Le contrôle d'accès des réseaux et grandes infrastructures critiques distribuées

Abdeljebar Ameziane El Hassani

THÈSE

En vue de l'obtention du

DOCTORAT DE L'UNIVERSITÉ DE TOULOUSE

Délivré par :

Institut National Polytechnique de Toulouse (INP Toulouse)

Discipline ou spécialité :

Réseaux, Télécommunications, Systèmes et Architecture

Présentée et soutenue par :

M. ABDELJEBAR AMEZIANE EL HASSANI

le samedi 23 avril 2016

Titre :

LE CONTROLE D'ACCES DES RESEAUX ET GRANDES INFRASTRUCTURES CRITIQUES DISTRIBUEES

Ecole doctorale :

Mathématiques, Informatique, Télécommunications de Toulouse (MITT)

Unité de recherche :

Institut de Recherche en Informatique de Toulouse (I.R.I.T.)

Directeur(s) de Thèse :

M. ANAS ABOU EL KALAM

M. ABDELLAH AIT OUAHMAN

Rapporteurs :

Mme ANA ROSA CAVALLI, TELECOM SUD PARIS

M. ZAHI JARIR, UNIV. DE CADI AYYAD MARRAKECH MAROC

Membre(s) du jury :

M. SALAH EDDINE LABHALLA, UNIV. DE CADI AYYAD MARRAKECH MAROC, Président

M. ABDELLAH AIT OUAHMAN, UNIV. DE CADI AYYAD MARRAKECH MAROC, Membre

M. ABDERRAHIM SEKKAKI, UNIVERSITE HASSAN II CASABLANCA MAROC, Membre

M. ANAS ABOU EL KALAM, INP TOULOUSE, Membre

M. HANAN EL BAKKALI, UNIV. MOHAMMED V RABAT MAROC, Membre

M. YAMINE AIT AMEUR, INP TOULOUSE, Membre

Dédicaces

A mon père, ma mère et mon frère, ces êtres chers à qui je témoigne une sincère et profonde gratitude pour tout le soutien, l'amour et l'affection dont ils m'ont bordé depuis que j'existe. Sans cela, il aurait été difficile de tenir jusque-là.

A mes grands-parents ainsi qu'à toutes mes familles, AMEZIANE EL HASSANI, KOJMANE, DEBBARH, BERRADA, TAHRI, SKIREDJ, KADIRI, KHATIB et BENNANI, je tiens à dédier ce modeste travail, en leur témoignant ma profonde gratitude pour leur confiance, leurs encouragements et leur amour.

A ma chère épouse Sara pour son amour, son affection, sa confiance et son soutien inconditionné.

A ma belle-famille, je dédie ce modeste travail, en les remerciant de leur confiance et leur soutien.

A mes amis et à leurs familles, je dédie le fruit de ces années de travail, en les remerciant de m'avoir comblé de tellement de moments de joie et d'avoir toujours été à mes côtés pendant les moments difficiles.

A tous ceux que j'aime et qui m'aiment.

Remerciements

Les travaux de recherche présentés dans ce mémoire ont été réalisés, en alternance, au sein des laboratoires « Optimisation des Systèmes de Communications Avancés, Réseaux et Sécurité » de l'Ecole Nationale des Sciences Appliquées de Marrakech (OSCARS - ENSAM) et « Institut de Recherche en Informatique » de Toulouse (IRIT - CNRS/INPT). Je tiens à remercier, tout d'abord, les directeurs successifs de ces structures de m'avoir permis de mener mes recherches au sein de leurs établissements.

Ma reconnaissance se tourne aussi particulièrement vers les responsables d'équipes de recherche pour m'avoir accueilli au sein de leurs groupes de travail.

Bien évidemment, je tiens à adresser mes profonds remerciements et gratitude à Monsieur Anas ABOU EL KALAM, Professeur Habilité à Diriger les Recherches à l'Institut National Polytechnique de Toulouse, en sa qualité de directeur de mes travaux de thèse. Son engagement, sa présence, ses efforts, ses qualités humaines, ses compétences et son expérience scientifiques ainsi que ses recommandations m'ont, durant toutes ces années, guidé sur la bonne voie.

Aussi, je témoigne, tout particulièrement, mes profonds respects et gratitude à Monsieur Abdellah AIT OUAHMAN, Professeur de l'Enseignement Supérieur à l'Ecole Nationale des Sciences Appliquées de Marrakech, pour m'avoir honoré en sa qualité de directeur de mes travaux de thèse. Sa sagesse, ses qualités humaines, son soutien, sa disponibilité, son écoute et ses conseils m'ont inspiré tout au long de ces années et m'ont permis de mener mes recherches dans un cadre serein.

Que Monsieur M. LABHALLA Salah-Eddine, Professeur à la Faculté des Sciences Semlalia de Marrakech, accepte l'expression de ma profonde gratitude pour l'honneur qu'il me fait en présidant le jury de ma thèse, ainsi que l'ensemble des honorables membres de ce jury :

- Mme. CAVALLI Ana Rosa, Professeur à l'Institut Mines-Télécom/Télécom SudParis de Paris ;
- Mme. EL BAKKALI Hanan, Professeur à l'Ecole Nationale Supérieure d'Informatique et d'Analyse des Systèmes de Rabat ;
- M. AIT AMEUR Yamine, Professeur à l'Ecole Nationale Supérieure Electronique Electrotechnique Informatique Hydraulique de Toulouse ;

- M. JARIR Zahi, Professeur à la Faculté des Sciences Semlalia de Marrakech ;
- M. SEKKAKI Abderrahim, Professeur à la Faculté des sciences Ain Chock de Casablanca.

Je remercie tout particulièrement, Mme CAVALLI et Mr JARIR et d'avoir accepté d'être les rapporteurs de ces travaux de recherche.

Mes sincères remerciements s'adressent également à Monsieur Adel BOUHOULA, Professeur à l'Ecole Supérieur des Communications de Tunis, ainsi qu'à Mademoiselle Ryma ABBASSI, Professeur assistant à l'Institut Supérieur des Etudes Technologiques en Communications de Tunis, pour l'aide, les conseils ainsi que les éclairages qu'ils m'ont prodigués durant mon stage à l'Ecole Supérieur des Communications de Tunis.

Aussi, je tiens à adresser mes sincères remerciements aux Professeurs Touria HASBOUNE, Raja ELASSALI, Younes JABRANE, Noureddine IDBOUFKER et Khalid EL BAAMRANI pour leur aide, leur soutien et leur confiance.

Aux membres de la filière Génie Réseaux et Télécommunications, aux membres des corps professoral et administratif de l'Ecole Nationale des Sciences Appliquées de Marrakech ainsi qu'aux membres de l'équipe administrative de l'Institut de la Recherche en Informatique de Toulouse, je tiens à adresser mes remerciements les plus sincères pour vos efforts et votre dévouement au bon déroulement des activités scientifiques.

Je tiens exprimer une sincère sympathie à tous les amis qui, de près ou de loin, m'ont soutenu durant ces années. Je tiens à citer, tout spécialement, des noms qui ont particulièrement marqué cette période : Zakaria BOULGHASSOUL, Abdelhamid LOULIEJ, Abdessamad KLILOU, Mohamed MAACHAOUI, les frères JAKJOUD, Ferdaouss CHAKIB et Omar AKHADDAM, Kawtar MACHHOUD et Rachid LAAZOUZI, Tarik DAOUDI, Myriam EL MESBAHI, Younes AIT DRISS et Lamia HAMMADI.

Que ceux dont le nom ne figure pas sur cette page et qui se considèrent comme oubliés, veuillent bien m'en excuser et qu'ils sachent que je les porte dans mon cœur.

ملخص

نمط حياتنا يحكمه العديد من البنيات التحتية الأساسية الازمة لتوفير راحتنا، استقرارنا وتنمية أوطاننا. لهذا تم تصنيفها كبنيات تحتية حيوية (IC). نظرا لأهميتها، فإنها معرضة للعديد من التهديدات؛ و لا يسمح لها بأي توقف، فشل أو عطل. من بين الأخطار التي تهدد أنظمتها المعلوماتية - المعروفة باسم " البنيات المعلوماتية الحيوية "(IIC)، اثنان منهم نولي لهما اهتماما خاصا، أولهما يتمثل في انتهاك تمامية البيانات الخاصة بها و عملياتها الحاسوبية و ثانيهما يخص التجاوزات التي قد تحدث خلال التعاون مع أطراف أخرى. فيما يتعلق بالخطر الأول، تمامية المعلومة، المتجلية في عدم تدهورها، هي خاصية ضرورية للبنيات المعلوماتية الحيوية، من منطلق أنها تحتاج إلى معلومات صحيحة لخلق نتائج موثوقة، عقب الانتهاء من عمليات داخلية. أما بالنسبة للخطر الثاني، فهو مرتبط بتحديات العولمة الحالية، حيث لا يمكن أن نتحدث عن تطوير البنيات التحتية الحيوية بدون إشراك فاعلين من محيطها الخارجي. بما أن جميع الموارد المستعملة من قبل البنيات التحتية الحيوية يمكن أن تكون عرضة للعبث بسبب المنافسة الغير الشريفة، لذا فهذه الشراكات لا تخلو من مخاطر.

في محاولة للحد من مخاطر الفساد المعلوماتي القادم من الداخل أو الخارج، ركزنا اهتمامنا على تحسين ألية مراقبة المداخل. يهدف هذا الخط الدفاعي الأساسي إلى تقييد تدخلات المستعملين الشرعيين للنظام، وفقا للسياسة المعتمدة من قبل المنظمة. أهمية و دقة هذه السياسة تؤثر بشكل كبير على فعالية الألية. لهذا السبب يتم استخدام نماذج التحكم في المداخل ليسهل التعبير، التجريد، إدارة السياسات و كذلك ليتم الاستجواب، المنطق و الحسابات بطريقة أوتوماتكية مما يتيح لنا الكشف عن العديد من الصراعات المحتملة. OrBAC نموذج يحظى بأهمية خاصة لثروته و طبيعته الديناميكية: بالإضافة إلى السياقات فهو يضم عدة مفاهيم – تتمثل في الأدوار، الرؤى و الأنشطة – كما يحدد هذا النموذج أربعة طرق للولوج، الكل مرتبط بمفهوم المنظمة. هذا النموذج يلبي العديد من احتياجات البنيات المعلوماتية الحيوية، لكنه يظل محدود فيما يخص توفير التمامية في كلا المجالين المحلي والموزع.

في هذا الخضم، اقترحنا امتدادا يخص المجالات المحلية، I-OrBAC) -Integrity OrBAC)، و يأخذ بعين الاعتبار الإكراهات الحقيقية المتعلقة بالتمامية حتى يتم التقرير في طلبات الولوج. I-OrBAC يدمج الإعدادات المقتبسة من أساليب تحليل المخاطر من أجل التعبير عن السياسات التي تعكس الاحتياجات للموارد الغير النشيطة و تقدير مهارات المستعملين. إدماج هذه الإعدادات داخل OrBAC وجهنا نحو استعمال نماذج متعددة المستويات. هذا النهج يمكننا من تعزيز أولويات الممتلكات الحساسة كما هو منصوص عليه في برامج حماية البنيات التحتية الحيوية. في نموذجنا يتم استخدام مستويات التمامية للحد من توزيع الامتيازات هذا من جهة، و من جهة أخرى

لجعلها أكثر مرونة. لوضوح أكثر، هذه المستويات هي وسيلة أخرى لتقييد المداخل، تتيح فقط للمستخدمين دوي الخبرة استعمال الموارد الحساسة. فيما يتعلق بالمرونة ووفقا لاختصاصات المنظمة يمكننا القول أن كل مهمة يمكن أن يقوم بها أشخاص لهم أدوار مختلفة علما أن كل دور يخضع لقيود معينة.

اقتصار نموذج التحكم في المداخل على تصنيف طلبات الدخول قد يكون محدودا بالنسبة للبنيات المعلوماتية الحيوية، اقترحنا أيضا خوارزمية تم التعبير عنها باستعمال نظام استدلالي مما يجعل امتدادنا استباقي. هذا النظام الرياضي يسهل فهم الخوارزمية المقترحة مع تعزيز مسار التفكير المنطقي و أخيرا استخلاص الاستنتاجات. تهدف هذه الخوارزمية إلى اختيار الدور الأنسب من بين الأدوار ذات الأولوية حتى يتم إنجاز مهمة دون انتظار الطلب من طرف العضو. لقد اقترحنا برمجة نموذجنا في إطار دراسة للحالات مستخلصة من المشروع الأوربي FP7 CRUTIAL والمتعلق بشبكات نقل وتوزيع الكهرباء. و تشمل هذه البرمجة جل ما تم ذكره أعلاه.

و أخيرا، للتغلب على المشاكل الناجمة عن التعاون قمنا باستعمال العقود الإلكترونية ليشمل I-OrBAC المجالات الموزعة. هذه العقود و بالإضافة إلى كونها تحدد السياق، الشروط و الأنشطة، فهي تقوم بتنبؤ وقوع النزاعات و تساهم في حلها. لتمكن من استعمالها في أمثل الظروف، كان من الضروري تصميم أليات، مناسبة لنموذجنا، تمكننا من تسهيل مفاوضتها و تنفيذها.

كلمات البحث: البنيات التحتية الحيوية، البنيات المعلوماتية الحيوية، I-OrBAC، مستويات التمامية، الحرجية، المصداقية، DI-OrBAC، العقود الإلكترونية.

Résumé

Notre existence est régie par des infrastructures vitales à notre confort, à la stabilité et au développement de nos pays. Notre dépendance est telle qu'elles sont décrétées comme « *Infrastructures Critiques* » (IC). Compte tenu de leur importance, de nombreuses menaces les guettent ; seulement nulle indisponibilité, défaillance ou erreur de fonctionnement n'est tolérée dans leurs cas. Parmi les menaces qui guettent leurs systèmes d'information – connus sous le nom d'« *Infrastructures d'Information Critiques* » (IIC) – deux nous intéressent particulièrement en l'occurrence : les atteintes à l'intégrité de leurs données et processus informatisés ainsi que les abus pouvant survenir au cours des collaborations avec d'autres parties. Concernant le premier volet, l'intégrité d'une information, qui se définit comme étant sa propriété de ne pas être altérée, est primordiale pour les IIC du fait qu'elles manipulent des informations devant nécessairement être correctes et génèrent, à l'issue de processus internes, des résultats devant indiscutablement être fiables. Le second volet se rapporte quant à lui au contexte actuel de mondialisation et d'ouverture où il est inconcevable que les IC puissent évoluer sans collaborer avec des acteurs extérieurs. Collaborer n'est toutefois pas sans risques puisque les ressources engagées par l'IC peuvent faire l'objet de tentatives de sabotage dues à une compétitivité déloyale.

Tentant de réduire les risques de corruptions pouvant émaner aussi bien de l'intérieur que de l'extérieur, nous nous sommes focalisés sur l'amélioration du mécanisme de contrôle d'accès. Cette ligne de défense incontournable vise à limiter les actions auxquelles peuvent prétendre les utilisateurs légitimes du système, et ce conformément à la politique de sécurité de l'organisation. La pertinence et la finesse de cette dernière impacte grandement l'efficacité du mécanisme. Pour cela, des modèles de contrôle d'accès sont utilisés pour faciliter entre autres l'expression, l'abstraction et l'administration des politiques, mais aussi pour automatiser leur interrogation, les raisonnements et les calculs notamment pour détecter les éventuels conflits. Le modèle OrBAC suscite bien des intérêts notamment en raison de sa richesse et de son caractère dynamique : il conjugue plusieurs concepts – rôles, vues et activités – en plus des contextes et définit quatre modes d'accès, le tout autour du concept de l'organisation. Ce modèle satisfait maints besoins des IIC, en revanche il reste limité quant à la prise en charge de l'intégrité, aussi bien en contexte localisé que distribué.

Ainsi, nous avons proposé une extension d'OrBAC pour les environnements localisés, *Integrity-OrBAC* (I-OrBAC), qui tient compte de contraintes réelles liées à l'intégrité pour statuer sur les requêtes d'accès. I-OrBAC intègre des paramètres issus de

l'application de méthodes d'analyse de risques afin d'exprimer des politiques reflétant les besoins des ressources passives et appréciant, à leur juste valeur, les habilitations des sujets. Intégrer ces paramètres à OrBAC nous a orientés vers une nouvelle vision de modélisation en multi-niveaux d'intégrité ; approche favorisant la priorisation des biens sensibles à l'image des programmes de protection des IC. Dans notre modèle, les niveaux d'intégrité servent aussi bien à contraindre l'attribution des privilèges qu'à la rendre plus flexible. Plus clairement, ces niveaux sont un moyen supplémentaire de restriction des accès pour garantir que seuls des utilisateurs chevronnés accéderont aux ressources sensibles. Concernant la flexibilité, selon le métier de l'organisation, nous pensons qu'une tâche peut être réalisée par les sujets de différents rôles, à la différence que chaque rôle sera assujetti à des contraintes spécifiques.

Un modèle de contrôle d'accès restreint à statuer sur les requêtes d'accès risque de s'avérer limitatif pour les IIC, nous avons aussi proposé un algorithme, décrit par un système d'inférence, rendant notre extension proactive. Ce système formel facilite la compréhension de notre algorithme tout en favorisant la conduite de raisonnements logiques et la dérivation de conclusions. Le but de l'algorithme est de déterminer le sujet le plus adéquat, parmi les rôles prioritaires, pour la réalisation d'une tâche sans attendre que les sujets n'en fassent la requête. Nous avons proposé une implémentation de notre modèle dans le cadre d'une étude de cas tirée du projet européen FP7 CRUTIAL relatif aux réseaux de transport et de distribution d'électricité. Cette implémentation a porté sur la majorité des briques précédemment évoquées.

Finalement, pour pallier les problèmes issus des collaborations, nous avons fait appel aux contrats électroniques pour étendre I-OrBAC aux environnements distribués – l'extension *Distributed I-OrBAC* (DI-OrBAC). Ces pactes servent non seulement à définir le contexte, les clauses ainsi que les activités à réaliser mais aussi à prévenir l'occurrence de litiges et à les résoudre. Toutefois, nous avons dû concevoir des mécanismes adaptés à notre modèle I-OrBAC pour leur négociation et leur application.

Mots-clés : infrastructures critiques, infrastructures d'informations critiques, I-OrBAC, niveaux d'intégrité, criticité, crédibilité, DI-OrBAC, contrat électronique.

Abstract

Our existence is governed by infrastructures that are essential to our comfort, to the stability and the development of our countries. Our dependence is such that they are decreed as "Critical Infrastructures" (CI). Considering their importance, many threats target them; unfortunately, downtimes, failures or operational errors are not tolerated in their cases. Among the threats on their information systems – better known as "Critical Information Infrastructures" (CII) – two are of a particular interest, namely the attacks against integrity of their data and computerized processes and also the abuses that may occur during collaborations with other parties. Regarding the first threat, the information integrity property, which is defined as its property not to be corrupted, is of paramount importance to the CII because they manipulate information that must be necessarily correct and generate, as the output of internal processes, results that should be undoubtedly reliable. Concerning the second threat, it relates to the actual context of globalization and openness, where it is inconceivable that CI could evolve without collaborating with foreign actors. Collaborations, however, are not without risks, since the resources provided by the CI can be subject to tampering due to unfair competition.

Trying to reduce corruption risks that may occur both from inside and outside, we focused on improving the access control mechanism. This essential line of defense aims to limit actions of the system legitimate users in accordance with the organization security policy. The relevance and the fine-grained property of this policy impact greatly the effectiveness of access control. Therefore, access control models are used to facilitate not only the expression, the abstraction and the administration of such policies but also to automate the reasoning and the queries to, particularly, detect possible conflicts. The OrBAC model raises many interests particularly because of its richness and its dynamicity: it combines, around the concept of organization, several concepts – roles, views and activities – in addition to the contexts and defines four access modes. This model meets many CII needs; however it remains limited as to the support of integrity, both in local and distributed environments.

In this sense, we proposed *Integrity-OrBAC* (I-OrBAC), an OrBAC extension for local environments, which takes into account real integrity constraints to rule on access requests. I-OrBAC includes some parameters extracted from the application of risk analysis methods in order to express policies that reflect the needs of passive resources and appreciate pertinently subjects' abilities. Introducing these parameters to OrBAC led us to a new vision of multi integrity levels modeling; this approach promotes the prioritization of

sensitive resources just like the CI protection programs do. In our model, the integrity levels are used both to constraint the assignment of privileges and to make it more flexible. In other words, these levels represent an additional way of restricting accesses in order to ensure that only experienced users can access sensitive resources. Regarding flexibility, we believe that, according to the organization's business, a task may be carried out by the subjects of different roles, except that each role will be subjected by specific constraints.

In the context of CII, an access control model only restricted to approve subjects' access requests would be limited; therefore, we proposed an algorithm, described by an inference system, which makes our extension proactive. This formal system aims to facilitate the understanding of our algorithm while promoting the conduct of logical reasoning and deriving conclusions. The algorithm's goal is to determine the most appropriate subject, among the priority roles, for achieving a task without waiting for some subjects to request it. Also, we proposed an implementation of our model through a case study drawn from the FP7 European project (CRUTIAL) on electrical energy transmission and distribution. This implementation covered the majority of the components mentioned above.

Finally, to address problems that arise from collaborations, we used electronic contracts to enrich and extend I-OrBAC to serve in distributed environments – the extension is called *Distributed I-OrBAC* (DI-OrBAC). These agreements aim, on the one hand, to define the context, terms and activities to be achieved and serve, on the other hand, to prevent and resolve the disputes. However, we had to design appropriate mechanisms for our I-OrBAC model in order to lead correct negotiations and rigorous enforcement of these contracts.

Keywords : critical infrastructures, critical information infrastructures, I-OrBAC, integrity levels, criticality, credibility, DI-OrBAC, electronic contracts.

TABLE DES MATIÈRES

Liste des figures

Liste des tableaux

Liste des acronymes

ACLU	*American Civil Liberties Union*
AEA	*Activity Enablement Authority*
ANSSI	*Agence Nationale de la Sécurité des Systèmes d'Information*
BSA	*Bank Secrecy Act*
COTS	*Commercial Off-The-Shelf*
CA	*Contrôle d'accès*
CDI	*Constrained Data Items*
CIA	*Central Intelligence Agency*
CIPS	*Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks*
CRUTIAL	*CRitical UTility InfrastructurAL resilience project*
DAC	*Discretionary Access Control*
DCSSI	*Direction Centrale de la Sécurité des Systèmes d'Information*
DoD	*Department of Defense*
DoS	*Denial of Service*
DSD	*Dynamic Separation of Duty*
ECPA	*Electronic Communications Privacy Act*
EFF	*Electronic Frontier Foundation*
EPCIP	*European Program for Critical Infrastructure Protection*
FBI	*Federal Bureau of Investigation*
FIRST	*The Forum of Incident Response and Security Teams*
FISA	*Foreign Intelligence Surveillance Act*
G8	*Group of Eight*
IC	*Infrastructure critique*
IIC	*Infrastructure d'informations critiques*
I-OrBAC	*Integrity Organization Based Access Control*
ISO	*International Organization for Standardization*
IVP	*Integrity Verification Procedure*

MAC	*Mandatory Access Control*
MLCA	*Money Laundering Control Act*
MP6	*Modèles et Politiques de Sécurité pour les Systèmes d'Information et de Communication en Santé et Social*
NATO	*North Atlantic Treaty Organization*
NDHS	*National Department of Homeland Security*
NIPP	*National Infrastructure Protection Plan*
NPS	*National Preparedness System*
NSA	*National Security Agency*
NSL	*National security letter*
O2O	*Organization 2 Organization*
OECD	*Organization for Economic Co-operation and Development*
OrBAC	*Organization Based Access Control*
P2P	*Peer to Peer*
PAP	*Policy Administration Point*
PCCIP	*President's Commission on Critical Infrastructure Protection*
PCS	*Process Control System*
PDP	*Policy Decision Point*
PEP	*Policy Enforcement Point*
PIC	*Protection des Infrastructures Critiques*
PIIC	*Protection des Infrastructures d'Informations Critiques*
PIP	*Policy Information Point*
Poly-OrBAC	*Poly-Organization Based Access Control*
PS	*Politique de Sécurité*
QoS	*Quality of Service*
RBAC	*Role Based Access Control*
REA	*Role Enablement Authority*
RNRT	*Réseau National de Recherche en Télécommunications*
RSSO	*Role Single Sign On*
SCADA	*Supervisory Control And Data Acquisition*
SdF	*Sûreté de Fonctionnement*
SI	*Système d'information*

SLA	*Service Level Agreement*
SMSI	*Sommet Mondial sur la Société de l'Information*
SNRA	*Strategic National Risk Assessment*
SoD	*Separation of Duty*
SSA	*Sector-Specific Agency*
SSD	*Static Separation of Duty*
SSO	*Single-Sign-On*
TBAC	*Task Based Access Control*
TC	*Trust Class*
TIC	*Technologie de l'information et de la communication*
TMAC	*Team Based Access Control*
TP	*Transformation Procedure*
TOC	*Trust Organization Class*
TSC	*Trust Subject Class*
UDDI	*Universal Description Discovery and Integration*
UDI	*Unconstrained Data Items*
UE	*Union Européenne*
UN	*United Nations*
VEA	*View Enablement Authority*
VO	*Virtual Organization*
VPO	*Virtual Private Organization*
XACML	*eXtensible Access Control Markup Language*
XML	*eXtensible Markup Language*

INTRODUCTION GÉNÉRALE

SOMMAIRE

1. Contexte de la thèse

Les infrastructures critiques : définition et propriétés

A l'heure actuelle, nos vies dépendent d'infrastructures qui satisfont certains de nos besoins de première nécessité : approvisionnement en eau, en électricité, soins médicaux, etc. Ces infrastructures sont jugées « *critiques* » en raison du rôle vital qu'elles jouent, aussi bien pour assurer la stabilité et le développement des nations que pour garantir le confort des citoyens. Ces « *Infrastructures Critiques* » (IC) sont définies comme « *les systèmes, actifs et réseaux, physiques ou virtuels, tellement vitaux pour une nation que leur incapacité ou destruction aurait un impact débilitant sur la sécurité, la sécurité économique du pays, la santé ou la sûreté publique, ou toute combinaison de ces secteurs* » [1]. Vu leur importance, elles peuvent, à tout instant, être victimes de dysfonctionnements causés par quelconque source de malveillance [2, 3, 4] ou d'inadvertance [5, 6], infligeant des pertes financières considérables [7] et menaçant la stabilité du pays [8]. Veiller à leur bon fonctionnement requiert l'élaboration et l'application de multiples programmes et activités, connus sous le nom de « *Protection des Infrastructures Critiques* » (PIC). L'objectif de la PIC consiste à garantir un niveau de sécurité acceptable aux IC afin de minimiser, voire d'éradiquer, les risques pouvant causer leur indisponibilité ou leur corruption. Pour cela, tous les aspects de la sécurité sont considérés, à savoir les aspects physique, technique, humain et organisationnel. Traiter ces aspects se concrétise par la mise en place de plu-

sieurs barrières de sécurité [9] ; chacune destinée à couvrir certains volets de la défense, principalement la *prévention*, la *protection* et la *récupération* [10]. Pour parfaire la conception, l'implémentation et l'imbrication de ces barrières, il est primordial de se focaliser sur les besoins et propriétés de ces IC [11, 12], entre autres, les besoins de sécurité, de *Sûreté de Fonctionnement* (SdF), etc., et leurs caractères complexe, interdépendant [13], etc.

Les IC et les Technologies de l'Information et de la communication (TIC)

Le renforcement des interdépendances entre IC est dû, en partie, à l'utilisation accrue des *technologies de l'information et de la communication* (TIC). Leur développement exponentiel, l'accroissement de leur potentiel d'inter-connectivité ainsi que l'utilisation effrénée d'Internet sont les principaux facteurs responsables de la métamorphose radicale des méthodes et des moyens utilisés jadis par les gouvernements, les organisations et les citoyens pour communiquer et exercer leurs métiers. Ne faisant pas l'exception, les IC se sont dotées de TIC et continuent inlassablement de s'armer de technologies de pointe. Des avantages, ces nouveaux outils en offrent énormément, ce qui les rend incontournables au fonctionnement des IC. Néanmoins, ces privilèges voilent une face cachée qui n'est pas sans dangers pour les IC ainsi que toutes les sphères qui en usent. En effet, elles sont à l'origine de nouvelles menaces, tant par les vulnérabilités qu'elles contiennent que par les nouvelles formes d'actes de sabotage pouvant émaner de partout à travers le monde – faisant fi des frontières géographiques – et ne nécessitant pas d'importants moyens pour leur exécution – des micro-ordinateurs souvent suffisent [4]. Les cibles de ces attaques sont les s*ystèmes d'information*[1] (SI) se trouvant au cœur des IC. Ces systèmes sont très généralement constitués d'un ensemble de sous-systèmes interconnectés, désignés, en jargon spécialisé, par l'appellation : « *Infrastructures d'Informations Critiques* » (IIC). Cette désignation s'explique par le fait que ces systèmes traitent des données et exécutent des processus vitaux pour le bon fonctionnement de leurs IC. Tout comme les IC, les IIC doivent aussi répondre à une multitude de contraintes conceptuelles et fonctionnelles [11, 12].

La sécurité des IIC

Dans son rapport, le président de la Commission Présidentielle américaine pour la Protection des Infrastructures Critiques (PCCIP) déclare clairement qu'une sécurité de l'information fragile ou insuffisante engendrerait des conséquences dévastatrices pour la nation [15]. Actuellement, une large communauté scientifique tente de développer des solutions qui réduiraient et maîtriseraient les risques de ces TIC. Cependant, l'accroissement perpétuel de leur potentiel d'interconnexion intensifie les interdépendances entre leurs dif-

[1] *Système d'information* : ensemble des moyens informatiques ayant pour finalité d'élaborer, de traiter, de stocker, d'acheminer, de présenter ou de détruire l'information [14].

férents usagers, dont les IIC, qui demeurent, entre autres, sous la menace de phénomènes de *cascade* – la défaillance d'une IIC entraînant la défaillance d'autres IIC – et d'*escalade* – des dysfonctionnements mineurs se combinant et engendrant des conséquences graves. Maints défis sont donc à relever pour bénéficier confortablement des bienfaits de ces TIC.

Assurer la sécurité des SI – d'un point de vue immunité[2] et non innocuité[3] – se décline à travers la garantie de trois propriétés principales : la *confidentialité*, l'*intégrité* et la *disponibilité*. Dans cet ordre, nous les définissons sommairement : la *confidentialité* d'une information est sa propriété de ne pas être révélée à des utilisateurs non autorisés à la connaître ; l'*intégrité* est sa propriété de ne pas être altérée et enfin la *disponibilité* est sa propriété d'être accessible lorsqu'un utilisateur autorisé la requiert [16]. Négligée durant des années au profit de la confidentialité [17], l'intégrité s'avère être une propriété primordiale. En effet, à quoi bon dissimuler un secret corrompu ? Ou encore, à quoi bon veiller à la disponibilité d'une information erronée ou d'un service défectueux ? Pour les IIC, cette propriété est incontournable puisqu'elles manipulent des informations devant nécessairement être correctes et génèrent, à l'issue de processus internes, des résultats devant être fiables.

Politique de sécurité et analyse de risque

Parfaire la conception et le déploiement d'une IIC est primordial pour toute IC, néanmoins, il est bien plus important de la sécuriser en vue de lui garantir un fonctionnement correct le plus longtemps possible. En réalité, tout SI s'accompagne d'une *Politique de Sécurité*[4] (PS) qui établit les règles régissant son utilisation. Ces règles décrivent les actions autorisées, interdites ou obligées pour chaque utilisateur. Protéger les ressources de l'IIC est certes primordial, le faire à un coût raisonnable serait une aubaine. Pour cela, il faut, d'une part, se concentrer sur les ressources les plus sensibles, celles dont la perte causerait de sérieux dommages à l'organisation. D'autre part, il convient d'identifier les éléments potentiellement menaçants pour la sécurité du système ainsi que les moyens et les failles qu'ils pourraient exploiter. Pour ne rien omettre, l'application des méthodes d'analyse de risques est fortement recommandée du fait de leurs démarches méthodologiques [10, 19, 20, 21]. Après avoir énuméré les ressources de l'organisation et leurs degrés de sensibilité ainsi que la liste des menaces et leurs dangers potentiels, les confronter

[2] *Sécurité-immunité* : Relative au concept « *security* », fait référence à la capacité d'un système à résister aux agressions physiques (incendies, …) ou logiques (erreurs de saisie, piratage, …) ou encore à sa capacité à préserver trois propriétés des informations qui sont, la confidentialité, l'intégrité et la disponibilité [16].
[3] *Sécurité-innocuité* : Relative au concept « *safety* », fait référence à la prévention des catastrophes, c'est-à-dire que les défaillances éventuelles ne provoqueront pas d'importants dégâts et que l'occurrence de défaillances graves est très peu probable (ex : domaine du transport aérien, les stations nucléaires) [16].
[4] *Politique de sécurité organisationnelle* : Ensemble de règles, de procédures, de codes de conduite ou de lignes directrices de sécurité imposées par une organisation pour son fonctionnement [18].

permettra de trier pertinemment les ressources les plus critiques. Seront identifiés, ensuite, de façon abstraite et organisationnelle, les objectifs de sécurité[5] nécessaires à leur protection ; lesquels seront traduits en exigences fonctionnelles[6] de sécurité devant être déployées afin d'assurer la protection voulue. Finalement, sur le plan concret, des composants fonctionnels[7] de sécurité implémenteront ces exigences pour contrer réellement les menaces.

Le contrôle d'accès : ligne de défense et modèles

Un objectif de sécurité est sans cesse identifié, il s'agit, sans doutes, du *contrôle d'accès* (CA). Cette ligne de défense, importante et incontournable, permet de se prémunir des menaces internes et externes. Il vise à limiter les actions auxquelles peuvent prétendre les utilisateurs légitimes d'un système [23]. Dans ce sens, il statue sur les requêtes d'accès émanant des utilisateurs : les acceptant avec ou sans contraintes, ou les refusant. Les décisions prises se conforment aux règles traduisant la PS de l'organisation, plus précisément sa politique de contrôle d'accès. Il agit ainsi directement sur les actions que peut réaliser l'utilisateur et aussi indirectement, en contrôlant les actions effectuées par les programmes opérant pour son compte. Le but ultime est de réduire au maximum l'occurrence d'actions illicites pouvant générer des failles ou causer des incidents au sein du système [23].

Utiliser des modèles de sécurité facilite aussi bien l'expression et l'abstraction des PS que leur administration, la détection et gestion automatique des conflits, etc. Ces modèles favorisent aussi la compréhension et la maîtrise de la complexité du système et contribuent aux processus de preuve et de vérification nécessaires pour placer une confiance élevée dans le système. Les premiers modèles de sécurité [24, 25, 26] faisaient intervenir un niveau d'abstraction pour exprimer les PS – le niveau d'abstraction natif, comprenant les *sujets*[8], les *objets*[9] et les *actions*[10] – ; la conception des PS était compliquée et leur administration fastidieuse. Par la suite, de nouveaux modèles [27, 28, 29] ont pallié ces limitations en introduisant les briques d'un deuxième niveau d'abstraction agrégeant les sujets,

[5] *Objectif de sécurité* : Déclaration de l'intention de contrer les menaces identifiées et/ou satisfaire des politiques de sécurité organisationnelles et/ou des hypothèses émises [18].
[6] *Exigences fonctionnelles de sécurité* : Elles décrivent le comportement de sécurité souhaité qui est attendu d'un système conformément aux objectifs de sécurité arrêtés par l'organisation. Ces exigences décrivent les propriétés de sécurité que les utilisateurs pourront détecter par interaction directe avec le système (i.e. entrées, sorties) ou par sa réponse aux différentes excitations [22].
[7] *Composants fonctionnels de sécurité* : Ils traduisent les exigences de sécurité destinées à contrer les menaces dans l'environnement opérationnel supposé du système et/ou à couvrir toutes les politiques de sécurité organisationnelles et les hypothèses identifiées [22].
[8] *Sujet* : Entité active d'un système réalisant des actions sur des objets [18]. Il désigne le plus souvent un utilisateur ou une application s'exécutant pour le compte d'un utilisateur [17].
[9] *Objet* : Entité passive d'un système contenant ou accueillant des informations, et sur lesquels les sujets peuvent réaliser des actions [18].
[10] *Action* : Type spécifique d'opération réalisé par un sujet sur un objet [18].

les objets et les actions, respectivement, dans des *rôles*, des *vues* et des *tâches*. D'autres modèles ont facilité l'expression des PS en intégrant les notions d'obligations [30] et d'interdictions [31] pour mieux exprimer les exceptions. Un modèle en revanche, OrBAC [32, 33], conjugue tous les concepts précités, outre les contextes, les obligations, les interdictions et introduit la notion de recommandation, autour du concept de l'*organisation*. OrBAC satisfait bon nombre de besoins des IIC vu qu'il a été conçu dans le cadre d'un projet RNRT intitulé MP6[11] visant à tenir compte des contraintes liées au secteur de la santé pour développer des modèles de sécurité répondant à ses exigences. Nous montrerons dans ce rapport que malgré ses avantages, OrBAC ne couvre pas tous les besoins de sécurité des IC, notamment les besoins d'intégrité et de collaboration.

Les IC et le besoin de collaborer

Dans un contexte de mondialisation et d'ouverture, il est inconcevable que les IC puissent évoluer à l'écart de leurs environnements extérieurs. Ces interactions visent principalement à fournir des services ou à en bénéficier. Collaborer sous-entend la conjugaison d'efforts pour réaliser des objectifs qui satisfont les intérêts communs ou complémentaires des partenaires. Cela présente des risques puisque les parties fournissent leurs propres ressources au profit de la collaboration, ce qui n'exclut pas d'éventuelles tentatives de sabotage. Pour ainsi dire, les problèmes de sécurité ne se limitent plus uniquement au périmètre local de l'organisation, au contraire, ils dépendent désormais de nouveaux facteurs relatifs aux partenaires. Pour réduire ces risques tout en régissant ces coopérations, les contrats électroniques sont très souvent sollicités [34]. Ils visent, d'une part, à définir le contexte, les clauses ainsi que les activités à réaliser et servent, d'autre part, à prévenir l'occurrence de litiges et à les résoudre. De nouveau, les TIC facilitent et accroissent grandement l'efficacité des collaborations, néanmoins, leurs failles font courir aux organisations de grands risques. Il est donc primordial d'assurer aux IC une pleine protection tout au long de leurs collaborations pour satisfaire leurs importants besoins en matière de sécurité.

2. Contributions

Durant cette thèse, nous avons proposé des solutions pour pallier certains problèmes auxquels sont confrontés les IIC. Brièvement, nous énumérons ces contributions :

Proposition d'un modèle de contrôle d'accès tenant compte de contraintes liées à l'intégrité : Le bon fonctionnement des IIC est tributaire de l'intégrité de leurs services et ressources. Dans ce sens, nous proposons un modèle de contrôle d'accès tenant compte

[11] MP6 : MPSSICSS – *Modèles et Politiques de Sécurité des Systèmes d'Information et de Communication en Santé et Social*)

de contraintes tirées de la réalité des IIC – contraintes de *criticité* et de *crédibilité* – pour statuer sur les requêtes d'accès. Les PS exprimées grâce à I-OrBAC reflètent les besoins des ressources passives et apprécient, à leur juste valeur, les habilitations des agents.

Modélisation en niveaux d'intégrité : Pilier des programmes de PIC, la priorisation des biens sensibles figure parmi les points forts de notre modélisation. Les niveaux d'intégrité permettront de restreindre les accès afin de s'assurer que seuls des utilisateurs chevronnés accéderont aux biens sensibles. Aussi avons-nous proposé un moyen pour accroître et dégrader les niveaux d'intégrité des sujets, en accord avec leur comportement.

Les niveaux d'intégrité au service de la flexibilité : Soucieux de répondre au besoin de flexibilité lors de l'attribution des privilèges d'accès, nous avons proposé un moyen qui, tenant compte des spécificités du métier de l'organisation, permet d'établir une hiérarchie de rôles pour réaliser une tâche donnée. Les rôles de la hiérarchie seront soumis à des contraintes différentes (seuils différents) pour réaliser ladite tâche.

Un modèle proactif : Dans le contexte des IIC, un modèle restreint à statuer sur les requêtes d'accès serait quelque peu limitatif. Pour cette raison, I-OrBAC se veut proactif vu qu'il cherchera à déterminer le sujet le plus adéquat parmi les rôles retenus pour la réalisation d'une tâche, sans attendre que les sujets n'en fassent la requête. L'algorithme permettant cette pro-activité est décrit par un système d'inférence.

Une implémentation d'I-OrBAC : Nous avons proposé une implémentation de notre modèle dans le cadre d'une étude de cas tiré du projet européen FP7 CRUTIAL relatif aux réseaux de transport et de distribution d'énergie électrique.

Proposition d'une extension d'I-OrBAC pour les environnements distribués : Pour pallier les problèmes issus des collaborations, nous avons enrichi I-OrBAC de moyens permettant d'optimiser le choix des partenaires et avons intégré les contrats électroniques, dans le cadre de l'extension *Distributed I-OrBAC* (DI-OrBAC). Nous avons dû concevoir des mécanismes adaptés à I-OrBAC pour négocier lesdits contrats correctement.

3. Organisation du mémoire

Les contributions préalablement évoquées seront détaillées, tout au long de ce mémoire, selon le plan exposé dans la Fig. 1, qui se présente comme suit :

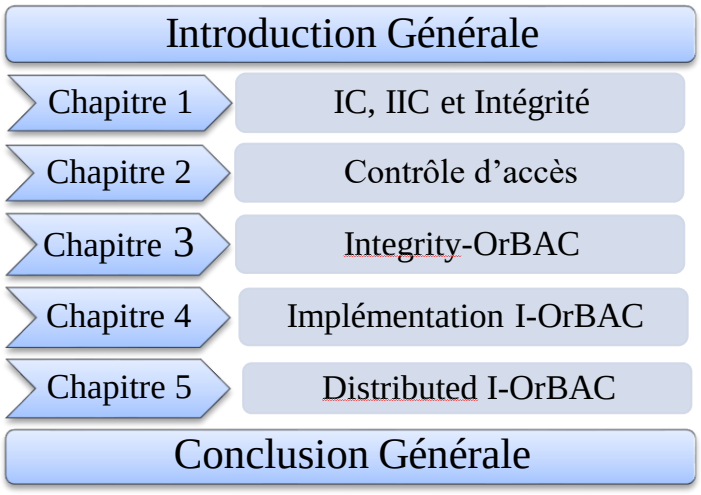

Fig. 1. Plan du mémoire

Le premier chapitre présentera, en détails, les notions d'IC et de PIC. Nous rappellerons certains événements à l'origine des principaux changements en matière de législations et de programmes de PIC. Nous exposerons deux approches, l'une nationale et l'autre internationale, d'efforts en matière de PIC. Nous aborderons l'importance des IIC dans le rayonnement des IC, en faisant état de certains problèmes auxquels elles sont confrontées. Puis, nous expliciterons l'importance de la gestion des risques dans le domaine de la PIC, en faisant état de certains défis devant être relevés pour une meilleure protection. Ensuite, une liste détaillée de leurs propriétés et besoins est présentée, puisque tout effort de protection serait vain sans la prise en compte de ces caractéristiques. Nous nous focaliserons enfin sur l'importance de la propriété d'intégrité dans le cas des IIC tout en présentant certains principes et mécanismes permettant de la fournir.

Le deuxième chapitre sera lui axé sur le contrôle d'accès et son importance dans la garantie de la sécurité du SI. Nous en rappellerons les fondements ainsi que les mécanismes auxquels il doit être couplé pour en optimiser les performances. Nous présenterons EBIOS, une méthode de gestion des risques, qui permet de parfaire l'expression des PS. Puis, nous établirons un état de l'art couvrant certains modèles classiques et certaines de leurs extensions, en étudiant leurs forces et faiblesses. Nous nous intéresserons aussi aux modèles d'intégrité et aux modèles collaboratifs. Pour clore ce chapitre, nous énumérerons les forces d'OrBAC et présenteront ses limitations quant à la prise en compte de l'intégrité.

Le troisième chapitre détaillera le modèle Integrity-OrBAC (I-OrBAC) proposé pour tenir compte des contraintes d'intégrité dans la décision de contrôle d'accès. Nous commencerons par les motivations de l'approche que nous proposons, puis, nous établirons une terminologie adaptée aux déclinaisons de l'intégrité dans le contexte des IIC. Nous définirons l'intégrité selon les différentes entités d'OrBAC. L'imbrication de la modélisa-

tion en niveaux à OrBAC sera présentée et seront justifiés les choix des entités qui se verront affecter les niveaux. Nous listerons par la suite les éléments d'I-OrBAC en explicitant la démarche de la prise de décision du contrôle d'accès. A titre explicatif, nous détaillerons un exemple aidant à l'assimilation du modèle tout en démontrant comment I-OrBAC permet aussi de mieux exprimer certains principes liés à la fourniture de l'intégrité. Aussi, proposerons-nous des moyens pour pallier la limitation des niveaux d'intégrité fixes : dans I-OrBAC les niveaux d'intégrité sont dynamiques et sont évalués tout au long de l'activité des sujets Enfin, nous révélerons comment I-OrBAC accroitra la flexibilité du contrôle d'accès en tenant compte de certaines caractéristiques propres au métier de l'organisation. Cette flexibilité sera traduite par un algorithme décrit par le biais d'un système d'inférence.

Dans le quatrième chapitre, nous présenterons les choix technologiques et les scénarios conçus pour tester l'implémentation du modèle que nous avons proposé. Nous présenterons brièvement les briques ainsi que les étapes de la prise de décision de contrôle d'accès proposées par le standard XACML, choisi comme base de notre implémentation en raison de ses divers avantages. Nous ajusterons la version 2.0 du standard afin de tenir compte de toutes les entités abstraites d'I-OrBAC, puis nous détaillons les nouvelles étapes de la prise de décision de contrôle d'accès pour les deux cas de figure : les requêtes normales et les requêtes proactives. Pour clore le chapitre, nous décrirons la plateforme adoptée pour mener les tests qui témoigneront du bon fonctionnement de notre modèle. L'implémentation de cette plateforme sera couplée à notre modèle et les requêtes émanant de la plateforme seront capturées et traitées conformément aux étapes détaillées plus tôt.

Le cinquième chapitre abordera les aspects liés à l'intégrité dans un environnement collaboratif distribué. Ainsi nous présenterons une extension d'I-OrBAC, intitulée Distributed I-OrBAC, qui vise la satisfaction de ces besoins. Cette extension se base sur le concept des « organisations virtuelles » (VO) pour mettre en place les collaborations. Au sein de ces VO, les ressources propres à chaque organisation seront manipulées conformément à un contrat conclu entre les parties. Afin de favoriser la réussite de ces collaborations, DI-OrBAC introduit un pseudo-protocole permettant aux organisations d'interroger leurs partenaires et de recueillir leurs jugements au sujet d'organisations potentiellement crédibles. Les jugements collectés permettront par la suite de calculer localement des niveaux de crédibilité relatifs aux organisations et à établir la carte des partenaires. Ainsi, ne seront sélectionnées que les organisations de confiance, avec lesquels seront négociés des contrats électroniques, dynamiquement, grâce à un langage enrichi d'I-OrBAC. L'enrichissement en question consiste en des prédicats permettant de tenir compte de l'aspect collaboratif. Les conflits pouvant survenir durant les différentes étapes de la négociation des contrats, sont résolus par des systèmes d'inférence.

CHAPITRE 1 :

IC, IIC ET INTÉGRITÉ

SOMMAIRE

I. 1. Préambule

Le présent chapitre vise deux principaux objectifs : (1) exposer, en détail une multitude de notions connexes aux domaines des IC, des IIC et de la PIC ; (2), mettre en exergue l'importance de la propriété d'intégrité dans le fonctionnement des IC et de leurs IIC. La première partie s'articule autour des axes suivants :

Nous commençons par définir les IC en exposant quelques conséquences résultant de leur indisponibilité pour mieux en apprécier l'importance. Puis, la notion de PIC est explicitée afin d'établir le contexte au sein duquel s'inscriront nos travaux. Nous enchainons par un bref rappel des principaux événements ayant conduit à l'intensification des efforts de PIC. Ces derniers se déclinent aussi bien à l'échelle des pays qu'à l'échelle internationale. Nous en étudions les caractéristiques en nous intéressant au modèle américain (le cas des activités nationales) et au modèle européen (le cas des activités internationales).

Par la suite, nous évoquons le rôle vital que jouent, de nos jours, les TIC dans la gestion et l'administration des activités propres aux IC, sans oublier d'exposer les inconvénients qui s'en suivent. Cependant, nous abordons un moyen favorisant la maitrise de ces dangers : la gestion des risques. Elle représente un pilier des programmes de PIC ; nous en rappelons les principes généraux en détaillant son application dans le cas de la PIC. Ensuite, nous énumérons quelques défis que doivent relever les programmes de PIC, à savoir, la délimitation pertinente du périmètre à protéger, la maitrise des interdépendances inter-IC, la maitrise de la diversité des menaces et enfin la réduction des vulnérabilités des IC.

Pour clôturer cette première partie, nous listons une série de propriétés et de besoins des IC et IIC, recueillis durant l'état de l'art. La prise en compte de ces caractéristiques est de mise car toute démarche sécuritaire les négligeant serait vaine.

La deuxième partie, quant à elle, traite de la propriété d'intégrité. Nous l'entamons par des définitions, puis nous illustrons son importance, dans le cas des IC, par des exemples ; pour finir sur un rappel de certains principes de sécurité visant à la garantir.

I. 2. Première partie : IC, IIC et PIC

I.2.1. IC et PIC : Contexte et définitions

Vu nos exigences en matière de confort, il nous est impensable de vivre sans électricité, sans services de santé, sans moyens de télécommunications ou encore sans moyens de locomotion. Nous sommes donc grandement dépendants d'infrastructures garantes de qualité de vie et de croissance économique. Pour preuve, une panne de courant durant une vingtaine de minutes occasionne une gêne considérable chez les citoyens et se répercute,

par exemple, chez un fabricant de circuits intégrés par un manque à gagner pouvant se chiffrer à 30 millions de dollars US [5]. Les, « *infrastructures critiques* » sont incontournables au développement des nations d'où les attentions particulières qu'elles suscitent puisqu'elles interviennent dans des secteurs comme la défense de l'unité nationale, les activités économiques, politiques et sociales ou encore la survie de l'état en cas de crise [35].

A ce jour, ni le sens ni le périmètre du terme IC ne font l'objet de définitions définitives. Au fil des années, ce terme s'est vu accordé une multitude de définitions et continue d'être au cœur de maints débats quant à celle à adopter en définitive [36]. A la lecture de diverses définitions leur ayant été accordées par différents états et organismes internationaux, toutes regroupées dans [37], nous constatons qu'elles évoquent communément la notion de « *biens matériels et immatériels vitaux à la stabilité et au développement des nations* ». Nous retenons celle du PATRIOT Act [1], loi antiterroriste votée par le Congrès américain suite aux attentats du 11/09/2001 [2]. La section 1016 (e) définit les IC comme « *les systèmes, les actifs et les réseaux, physiques ou virtuels, tellement vitaux pour une nation que leur incapacité ou leur destruction aurait un impact débilitant sur la sécurité, la sécurité économique du pays, la santé ou la sûreté publique, ou toute combinaison de ces secteurs* ». Une chose est sûre, ces installations nécessitent d'importants fonds tant pour les édifier que pour les faire fonctionner et les maintenir. Leur valeur n'en est pas moindre : par exemple, en l'an 2000 déjà, des analystes avaient estimé la valeur du réseau Nord-Américain d'électricité à plus de 800 milliards de dollars US. A l'époque, ce réseau comptait plus de 15 000 générateurs, installés dans 10 000 centrales, le tout raccordé aux usagers par des centaines de milliers de kilomètres de câbles. De plus, ces investissements sont conçus pour durer et sont liés à l'essor et à la croissance des nations : toujours en 2000, la valeur des activités de ladite compagnie, s'élevait à 358 milliards de dollars US [5]. Ceci dit, protéger ces IC revêt une dimension stratégique s'élevant au rang de priorité nationale.

Envisager les conséquences de leur dysfonctionnement suite à l'effet d'une quelconque menace, délibérée ou accidentelle, permet de mieux apprécier leur importance ainsi que les efforts déployés pour les protéger. En effet, un attentat cybernétique altérant les commandes d'installations chimiques ou de stations nucléaires causerait des pertes humaines et matérielles considérables. Autre illustration, une défaillance technique survenant au niveau d'installations électriques engendrerait, non seulement, une interruption de la distribution d'électricité mais paralyserait aussi les installations d'épuration et de distribution d'eaux ainsi que tous les secteurs dépendants d'électricité. Moins alarmantes sont les interruptions liées à la maintenance des IC, néanmoins, des précautions doivent être prises pour faire en sorte que ces interventions soient courtes, exceptionnelles, aisément gérables, géographiquement isolées et à faible impact sur les citoyens et les états [1, 38].

Prioriser la défense de ces installations remonte au début du 20ème siècle ; toutefois, les efforts de protection ne cessent de s'intensifier pour tenter de contenir l'actuelle croissance d'actes terroristes. Cette volonté se décline à travers les budgets colossaux – pouvant avoisiner les deux milliards de dollars US [39] – alloués à la recherche et au développement de nouvelles solutions pour réduire, voire éliminer, les vulnérabilités des IC ainsi qu'au financement des agences chargées d'élaborer des plans d'actions, de soumettre des projets de lois et d'assurer, sans relâche, leur protection sur le terrain. La PIC se définit telle « *les programmes et activités menés par les propriétaires d'infrastructures, les opérateurs, les fabricants, les usagers et les autorités réglementaires visant à maintenir la performance de l'IC au-dessus d'un niveau de service minimal défini, même en cas de pannes, d'attaques ou d'accidents et visant aussi à minimiser les efforts de récupération et les dommages* » [37]. Les démarches de PIC visent à élaborer des stratégies de protection qui définissent des niveaux de réactions appropriés aux différentes alertes et menaces recensées ainsi que celles anticipées. Concevoir des programmes couvrant un maximum d'événements indésirables exige l'instauration de partenariats propices au partage d'informations relatives aux menaces et aux vulnérabilités, entre les différentes parties concernées. Il en résultera ainsi une meilleure coopération dans l'élaboration des solutions et des plans d'intervention, qui sera renforcée par une meilleure coordination des actions de protection en cas de crise.

Cependant, protéger toutes les infrastructures d'un pays serait déraisonnable et entrainerait des dépenses aussi colossales qu'insensées. Par conséquent, cerner méthodologiquement le périmètre auquel s'appliqueront les programmes et les mesures de protection est de mise : ne doivent être retenus que les infrastructures dont l'indisponibilité ou la destruction causeraient des dommages catastrophiques à la nation. Pour ces raisons, les programmes de PIC ont beaucoup évolué depuis le tout-premier programme américain du genre. Jadis, ce dernier ne se focalisait, quantitativement, que sur les installations du secteur public, tandis que les programmes actuels incluent davantage d'infrastructures issues du secteur privé, notamment en raison des politiques de privatisation largement adoptées à travers le monde. Le secteur privé détient de plus en plus d'IC dans divers secteurs tels que les énergies, les services d'urgences, etc. Compte tenu de cette nouvelle situation, les propriétaires et exploitants de ces IC deviennent donc les premiers responsables de la gestion des risques au niveau de leurs établissements. Comme conséquence directe, le rôle des gouvernements devient plus restreint, consistant soit à imposer une régulation soit à coopérer avec les acteurs du secteur privé, voire parfois les deux conjointement [40]. La régulation, opérée par les gouvernements, exige des exploitants d'IC de mettre en place certains mécanismes de protection pour répondre à des normes et des standards éprouvés et reconnus. Les coopérations public-privé, quant à elles, visent plus à instaurer un climat de partage, sous couvert de confidentialité, favorisant des échanges constructifs sur les moyens

d'assimilation des besoins et des réponses en situation de crises. L'approche de la collaboration est largement adoptée de nos jours. Cette hausse des collaborations est en partie due au fait que les citoyens s'attendent à ce que les IC continuent de fonctionner indépendamment de la connaissance de leurs exploitants ; autrement dit, ils estiment que les états ont un rôle vital à jouer dans la PIC [40, 41]. Soulignons aussi que ces actions de PIC, censées être des initiatives nationales, revêtent progressivement un caractère international, puisqu'elles figurent sur les agendas de plusieurs organismes internationaux.

Qualitativement parlant, le périmètre de protection s'est nettement élargi au fil des décennies pour intégrer des secteurs et infrastructures ayant gagné de l'importance, tels que les télécommunications et les TIC. En effet, protéger ces deux secteurs ne figurait pas dans les premiers programmes de PIC de 1983 et 1988 ; ils ne furent intégrés qu'à partir, respectivement, de 1996 – l'*Executive Order* EO 13010 [42] – et 1998 – à la suite de la « *Presidential Decision Directive 63* » de Bill Clinton [43]. Le tableau (Tab. 18), en annexe, tiré de [36] et que nous avons soigneusement mis-à-jour après l'étude des deux référentiels publiés en 2009 [44] et en 2013 [45], illustre clairement cela. Une liste exhaustive de secteurs et infrastructures critiques est dressée par le Département de la Sécurité Intérieur américain (NDHS) dans le « *National Infrastructure Protection Plan* » (NIPP)[12] [45]. La figure (Fig. 2) ci-après expose les secteurs critiques recensés, en les répertoriant en quatre catégories : des infrastructures industrielles, d'autres chargées des services tertiaires, certaines responsables des divers approvisionnements – en eau, en énergie et en vivres – et enfin des infrastructures à caractères identitaires – tels que les monuments et les icônes.

I.2.2. Historique de la PIC : des actions nationales et internationales

Contrairement à ce que l'on pourrait penser, la notion de PIC naquit durant la 2ème guerre mondiale, lorsque certains pays se souciaient déjà du bon fonctionnement de leurs installations essentielles. Au milieu des années 80, elle commença à faire l'objet d'écrits et de programmes de protection mieux élaborés, plus structurés et surtout plus officiels [46]. Aux Etats Unis, pays pionnier en matière de législation relative à la PIC, les premiers programmes se concentraient uniquement sur les IC du secteur public. Face à l'accroissement de la menace terroriste au milieu des années 90, – plus particulièrement après les attentats perpétrés en 1993 contre le World Trade Center [47] et en 1995 à Oklahoma City [48] – le gouvernement américain a élargi le périmètre de définition de ce terme, incluant ainsi de nombreux nouveaux secteurs et autres infrastructures privées jugées critiques.

[12] *NIPP* : Document élaboré par le NDHS, visant à décrire les démarches adoptées par le gouvernement et ses collaborateurs du secteur privé pour assurer la sécurité des IC et à couvrir les risques qui pèsent dessus.

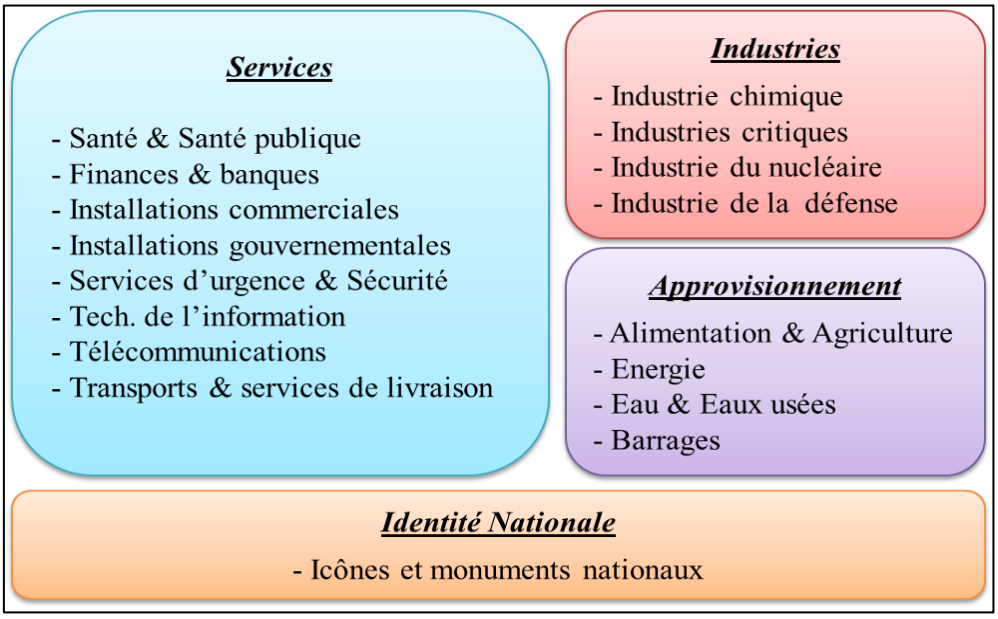

Fig. 2. Secteurs et IC recensés par le gouvernement américain.

Les attentats du 11/09/2001 demeurent, néanmoins, les événements ayant marqué un tournant dans la PIC : depuis, l'ampleur et l'intensité des démarches de PIC se sont accrues, notamment avec l'adoption de politiques drastiques à l'image du PATRIOT Act. Adoptée quelques jours seulement après les attentats comme un texte de loi temporaire, la loi a été renouvelée en 2006 et 2011 pour des raisons de sécurité nationale [49, 50]. Cette loi a amendé bien d'autres [51], telles que la « *Foreign Intelligence Surveillance Act* » (FISA) [52], l'« *Electronic Communications Privacy Act* » (ECPA) [53], la « *Money Laundering Control Act* » (MLCA) [54, 55] et la « *Bank Secrecy Act* » (BSA) [55]. Elle est vivement critiquée par des juristes et des organisations de défense des droits et libertés individuelles – telles que l'Union Américaine pour les Libertés Civiles (ACLU)[13] [56] et l'*Electronic Frontier Foundation* (EFF)[14][57] – qui la considère liberticide [58, 59, 60]. En effet, cette loi renforce énormément les pouvoirs des différentes agences gouvernementales de l'état (FBI, CIA, NSA, etc.) et de l'armée américaine à travers la détention sans limite et sans inculpation de toute personne soupçonnée de projet terroriste, l'accès aux données

[13] *American Civil Liberties Union* (ACLU) : Organisme américain pour la défense des droits et libertés individuelles des citoyens américains. L'ACLU s'implique dans diverses causes sociales parmi elle la protection de la vie privée des citoyens dans le monde du numérique [56].
[14] *Electronic Frontier Foundation* (EFF) : Organisme à but non lucratif, fondé en 1990, qui œuvre pour la défense des libertés civiles dans l'univers du numérique ; parmi ses préoccupations : la vie privée des utilisateurs, la liberté d'expression, l'analyse des politiques et le développement des technologies [57].

informatiques et la fouille de domiciles et bureaux sans même le consentement ni l'avis de leurs propriétaires ainsi que l'utilisation des lettres de sécurité nationale[15] (NSL).

I.2.2.1. Exemple d'actions nationales : le contexte américain

A la lumière du PATRIOT ACT, fut élaboré en 2006 [62], le NIPP, programme de PIC d'après 11/09/2001. Il fut mis-à-jour en 2009 [44] puis à nouveau en 2013 [45] à la suite de certaines directives [63, 64, 65] ayant souligné la nécessité de considérer la menace cybernétique en améliorant les aspects cyber-sécurité dans les programmes. La dernière version du NIPP liste seize secteurs critiques et affecte à la tête de chacun une agence ou un département fédéral, connus sous le nom d'« *agence spécifique à un secteur* » (SSA), pour coordonner les actions. Tous les programmes établis jusque-là déclarent que, pour garantir la sécurité et la résilience[16] des IC, les acteurs directs et indirects de ces installations doivent œuvrer collectivement à l'identification des priorités et à la formulation d'objectifs clairs, s'efforcer de limiter et d'atténuer les risques, évaluer sans cesse les progrès et l'efficacité des mesures déployées en les adaptant continuellement aux changements potentiels [45]. Pour ainsi dire, les démarches ci-avant évoquées reflètent fidèlement les briques du processus de gestion des risques, pierre angulaire des différentes versions du NIPP. De plus, le NIPP encourage l'instauration de partenariats favorisant les échanges d'informations entre les différentes sphères impliquées dans le processus de PIC, principalement, les propriétaires/exploitants des IC, les agences gouvernementales, les associations à but non lucratif et les acteurs du milieu académique. Dans ce qui suit, nous résumons trois des quatre principaux axes détaillés dans la dernière version du NIPP, l'axe portant sur la démarche de gestion de risques sera abordé plus loin en section (I.2.4.2).

I.2.2.1.1. Volets de la défense exigés

La communauté chargée d'appliquer le NIPP doit déployer ses efforts sur cinq fronts, exigés par « Système National de Préparation » (NPS) qui sont, la *prévention*, la *protection*, l'*atténuation*, la *réponse*, et le *recouvrement* [63] :

- La « *prévention* » fait référence aux mesures nécessaires pour éviter et prévenir l'occurrence d'incidents. Elles ont pour objectif de dissuader, d'anticiper, de réduire les failles etc. ; par exemple : l'échange d'informations et alertes; lutte contre le terrorisme interne; les activités de maintenance, etc.

[15] *Lettre de Sécurité Nationale* (NSL) : Procédure d'investigation extraordinaire conférant aux agences fédérales américaines le droit d'accéder et d'obtenir d'organismes, publics ou privés, toute information nominative à des fins de surveillance et sans la moindre supervision judiciaire [61].
[16] Résilience : Propriété d'adaptation face à l'évolution des conditions, de résistance et de récupération rapide à la suite de perturbations engendrées par des urgences [63].

- La « *protection* » renvoie aux moyens nécessaires pour sécuriser le pays contre les différents sinistres humains ou naturels. Il est question de détecter, de contrer et de contenir les sinistres en s'appuyant sur des techniques de détection, de lutte, de confinement, de réaction défensive, de résistance et de résilience, etc.
- L'« *atténuation* », quant à elle, fait référence aux mesures de minimisation de l'impact des catastrophes en limitant les pertes humaines et matérielles. Parmi ces mesures, nous citons, les projets communautaires pour la réduction impacts post-incidents, la réduction des risques causés par des phénomènes naturels, etc.
- La « *réponse* » traite, pour sa part, des capacités de réaction offensive à développer pour sauver des vies, protéger les biens et l'environnement, et répondre aux besoins fondamentaux des citoyens à la suite d'incidents.
- Le « *recouvrement* » se rapporte aux moyens de soutien aux collectivités sinistrées en vue d'une récupération prompte et correcte. Ces mesures tentent de ramener les systèmes à des états initiaux stables et sûrs grâce à des moyens de récupération, de restauration, de compensation etc.

I.2.2.1.2. Les sept principes du NIPP

Mettre en œuvre ces cinq facettes de la défense requiert des efforts devant aboutir à l'élaboration de solutions capables, non seulement, d'identifier, de prévenir, de détecter et de contrer les menaces qui pèsent sur les IC, mais aussi réduire les vulnérabilités de ces actifs ainsi que les impacts potentiels en cas de sinistres. Parallèlement à cela, ils doivent aussi apprécier pertinemment la criticité de toute sorte d'actifs, et déterminer adéquatement les interdépendances entre ces IC. Pour cela, sept principes fondamentaux les guident :

1. *Identifier et gérer les risques de manière globale et coordonnée pour allouer pertinemment les mesures de protection* : Cela nécessite le partage des bonnes pratiques et des informations relatives aux vulnérabilités et aux menaces pour optimiser le déploiement des mesures de sécurité et réduire les coûts et efforts.
2. *Apprécier et traiter les risques doivent tenir compte des dépendances intersectorielles pour améliorer le déploiement des mesures de sécurité et de résilience* : Pour réduire l'occurrence des phénomènes de cascade et d'escalade, les interactions inter-IC doivent être maitrisées – les informations partagées, les fonctions communes – afin d'identifier un maximum de risques à traiter.
3. *Partager les informations sur les risques et les interdépendances* : Les informations utiles sur les risques et les interdépendances, recueillies durant les activités des IC, doivent être partagées pour asseoir la sécurité et la résilience aux IC.

Des mesures juridiques appropriées, des partenariats de confiance et des technologies favorisant ce partage doivent être mis en place.

4. *Exploiter la diversité de la communauté des IC pour conforter l'approche partenariale* : Les IC étant de plus en plus exploitées par des acteurs privés, les partenariats public-privé sont incontournables à la sécurité et à la résilience des IC. Fructifier ces partenariats exigent de la confiance, des objectifs clairement définis, une évaluation des résultats, de la flexibilité et de l'adaptabilité.
5. *Instaurer des partenariats régionaux pour établir une vision commune sur les carences et les actions à adopter pour améliorer la PIC* : Les risques impactent avant tout les régions, imposant ainsi le déploiement de solutions à une échelle régionale, renforçant inéluctablement les efforts nationaux.
6. *Multiplier les conventions d'assistance mutuelles et les coopérations internationales et transfrontalières* : La nature distribuée et interconnectée des IC augmente leur complexité ainsi que le spectre des risques qui pèsent sur elles, le cas de risques outre-frontaliers. En effet, bien des IC bénéficient de services ou d'informations traitées et stockées dans des endroits géographiquement distants.
7. *Tenir compte de la sécurité et de la résilience durant la phase de conception des installations, des systèmes et des réseaux* : La conception des IC et de leurs composants doit se conformer à la propriété de maintenabilité[17], en envisageant tous les moyens permettant d'identifier, de détecter, et de contrer les menaces ainsi que réduire les vulnérabilités et atténuer les impacts.

I.2.2.1.3. Appel à action du NIPP

Le NIPP inclut un « *appel à l'action* » censé orienter les efforts de la communauté des IC pour améliorer la sécurité et la résilience à travers la réalisation de trois familles d'activités : (1) l'appui sur les efforts des partenariats; (2) l'innovation en matière de gestion des risques et (3) la focalisation sur les résultats. Par conséquent, les agences fédérales et autres acteurs des IC devront s'efforcer d'accomplir les tâches suivantes en tenant compte des priorités et contraintes propres à chaque secteur. La liste ci-dessous ne se veut pas exhaustive, de plus tous les secteurs n'auront pas à appliquer toutes les actions listées.

1) S'appuyer sur les efforts des partenariats :
   a) Identifier les priorités nationales à travers des efforts conjoints.
   b) Déterminer les actions collectives grâce à une planification conjointe.

[17] *Maintenabilité* : Aptitude d'un système à évoluer et à être réparé [33].

c) Habiliter les partenariats locaux et régionaux pour renforcer les capacités à l'échelle nationale.

d) Profiter des mesures incitatives pour promouvoir la sécurité et la résilience.

2) Innover en matière de gestion des risques :

a) Adopter une prise de décision éclairée basée sur la connaissance des risques à travers une appréciation améliorée des conjonctures.

b) Analyser les dépendances au sein de l'infrastructure, les interdépendances, et les effets en cascade associés.

c) Identifier, évaluer et répondre aux effets en cascade imprévus durant et post incidents.

d) Promouvoir les efforts de récupération régionaux à la suite d'incidents.

e) Renforcer le développement conjoint et coordonné ainsi que la fourniture d'assistance en matière de technique, de formation, et d'éducation

f) Améliorer la PIC en perfectionnant les recherches et développements.

3) Se focaliser sur les résultats :

a) Évaluer les progrès en vue de la réalisation des objectifs.

b) Assimiler et s'adapter durant et après les exercices et les incidents.

Protéger les secteurs et infrastructures critiques américains consomme énormément d'efforts et de ressources aussi bien humaine, technique que financière. En effet, cela ne se faisant pas sans frais, les Etats-Unis allouent des budgets colossaux à la PIC : en 2014, pas moins de 1,187 milliard de dollars US furent alloués au financement du programme de PIC et de la sécurité de l'information. Le détail de ces subventions est présenté dans le tableau (Tab. 17), en annexe [39]. Le NIPP est à ce jour une référence en matière de programme de PIC, bon nombre de pays s'en inspirent en adaptant ses briques à leurs contextes.

I.2.2.2. Exemple d'actions internationales : le modèle européen

A l'image des Etats-Unis, d'autres pays ont développé une dynamique visant à garantir le bon fonctionnement de leurs IC. Cependant, seuls les pays industrialisés sont les plus actifs dans ce domaine [37], en chargeant des agences des différents volets de la PIC [66]. Des attentats terroristes sur le continent européen – celui de la gare ferroviaire de Madrid [67] et celui contre le métro londonien [3] – justifient l'implication vigoureuse d'organismes intergouvernementaux dans la lutte pour la PIC – tel que le NATO, l'OECD, le G8, l'UE, le FIRST, l'UN et le WBG [37]. Ces institutions initient des programmes de

recherche pour identifier les IC, leurs vulnérabilités ainsi que leurs interdépendances afin de mieux les protéger. Ces démarches se concluent par l'élaboration de politiques et de programmes de protection [38] et par la publication de recommandations pratiques [68, 69]. Aussi ces organismes se fixent pour tâche de collaborer avec les états afin de les aider à compléter leurs stratégies de PIC en leur fournissant des éléments issus d'études réalisées à grande échelle, en coordonnant les partenariats internationaux et en instaurant des politiques et des mécanismes communautaires. Pour illustrer les actions de ces organismes, nous prenons comme exemple l'Union Européenne (UE), remarquablement active dans la lutte pour la PIC européenne. Suite à la déclaration du Conseil Européen pour la lutte contre le terrorisme [70], la Commission Européenne a émis des communications [41, 71, 72] annonçant l'élaboration d'un programme de lutte contre le terrorisme qui allait bien évidemment intégrer la PIC. Un an plus tard, fut présenté un livre vert exposant un « Programme Européen pour la Protection des Infrastructures Critiques » (EPCIP) [38]. Le livre propose, non seulement, de multiples scénarios pour l'instauration du programme et un réseau d'alertes concernant les IC européennes [73], mais il soulève aussi des questions incitant à la concertation dans le but de recueillir les avis et propositions des états membres afin de déterminer et sélectionner les principes, mesures et instruments pertinents à adopter. Ledit programme vise, entre autres, à identifier les IC, leurs vulnérabilités et interdépendances, à leur assurer des niveaux de sûreté suffisants et uniformes, à minimiser leurs défaillances et à fournir à l'UE des moyens éprouvés de réaction rapide.

Une chose est sure, protéger toutes les infrastructures européennes est chose impossible pour l'UE. Partant de ce fait, l'UE se focalise sur les infrastructures à caractère transnational et laisse les autres à la charge des états membres tout en veillant à appliquer un cadre de protection commun. Ce dernier sert à garantir que tous les états membres fournissent des niveaux de protection suffisants et uniformes à leurs IC ; sa mise en œuvre est simplifiée grâce aux actions entreprises par l'UE visant à recenser, échanger et diffuser les meilleures pratiques en matière de PIC. Ce livre introduit deux concept distincts, les « *Infrastructures Critiques Européennes* » (ICE) et les « *Infrastructures Critiques Nationales* » (ICN) à la lumière de la définition suivante : « *Les ICE incluent les ressources physiques, les services et installations propres aux technologies de l'information, les réseaux et les actifs d'infrastructures, dont l'interruption ou la destruction aurait un impact sérieux sur la santé, la sûreté, la sécurité, le bien-être économique ou social de deux états membres ou plus. La définition de ce qui constitue une infrastructure critique de l'UE est déterminée par son effet transfrontalier qui détermine si un incident pourrait avoir un impact sérieux au-delà de deux États membres ou plus de territoires nationaux d'états membres* » [38]. Les niveaux de protection ne seront certes pas les mêmes pour toutes les IC – cela dépendra d'évaluations se rapportant à la gravité des effets suite à la défaillance de chaque IC –, néanmoins le programme est pensé pour être évolutif, faisant l'objet de réexamens régu-

liers. Il est important de mentionner que même en donnant la priorité à la menace terroriste, l'UE n'écarte pas moins les risques pouvant résulter des catastrophes naturelles, des activités criminelles ou encore de toute présumée cause de sinistres. Les états membres devront identifier dans chaque secteur, les infrastructures considérées critiques sur leur territoire, selon une formule harmonisée au niveau de l'UE en collaboration avec la communauté chargée de la sécurité des IC. Suite aux débats, une communication de la Commission [74] détailla les principes, procédures et instruments adoptés pour la mise en œuvre de l'EPCIP. Après l'étude de ce dernier, cinq briques principales sont repérées :

(1). *Une procédure pour l'identification et la désignation des ICE* et une approche commune pour évaluer le besoin d'améliorer leur protection. Cette procédure se veut pluraliste puisqu'elle vise à tenir compte de toutes les menaces recensées, tout en accordant la priorité à la menace terroriste.

(2). *Des mesures visant à faciliter la mise en place de l'EPCIP*, parmi elles :

i. Un plan d'action, non seulement, pour établir les aspects stratégiques du programme et développer les mesures applicables à n'importe quel projet de PIC, mais aussi, pour élaborer une procédure de recensement et de classement des ICE ainsi que la conception et le déploiement de mécanismes de réduction des vulnérabilités. Pour cela, la Commission adopte une *approche sectorielle* qui considère les spécificités, contraintes et besoins de chaque secteur dans l'élaboration de protections sur mesure. La dimension nationale des états membres est un facteur clé du processus de protection puisque l'UE considère que la PIC demeure une responsabilité nationale. Ainsi, le plan d'action repose sur cinq principes clés qui sont : la *subsidiarité*[18], la *complémentarité*[19], la *confidentialité*[20], la *coopération des acteurs concernés*[21], l'*approche sectorielle* et enfin la *proportionnalité*[22].

[18] *Subsidiarité* : Principe basé sur le fait que la PIC est avant tout une responsabilité nationale et stipule que les états membres, les propriétaires ou exploitants d'IC doivent, en accord avec un cadre commun, prendre leurs propres décisions et adopter leurs propres plans de protection de leurs infrastructures [38].

[19] *Complémentarité* : Ce principe stipule que le cadre commun de l'EPCIP représente un complément des mesures existantes, autrement dit, les mesures communautaires déjà en place devraient continuer à être utilisées participant ainsi à la mise en œuvre globale de l'EPCIP [38].

[20] *Confidentialité* : Ce principe stipule que les échanges d'informations concernant la PIC se dérouleront dans un climat de confiance et dans le respect de la confidentialité. Dans ce sens, les informations seront classifiées et leur manipulation respectera le principe du « *besoin d'en connaître* » [38].

[21] *Coopération des acteurs concernés* : Les acteurs concernés, à savoir les états membres, la Commission, les associations professionnelles et sectorielles, les organismes de normalisation, les propriétaires et les exploitants doivent tous coopérer et contribuer à la mise en œuvre de l'EPCIP en fonction de leurs rôles respectifs et des responsabilités qui leur incombent [38].

[22] *Proportionnalité* : Les stratégies et les mesures de protection doivent être proportionnées au niveau de risque évalué par des techniques appropriées de gestion de risques [38].

ii. Mise en place, au sein de l'UE, de groupes d'experts en PIC pour chaque secteur. Ils aideront aussi bien, à l'identification des vulnérabilités, des interdépendances et des meilleures pratiques liées aux secteurs, qu'au développement de mesures visant à pallier ces vulnérabilités et des métriques pour évaluer les performances. Ces experts seront des points de contact favorisant la coordination des actions et des coopérations stratégiques.

iii. « *Critical Infrastructure Warning Information Network* » (CIWIN) [73] est un réseau à double fonction : (1) un système d'alerte rapide permettant aux états membres et à la Commission de signaler les menaces et les risques pesant sur les IC ; (2) un forum électronique pour encourager et faciliter le partage d'informations au sujet des vulnérabilités, des interdépendances ainsi qu'au sujet des stratégies et des bonnes pratiques. Bien entendu, les échanges s'opèrent de façon sécurisée de sorte à préserver la sécurité-immunité des données ; puis il incombe aux états membres de les communiquer aux agences concernés.

(3). *Le soutien aux états de l'Union* : l'UE assiste ses états membres dans la protection de leurs ICN pouvant optionnellement être utilisées par d'autres états et s'active aussi à concevoir et à mettre en place des plans d'intervention Les états, à leur tour, assistent les propriétaires et exploitants d'IC, premiers responsables de la gestion des risques au sein de leurs installations.

(4). *Une dimension externe* : l'UE renforce ses coopérations internationales en matière de partage d'informations concernant les dépendances externes dans la mesure où le dysfonctionnement de certaines IC externes à l'UE peut l'impacter et vice-versa. Notons toutefois que ces échanges avec l'extérieur se limitent pour l'instant au partage de bonnes pratiques avec les Etats-Unis.

(5). *L'accompagnement des mesures financières* : Dans le cadre d'un projet pilote (2005-2006), la Commission accorda un budget de 7 millions d'euros pour financer des mesures de prévention, de préparation et de réponse contre les attaques terroristes. Puis, la Commission a alloué pas moins de 140 millions d'euros (2007-2013) au programme « *Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks* » (CIPS) [38, 75] destiné au recensement des besoins en matière de sécurité et à l'élaboration de normes techniques communes pour la PIC. De plus, depuis 2007, plus de soixante projets liés, de près ou de loin, à la PIC furent élaborés.

Un autre point important est abordé dans le programme, celui de la collaboration public-privé. Ce point est repris dans la directive 2008/114/CE [76] qui établit une procédure cadre pour l'identification et la désignation des ICE. Cette directive ainsi que le pro-

gramme EPCIP furent tous deux révisés en 2012. En définitive, mentionnons que les différentes démarches et publications de la Commission Européenne évoquent, sans exception, l'importance de l'intégration des TIC dans les programmes de PIC notamment en raison de leur rôle primordial dans le bon fonctionnement des IC [70]. Dans ce sens, des budgets considérables sont alloués à la recherche en matière de sécurité en général et de sécurité des TIC en particulier. Pour exemple, le montant total des crédits en 2004 et 2005 s'élevait à 30 millions d'euros ; en 2006, la Commission proposa un montant de 24 millions d'euros. Au titre du 7ème programme-cadre, la Commission proposa pour les activités de recherche liées à la sécurité et à l'espace, en coopération, le budget de 3,96 milliards d'euros [77].

I.2.3. IC et IIC

Loin des attentats terroristes nécessitant une préparation de longue haleine, une logistique parfaite et des armes de destruction ; d'autres menaces guettent les IC et s'avèrent aussi graves en conséquences. En effet, l'horizon des menaces s'est élargi depuis que les TIC se sont incrustées dans la quasi-totalité des secteurs et institutions de notre quotidien. Ne faisant pas l'exception, les IC accueillent une panoplie de TIC qui constitue désormais un point névralgique de leur fonctionnement. L'adoption rapide et inconditionnée de ces outils est due aux différents services qu'ils offrent, à commencer par l'utilisation du protocole IP, puissant moyen de communication, en passant par l'accès à Internet qui permet de concevoir et de déployer toute sorte de services à forte valeur ajoutée, sans oublier les moyens de géolocalisation et de radionavigation par satellite, etc. De plus, ces technologies sont à l'origine d'une multitude d'avantages alliant rapidité, disponibilité, fiabilité et efficacité des communications et des processus métiers ; autant de facteurs favorisant considérablement la gestion et l'administration des processus propres aux IC. Aussi, ces technologies accroissent la productivité, améliorent la qualité des produits et services, réduisent les délais et les coûts et optimisent aussi les collaborations pour tirer le meilleur profit des partenaires. Les SI sont l'ensemble des matériels et logiciels destinés à élaborer, traiter, stocker, acheminer, présenter ou détruire l'information [14]. Ayant des besoins délicats, les IC déploient des SI complexes, interconnectant maints sous-systèmes. Pour les IC, ces SI sont désignés par l'appellation : « *Infrastructures d'Informations Critiques* » (IIC) ; celle-ci se rapporte à deux principaux facteurs : (1) soit ces technologies sont l'essence même de secteurs critiques tels que les télécommunications et les TIC, (2) soit elles sont essentielles au bon fonctionnement d'autres IC, comme c'est le cas de tous les autres secteurs critiques [38]. La compromission ou destruction de ces IIC porterait préjudice au bon fonctionnement des IC, impactant inévitablement la stabilité et le développement des états [4, 8].

Malheureusement, cette révolution numérique n'est pas sans dangers, non pas seulement pour les IC, mais pour toute personne ou organisation qui en use. L'interconnexion grandissante qu'offre ces outils, introduit de nouveaux risques tant par les vulnérabilités

qu'ils comportent que par la multitude de nouvelles formes de corruption qui en visent les brèches et qui peuvent émaner de partout à travers le monde sans nécessiter d'importants moyens pour leur exécution. Actuellement, tout le tissu social, économique et politique dépend fortement d'informations et de services en réseau, rendant ainsi toute la nation vulnérable. De plus, l'utilisation abondante des TIC ainsi que la démocratisation de l'accès à l'information amenuisent nettement les capacités de contrôle des états sur les informations que consultent leurs citoyens, fragilisant ainsi les régimes. Autre point négatif, la profusion et la sophistication des méthodes d'attaques rendent difficile la localisation et le pistage des attaquants. Sans oublier non plus le bouleversement actuel des critères conventionnels des guerres, puisque la force des états ne se mesure plus seulement à la force de leurs armées mais aussi en fonction de la maitrise des TIC [4, 8, 35]. Ceci dit, les IC se retrouvent aussi vulnérables que tout autre système connecté, à la différence que leurs dysfonctionnements ne sont pas tolérés en raison des impacts dramatiques engendrés. L'infortune est, qu'en plus des vulnérabilités « *physique* » que redoutaient les IC, voilà que s'ajoutent les failles « *logicielles* » de ces technologies, favorisant l'occurrence d'attaques de type électronique et radio. Plus grave encore, l'exploitation des unes n'exclue pas l'exploitation conjointe des autres, en effet, les cyber-attaques peuvent être couplées à des attaques terroristes physiques. Pour exemple, un attentat terroriste à la bombe combiné à cyber-attentat visant le réseau de distribution de l'électricité ou encore celui des télécommunications ; les dégâts n'en seront que plus catastrophiques [41]. En général, ces menaces peuvent compromettre la *sécurité-immunité* – à savoir l'intégrité, la confidentialité ou la disponibilité – des données et services de ces IC ; tout comme elles peuvent mettre en défaut d'autres propriétés propres à la *sûreté de fonctionnement* telles que la « *sécurité-innocuité* » – propriété incontournable dans les secteurs à hauts risques tel que l'industrie du nucléaire ou encore l'aviation civile – et ainsi causer des pertes humaines et financières catastrophiques.

Conscients de l'importance de l'information numérique à notre ère, tous les organismes internationaux insistent sur la nécessité de promouvoir une culture orientée sécurité. Ce fut exprimé lors de maints événements internationaux ainsi qu'au travers de nombreuses déclarations, résolutions, engagements [78] et plans d'action [79]. A titre illustratif, la déclaration de Principes du Sommet Mondial sur la Société de l'Information (SMSI) [80] ainsi que des résolutions des Nations Unies [81, 82] stipulent qu'une culture mondiale de la cyber-sécurité est une condition préalable pour le développement de la société de l'information ainsi que pour instaurer la confiance parmi les utilisateurs des TIC. Pour sa part, l'UE insiste sur la nécessité d'optimiser l'efficacité des SI [70] et de renforcer les actions de recherche scientifique en matière de sécurité, particulièrement de cyber sécurité, pour accompagner convenablement le développement de l'*économie numérique* [71].

Tout comme existe la notion de PIC, la notion de « *Protection des Infrastructures d'Information Critiques* » (PIIC) existe aussi. Elle est définie comme « *les programmes et les activités menés par les propriétaires d'infrastructures, les exploitants, les fabricants, les utilisateurs et les autorités de réglementation visant à maintenir les performances des infrastructures d'informations critiques au-dessus d'un niveau minimum de services défini et à réduire le temps de recouvrement et les dommages, en cas de pannes, d'attaques ou d'accidents* » [38]. Notons que la PIC et la PIIC sont plus complémentaires que concurrentes puisque la PIIC est une composante de la PIC. La différence réside dans le fait que la PIC s'intéresse à tous les secteurs et infrastructures critiques tandis que la PIIC se focalise sur les IIC [37]. Ces programmes ont, dans l'absolue, deux principaux buts [35] :

- Tout d'abord, fournir un service de protection courant, servant à contrer les menaces d'un niveau d'hostilité normal – pannes imprévues, phénomènes naturels, vandalisme électronique ou encore activités criminelles de petite envergure. Ce niveau de protection garantit le fonctionnement correct des services du quotidien, tels que l'*e-business*, l'*e-governement*, etc. A ce niveau, il est d'usage de s'appuyer sur des programmes de sensibilisation, des mécanismes d'assurance, une législation relative à la cryptographie et à l'authentification, des contrôles cybernétiques et un arsenal juridique adéquat pour réprimer les cas d'abus.
- Un second niveau plus avancé, garantissant une protection contre des attaques de plus grande envergure, celles perpétrées par des activistes politiques déterminés, des cellules terroristes, ou par des états hostiles.

Qu'il s'agisse de PIC en général, ou de PIIC en particulier, des études méthodiques et rigoureuses devront être menées en vue d'identifier méticuleusement les objectifs cibles garantissant l'atteinte des deux buts cités ci-avant pour réduire les risques qui pèsent sur les IC. En définitive, nul effort permettant de les réaliser ne doit être ménagé. Dans ce qui suit, nous dressons une liste non exhaustive de ces objectifs.

I.2.4. Fondement de la PIC : la gestion des risques au profit de la PIC

I.2.4.1. Présentation du concept de l'analyse de risques

Aussi bien dans l'EPCIP que dans le NIPP, il est clairement soutenu que la sécurité et la résilience des IC sont grandement renforcées par l'application d'un processus de gestion des risques [45]. La notion de risque se rapporte à « *l'éventuelle occurrence de conséquences non désirées suite à un incident ou sinistre et qui est déterminée par sa probabilité [qui dépend des menaces et des vulnérabilités] et par les impacts engendrés* » [83]. Gérer les risques se définit comme le « *processus permettant d'identifier, d'analyser et de communiquer sur les risques tout en les traitant soit en les acceptant, en les évitant, en les*

transférant ou en les contrôlant à un niveau acceptable et à un coût acceptable » [83]. Gérer les risques n'est pas un concept nouveau, il fut conçu dans le cadre du domaine financier pendant les années 50. S'intégrant aux processus organisationnels et de prise de décision, la gestion des risques est une démarche participative, dynamique, itérative et réactive aux changements s'appuyant sur les données réelles des organisations pour rationaliser leurs conjonctures, les menant vers une prise de décision plus éclairée. Grâce à cela, les organisations ont pu, entre autres, intégrer et considérer des paramètres moins objectifs (facteurs humains et culturels), créer de la valeur et améliorer les stratégies [84]. Par conséquent, ce concept fut adopté et adapté par la suite à de nombreux autres domaines tels que la gestion de projet, la *SdF*, la sécurité de l'information, etc. [10]. Il existe donc un grand nombre de méthodes d'analyse de risques, certaines conçues pour des domaines et des applications particulières [10, 19], tandis que d'autres sont plus générales [85]. Malgré la pluralité actuelle des méthodes de gestion des risques, il est facile de repérer les principes fondamentaux communs à toutes ces démarches, lesquels sont décrits dans des normes internationales tel que le guide 73 de l'ISO [86]. Les étapes du processus de gestion des risques y sont énumérées, à savoir, tout d'abord l'étude du contexte, puis les étapes de l'appréciation des risques, de leur traitement et de la validation dudit traitement, pour aboutir aux étapes de la communication relative aux risques et du contrôle continu de l'efficacité des mesures entreprises. Dans l'absolu, les étapes d'appréciation et de traitement des risques consistent, en premier lieu, à identifier les biens sensibles à protéger, à déterminer leurs vulnérabilités ainsi que les éléments pouvant menacer leur sécurité, à combiner menaces et vulnérabilités pour énumérer les scénarios de risques pertinents puis d'en évaluer les impacts potentiels. Par la suite, des actions visant à réduire les risques à des niveaux acceptables doivent être entreprises. Dans ce qui suit, nous aborderons la gestion des risques appliquée aux IC en décrivant la démarche adoptée dans le NIPP [45].

I.2.4.2.Analyse des risques pour les IC

La gestion des risques est le fondement même du programme NIPP. Elle fournit les moyens de se focaliser sur les menaces susceptibles de causer des dégâts catastrophiques et emploie des approches visant à prévenir et à atténuer les impacts. Elle permet également d'accroître la sécurité et la résilience par le biais de l'identification et de la priorisation des actions nécessaires à la garantie de la continuité des fonctions et des services essentiels et de favoriser les activités de réponse et de restauration adaptées. Considérons le cadriciel de gestion des risques du NIPP (Fig. 3) et décrivons brièvement la démarche adoptée :

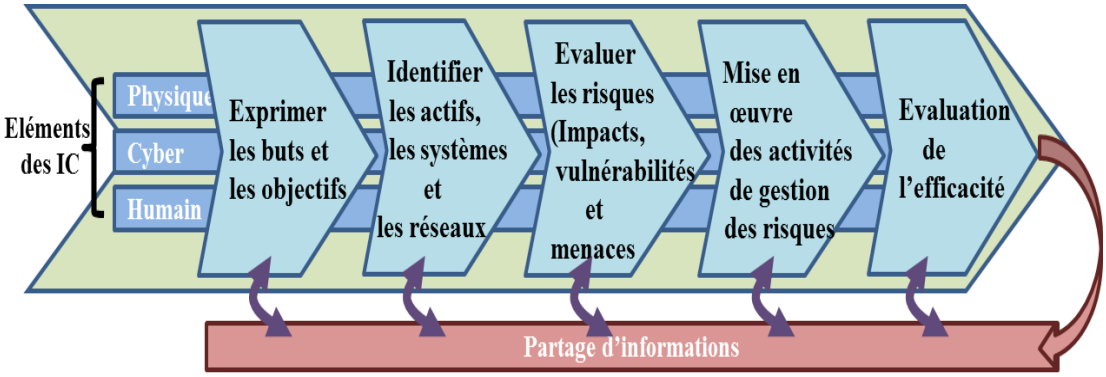

Fig. 3. Etapes du processus de gestion des risques du NIPP.

1) *Expression des buts et des objectifs* : Le NIPP établit une liste d'objectifs nationaux pour la sécurité et la résilience des IC. Ils se déclinent au travers de priorités identifiées au niveau sectoriel et exprimées dans les « plans sectoriels spécifiques » (SSP) servant de bases à la planification entre les SSA et leurs partenaires. Les exploitants d'IC et les entités régionales peuvent aussi identifier des priorités pour leurs IC. Ces priorités présentent l'avantage de refléter les spécificités opérationnelles, toutefois, elles doivent se conformer aux objectifs nationaux et aux priorités du secteur.

2) *Identification des actifs, systèmes, réseaux et fonctions* : Le gouvernement fédéral identifie et priorise les IC à l'échelle nationale. Notons que les acteurs des IC aperçoivent la criticité différemment, selon leurs conditions singulières, leurs modèles d'exploitation, et les risques auxquels ils font face. Cependant, pour gérer efficacement les risques, ces acteurs doivent identifier les actifs, systèmes et réseaux essentiels à la continuité de leur fonctionnement, en considérant les interdépendances.

3) *Evaluation des risques (impacts, vulnérabilités et menaces)* : L'évaluation des risques est menée conjointement par l'exploitant de l'IC et certains de ses partenaires en utilisant des méthodes. Concrètement, les risques se mesurent en termes de menace[23], de vulnérabilité[24] et d'impact[25]. Ces évaluations permettent aux dirigeants d'IC de mieux apprécier les incidents les plus probables et les plus graves pouvant affecter leurs IC en vue d''allouer les ressources de manière pertinente.

4) *Mise en œuvre des activités de gestion des risques* : Celles-ci sont adoptées et priorisées sur la base du degré de criticité de l'infrastructure, du coût de l'activité et de

[23] *Menace* : Phénomène d'origine naturel ou humaine, individu, entité ou action, présentant un potentiel danger à la vie, à l'information, aux fonctions, à l'environnement et/ou propriétés [45].
[24] *Vulnérabilité* : Caractéristique physique ou attribut fonctionnel qui rend une entité accessible à l'exploitation ou exposée à un certain risque [45].
[25] *Impact* : Conséquence directe ou indirecte suite à l'effet d'un incident ou d'un sinistre [45].

la gravité des impacts potentiels. Ces activités peuvent être répertoriées selon différentes approches ; pour chaque approche, nous mentionnerons certains exemples :

a) Approche d'identification, de dissuasion, de détection et de préparation pour prévenir les menaces potentielles (prévention) :
   - Etablir des processus d'évaluations des améliorations nécessaires en matière de sécurité et de résilience, conformément aux alertes et rapports.
   - Effectuer un suivi permanent des systèmes informatiques.
   - Mettre en place des systèmes de protection pour détecter ou retarder les activités malveillantes qui menacent l'IC.

b) Approche de réduction des vulnérabilités (protection) :
   - Intégrer les contraintes de sécurité et de résilience aussi bien durant la conception que l'exploitation des actifs, des systèmes et des réseaux.
   - Tenir compte de considérations géologiques lors de l'implantation des nouvelles IC, telles que les plaines inondables, les zones sismiques, etc.
   - Promouvoir des formations favorisant la sensibilisation et l'assimilation des vulnérabilités communes et les stratégies d'atténuation possibles.

c) Approche d'atténuation des conséquences (réponse et recouvrement)
   - Restauration des activités des IC à la suite d'incidents et à la garantie d'un approvisionnement continu en services essentiels (groupes électrogènes, stocks de carburants, moyens de communications mobiles, etc.).
   - Exécuter les activités de redondance en sauvegardant les informations essentielles sur des serveurs distants.
   - Retirer les opérations critiques du réseau Internet, réduisant ainsi les compromissions des services essentiels.

5) Evaluation de l'efficacité pour des rétroactions correctives permanentes dans le cadre d'une approche flexible.

Pour évaluer l'efficacité des efforts de gestion des risques, la communauté des IC se base sur des indicateurs propres aux secteurs et d'autres reflétant l'efficacité au niveau national, régional et local. Les SSA coopèrent avec des partenaires pour établir les SSP afin de développer des attributs répondant aux objectifs nationaux et aux priorités sectorielles. Ces mesures permettent d'établir un tableau de bord indiquant le degré de progrès atteint conformément aux buts arrêtés dans le NIPP. L'évaluation des progrès – consistant à vérifier la réalisation des objectifs et des priorités – est un processus continu visant à :

- Ajuster la vision, les priorités et les objectifs nationaux périodiquement.
- Recueillir des indices de performance pour évaluer les progrès.
- Actualiser le processus de gestion des risques en accord avec les ajustements des priorités nationales.

Tout comme l'évaluation régulière des progrès informe de l'évolution des pratiques de sécurité et de résilience, les exercices de formations planifiés et les incidents réels représentent eux aussi des occasions d'apprentissage et d'adaptation. Dans ce qui suit, nous dévoilerons quatre défis que doivent relever les concepteurs des programmes de PIC.

I.2.5. Quelques défis de la PIC

I.2.5.1. Cerner le périmètre

Toutes les stratégies de PIC élaborées jusque-là se basent sur les démarches de gestion de risques [62], comme celle élaborée dans la norme australienne (AS/NZS, 1999) [87] ou l'ISO 31000 [84]. Toutes les stratégies reposent donc sur le principe de *priorisation* des biens pour délimiter pertinemment le périmètre et les actifs à défendre. Recourir à ce principe découle, d'une part, du souhait d'optimiser les dépenses, et d'autre part, du fait que les ressources financières et humaines, aussi abondantes soient-elles, demeurent limitées : par exemple, les réseaux d'électricité sont trop longs pour être protégés par des grillages ou être surveillés intégralement. Il est donc primordial de canaliser et d'exploiter les ressources à bon escient pour minimiser les risques d'indisponibilités graves des IC. L'application du principe de priorisation permet de concentrer les efforts autour des points à hauts risques pour que les mesures de protection déployées puissent couvrir, intégralement ou partiellement, les risques. La sélection n'est toutefois pas si évidente car, à première vue, tous les secteurs sont sensibles. Le tri devra donc se faire sur la base de critères objectifs et impartiaux reflétant les impacts qualitatifs et quantitatifs susceptibles d'être subits suite à l'arrêt ou à la destruction d'une infrastructure. Parmi les paramètres devant être considérés, nous citons : le danger de la menace, le degré de vulnérabilité, le niveau actuel de protection et l'efficacité des stratégies existantes pour limiter les incidents et assurer la continuité de l'activité, les impacts encourus en cas d'indisponibilité, etc.

Le principe de priorisation adapté dans le contexte des IC repose sur deux piliers tout aussi importants l'un que l'autre : (1) énumérer, avant tout, les secteurs et infrastructures critiques, dont le dysfonctionnement risque d'entraîner des dégâts catastrophiques sur les plans social, politique, économique, ou toute combinaison de ceux-ci ; (2) puis, analyser chacun de ces secteurs et infrastructures pour en recenser les biens clés et quantifier leurs sensibilités. L'étape de quantification des sensibilités permet d'étayer les programmes de PIC de sorte à ce qu'ils satisfassent correctement les exigences recueillies.

Pour illustrer ces deux piliers, nous citons un extrait de la stratégie nationale américaine pour la sécurité du territoire qui stipule que « *les actifs, les fonctions et les systèmes au sein de chaque secteur des infrastructures critiques ne sont pas tous d'égale importance. Le secteur des transports est vital, seulement tous les ponts ne sont pas essentiels à la nation dans son ensemble. Par conséquent, le gouvernement fédéral appliquera une méthodologie cohérente pour concentrer ses efforts sur les plus hautes priorités, ainsi que le budget fédéral différenciera les ressources requises pour la protection des infrastructures critiques des ressources nécessaires pour la protection d'autres activités importantes* » [88].

Concernant le premier pilier, la Commission de l'UE propose de prendre en considération certains facteurs pour déterminer la criticité d'une infrastructure [41] :

- *Portée de l'impact* : Ce facteur se mesure à l'étendue de la zone géographique affectée (échelle régionale, nationale, internationale) par l'indisponibilité ou la perte d'une IC ou de l'un de ses éléments.
- *Ampleur* : Ce paramètre reflète le degré de l'impact suite à l'indisponibilité ou à la perte de l'IC ou de l'un de ses éléments. Généralement, quatre degrés sont dénombrés : « *néant* », « *mineur* », « *modéré* » et « *majeur* ». Parmi les critères d'évaluation de l'ampleur potentielle d'un incident :
    - Impact sur la population (nombre de citoyens touchés, épidémies, etc.) ;
    - Impact économique (dégradation de services, pertes économiques, etc.) ;
    - Impact environnemental (marées noires, incendies, etc.) ;
    - Impact politique (capacité du gouvernement à faire face, etc.).
- *Effets de l'indisponibilité dans le temps* : Ce critère permet de déterminer à partir de quel moment, la perte d'un élément de l'IC ou même de l'IIC, peut entrainer des impacts graves (par exemple, immédiatement après son arrêt, dans un délai de 24h, 48h, une semaine, etc.)
- Les effets psychologiques sont très souvent un maître-mot dans la mesure de la criticité d'une infrastructure ou d'un secteur.

Un autre facteur est capital dans la détermination des IC, il s'agit des interdépendances pouvant engendrer des phénomènes de cascade et d'escalade. Tous les facteurs cités précédemment risquent d'être amplifiés si des dysfonctionnements en chaîne venaient à se produire. Par exemple, dans le cadre de la dérégulation des marchés, une compagnie d'électricité qui subit une panne et qui n'honore plus ses engagements envers d'autres compagnies, causera l'incapacité de ces dernières à distribuer de l'électricité à leurs clients. Ainsi la portée de l'impact et son ampleur n'en seront qu'amplifiés, l'indisponibilité dans le temps risque d'être prolongée surtout pour les clients des compagnies dépendantes, en-

gendrant un impact psychologique au sein de la communauté de citoyens dépendant de ces deux compagnies. La partie qui suit aborde plus en détails la notion d'interdépendances.

I.2.5.2. Maîtriser la complexité croissante et interdépendances

Nul ne peut affirmer que les IC sont totalement autonomes dans leur fonctionnement : en effet, elles sont liées par des *dépendances réciproques* d'origines structurelles ou fonctionnelles. Pour exemple, toutes les IC dépendent du secteur de l'énergie électrique. De plus, l'activité des IC est évidemment tributaire du bon fonctionnement de leurs IIC, car sans cela toutes les tâches informatisées seraient entravées. Ces IIC connaissent également le phénomène d'interdépendance, lequel est accru par la multitude d'interconnexions qui accentue la complexité des systèmes et multiplie irrémédiablement leurs vulnérabilités. L'étude des interdépendances contribue à l'analyse de l'impact potentiel des menaces sur les IC, néanmoins, pallier totalement ces failles est inconcevable puisqu'une analyse complète et rigoureuse de tous les scénarios de défaillances est impossible. Pour finir, il suffirait qu'une panne survienne au niveau d'une IC, ou d'une IIC, pour que ces dépendances engendrent des phénomènes de *cascade* et d'*escalade*. La figure (Fig. 4) illustre les interdépendances existant entre certains secteurs et IC. Le sens des flèches indique que l'IC de départ fournit un service à l'IC d'arrivée qui dépend, par conséquent, de la première.

Formellement, quatre cas d'interdépendance entre IC sont dénombrés [13] :

- « *Entrée* » : Lorsqu'une IC, respectivement IIC, prend en entrée un ou plusieurs services d'une autre IC ou IIC afin de fournir un service. A titre d'exemple, les services des infrastructures d'énergie électrique sont nécessaires au fonctionnement de la quasi-totalité des autres IC.
- « *Partage* » : Lorsque certains composants et/ou activités de l'infrastructure, nécessaires à la fourniture du service, sont communément utilisés par plusieurs infrastructures. A ce titre, Internet et les réseaux de télécommunications peuvent être utilisées par les agents de toutes les IC.
- « *Exclusivité mutuelle* » : Lorsqu'un composant, nécessaire à la prestation de plusieurs services, ne peut être utilisé que par une seule infrastructure à la fois. Par exemple, un règlement interne peut stipuler qu'un générateur mobile d'énergie ne soit utilisé par les services d'urgence ou par les services de télécommunications, mais non les deux à la fois [13].
- « *Colocation* » : Lorsque les composants physiques ou activités de deux ou plusieurs infrastructures sont localisés au sein d'une même zone géographique (non. restreinte à une superficie donnée). Pour exemple, les des gratte-ciels regroupent, dans un même bâtiment, des équipements du secteur des TIC, ceux du

secteur des télécommunications, des succursales de banques et des locaux de directions de grandes firmes électriques, chimiques ou encore nucléaires.

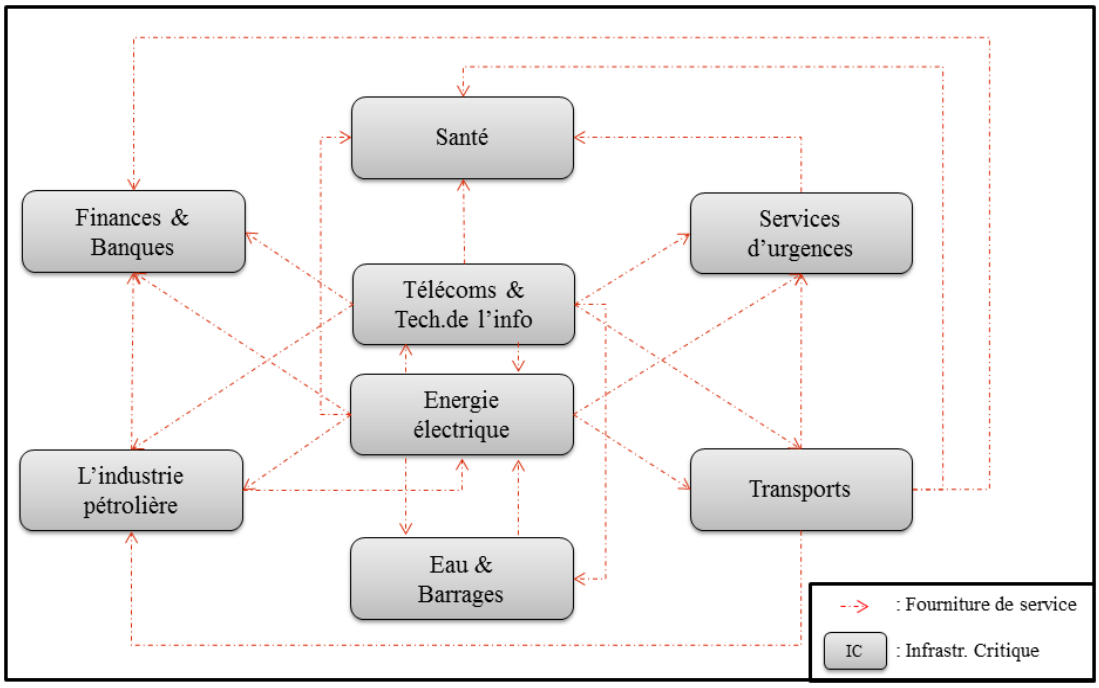

Fig. 4. Interdépendances entre certaines infrastructures critiques

En plus de ces interdépendances natives entre les IC, il existe d'autres dépendances entre les différents acteurs opérant sur le terrain, plus particulièrement entre les fournisseurs, les régulateurs, les transformateurs, les fabricants les distributeurs et les détaillants [41, 89]. Une autre infortune réside dans le fait que nombre de dépendances physiques, virtuelles ou encore logiques n'apparaissent malheureusement qu'en période de crise [69].

I.2.5.3. Maîtriser la diversité des nouvelles formes de terrorisme

Un autre élément à considérer est celui de la diversité et de la multiplication des formes de terrorisme outrepassant désormais toute frontière politico-géographique. Ces actes peuvent émaner aussi bien de l'intérieur comme de l'extérieur des IC et être perpétrés soit grâce à un arsenal d'équipements ou tout simplement par un micro-ordinateur. Rappelons que l'horizon des menaces s'est étendu depuis que les TIC sont utilisées en masse : les questions cybernétiques concurrencent de plus en plus les préoccupations d'ordre physique [45]. Aux Etats-Unis, une cellule nationale chargée de l'évaluation des risques (SNRA) a établi une taxinomie des menaces pesant sur la sécurité du pays en général et des IC en particulier ; les principales catégories des menaces recensées sont illustrées dans la figure (Fig. 5). Pour ce qui est des dangers externes, ils sont nombreux, à commencer par le piratage informatique, en passant par les actes terroristes ou criminels, sans oublier tous types

de catastrophes naturelles (tsunamis, montée du niveau des mers, etc.). Ces menaces peuvent convoiter divers desseins tels que la corruption des données et fonctions, l'espionnage et le vol de secrets industriels, le déni de service (DoS) à des fins de sabotage ou de concurrence malhonnête. Plus grave encore, ces menaces peuvent causer des dommages corporels, matériels et économiques, plongeant par conséquent les populations dans des tourments psychologiques perpétuels (i.e. inquiétude constante, perte de confiance, etc.).

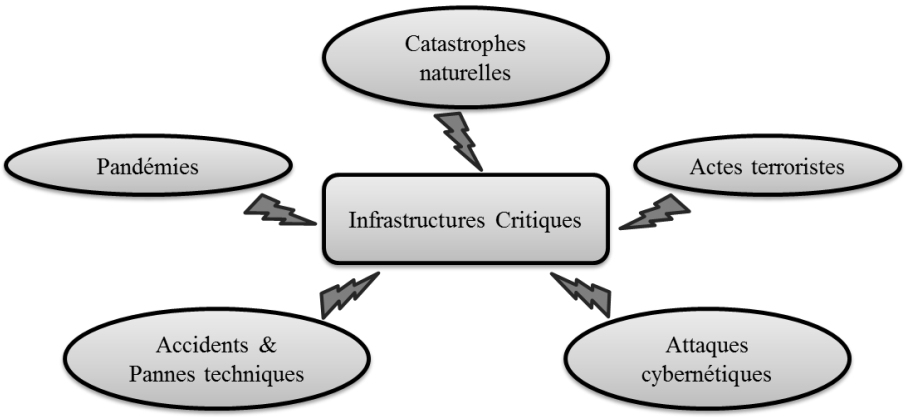

Fig. 5. Les menaces qui pèsent sur les IC

La menace interne n'est pas non plus à prendre à la légère. En effet, les ressources des IIC peuvent être la cible d'agents internes mécontents et malintentionnés désirant délibérément se venger. Des études ont conclu que les attaques de l'intérieur étaient bien plus nombreuses que celles émanant de l'extérieur : les proportions sont déséquilibrées, entre 60% et 80% des menaces proviendraient de l'intérieur [90]. L'intrusion de ces employés mécontents est d'autant facilitée par le fait qu'ils ont accès directement au système en plus de leur connaissance de l'architecture et des technologies utilisées. Ces menaces peuvent aussi être dues à des facteurs accidentels tels que les catastrophes liées à l'intervention humaine (défaillance d'un barrage, d'un réacteur nucléaire, etc.), les pénuries de personnel (grèves, épidémies), les erreurs humaines accidentelles, lacunes organisationnelles, défaillances ou pannes techniques, dépendances et pénuries d'approvisionnement [37].

Les attaques visant les TIC visent généralement à porter atteinte à la propriété de disponibilité, de confidentialité ou encore d'intégrité. Les attaquants tentent très souvent de brouiller les pistes en camouflant leurs identités et leurs localisations en utilisant des réseaux zombies, connus sous le nom de botnets[26], rendant ainsi leur traçage lent et difficile.

[26] Botnet : terme générique désignant des ordinateurs infectés et contrôlés par un pirate à distance. Celui-ci les contrôle pour générer du spam ou mener des attaques de grandes envergures contre des serveurs [91].

L'ensemble de ces menaces ne saurait mettre en péril les IC si ces derniers ne présentaient pas de vulnérabilités. Il est donc primordial pour ces installations d'identifier leurs faiblesses et d'œuvrer activement à leur correction.

I.2.5.4. Pallier les vulnérabilités des IC et des IIC

Dans son ouvrage « L'Art de la guerre », Sun Tzu déclare : « *Qui connaît l'autre et se connaît lui-même, en cent batailles ne sera point défait. Qui ne connaît pas l'autre mais se connaît lui-même, pour chaque victoire connaîtra une défaite. Qui ne connaît ni l'autre ni lui-même, perdra inéluctablement toutes les batailles* ». A la lecture de cette citation, nous dégageons un des piliers de la victoire celui de bien se connaître. Concrètement, cela se traduit par la connaissance de ses failles propres pour les corriger ou du moins pour les dissimuler. Pour les IC, cela est capital à la garantie leur sécurité, résilience et *SdF* surtout dans le contexte actuel d'ouverture, où règne un climat d'une hostilité sans précédent [92, 93, 94]. Nous commençons cette démarche introspective par une analyse des architectures des IIC : en quelques années, ces architectures ont subi une transition rapide, soudaine et surtout radicale. Les modèles isolés et centralisés de jadis furent délaissés au profit de modèles plus flexibles, convergents et décentralisés ; toutefois, ces derniers sont de plus en plus constitués de « *composants pris sur étagère* » (COTS) criblés de vulnérabilités [95]. Ces faiblesses sont dues essentiellement au fait qu'ils sont connectées à Internet et que leur développement ne tient pas toujours compte des aspects sécurité pour des raisons de réduction du Time-to-Market[27] [37].

D'autre part, les IC sont souvent constituées de processus physiques ou mécaniques contrôlés électroniquement par des systèmes informatisés tels que les « *systèmes de contrôle et d'acquisition de données* » (SCADA) et des « *systèmes de contrôle de processus* » (PCS). Ces systèmes étaient souvent propriétaires, ce qui fournissait un certain niveau de sécurité par le biais de l'*obscurité* (*Security by Obscurity*). Seulement cet avantage n'existe plus puisque les IC se sont tournées vers les COTS – systèmes d'exploitation connus, protocoles de transmission basés sur IP dont les vulnérabilités sont connues de tous, etc. – pour réduire coûts et délais de développement des solutions [89]. Dans de telles conditions, ces actifs peuvent, à tout instant, être victimes de dysfonctionnements causés par quelconque source de malveillance ou d'inadvertance, infligeant des répercussions catastrophiques tant sur le plan pécuniaire que sur le plan de la stabilité du pays.

Pour réduire les risques pouvant causer l'indisponibilité de ces IC, il faut œuvrer à leur garantir un niveau de sécurité acceptable. La tâche est rendue plus difficile du fait que

[27] Time-to-Market : Durée de temps nécessaire à la conception et à la fabrication d'un produit avant qu'il ne soit disponible à la vente [96].

l'efficacité des mesures de protection se mesure à celle du maillon le plus faible ce qui témoigne d'une totale asymétrie entre les attaquants et les responsables de la sécurité des IC. Pour cela, nul aspect de la sécurité ne doit être négligé, à savoir les aspects physiques – la sécurité des locaux et des équipements, etc., les aspects techniques – mécanismes, configurations, etc. – et les aspects organisationnels – sensibilisation du personnel, formation etc. Traiter ces aspects se concrétise par la mise en place de plusieurs barrières de sécurité [9]. L'aspect humain est tout aussi important dans la démarche de réduction des vulnérabilités, puisqu'une main d'œuvre bien formée œuvrera à une bonne maintenance des IC, chose qui concourt à la garantie de leur sécurité et de leur résilience [45]. Ces facettes de la protection doivent être considérées conjointement avec les propriétés et besoins des IC et IIC. Ces caractéristiques permettront non seulement de sélectionner les mécanismes adaptés, de les déployer et de les configurer convenablement afin de répondre aux besoins identifiés ; mais aussi, d'élaborer des manœuvres d'intervention en cas de sinistres, visant à réduire leurs effets indésirables. Dans ce qui suit, sera énuméré un ensemble de propriétés et de besoins recueillis au cours de l'état d'art.

I.2.6. Propriétés et besoins des IC et IIC

I.2.6.1. Propriétés des IC et IIC

N'importe quelle démarche de PIC ne saurait aboutir sans la considération des propriétés et besoins de ces IC et IIC. Ces deux facteurs sont d'une importance capitale puisqu'ils permettront de parfaire la conception de ces systèmes puis de veiller à leur bon fonctionnement tout au long de leur exploitation sans entrainer des dépenses inutiles. De nombreux travaux [11, 12, 89, 98] tentent d'identifier ces propriétés, nous en citons :

- *Complexité des IC et IIC* : De nature, une IC est constituée d'un ensemble de filiales et de départements – du point de vue métier, sécurité, gestion et administration. Par conséquent son IIC est constituée, à son tour, d'une multitude de *sous-systèmes d'information* interconnectés faisant de l'ensemble un système très complexe. Cette complexité est accentuée par les contraintes que doit satisfaire l'IIC telles que l'ouverture, la prédisposition aux collaborations, etc.
- *Caractère multinational et conformité à des régulations et législations diverses* : Pour des raisons économiques, une IC implante ses filiales dans divers pays. De nouvelles contraintes sont donc à prendre en compte, parmi elles : les procédures légales de création, d'administration et d'exploitation, les réglementations et législations en vigueur à respecter au sein de chaque pays, etc.
- *Caractère multi-organisationnel* : D'un point de vue collaboratif, les IIC peuvent s'interconnecter pour assurer la réalisation d'objectifs communs. Pour cela,

des négociations concernant l'utilisation des ressources s'imposeront, à l'issue desquelles, les utilisateurs d'une IC manipuleront les ressources d'autres IC.

- *Interdépendance* : Partager un espace physique ou être interconnecter entraînent des interdépendances entre les IC et entre leurs IIC aussi. Pour éviter les problèmes qui s'y rapportent, les questions de sécurité doivent être gérées conjointement, et surtout de manière cohérente, au sein des IC et IIC. Les actions devront avoir une portée aussi bien locale – gérer les actions internes à l'IC et l'IIC – que globale – gérer les actions se rapportant aux collaborations.

- *Concurrence et suspicion* : Contraintes de collaborer, les IC peuvent collaborer tout en étant méfiantes et suspicieuses. Ces craintes sont davantage exagérées lorsque les parties sont en concurrence et que leurs intérêts sont en conflits.

D'autres facteurs sont aussi importants que ces propriétés : il s'agit des besoins des IC. Ci-après, une liste détaillée des besoins de ces IC, qui cadre les axes de recherche et de développement de leurs solutions, est dressée.

I.2.6.2. Les besoins des IC et IIC

Bien plus important encore sont le besoins devant être satisfaits afin de garantir un fonctionnement pérenne aux IC et IIC. En effet, conformément à ces besoins seront conçus, sélectionnés et mis en œuvre des moyens de protection sur mesure. Cela permettra de contrer convenablement les menaces identifiées et participera ainsi à la réduction notable des frais de protection. Ci-après une liste exhaustive de ces besoins :

- *Audits et évaluations* : La PS doit détailler certains aspects liés à la journalisation des actions d'exploitation du système (données spatio-temporelles, etc.). Grâce à cela, les audits favoriseront la détection des lignes de défense ne remplissant pas correctement leurs missions afin de pouvoir les réajuster.
- *Autonomie* : Pour réduire les problèmes de sécurité pouvant résulter d'un fort couplage entre IC, celles-ci doivent jouir d'une pleine et entière indépendance lors de l'élaboration de la PS qui répond au mieux à leurs objectifs de sécurité. S'en suivra donc une liberté dans le choix des techniques et mécanismes à déployer. Pour les collaborations, des clauses sont négociées ; elles seront traduites conformément aux techniques et mécanismes utilisés dans chaque IC.
- *Cohérence des politiques de sécurité* : Les PS, statuant sur ce qui est autorisé et ce qui ne l'est pas, se doivent d'être cohérentes. Dans ce sens, elles doivent être dépourvues d'ambiguïtés et de contradictions et doivent refléter fidèlement les

objectifs de sécurité arrêtés. Le défi est d'autant plus grand lorsqu'il s'agit de tenir compte de collaborations, lorsqu'il faut négocier ou combiner des PS.

- *Contrôle d'accès et sphère d'autorité* : Pour contrôler et limiter efficacement les accès des utilisateurs aussi bien internes qu'externes, un mécanisme incontournable est déployé : le contrôle d'accès. Il représente un moyen, parmi d'autres, d'implémentation de la PS. Son objectif est de statuer sur les requêtes d'accès, formulées par les utilisateurs à l'égard des objets, conformément aux règles de sécurité traduisant les objectifs de sécurité de l'organisation.
- *Contrôle d'accès – richesse, dynamique, granularité et évolutivité des mécanismes de utilisés* : L'efficacité du contrôle d'accès se mesure à la pertinence des règles de sécurité exprimées. Cela tient compte des attributs retenus et de leur granularité, mais aussi de la prise en compte du caractère dynamique des requêtes d'accès. L'évolutivité des règles et la capacité à exprimer des principes de sécurité tels que le « *moindre privilège* » et la « *séparation des tâches* » sont aussi des critères importants. Sans oublier aussi l'expression des exceptions, des interdictions et l'utilisation de techniques de résolution de conflits.
- *Convivialité et la facilité d'administration de la politique de sécurité* : Administrer aisément la politique de sécurité d'une IC est une propriété décisive qui permet d'éviter grandement l'occurrence d'erreurs humaines de conception, configuration ou encore de manipulation.
- *Défense en profondeur* : Les IC ne peuvent se fier qu'à un mécanisme de défense, au contraire, maintes lignes de défense doivent être déployées. Chacune jouera un rôle – affaiblir, gêner ou retarder l'attaque – pour assurer une protection globale. L'idée est de considérer chaque dispositif de sécurité comme vulnérable et le renforcer par un autre. Pour plus d'efficacité, ces lignes doivent être autonomes, ordonnées et coordonnées ; de plus, la perte d'une ligne ne doit affecter en rien la robustesse de la suivante, au contraire, elle doit la renforcer ne serait-ce que par le recueil de renseignements. Chaque ligne doit comporter diverses parades pour contrer le plus d'attaques possibles. Ces barrières peuvent tout aussi bien confiner les menaces internes – cas des stations nucléaires [9].
- *Evolutivité* : Forte de sa dynamique, une IC évolue sans cesse : acquérant de nouvelles ressources, augmentant ou réduisant ses effectifs, etc. Cela impose donc des changements permanents aussi bien au niveau de l'IC que de son IIC. Par conséquent, il faut considérer les forts besoins de flexibilité et d'extensibilité requis dans l'administration des IC et de leurs IIC.

- *Interopérabilité et Inter-connectivité* : Permettre aux IIC de communiquer et d'interagir implique que celles-ci doivent se comprendre ; des protocoles d'échange leur permettant de négocier leurs services et d'échanger les données devront être édifiés ou adoptés. Outre cela, l'interconnexion des sites devra être garantie à travers la mise en place d'équipements d'interconnexion permettant d'acheminer les données de bout en bout.
- *Résilience et auto-recouvrement* : Dans les différentes versions du NIPP, la propriété de résilience est citée autant de fois que l'est la propriété de sécurité, cela témoigne donc de son importance. La résilience est définie dans le PPD-21[64], comme étant « *la capacité à se préparer et à s'adapter aux conditions changeantes ainsi que l'aptitude à résister et à récupérer rapidement suite aux perturbations* ». Ces dernières peuvent être d'origine délibérées ou accidentelles [45]. Les systèmes doivent être capables de détecter des états de fonctionnement incorrects et opérer les ajustements nécessaires pour recouvrer un fonctionnement normal par des moyens de recouvrement proactifs et réactifs.
- *Sécurité-immunité des réseaux et des SI* : Veiller à la continuité de l'activité des réseaux nécessite la garantie de la sécurité de leurs composants à travers trois propriétés : confidentialité, intégrité et disponibilité. En particulier, nous rappelons l'importance des exigences des IC en matière d'intégrité.
- *Sécurisation des collaborations* : Ne pouvant évoluer sans fournir ni bénéficier de services, les IC se doivent de collaborer. Cela n'est toutefois pas sans risques : cela entraîne une mise à disposition des ressources propres de l'IC (i.e. utilisateurs et objets) au profit de ses collaborateurs. Soucieuse d'imposer ses conditions d'utilisation en vue de protéger ses ressources, chaque organisation assoit son autorité sur ses biens favorisant ainsi des collaborations dont la gestion est le plus souvent décentralisée [99, 100].
- *Sécurité des collaborations – Application et suivi en temps réel des contrats inter-organisation* : Maîtriser les collaborations s'accomplit par l'établissement de contrats visant à clarifier les objectifs par l'énumération des tâches à accomplir, l'attribution des responsabilités et la précision des sanctions en cas de non-respect des clauses. Leur mise en œuvre et leur supervision sont essentielles pour assurer des collaborations sans litiges.
- *Sûreté de fonctionnement (SdF)* : A travers ses six attributs – confidentialité, intégrité, disponibilité, maintenabilité, fiabilité et sécurité-innocuité – la SdF permet non seulement aux agents de l'IC de placer une confiance justifiée dans

leur IIC, mais aussi de préserver l'environnement de l'IC de répercussions catastrophiques en cas d'éventuels dysfonctionnements.

- *Systèmes d'alertes et de partage d'informations sur les menaces et les vulnérabilités pour être en mesure d'élaborer des plans d'urgence et de les appliquer rapidement en cas de crise* [38, 45].
- *Tolérance aux intrusions* : Etre immunisé contre toutes les menaces existantes relève de l'utopie ; par conséquent, il faut garantir aux IC un fonctionnement normal, ou en mode dégradé, même après avoir essuyé des intrusions. Leurs IIC doivent donc faire face à un haut degré d'hostilité pouvant émaner de l'intérieur comme de l'extérieur sans interrompre l'activité.

I. 3. Deuxième partie : Importance de l'intégrité dans le cas des IC

Parmi toutes les exigences citées ci-avant, nous avons choisi de nous focaliser sur le besoin en intégrité des IIC. Cet intérêt émane du fait que les IC comptent sur le bon fonctionnement et la fiabilité de leurs IIC, vu que ces systèmes manipulent des données devant nécessairement être correctes et fournissent également des données devant aussi être correctes et fiables. L'intégrité fut négligée par rapport à la confidentialité, notamment, en raison de l'importance de la confidentialité dans le domaine militaire ainsi que l'émergence quelque peu tardive des systèmes commerciaux utilisant des SI. L'intégrité s'avère être, malgré tout, primordiale : à quoi bon dissimuler un secret corrompu ? A quoi bon veiller à la disponibilité d'un service défectueux ou d'une information erronée.

L'intégrité, dans son sens le plus large, a été définie dans le dictionnaire Webster [26, 101] comme étant la propriété de correspondre fidèlement à une condition ou à un état initial. Ainsi, une personne intègre n'est autre qu'une personne agissant, en permanence, conformément à un code ou un standard. Aucun jugement sur la qualité de ce code ne peut être avancé, néanmoins la seule garantie est que la personne ne se détournera point de ce code. Il en va de même pour les systèmes : un système possède la propriété d'intégrité si l'on peut faire confiance à son adhérence à un code de comportement bien défini. On distingue deux définitions de la propriété d'intégrité : l'intégrité de l'information et l'intégrité du système. L'intégrité de l'information est la propriété d'une information d'être exact – correcte, non corrompue – [16], en ce sens, le système devrait :

- Empêcher toute modification – création, mise à jour ou destruction – illégitime – incorrecte ou effectuée par un utilisateur non autorisé – de l'information ;
- Nul utilisateur ne doit entraver une modification légitime de l'information.

L'intégrité du système se mesure à sa propriété d'être « sans états initiaux invalides et de ne pas aboutir à des états invalides à partir d'un état initial. Si un état invalide est initial ou accessible à partir d'un état initial, alors toutes les transitions qui s'en suivent sont définis comme invalides » [102]. Aussi l'intégrité d'un système peut se décliner à travers une multitude de facettes [103], dont nous citons quelques-unes :

- Robustesse : Les auteurs soutiennent que la capacité d'un système à gérer les événements inattendus est directement proportionnelle à son intégrité, ainsi, plus un système est robuste plus il est apte à préserver son intégrité.
- Cohérence des données : Les informations copiées ou distribuées au sein d'un système doivent préserver leur cohérence indépendamment du facteur temporel et du changement des conditions du système.
- Innocuité : L'intégrité d'un système se décline aussi à travers l'absence de conséquences catastrophiques suite à des pannes ou des incidents.
- Fiabilité : Une autre caractéristique d'un système intègre est sa fiabilité, autrement dit, sa probabilité de réaliser adéquatement ses objectifs pour une période donnée, dans des conditions d'exploitation bien précises.

Assurer l'intégrité d'un système sous-entend l'élaboration de politiques de sécurité et des mécanismes permettant d'offrir l'isolation nécessaire le protégeant contre les sources de compromission. Beaucoup de principes peuvent être mis en œuvre afin de préserver l'intégrité des données et des procédures, nous citons par exemple :

- Principe du « *moindre privilège* » (*least privilege*) : Pour empêcher l'acquisition et/ou la modification illégitime des informations, ce principe stipule que seul le minimum de droits nécessaires à la réalisation d'une tâche doit être accordé à un sujet demandant l'accès à une ressource. Ces droits doivent lui être accordés durant la durée minimale nécessaire à la réalisation de cette tâche [104].
- Principe de la « *Séparation des privilèges* » (*Separation of privilege*) : stipule, que dans certaines situations, un système ne doit pas se contenter de vérifier une seule condition lors de l'octroi de permissions, au contraire, il doit s'assurer de la validation de plusieurs conditions [105]. Il représente un moyen robuste de protection, puisqu'un attaquant parvenant à obtenir un privilège sans obtenir le second, ne réussira pas son attaque. La règle "Two-man rule" compte parmi les déclinaisons de ce principe [106].
- Principe de la « Séparation des Tâches » (*Separation of duties*) : stipule, pour sa part, que la réalisation d'une tâche critique nécessite le concours de deux ou plusieurs utilisateurs distincts, autrement dit, la tâche devra être subdivisée en

sous-tâches, chacune réalisée par un utilisateur. Cela permettra, non seulement, de vérifier les erreurs humaines pouvant survenir mais aussi de dissuader bon nombre d'utilisateurs mal intentionnés [104].

Compte tenu de l'importance des IC, il est clair que la propriété d'intégrité figure parmi les priorités que se fixent les administrateurs lors de l'élaboration des politiques de sécurité. Ils essayent donc de tenir compte des différents principes cités ci-avant.

I. 4. Conclusion du chapitre

Ce premier chapitre a permis de souligner l'importance des infrastructures auxquelles sont dédiés nos efforts. Nous avons, entre autres, exposé dans le détail les notions d'IC, d'IIC et de PIC ainsi qu'explicité les principes des démarches de gestion des risques, notamment en raison de leur importance dans les programmes de PIC. Nous avons aussi fait le point sur les besoins et propriétés des IC et IIC afin d'être plus apte à répondre à leurs exigences. Nous nous intéresserons par la suite à trois de ces besoins qui ne sont autres que les besoins d'intégrité, de contrôle des accès et de collaborations.

Dans le prochain chapitre, nous aborderons le mécanisme de contrôle d'accès. Nous établirons un état de l'art de certains modèles de contrôle d'accès : certains sont classiques, d'autres tiennent compte de l'intégrité tandis que d'autres tentent de répondre aux besoins de collaborations. Nous décrirons les principes de chacun, leurs forces et leurs faiblesses, tout en analysant comment chacun d'eux nous servirait pour répondre aux besoins des IIC.

CHAPITRE 2 :

CONTRÔLE D'ACCÈS

SOMMAIRE

II. 1. Préambule

Tout au long du précédent chapitre, nous avons exposé l'importance ainsi que la sensibilité des organisations auxquelles s'appliqueront nos contributions. Nous avons aussi listé les besoins et propriétés devant être prises en considération dans notre proposition.

Dans ce chapitre, notre intérêt portera sur le mécanisme de contrôle d'accès. Une définition et une description de ses composantes sont pourvues. L'importance d'une conception pertinente de la PS est aussi soulignée favorisant ainsi une meilleure protection.

Ensuite, nous soulignons l'importance de l'analyse des risques dans l'élaboration d'une PS adaptée à une organisation. L'analyse aura pour but d'identifier les objectifs de sécurité nécessaires et suffisants à la satisfaction des besoins de sécurité de l'organisation suite à une formalisation exhaustive de scénarios de risques à éviter.

Avant d'entamer l'état de l'art des modèles de contrôle d'accès, nous rappelons l'importance de la modélisation et ses atouts en termes d'expression et d'administration des PS. Puis nous enchainons, dans cet ordre, par une présentation de certains modèles de contrôle d'accès classiques, suivie de certains modèles d'intégrité pour finir enfin par quelques modèles collaboratifs. Une description détaillée de chacun est établie, soulignant ses concepts fondamentaux, son fonctionnement ainsi que ses avantages et inconvénients.

Pour clore ce chapitre, nous faisons le point sur les forces et faiblesses du modèle OrBAC ainsi que ses extensions conformément aux besoins et propriétés des IIC. Nous montrons sa faiblesse quant à la prise en compte de l'intégrité à travers un exemple de PS.

II. 2. Importance du contrôle d'accès : définition et composantes

Contraintes à déployer des réseaux et des SI complexes, les organisations sont acculées à s'assurer de l'identité des utilisateurs et à restreindre leurs droits relatifs à la manipulation des ressources aussi bien actives (i.e. autres sujets) que passives (i.e. équipements et informations). Ces actions visent à se prémunir des menaces pouvant émaner tant de l'intérieur que de l'extérieur. Pour tenter d'y parvenir, les organisations recourent à une ligne de défense incontournable : le contrôle d'accès. Son but est de limiter les actions auxquelles peut prétendre un utilisateur légitime du système tout en interdisant strictement toute action voulant être réalisée par un utilisateur non autorisé. Plus clairement, il statue sur les différentes requêtes d'accès émanant des utilisateurs : les acceptant avec ou sans contraintes, ou tout simplement les refusant. Il agit soit directement sur les actions que peut réaliser l'utilisateur, soit indirectement, en contrôlant les actions effectuées par les sujets opérant en son nom. L'objectif étant de réduire au maximum l'occurrence d'actions illicites pouvant causer ou exploiter des failles et ainsi créer des incidents dans le système [23].

Fondamentalement, le contrôle d'accès repose sur cinq éléments de base : des ensembles de *sujets*, d'*objets* et d'*actions*, un *moniteur de référence* et des *règles de sécurité*. Les sujets sont les entités actives du système (utilisateurs, programmes) ; du fait qu'ils réalisent des actions sur les objets [17]. Les objets, en revanche, sont des conteneurs de l'information (fichiers, base de données, etc.) et sont manipulés par les sujets : ce sont donc

des entités passives du système [17]. Notons que les sujets sont aussi considérés des objets. Les actions, quant à elles, sont des types d'opérations réalisées par les sujets sur les objets [17], elles sont donc responsables du changement d'états des objets. Nous distinguons généralement les actions suivantes [26] :

- *Observation* : consultation, par un sujet, d'informations contenues dans un objet. Les états d'observation sont différents selon le sujet requérant l'accès.
- *La Modification* : transformation de l'état d'une information, et par conséquent de l'état de l'objet aussi, par rapport à de précédentes observations.
- *L'Invocation* : requête logique adressée par un sujet à un autre pour bénéficier d'un service – peut être considérée comme une modification.
- *L'Exécution* : différente de l'invocation et permet à un sujet d'obtenir des instructions depuis un objet, ainsi l'exécution peut être assimilée à l'observation.

Pour sa part, le moniteur de référence s'intercale entre les sujets et les objets, comme l'illustre la figure (Fig. 6), et a pour mission d'évaluer toutes les requêtes émises par les sujets du système et de statuer sur leur légitimité. Ses décisions sont conformes à la PS de l'organisation qui traduit, à son tour, un ensemble d'objectifs de sécurité identifiés.

Pour garantir que ses jugements sont justes et qu'aucune requête n'échappe à son contrôle, certaines contraintes conceptuelles et fonctionnelles lui sont imposées [26] :

- *Complet/Incontournable* : Toutes les requêtes d'accès doivent être contrôlées et une décision d'accès – accord ou déni – doit être émise à leur égard.
- *Protégé* : Ses fonctions ne doivent aucunement être compromises, par quelconque source de danger, accidentelle soit-elle ou délibérée.
- *Fonctionnement correct prouvé* : Des preuves doivent être fournies quant à l'application fidèle, en tout temps, de la politique de protection spécifiée.

Il va sans dire que le contrôle d'accès ne résout pas à lui seul tous les problèmes de sécurité. Dans ce sens, il doit être couplé à d'autres mécanismes effectuant des contrôles et des traitements, *a priori* tel que l'authentification et *a posteriori* comme la journalisation. Ces couplages, illustrés dans la figure Fig. 7, favorisent non seulement le fonctionnement correct du contrôle d'accès mais aussi l'amélioration continue de la pertinence des décisions prises tout au long de son fonctionnement. Clairement, avant d'accorder ou de refuser un accès à un utilisateur, il faut d'abord s'assurer de son identité prétendue, cela relève de l'authentification. Par conséquent, l'efficacité du contrôle d'accès dépend de l'acuité de l'authentification. Concernant les contrôles *a posteriori*, la journalisation et l'audit offrent la possibilité d'une analyse postérieure de toutes les requêtes collectées et activités réali-

sées au sein du système dans le but de contrôler les comportements des utilisateurs et d'effectuer des corrélations pour détecter d'éventuelles fuites dans le système de sécurité. Ces contrôles permettront de réajuster en permanence la PS ainsi que les configurations jugées défaillantes. Notons que l'audit présente un autre avantage se déclinant à travers son rôle dissuasif – les contrôles *a posteriori* découragent un grand nombre de fraudeurs [23, 26].

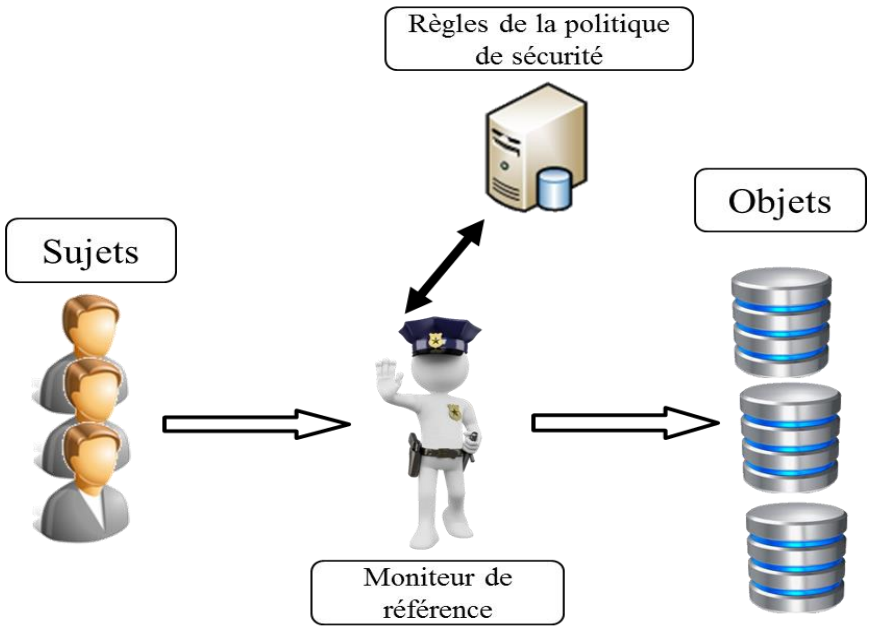

Fig. 6. Schéma du moniteur de référence.

Pour fonctionner, le moniteur de référence a besoin d'appliquer une PS, consistant en un ensemble de règles de sécurité qu'il peut interpréter. Ces règles de sécurité sont administrées dans une base de données des autorisations. En parlant de PS, il serait intéressant d'expliciter ce concept d'une façon toute simple. Pour protéger un système, deux approches triviales s'offrent : la politique fermée ou la politique ouverte. Dans le cas de la première, tous les accès sont interdits sauf ceux explicitement autorisés ; l'ennui est qu'en cas de mauvaise spécification de la politique, certains services importants risquent d'être abolis. En revanche, en présence de la seconde, tous les accès sont autorisés hormis ceux explicitement interdits, l'inconvénient ici est que les accès sont facilités au risque de laisser des portes ouvertes aux attaquants [107]. Cela nous mène vers la conclusion suivante : il est difficile d'affirmer qu'une politique est meilleure qu'une autre, en revanche il est possible de garantir qu'une politique offre une meilleure protection. En effet, toute politique est conçue dans l'objectif de répondre à certains besoins et à couvrir certains risques, ainsi des politiques strictes et rigides comme celles utilisées dans le domaine militaire sont inadaptées dans le contexte de systèmes commerciaux et vice-versa. Le choix des politiques dépend des propriétés et de l'environnement du système [23].

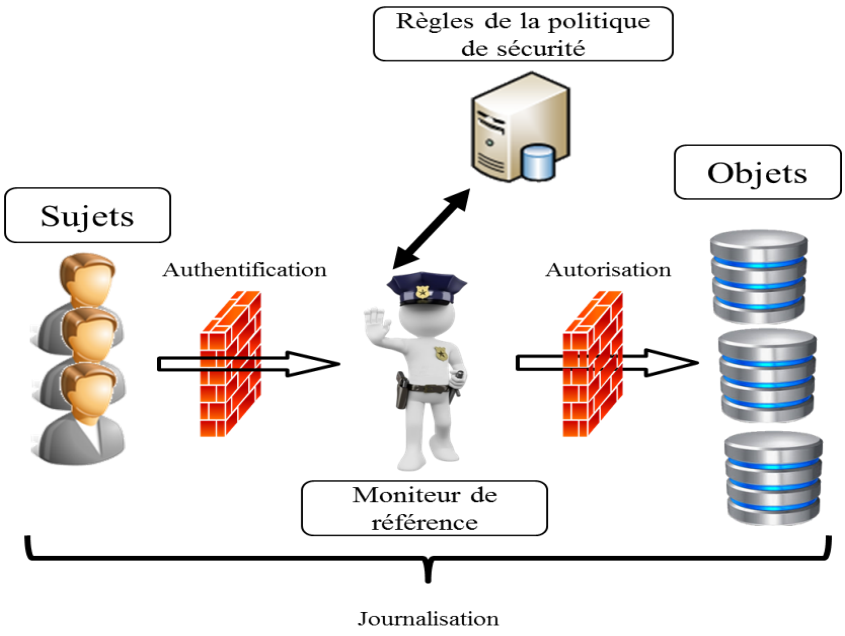

Fig. 7. Contrôle d'accès couplé à l'authentification et la journalisation

Afin d'optimiser ce choix et de concevoir une politique qui réponde aux besoins du système, il faut avant tout déterminer ses exigences ainsi que les objectifs de sécurité qu'il doit satisfaire. Le meilleur moyen pour y parvenir serait de suivre une démarche structurée et méthodologique à l'issue de laquelle seront cernés ces objectifs de sécurité à atteindre. Les démarches en question sont les méthodes d'analyse et de gestion des risques. Vitales dans le domaine de la PIC, elles le sont aussi dans le domaine des systèmes d'informations.

II. 3. Importance de l'analyse de risque

La relation qui lie la sécurité à la gestion des risques est très contiguë. En effet, gérer la sécurité est un processus délibéré visant à identifier et à quantifier les risques afin de déployer des contremesures destinées à les réduire ou à les couvrir à coût raisonnable [41]. Ainsi, afin d'optimiser l'expression des PS pour qu'elles satisfassent les exigences des systèmes, il faut avant tout étudier le système en question : déterminer ses éléments sensibles et leurs propriétés à préserver, identifier ses vulnérabilités et les menaces pouvant les exploiter. A l'issue de cela, il devient possible de dresser les scénarios des risques éventuels – en confrontant les besoins aux menaces, en considérant les vulnérabilités pour mesurer la faisabilité de l'attaque – pour déterminer les objectifs de sécurité que doit remplir le système. Affiner ces objectifs de sécurité permettra d'extraire la PS devant être implémentée par les mécanismes de sécurité, dont le contrôle d'accès. Cependant l'application de ces démarches n'est pas ponctuelle, bien au contraire, elles sont dynamiques, itératives et réactives aux changements afin d'accompagner l'évolution permanente du système.

Dans ce qui suit, nous exposons brièvement les piliers d'une méthode de gestion des risques adaptée au domaine des SI. La méthode s'intitule : « Expression des Besoins et Identification des Objectifs de Sécurité » (EBIOS) ; elle fut conçue en 1995 par la « Direction Centrale de la Sécurité des Systèmes d'Information » (DCSSI), aujourd'hui remplacée par l'« Agence Nationale de la Sécurité des Systèmes d'Information » (ANSSI). Cette méthode est une référence en France et jouit d'une importante notoriété dans les secteurs public et privé. La démarche itérative proposée s'articule autour de cinq grandes étapes :

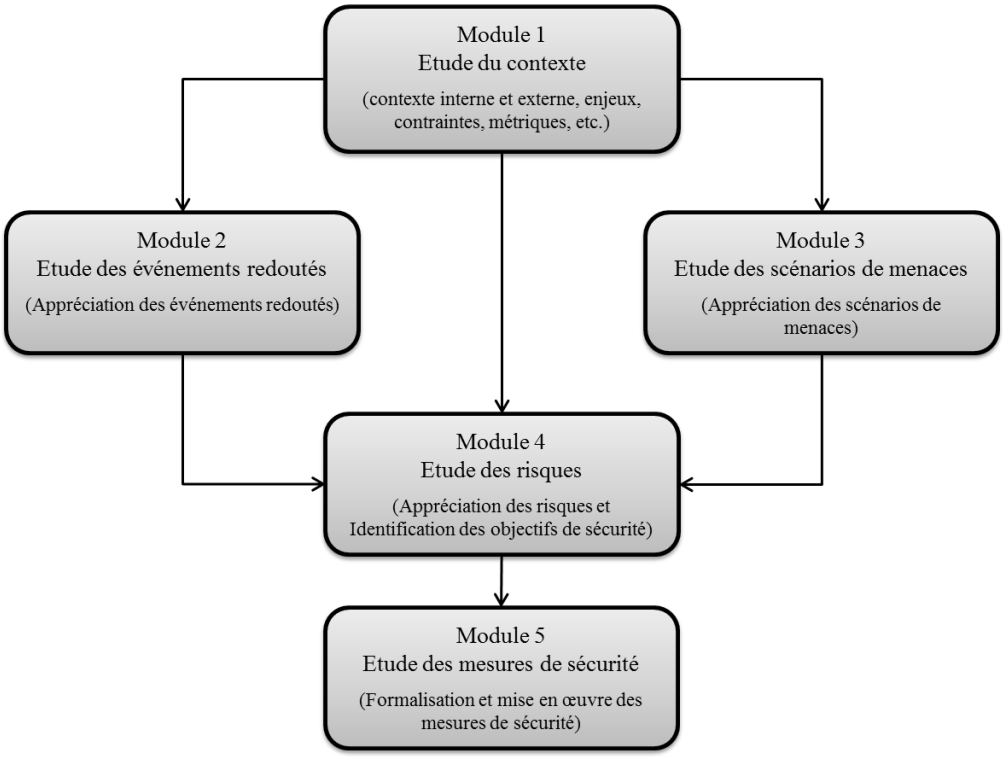

Fig. 8. Schéma de la méthode EBIOS

Module 1 : *Etude du contexte*

Pour commencer, un contexte bien défini permet de gérer les risques de manière parfaitement appropriée, et ainsi de réduire les coûts à ce qui est nécessaire et suffisant au regard de la réalité du sujet étudié. Dans ce sens, ce module a pour objectif de [10] :

- Collecter les éléments nécessaires à la gestion des risques afin d'en délimiter le cadre : caractéristiques internes et externes, enjeux et diverses contraintes (politique, stratégique, structurelle, fonctionnelle, budgétaire, etc.)
- Préparer les métriques en définissant les critères de sécurité et les échelles de besoin représentatives ainsi qu'en élaborant des échelles de niveaux de gravité et de niveaux de vraisemblance.

- Cerner le périmètre de l'étude à savoir les biens essentiels[28], les biens supports[29] sur lesquels ils reposent et les mesures de sécurité déjà existantes.

Module 2 : *Etude des événements redoutés*

Cette deuxième étape vise à identifier les situations indésirables qu'il est souhaitable d'éviter. Il s'agit d'un premier pas vers l'appréciation des risques. A ce stade, il sera possible (1) d'identifier et d'estimer les besoins de sécurité[30] (particulièrement de confidentialité, d'intégrité et de disponibilité) des biens essentiels, (2) d'identifier et de mesurer les différents impacts pouvant survenir si certains de ces besoins ne sont pas satisfaits et enfin (3) les sources de menaces[31] pouvant causer la non satisfaction desdits besoins. La combinaison d'une source de menace, d'un besoin de sécurité potentiellement violé et les impacts que cela entraine permet d'identifier un événement redouté. Les événements redoutés se verront par la suite affecter des niveaux de gravité en vue de les hiérarchiser [10].

Module 3 : *Etude des scénarios de menaces*

Le troisième module s'inscrit aussi dans l'appréciation des risques, puisque l'activité vise à déterminer les scénarios de menaces, c'est-à-dire, les enchainements d'opérations portant atteinte à la sécurité des biens essentiels. Pour cela, seront identifiées les différentes menaces[32] pesant sur le système, les sources de menaces les utilisant ainsi que les failles qu'elles peuvent exploiter. Il est question d'un scénario de menace lorsque se combine une source de menace, une menace et une vulnérabilité. Une fois les scénarios de menaces établis, reste à en estimer l'estimation de sa possibilité d'occurrence (la vraisemblance) [10].

Module 4 : *Etude des risques*

A ce stade, deux activités importantes sont à réaliser : (1) l'appréciation des risques et (2) l'identification des objectifs de sécurité. La méthode stipule qu'il existe un risque lorsqu'un couple (*événement redouté, scénario de menace*) existe. Ainsi, l'activité (1) consiste à corréler les événements redoutés avec les scénarios de menaces pour ne retenir que les scénarios pertinents en déterminant leur gravité et vraisemblance. Ensuite, il s'agira de les hiérarchiser pour décider de ceux qui seront traités et ceux qui seront écartés. L'activité

[28] Bien essentiel : Information ou processus jugé comme important pour l'organisme [10]. Pour ce type de biens, il est question d'apprécier les besoins de sécurité plutôt que les vulnérabilités.
[29] *Bien support* : Bien sur lequel reposent des biens essentiels [10].Pour ce type de biens, il est question d'apprécier les vulnérabilités plutôt que les besoins de sécurité.
[30] *Besoin de sécurité* : Définition précise et non ambiguë du niveau d'exigences opérationnelles relatives à un bien essentiel pour un critère de sécurité donné (disponibilité, confidentialité, intégrité…) [10].
[31] *Source de menace* : Chose ou personne à l'origine de menaces. Elle peut être caractérisée par son type (humain ou environnemental), par sa cause (accidentelle ou délibérée) et selon le cas par ses ressources disponibles, son expertise, sa motivation, etc. [10]
[32] *Menace* : Moyen type utilisé par une source de menace (vol de support, écoute passive, crue, etc.) [10].

quant à elle permettra de choisir, suite à l'évaluation de chaque risque, la manière par laquelle il sera traité afin de rendre le niveau du risque résiduel[33] acceptable. Par conséquent, pour chaque risque, un parmi ces quatre statuts sera retenu : évitement[34], réduction[35], maintien[36] ou transfert[37]. A ce niveau-là, le traitement est plus abstrait que fonctionnel [10].

Module 5 : *Etude des mesures de sécurité*

Cette dernière étape s'inscrit dans le cadre du traitement des risques. Elle vise à déterminer les moyens de traitement des risques ainsi que le suivi de leur déploiement. Les moyens identifiés devront permettre d'atteindre les objectifs de sécurité fixés. Les mesures de sécurité seront sélectionnées et appliquées telles qu'elles sont fournies dans les référentiels ou elles peuvent être adaptées ou conçues. Le déploiement des mesures devra faire l'objet d'un suivi pour vérifier que les objectifs de sécurité sont en tout temps atteints [10].

II. 4. Des modèles de sécurité pour exprimer les politiques de sécurité

II.4.1. Importance de la modélisation

Utiliser des modèles de sécurité facilite considérablement l'expression et la gestion des PS surtout pour des organisations dotées d'un grand nombre de ressources. Modéliser revient à user de formalismes, souvent mathématiques, pour abstraire et représenter subjectivement, mais pertinemment, un système. D'une part, cela favorise la compréhension du système, l'anticipation de son fonctionnement – en prévoyant ses propriétés –, la spécification de sa structure et de son comportement, la maîtrise de sa complexité et enfin la documentation de ses propriétés. D'autre part, la modélisation contribue au processus de preuve et de vérification nécessaire pour avoir une confiance élevée dans le système. En sécurité, il est prouvé que l'usage de modèles de sécurité offre tous les avantages précités et participe à la vérification de la complétude et de la cohérence des politiques de sécurité [33].

II.4.2. Etat de l'art des modèles de contrôle d'accès

Exprimer et administrer des politiques de contrôle d'accès grâce à des modèles discrétionnaires (DAC) [24] ou mandataires (MAC) [25, 26] complique considérablement cette tâche sensible, du fait de l'utilisation toute simple des concepts natifs du contrôle d'accès, à savoir les sujets, les objets et les actions. De nombreux autres concepts ont été, au fil des années, introduits pour remédier à cela : il s'agit principalement des concepts de

[33] *Risque résiduel* : Risque subsistant après le traitement du risque [86].
[34] Eviter un risque : changer le contexte pour ne plus y être exposé [10].
[35] Réduire un risque : mettre des mesures de sécurité pour réduire l'impact et/ou la vraisemblance [10].
[36] Prendre un risque : assumer les conséquences sans prise de mesure de sécurité supplémentaire [10].
[37] Transférer un risque : partager les pertes causées par un sinistre ou imputer la responsabilité à un tiers [10].

rôles [27], de vues [28] et de tâches [29] visant à agréger, dans l'ordre, les précédents éléments. Ils forment une deuxième couche d'abstraction supérieure à celle constituée par les éléments natifs. Conscients de l'importance du contexte de la requête dans le processus de la prise de décision, des modèles utilisant des règles de contrôle d'accès dynamiques ont été développés, tel que Rule-BAC [17]. Puis, pour répondre à la diversité croissante des contraintes du contrôle d'accès, d'autres modèles se sont focalisés sur la description des notions d'interdictions [31] et d'obligations [30] pour mieux exprimer les exceptions.

II.4.2.1. Les modèles classiques

II.4.2.1.1. Modèles discrétionnaires (DAC)

Les touts-premiers modèles de sécurité furent les modèles discrétionnaires où l'administration des droits d'accès reposait sur la notion de propriétaire. Cela procure un caractère décentralisé à l'administration des droits puisque chaque sujet dispose d'un contrôle absolu sur les objets dont il est propriétaire et qu'il est donc en mesure d'accorder quelconques droits, sur ses objets, à n'importe quel autre sujet du système [24]. D'autres variantes ont par la suite développé des commandes plus élaborées et ont introduit la notion de délégation des droits d'accès, dans le sens où le propriétaire d'un objet peut permettre à un autre sujet d'accorder certains droits sur l'objet en question [108, 109].

Dans les modèles DAC, les privilèges sont organisés sous forme d'une matrice dont les lignes représentent les sujets, les colonnes représentent les objets, alors que les cellules renseignent sur les droits détenus par le sujet de la ligne sur l'objet de la colonne (Fig. 9), il s'agit généralement d'actions élémentaires tel l'observation ou la modification [24]. La matrice est dynamique dans la mesure où des lignes et des colonnes sont rajoutées pour les nouveaux sujets et objets du système, néanmoins son administration devient fastidieuse au fur et à mesure qu'elle grandit, puisqu'il faut renseigner toutes les cellules de la matrice. Pouvant devenir complexe à implémenter, à stocker et à administrer, deux implémentations sont proposées dans [24, 108] : les *capacités* et les *listes de contrôle d'accès*.

Hormis leur simplicité, leur flexibilité et leur caractère décentralisé, les modèles discrétionnaires souffrent de plusieurs limitations ; tout d'abord, ils se limitent seulement à l'expression d'autorisations sans nulle considération des contextes des accès : le contrôle des accès n'est donc pas dynamique. Une autre faiblesse est due à la confiance que requièrent ces modèles, en effet, en accordant un droit à un autre sujet sur un objet, celui est en mesure d'en recopier le contenu dans un autre fichier et de le mette à disposition d'un sujet non autorisé. De plus, les modèles discrétionnaires sont impuissants contre la menace des chevaux de Troie et des canaux cachés puisque nul contrôle des flux n'est opéré. Dans ce sens, les modèles s'intéressent simplement à la vérification instantanée des privilèges

d'accès, sans se soucier des manipulations opérées par la suite. Pour finir, le concept de délégation n'est pas sûr puisqu'il n'est pas possible d'assurer, qu'après une séquence de délégations, un utilisateur non autorisé à accéder à un objet l'est toujours.

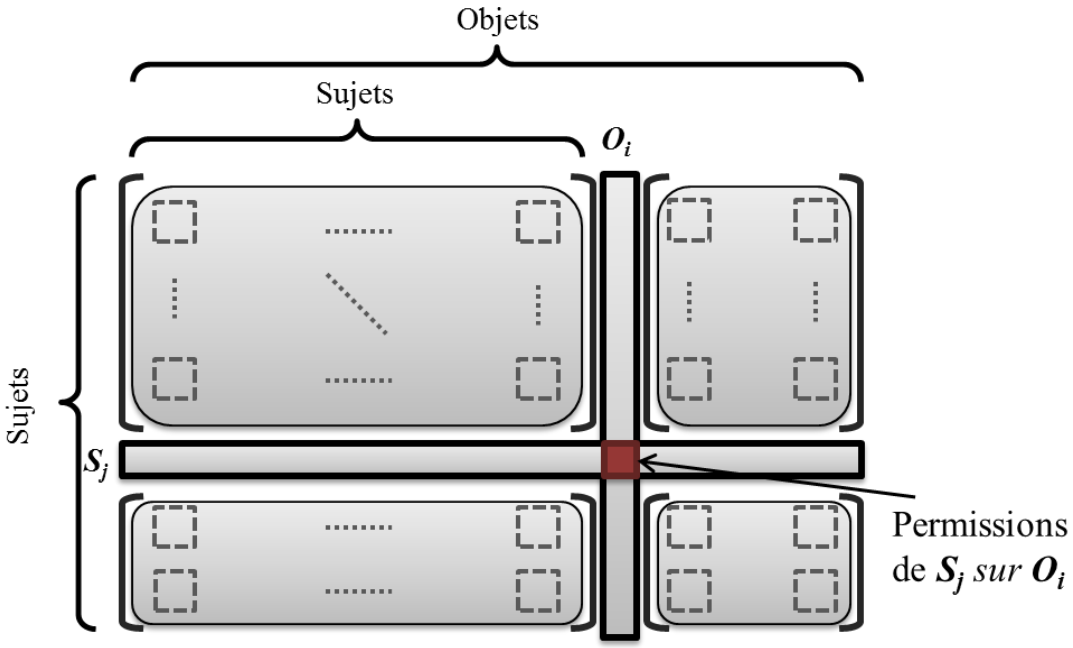

Fig. 9. Matrice de contrôle d'accès des modèles DAC.

D'autres modèles par la suite ont tenté de remédier à ces limitations : les modèles mandataires ont corrigé la limitation du contrôle de flux, nous détaillerons l'un de ces modèles, en section (II.4.2.2.1) ; le problème de complexité a été traité par les modèles qui ont introduit des entités abstraites tels RBAC [27], VBAC [28], TBAC [29], TMAC [110] et ORBAC [32]. OrBAC ainsi que d'autres modèles, ont aussi pallié la limitation du statisme lors de la prise de décision de contrôle d'accès, comme nous le verrons par la suite.

II.4.2.1.2. Modèles basés sur les rôles (RBAC)

RBAC est le tout premier modèle à introduire une entité abstraite pour gérer les entités natives du contrôle d'accès. S'inspirant de la réalité des organisations, RBAC fait intervenir le concept de rôle pour abstraire une fonction spécifique au sein de ces structures (directeur, comptable, etc.). Ainsi, à la lecture de la PS, il est facile d'assimiler la structure de l'organisation [111]. Par conséquent, un rôle agrège tous les sujets occupant une même fonction (i.e. réalisant les mêmes tâches) ce qui implique donc que tous les sujets d'un rôle jouissent des mêmes privilèges au sein du système. Cela réduit grandement la complexité des PS et améliore leur administration. En effet, les privilèges ne sont plus accordés à chaque sujet à part mais plutôt au rôle, comme l'illustré (Fig. 10). Soulignons que les rôles

sont, généralement, nettement moins nombreux que les sujets. Concrètement, plusieurs permissions peuvent être attribuées à un rôle et une même permission peut être accordée à plusieurs rôles ; aussi un sujet peut-être affecté à plusieurs rôles et à l'inverse un rôle peut-être attribué à plusieurs sujets. Dans le cas de sujets jouant plusieurs rôles, les sujets jouiront, simultanément sauf contraintes, des privilèges accordés aux rôles qu'ils jouent [112].

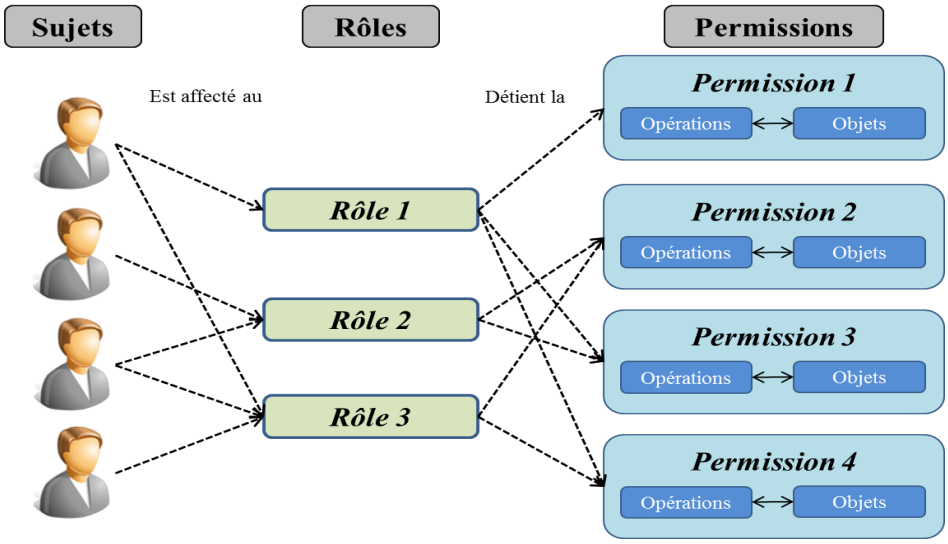

Fig. 10. Attribution des permissions dans RBAC

De multiples extensions de RBAC ont été développées au fil des années introduisant plusieurs concepts, tel que celui des sessions, celui des hiérarchies de rôles et celui des contraintes de séparation de tâches [27, 113, 114, 115, 116] . Pour des raisons de praticité, nous nous référons à la proposition de standard publiée en 2001 [27] et qui fait état de quatre modèles, comme présenté dans la figure (Fig. 11).

RBAC de base ou *Core RBAC*

Core RBAC est le modèle de base sur lequel s'appuient toutes les extensions développées. En plus du concept de rôle, il intègre aussi le concept de sessions offrant la possibilité de sélectionner les rôles à activer pour la réalisation d'une tâche. Plus en détail, à l'initialisation d'une session, l'utilisateur s'authentifie puis active certains de ses rôles ; il est donc capable de réaliser les tâches permises par les privilèges accordés aux rôles activés. L'intérêt de la session est de ne pas forcer le sujet à se ré-authentifier pour chaque accès ; en outre, cela permet de restreindre, dans une certaine mesure, les privilèges d'un utilisateur conformément au principe du moindre privilège. Ci-après, nous nous limiterons à la description de certains éléments de Core-RBAC (plus de détails sont pourvus en [27]) :

- *U*, *R*, *O*, *Op*, *P*, *S* sont respectivement les ensembles d'utilisateurs, de rôles, d'objets, d'opérations, de permissions et de sessions ;

- $P = 2^{(Op \times O)}$, est l'ensemble des permissions ;
- $UA \subseteq U \times R$, une relation affectant les rôles aux utilisateurs ;
- $PA \subseteq P \times R$, une relation affectant les permissions aux rôles ;
- $util\_assignés(r) = \{u \in U \mid (u, r) \in UA\}$, fonction permettant d'établir les sujets assignés à un certain rôle *r* ;
- $perm\_assignés(r) = \{p \in P \mid (p, r) \in PA\}$, fonction permettant d'établir les permissions assignées à un certain rôle *r* ;
- $roles\_session(s) \subseteq \{r \in R \mid (util\_session(s), r) \in UA\}$, fonction permettant d'établir les rôles activés durant une session *s*, avec *util_session(s)* retourne l'utilisateur initiateur de la session *s* ;

Outre la facilité d'exprimer des politiques reflétant la structure des organisations ainsi que la gestion de leur complexité, ce modèle demeure très basique. Il est néanmoins enrichi par les concepts introduits dans les extensions suivantes.

RBAC hiérarchisé ou *Hierarchical RBAC*

Le concept de hiérarchie est traduit mathématiquement par une relation d'ordre partiel définissant une supériorité entre les rôles : les rôles seniors acquérant les privilèges de leurs juniors, rendent inéluctablement les utilisateurs des rôles seniors, des membres des rôles juniors. Ce concept améliore beaucoup l'administration des PS puisqu'il instaure un mécanisme d'héritage des privilèges entre les rôles. L'idée provient du fait que dans les organisations, certains privilèges sont généraux et doivent être accordés à plusieurs rôles ; au lieu de les accorder à chaque rôle à part, il est plus simple de les accorder à un rôle puis d'en faire hériter les autres. En général, il est question d'héritage dans deux cas de figures : (1) les relations de hiérarchie organisationnelle ou (2) les relations de spécification ou de généralisation. Concernant la première, un exemple simple serait de citer la relation entre un directeur d'hôpital et ses médecins, le directeur n'étant pas nécessairement un médecin. En revanche, pour le deuxième cas, nous évoquons le cas des cardiologues et urologues qui sont des médecins généralistes s'étant spécialisés. Dans [27], les auteurs distinguent deux concepts de hiérarchies, des « *hiérarchies généralisées* » et d'autres « *limitées* ».

RBAC avec contraintes statiques de séparation des tâches (SSD)

Le principe de la séparation des tâches a été intégré à RBAC en vue de pouvoir exprimer des politiques tenant compte d'éventuels conflits d'intérêts. Dans le cas de RBAC, les conflits d'intérêts peuvent se matérialiser lorsqu'un utilisateur se voit accorder des privilèges propres à des rôles en conflit. Pour résoudre ces problèmes de conflits d'intérêts, une solution statique est proposée dans cette variante ; elle consiste à établir tous les rôles

en conflits afin d'éviter de les accorder conjointement aux utilisateurs du système (exclusion mutuelle des rôles). Ces contraintes risquent cependant d'introduire des incohérences lorsqu'elles sont couplées au concept de hiérarchies ; ceci dit, les auteurs proposent de tenir compte, simultanément, des rôles hérités et de ceux directement accordés à l'utilisateur et de leur appliquer les contraintes de séparation des tâches.

RBAC avec contraintes dynamiques de séparation des tâches (DSD)

Similairement à l'approche adoptée dans la variante précédente, celle-ci aussi vise à respecter les conflits d'intérêts lors de la description de la PS, à la différence, que les contrôles s'opèrent au moment de l'activation des rôles au cours d'une session. Partant de ce fait, un utilisateur peut se voir accorder des rôles en conflit, en revanche, il ne pourra pas les activer simultanément. Nous pouvons affirmer qu'il s'agit là de la variante la plus adaptée à l'application du principe de *moindre privilège*.

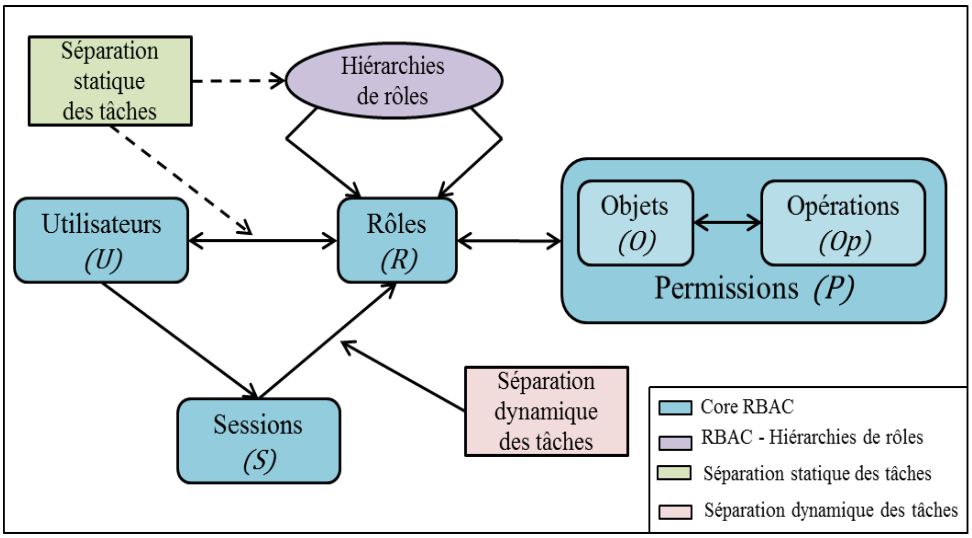

Fig. 11. Les types de RBAC

En définitive, RBAC facilite grandement l'expression ainsi que l'administration des PS, toutefois, il demeure limiter quant à la prise en compte des contextes dans la prise de décision de contrôle d'accès. En effet, prenons le cas de règles telles que « seuls les médecins traitants peuvent lire les informations médicales du dossier d'un patient », ce genre de règles ne peut être exprimé avec RBAC. Un autre point faible est sensiblement critique, il est question de la granularité des politiques, puisque RBAC n'intègre pas de mécanisme de gestion des exceptions, en plus du fait que tous les sujets d'un rôle héritent tous les mêmes privilèges, or dans certains organisations, des contraintes d'expertise et d'expérience peuvent limiter cela. D'autres critiques concernant l'établissement des sessions, la gestion des relations de dominance au sein des hiérarchies ont été énoncées dans [117].

A l'image de RBAC, d'autres modèles tels que que VBAC, TBAC et TMAC ont introduit des concepts d'abstraction. OrBAC, en revanche, les conjugue tous autour du concept de l'organisation pour fournir un modèle encore plus adapté à la réalité des entreprises et ce en palliant aussi le problème des décisions de contrôle d'accès contextuelles.

II.4.2.1.3. Modèle OrBAC

Conçu dans le but de pallier les limitations des modèles auxquels il succède, OrBAC apporte des solutions au manque de dynamisme et aux politiques exclusivement fermées exprimées grâce à ceux-ci. OrBAC est une extension de RBAC visant à conjuguer les points forts de ses prédécesseurs en vue d'offrir un modèle riche pour l'expression de PS fines et pertinentes tout en minimisant la charge administrative – réduisant les coûts et les erreurs humaines pouvant en résulter. OrBAC facilite grandement la gestion des PS en réduisant leur complexité à travers, entre autres, la réduction du nombre de règles de sécurité constituant les PS. Aussi, afin d'assurer un compromis entre le respect du principe du *moindre privilège* et la flexibilité requise par le contrôle d'accès, OrBAC tient compte de la dimension contextuelle dans la décision de contrôle d'accès [32]. Pour atteindre ces objectifs, OrBAC met en place deux niveaux complets d'abstraction : un niveau abstrait et un niveau concret. En effet, les entités *rôle*, *vue* et *activité* du niveau abstrait agrègent respectivement les *sujets*, les *objets* et les *actions*. Il s'articule autour du concept d'organisation. Celle-ci se définit comme un groupement organisé et structuré d'entités actives jouant des rôles – néanmoins, tout groupement de sujets ne constitue pas nécessairement une organisation [33]. Chaque organisation définit les différentes entités abstraites en accord avec son métier, ses contraintes et ses spécificités. Plus encore, OrBAC permet de décrire des politiques très élaborées, puisque chaque département d'une organisation peut être vu comme une organisation à part entière et ainsi se voir exprimer une politique adaptée à ses besoins.

Structurer les différentes entités concrètes sur la base de propriétés et critères communs facilite l'affectation et la mise-à-jour de leurs privilèges d'accès, comme le montre la figure (Fig. 12). La politique décrite à l'aide d'entités abstraites reflète fidèlement la politique organisationnelle de l'organisation – ce type de politiques sont souvent évolutives et reproductibles – et permet un détachement de l'implémentation concrète de celle-ci. Il en découle une meilleure structuration, plus de flexibilité et une réduction notable de la complexité. Aussi est-il important de noter qu'importe les réajustements éventuels au niveau concret, ces derniers n'engendreront pas des conflits difficilement corrigeables [107]. En résumé, l'intérêt de l'utilisation de deux niveaux d'abstraction se décline comme suit [32] :

- Niveau abstrait : permet de décrire la PS grâce à des entités abstraites sans se soucier de la manière avec laquelle chaque organisation les implémente.

- Niveau concret : répond aux requêtes d'accès des sujets en leur accordant les privilèges sur la base des règles définissant l'organisation, le rôle du sujet, l'action requise (i.e. l'activité), l'objet cible (i.e. la vue) et le contexte.

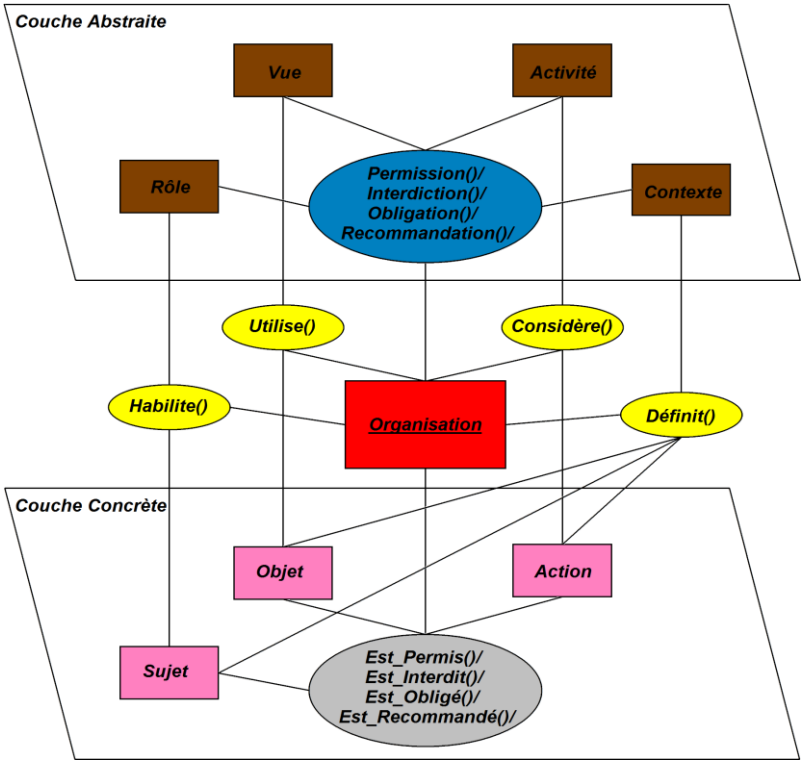

Fig. 12. Représentation des couches d'abstraction du modèle OrBAC.

L'entité *contexte* permet de spécifier les conditions régissant la validité d'une règle relativement aux diverses conjonctures rencontrées par l'organisation. Le contexte peut se rapporter à n'importe quelle entité abstraite, décrivant sa situation et ses contraintes à un instant donné. Pour illustrer ce concept, nous citons quelques exemples de contextes : l'urgence, les contraintes de s*éparation de tâches* (SoD), les attributs spatio-temporels, etc. Les contextes aident à mieux appliquer le principe du *moindre privilège* et à offrir un contrôle d'accès d'une plus grande granularité. Aussi avant d'accorder ou de refuser toute requête d'accès, le système doit tout d'abord vérifier le contexte courant en tenant compte du rôle (i.e. le sujet), de la vue (i.e. l'objet) et de l'activité (i.e. l'action).

En résumé ; les entités constituant la politique de contrôle d'accès d'une organisation *Org*, exprimée grâce à OrBAC, sont les suivantes :

S, R, O, V, AC, AY, C : Ensembles respectifs des *sujets*, des *rôles*, des *objets*, des *vues*, des *actions*, des *activités* et des *contextes* d'*Org*.

Pour gérer les affectations respectives, des rôles aux sujets, des objets aux vues et des actions aux activités, OrBAC introduit trois prédicats (relations). Le point commun entre ces prédicats est le paramètre central « *Organisation* ». Nous considérons les éléments suivants de la politique de sécurité d'une organisation *Org* : $s \in S$, $r \in R$, $o \in O$, $v \in V$, $ac \in AC$, $ay \in AY$, $c \in C$ et détaillons ces prédicats :

- *Habilite*(*Org, s, r*) : Prédicat pour l'affectation d'un rôle à un sujet ; il signifie qu'au sein d'*Org*, le sujet *s* est habilité au rôle *r*.
- *Utilise*(*Org, o, v*) : Prédicat pour l'affectation d'un objet à une vue ; il signifie qu'au sein d'*Org*, l'objet *o* est répertorié au sein de la vue *v*.
- *Considère*(*Org, ac, ay*) : Prédicat pour l'affectation d'une action à une activité : au sein d'*Org*, l'action *ac* est incluse dans l'activité *ay*.

Afin de pallier la limitation des politiques fermées, OrBAC propose quatre modes d'accès (Fig. 13) pour répondre à la richesse des contraintes du contrôle d'accès. Le modèle ne se limite pas uniquement aux permissions ; bien au contraire, il introduit trois autres modes d'accès : « *Interdiction* », « *Obligation* » et « *Recommandation* ». Les interdictions expriment explicitement le refus d'accorder une permission à un rôle *r* pour la réalisation d'une activité *ay* sur une vue *v*. Elles sont le moyen idéal pour spécifier les exceptions : par exemple, lorsque tous les sujets d'un rôle sont autorisés à réaliser tâche sauf un sujet bien déterminé. Les obligations, quant à elles, se rapportent à des activités/actions devant nécessairement être réalisées sous peine de mener le système vers un état non sûr. Par conséquent, elles sont considérées comme des permissions dont la nécessité de réalisation est stricte. Enfin, les recommandations sont aussi des permissions n'atteignant pas le même degré de contrainte qu'une obligation. Ce mode d'accès est quelque peu préventif.

Les prédicats OrBAC détaillant l'octroi des privilèges sont décrits, syntaxiquement et sémantiquement, comme suit :

- *Permission*(*Org, r, v, ay, c*) (resp. *Interdiction*(), *Obligation*(), *Recommandation*()) : Prédicat regroupant les entités abstraites pour la définition des règles d'accès au niveau abstrait : au sein d'*Org*, le rôle *r* est autorisé à réaliser l'activité *ay* sur la vue *v* en présence du contexte *c*.
- *Définit*(*Org, s, o, ac, c*) : Prédicat réunissant les éléments concrets de la tâche ciblée par la requête d'accès : au sein d'*Org*, l'accès est défini par le sujet *s* réalisant l'action *ac* sur l'objet *o* en présence du contexte *c*.
- *Est_Permis*(*s, o, ac*) (resp. *Est_Interdit*(), *Est_Recommandé*(), *Est_Obligé*()) : Prédicat regroupant les entités concrètes pour la définition des règles d'accès au niveau concret : le sujet *s* est autorisé à réaliser l'action *ac* sur l'objet *o*.

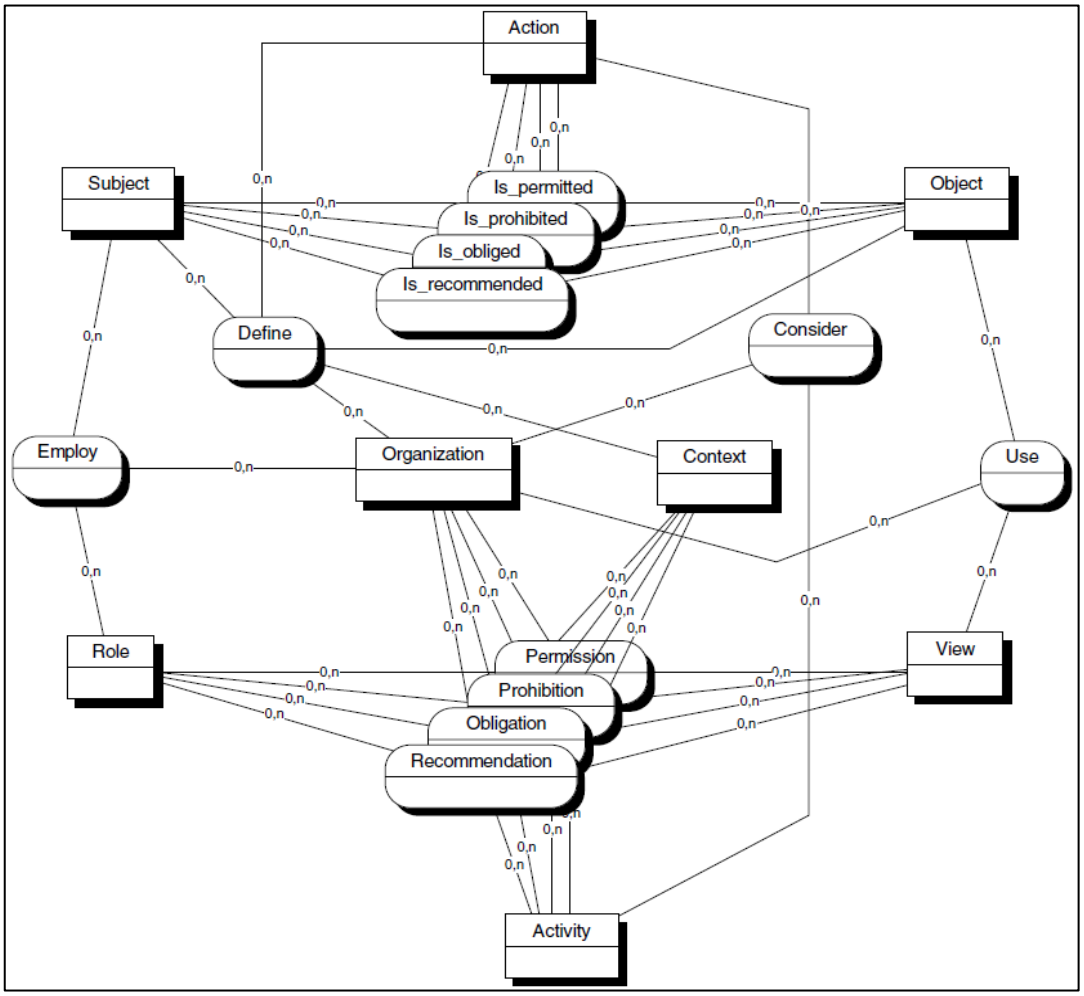

Fig. 13. Modèle OrBAC [32].

Généralement, les règles de sécurité assurant concrètement le contrôle d'accès sont de type (*s*, *o*, *a*), comme celles décrites dans le modèle HRU [108]. Dans OrBAC, ce type de règles est exprimé par les prédicats *Est_Permis*(), *Est_Interdit*(), *Est_Obligé*() et *Est_Recommandé*(). Avec OrBAC, il n'est pas nécessaire d'éditer toutes les règles du type (*s*, *o*, *a*) puisqu'elles seront dérivées au fur et à mesure que les requêtes seront adressées au système, à la suite de l'inférence entre les règles ci-après :

$$
\begin{aligned}
&Permission(\mathrm{Org}, \mathrm{r}, \mathrm{v}, \mathrm{ay}, \mathrm{c}) \\
&\wedge\ Habilite(\mathrm{Org}, \mathrm{s}, \mathrm{r}) \\
&\wedge\ Utilise(\mathrm{Org}, \mathrm{o}, \mathrm{v}) \\
&\wedge\ Considère(\mathrm{Org}, \mathrm{ac}, \mathrm{ay}) \\
&\wedge\ Définit(\mathrm{Org}, \mathrm{s}, \mathrm{o}, \mathrm{ac}, \mathrm{c}) \\
&\Longrightarrow\ Est\_Permis(\mathrm{s}, \mathrm{o}, \mathrm{ac})
\end{aligned}
$$

En définitive, nous pouvons affirmer que le modèle OrBAC présente bien des avantages par rapport aux autres modèles. Il reste néanmoins limité en ce qui concerne la fourniture de l'intégrité, comme nous le montrerons par la suite (II.5.2).

II.4.2.2. Les modèles d'intégrité

Contrairement aux modèles préservant la confidentialité, les modèles d'intégrité visent à préserver l'état des objets et informations contre les éventuelles corruptions et altérations possibles. Selon [118], le premier modèle visant à assurer l'intégrité fut Biba [26], puis lui succédèrent d'autres modèles notamment Goguen Meseguer [119], Sutherland [118], Clark & Wilson [120], Brewer Nash (i.e. Muraille de Chine) [121] et plus récemment Totel [122]. Cet intérêt grandissant a eu pour objectif la satisfaction des besoins en intégrité des systèmes commerciaux ne tolérant pas les altérations. Ces modèles d'intégrité ne satisfont pas correctement les besoins d'intégrité des IIC, soit faute d'un excès de rigidité ou encore à cause de la non-prise en compte de ces besoins lors de leur conception.

II.4.2.2.1. Modèle de Biba

Biba est le premier à avoir proposé un modèle mandataire traitant les questions d'intégrité. Il succède au modèle de confidentialité de Bell-LaPadula [25], dont il est considéré le dual. Biba considère que la compromission de l'intégrité d'un système est définie comme une modification de son état laquelle ne figure pas parmi l'ensemble de ses états sûrs. Une politique d'intégrité aura ainsi pour but de n'autoriser que les modifications qui préserveront la validité des éléments et les propriétés attendues du système [26]. Etant le dual du modèle de Bell-LaPadula, le modèle de Biba se base aussi sur les mécanismes de labels et de treillis. Ainsi, le modèle intègre des classes d'intégrité (*Important*, *Très important* et *Crucial*) ainsi que des compartiments d'intégrité (i.e. les catégories) dont l'objectif est de partitionner les ensembles de sujets et d'objets sur la base de critères fonctionnels. Par suite, chaque élément du système est défini par un couple (*compartiment d'intégrité, classe d'intégrité*). Les classes d'intégrité seront déclarées des *niveaux d'habilitation* lorsqu'il s'agira de sujets, ou des *niveaux de classification* s'il s'agit d'objets. Les niveaux de classifications sont accordés aux objets en accord avec les dommages potentiels suite à la corruption de l'information qu'ils contiennent. Tandis que l'octroi des niveaux d'habilitation aux sujets est contraint par le niveau d'intégrité de leurs utilisateurs ainsi que par le principe de *moindre privilège*. Biba vise deux objectifs principaux, à travers son modèle : (1) l'interdiction de toute propagation d'une information issue d'un objet de piètre niveau d'intégrité vers un objet de niveau d'intégrité supérieur et (2) l'interdiction à tout sujet d'un certain niveau d'intégrité de modifier un objet de niveau d'intégrité supérieur.

Biba propose trois familles de politiques d'intégrité mandataires, basés toutes sur les éléments suivants :

- S, O, I : Ensemble respectifs de *sujets*, d'*objets* et de *niveaux d'intégrité* ;
- $il : S \times O \rightarrow I$, fonction affectant un niveau d'intégrité à tout sujet ou objet ; les sujets et objets sont caractérisés par un niveau d'intégrité à tout instant ;
- $\leq$: une relation de dominance définie sur un sous-ensemble de $I \times I$;
- obs : une relation définie sur un sous-ensemble de $S \times O$ définissant la capacité d'un sujet $s \in S$ de consulter un objet $o \in O$;
- mod : une relation définie sur un sous-ensemble de $S \times O$ définissant la capacité d'un sujet $s \in S$ à modifier un objet $o \in O$;
- inv : une relation définie sur un sous-ensemble de $S \times S$ définissant la capacité d'un sujet $s_1 \in S$ d'invoquer un autre sujet $s_2 \in S$.

Dans ce qui suit, nous rappelons lesdites politiques :

- *Politique d'intégrité stricte* : Cette politique vise à garantir que l'intégrité d'un sujet ou d'un objet ne pourra pas être altérée volontairement ou accidentellement par un sujet de niveau d'intégrité inférieur. Les niveaux d'intégrité des sujets et des objets sont fixes et sont régis par trois règles mandataires qui sont :
  - Règle d'observation : $\forall (s, o) \in S \times O,\ s\ obs\ o \Longrightarrow il(s) \leq il(o)$ (1)
  - Règle de modification : $\forall (s, o) \in S \times O,\ s\ mod\ o \Longrightarrow il(o) \leq il(s)$ (2)
  - Règle d'invocation : $\forall (s_1, s_2) \in S \times S,\ s_1\ inv\ s_2 \Longrightarrow\ il(s_2) \leq il(s_1)$ (3)

  Les règles (1) et (2) portent les noms respectifs de « *No Read Down* » et « *No Write Up* » ; elles garantissent respectivement qu'un sujet ne peut accéder à une information de niveau inférieur au sien et qu'un objet ne peut être corrompu par un sujet de niveau inférieur au sien. La règle (3) quant à elle préserve un sujet des perturbations pouvant émaner d'un sujet de niveau inférieur ; elle est interprétée comme la prévention contre la modification de l'état d'un sujet par un autre de moindre intégrité. En plus des niveaux d'intégrité statiques, ces règles sont relativement contraignantes et peuvent entraver la réalisation des tâches. Mentionnons aussi que cette politique souffre de la dégradation des niveaux d'intégrité des informations, puisqu'une information copiée depuis un objet de haute intégrité vers un objet de moindre intégrité fait que son niveau chute.

- *Politiques Low Water Mark (politique du plus bas niveau)* : Cette famille regroupe trois politiques distinctes. Leur point commun est qu'elles sont dynamiques, comparées à la précédente. L'aspect dynamique se décline à travers des niveaux d'intégrité n'étant pas fixes.

  - *Low Water Mark pour les sujets* : Cette politique stipule qu'un sujet peut consulter tous les objets du système, sauf que son niveau d'habilitation changera pour refléter le niveau d'intégrité de l'information la plus basse qu'il ait consulté. La règle (1) devient ainsi :

    $$\forall (s,o) \in S \times O, \qquad s\ obs\ o \Longrightarrow il'(s) = \min(il(s), il(o)) \qquad (4)$$

    avec $il'(s)$ est le nouveau niveau d'intégrité de s après la consultation de l'objet o, tandis que $il(s)$ est le niveau d'intégrité du sujet juste avant la consultation. La limitation de cette politique est que les niveaux des sujets ne peuvent que décroître sans moyen de réhabilitation. Ainsi, à un moment donné, les objets de haute intégrité risquent d'être marginalisés faute de sujets de bas niveau.

  - *Low Water Mark pour les objets* : Comme la précédente politique, celle-ci est aussi dynamique, cependant, ce sont les niveaux de classification qui changent. La politique stipule qu'un objet peut être modifié par n'importe quel sujet, mais son niveau reflétera le niveau de l'information lui ayant été fournie par le sujet. Le niveau de l'information égale le niveau du sujet qui l'a communiqué. Ainsi la règle (4) est maintenue et la (2) devient aussi :

    $$\forall (s,o) \in S \times O, \qquad s\ mod\ o \Longrightarrow il'(o) = \min(il(s), il(o)) \qquad (5)$$

    avec $il'(o)$ le niveau d'intégrité de o après avoir été modifié par s, alors que $il(o)$ est le niveau de l'objet juste avant la modification. Avec cette politique, les objets ne sont plus protégés contre les modifications inappropriées ; les modifications sont juste mises en évidence à travers la dégradation des niveaux des objets. Plus grave encore, il existe un état où tous les éléments du système, sujets et objets, seront au plus bas niveau d'intégrité.

  - *Low Water Mark Integrity Audit* : Contrairement aux deux précédentes variantes, celle-ci préserve les niveaux d'intégrité intacts en gardant trace des actions dans de nouveaux paramètres : les « *niveaux de corruption* » (cl). Le principe ainsi que le calcul de ces niveaux de corruption est le même que dans les deux précédentes politiques. Ainsi à l'issu de l'observation d'un objet o par un sujet s, le niveau de corruption du sujet est :

    $$\forall (s,o) \in S \times O, \qquad s\ obs\ o \Longrightarrow cl'(s) = \min(cl(s), cl(o)) \qquad (6)$$

    La modification de o par s fait que le niveau de corruption de o devient :

$$\forall (s,o) \in S \times O, \qquad s\ mod\ o \Longrightarrow il'(o) = \min(il(s), il(o)) \qquad (7)$$

Pour cette variante, Biba évoque une possibilité de recouvrement des niveaux de corruptions des objets. Toutefois, la protection contre les modifications inappropriées n'est pas assurée, elles sont juste mises en évidence.

- *Politique en anneau* : L'intégrité des données étant plus menacée par les modifications que par les observations, cette variante se base sur ce constat pour rajouter plus de flexibilité. Dans ce sens, cette politique stipule que les observations ne sont nullement contraintes, ainsi tout sujet peut consulter n'importe quel objet du système ; en revanche les modes modification et invocation sont régis par les mêmes règles (2) et (3) de la politique d'intégrité stricte.

Biba propose aussi un modèle discrétionnaire pour la fourniture de l'intégrité, néanmoins, nous préférons nous limiter à ses politiques mandataires considérées comme références en la matière. Les fondements du modèle de Biba furent étendus par Totel [122, 123] afin de permettre la collaboration de logiciels ayant des niveaux de criticité différents au sein d'un système. D'autres extensions ont tenté de rendre les politiques de Biba plus flexibles en appliquant, entre autres, les règles mandataires sur des intervalles formés par des plus bas niveaux de consultation et des plus hauts niveaux de modification [124].

En définitive, vu son caractère centralisé, Biba répond ainsi au besoin d'autonomie des IIC puisqu'il leur permet d'exprimer des PS locales. Aussi l'administration des PS est assez aisée puisque le concept de treillis automatise les décisions de contrôle d'accès et que les niveaux d'intégrité sont fixés une fois pour toutes. Un autre besoin des IIC auquel répond relativement bien Biba est le concept de priorisation, en effet, les exigences d'intégrité des objets et sujets sont quantifiés. Cependant, les exigences d'intégrité propres aux actions et aux contextes ne sont pas mesurées. En outre, les PS ne sont pas dynamiques vu que les règles mandataires s'appliquent impérativement quel que soit le contexte. De plus, les niveaux d'intégrité sont soit figés soit d'une monotonie décroissante sans possibilité de recouvrement. En revanche, nous pouvons affirmer que les PS décrites par Biba s'adaptent au facteur d'échelle puisque tous les sujets d'un même niveau d'intégrité ont les mêmes privilèges ; toutefois, il n'existe pas de mesures d'agrégation visant à améliorer la structuration des ressources au sein des catégories. De plus, les règles mandataires empêchent une description granulaire et flexible des PS tout en respectant le principe du *moindre privilège*, puisque les exceptions et les contraintes de séparations de tâches ne peuvent être exprimées, sans oublier aussi que les sujets de haute intégrité ne peuvent pas lire des objets de basse intégrité, même si dans certains cas, cela s'avère nécessaire.

II.4.2.2.2. Clark & Wilson

Contrairement à Biba, le modèle de Clark & Wilson (CW) [120] fut conçu pour satisfaire les besoins d'intégrité des systèmes commerciaux, principalement la prévention des fraudes et des erreurs. CW est un modèle mandataire basé sur deux principaux concepts : la *séparation des tâches* et les *transactions bien formées*. Le premier a été expliqué en section (I. 3) tandis que le second stipule que les données ne peuvent être modifiées que par des *procédures de transformation* (TP) certifiées, garantissant leur intégrité. Ce modèle vise la préservation de la cohérence interne et externe. Soulignons que le concept des TP est très abstrait, ceci dit, concrètement, ces procédures doivent être correctement conçues et implémentées ; leur installation sur le système ainsi que leur mise-à-jour doivent être contrôlée et enfin les données qu'elles génèrent doivent être vérifiées. La vérification est réalisée par des composants nommés « *procédures de vérification de l'intégrité* » (IVP). En plus, le modèle distingue deux types de données : « *données contraintes* » (CDI) et « *données non contraintes* » (UDI). Les premières sont celles soumises aux règles de manipulation mandataires pour préserver leur intégrité ; elles ne sont donc manipulées qu'à travers les TP uniquement. Suite à chaque exécution d'une TP, les IVP s'exécutent pour confirmer que toutes les CDI sont conformes à la spécification de leur intégrité. En revanche, la deuxième catégorie regroupe les données dont l'intégrité n'a pas encore validé et qui sont donc manipulées arbitrairement. Cette catégorie est essentielle puisque toute donnée nouvellement introduite au système passe par elle avant d'être manipulée par une TP qui la transformera en CDI dont l'intégrité est vérifiée par une IVP. Cette fonction est interprétée comme un moyen d'augmenter le niveau d'intégrité d'une donnée lorsque cela s'avère nécessaire.

Les PS décrites grâce à CW s'expriment par le biais de triplets du genre :

$$(\text{utilisateur authentifié}, \text{TP}_i, \text{sous} - \text{ensemble de CDI})$$

ainsi le système devra garantir que seuls les TP autorisées pourront manipuler les CDI. Si cela se vérifie, cela impliquera qu'en tout temps l'intégrité d'une CDI est préservée. De plus, les politiques sont soumises à cinq « *règles de certification* » (*certification rules*) et à quatre « *règles d'application* » (*enforcement rules*) [120].

Quoique proche des exigences des systèmes commerciaux, CW présente certaines limitations vis-à-vis des besoins des IIC. En effet, les PS ne sont ni dynamiques – nul considération des contextes – ni évolutives –pour chaque CDI, l'administrateur doit déclarer les TP et IVP devant la manipuler –, cela rend donc l'administration ardue. A l'inverse, déterminer pour chaque CDI, les TP et IVP qui le manipuleront, rend les PS granulaires. Aussi, les catégories CDI et UDI peuvent être interprétées comme un moyen d'application du concept de priorisation, toutefois, cela ne reflète pas vraiment la réalité des IIC. Dans ce sens, certaines variantes ont tenté de pallier les problèmes d'évolutivité et de priorisation

en introduisant, entre autres, une deuxième couche d'abstraction – formée de rôles, de domaines et de types – ainsi qu'une modélisation en multi-niveaux d'intégrité [125].

II.4.2.3. Les modèles distribués

Les environnements collaboratifs sont constitués d'une multitude d'organisations coopérant, échangeant des données et interagissant en vue d'atteindre des objectifs fixés. Toutefois, les comportements de ces partenaires demeurent imprévisibles. En effet, pour des raisons de compétitivité déloyale, certains peuvent fournir des services non conformes, divulguer des secrets industriels voire même corrompre les ressources des partenaires. Pour ces raisons, chaque organisation doit garder le contrôle sur ses propres ressources, conformément au besoin d'autonomie. Ainsi, développer une politique globale régissant la collaboration puis l'imposer aux différentes parties n'est tout simplement pas concevable à cause, notamment, des intérêts parfois divergents des participants en plus de la suspicion. Cela sous-entend donc que chaque organisation se chargera de contrôler les accès d'agents externes à ses ressources sur la base de la PS qu'elle aura établie. Nous étudions, dans ce qui suit trois approches différentes visant à mettre en place des collaborations sécurisées.

II.4.2.3.1. Modèle PolyOrBAC

Pour pallier les limitations de MultiOrBAC [126], une extension d'OrBAC aux environnements distribués, un autre modèle fut proposé pour mieux satisfaire les besoins collaboratifs des IC. Ce modèle porte le nom de « Poly-OrBAC » [127, 128]. Basé sur OrBAC – notamment pour répondre au besoin d'autonomie des IC – l'extension bénéficie bien évidemment de la multitude d'avantages offerts par ce modèle. Cette extension enrichit OrBAC de mécanismes fournissant aux organisations un cadre sécurisé pour l'échange de services et de ressources afin de réaliser les objectifs des collaborations. A cette fin, Poly-OrBAC repose sur deux piliers principaux : les « *Services Web* » et les « *contrats électroniques* » [34]. La technologie des services web offre une plateforme indépendante de protocoles et de standards pour l'échange de services et de données hétérogènes, tandis que les contrats électroniques permettent d'établir les termes d'accords en spécifiant les clauses, les conditions et les pénalités encourues en cas de manquement aux accords. Durant la collaboration, les contrats électroniques permettent d'effectuer un suivi des actions en vue de détecter quelconques abus. En somme, Poly-OrBAC est un framework qui offre, d'une part le contrôle d'accès en interne, assuré grâce à OrBAC, et d'autre part il permet d'instaurer des collaborations sécurisées entre les organisations.

Plus en détail, une organisation (*Org*) désirant bénéficier d'un service, consulte tout d'abord un annuaire UDDI [129] regroupant l'ensemble des services web offerts par les fournisseurs. Une fois le service choisi, *Org* contacte le fournisseur, puis un accord est

conclu entre ce dernier et *Org*. L'accord est ensuite formalisé par un contrat électronique servant à spécifier les fonctions et paramètres du service web, les responsabilités de chaque partie ainsi que les règles de sécurité qui régiront la collaboration. Des alarmes sont automatiquement générées en cas d'abus ; ceux-ci sont imputés à leurs acteurs à l'issue d'audits. Les règles de sécurité du contrat sont exprimées par le biais de la syntaxe d'OrBAC. Cependant, pour rester fidèle à la sémantique des prédicats d'OrBAC, qui est un modèle centralisé, deux nouveaux concepts lui ont été introduits pour intégrer les aspects distribués, « *l'utilisateur virtuel* » et « *l'image du service* », qui seront utilisés comme suit :

- Côté fournisseur : Un agent externe issu de l'organisation cliente souhaitant accéder au service web du fournisseur sera considéré comme un *utilisateur virtuel*. Un rôle interne lui sera affecté pour accéder au service.
- Côté client : Le service web du fournisseur est perçu tel un objet externe qui sera représenté par son image au sein de l'organisation cliente.

Ces deux concepts favorisent le traitement des requêtes externes, émises par des agents externes ou ciblant des ressources externes, comme étant des requêtes internes. Autrement dit, les ressources et utilisateurs distants seront considérés comme des éléments internes de l'organisation. Par conséquent, l'expression d'une politique de contrôle d'accès en environnement distribué grâce aux prédicats d'OrBAC sera grandement facilitée.

Ci-après, nous illustrons le fonctionnement de Poly-OrBAC (Fig. 14) : un sujet de l'organisation cliente *Org B*, demandant l'accès à l'image du service de l'organisation fournisseur *Org A*, commence d'abord par s'authentifier auprès de son organisation. Celle-ci détermine s'il est autorisé à invoquer le service distant en consultant sa PS_B. Si la requête est autorisée par PS_B, elle est adressée à *Org A* qui statuera à son tour sur la légitimité de la requête en consultant sa PS_A. Dans le cas où un contrat autorisant *Org B* à bénéficier du service est trouvé, *Org A* donnera alors suite à la requête du sujet d'*Org B* en lui accordant le rôle virtuel réservé aux utilisateurs externes d'*Org B* pour ce service. Des traces relatives à chaque accès sont journalisées localement au niveau des partenaires pour détecter, *a posteriori*, les abus ou éventuellement faire office de preuve en cas de litige.

Afin d'assurer le suivi en temps réel des collaborations, les contrats électroniques ont été implémentés par le biais d'automates temporisés. Les différents modes d'accès ont donc été traduits par des automates. Les permissions ont été spécifiées par des transitions. En revanche, pour les interdictions, les transitions non décrites dans le système représentent des interdictions implicites tandis que les interdictions explicites sont exprimées par l'ajout de transitions vers des états non désirés. Les obligations quant à elles sont représentées par transitions soumises à des contraintes (timers par exemple).

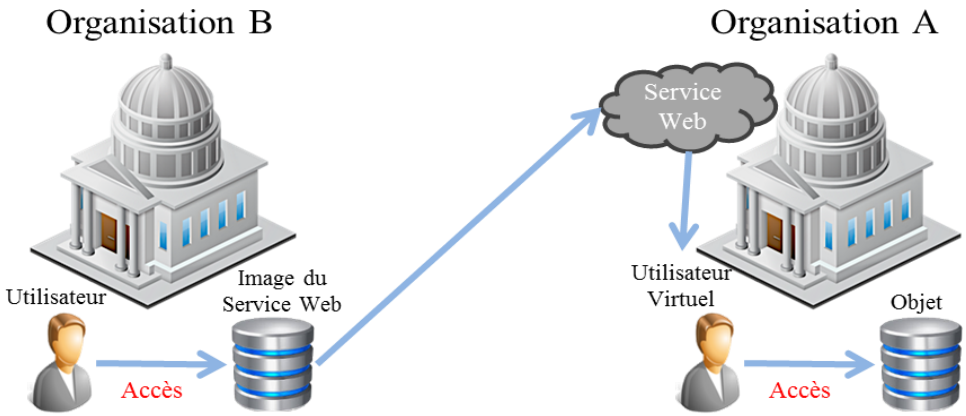

Fig. 14. PolyOrBAC

Poly-OrBAC introduit des concepts très intéressant pour gérer des politiques de collaborations, à savoir, les concepts d'utilisateur virtuel et d'image de l'objet. Toutefois, le processus de négociation des contrats ainsi que ses étapes ne sont nullement abordé. En effet, pour utiliser un service web, l'organisation cliente doit s'aligner par rapport aux conditions de celui-ci. Aussi nous soulignons que dans certains cas, la création d'utilisateurs virtuels peut entrainer la création de « rôles virtuels » – le cas des tâches externes à l'organisation d'accueil – ce qui suscitera bien plus d'efforts d'administration, puisqu'il ne s'agira pas seulement d'affecter les utilisateurs virtuels aux rôles internes de l'organisation.

II.4.2.3.2. Modèle O2O

« *Organization 2 Organization* » (O2O) [107, 130] est aussi une extension du modèle OrBAC qui vise à tenir compte des collaborations et tente ainsi de fournir des mécanismes et des techniques pour garantir un contrôle d'accès en environnements distribués. O2O utilise OrBAC pour assurer un contrôle des accès en interne ; en revanche, le modèle aborde l'aspect collaboratif par le biais de deux nouveaux concepts : les « *organisations virtuelles privées* » (VPO) et « *l'authentification unique du rôle* » (RSSO). Les VPO visent à garantir à toute organisation désirant collaborer, le contrôle de ses ressources en gérant les accès externes vers celles-ci. Alors que le RSSO permet à un sujet de garder son rôle lorsqu'il accède à des ressources externes, toutefois les privilèges dont il jouira seront ceux définis dans la VPO, et seront, par la force des choses, quelque peu différents.

Afin de bien illustrer ces concepts, considérons deux organisations qui collaborent : chacune engagera des ressources, actives ou passives, pour réaliser les objectifs de la collaboration. Les ressources engagées seront considérées comme les ressources d'une « *organisation virtuelle* » (VO) [131].Cela n'empêchera pas toutefois l'occurrence d'éventuels abus, par conséquent, les parties prenant part à la collaboration devront adapter leurs PS pour gérer les futurs accès externes vers leurs ressources. Pour se faire, chaque organisa-

tion définira une VPO détaillant les privilèges accordés à l'organisation collaboratrice. Ainsi, la VPO édifiée est une organisation dynamique créée uniquement dans l'objectif de permettre l'interopérabilité : une fois la collaboration achevée la VPO est dissoute.

A chaque VPO sont associées deux attributs : un *prestataire*, disons Org_A, et un client, disons Org_B. Clairement, la VPO *B2A*, créée par Org_A, détaillera les privilèges à accorder aux utilisateurs issus d'Org_B. Par conséquent, la VPO *B2A* en question appartiendra à la sphère d'autorité[38] d'Org_A. Le contrôle d'accès s'opère une seule fois au niveau du point d'entrée de l'organisation collaboratrice. (Fig. 15) illustre les concepts de VPO et de sphère d'autorité. La définition des règles de la VPO sont soumises à certaines contraintes :

- Un sujet habilité dans un rôle dans la *VPO* implique qu'il est issu du client de la *VPO*, laquelle est définie pour limiter les accès d'agents externes au prestataire.
- Les objets et vues ciblés par les règles de la *VPO* proviennent du prestataire : la *VPO* permet au prestataire d'accorder des privilèges relatifs à ses objets.

Les actions réalisées durant la collaboration sont des activités du prestataire, autrement dit, implémentées par ce dernier (cas d'un service web). Dans le cas contraire, si l'action est implémentée par le client (cas d'un code d'applet), la situation est plus délicate. Le prestataire sera confronté à trois cas de figure : (1) être méfiant et donc refuser l'exécution du code ; (2) l'exécuter dans un espace confiné ou (3) exiger certaines garanties au client, ce qui ferait donc appel à un protocole de négociation.

Dans une *VPO*, il n'est pas toujours impératif de créer de nouveaux rôles. En effet un sujet d'Org_B, accédant aux ressources d'Org_A, peut garder les rôles qui lui ont été affectés par Org_B. En revanche, les privilèges accordés à ces rôles ne seront pas nécessairement les mêmes que ceux définis au sein de la VPO *B2A*. C'est ainsi que O2O généralise le concept d'« *authentification unique* » (SSO) pour les rôles définissant ainsi le concept de RSSO. Dans ce sens, O2O profite du fait que la PS soit exprimée par les entités organisationnelles d'OrBAC, ce qui rend possible la détection d'éventuelles compatibilités, ou similitudes, entre ces entités. Par conséquent, les organisations peuvent s'accorder sur la compatibilité de certains de leurs rôles, vues, activités ou encore contextes. Par exemple, si Org_A et Org_B s'accordent que leurs rôles r_A et r_B sont compatibles, alors un sujet jouant le rôle r_B au sein d'Org_B se verra accorder les privilèges de r_A lorsqu'il accèdera à Org_A. Aussi, si Org_A et Org_B s'accordent que leurs vues v_A et v_B sont compatibles (resp. leurs activités ay_A et ay_B ou leurs contextes c_A et c_B) ; alors si le rôle r_A d'Org_A est autorisé à réaliser

[38] Une organisation Org_A est dite "soumise" à la sphère d'autorité d'une organisation Org_B, si la politique qui s'applique à Org_A est définie et administrée par Org_B.

l'activité ay_A sur la vue v_A en présence du contexte c_A, alors r_A sera certainement autorisé à réaliser l'activité ay_B sur la vue v_B en présence du contexte c_B au sein d'Org_B.

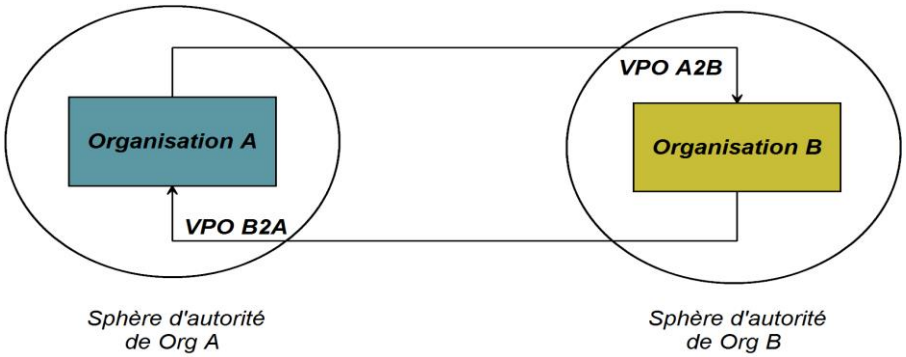

Fig. 15. Organisations virtuelles privées et sphères d'autorité

Adopter un raisonnement fidèle à celui des organisations virtuelles implique que la politique de sécurité de la VO résultante ne sera autre que l'union de toutes les politiques établies pour les VPO. La gestion de ces politiques de sécurité partielles se doit d'être abordée. Trois principales approches de gestion des VPOsont avancées :

- Gestion décentralisée : Chaque organisation se charge de gérer les *VPO* qu'elle a créées. Les processus de négociation, d'authentification et d'autorisation se dérouleront entre les organisations, suite à la requête d'accès d'un sujet.
- Gestion centralisée : Une *VPO* est incluse non seulement dans la sphère d'autorité de l'organisation qui s'en charge mais aussi dans la sphère d'autorité d'un serveur central de confiance gérant toutes les politiques d'interopérabilité des organisations. Toutes les requêtes d'accès sont forcément dirigées vers le serveur qui se charge d'authentifier le sujet et d'appliquer la politique de la *VPO* adéquate en vue de statuer sur la demande d'accès.
- Gestion hybride : Cette technique introduit un facteur lié à la sensibilité des collaborations. Dans le cas d'IC ayant de forts besoins de confidentialité et d'intégrité, celles-ci peuvent ne pas faire confiance à un serveur central externe pour gérer leurs *VPO*. Dans ce cas, les *VPO* sensibles des IC seront gérés par les organisations mêmes, tandis que les moins sensibles – ceux d'organisations de moindre importance – peuvent être déléguées à un serveur central.

L'extension O2O introduit elle aussi des concepts intéressant pour l'expression de politiques de collaboration, toutefois les auteurs mentionnent que la PS globale de la VO est l'union des PS partielles des VPO. Si toutes les politiques des VPO sont cohérentes, cela n'implique pas nécessairement que leur union sera cohérente. De plus, ce modèle non plus ne détaille pas le processus et les étapes de la négociation préalable à l'établissement

des VPO. Aussi dans le cas d'organisations opérant dans des domaines différents, le concept de RSSO et de compatibilité des rôles, vues et activités, risquent de ne pas être utiles.

II.4.2.3.3. Modèle Trust-OrBAC

Il est largement accepté que les modèles basés sur la confiance constituent une solution innovante permettant de garantir un certain niveau de sécurité pour les organisations en milieu distribué. La présente extension d'OrBAC a été pensée pour satisfaire les besoins collaboratifs des organisations en s'appuyant sur une approche orientée vers les techniques de gestion de la confiance. L'intérêt de cette approche est que les décisions de contrôle d'accès tiennent compte de certains facteurs reflétant la fiabilité et la droiture des parties collaboratrices – aussi bien les organisations que les utilisateurs – afin de réduire, voire même d'éviter d'éventuels abus pouvant causer des dommages aux ressources propres de l'organisation. L'idée proposée par Trust-OrBAC [131] consiste à introduire deux vecteurs de confiance, l'un destiné pour les organisations et l'autre aux utilisateurs. Ces vecteurs sont calculés sur la base de critères tels que l'*expérience*, la *réputation* et la *connaissance* [133, 134] et l'*impact de la confiance inspirée par une organisation sur ses utilisateurs*.

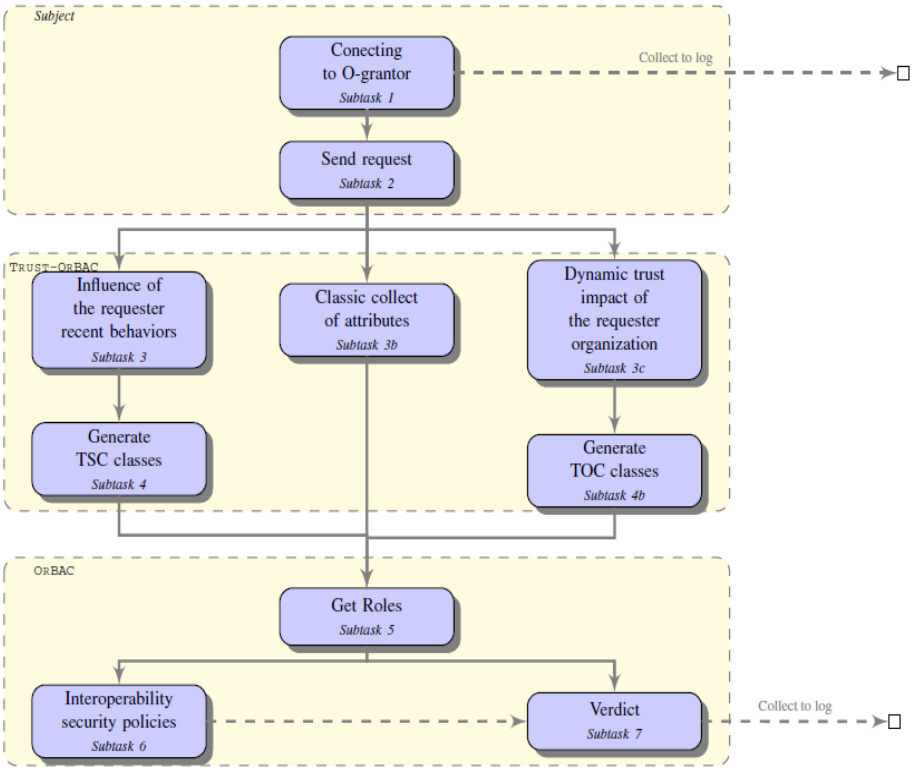

Fig. 16. Etapes de l'affectation des rôles dans Trust-OrBAC [132].

Le modèle définit deux relations d'évaluation de la confiance pour mesurer les deux vecteurs préalablement évoqués, fait intervenir des classes de confiance relatives aux sujets (*TSC*), aux organisations (*TOC*) et à la combinaison de celles-ci [*TC*=(*TSC*,*TOC*)] et établit

un algorithme combinant ces informations en vue de calculer les ensembles de rôles à attribuer aux utilisateurs externes. Les étapes préalables à l'octroi des rôles sont décrites par la figure (Fig. 16). Aussi, les auteurs présentent des formules pour l'évaluation des critères de confiance, à savoir l'évaluation de l'expérience, de la réputation et de la connaissance.

Dans le contexte des IIC, nous pouvons affirmer que ce modèle présente bien des avantages : il est basé sur OrBAC qui est un modèle riche pour l'expression de PS locales et il introduit des techniques pour la mise en place de collaborations sécurisées tout en tenant compte de paramètres liés à la gestion de confiance pour contrôler les accès externes. En revanche, ce modèle reste limiter quant à la prise en compte de la propriété d'intégrité dans les décisions de contrôles d'accès.

II. 5. Discussion sur OrBAC et extensions

II.5.1. OrBAC et ses extensions au service des besoins des IC

Dans le contexte des IIC, nous pouvons affirmer qu'OrBAC offre de nombreux avantages par rapport aux autres modèles cités préalablement. Dans ce qui suit, nous justifions comment, grâce à OrBAC et à ses extensions, il est possible de couvrir un nombre important d'exigences relatives aux IIC, citées en (I.2.6.2).

De par sa conception, OrBAC est un modèle de contrôle d'accès centralisé pour la description de PS conformes aux objectifs de sécurité des organisations. Cette propriété répond ainsi au besoin d'*autonomie*. De plus, OrBAC peut être enrichi par de nombreux mécanismes améliorant l'élaboration de PS cohérentes et homogènes, tel que les mécanismes d'expression des exceptions ou encore de détection et de résolution de conflits [135]. Soulignons qu'exprimer les exceptions rend les PS plus fines et plus pertinentes.

Dans OrBAC, l'aspect *dynamique* du contrôle d'accès est assuré grâce aux contextes, qui permettant la prise en compte de toute une panoplie de contraintes spatio-temporelles, géographiques, etc. En effet, le concept « *contexte* » est défini comme un état logique qui se caractérise par certaines conditions logiques. Les règles de sécurité ne sont activées qu'après la vérification du contexte, ce qui sous-entend qu'une action peut être autorisée en présence d'un certain contexte et interdite en présence d'un autre [136].

La puissance de la logique déontique ainsi que la richesse du langage OrBAC fournissent une base solide pour une description *granulaire* et *structurée* des politiques de sécurité. Plusieurs types de contraintes, telles que la *séparation des tâches* (SoD) et les hiérarchies, peuvent également être exprimées en utilisant OrBAC [137].

Grâce aux deux niveaux complets d'abstraction, OrBAC offre la possibilité de décrire des PS *évolutives*. En effet, une PS décrite par le biais d'éléments abstraits, reflétant

la structure organisationnelle, évite le traitement de chaque accès en particulier – i.e. le traitement de chaque triplet (*s*, *o*, *a*). Clairement de telles PS nécessitent bien moins de règles que s'il était question de les décrire par des éléments concrets. La politique concrète effective devant être appliquée est ensuite dérivée de la politique organisationnelle [33].

Pour administrer les PS OrBAC, les administrateurs peuvent s'appuyer sur le modèle d'administration AdOrBAC [138]. Celui-ci utilise le langage de description d'OrBAC pour l'administration des PS. OrBAC est ainsi un modèle auto-administré.

En raison de son approche centralisée, des extensions ont été développées pour répondre au besoin des collaborations sécurisées, nous citons les modèles MultiOrBAC [126], PolyOrBAC [127, 128] et O2O [130]. Basés sur des approches différentes, nous nous proposons, dans les sous-sections qui suivent, de présenter leurs concepts clés.

Ceci dit, nous pouvons affirmer qu'OrBAC, appuyé par ses multiples extensions, est un excellent candidat pour la spécification de PS pour les IC. En revanche, il demeure limité quant à la prise en de l'intégrité comme nous le montrerons ci-après.

II.5.2. Limitations d'OrBAC quant à la fourniture de l'intégrité

Malgré les atouts mentionnés ci-avant, OrBAC n'inclut pas de mécanismes permettant de restreindre les accès en fonction de contraintes liées à la propriété d'intégrité. En outre, un élément clé de la protection des IIC qu'est le concept de priorisation, consistant à cerner les éléments les plus sensibles n'est pas non plus pris en compte. En effet, les PS exprimées par OrBAC n'intègrent aucun indicateur traduisant l'importance d'une vue, la sensibilité d'une activité, l'urgence d'un contexte ou encore le degré d'expertise d'un sujet. Dans ce sens, les vues (i.e. les objets) et les activités (i.e. les actions) du système sont toutes considérées de même importance, alors que ce n'est absolument pas le cas pour les IIC. De plus, tous les sujets affectés à un rôle héritent des privilèges accordés à ce dernier sans aucune prise en compte de critères reflétant la fiabilité et le degré de maîtrise du sujet.

Afin de mieux éclaircir ces limitations, nous présentons ci-après un exemple de PS exprimé dans un hôpital. D'une part, cela aidera à une compréhension plus aisée de la faiblesse d'OrBAC ; d'autre part, il facilitera la compréhension du modèle que nous proposons dans la suite du manuscrit. L'exemple expose le cas d'un patient atteint d'un cancer qui nécessite une intervention chirurgicale – une ablation – pour augmenter ses chances de guérison et de survie. Pour s'assurer de la réussite de cette opération, de nombreux facteurs doivent être considérés par l'administration de l'hôpital, nous citons à titre d'exemple :

- L'état du patient : Atteint d'un cancer, le patient requiert des soins urgents devant être administré minutieusement ; ne sont pas tolérées dans ce cas, les erreurs médicales d'appréciation et d'administration des soins.
- La réussite de l'opération favorisera la guérison du patient : L'issue de l'opération, requérant méticulosité, statuera sur les chances de rétablissement du patient. L'échec n'est donc pas toléré.
- Le contexte de l'ablation est très sensible, puisqu'elle doit être réalisée rapidement et que les chances de sa réussite ne sont pas très grandes.

Pour les différentes raisons citées ci-avant, il est crucial de choisir pertinemment un chirurgien chevronné pour mener à bien cette ablation. Le chirurgien doit donc être hautement qualifié et doit jouir d'un taux de réussite élevé en ablations réalisées. Procéder à la sélection du chirurgien le plus apte s'inscrit dans le raisonnement que tous les sujets du rôle « chirurgien » ne sont pas identiquement qualifiés, reflétant ainsi une réalité du terrain.

Tenir compte de paramètres pour désigner le sujet le plus qualifié pour la réalisation d'une action sur un objet n'est malheureusement pas possible grâce à OrBAC. En effet, d'une part, OrBAC ne fournit pas de moyens permettant de quantifier la sensibilité des objets, des actions et des contextes ; et d'autre part, il n'existe pas de moyens permettant de distinguer les différents sujets. C'est dans cette optique que nous œuvrerons à enrichir OrBAC avec des concepts et des mécanismes permettant de couvrir le besoin en intégrité et ce conformément au concept de priorisation.

II. 6. Conclusion du chapitre

Dans ce chapitre, nous avons analysé certains modèles de contrôle d'accès : des modèles traditionnels, des modèles d'intégrité et des modèles collaboratifs. Pour chaque modèle, nous avons détaillé les limites et les avantages. A travers cela, nous avons tenté d'identifier le modèle qui conviendrait le mieux comme base de notre extension. Notre choix s'est arrêté sur OrBAC. Aussi l'étude des autres modèles nous a permis de déterminer les points forts qui pourront nous inspirer ainsi que les faiblesses que nous devrons soit éviter soit corriger.

Dans le chapitre suivant, nous présenterons l'extension I-OrBAC que nous proposons pour tenir compte des contraintes d'intégrité dans la prise de décision de contrôle d'accès. Nous détaillerons les fondements de notre modèle, ces composantes, son fonctionnement ainsi que les différents avantages qu'il offre, aussi bien du point de vue de la flexibilité que de la proactivité.

CHAPITRE 3 :

I-ORBAC : INTEGRITY-ORBAC

SOMMAIRE

III.1. Préambule

Le présent chapitre traite de l'extension d'OrBAC que nous proposons pour tenir compte de la propriété d'intégrité dans la prise de décision de contrôle d'accès. Pour introduire I-OrBAC, nous commençons par argumenter les motivations qui justifient le choix d'une modélisation en multi-niveaux. Nous dévoilons aussi la terminologie et les indicateurs qui sont utilisés tout au long du chapitre ainsi que les différentes interprétations de la propriété d'intégrité en accord avec les entités du modèle OrBAC.

Nous argumentons ensuite nos choix concernant les entités qui se verront affecter les niveaux d'intégrité. Ces choix reposent sur des contraintes tirées de la réalité des IIC et sont pensés afin de faciliter l'administration des politiques exprimées grâce à I-OrBAC. Succédera à cela, une présentation détaillée des composantes de notre extension ainsi que des ajustements introduits à OrBAC en vue de l'adapter aux spécificités de notre modèle.

Puis, nous détaillons les mécanismes de la prise de décision de contrôle d'accès et les moyens de son automatisation. Nous présentons aussi la caractéristique proactive d'I-OrBAC, consistant à se détacher du paradigme normal des requêtes d'accès et permettant au système, dans le cas de tâches critiques, de désigner les sujets les plus aptes à les réaliser correctement. Nous exposons aussi des moyens permettant de pallier la limitation des niveaux d'intégrité fixes ; par conséquent, ces niveaux seront dynamiques et seront évalués à l'issue de chaque tâche. Afin de mieux illustrer la prise de décision dans I-OrBAC, nous présentons un exemple, tiré du domaine médical, permettant d'éclaircir le fonctionnement de notre modèle. Puis nous veillons à exprimer un principe d'intégrité grâce à OrBAC et à I-OrBAC afin de pouvoir souligner l'amélioration qu'introduit notre extension.

Aussi abordons-nous un autre avantage lié à la modélisation en multi-niveaux, outre la priorisation des biens sensibles, celui de la flexibilité des décisions de contrôle d'accès. Ainsi, nous démontrons comment les seuils des niveaux d'intégrité fournissent cela.

Enfin, nous exposons un système d'inférence destiné à exprimer formellement l'algorithme de la prise de décision de contrôle d'accès dans le cas du mode proactif.

III.2. I-OrBAC : Integrity-OrBAC

III.2.1. Importance de la priorisation dans la politique de sécurité

La notion de priorisation est très importante dans le cadre de la PIC et de la PIIC. Concrètement, au sein d'une IIC, de nombreux types d'informations et de données – i.e. des objets et des vues, au sens OrBAC – coexistent. Ces données ne présentent pas toutes les mêmes besoins de sécurité, plus particulièrement, en matière d'intégrité. Pour exemple,

l'objet contenant la formule d'un secret industriel exige bien plus d'attention, d'un point de vue intégrité, que l'objet où sont renseignés les congés des personnels.

Par ailleurs, concernant les actions entreprises dans le cadre du métier d'une organisation ; celles-ci – plus généralement les activités au sens OrBAC – n'entrainent pas toutes les mêmes risques ni les mêmes impacts sur le fonctionnement de l'organisation en cas d'échec. Indiscutablement, une plus grande attention doit être prêtée aux actions pouvant impliquer de graves conséquences en cas d'abus. Ainsi, la PS doit pouvoir traduire cette distinction entre les actions de façon claire et d'en tenir compte lors de la prise de décision de contrôle d'accès afin de n'accorder les privilèges des actions sensibles qu'aux sujets les plus aptes à les réaliser avec succès.

Sur un plan plus organisationnel, lorsqu'un rôle est affecté à un groupe d'utilisateurs – indirectement à des sujets –, il est clair que ces derniers ne jouissent pas tous des mêmes compétences ni de la même expertise et encore moins de la même conscience professionnelle. Ainsi, les sujets doivent être caractérisés par des indices de fiabilité et de confiance en plus des critères techniques. Aussi est-il important d'être en mesure, en cas d'abus, de pénaliser les sujets proportionnellement à leurs actes, en les soumettant, à titre d'exemple, à des restrictions de privilèges momentanées ou définitives.

Sur le plan conjoncturel, une organisation est confrontée à une multitude de circonstances tout au long de son activité. Certaines sont courantes et sans répercussions graves alors que d'autres sont beaucoup moins propices : situations à caractère urgent, situations requérant de la méticulosité en raisons de hauts risques, etc. Catégoriser ces conjonctures – autrement dit les contextes au sens OrBAC – en vue de réagir correctement en présence de chacune d'elle se trouve donc être une nécessité pour favoriser la préservation de l'intégrité des ressources de l'IIC.

Tenant compte de cela, les coûts de déploiement des mesures de sécurité au sein des IIC seraient considérablement réduits tout comme les coûts des procédures de certification puisque, d'une part, les moyens de protection mis en œuvre répondront pertinemment aux besoins des objets ; et d'autre part, ne seront certifiés que les processus critiques. Pour toutes les raisons précédemment citées, nous concluons que la politique de sécurité des IIC doit permettre l'expression et la quantification des propriétés et des besoins de sécurité de chaque élément du SI. La prise en compte de ces exigences permettra de mettre en place des moyens de protection pertinents et adaptés à chaque IIC en fonction de ses éléments.

III.2.2. Motivations pour une modélisation en multi-niveaux

Pour concevoir une politique d'intégrité qui puisse répondre aux besoins des IIC, tout en respectant le principe de priorisation, une démarche d'analyse de risque doit être

menée à terme. A l'issue de celle-ci, seront distingués les objets, les actions et les contextes du SI qui sont les plus sensibles et pour lesquels les mesures de protection se doivent d'être en adéquation avec l'ampleur de l'impact causé par leur perte ou leur compromission.

Dans ce sens, l'extension d'OrBAC que nous proposons, Integrity-OrBAC [139], tient compte des différentes notions citées préalablement. Le choix d'OrBAC comme modèle de base est dû à la multitude d'avantages qu'il offre ainsi qu'à sa prédisposition à être aisément couplé à de nouveaux concepts et mécanismes. A ce titre, nous œuvrons à l'enrichir grâce à certains éléments issus de l'application des méthodes d'analyse de risques afin d'exprimer des politiques reflétant les besoins des ressources passives et appréciant, à leur juste valeur, les habilitations des sujets.

En effet, nous pensons que les étapes menant à l'identification des objectifs de sécurité sont d'une importance capitale dans le processus de priorisation ; des traces de ces étapes doivent figurer dans la PS. L'idée que nous retenons consiste à exploiter les fiches de spécification des besoins relatifs aux éléments (i.e. objets) et fonctions (i.e. actions) essentiels. Ainsi, nous comptons extraire certains paramètres de ces fiches et les intégrer à la PS en vue de fournir au moniteur de référence des éléments poignants pour statuer sur les requêtes d'accès. Par conséquent, tous les objets d'une même vue peuvent ne pas être soumis aux mêmes règles. D'autre part, les actions à leur tour feront l'objet de distinctions, afin que les actions sensibles ne soient accordées qu'aux sujets aptes à les réaliser avec succès. Ceci sous-entend bien sûr que les sujets aussi se verront affecter des attributs qui refléteront leurs habilitations ; ces dernières tiendront compte de paramètres de confiance en plus des paramètres techniques. Sans oublier bien sûr que les contextes feront aussi l'objet de discernement afin de tenir compte des particularités de chacun.

Intégrer ces paramètres à OrBAC nous a orientés vers une nouvelle vision de modélisation en multi-niveaux d'intégrité, approche favorisant la priorisation des biens sensibles conformément aux programmes de PIC. En plus, dans notre modèle, les niveaux d'intégrité sont pensés aussi bien pour contraindre l'attribution des privilèges qu'à la rendre plus flexible, comme nous le montrerons dans la suite du chapitre.

III.2.3. Terminologie

III.2.3.1. Les indicateurs d'intégrité

Pour fournir un modèle de contrôle d'accès répondant aux besoins d'intégrité des IIC et considérant les contraintes citées ci-avant, nous commençons d'abord par étudier les diverses facettes possibles de cette propriété. Outre les facettes de l'intégrité énumérées dans [103], nous avons mesuré l'intégrité, selon notre perception, par le biais de deux principaux indicateurs: la *crédibilité* et la *criticité* [140].

Nous considérons la *crédibilité* comme un aspect de l'intégrité car elle est définie comme étant le caractère de quelque chose qui peut être crue, en laquelle une confiance peut être placée. Nous pouvons, sans aucune ambiguïté, établir un lien avec la définition de l'intégrité évoquée en Chapitre I : la définition stipule que l'intégrité est la propriété de correspondre fidèlement à une condition ou à un état initial [101]. Par conséquent, un élément intègre est un élément qui ne se détourne ni ne s'écarte, à aucun moment, d'un code ou d'un standard ; une confiance justifiée peut donc être placée en celui-ci lui conférant ainsi le statut d'élément crédible. Cela peut s'appliquer à toutes les composantes d'un système (i.e. sujets, données, procédures, …), néanmoins, nous jugeons que ce concept se rapporte cependant plus aux entités actives. Ainsi, la crédibilité d'un sujet doit être mesurée sur la base de certains critères tels que la fiabilité, l'historique des actes et la réputation.

Parallèlement, nous définissons la *criticité* comme la caractéristique d'un système (respectivement, un processus, un objet) ne tolérant ni dysfonctionnements ni corruptions et devant préserver ses propriétés indépendamment des événements internes et externes. Cette sensibilité naît de l'importance du système (respectivement, du processus, de l'objet) dans le développement socio-économique d'une nation, ou d'une organisation, ainsi qu'aux graves conséquences pouvant survenir à la suite d'une interruption de service causée par quelconque inadvertance ou malveillance. Dans bien des méthodes de gestion des risques, la criticité se mesure grâce à la formule $criticité = probabilité \times gravité$. La valeur de la criticité est alors égale au produit de la probabilité d'occurrence d'un incident par la gravité de ses impacts. Ceci dit, nous ne portons pas un grand intérêt à la mesure de la criticité puisque chaque IC utilise ses propres moyens pour la calculer, toutefois, nous retenons que la criticité reflète l'importance de l'élément dans le bon fonctionnement de l'IIC.

Dans ce qui suit, nous traduisons différentes lectures et interprétations de la propriété d'intégrité en accord avec les diverses entités du modèle OrBAC en nous appuyant sur les deux indicateurs précédemment cités [140, 141].

III.2.3.2. Lectures de la propriété d'intégrité selon les entités d'OrBAC

Les entités d'OrBAC sont au nombre de huit ; nous tentons de cerner les interprétations possibles de la propriété d'intégrité selon chacun de ces éléments.

Intégrité d'une Organisation :

Selon notre conception, nous associons l'intégrité d'une organisation *Org* à sa *crédibilité* ainsi qu'à sa *criticité*. En environnement collaboratif, la *crédibilité* d'*Org* fait référence à la confiance placée par les autres organisations en elle. Cette confiance se développe au gré des collaborations regroupant *Org* et ses partenaires, à travers les informations

qu'elles leur communiquent et le degré de satisfaction qu'inspirent les agents opérant pour son compte. La *criticité* d'*Org* se mesure, quant à elle, à :

- L'importance de son bon fonctionnement dans l'activité socio-économique à une échelle régionale, suprarégionale, nationale ou même internationale.
- Son degré de méfiance dans ses relations avec l'extérieur.

Intégrité d'un Sujet :

Au sein d'une organisation, nous définissons l'intégrité d'un sujet, dans un rôle, par rapport à ses agissements, plus précisément à sa *crédibilité*, à sa réputation et à la fiabilité dont il fait preuve lors de l'accomplissement des tâches qui lui sont dévolues. Un sujet intègre est donc un utilisateur du système (i.e. un programme) qui réalise correctement ses missions et qui ne s'écarte aucunement d'une certaine éthique.

Intégrité d'un Rôle :

Il est difficile de définir la notion d'intégrité par rapport à l'entité rôle du fait qu'il s'agisse d'une entité abstraite ayant, avant tout, un but organisationnel et structurel, qui n'est autre qu'une agrégation de sujets n'affectant en rien l'état des objets. Néanmoins, nous assimilons l'intégrité d'un rôle à la sensibilité des tâches réalisées par les sujets qui lui sont affectés ou encore si ses sujets se trouvent être les plus aptes à effectuer correctement une certaine tâche sans altérer les objets qu'ils manipulent (i.e. nous assimilons l'intégrité d'un rôle à une priorité qui lui est accordée concernant une certaine tâche).

Intégrité d'un Objet :

Nous mesurons l'intégrité d'un objet au degré de *criticité* de l'information qu'il contient et à l'importance accordée à sa non-corruption. Pour mieux approcher cela, considérons le cas du domaine de l'avionique : avant le décollage, le pilote se doit d'attendre la réception de la vitesse de décollage calculée par les autorités aéroportuaires. Ce paramètre de vol est calculé sur la base de plusieurs facteurs : poids de l'avion, pression extérieur, vitesse du vent, etc. Il est clair que cette information ainsi que son conteneur (i.e. l'objet) ne doivent pas être altérés.

Intégrité d'une Vue :

L'entité *vue* est une entité abstraite pouvant regrouper une multitude d'objets dont les propriétés et les besoins sont différents. Cependant, nous lions l'intégrité d'une vue à sa *criticité*, c'est-à-dire, à quel point ses objets ne tolèrent pas les altérations, ou encore à quel point ses objets sont importants dans le bon fonctionnement de l'organisation.

Intégrité d'une action :

L'intégrité d'une action est liée à l'importance accordée à sa réalisation correcte, écartant ainsi des répercussions graves à l'organisation. Elle se rapporte donc à sa *criticité*.

Intégrité d'une activité :

En extrapolant la définition de l'intégrité d'une action, nous définissons l'intégrité d'une activité par rapport à sa *criticité*, c'est-à-dire par rapport à l'importance accordée à la bonne réalisation des actions qui lui sont associées.

Intégrité d'un contexte :

Au sein d'une organisation, un contexte représente une situation pouvant alléger ou renforcer les contraintes relatives à la réalisation d'une action sur un objet. Selon notre conception, l'intégrité d'un contexte est reliée à sa *criticité*, c'est-à-dire que les actions entreprises et les objets manipulés en présence de ce contexte sont critiques, le succès des actions est donc primordiale.

III.2.3.3. Synthèse

Pour consolider et résumer les différentes définitions de l'intégrité énoncées ci-avant, nous dressons le tableau suivant.

Entité	Indicateur d'intégrité	Est évalué sur la base de
Organisation	Criticité	L'importance de son bon fonctionnement dans l'activité socio-économique d'une nation ou à l'internationale.
		Son degré de méfiance dans ses interactions avec l'extérieur.
	Crédibilité	La confiance que suscite l'organisation auprès de ses collaborateurs.
Rôle	Crédibilité & Priorité	La sensibilité des tâches réalisées par ses sujets.
		Le degré de priorité qui lui est attribué pour la réalisation de certaines tâches.
Sujet	Crédibilité	La fiabilité dont il fait preuve durant l'accomplissement de ses missions, sa réputation.
Vue	Criticité	L'importance accordée à la non-altération des objets qui lui sont associés.

Objet	Criticité	L'importance accordée à la non-altération de l'information qu'il contient.
Activité	Criticité	L'importance accordée à la bonne réalisation des actions qui lui sont associées et le degré de gravité des conséquences, le cas échéant.
Action	Criticité	L'importance accordée à sa bonne réalisation et le degré de gravité des conséquences, le cas échéant.
Contexte	Criticité	La criticité des objets manipulés et des actions réalisées durant ce contexte.

Tab. 1. Synthèse des définitions de la propriété d'intégrité relativement aux entités d'OrBAC.

III.3. Modélisation en niveaux d'intégrité des besoins et des habilitations

Tout au long du processus d'élaboration de la PS d'une IIC, l'administrateur sécurité doit veiller à la bonne application du concept de priorisation pour une protection adaptée aux spécificités des divers éléments du SI. Pour cela, il doit correctement déterminer les attributs ainsi que les propriétés et quantifier les besoins de chaque objet, ou plus généralement de chaque type d'objet. Aussi se doit-il de distinguer les actions routinières des actions à haute sensibilité et d'attribuer correctement les privilèges aux sujets sur la base de critères pertinents pour empêcher, ou du moins limiter, les impacts d'éventuels abus. Autre aspect important de la priorisation appliquée aux SI est d'identifier les différents contextes possibles pouvant survenir afin de statuer sur ce qui sera permis, obligé, recommandé ou interdit en présence de chacun d'eux.

Soucieux d'appliquer correctement le concept de priorisation dans la décision de contrôle d'accès, nous proposons un modèle en multi-niveaux d'intégrité qui considère les différentes contraintes et définitions citées ci-avant. La première étape de cette modélisation consiste à déterminer les entités du modèle OrBAC auxquelles nous affecterons les niveaux d'intégrité. Dans ce qui suit, nous justifions nos choix en nous aidant d'exemples diversifiés pour souligner l'étendue de l'utilisation de notre modèle.

III.3.1. La priorité des rôles

L'affectation des niveaux d'intégrité aux rôles se trouve être une tâche difficile, car ce sont des entités abstraites représentant une agrégation de sujets n'ayant pas nécessairement les mêmes crédibilités et compétences. En outre, le niveau d'intégrité d'un rôle ne devrait pas être dégradé suite à une action abusive commise par l'un de ses sujets. Nous

préférons donc parler du « *niveau de priorité d'un rôle* » plutôt que de son niveau d'intégrité. Ainsi, pour un triplet particulier (*contexte, vue, activité*), nous pensons qu'il est envisageable de sélectionner les rôles les plus appropriés pour l'exécution de la tâche en question. Une fois les rôles choisis, ils seront ordonnés selon leur degré de *priorité* pour la réalisation de l'activité ; ensuite, sur la base de cet ordre, des *niveaux de priorité* leur seront affectés. Ces derniers offriront plus de flexibilité lors de l'expression de la politique de sécurité, comme nous le montrerons par la suite.

Les niveaux de priorité des rôles, pour la réalisation d'une certaine tâche en présence d'un contexte, seront spécifiés en mode hors-ligne. Ils dépendront du métier de l'organisation, de l'organigramme et aussi des compétences présumées des différents rôles.

III.3.2. La crédibilité des sujets

Au sein d'une organisation *Org*, le niveau d'intégrité $l_{s/r}$ reflète le degré de *crédibilité* d'un sujet *s* dans un rôle *r*. Ce niveau d'intégrité est étroitement lié à la confiance que peut avoir *Org* en ses agissements, en sa capacité à réaliser les tâches qui lui sont attribuées, autrement dit sa fiabilité. Le niveau de crédibilité est déterminé sur la base de critères tels que, la réputation du sujet dans le domaine, son passé, son expérience, ses antécédents, ses certificats et autres attestations de compétence. Dans le domaine avionique, aucune compagnie aérienne ne se hasarderait à mettre la vie de centaines de passagers, son image de marque et bien d'autres enjeux entre les mains de pilotes débutants. C'est pour ces raisons que, dans le rôle « *Commandant de bord* », les pilotes sont sélectionnés sur la base de leurs degrés d'expertise ainsi que leurs réputations calculées en termes d'heures de vol effectuées et notamment en considérant les situations critiques qu'ils ont pu assurer. L'attribution de ces niveaux de crédibilité pourrait se faire aussi bien en mode hors-ligne (i.e. le cas de sujets créés lors de la mise en place du système d'information) qu'en mode en ligne (i.e. le cas de nouveaux sujets créés durant l'exploitation du système). Certaines assignations de niveaux de crédibilité peuvent être automatisées en adoptant des valeurs d'initialisation par défaut (i.e. les sujets nouvellement créés dans un rôle se voient attribuer des niveaux de crédibilité égaux à 1).

Affecter des niveaux d'intégrité aux sujets permet au modèle, non seulement :

- D'être plus réaliste puisque tous les sujets d'un même rôle ne se valent pas,
- De pénaliser tout sujet ayant commis un acte abusif, proportionnellement à la gravité de son acte – entre autres, par la dégradation, momentanée ou permanente, de son niveau d'intégrité – et non tous les sujets du rôle.

De plus, un sujet peut jouer plusieurs rôles au sein d'*Org*, il sera donc utile de pouvoir statuer sur ses compétences dans ses diverses fonctions dans le but de l'affecter aux

tâches qu'il maîtrise le mieux. Par conséquent, les sujets se verront attribuer autant de niveaux d'intégrité que de rôles joués. A cet effet, les niveaux de crédibilité des sujets seront organisés sous forme de vecteurs, comme l'illustre le tableau (Tab. 2) présentant le cas où des médecins peuvent jouer plusieurs rôles au sein d'un hôpital. Chaque cellule du tableau qui contient une valeur signifie que le sujet, représenté par la ligne, joue le rôle décrit par la colonne. La valeur de la cellule reflète son niveau de crédibilité dans le rôle. Les lignes du tableau renseignent donc sur les rôles joués par le sujet ainsi que ses niveaux d'intégrité dans chacun de ces rôles. En revanche, la lecture verticale du tableau permet de déterminer quels sujets sont les plus crédibles dans chaque rôle.

Rôles / Sujets	Généraliste	Chirurgien	Réanimateur	Anesthésiste	Rééducateur	Cardiologue	Neurologue	Neurologue	Traumatologue
Bob	3	3	2	2	-	3	-	-	-
Alice	2	-	-	-	3	-	-	3	-
Eve	2	3	3	3	-	-	-	-	-

Tab. 2. Représentation vectorielle des niveaux d'intégrité des sujets.

III.3.3. Criticités des vues et des objets

Nous considérons que l'administrateur regroupe tous les objets de même sensibilité, c'est-à-dire ayant les mêmes attributs et besoins de sécurité, au sein d'une même vue. Cela permettra donc d'affecter, par extrapolation, le niveau d'intégrité à la vue et non aux objets. Ce niveau est déterminé sur la base de la *criticité* de la vue, autrement dit, sur la base de l'impact encouru si un abus venait à les corrompre. L'objet hérite bien évidemment du niveau de la vue à laquelle il appartient. L'héritage améliore l'expressivité de la PS et facilite considérablement son administration. Pour illustrer l'aspect de la *criticité* d'une vue, considérons un exemple issu du domaine de l'avionique, plus particulièrement au sein d'une compagnie aérienne : prenons les deux vues "*Paramètres_vol*", contenant les éléments : $Trajet_x$, $Vit\_décollage_y$, $Altitude_z$, etc., et la vue "*Données_passagers*" qui contient les éléments : $Classe\_voyage_x$, $Personnalisation\_services_y$, etc. Il est clair que les objets de la première vue sont plus sensibles que ceux de la deuxième. Nous attribuerons donc un niveau d'intégrité plus important à la vue "*Paramètres_vol*" pour préserver la propriété de sécurité-innocuité durant les vols. Par héritage, les objets de ces vues se verront attribuer les niveaux d'intégrité de leurs vues respectives.

Les niveaux de criticité des vues et des objets peuvent être, eux aussi, spécifiés en mode hors ligne (i.e. le cas des objets et des vues créés lors de la mise en place du système d'information) ou en mode en ligne (i.e. le cas des nouveaux objets et vues créés pendant le fonctionnement du système). Ici aussi, il serait possible d'automatiser l'affectation des niveaux de criticité aux objets et aux vues en tenant compte de mécanismes d'héritage, tel le cas où un objet créé et répertorié au sein d'une vue hériterait son niveau de criticité, ou encore, il serait possible de tenir compte du niveau de crédibilité du sujet l'ayant créé.

Dans un souci de bonne structuration des vues et objets, l'administrateur est libre de créer autant de vues jugées nécessaires pour organiser les objets de même niveau d'intégrité mais d'utilités différentes. Ces vues auront toutes le même niveau d'intégrité, comme l'illustre la figure (Fig. 17).

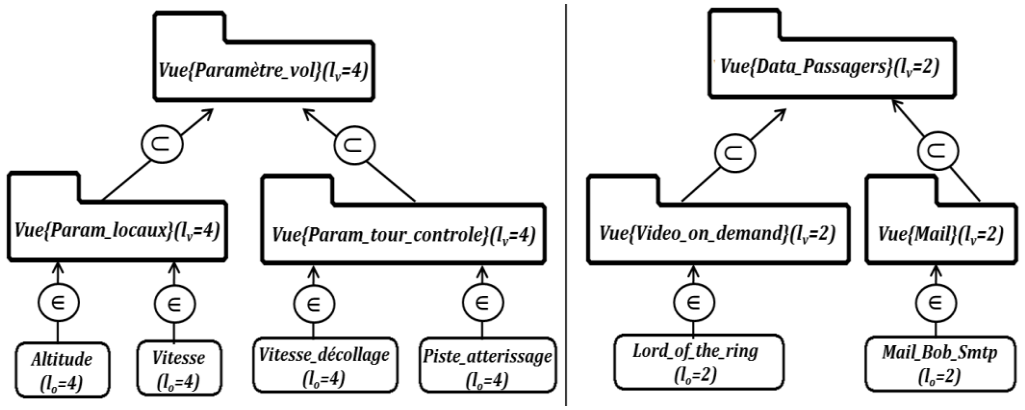

Fig. 17. Représentation des vues (objets) nivelées et structurées

III.3.4. Criticités des activités et des actions

Pour les actions aussi, nous considérons que l'administrateur regroupe au sein d'une même activité, toutes les actions de même sensibilité et présentant les mêmes risques pour l'organisation. Dans ce cas aussi, nous attribuons le niveau d'intégrité, par extrapolation, aux activités et non aux actions. Le niveau d'intégrité d'une activité est évalué sur la base de la criticité des actions qu'elle contient, en d'autres termes, selon la gravité de l'impact sur l'organisation en cas d'échec de leurs réalisations. Par héritage, le niveau d'une action est celui de l'activité qui la contient. Toujours dans le domaine de l'avionique, considérons les activités « *Cockpit_maintenance* » et « *Zone_passagers_maintenance* », relatives respectivement à la maintenance des équipements du cockpit et à la maintenance des équipements de la cabine. Il apparaît clairement que les actions se rapportant à la maintenance du cockpit sont plus critiques que celles relatives à la maintenance de la cabine et se verront donc affecter un niveau d'intégrité plus grand. L'affectation des niveaux de cri-

ticité aux activités se fera en mode hors ligne du fait que les actions sont connues au moment de la mise en place du système.

Là encore, pour des raisons de bonne structuration, l'administrateur est habilité à créer autant d'activités jugées nécessaires pour organiser significativement les actions selon leur utilisation. Ces activités auront toutes le même niveau d'intégrité que la première activité, comme l'indique l'exemple proposé dans la figure (Fig. 18).

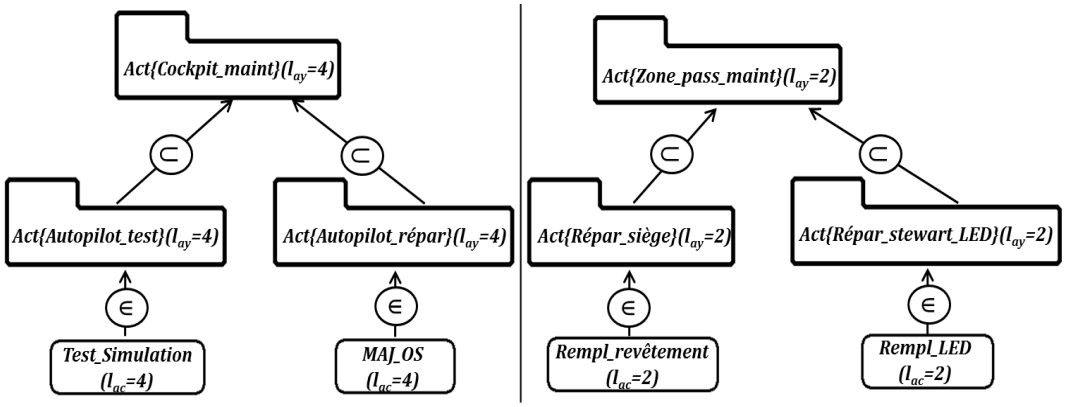

Fig. 18. Représentation des activités (actions) nivelées et structurées

III.3.5. Criticité des contextes

Maints types de contraintes permettent de caractériser correctement le contexte d'une requête d'accès, nous en citons : les contraintes temporelles et spatiales, l'objectif de la requête ainsi que l'historique des actions antérieures, etc. Les niveaux d'intégrité attribués aux contextes tiennent compte des criticités respectives de l'objet demandé et de l'activité à effectuer, de l'instant de la requête d'accès, de la localisation du sujet et de bien d'autres paramètres encore. L'affectation des niveaux de criticité aux contextes se fera aussi en mode hors ligne du fait que les contextes sont connus d'avance.

III.3.6. Exemples d'échelles de besoins

En vue de quantifier correctement les besoins en intégrité des différentes entités précédemment identifiées, il s'agit d'établir des échelles significatives avec autant de niveaux jugés nécessaires pour refléter les différents degrés de besoins. La figure, Fig. 19, présente des exemples d'échelles établies pour les priorités des rôles, les crédibilités des sujets et les criticités respectives des vues, des activités et des contextes. Toutefois d'autres échelles peuvent être définies selon les besoins de chaque IIC.

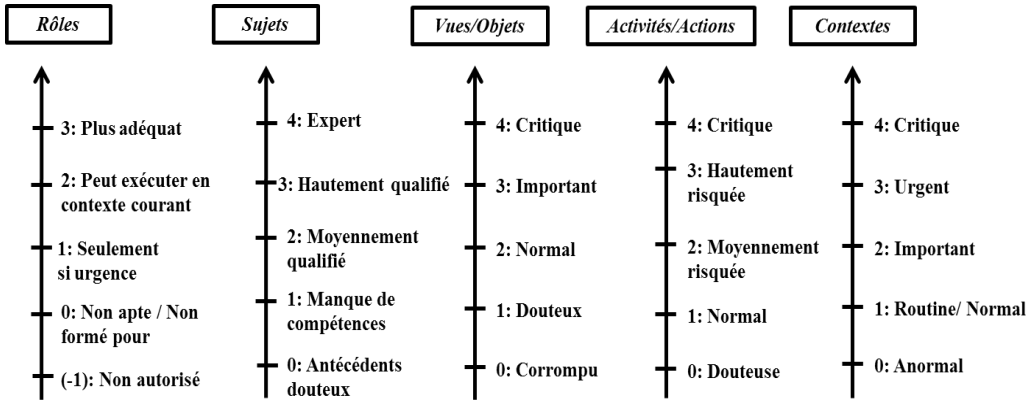

Fig. 19. Exemple d'échelles d'expression des besoins

III.4. Composantes du modèle I-OrBAC

I-OrBAC est une extension d'OrBAC qui tient compte de l'intégrité. De ce fait, notre extension s'appuie sur les entités, les relations, le langage et l'axiomatique de son prédécesseur. Par conséquent, l'organisation continue d'être l'entité centrale de notre modèle. Dans ce qui suit, nous considérons une organisation *Org*, puis nous exposons les différentes modifications apportées au langage d'OrBAC pour répondre aux nouvelles contraintes liées à la modélisation en multi-niveaux et à la fourniture de l'intégrité. Les éléments utilisés dans l'expression de la politique de contrôle d'accès d'*Org* sont les suivants : $s \in S$, $r \in R$, $o \in O$, $v \in V$, $ac \in AC$, $ay \in AY$, $c \in C$.

Aux entités et aux prédicats d'OrBAC, nous avons rajouté les éléments suivants :

- L_S, L_V, L_{AY}, L_C : sont les ensembles respectifs des niveaux d'intégrité des sujets, des vues, des activités et des contextes. L_O et L_{Ac} sont les ensembles respectifs des niveaux d'intégrité des objets et actions. Ils sont identiques à L_V et L_{AY} respectivement. Nous considérons aussi un ensemble des niveaux de priorité des rôles, que nous notons L_R.
- $\leq$: Relation d'ordre dans $L_S \times L_S$, $L_V \times L_V$, $L_{AY} \times L_{AY}$, $L_C \times L_C$, $L_O \times L_O$ et $L_{Ac} \times L_{Ac}$ respectivement, exprimant la relation « inférieur ou égale ». Cette relation d'ordre est aussi définie dans $L_R \times L_R$ pour comparer les priorités affectées aux rôles.

D'autre part, pour affecter les niveaux d'intégrité aux entités précédemment identifiées, nous avons modifié certains prédicats. Puisque les niveaux de criticité du contexte, de la vue et de l'activité sont d'importants paramètres nécessaires à la détermination des contraintes à imposer aux sujets d'un rôle, ils doivent donc apparaître avant le prédicat *Habilite()*. Les modifications que nous avons apportées aux prédicats sont les suivantes :

- *Permission(Org, r, v, ay, c)* $\Rightarrow$ *Permission(Org, r, v, ay, c,* l_c*)*, avec (l_c) la valeur du niveau de *criticité* du contexte *c* sur l'échelle des niveaux d'intégrité des contextes. Les prédicats décrivant les autres modes d'accès, à savoir *Obligation(), Interdiction()* et *Recommandation()*, connaîtrons la même modification.
- *Utilise(Org, o, v)* $\Rightarrow$ *Utilise(Org, o, v,* l_v*)*, avec (l_v) la valeur du niveau de *criticité* de la vue *v* ainsi que de l'objet *o*, par héritage, sur l'échelle des niveaux d'intégrité des vues.
- *Considère(Org, ac, ay)* $\Rightarrow$ *Considère(Org, ac, ay,* l_{ay}*)*, avec (l_{ay}) la valeur du niveau de *criticité* de l'activité *ay* ainsi que de l'action *ac*, par héritage, sur l'échelle des niveaux d'intégrité des activités.
- *Habilite(Org, s, r)* $\Rightarrow$ *Habilite(Org, s, r,* l_s*)*, avec (l_s) la valeur du niveau de *crédibilité* du sujet *s*, dans le rôle *r*, sur l'échelle des niveaux d'intégrité des sujets.

III.5. La prise de décision de contrôle d'accès dans I-OrBAC

Pour assurer l'intégrité des ressources, nous assujettissons l'octroi des privilèges à la prise en compte de trois paramètres jugés importants : les *niveaux de criticité du contexte*, de *la vue* (i.e. *l'objet*) et de *l'activité* (i.e. *l'action*). La connaissance de ces trois paramètres permettra tout d'abord d'identifier les différents rôles pouvant réaliser ladite activité – sur ladite vue en présence dudit contexte – sur la base de certificats, de compétences, etc. Puis, l'administrateur sera en mesure de déterminer les contraintes relatives à la crédibilité requise pour les sujets de chaque rôle. Bien évidemment, la priorité du rôle aura un impact direct sur les seuils de crédibilité imposés aux sujets de chaque rôle. En effet, pour une certaine action, les sujets du rôle hautement prioritaire se verront imposer un seuil de crédibilité plus bas que les sujets des rôles de plus faibles priorités.

III.5.1. I-OrBAC, modèle de contrôle d'accès proactif

A partir de là, nous avons pensé à un contrôle d'accès proactif, c'est-à-dire que le système cherche à déterminer le sujet le plus adéquat parmi les rôles prioritaires pour la réalisation d'une tâche, sans attendre que le sujet n'en fasse la requête. Ce raisonnement proactif peut être restreint aux triplets (*contexte, vue, activité*) critiques – lorsqu'il s'agit, par exemple, d'amorcer des manœuvres de prévention et de contournement lorsqu'un incident se déclenche – tout comme il peut s'appliquer à n'importe quel triplet (*contexte, vue, activité*) du système. Cette fonctionnalité s'avèrera très importante dans le cas d'actions hautement critiques, ou lorsqu'il est question d'actions urgentes à réaliser ou encore pour des tâches pouvant être programmées. Cette dimension proactive confère un caractère préventif, en plus de la fonction de contrôle d'accès garantie par les décisions prises par le moniteur de référence en réponse aux requêtes des sujets. Ce caractère préventif se concré-

tise lorsque le système cherche lui-même à sélectionner le sujet le plus adéquat pour réaliser une action afin de minimiser, par prévention, les risques d'occurrence d'abus, préservant de ce fait l'intégrité des ressources.

Pour automatiser et rendre plus aisée la tâche d'affectation des seuils de crédibilité aux sujets des rôles appelés à réaliser une tâche, nous proposons d'établir des formules mathématiques, plus ou moins élaborées, selon les besoins de l'organisation, faisant intervenir les trois paramètres clés précédemment cités. Ces formules permettront de calculer les niveaux seuils de crédibilité à imposer aux sujets des rôles. D'un point de vue administratif, cela évitera à l'administrateur de fixer un niveau seuil pour tous les triplets possibles (*contexte, vue, activité*). Nous présentons, dans ce qui suit, quelques exemples simples de formules pouvant être établies pour le calcul des niveaux seuils de crédibilité :

- La formule $L_{SLimit} = max\ (lc\ , lv\ , lay)$ stipule que le niveau de crédibilité du sujet doit être supérieur ou égal à la valeur maximale des trois niveaux de criticité des éléments du triplet. Cette approche peut être considérée comme une approche « prudente ».
- La formule $L_{SLimit} = \frac{(lc + lv + lay)}{3}$ impose au niveau d'intégrité du sujet d'être supérieur ou égal à la moyenne arithmétique des trois niveaux de criticité des éléments du triplet. Cette formule peut être utilisée si les trois éléments – *contexte, vue* et *activité* – ont la même importance.
- La formule $L_{SLimit} = \frac{(C_c \times l_c + C_v \times l_v + C_{ay} \times l_{ay})}{(C_c + C_v + C_{ay})}$, contraint le niveau de crédibilité du sujet à être supérieur ou égal à la moyenne pondérée des trois niveaux d'intégrité des paramètres. Cette formule quant à elle peut être utilisée si les trois entités ne sont pas de même importance.

La liste des formules exposées n'est pas exhaustive, nous n'avons cité que les plus simples en guise d'illustration. Conformément à la politique de chaque organisation, des formules plus développées et plus complexes peuvent être adoptées pour répondre convenablement aux exigences de l'organisation. Plusieurs relations peuvent être utilisées simultanément, selon le contexte, les objets protégés, et les actions à effectuer. Cela offre une plus grande flexibilité lors de l'expression de la politique de sécurité pour une protection plus efficace de l'intégrité tout en rendant plus aisée la tâche de l'administrateur de sécurité.

Dans le cas d'un acte abusif commis par un sujet, ce dernier voit son niveau d'intégrité se dégrader en guise de pénalité. Ceci aura un impact direct sur les privilèges et les permissions qui lui seront accordés – ses privilèges seront de plus en plus limités.

Néanmoins, les niveaux de crédibilité des sujets sont recouvrables progressivement à la lumière des performances ultérieures des sujets.

III.5.2. Affectation, gradation et dégradation des niveaux de crédibilité

Lors de son admission au sein de l'IC, plus particulièrement au sein de l'IIC, un sujet peut se voir attribuer n'importe quel niveau de crédibilité sur l'échelle établie par l'IIC. Le niveau qui lui est accordé dépend de la notoriété dont il jouit dans son domaine ainsi que les certificats qu'il détient ; pour illustrer cela, nous considérons le domaine de l'avionique, une compagnie aérienne recrutant un commandant de bord chevronné ne lui accordera pas le niveau de crédibilité « 1 – Manque de compétences », sur l'échelle établie en (Fig. 19), comme elle le ferait pour un pilote débutant.

Contrairement à [26], les niveaux de crédibilité affecté à un sujet lors de son intégration ne demeurent pas figer ; bien au contraire, au gré de ses actions, ces niveaux s'accroitront ou décroitront. Bien évidemment, toute action correctement réalisée donnera lieu à une augmentation du niveau de crédibilité, alors que les abus, selon leur gravité, donneront lieu ou non, selon la PS, à des pénalités différentes.

Notons que les opérations de dégradation et de recouvrement des niveaux de crédibilité se font à l'issue de chaque tâche (i.e. traitements post-tâche). Les calculs réalisés par le moniteur de référence, chargé d'effectuer des inférences pour statuer sur les requêtes d'accès, sont quant à eux des traitements en amont (i.e. traitements pré-tâche) : c'est-à-dire qu'en entrée du moniteur de référence, seront renseignés des niveaux fixes de crédibilité (à chaque instant, nous considérons que les niveaux d'intégrité ont des valeurs fixés). Si le moniteur de référence venait à traiter des requêtes alors que certains des sujets sont en train de réaliser des tâches, à ce moment-là, il considérera leurs niveaux de crédibilité courants, autrement dit, avant de subir les modifications suite à l'issue des tâches qu'ils réalisent.

Principalement, le processus d'affectation, de dégradation et de recouvrement des niveaux de crédibilité reste à la discrétion de l'IC ; autrement dit, il ne serait pas possible de proposer un système qui réponde aux exigences de toutes les IIC. Il incombera donc à l'administrateur de paramétrer ce système pour l'adapter aux besoins de son infrastructure.

a) Exemple de gradation du niveau d'intégrité

Dans ce qui suit, nous proposons un exemple de système de gradation des niveaux de crédibilité. Considérons un sujet de niveau (l_S), pour que son niveau évolue, le sujet doit au moins réaliser 20 actions de criticité équivalente à son niveau ($l_{ac} = l_S$), sur des objets de criticité équivalente à son niveau ($l_o = l_S$) en présence de contextes de criticité équiva-

lente à son niveau ($l_c = l_S$). Toutefois, s'il est autorisé à réaliser des tâches plus sensibles et que l'issue de ces réalisation sont des réussites, alors son niveau s'accroitra plus vite.

La formule retenue pour le calcul du facteur de l'évolution est :

$$\frac{l_o + l_{ac} + l_c}{3 \times l_S} \Big/ 20$$

Ainsi pour une tâche de criticité équivalente à son niveau – c'est-à-dire $l_{ac} = l_o = l_c = l_S$ – son niveau évoluera de 1/20. Autrement si un niveau parmi les trois (l_{ac}, l_o, l_c) est supérieur à l_S alors le facteur d'évolution sera plus grand que 1/20.

Le nouveau niveau du sujet sera donc

$$l_{Snew} = l_{Sold} + \frac{\frac{l_o + l_{ac} + l_c}{3 \times l_S}}{20}$$

Ainsi au fil des actions réalisées avec succès, le niveau de crédibilité du sujet continuera de s'incrémenter ; toutefois, au vu de la réalisation des tâches, le niveau que le système continuera de considérer sera toujours la partie entière de l_{Snew}, grâce à la formule suivante :

$$l_S = \lfloor l_{Snew} \rfloor$$

avec $\lfloor x \rfloor$, la notation anglo-saxonne de la partie entière par défaut.

b) Exemple de dégradation du niveau de crédibilité

Etant à la discrétion des administrateurs d'IIC de mettre au point leurs systèmes de gradation et de dégradation des niveaux d'intégrité, nous proposons malgré tout un exemple de formule pour la dégradation des niveaux de crédibilité des sujets abusifs. Dans le cas où l'administrateur veuille sanctionner plus sévèrement les abus, il pourrait opter pour la formule suivante :

$$\frac{\max(l_c, l_o, l_{ac})}{10}$$

Ainsi, si l'évolution se fait au minimum par un facteur de $1/20$, la dégradation, elle, se fera par un facteur minimal de $1/10$. Toujours est-il que le choix des formules doit se faire méthodologiquement afin d'éviter de se retrouver dans les cas extrêmes : soit tous les sujets sont chevronnés ou l'inverse.

III.5.3. Un exemple de politique de sécurité exprimé grâce à I-OrBAC

Afin d'expliquer plus en détail le fonctionnement de notre modèle, nous proposons un exemple de scénario inspiré du domaine médical. Au sein d'un hôpital « *H* » (i.e., organisation), nous considérons la situation suivante :

Un patient cancéreux « *Tom* » (i.e., objet) nécessite une « *Ablation* » (i.e., action *Ab*). « *Tom* » est répertorié dans la vue « *Patient_Ablation* » (i.e. vue *Pat_Ab*) et l'action « *Ablation* » appartient à l'activité « *Opérations_Critiques* » (i.e. activité *Op_Cr*). Etant donné que la vie du patient est menacée et que son rétablissement dépend de l'issue de l'opération, le contexte de cet acte chirurgicale est considéré donc « *Hautement_Risqué* » (i.e. contexte *H_R*).

Tenant compte des échelles de niveaux d'intégrité déjà établies et conformément à la description ci-dessus, nous considérons que le contexte « *Hautement_risqué* » est jugé critique – vu que la vie du patient dépend de la réussite de l'opération – le niveau de criticité affecté à ce contexte est donc $l_c = 4$. L'activité « *Opérations_Critiques* » regroupe toutes les opérations à hauts risques. De ce fait, l'« *Ablation* » ainsi que les autres opérations de ladite activité se verront attribué le niveau d'intégrité $l_{ay} = l_{ac} = 4$ pour refléter leurs criticités. La vue « *Patient_Ablation* », pour sa part, inclut les patients nécessitant des ablations ; l'état de ces patients est donc grave, par conséquent ladite vue ainsi que les objets (i.e. *Tom*) qu'elle regroupe se verront affectés d'importants niveaux de criticité $l_v = l_o = 4$.

Parmi les rôles présentant les compétences requises pour la réalisation de l'ablation, nous considérons, pour simplifier, le rôle « *Chirurgien* » (i.e. rôle *Chir.*). La prochaine étape consistera à déterminer la contrainte à imposer sur le niveau d'intégrité des chirurgiens pour pouvoir mener à bien l'ablation. La contrainte consiste en un niveau d'intégrité minimum, en d'autres termes un seuil, devant être dépassé par les chirurgiens pour se voir accorder la permission d'effectuer l'opération d'ablation.

Trois importants paramètres relatifs au triplet (*Hautement_Risqué*, *Patients_Ablation*, *Opérations_Critiques*) seront pris en considération pour le calcul du niveau seuil, à savoir :

- le niveau d'intégrité du contexte « *Hautement_Risqué* »,
- le niveau d'intégrité de la vue « *Patients_Ablation* »,
- le niveau d'intégrité de l'activité « *Opérations_Critiques* ».

Pour simplifier, nous considérons que l'administrateur adopte la formule $L_{SLimit} = max\ (lc\ , lv\ , lay)$ pour le calcul du seuil de crédibilité des chirurgiens appelés à assurer la tâche relative au triplet (*Hautement_Risqué*, *Patients_Ablation*, *Opérations_Critiques*).

D'après les valeurs de criticité fixées ci-avant – $l_c = 4$, $l_v = 4$ ($l_v = l_o = 4$) et $l_{ay} = 4$ ($l_{ay} = l_{ac} = 4$) – le seuil de crédibilité à imposer aux chirurgiens sera égal à $L_{Slimit} = 4$. Les chirurgiens dont le niveau de crédibilité sera supérieur ou égal à *4* seront en mesure de réaliser l'activité « *Opérations_Critiques* » sur les patients de la vue « *Patients_Ablation* » en présence du contexte « *Hautement_Risqué* ».

Par conséquent, la base de données regroupant les enregistrements *Rôles–Sujets* sera interrogée pour déterminer les sujets du rôle « *Chirurgien* » ayant un niveau de crédibilité supérieur ou égal à *4* pour leur assigner la tâche relative au triplet (*Hautement_Risqué*, *Patients_Ablation*, *Opérations_Critiques*). La base de données retourne, à titre d'exemple, le profil du chirurgien « *Bob* » qui remplit la contrainte relative au seuil et qui est momentanément libre ; par conséquent le privilège propre à la réalisation de l'action « *Ablation* » sur le patient « *Tom* » en présence du contexte « *Hautement_Risqué* » lui sera octroyé.

Les règles de la politique de sécurité de l'hôpital « *H* » qui autoriseront le chirurgien « *Bob* » à réaliser l'« *Ablation* », sur le patient « *Tom* » dans le contexte « *Hautement_Risqué* », seront exprimées grâce au langage I-OrBAC comme suit :

$$
\begin{aligned}
&Permission(H, Chir, Pat\_Ab, Op\_Cr, H\_R, lc = 4);\\
&\wedge\ Utilise(H, Tom, Pat\_Ab, lv = 4);\\
&\wedge\ Considère(H, Ab, Op\_Cr, lay = 4);\\
&\wedge\ Habilite(H, Bob, Chir, ls = 4);\\
&\wedge\ Définit\ (H, Bob, Tom, Ab, H_R)\\
&\Longrightarrow\ Est\_Permis(Bob, Tom, Ab)
\end{aligned}
$$

En utilisant OrBAC, ce même privilège aurait été exprimé comme suit :

$$
\begin{aligned}
&Permission(H, Chir, Pat\_Ab, Op\_Cr, H\_R);\\
&\wedge\ Utilise(H, Tom, Pat\_Ab);\\
&\wedge\ Considère(H, Ab, Op\_Cr);\\
&\wedge\ Habilite(H, Bob, Chir);\\
&\wedge\ Définit\ (H, Bob, Tom, Ab, H_R)\\
&\Longrightarrow\ Est\_Permis(Bob, Tom, Ab)
\end{aligned}
$$

La spécification des exigences d'intégrité des éléments de la politique de sécurité de l'hôpital « *H* » ne peut être adéquatement exprimée uniquement grâce aux concepts du modèle OrBAC et de son langage. En effet, avec OrBAC seulement, il n'est pas possible de spécifier les besoins en intégrité des contextes, des vues ou encore des activités comme le stipule le concept de priorisation. En outre, la capacité de déterminer parmi les sujets du rôle « *Chirurgien* » lesquels sont les plus aptes à réaliser les opérations de l'activité « *Opé-*

rations_Critiques » sur les patients de la vue « *Patients_Ablation* » n'est pas permise par OrBAC ; alors que cette sélection renforce considérablement la protection des ressources des IC. Malheureusement, dans OrBAC, tous les sujets d'un rôle héritent des privilèges accordés à ce dernier et peuvent ainsi réaliser toutes les activités assignées à ce rôle malgré des degrés de crédibilité et de compétences différents.

III.5.4. Expression d'un principe d'intégrité grâce à I-OrBAC

Dans ce qui suit, nous nous proposons de comparer l'expression d'un principe d'intégrité, qu'est la « *Two Man Rule* », grâce à OrBAC et à I-OrBAC. La règle « *Two Man Rule* » est un mécanisme de contrôle d'accès destiné à assurer un haut niveau d'intégrité, surtout en présence de tâches de haute criticité – lancement d'ogives nucléaires, par exemple. Ce principe appliqué, tout accès ou action nécessite la présence d'au moins deux sujets autorisés tout au long de la tâche. Pour l'illustration, nous considérons une organisation *Org* et les éléments suivants de sa PS : $c \in C$, $v \in V$, $o \in O$, $ay \in AY$, $ac \in AC$. Les éléments *c*, *v*, *o*, *ay* et *ac* sont tous critiques et la réalisation de l'action *ac* nécessite le concours obligé de deux sujets différents, de qualifications bien déterminées mais pas nécessairement de même niveaux.

c) Le cas de sujets du même rôle r :

Considérons deux sujets distincts s_1 et s_2 jouant le rôle *r*, de niveaux de crédibilité ls_1 et ls_2 respectivement ; avec ls_1 et ls_2 nécessairement supérieur à un certain niveau donné. Avant tout, il s'agira d'interdire à tout sujet de *r* de réaliser, à lui seul, l'action *ac* sur l'objet *o* en présence du contexte *c*. Ainsi la formulation grâce à OrBAC sera la suivante :

$$
\begin{aligned}
&Interdiction(Org, r, v, ay, c);\\
&Obligation(Org, r \wedge r, v, ay, c);\\
&\wedge\ Utilise(Org, o, v);\\
&\wedge\ Considère(Org, ac, ay);\\
&\wedge\ Habilite(Org, s_1, r\ );\\
&\wedge\ Habilite(Org, s_2, r\ );\\
&\wedge\ Définit\ (Org, s_1 \wedge s_2, o, ac, c)\\
&\Longrightarrow\ Est\_Obligé(s_1 \wedge s_2, o, ac)
\end{aligned}
$$

Tandis que l'expression de ce principe grâce à I-OrBAC sera la suivante

$$Interdiction(Org, r, v, ay, c, l_c);$$
$$Obligation(Org, r \wedge r, v, ay, c, l_c);$$
$$\wedge\ Utilise(Org, o, v, l_v);$$
$$\wedge\ Considère(Org, ac, ay, l_{ay});$$
$$\wedge\ Habilite(Org, s_1, r\ , l_{s1});$$
$$\wedge\ Habilite(Org, s_2, r, l_{s2});$$
$$\wedge\ Définit\ (Org, s_1 \wedge s_2, o, ac, c)$$
$$\Longrightarrow\ Est\_Obligé(s_1 \wedge s_2, o, ac)$$

d) Le cas de sujets jouant des rôles différents :

Considérons deux sujets distincts s_1 et s_2 jouant deux rôles distincts, respectivement r_1 et r_2, de niveaux de crédibilité ls_1 et ls_2 respectivement ; avec ls_1 et ls_2 nécessairement supérieur à un certain niveau donné. Avant tout, il s'agira d'interdire à tous les sujets de r_1 ou r_2 de réaliser, à eux seuls, l'action *ac* sur l'objet *o* en présence du contexte *c*. Ainsi la formulation grâce à OrBAC sera la suivante :

$$Interdiction(Org, r_1, v, ay, c);$$
$$Interdiction(Org, r_2, v, ay, c);$$
$$Obligation(Org, r_1 \wedge r_2, v, ay, c);$$
$$\wedge\ Utilise(Org, o, v);$$
$$\wedge\ Considère(Org, ac, ay);$$
$$\wedge\ Habilite(Org, s_1, r_1\ );$$
$$\wedge\ Habilite(Org, s_2, r_2\ );$$
$$\wedge\ Définit\ (Org, s_1 \wedge s_2, o, ac, c)$$
$$\Longrightarrow\ Est\_Obligé(s_1 \wedge s_2, o, ac)$$

Alors que l'expression avec I-OrBAC sera comme suit :

$$Interdiction(Org, r_1, v, ay, c, l_c);$$
$$Interdiction(Org, r_2, v, ay, c, l_c);$$
$$Obligation(Org, r_1 \wedge r_2, v, ay, c, l_c);$$
$$\wedge\ Utilise(Org, o, v, l_v);$$
$$\wedge\ Considère(Org, ac, ay, l_{ay});$$
$$\wedge\ Habilite(Org, s_1, r_1\ , l_{s1});$$
$$\wedge\ Habilite(Org, s_2, r_2, l_{s2});$$
$$\wedge\ Définit\ (Org, s_1 \wedge s_2, o, ac, c)$$
$$\Longrightarrow\ Est\_Obligé(s_1 \wedge s_2, o, ac)$$

e) Analyse de la comparaison

Tout d'abord, l'emploi des niveaux d'intégrité pour refléter l'importance des différentes entités permet d'exprimer de façon plus réaliste les contraintes visant à préserver l'intégrité de l'objet, de l'action et du contexte. De plus, à la lecture des règles d'OrBAC, l'interprétation de celles-ci indique que **tous** les sujets du rôle *r* (premier cas), ou sujets des rôles r_1 et r_2 (deuxième cas), sont autorisés à prendre part à la réalisation de l'action *ac* en compagnie de n'importe quel autre sujet du même rôle *r* (premier cas), ou de n'importe quel autre sujet de l'autre rôle (deuxième cas). Or l'objectif escompté n'est pas celui-ci, bien au contraire, les sujets devant prendre part à la réalisation de ladite action doivent être de confiance et jouissant d'une certaine expertise vu l'ampleur de l'action *ac*. Pour tenter d'approcher l'écriture d'I-OrBAC, avec seulement le langage OrBAC, il faudra créer une hiérarchie de sous-rôles pour chaque rôle du système afin de pouvoir quantifier la différence des grades au sein d'un même rôle.

III.6. Plus de flexibilité grâce à I- OrBAC

III.6.1. La flexibilité offerte par la modélisation en multi-niveaux

Dans I-OrBAC, les niveaux d'intégrité représentent certes un moyen de restriction des accès pour garantir que seuls des utilisateurs chevronnés accéderont aux ressources sensibles ; cependant, ils peuvent tout aussi bien contribuer, selon le métier de l'organisation, à rendre le contrôle des accès plus flexible. En effet, nous pensons qu'en pratique, certaines actions peuvent ne pas être réalisées seulement par les sujets d'un rôle unique, mais par bien d'autres sujets jouant d'autres rôles, à la différence que ces sujets seront assujettis à d'autres contraintes. Ce fait est d'une importance capitale surtout lorsqu'il s'agit d'urgences, lorsqu'une intervention s'impose dans de brefs délais ou encore lorsque le sujet responsable de l'action est absent.

A partir de là, nous avons pensé à un modèle de contrôle d'accès proactif qui sera en mesure de déterminer – dans le cas des triplets (l_c, l_v, l_{ay}) critiques – le sujet le plus adéquat issu des rôles prioritaires en vue d'assurer la réalisation de la tâche sans être obligé d'attendre qu'un sujet fasse la requête pour la réaliser. Ce raisonnement peut s'appliquer aux triplets (*contexte*, *vue*, *activité*) critiques d'une IC, comme il peut tout aussi bien être généralisé à tous les triplets du système d'information.

Dans notre modèle, nous proposons qu'il faille tout d'abord, pour chaque triplet (*contexte, vue, activité*), déterminer les différents rôles qui ont les compétences fondamentales requises pour effectuer l'activité. Après cela, les rôles seront classés en fonction de leur degré de maîtrise de l'activité et des compétences additionnels qu'ils peuvent mettre au profit de sa réussite. Sur la base de ce classement seront affectées les priorités aux rôles.

Bien évidemment, les sujets des différents rôles ne seront pas soumis aux mêmes contraintes pour se voir accorder le privilège d'effectuer l'activité : à cet effet, différents seuils minimaux de niveaux d'intégrité seront imposés aux sujets des différents rôles. Concrètement, pour un triplet donné, le système commence par vérifier s'il existe un sujet libre satisfaisant la contrainte du rôle de plus haute priorité. Dans le cas où le sujet identifié est libre, le privilège lui est alors accordé, autrement, le système passe de manière récursive au rôle suivant de priorité plus basse ; il cherche une fois encore un sujet libre répondant à la contrainte liée à ce nouveau rôle; si un tel sujet existe, le privilège lui sera accordé, sinon le système continu d'appliquer l'algorithme itératif jusqu'à trouver un sujet libre répondant à la contrainte imposée à son rôle.

Pour mieux expliciter ce point, nous continuons de nous intéresser au cas du patient nécessitant une ablation, évoqué dans l'exemple précédent. Cette fois-ci, nous considérons que trois rôles présentent les compétences requises pour réaliser cette opération, nous citons les rôles : (1) *chirurgien spécialisé en ablation* (*Chir_Ab*), (2) *chirurgien esthéticien* (*Chir_Esth*) et (3) *chirurgien* (*Chir.*). Il va sans dire que les technicités de ces trois rôles ne sont pas identiques et il apparait clairement que le rôle le plus apte est le rôle « *chirurgien spécialisé en ablation* », suivi du rôle « *chirurgien esthéticien* » et enfin suivi du rôle « *chirurgien* ». Dans ce cas, la PS imposera des seuils de niveaux d'intégrité différents à chacun de ces rôles en vue de la réalisation de cette ablation.

Nous considérons que l'administrateur définit les formules suivantes afin de déterminer les niveaux d'intégrité minimums à imposer aux sujets de chaque rôle :

- Pour le rôle « *Chir_Ab* » :

$$l_{SLimit} = \left\lfloor \frac{l_c}{2 * card(C)} + \frac{l_v}{card(V)} + \frac{l_{ay}}{card(AY)} \right\rfloor \quad (8)$$[39]

- Pour le rôle « *Chir_Esth* » :

$$l_{SLimit} = \left\lceil \frac{l_c}{2 * card(C)} + \frac{l_v}{card(V)} + \frac{l_{ay}}{card(AY)} \right\rceil \quad (9)$$[40]

- Pour le rôle « *Chir.* »:

$$l_{SLimit} = \max\left(l_c + l_v + l_{ay}\right) \quad (10)$$

Connaissant les trois paramètres l_c, l_v et l_{ay}, nous déduisons, par calcul, les niveaux de crédibilité à imposer aux sujets des différents rôles cités précédemment. A partir de

[39] $\lfloor x \rfloor$: Notation anglo-saxonne de la partie entière par défaut.
[40] $\lceil x \rceil$: Notation anglo-saxonne de la partie entière par excès.

l'équation (1), nous calculons $l_{SLimit(Chir\_Ab)} = 2$; l'équation (2) permet le calcul de $l_{SLimit(Chir\_Esth)} = 3$ et enfin à partir de l'équation (3), nous déduisons que $l_{SLimit(Chir)} = 4$.

Dans l'ordre des priorités, notre moniteur de référence cherchera tout d'abord un « *chirurgien spécialisé en ablation* » de niveau de crédibilité supérieur ou égal à 2. Dans le cas où cas tous les sujets éligibles sont occupés ou absents, le système cherchera alors un sujet de niveau de crédibilité supérieur ou égal à 3 dans le rôle « *chirurgien esthéticien* », si aucun chirurgien esthéticien n'est libre, le système finira par chercher un « *chirurgien* » de niveau de crédibilité supérieur ou égal à 4 .

Cette flexibilité peut aisément être interprétée comme une déclinaison de la notion de recommandation [32, 142] introduite dans OrBAC. En effet , nous pouvons considérer la combinaison des priorités des rôles et des seuils des niveaux d'intégrité imposés à chaque rôle comme un moyen de fourniture de la recommandation, plus explicitement, la politique recommande, en premier lieu, qu'une action soit effectuée par un sujet du rôle le plus prioritaire, sinon, elle recommande, en second lieu, qu'elle le soit par un sujet du rôle de moindre priorité , et ainsi de suite.

Les règles qui correspondront à ces contraintes sont les suivantes :

$$Permission(H, Chir\_Ab, Pat\_Ab, Op\_Cr, H\_R, lc = 4);$$
$$\wedge\ Habilite(H, Abdel, Chir\_Ab, ls = 2);$$

Ou encore :

$$Permission(H, Chir\_Esth, Pat\_Ab, Op\_Cr, H\_R, lc = 4);$$
$$\wedge\ Habilite(H, Alice, Chir\_Esth, ls = 3);$$

Ou encore :

$$Permission(H, Chir, Pat\_Ab, Op\_Cr, H\_R, lc = 4);$$
$$\wedge\ Habilite(H, Bob, Chir, ls = 4);$$

III.6.2. Représentation formelle de l'algorithme de flexibilité

Dans ce qui suit, nous proposons une expression mathématique de l'algorithme décrivant la flexibilité de la prise de décision de contrôle d'accès. Nous avons exprimé le raisonnement déductif de l'algorithme par un système d'inférence.

Tout au long de cette section, nous considérons une organisation *Org* et les éléments suivants de sa politique de sécurité : $c \in C$, $v \in V$, $o \in O$, $ay \in AY$, $ac \in AC$. A par-

tir du triplet abstrait (*c, v, ay*) – statuant que l'activité *ay* peut être réalisée sur la vue *v* en présence du contexte *c* – une multitude de triplets faisant intervenir des éléments concrets de la politique de sécurité peuvent être dérivés. Nous nous concentrons plus particulièrement sur le triplet (*c, o, ac*) qui statut que l'action *ac* (répertoriée dans l'activité *ay*) peut être réalisée sur l'objet *o* (répertorié dans la vue *v*) en présence du contexte *c*. En langage I-OrBAC, ces triplets sont extraits suite à la combinaison des prédicats suivants : *Permission*(*Org, r, v, ay, c,* l_c) ; *Utilise*(*Org, o, v,* l_v) et *Considère*(*Org, ac, ay,* l_{ay}).

Le triplet (*c, v, ay*) se retrouve donc concrètement caractérisé par les niveaux d'intégrité de ses éléments (l_c, l_v, l_{ay}) et détermine par conséquent un ensemble de rôles aptes à la réalisation de l'activité *ay* sur la vue *v* dans le contexte *c* – plus particulièrement appropriés à la réalisation de l'action *ac* sur l'objet *o* dans le contexte *c*. Ces rôles seront par la suite classés selon leurs aptitudes et se verront affectés des niveaux de priorité « l_r ». Nous notons l'ensemble des paires (r, l_r) relatives aux rôles pertinents – déterminés par le triplet (*c, v, ay*) – par « *RP* ».

Afin de déterminer le sujet le plus approprié issu de chaque rôle, nous définissons la fonction L_{SLimit} qui calcule le niveau d'intégrité seuil sur la base des paramètres l_c, l_v, l_{ay} et l_r, ainsi $(l_{smin})_r = L_{SLimit}(l_c, l_v, l_{ay}, l_r)$.

Une fois que l'algorithme sélectionne un sujet *s* adéquat d'un rôle *r* de *RP*, cela correspond à un état de succès (i.e., état Succès). Nous affirmons alors que la permission relative au triplet (*c, v, ay*) est accordée au rôle *r*, que nous notons *Perm(r)*. Concrètement, *Perm(r)* est l'ensemble des prédicats d'I-OrBAC permettant d'octroyer le privilège au sujet *s* de *r* ; ces prédicats sont *Habilite(), Définit()* et *Est_Permis()*. Nous définissons donc :

Perm(r) = *Habilite*(*Org, s, r,* l_s) $\wedge$ *Définit*(*Org, s, o, ac, c*) $\wedge$ *Est_Permis*(*s, o, ac*).

Le système d'inférence décrivant l'algorithme se présente comme suit :

- A l'initialisation du système, nous considérons l'ensemble des rôles *R* et le triplet (*c, v, ay*) dont il est question. Ces paramètres permettront de déterminer et de délimiter l'ensemble des rôles pertinents *RP* ; plus concrètement, l'ensemble des paires (r, l_r) représentant les rôles pertinents pour ledit triplet.
- Par la suite, l'algorithme commence par calculer le $(l_{smin})_r$ pour le rôle le plus prioritaire puis entame la recherche d'un sujet libre satisfaisant la contrainte $(l_s)_r \geq (l_{smin})_r$. Si un tel sujet existe, il se voit accorder la permission et l'état de succès est considéré atteint. *Perm(r)* est donc valide et par conséquent les prédicats le sont aussi. Cet état est décrit par la règle *Succès*.

- Si les sujets satisfaisant la contrainte ne sont pas libres et que les sujets libres ne répondent pas au critère de choix $(l_s)_r \geq (l_{smin})_r$, l'algorithme passe au rôle de seconde priorité, calcule le nouveau $(l_{smin})_r$, vérifie l'existence d'un sujet libre répondant à cette nouvelle contrainte. Si cette recherche est couronnée de succès, l'algorithme s'arrête et la permission est accordée au sujet sélectionné. Autrement, cette itération est répétée autant de fois qu'il existe de rôles pertinents dans *RP*. Ce processus est décrit par la règle *Suit*.
- Finalement, si l'algorithme parcourt tous les rôles de *RP* et qu'aucun sujet adéquat n'est sélectionné, nous considérons que le système est en état d'échec car la tâche ne peut être réalisée. A ce moment-là, nous pouvons développer les aspects relatifs aux collaborations et tenter de trouver des effectifs qualifiés auprès des partenaires.

Dans un premier temps, nous considérons que le moteur d'inférence s'arrête au premier profil (i.e. sujet) adéquat libre. Les autres profils, qui seraient retenus si les inférences venaient à se poursuivre, seraient soit des profils similaires soit moins prioritaires, puisque nous considérons que les rôles et les sujets sont parcourus selon la décroissance de leur priorité, en vue de la réalisation de ladite tâche.

L'écriture mathématique de l'algorithme est présentée, en Tab. 3, ci-après :

Init	$\frac{R, (l_c, l_v, l_{ay})}{RP}$	*avec RP contient l'ensemble des couples prioritaires* (r, l_r)*pour le triplet* (c, v, ay)
Succès	$\frac{(r, l_r) \cup RP, (l_c, l_v, l_{ay})}{Perm(r)}$	*si* $\exists\ s \in r\ /(l_s)_r \geq L_{SLimit}(l_c, l_v, l_{ay}, l_r)$
Suit	$\frac{(r, l_r) \cup RP, (l_c, l_v, l_{ay})}{RP, (l_c, l_v, l_{ay})}$	*si la règle Succès n'est pas valide*
Echec	$\frac{\emptyset, (l_c, l_v, l_{ay})}{Echec}$	*si nulle autre règle ne s'applique*

Tab. 3. Système d'inférence décrivant la proactivité d'I-OrBAC.

III.7. Conclusion du chapitre

Tout au long de ce chapitre, nous avons présenté notre extension du modèle OrBAC qui tient compte de l'intégrité dans la prise de décision de contrôle d'accès. Cette extension se base sur une modélisation en multi-niveaux d'intégrité pour répondre au principe de priorisation des biens sensibles, lequel constitue la base de tout programme de PIC. Nous avons aussi argumenté nos choix par rapport aux entités qui se verront affecter les niveaux

d'intégrité. Aussi avons-nous détaillé les mécanismes de la prise de décision de contrôle d'accès et les moyens de son automatisation notamment dans le cadre de la proactivité d'I-OrBAC ; sans oublier la proposition de moyens permettant de rendre les niveaux d'intégrité dynamiques, à travers leur gradation et leur dégradation. Nous avons ensuite illustré l'utilité de notre approche à travers un exemple inspiré du domaine médical ainsi qu'à travers l'expression d'un principe d'intégrité, le « *Two-Man Rule* ». Puis, nous avons montré comment la modélisation en multi-niveaux pouvait offrir une certaine flexibilité dans le processus de décision de contrôle d'accès en manipulant des niveaux d'intégrité seuils. Pour finir nous avons présenté une expression formelle de l'algorithme de décision proactif visant à identifier le sujet le plus apte parmi une série de rôles prioritaires.

Dans le chapitre suivant, seront abordés nos choix technologiques en termes d'architecture de contrôle d'accès, de langage de programmation, etc. Nous présenterons une étude de cas qui permettra de bien apprécier l'utilité du modèle que nous proposons. L'étude de cas s'inspire d'un projet européen dans le domaine des infrastructures de transport et de distribution de l'énergie électrique.

CHAPITRE 4 :

IMPLÉMENTATION DU MODÈLE I-ORBAC

SOMMAIRE

IV.1. Préambule

Dans ce chapitre, nous présentons les choix technologiques ainsi que les scénarios de test utilisés pour tester l'implémentation du modèle que nous avons proposé.

Ainsi, nous avons opté pour le standard XACML comme base de notre implémentation en raison de ses multiples avantages. Nous présentons brièvement les briques du standard ainsi que les étapes de la prise de décision de contrôle d'accès qu'il propose. Toutefois, les différentes versions du standard sont inadaptées par rapport aux spécificités de notre modèle I-OrBAC, nous tâchons donc de réajuster la version 2.0 afin qu'elle tienne compte de toutes les entités abstraites d'I-OrBAC.

Ensuite, nous détaillons les étapes de la prise de décision à l'issue des ajustements réalisés pour les deux cas de figure : (1) celui des requêtes normales, formulées par les sujets, et (2) celui des requêtes formulées par le système dans le cadre de la pro-activité.

Puis, nous décrivons la plateforme adoptée pour mener les tests qui témoigneront du bon fonctionnement de notre modèle. La plateforme est inspiré d'un projet européen ayant traité les aspects sécurité et résilience dans les réseaux de distribution d'électricité.

L'implémentation de cette plateforme sera ensuite couplée au modèle, les requêtes émanant de celle-ci seront capturées et traitées conformément aux étapes détaillées.

IV.2. XACML, un standard de description des politiques de sécurité

IV.2.1. Le standard XACML

XACML [143] est un standard largement utilisé non seulement pour l'expression des politiques de sécurité mais aussi pour la description de langages de décision requêtes/réponses pour le contrôle d'accès. Il est utilisé pour sa portabilité ainsi que pour ses mécanismes offrant un contrôle d'accès granulaire pour l'octroi ou le déni des privilèges. En outre, XACML offre la possibilité d'exprimer des politiques de contrôle d'accès distribuées. Cette dernière caractéristique nous sera très utile pour le volet suivant se rapportant aux aspects collaboratif du contrôle d'accès.

Dans XACML, chaque décision d'accès est élaborée à la suite des étapes indiquées sur la figure (Fig. 20). Tout d'abord, le « *Policy Administration Point* » (*PAP*) fournit la politique de sécurité complète au « *Policy Decision Point* » (*PDP*). Toute requête d'accès arrive au « *Policy Enforcement Point* » (*PEP*) qui se charge de créer une requête XACML puis l'envoie au *PDP* – le « *Gestionnaire des Contextes* » (*Context Handler*) [143] est considéré faisant partie du *PDP*. Ce dernier invoque ensuite les services du « *Policy Information Point* » (*PIP*) afin de récupérer les valeurs des attributs relatifs aux sujets, aux objets, aux actions et au contexte. Le *PDP* évalue la requête sur la base des règles fournies par le *PAP* et les différents attributs collectés depuis le *PIP*. La décision d'accès prise, à l'issue de ce processus, par le *PDP* est ensuite envoyée au *PEP* : la décision consiste soit en une permission soit en une interdiction, l'une ou l'autre couplée à des obligations. Le *PEP* s'assure des obligations puis autorise ou dénie l'accès, conformément à la décision *PDP*.

En analysant les étapes citées ci-avant, nous remarquons le standard XACML, dans sa version de base, ne prend pas en charge les attributs des entités abstraites, à savoir les rôles, les vues et les activités. La version 2.0 du standard remédie certes à cela, en introduisant un nouveau composant chargé des attributs des rôles, comme support au modèle RBAC ; cela demeure insuffisant dans le contexte d'I-OrBAC. Nous allons donc l'enrichir afin compléter les composants chargés des entités abstraites, ainsi seront rajoutés deux composants : un pour les vues et l'autre pour les activités. Ces composants géreront, entre autres, les niveaux d'intégrité attribués par extrapolation aux entités abstraites.

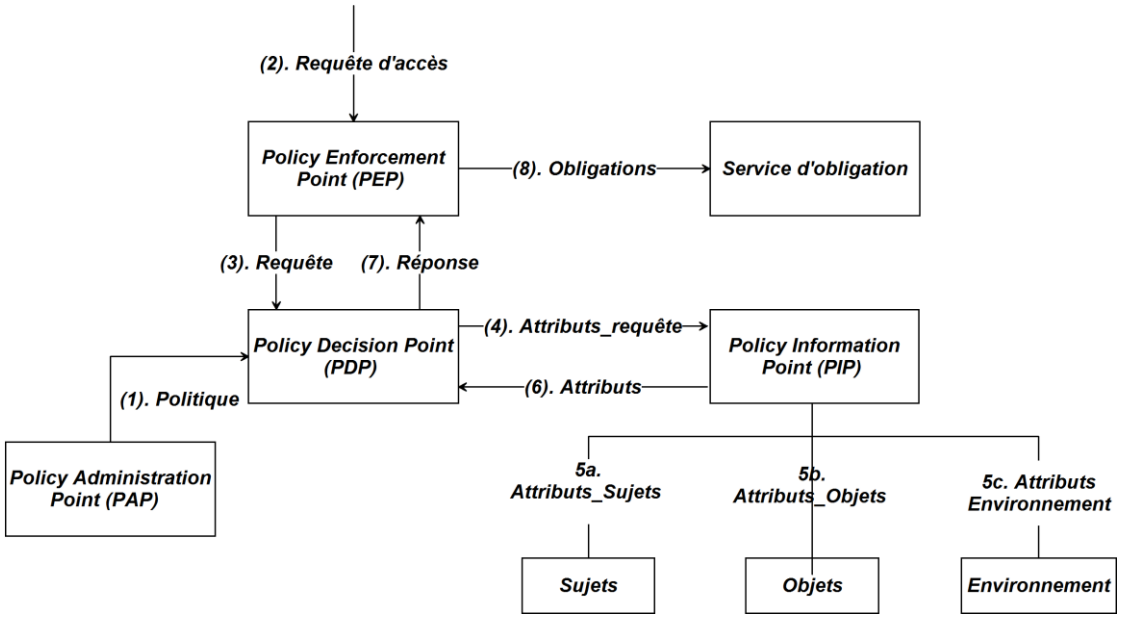

Fig. 20. Prise de décision de contrôle d'accès dans le standard XACML

IV.2.2. Adaptation de XACML pour l'implémentation d'I-OrBAC

Comme dit précédemment, nous avons basé l'implémentation d'I-OrBAC sur le standard XACML. Nous avons dû l'enrichir afin de répondre aux spécificités de notre extension, à savoir les deux couches d'abstraction et les niveaux d'intégrité. Pour cela, nous avons rajouté quelques mécanismes et avons modifié les propriétés de certaines entités.

La version 2.0 du standard XACML a introduit une amélioration majeure qui consiste à considérer le concept de rôles; ce qui permet d'exprimer des politiques de type RBAC. Cette nouveauté est appelé « *Role Enablement Authority* » (*REA*) [144]. La *REA* est une entité qui remplit deux fonctions principales : l'affectation des attributs de rôle et de leurs valeurs aux utilisateurs ainsi que l'activation de ces attributs et de ces valeurs au cours d'une session d'un utilisateur. Pour adapter le standard aux deux autres concepts d'agrégation qu'intègre I-OrBAC – à savoir les vues et les activités –, nous avons introduit à l'architecture décrite dans la version 2.0 deux nouvelles autorités : « *View Enablement Authority* » (*VEA*) et « *Activity Enablement Authority* » (*AEA*), comme le montre la figure (Fig. 21). De cette façon et similairement aux fonctions jouées par le *REA*, la *VEA* et l'*AEA* gèrent les autres entités abstraites d'I-OrBAC et affectent les attributs et leurs valeurs, respectivement, aux vues et aux activités ainsi qu'aux objets et actions, respectivement.

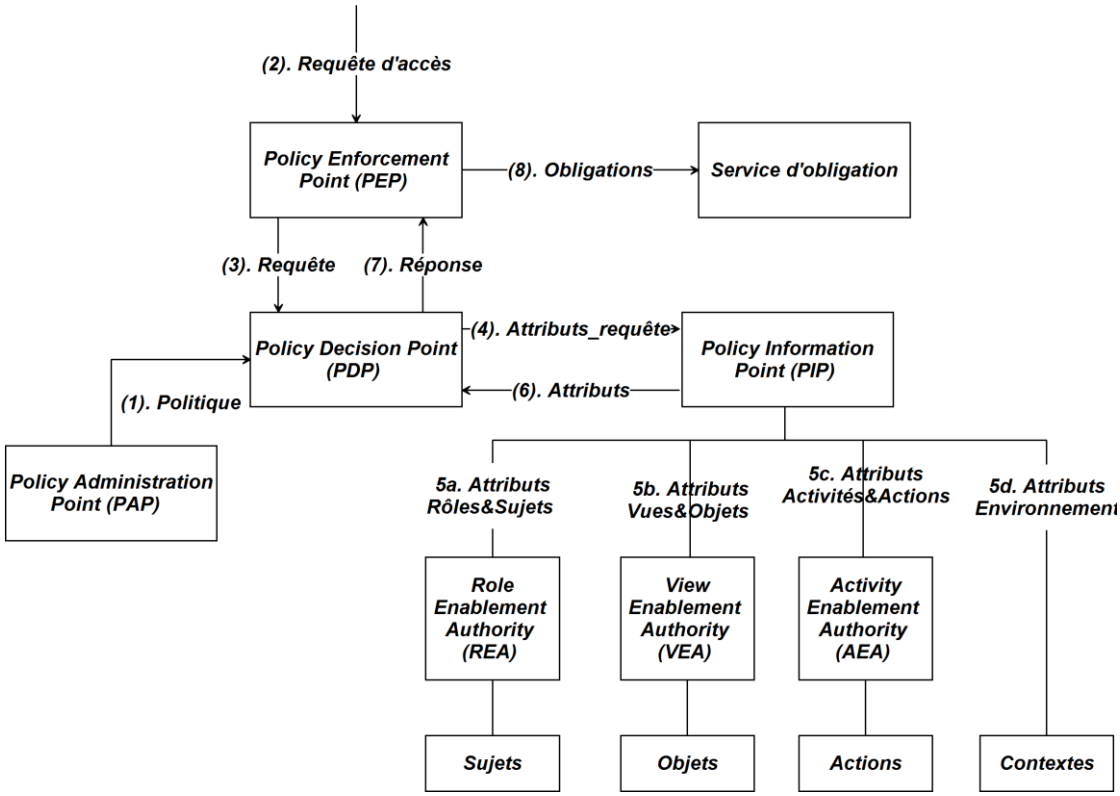

Fig. 21. Prise de décision après modification du standard XACML.

Parmi les attributs à affecter aux entités d'I-OrBAC, se trouvent les niveaux d'intégrité ; nous avons donc traité l'aspect relatif à leur attribution. Ainsi, la *VEA* et l'*AEA* ont pour tâche d'affecter, par héritage, les niveaux d'intégrité aux objets et aux actions respectivement. Les niveaux d'intégrité des vues et des activités sont attribués par l'administrateur sécurité.

En ce qui concerne la prise de décision de contrôle d'accès, nous distinguons deux cas de figure : le cas normal (1) où le système répond à une requête d'accès émise par un sujet demandant l'accès à un objet et le cas de la pro-activité (2) où une tâche programmée/inopinée doit être effectuée et qu'il incombe au système de déterminer le sujet le plus approprié à sa réalisation.

Pour le premier cas, nous présentons la démarche de la prise de décision de contrôle d'accès qui sont quelque peu semblables à celles utilisées dans le standard XACML. En effet, au sein d'une organisation :

- La demande d'accès est adressée par un sujet au *PEP* qui la relaie ensuite au *PDP*. La requête contient certains attributs des entités en question – tel que, le rôle, le sujet, l'objet, l'action et le contexte. Nous nous sommes assurés de

transmettre le rôle activé par le sujet au cours de la session car, comme déjà indiqué, un sujet peut jouer différents rôles au sein d'une organisation, ce qui lui permettrait éventuellement d'accéder à une ressource même sans activer le bon rôle. Cette mesure est prise conformément au principe du « *moindre privilège* ».

- Le *PDP* demande alors au *PIP* de lui communiquer le reste des attributs propres aux entités, à savoir :
    - la vue et l'activité auxquelles appartiennent respectivement l'objet et l'action ainsi que leurs niveaux d'intégrité,
    - le niveau d'intégrité du sujet dans le rôle déclaré,
    - le niveau d'intégrité du contexte.
- A son tour, le *PIP* collecte ces informations auprès des différentes autorités responsables – *REA, VEA, AEA* – puis les relaie par la suite au *PDP*.
- Le *PDP* vérifie les règles abstraites de la politique de sécurité (i.e. les règles *Permission()* / *Obligation()* / *Recommandation()* / *Interdiction()*).
- Le *PDP* calcule ensuite le seuil l_{SLimit} imposée aux sujets du rôle déclaré, puis il vérifie si le niveau d'intégrité du sujet est supérieur au seuil l_{SLimit} pour statuer sur la décision d'accès.
- La décision d'accès est ensuite envoyée au *PEP* qui s'assure de remplir les obligations et/ou informer le sujet des recommandations puis applique la décision.

Pour le second cas, nous pensons que, en raison de leur intelligence, les SI sont de plus en plus aptes à réagir à certains événements internes ou externes, à prendre des décisions, à programmer des tâches, etc. Dans le cas de certains triplets (contexte, vue, activité), le système peut décider du sujet le plus approprié pour la réalisation de la tâche. Dans ce cas, la prise de décision de contrôle d'accès suit les étapes suivantes :

- Le système adresse une requête au *PEP* qui la relaie ensuite au *PDP*. La demande contient des attributs propres au contexte, à l'objet et à l'action.
- Le *PDP* demande au *PIP* de lui fournir les valeurs des autres attributs :
    - la vue et l'activité auxquelles l'objet et l'action appartiennent respectivement ainsi que leurs niveaux d'intégrité,
    - le niveau d'intégrité de contexte est aussi demandé.

  Ces attributs permettront au PDP de déterminer les rôles appropriés qui peuvent réaliser la tâche ainsi que leurs priorités vis-à-vis de cette dernière.

- A son tour, le *PIP* adresse des requêtes aux différentes autorités pour recueillir ces informations. Une fois ces dernières reçues, il les envoie au *PDP*.
- Le *PDP* vérifie les règles abstraites de la politique de sécurité qui lui sont communiquées par le *PAP*, puis il applique l'algorithme de sélection d'un sujet.
- Le *PDP* calcule ensuite le seuil l_{SLimit} imposé aux sujets du rôle de plus haute priorité puis il recherche un sujet libre jouant ce rôle et respectant le l_{SLimit}.
    - Si un tel sujet est trouvé, le *PDP* statue sur la décision à prendre puis envoie la réponse au *PEP* qui s'assure de remplir les obligations.
    - Si aucun sujet libre n'est trouvé, le *PDP* entame une nouvelle itération de l'algorithme et passe ainsi au rôle suivant de seconde priorité et recalcule le nouveau l_{SLimit} puis recherche un sujet libre.

Pour plus d'efficacité et afin de répondre plus rapidement aux requêtes d'accès répétitives, nous avons implémenté un système de cache. En effet, une fois qu'une décision de contrôle d'accès est prise par le *PDP*, ce dernier l'enregistre pour une période de temps afin de traiter les demandes ultérieures similaires.

IV.3. Scénarios de test de notre implémentation I-OrBAC

IV.3.1. Implémentation de la plateforme électrique

En vue de tester le bon fonctionnement de notre implémentation, nous avons implémenté une plateforme simulant le fonctionnement d'une infrastructure électrique inspirée du contexte du projet « *CRitical UTility InfrastructurAL resilience project* » (CRUTIAL) [145] qui abordait les questions de résilience et de sécurité dans les infrastructures de transport et de distribution de l'énergie électrique. Par souci de praticité, nous avons choisi de restreindre la plate-forme à une sous-station approvisionnée par une centrale hydroélectrique et qui distribue l'énergie électrique aux charges par l'intermédiaire d'un réseau de lignes, comme l'illustre la Fig. 22 ci-dessous. Dans nos scénarios de test, nous considérons que la sous-station, la centrale hydroélectrique, les lignes de transport et de distribution et les charges font partie d'une même organisation.

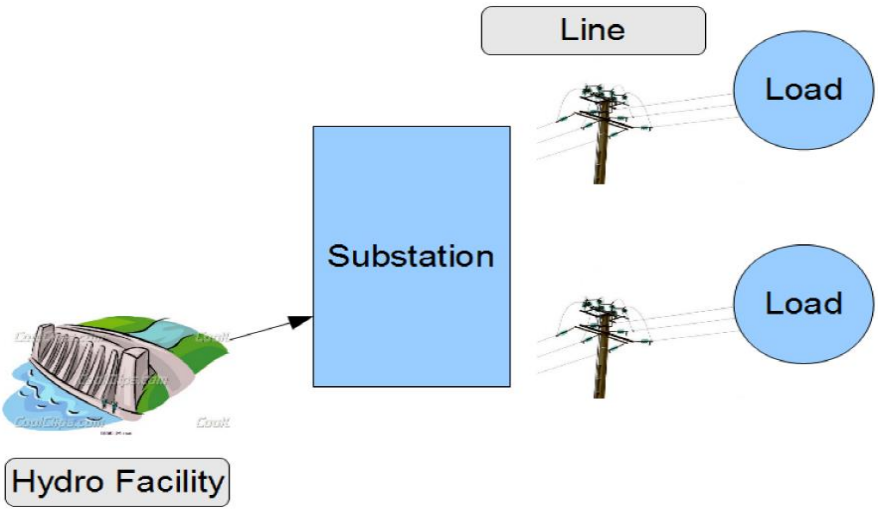

Fig. 22. Schéma de la plateforme

Nous avons structuré les entités concrètes, à savoir les sujets, les objets et les actions, en rôles (les techniciens, les agents, etc.), en vues (les charges, les lignes, les factures, les clients, etc.) et en activités (production et adaptation de l'énergie, réparation et entretien des lignes et installations, audit de l'énergie distribuée aux charges, etc.). Nous avons implémenté quelques contextes. La figure (Fig. 23) montre les principales classes que nous avons implémentées dans la plate-forme. Les noms de classes sont intuitifs.

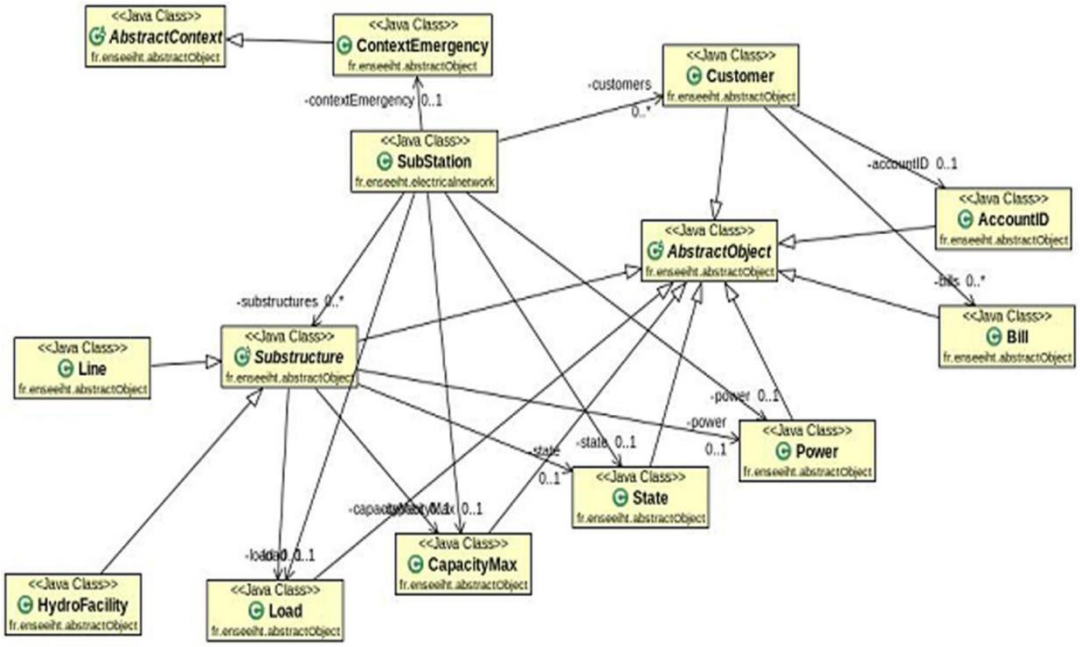

Fig. 23. Le diagramme de classes de plate-forme.

D'un point de vue technique, nous avons opté pour le langage de programmation Java. Les objets et les actions étendent deux classes abstraites, respectivement, la classe AbstractObject et la classe AbstractAction. Tous les éléments concrets de la politique de sécurité – à savoir les sujets, les objets et les actions – sont définis par un identifiant. Lorsqu'un utilisateur de la sous-station demande l'accès à une ressource, les trois identifiants sont collectés puis sont communiqués au modèle afin qu'il puisse statuer sur la requête. Pour ce faire, la plateforme implémente l'interface DataCollector fournie par le modèle.

IV.3.2. Implémentation du modèle I-OrBAC

Nous avons opté pour une architecture en mode client-serveur. Concrètement, les commandes exécutées au sein de la sous-station sont considérées comme que les requêtes d'accès adressées au *PEP* du modèle I-OrBAC de sorte que la décision puisse être évaluée selon les étapes décrites ci-dessus. Lorsque la plateforme est connectée au modèle, un certain nombre de tests est lancé pour vérifier que la politique de contrôle d'accès mise en œuvre fonctionne correctement. La figure Fig. 24 affiche un exemple de ces tests initiaux lancés lorsque la plateforme et le modèle sont couplés.

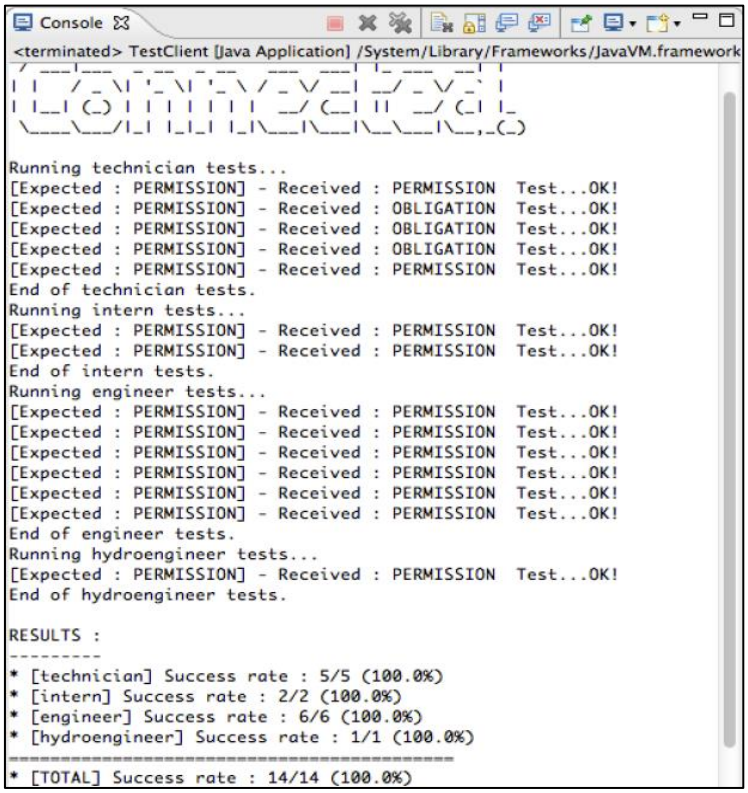

Fig. 24. Tests automatisés d'initialisation

Côté client, un agent de la sous-station se connecte à la plateforme puis exécute la commande d'une action à effectuer sur un objet donné. Les identifiants de ces trois entités sont collectées puis transmis au côté serveur qui représente le modèle I-OrBAC. Le diagramme de classes du modèle est présenté dans la figure Fig. 25. Tout d'abord, les identifiants sont recueillis par le *PEP* qui les adresse en suite au *PDP* pour statuer sur la requête conformément aux règles de la politique de sécurité et des valeurs d'attributs stockées respectivement dans le *PAP* et le *PIP*. Le *PAP* sauvegarde les règles relatives aux modes d'accès abstraits – c'est-à-dire les règles de type *Permission()*/*Obligation()*/*Interdiction()* – tandis que les autres règles à savoir *Habilite()*, *Utilise()* et *Considère()* sont stockées dans les différents bases de données du *PIP*. Nous avons choisi de stocker toutes les règles dans des fichiers XML comme l'illustré la figure Fig. 26, où quelques exemples de règles *Considère()* sont représentées.

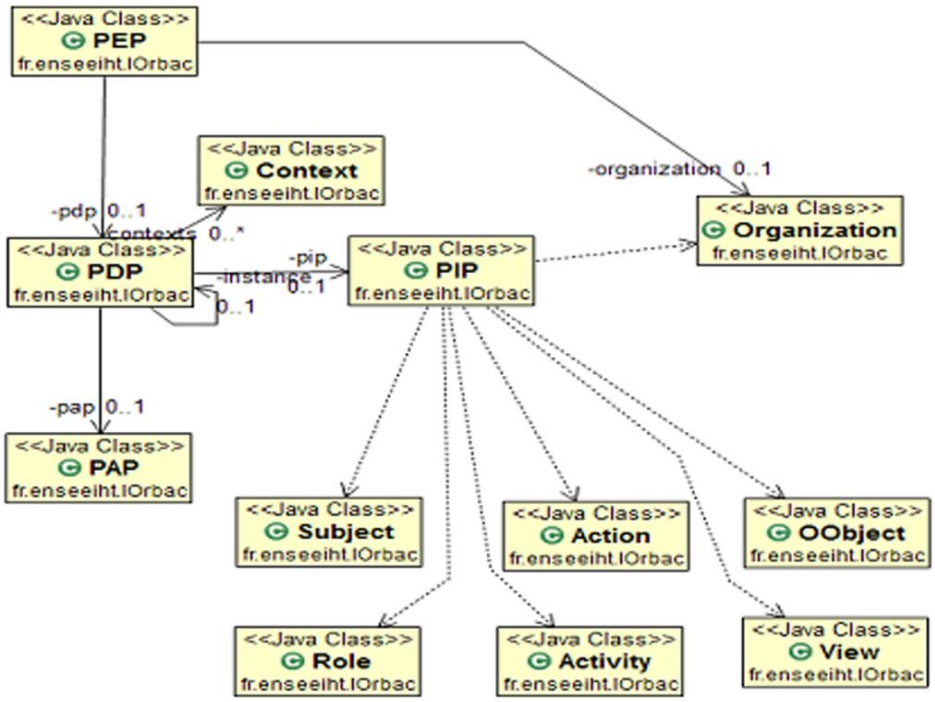

Fig. 25. Diagramme de classes du modèle I-OrBAC.

Pour gérer le deuxième type de décisions de contrôle d'accès, nous avons implémenté un module qui traite les tâches générées par le système puis entame le processus de sélection visant à déterminer le sujet/utilisateur le plus approprié conformément à la démarche itérative décrite précédemment.

```
<consider>
  <activities>

    <activity>
      <id>1</id>
      <integrity>0</integrity>
      <actions organization="0">
        <action>
          <id>1</id>
        </action>
      </actions>
    </activity>

    <activity>
      <id>2</id>
      <integrity>2</integrity>
      <actions organization="0">
        <action>
          <id>2</id>
        </action>
        <action>
          <id>3</id>
        </action>
```

Fig. 26. Un exemple de fichier XML pour les prédicats *Considère()*.

Ci-après, nous présentons un scénario simple de test mis en œuvre pour vérifier le bon fonctionnement de notre implémentation. Le scénario fait intervenir un sujet *Bob* jouant le rôle « *Technicien* » et étant caractérisé par un niveau d'intégrité égal à 2. *Bob* se connecte à la plate-forme et demande d'effectuer la maintenance d'une ligne – concrètement, l'action de maintenance est exécuté grâce à la commande « *ms* ». L'identifiant de la ligne cible à maintenir est « *2* » ; elle est considérée critique puisqu'elle dessert une importante usine. L'activité consistant à maintenir les lignes de distribution desservant les usines est également considérée critique quel que soit le contexte. Compte tenu de ces criticités, le niveau d'intégrité minimale imposé aux techniciens pour être apte à effectuer la maintenance de ces lignes est jugé égal à 3, ainsi *Bob* se voit refuser l'autorisation de réaliser la maintenance de la ligne. La figure (Fig. 27) illustre la réponse de refus du modèle qui signifie que *Bob* n'est pas autorisé à effectuer la maintenance de la ligne.

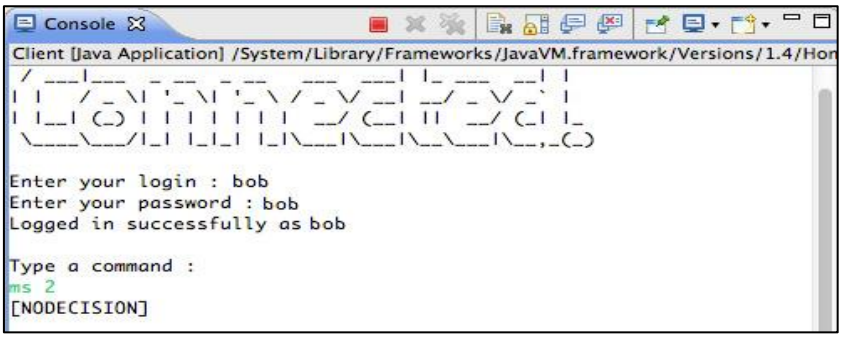

Fig. 27. Décision d'accès I-OrBAC

IV.4. Conclusion du chapitre

Dans ce chapitre nous avons présenté nos choix technologiques en matière d'architecture de contrôle d'accès ainsi que les ajustements réalisés pour adapter les standards existants au modèle que nous avons proposé. Nous avons aussi exposé les nouvelles étapes de la prise de décision de contrôle d'accès, impliquées par les modifications introduites, qui répondent au mode proactif proposé. Ensuite nous avons décrit la plateforme de l'étude de cas retenue pour tester le bon fonctionnement de notre modèle. Celle-ci est inspirée d'un projet européen abordant les questions de sécurité et de résilience dans les IC électriques. Pour finir, nous avons détaillé les choix de l'implémentation du modèle ainsi que les différents tests effectués.

Le prochain chapitre sera dédié à l'extension de notre modèle I-OrBAC pour la prise en compte des contraintes de collaboration. Dans ce sens, nous présenterons les enrichissements apportés à I-OrBAC ainsi que les démarches de négociation des contrats électroniques visant à régir les actes de collaboration.

CHAPITRE 5 :

DI-ORBAC : DISTRIBUTED I-ORBAC

SOMMAIRE

V.1. Préambule

Ce dernier chapitre aborde l'extension de notre modèle I-OrBAC aux environnements distribués afin de répondre aux exigences des IIC en matière d'intégrité et de colla-

borations sécurisées. Nous l'entamons par un rappel de l'importance des collaborations dans la réalisation d'objectifs jusque-là non atteints. Toutefois, nous insistons sur la gravité des dangers auxquelles sont exposées les organisations durant ces coopérations.

Notre extension Distributed I-OrBAC (DI-OrBAC) s'attache au concept central d'I-OrBAC qu'est l'organisation. Ainsi, pour exprimer des PS cohérentes pour les collaborations, DI-OrBAC intègre le concept d'organisation virtuelle (VO). Nous montrons donc comment les VO favorisent l'expression de PS cohérentes puisqu'elles fédèrent l'ensemble des biens engagés par les partenaires au sein d'une même organisation, permettant ainsi d'avoir une vision globale des ressources.

Puis, soucieux de ne pas imposer une PS centrale qui risquerait de ne pas satisfaire tous les partenaires, nous présentons le concept de contrat électronique qui permet non seulement de négocier les conditions d'utilisation imposées, d'imputer les responsabilités aux différentes parties mais aussi de préciser les pénalités en cas d'abus.

Nous enchainons ensuite par la présentation du modèle DI-OrBAC qui enrichit I-OrBAC grâce aux concepts de VO et de contrats électroniques. DI-OrBAC s'intéresse à deux axes principaux : la recherche des partenaires potentiels et la négociation des contrats électroniques. Concernant le premier axe, nous détaillons l'approche adoptée qui combine un processus de découverte proche de celui des protocoles de routage dynamique ainsi que des techniques de sélection des partenaires similaires aux techniques utilisées dans les modèles de gestion de la confiance. Pour optimiser la sélection des partenaires, nous introduisons un pseudo-protocole, adapté à I-OrBAC, permettant d'interroger et de recueillir les jugements des partenaires sur les organisations potentiellement crédibles. Les jugements collectés permettront par la suite de calculer localement des niveaux de crédibilité relatifs aux organisations et à établir la carte des partenaires. En revanche, pour établir le second axe, nous enrichissons I-OrBAC de certains prédicats afin de permettre aux organisations d'inviter des partenaires aux collaborations, de décrire les ressources qu'elles engagent ainsi que les conditions qu'elles imposent à l'utilisation de leurs ressources. Ces négociations permettront dans un premier temps d'élaborer la PS de la VO, qui une fois approuvée, sera traduite et adaptée au niveau des PS locales des partenaires. L'automatisation des négociations est soumise à des systèmes d'inférence qui statuent sur l'issue de celles-ci.

V.2. L'importance des collaborations :

De nos jours, rares sont les organisations évoluant à l'écart de leur environnement extérieur. En effet dans un contexte de compétitivité et d'innovation, les organisations cherchent davantage à offrir ou à bénéficier de services leur permettant de fournir des produits de qualité et d'affiner leurs techniques afin de garantir leur pérennité. Les relations

qui existent entre les organisations sont complexes et peuvent être répertoriées en cinq catégories : des intentions de *compétition*, d'*accommodation*, de *compromis*, d'*évitement* ou de *collaboration* [146, 147]. Brièvement, nous définissons ces cinq types de relations :

- La *compétition* : est une relation « *gagnant-perdant* » où les organisations tentent de défaire leurs rivales en gagnant leurs positions. Il est question donc de satisfaire les intérêts des unes au détriment des autres.
- L'*accommodation* : tente de satisfaire les intérêts d'autres organisations en négligeant ses propres intérêts. Il s'agit là d'une relation « *donnant-perdant* » où une organisation aide une autre à parvenir à ses objectifs sans rien y gagner.
- Le *compromis* : est une relation à mi-chemin entre la compétition et l'accommodation dépeignant la situation où des organisations ne sont ni pleinement satisfaites ni pleinement insatisfaites.
- L'*évitement* : décrit le cas où des organisations s'évitent en ne cherchant aucunement ni à satisfaire leurs besoins ni ceux des autres.
- La *collaboration* : est la relation qui cherche à satisfaire pleinement les intérêts de toutes les parties en réalisant des résolutions conjointement arrêtées. Il est question donc d'une relation « *gagnant-gagnant* ».

Collaborer sous-entend la conjugaison des efforts des partenaires en vue de réaliser des objectifs arrêtés satisfaisant des intérêts communs ou complémentaires chez les partenaires. Dans certains cas, ces actes de coopération peuvent ne pas aboutir ; ils risquent même de provoquer des incidents infligeant des dommages à certaines parties pour des raisons de fraude et de sabotage. Ces risques sont principalement dus au fait que les organisations engagent certaines de leurs ressources propres (actives ou passives) au profit de la collaboration afin de parvenir aux objectifs fixés. Ceci n'exclut donc pas de potentielles tentatives de sabotage pouvant cibler aussi bien les installations matérielles que le personnel actif sans oublier les propriétés intellectuelles. Ainsi, les questions de sécurité ne se limitent plus uniquement au périmètre local de l'organisation mais tendent à s'intéresser à de nouveaux paramètres relatifs à leurs collaborateurs. Leur assurer une sécurité adéquate tout au long de ces actes de collaboration permettra, entre autres, de leur garantir une continuité d'activité, d'améliorer leur compétitivité et de préserver leur image de marque.

Nous nous intéressons aux processus de collaboration qui sont motivés par une volonté de « complémentarité » ou de « carence en ressources ». Dans le premier cas, une organisation entame une collaboration puisqu'elle ne jouit pas de toutes les compétences nécessaires pour parvenir à ses objectifs qui requièrent des compétences dépassant le métier de l'organisation. Cette situation est rencontrée souvent chez les organisations qui

sous-traitent certains de leurs processus pour des raisons financières ou autres. En revanche, le deuxième cas survient lorsqu'une organisation est à cours de ressources et que pour respecter les contraintes calendaires, l'organisation fait appel à des organisations du même domaine pour lui fournir les ressources afin de réaliser les tâches qui lui incombe.

Pour satisfaire ces nouvelles contraintes de collaboration, les architectures de type client-serveur se retrouvent dépasser. En effet, d'autres types d'architectures, favorisant les collaborations, entrent en jeu telles les architectures « pairs à pairs » (P2P), les grids, etc. Au sein de ces architectures, les nœuds sont considérés tels des pairs, chacun caractérisé par ses propres spécificités. Le tout étant hétérogène, il est nécessaire de prendre cela en compte afin d'assurer une interopérabilité saine, ce qui implique concrètement la cohabitation de différents niveaux de sécurité répondant aux exigences de chacun et le protégeant des abus pouvant émaner de ses voisins. Cela se répercute inévitablement sur la gestion des PS qui régissent le fonctionnement des nœuds, puisqu'il est inconcevable d'élaborer une PS centralisée qui satisfasse les contraintes de tous. Cet état de fait permet de conclure que les modèles centralisés sont eux aussi inadaptés dans ce genre de situation vu que chaque pair doit pouvoir gérer sa PS indépendamment des autres et pouvoir collaborer de façon autonome. Dans ce sens, les concepts de VO et de contrats électroniques permettent de mettre en place des collaborations en toute souplesse, sans impacter les PS locales des nœuds. Dans ce qui suit, nous étudions ces deux concepts et essayons de faire le point sur leurs forces et leurs faiblesses.

V.2.1. Les organisations virtuelles

Afin de répondre aux besoins d'intégrité des IC dans un contexte distribué et collaboratif, nous développons une extension d'I-OrBAC. Celle-ci ne devra pas s'écarter du concept de l'organisation, fondamental dans I-OrBAC, pour continuer à élaborer des PS cohérentes et sans ambiguïtés. Pour cela, nous pensons cerner une collaboration multi-organisations dans les limites d'une organisation temporaire qui régirait l'accès aux ressources des différents partenaires comme s'il s'agissait de ses propres ressources. Dans la littérature, le concept de VO s'inscrit fidèlement dans la logique de ce raisonnement. Par définition, une VO est une coalition dynamique d'utilisateurs et de ressources issus de différents domaines, géographiquement dispersés, et qui sont unis par des objectifs communs [148, 149, 150]. Le caractère dynamique s'explique par le fait que les relations sont temporaires : elles naissent au début des collaborations et sont dissoutes lorsque les objectifs sont atteints ou lorsque des litiges surviennent. Le concept de VO se décline à travers une multitude d'applications [131, 151] : bureaux virtuels, entreprises virtuelles, mémoires virtuelles, équipes virtuels, etc. En pratique, les objectifs arrêtés par les collaborateurs ainsi que les ressources qu'ils fournissent constituent respectivement les objectifs et le patrimoine de la VO. Cette centralisation des objectifs et des ressources facilitera leur gestion et

leur administration. Soulignons que cette dernière déclaration ne s'oppose aucunement à la gestion décentralisée des PS des collaborateurs citée plus tôt [131, 151].

Les VO sont ainsi un outil de gestion qui reconnait explicitement la distinction entre les besoins fonctionnels et les moyens de leur réalisation concrète pour des activités orientées objectif. Concrètement, quatre activités sont nécessaires à la mise en place des VO [151] :

(1). Formulation des besoins abstraits.

(2). Recherche et analyse des moyens concrets de satisfaction des besoins.

(3). Affectation dynamique des moyens concrets aux besoins abstraits sur la base de critères explicites.

(4). Exploration et analyse des critères d'affectation.

A la lecture de ces activités, nous remarquons bien qu'elles concordent parfaitement avec les préoccupations suscitées chez les organisations acculées à collaborer. Ainsi, le concept de VO améliore l'efficacité et accroît le rendement grâce à une utilisation flexible et optimisée des ressources. Cette gestion optimisée des ressources est rendue possible grâce au contrôle managérial renforcé qui permet d'atteindre une meilleure qualité des produits et des services ainsi qu'une réduction notable des coûts [131].

En analysant ces activités dans le cadre de notre extension, nous remarquons que les deux premières activités s'appliquent au sein de toutes les organisations qui comptent entamer un processus de collaboration. Conformément à l'esprit d'I-OrBAC qui vise à préserver l'intégrité des ressources en amont, nous accorderons une grande importance à la deuxième activité. Dans ce sens, le choix des collaborateurs sera crucial afin de réduire les risques d'abus et de corruptions et de maximiser les chances de réussite de la collaboration. De plus, en appliquant les activités précédemment citées, les partenaires seront plus incités à penser aux objectifs organisationnels, sans plus se limiter uniquement aux tâches qui sont de leur ressort. Le recours aux VO offre un apport par rapport à l'approche P2P (fonctionnant en mode Ad-Hoc) dans le sens où il permet aux organisations d'avoir une vue d'ensemble du projet de collaboration et ainsi d'optimiser l'affectation des ressources. Un autre point positif des VO se rapporte au fait que toutes les transactions nécessitent au préalable l'établissement d'accords (contrats) implicites ou explicites ; ce qui garantit que les partenaires ne seront point lésés et que des négociations permettront de parvenir à des compromis justes.

Négocier les clauses et les conditions d'un contrat s'apparente la négociation des règles de sécurité d'une VO. Par conséquent, nous pensons que les contrats – dépourvus

des clauses relatives aux pénalités – peuvent être représenté par des PS. Ce constat profitera grandement lorsqu'il s'agira d'exprimer les règles relatives aux collaborations au niveau des PS propres aux partenaires. En effet, dans un premier temps, au lieu de se soucier des PS des collaborateurs, tout l'intérêt sera porté sur la négociation des règles de bon usage des ressources fournies dans le cadre de la VO. Dans ce sens, les efforts des partenaires seront canalisés dans l'élaboration et la négociation de la PS générale de la VO, vu que le bon fonctionnement de cette dernière satisfera leurs intérêts. Puis une fois l'ensemble des règles de la PS globale établies et approuvées, chaque organisation devra traduire la partie qui la concerne conformément au modèle et au langage qu'elle utilise. En d'autres termes, chaque organisation traduire tout bonnement la partie qui l'intéresse du contrat.

En définitive, l'application de la notion de VO favorisera l'utilisation des concepts d'I-OrBAC puisque le passage du distribué au localisé se fera aisément puisque les PS des partenaires ne constitueront que des traductions partielles de la PS globale de la VO. La section suivante abordera le concept de contrat électronique, en détaillant son importance, la structure de ces contrats ainsi que les briques qui les constituent.

V.2.2. Les contrats électroniques

Dans l'objectif de régir correctement ces actes de coopération, il est important d'établir des chartes – aussi connues sous le nom de contrats – qui permettront d'une part de définir le contexte, les clauses ainsi que les activités à réaliser et d'autre part, de prévenir l'occurrence de litiges et de les résoudre. En effet, en plus de clarifier les clauses de la collaboration et d'imputer à chaque partie les tâches qui lui incombe de réaliser, un contrat permet implicitement de dissuader les collaborateurs malhonnêtes – pensant aux pénalités encourues – et explicitement de résoudre les litiges auprès d'un magistrat. Ces contrats étaient généralement établis sur papier, ce qui rendait leur gestion et leur supervision fastidieuses surtout lorsque l'organisation est engagée dans plusieurs actes de collaboration. De plus, ils étaient exprimés en langage littéraire ce qui laissait souvent place aux ambiguïtés et aux interprétations. C'est alors que furent conçus les contrats électroniques exécutables dans l'objectif de faciliter leur gestion et leur supervision.

En général, les contrats sont définis comme des accords entre des parties en vue de créer et de mener à bien des affaires tout en respectant des contraintes légales. Dans ce sens, les contrats peuvent être vus tels des ensembles d'activités satisfaisant des termes bien définis, des conditions, des clauses et assujettis à des pénalités en cas de manquement. Dans la plupart des cas, la mise en place de contrats se conforme à un cycle de vie plutôt intuitif, en commençant par (1) l'identification des parties prenantes, suivie (2) d'une confrontation des besoins aux offres, puis (3) une négociation des termes, les conditions, des prix et des pénalités, qui une fois réussie donne lieu à (4) la signature dudit contrat qui

donne le feu vert à (5) son exécution. Une fois achevé, (6) le contrat est ensuite archivé. Ces pactes sont souvent structurés en cinq sections :

- Les parties : autrement dit les organisations et entreprises enrôlées.
- Les ressources et les activités : en d'autres termes les biens engagés par les parties ainsi que les tâches et services devant être exécutées.
- Les clauses : ne sont autres que les restrictions relatives à l'exécution des tâches, à savoir, les obligations, les paiements, les permissions et les interdictions.
- Les pénalités : stipulent les sanctions encourues par les parties en cas de manquement au contrat ou d'abus.
- L'arbitrage : ou les éléments de résolution des litiges.

Quand il s'agit de vérifier le respect des clauses, les solutions sollicitées ont recours à des paramètres booléens (succès ou échec), des indices ou contraintes temporelles, des événements externes, des automates temporisés [128], etc. D'autres paramètres de disponibilité et de « qualité de service » (QoS), exprimés dans les « accords de niveau de service » (SLA), peuvent aider à superviser le bon déroulement des activités liées à un contrat.

De nombreux travaux ont œuvré à représenter les contrats électroniques et à proposer des frameworks et des architectures pour les mettre en œuvre. Ainsi, une approche s'est basée sur la logique modale afin de préciser formellement les contraintes temporelles et les moyens de recouvrement des erreurs [152]. D'autres travaux ont proposé des architectures pour la négociation, la médiation, l'exécution et l'arbitrage des contrats électroniques [153], qui furent par la suite suivis d'efforts visant à décrire formellement la spécification des contrats en faisant appel à la logique non monotone et à la logique déontique [154]. Une autre approche très intéressante utilise le concept d'automates finis pour décrire les contrats et propose un système de contrats exécutables pour traiter les ambiguïtés et procéder à l'application et à la supervision des contrats durant l'exécution [155, 156]. Ces travaux furent par la suite enrichis pour tenir compte des règles métiers pour la spécification des clauses des contrats, permettant ainsi un meilleur contrôle de conformité à l'exécution des contrats [157].

La technologie des contrats électroniques offre de multiples avantages, à commencer par une productivité améliorée et une accélération considérable du cycle de vie des contrats. Notons aussi que les contrats électroniques permettent une meilleure supervision de l'exécution des tâches, ce qui concourt à la réduction des risques et à l'amélioration de la sécurité, impliquant ainsi une nette augmentation des profits. Sur le plan pratique, les contrats électroniques offre l'avantage d'une expression plus explicite et plus compréhensible des détails et implications propres aux clauses, comparées aux contrats traditionnels ;

de plus leur gestion et leur supervision sont plus aisées. Il devient donc plus facile de détecter les violations et de les arbitrer : la résolution des conflits est favorisée par le recours aux informations pertinentes stockées dans les fichiers journaux.

Dans ce qui suit, nous présenterons un langage spécialement conçu et adapté pour le modèle I-OrBAC afin de permettre la négociation des contrats entre les organisations. L'idée est de fournir aux organisations un modèle complet leur permettant d'entamer des collaborations sans avoir à changer de modèle de sécurité pour gérer les accès externes ni même un nouveau langage, qui risquerait d'être incompatible, pour négocier et mettre en place les contrats électroniques.

V.3. DI-ORBAC

V.3.1. Origine des ressources de la VO

Pour s'aligner sur les exigences de suspicion et de discrétion des IC, nous optons pour une gestion décentralisée des collaborations (cf. II.4.2.3.2). Dans ce sens, chaque organisation régira les accès relatifs à ses ressources. Seulement, pour assurer une cohérence tout au long de la collaboration et éviter des restrictions au cours de la réalisation des tâches, nous insistons sur le fait que les organisations devront, au préalable, se mettre d'accord conjointement sur les clauses et les conditions des opérations, autrement dit, les parties devront négocier des contrats qui seront par la suite scrupuleusement appliqués pour écarter tout litige et atteindre les objectifs dans les meilleures conditions.

Afin de réaliser les tâches de la collaboration, les organisations doivent mobiliser certaines de leurs ressources aussi bien actives que passives. Dans le cas général, une organisation fournira les sujets tandis que l'autre fournira les objets. Reste les activités, celles-ci peuvent être fournies par l'une ou l'autre (Fig. 28). En effet, nous pouvons discerner deux cas de figure : (1) lorsqu'il est question de collaborations dans un cadre de complémentarité, les sujets utilisent leur savoir-faire puisque les tâches dépassent le domaine de compétence de l'organisation qui fournit les objets ; (2) alors que dans le cas de collaborations dans un contexte de carence en ressources, les activités sont elles aussi fournies par l'organisation qui fournit les objets, puisque ces derniers font partie de sa sphère d'autorité, ils sont donc régis conformément à la politique qu'elle a établie.

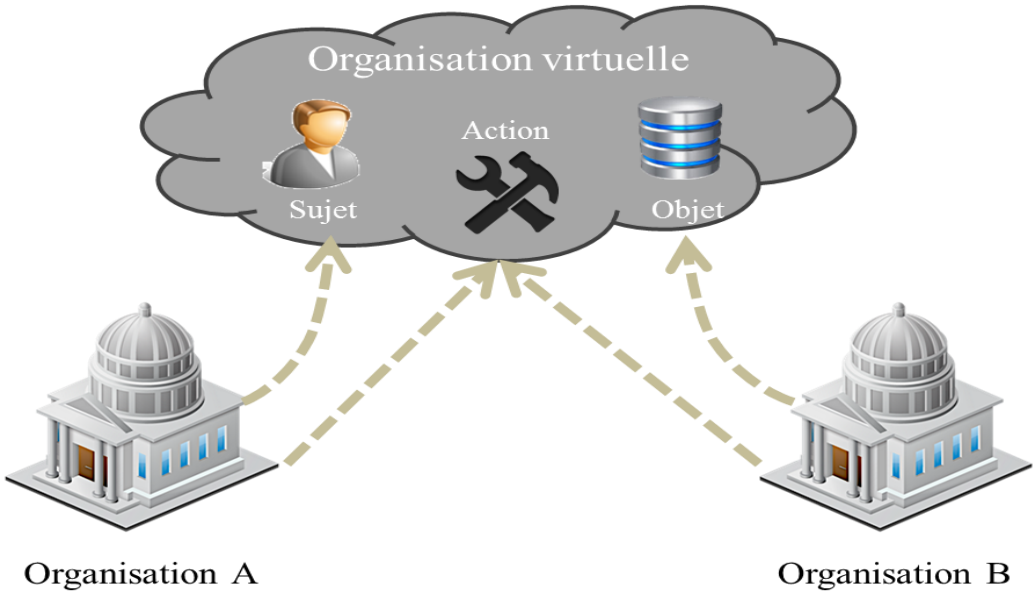

Fig. 28. Origines des ressources de la VO

V.3.2. Déroulement des collaborations

Mettre en place des collaborations nécessite une démarche consistant en cinq étapes :

(1). *La recherche des collaborateurs* : est une étape cruciale puisque le succès de la collaboration en est tributaire. En effet, un mauvais choix du collaborateur peut non seulement freiner ou compromettre la réalisation des objectifs, voire pire encore, entrainer la perte ou la corruption (d'un point de vue intégrité) des ressources engagées.

(2). *L'accord sur les termes du contrat de collaboration* : est une étape tout aussi importante que la première puisqu'elle permettra d'imputer les responsabilités, d'éclaircir les ambiguïtés et de départager les parties en cas de litige.

(3). *L'exécution des tâches* : est entamée suite à la négociation du contrat et à l'imputation des responsabilités aux différentes parties, puisqu'il s'agit dès lors de concrétiser de façon effective la collaboration ; ainsi chaque partie réalise les tâches qui lui sont attribuées conformément aux clauses négociées. Sur le plan pratique, ces clauses sont traduites en des règles de sécurité pour contrôler concrètement les accès aux ressources.

(4). *Le suivi de la collaboration* : s'étend tout au long du déroulement de la collaboration. Pour ce faire, il est impératif de disposer d'indicateurs et de mesures permettant aussi bien d'évaluer l'état d'avancement des travaux, leurs chances

de réussite, les causes du retard, que de déceler précocement d'éventuelles manœuvres frauduleuses pouvant causer la perte ou la corruption des ressources engagées.

(5). *La clôture et l'archivage de la collaboration* : A la fin d'une collaboration, il est important de statuer sur son issue. Dans ce sens, une synthèse est de mise faisant le point sur le déroulement des activités, les objectifs atteints et ceux non achevés, les éventuelles causes des retards et leurs origines. Tous ces paramètres devront permettre à l'organisation de se constituer un avis sur les partenaires et surtout de décider si d'autres projets communs pourront être démarrés avec ces partenaires.

Dans le cadre de notre extension, nous nous intéresserons tout particulièrement aux deux premières étapes vu qu'elles sont directement liées au développement et à l'expression de la PS. Nous écartons les trois étapes suivantes qui se rapportent plus à l'exécution et au suivi des tâches de la collaboration suite à l'établissement de la PS durant les deux premières étapes.

V.3.2.1 Recherche des collaborateurs

Comme précédemment mentionné, cette étape est très importante puisque le bon choix des collaborateurs favorisera la réussite de la coopération et la préservation des ressources de l'organisation. Pour optimiser ce choix, plusieurs critères devront être considérés, parmi eux : l'expérience, la réputation, la connaissance, l'absence de conflits d'intérêts, les certifications, etc. Dans notre cas, nous comptons coupler certaines techniques de gestion de la confiance à notre modèle I-OrBAC en les adaptant au besoin d'intégrité des IC afin d'optimiser le choix des partenaires. En effet, du point de vue de l'intégrité, il est important de choisir des collaborateurs qui soient crédibles et intègres : des partenaires qui réaliseront leurs tâches correctement sans menacer l'intégrité des ressources engagées. Ce raisonnement est analogue au mode proactif proposé dans I-OrBAC qui consiste à attribuer l'exécution d'une tâche au sujet le plus apte à la réaliser.

Ainsi, nous devrons fournir aux organisations des moyens leur permettant de découvrir, d'évaluer et de statuer sur la crédibilité de chacune des organisations les environnant. Cela consiste à élaborer des outils de catégorisation et de classement des organisations selon leurs compétences dans leurs domaines d'expertise. Ainsi, nous œuvrerons à étendre la notion de priorités des rôles et de niveaux de crédibilité du modèle I-OrBAC aux collaborations. Dans ce sens, nous assimilons la conduite de cette prospection des collaborateurs au processus utilisé dans les protocoles de routage dynamique utilisés dans les réseaux. Le routage est le mécanisme grâce auquel sont calculés puis sélectionnés des chemins pour acheminer des données, depuis un émetteur jusqu'au(x) récepteur(s), à travers

un réseau. Ainsi les protocoles de routage dynamique décrivent des processus actifs d'échanges de données d'accessibilité afin d'établir une carte du voisinage puis de déterminer les meilleurs chemins pour relayer les données aux différentes destinations du réseau. Ces protocoles reposent sur trois piliers fondamentaux (Fig. 29) :

- *Un protocole* : pour permettre aux nœuds d'échanger des informations d'accessibilité relatives à leurs voisins. Ces échanges permettront à chaque nœud d'établir une carte de son réseau environnant, avec les voisins directs, les voisins des voisins et ainsi de suite.
- *Un algorithme* : qui calculera sur la base de ladite carte, le meilleur chemin vers chaque destination de la carte, pour cela, l'utilisation de métriques et de critères de choix s'impose.
- *Une table* : qui regroupera et stockera tous les chemins sélectionnés par l'algorithme et qui sera consulté pour l'envoi de chaque paquet.

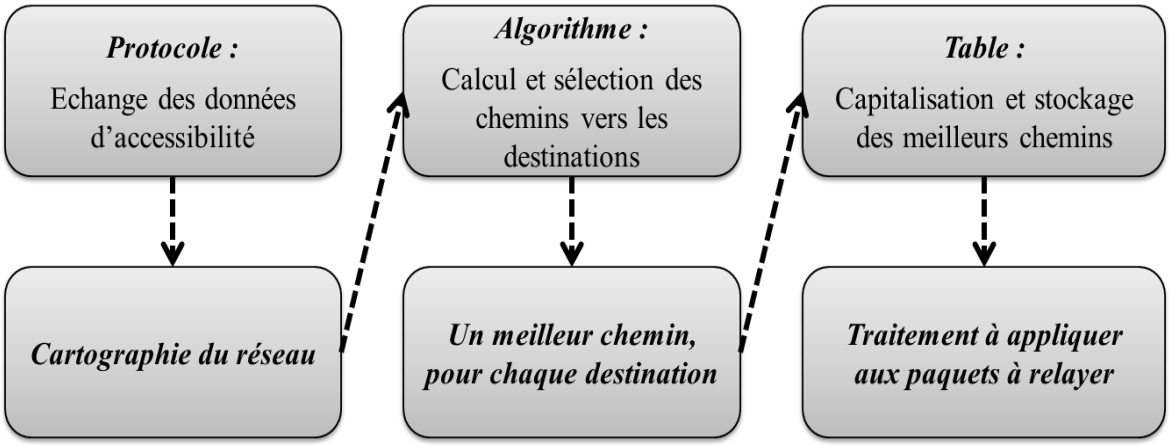

Fig. 29. Piliers des protocoles de routage

A l'image de cette démarche appliquée aux nœuds d'un réseau, une organisation *Org*, à son tour, devra commencer par découvrir et répartir son environnement pour établir une cartographie de ses partenaires. Pour ce faire une idée sur les organisations, deux cas de figure s'offrent à *Org* : (1) l'interaction directe avec celles-ci (2) ou bien l'analyse d'échos et informations relatives à ces entités lui parvenant d'autres organisations. Pour ce qui est du premier cas, *Org* doit coopérer avec l'organisation pour être en mesure de statuer directement sur sa crédibilité, en jugeant la qualité du service fourni, le respect des délais, la non dégradation de ses ressources, etc. En revanche, si nul acte de collaboration n'a eu lieu avec une certaine organisation, *Org* devra collecter, sélectionner puis se fier à certains jugements portés par d'autres organisations à l'égard du collaborateur potentiel. Nous retrouvons ce procédé collaboratif permettant l'échange des jugements relatifs aux parte-

naires dans les modèles basés sur la confiance. La figure (Fig. 30) représente le processus abstrait du choix des collaborateurs qui sera adopté dans DI-OrBAC.

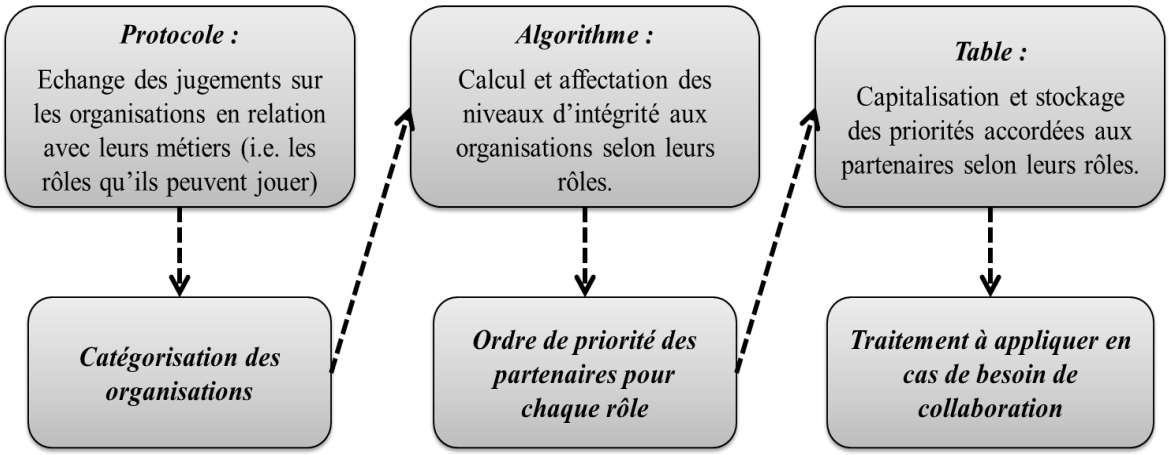

Fig. 30. Processus du choix des collaborateurs

V.3.2.1.1. Echange des informations relatives aux organisations

Echanger des avis concernant les habilitations des organisations n'est pas envisageable grâce au langage d'I-OrBAC puisque nul prédicat ne permettrait cela. Dans le cadre de l'élaboration d'un pseudo-protocole qui permettra aux organisations de communiquer leurs avis sur les éventuels partenaires, nous introduisons deux nouveaux prédicats : l'un pour l'interrogation des organisations sur leurs opinions au sujet d'une autre organisation, l'autre servira aux organisations interrogées de renseigner leur évaluation. Ainsi, le prédicat d'interrogation se présente syntaxiquement comme suit :

$$Statut(Org_{req}, Org_{inter}, Org_{cible}, r_{cible}) \qquad (11)$$

Le prédicat (11) stipule que l'organisation « Org_{req} » interroge l'organisation « Org_{inter} » (organisation interrogée) au sujet de l'organisation cible « Org_{cible} » au sujet d'un rôle particulier « r_{cible} ». Une écriture plus élaborée permettrait d'interroger simultanément plusieurs organisations au sujet d'une organisation cible concernant de multiples rôles cibles. L'écriture serait de la forme (avec $\{(p,q) \in \mathbb{N}^2 et\ p > 1\ et\ q > 1\}$) :

$$\begin{aligned} &Statut(Org_{req}, Org_{inter(1)} \wedge \dots \wedge Org_{inter(p)}, Org_{cible}, r_{cible(1)} \wedge \dots \wedge r_{cible(q)}) \\ &\quad = Statut(Org_{req}, Org_{inter(1)}, Org_{cible}, r_{cible(1)} \wedge \dots \wedge r_{cible(q)}) \wedge \dots \\ &\quad \wedge\ Statut(Org_{req}, Org_{inter(p)}, Org_{cible}, r_{cible(1)} \wedge \dots \wedge r_{cible(q)}) \qquad (12) \end{aligned}$$

En réponse à cette requête, les organisations énonceront leurs jugements grâce au prédicat *Evalue*() dont la syntaxe est la suivante :

$$Evalue(Org_{inter}, Org_{req}, Org_{cible}, r_{cible}, l_{Org_{cible}}) \qquad (13)$$

Le prédicat (13), pour sa part, stipule qu'« Org_{inter} » répond à « Org_{req} » en évaluant l'habilitation d'« Org_{cible} » dans le rôle « r_{cible} » à un niveau de crédibilité $l_{Org_{cible}}$. Les niveaux de crédibilité renseignés sont issus d'une échelle représentative préalablement négociée entre les différentes organisations partenaires – nous pouvons considérer comme exemple l'échelle de crédibilité établie dans (Fig. 19). En récupérant tous les $l_{Org_{cible}}$émis par les différentes organisations interrogées, « Org_{req} » pourra à ce moment-là, les fournir comme entrées à l'algorithme qui lui permettra de statuer sur le niveau de crédibilité final à accorder à « Org_{cible} » dans le rôle « r_{cible} ». Dans ce qui suit, nous aborderons l'aspect relatif à l'algorithme de catégorisation des organisations.

V.3.2.1.2. Phase catégorisation des organisations

Dans l'absolu, les relations liant les organisations peuvent être catégorisées en trois classes génériques : des relations de *confiance*, de *neutralité*, de *doute* (Fig. 31). Le premier cas se manifeste lorsque des organisations ont déjà collaboré et que les collaborations ont été fructueuses et satisfaisantes ou que des partenaires de confiance recommandent une organisation (amis de mes amis). Le deuxième cas, quant à lui, reflète le cas où des organisations n'ont jamais collaboré avant et que les avis des partenaires de confiance sont partagés. Le troisième cas, en revanche, se manifeste lorsque d'antérieures collaborations se sont soldées par des résultats non satisfaisant ou que les partenaires de confiance portent des avis plutôt mitigés concernant une organisation. Notons que lorsqu'il s'agit d'identifier les organisations à interroger, il est possible de se limiter seulement aux organisations partenaires de confiance, tout comme les requêtes peuvent être généralisé à toutes les organisations, en faisant bien sûr intervenir des formules pondérées pour souligner la distinction entre les avis. Dans le cadre de DI-OrBAC, nous optons pour la première solution consistant à ne se tourner que vers les partenaires de confiance.

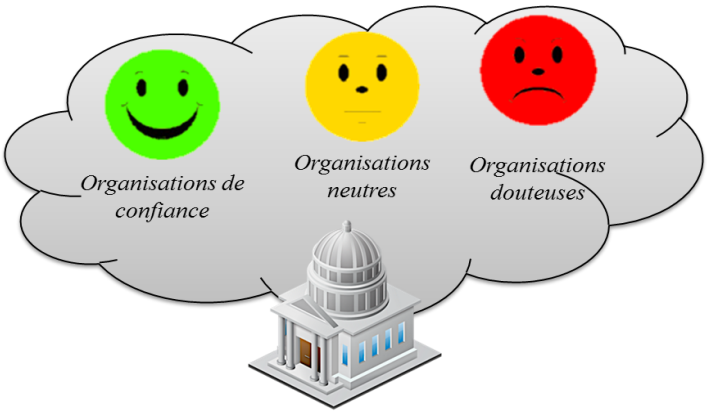

Fig. 31. Classes de partenaires environnant une organisation.

Durant cette phase de catégorisation, *Org* peut se limiter seulement à l'évaluation de la crédibilité de chaque organisation dans son ensemble. Dans ce cas, le niveau de crédibilité accordé à chaque organisation sera hérité par l'ensemble de ses sujets. Une autre option est envisageable, surtout dans les cas de suspicion extrême, *Org* peut recueillir aussi des informations sur la crédibilité des sujets de ces partenaires potentiels, ne se limitant pas seulement à la crédibilité de l'organisation. Ce deuxième cas risque de devenir très complexe pour différentes raisons : des organisations à effectifs importants, échange massif d'informations de crédibilité concernant l'ensemble des sujets de toutes les organisations, formules et algorithmes complexes pour le calcul interne des crédibilités relatives aux sujets externes. Dans un premier temps, nous optons pour la première option qui propose d'évaluer la crédibilité de l'organisation dans son ensemble sans soucier de chaque sujet à part. Nous laissons ainsi aux organisations la tâche de la sélection d'agents crédibles pour les représenter, afin de ne pas subir les pénalités précisées dans les contrats ou se voir marginalisées lors de futures collaborations, en raison de la chute de leur crédibilité en milieu collaboratif.

Pour réduire la complexité du contrôle d'accès en environnement distribué, les organisations partenaires d'*Org* seront considérées comme des sujets internes. Ainsi, conformément à l'esprit d'I-OrBAC, ces organisations se verront affecter des rôles en accord avec leurs compétences, les services et les activités qu'ils pourront fournir ou réaliser pour *Org*. Aussi ces partenaires se verront attribuer des niveaux de crédibilité pour chaque rôle affecté dans *Org*. De ce fait, *Org* pourra traiter le problème du choix d'un sujet externe tel un simple choix de sujet interne. Le tableau ci-après (Tab. 4) illustre une matrice de niveaux de crédibilité où sont affectés des niveaux à des *organisations ayant déjà collaboré avec Org* dans le cadre de certains rôles. Ces organisations sont considérées comme des sujets internes.

Rôles / Sujets	Rôle 1	Rôle 2	Rôle 3
Sujet interne 1	4	2	1
Sujet interne 2	2	3	-
Sujet interne 3	0	2	3
Org A	2	0	1
Org B	2	-	3

Tab. 4. Représentation des niveaux de crédibilités des sujets et des partenaires ayant déjà collaboré avec *Org*.

En revanche, dans le cas d'organisations n'ayant jamais collaboré avec *Org*, celle-ci devra interroger ses partenaires de confiance afin de collecter leurs jugements relatifs à ces nouvelles organisations dans certains rôles. Ainsi, *Org* utilisera le prédicat *Statut*() pour émettre ses requêtes puis récupérera les réponses des partenaires à travers les prédicats *Evalue*() dont elle extraira les niveaux de crédibilités émis par ses partenaires. Ces niveaux de crédibilité seront fournis comme entrées à l'algorithme de calcul des niveaux de crédibilité locaux d'*Org*. L'algorithme en question est constitué d'une formule pour le calcul des niveaux de crédibilité. Il n'est guère possible d'établir une formule qui pourrait servir à tous les contextes d'IC ; nous proposons donc la formule suivante en guise d'exemple :

$$(l_{Org_{cible}})_{Org} = \left\lfloor \sum_i \left\lceil \frac{l_{Org_{inter(i)}} \times l_{Org_{cible(i)}}}{card(L_S)} \right\rceil \Big/ card(ORG_{inter}) \right\rfloor \qquad (14)$$

Avec :

- $(l_{Org_{cible}})_{Org}$: le niveau de crédibilité relatif à « Org_{cible} », dans le rôle « r_{cible} » calculé par *Org*.
- $l_{Org_{inter(i)}}$: le niveau de crédibilité qu'accorde *Org* à l'organisation interrogée d'indice i « $Org_{inter(i)}$ » (avec $i \in \mathbb{N}^*$).
- $l_{Org_{cible(i)}}$: le niveau de crédibilité accordé par « $Org_{inter(i)}$ » à l'organisation cible « Org_{cible} » dans le rôle « r_{cible} ».
- $card(L_S)$: le cardinal de l'ensemble des niveaux de crédibilité négociés entre les organisations.
- ORG_{inter} : le sous-ensemble des organisations interrogées par *Org*.
- $\lfloor x \rfloor \; et \; \lceil x \rceil$ sont respectivement les notations anglo-saxonnes de la partie entière par défaut et par excès.

La formule (14) ne représente qu'un exemple ; chaque administrateur d'IIC est en mesure d'élaborer les formules qui répondront au mieux à ses contraintes et à ses exigences. Une fois $(l_{Org_{cible}})_{Org}$ calculé, le niveau est ensuite inséré dans la matrice des niveaux de crédibilité que tient *Org*, afin de faire appel, le moment venu, aux services d'« Org_{cible} » dans le rôle « r_{cible} », si bien sûr $(l_{Org_{cible}})_{Org}$ le permet. Tout au long du processus de découverte, *Org* calculera des niveaux de crédibilité pour les différentes organisations de son environnement dans divers rôles.

V.3.2.2 L'accord sur les termes du contrat

Après avoir cartographié l'environnement, identifié les partenaires potentiels et spécifié leurs rôles d'intervention ainsi que leurs niveaux d'intégrité, il s'agira de les inviter à collaborer en leur proposant un contexte de collaboration. Une fois la mission et le contexte acceptés, la négociation et l'établissement du contrat qui régira la collaboration pourront être entamés. Comme précédemment évoqué, le contrat de la VO comptera cinq sections (cf. V.2.2). Nous nous limiterons à la négociation des trois premières sections, celles relatives aux collaborateurs, aux ressources engagées et aux clauses. A l'issue de ces trois phases de négociation, sera établie la PS globale de la VO. Puis une ultime étape s'imposera pour finaliser les PS locales des partenaires. Cette négociation se fera, en partie, grâce au langage d'I-OrBAC ; celui-ci sera toutefois enrichi par de nouveaux prédicats pour répondre aux aspects distribués. Les nouveaux prédicats, qui constitueront le langage de DI-OrBAC, seront présentés au fur et à mesure que les étapes de négociation seront explicitées (Fig. 32).

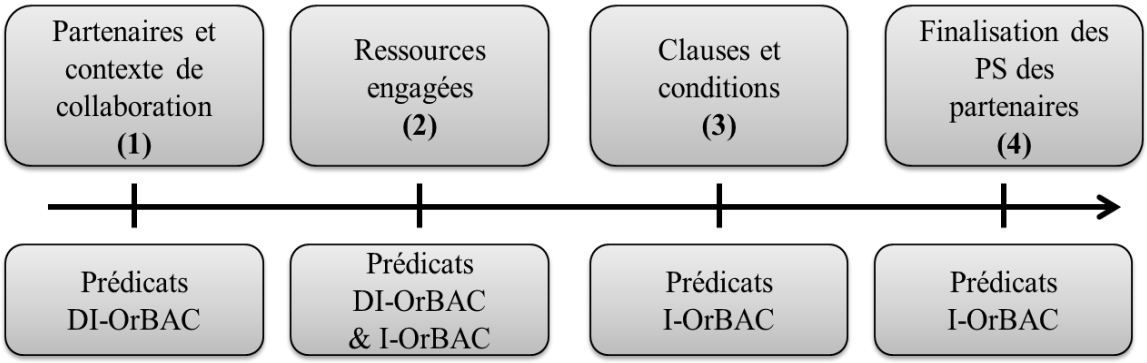

Fig. 32. Etapes de la négociation des contrats dans DI-OrBAC.

Notons aussi qu'à l'issue de chacune des trois premières étapes de cette négociation, des étapes charnières de résolution de conflits sont insérées (Fig. 33). Cela aura pour but, entre autres, de rendre la négociation dynamique, de repérer précocement les négociations qui n'aboutiront pas et de réajuster au fur et à mesure certains paramètres afin d'augmenter les chances de la collaboration.

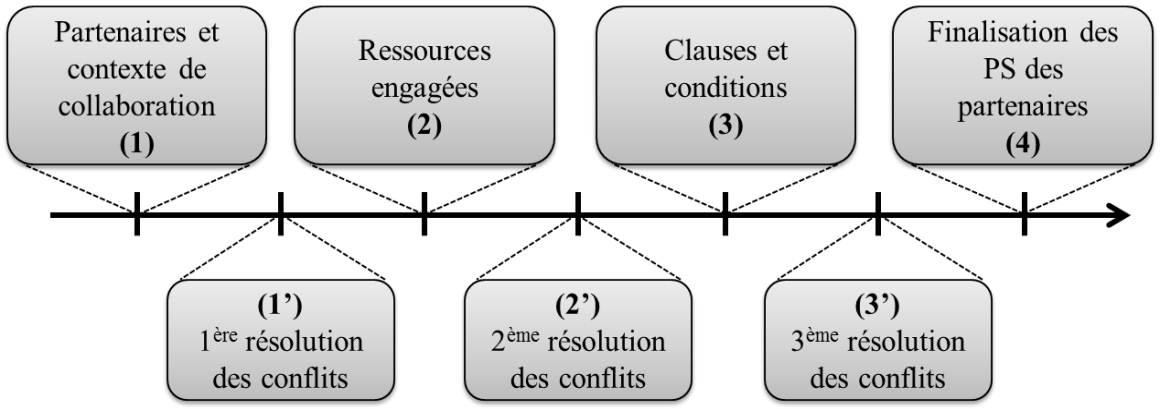

Fig. 33. Les étapes de résolution de conflits.

Tout au long de cette section, nous considérons les ensembles *ORG*, *C*, *V*, *O*, *AY*, *AC*, *R* et *S*, regroupant respectivement les organisations, les contextes, les vues, les objets, les activités, les actions, les rôles et les sujets. Aussi nous considérons les ensembles des niveaux d'intégrité L_V, L_{AY}, L_C, L_S relatifs respectivement aux vues, aux activités, aux contextes et aux sujets ainsi que des échelles de niveaux génériques (par exemple, Fig. 19) acceptées par l'ensemble des organisations afin d'établir une base commune pour les négociations des contrats.

V.3.2.2.1 Etape (1) : Fédération des partenaires et proposition du contexte de collaboration

Inviter un partenaire à la collaboration, tout en lui présentant le contexte, ne peut être décrit grâce au langage d'I-OrBAC ; dans ce sens, nous introduisons un nouveau prédicat qui permettra aux administrateurs des organisations d'inviter les partenaires à la collaboration en précisant les paramètres suivants : l'*identifiant de l'organisation initiatrice* ($Org_{init} \in ORG$), les *identifiants des partenaires souhaités* ($(Org_1, \ldots, Org_n) \in ORG^n$), le *contexte de la collaboration* ($c \in C$) ainsi que son *niveau de criticité* (l_c). Le prédicat *Invite*() se présentera syntaxiquement comme suit :

$$Invite(Org_{init}, Org_1, \ldots, Org_n, c, l_c) \qquad (15)$$

Sémantiquement, le prédicat (15) stipule que l'organisation Org_{init} souhaite entamer une coopération qui nécessitera le concours des organisations (Org_1, …, Org_n) précisés en arguments. Le contexte de la collaboration ainsi que son niveau de criticité sont déclarés en dernier, par analogie à I-OrBAC. Afin de mieux gérer les négociations ultérieures, nous optons pour une subdivision de la collaboration globale en des collaborations bilatérales. Dans ce sens, le prédicat (15) sera traduit comme suit :

$$Invite(Org_{init}, Org_1, c, l_c) \wedge \ldots \wedge Invite(Org_{init}, Org_n, c, l_c) \qquad (16)$$

Après la consultation de leurs PS pour décider de leur enrôlement dans la collaboration, chaque organisation souhaitant prendre part à la collaboration le déclarera en utilisant le prédicat *Confirme*() qui se présente comme suit :

$$Confirme\left(Org_i, Org_{init}, c'_i, l_{c'_i}\right) \qquad (17)$$

Les confirmations, quant à elles, ne peuvent être que nominatives : elles ne contiennent que l'*identifiant de l'organisation favorable à la collaboration*, l'*identifiant de l'organisation initiatrice,* le *contexte* ainsi que son *niveau de criticité tels qu'elle les perçoit*. A l'issue de cette première étape, une première résolution de conflits aura lieu afin de déterminer les organisations qui prendront part à la collaboration, s'assurer que ces dernières acceptent bien le contexte proposé et que le niveau déclaré dans l'invitation n'est pas exagéré.

V.3.2.2.2 Etape (1') : Première résolution de conflits

L'objectif de n'importe quelle collaboration, aussi complexe soit-il, peut être subdivisé en plusieurs sous-tâches de type (*c, v, ay*) – caractérisées par (l_c, l_v, l_{ay}) réalisées dans un cadre bilatéral. Compte tenu de cela, une organisation initiatrice, prodiguant soit les vues soit les activités, est en mesure de reconnaitre sa carence, laquelle sera soit l'activité à réaliser ou bien les vues à utiliser. Par conséquent, l'organisation sera en mesure de déterminer les rôles pouvant réaliser la tâche (*c, v, ay*) et de repérer les organisations de confiance dans chacun de ces rôles. Le sous-ensemble d'organisations capables de réaliser ladite tâche est noté « *SOrg* », tout rôle confondu (i.e. état Initialiation). Evidemment, pour les différentes priorités de rôles seront calculés différents niveaux seuils pour déterminer les organisations aptes à réaliser la tâche selon le rôle qui lui est affecté.

Les organisations choisies seront invitées à la collaboration grâce à la formule (16) :

$$Invite(Org_{init}, Org_1, c, l_c) \wedge \ldots \wedge Invite(Org_{init}, Org_n, c, l_c) \qquad (16)$$

Les confirmations des organisations seront décrites par des formules (17) :

$$Confirme\left(Org_i, Org_{init}, c'_i, l_{c'_i}\right) \qquad (17)$$

Les prédicats *Invite*() et *Confirme*(), émis par les différents partenaires, sont recueillis et confronter pour mettre en place la VO qui soutiendra cette coopération. Les contextes récupérés depuis ces prédicats permettront de réajuster les contraintes générales de la collaboration. Dans le cas où certaines organisations ne répondent pas favorablement à l'appel

de la collaboration, l'organisation initiatrice devra inviter d'autres organisations à prendre part à la coopération. Pour décrire formellement les étapes de cette négociation, nous proposons le système d'inférence suivant :

Init	$\frac{ORG,(v,ay,c)}{SOrg}$	*avec SOrg contient l'ensemble des organisations appropriées à la collaboration pour la réalisation du triplet* (c,v,ay)
Succès	$\frac{\{Org_i\} \cup SOrg,(v,ay,c)}{Collabore(VO_i,Org_{init},Org_i,c,l_c)}$	*si* $\exists\, i \in \mathbb{N} \,/\, Confirme(Org_i,Org_{Orig},c'_i,l_{c'_i}) \wedge c \sim c'_i \wedge l_c = l_{c'_i} \mp 1$
Suit	$\frac{\{Org_i\} \cup SOrg,(v,ay,c)}{SOrg,(v,ay,c)}$	*si la règle Succès n'est pas valide*
Echec	$\frac{\emptyset,(v,ay,c)}{Echec}$	*si nulle autre règle ne s'applique*

Tab. 5. Système d'inférence régissant l'étape 1 de la négociation

Les prédicats *Invite*() et *Confirme*() seront confrontés deux à deux afin de statuer sur la possibilité de collaboration entre Org_{init} et chaque Org_i, sur la base de la comparaison des contextes et des niveaux de criticité déclarés.

$$Invite(Org_{init},Org_i,c,l_c) \wedge Confirme(Org_i,Org_{init},c'_i,l_{c'_i}) \quad (18)$$

Ainsi dans (18), si *c* et *c'* sont équivalents et que $l_c = l_{c'_i} \mp 1$, cela veut dire que les organisations sont relativement d'accord sur les termes généraux de la collaboration (i.e. état Succès). Par conséquent, une collaboration partielle sera établie entre Org_{init} et Org_i ayant confirmé. Cette collaboration sera conclue et insérée dans la politique de la VO_i grâce au prédicat :

$$Collabore(VO_i,Org_{init},Org_i,c,l_c) \quad (19)$$

Le prédicat (19) initie la PS de la sous-VO, identifiée par le paramètre VO_i, qu'elle a été instauré à la demande de l'organisation Org_{init}, que l'organisation Org_i y participe, que le contexte retenu pour la collaboration est *c* et que son niveau d'intégrité est l_c. Si toutes les organisations répondent favorablement alors la collaboration globale sera l'union des collaborations partielles est sera instanciée comme suit :

$$Collabore(VO_i,Org_{init},Org_1,\dots,Org_n,c,l_c) \quad (20)$$

Tous les couples de prédicats *Invite*() et *Confirme*() seront confrontés pour déterminer les organisations qui prendront part à la collaboration. Toutefois, si une confrontation donne lieu à des contextes non équivalents (i.e. *c* et *c'* non équivalents) et/ou des niveaux

de criticité largement différents, les organisations pourront rectifier leurs déclarations ou bien Org_{init} devra inviter d'autres organisations (i.e. état Suit).

Finalement, si Org_{init} invite toutes les organisations de l'ensemble *SOrg* et que celles-ci ne confirment pas ou qu'elles ne s'entendent pas sur le contexte. La collaboration de base échouera. A ce moment-là, Org_{init} devra soit se contenter des collaborations partielles établies soit, revoir le contexte qu'elle a proposé.

V.3.2.2.3 Etape (2) : Déclaration des ressources engagées

Lors de cette étape, chaque organisation sera appelée à décrire les ressources qu'elle compte engager dans le cadre de la collaboration. Cette description devra contenir des informations reflétant le degré d'importance de la ressource afin de pourvoir sensibiliser les collaborateurs et les inciter à proposer des sujets crédibles pour la collaboration. Informer les collaborateurs de la criticité des ressources permettra aussi d'imposer des sanctions radicales qui seront plus aisément acceptées. Pour exprimer cette déclaration, le langage I-OrBAC se retrouve, encore une fois, limité de par sa nature localisée. Nous allons donc introduire de nouveaux prédicats permettant de déclarer les entités engagées – aussi bien actives (rôles et sujets) que passives (vues, activités, objets et actions) – par les partenaires dans le cadre de la VO. Ainsi, afin de déclarer les sujets et rôles, nous introduisons le prédicat *Charge*(), alors que pour déclarer les vues et les objets, nous avons recours au prédicat *Fournit*() et enfin pour déclarer les activités et les actions, nous introduisons le prédicat *Réalise*(). Syntaxiquement, ces prédicats se présenteront comme suit :

$$Charge(VO_i, Org_{déclare}, r, Org_{sujet}) \quad (21)$$

$$Fournit(VO_i, Org_{origine}, v, o, l_v) \quad (22)$$

$$Réalise(VO_i, Org_{origine}, ay, ac, l_{ay}) \quad (23)$$

Sémantiquement, le prédicat (21) stipule que l'organisation $Org_{déclare}$, qui déclare le prédicat, charge l'organisation Org_{sujet}, habilité au rôle *r*, d'effectuer des tâches au sein de la VO_i. Comme nous le verrons par la suite, ces prédicats seront utilisés par toutes les organisations de la VO_i, non uniquement par les organisations détentrices des ressources, afin de procéder à la résolution des conflits. Le prédicat *Charge*() n'intègre pas de déclaration de niveau de crédibilité car les organisations en négociation se font confiance. Le prédicat (22), quant à lui, précise que l'organisation $Org_{origine}$ fournit l'objet *o*, répertorié dans la vue *v* et caractérisé par le niveau d'intégrité l_v, afin d'être utilisé dans la VO_i. Finalement, le prédicat (23) stipule que l'organisation $Org_{origine}$ compte réaliser l'action *ac*, faisant partie de l'activité *ay* et caractérisée par le niveau de criticité l_{ay}, dans le cadre de la VO_i.

Les niveaux de criticité déclarés dans ces prédicats seront conformes à des échelles établies conjointement par les organisations. Quelques soient les échelles utilisées localement par les organisations, les échelles utilisées lors de la déclaration devront être simples et génériques, afin de faciliter les déclarations ainsi que la deuxième étape de résolution des conflits. Certes la déclaration des niveaux d'intégrité présente deux limitations évidentes : d'une part, cela peut représenter une divulgation d'informations confidentielles propres à l'organisation, d'autre part, les organisations peuvent tendre toutes à exagérer les niveaux de criticité de leurs ressources afin de négocier de lourdes pénalités. La seconde limitation se posera surtout lorsqu'une organisation fournit le sujet et l'activité en même temps tandis que l'autre fournit l'objet, cette dernière aura tendance à exagérer le niveau des vues qu'elle engage. Pour limiter cela, il s'agira de comparer les niveaux de criticité des vues et des activités, en effet, il est rare d'effectuer une action de très faible niveau d'intégrité sur un objet de très haut niveau d'intégrité, hormis la consultation.

En revanche cette approche de description détaillée permettra aux organisations de mieux préciser leurs besoins et attentes, en affichant les contraintes en présence desquelles devra se dérouler la coopération. Il en résultera donc une meilleure sensibilisation des partenaires, ce qui favorisera le bon déroulement des activités de collaboration. Pour limiter les exagérations des niveaux d'intégrité des ressources, chaque organisation sera aussi appelée à exprimer des règles concernant les ressources engagées par les partenaires ainsi que leurs niveaux d'intégrité. Ces règles seront anticipées et permettront d'effectuer les confrontations nécessaires à la négociation des termes propres aux ressources engagées.

V.3.2.2.4 Etape (2') : Deuxième résolution des conflits

Cette étape de résolution de conflits permettra aux organisations de confronter les niveaux de criticité déclarés pour les différentes ressources engagées. Pour cela, chaque organisation devra décrire aussi bien les ressources qu'elle compte engager, en déclarant leurs niveaux d'intégrité, ainsi que celles qu'elle compte manipuler, en prévoyant leurs niveaux d'intégrité, tout en se basant sur le contexte de la collaboration et la nature de la tâche. La confrontation des niveaux réels déclarés et ceux anticipés permettra de détecter les éventuelles exagérations, forçant ainsi les organisations à revoir leurs déclarations ou éventuellement à chercher de nouveaux partenaires. L'étape de la résolution de conflits portant sur les vues et objets sera régie grâce au système d'inférence suivant (Tab. 6) :

Init	(j,p)	*avec j un compteur entier, permettant de mémoriser la valeur de la tentative de négociation et p le nombre maximale de négociation tolérées.*
Succès	$\frac{Fourniture(VO,v),j,p}{Utilise(VO,v,o,l_v)}$	*si* $\exists\, j \in \mathbb{N},\ j < p\ /\ l_v = l_{v_{virt}} \mp 1$
Suit	$\frac{Fourniture(VO,v),j,p}{Fourniture(VO,v),j+1,p}$	*si la règle Succès n'est pas valide*
Echec	$\frac{Fourniture(VO,v),p,p}{Echec}$	*si nulle autre règle ne s'applique*

Tab. 6. Système d'inférence régissant l'étape 2 de la négociation : vues engagées

Cette étape de résolution de conflits démarre par l'initialisation d'un compteur destiné à calculer le nombre de renégociation à la suite d'un malentendu concernant les niveaux d'intégrité déclarés dans les prédicats. Ces renégociations ne devant pas se répéter indéfiniment, un paramètre *p* indique le nombre maximal de tentatives.

Puis, nous récupérons les deux prédicats relatif à une même ressource et fournis par les partenaires. Ainsi, nous considérons, comme exemple, les deux formules suivantes :

$$Fournit(VO_i, Org_{orig}, v, o, l_v) \quad et \quad Fournit(VO_i, Org_{orig}, v_{virt}, o_{virt}, l_{v_{virt}})$$

La première est exprimée par l'organisation détentrice de la vue, dite *organisation d'origine* de la ressource, qui stipule que sa ressource est d'un niveau l_v. La seconde formule, en revanche, est exprimée par l'organisation qui manipulera la vue et qui s'attend à ce que celle-ci soit d'un certain niveau $l_{v_{virt}}$. Lors de la confrontation, tout l'intérêt sera porté sur la comparaison des niveaux l_v et $l_{v_{virt}}$; les autres paramètres seront pris depuis la première formule, exprimée par l'organisation d'origine. Ainsi, si $l_v = l_{v_{virt}} \mp 1$, alors il s'agira d'une négociation réussie (i.e état Succès) qui impliquera l'adoption des paramètres de la première formule et établira de ce fait une nouvelle règle de la PS de la VO, puisque l'issue d'une confrontation réussie génère une règle de type *Utilise*() dans ladite PS. L'écriture *Fourniture*(VO, *v*) du système d'inférence permet d'abréger l'écriture suivante :

$$Fourniture(VO,v) = Fournit(VO_i, Org_{orig}, v, o, l_v) \wedge Fournit(VO_i, Org_{orig}, v_{virt}, o_{virt}, l_{v_{virt}})$$

En revanche, si les niveaux avancés par les partenaires sont largement différents, *p* tentatives leur seront possible pour tenter de se mettre d'accord sur un niveau d'intégrité qui soit le plus proche de leurs attentes (i.e. état Suit).

Au bout de *p* tentatives échouées (i.e. état Echec), la vue *v* n'est pas intégrée à la VO, à ce moment-là, certaines issues sont possibles : proposition d'une autre vue ou éventuellement la rupture de la collaboration.

Le même raisonnement est adopté aussi pour la négociation des activités proposées dans le cadre de la collaboration. Par conséquent, la négociation démarre par l'initialisation d'un compteur. Puis seront recueillis les prédicats *Réalise*() déclarés par les partenaires. Si les niveaux d'intégrité déclarés sont relativement proches, autrement dit, $l_{ay} = l_{ay_{virt}} \mp 1$, alors l'issue de la négociation permettra de dériver le prédicat *Considère*() (Tab. 7) qui fera partie de la PS de la VO (i.e. état Succès). L'écriture *Réalisation*(VO, *ay*) utilisée dans le système d'inférence permet d'abréger la formule :

$$Réalisation(VO, ay) = Réalise\left(VO_i, Org_{orig}, ay, ac, l_{ay}\right) \wedge Réalise\left(VO_i, Org_{orig}, ay_{virt}, ac_{virt}, l_{ay_{virt}}\right)$$

Eventuellement si les niveaux déclarés ne sont pas très proche, alors les organisations auront au maximum *p* tentatives pour s'entendre sur des niveaux d'intégrité reflétant la réalité de l'activité à réaliser (i.e. état Suit). Si au bout de *p* tentatives infructueuses, soit de nouvelles activités devront être proposées soit la collaboration peut éventuellement être dissoute (i.e. état Echec).

Init	(k, p)	*avec k un compteur entier, permettant de mémoriser la valeur de la tentative de négociation et p le nombre maximale de négociation tolérées.*
Succès	$\frac{Réalisation(VO, ay), k, p}{Considère(VO, ay, ac, l_{ay})}$	*si* $\exists\, k \in \mathbb{N},\ k < p\ /\ l_{ay} = l_{ay_{virt}} \mp 1$
Suit	$\frac{Réalisation(VO, ay), k, p}{Réalisation(VO, ay), k+1, p}$	*si la règle Succès n'est pas valide*
Echec	$\frac{Réalisation(VO, ay), p, p}{Echec}$	*si nulle autre règle ne s'applique*

Tab. 7. Système d'inférence régissant l'étape 2 de la négociation : activités engagées

Suite aux négociations réussies entre les partenaires, les règles *Utilise*() et *Considère*() de la PS de la VO seront générées automatiquement.

Arrivé à ce stade, il ne restera plus à négocier que l'entité qui se chargera de la réalisation de l'activité, autrement dit, de l'organisation qui se verra attribué le rôle pour exécuter la tâche de la collaboration. Nous adopterons le même raisonnement que celui utilisé

lors des deux précédentes résolutions de conflits. Ainsi la négociation démarrera par l'initialisation d'un compteur. Puis seront recueillis les prédicats *Charge*() déclarés par les partenaires. Vu que ces prédicats ne contiennent pas de niveaux de crédibilité, la résolution de conflits consistera juste à vérifier si les partenaires s'accordent à accorder la responsabilité à une seule organisation. Si c'est le cas, alors le système d'inférence générera le prédicat *Habilite*() de la PS de VO (i.e. état Succès) (Tab. 8). L'écriture *Affectation*(VO, *r*) utilisée dans le système d'inférence permet d'abréger la formule :

$$Affectation(VO, r) = Charge(VO_i, Org_{déclare}, r, Org_{sujet}) \wedge Charge(VO_i, Org_{déclare}, r, Org_{sujet'})$$

Eventuellement si les organisations n'affectent pas une même organisation dans le rôle, alors ils auront au plus p tentatives pour parvenir à un accord (i.e. état Suit). Si au bout de p tentatives, le désaccord persiste toujours, la collaboration peut éventuellement être dissoute (i.e. état Echec).

Init	(m, p)	*avec m un compteur entier, permettant de mémoriser la valeur de la tentative de négociation et p le nombre maximale de négociation tolérées.*
Succès	$\frac{Affectation(VO, r), m, p}{Habilite(VO, r, org_{sujet})}$	*si* $\exists\, k \in \mathbb{N},\ k < p\ /\ org_{sujet} = org_{sujet'}$
Suit	$\frac{Affectation(VO, r), m, p}{Affectation(VO, r), m+1, p}$	*si la règle Succès n'est pas valide*
Echec	$\frac{Affectation(VO, r), p, p}{Echec}$	*si nulle autre règle ne s'applique*

Tab. 8. Système d'inférence régissant l'étape 2 de la négociation : l'organisation chargée de réaliser la tâche

V.3.2.2.5 Etape (3) : Accord sur les clauses et les conditions

Une fois que les étapes (2) et (2') sont conclues avec succès, il s'agira ensuite de négocier les clauses et conditions du déroulement des activités de la collaboration, autrement dit, les modes d'accès propres à chaque tâche. A ce stade, chaque partenaire de la collaboration entrevoit, selon sa perception, le déroulement des activités supposées aboutir à la réalisation des objectifs. Ainsi, chaque partenaire devra exprimer les règles de sécurité régissant les modes d'accès de la PS de la VO comme s'il conçoit sa propre PS locale, en considérant les ressources externes comme des ressources internes et en utilisant cette fois-ci les prédicats *Permission*(), *Interdiction*(), *Obligation*() et *Recommandation*() définis dans I-OrBAC. Les arguments des prédicats *Permission*(), *Interdiction*() et *Obligation*() et

Recommandation() seront ceux de la PS de la VO, aboutissements des précédentes confrontations.

V.3.2.2.6 Etape (3') : Troisième étape de résolution des conflits

Les règles de sécurité exprimées par les différents partenaires seront confrontées afin de vérifier que les perceptions des différents partenaires s'accordent. A ce moment précis, les risques d'incohérence sont grands puisque une organisation peut permettre une certaine tâche, tandis que l'autre peut l'interdire. Par conséquent, il s'agira de détecter les conflits et de tenter de les résoudre afin de garantir une PS cohérente pour la VO. Pour ce faire, les prédicats relatifs à des mêmes arguments (*VO, r, v, ay, c,* l_c) seront regroupés puis confrontés pour enfin ne retenir qu'un seul mode d'accès pour les 6-uplets. Les différentes combinaisons possibles de modes d'accès possible pour un 6-uplet sont décrits dans le tableau suivant :

Règle exprimée par Org_i	Règle exprimée par Org_j	Règle retenue dans la PS de la VO
Permission()	*Permission*()	*Permission*()
Interdiction()	*Interdiction*()	*Interdiction*()
Obligation()	*Interdiction*()	*Interdiction*()
Recommandation()	*Recommandation*()	*Recommandation*()
Permission()	*Recommandation*()	*Recommandation*()
Permission()	*Obligation()*	*Obligation()*
Permission()	*Interdiction*()	*Interdiction*()
Obligation()	*Recommandation*()	*Obligation()*
Interdiction()	*Recommandation*()	*Interdiction*()
Interdiction()	*Obligation()*	Négociation imposée

Tab. 9. Combinaison des modes d'accès pour un 6-uplet (*VO, r, v, ay, c,* l_c).

Lorsque les règles de sécurité exprimées par les partenaires, pour un même 6-uplet, sont les mêmes, c'est-à-dire que les partenaires prévoient le même mode d'accès pour le 6-uplet, alors celui-ci est retenu (i.e. les lignes 1, 2, 3 et 4 du tableau). En revanche, lorsqu'une organisation accorde une permission pour un 6-uplet, tandis que l'autre accorde n'importe quel autre mode, c'est ce dernier qui sera retenu (i.e. les lignes 5, 6, 7) car pour préserver l'intégrité des ressources la priorité est accordée à l'interdiction, de plus l'obligation et la recommandation sont des permissions plus fortes [33], elles l'emportent donc sur les permissions. La ligne 8 décrit le cas où l'une des organisations accorde une

obligation alors que l'autre n'accorde qu'une recommandation, dans ce cas-là, l'obligation est retenue puis sémantiquement, l'obligation est plus forte que la recommandation [Article Nada]. Les lignes 9 et 10 décrivent respectivement les cas où une organisation accorde une interdiction tandis que l'autre accorde une recommandation ou une obligation : pour le premier cas Recommandation()/Interdiction(), l'interdiction est retenue par souci de préservation de l'intégrité, en revanche lorsqu'une organisation envisage l'obligation de réaliser une tâche alors que l'autre l'interdit, à ce moment-là une négociation s'impose. Les organisations seront appelées à négocier pour arriver au mode d'accès conviendra aux deux organisations.

V.3.2.2.7 Etape (4) : Finalisation des PS

A l'issue d'une ultime étape de négociation (3') positive, peut enfin commencer le processus de finalisation des PS locales des partenaires en vue de pouvoir répondre concrètement aux requêtes d'accès des partenaires. A ce stade, la PS de la VO répond aux spécifications de tous les partenaires et elle est achevée, dans la mesure où toutes les règles *Habilite*(), *Utilise*(), *Considère*() et *Permission*() (respectivement *Interdiction*(), *Obligation*() et *Recommandation*()) ont été énoncées. Ainsi, il sera question pour les organisations de se conformer à ce consensus pour mettre à jour leurs politiques locales, lesquelles seront consultés pour accorder les accès aux utilisateurs externes. Les règles de type *Définit*() et *Est_Permis*() (respectivement, *Est_Obligé*(), *Est_Interdit*() et *Est_Recommandé*()) seront dérivées au fur et à mesure que les requêtes émaneront des utilisateurs.

Pour expliquer le fonctionnement de notre modèle, nous proposons ci-après un exemple illustratif afin de décrire plus en détails, les différentes phases opératoires de notre modèle.

V.3.2.3 Exemple de collaboration :

Nous reprenons l'exemple décrivant le cas du patient « *Tom* » – répertorié dans la vue « *Patients_Ablation* » (*Pat_Ab* de niveau $l_{Pat\_Ab} = 4$) – devant subir une « *Ablation* » – faisant partie de l'activité « *Opérations_Critiques* » (*Op_Cr* de niveau $l_{Op\_Cr} = 4$) – dans un contexte « *Hautement_Risqué* » (*H_R* de niveau $l_{H\_R} = 4$) au sein de l'hôpital « *H* ». Suite à l'application du système d'inférence, décrivant la proactivité d'I-OrBAC (cf. Tab. 3), au tripet (l_{Pat_Ab}, l_{Op_Cr}, l_{H_R}), nous considérons que tous les sujets de « *H* » qualifiés dans les différents rôles adéquats – i.e. le sous-ensemble *SR* constitué des rôles « *chirurgien spécialisé en ablation* » (*Chir_Ab*), « *chirurgien esthéticien* » (*Chir_Esth*) et « *chirurgien* » (*Chir*) – ne sont pas libre pour la réalisation de ladite tâche. Dans ce cas, l'hôpital *H* doit collaborer avec un autre hôpital afin de pouvoir réaliser l'opération dans les délais impartis.

Rappelons que la PS de l'hôpital *H* stipule que les seuils minimums de crédibilité imposés aux rôles de *SR*, pour la réalisation de la tâche (*Pat_Ab*, *Op_Cr*, *H_R*), sont $l_{SLimit(Chir\_Ab)} = 2$, $l_{SLimit(Chir\_Esth)} = 3$ et $l_{SLimit(Chir)} = 4$.

Etape (1) et (1') : Invitation des partenaires et 1ère résolution des conflits

Ainsi, *H* devra sélectionner un partenaire satisfaisant l'une des trois contraintes précitées. Nous considérons le tableau suivant (Tab. 10) détaillant les vecteurs des habilitations de certains hôpitaux partenaires de *H* :

Rôles / Sujets	Ch. spéc. Ablation (*Chir_Ab*)	Ch. esthéticien (*Chir_Esth*)	Chirurgien (*Chir*)	Anesthésiste	Rééducateur
Hôpital H_1	**3 (1)**	**4 (3)**	2	2	-
Hôpital H_2	1	-	2	-	3
Hôpital H_3	**2 (2)**	**3 (4)**	3	3	-
Hôpital H_4	1	2	**4 (5)**	3	-

Tab. 10. Habilitations des hôpitaux partenaires de *H*.

L'hôpital *H* proposera des collaborations aux autres hôpitaux, selon l'ordre de priorité décrit entre parenthèses dans le tableau ci-avant. *H* commencera par inviter H_1, dans le rôle « *Chir_Ab* ». Il lui adresse donc une invitation décrite par le prédicat :

$$Invite\left(H, H_1, H\_R, l_{H\_R} = 4\right)$$

A cette invitation, l'hôpital H_1 répond par la confirmation suivante :

$$Confirme\left(H_1, H, Chir\_occupés, l_{Chir\_occupés} = 2\right)$$

La confrontation des deux précédentes règles indique la collaboration avec H_1 n'est pas envisageable : d'une part car les chirurgiens spécialisés en ablations de H_1 sont occupés et aussi car le niveau d'intégrité du contexte soumis par H_1 est inférieur à 3. Par conséquent, *H* se tourne vers H_3 et lui adresse l'invitation suivante :

$$Invite\left(H, H_3, H\_R, l_{H\_R} = 4\right).$$

L'hôpital H_3 répond par la confirmation :

$$Confirme(H_3, H, Hauts\_Risques, l_{Hauts\_Risques} = 3)$$

Cette fois-ci, la confrontation donne un résultat positif puisque les contextes « *H_R* » et « *Hauts_Risques* » sont équivalents et que leurs niveaux sont sensiblement proches puisque $l_{H\_R} = l_{Hauts\_Risques} + 1$. Ainsi la collaboration est entamée et la $VO_{H–H3}$ initiée grâce au prédicat :

$$Collabore(H - H_3, H, H_3, H\_R, l_c = 4)$$

Etape (2) et (2') : Déclaration des ressources engagées et 2ème résolution des conflits

Une fois la collaboration conclue, *H* et H_3 devront déclarer les ressources qu'elles comptent engager ainsi que celles qu'elles comptent manipuler. Ces déclarations devront afficher les niveaux d'intégrité de ces ressources afin de pouvoir renseigner les partenaires sur la criticité des biens et aussi pour procéder à la 2ème résolution de conflits qui permettra éventuellement de déceler des déclarations exagérées. Le tableau ci-après (Tab. 11) regroupe les déclarations émises par *H* et H_3.

Déclarations de H	*Déclarations de H_3*
$Fournit(H - H_3, H, Pat\_Ab, Tom, l_{Pat\_Ab} = 4)$	$Fournit(H - H_3, H, v_{virt}, o_{virt}, l_{v_{virt}} = 3)$
$Réalise(H - H_3, H_3, Op\_Cr, Ab, l_{Op\_Cr} = 4)$	$Réalise(H - H_3, H_3, Op, Ab, l_{Op} = 2)$
$Charge(H - H_3, H, Chir\_Ab, H_3)$	$Charge(H - H_3, H_3, Ch\_Ab, H_3)$

Tab. 11. Déclarations des ressources engagées par les partenaires.

Les prédicats *Fournit*(), *Réalise*() et *Charge*() établis dans (Tab. 11) seront ensuite confrontés, deux à deux, grâce aux systèmes d'inférence décrits dans (Tab. 6), (Tab. 7) et (Tab. 8). La confrontation des prédicats *Fournit*() sera couronnée de succès puisque $l_{Pat\_Ab} = l_{v_{virt}} + 1$. Cela permettra de générer le prédicat *Utilise*(*H–H3, Pat_Ab, Tom,* $l_{Pat\_Ab} = 4$) de la $VO_{H–H3}$ qui ajoutera une vue et un objet à cette VO.

En revanche, la confrontation des prédicats *Réalise*() ne donnera pas directement lieu à la génération du prédicat *Considère*() puisque $l_{Op\_Cr} \neq l_{Op} \mp 1$. Par conséquent, *H* et H_3 auront au plus *p* tentatives de renégociation pour se mettre d'accord sur le niveau de l'activité. Pour aboutir à un état de succès, il faudra que *H* réduise le niveau de criticité de l'activité *Op_Cr* d'au moins 1 ou que H_3 augmente de 1 le niveau de l'activité *Op*. Nous considérons que la seconde supposition s'est réalisée, le système d'inférence (Tab. 7) génère donc le prédicat *Considère*(*H–H3, Op_Cr, Ab,* $l_{Op\_Cr} = 4$).

Pour ce qui est de la confrontation des prédicats *Charge*(), elle sera couronnée de succès puisque *H* et H_3 ont tous deux déclaré que H_3 sera habilitée dans le *Chir_Ab*. Par conséquent l'état Succès est atteint et permettra ainsi de générer le prédicat *Habilite*(*H–H3, Chir _Ab, H3*) de la $VO_{H–H3}$ qui ajoutera un rôle et un sujet à cette VO.

Suite aux étapes (2) et (2'), les biens actifs et passifs de $VO_{H–H3}$ sont tous déterminés comme le montre le tableau suivant :

Prédicats décrivant les ressources de $VO_{H–H3}$
Utilise(*H–H3, Pat_Ab, Tom,* $l_{Pat\_Ab} = 4$)
Considère(*H–H3, Op_Cr, Ab,* $l_{Op\_Cr} = 4$)
Habilite(*H–H3, Chir_Ab, H3*)

Tab. 12. Ressources de l'organisation virtuelle $VO_{H–H3}$

Sur la base de ces ressources seront ensuite énoncés les prédicats régissant les modes d'accès à ces biens.

Etape (3) et (3') : Accord sur les clauses et les conditions et 3ème résolution de conflits

Une fois les ressources de $VO_{H–H3}$ négociées, il est question par la suite de se mettre d'accord sur les conditions de leur utilisation. Ces conditions ne sont autres que les modes d'accès qui accorderont ou refuserons les accès aux sujets requérant l'accès à ces ressources. A cette étape, *H* et H_3 devront spécifiés les règles de sécurité de type *Permission*(), *Interdiction*(), *Obligation*() et *Recommandation*() afin d'achever la PS de $VO_{H–H3}$. Afin de simplifier, nous considérons que *H* et H_3 n'éditent qu'une règle de type *Permission*() pour autoriser H_3 à réaliser la tâche (*Pat_Ab*, *Op_Cr*, *H_R*) comme le montre le tableau suivant (Tab. 13) :

Déclarations de *H*
$Permission(H-H3, Chir\_Ab, Pat\_Ab, Op\_Cr, H\_R, l_{H\_R} = 4)$
Déclaration de H_3
$Permission(H-H3, Chir\_Ab, Pat\_Ab, Op\_Cr, Hauts\_Risques, l_{Hauts\_Risques} = 3)$

Tab. 13. Déclarations des modes d'accès par les partenaires

En se référant au tableau (Tab. 9) qui précise l'issue des confrontations entre les différents modes d'accès émis par les partenaires, nous concluons qu'une règle de type

Permission() sera générée au sein de la PS de VO_{H-H3}. Ainsi, la PS de VO_{H-H3} comptera la règle suivante :

$$Permission(H-H3, Chir\_Ab, Pat\_Ab, Op\_Cr, H\_R, l_{H\_R} = 4)$$

Pour résumer les règles de la PS de VO_{H-H3}, nous dressons le tableau (Tab. 14) :

Règles de sécurité de VO_{H-H3}
$Collabore(H - H_3, H, H_3, H\_R, l_c = 4)$
$Permission(H-H3, Chir\_Ab, Pat\_Ab, Op\_Cr, H\_R, l_{H\_R} = 4)$
$Utilise(H–H3, Pat\_Ab, Tom, lPat\_Ab=4)$
$Considère(H-H3, Op_{Cr}, Ab, l_{Op\_Cr} = 4)$
$Habilite(H-H3, Chir\_Ab, H_3)$

Tab. 14. PS de l'organisation virtuelle VO_{H-H3}.

Etape (4) : Finalisation des PS locales des partenaires

Suite à l'aboutissement à un accord entre *H* et H_3, matérialisé par la PS de VO_{H-H3} qui est le résultat de négociations, il s'agit à ce moment précis de mettre à jour les PS locales de *H* et H_3 afin qu'elles puissent tenir compte des nouveaux éléments propres à la collaboration. Pour cela, les partenaires n'auront qu'à adapter les règles du tableau (Tab. 14) à leurs situations en intégrant les éléments à leurs PS, les éléments qui leurs sont étrangers. Pour finir, aux PS locales de *H* et H_3 seront ajoutées les règles suivantes (Tab. 15) :

Ajustements à la PS de *H*
$Collabore(H - H_3, H, H_3, H\_R, l_{H\_R} = 4)$
$Permission(H, Chir\_Ab, Pat\_Ab, Op\_Cr, H\_R, l_{H\_R} = 4)$
$Habilite(H, Chir\_Ab, H_3, l_{(H_3)Ch\_Ab} = 2)$
Ajustements à la PS de H_3
$Collabore(H_3 - H, H_3, H, Hauts\_Risques, l_{Hauts\_Risques} = 3)$
$Permission(H_3, Chir\_Ab, H, Op, Hauts\_risques, l_{Hauts\_risques} = 4)$
$Utilise(H_3, H, Tom, l_{(Pat\_Ab)H} = 4)$

Tab. 15. Ajustements des PS locales des partenaires

Les règles de sécurité des PS de *H* et H_3 qui seront utilisées pour répondre concrètement à la collaboration sont les suivantes (Tab. 16) :

Règles de sécurité de la PS de *H* qui régissent la collaboration
$Collabore(H - H_3, H, H_3, H\_R, l_{H\_R} = 4)$ $\wedge Permission(H, Chir\_Ab, Pat\_Ab, Op\_Cr, H\_R, l_{H\_R} = 4)$ $\wedge Utilise(H\text{–}H_3, Pat\_Ab, Tom, l_{\text{Pat\_Ab}} = 4)$ $\wedge Considère(H\text{–}H_3, Op_{Cr}, Ab, l_{Op\_Cr} = 4)$ $\wedge Habilite(H, Chir\_Ab, H_3, l_{(H_3)Ch\_Ab} = 2)$ $\wedge Définit(H, H_3, Tom, Ab, l_{H\_R} = 4)$ $\Rightarrow Est\_Permis(H, Tom, Ab)$
Règles de sécurité de la PS de H_3 qui régissent la collaboration
$Collabore(H_3 - H, H_3, H, Hauts\_Risques, l_{Hauts\_Risques} = 3)$ $\wedge Permission(H, Chir\_Ab, H, Op, Hauts\_risques, l_{Hauts\_risques} = 4)$ $\wedge Utilise(H_3, H, Tom, l_{(Pat\_Ab)H} = 4)$ $\wedge Considère(H_3, Op, Ab, l_{Op} = 3)$ $\wedge Habilite(H_3, Ch\_Ab, Alice, l_{(Alice)Ch\_Ab} = 3)$ $\wedge Définit(H_3, Alice, Tom, Ab, l_{Hauts\_Risques} = 3)$ $\Rightarrow Est\_Permis(H_3, Alice, Ab)$

Tab. 16. Règles de sécurité des PS de *H* et H_3 traitant la collaboration.

Arrivées à ce point, les PS locales des organisations ont été mises à jour afin de tenir compte des accès externes destinés à favoriser la réalisation des tâches dans l'objectif de répondre aux intérêts des différents partenaires. Pour conclure, DI-OrBAC offre un framework regroupant des moyens de sélection des partenaires, de négociation des contrats électroniques et d'adaptation des résultats de la négociation aux PS locales des partenaires.

V.4. Conclusion du chapitre

Dans ce chapitre, nous avons présenté l'extension DI-OrBAC qui étend I-OrBAC aux environnements distribués, afin de tenir compte conjointement des besoins d'intégrité et de collaborations sécurisées. Pour se faire, nous avons commencé par rappeler l'importance des collaborations dans la réalisation de nouveaux objectifs ainsi que les dan-

gers qu'elles pouvaient engendrer. Nous avons introduit ensuite les deux concepts clés qui seront combinés à I-OrBAC afin de concevoir des PS cohérentes pour les collaborations, à savoir les concepts de VO et de contrat électronique.

Suite à cela, nous avons détaillé les composantes de notre modèle DI-OrBAC qui vise à instaurer des collaborations, entre des organisations pertinemment sélectionnées, régies par des clauses négociées et non imposées. Ainsi, nous avons présenté le processus de découverte et de sélection des partenaires adopté, qui s'inspire des protocoles de routage et des modèles de gestion de la confiance. Afin de mener à bien cette sélection, nous avons proposé un pseudo-protocole permettant d'interroger et de recueillir les jugements des partenaires sur les organisations potentiellement crédibles. Puis nous avons exposé les étapes de la négociation des contrats électroniques réalisée grâce à un langage enrichi d'I-OrBAC, qui permet non seulement, la négociation des clauses mais aussi l'établissement de la PS de la VO et enfin la finalisation des PS des différents collaborateurs engagés. Nous avons aussi veillé à automatiser les négociations de contrats en développant des systèmes d'inférence chargés de statuer sur leurs issues.

Conclusion générale

Comme leur nom l'indique, les infrastructures critiques (IC) sont des organisations tellement vitales à la stabilité et au développement des nations que leurs dysfonctionnements sont intolérables. Qu'importe l'origine, délibérée ou accidentelle, de ces indisponibilités ; des parades et des mécanismes adéquats doivent nécessairement être déployés afin d'en maîtriser et d'en réduire les pertes et les impacts. Pour élaborer ces contre-mesures, il est impératif de tenir compte des propriétés et exigences des IC et de leurs infrastructures d'informations critiques (IIC). Durant cette thèse, nous nous sommes focalisés sur leurs besoins en intégrité et en collaborations sécurisées. Ces exigences sont cruciales, d'une part, puisque les IC manipulent des informations devant nécessairement être correctes et génèrent, à l'issue de processus internes, des résultats devant indiscutablement être fiables. D'autre part, en présence de l'actuel contexte de mondialisation et d'ouverture, il est inconcevable que les IC et IIC puissent évoluer sans collaborer avec des acteurs extérieurs ; ces collaborations ne sont pas sans risques puisque leurs ressources peuvent faire l'objet de sabotage et de corruption dus à une compétitivité déloyale.

Pour répondre à ces besoins, nous avons proposé deux extensions d'OrBAC : l'une s'appliquant localement au sein d'une organisation (Integrity-OrBAC, I-OrBAC), tandis que l'autre est destinée à aux environnements collaboratifs (Distributed Integrity-OrBAC, DI-OrBAC). I-OrBAC est un modèle proactif visant à tenir compte de contraintes liées à l'intégrité dans la prise de décision de contrôle d'accès localement au sein d'une organisation. Pour ce faire, notre modèle se base sur le principe de priorisation des biens, principe clé des programmes de protection des infrastructures critiques (PIC), qui vise à adapter les mesures de protection selon la sensibilité des biens et des impacts encourus en cas d'incidents. Nous avons aussi montré l'applicabilité de notre modèle à travers des exemples issus de différents secteurs critiques et aussi à travers une implémentation inspirée des réseaux d'énergie électrique. DI-OrBAC, pour sa part, est une extension d'I-OrBAC ayant pour objectif la satisfaction des exigences en matière d'intégrité dans un contexte distribué et collaboratif. A cette fin, DI-OrBAC enrichit son prédécesseur par l'établissement de contrats dont les clauses sont négociées en temps réel grâce à une syntaxe enrichie d'I-OrBAC, ce qui permet de sensibiliser les partenaires par rapport à la criticité des biens engagés dans la collaboration.

Logique adoptée et bilan des contributions

Ci-après, nous rappelons la logique adoptée au cours de ces travaux de recherche et énumérons les principales contributions :

- **Description détaillée des notions d'IC, d'IIC et de PIC** : Nous avons étudié et exposé deux référentiels de PIC, l'un national et l'autre international, pour en déceler les facteurs clés de la protection. Cela nous a permis d'apprécier l'importance des démarches de gestion des risques et du principe de priorisation des biens dans les efforts de protection. Aussi, avons-nous œuvré à établir un état de l'art exhaustif des propriétés et besoins des IC et IIC afin de les considérer durant la conception des solutions que nous proposons.
- **Etat de l'art des modèles de contrôle d'accès classiques, d'intégrité et de collaboration** : Nous avons élargi le spectre des modèles de contrôle d'accès étudiés afin de ne pas nous limiter aux mécanismes proposés par les modèles d'intégrité existants. Ainsi, suite à une analyse critique des forces et faiblesses des modèles étudiés, nous avons décidé d'enrichir OrBAC par des mécanismes en vue de garantir l'intégrité des ressources des IIC. Le choix d'OrBAC est justifié par sa richesse et par la multitude d'exigences des IIC qu'il satisfait.
- **Proposition d'un modèle de contrôle d'accès tenant compte de contraintes liées à l'intégrité dans un contexte localisé** : Le modèle de contrôle d'accès que nous proposons (I-OrBAC) tient compte de contraintes tirées de la réalité des IIC – contraintes de *criticité* et de *crédibilité* – pour statuer sur les requêtes d'accès. Il a été pensé pour utiliser, en les adaptant, les résultats issus de l'application de méthodes d'analyse de risques afin d'exprimer des PS reflétant les besoins des ressources passives et appréciant, à leur juste valeur, les habilitations des agents.
- **Modélisation en niveaux d'intégrité** : Conformément aux programmes de PIC, nous avons veillé à intégrer la priorisation des biens sensibles à notre modélisation. Outre les contextes, les niveaux d'intégrité permettront aussi de restreindre les accès pour s'assurer que seuls des utilisateurs chevronnés accéderont aux biens sensibles, garantissant ainsi une meilleure protection aux ressources. Aussi, pour pallier la limitation du statisme des niveaux d'intégrité, nous avons proposé un moyen permettant la dégradation et le recouvrement les niveaux d'intégrité des sujets, en accord avec leur rendement et leur comportement.
- **Les niveaux d'intégrité au service de la flexibilité** : Soucieux de répondre au besoin de flexibilité lors de l'attribution des privilèges d'accès, nous avons proposé un moyen qui, tenant compte des spécificités du métier de l'organisation,

permet d'établir une hiérarchie de rôles pour réaliser une tâche donnée. Les rôles de la hiérarchie seront soumis à des contraintes différentes (seuils différents) pour réaliser ladite tâche.

- **Un modèle proactif** : Dans le contexte des IIC, un modèle restreint à statuer sur les requêtes d'accès serait quelque peu limitatif. Pour cette raison, I-OrBAC se veut proactif vu qu'il cherchera à déterminer le sujet le plus adéquat parmi les rôles retenus pour la réalisation d'une tâche, sans attendre que les sujets n'en fassent la requête. L'algorithme permettant cette pro-activité est décrit par un système d'inférence.
- **Une implémentation d'I-OrBAC** : Nous avons proposé une implémentation de notre modèle dans le cadre d'une étude de cas tiré du projet européen FP7 CRUTIAL relatif aux réseaux de transport et de distribution d'énergie électrique. Nous avons donc présenté nos choix technologiques ainsi que les étapes de la prise de décision dans une version ajustée du standard XACML 2.0. Ces étapes concernent le cas du traitement normal des requêtes d'accès et le cas des requêtes proactives générées par le système.
- **Proposition d'une extension d'I-OrBAC pour les environnements distribués** : Pour pallier les problèmes issus des collaborations, DI-OrBAC enrichit I-OrBAC par les concepts d'organisation virtuelle et contrat électronique. DI-OrBAC s'inspire des techniques de gestion de la confiance pour permettre aux organisations de sélectionner leurs partenaires dans un milieu distribué. Pour réussir cette sélection, DI-OrBAC introduit un pseudo-protocole, adapté à I-OrBAC, permettant d'interroger et de recueillir les jugements des partenaires sur les organisations potentiellement crédibles. Les jugements collectés permettront par la suite de calculer localement des niveaux de crédibilité relatifs aux organisations et à établir la carte des partenaires. Une fois les collaborateurs choisis, DI-OrBAC fournit les moyens dynamiques de négociation des contrats, en utilisant un langage développé sur la base de celui d'I-OrBAC. Du point de vue du contrôle d'accès, DI-OrBAC aborde trois étapes de la négociation : le contexte de la collaboration, les ressources engagées et les conditions de leur utilisation. Chaque étape de la négociation est soumise à une confrontation des conditions exprimées par les partenaires dont l'aboutissement est décrit par des systèmes d'inférence.

Perspectives :

Avant de clôturer ce mémoire, il est important de renseigner sur les éventuelles pistes de développement envisageables à nos travaux de recherches :

- **Traitement des aspects liés à la dégradation et au recouvrement des niveaux de criticité des objets** : En effet, dans ce mémoire, nous n'avons fourni que des moyens de gradation et de dégradation des niveaux de crédibilité des sujets, il serait aussi intéressant de développer concrètement des moyens de vérification et de restauration de l'intégrité des objets (i.e. les IVP du modèle Clark et Wilson).

- **Conception d'une approche plus pointue de sélection des collaborateurs** : L'approche proposée dans DI-OrBAC se limite à la détermination de la crédibilité des organisations, sans se soucier de la crédibilité de leurs sujets, en estimant qu'il incombe à l'organisation de gérer ses ressources et de les affecter adéquatement afin d'éviter les pénalités. Une approche plus pointue consisterait à collecter et à diffuser des informations sur les sujets afin de permettre aux organisations d'étayer leurs choix en matière de collaborateurs.

- **Gestion avancée des conflits lors de la négociation des contrats** : Pour élaborer une politique de sécurité cohérente à la VO qui soutiendra les collaborations, il est important de détecter et de résoudre les situations de conflits. Les conflits les plus critiques surviennent lors de la négociation des privilèges d'accès aux ressources. DI-OrBAC propose une solution simple basée sur la puissance des privilèges, sans pour autant pouvoir trancher dans le cas où les politiques confrontées stipulent simultanément des interdictions et des obligations.

- **Extension du langage de DI-OrBAC pour en faire un outil de description des politiques de sécurité et de négociation intégrale des contrats** : Les contrats électroniques se composent de cinq briques fondamentales : les collaborateurs, les ressources engagées, les conditions d'utilisation, les délivrables et les pénalités. Le langage établis jusque-là ne couvre que l'expression des trois premières. Il serait donc intéressant de le compléter pour faire de DI-OrBAC un outil complet et autonome pour la mise en place des collaborations.

- **Développement d'outils d'interfaçage de DI-OrBAC avec les autres modèles de contrôle d'accès** : Chaque organisation adopte le modèle de sécurité qu'elle juge le mieux adapté à l'expression de sa politique de sécurité. Toutefois pour pouvoir mettre en place des collaborations grâce à DI-OrBAC, il sera nécessaire, non seulement, d'adapter les politiques au début des négociations mais aussi de traduire les politiques finales des VO selon les modèles de chaque organisation. Cela pourrait éventuellement se faire en mettant en place des éléments de médiation entre les politiques adoptées par les partenaires.

- **Développement d'une implémentation de DI-OrBAC et test des deux implémentations dans des conditions réelles** : Tout comme nous avons élaboré une implémentation d'I-OrBAC, il sera question par la suite de développer une implémentation de DI-OrBAC tout en spécifiant les moyens de concrétisation et de supervision des contrats, éventuellement à travers l'utilisation des automates temporisés à la manière de Poly-OrBAC. Il serait aussi intéressant d'utiliser nos extensions dans des conditions réelles, potentiellement dans les secteurs évoqués dans les exemples (santé et énergie électrique) où leurs applications sont déjà perceptibles.

ANNEXES :

Activité du projet de programme	Budget de 2013	Budget de 2014
Protection des Infrastructures	**260**	**263**
Identification, Analyse et Planification	*59*	*63*
Gestion des secteurs et de la gouvernance	*67*	*63*
Opérations régionales sur le terrain	*56*	*57*
Conformité de la sécurité des infrastructures	*78*	*81*
Cyber-sécurité	**756**	**792**
Coordination de la cyber-sécurité	*4*	*4*
Opérations de l'US-CERT	*93*	*102*
Sécurité du réseau fédéral	*236*	*200*
Déploiement de la sécurité des réseaux	*329*	*382*
Management de la cyber-sécurité globale	*26*	*26*
Cyber-protection des infrastructures critiques et sensibilisation	*63*	*73*
Opérations commerciales	*6*	*5*
Communications	**140**	**131**
Office des communications d'urgence	*39*	*37*
Services des télécommunications prioritaires	*53*	*53*
Réseaux de nouvelles générations	*24*	*21*
Programmes d'étude et d'amélioration des télécommunications	*13*	*10*
Protection des infrastructures critiques	*11*	*9*
Total	**1158**	**1187**

Tab. 17. Financement du Programme de PIC et de la sécurité de l'information (autorité budgétaire en millions de dollars) [39].

Secteurs et Infrastructures	Rapports et Ordres Exécutifs du Gouvernement									
	CBO (1983)	NCPWI (1988)	E.O. 13010 (1996)	PDD-63 (1998)	E.O. 13228 (2001)	NSHS (2002)	NSPP (2003)	HSPD-7 (2003)	NIPP (2009)	NIPP (2013)
Transports	X	X	X	X	X	X	X	X	X	X
Approvisionnement en eau / Traitement des eaux usées	X	X	X	X	X	X	X	X	X	X
Enseignement	X									
Santé Publique	X			X		X	X	X	X	X
Prisons	X									
Capacité industrielle	X									
Services sanitaires		X								
Télécommunications			X	X	X	X	X	X	X	X
Energies			X	X	X	X	X	X	X	X
Finances et système bancaire			X	X		X	X	X	X	X
Services d'urgences			X	X		X	X	X	X	X
Continuité des services gouvernementaux			X	X		X	X		X	X
Systèmes d'information				X	X	X	X	X	X	X
Installations nucléaires					X				X	X
Evénements spéciaux					X					
Agriculture / Approvisionnement alimentaire					X	X	X	X	X	X
Bases industrielles de défense						X	X	X	X	X
Industries chimiques						X	X	X	X	X
Services postaux et services d'expédition						X	X	X	X	
Icônes et monuments nationaux							X	X	X	
Industries clés et sites technologiques							X		X	X
Grands sites de rassemblement							X			
Installations commerciales									X	X
Barrages									X	X

Tab. 18. Secteurs et infrastructures critiques recensés dans les différents rapports et ordres exécutifs [36]

BIBLIOGRAPHIE

[1]. Public Law 107–56-Oct. 26, 2001, "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) ACT of 2001" (2001).

[2]. The National Commission on Terrorist Attacks Upon the United States : "The9/11 Commission Report" (2004).

[3]. Home Office : "Report of the Official Account of the Bombings in London on 7th July 2005". London : The Stationery Office (2006).

[4]. M. Lesk : "The New Front line : Estonia under cyber-assault". *IEEE Security & Privacy*, vol. 5 (4), pp. 76–79, IEEE, (2007). [ISSN : 1540-7993]

[5]. A. Massoud : "North America's electricity infrastructure: Are we ready for more perfect storms?". *IEEE Security & Privacy*, vol. 1 (5), pp. 19–25, IEEE, (2003). [ISSN : 1540-7993].

[6]. J. W. Bialek : "Why has it happened again ? Comparison between the UCTE blackout in 2006 and the blackouts of 2003". *IEEE Power Tech*, pp. 51–56, Lausanne, (2007).

[7]. J. Bram, J. Orr, C. Rapaport : "Measuring the Effects of the September 11 Attack on New York City". *Federal Reserve Bank of New York Economic Policy Review*, vol. 8 (2), Social Science Research Network (2002).

[8]. A. Jenik : "Cyberwar in Estonia and the Middle East". *Network Security*, vol. 2009 (4), pp. 4–6, Elsevier Science, (2009). [ISSN:1353-4858]

[9]. Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) : "La défense en profondeur appliquée aux systèmes d'information – Memento" (2004).

[10]. Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) : "Expression des besoins et identification des objectifs de Sécurité (EBIOS) : Méthode de gestion de risques" (2010).

[11]. A. Baina : "Contrôle d'accès pour les grandes infrastructures Critiques : Application au réseau d'énergie électrique". Thèse de Doctorat, INSA de Toulouse, Toulouse, France, Septembre (2009).

[12]. A. Abou El Kalam, Y. Deswarte : "Critical Infrastructures Security Modeling, Enforcement and Runtime Checking". *Critical Information Infrastructure Security*, vol. 5508, pp. 95–108, Springer, (2009).

[13]. D. Mendonça, W. A, Wallace : "Impacts of the 2001 World Trade Center Attack on New York City Critical Infrastructures". *Journal of Infrastructure Systems*, vol. 12 (4), pp. 260–270, American Society of Civil Engineers, (2006).

[14]. Division Protection et Sécurité de l'Etat : "Instruction Générale Interministérielle N°1300 sur la Protection du Secret de la Défense Nationale". Secrétariat général de la défense et de la sécurité nationale, N°1300 /SGDSN/PSE/PSD, (2011).

[15]. President's Commission on Critical Infrastructure Protection : "Critical Foundations: Protecting America's Infrastructures". (1997)

[16]. L. Mé, Y. Deswarte : "Sécurité des réseaux et systèmes répartis". Traité IC2, série Réseaux et Télécommunications, pp. 270, Hermès-Lavoisier, (2003).

[17]. L. Mé, Y. Deswarte : "Sécurité des systèmes d'information". Traité IC2, série Réseaux et Télécommunications, pp. 372, Hermès-Lavoisier, (2006).

[18]. ISO/IEC 15408 – Common Criteria for Information Technology Security Evaluation : "Part 1 : Introduction and general model". Version 3.1, Revision 4, (2012).

[19]. Club de la Sécurité de l'Information Français (CLUSIF) : "Mehari 2010 – Présentation générale". (2010).

[20]. R. A. Caralli, J. F. Stevens, L. R. Young, W. R. Wilson : "Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process". Technical Report CMU/SEI-2007-TR-012, ESC-TR-2007-012, Software Engineering Institute, Carnegie Mellon, (2007).

[21]. International Organization for standardization: "ISO/IEC 27005:2011 – Information technology : Security techniques – information security risk management", (2011).

[22]. ISO/IEC 15408 – Common Criteria for Information Technology Security Evaluation : "Part 2 : Security functional components". Version 3.1, Revision 4, (2012).

[23]. R. S. Sandhu, P. Samarati : "Access Control : Principles and Practice". *IEEE Communications Magazine*, vol. 32 (9), pp. 40–48, IEEE, (1994). [ISSN : 0163-6804]

[24]. B. Lampson : "Protection". *5th Princeton Symposium on Information Sciences and Systems*, pp. 437–443 (1971).

[25]. D. Bell, L. LaPadula : "Secure computer systems: unified exposition and multics interpretation". *Technical Report ESD-TR-75-306*, MTR-2997, MITRE, Bedford, MA, USA (1975).

[26]. K. Biba : "Integrity considerations for secure computer systems". *Technical Report ESD-TR-76-372*, ESD/AFSC, Hanscom AFB, Bedford, MA, USA (1977)

[27]. D. F. Ferraiolo, R. S. Sandhu, S. Gavrila, D. R. Kuhn, R. Chandramouli : "Proposed NIST standard for role-based access control". *ACM Transactions on Information and System Security*, vol. 4 (3), pp. 224–274, ACM, (2001).

[28]. T. Fink, M. Koch, C. Oancea : "Specification and enforcement of access control in heterogeneous distributed applications". *Web Services – ICWS-Europe 2003*, vol. 2853, pp. 88–100, (2003)

[29]. R. K. Thomas, R. S. Sandhu : "Task-based authorization controls (TBAC) : a family of models for active and enterprise-oriented authorization management". *Proceedings of the 11th IFIP International Conference on Database Security*, pp. 166–181, Chapman & Hall, (1998).

[30]. R. S. Sandhu, J. Park : "Usage control: a vision for next generation access control". *Computer Network Security*, vol. 2776, pp. 17–31 (2003).

[31]. S. Benferhat, R. El Baida, F. Cuppens : "A stratification-based approach for handling conflicts in access control". *Proceedings of the 8th ACM Symposium on Access Control Models and Technologies* (SACMAT'03), pp. 189–195 (2003).

[32]. A. Abou El Kalam, R. El Baida, P. Balbiani , S. Benferhat, F. Cuppens, Y. Deswarte, A. Miège, C. Saurel, G. Trouessin : "Organization based access control". *4th International Workshop on Policies for Distributed Systems and Networks (POLICY)*, pp. 120–131, IEEE, (2003).

[33]. A. Abou El Kalam : "Modèles et politiques de sécurité pour les domaines de la santé et des affaires sociales". Thèse de Doctorat, INP de Toulouse, Toulouse, France, Décembre 2003.

[34]. P. R. Krishna, K. Karlapalem : "Electronic Contracts". *IEEE Internet Computing*, vol. 12 (4), pp. 60–68, IEEE, (2008). [ISSN : 1089-7801]

[35]. A. Rathmell : "Protecting critical information infrastructure". *Computers & Security*, vol. 20 (1), pp. 43–52, Elsevier Science, (2001).

[36]. J. Moteff, P. Parfomak : "Critical infrastructure and key assets : Definition and identification". *CRS Report for Congress*, Congressional Research Service, The Library of Congress (2004).

[37]. E. M. Brunner, M. Suter : "International CIIP Handbook 2008/2009 : An inventory of 25 national and 7 international critical information infrastructure protection policies". *Center for Security Studies*, ETH Zurich, (2008)

[38]. Commission des Communautés Européennes : "Livre Vert sur un Programme Européen de Protection des Infrastructures Critiques". COM(2005) 576 final, Bruxelles, le 17.11.2005. (2005)

[39]. J. D. Moteff : "Critical Infrastructures : Background, Policy, and Implementation". *CRS Report*, Congressional Research Service, The Library of Congress (2014).

[40]. S. Orlowski : "Information Management – Protecting Critical Information assets". *Computer Law & Security Report*, vol. 17 (3), pp. 182–185, Elsevier Science, (2001).

[41]. Commission des Communautés Européennes : "Communication de la Commission au Conseil et au Parlement Européen – Protection des infrastructures critiques dans le cadre de la lutte contre le terrorisme". COM(2004) 702 final, Bruxelles, le 20.10.2004. (2004)

[42]. The White House : "Executive Order EO 13010 : Critical Infrastructure Protection". 61 Federal Register 37347, (1996).

[43]. The Clinton Administration : "Presidential Decision Directive 63 (PDD-63) : Policy on Critical Infrastructure Protection". (1998).

[44]. US Department of Homeland Security : "National Infrastructure Protection Plan – Partnering to enhance protection and resiliency". (2009)

[45]. US Department of Homeland Security : "National Infrastructure Protection Plan – Partnering for Critical Infrastructure security and resilience". (2013)

[46]. J. P. Galland : "Critique de la notion d'infrastructure critique". Flux 3/ 2010 (n° 81), pp. 6-18, (2010).

[47]. J. V. Parachini : "The World Trade Center Bombers (1993)". *Toxic Terror : Assessing Terrorist Use of Chemical and Biological Weapons*, pp. 185–206, MIT Press, Cambridge, MA (2000).

[48]. C. W. Lewis : "The Terror that Failed : Public Opinion in the Aftermath of the Bombing in Oklahoma City". *Public Administration Review*, vol. 60 (3), pp. 201–210, American Society for Public Administration, (2000). [ISSN : 1540-6210]

[49]. S. G. Stolberg : "Senates Passes Legislation to Renew Patrot Act". *The New York Times*, March, 3, (2006).

[50]. J. Abrams : "Patriot Act Extension Signed by Obama". *The Huffington Post*, May, 27, (2011).

[51]. K. Pauley : "USA PATRIOT Act (P.L 107-56) – Amendments Made by Key Provisions to : Electronic Communications Privacy Act, Communications Act, Foreign Intelligence Surveillance Act, Computer Fraud & Abuse Act". *Electronic Commerce &*

Privacy Practice Group, Piper Marbury Rudnick & Wolfe LLP, Washington, DC, (2001)

[52]. E. C. Liu : "Amendments to the Foreign Intelligence Surveillance Act (FISA) Extended Until June 1, 2015". *CRS Report for Congress*, Congressional Research Service, (2011).

[53]. C. Doyle : "Privacy : An Overview of the Electronic Communications Privacy Act". *CRS Report for Congress*, Congressional Research Service, (2012).

[54]. Financial Crimes Enforcement Network (FINCEN) : "History of Anti-Money Laundering Laws". *United States Department of the Treasury*.

[55]. Federal Financial Institutions Examination Council : "Bank Secrecy Act/Anti-Money Laundering Examination Manual". *Federal Financial Institutions*, (2010).

[56]. Site officiel de : "ACLU – American Civil Liberties Union".

[57]. Site officiel de : "Electronic Frontier Foundation – Defending your rights in the digital world".

[58]. American Civil Liberties Union : "Surveillance Under The USA PATRIOT Act". Site officiel de l'ACLU.

[59]. Electronic Frontier Foundation : "EFF Analysis of the Provisions of the USA PATRIOT Act". Site officiel de l'EFF.

[60]. Electronic Frontier Foundation : "Documents Obtained by EFF Reveal FBI PATRIOT Act Abuses". Site officiel de l'EFF.

[61]. Site: "Electronic Privacy Information Center – National Security Letters".

[62]. US Department of Homeland Security : "National Infrastructure Protection Plan". (2006)

[63]. The White House: "Presidential Policy Directive / PPD-8: National Preparedness". (2011)

[64]. The White House: "Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience". (2013)

[65]. The White House: "Executive Order 13636 – Improving Critical Infrastructure Cyber security". (2013)

[66]. J. M. Yusta, G. J. Correa, R. Lacal-Arantegui : "Methodologies and applications for critical infrastructure protection : State-of-the-art". *Energy Policy*, vol. 39 (10), pp. 6100 – 6119, Elsevier Science, (2001). [ISSN : 0301-4215]

[67]. European Union Committee : "After Madrid : The EU's response to terrorism – Report with Evidence". *5th Report of Session 2004-05*, House of Lords, London : The Stationery Office, (2005).

[68]. Ministère Fédéral de l'Intérieur Allemand : "Protection des infrastructures critiques – Concept de base de protection. Recommandations destinées aux entreprises". Ministère Fédéral de l'Intérieur, (2005).

[69]. Ministère Fédéral de l'Intérieur Allemand : "Protection des infrastructures critiques – gestion des risques et des crises. Manuel destiné aux entreprises et aux administrations". Division KM4, Ministère Fédéral de l'Intérieur, (2011).

[70]. Conseil Européen : "Déclaration sur la lutte contre le terrorisme". Bruxelles, le 25.03.2004. (2004)

[71]. Commission des Communautés Européennes : "Communication de la Commission au Conseil et au Parlement Européen – Attaques terroristes : prévention, préparation et réponse". COM(2004) 698 final, Bruxelles, le 20.10.2004. (2004)

[72]. Commission des Communautés Européennes : "Communication de la Commission au Conseil et au Parlement Européen – Lutte contre le terrorisme : préparation et gestion des conséquences". COM(2004) 701 final, Bruxelles, le 20.10.2004. (2004)

[73]. Commission des Communautés Européennes : "Proposition de Décision du Conseil relative au réseau d'alerte concernant les infrastructures critiques (CIWIN)". COM(2008) 676 final, Bruxelles, le 27.10.2008. (2008)

[74]. Commission des Communautés Européennes : "Communication de la commission sur un programme européen de protection des infrastructures critiques". COM(2006) 786 final, Bruxelles, le 12.12.2006. (2006)

[75]. Conseil de l'Union Européenne : "Décision 2007/124/CE du Conseil du 12 Février 2007 établissant, pour la période 2007-2013, dans le cadre du programme général « Sécurité et protection des libertés », le programme spécifique « Prévention, préparation et gestion des conséquences en matière de terrorisme et autres risques liés à la sécurité »". Journal officiel de l'Union européenne, 24.02.2007. (2007)

[76]. Conseil de l'Union Européenne : "Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection". Journal officiel de l'Union européenne, 23.12.2008. (2008)

[77]. Commission des Communautés Européennes : "Proposition de Décision du Parlement Européen et du Conseil relative au septième programme-cadre de la Communauté européenne pour des activités de recherche, de développement technologique

et de démonstration (2007-2013) -- Proposition de Décision du Conseil relative au septième programme-cadre de la Communauté européenne de l'énergie atomique (Euratom) pour des activités de recherche et de formation en matière nucléaire (2007-2011)". COM(2005) 119 final/2, Bruxelles, le 06.04.2005. (2005)

[78]. World Summit on the Information Society : "Tunis Commitment". Document WSIS-05/TUNIS/DOC/7-E, (2005).

[79]. World Summit on the Information Society : "Plan of Action". Document WSIS-03/GENEVA/DOC/5-E, (2003).

[80]. World Summit on the Information Society : "Declaration of Principles. Building the Information Society : A Global Challenge in the New Millennium". Document WSIS-03/GENEVA/DOC/4-E, (2003).

[81]. United Nations – General Assembly : "Resolution adopted by the General Assembly : 57/239. Creation of a global culture of cybersecurity". On the report of the Second Committee (A/57/529/Add.3), (2002).

[82]. United Nations – General Assembly : "Resolution adopted by the General Assembly : 58/199. Creation of a global culture of cybersecurity and the protection of critical information infrastructures". On the report of the Second Committee (A/58/481/Add.2), (2003).

[83]. Risk Steering Committee: "DHS Risk Lexicon – 2010 Edition". U.S. Department of Homeland Security, (2010).

[84]. International Organization for standardization: "ISO/IEC 31000:2009 – Risk Management – Principles and guidelines", (2009).

[85]. Y. Mortureux : "Analyse préliminaire de risques". Techniques de l'Ingénieur, se4010, (2002).

[86]. International Organization for Standardization: "ISO Guide 73 :2009 – Risk Management – Vocabulary", (2009).

[87]. Standards Australia/ Standards New Zealand: "AS/NZS 4360:2004 – Australian/New Zealand Standard for Risk Management", (2004).

[88]. U.S. Office of Homeland Security : "The National Strategy for Homeland Security". (2002)

[89]. A.N. Bessani, P. Sousa, M. Correia, N. F. Ferreira, P. Verissimo : "The Crutial Way of Critical Infrastructure Protection". *IEEE Security & Privacy*, vol. 6 (6), pp. 44–51, IEEE, (2008).

[90]. T. R. Peltier: "Information Security Fundamentals, Second Edition". CRC Press, pp. 438, Auerbach Publications, (2013).

[91]. D. Fisher: "Qu'est-ce qu'un botnet?". Site officiel du blog Kaspersky, (2013).

[92]. Kaspersky Global Research & Analysis Team (GREAT) : "Kaspersky Security Bulletin 2014". *Kaspersky Lab*, (2014).

[93]. Symantec : "Internet Security Threat Report". ISTR, vol. 20, (2015).

[94]. Cisco: "Cisco 2014 Annual Security Report", (2014).

[95]. Y. Laarouchi : "Sécurités (immunité et innocuité) des architectures ouvertes à niveaux de criticité multiples : application en avionique". Thèse de Doctorat, INSA de Toulouse, Toulouse, France, Septembre (2009).

[96]. Cambridge Dictionaries Online : "Home page for Business English Dictionary: Time to Market in Business English".

[97]. N. Mimura, K. Yasuhara, S. Kawagoe, H. Yokoki, S. Kazama : "Damage from the Great East Japan Earthquake and Tsunami – A quick report". *Mitigation and Adaptation Strategies for Global Change*, vol. 16 (7), pp. 803–818, Springer, (2011).

[98]. R. F. Dacey : "Critical Infrastructure Protection: Significant Challenges Need to Be Addressed". *United States General Accounting Office*, GAO-02-961T, (2002).

[99]. R. F. Dacey : "Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors". *United States General Accounting Office*, GAO-04-780, (2004).

[100]. A. J. Scholand, J. M. Linebarger, M. A. Ehlen: "Thoughts on Critical Infrastructure Collaboration". International ACM SIGGROUP Conference on Supporting Group Work (GROUP '05), pp. 344–345, Sanibel Island, Florida, USA, (2005).

[101]. Merriam-Webster Dictionary Online : "Integrity definition".

[102]. E. Amoroso, M. Merritt : "Composing system integrity using I/O automata". *10th Annual Computer Security Applications Conference*, pp. 34–43, Orlando, FL, USA, (1994).

[103]. O. Prnjat, L. E, Sacks : "Integrity Methodology for Interoperable Environments". *IEEE Communications Magazine*, vol. 37(5), IEEE, (1999).

[104]. M. Bishop : "Computer security : Art and Science – First Edition", pp. 1136, Addison-Wesley, Boston, MA (2003).

[105]. M. Gegick, S. Barnum: "Separation of privilege". *Official website of the Department of Homeland Security*, (2005).

[106]. V. C. Hu, D. F. Ferraiolo, D. R. Kuhn: "Assessment of Access Control Systems". *Interagency Report 7316*, Computer Security Division, Information Technology Laboratory, NIST, (2006).

[107]. C. Coma : Interopérabilité et cohérence de politiques de sécurité pour les systèmes auto-organisant. Thèse de Doctorat, ENST de Bretagne, Rennes, France, 2009.

[108]. M. A. Harrison, W. L. Ruzzo, J. D. Ullman: "Protection in Operating Systems". Communications of the ACM, vol. 19(8), pp. 461–471, (1976).

[109]. K. A. Jones, R. J. Lipton, L. Snyder: "A linear time algorithm for deciding security". *17th Annual Symposium on Foundations of Computer Science*, pp. 33–41, IEEE, (1976).

[110]. R. K. Thomas : "Team-based access control (TMAC): a primitive for applying role-based access controls in collaborative environments". 2nd ACM Workshop on RBAC, pp. 13–19, Fairfax, Virginia, USA, (1997).

[111]. L. G. Lawrence 1993: "The role of roles". *Computers & Security*, vol. 12(1), pp. 15–21, (1993).

[112]. S. H. von Solms, I. van der Merwe: "The Management of computer security profiles using role-oriented approach". *Computers & Security*, vol. 13(8), pp. 673–680, (1994).

[113]. R. S. Sandhu: "Role hierarchies and constraints for lattice-based access controls". *Computer Security – ESORICS 96*, vol. 1146, pp. 65–79, (1996).

[114]. R.S. Sandhu, E. J. Coyne, H. L. Feinstein, C. E. Youman: "Role-based access control models". IEEE Computer, vol. 29(2), pp. 38–47, (1996).

[115]. S. I. Garvila, J. F. Barkley: "Formal specification for Role Based Access Control User/Role and Role/Role Relationship Management". *3rd ACM Workshop on Role-based Access Control*, pp. 81–90, (1998).

[116]. G. J. Ahn, R. S. Sandhu: "Role-based authorization constraints specification". *ACM Transactions on Information and System Security* (TISSEC), vol. 3(4), pp. 207–226, (2000).

[117]. N. Li, J. W. Byun, E. Bertino : "A Critique of the ANSI Standard on Role-Based Access Control". *IEEE Security & Privacy*, vol. 5(6), pp. 41–49, IEEE, (2007). [ISSN: 1540-7993]

[118]. M. Krause, H. F. Tipton : "Handbook of information security management". Auerbach Publications/CRC Press LLC, Boca Raton, FL, USA (1998)

[119]. J. A. Goguen, J. Meseguer : "Security policies and security models". *IEEE Symposium on Security and Privacy*, pp. 11–20, Oakland, CA, USA, (1982).

[120]. D. Clark, D. Wilson : "A comparison of commercial and military computer security policies". *IEEE Symposium on Security and Privacy*, pp. 184–194, Oakland, CA, USA, (1987).

[121]. D. F. C. Brewer, M. J. Nash : "The Chinese wall security policy". *IEEE Symposium on Security and Privacy*, pp. 206–214, Oakland, CA, USA, (1988).

[122]. E. Totel, J. P. Blanquart, Y. Deswarte, D. Powell : "Supporting multiple levels of criticality". *28th IEEE International Symposium on Fault Tolerant Computing*, pp. 70–79, Munich, Germany, (1998).

[123]. E. Totel : "Politique d'intégrité multi niveau pour la protection en ligne de tâches critiques". Thèse de Doctorat, Institut National Polytechnique de Toulouse, Toulouse, France, Décembre (1998).

[124]. M. Zhang: "Strict Integrity Policy of Biba Model with Dynamic Characteristics and its Correctness". *International Conference on Computational Intelligence and Security* (CIS '09), pp. 521–525, Beijing, China, (2009).

[125]. Q. Xu, G. Liu: "Configuring Clark-Wilson Integrity Model to Enforce Flexible Protection". *International Conference on Computational Intelligence and Security* (CIS '09), pp. 15–20, Beijing, China, (2009).

[126]. A. Abou El Kalam, Y. Deswarte : "MultiOrBAC : A new access control model for distributed, heterogeneous and collaborative systems". *8th IEEE Symposium on Systems and Information Security*, Sao Paulo, Brazil (2006).

[127]. A. Baina, A. Abou El Kalam, Y. Deswarte, M. Kaaniche : "Collaborative access control framework for critical infrastructures". *2nd IFIP WG 11.10 International Conference on Critical Infrastructure Protection*, vol. 290, pp. 189–201, Arlington, USA (2008).

[128]. A. Abou El Kalam, Y. Deswarte, A. Baina, M. Kaaniche : "Poly-OrBAC : a security framework for critical infrastructures". *International Journal of Critical Infrastructure Protection*, vol. 2 (4), pp. 154–169, Elsevier Science, (2009).

[129]. OASIS: "UDDI Specifications TC, Universal Description, Discovery and Integration". OASIS standard v3.0.2, (2005).

[130]. F. Cuppens, N. CuppensBoulahia, C. Coma : "O2O : Virtual private organizations to manage security policy interoperability". *Proceeding of the 2nd International Conference on Information Systems Security*, vol. 4332, pp. 101–115, India (2006)

[131]. A. Mowshowitz: "Virtual Organization". Communications of the ACM, vol. 40(9), pp. 30–37, ACM, (1997).

[132]. K. Toumi, C. Andrés, A. Cavalli: "Trust-OrBAC: A Trust Access Control Model in Multi-Organization Environments". *Information Systems Security*, vol. 7671, pp. 89–103, (2012).

[133]. I. Ray, S. Chakraborty: "A Vector Model of Trust for Developing Trustworthy Systems". *Computer Security – ESORICS 2004*, vol. 3193, pp. 260–275, (2004).

[134]. I. Ray, I. Ray, S. Chakraborty: "An Interoperable Context Sensitive Model of Trust". *Journal of Intelligent Information Systems*, vol. 32(1), pp. 75–104, (2009).

[135]. F. Cuppens, N. CuppensBoulahia, M. B. Ghorbel : "High level conflict management strategies in advanced access control models". *Electronic Notes on Theoretical Computer Science*, vol. 186, pp. 3–26, Elsevier Science, (2007).

[136]. F. Cuppens, A. Miège : "Modeling contexts in the Or-BAC model". *Proceeding of the 19th Annual Computer Security Applications Conference*, pp. 416–425, Las Vegas, USA (2003).

[137]. F. Cuppens, N. CuppensBoulahia, A. Miège : "Inheritance hierarchies in the Or-BAC model and their application in a network environment". *2nd Foundations of Computer Security Workshop* (FCS'04), Turku, Finland (2004).

[138]. F. Cuppens, A. Miège : "Administration model for OrBAC". *On The Move to Meaningful Internet Systems* : OTM 2003 Workshops; Lecture Notes in Computer Science, vol. 2889, pp. 754–768, Italy (2003).

[139]. A. Ameziane El Hassani, A. Abou El Kalam, A. Ait Ouahman : "Integrity-organization based access control for critical infrastructure systems". *Critical Infrastructure Protection VI*, pp. 31–42, Washington, DC, USA, (2012)

[140]. A. Ameziane El Hassani, A. Abou El Kalam, A. Bouhoula, R. Abbassi, A. Ait Ouahman : "Integrity-OrBAC: A new model to preserve Critical Infrastructures integrity". *International Journal of Information Security*, vol. 14 (4) pp. 367–385, (2015). [ISSN : 1615-5262].

[141]. A. Abou El Kalam, A. Ameziane El Hassani, A. Ait Ouahman : "Integrity-OrBAC : an OrBAC enhancement that takes into account integrity". *8th International Conference on Intelligent Systems: Theories and Applications* (SITA), pp. 1–7, Rabat, Morocco, (2013).

[142]. N. Essaouini, A. Abou El Kalam, A. Ait Ouahman : "Access control policy: a framework to enforce recommendations". *International Journal of Computer Science and Information Technologies*, vol. 2 (5), pp. 2452–2463 (2011)

[143]. eXtensible Access Control Markup Language (XACML) Version 3.0, OASIS standard (2013).

[144]. Core and hierarchical role based access control (RBAC) profile of XACMLv2.0,OASIS standard (2005).

[145]. P. Verissimo, N.F. Neves, M. Correia, Y. Deswarte, A. Abou El Kalam, A. Bondavalli, A. Daidone : "The CRUTIAL architecture for critical information infrastructures". *Architecting Dependable Systems V*, LNCS, vol. 5135, Springer, pp. 1–27, (2008).

[146]. K. W. Thomas: "Conflict and Negotiation process in organizations". *Handbook of Industrial and Organizational Psychology – 2nd edition*, vol. 3, pp. 655–717, Consulting Psychologists Press, Inc. (1992)

[147]. S. G. Cohen, D. Mankin: "Collaboration in the Virtual Organization". *Trends in Organizational Behavior, vol. 6: The Virtual Organization*, (pp. 105–120), John Wiley & Sons. (1999)

[148]. R. Deitos, F. Kerschbaum, P. Robinson: "A comprehensive security architecture for dynamic, web service based virtual organizations for businesses". *3rd ACM Workshop on Secure Web Services*, pp. 103–104. (2006)

[149]. I. Foster, C. Kesselman, S. Tuecke: The anatomy of the grid: enabling scalable virtual organizations. *International Journal of High Performance Computing Applications*, vol. 15(3), pp. 200–222, Sage Publications, Inc. (2001)

[150]. J. Li, J. Huai, C. Hu, Y. Zhu: "A secure collaboration service for dynamic virtual organizations". Information Sciences, vol. 180(17), pp. 3086–3107, Elsevier, (2010).

[151]. A. Mowshowitz: "On the Theory of Virtual Organization". Systems Research and Behavioral Science, vol. 14(6), pp. 373–384, John Wiley & Sons, Ltd, (1997).

[152]. A. Daskalopulu, T. Maibaum: "Towards Electronic Contract Performance". 12th International Workshop on Database and Expert Systems Applications (DEXA 01), pp. 771–777, IEEE CS Press, (2001).

[153]. Z. Milosevic, A. Josang, T. Dimitrakos, M. A. Patton: "Discretionary Enforcement of Electronic Contracts". 6th International Enterprise Distributed Object Computing Conference (EDOC'02), pp. 39–50, IEEE, (2002).

[154]. G. Governatori, Z. Milosevic: "A Formal Analysis of a Business Contract Language". International Journal of Cooperative Information Systems, vol. 15(4), pp. 659–685, World Scientific, (2006).

[155]. C. Molina-Jimenez, S. Shrivastava, E. Solaiman, J.Warne: "Run-Time Monitoring and Enforcement of Electronic Contracts". Electronic Commerce Research and Applications, vol. 3(2), pp. 108–125, Elsevier, (2004).

[156]. C. Molina-Jimenez, S. Shrivastava, J.Warne: "A Method for Specifying Contract Mediated Interactions". 9th International EDOC Enterprise Computing Conference (EDOC'05), pp. 106–115, IEEE, (2005).

[157]. C. Molina-Jimenez, S. Shrivastava, M. Strano: "A Model for Checking Contractual Compliance of Business Interactions". IEEE Transactions on Services Computing, vol. 5(2), pp. 276–289, IEEE, (2012).