Diagramme de justification

Un outil pour la validation, la certification et l'accréditation

Thomas Polacsek

ONERA, Département Traitement de l'Information et Modélisation
2, avenue Edouard Belin BP74025,
31055 Toulouse Cedex 4, France

RÉSUMÉ. *Le but des diagrammes de justification est d'organiser et de visualiser, de manière synthétique, les principaux éléments prouvant la validité d'une propriété pour un produit. Un diagramme de justification ne représente pas un processus, il organise et donne à voir la rationalité sous-jacente à l'ensemble des documents de Vérification & Validation (V&V). En fait, il répertorie et structure tous les éléments de preuve nécessaires dans un cycle de développement. Cependant, la validation d'un diagramme de justification passe nécessairement par la validation et l'identification des éléments de preuve de chaque étape unitaire, de chaque étape intermédiaire, incluse dans le diagramme. Dans cet article, nous présenterons un modèle d'argumentation générique et ses dérivés qui permettent de structurer de façon logique tous les éléments de V&V pour chaque étape. Ce patron est issu de travaux provenant des sciences légales et des théories de l'argumentation et il est l'élément de base pour la construction des diagrammes de justification.*

ABSTRACT. *The aim of justification diagrams is to organize and visualize, in a synthetic way, all key elements proving the validity of a product's property. A justification diagram does not represent the process, but gives the rational behind all Verification & Validation (V&V) documents. In fact, it lists and organizes necessary evidence in a development life cycle. But the validity of the final assessment requires the validation and the identification of the evidence of each intermediate step. So, in this article, we introduce a generic argumentation pattern and its derivations whose support a rational organization of all V&V evidence at each step. This pattern stems from legal science and argumentation theory legacies, and it is the basic building block for the justification diagram construction*

MOTS-CLÉS : *argumentation, vérification et validation, ingénierie des exigences.*

KEYWORDS: *argumentation, verification et validation, requirements.*

DOI:10.3166/ISI.22.2.95-119

1. Introduction

Durant le cycle de développement d'un produit, peu importe que cela soit un objet réel, un logiciel ou le résultat d'une analyse, des activités de Vérification et de Validations (V&V) sont réalisées afin de garantir la conformité du produit avec ses attentes. Ces activités de V&V ne sont pas toujours cantonnées à un usage interne, elles peuvent aussi jouer un grand rôle dans les activités d'acceptation d'un produit par un client ou de certification d'un produit par une autorité. Un autre exemple d'acceptation peut être une revue par un comité d'experts pour passer un niveau de Technology Readiness Level [1] (TRL) ou jalon dans un projet. Nous utiliserons par la suite le terme générique « *autorité* », qui représente le client ou une autorité extérieure.

Nous pouvons ici opérer un rapprochement entre ce que nous appelons *acceptation* et les activités dites d'*accréditation* dans le domaine de la simulation. Ainsi, la *Vérification, Validation et Accréditation* (VV&A) (Balci, 1998) définit une activité d'accréditation (ou de certification) qui implique une autorité certifiant qu'un modèle ou une simulation peut être utilisé dans un contexte spécifique. Pour cela, il est nécessaire de disposer d'une documentation exhaustive, expliquant non seulement les résultats, mais aussi les données d'entrée, les hypothèses faites, les techniques appliquées, etc. La tâche d'accréditation consiste donc à recueillir cette documentation et à l'évaluer.

Pour bien comprendre les trois étapes de la VV&A, prenons l'exemple simple de l'application du *modus ponens* en logique. Considérons que nous avons a et $a \rightarrow b$, dès lors nous pouvons en déduire b. L'opération de vérification consiste à vérifier comment nous avons obtenu b (ici par application du *modus ponens*). L'opération de validation va consister à vérifier que nous avons effectivement a et que nous voulions réellement obtenir b. L'opération d'accréditation consiste à vérifier sur quel fondement se base a et $a \rightarrow b$, à vérifier que la logique formelle est un moyen acceptable pour démontrer b et à s'interroger sur la crédibilité de celui qui a réalisé cette démonstration. Si c'est un programme, est-il accrédité pour l'étude et si c'est un humain a-t-on confiance en lui ? Dans cet exemple, l'autorité qui réalise l'opération d'accréditation n'est pas forcément spécialiste en logique formelle, elle doit seulement établir si c'est un moyen acceptable de preuve dans ce cadre d'emploi précis.

De manière générale, il n'est nul besoin pour les activités de certification d'être un expert dans tous les domaines couverts par les opérations de V&V. Prenons pour exemple un ingénieur qui veut savoir si la conjecture de Fermat est un théorème ou non. Il se trouve qu'Andrew Wiles a fait une démonstration de la conjecture, mais, comme notre ingénieur n'est pas un expert en théorie des nombres, il n'en comprend pas la preuve. Est-ce à dire que notre ingénieur n'a pas confiance en la preuve de Wiles ? Bien sûr que non. S'il a confiance, c'est parce que suffisamment de chercheurs

1. Le TRL est une mesure de maturité technologique, historiquement employée par les agences gouvernementales américaines, elle est aujourd'hui largement utilisée dans le milieu industriel. C'est une échelle de 1 à 9, qui est employée pour évaluer le niveau de maturité d'une technologie.

ont validé la preuve et qu'il existe en science un système de relecture par les pairs. Par conséquent, il semble raisonnable de considérer que la preuve de Andrew Wiles est correcte.

Ainsi, à chaque étape du processus de développement des documents de V&V sont créés pour pouvoir montrer une propriété du produit ou que le produit répond bien à une exigence. Pour chaque étape, nous devons répondre aux questions suivantes:

– Quelle méthode a été utilisée pour soutenir [2] une propriété ?

– Pourquoi cette méthode est pertinente ?

– Quelles sont les restrictions concernant l'utilisation de cette méthode ?

– Sur quels éléments de preuve, ou quelles propriétés du produit, se base l'utilisation de cette méthode dans ce cas particulier ?

À partir des réponses à ces questions, nous pouvons articuler un modèle générique de raisonnement, que nous appellerons *modèle d'argumentation générique*, qui explique comment, sur la base d'éléments de preuve, il est possible d'affirmer une conclusion. De ce modèle générique, il sera possible de dériver des modèles plus spécifiques, *modèles d'argumentation spécifiques*, dédiés à chaque domaine et à chaque activité de V&V.

Dans la pratique, nous ne voulons pas nous concentrer seulement sur un unique pas de raisonnement, mais établir des conclusions complexes qui impliquent plusieurs étapes de raisonnement, plusieurs applications de nos modèles d'argumentation spécifiques, et toutes ces étapes de raisonnement, prises ensemble, forment ce que nous nommons un *diagramme de justification* [3].

Dans cet article, nous allons présenter les concepts de patrons d'argumentation et de diagrammes de justification. Pour définir nos différents patrons, nous nous sommes basés sur les travaux issus de la communauté argumentation. Le domaine de l'argumentation se concentre sur les liens entre hypothèses et conclusions, c'est-à-dire comment structurer le raisonnement d'un point de vue rhétorique. La notion d'argumentation se réfère bien évidemment à la notion de preuve, notion qui a largement évolué dans l'histoire des sciences et qui n'a pas la même signification selon que l'on se réfère aux méthodes formelles, aux sciences expérimentales ou aux sciences humaines. Ainsi, dans la section 2, nous présenterons un bref état de l'art de l'argumentation, puis, dans la section 3, nous introduirons notre modèle d'argumentation générique et le concept de patrons d'argumentation spécifiques. Dans la section 4, nous montrerons comment construire un diagramme de justification à partir de patrons spécifiques. Dans la section 5, nous mentionnerons brièvement comment nous avons

2. Nous pourrions être tenté d'employer le terme *démontrer*. Cependant, démontrer appelle une démonstration et sous-entend une preuve. Voulant éviter toute ambiguïté avec le domaine de la preuve formelle, nous lui préférerons l'usage du terme *soutenir* au sens de défendre avec des arguments.

3. Dans la première version de ce travail (Polacsek, 2016), nous avions appelé ce diagramme : *diagramme d'argumentation*, mais, afin d'éviter toute ambiguïté avec les nombreux travaux en argumentation dialogique, nous avons finalement opté pour l'appellation: *diagramme de justification*.

appliqué notre approche argumentative dans différents cas d'études et la section 6 sera dévolue à la conclusion.

2. Argumenter et justifier

2.1. Un besoin d'argumentation

Un produit, que cela soit un logiciel, un bien manufacturé comme un avion, voire même un service, est rarement un produit seul, il s'inscrit dans un processus industriel et répond à des attentes identifiées. Il possède des caractéristiques, des propriétés, qui répondent notamment à des exigences. C'est justement sur les fondements de ces propriétés que nous allons nous pencher. Dire qu'un produit a une propriété donnée signifie que nous considérons *savoir* que le produit possède cette propriété. Mais que revêt exactement le terme savoir ? Dans le Théétète, Platon propose diverses analyses de ce que pourrait être la connaissance. Celle que retiendra une grande partie de l'histoire de la philosophie est la définition dite tripartite qui consiste à dire qu'une chose est sue : (1) si elle est vraie, (2) si on la croit vraie et (3) si l'on possède des *justifications* sur cette croyance. On parle alors de *croyance vraie justifiée* (dite *JTB*, dans la littérature, pour *justified true belief* en anglais).

Si nous acceptons cette définition de la connaissance, le point focal devient la notion de justification. En effet, si nous considérons qu'un produit à une propriété donnée, nous pouvons raisonnablement penser qu'objectivement il possède cette propriété et que nous croyons qu'il la possède. Nous évacuons tout ce qui relèverait de la malhonnêteté, qui n'a pas lieu d'être ici. Dès lors, suivant la définition tripartite, il ne reste plus qu'à établir les justifications garantissant la propriété. Pour cela, nous pouvons nous pencher sur les travaux réalisés par la communauté de l'argumentation et certains logiciens.

Quand on s'intéresse à la justification d'une propriété, il n'est plus question de validité, au sens où la propriété serait vraie ou fausse, mais d'étudier pourquoi une propriété est jugée comme acceptable. Nous pouvons ici opérer un rapprochement avec les travaux de Charles Hamblin (Hamblin, 1970) qui remet en question l'utilisation de la logique formelle face à l'étude de l'argumentation. Plus précisément, il s'intéresse aux raisonnements fallacieux et reprend les travaux d'Aristote sur les sophismes. Le but d'Hamblin étant de comprendre ce qui rend une argumentation acceptable, il donne un nouveau modèle de la validité d'un raisonnement, la validité ne dépendant plus de critères logiques relatifs à la vérité des prémisses, mais à des critères dialectiques, à des justifications et à la façon de les organiser. La relation entre les prémisses et la conclusion n'est plus de l'ordre de l'implication logique mais d'une dialectique qui autorise, ou interdit, des comportements discursifs.

Notons que cette démarche coïncide avec deux autres travaux majeurs dans le domaine de l'argumentation. Premièrement, la publication de *Traité de l'argumentation : La nouvelle rhétorique* (Perelman, Olbrechts-Tyteca, 2008) où Perelman et Olbrechts-Tyteca définissent une nouvelle théorie de l'argumentation basée sur une approche

dialectique qui complète la logique. Pour eux, les logiciens, dans un idéal cartésien, n'admettent comme rationalité que la démonstration logique. Dès lors, il devient impossible d'établir des raisonnements autre que purement formels ce qui est « ... *une limitation indue et parfaitement injustifiée du domaine où intervient notre faculté de raisonner et de prouver* ». Deuxièmement, la création par Stephen Toulmin (Toulmin, 2003) d'un modèle présentant, de façon générique, comment passer de faits à une conclusion. Le modèle de Toulmin est aujourd'hui enseigné dans de nombreuses universités américaines pour expliquer les mécanismes de l'argumentation que cela soit dans ce que l'on nomme la pensée critique ou dans le cadre de l'argumentation légale.

Aujourd'hui, l'étude de la validité d'une argumentation et des mécanismes sous-jacents est étudiée par un ensemble de disciplines telles que : l'informatique (au travers de l'intelligence artificielle), la linguistique, l'épistémologie et les sciences légales.

2.2. Le modèle de Toulmin

Dans cette section, nous allons brièvement présenter le modèle d'argumentation de Toulmin. Comme nous le verrons par la suite (section 3), nous allons utiliser une version simplifiée de ce modèle pour définir et structurer, sous forme de diagramme, les justifications qui sous-tendent une propriété donnée. Ainsi, même si nous n'utiliserons pas le modèle de Toulmin à proprement parler, nous allons en donner un aperçu général afin de clarifier les concepts liés à l'argumentation.

Dans ce modèle (voir exemple figure 1), toute argumentation est composée d'une conclusion, ou thèse, notée C (pour *claim*), « *conclusion dont nous cherchons à établir la valeur* » comme le dit Toulmin, et des données, ou faits, notées D (pour *data*), « *faits que nous invoquons à l'appui de cette thèse* ». Très basiquement, pour Toulmin qui a une vue légaliste, bien argumenter consiste à énoncer une conclusion en s'appuyant sur des faits.

Dans la pratique, pour passer de faits à une conclusion on utilise, de manière parfois implicite, des données supplémentaires. Ces données relèvent plus du processus de raisonnement qui permet de passer des faits à la conclusion, typiquement dans le domaine légal, on s'appuie sur un article de loi. Dans le modèle de Toulmin, ces données sont appelées garanties et notées W (pour *warrant*). Distinguer ce qui relève des faits et des garanties n'est pas toujours une chose aisée. Les garanties sont générales, elles attestent de la solidité de l'argumentation, alors que les faits dépendent plus de données considérées avérées. Aux garanties s'ajoute le concept de fondements, noté B (pour *backing*), fondements qui sont la justification de pourquoi des garanties sont acceptables.

Une conclusion n'ayant pas toujours un caractère absolu, il est possible d'exprimer des réserves avec des *qualificateurs modaux*, notés Q (pour *qualifier*). Les qualificateurs modaux correspondent à des notions telles que « *possiblement* » ou « *probablement* ». Pour finir, se rajoute au modèle, des conditions de réfutation, notées R (pour

rebutal), qui expriment les circonstances dans lesquelles la conclusion ne serait pas vraie, en d'autres termes les exceptions possibles.

(D) les données sont cryptées avec OpenSSL et une clé de 128 bits	$\longrightarrow$	*Donc* (Q) certainement (C) les informations contenues dans le fichier ne sont pas accessibles à quelqu'un de non autorisé
	Vu que (W) une clé de 128 bits suffit pour protéger les données d'après l'Advanced Encryption Standard	
	En vertu de (B) l'Advanced Encryption Standard publié en 2001 préconise une taille de clé de 128 bits (FIPS PUB 197)	*Sauf si* (R) quelqu'un vole la clé

Figure 1. Exemple du schéma de Toulmin pour la propriété : "seules les personnes autorisées peuvent lire les données protégées"

Nous donnons, figure 1, un exemple d'application du modèle pour établir la propriété « *seules les personnes autorisées peuvent lire les données protégées* ». Dans cet exemple, nous avons le fait (D) « *les données protégées sont cryptées avec OpenSSL (AES) avec une clé de 128 bits* » et nous savons par ailleurs qu'« *une clé de 128 bits est suffisante pour protéger les données* » sur la base de l'« *Advanced Encryption Standard* » ce qui correspond dans notre raisonnement à, d'une part, la garantie et, d'autre part, la justification de cette garantie. Dans notre exemple, la conclusion n'est pas toujours vraie. En effet, la confidentialité des données n'est pas établie dans l'absolu : un attaquant peut voler la clé. Il faut donc ajouter la réfutation « *quelqu'un vole la clé* ».

Comme nous l'avons dit précédemment, nous ne sommes pas dans le cadre de la logique formelle, nous ne disposons donc pas d'un système axiomatique qui peut nous donner la valeur de validité de la formule $D \rightarrow C$. Nous sommes dans un cadre rhétorique où nous essayons de définir si nous sommes face à une « *bonne* » argumentation ou pas.

2.3. Modèles conceptuels pour la justification

Les modèles conceptuels, comme ceux employés dans le cadre de l'ingénierie des modèles, sont utilisés dans presque toutes les activités cognitives. Dans l'ingénierie, ils sont utiles non seulement pour définir et expliquer un système, mais aussi pour supporter le processus de création comme celui de décision. Aujourd'hui, dans de nombreux projets, l'utilisation de modèles est non seulement utile, mais elle est devenue indispensable. Ainsi, dans le cadre de l'ingénierie systèmes, nous trouvons des modèles pour à peu près toute les activités gérées par l'ingénierie que cela soit les processus (avec par exemple BPMN), le comportement du système (comme le modèle des machines à états ou les diagrammes d'activités), la structure du système (comme

les diagrammes de classes) ou pour les exigences (comme *KAOS* (van Lamsweerde, 2009)). En ce qui concerne les activités de design, nous retrouvons les modèles sur des activités telles que, par exemple, l'organisation des connaissances (comme (Grangel *et al*., 2007)) ou la prise de décision (comme *IBIS* (Kunz, Rittel, 1970)).

Malgré cette profusion de modèles, nous trouvons peu d'exemple dans la littérature de modèles conceptuels pour représenter la confiance. La confiance est une notion complexe, difficile à définir et qui soulève bien des débats philosophiques (Jones, 2002). Cependant, si nous cherchons à nous limiter seulement aux activités d'ingénierie, nous pouvons réduire le problème de la confiance à un problème de confiance dans un résultat ou un produit. Dans ce cas, la confiance en quelque chose correspond à disposer de suffisamment d'éléments de preuve, compréhensibles, qui établissent que quelque chose est vraie. Comme nous l'avons vu, pour établir la confiance en ingénierie nous avons besoin d'organiser un ensemble de connaissances.

Parmi les modèles visant à organiser un savoir, des idées, nous pouvons citer *IBIS* pour « *Issue-Based Information Systems* » (Kunz, Rittel, 1970). *IBIS* a été conçu pour aider et documenter les processus visant à produire de l'information. *IBIS* définit trois éléments clés : les *Questions*, les *Idées* et les *Arguments*. Les Questions sont des éléments représentant toutes les questions relatives au sujet du débat et les Idées sont simplement les réponses ou les solutions à une Question. Les Arguments, de leur côté, représentent des opinions, des faits, des données, etc. Un Argument peut prendre une coloration pour, ou contre, quand il soutient, ou attaque, une Idée. D'un point de vue représentation, tous les éléments d'*IBIS* sont reliés ensemble par des flèches formant un graphe appelé une carte d'argumentation. Dans (Kirschner *et al*., 2003), les auteurs présentent un ensemble d'études de cas et de commentaires sur la manière dont *IBIS* est utilisé dans la pratique.

Dans la lignée d'IBIS, de nombreuses notations ont vu le jour dans une optique d'aide à la conception. Elles ont toutes en commun de chercher à capturer les justifications et les raisons derrières les décisions prises durant la conception, ainsi que les différentes alternatives de conceptions qui n'ont finalement pas abouties. Citons pour exemple l'approche *Questions, Options and Criteria* (QOC) (MacLean *et al*., 1991) qui permet d'identifier les problèmes de conception à l'aide de questions et les alternatives à l'aide de réponses possibles. De plus, QOC dispose d'un principe d'évaluation basé sur les exigences à satisfaire et les propriétés souhaitées qui permet d'évaluer les différentes options.

Cependant, les approches de type IBIS se situent dans les phases amont de développement, lors du design et des choix de conception (Shum, Hammond, 1994). De notre côté, nous adressons un problème quelque peu différent, puisque nous nous intéressons à l'acceptation du produit. Il n'est donc plus question de garder une trace des alternatives, mais d'essayer, le plus finement et le plus formellement possible, d'expliciter les raisons et le contexte pour lesquels le produit est acceptable.

2.4. Sureté de fonctionnement et argumentation

Dans le domaine de la sûreté de fonctionnement, un *assurance case* est un document structuré qui fournit une justification et des arguments valables sur le fait qu'un système satisfait des propriétés relatives à sa sûreté. Pour le UK Ministry of Defence Standard $00-42$ [4], l'assurance case est « *une argumentation raisonnée et auditable, créée pour soutenir l'affirmation selon laquelle un système satisfait des exigences* » [5]. Dans la littérature, et suivant le domaine d'application, avionique, nucléaire, ferroviaire ou militaire, nous ne trouverons pas forcément le terme d'assurance case, mais : *safety assessment, accomplishment summary, safety case, certification evidence, security case, assurance case*.

Le lien entre *assurance case* et argumentation est clairement fait dans un standard du ministère de la Défense du Royaume-Uni où l'on trouve : « *Le Safety Case est composé d'une argumentation structurée, soutenue par un ensemble de données* » [6] (*Defence Standard 00-56 Safety Management Requirements for Defence Systems*, 2007, p9, section 9.1). Dans le même ordre d'idée, la norme ISO 150266 [7] propose, sans expliquer comment, d'assembler un ensemble structuré d'affirmations et de sous-affirmations (buts et sous-buts) pour disposer d'une argumentation pour des objectifs de haut niveau.

Concernant la forme des *assurance cases*, si les premières versions étaient un ensemble de documents sans le moindre diagramme, il semble aujourd'hui que la tendance soit de donner une représentation graphique de l'argumentation. Bien qu'il n'y ait pas de véritable consensus sur une unique représentation, notons une prédominance dans le milieu industriel pour la méthode Goal Structuring Notation (GSN). GSN est basée sur les travaux de (Kelly, Weaver, 2004) qui cherchent à définir une approche cohérente pour la construction, la présentation, la maintenance et la réutilisation des arguments d'une argumentation de sûreté de fonctionnement. L'approche est, en fait, une notation graphique et un ensemble de bonnes pratiques qui permettent de s'en servir.

Une des limitations de la notation GSN est qu'elle est entièrement axée sur la sûreté de fonctionnement. L'objectif d'un diagramme GSN est d'afficher, sous une forme graphique, la démonstration que les propriétés de sûreté sont satisfaites et que tous les risques ont été pris en compte. Des liens entre GSN et des normes d'*assurance cases* ont été établis, par exemple (Holloway, 2015) montre comment utiliser GSN pour définir des *assurance cases* dans le domaine de l'informatique embarquée avionique

---

4. Dans (*Defence Standard 00-42 Reliability and Maintainability Assurance Guide Part 3: R&M Case*, 2008, section 4.1)

5. Trad. « *a reasoned, auditable argument created to support the contention that a defined system will satisfy the . . . requirements* »

6. Trad. « *The Safety Case shall consist of a structured argument, supported by a body of evidence* »

7. La norme ISO/IEC 15026 (ISO/IEC 15026-2, 2011) est une norme applicable aussi bien à des systèmes qu'à des logiciels. Elle permet de définir des niveaux d'intégrité. Le but de ces niveaux d'intégrité est, par exemple, d'aider à assurer les caractéristiques de sûretés ou de sécurités d'un système.

(DO-178), mais seulement dans un but de sûreté de fonctionnement. Par ailleurs, toujours dans un but de sûreté de fonctionnement, (Sujan *et al*., 2015) expliquent comment GSN pourrait être utilisée par les organismes de santé et (Guiochet *et al*., 2013) s'intéressent au même problème dans le cadre de l'interaction homme-robot.

Ainsi, parce que nous ne voulons pas concevoir un schéma d'argumentation dédié seulement à la sûreté de fonctionnement (et, avec l'abondance des travaux sur GSN, nous n'avons même pas la prétention de couvrir le domaine de la sûreté de fonctionnement), GSN semble être beaucoup trop spécifique à un domaine pour nos besoins. En effet, même si historiquement la notation était basée sur le schéma Toulmin, elle n'est plus vraiment liée aux travaux de Toulmin (Cassano, Maibaum, 2014). Par exemple, les stratégies dans GSN sont décompositionnelles, l'approche est clairement orientée de la conclusion vers les données : elle part d'un but de sûreté pour le décomposer en éléments unitaires auxquels des solutions sont adressées. De plus, chez Toulmin, le *Warrant* (garantie), appelé *Strategy* dans GSN, est la pierre angulaire du raisonnement alors qu'il n'est qu'un élément optionnel dans GSN. Nous proposons donc de repartir du modèle de Toulmin pour concevoir un schéma d'argumentation générique orienté vers les besoins industriels.

3. Des patrons d'argumentation

L'approche par patrons de conception (Alexander *et al*., 1977) est un moyen de décrire un problème récurrent et sa solution associée avec un haut niveau d'abstraction. Un patron correspond généralement à un problème conceptuel et fournit une solution considérée comme « *bonne* ». Le but premier de l'approche par patron est de capitaliser des solutions basées sur l'expérience. L'utilisation de patrons est particulièrement efficace quand il s'agit de communiquer de bonnes pratiques d'ingénierie. Notons qu'il n'existe pas de langage unique pour exprimer des patrons puisque l'on trouve leur usage dans un large éventail de domaines très hétérogènes comme, par exemple, la conception de logiciels (Gamma *et al*., 1995) ou la conception de bâtiments (Alexander *et al*., 1977).

C'est dans cette idée que nous allons définir tout d'abord un patron générique d'argumentation puis expliquer comment, à partir de ce canevas, il est possible de définir des patrons plus spécifiques correspondants à de bonnes pratiques d'argumentation de propriétés.

3.1. Notre patron d'argumentation

Pour notre patron d'argumentation, nous ne reprenons pas le modèle de Toulmin *stricto sensu*. En effet, nous ne cherchons pas à définir un schéma pour l'argumentation légale, et encore moins à caractériser ce qu'est l'argumentation dans ses aspects philosophiques, mais bien à nous inscrire dans une pratique industrielle. Notre patron est le fruit de tâtonnements et d'expérimentations menés dans le cadre de divers projets que nous évoquerons dans la section 5.

Les différences notables entre notre patron et celui de Toulmin sont que :

– nous évacuons les qualificateurs modaux. Pour nous, une propriété est acceptable ou pas. Nous ne nous intéressons pas à des propriétés qui seraient « *en général* », « *parfois* », etc. acceptables. Le but n'est pas qu'un produit satisfasse parfois une propriété ou réponde souvent à une exigence, mais bien d'établir s'il y répond ou pas. Même pour une propriété non déterministe, comme le système qui consiste à « *envoyer une pièce de monnaie* » et la propriété « *pile* », nous n'avons pas besoin d'un qualificateur modal du type « *parfois* ». En effet, dans notre cas, les réserves exprimées par le qualificateur sont incluses dans la propriété. Dans l'exemple de la pièce de monnaie, la propriété serait « *peut être pile* ». Pour nous, le qualificateur fait partie intégrante de la propriété, ou l'exigence, il ne qualifie pas une propriété existante ;

– pour plus de simplicité, nous agrégeons ensemble les concepts de garantie et de fondement dans un seul concept que nous nommons *Justification* ;

– nous ajoutons le concept de *domaine d'usage*, qui correspond au fait que le patron s'applique dans un contexte précis qu'il peut être nécessaire d'expliciter ;

– nous renommons la notion de réfutation, cas particuliers où la conclusion ne s'applique pas, en *limitation* de la conclusion. Les limitations n'étant plus seulement un cas particulier, mais le cadre, les limites dans lesquelles la conclusion est vraie.

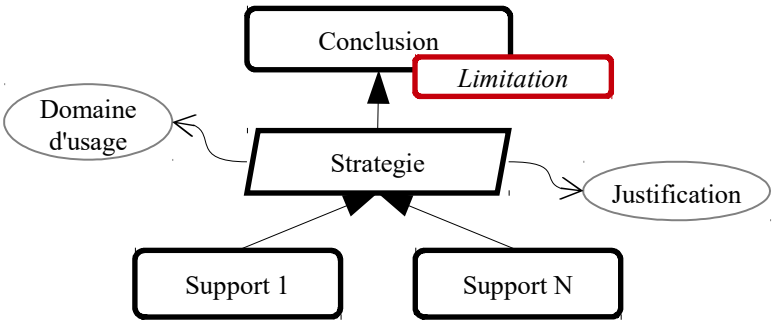

Figure 2. Patron d'argumentation

Notre modèle permet de capter comment s'établit une propriété, ou une conclusion, à partir de supports, ou d'éléments de preuve. Ainsi, le but de ce patron est de répondre aux quatre questions présentées en introduction qui sont : (1) quelle méthode est employée ? (2) Pourquoi cette méthode est applicable ? (3) Existe-t-il des restrictions ? Et (4) sur quelles hypothèses reposent la propriété ?

Il nous faut remarquer que, chez Toulmin, la garantie est ce qui permet de légitimer le passage des éléments de preuve à la conclusion : c'est la pierre angulaire du raisonnement. C'est la garantie qui explicite clairement comment, à partir de données, il est possible d'inférer une conclusion. Remarquons que ce que Toulmin appelle garantie correspond exactement à ce que l'ISO 15026 appelle *Arguments* et que GSN appelle *Strategy*. Pour l'ISO 15026, la stratégie est : « *la colle qui cimente l'assurance*

case en reliant ses supports immédiats - sous déclarations, preuves ou hypothèses - à la conclusion qu'ils supportent ». De la même manière, pour GSN « *la stratégie explique l'inférence entre le but et les sous-buts* ». Afin d'homogénéiser les différents termes, nous avons décidé de ne plus utiliser le terme de garantie de Toulmin, mais le terme *Stratégie*.

Nous proposons une représentation graphique (figure 2) de notre modèle d'argumentation, cette représentation étant librement inspirée de la notation GSN. Notre modèle d'argumentation est basé sur :

– **Conclusion/Propriété** : (unique et nécessaire)
C'est la propriété à démontrer. En général, cette propriété répond à une exigence.

– **Support/Elément de preuve** : (au moins un est nécessaire)
Support sur lequel se fonde la conclusion. Un support peut être intrinsèque (comme des données, un fait reconnu), ou se référer à une autre propriété. Si un support est une propriété, cette propriété est bien sûr la conclusion d'un autre pas d'argumentation et ainsi de suite.

– **Stratégie** : (unique et nécessaire)
Stratégie utilisée pour déterminer la conclusion. La stratégie correspond à la méthode utilisée pour établir le passage des supports à la conclusion. Par exemple, si la conclusion est « *les tests sont suffisants* », une stratégie possible pourrait être « *couverture des tests* », ou si nous avons la conclusion « *le modèle de turbulence est OK* » alors une stratégie possible serait « *déjà utilisé dans des projets similaires* ».

– **Justification** : (unique et facultative)
La justification est l'explication de pourquoi une stratégie est applicable dans un cas précis. La justification est donc forcement reliée à la stratégie. Elle détaille les raisons pour laquelle une stratégie, et donc une méthode, est acceptable. Imaginons une stratégie qui consiste à suivre un protocole défini dans une norme, alors la stratégie est l'application de ce protocole et la justification est la norme et les raisons pour lesquelles la norme est applicable.

– **Domaine d'usage** : (unique et facultatif)
Le domaine d'usage donne les conditions précises d'utilisation et les limites d'une méthode. Si nous reprenons l'exemple de l'application d'une norme alors le domaine d'usage décrira dans quels domaines et dans quelles conditions cette norme est applicable.

– **Limitation** : (facultatif)
Les limitations viennent s'ajouter à la conclusion. Ce sont des restrictions à la conclusion. Elles sont séparées de la conclusion car elles n'ont pas vocations à rester. Quand on rajoute explicitement une limitation à la conclusion c'est que l'on pense qu'elle sera levée. Un exemple peut-être une limitation du produit qui se pose actuellement, mais qui devrait disparaître dans le cadre d'une évolution future (évolution qui donnera lieu à une modification de l'argumentation).

Si nous reprenons notre exemple introductif sur l'application du *modus ponens* (figure 3), nous avons deux éléments de preuve a et $a \rightarrow b$ et une conclusion b. À cela,

nous devons ajouter la stratégie qui serait ici « *application de la logique formelle* ». Si nous voulions rentrer dans les détails, il est possible d'ajouter qu'ici c'est le modus ponens qui est appliqué, mais, comme nous l'avons déjà dit, dans une optique d'accréditation ce qui compte est plus de savoir si la logique est un moyen applicable que de savoir quel mécanisme logique a été appliqué.

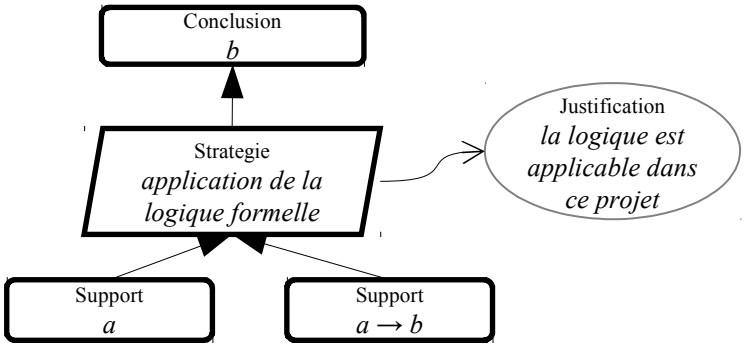

Figure 3. Exemple avec le modus ponens

Remarquons ici que dans notre modèle, comme pour le modèle de Toulmin, l'ensemble des supports est un ensemble sans relation entre ses éléments. Il n'y a aucune hiérarchie entre les supports, ni aucune dépendance. Dans la réalité, les choses peuvent être plus complexes. On peut, par exemple, s'intéresser au cas où un élément de preuve vient en renforcement d'un autre comme dans le cas où un expert garantit une propriété et qu'un autre expert garantit que le premier expert est compétent. L'étude de ces distinctions est présente dans de nombreux travaux (Walton, 2007), mais il nous semble difficile, dans notre cas, d'opérer de telles distinctions. En effet, n'oublions pas que notre but est de proposer un modèle simple et intuitif à des ingénieurs et des experts, pour les aider à organiser et à auditer une masse documentaire de justifications. Si caractériser finement les supports est une chose importante pour la compréhension du raisonnement argumentatif, elle est malheureusement porteuse d'une surcharge de travail beaucoup trop importante dans notre contexte.

3.2. Considérations sur les éléments de preuve

Focalisons nous sur les éléments de preuve d'une argumentation. Toute argumentation, ou démonstration, se fonde sur des vérités préétablies. Par exemple, une démonstration dans un système formel postulera toujours qu'un ensemble d'axiomes sont vrais. Ces axiomes sont vrais par nature, il n'existe pas de démonstration qui les prouve. Ils sont l'élément de base de tout raisonnement dans ce système. De façon analogue, toute argumentation repose sur un ensemble de postulats acceptés par celui qui énonce la démonstration ainsi que par son auditoire.

Dans le cadre de l'argumentation légale, (Rodney A. Reynolds, 2002) définissent les éléments de preuve comme : les données (faits et opinions) présentées comme des preuves pour une affirmation. Si l'on met de côté les vérités communément admises, les éléments de preuve ont la particularité de reposer sur l'autorité de celui qui les énonce. L'acceptation d'un fait ne repose donc plus sur le fait lui-même, mais sur la confiance que l'on accorde à celui qui l'énonce.

Pour nous, les supports se divisent en deux catégories :

1. les éléments de preuve comme un résultat donné dans un article scientifique, une information donnée par un expert, des résultats de tests, une pratique définie sans une norme ou des résultats donnés par un calcul (comme une simulation numérique ou du model checking),

2. des sous-conclusions, c'est-à-dire une conclusion résultant d'une autre étape d'argumentation.

3.3. Des patrons spécifiques

Dans la pratique, il est très difficile d'utiliser notre modèle *in extenso*. En effet, il est nécessaire de définir des modèles dédiés à des utilisations spécifiques. À partir de ce schéma générique d'argumentation, nous devons définir différents patrons, plus spécifiques, qui explicitent plus clairement chaque concept en fonction d'une stratégie donnée. Ces patrons d'argumentations peuvent être de différentes natures : très génériques, mais attachés à une activité, comme par exemple un patron pour les résultats obtenus à « *l'aide d'un logiciel X* » ou au contraire très spécifiques à un domaine comme, par exemple, « *la validation d'un modèle thermique d'équipement* ».

Ces patrons d'argumentation spécifiques peuvent être vus suivant deux dimensions : l'activité et le niveau de maturité (figure 4). L'activité correspond au moyen mis en œuvre pour démontrer la conclusion, c'est finalement l'objet de la stratégie. Par exemple, nous pouvons définir un patron d'argumentation pour l'activité « *calcul de solutions Pareto-optimales* ». La maturité dépend du niveau de détails attendu pour l'argumentation d'une propriété. Ainsi, un patron spécifique à une activité pourra se décliner sous plusieurs patrons, certains très simples, pour des activités peu critiques et/ou de faible niveau de maturité (à TRL bas) comme une étude de conception préliminaire, tandis que d'autres patrons pourront être très détaillés, avec beaucoup d'éléments, s'ils sont utilisés dans un contexte très strict comme la certification.

Bien évidemment, un patron d'argumentation spécifique est étroitement lié à la notion de stratégie. Il correspond à une activité particulière comme l'application d'un processus, l'utilisation d'un logiciel ou la validation par un comité. Cependant, un patron ne se résume pas à sa stratégie. Une activité définit une stratégie, mais aussi un domaine d'utilisation, une conclusion, une justification et une liste d'éléments de preuve obligatoires.

Prenons, à titre d'exemple, un patron d'argumentation pour l'utilisation de résultats fournis par un logiciel. Dans ce patron, la conclusion est le résultat donné par le

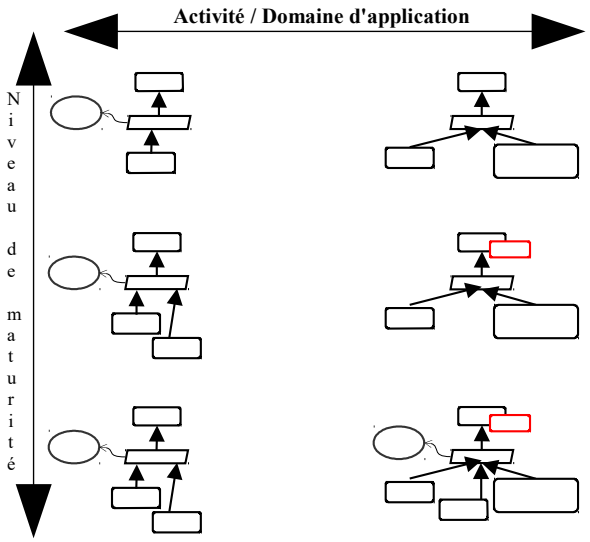

Figure 4. Deux dimensions pour les patrons d'argumentation dédiés

logiciel et les supports sont les informations dont a besoin le logiciel pour produire son résultat. Nous pouvons ici caractériser certains supports, l'usage d'un logiciel étant soumis à un ensemble de conditions, de prérequis. Par exemple, on peut imaginer un logiciel qui garantit des propriétés, mais seulement sur des systèmes déterministes. Par conséquent, l'ensemble des supports pour l'utilisation d'un logiciel devra contenir les conditions d'utilisation dans lesquelles est utilisé le logiciel. Pour vérifier si ces conditions d'utilisation sont adéquates, il est nécessaire d'expliciter clairement le domaine d'usage afin de vérifier que celui-ci couvre correctement les conditions d'utilisation données dans l'argumentation. Notons que la vérification de l'adéquation entre le domaine d'usage et les conditions d'utilisation doit être faite. Suivant les projets, elle peut se faire automatiquement (si les conditions sont exprimées formellement) ou par une personne chargée de la validation.

Le patron d'utilisation d'un outil logiciel est encore assez générique, il est possible d'en dériver des formes plus dédiées pour chaque outil. Considérons l'utilisation d'un logiciel pour calculer le temps d'exécution pire cas d'une application (WCET) [8], le patron pour ce cas précis aura pour stratégie l'utilisation de ce logiciel, le domaine d'usage listera les types de processeurs et les compilateurs utilisables avec ce logiciel et nous trouverons dans les supports le type de processeur et le compilateur utilisé.

8. Worst-Case Execution Time, la durée maximale d'exécution d'une tâche pour une plateforme matérielle donnée

Suivant le projet, on pourra ajouter à ce patron les justifications de pourquoi l'utilisation de ce logiciel est admise.

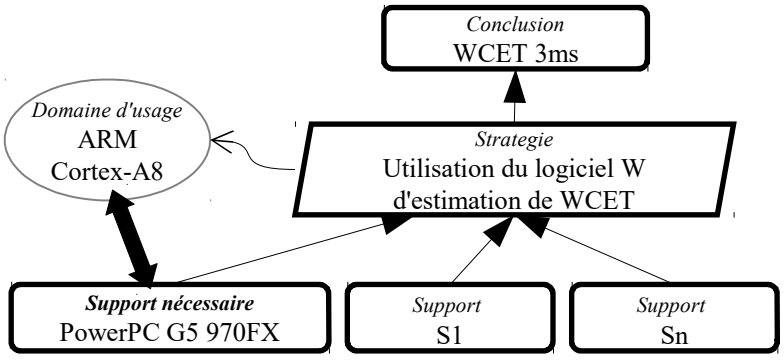

Figure 5. Exemple de problème : WCET

Dès lors, si dans le cadre d'un développement d'application un logiciel de WCET est utilisé, il sera possible d'utiliser un tel patron pour argumenter les résultats donnés par le logiciel. Prenons l'exemple suivant : nous avons un logiciel de WCET qui a calculé que « *pire temps d'exécution pour une application est de 3 millisecondes* », c'est la conclusion, ce logiciel est prévu pour calculer sur un modèle formel de processeur ARM Cortex-A8, c'est le domaine d'usage et le support nécessaire indiquant le processeur sur lequel doit s'exécuter l'application correspond à un PowerPC G5 970FX. Une instanciation partielle du patron à l'aide de cet exemple est donnée figure 5. Remarquons qu'ici, l'argumentation ne tient pas puisque le support nécessaire ne fait pas partie du domaine d'utilisation.

3.4. De l'usage des patrons d'argumentation

Un des objectifs de nos patrons est de pouvoir être utilisés par des êtres humains. Suivant les projets, et suivant le degré de formalisation, ils pourront être considérés comme une *check-list* des éléments nécessaires à produire pour établir une propriété, ils peuvent servir à organiser et structurer l'ensemble des documents de V&V, être intégrés dans des outils informatiques pour faire le lien avec les exigences ou encore indiquer lorsque certaines informations sont manquantes (comme le domaine d'usage ou un support), etc.

De plus, nos patrons fournissent une vue d'ensemble de l'étape d'argumentation qui, bien qu'étant une vue simplifiée, permet de saisir rapidement les tenants et les aboutissants. Bien évidemment, cette représentation n'est qu'une représentation visuelle, mais, mise en œuvre dans un logiciel, chaque boîte de ce diagramme qui représente soit un support, soit une justification, soit un domaine d'usage, est sensée renvoyée à des documents.

Malgré leur caractère générique, une des limitations des patrons d'argumentation est leur réutilisation dans différents contextes, différents projets. En effet, les patrons spécifiques sont très orientés projets et il est difficile de les utiliser d'un projet à un autre, à moins que les deux projets n'aient les mêmes activités. Cependant, les patrons d'argumentation sont utiles parce qu'une fois qu'ils sont définis pour des activités spécifiques, ils sont établis une fois pour toutes. Ainsi, ils guident et donnent un cadre à la fois pour établir les justifications d'une propriété mais aussi pour vérifier ces justifications.

4. Diagrammes de justification

Comme pour le modèle de Toulmin, nos patrons représentent un *pas d'argumentation*, ou *pas de justification*, c'est-à-dire comment, à partir de faits, il est possible d'inférer une conclusion. Dans la pratique, nous ne voulons bien évidemment pas nous concentrer sur une unique étape de raisonnement, mais établir des conclusions complexes qui impliquent plusieurs pas de justification, plusieurs étapes de raisonnement, ces pas de justification pris ensemble formant ce que l'on nomme un : diagramme de justification.

Un diagramme de justification est un diagramme qui capture la structure logique, le raisonnement, de tous les éléments de preuve qui conduisent à accepter une propriété. Dans un diagramme de justification, la racine est une propriété de haut niveau et les feuilles sont les supports de cette propriété. De plus, un diagramme de justification n'est pas seulement une représentation graphique de la façon dont l'ensemble des éléments qui conduisent à une conclusion sont structurés, dans la pratique, chaque élément du diagramme doit se référer à un document stocké dans le système d'information.

En fait, un diagramme de justification est l'agrégation d'instances spécifiques de notre modèle d'argumentation générique. L'objectif principal du diagramme de justification est de fournir une vue d'ensemble de toute la documentation V&V. En effet, le diagramme de justification montre clairement, à chaque étape du raisonnement, les tenants, les aboutissants et les éléments de preuve dans une structure auditable. Le diagramme de justification supporte aussi bien les autorités, les comités de revue que les différentes parties prenantes dans la tâche de comprendre, dans une perspective globale, les activités de V&V. Disposer d'un tel diagramme permet de naviguer facilement dans les documents. Enfin, l'usage de diagrammes de justification s'inscrit également dans une idée de modularité et réutilisablitité. En effet, si une partie de la V&V change alors il est plus facile de comprendre l'impact de ce changement du niveau global.

Notons qu'il existe une similitude de démarche entre l'ingénierie des exigences et une approche argumentative. Dans le cadre des exigences, un des problèmes consiste à raffiner une exigence de haut niveau en exigences de bas niveau. Nous avons un mécanisme de décomposition où se posent entre autre des problèmes de traçabilité et d'exhaustivité. La démarche présentée ici se base sur un procédé argumentatif et

fonctionne, non plus dans une optique de raffinement, mais suivant un mécanisme d'agrégation : c'est à partir d'éléments de base que nous cherchons à établir une propriété de haut niveau (propriété qui est généralement la réponse à une exigence, elle aussi de haut niveau).

Nous construisons un diagramme de justification à partir des patrons spécifiques que nous instancions. Pour chaque pas de raisonnement, un patron spécifique est appliqué et la conclusion de ce patron devient un support du prochain patron appliqué (voir figure 6). En fait, nous utilisons un mécanisme de chaînage entre les pas de justification : chaque conclusion d'un niveau devient un support au niveau suivant.

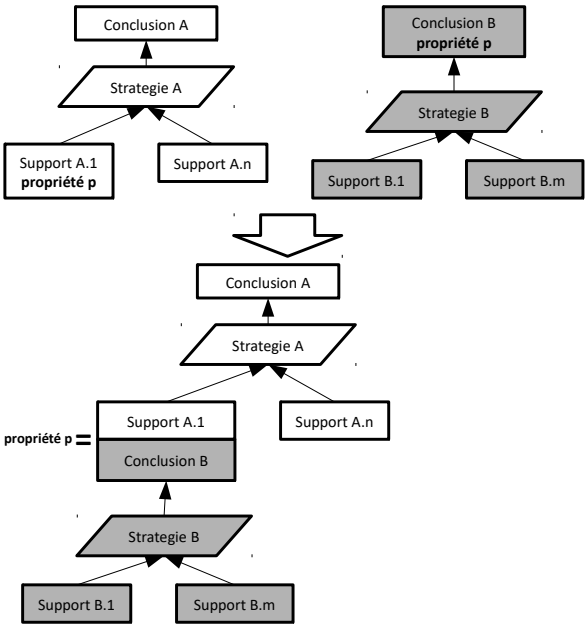

Figure 6. Chaînage entre les pas de justification

Le mécanisme de chaînage doit être utilisé avec précaution, car, premièrement, la conclusion d'un niveau peut être proche du support utilisé au niveau suivant : proche, mais pas exactement identique. Deuxièmement, deux patrons instanciés peuvent être incompatibles pour le chaînage. En effet, leurs domaines d'usages respectifs, ou leurs justifications, peuvent être mutuellement exclusifs.

Un des effets du mécanisme de chaînage de deux étapes de raisonnement est que, dans certains cas, il peut permettre de lever, supprimer, des restrictions. Une conclusion peut être restreinte à un niveau et, si certaines conditions sont remplies, cette restriction est levée au niveau suivant. Prenons la conclusion « *l'équipement est validé, mais seulement en dessous de* 70° ». Deux choix s'offrent à nous, nous pouvons prendre toute la phrase comme conclusion ou la diviser en deux parties, dont l'une est la conclusion et l'autre est la restriction suivante : « *en dessous de* 70° ». Si dans

l'étape d'argumentation suivante, il est établi que le système, et donc l'équipement, est toujours en dessous de 70°, alors l'utilisation d'une restriction est plus efficace que de tout mettre dans une unique conclusion. En effet, dans ce cas-là, nous avons la même conclusion aux deux étapes, mais, dans la deuxième étape de l'argumentation, la restriction est supprimée (voir l'illustration du deuxième cas figure 7).

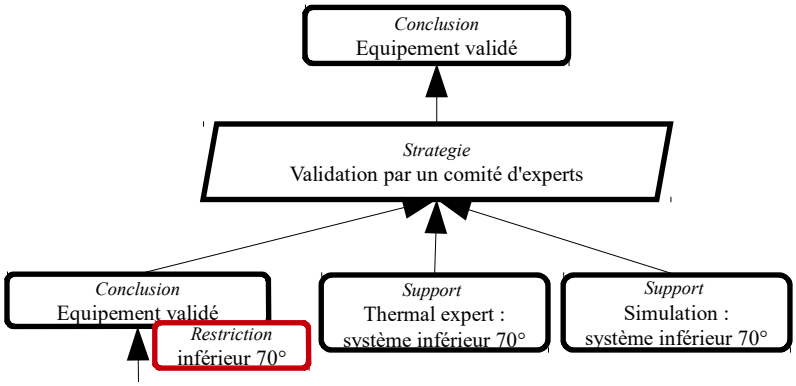

Figure 7. Exemple de suppression d'une limitation

5. Cas d'études

Nous avons appliqué notre méthodologie des patrons d'argumentation dans le cadre de deux projets :

– le projet européen Thermal Overall Integrated Conception of Aircraft [9] (TOICA) qui vise notamment à définir une approche pluridisciplinaire, multi-niveaux, flexible et intégrée pour les phases d'aide à la conception d'architectures aéronautiques ;

– le projet MIMOSA dont le but est de définir un cadre pour aider à la certification avionique de logiciels embarqués.

Nous allons, dans cette section, nous focaliser sur trois exemples où les diagrammes de justification ont permis :

– de partager les connaissances entre les parties prenantes d'un projet ;

– de définir les documents de V&V à produire dans le cadre d'un nouveau processus d'évaluation de la charge de travail pour construire un avion suite à un changement d'architecture ;

– de poser un cadre pour aider à la certification de l'avionique embarquée.

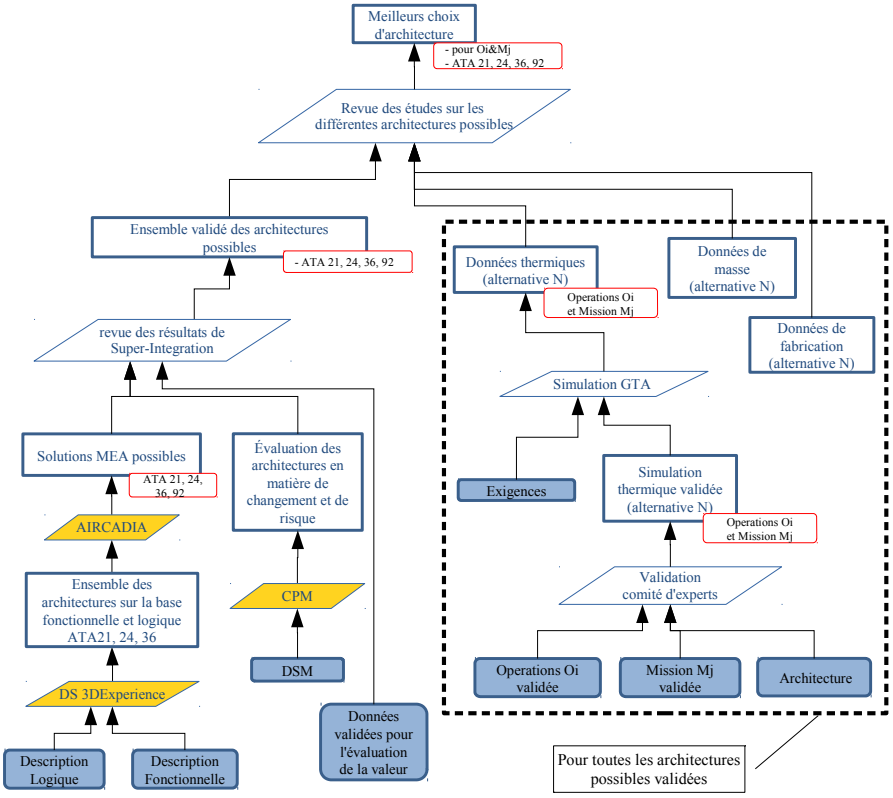

Figure 8. Diagramme de justification : meilleures architectures avion candidates

5.1. Des diagrammes de justification pour partager et comprendre

Dans le cadre du projet TOICA, une méthode innovante a été créée pour déterminer les types d'architectures prometteuses pour un futur avion (Sharma *et al.*, 2016). Cette méthode fait notamment appel à des simulations numériques, des méthodes de choix, des analyses d'experts et l'emploi de logiciels. Nous sommes face à une méthode difficile à comprendre. Il est, par conséquent, très difficile d'évaluer le bien fondé des architectures proposées car : il y a de nombreuses données d'entrées, des critères de sélection, des contraintes spécifiques et des résultats intermédiaires s'appuyant sur des prérequis complexes. Nous avons décidé de réaliser un diagramme de justification pour faciliter la communication entre les parties prenantes et mettre en évidence des éléments clés qui permettent de comprendre pourquoi nous pouvons avoir confiance dans le résultat final. Pour ce faire, nous avons interrogé des spécialistes dans divers domaines, des architectes avion et nous avons étudié 70 documents

9. http://www.toica-fp7.eu/

différents (des supports de présentations, des géométries numériques, des documents sur les simulations, de la documentation informelle et des feuilles de calcul).

Nous donnons une vue simplifiée du diagramme de justification que nous avons réalisé figure 8. Ici, la conclusion finale est que nous disposons des meilleurs choix d'architecture. Cette conclusion s'appuie, d'une part, sur le fait que nous avons l'ensemble des architectures possibles, partie gauche du diagramme, et, d'autre part, sur un ensemble de résultats d'analyses basées sur des critères tels que les performances thermiques ou la masse de l'avion. La stratégie permettant de passer à la conclusion est une revue d'architecture réalisée par un comité d'experts.

Si nous nous focalisons sur la partie gauche du diagramme, représentant les justifications qui permettent de conclure que nous disposons bien de l'ensemble validé des architectures possibles, nous avons, en bas du diagramme, les éléments de preuve suivant : les modèles logiques et fonctionnels, validés, qui décrivent les contraintes, les exigences, que doit satisfaire l'architecture ; une architecture de base nommée *Design Structure Matrix* (DSM) et l'ensemble des critères qui permettent d'évaluer une architecture (cet ensemble étant constitué de feuilles de calcul donnant les critères de préférences). Dans une optique de visibilité, nous avons créé une représentation graphique spéciale pour l'utilisation de stratégie purement logiciel (basée sur un code couleur différent de celui employé pour les autres stratégies). Dans cette partie du diagramme, trois stratégies purement logiciel sont employées : *Aircadia*, *DS 3DExperience* et *CPM*.

Pour des problèmes de place, nous n'avons pas fait figurer les domaines d'usage ni les justifications sur le diagramme. À titre d'exemple, la justification pour l'emploi d'Aircadia renvoie à un document validant l'emploi de ce logiciel dans le cadre de TOICA et son domaine d'emploi renvoie à une liste des contraintes minimales que doit remplir toute architecture étudiée dans le cadre de ce projet. Dans cette étude, seule une partie de l'architecture est étudiée, ainsi les architectures générées ne couvrent que les domaines de l'air conditionné et la pressurisation, la génération électrique, le pneumatique et l'installation électrique. Cette restriction apparaît clairement sur le diagramme au moyen d'une limitation attachée à la conclusion : « *ATA 21, 24, 36, 92* ». Les chapitres ATA sont un système utilisé par tous les acteurs de l'aéronautique (constructeur, pilotes, compagnies, maintenance, etc.) qui permet de classer la documentation suivant des rubriques (chapitres), chaque rubrique correspondant à un système de l'avion.

La partie droite du diagramme représente les justifications pour les résultats d'analyses pour une architecture donnée. En effet pour chaque architecture possible, un ensemble d'analyses est réalisé. Sur le diagramme, nous avons encadré en pointillés le sous-diagramme de justification correspondant aux analyses pour une architecture, mais, dans les faits, il y a autant d'analyses, et donc de sous-diagrammes, que d'architectures possibles. De plus, nous avons seulement fait figurer sur ce diagramme les aspects relatifs à l'étude thermique (les autres études n'étant pas couvertes par TOICA). Le fait d'avoir des données thermiques dans lesquelles nous avons confiance s'appuie sur le fait que nous disposons d'une simulation thermique globale crédible :

le *Global Thermal Aircraft* (GTA). Naïvement, nous pouvons voir le GTA comme une agrégation de plusieurs simulations. Les résultats du GTA sont des éléments clés pour des prises de décision comme des choix de matériaux, l'identification de certains risques thermiques, la qualification d'équipement ou des choix d'architecture. Il existe un besoin fort de confiance dans les résultats du GTA et nous avons conçu, avec des experts thermiques, un diagramme de justification pour justifier la confiance dans ces résultats. Là encore, nous avons défini des patrons d'argumentation spécifiques dédiés au domaine de la simulation et réalisé un diagramme de justification validant l'usage du GTA pour une mission donnée. Cependant, dans l'exemple donné ici, nous nous situons sur un diagramme qui porte sur le choix d'architecture et non sur les simulations thermiques : le seul élément d'information intéressant est de savoir que la stratégie GTA est validée. Les raisons de cette validation sont présentes dans la justification de la stratégie (non présentes sur le diagramme pour des raisons de place) et cette justification renvoie au diagramme de justification du GTA.

Notons que le diagramme de justification ne s'inscrit pas dans une optique temporelle. Il donne l'enchaînement logique des justifications, mais ne donne pas à voir le processus. Ce n'est pas un diagramme de comportement comme le diagramme d'activités. Le but de l'argumentation est de montrer la rationalité et de construire la confiance dans le résultat final. Ainsi, dans ce diagramme, la temporalité n'est pas décrite et les entrées et les sorties sont en termes de rationalité et non en termes de processus temporel.

Dans cet exemple précis, nous avons pu mesurer l'utilité des diagrammes de justification face à ce que nous appelons le tsunami documentaire. En donnant une image globale, une représentation graphique de la justification, le diagramme de justification permet d'aider le décisionnaire à aller à l'essentiel. Par exemple, le diagramme de justification de la figure 8 renvoie à 16 des 70 documents initiaux. Il n'est cependant pas possible d'y représenter explicitement les liens avec les documents pour des raisons de lisibilité. Ainsi, l'élément de preuve « *Mission M_j validée* » renvoie à un document de la validation de la mission M_j, ou l'élément « *Description fonctionnelle* » renvoie à un modèle CATIA décrivant les flux entre les fonctions et des feuilles de calcul contenant toutes les informations sur les fonctions.

Dans TOICA, nous avons utilisé ce diagramme de justification lors d'une revue des architectures possibles. En montrant les éléments clés (principalement des éléments V&V), ce diagramme a aidé les décideurs à comprendre pourquoi le résultat est fiable et quels sont les points faibles. De plus, *Dassault Systèmes* a mis en place un prototype de diagramme de justification dans son logiciel 3DExperience. Le logiciel offre de nouvelles possibilités par rapport à la version papier. Par un simple clic, il est possible d'accéder à toutes les données et documents liés au diagramme. Cette fonctionnalité augmente la confiance grâce à un accès direct aux informations liées à l'argumentation.

5.2. Des diagrammes de justification pour définir les documents de V&V à produire

Afin d'éviter que les coûts de production ne soient pris en compte de façon trop tardive dans le processus de conception d'un avion, il devient crucial d'intégrer une évaluation de ces coûts au plus tôt. Ces coûts deviennent alors un des critères de sélection entre différentes architectures possibles comme la masse, les aspects thermiques, etc. Pour ce faire, il est nécessaire d'établir une interaction forte entre l'ingénierie et l'outil de production dans le but de pouvoir réaliser rapidement, et de façon fiable, une estimation de la charge de travail nécessaire à la fabrication d'un avion qui n'est encore qu'en devenir.

Dans le cadre du projet TOICA, nous avons utilisé les diagrammes de justification pour définir les documents et les opérations de validation nécessaires pour établir la confiance dans un processus. Contrairement au cas d'étude précédent, nous n'avons pas cherché à organiser une documentation existante a posteriori, mais à nous situer *a priori* et à utiliser les diagrammes de justification pour définir les exigences de justification. Plus précisément, dans le cadre de la définition d'un processus d'évaluation de la charge de travail sur une chaîne de production, les diagrammes de justification ont été utilisés pour définir quels étaient les éléments qui permettaient d'avoir confiance dans cette évaluation.

Le processus actuel pour l'évaluation de la charge de travail repose sur une conception très détaillée de l'avion et demande un certain nombre de calculs complexes et coûteux en temps. Pour avoir une estimation plus rapide, mais moins fiable, un nouveau processus a été défini. C'est un processus itératif qui commence avec des conceptions très préliminaires et finit avec des conceptions détaillées. Avec ce processus, il devrait être possible d'évaluer la charge de travail très rapidement, dans la phase préliminaire, avec peu d'informations et beaucoup d'incertitudes.

Afin d'expliciter les exigences de justification, nous avons défini, avec les experts, des patrons d'argumentation spécifiques qui assurent un certain degré de confiance dans le résultat de l'évaluation. À l'aide de ces patrons, nous avons pu clairement expliciter les différentes opérations de V&V et définir la liste des éléments de preuve nécessaires.

Concrètement, dans la première étape de cette étude, nous nous sommes concentrés sur la compréhension de comment font, à l'heure actuelle, les départements de production pour évaluer la charge de travail. Pour cela, nous avons interviewé des architectes avion, des experts en mesure de charge de travail, des experts en équilibrage, ainsi qu'un ensemble de personnes impliquées dans le processus d'évaluation de la charge de travail. Nous avons également passé deux jours sur la ligne d'assemblage pour acquérir une connaissance plus directe.

Nous avons ensuite, dans une deuxième étape, défini l'ensemble des patrons d'argumentation correspondant à l'évaluation de la charge de travail. Ces patrons nous ont permis d'identifier les étapes nécessaires de validation et les éléments de preuve

qui devaient absolument être produits dans le cadre du processus d'évaluation. Nous retrouvons ici la dimension de maturité des patrons puisque ces patrons ont été déclinés en plusieurs versions, chaque version étant associée à une étape du cycle itératif d'évaluation.

Grâce à ces patrons, nous avons une vision plus claire des justifications et des opérations nécessaires pour établir la confiance. De plus, de par l'aspect de raffinement des patrons, nous nous somme appuyés le plus possible sur la réutilisation des éléments de preuve produits aux étapes précédentes du processus.

5.3. Des diagrammes de justification pour la certification

Nous avons aussi appliqué nos diagrammes de justification dans le cadre du projet MIMOSA (Bieber *et al.*, 2016). Dans ce projet, un processus de certification pour le logiciel embarqué avionique a été défini en étroite collaboration avec les autorités de certification. La certification consiste à faire agréer par une autorité la conformité d'un système. Dans MIMOSA, le système est constitué d'une partie du logiciel avionique qui doit, comme tout le reste de l'avion, être certifié pour avoir l'autorisation de voler.

Durant ce projet, nous avons défini, avec l'aide d'experts, des patrons d'argumentation spécifiques aux problématiques temps réel du logiciel embarqué. Le but de ces patrons est d'aider l'autorité de certification à trouver les manques ou la mauvaise utilisation d'éléments de preuve. De plus, nous avons montré comment, à l'aide des diagrammes de justification, il était possible de structurer la documentation fournie à l'autorité et comment ces diagrammes permettent d'avoir une vue claire de l'ensemble de la documentation.

6. Conclusion

Dans cet article, nous avons montré comment la question de la validité d'une propriété de haut niveau pour un produit doit être remplacée par la question de son acceptabilité. Sur la base des travaux existants et, plus précisément, sur les travaux de Stephen Toulmin, nous avons essayé de définir les bases de ce que doit être une « *bonne argumentation* », au sens de bien formée et vérifiable. Aujourd'hui, l'idée de structurer les éléments V&V sous la forme d'un diagramme commence à s'imposer principalement au travers des concepts tels que l'*assurance case*, mais uniquement dans le cadre de la sûreté de fonctionnement. Pour nous, il nous semble essentiel que les diagrammes de justification ne se limitent pas à des boîtes et des flèches, mais qu'ils soient construits sur l'héritage des travaux menés précédemment en linguistique et en droit. Dans cette optique, les travaux futurs devraient tenir compte des progrès de la théorie de l'argumentation. Par exemple, citons les travaux de Douglas Walton (Walton, 1996) qui définit des modèles de questions critiques pour interroger la validité des témoignages des experts. Sur ce modèle, nous pourrions définir des ensembles de questions attachées aux modèles d'argumentation spécifiques, ces questions pourraient soutenir l'examen du diagramme de justification ou pourraient contribuer à aider un ingénieur à comprendre comment instancier un modèle d'argumentation spécifique.

Pour finir, une tendance lourde dans les projets actuels est de privilégier une approche modulaire, orientée composants. Si cela présente des avantages indéniables en matière d'évolution et de réutilisation, cela induit malheureusement une grande perte de structure dans l'organisation de la V&V. De part la nature même de l'approche composant, les opérations de V&V se retrouvent disséminées de façon parcellaire dans l'ensemble du cycle de développement, sans forcément de structure par niveau d'abstraction ou par niveau de maturité. Finalement, dans bien des projets, la documentation se retrouve assez mal organisée, bien souvent disséminée, parfois redondante avec la même information apparaissant dans de nombreux documents ou inversement devenir introuvable. Les diagrammes de justification, parce qu'ils formalisent la structure et sont un point d'entrée unique sur l'ensemble des documents, nous semblent être une réponse possible à ce problème.

Remerciements : les travaux de recherche menant à ces résultats ont été financés par le 7e programme cadre de l'Union européenne (FP7 / 2007-2013) en vertu de la convention de subvention n°604981.

Bibliographie

Alexander C., Ishikawa S., Silverstein M. (1977). *A pattern language: Towns, buildings, construction*. New York, Oxford University Press. Hardcover.

Balci O. (1998). Verification, validation, and accreditation. In *Proceedings of the 30th conference on winter simulation*, p. 41–4.

Bieber P., Boniol F., Durrieu G., Poitou O., Polacsek T., Wiels V. *et al*. (2016). MIMOSA: Towards a model driven certification process. In *Proc. 8th int. congress on embedded real time software and systems (erts'16).*

Cassano V., Maibaum T. S. E. (2014). The definition and assessment of a safety argument. In *25th IEEE international symposium on software reliability engineering workshops, ISSRE workshops*, p. 180–185. IEEE Computer Society.

Defence Standard 00-42 Reliability and Maintainability Assurance Guide Part 3: R&M Case. Standard n° Def Stan 00-42 Part 3 Issue 3. (2008). UK Defence Standardization.

Defence Standard 00-56 Safety Management Requirements for Defence Systems. Standard n° Def Stan 00-56 Part 1 Issue 4. (2007). UK Ministry of Defence.

Gamma E., Helm R., Johnson R., Vlissides J. (1995). *Design patterns: Elements of reusable object-oriented software*. Boston, MA, USA, Addison-Wesley Longman Publishing Co., Inc.

Grangel R., Chalmeta R., Campos C. (2007). Knowledge-based intelligent information and engineering systems: 11th international conference, kes 2007, xvii italian workshop on neural networks, vietri sul mare, italy, september 12-14, 2007. proceedings, part ii. In B. Apolloni, R. J. Howlett, L. Jain (Eds.),, p. 1230–1237. Berlin, Heidelberg, Springer Berlin Heidelberg.

Guiochet J., Do Hoang Q. A., Kaâniche M., Powell D. (2013). Model-Based Safety Analysis of Human-Robot Interactions: the MIRAS Walking Assistance Robot. In *International Conference on Rehabilitation Robotics (ICORR)*, p. 1-7. Seattle, United States.

Hamblin C. (1970). *Fallacies*. Methuen.

Holloway C. M. (2015, February). Explicate '78: Uncovering the implicit assurance case in do-178c. In *23rd safety-critical systems club (scsc) annual symposium.*

Jones A. J. I. (2002, July). On the concept of trust. *Decis. Support Syst.*, vol. 33, n° 3, p. 225–232.

Kelly T., Weaver R. (2004). The goal structuring notation /- a safety argument notation. In *Proc. of dependable systems and networks 2004 workshop on assurance cases.*

Kirschner P. A., Buckingham-Shum S., Carr C. S. (2003). *Visualizing argumentation : Software tools for collaborative and educational sense-making*. Springer.

Kunz W., Rittel H. (1970). *Issues as elements of information systems*. Working Paper n° 131. Berkeley, California, Institute of Urban and Regional Development, University of California.

MacLean A., Young R. M., Bellotti V. M. E., Moran T. P. (1991, September). Questions, options, and criteria: Elements of design space analysis. *Hum.-Comput. Interact.*, vol. 6, n° 3, p. 201–250.

Perelman C., Olbrechts-Tyteca L. (2008). *Traité de l'argumentation: La nouvelle rhétorique*. Éditions de l' Université de Bruxelles.

Polacsek T. (2016). Validation, accreditation or certification: A new kind of diagram to provide confidence. In *Tenth IEEE international conference on research challenges in information science, RCIS 2016, grenoble, france, june 1-3, 2016*, p. 1–8. IEEE.

Rodney A. Reynolds J. L. R. (2002). Evidence. In M. P. James Price Dillard (Ed.), *The persuasion handbook: Developments in theory and practice*, p. 427-446. SAGE Publications, Inc.

Sharma S., Levandowski C., Molina-Cristobal A., Kipouros T., Isaksson O., Robinson T. (2016). Super Integration: seeking novel valued solutions. In *European Congress on Computational Methods in Applied Sciences and Engineering (ECCOMAS 2016).*

Shum S. B., Hammond N. (1994). Argumentation-based design rationale: what use at what cost? *International Journal of Human-Computer Studies*, vol. 40, n° 4, p. 603–652.

Sujan M., Spurgeon P., Cooke M., Weale A., Debenham P., Cross S. (2015). The development of safety cases for healthcare services: Practical experiences, opportunities and challenges. *Rel. Eng. & Sys. Safety*, vol. 140, p. 200–207.

Systems and software engineering – Systems and software assurance – Part 2: Assurance case. Standard. (2011). International Organization for Standardization.

Toulmin S. E. (2003). *The uses of argument*. Cambridge, UK, Cambridge University Press. (Updated Edition, first published in 1958)

van Lamsweerde A. (2009). *Requirements engineering - from system goals to uml models to software specifications.* Wiley.

Walton D. (1996). Practical reasoning and the structure of fear appeal arguments. *Philosophy and Rhetoric*, vol. 29, n° 4, p. 301–313.

Walton D. (2007). Visualization tools, argumentation schemes and expert opinion evidence in law. *Law, Probability and Risk*, vol. 6, n° 1-4, p. 119-140.