consequence (plant damage state) y results when x takes place at time t.

Depending on the time perspective, the evaluation of risks can be divided into three categories.[2] (1) Risk follow-up, if a past hazard rate is considered; (2) risk monitoring, if the current hazard rate is considered; and (3) risk prediction, if a future hazard rate is considered.

The objective of the risk follow-up is to use PSA in

* To whom correspondence should be addressed.

the evaluation of the significance of the events that have occurred. Risk assessment by using a static plant model and even the monitoring of the safety status by a dynamic model may leave important interdependent risk scenarios outside of consideration unless the events are re-examined and evaluated again. By risk follow-up, we can adjust the PSA model to correspond to specific conditions at the plant and compare 'historical' risks with predicted operational risks, in order to get feedback for modifications in PSA and for improvements in operational practices.[3]

A retrospective risk analysis requires that certain definitions and assumptions must be agreed upon. One could say that the 'risk' was *zero* because no accident happened. This is, of course, a meaningless attitude, and hence we need to distinguish events which are observed from those which remain latent, unobserved. Conventional follow-up methods are difficult to apply in this context because the PSA models are typically static, expressing average conditions in the safety systems.

The Reactor Safety Study[4] (app. XI) included a retrospective risk assessment of the fire incident which occurred at Browns Ferry plant in 1975. Since then efforts have been made to estimate core damage hazard rate of PSA by using significant events, called *precursors* (see a special issue on the subject in *Reliability Engineering and System Safety*[21]). In the accident precursor study program carried out by the US Nuclear Regulatory Commission, the licensee event reports (LER) from US light water reactors have been surveyed annually, and as a result hundreds of precursors have been evaluated.[5] The precursors are divided into two classes: (1) initiating events, possibly followed by safety system failures, and (2) unavailabilities in the safety systems.

Accident sequence precursor study is a retrospective approach, in the sense that precursors are interpreted as near misses of accidents to complement the data. While an accident is an observed event, a precursor is a 'partial observation' weighted by the retrospectively evaluated core damage probability. There are some shortcomings in the method which is used for evaluating retrospective core damage probabilities, not to mention the inevitable problems in the estimation of core damage hazard in this way (see Ref. 6). Concerning the retrospective evaluation of a precursor, the so called 'failure memory'[2] approach is usually applied, i.e. failed (unavailable) components are assumed as failed (recovery may be considered), but functioning components have a positive probability of failure. Secondly, initiating events are compared with events in safety systems by using the retrospectively evaluated conditional core damage probabilities. However, the conditions for the evaluations are different. When initiating events are evaluated, the initiating events are applied as near misses, but when events in safety systems are evaluated, the (non)occurrence of initiating events is not acknowledged. Thirdly, no proper interpretation is given to the evaluated retrospective probabilities.

In the Nordic research project 'Safety evaluation by use of living probabilisitic safety assessment and safety indicators, NSK/SIK-1', it was found useful to test the living PSA concept by performing risk follow-up case studies.[7] The first case studies were related to operating period events (see Refs 8–10). In addition to the 'risk follow-up with failure memory', approaches called 'off-line risk monitoring' in which on-line risk monitoring was simulated, and 'risk follow-up with total memory' were defined. However, when comparing different methods and assumptions in various case studies, it was obvious that the definitions should be clarified further. Retrospective risk evaluations need a formalism, too.

In this paper we construct a living PSA model by applying the general framework of marked point processes. We apply this framework especially in risk follow-up. In Section 2, we introduce the basic definitions aimed at evaluating retrospective hazards. In Section 3, we consider importance measures in an attempt to express the importance of observed events to safety. Section 4 contains a numerical example. In Section 5, we discuss the consequences of this

Table 1. Notation index

X_n	a mark of the ith event
T_n	time of the ith event
(X_n, T_n)	a marked point
E	set of marks
$\hat{E}/\tilde{E}$	set of observable/unobservable marks
E^0	set of initiating event categories
$N_t(A)$	counting process of marks $x \in A$
$H_t/\hat{H}_t$	full/observed process history
$H_t^0/\hat{H}_t^0$	full/observed initiating event history
$H_t^*/\hat{H}_t^*$	full/observed safety system history
$\tilde{H}_\tau$	counterfactual process history
h	a sample path of the full process history
h^0/h^*	a sample path of the initiating event/safety system history
$\mathbf{H}$	space of process histories
$\lambda_t(y)$	core damage hazard rate of category y core damage at t
$\hat{\lambda}_t(y)$	core damage hazard rate in risk monitoring
$\hat{\lambda}_t'(y)$	core damage hazard rate in risk follow-up by hazard rate approach
$\hat{\lambda}_t^*(y)$	core damage hazard rate in risk follow-up by safety system approach
$\mathrm{d}\hat{\Lambda}_t^0(y)$	core damage hazard in risk follow-up by initiating event approach
$\lambda_t(x)$	initiating event intensity of category $x \in E^0$
$c(t, x; y)$	conditional probability of consequence y when x takes place at t
J_τ	cumulative monitored hazard in $[0, \tau]$
r_{t_0,t_1+1}	relative cumulative hazard
$m(t)$	momentary change in the hazard rate at t
$d(t)$	importance of follow-up knowledge at t

approach in the PSA modelling context and its practical applicability. Section 6 concludes the paper. The basic notations are given in Table 1.

2 BASIC CONCEPTS AND DEFINITIONS

2.1 A marked point process model

A marked point process $\{(T_n, X_n); n = 1, 2, \ldots\}$ is an ordered sequence of time points T_n and marks X_n associated with the time points. The mark X_n taking values in a set of marks E describes the event occurring at T_n, for example by indicating the type of an initiating event or reporting a change in the condition of the safety systems. A counting process $N_t(A)$ counts the number of marked points (T_n, X_n) with marks in a set A up to time t, i.e.,

$$N_t(A) = \sum_n 1_{\{T_n \le t, X_n \in A\}}, \quad t \ge 0, \quad N_0(A) = 0. \tag{2}$$

$N_t(A)$ is thus a step function taking a jump of size 1 when a mark belonging to A occurs. In the particular case where A is a singleton, say $A = \{x\}$, $x \in E$, we denote the counting process by $N_t(x)$.

The history process H_t is formed by marked points up to time t

$$H_t = \{(T_n, X_n); T_n \le t\}, \tag{3}$$

and H_{t-} is defined in the same way except that the inequality is strict: $T_n < t$. H_t takes values in the space $\mathbf{H}$ which is a subset of $[0, \infty) \times E$.

The x-specific hazard rate or intensity at t given the history H_{t-} can be written as

$$\lambda_t(x) = P(\mathrm{d}N_t(x) = 1 \mid H_{t-})/\mathrm{d}t = \lambda(t, x \mid H_{t-}), \tag{4}$$

where it has been assumed that the corresponding measure is absolutely continuous with respect to the Lebesgue measure. More generally, if absolute continuity cannot be assured, we can use a hazard measure with the interpretation

$$\mathrm{d}\Lambda_t(x) = P(\mathrm{d}N_t(x) = 1 \mid H_{t-}). \tag{5}$$

In the general theory of point processes, the cumulative hazard $\Lambda_t(x) = \int_0^t \mathrm{d}\Lambda_s(x)$ is called the compensator of the counting process $N_t(x)$.[11,12]

2.2 Decomposition of process histories

2.2.1 Full and observed process histories

The marked point process model represents only the most important part of the actual process history, forming a 'landmark process'. From an observer's point of view, the landmark process may contain marked points that remain *latent*, unobserved, at least for a while. We divide the *full* set of marks, E, into the set of observable marks, $\hat{E}$, and the set of unobservable marks, $\tilde{E}$. We assume that $\hat{E}$ is countable.

Let $\hat{H}_t$ denote the *observed* pre-t process history data,

$$\hat{H}_t = \{(T_n, X_n); T_n \le t, X_n \in \hat{E}\}. \tag{6}$$

Each observed history $\hat{H}_t$ is fully determined by the underlying full marked point process history H_t. Consequently, the observed hazard rate can be expressed as an expected hazard rate as follows

$$\begin{aligned} \hat{\lambda}_t(x) &= P(\mathrm{d}N_t(x) = 1 \mid \hat{H}_{t-})/\mathrm{d}t \\ &= \int_{h \in \mathbf{H}} P(H_{t-} \in \mathrm{d}h \mid \hat{H}_{t-}) \lambda(t, x \mid h) \\ &= E[\lambda(t, x \mid H_{t-}) \mid \hat{H}_{t-}], \end{aligned} \tag{7}$$

where $P(H_{t-} \in \mathrm{d}h \mid \hat{H}_{t-})$ is the conditional probability that the full process history H_{t-} is in the elemental volume $\mathrm{d}h$ of $\mathbf{H}$, given the observed, strict pre-t process history. A sample path of the full process is denoted by $h = \{(t_n, x_n); n \ge 1\}$, and the corresponding pre-t histories by $h_t = \{(t_n, x_n); t_n \le t\}$ and $h_{t-} = \{(t_n, x_n); t_n < t\}$.

For the purpose of drawing statistical inferences concerning the hazard rate (7) from observed history (data), we need an expression for the corresponding likelihood function. It is well known to have the following canonical form

$$\begin{aligned} L(\hat{\lambda}_s; 0 \le s \le t \mid \hat{H}_t) = &\left[\prod_{X_n \in \hat{E}, T_n \le t} \hat{\lambda}_{T_n}(X_n) \right] \\ &\times \exp\left\{ - \sum_{x \in \hat{E}} \int_0^t \hat{\lambda}_s(x)\, \mathrm{d}s \right\}. \end{aligned} \tag{8}$$

2.2.2 Parameters

Parameters are hidden, auxiliary random variables of the model, such as initiating event rates and failure rates. In our framework, we can conveniently define parameters as latent marks. Their randomness is here merely an expression that their values are not observable, with probabilities quantifying the uncertainty involved.

As a further mathematical convention, we embed the parameters into the full process history, H_t as a single marked point at the time origin, i.e., if known, then the parameters are constant in time. Prior knowledge about the parameters is described by suitably defined probability densities on the corresponding subset of $\tilde{E}$. As time t increases, these distributions are updated, according to Bayes' rule, by the observed events in $\hat{H}_t$.

2.3 Core damage hazard

2.3.1 Core damage hazard in risk monitoring

Consider core damage of some particular category y, and let $c_t(x, y) = c(t, x; y \mid H_{t-})$ (resp. $\hat{c}_t(x, y) = \hat{c}(t, x; y \mid \hat{H}_{t-})$) be the conditional probability that it occurs if the full process history H_{t-} (resp. observed process history $\hat{H}_{t-}$) is followed at time t by an initiating event $x \in E^0$. In ordinary risk monitoring, the core damage hazard rate is based dynamically on the observed history $\hat{H}_{t-}$, and we have

$$\begin{aligned}\hat{\lambda}_t(y) &= \sum_{x \in E^0} \hat{\lambda}_t(x)\hat{c}_t(x, y) \\ &= \sum_{x \in E^0} \hat{\lambda}(t, x \mid \hat{H}_{t-})\hat{c}(t, x; y \mid \hat{H}_{t-}) \\ &= \sum_{x \in E^0} \Big(\int_{h \in \mathbf{H}} P(H_{t-} \in \mathrm{d}h \mid \hat{H}_{t-}) \\ &\quad \times \lambda(t, x \mid h) c(t, x; y \mid h) \Big). \end{aligned} \tag{9}$$

The process history, i.e., the operating experience of the plant, is divided into two histories:

(1) initiating event history, and

(2) safety system history.

We denote the initiating event history by H_t^0 and the safety system history by H_t^*. The full process history is the superposition $H_t = (H_t^0, H_t^*)$, where we use the convention that if both histories contain a marked point whose time of occurrence is the same, say (s, x^0) and (s, x^*), then the full process history contains simply the point $(s, (x^0, x^*))$. For instance, a core damage can be realized by a sequence of marks $(x^0, x_1^*, \ldots, x_m^*)$, occurring at the same time epoch, and y can then be viewed as a particular set of such points. In a similar manner, we divide the observed histories $\hat{H}_t$ into $\hat{H}_t^0$ (for observed initiating event history) and $\hat{H}_t^*$ (for observed safety system history), so that $\hat{H}_t = (\hat{H}_t^0, \hat{H}_t^*)$. Let h^0 (resp. h^*) denote the sample path of the initiating event (safety system) history. We assume that also the parameters can be divided into two classes: parameters of the initiating event process, and parameters of the safety system process.

We assume that initiating events are observable, i.e. $E^0 \subset \hat{E}$. This does not necessarily mean that $\hat{H}_t^0 = H_t^0$ since H_t^0 may include other relevant unobservable marks, such as unknown parameters. Similarly, some marks in safety systems remain typically unobservable.

We now list a number of natural conditional independence assumptions under which the monitored hazard rate obtains a simpler form.

Assumption A. (i) H_t^0 and H_t^* are conditionally independent given the observed pre-t history $\hat{H}_t$.

(ii) The hazard of initiating events, given the full history of initiating events H_{t-}^0, does not depend on the history of safety systems H_{t-}^*.

(iii) The probability of response y when x occurs, given the full history of safety systems H_{t-}^*, does not depend on the history of initiating events H_{t-}^0.

Item (i) means that initiating event and safety system processes do not excite each other, except possibly through events which are observable. Item (ii) (resp. (iii)) states that initiating event intensities (safety system failure probabilities) depend only on the history of initiating events (safety systems).

Under assumption A, expression (9) can be written in the form

$$\begin{aligned}\hat{\lambda}_t(y) = \sum_{x \in E^0} &\Big(\int_{h^0 \in \mathbf{H}^0} P(H_{t-}^0 \in \mathrm{d}h^0 \mid \hat{H}_{t-}) \lambda(t, x \mid h^0) \Big) \\ &\times \Big(\int_{h^* \in \mathbf{H}^*} P(H_{t-}^* \in \mathrm{d}h^* \mid \hat{H}_{t-}) c(x, t; y \mid h^*) \Big). \end{aligned} \tag{10}$$

We find these assumptions quite reasonable in the present PSA context. Observable events that affect both histories do not violate these assumptions, since those events may appear as simultaneous marked points in each history carrying the necessary information for each history process. For instance, initiating events are such events, and so called common cause initiators (floods, fires, earthquakes) make no difference in that sense.

However, item (i) does not hold if there could be unobservable events affecting both initiating event and safety system history. In that case, we either have to reject the above decomposition or else we must modify the model so that such latent events belong to either of the history processes.

Assumption B. (i) H_t^0 and $\hat{H}_t^*$ are conditionally independent given $\hat{H}_t^0$.

(ii) H_t^* and $\hat{H}_t^0$ are conditionally independent given $\hat{H}_t^*$.

Item (i) means that the full initiating event (resp. in (ii) safety system) history cannot provide any additional information concerning the observed safety system (initiating event) history given the observed initiating event (safety system) history. As before, we find these assumptions reasonable, if we exclude unobservable events affecting both histories.

Under assumption B, expression (10) can be further written as

$$\begin{aligned}\hat{\lambda}_t(y) = \sum_{x \in E^0} &\Big(\int_{h^0 \in \mathbf{H}^0} P(H_{t-}^0 \in \mathrm{d}h^0 \mid \hat{H}_{t-}^0) \lambda(t, x \mid h^0) \Big) \\ &\times \Big(\int_{h^* \in \mathbf{H}^*} P(H_{t-}^* \in \mathrm{d}h^* \mid \hat{H}_{t-}^*) c(t, x; y \mid h^*) \Big). \end{aligned} \tag{11}$$

Therefore, under assumptions A and B, the core damage hazard rate has the form $\sum_x \hat{\lambda}(t, x \mid \hat{H}_{t-}^0)\hat{c}(t, x; y \mid \hat{H}_{t-}^*)$.

2.3.2 Core damage hazard in risk follow-up

In risk follow-up, the hazard of core damage is evaluated synthetically at time points in the past, by using some observable events as a fixed scenario (*logged history*) and combining it with re-evaluated potential hazards. Let $\hat{H}_\tau$ be the observed process history, and let $t < \tau$ be the time point at which the hazard rate is evaluated. Denote similarly by $\hat{H}^0_\tau$ and $\hat{H}^*_\tau$ the observed pre-τ histories of initiating events and of the safety system.

Perhaps the simplest form of conditioning is to use the logged history $\hat{H}_\tau$, and just pick out the (observed) initiating events from this history in order to reassess the probabilities that they produce a core damage belonging to category y. In this way we arrive at the discrete hazard measure

$$\mathrm{d}\hat{\Lambda}^I_t(y) \stackrel{\text{def}}{=} \sum_{x \in E^0} 1_{\{\mathrm{d}N_t(x)=1\}} \times \left(\int_{h \in \mathbf{H}} P(H_{t-} \in \mathrm{d}h \mid \hat{H}_\tau) c(t, x; y \mid h) \right), \quad (12)$$

with point masses at the time epochs when an initiating event was observed to happen. But, in practice, the information in $\hat{H}_\tau$ may be so complete that the result becomes trivial, i.e., the integral in (12) is either 0 or 1.

To avoid a trivial definition, we can restrict the follow-up only to the logged initiating event history $\hat{H}^0_\tau$, and consider

$$\mathrm{d}\hat{\Lambda}^0_t(y) \stackrel{\text{def}}{=} \sum_{x \in E^0} 1_{\{\mathrm{d}N_t(x)=1\}} \times \left(\int_{h \in \mathbf{H}} P(H_{t-} \in \mathrm{d}h \mid \hat{H}^0_\tau) c(t, x; y \mid h) \right). \quad (13)$$

We denote the integral in (13) by $\hat{c}^0(t, x; y \mid \hat{H}^0_\tau)$.

Another alternative to the above *initiating event history* approach is to use a definition where, instead of directly copying the logged initiating events from $\hat{H}_\tau$, we re-evaluate the corresponding hazards locally at t, considering all possible pre-t histories H_{t-}. We call this the *hazard rate* approach. It leads to the hazard rate

$$\hat{\lambda}'_t(y) \stackrel{\text{def}}{=} \sum_{x \in E^0} \left(\int_{h \in \mathbf{H}} P(H_{t-} \in \mathrm{d}h \mid \hat{H}_\tau) \times \lambda(t, x \mid h) c(t, x; y \mid h) \right). \quad (14)$$

Under assumptions A and B, the formula can be further decomposed into

$$\hat{\lambda}'_t(y) = \sum_{x \in E^0} \left(\int_{h^0 \in \mathbf{H}^0} P(H^0_{t-} \in \mathrm{d}h^0 \mid \hat{H}^0_\tau) \lambda(t, x \mid h^0) \right) \times \left(\int_{h^* \in \mathbf{H}^*} P(H^*_{t-} \in \mathrm{d}h^* \mid \hat{H}^*_\tau) c(t, x; y \mid h^*) \right). \quad (15)$$

As in the case of risk monitoring (11), the hazard rate has the form $\sum_x \hat{\lambda}'(t, x \mid \hat{H}^0_\tau) \hat{c}'(t, x; y \mid \hat{H}^*_\tau)$.

Sometimes we may want to restrict the follow-up only to the logged safety system history, $\hat{H}^*_\tau$. Replacing $\hat{H}_\tau$ by $\hat{H}^*_\tau$ in (14) can cause ambiguities. The history $\hat{H}^*_\tau$ often contains indirect information concerning initiating events since a part of the safety systems history typically arises as a response to initiating events. To define a simple approach, we apply, on purpose, only prior information concerning the initiating event process, using then the history $\hat{H}^*_\tau$ as the condition for the safety system process. Starting now from formula (15), we define the *safety system history* approach hazard rate

$$\hat{\lambda}^*_t(y) \stackrel{\text{def}}{=} \sum_{x \in E^0} \hat{\lambda}(t, x \mid \hat{H}_0) \times \left(\int_{h^* \in \mathbf{H}^*} P(H^*_{t-} \in \mathrm{d}h^* \mid \hat{H}^*_\tau) c(t, x; y \mid h^*) \right), \quad (16)$$

where $\hat{\lambda}(t, x \mid \hat{H}_0)$ indicates that only prior information is used for the initiating event process. The hazard rate has the form $\sum_x \hat{\lambda}(t, x \mid \hat{H}_0) \hat{c}'(t; x; y \mid \hat{H}^*_\tau)$.

We point out that these three sets of definitions, called here by the names *initiating event approach*, *hazard rate approach*, and *safety approach*, are by no means the only ones possible. Even when the logged history has been chosen, one can apply different degrees of control between events which are taken directly from the conditioning history, and those considered random and evaluated by using probabilities.

2.4 Model for initiating events

Most PSA's apply the time-homogeneous Poisson process model for initiating events $x \in E^0$. In the present Bayesian framework, we consider the corresponding initiating event intensity as an unknown parameter $\mu(x)$ with a prior probability density $\pi[\mu(x)]$. We assume prior independence between the initiating event intensities. In risk monitoring, the intensity is updated by the operating experience $\hat{H}^0_t$ (all initiating events are observable). The monitored initiating event intensity is the posterior expected value, i.e.,

$$\begin{aligned} \hat{\lambda}(t, x \mid \hat{H}^0_{t-}) &= \int_{h^0 \in \mathbf{H}^0} P(H^0_{t-} \in \mathrm{d}h^0 \mid \hat{H}^0_{t-}) \lambda(t, x \mid h^0) \\ &= a^{-1} \int_0^\infty \mu(x) L(\mu(x) \mid \hat{H}^0_{t-}) \pi[\mu(x)] \, \mathrm{d}\mu(x) \\ &= a^{-1} \int_0^\infty (\mu(x))^{N_t(x)+1} \exp\{-\mu(x)t\} \\ &\quad \times \pi[\mu(x)] \, \mathrm{d}\mu(x), \end{aligned} \quad (17)$$

where $L(\mu(x) \mid \hat{H}^0_{t-})$ is the likelihood of $\hat{H}^0_t$ (cf. (8))

and a is a normalizing constant. In the special case, where the prior is a gamma distribution with a shape parameter $\alpha(x)$ and scale parameter $\beta(x)$, the monitored initiating event intensity has the well-known simple form

$$\hat{\lambda}(t, x \mid \hat{H}_{t-}^{0}) = \frac{\alpha(x) + N_{t-}(x)}{\beta(x) + t}. \tag{18}$$

Similarly, in the case of risk follow-up (15), knowledge about the history up to τ gives the intensity

$$\hat{\lambda}(t, x \mid \hat{H}_{\tau}^{0}) = \frac{\alpha(x) + N_{\tau}(x)}{\beta(x) + \tau}. \tag{19}$$

This framework is general enough for considering time-dependent initiating event intensities, as well. For instance, the intensity could follow a jump process model

$$\mu(t) = \sum_{i \geq 1} 1_{\{T_{i-1} < t \leq T_i\}} \mu_i, \tag{20}$$

where $0 = T_0 < T_1 < T_2 < \cdots$ is an increasing sequence of jump times, and $\mu_i > 0$ are the corresponding levels of the piecewise constant intensity. The jump times can be observable or latent. For the numerical evaluation of the posterior distribution, simulation, in particular the Gibbs sampler, can be applied.[13]

2.5 Model for safety system failures

Conventionally, event tree/fault tree methodology is applied in the modelling of safety systems failures. In the present context, we consider a safety system failure as an event in which a critical sequence of components fails. The risk analyst may choose an appropriate methodology and level of complexity in modelling the interactions between components.

We apply the marked point process model by postulating that an initiating event generates a mark $(\xi_0, \xi_1, \ldots, \xi_n)$, called *event sequence*, where ξ_0 denotes the initiating event category and $\xi_1, \ldots, \xi_n$ correspond to the performance of components $1, \ldots, n$ after the initiating event. The category of the sequence is determined by a multi-state system structure function $\phi(\xi_1, \ldots, \xi_n)$. If $\phi(\xi_1, \ldots, \xi_n) = y$, then a core damage of type y occurs.

The mark ξ_i is an indicator of the state of component i in the event sequence. All components are not necessarily relevant for determining the category of the sequence, and in that case the corresponding indicator can remain dummy. The indicator ξ_i has two possible states: one corresponding a down state, and another a functioning state.

The probability of a state depends on the process history and the position of the component in the sequence. In this section, we discuss how the probability depends on the observed process history. Using the term *failure mode* for the reason why a considered component is down, we list typical failure mode categories used in system models. The categorization helps explaining and understanding the differences in the results when different approaches to risk follow-up are taken. See also Refs 2 and 14 on the categorization of failure modes of standby safety systems.

A failure mode is *evident* (directly observable) if the state of the corresponding indicator in a potential event sequence can be determined at the time of occurrence. For instance, maintenance or repair of a component are evident failure modes. The indicator of that the component is down can be expressed as the function

$$u_t(\hat{x}^1, \hat{x}^2) = N_t(\hat{x}^1) - N_t(\hat{x}^2), \quad \hat{x}^1, \hat{x}^2 \in \hat{E}$$
$$= \begin{cases} 1 & \text{if the component is maintained,} \\ 0 & \text{if component is not in maintenance} \end{cases} \tag{21}$$

where $\hat{x}^1$ is the mark indicating the beginning and $\hat{x}^2$ the mark indicating the end of maintenance of the component in question.

Other failure modes are (directly) *unobservable.* They can be divided further into *latent* and *demand related* failure modes, depending on whether the component enters the failed state before the initiating event (latent) or whether the failure epoch comes only after an initiating event has occurred in a situation where this component is needed (demand related).

Latent failures appear as two marked points in the process history: (1) the failure epoch (latent), and (2) the detection epoch. If the latent failure epochs are related only to observed time points, the failure mode is called *time-independent.* An example of a latent time-independent failure is a failure in the restoration of a component after a test. The probability that the component is down does not depend on time elapsed from the latest detection epoch. The potential down state is then detected later, for instance, in a surveillance test. In risk follow-up, this failure mode becomes evident.

If the latent failure can occur at any time, then the failure mode is called *time-dependent.* For instance, the wear of a component can be such a failure mode. Wear may progress latently to a state that makes the component unavailable. The degree of wear is detected in periodical surveillance tests. In risk monitoring, the probability of the down state depends on the time from the previous test, or some other renewal point. In risk follow-up, we may assume that if the condition of the component is acceptable in the test, it would have operated correctly in a potential demand during the previous test interval. Otherwise, we must calculate the conditional probability, given the observed history, that a latent marked point

corresponding to the failure occurred before the considered time point in the risk follow-up.

For demand related failure modes, such as operator errors, the failure epoch and detection epoch are interrelated. Corresponding indicators in the event sequence do not become evident even in risk follow-up. For instance, it does not seem to be reasonable to conclude from later observed operator errors (or successful actions) that the operator would have failed (succeeded) at some other time in a similar action. Of course the failure probability may be updated by using such operating experience.

3 RISK IMPORTANCE MEASURES

The ordinary risk or reliability importance measures used in PSA are designed to indicate the relative importance of a component, or a group of components, to the core damage hazard rate.[15] The three basic measures in the ranking of the components are: risk increase factor, risk decrease factor, and fractional contribution. In the present marked point process framework, we consider risk importance measures related to events rather than to component states. The following measures are preliminary suggestions for such.

3.1 Cumulative hazards

The cumulative monitored hazard, i.e.,

$$J_\tau = \int_0^\tau \hat{\lambda}_t(y)\,\mathrm{d}t, \tag{22}$$

expresses the locally observed hazard over the observation period. Similarly, we define the cumulative hazard arising from the three approaches to risk follow-up considered in Section 2.3.2, i.e.,

$$J_\tau^0 = \int_0^\tau \mathrm{d}\hat{\Lambda}_t^0(y), \tag{23}$$

$$J'_\tau = \int_0^\tau \hat{\lambda}'_t(y)\,\mathrm{d}t, \tag{24}$$

or

$$J_\tau^* = \int_0^\tau \hat{\lambda}_t^*(y)\,\mathrm{d}t. \tag{25}$$

By dividing the observation interval into suitable subintervals $(t_i, t_{i+1}]$, $0 = t_0 < t_1 < \cdots < t_k = \tau$, the relative importance of the periods can be expressed in terms of the ratios

$$r_{t_i,t_{i+1}} = \frac{J_{t_i,t_{i+1}}}{J_\tau}, \quad i = 0, 1, \ldots, k-1, \tag{26}$$

where

$$J_{t_i,t_{i+1}} = \int_{t_i}^{t_{i+1}} \hat{\lambda}_t(y)\,\mathrm{d}t. \tag{27}$$

Corresponding importance measures, denoted by r^0, r' and r^*, can be defined starting from (23)–(25). The subintervals may be of a fixed length, e.g. a week, or they may also be chosen according to events of interest, e.g. so that $(t_i, t_{i+1}]$ always contains one such event.

3.2 Momentary change in the hazard rate

In risk monitoring the importance of the observed marked point is evaluated by

$$m(t) = \hat{\lambda}_{t+}(y) - \hat{\lambda}_t(y), \tag{28}$$

where $\hat{\lambda}_{t+}(y)$ is the right limit $\hat{\lambda}_{t+}(y) = \lim_{s \downarrow t} \hat{\lambda}_s(y)$.

The difference $m(t)$ is typically zero at times which are between two observed marked points and nonzero at such points. Momentary change can be used to calculate increases or decreases in core damage hazard rate when the states of evident indicators change. On the other hand, they reflect the influence of the updated probability distributions of the model parameters.

3.3 Importance of follow-up knowledge

Comparison of monitoring and follow-up hazard rates provides information about the importance of events that are latent in monitoring but evident in follow-up. Hence we define importance of follow-up knowledge by the difference

$$d(t) = \hat{\lambda}'_t(y) - \hat{\lambda}_t(y). \tag{29}$$

3.4 Event importance

The use of the relative importance of a time interval as defined in (26) provides one way of ranking significant events. Another possibility is to define a counterfactual history in which the considered event is replaced by another event, or it can be completely removed from the observed history. Defining such modified histories $\tilde{H}_\tau$ for each event of interest, the reduction (or change) in the cumulative hazard

$$\Delta J = J_\tau - \tilde{J}_\tau, \tag{30}$$

can be used in the ranking of events. Here $\tilde{J}_\tau$ is the cumulative hazard if $\tilde{H}_\tau$ is observed instead of $\hat{H}_\tau$. Corresponding measures, ΔJ^0, $\Delta J'$, and ΔJ^*, can be defined for the three approaches to risk follow-up. ΔJ is positive if the considered event is hazardous. In this case the relative reduction, $\Delta J / J_\tau$, seems an appropriate measure of risk importance.

We may, however, consider also events that have contributed to safety, such as a test where a latent failure has been detected. The counterfactual event could be that the test was not done, and the failure is detected much later. Also, excluding (resp. including) an event would exclude (resp. include) its impact on Bayesian updates of the parameters. All in all, this importance measure involves additional 'manual' modelling work.

4 EXAMPLE

4.1 System model

In this section, we consider a simple example in order to illustrate the application of the general framework. Consider a plant with a single initiating event category and a safety system consisting of a single component and a recovering operator action. An initiating event thus produces a mark which is three digits long and has the form (ξ_0, ξ_1, ξ_2). Here ξ_0 which is the mark indicating the initiating event, is always 0. Similarly, $\xi_1 = 1$ (resp. $\xi_1 = -1$) indicates the functioning (failure) of the component, and $\xi_2 = 2$ (resp. $\xi_2 = -2$) a correctly performed (failed) operator action. Let $y = \mathrm{CD}$ denote the core damage category, and let $y = \mathrm{OK}$ be the safe end state category. Since core damage is the sequence $(\xi_0, \xi_1, \xi_2) = (0, -1, -2)$, we arrive at a system state function

$$\phi(\xi_1, \xi_2) = \begin{cases} \mathrm{CD} & \text{if } \xi_1 = -1, \text{ and } \xi_2 = -2, \\ \mathrm{OK} & \text{otherwise.} \end{cases} \quad (31)$$

The component may be unavailable due to a latent failure or due to preventive maintenance. If the component is unavailable when an initiating event occurs, then the situation can be recovered by the operator. When a latent failure is detected, the component is repaired immediately. Mark '5' denotes the end of repair.

The hazard rate of the component failure is an unknown constant $\lambda(1)$. The prior distribution π_0^1 of $\lambda(1)$ is here assumed to be a gamma distribution with a shape parameter $\alpha(1) = 2$ and scale parameter $\beta(1) = 10\,000$ h. The prior hazard rate is therefore $E[\lambda(1)] = 2 \times 10^{-4}$ 1/hr. The component is tested periodically after 720 hour intervals, and it is assumed to be as good as new after a test.

Preventive maintenance takes place annually at a predetermined time, and it lasts 24 hours. If an initiating event occurs during this period, there is no time to restore the component to an operational state. The maintenance period starts always with a component test, and the component is assumed to be as good as new when restored to a standby state. This unavailability mode is evident. The mark indicating the beginning of the maintenance is '3' and the mark indicating the end is '4'.

The probability of a failed operator action, p, is based on a subjective judgement. The prior distribution π_0^2 of p is Beta with parameters $\alpha(2) = 1$ and $\beta(2) = 99$, leading to prior failure probability $E[p] = \alpha(2)/(\alpha(2) + \beta(2)) = 0{\cdot}01$. This failure mode is demand related.

Given $\hat{H}^*_{t-}$, $\lambda(1)$ and p, the probability of the safety system failure is

$$\hat{c}(t, 0, \mathrm{CD} \mid \hat{H}^*_{t-}, \lambda(1), p) = \hat{q}_1(t \mid \hat{H}^*_{t-}, \lambda(1))p, \quad (32)$$

where $\hat{q}_1(t \mid \hat{H}^*_{t-}, \lambda(1))$ is the probability that the component is down given $\hat{H}^*_{t-}$ and $\lambda(1)$. It can be decomposed into two terms (depending on whether the component is maintained or not) as follows

$$\hat{q}_1(t \mid \hat{H}^*_{t-}, \lambda(1)) = u_t(3, 4) + (1 - u_t(3, 4)) \times P(\text{component is latently failed at } t \mid \hat{H}^*_{t-}, \lambda(1)), \quad (33)$$

where $u_t(3, 4)$ tracks the maintenance related marks '3' and '4'.

Assuming A and B, the probability of the safety system failure is obtained by integrating (32) over the probability distribution of the parameters as follows,

$$\hat{c}(t, 0; \mathrm{CD} \mid \hat{H}^*_{t-}) = \int\int \hat{q}_1(t \mid \hat{H}^*_{t-}, \lambda(1))p \times \pi(\lambda(1), p \mid \hat{H}^*_{t-})\, \mathrm{d}\lambda(1)\, \mathrm{d}p. \quad (34)$$

A priori, we assume the independence of the parameters $\lambda(1)$ and p. In this example, they will be also independent *a posteriori*, except in the initiating event approach of risk follow-up when the system level observation couples the two probability distributions together (see Section 4.4.1). If the parameters are independent *a posteriori*, then

$$\begin{aligned} \hat{c}(t, 0, \mathrm{CD} \mid \hat{H}^*_{t-}) &= \int \hat{q}_1(t \mid \hat{H}^*_{t-}, \lambda(1)) \times \pi^1(\lambda(1) \mid \hat{H}^*_{t-})\, \mathrm{d}\lambda(1) E[p \mid \hat{H}^*_{t-}] \\ &= \hat{q}_1(t \mid \hat{H}^*_{t-}) E[p \mid \hat{H}^*_{t-}]. \end{aligned} \quad (35)$$

The prior distribution π_0^0 of the initiating event intensity $\lambda(0)$ is assumed to be gamma with shape parameter $\alpha(0) = 2$ and scale parameter $\beta(0) = 10\,000$ hr. Prior knowledge about parameters is summarized in Table 2.

4.2 Operating experience

We study a ten month period of operation between two major annual overhauls. The component was tested altogether ten times, resulting in one failed performance in a test. Preventive maintenance took place after the fifth test. An initiating event occurred once at time 1000 hr, and the component functioned

Table 2. Prior probability distributions of the parameters

	Parameter	Distribution	Hyperparameters	Mean
Initiating event intensity	$\lambda(0)$	gamma	$\alpha(0) = 2{\cdot}0$ $\beta(0) = 10\,000$	2×10^{-4}
Component failure intensity	$\lambda(1)$	gamma	$\alpha(1) = 2{\cdot}0$ $\beta(1) = 10\,000$	2×10^{-4}
Operator error probability	p	beta	$\alpha(2) = 1{\cdot}0$ $\beta(2) = 99$	0·01

as required. The operating experience is presented in Fig. 1.

In this example, we know all occurrences of the initiating events. Concerning the safety system, we miss the exact time at which the component had failed between the tests at 4320 and 5040 hours.

4.3 Risk monitoring hazard

Assuming A and B, the core damage hazard rate can be calculated from (11) and (35) by

$$\begin{aligned}\hat{\lambda}_t(\mathrm{CD}) &= \hat{\lambda}(t, 0 \mid \hat{H}^0_{t-})\hat{c}(t, 0, \mathrm{CD} \mid \hat{H}^*_{t-}) \\ &= \hat{\lambda}(t, 0 \mid \hat{H}^0_{t-})\hat{q}_1(t \mid \hat{H}^*_{t-})E[p \mid \hat{H}^*_{t-}]. \quad (36)\end{aligned}$$

For the initiating event intensity, we apply

$$\hat{\lambda}_t(0) = E[\lambda(0) \mid \hat{H}^0_{t-}] = \frac{\alpha(0) + N_{t-}(0)}{\beta(0) + t}. \quad (37)$$

The operator error probability is equal to the prior expected value, i.e.,

$$E[p \mid \hat{H}^*_{t-}] = 0{\cdot}001, \quad t \in [0, 7200]. \quad (38)$$

Next, we consider the probability that a latent failure of the component has occurred since the latest check. Given $\lambda(1)$, we have

$$\begin{aligned}&P(\text{component is latently failed at } t \mid \hat{H}^*_{t-}, \lambda(1)) \\ &\qquad = 1 - \exp\{-\lambda(1)(t - \rho_t^-)\} \quad (39)\end{aligned}$$

where ρ_t^- is the latest renewal point. In this case, tests and ends of maintenance or repair are such points, i.e., $\rho_t^- = \sup_{T_n}(T_n < t : X_n \in \{1, 4, 5\})$.

Let $\{S_i^1\}$ ($\{S_i^{-1}\}$) be the sequence of the ages of the component when it is tested and it functions (fails). Then the likelihood function of $\lambda(1)$ is

$$\begin{aligned}&L(\lambda(1) \mid \hat{H}^*_{t-}) \\ &= \begin{cases} \exp\left\{-\lambda(1) \sum_{i=1}^{N_{t-}(1)} S_i^1\right\} & \text{if } N_{t-}(-1) = 0 \\ \exp\left\{-\lambda(1) \sum_{i=1}^{N_{t-}(1)} S_i^1\right\} & \\ \times \prod_{i=1}^{N_{t-}(-1)} (1 - \exp\{-\lambda(1) S_i^{-1}\}) & \text{if } N_{t-}(-1) > 0. \end{cases} \quad (40)\end{aligned}$$

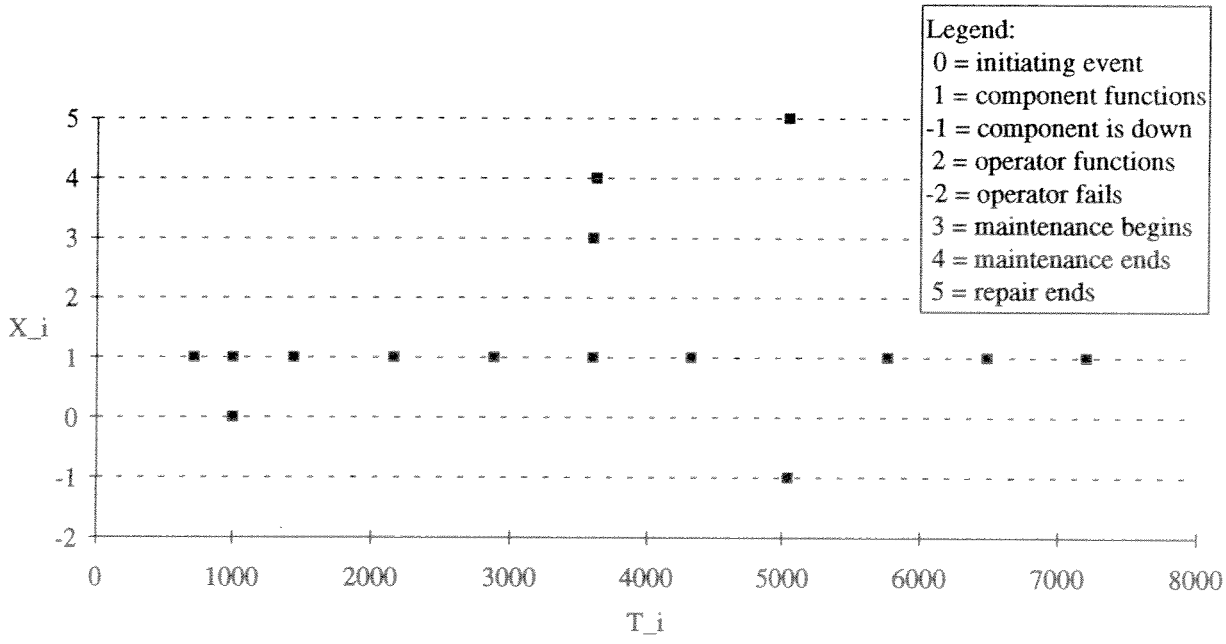

Fig. 1. Example of an observed process history.

The posterior probability of there being a latent failure at time t is therefore

$$P(\text{component is latently failed at } t \mid \hat{H}^*_{t-})$$

$$= \int (1 - \exp\{\lambda(1)(t - \rho_t^-)\})\pi^1(\lambda(1) \mid \hat{H}^*_{t-})\, d\lambda(1)$$

$$= \begin{cases} 1 - \left(\dfrac{\beta(1) + \sum_{i=1}^{N_{t-}(1)} S_i^1}{\beta(1) + \sum_{i=1}^{N_{t-}(1)} S_i^1 + t - \rho_t^-} \right)^{\alpha(1)} & \text{if } N_{t-}(-1) = 0 \\ 1 - \dfrac{1}{\omega} \left[\dfrac{1}{\left(\beta(1) + \sum_{i=1}^{N_{t-}(1)} S_i^1 + t - \rho_t^-\right)^{\alpha(1)}} \right. & \\ \left. - \dfrac{1}{\left(\beta(1) + \sum_{i=1}^{N_{t-}(1)} S_i^1 + \sum_{i=1}^{N_{t-}(-1)} S_i^{-1} + t - \rho_t^-\right)^{\alpha(1)}} \right] & \text{if } N_{t-}(-1) > 0 \end{cases} \quad (41)$$

where

$$\omega = \frac{1}{\left(\beta(1) + \sum_{i=1}^{N_{t-}(1)} S_i^1\right)^{\alpha(1)}} - \frac{1}{\left(\beta(1) + \sum_{i=1}^{N_{t-}(1)} S_i^1 + \sum_{i=1}^{N_{t-}(-1)} S_i^{-1}\right)^{\alpha(1)}}. \quad (42)$$

Applying (41) in (33) and then (33) together with (38), we obtain the safety system probability term of the core damage hazard rate in (36). When it is multiplied by the initiating event intensity (37), the monitored core damage hazard rate illustrated in Fig. 2 is obtained. The maximum hazard rate, $\hat{\lambda}_t(y) = 2{\cdot}2 \times 10^{-6}$ 1/hr, is monitored at $3600 \le t \le 3624$ when the component is being maintained.

4.4 Risk follow-up hazard

4.4.1 Initiating event history approach

In the initiating event history approach (eqn (13)), only initiating events which have actually occurred need to be considered, and in this case there is only one. The core damage hazard is simply a 'pulse' at the time of the initiating event (1000 hr) of size

$$d\hat{\Lambda}^0(t) = \begin{cases} \hat{c}^0(t, 0, \text{CD} \mid \hat{H}^0_\tau) & \text{if } t = 1000 \\ 0 & \text{otherwise} \end{cases}$$

$$= \begin{cases} \iint c(t, 0, \text{CD} \mid \hat{H}^0_\tau, \lambda(1), p) \\ \times \pi(\lambda(1), p \mid \hat{H}^0_\tau)\, d\lambda(1)\, dp & \text{if } t = 1000 \\ 0 & \text{otherwise.} \end{cases} \quad (43)$$

The integration of the safety system failure probability is somewhat complicated by the fact that the observation of an initiating event without a core damage at 1000 hr is system level evidence, making $\lambda(1)$ and p conditionally dependent. The joint likelihood of p and $\lambda(1)$ is

$$L(\lambda(1), p \mid \hat{H}^0_\tau) = 1 - (1 - \exp\{-\lambda(1) S_1^1\})p, \quad (44)$$

where $S_1^1 = 1000 - 720 = 280$ is the time from the test preceding the initiating event. Test epochs and timing of the preventive maintenance are assumed to be included in the prior knowledge. The probability of a

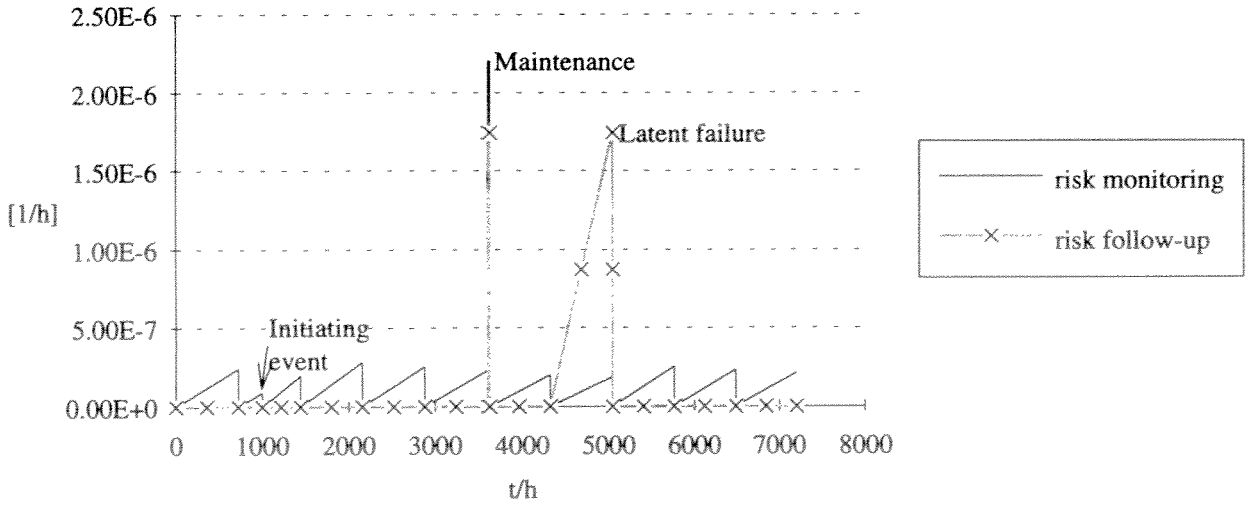

Fig. 2. Core damage hazard rate in risk monitoring and risk follow-up (hazard rate approach).

core damage given an initiating event becomes then

$$\hat{c}^0(t, 0, \mathrm{CD} \mid \hat{H}_\tau^0) = \begin{cases} \dfrac{1}{\omega'} \iint (1 - \exp\{-\lambda(1)(t - \rho_t^-)\}) p \\ \quad \times L(\lambda(1), p \mid \hat{H}_\tau^0) \pi_0^1(\lambda(1)) \pi_0^2(p)\, \mathrm{d}p\, \mathrm{d}\lambda \\ \qquad\qquad\qquad\qquad\qquad\qquad \text{if } t = 1000 \\ 0 \qquad\qquad\qquad\qquad\qquad\qquad \text{otherwise} \end{cases}$$

$$= \begin{cases} \dfrac{1}{\omega'} \dfrac{\alpha(2)}{\alpha(2) + \beta(2)} \left[\left\{ 1 - \dfrac{\alpha(2) + 1}{\alpha(2) + \beta(2) + 1} \right\} \right. \\ \quad \times \left\{ 1 - \left(\dfrac{\beta(1)}{\beta(1) + t - \rho_t^-} \right)^{\alpha(1)} \right\} \\ \quad - \dfrac{\alpha(2) + 1}{\alpha(2) + \beta(2) + 1} \left\{ \left(\dfrac{\beta(1)}{\beta(1) + t - \rho_t^- + S_1^1} \right)^{\alpha(1)} \right. \\ \quad \left. \left. - \left(\dfrac{\beta(1)}{\beta(1) + S_1^1} \right)^{\alpha(1)} \right\} \right] \qquad \text{if } t = 1000 \\ 0 \qquad\qquad\qquad\qquad\qquad\qquad \text{otherwise,} \end{cases} \tag{45}$$

where

$$\omega' = 1 - \frac{\alpha(2)}{\alpha(2) + \beta(2)} \left[1 - \left(\frac{\beta(1)}{\beta(1) + S_1^1} \right)^{\alpha(1)} \right]. \tag{46}$$

is a normalizing constant.

In this case, the evidence in $\hat{H}_\tau^0$ does not change the prior distribution of $\lambda(1)$ and p very much, but in principle, this approach may lead to a rather complicated evaluation of posterior distributions. Anyhow, $\mathrm{d}\hat{\Lambda}_t^0(y)$ has a jump of size $5{\cdot}4 \times 10^{-4}$ at the time of the initiating event (1000 hr).

4.4.2 Hazard rate approach

In the hazard rate approach we apply definition (15), so that the initiating event hazard is constant

$$\hat{\lambda}(t, 0 \mid \hat{H}_\tau^0) = E[\lambda(0) \mid \hat{H}_\tau] = \frac{\alpha(0) + N_\tau(0)}{\beta(0) + \tau} = 1{\cdot}7 \times 10^{-4}\ 1/\mathrm{hr}, \quad t \in [0, 7200]. \tag{47}$$

The safety system failure probability (the second integral of the right-hand side of (15)) can be expressed in the product form

$$\hat{c}'(t, 0, \mathrm{CD} \mid \hat{H}_\tau^*) = \hat{q}_1'(t \mid \hat{H}_\tau^*) E[p \mid \hat{H}_\tau^*]. \tag{48}$$

Here $E[p \mid \hat{H}_\tau^*]$ is the same as in risk monitoring since no further evidence has been obtained. As in risk monitoring, $\hat{q}_1'(t \mid \hat{H}_\tau^*) = 1$ when the component is being maintained, and otherwise $\hat{q}_1'(t \mid \hat{H}_\tau^*) = 0$ except during the test interval in which the latent failure occurred. Given $\lambda(1)$, the component unavailability is

$$\hat{q}_1'(t \mid \hat{H}_\tau^*, \lambda(1)) = \begin{cases} 1 & 3600 \le t \le 3624, \\ \dfrac{1 - e^{-\lambda(1)(t - 4320)}}{1 - e^{-\lambda(1) 720}} & 4320 \le t \le 5040, \\ 0 & \text{otherwise.} \end{cases} \tag{49}$$

Since the mass of the distribution $\pi^1(\lambda(1) \mid \hat{H}_\tau^*)$ is concentrated in small values of $\lambda(1)$, we approximate linearly the fraction term in (49), i.e.,

$$\hat{q}_1'(t \mid \hat{H}_\tau^*) \approx \begin{cases} 1 & 3600 \le t \le 3624, \\ \dfrac{t - 4320}{720} & 4320 \le t \le 5040, \\ 0 & \text{otherwise.} \end{cases} \tag{50}$$

The core damage hazard rate is obtained as the product of (47) and (48), i.e.,

$$\hat{\lambda}_t'(y) = \hat{\lambda}(t, 0 \mid \hat{H}_\tau^0) \hat{q}_1'(t) E[p \mid \hat{H}_\tau^*], \tag{51}$$

and it is presented by a thick grey line with cross marks in Fig. 2. It vanishes except when the component was maintained and during the test interval preceding the detected latent failure. The maximum value of this hazard rate $1{\cdot}7 \times 10^{-6}$ 1/hr at $t = 3600$ hr. This is less than in risk monitoring (where the maximum is $2{\cdot}0 \times 10^{-6}$ 1/hr) since the initiating event intensity according to follow-up knowledge is smaller.

4.4.3 Safety system approach

In the safety system approach (definition (16)), we regard the marked point of the initiating event $(1000, (0, 1))$ contained in $\hat{H}_\tau$ as the marked point $(1000, 1)$, i.e., as a test of the component. The formula for core damage rate is the same as in (51) except that the initiating event intensity is the prior expected value

$$\hat{\lambda}(t, 0 \mid \hat{H}_0) = E[\lambda(0) \mid \hat{H}_0] = 2{\cdot}0 \times 10^{-4}\ 1/\mathrm{hr}, \tag{52}$$

i.e., slightly higher than in (47). Since the safety system failure probability remains unchanged from (48), the profile of the core damage hazard rate is similar as in hazard rate approach, but takes always slightly higher values.

4.5 Importance measures

4.5.1 Momentary change of the hazard rate

The greatest momentary change (definition (28)) is related to the maintenance of the component. The start of maintenance, corresponding here to the marked point $(3600, (1, 3))$, causes the monitored core damage hazard rate to jump to a $2{\cdot}0 \times 10^{-6}$ 1/hr

higher value. At the end of the maintenance, at the marked point (3624, 4), there is again a downward jump of size $2{\cdot}2 \times 10^{-6}$ 1/hr. Test epochs result in downward jumps of the order $0{\cdot}2 \times 10^{-6}$ 1/hr whereas the initiating event causes a downward jump of $0{\cdot}1 \times 10^{-6}$ 1/hr. The evident failure is the most important event according to this importance measure. Figure 3 contains a scatter diagram of the momentary changes at the observed marked points.

4.5.2 Importance of follow-up knowledge

According to follow-up knowledge (definition (29)) the most important event is the detection of the latent failure in the test at time $t = 5040$ hr, $d(5040) = 1{\cdot}6 \times 10^{-6}$ 1/hr. At the other tests epochs and at the time at which the initiating event occurred, this measure is equal to the momentary importance. During the maintenance of the component, $d(t)$ is approximately $-0{\cdot}5 \times 10^{-6}$ 1/hr, i.e., according to this measure, maintenance was not an important event since it is evident. Importance of follow-up knowledge is presented in Fig. 4.

4.5.3 Event importance

We analyzed specifically the importance of the following three events: (1) initiating event at 1000, (2) maintenance between 3600 and 3624, and (3) latent failure between 4320 and 5040. Table 3 presents the relative importances based on cumulative hazards over the time intervals related to the events. Risk monitoring does not indicate the importance of the latent failure. In the hazard rate approach to risk follow-up, the relative contribution of the latent failure was 94%, the rest (6%) coming from the maintenance. The relative contribution of the initiating event is meaningful to consider only in the initiating event approach to risk follow-up, and then this event is the only contributor to the hazard.

Then, we analyzed the events by defining corresponding counterfactual process histories. The considered counterfactual history for the initiating event simply deletes the marked point (1000, (0, 1)). In the case of maintenance, the mark (1, 3) at 3600 is replaced by a test (1), and the marked point (3624, 4) is removed from the history. In the case of latent failure, the mark (−1, 5) at 5040 is replaced by a mark functioning component (1).

The relative reductions of the cumulative hazard by each counterfactual case and in each approach are summarized in Table 4. The first column (risk monitoring) can be used to compare the importance of the above three events with respect to updated probability distributions of parameters. In this sense, the initiating event (1) is more important than the two other events (2) and (3). This is perhaps the only meaningful way to compare the importance of initiating events with events in the safety system history. In follow-up approaches these two types of events are always treated separately.

In the hazard rate and safety system approaches (the third and fourth columns in Table 4), maintenance (2) and latent failure (3) have almost exactly the same importance (maintenance 6%, and latent failure 94%) as when relative importance was measured (cf. Table 3). If no initiating event occurs (1), then the relative reduction is 33% in the hazard rate approach. This reduction is explained by the lower posterior initiating event rate.

5 DISCUSSION

5.1 Implications to PSA modelling

In essence, a living PSA model should represent the hazard of a core damage as a function of observed

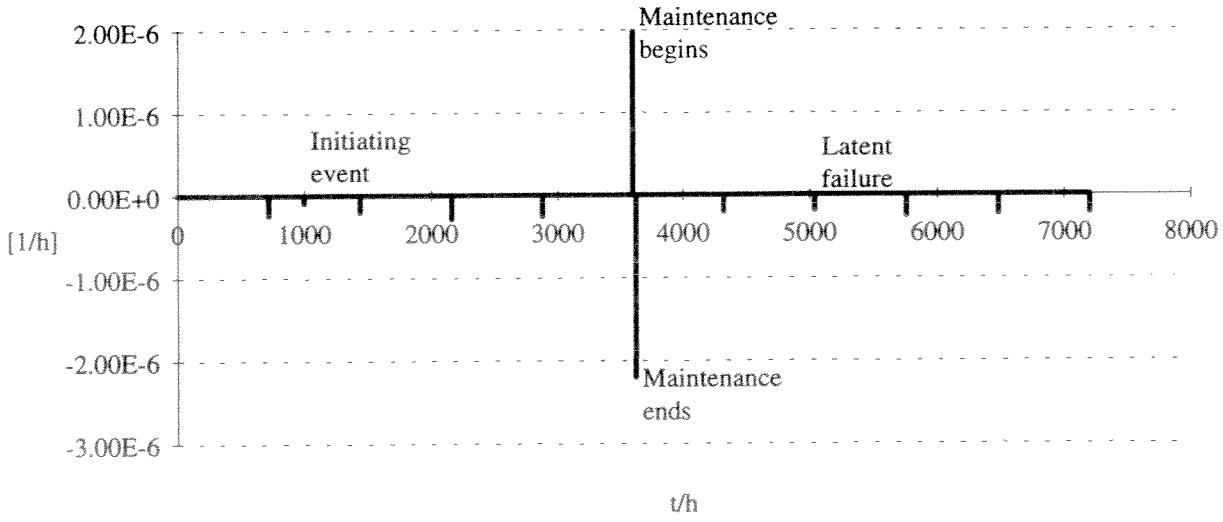

Fig. 3. Momentary changes in the monitored core damage hazard rate.

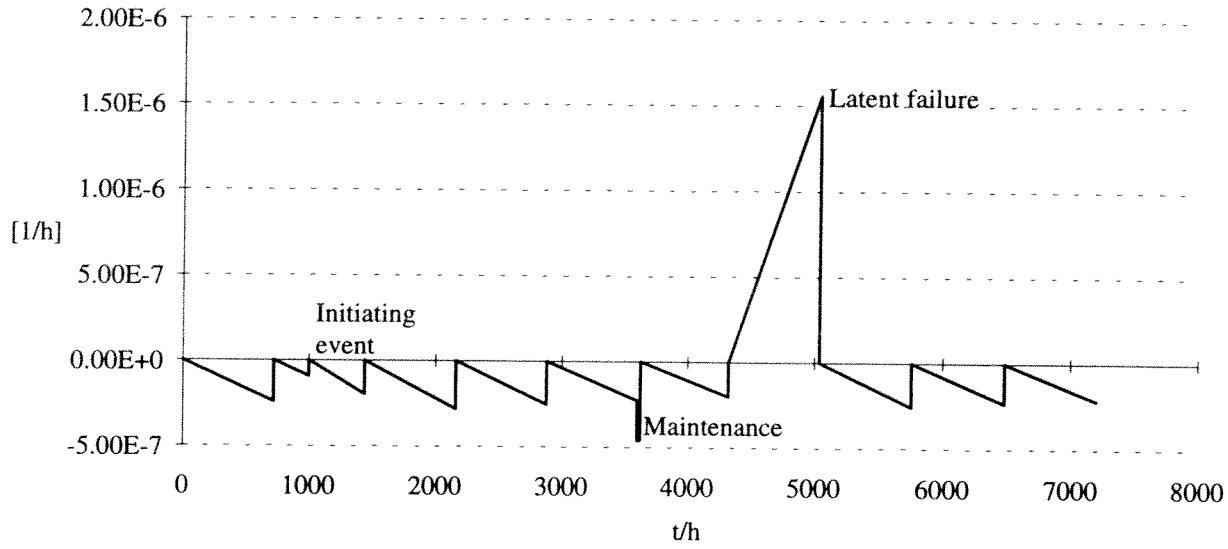

Fig. 4. Importance of follow-up knowledge.

conditions at the plant. A marked point process framework seems well suited for such a purpose. In the application of PSA to risk monitoring or follow-up, a marked point process framework focuses on relationships between observed and latent events. The framework itself is flexible in handling many kinds of dynamic reliability models.

The assumptions A and B used in this paper are quite reasonable in the present PSA context. New assumptions are needed in the categorization of failure modes (especially non-observable failure modes), since they behave differently in risk follow-up. On the other hand, this stresses the importance of explicit modelling assumptions.

We have relied on the Bayesian framework in the modelling of uncertainties. Operating experience reduces the uncertainty arising from unknown parameter values, in our framework formally represented as latent marks at time 0. The importance of this experience is in a similar position in the risk follow-up as the importance of knowing the component states exactly, e.g., in surveillance tests.

We suggest the application of jump process models for initiating event intensities to describe the ageing of systems. The jump process model could also be considered as an alternative to the modelling of common cause failures. It seems quite reasonable to interpret some common cause failure modes as simultaneous jumps in the failure intensities of redundant components (cf. simultaneous failures of redundant components).

Table 3. Relative cumulative hazards of the events

Event	Time interval	r	r^0	r'	r^*
Initiating event	[1000]	—	1·0	—	—
Maintenance	[3600, 3620]	0·060	0·0	0·063	0·063
Latent failure	[4320, 5040]	0·078	0·0	0·937	0·937

5.2 Practical performance of risk follow-up

There are many living PSA systems that manage risk monitoring evaluation, e.g. ESSM,[16] SAIS,[17] STARS,[18] STUK PSA,[19] and Risk Spectrum.[20] In risk follow-up applications, the computer code should be able to read a log file of observed events, and it can then evaluate the desired hazard profile. This feature is included optionally in STUK PSA and Risk Spectrum. Accurate performance of risk follow-up may be laborious, however. The treatment of latent failure modes is a problem, particularly if the observed history provides only partial information. This is the case when only system level information has been obtained, e.g., we know that the system has functioned as a whole. Common cause failure models may complicate the situation additionally.

The integration of posterior distributions of the parameters is computationally extremely demanding with a comprehensive PSA model. In simple cases, e.g. for time-independent failure probabilities, the posterior expected values of the parameters or component and system reliabilities can be solved

Table 4. Relative reductions in the cumulative hazards in the hypothetical histories

History	$\Delta J/J_\tau$	$\Delta J^0/J_\tau^0$	$\Delta J'/J_\tau'$	$\Delta J^*/J_\tau^*$
No initiating event	0·250	1·0	0·333	0·0
No maintenance	0·055	0·0	0·062	0·062
No latent failure	0·098	0·0	0·938	0·938
$J_\tau, J_\tau^0, J_\tau', J_\tau^*$	$8{\cdot}6\times10^{-4}$	$5{\cdot}4\times10^{-4}$	$6{\cdot}7\times10^{-4}$	$7{\cdot}7\times10^{-4}$

analytically. Otherwise numerical methods, such as Monte Carlo simulation, are needed. Simplifying algorithms are definitely needed for risk follow-up, where the evaluations are carried out at several time epochs.

We emphasize once more that, in any approach of risk follow-up, some events must be ignored so that non-trivial hazard measures are obtained. Therefore, in retrospective risk assessment, events in the recorded history may turn out to be important in different ways. In order to highlight such differences, several alternative approaches and risk importance measures should be used in parallel. For instance, initiating events and events in safety systems can be compared only by calculating their influence on the updating of probability distributions of the model parameters. The hazard rate follow-up approach ($\hat{\lambda}_t'(y)$ or $\hat{\lambda}_t^*(y)$) seems more suitable for the follow-up of events in safety systems than the initiating event approach ($\mathrm{d}\hat{\Lambda}_t^0(y)$). On the other hand, the suggested initiating event approach may be appropriate in the comparison of the importance of initiating events.

The application of hypothetical histories in the evaluation of the importance of events requires additional modelling work. However, such a reasoning may be supported by AI techniques. Other suggested risk importance measures can be computed automatically.

Concerning precursor programs, our approach may provide new perspectives to the ranking of recorded incidents. The definitions are even applicable in the monitoring and follow-up of several plants, in which case $\hat{\lambda}_t(y)$ can be regarded as a hazard of category y core damage in the plant population.

6 CONCLUSIONS

Marked point process models can be applied as a general framework for describing the dynamics of events in a nuclear power plant. The framework itself is very flexible and does not particularly restrict the selection of the PSA modelling approach.

The risk follow-up approach presented here provides theoretically rigorous methods for evaluating posterior hazards. It is then natural to treat initiating events and events in safety systems in different ways. These two types of events can be compared by calculating the influence to the updating of probability distributions of the model parameters.

The suggested risk importance measures are related to events rather than to component states. The importance of observable failures modes can be assessed in terms of momentary changes of the hazard rate. In the evaluation of the importance of the detection of latent failures, risk follow-up related importance measures are needed. The importance of more complicated events must be assessed by means of counterfactual process histories.

In risk follow-up the computer code should be able to read a log file of observed events, and it can then evaluate the desired hazard profile. The current living PSA systems designed for risk monitoring manage to some extent repetitive evaluations of hazards levels following the logged history. However, practical computation algorithms for risk follow-up area including Bayesian inference must be developed further.

ACKNOWLEDGEMENT

This paper originated from the studies made in the Nordic research project 'Safety evaluation by use of living PSA and safety indicators, NKS/SIK-1 (1990–93)'. We thank Dr Urho Pulkkinen at VTT Automation for helpful comments. The writing was supported by a grant from the Academy of Finland.

REFERENCES

1. Bonaca, M. (ed.), *Living probabilistic safety assessment for nuclear power plant management.* Organization for Economic Co-operation and Development, Paris, 1990.
2. Holmberg, J., Johanson, G. & Niemelä, I., *Risk measures in living probabilistic safety assessment.* VTT Publications 146, Technical Research Centre of Finland, Espoo, 1993.
3. Holmberg, J., Operating experience feedback in probabilistic safety assessment. Licentiate thesis, Helsinki University of Technology, 1993.
4. Reactor Safety Study. An assessment of accident risks in U.S. commercial nuclear power plants. *Report WASH-1400, NUREG-75/014,* US Nuclear Regulatory Commission, Washington D.C., 1975.
5. Minarick, J. W., The US NRC accident sequence precursor program: present methods and findings. *Reliab. Engng & System Safety,* **27** (1990) 23–51.
6. Bier, V., Statistical methods for the use of accident precursor data in estimating frequency of rare events. *Reliab. Engng & System Safety,* **41** (1993) 267–280.
7. Johanson, G. & Holmberg, J. (eds), Safety evaluation by living probabilistic safety assessment. In *Procedures and Applications for Planning of Operational Activities and Analysis of Operating Experience,* SKI Technical Report 94:2, Swedish Nuclear Power Inspectorate, Stockholm, 1994, 108 p. + app.
8. Erhardsson, U.-K. & Flodin, Y., Momentaneous risk. R & D-project for living PSA. *Report PK-79/91, NKS/SIK-1(91)30,* Vattenfall, Stockholm, 1991 (in Swedish).
9. Holmberg, J., Pulkkinen, U., Laakso, K. & Mankamo, T., The risk follow-up by PSA—report of the Finnish pilot study. *Report VTT/SÄH 14/91, RISKI*(91)2, *NKS/SIK-1(91)27.* Technical Research Centre of Finland, Espoo, 1992.

10. Sandstedt, J., Demonstration studies on living PSA. *Report RELCON 13/92, NKS/SIK-1(92)49,* Relcon Ab, Sundbyberg, 1992.
11. Karr, A. F., *Point Processes and Their Statistical Inference.* Second Edition. Dekker, New York, 1991.
12. Arjas, E., Survival models and martingale dynamics. *Scandinavian J. Stat.,* **16** (1989) 177–225.
13. Arjas, E. & Gasbarra, D., Nonparametric Bayesian inference from right censored survival data, using the Gibbs sampler. *Statistica Sinica* **4** (1990) 505–524.
14. Lehtinen, E., Mankamo, T. & Pulkkinen, U., Optimum test interval of closing valves, *Nucl. Engng & Design,* **81** (1984) 99–104.
15. Vesely, W. E., Davis, T. C., Denning, R. S. & Saltos, N., Measures of risk importance and their applications. *Report NUREG/CR-3385,* Battelle Columbus Laboratories, Columbus, 1983, 107 p.
16. Horne, B. E., The use of probabilistic safety analysis methods for planning maintenance and testing unavailabilities of essential plant at Heysham 2 AGR power station. In *Use of probabilistic safety assessment to evaluate nuclear power plant technical specifications. Report IAEA-TECDOC-599,* Technical Committee meeting, Vienna, 18–22 June, 1990. International Atomic Energy Agency, Vienna, 1990, pp. 165–175.
17. Balfanz, H.-P., Dinsmore, S., Hussles, U., Musekamp, W. & Stuber, Safety analysis and information system (SAIS)—A living PSA computer system to support NPP-safety management and operator. *Reliab. Engng & System Safety,* **38** (1992) 181–191.
18. Poucet, A., STARS: Knowledge-based tools for safety and reliability analysis. *Reliab. Engng & System Safety,* **30** (1990) 379–397.
19. Niemelä, I., Properties of Finnish STUK PSA-code. In *Proc. 2nd TÜV-Workshop on Living-PSA-Application,* Hamburg, 7–8 May, 1990 (ed. H.-P. Balfanz) TÜV-Norddeutschland, 1990.
20. *Risk Spectrum PSA Users Manual,* Relcon Teknik AB, Sundbyberg, 1992.
21. Special Issue. *Reliab. Engng & System Safety,* **27** (1990).