



Arbre-Analyst – Présentation des évolutions du moteur de calculs XFTA

CLEMENT Emmanuel
Thales

Brest
emmanuel.clement@fr.thalesgroup.com

THOMAS Thierry
Naval Group

Brest
thierry-a.thomas@naval-group.com

RAUZY Antoine
NTNU

Richard Birkelands vei 2B, 7491
Trondheim
antoine.rauzy@ntnu.no

MILCENT Frédéric
Naval Group

Ruelle Sur Touvre
frederic.milcent@naval-group.com

Résumé — Arbre-Analyst est un outil libre de diffusion et libre d'utilisation dont la première version remonte à 2013. Arbre-Analyst intègre le moteur de calcul XFTA et respecte un format libre et documenté « Open-PSA ». Arbre-Analyst évolue pour intégrer notamment une nouvelle version du moteur de calcul XFTA. Cette nouvelle version du moteur apporte deux nouveaux algorithmes permettant pour l'un, de calculer de façon exacte des arbres de tailles importantes et, pour l'autre, de calculer des arbres de très grandes tailles de façon beaucoup plus précise, notamment pour l'évaluation particulière d'événements initiateurs à probabilité élevée (proche de 1).

Mots-clés — *Arbre de défaillance, diagramme de décision binaire, Open-PSA, XFTA, EPS*

Abstract— Arbre-Analys is a free of use and free to distribute fault tree editor software. The first version was released in 2013. Arbre-Analyst includes the XFTA engine and is compliant with the Open-PSA standard. The Open-PSA standard is a well-documented format to characterize fault tree models. The new release of XFTA provides two new algorithms. The first one allows computing exact results from fault trees even for big models. The second one allows computing very big fault tree models with a more accurate precision than the older XFTA release.

Keywords — *Fault tree, reliability, Binary decision diagram, Open-PSA, XFTA*

I. INTRODUCTION

La complexité croissante des systèmes associée à des objectifs en terme de sécurité de plus en plus sévères entraînent la nécessité de proposer des outils de modélisation et d'évaluation des arbres de défaillances de plus en plus efficaces. Un peu moins de 10 ans après la diffusion de la première version de l'applicatif Arbre-Analyst [2] et du moteur XFTA [3], nous proposons une nouvelle version majeure de ces outils qui intègrent notamment les dernières évolutions en terme d'algorithme d'évaluation des paramètres de sûreté de fonctionnement.

Le moteur de calcul XFTA, dans sa première version, visait les études probabilistes de sûreté comprenant des centaines à milliers d'événements de base. Pour permettre l'analyse et la résolution de modèles de cette taille, les

algorithmes retenus pouvaient entraîner, dans certains cas, une approximation cependant toujours conservatrice, et particulièrement adaptée pour l'évaluation d'événements redoutés à faible probabilité, analysés dans les études de sécurité. La nouvelle version du moteur apporte deux nouveaux algorithmes [4] permettant pour l'un, de calculer de façon exacte des arbres de tailles importantes et, pour l'autre, de calculer des arbres de très grandes tailles de façon beaucoup plus précise, notamment pour l'évaluation particulière d'événements initiateurs à probabilité élevée (proche de 1).

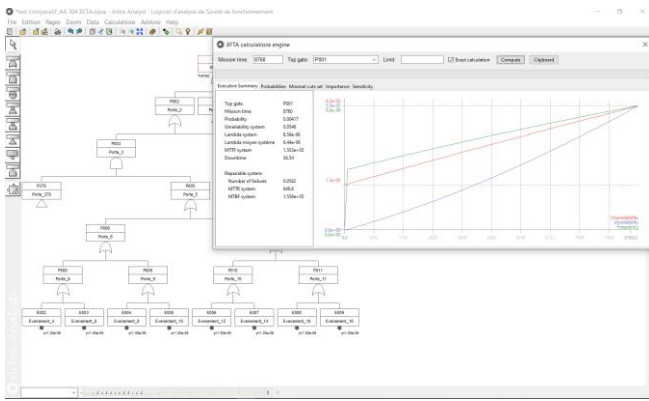
II. ARBRE-ANALYST

A. Présentation

Arbre-Analyst est un outil dédié à l'édition, à la visualisation et à l'évaluation de modèle d'arbre de défaillance. Arbre-Analyst a été conceptualisé et développé par des ingénieurs spécialistes des études probabilistes de sûreté pour répondre au mieux d'une part aux besoins des études et, d'autre part, aux contraintes techniques et industriels des projets.

Arbre-Analyst est proposé en libre diffusion et en libre utilisation au travers du site Internet. La première version de l'outil a été diffusée en 2013 et des évolutions successives lui ont permis de gagner en maturité.

FIGURE 1: CAPTURE D'ECRAN D'ARBRE-ANALYST



Les objectifs clés d'Arbre-Analyst sont :

- Proposer une ergonomie de saisie qualitative ;
- Permettre la résolution de modèles de toutes tailles ;
- Proposer des sorties pour la construction de rapports ;
- Assurer une totale interopérabilité :
 - **Dans le temps long** : au travers de la libre diffusion et utilisation de l'outil ainsi que de sa compatibilité avec toutes les versions des projets sources ;
 - **Dans les organisations** : au travers de l'utilisation du format documenté et ouvert Open-PSA et de sa compatibilité avec des outils du marché.

Le développement d'Arbre-Analyst est réalisé au travers de l'intégration continue. L'intégration continue est un ensemble de pratiques qui consistent à vérifier à chaque évolution du code source que le résultat des modifications ne produit pas de régression dans l'application concernée. L'objectif de cette pratique est de détecter les problèmes d'intégration au plus tôt dans le cycle de développement.

Arbre-Analyst est construit sur deux piliers fondamentaux :

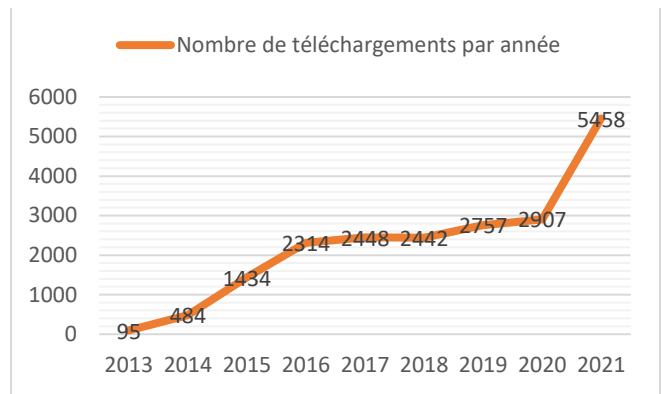
- Le moteur de calcul XFTA [4];
- Le format de donnée Open-PSA [5].

B. Adoption

Mesurer précisément l'adoption d'un outil proposé en libre téléchargement, autorisant sa libre diffusion et n'employant pas de système de « jeton » n'est pas sérieusement possible. Cependant, et au travers de quelques statistiques issues du site Internet et des retours que nous avons de différentes entités, nous pouvons arriver à mesurer une certaine dynamique.

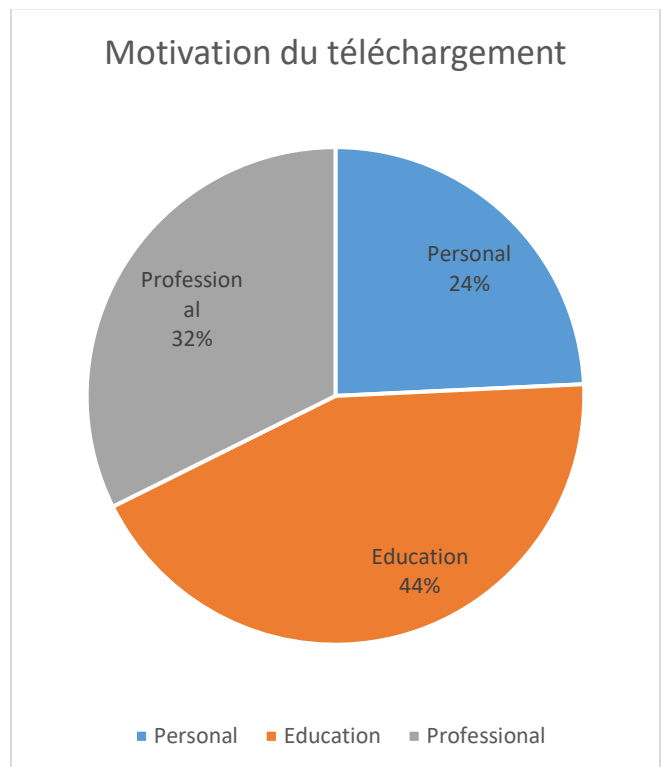
Premièrement, une information que nous avons est le nombre de téléchargements depuis le site internet. Cette donnée, qui est présentée en figure n°2, est une donnée qu'il faut relativiser pour deux raisons. D'une part, elle mesure un intérêt probable des utilisateurs pour Arbre-Analyst mais ne permet pas d'en connaître l'usage réel qui en est fait. Et, d'autre part, cette donnée ne comptabilise pas la diffusion de l'outil au travers d'autres vecteurs comme l'installation automatique par les systèmes d'information des entreprises.

FIGURE 3:EVOLUTION DU NOMBRE DE TELECHARGEMENT PAR ANNEE



Deuxièmement, nous avons la possibilité de recueillir, par l'utilisation d'un formulaire, des informations qui sont saisies directement par l'utilisateur. Parmi ces informations, nous avons la « raison » qui motive ce téléchargement. Bien entendu, et même si l'utilisateur est appelé à renseigner sincèrement ce formulaire, il est probable que la raison renseignée ne soit pas toujours celle qui motive réellement le téléchargement.

FIGURE 4: MOTIVATION DU TELECHARGEMENT



Troisièmement et au travers de discussions, d'échanges, et de publications, des exemples pratiques d'adoption sont partagés comme les cas particuliers ci-après :

- **Naval Group** : réalisation de démonstrations probabilistes de fiabilité de sécurité générale, de sûreté (infrastructures nucléaires, pyrotechnie, système de combat...);
- **DGA** : réalisation des démonstrations probabilistes de sécurité (aéro) ;
- **ESID** : réalisation de démonstrations probabilistes de sûreté (infrastructures nucléaires) ;

- **Thales** : réalisation de démonstrations probabilistes de sécurité et de fiabilité (aéro, naval).

Finalement, et même s'il est difficile de mesurer précisément l'adoption ainsi que les usages qui sont faits d'Arbre-Analyst, nous observons une croissance constante jusqu'à atteindre 5500 téléchargements sur l'année 2021 dont un tiers pour un besoin dit « professionnel » et près de la moitié pour un besoin de formation. Plus d'une cinquantaine d'entreprises ou d'entités publiques ont montré leur intérêt pour Arbre-Analyst ainsi qu'une vingtaine d'universités et de grandes écoles. Cette dynamique reflète l'intérêt qui peut être porté sur un outil d'arbres de défaillances libre de diffusion et d'utilisation et cela malgré les réticences et préjugés souvent non avérés liés au choix de proposer Arbre-Analyst « gratuitement ».

C. Roadmap

Arbre-Analyst est un outil dédié à l'édition d'arbres de défaillances statiques pour les besoins des études de sécurité et de fiabilité et cela sur le temps long. Les travaux de développement visent à apporter de nouvelles fonctionnalités telles que de nouvelles distributions de probabilités, de nouveaux outils d'édition et la correction de bogues. Il n'est en revanche pas prévu de couvrir d'autre formalisme comme les arbres de défaillances dynamiques.

Par ailleurs, des discussions sont en cours avec des industriels / donneurs d'ordre dans le but de démarrer une activité de rédaction d'un document interindustriel de qualification.

Parallèlement, les travaux de développement de « System-Analyst » [7] se poursuivent et entraînent des évolutions d'Arbre-Analyst notamment pour améliorer la compatibilité entre ces deux outils.

III. XFTA

A. Presentation

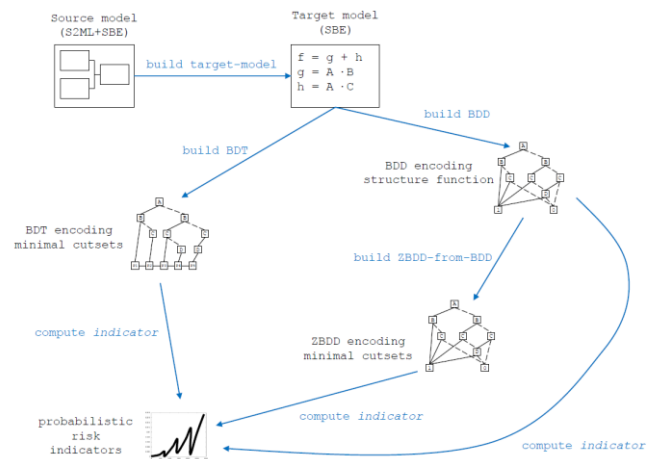
XFTA est un moteur de calcul pour les modèles Booléens d'analyse du risque (arbres de défaillances, blocs diagrammes de fiabilité) développé par Antoine Rauzy [3]. Il prend en entrée des modèles définis au travers du formalisme Open-PSA et permet d'en obtenir l'ensemble des résultats attendus notamment :

- Les coupes minimales ;
- Les probabilités de l'évènement de tête ;
- Les facteurs d'importance des événements de base ;

Ce projet, démarré en 2012, a évolué en 2020 pour intégrer un certain nombre d'évolutions majeures notamment :

- La définition de modèle sous le formalisme S2ML+SBE en plus de l'Open-PSA;
- La résolution d'arbres de défaillances au travers de diagrammes de décisions binaires afin d'en obtenir des résultats exacts;
- Le calcul approximatif des valeurs de l'évènement de tête au travers d'un nouvel algorithme : « Pivotal Upper Bound ».

FIGURE 5:FLUX D'ANALYSE D'XFTA



Résoudre des arbres de défaillances de grandes tailles est un problème complexe pour lequel il n'existe pas de solution universelle. XFTA comprend deux méthodes très efficaces. D'une part, pour des arbres de tailles moyennes, l'utilisation des diagrammes de décisions binaires permet d'obtenir l'ensemble des résultats de façon exacte et efficace. Cette approche ne permet cependant pas de résoudre les arbres de très grandes tailles. Pour cela, XFTA intègre une deuxième solution d'analyse au travers d'une structure de données représentative des coupes minimales. Ainsi cette solution permet d'extraire les coupes minimales en éliminant au plus tôt les coupes minimales les moins probables (limite donnée par l'utilisateur en terme de probabilité ou de cardinalité). De cette façon, les arbres de très grandes tailles sont traités efficacement, les probabilités de l'évènement sommet étant approximées au travers des coupes minimales.

XFTA étant écrit en C++ ANSI, il est portable sous toute plate-forme disposant d'un compilateur C++. Il est aujourd'hui porté sous Windows, Linux et MacOS.

B. Pivotal upper bound

Le Pivotal Upper Bound est une nouvelle méthode de calcul des probabilités de l'évènement sommet à partir des coupes minimales. Cette méthode est intéressante dans le cas où la taille des arbres ne permet pas d'utiliser les diagrammes de décisions binaires.

Le Pivotal Upper Bound remplace les deux méthodes historiques que sont l'approximation par évènement rares et le Min Cut Upper Bound en apportant une précision bien plus élevée que les deux précédentes.

Attention cependant, les trois approximations précédentes sont très efficaces dans le cas où les événements de bases ont des probabilités faibles et / ou ne sont pas fortement présents dans les coupes minimales à faible cardinalité. Si les conditions précédentes ne sont pas réunies, l'approximation qui est toujours pessimiste peut devenir non négligeable.

C. Diagramme de décision binaire

Dans le cas d'arbres de défaillances de tailles moyennes et dont la probabilité des événements de base ne respecte pas les conditions présentées dans le paragraphe précédent, les résultats obtenus au niveau de l'évènement de tête et des facteurs d'importance peuvent être sensiblement surestimés.

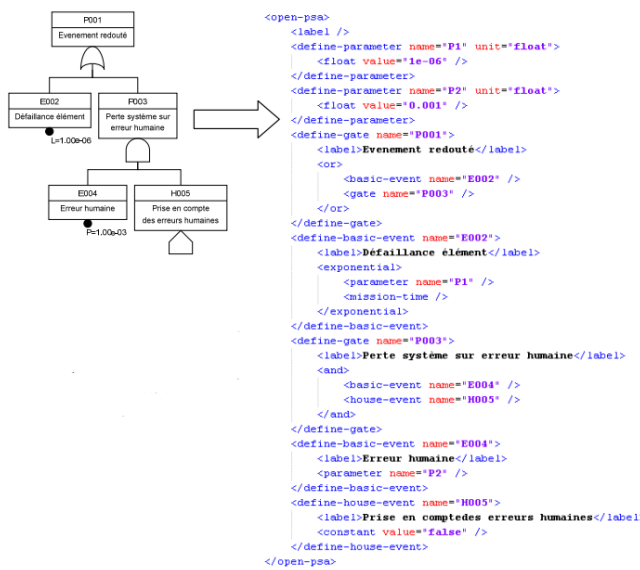
Dans ce cas, XFTA intègre maintenant la possibilité de résoudre les arbres de défaillance au travers d'une structure de

données appelée « diagramme de décision binaire ». Cette structure permet de représenter la structure de l'arbre de défaillance de façon efficace et ainsi de pouvoir y réaliser l'ensemble des traitements. Les résultats obtenus sont exacts. Cependant, cette structure n'autorise pas de pouvoir tronquer les traitements suivant une limite prédéfinie. Par conséquent, le traitement peut ne pas aboutir pour les arbres de très grandes tailles,

IV. OPEN-PSA

Open-PSA est un format ouvert et documenté dont le but est de décrire un arbre de défaillances au travers de l'XML. XML, pour eXtensible Markup Language (langage de balisage extensible), est un langage de balisage généraliste. Le format d'échange « Open-PSA » a été publié en 2008 [8] et vise à améliorer l'interopérabilité des modèles.

FIGURE 6: EXEMPLE DE MODELE "OPEN-PSA"



V. APPLICATIONS INDUSTRIELLES

A. Présentation de Naval Group et du contexte industriel

Naval Group conçoit et produit des sous-marins, des bâtiments de surface et les infrastructures associées. Ces produits présentent de forts enjeux en termes de sécurité (notamment pour les installations nucléaires ou mettant en œuvre des armes) et en termes de disponibilité (plusieurs dizaines d'années de service actif).

Les arbres de défaillances réalisés visent à évaluer des probabilités faibles dans le cadre des études de sécurité et plus élevées dans le cas des études de disponibilité.

La version 3 d'Arbre-Analyst embarque un moteur de calcul polyvalent permettant d'obtenir des résultats précis quel que soit le niveau de probabilité.

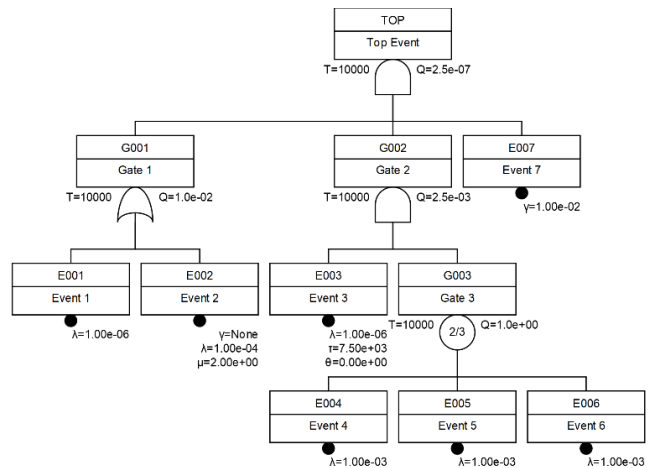
Arbre-Analyst est largement utilisé au sein de Naval Group parce qu'il est simple d'utilisation, qu'il s'agit d'une alternative satisfaisante aux outils sous licence et qu'il permet de travailler hors connexion dans un contexte où le télétravail est en plein essor.

Trois cas test utilisés pour la qualification interne du logiciel sont présentés dans les paragraphes suivants.

B. Cas 1

Le premier cas test correspond à un arbre de taille modeste (voir figure 7) permettant une résolution analytique sans passer par un logiciel / moteur de calcul. Il est ainsi possible de vérifier le niveau de précision des résultats sans recourir à un logiciel tiers. Il est constitué des principales portes et lois utilisées usuellement et permet de tester des cas où la probabilité de certaines portes est proche de 1, valeurs pour lesquelles un écart est fréquemment constaté, notamment avec la méthode Mean Cut Upper Bound utilisée dans la précédente version d'Arbre Analyst (approximation pessimiste).

FIGURE 7: ARBRE DU CAS TEST N° 1



Là où des écarts étaient constatés auparavant, les résultats obtenus avec la nouvelle version d'Arbre-Analyst (et le moteur de calcul XFTA) sont conformes aux calculs analytiques que ce soit avec la méthode Binary Decision Diagram ou avec la méthode Pivotal Upper Bound.

TABLE I. PROBABILITES – CALCULS ANALYTIQUES ET RESULTATS

	Probabilité			
	Analytique	Min Cut Upper Bound (V2)	Binary Decision Diagram (V3)	Pivotal Upper Bound (V3)
E001	9,95E-03	9,95E-03	9,95E-03	9,95E-03
E002	5,00E-05	5,00E-05	5,00E-05	5,00E-05
E003	2,50E-03	2,50E-03	2,50E-03	2,50E-03
E004	1,00E+00	1,00E+00	1,00E+00	1,00E+00
E005	1,00E+00	1,00E+00	1,00E+00	1,00E+00
E006	1,00E+00	1,00E+00	1,00E+00	1,00E+00
E007	1,00E-02	1,00E-02	1,00E-02	1,00E-02
G001	1,00E-02	1,00E-02	1,00E-02	1,00E-02
G002	2,50E-03	7,49E-03	2,50E-03	2,50E-03
G003	1,00E+00	1,00E+00	1,00E+00	1,00E+00
TOP	2,50E-07	7,49E-07	2,50E-07	2,50E-07

TABLE II. FACTEUR D'IMPORTANCE – CALCUL ANALYTIQUE

	PS(E)	PS(Inst E)	MIF	CIF	DIF	RAW	RRW	DIM	BPF
E001	2,50E-05	1,25E-09	2,50E-05	0,995	0,99505	100,003	200,003	0,142955	9,52E-03
E002	2,50E-05	2,48E-07	2,47E-05	4,95E-03	5,00E-03	100,003	1,00497	0,141540	9,52E-01
E003	1,00E-04	0	1,00E-04	1	1	400,5002	NC	0,572546	3,84E-02
E004	2,50E-07	2,50E-07	2,27E-11	9,08E-05	0,999955	1,000000	1,00009	1,30E-07	3,96E-10
E005	2,50E-07	2,50E-07	2,27E-11	9,08E-05	0,999955	1,000000	1,00009	1,30E-07	3,96E-10
E006	2,50E-07	2,50E-07	2,27E-11	9,08E-05	0,999955	1,000000	1,00009	1,30E-07	3,96E-10
E007	2,50E-05	0	2,50E-05	1	1	100	NC	0,142958	0

TABLE III. FACTEURS D'IMPORTANCE – RESULTATS OBTENUS AVEC ARBRE-ANALYST V3

	PS(E)	PS(Sint E)	MF	CF	DF	RAW	RRW	DM	BPF
E001	2.50E-05	1.25E-09	2.50E-05	0.995	0.99955	100.003	200.003	0.142958	9.52E-03
E002	2.50E-05	2.48E-07	2.47E-05	4.95E-03	5.00E-03	100.003	1.00497	0.141540	9.52E-01
E003	1.00E-04	0.00E+00	1.00E-04	1	1	400.5	0	0.572546	3.84E-02
E004	2.50E-07	2.50E-07	2.27E-11	9.08E-05	0.999955	1	1.00009	1.30E-07	3.97E-10
E005	2.50E-07	2.50E-07	2.27E-11	9.08E-05	0.999955	1	1.00009	1.30E-07	3.97E-10
E006	2.50E-07	2.50E-07	2.27E-11	9.08E-05	0.999955	1	1.00009	1.30E-07	3.97E-10
E007	2.50E-05	0	2.50E-05	1	1	100	0	0.142958	0

C. Cas 2

La second cas test vise à valider le traitement d'un arbre de défaillances de grande taille. L'arbre de défaillances utilisé présente donc volontairement un grand nombre d'événements de base (800) et de portes (306) au-delà des tailles généralement rencontrées sur les arbres de défaillances réalisés par Naval Group. Cet arbre de défaillances comporte plus de 86 400 coupes d'ordre 2 à 7 et la probabilité de l'événement sommet est de $3,45.10^{-4}$.

Ce type d'arbre de défaillances met en difficulté certains moteurs de calcul avec un calcul qui se solde parfois par un message d'erreur. Le test réalisé consiste à vérifier que le calcul aboutit et à mesurer le temps nécessaire pour obtenir les résultats. La précédente version d'Arbre Analyst donne un résultat satisfaisant sans limitation sur les coupes ou les probabilités au bout d'environ 15 secondes (Min Cuts Upper Bound). Avec la version 3 et dans les mêmes conditions (pas de limitation et matériel identique), le temps de calcul est équivalent avec la méthode Binary Diagram Decision et augmente sensiblement (de l'ordre de 3 minutes) en utilisant la méthode Pivotal Upper Bound avec toutefois l'obtention d'un résultat totalement valide.

TABLE IV. CAS TEST 2 – RESULTATS OBTENUS AVEC ARBRE-ANALYST V3

	Min Cut Upper Bound (V2)	Pivotal Upper Bound (V3)	Binary Decision Diagram (V3)
Résultat (Probabilité)	3,47E-04	3,46E-04	3,45E-04
Temps de calcul	Environ 15 s	Environ 3 min	Environ 15 s

Ce résultat montre que dans certains cas (y compris avec un nombre d'événements important), la méthode Binary Diagram Decision peut s'avérer très efficace.

D. Cas 3 : application industrielle

1) 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 événements redoutés relatifs à ces installations, sont ainsi liés à des pertes de prestations, pouvant résulter:

- De défaillances systémiques, pouvant être à l'origine d'un événement 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 [1].

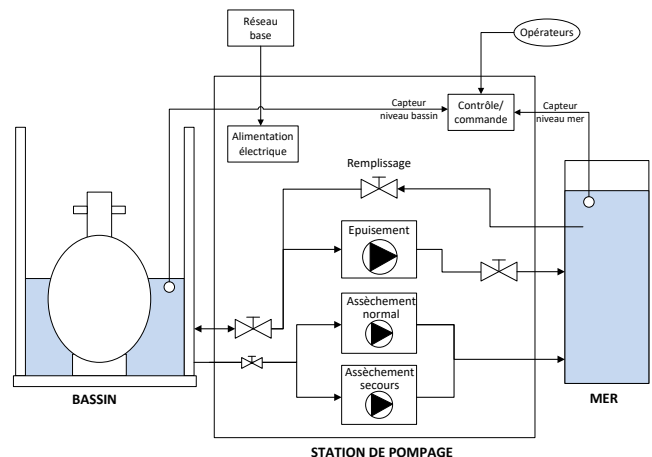
2) Présentation du cas d'étude industriel

Le cas d'étude industriel présenté 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).

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.

L'évènement redouté associé à cette installation est ainsi le déséchouage intempestif d'un SNM provoqué par une indisponibilité, sur un temps suffisamment long, des moyens de pompage.

FIGURE 8: ARCHITECTURE SIMPLIFIEE D'UNE STATION DE POMPAGE



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, ...).

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.

Cette installation doit respecter plusieurs objectifs de sûreté probabilistes, dont deux en particulier nous serviront à illustrer l'impact des évolutions de la nouvelle version d'Arbre-Analyst et les gains apportés.

Les objectifs considérés par la suite sont ainsi :

- L'évènement redouté (ER) : l'évènement redouté doit être avoir une FAO inférieure à 10^{-7} , afin de pouvoir exclure le risque
- L'évènement initiateur (EI) correspondant à la perte d'une ligne de pompage normale doit avoir une FAO inférieure à 1

Ce cas d'étude nous permettra de couvrir à la fois l'évaluation d'un évènement à probabilité faible et d'un évènement à probabilité élevée.

3) Analyse comparative du cas d'étude

La finalité de la présente analyse est de comparer les résultats obtenus avec la nouvelle version d'Arbre Analyst, en se basant sur une étude existante réalisée avec la version précédente.

Les lois utilisées dans les arbres de défaillances sont de type exponentielle pour l'EI et de type GLM et test périodique pour l'ER.

Les écarts constatés entre les résultats obtenus avec la version 2 (Min Cuts Upper Bound) et la version 3 (Pivotal Upper Bound et Binary Decision Diagram) d'Arbre Analyst sont présentés dans le tableau ci-après.

TABLE V. CAS INDUSTRIEL – ECARTS CONSTATES ENTRE RESULTATS OBTENUS AVEC ARBRE-ANALYST V2 ET V3:

Paramètres SDF	ER (Probabilité faible)		EI (Probabilité élevée)	
	Pivotal Upper Bound (V3)	Binary Decision Diagram (V3)	Pivotal Upper Bound (V3)	Binary Decision Diagram (V3)
Probabilité	0%	0%	0%	0%
WTOP	-1%	-1%	-18%	-18%
Défiabilité système	0%	0%	-9%	-9%
Lambda système	3%	3%	-21%	-21%
MTTF système	0%	0%	28%	28%
Durée d'indisponibilité	-1%	-1%	0%	0%
Nombre de pannes	0%	0%	-9%	-9%
MTTR système	0%	0%	0%	0%
MTBF système	0%	0%	10%	10%

Les résultats obtenus avec les nouveaux algorithmes de calcul permettent ainsi de constater que:

- pour un évènement à probabilité faible, ils restent identiques ou très proches des résultats obtenus avec l'ancien algorithme ;
- pour un évènement à probabilité élevée (proche de 1), les résultats obtenus sont beaucoup plus précis que ceux obtenus avec l'ancien algorithme. Les gains constatés sur les paramètres liés à la fiabilité varient ainsi de 10 à 30%.

Les nouveaux algorithmes de calcul du moteur de calcul XFTA (Pivotal Upper Bound et Binary Decision Diagram) intégrés dans la nouvelle version d'Arbre Analyst sont donc toujours aussi performants pour évaluer les paramètres SDF d'évènement à probabilité faible.

Ils améliorent cependant de manière significative l'évaluation des paramètres SDF pour les évènements à

probabilité élevé (proche de 1). Ce gain présente un grand intérêt sur le plan industriel, car il permettra de définir les solutions adaptées pour répondre aux objectifs spécifiés au juste besoin, notamment au niveau des choix architecturaux et matériels, et au niveau des contraintes liées au soutien logistique.

E. Synthèse

Les trois cas présentés montrent que les nouvelles méthodes de calcul proposées (à travers le moteur de calcul embarqué XFTA) permettent à Arbre-Analyst d'être toujours aussi performant pour les arbres de défaillances de grande taille tout en améliorant la précision des valeurs obtenues avec des résultats conformes à ceux obtenus par voie analytique (probabilités fortes et facteurs d'importances notamment).

VI. CONCLUSION

Les évolutions majeures apportées au moteur de calculs XFTA permettent à l'applicatif Arbre-Analyst de gagner en maturité pour continuer à répondre aux besoins des études de sécurité et de fiabilité de systèmes de grandes tailles.

Nous avons présenté des cas applicatifs qui, d'une part, montrent que les évolutions n'entraînent pas de régression vis-à-vis de la version précédente d'Arbre-Analyst et, d'autres parts, montrent que les gains qui peuvent être obtenus en terme de précision des résultats peuvent être non négligeables.

La prise en compte du temps long des projets et de la nécessaire interopérabilité entre toutes les parties prenantes d'un programme a été un des axes de développement prioritaire d'Arbre-Analyst et cela dès le début notamment au travers de l'emploi du format documenté « Open-PSA ».

Finalement, nous observons une dynamique positive dans l'adoption d'Arbre-Analyst, d'Open-PSA et d'XFTA ce qui nous encourage à poursuivre le développement de ces outils, qui est le fruit d'une collaboration fructueuse entre le milieu de la recherche académique et celui de l'industrie.

- [1] Autorité de Sûreté Nucléaire, "RFS 2002-01 – Développement et utilisation des études probabilistes de sûreté", 2003
- [2] E. Clement, T. Thomas, A. Rauzy, Arbre-Analyste : un outil d'arbres de défaillances respectant le standard Open-PSA et utilisant le moteur XFTA, Lambda-Mu 19
- [3] A. Rauzy, Probabilistic Safety Analysis with XFTA, AltaRica Association
- [4] Site Internet XFTA <http://www.altarica-association.org/members/arauzy/Software/XFTA/XFTA2.html>
- [5] S. Epstein, A. Rauzy, « Open-PSA Model Exchange Format » 2008 Site Internet d'Open-PSA : <https://open-psa.github.io/>
- [6] Site Internet Arbre-Analyste : <https://www.arbre-analyste.fr/>
- [7] S. Breton, P. Le-Com, T. THOMAS and E. Clement, "System-Analyst – un outil pour l'analyse des risque, libre de diffusion et compatible avec Arbre-Analyste et Open-AltaRica" Lambda-Mu 21
- [8] Site Internet « System-Analyst » <https://www.system-analyst.fr>