# Vers une meilleure intégration de la gestion des stocks de rechanges dans les évaluations probabilistes de sûreté

Nicolas Le Berre, David Le Galliot, Thierry Thomas

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

# Vers une meilleure intégration de la gestion des stocks de rechanges dans les évaluations probabilistes de sûreté
# For an improved integration of spare parts management in probabilistic safety assessments

Nicolas LE BERRE
THALES Defense & Mission Systems
Brest, France
nicolas.leberre@fr.thalesgroup.com

David LE GALLIOT
SOM LIGERON®
Guipavas, France
david.le.galliot@ligeron.com

Thierry THOMAS
NAVAL GROUP
Brest, France
thierry-a.thomas@naval-group.com

***Résumé*— Nous proposons une méthodologie destinée à améliorer la prise en compte de paramètres logistiques tels que les délais d'approvisionnement dans le cadre d'études probabilistes de sûreté réalisées par la méthode des arbres de défaillance.**

***Mots-clés*— Sûreté nucléaire, démonstrations probabilistes, arbres de défaillance, gestion des stocks de rechanges**

**Summary— We propose a methodology to improve the integration of logistic parameters such as supply times in probabilistic safety studies carried out by fault tree method.**

***Keywords*—Nuclear Safety, probabilistic demonstrations, fault tree method, spare parts management**

## I. INTRODUCTION

### A. Contexte réglementaire

Les Installations de Soutien à Terre (IST) des Systèmes Nucléaires Militaires (SNM) sont soumises à des exigences probabilistes de sûreté qui prennent usuellement la forme d'exigences de disponibilité ou de fréquence de panne sur une période donnée. Ces exigences sont traitées dans le cadre de démonstrations de sûreté qui doivent obtenir l'approbation de l'autorité de sûreté nucléaire : à cet effet l'outil privilégié pour ces démonstrations reste l'arbre de défaillances.

Pour la réalisation sûre de leur mission ces installations s'appuient généralement sur des architectures fortement redondées. Dès lors la démonstration d'exigences de disponibilité ou de fréquence de panne repose, outre la fiabilité des matériels, sur le délai de remise en service d'un équipement défaillant, et par extension sur des problématiques logistiques telles que l'état des stocks de rechanges disponibles ou l'engagement des fournisseurs en termes de délai de réparation ou de réapprovisionnement.

Aujourd'hui l'usage communément admis consiste à confier aux équipes de sûreté de fonctionnement chargées de justifier les exigences probabilistes la tâche d'identification des équipements, dits articles de rechange SN, pour lesquels il sera nécessaire de disposer localement d'un stock de rechanges ; dans le cadre des démonstrations il sera alors considéré dans l'analyse de sûreté que le stock de rechanges est suffisamment dimensionné.

Le dimensionnement des stocks de rechanges est pour sa part confié aux équipes du soutien logistique intégré ; l'usage consiste alors à justifier, pour chaque équipement nécessaire, d'une probabilité de non rupture de stock forfaitaire, hors considérations liées aux exigences probabilistes.

Dès lors la démarche de justification des exigences probabilistes ainsi conduite apparaît lacunaire puisqu'elle n'envisage pas l'hypothèse d'une rupture de stock pour l'un ou l'autre des articles de rechange SN, alors même que le dimensionnement du stock associé à ces articles est basé sur le calcul de la probabilité qu'une rupture de stock survienne.

### B. Objectifs

La méthode que nous proposons ici vise à intégrer à la démonstration de sûreté une politique de gestion des stocks de type réapprovisionnement à la demande, afin de consolider les hypothèses des démonstrations de sûreté en termes de Mean Down Time (MDT) en tenant compte de paramètres logistiques tels que l'état des stocks et les délais de réapprovisionnement.

Puis nous proposons d'automatiser la définition d'un stock minimal de rechanges optimisé en regard de sa valeur et du respect des exigences.

### C. Approche

Nous détaillons dans un premier temps un cas d'application de la théorie des files d'attente pour un équipement considéré URL soutenu par une chaîne logistique simple constituée localement d'un stock de rechanges et d'une équipe apte à son remplacement, ainsi que d'un atelier de réparation (ou fournisseur) distant. Nous définirons ainsi un temps d'attente logistique moyen pour le remplacement de cet équipement en cas de défaillance.

Nous tirons ensuite avantage de l'Interface Applicative de Programmation (API) intégrée au logiciel d'arbres de défaillance « Arbre-Analyst » [1][2], pour gérer directement dans l'arbre de défaillance les paramètres logistiques précédemment évoqués, par réactualisation automatisée des paramètres de l'arbre associés aux temps de réparation (paramètres « TR » associé à une loi réparable) des différentes URL.

Nous proposons enfin une méthode de recherche de solutions optimales en termes de niveau de performance atteint vis-à-vis du coût du stock envisagé.

Nous conclurons enfin sur l'application de cette méthode à un cas industriel réel et confronterons les résultats ainsi obtenus à ceux issus de l'approche plus traditionnelle.

## II. CAS INDUSTRIEL

### A. *Contexte réglementaire*

La méthodologie de sûreté nucléaire imposée par les autorités françaises pour les Systèmes Nucléaires Militaires (sous-marins nucléaires, porte-avions, …) intègre notamment la justification d'objectifs de sûreté probabilistes.

Les Installations de Soutien à Terre (IST) assurent des fonctions importantes pour la sûreté des chaufferies nucléaires embarquées lorsque le SNM est à quai ou au bassin. En particulier, lors des interventions pour entretiens, les IST assurent des fonctions de servitudes essentielles, qui sont normalement assurées par les installations propres du navire (alimentation électrique, réfrigération, …).

Une grande partie des évènements redoutés (ER) relatifs à ces installations, sont ainsi liés à des pertes de prestations, pouvant résulter:

- de défaillances systémiques, pouvant être à l'origine d'un évènement initiateur ou à la perte d'une barrière de sûreté ;
- d'agressions internes ou externes (incendie, explosion, séisme, foudre, …).

Les objectifs de sûreté probabilistes associés à ces ER sont exprimés sous la forme de Fréquence Annuelle d'Occurrence (FAO), souvent associée à une durée (> x h).

Parmi les méthodes de modélisation disponibles en sûreté de fonctionnement et permettant de justifier ces objectifs, c'est la méthode des arbres de défaillances, qui s'est imposée jusqu'à présent [4], notamment en raison :

- de la diversité des scénarios à analyser, qui nécessite une méthode pouvant s'adapter à des cas des figures variés, des architectures complexes et des évènements hétérogènes,
- d'une simplicité de relecture (apparente) par un tiers, nécessaire lors d'un processus d'instruction avec de multiples relecteurs/approbateurs, au profil différent.

Au niveau de la modélisation, les règles de conception imposent en particulier que la prise en compte des temps de réparation dans les calculs de fiabilité soit limitée autant que faire se peut, et justifiée précisément dans tous les cas.

Afin de respecter cette exigence, il est nécessaire de mettre en place une démarche d'optimisation, visant à déterminer pour chaque équipement, la logistique (nature et périodicité des maintenances, rechanges, etc.) indispensable pour démontrer les objectifs de sûreté probabiliste.

### B. *Cas d'étude industriel*

Le cas d'étude industriel servant à illustrer la démarche est une station de pompage d'un bassin. La fonction de cette IST est de permettre l'échouage et le déséchouage du navire dans le bassin, ainsi que le maintien du niveau d'eau à un niveau souhaité (à sec ou en eau).

Cette installation est essentiellement composée d'installations de pompage, de moyens d'isolement assurant l'étanchéité du bassin (génie civil, vannes, aqueducs, …) et de servitudes (électrique, hydraulique, …).

Au niveau de la sûreté nucléaire, elle peut être à l'origine d'une perte de servitudes essentielles du SNM (alimentation électrique, réfrigération, …) en cas de baisse ou de montée intempestive du niveau d'eau.

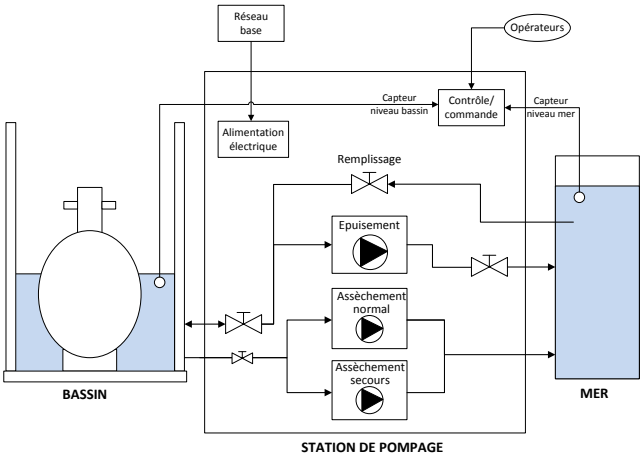


Fig. 1. Architecture simplifiée d'une station de pompage

L'architecture de cette installation est fortement redondée à de multiples niveaux et permet ainsi d'envisager de nombreux scénarios de reconfiguration en cas de défaillance.

Enfin, sur une base navale, il peut exister plusieurs bassins : ainsi, un même stock de rechanges doit permettre de couvrir les besoins de plusieurs stations de pompage identiques.

L'évènement redouté que nous devons analyser concerne le déséchouage intempestif d'un SNM provoqué par une indisponibilité, sur un temps suffisamment long, des moyens de pompage.

### C. *Problématique rencontrée*

A ce jour, en l'absence d'outils spécifiques, la procédure d'établissement de la liste des candidats aux rechanges dans le cadre des études de sûreté consiste en un processus itératif, qui partant d'une liste initiale vide, abouti à une première évaluation de la sûreté de l'installation ; puis lorsque celle-ci ne respecte pas les objectifs qui lui sont alloués, vient rajouter progressivement les composants les plus critiques en rechange et ce jusqu'à ce que cette liste minimale de rechanges soit suffisante pour démontrer la tenue des objectifs de sûreté.

La hiérarchisation des composants suivant leur criticité repose usuellement sur le choix de facteurs d'importance, dont les plus couramment utilisés dans le cadre de cet exercice sont le facteur d'importance de Fussel-Vesely (FV)

et le facteur d'importance d'augmentation du risque (FAR). Ce processus est illustré par le synoptique suivant.

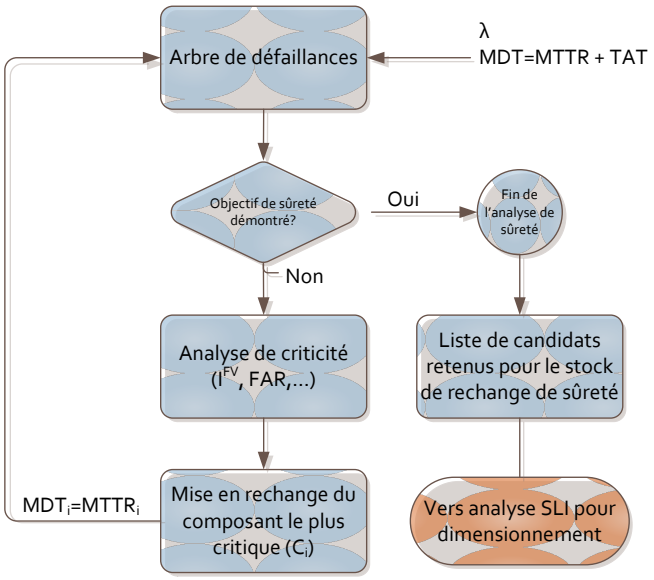


Fig. 2. Processus actuel d'élaboration du stock de rechange SN

La signification des acronymes utilisés ci-dessus est détaillée aux paragraphes III.B et III.C ; très rapidement ils désignent :

- λ : le taux de défaillance d'un équipement,
- MDT : Mean Down Time
- MTTR : Mean Time To Repair
- TAT : Turn-Around Time

Cette méthode présente un certain nombre d'inconvénients ; à commencer par celui d'être très chronophage puisqu'il s'agit d'un processus itératif réalisé manuellement en l'absence d'outils dédiés intégrés nativement dans les logiciels d'arbre de défaillances. Ce processus itératif doit de plus être entièrement relancé à chaque modification d'architecture (rajout ou suppression de composants, modifications des données de fiabilité,…).

Elle repose également sur le choix des facteurs d'importance retenus pour hiérarchiser les composants suivant leur criticité, dont le choix, les significations et les interprétations peuvent faire débat. Dans tous les cas ces facteurs d'importance ($I^{FV}$, FAR) correspondent à une analyse événement de base par événement de base, et ne permettent donc pas de tenir compte de la mutualisation des rechanges entre plusieurs composants identiques.

Pour finir, ce processus transfère entièrement la responsabilité du dimensionnement du stock SN à l'ingénierie du Soutien Logistique Intégré (SLI), dont l'activité porte par définition sur le soutien et non sur la sûreté, a fortiori sur l'aspect probabiliste des études SN.

Ainsi le dimensionnement du stock de rechange SN est réalisé indépendamment du niveau d'exigence auquel est soumise l'installation ; les études SLI portent généralement sur la justification d'un niveau de Probabilité de Non-Rupture de Stock (PNRS). S'agissant d'un stock de sûreté cet objectif de PNRS peut être sévérisé, pouvant atteindre 95% ; mais il reste sans lien direct avec les objectifs probabilistes de sûreté.

La problématique ainsi posée est donc la suivante : pouvons-nous trouver une solution permettant d'assurer la continuité de la démonstration de l'exigence de sûreté jusqu'au dimensionnement du stock de rechange adapté ?

## III. DESCRIPTION DE LA METHODE PROPOSEE

La recherche d'une réponse adaptée à la problématique précédemment introduite appelle deux axes de réflexion :

- Dans un premier temps il s'agira de rechercher, pour une Unité Remplaçable en Ligne (URL) donnée, une expression réaliste du temps moyen d'indisponibilité, ou Mean Down Time (MDT), à partir des caractéristiques du modèle de soutien adapté. Une fois établie cette expression nous l'intègrerons dans un modèle d'arbre de défaillances.
- Dans un second temps nous chercherons à définir un algorithme destiné à automatiser la tâche itérative visant à extraire le stock minimal le plus pertinent vis-à-vis du niveau d'exigence fixé.

### A. *Solutions existantes*

Parmi les solutions commerciales existantes plusieurs pourraient être envisagées pour répondre à la problématique traitée dans le cadre de cet article.

Une première voie consisterait à se tourner vers les nombreux outils de modélisation par réseaux de Pétri, qui permettent la simulation du comportement dynamique d'un système à évènements discrets, dans notre cas l'évolution temporelle de l'état d'un stock et son impact sur la fiabilité d'un système.

Si d'un point de vue technique cette solution s'avère pertinente, il doit être gardé à l'esprit que la finalité d'une étude probabiliste de sûreté reste d'obtenir l'assentiment de l'Autorité de Sûreté Nucléaire Défense (ASND) ; en l'état actuel cette dernière doit généralement se prononcer sur la validité d'un modèle sur la base, non pas du modèle en lui-même, mais de sorties graphiques intégrées au référentiel documentaire portant la justification de sûreté. Cela explique la prééminence, dans ce domaine, des modélisations statiques notamment par arbres de défaillances, du fait de leur relative facilité d'interprétation et de validation « sur papier ».

Regardons maintenant du côté des outils centrés sur le Soutien Logistique Intégré (SLI). Les deux logiciels commerciaux suivants, reconnus dans le domaine de la défense et notamment utilisés par la Direction Générale de l'Armement (DGA), nous ont plus particulièrement intéressés en regard de notre problématique :

- OPUS10, édité par Systecon.
- SIMLOG, édité par Apsys.

D'une manière générale ces deux logiciels sont destinés, à partir d'une représentation du système étudié, d'une description du système de soutien associé et d'informations sur la structure de coûts de l'ensemble, à la recherche d'une solution permettant de maximiser la disponibilité du système tout en minimisant les dépenses induites par son soutien.

Qu'il s'agisse de la structure de soutien ou de la structure de coûts, les capacités de modélisation de ces solutions sont très avancées et vont bien au-delà de ce qui est recherché dans cet article.

En revanche les capacités de modélisation d'un système fonctionnel y sont limitées. OPUS10 permet essentiellement la modélisation d'un système « série » ; il est possible d'y intégrer des principes de redondance, mais dans un cadre restrictif. Simlog n'a pu être testé mais autoriserait une modélisation de type Bloc Diagramme de Fiabilité (BDF).

Dans le cas de la sûreté nucléaire la modélisation par Arbres de Défaillances (AdD) est quasi-systématiquement privilégiée aux BDF et promue par l'autorité de sûreté nucléaire [4]. La construction déductive d'un arbre de défaillance, partant d'un évènement redouté directement issu des exigences de sûreté, se prête idéalement à ce type de démonstration ; cette méthode permet également la prise en compte de barrières tierces (intervention humaine, reconfiguration, moyens de mitigation externes…) qui sont difficilement envisageables pour un BDF.

A ce stade aucune solution existante ne nous semble donc parfaitement répondre au besoin.

### *B. Notations*

Nous précisons ci-après certaines notations d'usage dans le domaine de la sûreté nucléaire de défense. Ces notations ne correspondent pas nécessairement aux définitions normalisées ou communément admises ; elles seront néanmoins appliquées par la suite.

Par Mean Time To Repair (MTTR) est désigné le délai entre l'occurrence d'une panne et la remise en service de l'équipement concerné, considérant la pièce de rechange nécessaire disponible dans le stock de l'exploitant. Ainsi le MTTR couvre dans notre cas :

- le délai d'identification et de localisation de la défaillance,
- les délais administratifs notamment liés à l'obtention des nécessaires autorisations d'intervention sur une installation nucléaire,
- les délais associés aux tâches de dépose (puis pose) de l'équipement en panne,
- les délais logistiques liés aux opérations internes : transfert de pièces entre le stock de l'exploitant et l'installation nucléaire.

Le Mean Down Time (MDT) désigne quant à lui le délai entre l'occurrence d'une panne et la remise en service de l'équipement concerné, que la pièce de rechange nécessaire soit disponible dans le stock de l'exploitant ou non.

Le Mean Waiting Time (MWT) désigne enfin le temps moyen d'attendu de commande, c'est-à-dire le délai s'écoulant entre l'arrivée d'une demande au stock de l'exploitant et son service, hors temps liés à la logistique interne du stock.

A partir de ces trois notations nous pouvons finalement écrire l'égalité suivante :

$$MDT = MTTR + MWT \quad (1)$$

### *C. Organisation du soutien*

Nous considérons dans un premier temps un système simple constitué d'un seul type d'Unité Remplaçable en Ligne, en n exemplaires. Pour ce type d'URL le taux de défaillance est désigné λ.

La structure de soutien que nous souhaitons considérer est alors illustrée ci-après.

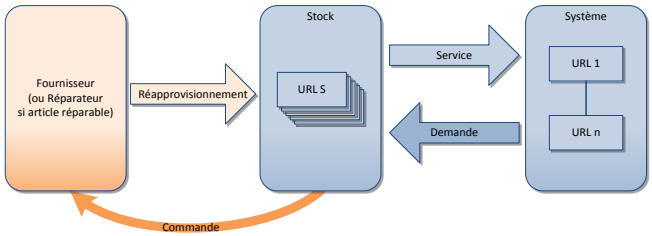


Fig. 3. Stucture de soutien considérée

Le système de soutien est donc constitué de deux niveaux :

- Au premier niveau, un stock de pièces de rechanges, sous responsabilité de l'exploitant de l'installation et situé à proximité de cette dernière, permet de répondre rapidement aux demandes émises suite à la défaillance d'un équipement,
- Au second niveau, un fournisseur (s'il s'agit d'un article consommable) ou un réparateur (si l'article peut être réparé) permettent de soutenir et recompléter le stock dans un second temps.

Le système émet une demande au stock dès lors que l'un des composants connaît une défaillance. Le taux de demandes reçues par le stock s'écrit ici simplement nλ.

Pour un article donné le stock est considéré soumis à une politique de gestion de type (S-1, S) ; c'est-à-dire qu'une opération de recomplètement, soit par rachat d'un consommable, soit par envoi en réparation de l'article défaillant, est déclenchée dès lors qu'une demande est reçue.

En parallèle du recomplètement, en fonction du nombre de pièces de rechanges disponibles, deux réponses peuvent être apportées par le stock à la réception d'une demande :

- Soit le stock contient au moins une pièce de rechange : alors la demande peut être servie immédiatement, le temps d'attente est nul ;
- Soit le stock est vide : la demande doit alors être mise en attente et ne pourra être servie qu'à réception du prochain réapprovisionnement.

Le fournisseur est quant à lui considéré engagé sur un temps d'approvisionnement ; de même si l'article est réparable, le réparateur est considéré engagé sur un temps de réparation. Dans les deux cas le temps courant du départ du stock (d'une commande ou de la pièce à réparer) jusqu'au retour en stock d'une pièce fonctionnelle sera désigné TAT, pour Turn Around Time.

La figure suivante illustre, pour un cas fictif, l'évolution d'une variable s(t) représentative de l'état du stock ; cette variable temporelle correspond au nombre de pièces de rechange (si le stock n'est pas épuisé) ou au nombre de demande en attente (si le stock est vide). Le stock nominal de rechange sur site pour l'URL étudiée sera désigné S (S = 3 sur l'illustration suivante).

Soit $D_1$ la date d'arrivée de la première panne : si S est non nul, alors le temps d'attente associé à cette demande sera nul puisqu'une pièce de rechange est disponible sur site. On

notera $R_1$ la date de retour de la pièce réparée (ou remplacée) ; $D_i$ et $R_i$ sont liés par la relation :

$$R_i = D_i + TAT \quad (2)$$

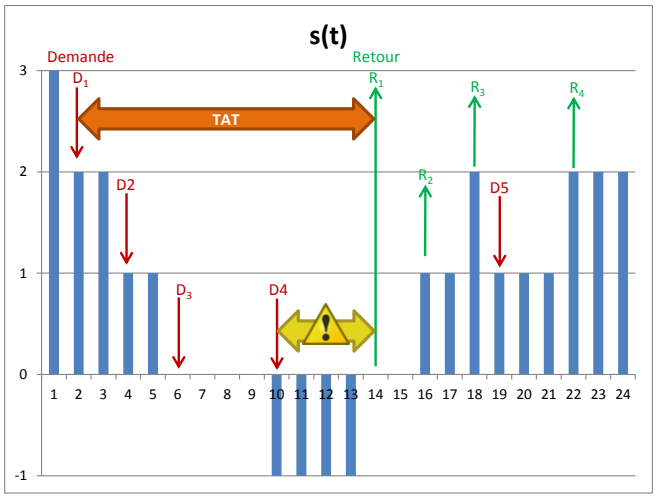


Fig. 4. Evolution de l'état du stock et illustration du risque de rupture sur un cas fictif

De même jusqu'à la $S^{ème}$ défaillance : le temps d'attente sera toujours nul.

Prenons maintenant la défaillance suivante, désignée $D_{s+1}$. Deux situations peuvent se produire :

- $D_{s+1} \geq R_1$ : l'opération de recomplètement du stock lancée à $D_1$ est terminée ; dans ce cas le temps d'attente est nul,
- $D_{s+1} < R_1$ : l'opération de recomplètement du stock lancée à $D_1$ est toujours en cours ; avant de pouvoir satisfaire cette demande il faudra alors observer un temps d'attente correspondant à $R_1 - D_{s+1}$, ou encore : $TAT - (D_{s+1} - D_1)$.

Ainsi le temps d'attente sera variable ; nous sommes donc à la recherche d'une formule analytique qui permettrait de l'évaluer efficacement. Nous nous tournons pour cela vers la théorie des files d'attente.

*D. Brève incursion du côté des files d'attente*

Les travaux visant à évaluer le temps passé dans une file d'attente, ou encore la longueur de cette file, remontent au début du $XX^e$ siècle et sont regroupés sous la désignation de théorie des files d'attente. A l'époque, A.K. Erlang, ingénieur de la compagnie de téléphone de Copenhague, cherchait à optimiser le nombre de lignes téléphoniques et d'opérateurs (indispensables pour relier les interlocuteurs entre eux) pour assurer un bon fonctionnement du réseau dans la capitale.

Cette discipline fait depuis l'objet d'une littérature abondante, signe d'une recherche dynamique : la prise de conscience par les différents acteurs économiques des coûts induits par un stockage inadapté les incite à optimiser leur stratégie de gestion. Prenons l'exemple d'une plateforme de vente en ligne : une gestion inadaptée pourra se traduire, soit par des délais de livraison inacceptables pour le client, et donc des ventes perdues, soit par une immobilisation excessive de ressources trésorières.

La variable s(t) a été définie précédemment comme représentative de l'état du stock, correspondant respectivement au nombre de pièces de rechange si le stock n'est pas épuisé ou au nombre de demande en attente si le stock est vide.

Nous désignerons par la suite par $N_C(t)$ le nombre de commande en cours à l'instant t ; on a alors :

$$S = s(t) + N_C(t) \quad (3)$$

Nous pouvons alors, comme proposé par [5], nous appuyer sur le théorème de Palm pour chercher une expression de la valeur moyenne de $N_C$.

Notre système peut être considéré comme un système de files d'attentes répondant aux critères suivants :

- Les arrivées des demandes suivent une loi de Poisson (défaillance des équipements caractérisée par une loi exponentielle de paramètre λ),
- Les durées de traitement sont uniquement caractérisées par leur valeur moyenne (TAT),
- Le nombre de files n'est pas limité (i.e. le TAT n'augmente pas en fonction du nombre de demande en cours, le fournisseur est supposé en mesure d'absorber toutes les demandes qu'il reçoit).

La notation de Kendall couramment utilisée dans le domaine des files d'attente désigne un tel système par le sigle M/G/∞ : M traduit le caractère poissonien du processus d'arrivée, G le caractère général du processus de service.

Dans une telle configuration, le théorème de Palm établit que le nombre de commande en cours de traitement suit une loi de Poisson de moyenne $\lambda_t$*TAT, où $\lambda_t$ correspond au taux de demandes total reçues par le stock (soit nλ dans notre cas). En conséquence l'espérance de $N_C$ s'écrit alors :

$$E(N_C) = \sum_{k=1}^{+\infty} k.\frac{(n\lambda.TAT)^k}{k!}.e^{-n\lambda.TAT} \quad (4)$$

Soit $N_A(t)$ le nombre de demande en attente d'être servies à l'instant t ; une expression de $N_A(t)$ est :

$$N_A(t) = \begin{cases} 0, & si\ N_C(t) \leq S \\ N_C(t) - S, & si\ N_C(t) > S \end{cases} \quad (5)$$

De (4) et (5) vient alors l'expression de l'espérance de $N_A(t)$ sous la forme :

$$E(N_A) = \sum_{k=S+1}^{+\infty} (k-S).\frac{(n\lambda.TAT)^k}{k!}.e^{-n\lambda.TAT} \quad (6)$$

La loi de Little permet ensuite de lier très rapidement le nombre de demande en attente $N_A$ et le temps moyen d'attente MWT, par la relation :

$$E(N_A) = \lambda_t.MWT \quad (7)$$

Nous aboutissons donc ainsi à une première expression du temps moyen d'attente :

$$MWT = \frac{1}{n\lambda}.\sum_{k=S+1}^{+\infty}(k-S).\frac{(n\lambda.TAT)^k}{k!}.e^{-n\lambda.TAT} \quad (8)$$

Néanmoins cette première expression n'est pas totalement satisfaisante puisqu'elle implique une somme à l'infini qui ne se prête pas à une résolution analytique rapide. Nous tirons alors profit d'une propriété constitutive des factorielles pour écrire :

$$k! = k.(k-1)! \quad (9)$$

Grâce à (9) nous pouvons alors réécrire (8) sous la forme suivante :

$$MWT = TAT.\left(\sum_{k=S}^{+\infty}\frac{(n\lambda.TAT)^k}{k!}.e^{-n\lambda.TAT}\right) - \frac{S}{n\lambda}.\left(\sum_{k=S+1}^{+\infty}\frac{(n\lambda.TAT)^k}{k!}.e^{-n\lambda.TAT}\right) \quad (10)$$

On retrouve ici l'expression de la loi de Poisson ; sachant alors que :

$$\sum_{k=0}^{+\infty}\frac{(n\lambda.TAT)^k}{k!}.e^{-n\lambda.TAT} = 1 \quad (11)$$

nous aboutissons finalement à l'expression de MWT suivante :

$$MWT = TAT.\left(1-\sum_{k=0}^{S-1}\frac{(n\lambda.TAT)^k}{k!}.e^{-n\lambda.TAT}\right) - \frac{S}{n\lambda}.\left(1-\sum_{k=0}^{S}\frac{(n\lambda.TAT)^k}{k!}.e^{-n\lambda.TAT}\right) \quad (12)$$

En vue d'intégrer cette expression dans un algorithme, cette formulation est bien plus satisfaisante ; les deux sommations ne comportent chacune qu'un nombre restreint de membres (respectivement S et S+1) et pourront être aisément calculées sans recourir à une quelconque approximation.

### *E. Illustration par un cas applicatif*

Considérons une installation constituée uniquement de trois pompes électriques, destinées à assurer le maintien du niveau d'eau à une hauteur donnée dans un bassin. Ces trois pompes sont identiques, redondantes, et fonctionnent alternativement.

Le taux de défaillance λ de chaque pompe est pris égal à $10^{-4}$/h ; le MTTR vaut 72h, et le TAT convenu avec le fournisseur est fixé à 1 an, soit 8760 h.

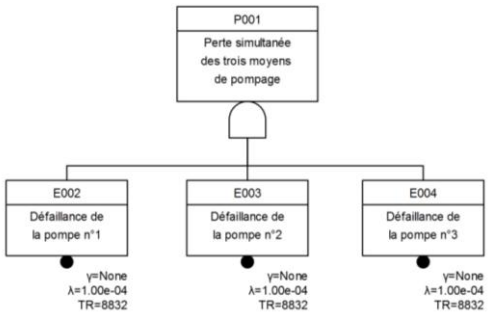


Fig. 5. Arbre de défaillance associé au cas applicatif, pour un stock nul

Supposons enfin cette installation soumise à une exigence de type : « *la fréquence annuelle d'occurrence d'une perte totale des moyens de pompage supérieure à 24 h doit être inférieure à* $10^{-4}$ »

Le tableau ci-après établit, pour un niveau de stock nominal S donné, le MDT qui sera considéré dans l'étude de sûreté suivant que l'on applique la méthode illustrée par Fig. 2 ou les équations (1) et (12). Il précise également le niveau de PNRS atteint pour chaque valeur de S : le dimensionnement du stock est jugé suffisant si la valeur de 95 % est atteinte.

TABLE I. EVALUATION DES MDT SUIVANT LA METHODE RETENUE

| Valeur de S | Position SLI | | MDT (h) | |
|---|---|---|---|---|
| | PNRS | Stock SN suffisant | Suivant Fig. 2 | Suivant Eq. (1) & (12) |
| 0 | 7 % | Non | 8 832 | 8 832 |
| 1 | 26 % | Non | 8 832 | 5 739 |
| 2 | 51 % | Non | 8 832 | 3 279 |
| 3 | 73 % | Non | 8 832 | 1 651 |
| 4 | 87 % | Non | 8 832 | 751 |
| 5 | 95 % | Oui | 72 | 329 |
| 6 | 98 % | Oui | 72 | 158 |

L'application de la méthode illustrée par la Fig. 2 conduit à envisager deux états de stock, suivant le résultat obtenu en considérant un stock nul :

- Soit l'exigence est tenue ; alors le MDT d'une pompe sera pris égal à 8 832 h et aucun stock ne sera prévu,
- Soit l'exigence n'est pas tenue ; alors :
  - la pompe sera incluse dans la liste des articles de rechange imposés par la sûreté nucléaire (SN),
  - le SLI dimensionnera le niveau de stock requis en fonction d'un niveau de PNRS, généralement fixé pour les articles de sûreté à 95%. Dans cet exemple cela conduirait à fixer à 5 le stock de rechange requis,
  - il sera considéré dans les études de sûreté un MDT de 8 832 h si le stock SN n'est pas suffisant du point de vue SLI, de 72 h sinon.

Avant même de lancer un calcul, cet exemple montre que cette approche peut conduire à retenir des hypothèses optimistes dans les démonstrations de sûreté. Ici, pour un

stock fixé à 5 unités, le MDT retenu (72h) est très inférieur à celui obtenu par la méthode proposée (12), évalué dans les mêmes conditions à 329 h.

Passons maintenant au calcul du nombre de pannes annuelles supérieures à 24h ; nous ferons pour cela appel aux deux formules suivantes, issues de [6] :

- $MDT_{sys}$ désigne le temps moyen d'indisponibilité de l'installation, à l'occurrence d'une panne système (i.e., perte de toutes les redondances). Pour un système parallèle pur constitué de n redondances tel qu'envisagé ici il peut être évalué sous sa forme asymptotique par :

$$\frac{1}{MDT_{sys}} = \sum_{i=1}^{n} \frac{1}{MDT_i} \tag{13}$$

- La Maintenabilité M(t) est la probabilité que le système, tombé en panne à l'instant $t_0$, soit remis en service à l'instant $t_0$+t . Elle s'écrit :

$$M(t) = 1 - e^{-\left(\frac{t}{MDT_{sys}}\right)} \tag{14}$$

Le graphe suivant illustre la fréquence annuelle d'occurrence des pannes « système » supérieures à 24 h, selon qu'elle soit calculée suivant la méthode A (Fig. 2) ou B (éq. (1) et (12)), en fonction du niveau de stock initial considéré.

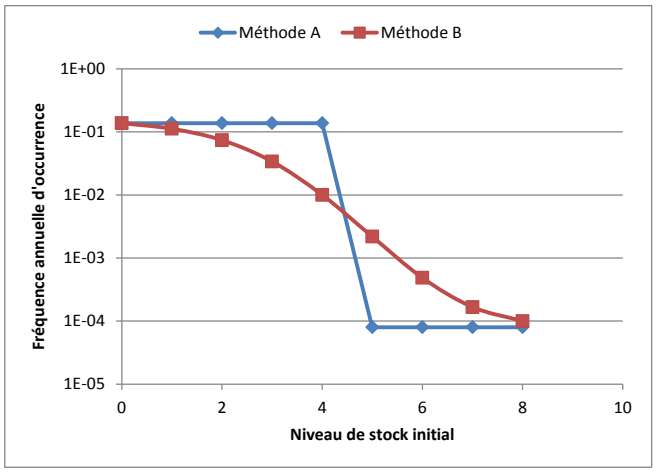


Fig. 6. FAO des pannes > 24 h vs Stock initial

Il a été vu précédemment que l'application de la méthode A conduirait en réalité à définir un stock initial constitué de 5 pièces de rechanges, répondant ainsi à la fois au classement des pompes comme article de rechanges SN et à la PNRS de 95% retenue pour les articles de sûreté. Alors, si l'on s'en tient à cette méthode, l'exigence de FAO fixée à $10^{-4}$ apparaît tenue.

En revanche la conclusion est tout autre si l'on analyse les résultats obtenus par la méthode B : pour un stock initial constitué de 5 pièces de rechanges, la FAO calculée est supérieure à l'objectif de plus d'une décade. Pour que l'exigence soit tenue il conviendrait ici de fixer un stock initial de 8 rechanges.

Au-delà du caractère plus ou moins réaliste de cette simulation, elle permet donc de mettre en évidence une limite de la méthode actuelle, qui consiste à définir une quantité de rechanges dits « SN » quasi-indépendamment de la sévérité des exigences de sûreté à démontrer. Ainsi, dans cet exemple, le niveau du stock déterminé par l'approche actuelle serait fixé à 5 que l'exigence soit fixée à $10^{-1}$ ou à $10^{-4}$.

A contrario, la méthode développée dans cet article permet d'ajuster le niveau du stock et donc des investissements associés, au juste besoin du point de vue de la sûreté, par exemple à 4 pour un objectif à $10^{-2}$, ou à 2 pour un objectif à $10^{-1}$.

### *F. Logique d'optimisation*

Comme évoqué au paragraphe II.C, le processus actuel d'identification des candidats au stock de rechange SN s'appuie notamment sur les analyses d'importance, et plus particulièrement sur le facteur d'importance de Fussel-Vesely (FV) et le facteur d'importance d'augmentation du risque (FAR).

Ces facteurs d'importance sont calculés pour chaque événement de base représentant la défaillance d'un composant, ce qui constitue une limite de cette démarche s'agissant de définir un stock de rechange. En effet, un article placé en rechange sera destiné à soutenir non pas un composant isolé, mais toute la famille de composants identiques intégrés à l'installation.

Nous nous appuierons, pour la suite de l'article, sur le logiciel d'arbre de défaillances « Arbre-Analyst » [1][2]. Il s'agit d'un outil libre d'utilisation, basé sur :

- le respect du format Open-PSA, permettant ainsi une parfaite interopérabilité,
- l'utilisation des moteurs de calcul XFTA et MCEP, permettant de bénéficier d'algorithmes de calculs récents et efficaces.

Au-delà de cette rapide présentation, deux caractéristiques du projet « Arbre-Analyst » expliquent l'intérêt particulier de cet outil dans le cadre de l'article :

- d'une part cet outil intègre une Interface Applicative de Programmation (API) [3] qui permet à l'utilisateur d'ajouter librement des fonctionnalités personnalisées : il est ainsi possible, par exemple, de lancer un grand nombre de calculs en faisant varier l'un ou l'autre des paramètres,
- d'autre part le projet « Arbre-Analyst » met à disposition une bibliothèque de modules destinée au développement et au partage de nouvelles fonctionnalités orientés métiers. Cette bibliothèque a vocation à être enrichie par les utilisateurs ; à ce titre, le module embarquant les travaux présentés ici sera in fine mis à la libre disposition de la communauté [2].

Compte-tenu des capacités d'automatisation des tâches via l'API d'Arbre-Analyst nous pouvons donc envisager de réaliser un nombre de calculs important, tout en respectant des délais de réalisation cohérent pour ce type d'analyse.

Soit G la grandeur associée au type de performance recherchée ; G peut être un niveau d'indisponibilité, une fréquence d'occurrence…

Considérons un arbre de défaillances correspondant à un événement redouté pour lequel il doit être démontré que G est inférieur à une exigence donnée. On supposera dans un premier temps que cet arbre modélise l'installation concernée jusqu'à un niveau de détail matériel cohérent du niveau technique d'intervention envisageable sur site, autrement dit les événements de base correspondent au niveau des URL.

Le comportement des composants dits réparables peut être modélisé à l'aide de la loi « Réparable (TT) », régie par deux paramètres principaux : le taux de défaillance λ, et le temps de remise en service désigné TR (correspondant dans notre cas au MDT).

Nous considérons par la suite que tous les composants identiques de l'installation présentent un MDT également identique ; cela vient naturellement pour la partie MWT, en revanche la partie MTTR pourrait théoriquement varier entre deux composants identiques (accessibilité différente par ex.).

L'usage, dans Arbre-Analyst, sera alors de définir un unique paramètre nommé de type TR auquel nous donnerons un nom -par exemple «TR_i » pour la famille i- et une valeur, $MDT_i$ en l'occurrence. Ainsi pour une famille de composants identiques, toutes les instances où qu'elles soient dans l'arbre partageront le même paramètre TR.

Comme nous l'avons vu précédemment $MDT_i$ est une variable qui peut être évaluée en fonction de la quantité nominale $S_i$ de pièces de rechanges en stock pour la famille i. $MDT_i(S_i)$ désignera donc par la suite la valeur du MDT évalué pour la famille i considérant un stock nominal de rechange $S_i$.

En première approche la démarche d'optimisation pourrait alors consister à :

- calculer $G_0$, valeur de G obtenue en considérant le stock de chaque famille i dans un état initial donné :

$$G_0 = G(MDT_1(S_1), \dots, MDT_i(S_i), \dots . MDT_n(S_n)) \quad (15)$$

- calculer $G_1(i)$, valeur prise par G si l'on augmente le stock de rechange de la famille de composants i d'une unité :

$$G_1(i) = G(MDT_1(S_1), \dots, MDT_i(S_i + 1), \dots . MDT_n(S_n)) \quad (16)$$

- Puis retenir, pour cette itération, la famille i qui permet de maximiser (si G correspond à une grandeur supposée croissante, fiabilité notamment) ou minimiser (si G correspond à une grandeur supposée décroissante, fréquence d'occurrence par exemple) la fonction d'optimisation définie comme :

$$Opt(i) = G_1(i) - G_0 \quad (17)$$

- Enfin, itérer ce processus jusqu'à obtenir une valeur satisfaisante de G (et un état de stock associé).

Une limite de cette première proposition revient à ne pas différencier les implications de la mise en stockage de l'un ou l'autre des composants. Or si le stock retenu doit permettre la démonstration aux autorités des exigences de sûreté, il doit également répondre aux exigences des industriels en charge de la maintenance de l'installation.

Parmi les préoccupations des industriels sur ce point, viendra en premier lieu la nécessité de minimiser l'investissement financier lié à l'achat des pièces de rechange. Les coûts récurrents liés à la gestion du stock peuvent également entrer en considération : immobilisation de liquidités, coût de personnel, mise au rebut… Au-delà de l'aspect financier, des contraintes d'espace peuvent également apparaître.

Aussi, afin de hiérarchiser les différentes familles de composants nous avons introduit un paramètre $V_i$ qui se veut représentatif de la valeur d'une pièce de rechange pour la famille i. Le mode de définition de la valeur de $V_i$ est laissé libre pour chaque projet ; dans notre pratique $V_i$ représente le coût d'achat d'une pièce de rechange pour la famille i.

Nous corrigeons alors la fonction d'optimisation définie en (17) comme suit :

$$Opt(i) = \frac{G_1(i) - G_0}{V_i} \quad (18)$$

### *G. Automatisation de la tâche d'optimisation*

Certains des paramètres nécessaires à la mise en œuvre de la démarche présentée ci-dessus ne sont pas nativement intégrés en tant que tels dans « Arbre-Analyst ». C'est le cas :

- du TAT,
- du MTTR,
- de la valeur V,
- également, une valeur de stock initial pourrait être intéressante, par exemple afin d'intégrer un stock déjà existant.

Pour remédier à cela nous avons exploité la plage de données « Description » associée à chaque paramètre nommé et avons défini des règles d'écriture spécifiques au niveau des paramètres du type « mttr ». Ainsi les paramètres que nous souhaitons introduire sont délimités de part et d'autre par les chaînes de caractères « #ParamLog » et « #End » tel qu'illustré par Fig. 7 ; une fonction permettant de renseigner ou d'éditer l'ensemble de ces paramètres à la volée via un tableur est en cours de développement.

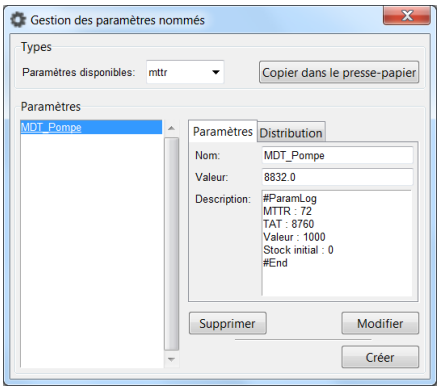


Fig. 7. Introduction de paramètres logistiques dans Arbre-Analyst

Dès lors, à son lancement, le module vient balayer l'ensemble des paramètres de type « mttr » et lire les paramètres logistiques quand ils sont définis. L'API s'appuie sur les opérateurs du langage Python, qui permettent de traiter très efficacement ce type de chaines de caractère : une fois lus, les paramètres introduits sont stockés sous forme de dictionnaire.

Il est également nécessaire de stocker dans ce dictionnaire le taux de demande total associé à la famille de composants considérée. Pour cela, dès lors qu'un paramètre « mttr » est affecté de paramètres logistiques nous récupérons la liste des événements de base pour lesquels il intervient dans la loi de comportement, puis sommons les taux de défaillance de ces événements de base.

Nous disposons alors de l'ensemble des paramètres nécessaires à la mise en œuvre de la formule (12) et pouvons ainsi définir les valeurs que prend le MWT de la famille de composants pour n'importe quel niveau de stock nominal.

Reste alors à sélectionner le calcul programmé, ainsi que la grandeur, pour lesquels nous souhaitons optimiser le stock de rechanges. A cet effet une invite de commande permet, via un menu déroulant, de renseigner le choix de l'utilisateur.

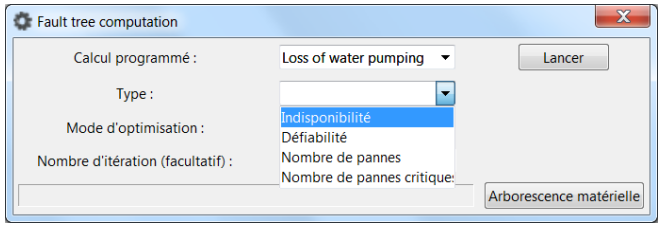


Fig. 8. Invite de commande du module

Le module itère alors jusqu'à atteindre le nombre maximal d'itérations (fixé à 50 par défaut, modifiable par l'utilisateur). Les résultats sont enregistrés pour chaque pas de calcul dans un tableur au format .xlsx.

## IV. APPLICATION AU CAS INDUSTRIEL

Le cas industriel retenu dans le cadre de cet article est présenté au paragraphe II.

Les fonctions du système concernées par la sûreté nucléaire sont assurées, pour l'ensemble de l'installation, par environ 850 URL ; compte tenu d'un certain degré de symétrie il a été possible de réduire à 700 le nombre d'URL directement considérées dans l'analyse de sûreté.

Dans le cadre de cet article nous nous concentrerons par la suite sur une seule des fonctions de sûreté assurée par l'installation, réduisant ainsi finalement le nombre d'URL considérées à 370, de 54 références différentes.

Contrairement à l'une des hypothèses prises au paragraphe III.F, compte tenu de la complexité de l'installation les arbres de défaillances n'ont pas été construits systématiquement jusqu'au niveau des URL. Certaines URL, considérées en série, ont été regroupées par bloc fonctionnel, via un tableau de consolidation de la quantification ; leurs taux de défaillance et MDT sont alors consolidés pour constituer un événement de base de l'arbre.

Finalement, nous construisons un arbre de défaillance constitué d'environ 120 événements de base regroupés sous 112 portes logiques.

Du fait que certains événements de base de cet arbre représentent non pas la défaillance d'une URL, mais d'un groupe d'URL, il n'est pas possible d'appliquer directement la méthodologie proposée précédemment : ici un paramètre nommé de type « mttr » n'est plus associé à une seule famille d'URL, et inversement l'évolution du MDT d'une famille d'URL est susceptible d'impacter plusieurs paramètres nommés.

Nous avons opté ici pour la construction d'un tableur excel contenant d'une part l'ensemble des données logistiques des URL (MTTR, TAT, Valeur, Stock initial), d'autre part les taux de défaillances et relations hiérarchiques entre les différents niveaux matériels du système. Au lancement le module charge les informations contenues dans ce tableur et reconstruit les relations entre les différents niveaux hiérarchiques. Ainsi l'évolution du niveau de stock d'une URL donnée se traduit par la mise à jour dans l'arbre de l'ensemble des paramètres nommés de type « mttr » impactés.

Un avantage indirect de cette approche est de permettre de tenir compte, dans la définition du stock de rechange, de l'ensemble des URL du système dès lors qu'elles sont identifiées dans le tableau de quantification ; par exemple, les membres de l'une des 54 familles d'URL qui n'ont pas été modélisés dans les arbres du fait des symétries existantes dans l'installation, ou parce qu'utilisés pour d'autres fonctions de sûreté, sont bien considérés dans la définition du stock.

Ces adaptations faites, nous avons pu procéder à la recherche d'une solution optimale de stock de rechanges pour les 54 références d'URL considérées. La démonstration vise à justifier le respect d'une exigence du type « FAO des pannes supérieures à une durée donnée ». ; les pannes supérieures à cette durée sont désignées « pannes critiques » par la suite.

Il s'agit d'une analyse a posteriori, la démarche proposée ici ayant été développée après la réalisation de l'étude de sûreté. Nous allons donc comparer, sous forme banalisée :

- le résultat -en termes de stock de sûreté et de niveau atteint- tel qu'établi par l'analyse de sûreté suivant la démarche illustrée par Fig. 2, considérant une PNRS cible de 95%,
- le résultat recalculé sur la base du stock défini au terme de l'analyse de sûreté, réévalué en tenant compte des équations (1) et (12),
- puis les résultats obtenus en lançant deux fois la démarche d'optimisation présentée précédemment :
  - une première fois, considérant un stock initial vierge,
  - une seconde fois, considérant comme stock initial le stock issu de l'analyse de sûreté.

Ces résultats sont illustrés par Fig. 9 et Fig. 10.

A titre informatif, le processus d'optimisation appliqué sur ce cas industriel (pour 50 itérations) dure environ ½ h sur un portable de bureautique; ce délai n'est pas négligeable mais reste de notre point de vue acceptable, s'agissant d'une tâche ponctuelle et pouvant être réalisée en temps masqué.

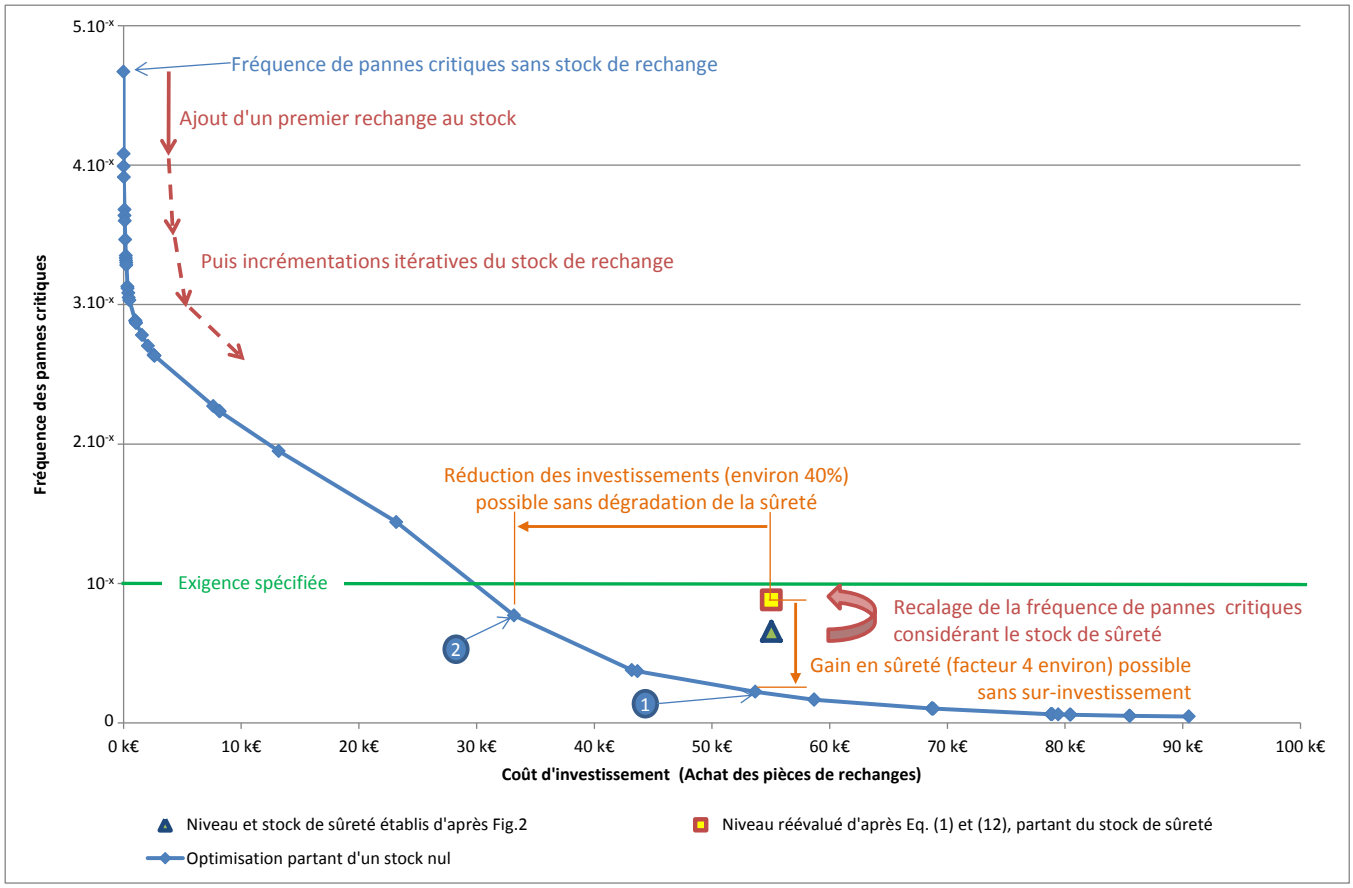


Fig. 9. Application de la démarche au cas industriel

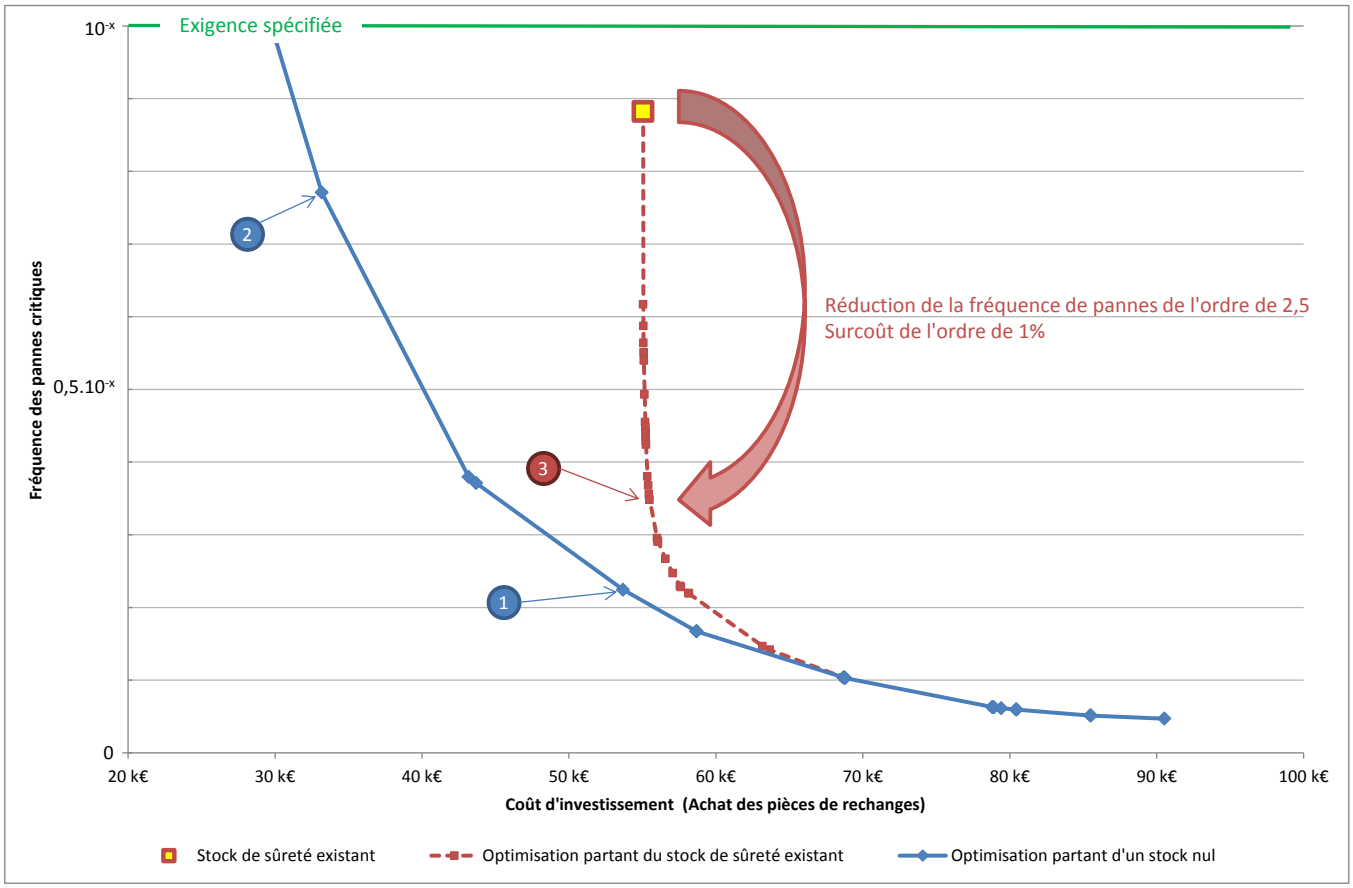


Fig. 10. Optimisation du stock de sûreté existant

L'analyse de Fig. 9 apporte de nombreux enseignements. Considérons tout d'abord la situation existante, basée sur le stock de rechanges issu de l'analyse de sûreté. Il apparaît alors que la fréquence des pannes critiques établie en appliquant la méthodologie décrite en Fig. 2 est sous-évaluée, de l'ordre de 30%, par rapport au résultat obtenu en intégrant directement au calcul le risque de rupture de stock des différentes URL.

Dans le cas présent cela resterait sans conséquences, l'objectif considéré étant fixé à 1 (valeur banalisée). Néanmoins ce constat illustre l'incertitude induite par l'approche actuelle qui, du fait d'un effet de seuil important montré en Fig. 6, peut mener à des résultats aussi bien optimistes que pessimistes, sans qu'il puisse être aisément déterminé par l'analyste s'il se trouve dans un cas ou dans l'autre.

L'analyse des résultats de la démarche d'optimisation, partant d'un stock vierge, est également intéressante. Chaque point sur la courbe bleue de Fig. 9 correspond à une itération (autrement dit, un état de stock) ; ces résultats peuvent être considérés sous deux angles :

- Pour un même niveau d'investissement nous aurions pu réduire la fréquence des pannes critiques d'un facteur 4 (point 1),

  ou alors

- Partant du niveau d'exigence fixé à $10^{-x}$, nous aurions pu définir un stock de sûreté mieux ciblé (point 2), et ainsi réduire l'investissement en stock de rechange de l'ordre de 40%.

Enfin la dernière analyse a consisté à relancer une tâche d'optimisation, en considérant cette fois le stock de sûreté comme stock initial. L'idée, derrière ce calcul, est de regarder comment il serait possible de diminuer la fréquence des pannes critiques en complétant le stock de sûreté tel qu'actuellement défini.

La courbe en rouge sur Fig. 10 montre qu'il est effectivement possible d'améliorer significativement le niveau de performance pour un investissement minime. Ainsi nous pouvons voir (point 3) qu'un investissement ciblé correspondant à environ 1% du coût du stock de sûreté permet de réduire la fréquence de pannes critiques d'un facteur 2,5. Une convergence rapide apparaît également possible vers la courbe des solutions optimales obtenues en partant d'un stock vide (courbe en bleu).

## V. CONCLUSIONS ET PERSPECTIVES

La méthodologie que nous avons exposée dans cet article permet donc de répondre aux deux objectifs que nous nous étions fixés initialement.

D'une part, nous avons identifié une formulation du temps d'attente moyen qui soit à la fois acceptable et aisément calculable, tout en évitant les effets de seuil inhérents à la méthodologie actuelle.

D'autre part, nous avons développé une méthodologie et un outil permettant d'automatiser la recherche d'un stock de rechange optimisé, sans que la démarche de sûreté de fonctionnement ne s'en trouve significativement alourdie.

L'outil développé donne pleine satisfaction au regard de l'objectif recherché : son application sur un cas industriel a permis de mettre en évidence les multiples gains que peut apporter cette démarche. Il améliore la prise en compte de la probabilité de rupture de stock et son intégration dans les calculs de sûreté, et peut également permettre, suivant le point de vue, d'améliorer le niveau de performance sans augmentation des dépenses, ou de diminuer les dépenses sans dégrader les performances.

S'il ne nous a pas gênés ici, suivant les usages, le temps de calcul induit par l'approche adoptée pourrait se révéler problématique. Les développements en cours visent notamment à améliorer l'efficacité de l'algorithme, d'une part en parallélisant certaines tâches afin d'exploiter les architectures multi-cœurs des processeurs actuels, d'autre part en regardant les possibilités de s'appuyer sur des facteurs de sensibilité autres que ceux précédemment cités.

Enfin, au titre des perspectives de développements futurs, la question de la prise en compte de politiques de gestion de stock différentes reste à envisager, notamment les notions de réapprovisionnement par lots ou à échéances fixes.

## REFERENCES


[1] E. CLEMENT, T. THOMAS, A. RAUZY - Arbre-Analyste: un outil d'arbres de défaillances respectant le standard Open-PSA et utilisant le moteur XFTA - Congrès LAMBDA-MU 19 (Octobre 2014)

[2] www.arbre-analyste.fr

[3] www.arbre-analyste.fr/doc/doku.php/api

[4] Autorité de Sûreté Nucléaire, "RFS 2002-01 – Développement et utilisation des études probabilistes de sûreté", 2003

[5] S.C. Graves, A.H.G. Rinnooy Kan, P.H. Zipkin, "Logistics of Production and Inventory", Elsevier, 1993

[6] A. Villemeur, "Sûreté de fonctionnement des systèmes indutriels', Edition Eyrolles, 1988