Vérification automatique d'exigences pour les politiques d'échange d'information

Exigences de diffusion et de non-diffusion de l'information

Rémi Delmas, Thomas Polacsek

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

RÉSUMÉ. *De la surveillance de la Terre aux relations inter-entreprises, de plus de plus d'organisations forment des systèmes décentralisés avec des échanges d'information. Dès lors, il devient crucial de régir la diffusion de l'information entre les différents partenaires à l'aide de règles précises, c'est-à-dire à l'aide de politiques d'échange d'informations. Ce papier propose une approche formelle pour la spécification de politiques d'échange accompagné d'un outil per- mettant à l'utilisateur de définir une politique et de vérifier automatiquement sa conformité à un ensemble d'exigences. Dans cet article, nous considérons d'abord un ensemble d'exigences logiques génériques, puis nous formalisons deux types d'exigences antagonistes : d'une part, la nécessité de partager de l'informationn, et d'autre part, l'obligation de ne pas diffuser certaines informations. Nous expliquons ensuite comment les concilier dans une même politique à l'aide d'une opération de filtrage d'information dont la spécification apparaît naturellement.*

ABSTRACT. *From Earth observation to inter-companies relations, more and more organizations form decentralized systems in which information gets exchanged. In such settings it becomes crucial to explicit the rules governing information diffusion between parties, in what is called information exchange policies. This paper proposes a formal approach to exchange policies specification and analysis, together with a tool allowing the user to define policies and verify a number of formal requirements. In this paper, we first focus on a set of generic logical requirements, then we formalize two types antagonist requirements, the first being about enforcing necessary information diffusion, and the second about restricting the diffusion of specific kinds of information. Finally we explain how to reconcile these conflicting requirements in a single policy, thanks to an information filtering operator, the specification of which emerges naturally.*

MOTS-CLÉS : *analyses de politique d'échange, exigences, méthodes formelles, vérification, solveurs SMT.*

KEYWORDS: *exchange policy analysis, requirements, formal methods, verification, SMT solvers.*

DOI:10.3166/ISI.21.2.39-63 @ 2016 Lavoisier

1. Introduction

Les travaux présentés dans ce papier sont motivés par le problème de l'échange d'information dans le cadre d'une gouvernance partagée pour la prévention et la gestion des situations de crise. Par crise, nous entendons des problèmes de portée globale en matière de santé, tels qu'une épidémie, une catastrophe naturelle, ou bien encore des collisions entre objets spatiaux, etc. Comme nous allons le voir, ce type de problèmes doit aujourd'hui être géré à une échelle globale par les acteurs concernés, il est en effet illusoire de penser qu'un seul acteur soit en mesure de les gérer convenablement. Ceci implique la mise en place d'échanges d'information, et il existe aujourd'hui une volonté de se doter de systèmes d'alertes coopératifs ayant pour vocation la prévention et la gestion des risques. Une alerte (nous utiliserons indifféremment les termes alertes et alarmes) est une information particulière qui concerne un danger imminent et qui peut, éventuellement, contenir des informations de contexte décrivant la nature, le lieu ou l'aspect temporel du danger. Comme nous le verrons par la suite, le fait qu'une alerte ne soit pas envoyée à la bonne personne, ou au bon groupe de personnes, ou encore qu'elle ne contienne pas les informations nécessaires, peut avoir des conséquences graves pour les parties coopérantes du système. Cependant, les entreprises, les agences, les organisations et les états impliqués dans ces échanges ne communiquent de façon transparente et sans contraintes, généralement par souci de confidentialité et par crainte de perdre la maîtrise des l'information qu'ils possèdent. Pour répondre à ce problème de confiance que peuvent connaître les acteurs participant aux échanges d'information, nous soutenons l'idée qu'il faut, en amont de la réalisation de tout système coopératif de gestion de crise, se doter d'un cadre dans lequel les exigences de diffusion d'information et les exigences de confidentialité puissent être exprimées sans ambiguïté. Un tel cadre peut ensuite servir à établir, par analyse formelle et automatique des exigences, des garanties sur la bonne circulation de l'information permettant aux acteurs du système de réaliser leurs missions, ainsi que des garanties importantes relatives à la confidentialité. Grâce à la maîtrise de la correction des exigences de (non-)diffusion d'information, obtenue au moyen d'une approche formelle de l'ingénierie des exigences, nous pensons pouvoir augmenter le niveau de confiance en ces systèmes, aujourd'hui trop souvent bridés par le manque de coopération entre acteurs, et ainsi contribuer à réduire la réticence de certains acteurs à y diffuser des informations utiles.

Citons comme premier exemple de systèmes d'alerte les *systèmes de surveillance de l'environnement spatial* (SSA [1]) (Dal Bello, 2011). Dans ces systèmes, des capacités d'observation de l'espace, appartenant à différentes nations, organismes étatiques ou privés et autres opérateurs de satellites, sont mutualisées afin de collecter un ensemble de données complexes sur les trajectoires des objets orbitant, de les analyser et de générer des alertes. En fait, la mission d'un système SSA est d'avertir les acteurs concernés lorsqu'une potentielle collision entre deux objets en orbite, ou entre objets en orbite et des débris spatiaux, est détectée. Ainsi, en cas de risque, il faut que les

1. SSA pour *Space Situation Awareness*.

bons agents (nations, opérateurs de satellites, etc.) reçoivent une alerte pertinente de manière à leur permettre d'éviter la collision. Notons que, étant donné que l'investissement requis pour placer un satellite en orbite se compte en dizaines voire centaines de millions d'euros, les différents acteurs d'un système SSA sont fortement motivés pour éviter les collisions spatiales.

Nous retrouvons d'autres systèmes d'alarme dans le cadre du *Système mondial des systèmes d'observation de la Terre* (GEOSS [2]). Une des nombreuses applications possibles de GEOSS est la surveillance et la gestion des risques sismiques. Ici, nous avons une collaboration entre les fournisseurs de données satellitaires, les fournisseurs de données sismiques et la communauté scientifique formant un réseau d'échange d'information à l'échelle mondiale. L'objectif principal d'un tel système est d'assurer que l'information sur les catastrophes sismiques parvienne toujours aux autorités compétentes, le rôle de ces autorités étant d'identifier clairement les risques à partir des données recueillies et d'établir les mesures de protection de la population.

Toujours dans une idée de prévention de risques, nous pouvons citer les systèmes de veille sanitaire. La surveillance sanitaire est maintenant un enjeu majeur à l'échelle mondiale et cela pour deux raisons. Premièrement, dans les zones du monde frappées par la pauvreté, les infections se propagent rapidement et il peut être extrêmement difficile de les contenir en appliquant des mesures et moyens cantonnés à un seul pays. Deuxièmement, à une époque où le transport des personnes et des marchandises à travers le monde atteint une ampleur sans précédent, les questions de santé exigent que les gouvernements et les organismes de santé utilisent une approche globale, fondée sur le partage de l'information, pour être en mesure de délivrer rapidement les recommandations de santé publique en réponse au risque sanitaire (Heymann, Rodier, 2001). Dans ces applications, des données de terrain, telles que des rapports de cas de maladies, sont collectées et envoyées à des experts en épidémiologie qui surveillent et tentent de prédire les risques d'épidémies ou d'éventuelles pandémies. Lorsque des épidémies sont susceptibles de se produire, les experts alertent alors les autorités compétentes, telles que les organisations intergouvernementales ou les organismes internationaux, qui évaluent la gravité du risque identifié et prennent les mesures sanitaires appropriées.

Loin de la problématique de la protection des personnes, nous retrouvons ce qui peut se concevoir comme des systèmes d'alerte dans le cadre de *l'entreprise étendue* (Browne, Zhang, 1999) (Dyer, Singh, 1998). L'entreprise étendue dénote une association d'entreprises partageant un objectif commun, généralement la fabrication ou la commercialisation d'un produit complexe, et qui, grâce à des alliances telles que des consortiums, partagent des ressources et de la connaissance. Prenons pour exemple un consortium de grandes entreprises et leurs sous-traitants qui doivent échanger des informations sensibles telles que des spécifications techniques avancées, des modèles d'ingénierie ou encore des données financières. Ces échanges se réalisent par l'interconnexion de leurs systèmes d'information ou au sein de plates-formes fédérées, voire,

2. GEOSS pour *Global Earth Observation System of Systems*.

plus trivialement, par des échanges de fichiers entre des individus. Chaque entreprise, étant relativement indépendante, peut être impliquée dans plusieurs sous-systèmes sur la base d'accords, de partenariats, de sous-traitances, ou de par leur statut de filiale de différents groupes industriels, etc. Dans un tel contexte, les informations relatives au changement d'une spécification, à la modification d'un modèle de conception ou encore aux résultats d'une validation doivent absolument être communiquées, telles des alertes, aux partenaires concernés, afin de garantir le succès de l'entreprise étendue.

Le papier est structuré de la manière suivante: en section 2, nous présentons, au travers d'exemples, les caractéristiques saillantes des systèmes d'alerte auxquels nous nous intéressons. La section 3 présente un rappel du langage PEPS [3], précédemment défini dans (Delmas, Polacsek, 2013) (Delmas, Polacsek, 2014), qui permet de spécifier formellement une politique d'échange d'information, ainsi qu'un exemple de politique qui permettra d'illustrer l'ensemble des concepts étudiés dans les sections suivantes. En section 4, nous définissons en ensemble de propriétés génériques pour les politiques d'échanges et nous voyons comment il est possible de vérifier ces propriétés à l'aide d'outils automatiques. La section 5 est dédiée à la définition des exigences liées à la diffusion et à la non-diffusion d'information. Malgré l'antagonisme de ces deux types d'exigences, nous verrons dans la section 6 comment un opérateur de filtrage d'information permet de les concilier dans une même politique sans incohérence. Enfin, la section 7 conclut le papier et donne quelques perspectives à ces travaux.

2. Des systèmes avec une exigence de diffusion d'information

Que cela soit pour la surveillance spatiale, épidémiologique ou des catastrophes naturelles, l'ensemble des systèmes d'échange d'information considérés ont une caractéristique commune évidente: certains agents du système doivent absolument connaître toutes les informations disponibles relatives à un sujet donné afin d'être en mesure d'accomplir correctement leur mission. L'acquisition d'une connaissance seulement partielle de la situation peut grandement nuire à la performance du système dans son ensemble, voire avoir des conséquences critiques. En outre, cette nécessité d'être tenu informé n'est pas forcément liée à un agent (ou à un groupe d'agents) de façon unique et définitive, mais peut dépendre du domaine et du contexte courant. En effet, si nous prenons l'exemple du SSA, l'agent qui doit absolument recevoir une alarme de collision est l'opérateur à même de changer la trajectoire du satellite, pouvant ainsi éviter la collision. Puisque de nombreuses entreprises et organisations exploitent des satellites, l'agent qui doit être informé peut être différent pour chaque alarme. Si nous prenons l'exemple des systèmes GEOSS, dans le cadre de la gestion des catastrophes naturelles, nous avons des informations devant absolument parvenir aux autorités compétentes, qui peuvent dépendre de l'emplacement géographique de

3. PEPS est l'acronyme récursivement défini par : PEPS *for exchange policy specification*.

la catastrophe potentielle, potentiellement différente de celui d'acquisition des informations.

Par conséquent, dans l'ensemble de ces exemples, nous sommes face à des systèmes où des agents peuvent échanger de l'information et où un agent, ou un groupe d'agents, dépendant du contexte, doit absolument être prévenus de la situation les concernant. Nous avons donc des systèmes dans lesquels l'exigence principale est que certains agents *doivent absolument être avertis* selon la situation. En fait la véritable exigence est un *besoin de connaître* des agents, qui doivent connaître certaines informations pour pouvoir accomplir leur mission. Cependant, comme nous nous intéressons aux échanges d'information, nous pouvons reformuler cette exigence en une exigence de *diffusion* qui signifie que puisqu'un agent a besoin d'une information, quand celle-ci est connue par un autre agent du système, elle doit lui être absolument transmise.

En plus de l'exigence de diffusion, nos différents exemples ont également en commun l'hétérogénéité de leurs composants et l'utilisation d'architectures décentralisées. Ils sont hétérogènes dans le sens où les agents du système peuvent êtres de différentes natures, comme une nation, une agence ou plus simplement un individu, et où chacun de ces agents peut avoir une mission différente. De plus, de nos jours, partage d'information ne rime plus forcément avec centralisation d'information. Utiliser un dépôt partagé, même avec contrôle d'accès, signifie placer une confiance aveugle dans l'organisme responsable de la gestion et de l'administration de ce dépôt. De par les réticences des différents partenaires à mettre à disposition leurs informations, les architectures d'échanges d'information de gré à gré semblent aujourd'hui s'imposer face aux dépôts centralisés. Par conséquent, nous pouvons faire l'hypothèse qu'aucun agent du système n'a une connaissance complète de toutes les informations existant dans le système (si cela était le cas, l'échange d'information deviendrait superficiel, puisque cet agent omniscient pourrait répondre à toutes les requêtes et générer toutes les alertes à destination de n'importe quel autre agent).

Nous proposons de regrouper l'ensemble des systèmes décrits dans les exemples précédents sous le terme de *Système avec Criticité dans l'Echange d'Information* (CIDS [4])(Delmas, Polacsek, 2015a).

DÉFINITION 1. — CIDS *Critical Information Diffusion System*
CIDS désigne un système décentralisé *avec* échanges d'information *entre agents, possiblement hétérogènes, et où certains échanges sont de nature* critique *pour certains agents (critique d'un point de vue sûreté, sécurité, stratégique, économique,* etc.*).*

Nous utilisons le terme *critique* dans la même acceptation que celle utilisée dans les domaines ferroviaire, aéronautique, nucléaire, etc. En ce sens, s'il est impossible de garantir la diffusion d'information voulue dans un CIDS, et par conséquent de garantir que ses agents recevront effectivement les informations dont ils ont besoin, des effets dangereux, voire catastrophiques, peuvent se produire, comme la collision

4. CIDS pour *Critical Information Diffusion System*.

de satellites entraînant leur destruction, l'absence de réaction face à une catastrophe naturelle, ou encore la propagation rapide d'une maladie pouvant mener à une pandémie. Nous pouvons bien évidemment étendre la notion de criticité pour englober les risques économiques et financiers qui peuvent avoir des conséquences graves pour une entreprise. Dans ce cas, la diffusion de l'information au sein de l'entreprise, et a fortiori de l'entreprise étendue, peut être considérée comme critique, dans le sens où elle conditionne l'efficacité de l'entreprise et sa réussite économique. Par conséquent, nous considérons qu'un système d'information diffusant des informations possède une dimension critique à partir du moment où un défaut dans les échanges peut avoir des conséquences indésirables voire dangereuses.

Un exemple simple de CIDS sont les systèmes de type SSA. Si au début de la conquête spatiale, l'espace était seulement occupé par une poignée de nations pionnières, il est devenu au fil du temps un espace partagé, peuplé par une multitude de satellites appartenant à un nombre croissant de nations et d'entreprises ayant des objectifs et des intérêts potentiellement conflictuels. En conséquence, toutes ces organisations peuvent être réticentes à partager des informations, sans aucune restriction, au sein d'un système SSA globalisé qui pourrait révéler la nature de tous les objets en orbite autour de la Terre et leurs trajectoires (l'ensemble de ces informations étant considérées comme des sensibles par leurs propriétaires). De plus, la plupart des moyens d'observation de l'espace appartiennent aujourd'hui à des forces militaires qui considèrent ces moyens comme stratégiques et ne souhaitent pas forcément partager des informations qui pourraient directement, ou indirectement, révéler leurs véritables capacités et performances. Aujourd'hui, la plupart des experts SSA s'accordent sur le point que beaucoup de données d'observation de l'espace sont déjà disponibles mais sous-exploitées, le nœud du problème étant un manque d'accords de partage d'information entre les différentes parties prenantes.

L'observation de la Terre est aussi un problème global qui implique de nombreuses organisations dans différents pays. Dans le cadre de la gestion des catastrophes naturelles, en cas de détection d'un risque, s'il faut absolument informer les autorités compétentes, il ne faut pas nécessairement communiquer cette information de façon brute au grand public, principalement pour éviter les mouvements de panique qui pourraient être catastrophiques pour la population. Ainsi, ce sont les autorités compétentes, une fois averties, qui vérifient si le risque est réel et, le cas échéant, organisent la communication officielle et les évacuations qui s'imposent.

Nous retrouvons le même type de problèmes dans le cadre des systèmes de veille sanitaire. Avec la prolifération des réseaux sociaux, la diffusion d'une mauvaise information au public via différents médias ou l'absence de recommandations officielles laissent la porte ouverte aux rumeurs et à la désinformation, ce qui peut avoir des conséquences désastreuses, comme ce fut le cas avec l'épidémie d'Ebola en Afrique de l'Ouest (Taverne, 2015) (Varraine-Leca, 2015). Ces contraintes de contrôle d'information peuvent être vues comme une forme d'exigence de confidentialité que le système doit satisfaire. En marge des systèmes de surveillance sanitaire, il existe des systèmes de surveillance qui impliquent des agences de renseignement et parfois même

des moyens militaires. Le but de tels systèmes est de détecter au plus tôt les actes de terrorisme biologique (Mandl *et al*., 2004) (Meynard *et al*., 2008). Bien évidemment, les informations circulant dans ces systèmes sont excessivement sensibles et sont soumises à des exigences de confidentialité.

Notons que, comme pour les contraintes de diffusion, nous retrouvons des contrain-tes de confidentialité dans le cadre de l'entreprise étendue. En effet, les coopérations industrielles sont gérées à l'aide, entre autres, d'accords de non-divulgation passés entre sociétés concurrentes, pouvant être forcés de partager des informations dans le contexte de projets collaboratifs ou encore d'interactions en tant que sous-traitants sous l'égide d'un même client (dans le domaine des smartphones par exemple, une société peut commercialiser son propre produit, tout en fabriquant certains composants d'un produit concurrent). Dans le contexte de l'entreprise étendue, nous avons encore une fois des agents qui doivent recevoir de l'information tout en étant soumis à différents ensembles de règles de partage et de confidentialité, l'ensemble de ces règles pouvant être contradictoire ou incomplet. Ceci fait de la gestion de l'information au sein de l'entreprise étendue une question très complexe.

3. Spécification de politiques d'échange

Etant donné la complexité des échanges d'information dans les CIDS, il faut, en amont de la réalisation de tout système, se doter d'un cadre non-ambigu dans lequel exprimer les exigences relatives aux échanges et à la (non-)diffusion d'information. Si de plus un tel cadre permettait d'analyser ces exigences et de démontrer formellement qu'elles satisfont bien les besoins d'alertes tout en garantissant la maîtrise de la diffusion d'information, il permettrait, in fine, d'établir une base solide de confiance entre les différents partenaires devant coopérer dans le système. Dans les sections suivantes, nous présentons un cadre formel, qui se veut être un premier pas dans cette direction.

3.1. Un langage pour les politiques d'échange

Nous appelons une *politique d'échange*, la spécification des conditions sous lesquelles un agent a l'obligation, l'autorisation ou l'interdiction de communiquer des informations à d'autres agents. Nous pouvons dresser un parallèle entre les politiques d'échange, qui spécifient *quand un agent a l'interdiction, la permission ou l'obligation de communiquer* et les *politiques de sécurité* et plus précisément, les *politiques de contrôle d'accès*.

L'Orange Book du *DoD* [5] (Department Of Defense, 1985) donne la définition suivante d'une politique de sécurité : *«Ensemble de règles qui sont utilisés par le système pour déterminer si un sujet donné peut être autorisé à accéder à un objet spécifique»* [6].

5. DoD pour *United States Department of Defense*, le département de la défense des États-Unis.

6. Traduction de : *set of rules that are used by the system to determine whether a given subject can be permitted to gain access to a specific object*.

Cette définition est très générale. Si nous nous focalisons sur les systèmes d'information, nous pouvons nous concentrer sur le contrôle d'accès c'est-à-dire la réglementation qui régit l'accès des agents aux sources d'information telles que des bases de données, divers fichiers, etc. Le contrôle d'accès est axé sur la spécification des autorisations et des interdictions, c'est à dire sur ce qu'un agent *peut faire* ou *ne peut pas faire*, or un point important des CIDS est *l'obligation de faire*: l'obligation d'avertir l'acteur concerné.

Certains travaux associent un aspect normatif aux politiques de sécurité avec la notion d'obligation (Bieber, Cuppens, 1993) (Kalam, Baida *et al*., 2003) (Barhamgi *et al*., 2013). Mais, même si dans ces travaux il est possible d'exprimer les obligations, les autorisations et les interdictions d'effectuer une action, ils ne considèrent que les actions d'un agent sur un objet. Ces politiques ne régulent donc que des actions correspondant aux verbes divalents comme, par exemple, «l'agent A ne peut pas lire la base de données D». Dans le contexte des CIDS, nous ne nous intéressons pas à la réglementation des actions en général, mais à des actions bien particulières qui correspondent à des verbes trivalents comme dire, donner, envoyer, échanger «quelque chose à (avec) quelqu'un». Par conséquent, les cadres de modélisation de contrôle d'accès, et leurs extensions, ne sont pas utilisables tels quels pour capturer les exigences propres aux CIDS.

La notion de politique d'échange est étroitement liée à la notion de norme. Une norme dans un système est un ensemble de règles qui régissent le comportement des agents. Elle exprime quelles actions sont obligatoires, permises ou défendues, pour qui et dans quelles conditions. Selon la définition de *Information Technology Security Evaluation Criteria*, *«Une politique de sécurité d'un système spécifie l'ensemble des lois, règles et pratiques qui régissent la façon dont les informations confidentielles et autres ressources sont gérées, protégées et distribuées dans un système spécifique»* [7] (ITSEC, 1991). Cette définition est très générale et de nombreux travaux proposent des définitions formelles de certains types de normes (Bieber, Cuppens, 1992)(Jones, Sergot, 1992)(Bieber, Cuppens, 1993)(Cholvy, Cuppens, 1997)(Cuppens-Boulahia, Cuppens, 2008). Tous ces travaux ont en commun l'utilisation d'une logique modale et, plus précisément, l'utilisation d'un opérateur déontique pour modéliser les aspects normatifs inhérents à toute politique.

Si la logique modale fournit un cadre formel, avec une sémantique, qui permet de modéliser et de raisonner clairement et sans ambiguïté, elle n'est pas sans limites. Ainsi, dans (McCarthy, 1997) McCarthy n'hésite pas à déclarer que si la logique modale permet de manipuler clairement des concepts elle est difficile à utiliser par le commun des mortels et reste un outil dont l'usage est limité aux seuls logiciens. Dans (Edmonds, 2002), Edmonds renforce cette vision en allant plus loin: pour lui les approches de modélisation basées sur les logiques formelles, étant donné leur complexité, sont simplement inutilisables par des non logiciens, et restent donc abscons

7. Traduction de : *A System Security Policy specifies the set of laws, rules and practices that regulate how sensitive information and other resources are managed, protected and distributed within a specific system.*

pour tout utilisateur «métier». Dès lors, il serait possible d'objecter que seul le langage naturel peut être compris par tous, ce qui nous ramène à toutes les questions liées aux ambiguïtés inhérentes au langage naturel, qui sont précisément une des raisons ayant mené à la définition des logiques formelles.

Loin de cette polémique, pour notre part, nous soulignons que l'une des limitations techniques de la logique modale est le manque d'outils de vérification efficaces. Notre objectif étant de fournir des analyses automatiques pour l'aide à la conception et la validation d'une politique d'échange, nous nous orientons délibérément vers les formalismes supportés par des outils efficaces de vérification formelle. Par conséquent, nous avons choisi d'utiliser la logique classique, les outils de vérification, tel que les SAT solveurs ou les SMT solveurs étant largement plus efficaces que les outils dédiés à la logique modale (Sebastiani, Vescovi, 2009). Notons qu'en choisissant de modéliser les aspects normatifs à l'aide de prédicats nous perdons en expressivité mais, comme nous le verrons dans la section suivante, ceci n'est pas un véritable problème étant donné la structure des règles d'échanges qui nous intéressent, et le fait que nous gagnions en capacité d'analyse automatique.

3.2. Spécification et analyse de politiques d'échange d'information : PEPS

Pour exprimer les politiques d'échange d'information au sein des CIDS, nous proposons l'utilisation du langage formel PEPS [8] qui est accompagné d'un outil d'analyse automatique PEPS-analyzer et permet d'analyser un ensemble de propriétés sémantiques des politiques. Le langage PEPS et l'outil sont décrits dans les détails dans (Delmas, Polacsek, 2013) (Delmas, Polacsek, 2015b).

PEPS est un cadre formel outillé pour la spécification et la vérification de politiques de diffusion d'information. Techniquement PEPS est bâti sur la logique du premier ordre multi-sortée [9] avec égalité (MSFOL) (Gallier, 1987). Il permet l'utilisation de sortes (i.e. de *types*), de constantes, de fonctions, de prédicats, de variables x de sorte $\mathcal{S}$ (déclarées $x : \mathcal{S}$), de quantificateurs universels ($\forall$) et existentiels ($\exists$), et enfin de l'égalité ($=$) et des connecteurs logiques usuels ($\neg$, $\wedge$, $\vee$, $\implies$).

Le langage PEPS est extensible, l'utilisateur peut déclarer ses propres sortes, fonctions et prédicats. Toutefois, il est pourvu de sortes, fonctions et prédicats prédéfinis couvrant les concepts de base des politiques. Ainsi, les sortes $\mathcal{A}$, $\mathcal{I}$ et $\mathcal{T}$ représentent respectivement les agents, les informations et les sujets sur lesquels les informations portent; le prédicat $K(a, i)$ signifie que l'agent a connaît l'information i et le prédicat $Topic(i, t)$ signifie que l'information i se rapporte au sujet t (appelés *D-prédicats* pour prédicats de domaine).

Contrairement à la logique déontique standard (une logique modale des obligations, interdictions et permissions), notre langage ne dispose pas d'un opérateur d'obli-

8. PEPS est l'acronyme récursif pour *Peps for Exchange Policy Specification*.
9. On peut voir une *sorte* comme un *type*.

gation générique (Castanẽda, 1975). En effet, nous nous concentrons uniquement sur la notion d'*obligation d'envoyer une information d'un agent vers un autre* et pas sur la notion d'obligation en général. Par conséquent, nous avons trois prédicats dédiés, appelés *prédicats normatifs* (*N-prédicats*, par opposition aux D-prédicats): $O_{Send}(a, b, i)$, $P_{Send}(a, b, i)$ et $F_{Send}(a, b, i)$, qui modélisent respectivement l'obligation, l'autorisation et l'interdiction pour un agent a d'envoyer à un agent b une information i.

En logique déontique standard, les modalités d'obligation et de permission sont reliées par l'axiome (D) qui exprime que si p est obligatoire alors p est également permis. Dans PEPS, nous traduisons cet axiome par une formule de logique classique, que nous appelons également (D) et qui exprime le fait que s'il est obligatoire pour un agent d'envoyer une information à un autre agent alors il lui est également permis de lui envoyer.

DÉFINITION 2. — *Axiome D*

$$(D) \quad \forall a, \forall b, \forall i, O_{Send}(a, b, i) \implies P_{Send}(a, b, i)$$

De plus, nous définissons les *règles d'échange* comme des formules qui spécifient sous quelles conditions un agent à l'obligation, l'interdiction ou la permission d'envoyer une information à un autre agent. Nous appelons une *politique d'échange* (EP) un ensemble de règles d'échange.

DÉFINITION 3. — *Règle d'échange*
Une règle d'échange est une formule PEPS fermée *de l'une des formes suivantes :*

$$\forall x_1, \ldots, \forall x_n, \ (\phi \implies O_{Send}(t_1, t_2, t_3))$$
$$\forall x_1, \ldots, \forall x_n, \ (\phi \implies P_{Send}(t_1, t_2, t_3))$$
$$\forall x_1, \ldots, \forall x_n, \ (\phi \implies F_{Send}(t_1, t_2, t_3))$$

où :

- $x_1, \ldots, x_n$ *sont toutes les variables présentes dans* ϕ, t_1, t_2 *et* t_3*;*
- ϕ *est une formule sans quantificateur et sans* N-prédicats *;*
- t_1, t_2 *sont des termes de sorte* $\mathcal{A}$*;*
- t_3 *est un terme de sorte* $\mathcal{I}$*.*

À cela nous devons ajouter une description formelle du domaine, notée Σ. La déclaration des sortes et des prédicats nécessaires pour décrire le domaine associé à une application particulière est laissée à l'utilisateur. Techniquement, PEPS est extensible avec de nouveaux types, des fonctions et des D-prédicats, mais il n'est pas possible d'introduire de nouveaux N-prédicats.

Dans la suite, nous appellerons *spécification d'une politique d'échange*, dénotée par EPS, le couple formé par la politique d'échange proprement dite EP et par les contraintes du domaine Σ, auxquelles nous ajoutons la propriété (D). Nous distinguons la politique elle même, notée EP et composée de l'ensemble de déclarations

de types, de fonctions, de prédicats, de contraintes de domaine et de règles de diffusion, de la formule logique qui représente cette politique en logique, notée elle $\mathcal{EPS}$ et définie ainsi:

DÉFINITION 4. — *Spécification d'une politique d'échange*

$$\mathcal{EPS} \equiv \Sigma \wedge (\bigwedge_{r \in EP} r) \wedge D$$

Enfin, nous utiliserons la notation $P \models Q$ pour dire que Q est une conséquence logique de P, *i.e.* que tout modèle de P est aussi un modèle de Q.

3.3. Vérification automatique de politiques d'échange : PEPS*-analyzer*

L'outil PEPS-analyzer offre une assistance à la création, la spécification et la mise au point d'une politique. En effet, en interagissant avec PEPS-analyzer, il est possible pour un concepteur de vérifier si une formalisation est conforme ou non à ses intuitions et de la modifier en conséquence en se servant de contre-exemples renvoyés par l'outil. Cette tâche de mise au point devient très difficile voire impossible pour un humain à mesure que la taille et/ou la complexité de la spécification augmente: ne serait-ce que sur des exemples simples d'une dizaine de règles seulement, la combinatoire des interactions les différentes règles fait qu'il est humainement impossible d'identifier toutes les incohérences entre règles, de garantir la complétude de la politique ou de garantir l'absence de redondance entre règles.

Concrètement, PEPS-analyzer ramène le problème de vérification d'une propriété sur une politique à un problème de satisfiabilité. Ainsi, vérifier que $P \models Q$ (Q est conséquence logique de P), avec P et Q des formules de la MSFOL, revient à vérifier à l'aide d'un solveur SMT (Satisfiability Modulo Theories) que la formule $P \wedge \neg Q$ est insatisfiable.

Si la première version de PEPS-analyzer implémentait un encodage purement booléen de la MSFOL dans un univers borné et utilisait un solveur SAT (Delmas, Polacsek, 2013), la nouvelle version de l'outil délègue le raisonnement dans la MSFOL à un solveur externe de type SMT, qui gère les quantificateurs nativement.

PEPS-analyzer s'appuie sur le solveur SMT Z3 (Moura, Bjørner, 2008). Il est développé en Scala et est compatible avec les plates-formes Linux (et Windows muni de Cygwin).

3.4. Un exemple

Nous introduisons à présent un exemple qui nous permettra d'illustrer l'utilisation de PEPS ainsi que les différentes notions développées dans les sections suivantes. Considérons des agents qui disposent de moyens d'observation de la Terre et qui décident de participer à une coalition pour la gestion des risques sismiques. Dans le

cadre de cette coalition, il existe un groupe d'agents particulier : le *Groupe de Gestion des Risques Sismiques*, noté GRS, dont la mission est de prévenir les fausses alertes, d'organiser les évacuations et de gérer la communication avec le public. La politique de ce système se compose pour le moment de deux règles :

- $r1$ *«Tout agent non membre du GRS doit communiquer toute information relative aux risques sismiques à au moins un membre du GRS.»*
- $r2$ *«Il est interdit, pour tout agent non membre du GRS, de communiquer des informations relatives aux risques sismiques à toute personne non membre du GRS.»*

La règle $r1$ découle clairement de l'exigence de diffusion : il y a nécessité à ce que les agents communiquent toute information relative à une catastrophe sismique à un membre du GRS pour lui permettre d'accomplir sa mission. La règle $r2$ a pour but de prévenir tout risque de panique par la diffusion brutale d'informations au grand public.

Pour pouvoir modéliser cette politique en PEPS nous devons d'abord déclarer une nouvelle constante geo, de sorte $\mathcal{T}$, qui représente le sujet *risque sismique*. Nous déclarons aussi un nouveau prédicat de domaine GRS, qui s'applique sur la sorte $\mathcal{A}$, et qui modélise l'appartenance au groupe GRS. Ainsi, $GRS(a)$ est vrai lorsque l'agent a est élément du groupe GRS, et faux lorsqu'il ne l'est pas [10]. La politique de notre exemple se modélise donc en PEPS comme suit :

$$
\begin{array}{lll}
r1: & \forall a, \forall i, \exists b, K(a,i) \wedge Topic(i, geo) \wedge \neg GRS(a) \wedge \ GRS(b) & \Longrightarrow \ O_{Send}(a,b,i) \\
r2: & \forall a, \forall i, \forall b, K(a,i) \wedge Topic(i, geo) \wedge \neg GRS(a) \wedge \neg GRS(b) & \Longrightarrow \ F_{Send}(a,b,i)
\end{array}
$$

Nous rajoutons enfin la contrainte de domaine *«Toute information concerne au moins un sujet»* : $d: \ \forall i, \exists t, \ Topic(i,t)$.

4. Des propriétés génériques pour les politiques d'échange

Pour gérer le partage de l'information au sein de systèmes tels que les CIDS, nous proposons non seulement l'utilisation d'un langage formel de modélisation pour spécifier les politiques d'échange d'informations, mais aussi l'utilisation de méthodes formelles pour valider sémantiquement les politiques. En effet, il est crucial de pouvoir adosser à un langage de spécification des opérations de vérification visant à éliminer au plus tôt les inconsistances, incomplétudes et autres problèmes que pourrait contenir la spécification d'une politique d'échanges. Le but de ces opérations est de détecter les erreurs au plus tôt, car toute erreur non détectée avant les phases d'implémentation ne fait qu'accroître les coûts de développement et, d'un point de vue applicatif

10. Nous avons choisi de modéliser l'appartenance à un groupe de la façon la plus simple possible. Ici, chaque groupe est caractérisé par un prédicat portant sur des agents et indiquant l'appartenance ou pas de l'agent au groupe. Nous aurions tout aussi bien pu introduire une sorte pour les groupes et un prédicat d'appartenance à un groupe de la forme $member(g,a)$.

les risques critiques pour les acteurs du système ou encore la diffusion non maîtrisée d'informations sensibles.

Nous nous intéressons à caractériser et à vérifier automatiquement les propriétés de *consistance*, de *complétude*, d'*applicabilité* et de *minimalité* d'une politique d'échanges d'information. Comme nous le verrons, la propriété de complétude correspond au fait qu'il n'existe pas de cas non couvert par la politique, la propriété de consistance, qu'il n'existe pas de cas où il est à la fois interdit et obligatoire (ou permis) pour un agent d'envoyer une information à un autre agent, la propriété d'applicabilité, qui veut que la politique ne couvre pas de cas qui est exclus par les contraintes du domaine, et la propriété de minimalité, qu'aucune règle de la politique ne peut se déduire des autres. Ces propriétés étant complètement indépendantes du domaine d'application de la politique, nous les nommons *propriétés génériques*.

Notons que notre outil, PEPS-analyser, permet de vérifier automatiquement ces quatre propriétés génériques.

4.1. Consistance d'une politique

En logique, une théorie est consistante si elle ne contient pas une contradiction, s'il n'est pas possible de démontrer à la fois un énoncé et sa négation. Dans le contexte des politiques de confidentialité, pour (Bieber, Cuppens, 1993), deux politiques sont consistantes entre elles si aucun utilisateur ne peut avoir à la fois la permission de savoir quelque chose, suivant la première politique, et l'interdiction selon la seconde de savoir cette même chose. Sur le même modèle, nous considérerons qu'une politique d'échange est inconsistante s'il existe un cas dans lequel il est pour un même agent à la fois obligatoire et interdit (ou autorisé et interdit), d'envoyer une information à un autre agent. La consistance d'une politique est un élément crucial. En effet, autoriser et à la fois interdire un même comportement rend l'ensemble du système incohérent. À partir d'un ensemble d'hypothèses inconsistantes, il est possible de démontrer n'importe quelle propriété, ce qui fait que l'on doit toujours vérifier la consistance des hypothèses avant de faire d'autres analyses.

L'algorithme 1 permet de vérifier la consistance d'une politique. Etant donnés une politique, il renvoie l'ensemble des paires de règles qui sont incompatibles entre elles dans une situation donnée. Pour chaque paire de règles ayant des prédicats normatifs contradictoires en conclusions, l'algorithme génère une formule qui, si elle est satisfiable, indique qu'il existe une situation dans laquelle les prémisses des deux règles sont vraies, et dans lequel les termes utilisés comme arguments des prédicats normatifs contradictoires s'unifient. Dès lors, nous sommes bien dans un cas où des exigences normatives contradictoires doivent être appliquées à des mêmes agents et sur une même information.

DÉFINITION 5. — *Consistance*
Soit $EPS = \langle \Sigma, EP \rangle$ *la spécification d'une politique d'échange,* EPS *est* consistante *si et seulement si le résultat de* Search for Non-Consistent rules $SNC(\Sigma, EP)$ *est vide.*

Algorithm 1 Search for Non-Consistent rules (SNC)

Require: $\langle \Sigma, EP \rangle$, an exchange policy specification
Ensure: S, a set of tuples (r, r', m) with r, r' exchange rules, m a model.

```
S ← ∅
for all r ∈ EP do
    if r is of the form ∀x_1, ..., ∀x_n, (φ ⟹ F_Send(t_1, t_2, t_3)) then
        for all r' ∈ EP do
            if (r' is of the form ∀x'_1, ..., ∀x'_m, (φ' ⟹ O_Send(t'_1, t'_2, t'_3))
                                or ∀x'_1, ..., ∀x'_m, (φ' ⟹ P_Send(t'_1, t'_2, t'_3))) then

                if (m is a model of ∃x_1, ..., x_n, x'_1, ..., x'_m,
                        φ ∧ φ' ∧ Σ ∧ (t_1 = t'_1) ∧ (t_2 = t'_2) ∧ (t_3 = t'_3)) then
                    S ← S ∪ (r, r', m)
                end if
            end if
        end for
    end if
end for
```

4.2. Complétude d'une politique

Une réglementation n'est pas complète lorsqu'il existe au moins un cas non prévu, c'est-à-dire lorsqu'il existe ce que l'on nomme un *vide juridique*. Nous pouvons définir la propriété de complétude dans le cadre des politiques d'échanges comme suit : *«dans toutes situations et pour toutes informations, la politique indique si un agent qui connaît cette information a l'obligation, la permission ou l'interdiction de l'envoyer aux autres agents.»* Cette définition est assez standard et correspond à celle donnée par (Akl, Denning, 1987) (Denning *et al*., 1987) dans le contexte des politiques de contrôle d'accès. Cependant, dans les phases préliminaires de conception d'un système, il peut être utile de n'avoir une politique complète que pour certains sous domaines de son domaine d'application. En effet, une politique peut être conçue dans le cadre d'une collaboration entre des parties bien distinctes, chacune portant seulement attention au sous-ensemble des sujets qui la concernent. Par exemple, dans le cadre de l'observation de la Terre, les opérateurs militaires peuvent vouloir s'assurer que la politique est complète pour tout ce qui concerne le sujet militaire sans s'intéresser aux autres sujets.

Nous proposons donc une définition paramétrée de la complétude, que nous appelons T-complétude. Une politique d'échange est dite T-complète si et seulement si pour tout agent qui connaît une information pertinente sur un sujet T, la politique spécifie si l'agent a l'obligation, la permission ou interdiction de l'envoyer à un autre agent.

DÉFINITION 6. — *T-complétude*
Soit $EPS = \langle \Sigma, EP \rangle$ la spécification d'une polique d'échange et T une constante de sorte $\mathcal{T}$. EPS est T-complète si et seulement si :

$$\mathcal{EPS} \models \forall a, \forall b, \forall i,$$
$$(K(a,i) \wedge Topic(i,T) \implies (P_{Send}(a,b,i) \vee O_{Send}(a,b,i) \vee F_{Send}(a,b,i)))$$

$r1b$ «Tout agent non membre du GRS a la permission de communiquer des informations relatives aux risques sismiques à n'importe quel membre du GRS.»

$r3$ «Les membres du GRS ont la permission de communiquer les informations relatives aux risques sismiques à quiconque.»

La règle $r1b$ complète la règle $r1$: tout agent externe au GRS sait ainsi s'il a le droit de communiquer une information relative aux risques sismiques aux autres agents du GRS en plus de celui avec lequel il a l'obligation de communiquer.

Notons que la règle $r3$ relève d'un processus d'appréciation qui n'est pas modélisé, et qui n'a pas forcément vocation à l'être au sein de la politique d'échange : le choix réalisé par un membre du GRS d'émettre ou pas un avertissement au public. Ici, c'est bien le prédicat de permission d'envoyer une information qui permet de modéliser la politique à ce niveau d'abstraction.

A l'aide de notre outil PEPS-analyzer, nous pouvons automatiquement vérifier que la spécification $\langle \{d\}, \{r1, r1b, r2, r3\} \rangle$ est geo-complète mais qu'elle n'est pas complète pour tous les sujets.

4.3. Applicabilité et minimalité d'une politique

Aux propriétés de consistance et de complétude nous rajoutons deux propriétés que sont l'applicabilité et la minimalité. Une politique est dite applicable si aucune de ses règles n'est inutile, autrement dit, il n'existe pas de règles qui s'intéressent à une situation impossible du système, et une politique est dite minimale si aucune de ses règles n'est déductible à partir des autres.

DÉFINITION 7. — *Applicabilité d'une règle*
Soit Σ un ensemble de contrainte du domaine et r une règle d'échange, i.e. $r = \forall x_1 \ldots \forall x_m(\phi \rightarrow \psi)$. *$r$ est applicable relativement à Σ si et seulement si*

$$\Sigma \wedge D \models \exists x_1 \ldots \exists x_m \phi$$

DÉFINITION 8. — *Applicabilité d'une politique*
Soit $EPS = \langle \Sigma, EP \rangle$ la spécification d'une politique d'échange, EPS est applicable si et seulement si pour chaque règle r de EP, r est applicable relativement à Σ.

L'applicabilité d'une règle est donc analysée comme un problème de satisfiabilité des prémisses d'une règle sous les hypothèses $\Sigma \wedge D$. La non-satisfiabililté des pré-

misses de la règle sous les contraintes d'environnement signifie que la règle est non applicable, *i.e.* qu'aucune situation du système ne peut satisfaire ses prémisses.

DÉFINITION 9. — *Minimalité d'une politique*
Soit $EPS = \langle \Sigma, EP \rangle$ *la spécification d'une politique d'échange avec* $EP = \{r_1, \ldots, r_n\}$. *EPS est minimale si et seulment si il n'existe pas de* i *tel que :*

$$\Sigma \wedge D \models (\bigwedge_{k \in [1,n], k \neq i} r_k) \implies r_i$$

De la même façon que pour l'applicabilité, établir la minimalité d'une politique correspond à résoudre une série de problèmes de satisfiabilité.

5. Exigences diffusion et de non-diffusion d'information

Dans le cadre des CIDS nous devons concilier deux exigences : d'une part, veiller à ce que des acteurs reçoivent toujours toutes les informations dont ils ont besoin pour accomplir leurs missions respectives (exigence de *diffusion d'information*) ; d'autre part, garantir la confidentialité, c'est-à-dire qu'aucune information sensible ne soit diffusée de manière incontrôlée (exigence de *non-diffusion d'information*). L'incapacité à gérer les conflits découlant de ces deux exigences antagonistes peut constituer un véritable obstacle à l'adoption et le déploiement de ces systèmes de surveillance collaboratifs par les nations, les organisations et les entreprises. Il est donc nécessaire de pouvoir spécifier clairement et sans ambiguïté les exigences de diffusion et de non-diffusion.

5.1. Exigence de diffusion : la propriété de vigilance

Dans les systèmes tels ques les CIDS, certains acteurs ont un rôle particulier : pour accomplir leur mission ils doivent absolument connaître toute information relative à un sujet donné. Dans notre exemple, les agents du groupe GRS doivent être prévenus de tout ce qui se rapporte au risque sismique. Par conséquent, nous définissons la propriété dite de T-*vigilance* pour un groupe comme le fait qu'un groupe d'agents est toujours correctement informé relativement à un sujet précis T.

DÉFINITION 10. — T*-vigilance pour un groupe* G *Soit* $EPS = \langle \Sigma, EP \rangle$ *la spécification d'une politique d'échange,* T *une constante de sorte* $\mathcal{T}$ *représentant un sujet d'information, et* G *un prédicat sur la sorte* $\mathcal{A}$ *caractérisant un groupe d'agents. Alors* G *est* T*-vigilant dans* EPS *si et seulement si :*

$$\mathcal{EPS} \models (\forall a, \forall i, \exists b, K(a,i) \wedge Topic(i,T) \wedge \neg G(a) \wedge G(b) \implies O_{Send}(a,b,i))$$

À l'aide de PEPS-analyzer nous pouvons vérifier $\langle \{d\}, \{r1, R1b, r2,\ idr3\} \rangle$ vérifie la propriété de geo-vigilance pour le groupe GRS. Notons qu'ici la règle $r1$ est l'instanciation directe de la propriété de vigilance pour le thème geo.

5.2. Exigence de non-diffusion : les propriétés de restriction

Si la propriété T-vigilance permet de vérifier qu'un groupe d'agents donné reçoit toujours toute information relevant du sujet T, il peut être intéressant, de façon duale, de vérifier que toute information traitant d'un sujet particulier (comme, par exemple, le sujet *confidentiel*) ne doit pas être envoyée à un groupe d'agents, à un agent unique ou bien ne doit simplement pas être envoyée du tout.

Nous définissons la propriété de *restriction de la diffusion d'information concernant un sujet à un groupe donné* selon trois cas : soit il est interdit aux agents hors du groupe de s'échanger une information de ce sujet ; soit il est interdit pour un agent hors du groupe de communiquer une information de ce sujet à un membre du groupe ; soit il est interdit aux membres du groupe de communiquer une information de ce sujet hors du groupe.

DÉFINITION 11. — *T-restriction à un groupe G Soit $EPS = \langle \Sigma, EP \rangle$ la spécification d'une politique d'échange, T une constante de sorte $\mathcal{T}$ et G un prédicat sur la sorte $\mathcal{A}$ caractérisant un groupe d'agents, nous avons alors :*

(a) T-out-out-restriction pour G dans EPS si et seulement si :

$$\mathcal{EPS} \models (\forall a, \forall b, \forall i, K(a,i) \wedge Topic(i,T) \wedge \neg G(a) \wedge \neg G(b) \implies F_{Send}(a,b,i))$$

(b) T-out-in-restriction pour G dans EPS si et seulement si :

$$\mathcal{EPS} \models (\forall a, \forall b, \forall i, K(a,i) \wedge Topic(i,T) \wedge \neg G(a) \wedge G(b) \implies F_{Send}(a,b,i))$$

(c) T-in-out-restriction pour G dans EPS si et seulement si :

$$\mathcal{EPS} \models (\forall a, \forall b, \forall i, K(a,i) \wedge Topic(i,T) \wedge G(a) \wedge \neg G(b) \implies F_{Send}(a,b,i))$$

Pour finir, nous ajoutons aux propriétés de restriction ci-dessus la propriété de T-restriction stricte qui signifie que tout échange d'information relative à T est interdit entre tous agents quels qu'ils soient (notons que cette propriété n'est qu'un cas particulier de la définition 11 avec G le groupe vide (modélisé par $\forall a, G(a) \equiv \bot$)).

DÉFINITION 12. — *T-restriction stricte*

Soit $EPS = \langle \Sigma, EP \rangle$ la spécification d'une politique d'échange et T une constante de sorte $\mathcal{T}$, nous avons la T-restriction stricte dans EPS si et seulement si :

$$\mathcal{EPS} \models (\forall a, \forall b, \forall i, K(a,i) \wedge Topic(i,T) \implies F_{Send}(a,b,i))$$

Sur notre exemple de surveillance de risques sismiques, nous pouvons vérifier, à l'aide de PEPS-analyzer, que la politique $\langle \{d\}, \{r1, r1b, r2, r3\} \rangle$ satisfait la geo-out-out-restriction pour le groupe GRS. En effet, aucune information relative à geo ne peut être envoyée entre agents hors du groupe GRS, par contre, les agents du GRS peuvent recevoir ces informations des agents extérieurs aux groupes et ils ont aussi la permission de communiquer ces informations avec les agents hors du groupe.

6. Gestion des exigences de diffusion et de non-diffusion dans un système

6.1. Incompatibilité entre la vigilance et la restriction

Enrichissons notre exemple en supposant qu'il existe dans le système des informations que nous qualifierons de *sensibles*. Pour prévenir la diffusion de telles informations nous rajoutons dans la politique de notre exemple la règle $r4$ suivante : *«il est interdit de s'échanger toute information relative au sujet sensible»*. Afin de pouvoir modéliser cette nouvelle règle dans PEPS, nous introduisons une nouvelle constante de sorte $\mathcal{T}$: $sens$, qui représente le sujet *sensible*.

$$r4 : \quad \forall a, \forall b, \forall i, K(a,i) \wedge Topic(i, sens) \implies F_{Send}(a,b,i)$$

À l'aide de PEPS-analyzer nous découvrons que l'ajout de $r4$ rend malheureusement la politique $\langle \{d\}, \{r1, r1b, r2, r3, r4\} \rangle$ inconsistante.

En effet, considérons le cas où un agent connaît une information relative à la fois à geo et à $sens$, comme par exemple une image prise par un satellite montrant un risque de catastrophe naturelle sur un site civil jouxtant un site militaire classifié. Dans ce cas là, la règle $r1$ oblige l'agent à envoyer cette information à au moins un agent du GRS, alors que $r4$ interdit à ce même agent d'envoyer l'information à quiconque et donc, à fortiori, à un agent du GRS, ce qui viole la propriété de consistance. Remarquons que les règles $r3$ et $r4$ entraînent également une inconsistance en permettant et en interdisant simultanément la diffusion d'information portant sur geo et $sens$.

Le problème d'inconsistance soulevé ici n'est pas spécifiquement lié à l'exemple, et peut se rencontrer dès que l'on considère une politique munie d'une propriété de T_1-vigilance pour un groupe G_1 et d'une propriété de T_2-restriction pour un groupe G_2. Alors, si les règles du domaine le permettent (et c'est souvent le cas), il peut être possible de construire des modèles satisfaisant les deux propriétés et où il est à la fois obligatoire et interdit d'envoyer une information. Ces modèles ont tous la même structure : au moins une information concerne les deux sujets, T_1 et T_2, et les prédicats de groupe G_1 et G_2 sont tels qu'il existe des agents à l'intérieur et à l'extérieur de G_1 et de G_2 qui satisfont les prémisses des propriétés de T_1-vigilance et T_2-restriction.

6.2. Une solution ad-hoc

Afin de prévenir les possibles conflits entre les exigences de diffusion et de non-diffusion, nous proposons d'introduire un nouvel opérateur, pour le moment sans signification particulière, de signature $p(i : \mathcal{I}) : \mathcal{I}$, qui prend en entrée une information et retourne une information.

Dans notre exemple, nous voulons que cet opérateur permette d'*oublier* la partie sensible d'une information. Par conséquent nous posons les deux contraintes de domaine suivantes pour représenter le comportement de notre opérateur abstrait : $(p1)$

une information produite par p n'est plus pertinente pour le sujet $sens$ et ($p2$) une information relative au sujet geo le reste après application de p.

$$\begin{array}{ll} p1: & \forall i, \neg Topic(p(i), sens) \\ p2: & \forall i,\ Topic(i, geo) \implies Topic(p(i), geo) \end{array}$$

Nous devons maintenant adapter la politique d'échange de notre exemple pour préciser dans quels cas l'opérateur abstrait p doit être utilisé.

Premièrement, nous séparons la règle $r1$ en deux nouvelles règles, $r11$ et $r12$, pour exprimer le fait que ($r11$) si une information est liée à des risques sismiques et qu'elle n'a pas de caractère sensible, alors il est obligatoire de l'envoyer à un membre du GRS au moins, mais ($r12$) si cette information est également sensible alors il faut envoyer non pas i elle même, mais l'information résultant de l'application de p.

$$\begin{array}{l} r11 : \forall a, \forall i, \exists b, K(a,i) \wedge Topic(i, geo) \wedge \neg Topic(i, sens) \wedge \\ \qquad\qquad \neg GRS(a) \wedge GRS(b) \implies O_{Send}(a, b, i) \\ r12 : \forall a, \forall i, \exists b, K(a,i) \wedge Topic(i, geo) \wedge Topic(i, sens) \wedge \\ \qquad\qquad \neg GRS(a) \wedge GRS(b) \implies O_{Send}(a, b, p(i)) \end{array}$$

Deuxièmement, sur le même modèle que $r1$ et pour les mêmes raisons, nous décomposons la règle $r1b$ en deux nouvelles règles $r1b1$ et $r1b2$:

$$\begin{array}{l} r1b1 : \forall a, \forall i, \forall b, K(a,i) \wedge Topic(i, geo) \wedge Topic(i, sens) \wedge \\ \qquad\qquad \neg GRS(a) \wedge GRS(b) \implies P_{Send}(a, b, p(i)) \\ r1b2 : \forall a, \forall i, \forall b, K(a,i) \wedge Topic(i, geo) \wedge \neg Topic(i, sens) \wedge \\ \qquad\qquad \neg GRS(a) \wedge GRS(b) \implies P_{Send}(a, b, i) \end{array}$$

Troisièmement, nous modifions la règle $r3$ en $r3'$ pour exprimer le fait que tout membre du GRS est autorisé à communiquer une information liée à des risques sismiques à tout autre agent, à la condition que cette information ne soit pas sensible.

$$\begin{array}{l} r3' : \forall a, \forall b, \forall i, K(a,i) \wedge Topic(i, geo) \wedge \neg Topic(i, sens) \wedge \\ \qquad\qquad GRS(a) \implies P_{Send}(a, b, i) \end{array}$$

Nous pouvons à présent vérifier à l'aide de PEPS-analyzer que cette nouvelle politique, $\langle \{d, p1, p2\}, \{r11, r12, r1b1, r1b2, r2, r3', r4\} \rangle$, est geo-complète, $sens$-complète, consistante, applicable, minimale et satisfait la restriction stricte pour le sujet $sens$.

Cependant, cette nouvelle politique ne satisfait pas la propriété de geo-vigilance pour le GRS. En effet, quand une information concernant un risque sismique est aussi de nature sensible, c'est le résultat de l'application de la fonction p à cette information qui est envoyée au GRS alors que la propriété de vigilance définie initialement

impose que cela soit l'information elle-même qui soit envoyée. Nous avions introduit la notion de vigilance afin de garantir que le GRS puisse réaliser sa mission, ce qui correspondait au fait que toute information relative à geo devait être envoyée au GRS. Finalement, l'important est qu'un membre du GRS soit prévenu et peu importe qu'il reçoive l'information initiale ou l'information après l'application de p, du moment que la partie concernant le sujet geo est préservée. Par conséquent, plutôt que de chercher à établir la geo-vigilance pour le groupe GRS, nous devons vérifier que la politique garantisse que si une information porte sur geo, alors doit être envoyée à un membre du GRS: soit cette information, soit le résultat de l'application de p, ce qui est résumé par la formule suivante :

$$\forall a, \forall i, K(a,i) \wedge Topic(i, geo) \wedge \neg GRS(a) \implies$$
$$(\exists b, GRS(b) \wedge (O_{Send}(a,b,i) \vee (Topic(p(i), geo) \wedge O_{Send}(a,b,p(i)))))$$

L'opérateur abstrait p agit comme un filtrage sur les sujets sur lesquels porte une information. Il correspond à une catégorie d'opérations effectuées régulièrement par les organismes qui gèrent des données sensibles, les opérations dites de *déclassification*, de *masquage*, d'*anonymisation*, *etc.*

6.3. Un opérateur générique de filtrage d'information

Afin de modéliser des opérations telles que la déclassification et ses variantes dans PEPS, nous introduisons un opérateur générique dit de *filtrage*, paramétré par des *modes de filtrage*. Chaque mode spécifie les sujets qui sont *conservés* ou *supprimés* par l'opérateur.

Pour cela, nous introduisons : une nouvelle sorte $\mathcal{M}$, dont les éléments représentent les différents modes de filtrage ; un opérateur de filtrage $filter(m : \mathcal{M}, i : \mathcal{I}) : \mathcal{I}$ ainsi que deux prédicats $preserves(m : \mathcal{M}, t : \mathcal{T})$ et $removes(m : \mathcal{M}, t : \mathcal{T})$. Les axiomes suivants expriment le comportement de l'opérateur de filtrage en fonction du mode :

DÉFINITION 13. — *F axiomes*

$$\begin{array}{rrcl}
\forall t, \forall m, & preserves(m,t) & \implies & \neg removes(m,t) \\
\forall i, \forall t, \forall m, & Topic(i,t) \wedge preserves(m,t) & \implies & Topic(filter(m,i),t) \\
\forall i, \forall t, \forall m, & Topic(i,t) \wedge removes(m,t) & \implies & \neg Topic(filter(m,i),t)
\end{array}$$

Le premier axiome garantit la cohérence entre les prédicats de préservation et de suppression: si un mode conserve un sujet, alors il ne le supprime pas. Le deuxième axiome stipule que si une information concerne un sujet qui est préservé par un mode, alors elle concerne toujours ce sujet après filtrage sous ce mode. Le troisième axiome est simplement le dual du deuxième concernant le prédicat de suppression.

L'opérateur ad-hoc p, défini dans la section précédente, est subsumé par l'opérateur filtrage générique. Dans notre exemple, nous introduisons une constante $filterSens$ de

sorte $\mathcal{M}$, qui représente le mode de filtrage pour les informations à contenus sensibles et qui préserve les contenus relatifs aux risques sismiques. Concrètement, nous ajoutons la contrainte de domaine suivante qui spécifie les propriétés du filtrage pour ce mode :

$$f : \ preserves(\mathit{filterSens}, geo) \wedge removes(\mathit{filerSens}, sens)$$

Il est important de noter que cette caractérisation des modes de filtrage à l'aide des prédicats $preserves$ et $removes$ n'est qu'une modélisation partielle des politiques de filtrage du monde réel. En effet, dans la pratique, d'autres conditions doivent être prises en compte pour l'utilisation de l'opérateur, telles que la capacité de l'agent à effectuer l'opération de filtrage, les caractéristiques du destinataire, *etc.* Toutes les conditions supplémentaires qui caractérisent les modes de filtrage pourraient être regroupées pour former une *politique de filtrage*, comparable à ce qui existe déjà pour les *politiques de déclassification*. Cependant, même si l'extensibilité de PEPS et la puissance expressive de la logique sous-jacente permettent de modéliser ces concepts, nous ne les développerons pas davantage dans cet article.

6.4. Propriétés génériques de vigilance et de restriction

Forts de la définition de l'opérateur de filtrage, nous pouvons redéfinir la propriété de vigilance en une version qui permette d'éviter le conflit avec les propriétés de restriction de diffusion d'information. Un groupe d'agents est dit T-vigilant si et seulement si tout agent, extérieur au groupe, connaissant une information relative au sujet T, a l'obligation d'envoyer à au moins un agent appartenant au groupe soit l'information soit l'information filtrée avec un mode de filtrage qui préserve les informations concernant le sujet T.

DÉFINITION 14. — *T-vigilance pour un groupe G Soit $EPS = \langle \Sigma, EP \rangle$ la spécification d'une polique d'échange, T une constante de sorte $\mathcal{T}$ et G un prédicat sur la sorte $\mathcal{A}$ caractérisant un groupe d'agents, G est T-vigilant dans EPS si et seulement si :*

$$\mathcal{EPS}, F \models (\forall a, \forall i, K(a,i) \wedge \mathit{Topic}(i,T) \wedge \ G(a) \implies$$
$$(\exists b, G(b) \wedge (O_{Send}(a,b,i) \vee \exists m, preserves(m,T) \wedge O_{Send}(a,b,\mathit{filter}(m,i)))))$$

Si nous revenons à notre exemple de prévention des risques sismiques, avec cette nouvelle définition de la vigilance, nous pouvons vérifier à l'aide de PEPS-analyser que la politique $\langle \{d, f\}, \{r11, r12, r1b1, r1b2, r2, r3', r4\} \rangle$, réécrite avec l'opérateur *filter* [11], satisfait à la fois la nouvelle geo-vigilance et la geo-out-out-restriction pour le groupe GRS, la $sens$-restriction stricte, mais aussi la geo-complétude, la $sens$-complétude, la consistance, l'applicabilité et la minimalité.

11. Toutes les occurrences de $p(i)$ dans les règles de la politique d'échange ont été remplacées par $\mathit{filter}(\mathit{filterSens}, i)$.

7. Conclusion

Dans cet article, après avoir donné un panorama des systèmes supportant la gestion et la prévention de risques via la génération d'alertes, que nous désignons par CIDS, nous avons présenté un bref rappel de la notion de politique, au sens normatif, pour la spécification de règles régissant les échanges d'information dans les CIDS. Nous avons ensuite rappelé les bases du langage PEPS, accompagné de l'outil PEPS-analyzer, qui permet l'expression et l'analyse formelle automatique de politiques d'échange d'information. Nous avons ensuite présenté les quatre propriétés logiques génériques principales des politiques (cohérence, complétude, applicabilité, minimalité), indépendantes du domaine d'application, et nous avons ensuite présenté deux classes de propriétés orientées métier : celles liées aux exigences de diffusion et celles liées aux exigences de non-diffusion. Nous avons ensuite montré que, dans certains cas, il s'avère impossible de les satisfaire simultanément sans introduire un nouvel opérateur de filtrage d'information. Enfin, nous avons donné à cet opérateur une définition générique et paramétrique, et redéfini les propriétés orientées métier en conséquence.

Nous espérons avoir démontré qu'une approche formelle pour la spécification et la vérification de politiques d'échange d'information est non seulement souhaitable mais aussi possible avec les moyens techniques actuels. Un tel niveau de maîtrise des exigences de diffusion nous semble nécessaire compte tenu de la nature critique des missions confiées à ces systèmes d'alerte. L'exemple développé au long de cet article illustre la plus value des analyses formelles automatiques, déjà manifeste sur un ensemble réduit de règles: sans elles, il est extrêmement difficile de rédiger une politique logiquement et applicativement correcte. La maîtrise de la correction des principes de fonctionnement fondamentaux d'un CIDS ainsi obtenue nous semble être un atout pour convaincre les acteurs du système de diffuser des informations plus largement.

Jusqu'à présent, nous nous sommes concentrés sur les concepts clés des politiques d'échange d'information. Dans des travaux futurs nous inclurons à ce cadre de spécification la modélisation des organisations qui composent le système. Nous devrons déterminer si certains concepts, comme ceux *d'organisation* et de *rôles*, issus des modèles tels que OrBAC (Kalam, Benferhat *et al.*, 2003), peuvent être transposés dans notre cadre, tout en adaptant si besoin les propriétés déjà définies pour les politiques de diffusion. Techniquement parlant, la nature extensive de PEPS permet de modéliser aisément de tels nouveaux concepts.

Des études théoriques relatives à la décidabilité des problèmes posés sur ces politiques nous semblent aussi nécessaires, pour délimiter précisément les garanties pouvant être obtenues (toute propriété est-elle prouvable ou invalidable en un temps fini?). Des travaux récents dans le domaine de la combinaison de procédures de décision vont dans ce sens (Chocron *et al.*, 2014), en identifiant des fragments décidables de la logique du premier ordre toujours plus expressifs. Nous souhaitons déterminer si les exigences de diffusion typiques appartiennent à ces fragments décidables ou si,

au contraire, elles nécessitent un pouvoir expressif strictement supérieur et nous replongent dans l'indécidabilité.

Enfin, il serait intéressant de faire le lien entre la spécification et l'implémentation de ces politiques. Dans le domaine des Architectures Orientées Services, (Barhamgi *et al*., 2013) montrent qu'il est possible, dans le contexte du contrôle d'accès à l'information, de définir des modèles d'exécution paramétrés par des politiques de confidentialité et d'appliquer ces politiques à l'exécution. Ici, le lien entre la spécification de la politique et sa mise en œuvre par composition des services, est explicite. Nous pourrions étudier si cette approche peut être adaptée dans le cadre du contrôle de la diffusion d'information.

Bibliographie

Akl S., Denning D. (1987). Checking classification constraints for consistency and completeness. In *Ieee symposium on security and privacy*, p. 196-201. IEEE Computer Society.

Barhamgi M., Benslimane D., Oulmakhzoune S., Cuppens-Boulahia N., Cuppens F., Mrissa M. *et al*. (2013). Secure and privacy-preserving execution model for data services. In C. Salinesi, M. C. Norrie, O. Pastor (Eds.), *Caise*, vol. 7908, p. 35-50. Springer.

Bieber P., Cuppens F. (1992). A logical view of secure dependencies. *Journal of Computer Security*, vol. 1, n° 1, p. 99-130.

Bieber P., Cuppens F. (1993). Expression of confidentiality policies with deontic logic. In J.-J. C. Meyer, R. J. Wieringa (Eds.), *Deontic logic in computer science: Normative system specification*, p. 103-123. John Wiley & Sons, Inc.

Browne J., Zhang J. (1999). Extended and virtual enterprises similarities and differences. *International Journal of Agile Management Systems*, vol. 1, n° 1, p. 30-36.

Castanẽda H. N. (1975). *Thinking and doing*. D. Reidel, Dordrecht.

Chocron P., Fontaine P., Ringeissen C. (2014). A gentle non-disjoint combination of satisfiability procedures. In S. Demri, D. Kapur, C. Weidenbach (Eds.), *ijcar*, vol. 8562, p. 122–136. Springer.

Cholvy L., Cuppens F. (1997, may). Analyzing consistency of security policies. In *Security and privacy, 1997. proceedings., 1997 ieee symposium on*, p. 103 -112.

Cuppens-Boulahia N., Cuppens F. (2008). Specifying intrusion detection and reaction policies: An application of deontic logic. In *Deon*, p. 65-80.

Dal Bello B. R. (2011). Managing risk in space. *Federation of American Scientists, Public Interest Report, Winter*, vol. 64, n° 4.

Delmas R., Polacsek T. (2013). Formal methods for exchange policy specification. In C. Salinesi, M. C. Norrie, O. Pastor (Eds.), *Caise*, vol. 7908, p. 288-303. Springer.

Delmas R., Polacsek T. (2014). Exigences de confidentialité et de diffusion concernant les politiques d'échanges d'information. *Génie Logiciel*, vol. 111, p. 49–53.

Delmas R., Polacsek T. (2015a). Critical information diffusion systems. In *New trends in databases and information systems - ADBIS 2015 workshops wisard*, vol. 539, p. 557–566. Springer.

Delmas R., Polacsek T. (2015b). Need-to-share & non-diffusion requirements verification in exchange policies. In *Caise'15: Proceedings of advanced information systems engineering - 27th international conference.* Springer.

Denning D. E., Akl S. G., Heckman M., Lunt T. F., Morgenstern M., Neumann P. G. *et al.* (1987). Views for multilevel database security. *IEEE Trans. Software Eng.*, vol. 13, n° 2, p. 129-140.

Department Of Defense. (1985). *Department Of Defense Standard Department Of Defense Trusted Computer System Evaluation Criteria.*

Dyer J. H., Singh H. (1998). The Relational View: Cooperative Strategy and Sources of Interorganizational Competitive Advantage. *The Academy of Management Review*, vol. 23, n° 4, p. 660–679.

Edmonds B. (2002). How formal logic can fail to be useful for modelling or designing mas. In G. Lindemann, D. Moldt, M. Paolucci (Eds.), *Regulated agent-based social systems, first international workshop, rasta 2002, bologna, italy, july 16, 2002, revised selected and invited papers*, vol. 2934, p. 1-15. Springer.

Gallier J. H. (1987). Logic for computer science: Foundations of automatic theorem proving. In, p. 448-476. Wiley.

Heymann D. L., Rodier G. R. (2001). Hot spots in a wired world: {WHO} surveillance of emerging and re-emerging infectious diseases. *The Lancet Infectious Diseases*, vol. 1, n° 5, p. 345 - 353.

ITSEC. (1991). *Information technology security evaluation criteria (itsec): Preliminary harmonised criteria*. Rapport technique n° Document COM(90) 314, Version 1.2. Commission of the European Communities.

Jones A. J. I., Sergot M. J. (1992). Formal specification of security requirements using the theory of normative positions. In *Proceedings of the second european symposium on research in computer security*, p. 103–121. Springer-Verlag.

Kalam A. A. E., Baida R. E., Balbiani P., Benferhat S., Cuppens F., Deswarte Y. *et al.* (2003). Organization based access control. In *Proceedings. policy 2003. ieee 4th international workshop on policies for distributed systems and networks, 2003.*

Kalam A. A. E., Benferhat S., Miège A., Baida R. E., Cuppens F., Saurel C. *et al.* (2003). Organization based access contro. In *Policy*, p. 120-131. IEEE Computer Society.

Mandl K. D., Overhage J., Wagner M. M., Lober W. B., Sebastiani P., Mostashari F. *et al.* (2004). Implementing syndromic surveillance: a practical guide informed by the early experience. *Journal of the American Medical Informatics Association*, vol. 11, p. 141 - 150.

McCarthy J. (1997). Modality, si! modal logic, no! *Studia Logica*, vol. 59, n° 1, p. 29-32.

Meynard J., Chaudet H., Texier G., Ardillon V., Ravachol F., Deparis X. *et al.* (2008). Value of syndromic surveillance within the armed forces for early warning during a dengue fever outbreak in french guiana in 2006. *BMC Med. Inf. & Decision Making*, vol. 8, p. 29.

Moura L. de, Bjørner N. (2008). Z3: An efficient smt solver. In *Tools and algorithms for the construction and analysis of systems, 14th international conference, tacas 2008*, vol. 4963, p. 337-340. Springer.

Sebastiani R., Vescovi M. (2009). Automated reasoning in modal and description logics via sat encoding: the case study of k(m)/alc-satisfiability. *J. Artif. Intell. Res. (JAIR)*, vol. 35, p. 343-389.

Taverne B. (2015). Anticiper les flambées épidémiques à virus Ebola : pas sans les sciences sociales ! *Global Health Promotion*, vol. 22, n° 2, p. 85–56.

Varraine-Leca A. (2015). Ebola : chronique d'une traque. *Humanitaire. Enjeux, pratiques, débats*, vol. 40, p. 80–87.