Modélisation de fiabilité et de disponibilité pour des systèmes relatifs à la sécurité soumis au vieillissement

Florent Brissaud, Cyrille Folleau, Benoit de Cournuaud

▶ **To cite this version:**

Florent Brissaud, Cyrille Folleau, Benoit de Cournuaud. Modélisation de fiabilité et de disponibilité pour des systèmes relatifs à la sécurité soumis au vieillissement. Congrès Lambda Mu 23 " Innovations et maîtrise des risques pour un avenir durable " - 23e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement, Institut pour la Maîtrise des Risques, Oct 2022, Paris Saclay, France. ⟨hal-03878145⟩

HAL Id: hal-03878145

https://hal.science/hal-03878145v1

Submitted on 29 Nov 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

HAL Authorization

Institut pour la Maîtrise des Risques
Sûreté de Fonctionnement - Management - Cindyniques

Modélisation de fiabilité et de disponibilité pour des systèmes relatifs à la sécurité soumis au vieillissement

Modelling reliability and availability of ageing safety-related systems

Florent BRISSAUD
Research & Innovation Centre for Energy (RICE), GRTgaz
1 rue du Commandant d'Estienne d'Orves, 92390 Villeneuve-la-Garenne
florent.brissaud@grtgaz.com

Cyrille FOLLEAU
SATODEV
25 rue Marcel Issartier
33700 Mérignac
cyrille.folleau@satodev.fr

Benoit DE COURNUAUD
SATODEV
25 rue Marcel Issartier
33700 Mérignac
benoit.decournuaud@satodev.fr

***Résumé* —** Cet article propose des modèles de fiabilité et de disponibilité pour des systèmes soumis au vieillissement et à deux types de défaillance : détectées en ligne ; et uniquement révélées par des tests d'épreuve. Sont notamment concernés les systèmes relatifs à la sécurité. Les défaillances sont modélisées par des lois de Weibull. Des modèles de type « *arithmetic reduction of age* » (ARA) sont utilisés pour les tests d'épreuve, tandis que la maintenance corrective est supposée sans effet sur l'âge. Pour les défaillances détectées en ligne, un taux de réparation est considéré. Pour chaque type de défaillance, des formules analytiques sont proposées pour l'âge « virtuel », le taux de défaillance et l'indisponibilité d'un élément. Celles-ci ont ensuite été implémentées dans un logiciel d'analyse par arbre de défaillance afin de modéliser des systèmes aux architectures variées et dont les éléments sont sujets à divers types de défaillance.

Mots-clefs — Système relatif à la sécurité, vieillissement, loi de Weibull, test d'épreuve, maintenance imparfaite

***Abstract*—** This paper proposes reliability and availability models for ageing systems with two types of failure: detected on-line; and only revealed by proof tests. This includes safety-related systems. The failures are modelled by Weibull distribution. "Arithmetic reduction of age" (ARA) models are used for proof tests, while corrective maintenance has no effect on the age. For on-line detected failures, a repair rate is assumed. For each type of failure, analytical formulas are proposed for the "virtual" age, the failure rate, and the unavailability of an element. These formulas have been implemented in a fault tree analysis software tool to model systems with various architectures and elements subject to different types of failure.

Keywords — safety-related systems, ageing systems, Weibull distribution, proof tests, imperfect maintenance

I. INTRODUCTION

Les systèmes relatifs à la sécurité sont utilisés pour prévenir des accidents et/ou réduire leur gravité, par la mise en œuvre de fonctions de sécurité. Une fonction de sécurité est ainsi conçue pour assurer ou maintenir l'état de sécurité d'un équipement/système/installation, par rapport à un évènement dangereux spécifique.

En pratique, les systèmes relatifs à la sécurité sont fréquemment utilisés dans de nombreuses industries pour la maitrise des risques technologiques.

Un système relatif à la sécurité (e.g. soupape, protection contre les excès de température, système d'anti-pompage de compresseur…) est communément sujet à deux types de « défaillances aléatoires du matériel » [1, 2] : celles détectées en ligne (e.g. par des autotests de diagnostic automatique) ; et celles non-détectées en ligne mais uniquement relevées par des tests d'épreuve (e.g. tests périodiques réalisées pour détecter des défaillances « cachées »). L'évaluation de la fiabilité et de la disponibilité de ces systèmes, en tenant compte de ces deux types de défaillance, est décrite dans des normes [1], rapports techniques [3], livres [4, 5] et papiers scientifiques [6, 7]. Des modèles ont aussi été spécialement développés pour prendre en compte des caractéristiques particulières de tests d'épreuve [8, 9, 10] et pour optimiser les politiques de tests [11, 12, 13]. Généralement, les taux de défaillance sont considérés comme constants, ce qui ne prend donc pas en compte les phénomènes d'usure (impliquant un taux de défaillance croissant) souvent observés, notamment pour des matériels mécaniques [4]. Pour évaluer des systèmes relatifs à la sécurité soumis au vieillissement, des taux de défaillance sont par exemple modélisés par des lois de Weibull dans plusieurs travaux [14, 15], mais seulement pour des défaillances non-détectées en ligne et sans prendre en compte d'effet de maintenance sur l'âge. Un test d'épreuve est vu ici comme une action de maintenance préventive, c'est-à-dire, « effectuée pour limiter la dégradation et réduire la probabilité de défaillance » [16].

Dans la présente communication, des modèles de fiabilité et de disponibilité sont développés pour des systèmes soumis au vieillissement et aux défaillances détectées et non-détectées en ligne. De plus, l'effet de la maintenance préventive (tests d'épreuve) sur l'âge est pris en compte *via* des modèles de réduction d'âge (ARA), dits avec une « mémoire de niveau 1 » (ARA1) ou une « mémoire infinie » (ARA∞) [17, 18].

II. ELEMENT SOUMIS AU VIEILLISSEMENT ET A DES DEFAILLANCES DETECTEES EN LIGNE

A. Modélisation des défaillances détectées en ligne

À l'instant initial $t_0 = 0$, l'élément est âgé de Age_0 et est disponible. Ensuite, l'âge de l'élément au temps t est $Age_D(t)$. Toutes les défaillances considérées dans cette partie sont détectées en ligne, par exemple, par des autotests de diagnostic automatique. Le taux de défaillance de l'élément est $h_D(t)$, modélisé par une loi de Weibull avec un paramètre de forme β et un paramètre d'échelle η (par unité de temps). Lorsqu'une défaillance (détectée en ligne) se produit, la maintenance corrective débute immédiatement et l'élément est indisponible pour une durée qui suit une loi Exponentielle avec un taux (de réparation) μ (par unité de temps). À la suite d'une maintenance corrective, l'élément est « *as bad as old* » (ABAO) et, si une maintenance préventive est effectuée, celle-ci est supposée sans effet sur le taux des défaillances détectées en ligne. La disponibilité de l'élément au temps t est $A_D(t)$ et son indisponibilité est $U_D(t) = 1 - A_D(t)$.

B. Âge de l'élément

D'après les hypothèses et notations précédentes, l'âge de l'élément au temps t est :

$$Age_D(t) = t + Age_0 \quad (1)$$

C. Taux de défaillance de l'élément

D'après les hypothèses et notations précédentes, le taux des défaillances détectées en ligne de l'élément au temps t est :

$$h_D(t) = \frac{\beta}{\eta^\beta} \cdot Age_D(t)^{\beta-1} \quad (2)$$

Soit, en remplaçant $Age_D(t)$ par l'expression (1) :

$$h_D(t) = \frac{\beta}{\eta^\beta} \cdot (t + Age_0)^{\beta-1} \quad (3)$$

D. Indisponibilité de l'élément

La disponibilité de l'élément au temps $t + dt$, i.e. $A_D(t + dt)$, avec $dt > 0$ et dt qui tend vers 0, dépend de la disponibilité de l'élément au temps t, i.e. $A_D(t)$, selon ces cas disjoints :

- l'élément est disponible au temps t et ne subit pas de défaillance entre t et $t + dt$;
- l'élément n'est pas disponible au temps t et est réparé entre t et $t + dt$.

La probabilité que l'élément soit disponible au temps t est $A_D(t)$ et la probabilité qu'il ne soit pas disponible au temps t est $1 - A_D(t)$. D'après les hypothèses et notations précédentes, si l'élément est disponible au temps t, la probabilité qu'il subisse une défaillance entre t et $t + dt$ est $h_D(t) \cdot dt$. De même, si l'élément n'est pas disponible au temps t, la probabilité qu'il soit réparé entre t et $t + dt$ est $\mu \cdot dt$. Nous avons donc la relation suivante :

$$A_D(t + dt) = A_D(t) \cdot [1 - h_D(t) \cdot dt] + [1 - A_D(t)] \cdot \mu \cdot dt \quad (4)$$

La dérivée de $A_D(t)$ est donc :

$$A'_D(t) = \frac{A_D(t+dt) - A_D(t)}{dt} = \mu - A_D(t) \cdot [h_D(t) + \mu] \quad (5)$$

Soit, en remplaçant $h_D(t)$ par l'expression (3) :

$$A'_D(t) = \mu - A_D(t) \cdot \left[\frac{\beta}{\eta^\beta} \cdot (t + Age_0)^{\beta-1} + \mu\right] \quad (6)$$

La disponibilité peut ensuite être obtenue par résolution de cette équation différentielle, avec la condition initiale $A_D(0) = 1$ (disponibilité à l'instant initial). La solution suivante est alors obtenue à l'aide d'un solveur mathématique :

$$A_D(t) = e^{-\left(\frac{t+Age_0}{\eta}\right)^\beta - \mu \cdot t} \times \left[\mu \cdot \left(\int_0^t e^{\left(\frac{x+Age_0}{\eta}\right)^\beta + \mu \cdot x} dx\right) + e^{\left(\frac{Age_0}{\eta}\right)^\beta}\right] \quad (7)$$

Enfin, l'indisponibilité est déduite de la disponibilité :

$$U_D(t) = 1 - e^{-\left(\frac{t+Age_0}{\eta}\right)^\beta - \mu \cdot t} \times \left[\mu \cdot \left(\int_0^t e^{\left(\frac{x+Age_0}{\eta}\right)^\beta + \mu \cdot x} dx\right) + e^{\left(\frac{Age_0}{\eta}\right)^\beta}\right] \quad (8)$$

Ce résultat peut être interprété comme un cas particulier de [19], proposé pour la première fois dans [20].

III. ELEMENT SOUMIS AU VIEILLISSEMENT ET A DES DEFAILLANCES NON-DETECTEES EN LIGNE

A. Modélisation des défaillances non-détectées en ligne

À l'instant initial $t_0 = 0$, l'élément est âgé de Age_0 et est disponible. Ensuite, l'âge de l'élément au temps t est $Age_U(t)$. Toutes les défaillances considérées dans cette partie sont non-détectées en ligne et uniquement relevées par des tests d'épreuve, par exemple, des tests périodiques réalisées pour détecter des défaillances « cachées ». Le taux de défaillance de l'élément est $h_U(t)$, modélisé par une loi de Weibull avec un paramètre de forme β et un paramètre d'échelle η (par unité de temps). Lorsqu'une défaillance (non-détectée en ligne) se produit, l'élément est indisponible jusqu'au prochain test d'épreuve. Le premier test d'épreuve (à partir de t_0) est réalisé à T_0 et les suivants sont réalisés selon la période T_1 (i.e. $T_0 + T_1$, $T_0 + 2 \cdot T_1$, $T_0 + 3 \cdot T_1$…). n est le nombre de tests d'épreuve réalisés dans l'intervalle $[t_0 ; t[$. Chaque test d'épreuve permet de détecter une éventuelle défaillance et, le cas échéant, la maintenance corrective est réalisée immédiatement et l'élément redevient disponible. Les durées de maintenance préventive et corrective ne sont pas considérées ici pour l'indisponibilité. En effet, les tests d'épreuve sont souvent réalisés lorsque l'équipement/système/installation est à l'arrêt et que la fonction de sécurité n'est donc pas requise, ou alors pendant que des mesures compensatoires sont à l'œuvre.

Les tests d'épreuve, en tant qu'action de maintenance préventive, ont un effet sur l'âge de l'élément, selon un modèle ARA (cf. ci-après) et une efficacité α (facteur de réduction d'âge). Cet effet est considéré juste après la maintenance préventive qui consiste, par exemple, en un nettoyage de pièce encrassée, un remplacement de composant usé, une lubrification de pièce mobile, ou le réétalonnage de certains paramètres. Si applicable, la maintenance corrective induite est sans effet additionnel sur l'âge.

La disponibilité de l'élément au temps t est $A_U(t)$ et son indisponibilité est $U_U(t) = 1 - A_U(t)$.

B. Âge de l'élément

a) Modèle ARA1

Le modèle ARA1 considère un effet limité à l'âge pris depuis la dernière action de maintenance. Ainsi, à la suite d'une maintenance préventive (avec ou sans maintenance corrective induite), l'âge de l'élément pris depuis la précédente maintenance préventive (ou, à défaut, t_0) est réduit d'un facteur α.

Avant la première action de maintenance préventive ($n = 0$), l'âge de l'élément est $Age_{U1}(t) = t + Age_0$ (en considérant l'âge initial de l'élément). À la première action de maintenance préventive, l'âge de l'élément pris depuis t_0 est égal à T_0 puis, parce que réduit d'un facteur α, l'âge de l'élément après cette date et avant la prochaine action de maintenance préventive ($n = 1$) est $Age_{U1}(t) = (1 - \alpha)\cdot T_0 + Age_0 + t - T_0 = t + Age_0 - \alpha\cdot T_0$. À partir de là, $Age_{U1}(t)$ est un âge dit « virtuel » (car l'âge « réel » serait simplement la durée calendaire écoulée depuis la mise en service de l'élément). De même, dans la prochaine période de maintenance ($n = 2$), $Age_{U1}(t) = t + Age_0 - \alpha\cdot T_0 - \alpha\cdot T_1$, puis dans la période de maintenance suivante ($n = 3$), $Age_{U1}(t) = t + Age_0 - \alpha\cdot T_0 - 2\cdot\alpha\cdot T_1$ et ainsi de suite. Selon un modèle ARA1 et d'après les hypothèses et notations précédentes, l'âge (virtuel) de l'élément au temps t est ainsi :

$$Age_{U1}(t) = \begin{cases} t + Age_0 & si\ n = 0 \\ t + Age_0 - \alpha \cdot (T_0 + (n-1)\cdot T_1) & si\ n \geq 1 \end{cases} \quad (9)$$

b) Modèle ARA∞

Le modèle ARA∞ considère un effet sur l'âge pris depuis l' « origine ». Ainsi, à la suite d'une maintenance préventive (avec ou sans maintenance corrective induite), l'âge (virtuel) de l'élément est réduit d'un facteur α.

Avant la première action de maintenance préventive ($n = 0$), l'âge de l'élément est $Age_{U\infty}(t) = t + Age_0$ (en considérant l'âge initial de l'élément). À la première action de maintenance préventive, l'âge (virtuel) de l'élément est réduit d'un facteur α et devient, après cette date et avant la prochaine action de maintenance préventive ($n = 1$), $Age_{U\infty}(t) = (1 - \alpha)\cdot Age_{U\infty}(T_0) + t - T_0$, avec $Age_{U\infty}(T_0)$ tel que défini dans la période précédente (avec $n = 0$). De même, dans la prochaine période de maintenance ($n = 2$), $Age_{U\infty}(t) = (1 - \alpha)\cdot Age_{U\infty}(T_0 + T_1) + t - T_0 - T_1$, avec $Age_{U\infty}(T_0 + T_1)$ tel que défini dans la période précédente (avec $n = 1$), puis dans la période de maintenance suivante ($n = 3$), $Age_{U\infty}(t) = (1 - \alpha)\cdot Age_{U\infty}(T_0 - 2\cdot T_1) + t - T_0 - 2\cdot T_1$, avec $Age_{U\infty}(T_0 - 2\cdot T_1)$ tel que défini dans la période précédente (avec $n = 2$) et ainsi de suite. Selon un modèle ARA∞ et d'après les hypothèses et notations précédentes, l'âge (virtuel) de l'élément au temps t est alors obtenu par récurrence [20] :

$$Age_{U\infty}(t) = \begin{cases} t + Age_0 & si\ n = 0 \\ t - T_0 - (n-1)\cdot T_1 & \\ +(1-\alpha)^n \cdot (T_0 + Age_0) & \\ +(\sum_{i=1}^{n-1}(1-\alpha)^i)\cdot T_1 & si\ n \geq 1 \end{cases} \quad (10)$$

Soit, pour tout $n \geq 0$:

$$Age_{U\infty}(t) = t - T_0 - n\cdot T_1 + (1-\alpha)^n \cdot (T_0 + Age_0) + (\sum_{i=0}^{n-1}(1-\alpha)^i)\cdot T_1 \quad (11)$$

Puis, en utilisant les propriétés d'une suite géométrique de coefficient $(1 - \alpha)$:

$$Age_{U\infty}(t) = \begin{cases} t + Age_0 & si\ \alpha = 0\ ou\ n = 0 \\ t + (1-\alpha)^n \cdot Age_0 & \\ +[(1-\alpha)^n - 1]\cdot T_0 & \\ +\left(\frac{1}{\alpha} - \frac{(1-\alpha)^n}{\alpha} - n\right)\cdot T_1 & sinon \end{cases} \quad (12)$$

C. Taux de défaillance de l'élément

D'après les hypothèses et notations précédentes, le taux des défaillances non-détectées en ligne de l'élément au temps t est :

$$h_U(t) = \frac{\beta}{\eta^\beta}\cdot Age_U(t)^{\beta-1} \quad (13)$$

Avec $Age_U(t)$ défini par $Age_{U1}(t)$ de l'expression (9) dans le cas d'un modèle ARA1, ou défini par $Age_{U\infty}(t)$ de l'expression (12) dans le cas d'un modèle ARA∞.

D. Indisponibilité de l'élément

D'après les hypothèses et notations précédentes :

- l'élément est disponible au temps $t_0 = 0$ et toute défaillance se produisant entre t_0 et T_0 n'est réparée qu'au temps T_0, ainsi l'indisponibilité au temps t avec $t \leq T_0$ est égale à la défiabilité entre t_0 et t ;
- l'élément est disponible au temps $T_0 + (n-1)\cdot T_1$ pour $n = 1, 2, 3\ldots$ et toute défaillance se produisant entre $T_0 + (n-1)\cdot T_1$ et $T_0 + n\cdot T_1$ n'est réparée qu'au temps $T_0 + n\cdot T_1$, ainsi l'indisponibilité au temps t avec $T_0 + (n-1)\cdot T_1 < t \leq T_0 + n\cdot T_1$ est égale à la défiabilité entre $T_0 + (n-1)\cdot T_1$ et t.

L'indisponibilité de l'élément au temps t est donc (pour $n = 1, 2, 3\ldots$) :

$$U_U(t) = \begin{cases} 1 - e^{-\int_0^t h_U(u)\cdot du} & pour\ t \leq T_0 \\ 1 - e^{-\int_{T_0+(n-1)\cdot T_1}^{t} h_U(u)\cdot du} & \\ pour\ T_0 + (n-1)\cdot T_1 < t \leq T_0 + n\cdot T_1 & \end{cases} \quad (14)$$

Soit, en remplaçant $h_U(t)$ par l'expression (13) :

$$U_U(t) = \begin{cases} 1 - e^{-\frac{1}{\eta^\beta}\left[(t+Age_0)^\beta - Age_0{}^\beta\right]} & pour\ t \leq T_0 \\ 1 - e^{-\frac{1}{\eta^\beta}\left[Age_U(t)^\beta - Age_U(T_0+(n-1)\cdot T_1)^\beta\right]} & \\ pour\ T_0 + (n-1)\cdot T_1 < t \leq T_0 + n\cdot T_1 & \end{cases} \quad (15)$$

Avec $Age_U(t)$ défini par $Age_{U1}(t)$ de l'expression (9) dans le cas d'un modèle ARA1, ou défini par $Age_{U\infty}(t)$ de l'expression (12) dans le cas d'un modèle ARA∞.

IV. CAS D'ETUDE

A. *Logiciel d'arbre de défaillance*

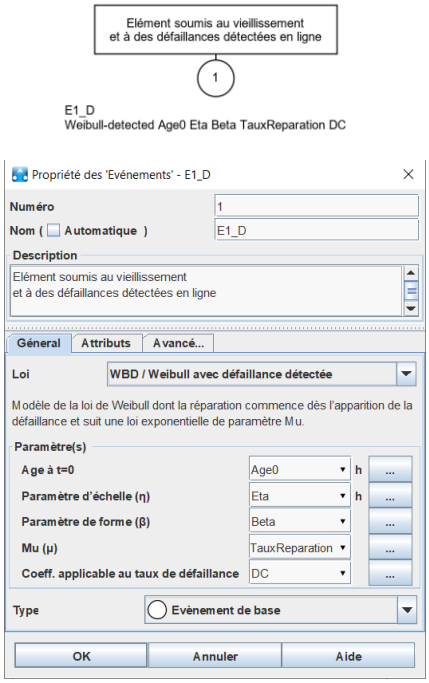

Fig. 1. Evènement de base pour un élément soumis au vieillissement et à des défaillances détectées en ligne

Pour faciliter l'utilisation des modèles développés, les formules ont été implémentées dans un logiciel d'analyse par arbre de défaillance (module Booléen du logiciel GRIF, développé par SATODEV pour le compte de TotalEnergies). En effet, les arbres de défaillance constituent un outil avec de nombreux avantages pour les ingénieurs [6] : aisé à utiliser et à (re)lire, avec de grandes capacités de modélisation et permettant des analyses performantes. Deux « lois » sont maintenant disponibles pour configurer un évènement de base : « *Weibull avec défaillance détectée* », qui correspond au modèle proposé dans la partie II ; et « *Weibull périodique* », qui correspond au modèle proposé dans la partie III. La représentation des évènements de base associés, avec les fenêtres de paramétrage correspondantes, sont présentés sur les figures 1 et 2 (captures d'écran du logiciel).

Pour la « *Weibull périodique* », le paramètre « *Modèle ARA* » est à *1* dans le cas d'un modèle ARA1 (sur la figure 2, le paramètre *ARA1 = 1*) et à *0* dans le cas d'un modèle ARA∞.

À noter qu'un « *coefficient applicable au taux de défaillance* » (dernier paramètre sur les figures 1 et 2) est aussi proposé parmi les paramètres. En accord avec l'expression du taux de défaillance d'une loi de Weibull (cf. expressions (3) ou (13)), multiplier le taux de défaillance par x est équivalent à multiplier le paramètre d'échelle η par $x^{-1/\beta}$. En pratique, ce coefficient est notamment utilisé pour décomposer un « taux de défaillance total » en combinaison de : « défaillances détectées en ligne » et « défaillances non-détectées en ligne », « défaillances indépendantes » et « défaillances de cause commune ». Il peut aussi être utile de considérer différents types de tests d'épreuve (par exemple, des tests partiels) avec différents paramètres (période, efficacité…).

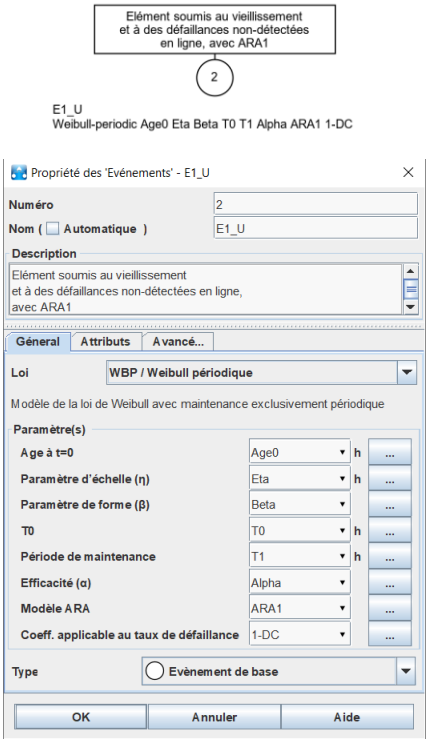

Fig. 2. Evènement de base pour un élément soumis au vieillissement et à des défaillances non-détectées en ligne

B. *Exemples de résultats pour un élément unique*

a) Element avec défaillances détectées en ligne

La figure 3 donne des exemples de résultats pour un éléments soumis au vieillissement et à des défaillances détectées en ligne, avec les paramètres suivants : $Age_0 = 4\,380$ *heures* (i.e. 6 mois), $\beta = 1{,}5$, $\eta = 10\,000$ *heures*, et $\mu = 0{,}0139$ *heures*$^{-1}$ (soit un temps moyen de réparation de 72 heures). De plus, le « coefficient applicable au taux de défaillance » est ici égal à *1*. Les résultats suivants sont obtenus par le logiciel d'analyse par arbre de défaillance (de haut en bas sur la figure 3) : taux de défaillance, fréquence de défaillance (qui ne doit pas être confondu avec le taux de défaillance [20]) et indisponibilité. À noter que les indisponibilités moyennes et fréquences moyennes de défaillance sont des mesures utilisées pour l' « intégrité de sécurité » [1, 2].

Le taux de défaillance et la fréquence de défaillance ne commencent pas à *0* parce que Age_0 n'est pas nul. La croissance rapide de l'indisponibilité en début d'analyse est due à l'hypothèse que le système est disponible à t_0. Lorsque le taux de défaillance est constant (i.e. $\beta = 1{,}0$), une valeur asymptotique est rapidement atteinte pour l'indisponibilité et la fréquence de défaillance (cf., par exemple, [4]). Cependant, les exemples de la figure 3 montrent que considérer uniquement des valeurs asymptotiques n'est pas approprié pour des éléments soumis au vieillissement.

b) Element avec défaillances non-détectées en ligne

La figure 4 donne des exemples de résultats pour un élément soumis au vieillissement et à des défaillances non-détectées en ligne, avec les paramètres suivants : $Age_0 = 4\,380$ *heures* (i.e. 6 mois), $\beta = 1{,}5$, $\eta = 10\,000$ *heures*, $T_0 = 4\,380$ *heures* (i.e. 6 mois), $T_1 = 8\,760$ *heures* (i.e. 1 an) et $\alpha = 0{,}3$. Deux modèles ARA sont considérés sur la figure 4 : ARA1 (en rouge) et ARA∞ (en bleu). De plus, le « coefficient applicable au taux de défaillance » est ici égal à *1*.

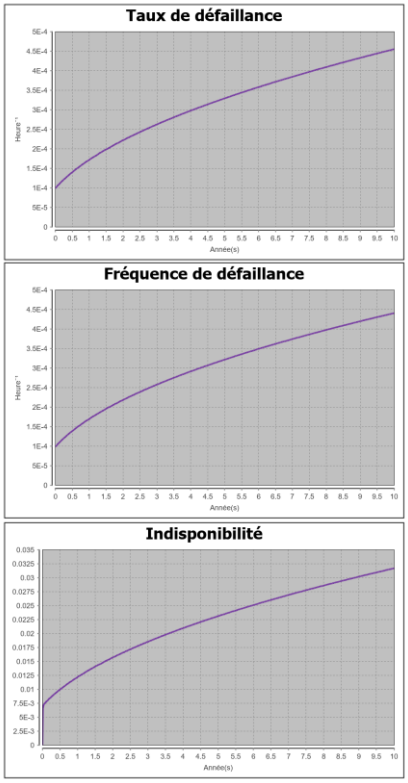

Fig. 3. Exemples de résultats pour un élément soumis au vieillissement et à des défaillances détectées en ligne

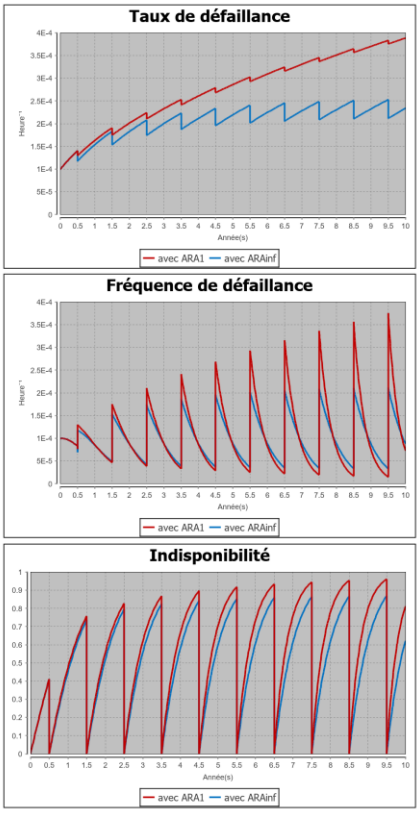

Fig. 4. Exemples de résultats pour un élément soumis au vieillissement et à des défaillances non-détectées en ligne

Afin de « valider » ces résultats obtenus par le logiciel d'analyse par arbre de défaillance, ceux-ci ont été comparés (et confirmés) par des simulations à l'aide de réseaux de Petri stochastiques à prédicats [22].

Dans les exemples de la figure 4, les taux de défaillance sont très différents des fréquences de défaillance (pour les calculs de fréquence de défaillance, voir [23]). Les tests d'épreuve impliquent des courbes en « dents de scie » : le premier test est réalisé à T_0 (0,5 an) et les suivants tous les T_1 (1 an). L'efficacité de maintenance (paramètre α) conditionne la taille de la « dent de scie » du taux de défaillance. Si cette efficacité était nulle, les deux modèles (ARA1 et ARA∞) produiraient les mêmes résultats. Les exemples de la figure 4 montrent qu'avec un modèle ARA1 le taux de défaillance a tendance à croître (en moyenne), tandis qu'avec un modèle ARA∞ il tend à atteindre un régime périodique. Les mêmes tendances sont observées pour l'indisponibilité et la fréquence de défaillance. Ainsi, l'utilisation de valeurs asymptotiques ne pourraient être une approximation valable que pour des valeurs moyennes dans le cas d'un modèle ARA∞.

c) Element avec défaillances détectées et non-détectées en ligne

La figure 5 donne un exemple d'arbre de défaillance et la figure 6 les résultats pour un élément soumis au vieillissement et à des défaillances détectées et non-détectées en ligne, avec les mêmes paramètres que les exemples précédents, à l'exception d'un « coefficient applicable au taux de défaillance » (nommé *DC* pour « *Diagnostic Coverage* ») égal à *0,9* pour les défaillances détectées en ligne et à *0,1* (i.e. *1 – DC*) pour les défaillances non-détectées en ligne. Ces deux types de défaillance sont connectées par une porte « OU » dans l'arbre de défaillance parce que l'élément peut être indisponible à cause de l'une ou l'autre de ces défaillances.

La figure 5 affiche aussi les valeurs moyennes d'indisponibilité (notée U_{avg}) et de fréquence de défaillance (notée W_{avg}) pour chaque évènement de base et porte logique, calculées sur 10 ans.

Avec le paramétrage défini ici, le taux de défaillance est égal à 90% du taux pour un élément soumis aux défaillances détectées en ligne (cf. figure 3) plus 10% du taux pour un élément soumis aux défaillances non-détectées en ligne (cf. figure 4). Ces résultats montrent que même si le taux et la fréquence de défaillance sont principalement impactés par les défaillances détectées en ligne, l'indisponibilité est quant à elle principalement due aux défaillances non-détectées en ligne. En effet, les défaillances détectées en ligne sont réparées très rapidement (ici, en 72 heures en moyenne) comparées aux défaillances non-détectées en ligne (révélées, et donc réparées, selon une période de 1 an). En pratique, la contribution des défaillances détectées en ligne est parfois même ignorée du calcul d'indisponibilité moyenne lorsque des approches « simplifiées » sont utilisées (cf., par exemple, [24]).

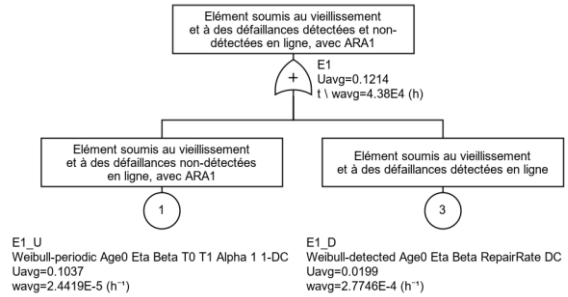

Fig. 5. Exemple d'arbre de défaillance pour un élément soumis au vieillissement et à des défaillances détectées et non-détectées en ligne

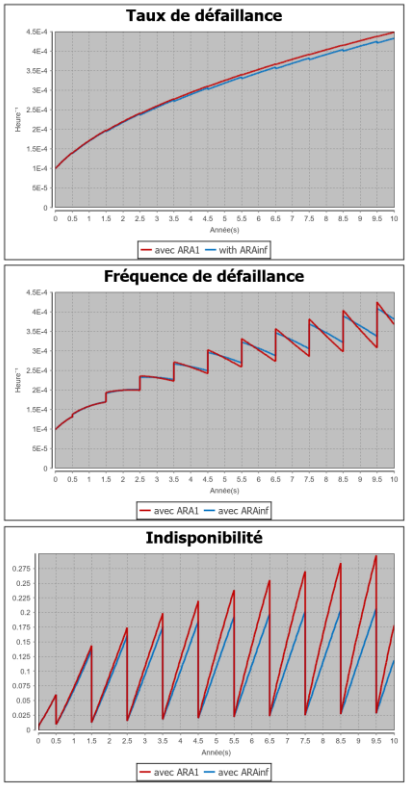

Fig. 6. Exemples de résultats pour un élément soumis au vieillissement et à des défaillances détectées et non-détectées en ligne

C. *Exemples de résultats pour un système*

a) Système avec trois éléments en série

L'exemple suivant concerne un système (S) composé de trois éléments en série : un transmetteur (T), une unité logique (LU) et une vanne (V). Chacun de ces éléments est sujet à des défaillances détectées et non-détectées en ligne, avec les données d'entrée de la table I. L'arbre de défaillance est présenté sur la figure 7 et les résultats sur la figure 8. Les valeurs moyennes d'indisponibilité (U_{avg}) et de fréquence de défaillance (W_{avg}) sont ici calculées sur 5 ans.

Ces résultats montrent que, dans cet exemple, le principal contributeur au taux de défaillance, à la fréquence de défaillance et (en grande partie) à l'indisponibilité du système est l'effet des défaillances non-détectées en ligne de la vanne. Une analyse de sensibilité portant sur le modèle de maintenance (ARA1 ou ARA∞) applicable à la vanne, ainsi que sur l'efficacité associée (α_V), est présentée sur la figure 9. Par rapport à la situation initiale (courbes rouges pour ARA∞ et milieu de l'axe des abscisses pour $\alpha_V = 0{,}5$), une hypothèse « *as good as new* (AGAN) » (i.e. $\alpha_V = 1{,}0$) conduirait à diviser l'indisponibilité moyenne par plus de deux.

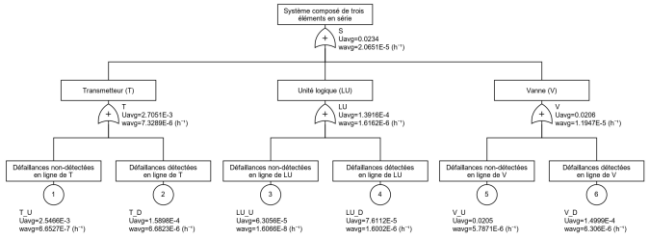

Fig. 7. Exemple d'arbre de défaillance pour un système composé de trois éléments en série, soumis au vieillissement et à des défaillances détectées et non-détectées en ligne

TABLE I. DONNEES D'ENTREE POUR UN SYSTEME COMPOSE DE TROIS ELEMENTS EN SERIE SOUMIS AU VIEILLISSEMENT

Élément	**Type de défaillance**	**Coefficient applicable au taux de défaillance**	**Paramètres (*m* : mois, *h* : heure)**	
Transmetteur (T)	Détectées en ligne	$DC_T = 0{,}90$	$Age_0 = 6\ m$ $\beta_T = 1{,}5$ $\eta_T = 1{\cdot}10^5\ h$	$\mu_T = 0{,}042\ /h$
	Non-détectées en ligne	$1\text{-}DC_T = 0{,}10$		ARA1 $T_0 = 6\ m$ $T_1 = 1\ an$ $\alpha_T = 0{,}3$
Unité Logique (LU)	Détectées en ligne	$DC_{LU} = 0{,}99$	$Age_0 = 6\ m$ $\beta_{LU} = 1{,}1$ $\eta_{LU} = 5{\cdot}10^4\ h$	$\mu_{LU} = 0{,}021\ /h$
	Non-détectées en ligne	$1\text{-}DC_{LU} = 0{,}01$		ARA1 $T_0 = 6\ m$ $T_1 = 1\ an$ $\alpha_{LU} = 0{,}1$
Vanne (V)	Détectées en ligne	$DC_V = 0{,}30$	$Age_0 = 6\ m$ $\beta_V = 2{,}0$ $\eta_V = 5{\cdot}10^4\ h$	$\mu_V = 0{,}042\ /h$
	Non-détectées en ligne	$1\text{-}DC_V = 0{,}70$		ARA∞ $T_0 = 6\ m$ $T_1 = 1\ an$ $\alpha_V = 0{,}5$

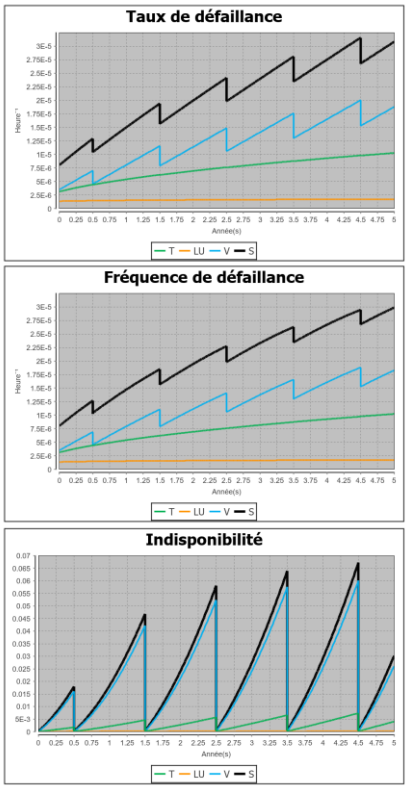

Fig. 8. Exemples de résultats pour un système composé de trois éléments en série, soumis au vieillissement et à des défaillances détectées et non-détectées en ligne

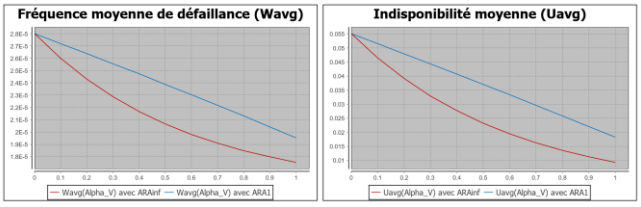

Fig. 9. Effet du modèle de maintenance préventive de la vanne et de l'efficacité associée sur l'indisponibilité et la fréquence moyenne de défaillance du système, caculées sur 5 ans

b) Système avec deux éléments en parallèle

L'exemple suivant concerne un système (S) composé de deux éléments en parallèle : deux vannes (V1 et V2) sujets à des défaillances non-détectées en ligne. De plus, des défaillances de cause commune (CCF) sont prises en compte *via* un modèle de facteur $\delta_V = 0{,}10$. Les données d'entrée sont présentées dans la table II, l'arbre de défaillance sur la figure 10 et les résultats sur la figure 11. Les valeurs moyennes d'indisponibilité (U_{avg}) et de fréquence de défaillance (W_{avg}) sont ici calculées sur 5 ans. Cet exemple montre que modéliser un système parallèle ne présente pas de difficulté particulière, même en considérant des défaillances de cause commune.

La figure 12 montre l'effet de différentes politiques de maintenance préventive sur les valeurs moyennes d'indisponibilité et de fréquence de défaillance du système. Les politiques de maintenance sont définies par une période de tests d'épreuve (T_1 = *6 mois*, *1 an*, ou *2 ans*) et une efficacité de maintenance (α_V = *0,25*, *0,50*, ou *0,75*). Ces résultats montrent que, par exemple, réduire la période de tests d'épreuve à *6 mois* ou améliorer l'efficacité de maintenance à *0,75* conduirait approximativement à une même réduction de l'indisponibilité moyenne d'environ 40%. Cependant, en termes de fréquence moyenne de défaillance, seule la seconde option conduirait à une réduction. Le choix d'une politique optimale de maintenance préventive doit ainsi dépendre des options possibles, des objectifs et des coûts.

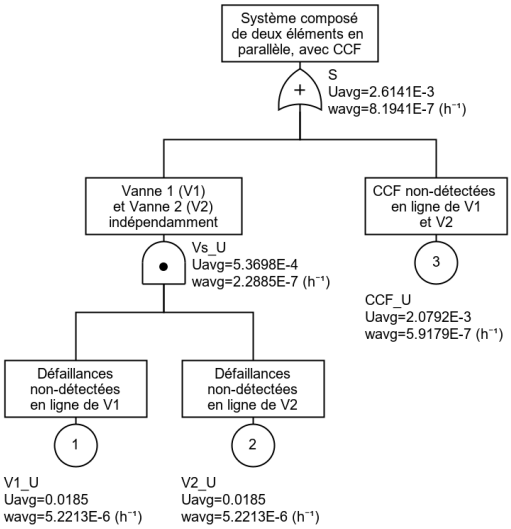

Fig. 10. Exemple d'arbre de défaillance pour un système composé de deux éléments en parallèle, soumis au vieillissement et à des défaillances non-détectées en ligne

TABLE II. DONNEES D'ENTREE POUR UN SYSTEME COMPOSE DE DEUX ELEMENTS EN PARALLELE SOUMIS AU VIEILLISSEMENT

Élément	**Type de défaillance**	**Coefficient applicable au taux de défaillance**	**Paramètres (*m* : mois, *h* : heure)**
Vanne 1 (V1)	Non-détectées en ligne	$1-\delta_V = 0{,}90$ $1\text{-}DC_V = 0{,}70$ $\underline{Total}$: 0,63	$Age_0 = 6\ m$ $\beta_V = 2{,}0$ $\eta_V = 5{\cdot}10^4\ h$ ARA∞ $T_0 = 6\ m$ $T_1 = 1\ an$ $\alpha_V = 0{,}5$
Vanne 2 (V2)	Non-détectées en ligne	$1-\delta_V = 0{,}90$ $1\text{-}DC_V = 0{,}70$ $\underline{Total}$: 0,63	
Défaillance de cause commune (CCF)	Non-détectées en ligne	$\delta_V = 0{,}10$ $1\text{-}DC_V = 0{,}70$ $\underline{Total}$: 0,07	

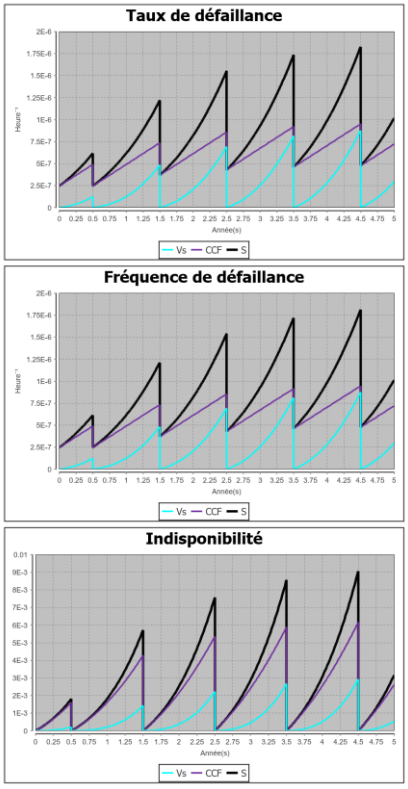

Fig. 11. Exemples de résultats pour un système composé de deux éléments en parallèle, soumis au vieillissement et à des défaillances non-détectées en ligne

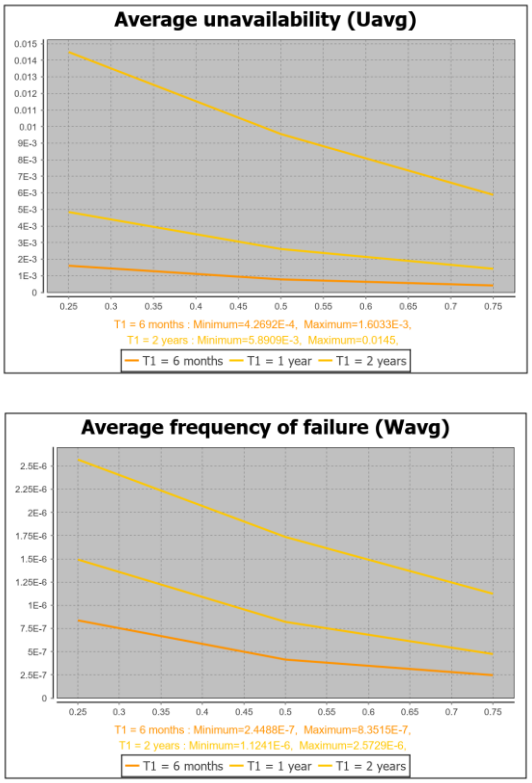

Fig. 12. Effet de différentes politiques de maintenance préventive sur l'indisponibilité et la fréquence moyenne de défaillance du système, caculées sur 5 ans

V. CONCLUSIONS

Des modèles de fiabilité et de disponibilité ont été développés pour des systèmes soumis au vieillissement, à des défaillances détectées en ligne et à des défaillances uniquement révélées par des tests d'épreuve, dont font notamment partie les systèmes relatifs à la sécurité. L'effet de la maintenance préventive (tests d'épreuve) sur l'âge est pris en compte via des modèles de réduction d'âge (ARA), dits avec une « mémoire de niveau 1 » (ARA1) ou une « mémoire infinie » (ARA∞).

Pour chaque type de défaillance, des formules analytiques ont d'abord été proposées pour l'âge « virtuel », le taux de défaillance et l'indisponibilité d'un élément. Ensuite, ces formules ont été implémentées dans un logiciel d'analyse par arbre de défaillance afin de modéliser des systèmes aux architectures variées, notamment des systèmes série/parallèle et, par exemple, aussi soumis à des défaillances de cause commune.

D'autres développements sont en cours afin notamment de prendre en compte l'effet de la maintenance corrective sur l'âge et d'estimer les paramètres des modèles à partir du retour d'expérience. Les méthodes d'estimation envisagées consistent par exemple à combiner des travaux sur l'estimation des taux de défaillance de systèmes relatifs à la sécurité [25] avec d'autres sur l'estimation de modèles et d'efficacité de maintenance [26].

Les modèles proposés permettent une meilleure évaluation de l'intégrité de sécurité de systèmes relatifs à la sécurité, lorsque certains éléments sont soumis au vieillissement et que des tests d'épreuve sont aussi utilisés pour maîtriser les dégradations/dérives/usures. Ces modèles peuvent alors éviter de sous-estimer l'indisponibilité et la fréquence de défaillance de certains systèmes (et donc des risques) grâce à une prise en compte de phénomènes de dégradation. Enfin, les résultats fournissent aussi une aide à la décision pour optimiser des politiques de maintenance, en particulier les choix concernant les tests d'épreuve. L'implémentation de ces modèles dans un logiciel d'analyse par arbre de défaillance a notamment déjà été exploité par GRTgaz dans le cadre de la gestion de ses actifs industriels [27].

REFERENCES

[1] IEC 61508: 2010. Functional safety of electrical / electronic / programmable electronic safety-related systems. International Electrotechnical Commission, 2010.

[2] IEC 61511: 2016. Functional safety – Safety instrumented systems for the process industry sector. International Electrotechnical Commission, 2016.

[3] ISO/TR 12489:2013. Petroleum, petrochemical and natural gas industries - Reliability modelling and calculation of safety systems. International Organization for Standardization, 2013.

[4] M. Rausand and A. Høyland, System Reliability Theory: Models, Statistical methods, and Applications. 2nd ed. Wiley, 2004.

[5] J.-P. Signoret and A. Leroy. "Reliability Assessment of Safety and Production Systems - Analysis, Modelling, Calculations and Case Studies," Springer, 2021.

[6] F. Brissaud and L. F. Oliveira. "Average probability of a dangerous failure on demand: Different modelling methods, similar results," 11th International Probabilistic Safety Assessment and Management Conference and Annual European Safety and Reliability Conference, Helsinki, Finland, 2012.

[7] J.-P. Signoret, S. Collas, and R. Ostebo. "Reliability modelling and calculation of safety systems: ISO/TR 12489: Presentation and application in TOTAL," 11th TÜV Rheinland International Symposium, Functional Safety in Industrial Applications, Cologne, Germany, 2014.

[8] F. Brissaud, A. Barros, and C. Bérenguer. "Probability of Failure of Safety-Critical Systems Subject to Partial Tests," Proceedings of the 56th Annual Reliability and Maintainability Symposium, San Jose, USA, 2010.

[9] H. Jin, and M. Rausand. "Reliability of safety-instrumented systems subject to partial testing and common-cause failures," Reliability Engineering & System Safety, vol. 121, p. 146-151, 2014.

[10] Y. Liu, and M. Rausand. "Proof-testing strategies induced by dangerous detected failures of safety-instrumented systems," *Reliability Engineering & System Safety*, vol. 145, p. 366-372, 2016.

[11] J. L. Rouvroye, and J. A. M. Wiegerinck. "Minimizing costs while meeting safety requirements: Modeling deterministic (imperfect) staggered tests using standard Markov models for SIL calculations," ISA Transactions, vol. 45, p. 611-621, 2006.

[12] F. Brissaud, A. Barros, and C. Bérenguer. "Probability of failure on demand of safety systems: impact of partial test distribution," Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, vol. 226(4), p. 426-436, 2012.

[13] F. Brissaud, C. Vinuesa, and C. Folleau. "Optimizing Proof test Policy for Redundant Safety-related Systems," Proceedings of the 29th European Safety and Reliability Conference, Hannover, Germany, 2019.

[14] E. Rogova, G. Lodewijks, and M. A. Lundteigen. "Analytical formulas of PFD and PFH calculation for systems with nonconstant failure rates," Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, vol. 231(4), p. 373-382, 2017.

[15] S. Wu, L. Zhang, M. A. Lundteigen, Y. Liu, and W. Zheng. "Reliability assessment for final elements of SISs with time dependent failures," Journal of Loss Prevention in the Process Industries, vol. 51, p. 186-199, 2018.

[16] IEC 60050-1992: 2015. International Electrotechnical Vocabulary (IEV) - Part 192: Dependability.

[17] H. Pham, and H. Wang. "Imperfect maintenance," European Journal of Operational Research, vol. 96, p. 452-438, 1996.

[18] L. Doyen, and O. Gaudoin. "Classes of imperfect repair models based on reduction of failure intensity of virtual age," Reliability Engineering and System Safety, vol. 84, p. 45-56, 2004.

[19] S. Bahri, F. Ghribi, H. Ben Bacha. "A Study of Asymptotic Availability Modelling for a Failure and a Repair Rates Following a Weibull Distribution," Reliability & Risk Analysis: Theory & Applications, p. 30-42, 2009.

[20] F. Brissaud, C. Folleau, and B. de Cournuaud. "Reliability and availability models for ageing safety-related systems," Journal of Loss Prevention in the Process Industries, vol. 75, 2022.

[21] F. Brissaud, and D. Turcinovic. "Functional Safety for Safety-Related Systems: 10 Common Mistakes," Safety and Reliability of Complex Engineered Systems, 2015.

[22] F. Brissaud, and C. Folleau. "Modeling Imperfect Maintenance with Stochastic Petri Nets," *Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference*, Venice, Italy, 2020.

[23] J.-P. Signoret, Y. Dutuit, S. Collas, P.-J. Cacheux, C. Folleau, and P. Thomas. "Assessment of the expected number and frequency of failures of periodically tested systems," Reliability Engineering and System Safety, vol. 118, p. 61-70, 2013.

[24] S. Hauge, T. Kråknes, S. Håbrekke, and H. Jin. Reliability Prediction Method for Safety Instrumented Systems, PDS Method Handbook. SINTEF, 2013.

[25] F. Brissaud. "Using field feedback to estimate failure rates of safety-related systems," Reliability Engineering and System Safety, vol. 159, p. 206-213, 2017.

[26] L. Doyen, and O. Gaudoin. "Modeling and Assessment of Aging and Efficiency of Corrective and Planned Preventive Maintenance," IEE Transactions on Reliability, vol. 60, p. 759-769, 2011.

[27] F. Brissaud. "Automatic fault trees generation and analysis for gas transmission units," Proceedings of the 31th European Safety and Reliability Conference, Angers, France, 2021.