# Système autonome de sécurité lors de la préparation d'un repas pour les personnes cognitivement déficientes dans un habitat intelligent pour la santé

Nicola Kuijpers

**THESE / UNIVERSITE DE BRETAGNE-SUD**
*sous le sceau de l'Université Bretagne Loire*

pour obtenir le titre de
**DOCTEUR DE L'UNIVERSITE DE BRETAGNE-SUD**

*Mention : STIC*
**Ecole doctorale SICMA**


Présentée par

Nicola Kuijpers

Préparée à l'unité mixte de recherche CNRS 6285
Université de Bretagne-Sud

Laboratoire Lab-STICC


# Système Autonome de Sécurité lors de la Préparation d'un Repas pour des Personnes Cognitivement Déficientes dans un Habitat Intelligent pour la Santé

**Thèse soutenue le 13 mars 2017**
devant le jury composé de :

**Jean-Luc Philippe**
Professeur, Université de Bretagne-Sud / Directeur de thèse

**Sylvain Giroux**
Professeur, Université de Sherbrooke / Co-directeur de thèse

**Florent de Lamotte**
Maître de conférences, Université de Bretagne-Sud / Membre invité

**Hélène Pigot**
Professeure, Université de Sherbrooke / Présidente du jury

**Fabrice Peyrard**
Maître de conférences, ENSEEIHT / Rapporteur

**Sébastien Gaboury**
Professeur agrégé, Université du Québec à Chicoutimi / Rapporteur

**Willy Allègre**
Docteur, CMRRF de Kerpape / Examinateur

# Sommaire

Dans les pays développés tels que le Canada ou la France, la population est vieillissante et le nombre de personnes atteintes de déficiences cognitives augmente en conséquence. Ces troubles ont des conséquences sur les activités de la vie quotidienne pour les personnes qui en souffrent. Selon l'autonomie de ces personnes et la sévérité de leur déficience, un hébergement en centre spécialisé peut être envisagé. Ces centres spécialisés représentent souvent un coût financier énorme tant pour la personne que pour la société. Afin de limiter ces coûts, une solution alternative a émergé : les habitats domotiques. Ce sont des habitats dans lesquels un ensemble de technologies permet de pallier aux déficiences des personnes et de leur donner une autonomie accrue. Pour ces personnes, certaines de ces activités de la vie quotidienne peuvent représenter des obstacles voire être dangereuses. Par exemple, l'activité de préparation d'un repas est une activité complexe qui peut présenter des risques variés pour des personnes atteintes de déficiences. Ces personnes sont alors assistées par des professionnels ou leurs aidants naturels lors de cette activité et peuvent perdre l'envie de préparer à manger. L'objectif de cette thèse est de concevoir un système permettant à ces personnes de réaliser l'activité de la préparation d'un repas en toute autonomie et en toute sécurité. D'une part, on retrouve la personne atteinte, qui selon sa déficience, aura une façon unique pour réaliser cette activité. Ces personnes vivent rarement seules, il faut tenir compte qu'un public varié puisse bénéficier du système pour la préparation d'un repas. D'autre part, cette activité aura lieu dans un environnement différent pour chaque habitat. Le système doit assurer la sécurité lors de l'activité de préparation de repas, par conséquent, la fiabilité du système est un critère important. Ces habitats sont généralement déjà équipés d'appareils, il devient nécessaire pour le système de pouvoir s'adapter à ces appareils existants. L'objectif de ces travaux est la réalisation d'un prototype permettant d'assurer la sécurité lors de l'activité de la préparation d'un repas par des personnes atteintes de la maladie d'Alzheimer et ses aidants (professionnels ou naturels). Ce prototype doit s'adapter aux besoins des usagers, de son environnement et du matériel sur lequel il est déployé.

Pour ce faire, le système, basé sur un système multi-agents, applique des règles de sécurité qui se personnalisent par le biais du profil médical des usagers. La réalisation de modèles pour chaque objectif a permis de réaliser une architecture d'un système flexible. Ces modèles ont été déployés sur deux applications distinctes. Nos travaux ont été menés au sein de deux laboratoires, qui chacun, disposent d'appareils de cuisine différents dans leurs habitats intelligents pour la santé. Les besoins en termes de capteurs et leur interfaçage avec le système sont présentés. Enfin, le système a pu être testé dans ces deux environnements, son adaptation vis-à-vis d'une clientèle variée et pour plusieurs risques de sécurité à travers des scénarios d'usage. Les résultats de ces expérimentations ont été concluants et ont permis de montrer que le prototype répond bien aux objectifs visés.

# Remerciements

Je tiens à remercier en premier mes encadrants de thèse Jean-Luc Philippe, Sylvain Giroux ainsi que Florent de Lamotte. C'est grâce à ces trois personnes que cette thèse a pu se dérouler dans de très bonnes conditions. Je tiens à remercier Jean-Luc Philippe pour sa vision claire.

Je tiens également à remercier Sylvain Giroux, qui, sans lui, cette thèse en cotutelle n'aurait pas pu avoir lieu. Sa bonne humeur et ses conseils précieux ont permis à ces travaux d'être complets et aboutis. Je remercie Florent de Lamotte pour sa disponibilité et les discussions fort intéressantes que j'ai pu entretenir avec lui. Je remercie Fabrice Peyrard et Sébastien Gaboury d'avoir accepté d'être mes rapporteurs. Je remercie Willy Allègre d'avoir apporté des conseils durant toute cette période et d'avoir examiné mes travaux.

Ensuite, je tiens à remercier toute l'équipe au laboratoire DOMUS pour leur accueil chaleureux. Les différents moments de discussions et de détente ont permis de travailler avec un esprit sain et d'autocritique. Je souhaite en particulier remercier Wathek Bellah Loued pour son aide et ses conseils qui ont été d'une grande utilité tout au long de ce doctorat. Je remercie également Stéphanie Pinard, Carolina Bottari, Fanny Lemorellec, Marisnel Olivares, Carolann Fecteau-Mathieu et Catherine Laliberté pour l'élaboration des règles de sécurité qui sont utilisés dans ces travaux.

Je tiens également à remercier les organismes qui m'ont financièrement aidé à réaliser cette recherche. En particulier la région Bretagne et le laboratoire DOMUS. Je tiens également à remercier Pascal Berruet d'avoir permis l'achat de matériel pour ce projet.

Je souhaite également remercier mes parents pour leur soutien lors de ce doctorat, en particulier ma mère qui n'est plus présente pour me voir aboutir ces travaux.

Enfin, je souhaite remercier ma conjointe, Kathy Lemelin, pour son support quotidien malgré les périodes difficiles induites par une cotutelle internationale.

# Table des matières

# Liste des abréviations

| | |
|---|---|
| ACL | Agent Communication Language |
| ADT | Android Development Toolkit |
| AMM | Agent Mobility Manager |
| AVQ | Activité de la Vie Quotidienne |
| CAN | Convertisseur Analogique Numérique |
| CCAH | Comité national Coordination Action Handicap |
| CMRRF | Centre Mutualiste de Rééducation et de Réadaptation Fonctionnelles |
| DLNA | Digital Living Network Alliance |
| DOMUS | DOmotique et informatique Mobile à l'Université de Sherbrooke |
| EIB | European Installation Bus |
| FIPA | Foundation for Intelligent Physical Agents |
| GPIO | General Purpose Input / Output |
| HIS | Habitat Intelligent pour la Santé |
| INSEE | Institut National de la Statistique et des Études Économiques |
| IPMS | Inter-Platform Mobility Service |
| ISQ | Institut des Statistiques du Québec |
| JADE | Java Agent DEvelopment framework |
| JVM | Java Virtual Machine |
| Lab-STICC | Laboratoire des Sciences et Techniques de l'Information, de la Communication et de la Connaissance |
| MAC | Media Access Control |
| NFC | Near Field Communication |
| OMS | Organisation Mondiale de la Santé |
| PPH | Processus de Production du Handicap |
| RFID | Radio Frequency IDentification |
| SMA | Système Multi-Agent |
| SPI | Serial Peripheral Interface |
| SSH | Secure SHell |
| SQL | Structured Query Language |
| TCC | Traumatisme Cranio-Cérébral |
| QoS | Quality of Service |
| UML | Unified Modeling Language |

| | |
|---|---|
| UPnP | Universal Plug and Play |
| Wi-Fi | Wireless Fidelity |

# Liste des tableaux

# Liste des figures

# Introduction

## Contexte

La population dans les pays développés comme la France et le Canada est vieillissante. L'INSEE (Institut National de la Statistique et des Etudes Economiques) projette que 31.9% de la population en France sera âgée de 60 ans ou plus en 2050, contre 22.6% en 2010 [1] (Figure 1). De la même manière, au Québec, l'ISQ (Institut de la Statistique du Québec) prévoit une forte hausse de personnes âgées de 71 ans et plus d'ici 2030 [2] (Figure 2). Les classes d'âge entre 0 et 70 ans demeurent relativement stables, tandis que la classe d'âge de 71 ans et plus est croissante.

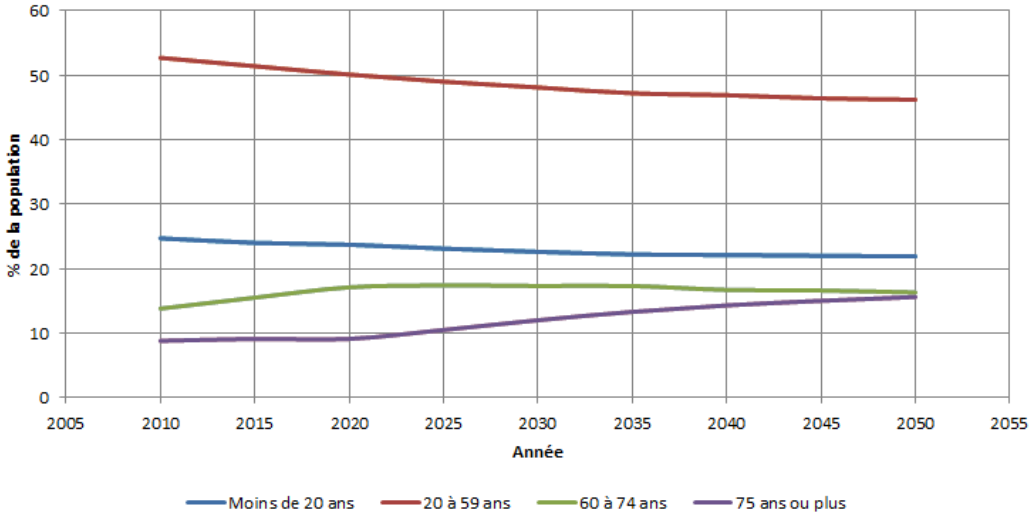



Figure 1 - Projection de l'évolution de la population en France à l'horizon 2050 [1].

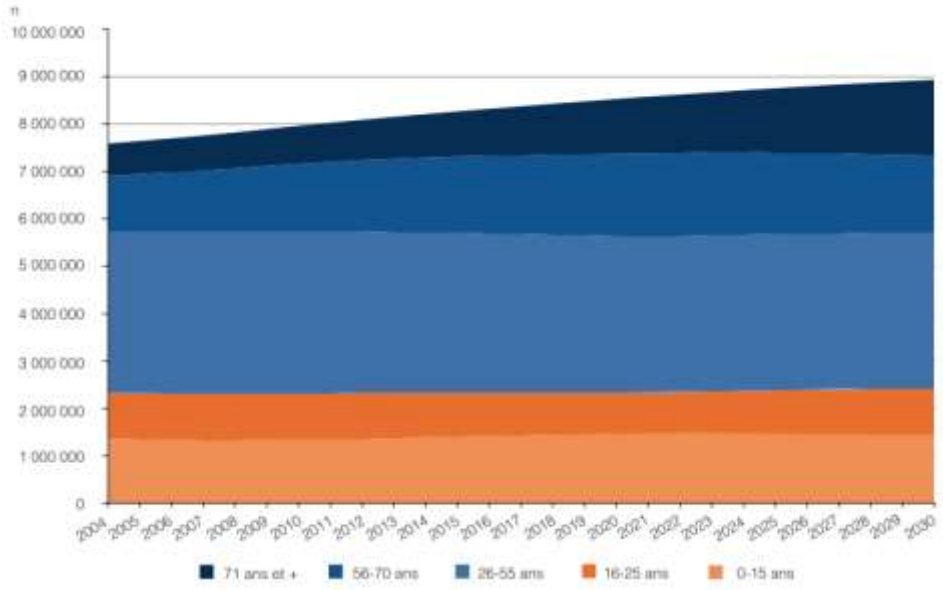



Figure 2 - Projection de l'évolution de la population au Québec à l'horizon 2030 [2].

Le vieillissement implique souvent des déficits cognitifs ou moteurs. Ces déficits ont des coûts humains, sociaux et économiques importants. Les personnes qui souffrent de ces déficits (traumatismes cranio-cérébraux (TCC), schizophrénies, déficiences intellectuelles, Alzheimer ou mobilité réduite) vivent au quotidien l'impact de leur déficience. Les coûts économiques sont ressentis par la rareté des ressources (matérielles et humaines) disponibles pour les intervenants professionnels. Le nombre de personnes en situation de handicap moteur ou cognitif augmente considérablement, le nombre d'aidants potentiels n'augmente pas en conséquence. Il faut donc penser à des solutions alternatives pour permettre à ces personnes en situation de handicap de conserver un niveau d'autonomie suffisant pour rester dans leur environnement domestique le plus longtemps possible. Actuellement, le manque de systèmes d'assistance cognitive ou moteur oblige trop souvent les personnes atteintes de ces déficits à quitter leur domicile pour vivre en institution spécialisée. Réaliser de tels systèmes soulève des problèmes complexes au plan électronique et informatique. L'électronique diffuse, l'informatique mobile, l'intelligence ambiante, la sensibilité au contexte, les interfaces tangibles et les réseaux de capteurs sont des domaines qui ont émergé récemment et qui sont au cœur des solutions à apporter pour construire des habitats intelligents capables de pallier les

déficits et d'offrir aux patients des services leur permettant d'atteindre une meilleure qualité de vie dans un environnement connu et sécurisé. Ces habitats intelligents sont alors une solution pour pallier aux déficiences d'une personne en situation de handicap pour qu'elle puisse réaliser ses activités de la vie quotidienne (AVQ) avec le moins de difficultés et le plus de sécurité possible.

## Objectifs

Ce document a pour objectif de présenter une solution permettant d'aider les personnes en situation de handicap dans un habitat intelligent pour la santé (HIS). Cette solution propose aux personnes atteintes de déficiences cognitives ou motrices une assistance dans leurs AVQ, et plus particulièrement une assistance lors de la préparation d'un repas. Ces personnes, par leur handicap, s'exposent à des dangers de brûlure et des risques d'incendie lors de l'utilisation d'appareils pour la préparation du repas. Dans nos travaux, nous définissons l'assistance par une aide d'amélioration de la sécurité. L'idée est d'assurer une sécurité d'usage et de réduire les risques d'incendie et de brûlure tout en laissant la personne autonome dans ses tâches. On entend par autonome que la personne gère lui-même ses actions et tâches. On ne veut pas créer un système permettant de déresponsabiliser la personne, mais de permettre à la personne déficiente de réaliser une AVQ complexe en toute autonomie. Cette solution doit personnaliser la sécurité selon les usagers et s'adapter à son environnement en toute autonomie en s'appuyant sur les domaines tels que l'intelligence ambiante, la personnalisation, l'informatique autonome ainsi que l'informatique omniprésente. L'objectif de ces travaux est la réalisation d'un système permettant d'assurer la sécurité lors de l'activité de la préparation d'un repas par des personnes atteintes de la maladie d'Alzheimer. Ce prototype doit s'adapter aux besoins des usagers, de son environnement et du matériel sur lequel il est déployé.

## Méthodologie

Cette recherche, a été menée au sein de deux laboratoires : Le Lab-STICC et le DOMUS. Chaque laboratoire est équipé d'équipements différents. Une étude a été réalisée permettant d'identifier les limitations des solutions actuelles concernant la sécurité dans la cuisine (pas adaptées pour une clientèle atteinte de déficiences, ne permettant pas de réaliser une AVQ au complet). Ensuite, pour repousser ces limitations, l'étude de différents thèmes scientifiques a permis de conceptualiser notre système vis-à-vis des différents objectifs. Un modèle a été développé et a été implémenté sur diverses applications au sein des deux laboratoires.

## Résultats

Le système développé, a été testé au sein des deux laboratoires. Des tests préliminaires ont permis de valider le fonctionnement du système. Ensuite, des expérimentations ont permis de valider le système par des étudiants volontaires. Ces expérimentations présentent des scénarios d'usage représentant des situations de mise en danger et qui mettent en œuvre différentes facettes du système. La réaction du système vis-à-vis de ces scénarios a été observée et analysée.

## Structure du mémoire

Ce document est découpé en cinq chapitres distincts. Le premier fait une présentation du public cible de ces travaux et détaille les caractéristiques de la maladie d'Alzheimer. Le deuxième chapitre présente les solutions actuelles, leurs limitations et les thèmes scientifiques adressés. Ce chapitre conclut avec les objectifs de nos travaux. Ensuite, le troisième chapitre présente la conception théorique du système pour être ensuite implémenté dans le chapitre 4. Le chapitre 5 développe les scénarios d'expérimentation menés dans les deux laboratoires et les résultats. Enfin, le document se termine par une conclusion détaillant les contributions de cette recherche ainsi que les pistes de recherches futures envisageables.

# Chapitre 1

# Les personnes déficientes

Ces travaux sont réalisés dans l'optique d'assister des personnes en situation de handicap cognitif. Dans ce chapitre, nous allons présenter les types de handicap qui existent et le public qu'on vise pour ces travaux. Ensuite, une présentation des dangers pour ce public vis-à-vis de l'activité de la préparation d'un repas est faite. Finalement, les défis sociétaux en sont dégagés.

L'article 2 de la loi française n°2005-102 du 11 février 2005 pour l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées définit le handicap comme suivant :

> *« Constitue un handicap, au sens de la présente loi, toute limitation d'activité ou restriction de participation à la vie en société subie dans son environnement par une personne en raison d'une altération substantielle, durable ou définitive d'une ou plusieurs fonctions physiques, sensorielles, mentales, cognitives ou psychiques, d'un polyhandicap ou d'un trouble de santé invalidant. »*

Une situation de handicap ne se définit pas seulement par les limites des capacités physiques ou cognitives d'un individu, mais cette situation est également influencée par l'environnement qui entoure l'individu [3]. Autrement dit, l'amélioration de l'environnement de la personne peut améliorer la situation de handicap de la personne. D'après l'Organisation Mondiale de la Santé (OMS) plus d'un milliard de personnes, soit environ 15% de la population mondiale, présente une forme de handicap [4]. Ces handicaps augmentent en raison du vieillissement de la population ainsi que l'augmentation des maladies chroniques. L'étendue des différents types de handicap est vaste et l'assistance doit être adaptée au type de handicap dont la personne est atteinte. Pour illustrer, une personne atteinte de la maladie d'Alzheimer n'a pas les mêmes besoins en termes d'assistance qu'une personne atteinte de troubles visuels. Le public visé par

ces travaux est constitué des personnes atteintes de la maladie d'Alzheimer. Cette maladie représente le plus grand nombre de patients dans la population.

Le handicap est vécu différemment selon la personne qui en est atteinte, l'assistance à apporter à cette personne doit alors être individuellement adaptée. Cette différence de handicap met en avant l'acceptabilité de notre solution par ce public. Dans ce sens, un modèle de développement humain a été développé [3] présentant le processus de production du handicap (PPH) (Figure 3). Ce PPH, permet de décrire la situation de handicap de la personne en considérant les facteurs personnels, environnementaux ainsi que ses habitudes de vie. Chacun de ces facteurs peut présenter des obstacles ou des incapacités pour la personne à cause de son handicap. Dans nos travaux, nous allons utiliser les concepts du PPH pour dresser un profil utilisateur tenant compte des facteurs personnels et environnementaux de la personne.

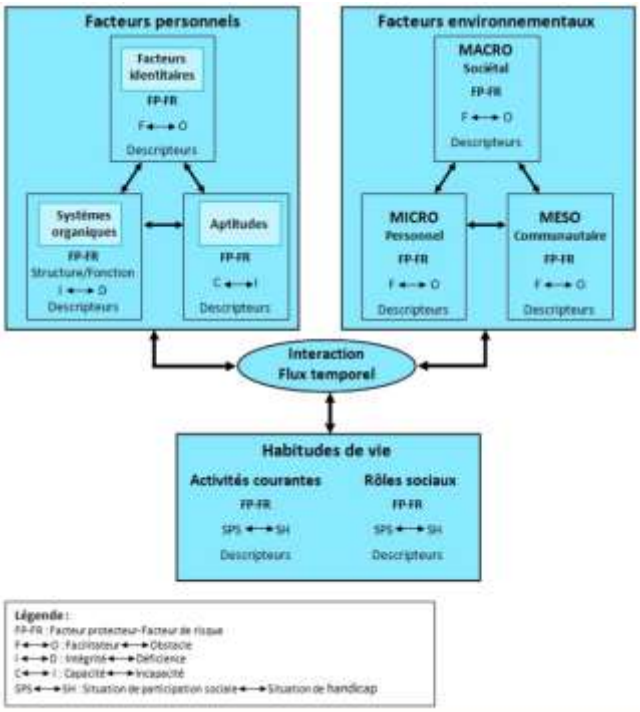



Figure 3 - Modèle de développement humain et Processus de production du handicap (PPH) [3].

## 1.1 La maladie d'Alzheimer

La maladie d'Alzheimer est une lente dégénérescence des neurones, elle est caractérisée par des troubles de la mémoire à court terme, des fonctions d'exécution et de l'orientation dans le temps et l'espace. Une personne atteinte de la maladie d'Alzheimer perd progressivement ses facultés cognitives et son autonomie. Cette maladie touche 35.6 million de personnes dans le monde en 2010 [5] et ce chiffre ne cesse de croitre : 46.8 millions en 2015 et estimé à 131.5 millions en 2050 [6]. Compte tenu de l'augmentation de l'espérance de vie, de plus en plus de personnes seront exposées à cette maladie [7]. Cette maladie se présente sous forme de plusieurs stades d'avancement : en partant du stade où la personne n'éprouve aucune difficulté dans la vie quotidienne, jusqu'au stade d'un déficit très grave. Ces différents stades constituent l'échelle de détérioration globale, également appelé l'échelle de Reisberg [8]. L'échelle de Reisberg est divisée en 7 stades.

### 1.1.1 Le stade léger

Le stade léger de la maladie d'Alzheimer est également appelé stade initial ou précoce. A ce stade, la personne conserve la plupart de ses capacités et n'a besoin que de peu d'aide. Sur l'échelle de Reisberg, cette étape de la maladie correspond aux stades 2 et 3 (le stade 1 correspond à pas de déficit). Ce stade se caractérise par de légères pertes de mémoire, de la difficulté à apprendre de nouvelles informations et de se concentrer et de légers problèmes d'orientation [9]. Lors de ce stade, la personne se rend compte de la maladie et peut devenir anxieuse pour son avenir.

### 1.1.2 Le stade modéré

Le stade modéré de la maladie d'Alzheimer, ou stade intermédiaire, correspond à une perte croissante des facultés cognitives et fonctionnelles de la personne. Une augmentation importante des soins est nécessaire et peut se traduire par un déménagement dans un centre spécialisé. Sur l'échelle de Reisberg, cette étape de la maladie d'Alzheimer correspond aux stades 4 et 5. Lors de ce stade, la personne subit des problèmes de mémoire plus prononcés,

elle est désorientée et a des difficultés pour se concentrer. Elle peut également ressentir des changements d'humeur tels que l'anxiété et la dépression ce qui peut provoquer un repli sur soi. Les capacités physiques sont également réduites et la personne a besoin d'une assistance pour des activités telles que s'habiller, s'alimenter ou se déplacer [10].

### 1.1.3 Le stade avancé

Le stade avancé, ou stade grave, se traduit par une aggravation des déficits cognitifs de la personne. Une personne atteinte de la maladie d'Alzheimer en stade avancé perd la capacité de se déplacer ou de faire une quelconque activité sans aide de la famille ou d'un aidant [11], elle a besoin d'une aide permanente.

## 1.2 Le public visé par ces travaux

Compte tenu de la situation de la personne atteinte de la maladie d'Alzheimer lors des différents stades, une assistance plus ou moins importante est nécessaire. Ces travaux visent particulièrement les personnes en stade modéré de la maladie d'Alzheimer car c'est lors de ce stade que le déménagement dans un centre spécialisé est le plus fréquent. Or, les habitats domotiques constituent une alternative intéressante au centre spécialisé. Les stades légers et sévères sont moins visés. D'une part, une personne en stade léger de la maladie d'Alzheimer a moins de difficultés à entreprendre en autonomie des activités et a donc besoin de moins d'assistance. D'autre part, le stade sévère implique une assistance telle qu'aucun système n'est capable de la fournir de nos jours. L'assistance par une personne physique reste nécessaire.

## 1.3 Les dangers liés à l'utilisation des appareils de cuisine

Les déficiences cognitives comme la maladie d'Alzheimer, une maladie où la mémoire est atteinte, a un impact important lors de l'utilisation de certains équipements d'un HIS. L'activité de la préparation d'un repas est une activité difficile pour les personnes atteintes de cette maladie, car il faut rester attentif sur plusieurs tâches en même temps, par exemple le temps et la température de la cuisson des aliments. Si par exemple, lors de la préparation d'un repas

chaud, la personne ne surveille pas sa poêle sur les plaques chauffantes de la cuisinière. L'huile dans cette poêle peut éclabousser et présenter un risque potentiel d'incendie dans la cuisine et mettre en danger les habitants. Ces oublis peuvent avoir de multiples causes : manque de concentration, un évènement externe (un appel d'un proche), etc... Il est important de réduire ces oublis et par conséquent les dangers.

## 1.4 Système déployable chez les résidents sur du matériel existant

Le système a pour vocation d'être installé chez les résidents. L'installation se fait sur les équipements de cuisine déjà présents dans leur environnement, ce qui représente deux avantages. D'une part, l'installation se fait au moindre coût pour le résident, il n'a nul besoin de se procurer de nouveaux appareils de cuisine pour bénéficier d'une sécurité accrue proposé par notre système. D'autre part, en gardant les équipements déjà présents, le résident garde son environnement habituel et ainsi ces habitudes d'usage de ces équipements. Le changement d'environnement peut déstabiliser voire désorienter une personne atteinte de maladies cognitives.

## 1.5 Défis sociétaux

Garder des personnes atteintes de handicaps cognitifs dans leur domicile domotisé pose plusieurs défis.

Dans un premier temps, ces personnes vivent rarement seules. Selon l'Institut de la Statistique du Québec [12], 55% des femmes et 70% des hommes âgés de plus de 70 ans vivent en couple. L'habitat domotisé doit être en mesure d'assister plusieurs personnes en simultané. Le handicap est vécu de manière unique par chaque personne qui en est atteinte, l'assistance doit être adaptée à leurs besoins.

| | |
|---|---|
| 1) | Comment fournir une assistance adaptée à des personnes, qui vivent dans un habitat intelligent pour la santé, atteintes de la maladie d'Alzheimer ou non, de façon continue et autonome, tout en tenant compte de leur profil médical ? |

Ensuite, les domiciles domotisés sont des habitats dans lesquels sont installés une multitude d'appareils électroniques intelligents et connectés permettant l'observation et l'assistance des occupants. De plus en plus, ces appareils se connectent sur des réseaux sans fil automatiquement, la plupart du temps à l'insu des habitants. L'habitat domotique doit en permanence gérer les équipements qui se connectent / déconnectent dynamiquement au sein de l'habitat et fournir les services en fonction de leur disponibilité. Ces équipements ont une durée de vie limitée. Ce qui implique que ces équipements peuvent tomber en panne et doivent être remplacés.

| | |
|---|---|
| 2) | Comment tenir compte de l'arrivée et de la disparition des équipements dans un habitat intelligent pour la santé et les utiliser pour mieux assister les habitants ? Comment gérer les défaillances qui peuvent surgir à tout moment et continuellement proposer une qualité de service élevée ? |

De plus, certains équipements disponibles dans l'habitat peuvent représenter des dangers pour les utilisateurs s'ils sont mal utilisés. Il faudra donc s'assurer que ces appareils disposent de suffisamment de connaissances pour réduire au minimum les risques liés à leur utilisation et assurer une sécurité optimale.

| | |
|---|---|
| 3) | Comment tenir compte des risques liés à l'utilisation de certains équipements et assurer la sécurité ? |

Finalement, le système a pour vocation d'être déployé chez les résidents, qui, chacun, ont un environnement unique avec des appareils électroménagers différents.

| | |
|---|---|
| 4) | Comment assurer le fonctionnement et le déploiement du système sur des équipements hétérogènes présents chez les résidents ? |

## 1.6 Conclusion

La maladie d'Alzheimer est la maladie cognitive qui touche le plus grand nombre de personnes et le nombre de personnes qui en sont atteintes ne cesse de croître. Ces travaux visent à assister ces personnes lors de leurs activités de la vie quotidienne. Des personnes atteintes d'autres types de handicap pourraient également bénéficier de ces travaux à condition d'avoir les capacités physiques et cognitives suffisantes. La réalisation d'une activité de la vie quotidienne complexe telle que la préparation d'un repas propose son lot de difficultés pour des personnes déficientes. Dans le chapitre suivant, on va observer comment d'autres travaux de recherche ont pu adresser ces difficultés.

# Chapitre 2

# Etat de l'art

Pour adresser les défis présentés dans le chapitre précédent, nous allons étudier plusieurs thèmes scientifiques à notre disposition, notamment l'informatique omniprésente, la personnalisation, la sensibilité au contexte, l'informatique autonome et la sécurité dans les habitats intelligents:

- L'informatique omniprésente permet d'obtenir des informations sur l'environnement en utilisant les réseaux de capteurs. Ce thème semble intéressant car ces travaux utiliseront un ensemble de capteurs pour récolter des informations de son environnement. Ce thème est détaillé dans la partie 2.1.

- La personnalisation des services permet d'adapter un système par rapport aux usagers qui s'en servent. Notre système doit s'adapter automatiquement aux besoins et aux capacités des usagers (partie 2.2).

- La sensibilité au contexte permet d'avoir un système qui s'adapte en fonction des évolutions de l'environnement. Dans un environnement domotique, l'environnement évolue sans cesse et de façon imprévisible (partie 2.3).

- L'informatique autonome permet au système d'évoluer tout seul sans l'intervention d'un humain. Étant donné que le système évoluera dans un environnement où il n'y aura pas de techniciens disponibles pour intervenir rapidement, il devra s'adapter aux changements de l'environnement, en particulier pour être robuste face à des pannes et être fiable (partie 2.4).

- Les Systèmes-Multi-Agents (SMA) sont une application de l'informatique autonome. Ces SMA peuvent présenter des intérêts pour nos travaux par leur flexibilité de déploiement (partie 2.5).

- La sécurité dans les habitats. Notre système doit assurer la sécurité lors de la préparation d'un repas (partie 2.6).

Cette liste de thèmes scientifique étudiés sera complétée par une présentation des objectifs de ces travaux. L'objectif de ces travaux est de réaliser un système de sécurité autonome lors de la préparation d'un repas. C'est-à-dire, réaliser un système qui gère ses actions lui-même et permet une utilisation en toute sécurité d'équipements ayant un danger potentiel d'utilisation pour des personnes atteintes de troubles de mémoire. L'utilisation du système sera modifiable en fonction du profil médical de la personne et ses contraintes (heures d'utilisation, nombre d'équipements disponibles, capacités cognitives). Ce système s'adapte aux évolutions et fonctionne de façon autonome dans l'environnement. Pour cela, dans ce chapitre, nous allons développer les différents thèmes scientifiques et montrer en quoi ils sont essentiels pour ces travaux.

## 2.1 L'informatique omniprésente pour le suivi des informations

L'informatique a connu plusieurs ères au cours de l'histoire. Partant d'une machine puissante utilisée collectivement par plusieurs personnes, vers l'ère où chaque personne dispose d'une multitude de petits appareils informatiques [13]. C'est ce qu'on appelle l'ère de l'informatique omniprésente ou *pervasive computing*. Dans un environnement domotique, l'HIS est constitué d'un ensemble de petits appareils informatiques tels que le téléphone portable, l'ordinateur, la télévision etc. mais également d'appareils intelligents moins visibles tels que des capteurs de présence, de température, etc. Tous ces appareils peuvent communiquer entre eux à travers des réseaux hétérogènes (bus domotiques, réseaux sans fil). L'informatique omniprésente a l'avantage d'être quasiment invisible dans un HIS, c'est-à-dire qu'un habitant n'a pas conscience de la technologie qui l'entoure et qui devient complètement transparente pour lui.

C’est par conséquent une solution très peu intrusive pour les occupants et qui leur permet de se sentir dans un environnement sécurisé et connu [14]. L’intelligence ambiante est l’ère informatique suivant l’ère de l’informatique omniprésente. Elle se caractérise par l’utilisation de l’informatique omniprésente pour servir les personnes. L’intelligence ambiante [15] peut être appréhendée sous quatre aspects :

- L’ubiquité, la capacité pour l’utilisateur d’interagir avec le système depuis une multitude d’appareils différents.
- La sensibilité au contexte, la faculté du système à analyser le contexte.
- L’interaction naturelle, la possibilité de l’utilisateur à interagir avec le système le plus naturellement possible, et si possible, en utilisant plusieurs sens (toucher, vue, sonore).
- L’intelligence du système, la faculté de s’adapter dynamiquement au contexte avec les analyses.

Ces quatre aspects permettent aux personnes d’utiliser leur environnement de façon intuitive et transparente.

L’inconvénient de l’informatique omniprésente est l’utilisation de la bande passante des réseaux. La sophistication des environnements augmente la quantité d’interactions entre les appareils et alourdit l’utilisation de la bande passante des réseaux [16]. Une solution est de prendre en considération seulement ce qui entoure les occupants et non l’ensemble de l’infrastructure de l’habitat, ainsi les communications demeurent moins nombreuses et le plus locales possibles. L’objectif de nos travaux est d’utiliser l’informatique omniprésente pour gérer la sécurité des résidents. C’est-à-dire de fournir à l’habitant une sécurité accrue via l’utilisation d’un réseau de capteurs.

Nos travaux vont utiliser un réseau de capteurs pour avoir une connaissance de l'environnement. Cet ensemble de capteurs enfouis dans l'environnement fournira des données, le système devra ensuite les analyser en fonction des personnes présentes dans l'environnement.

## 2.2 La personnalisation des services

Chaque handicap est vécu de façon unique par la personne qui en est atteinte, une assistance personnalisée est de mise. L'utilisation des équipements est personnalisable selon trois axes [17]:

- La personnalisation selon le profil médical de la personne. Cette personnalisation permet d'adapter le niveau d'assistance nécessaire pour que la personne puisse réaliser ses activités sans difficultés. Le profil médical permet également d'interdire ou de limiter l'accès à certains équipements pour la sécurité de la personne. Par exemple, limiter l'utilisation seulement à une seule plaque chauffante pour que la personne puisse se concentrer sur une activité à la fois.

- La personnalisation selon les préférences de la personne. Par exemple, la personne peut avoir une préférence pour des rappels visuels plutôt que sonores.

- La personnalisation selon le contexte. En fonction de la localisation de la personne, l'heure de la journée et les ressources disponibles, le fonctionnement du système sera impacté.

La difficulté liée à la personnalisation réside dans le fait qu'il faut identifier la personne. Identifier deux personnes dans une même pièce est une tâche difficile. La solution la plus simple serait que les personnes emportent avec eux une balise unique (sous forme de bracelet par exemple) [18], mais non adaptée dans le cadre d'un habitat domotique avec des personnes atteintes de déficiences cognitives. D'une part cette solution pourrait être intrusive, la personne

remarquerait la balise. D'autre part, la personne pourrait oublier de porter la balise et elle deviendrait invisible pour l'habitat. D'autres moyens de détection de la personne existent, tels que les tapis de sol actifs qui détectent une pression [19, 20]. Cependant ces tapis peuvent être imprécis lorsqu'il y a plusieurs personnes proches les unes des autres ; il faudra alors des moyens supplémentaires pour différencier plusieurs personnes. L'association de caméras aux tapis de sol actifs permet de différencier plusieurs personnes lorsqu'elles sont proches [21], mais c'est une solution intrusive et pas forcément acceptée par les habitants. De plus, ces tapis représentent également un coût élevé lorsqu'il faut couvrir une surface importante de l'habitat.

Les différentes solutions proposées sont soit intrusives, soit ne permettent pas de dissocier plusieurs personnes proches les unes des autres. Une solution serait d'utiliser un appareil mobile de la personne comme balise, d'une manière semblable à ce que propose [18]. Cependant, lorsque la personne oublie d'apporter l'appareil mobile avec elle, elle n'aura pas accès à l'interface du système. Sans cette interface, la personne ne pourra pas accéder à ses services.

La technologie RFID (Radio Frequency IDentification) permet de localiser une personne via une étiquette RFID à une distance relativement faible (jusqu'à quelques mètres). La personne peut ainsi s'identifier et utiliser le système. L'avantage de cette technologie est son coût très bas et sa facilité de mise en place. En effet, son fonctionnement nécessite seulement une étiquette unique pour identifier la personne ainsi qu'une antenne RFID. Cependant, l'utilisation d'étiquettes RFID revient aux problèmes d'oubli par la personne. Pour résoudre cette problématique, ces étiquettes peuvent être attachées avec un fil pour éviter tout risque de perte.

Notre système utilisera les trois niveaux de personnalisation afin de s'adapter au mieux aux personnes qui vont l'utiliser. Le système devra s'adapter au profil médical et aux préférences des personnes ainsi que le contexte dans lequel le système évolue. Le contexte, contrairement au profil médical et les préférences des personnes, est un élément qui évolue rapidement et de façon imprévisible.

## 2.3 La sensibilité au contexte

Pour cette raison, nous allons étudier la sensibilité au contexte. L'environnement est un facteur important car c'est lui qui demande une grande adaptabilité du système. Le contexte évolue continuellement et est imprévisible. De plus en plus d'équipements mobiles sont interconnectés en utilisant des réseaux sans fil. Ces équipements fonctionnent généralement avec des piles ou des batteries. Ces équipements mobiles se connectent et déconnectent en permanence au réseau domotique. Il est donc impossible de réaliser un système qui fonctionne correctement dans toutes les situations sans que ce dernier ne s'adapte à son contexte. C'est ce qu'on appelle « *context awareness* ». De tels systèmes peuvent régir selon des modèles basés sur le contexte en utilisant une boucle MAPE-K [22]. Cette boucle permet à un système de s'adapter automatiquement selon la configuration de l'environnement. Cette boucle est constituée de 5 parties (Figure 4):

- Monitor : Cette partie permet de surveiller l'environnement en utilisant les différents capteurs disponibles.
- Analyse : Les informations issues des capteurs sont analysées selon les modèles contextuels. Les analyses sont influencées par les configurations précédentes.
- Plan : L'analyse des informations peut provoquer un besoin d'un changement de configuration du système afin de s'adapter au mieux à l'évolution de l'environnement. Si une reconfiguration du système est nécessaire, le système planifie cette reconfiguration.
- Execute : Si cette nouvelle planification permet de mieux satisfaire les besoins des utilisateurs, elle sera exécutée en agissant sur les actionneurs dans l'environnement.

- Knowledge : Des données sont partagées entre les quatre parties précédentes, telles que les symptômes des reconfigurations et l'historique des configurations précédents. Cet ensemble constitue la connaissance du système.

Une fois que le système aura déployé sa nouvelle configuration, la boucle MAPE-K permet également de récupérer des informations de l'environnement. Cette boucle permet à un système de s'adapter selon le contexte de façon automatique. Nos travaux vont utiliser la boucle MAPE-K qui est assez représentative du fonctionnement d'adaptation des services. La boucle MAPE-K permettra aux services de s'adapter en permanence au contexte.

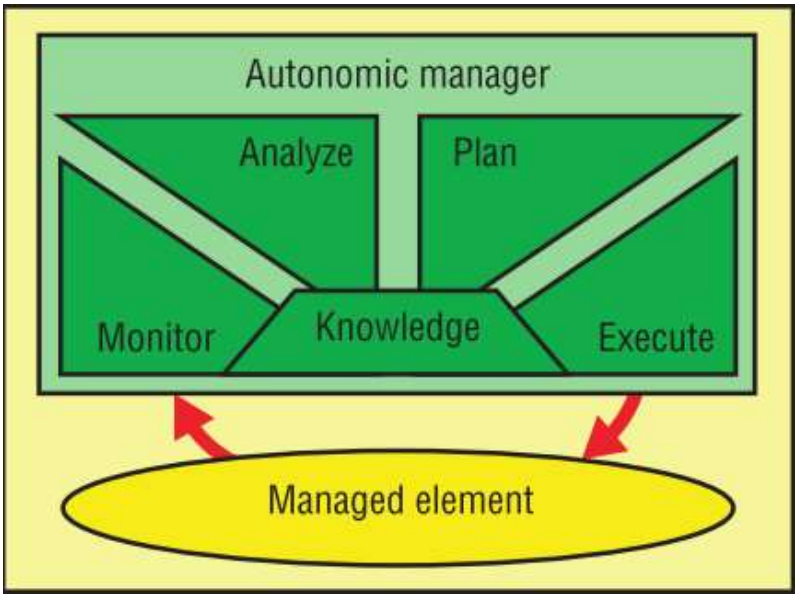



Figure 4 - L'architecture de la boucle MAPE-K [22].

En plus de devoir s'adapter au contexte, le système devra fonctionner dans un environnement où il n'y a aucune intervention rapide de la part d'un technicien. Le système doit être capable de se gérer en toute autonomie.

## 2.4 L'informatique autonome

Les systèmes informatiques devenant de plus en plus complexes et interconnectés avec d'autres applications et avec Internet, il devient alors très difficile, même pour un informaticien expérimenté, de configurer et d'améliorer ces systèmes complexes. L'informatique autonome est une vision d'un système informatique qui se veut complètement autonome et permet de prendre la relève des informaticiens. Il faut comparer l'informatique autonome à des fonctions vitales du corps humain tels que les battements de cœur ou la régulation de la température corporelle. Ces fonctions sont bien présentes dans chacun de nous mais notre cerveau nous épargne de nous en soucier. Ces fonctions, biens que vitales, sont autonomes. Dans ce cadre de ces travaux, le système devra évoluer de façon autonome dans l'habitat intelligent en considérant qu'un informaticien ne sera pas présent pour entretenir le système.

L'objectif de l'informatique autonome dans le cadre des serveurs est de pallier aux difficultés que rencontrent les informaticiens tels que la configuration, l'optimisation et l'entretien. L'essence même de l'informatique autonome est l'autogestion ou « s*elf-management* » [23]. L'objectif de l'autogestion est de libérer les administrateurs de systèmes des détails et de leur fournir un système qui fonctionne de façon optimale en permanence. Dans le cadre de la domotique, l'informatique autonome est nécessaire pour qu'un système puisse fonctionner longtemps sans intervention humaine. Le système fonctionnera dans un environnement en absence de techniciens pour entretenir l'ensemble, cet entretien doit alors être effectué par le système lui-même. L'autogestion est constituée de 4 parties qui sont nécessaires pour qu'un système puisse être considéré comme autonome :

- L'auto-configuration ou « *self-configuration* ».
- L'auto-optimisation ou « *self-optimization* ».
- L'autoréparation ou « *self-healing* ».

- L’autoprotection ou « *self-protection* ».

### 2.4.1 L’auto-configuration

Sur des systèmes classiques, les informaticiens doivent installer des modules, configurer les paramètres et intégrer des éléments manuellement, ce qui peut être coûteux en termes de temps et de ressources humaines. Les systèmes autonomes sont capables de se configurer automatiquement et de s’intégrer dans un méta-système pour que d’autres systèmes autonomes puissent s’adapter à leur présence. Lorsqu’un nouvel élément est introduit dans le système, il est automatiquement reconnu et le reste du système s’adapte à sa présence.

Dans le domaine de la domotique, c’est un aspect très intéressant lorsqu’on introduit de nouveaux appareils dans un habitat. Un système de découverte intègrera alors automatiquement ces nouveaux appareils et pourra selon la nature des éléments proposer de nouveaux services aux habitants. Un exemple d’utilisation de l’auto-configuration est dans la connexion sécurisée d’appareils à Internet dans un domicile domotisé. La configuration se fait avec une notion de confiance [24].

### 2.4.2 L’auto-optimisation

Les informaticiens doivent configurer les systèmes complexes manuellement, ce qui est souvent au détriment des performances des autres systèmes connectés. Cela peut engendrer des performances globales médiocres, souvent proches de l’élément le moins performant. Un système autonome cherche à optimiser les paramètres de chaque élément pour obtenir les meilleures performances globales.

En domotique, l’optimisation s’exprime dans le choix des capteurs et actionneurs pour réaliser un service donné. Le choix des capteurs dépend de plusieurs critères : Si, par exemple, un service de régulation de température ambiante est activé dans le salon d’un habitat intelligent, l’information du capteur de température du salon est plus pertinente que celle des capteurs de température des autres pièces. La position du capteur a donc une importance. Si l’on dispose

de beaucoup de capteurs dans une pièce, la fiabilité de l'information sera probablement plus importante. Les capteurs deviennent de plus en plus mobiles (Z-Wave, Zigbee, etc.) et cela facilite leur implantation dans un habitat intelligent. Les réseaux de capteurs sans fil (WSN : Wireless Sensor Networks) ont l'avantage de ne pas nécessiter de travaux dans la maison pour leur mise en place. Ces équipements sont composés d'un capteur et d'un émetteur pour transmettre le signal. Ces capteurs disposent d'une source d'alimentation limitée, généralement une batterie ou une pile, qui influence grandement la portée de l'émetteur et la durée de vie de fonctionnement du capteur [25]. Ces capteurs disposent de peu de puissance de calcul pour préserver la batterie et ne peuvent pas fournir de services complexes. De plus, la bande passante est plus faible dans les réseaux sans fil [26]. Il devient alors nécessaire d'optimiser l'utilisation des capteurs afin de préserver la batterie ainsi que la bande passante du réseau. En domotique, l'optimisation de la consommation d'électricité est un problème d'auto-optimisation [27].

### 2.4.3 L'autoréparation

Dans les systèmes classiques, les utilisateurs qui rencontrent des erreurs remontent l'information aux administrateurs du système. Souvent, l'information remontée est très vague car l'utilisateur n'est pas expert dans le domaine et n'a pas connaissance du fonctionnement interne du système. Retrouver l'origine de l'erreur et y remédier est une tâche très difficile pour un informaticien. L'autoréparation dans les systèmes autonomes a deux objectifs : 1) maintenir la santé du système et 2) maximiser son aptitude à survivre. L'autoréparation doit également détecter, diagnostiquer et récupérer les erreurs [28]:

- Détection : filtre les informations suspectes à partir des logs et établit un rapport à envoyer au diagnostic.
- Diagnostic : Analyse et calcule des plans de récupération basés sur des politiques (*policy based*).
- Récupération : Applique les adaptations planifiées.

Pour appliquer l'autoréparation dans le domaine de la domotique, une méthode possible de détection de panne est de tester par régression le système [23]. Cette méthode permet d'isoler un élément et de le tester en analysant ses données avec les données de log, ce qui sera très pratique dans un habitat intelligent pour pouvoir analyser une panne d'un capteur ou d'un actionneur. Si, par exemple, on dispose de plusieurs capteurs de température dans une pièce et que l'un d'entre eux relève une valeur très différente des mesures des autres capteurs, il peut être en panne [29]. Il est également envisageable d'analyser les données des capteurs via l'environnement et d'éliminer les données impossibles ou aberrantes. Par exemple, le système peut considérer une mesure de capteur de température d'une pièce de l'ordre de 100°C erronée car il est très improbable qu'il fasse réellement 100°C dans la pièce. Un autre exemple est qu'un capteur atteigne une valeur impossible, une valeur négative sur un capteur de luminosité.

Les données issues des capteurs sont différentes selon le modèle de capteur, la technologie utilisée, ou encore la marque. Lorsque le système ne reçoit pas d'informations du capteur, le problème peut se situer à une multitude d'endroits : le capteur, le système lui-même ou la connexion reliant les deux. Une fois que la panne a été localisée, une méthode afin de remédier aux pannes est d'associer les actions à effectuer avec les symptômes rencontrés [30]. Les pannes peuvent également se trouver à plus haut niveau, c'est-à-dire au niveau des services. Pour cela, il est possible d'utiliser un système de battement de cœur, ou *heartbeat*. Dans le protocole PSMP [31], chaque membre envoie un signal de battement de cœur. Si le destinataire ne reçoit pas ce signal d'un expéditeur durant un certain laps de temps, il pourra renvoyer un message d'alerte et finalement arrêter et redémarrer ce service. Il est très important d'éviter de redémarrer le système au complet. Le redémarrage au complet provoque une indisponibilité complète du système pendant un certain laps de temps. Le redémarrage d'un élément ne résout pas des problèmes de configuration, ni des problèmes matériels. Dans le cadre de nos travaux, un système de battement de cœur peut être utilisé pour vérifier l'état de fonctionnement de chaque composant du système.

### 2.4.4 L'autoprotection

Les systèmes autonomes se protègent de deux façons. D'une part, le système se défend dans son ensemble contre les attaques malveillantes externes. Par exemple en bloquant des connexions vers des éléments non connus. C'est très délicat à réaliser dans un habitat domotique où de nouveaux matériels peuvent se connecter à tout instant. En domotique, il est essentiel d'avoir de la sécurité au niveau de l'accessibilité des données. Les habitants ne sont généralement pas conscients des données récoltées et de leur portée. Ceci est encore plus vrai lorsqu'il s'agit d'appareils mobiles sans fil [32]. Ces appareils sont une cible très lucrative pour des développeurs de logiciels malveillants car elles contiennent énormément de données personnelles et peu protégées.

Une personne malveillante qui a accès aux équipements d'un habitat intelligent pourrait représenter un danger pour les habitants. Par exemple, cette personne pourrait récolter des données personnelles (les heures de présence à domicile par exemple) et s'introduire dans l'habitat lorsque les résidents sont absents sans laisser de traces (porte forcée, fenêtres brisées par exemple) en faisant croire au système qu'il est un habitant régulier (usurpation d'identité). Les données personnelles du HIS représentent les habitudes de la personne, elles reflètent la présence et les activités de la personne chez elle. En analysant ces données, une personne malveillante peut étudier ces données et planifier un cambriolage au moment où la personne est sortie de chez elle. L'autoprotection doit constater l'intrusion et l'empêcher d'avoir accès aux équipements et aux données de l'habitat.

### 2.4.5 Conclusion

Dans ces travaux, l'auto-configuration, l'auto-optimisation et l'autoréparation vont être mis en place pour permettre au système d'évoluer en toute autonomie le plus longtemps possible. Malgré que l'autoprotection soit un aspect très important en domotique, cette voie restera ouverte à des travaux futurs. L'informatique autonome permet également de rendre le système plus robuste et plus fiable.

## 2.5 Les systèmes Multi-Agents

Les systèmes multi agents (SMA) sont des systèmes autonomes. Ce sont des systèmes composés d'un ensemble d'éléments qui interagissent appelés *agents*. Ils bénéficient de l'autogestion de l'informatique autonome. En domotique, on peut utiliser un SMA en tant que système autonome, permettant de s'adapter à son contexte et proposer des services aux habitants. Avec une architecture orientée services, chaque agent remplit une ou plusieurs fonctions.

### 2.5.1 Les croyances, désirs et intentions

Un modèle d'architecture répandu est le modèle des croyances, désirs et intentions (BDI : Beliefs, Desires, Intentions) [33] (Figure 5). Un agent a des croyances, c'est ce qu'il connait de l'environnement via les données issues des capteurs. Il a également des désirs, les objectifs qu'il souhaite atteindre. L'agent interprète ces informations et planifie ses intentions, c'est-à-dire qu'il agit sur l'environnement. Le fonctionnement du BDI est semblable au fonctionnement de la boucle MAPE-K, c'est-à-dire qu'il y a pour ces deux modèles une partie de perception de l'environnement, de traitement des informations, puis une action sur l'environnement. Ce rapprochement entre la boucle MAPE-K et le BDI fait qu'un agent, représentant d'un service, pourra s'adapter au contexte et se configurer au besoin des utilisateurs.

Les SMA ont deux particularités par rapport aux systèmes autonomes. D'abord les agents sont des entités autonomes qui décident d'elles-mêmes de quoi elles ont besoin pour atteindre leurs objectifs. Ensuite les agents peuvent interagir entre eux, non seulement en échangeant des informations, mais en engageant un dialogue de plus haut niveau comme le font des humains : coopération, coordination et négociation [34].

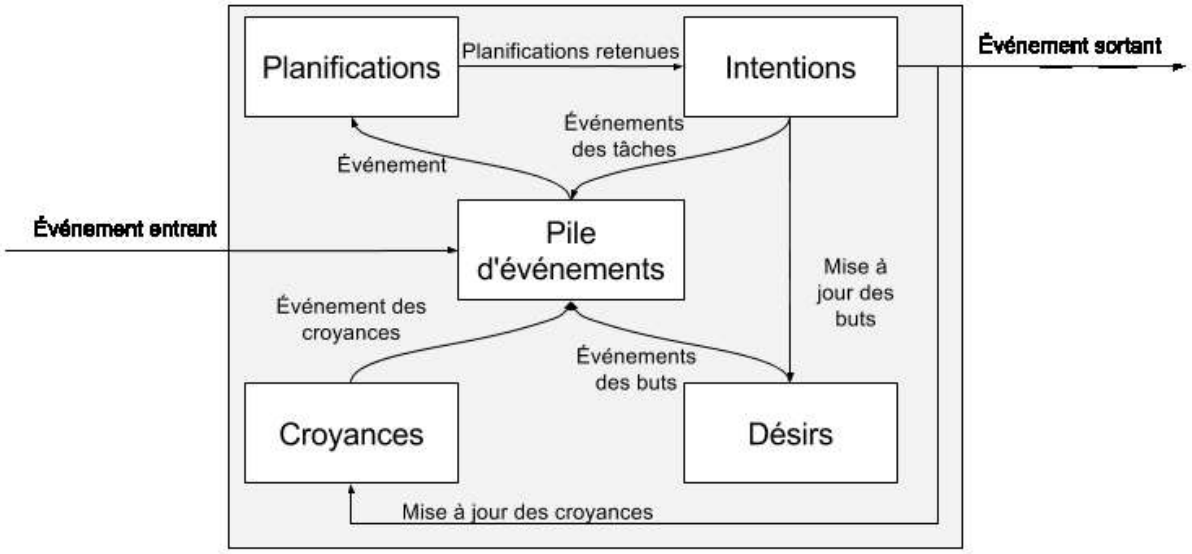



Figure 5 - Le modèle BDI d'un agent [33].

### 2.5.2 La communication entre agents

Le standard FIPA définit les protocoles de communication entre agents (FIPA-ACL : FIPA Agent Communication Language) [35] et des protocoles des actes de communication (FIPA-CA : FIPA Communicative Acts) [36]. Un acte de communication correspond à l'intention qu'un agent A veut transmettre à un agent B, dans le but de modifier les croyances de l'agent B. FIPA-ACL propose 20 performatifs permettant de définir l'intention d'un message. Par , un agent peut : informer, proposer, refuser, demander etc. [34]. Ces communications et dialogues de haut niveau sont nécessaires pour que les agents atteignent leurs buts. Un agent n'a pas forcément la connaissance nécessaire pour atteindre ses buts, il fait alors appel aux autres agents pour l'aider. Pour cela, il existe différentes organisations d'agents pour connaitre quels agents sont susceptibles d'aider.

### 2.5.3 Les différentes organisations entre agents

La communication entre agents est influencée par l'organisation du SMA. L'organisation d'un SMA peut être comparée à l'organisation d'une entreprise, où chaque acteur a un rôle, des relations et une autorité sur les autres acteurs. Il existe un ensemble d'organisations différentes pour les systèmes multi agents [37] (Tableau 1). Dans cette partie, nous allons présenter les organisations suivantes : hiérarchie, holarchie, coalition, équipe, congrégation, société, fédération, marché, matrice et composition.

#### 2.5.3.1 Hiérarchie

Une organisation en hiérarchie est comparable à un arbre, ou chaque nœud représente un agent. Les agents peuvent communiquer seulement avec les agents connectés dans la même branche. Chaque couche d'agent fonctionne comme un filtre, plus on monte dans la hiérarchie, plus l'agent a une connaissance globale du SMA. Cette structure est facile à mettre en place mais peut être fragile si l'agent au sommet ralentit l'ensemble du SMA ou cesse de fonctionner, évènement qui peut arriver lorsque tous les agents des niveaux inférieurs lui envoient des données simultanément. Dans le monde animalier, cette organisation peut se retrouver chez les lions ou les loups. MavHome [38] est un projet qui utilise un SMA avec une organisation hiérarchique pour rendre les services à l'utilisateur. Chaque agent dans ce SMA a une organisation similaire et contient une partie décisionnelle, une base de données et une partie permettant de communiquer avec la partie hiérarchiquement inférieure (un équipement ou un agent). L'inconvénient de ce système est la réponse du système lorsque la décision vient d'un agent au sommet de la hiérarchie, l'information doit d'abord traverser un ensemble d'agents avant de prendre effet sur un équipement.

#### 2.5.3.2 Holarchie

Une organisation holarchique peut être comparée à un groupement de hiérarchies. Par analogie, on peut imaginer que dans l'univers, il y a un certain nombre de galaxies qui, à leur tour sont composées de systèmes solaires. Chaque groupement dans ces systèmes est distinct des autres membres du groupe du niveau supérieur. Par analogie, chaque galaxie est distincte, mais est

composée des mêmes éléments. De plus, chaque galaxie est un élément constituant l'univers. Chaque groupement peut fonctionner de façon autonome. Les différents membres d'un groupement peuvent communiquer entre eux et les différents groupements également. Dans l'industrie, en particulier dans la fabrication, une organisation d'agents en holarchie est adaptée pour l'optimisation de la chaine de fabrication [39]. Chaque holarchie est autonome dans ses décisions et sa planification mais peut coopérer avec d'autres holarchies pour atteindre leurs objectifs. L'avantage des holarchies est leur robustesse et leur aptitude à coopérer. Cependant cette organisation a besoin d'une certaine répétition dans l'architecture, qu'on retrouve difficilement en domotique. Cette organisation n'est pas utilisée dans ce domaine.

#### 2.5.3.3 Coalition

Une coalition est un groupement d'agents qui ont les mêmes objectifs. Une fois les objectifs atteints, la coalition se dissout. La durée de vie d'une coalition est généralement courte. Un agent peut faire partie de plusieurs coalitions, ou plusieurs coalitions peuvent être liées lorsque leurs objectifs dépendent les unes des autres. L'existence brève d'une coalition peut avoir des bénéfices sur le court terme, mais le coût de construction et de destruction des coalitions peut engendrer des performances médiocres sur le long terme. Ce type d'organisation est présent en robotique [40], dans le domaine de l'énergie [41, 42] ou encore en génétique [43].

#### 2.5.3.4 Équipe

Les équipes sont constituées d'un groupe d'agents comme les coalitions. Cependant une équipe est constituée pour maximiser le but commun des agents participants tandis qu'une coalition met en avant les objectifs individuels. Dans le monde animalier, on peut retrouver cette organisation chez les araignées, s'entraidant pour tisser une toile plus grande et avoir de meilleures chances d'attraper des proies. Dans une équipe, il peut y avoir une hiérarchie. Une équipe peut adresser des problèmes plus complexes, que les agents individuellement ne peuvent pas résoudre. Cependant il y a plus de communication entre agents dans une équipe que des agents individuels. On peut retrouver cette organisation d'agents dans les compétitions de robotique [44, 45] ou d'intelligence artificielle [46].

#### 2.5.3.5 Congrégation

Les congrégations sont similaires à des équipes ou coalitions. Cependant, les congrégations ont une durée de vie bien plus longue que ces deux autres groupements. Elles ont généralement aussi plusieurs objectifs, qui peuvent être différents pour chaque membre, mais elles partagent un savoir commun qui peut être bénéfique pour chacun. On peut retrouver ce type d'organisation dans la société humaine dans les différents départements d'une université par exemple, ou encore dans le monde animalier chez les alligators. Les agents peuvent entrer et sortir d'une congrégation dynamiquement, ce qui peut faciliter la découverte de nouveaux agents [47, 48].

#### 2.5.3.6 Société

Les sociétés d'agents ont été inspirées de sociétés biologiques, par exemple les sociétés de fourmis. Les différents membres d'une société n'ont pas forcément les mêmes objectifs, ni les mêmes capacités, mais sont tous soumis aux mêmes lois. Les agents d'une société peuvent communiquer les uns avec les autres. La difficulté dans l'élaboration d'une organisation en société réside dans la mise en place de lois communes. Les organisations en société des agents sont utilisées dans le domaine de la robotique, pour optimiser l'utilisation des différentes machines [49].

#### 2.5.3.7 Fédération

Dans les fédérations, les agents sont séparés en groupes. Un agent est le représentant d'un groupe. Les membres du groupe peuvent seulement communiquer avec le représentant de leur groupe, qui fait office d'intermédiaire pour communiquer avec les autres fédérations. Cet agent peut devenir un goulot d'étranglement lorsque les fédérations contiennent beaucoup d'agents. Le mécanisme développé par Zhang [50] utilise une organisation en fédération pour réaliser une plateforme portable entre différentes services nuagiques (ou *cloud computing*).

#### 2.5.3.8 Marché

Les marchés sont des organisations de type producteur-consommateur. Il existe donc un groupement de consommateurs autour de producteurs. Cette organisation est efficace lorsqu'il s'agit de trouver une solution optimale, par exemple, le remplissage d'un emploi du temps d'une personne. Les agents vont organiser les différentes activités selon leur durée, leur priorité et la date d'échéance. Wellman [51] utilise une organisation en marché pour réaliser un emploi du temps dans une usine. Un système de producteur-consommateur est mis en place dans lequel l'usine représente le producteur de l'emploi du temps et les agents représentent les consommateurs de l'emploi du temps via des tâches à réaliser. Ces tâches ont chacune un coût et une date butoir. L'ensemble doit négocier pour atteindre un coût minimum et respecter les dates butoirs. Cette organisation est souvent ouverte, des agents peuvent entrer dans cette organisation et participer tant qu'ils respectent les lois communes. Les marchés bénéficient de des certains avantages et inconvénients de l'organisation en sociétés, comme par exemple les lois, car ils constituent des organisations ouvertes.

#### 2.5.3.9 Matrices

Les matrices permettent d'avoir plusieurs agents hiérarchiquement supérieurs, contrairement aux structures hiérarchiques, qui n'ont qu'un seul. Ceci est fait dans le but d'éliminer l'inconvénient du goulot d'étranglement dans la communication des hiérarchies. L'organisation en matrice peut être utilisée dans les réseaux de capteurs [52].

#### 2.5.3.10 Organisation composée

Les organisations composées sont une combinaison des différentes organisations dont nous avons discutées. En combinant plusieurs organisations différentes il est possible de profiter des avantages de chacune. Cependant les inconvénients sont également cumulés. Des organisations comme les sociétés permettent de faciliter la création dynamique de marchés [53] ou des hiérarchies permettent la création de coalitions [54]. En modifiant les interactions entre agents, il est possible de changer l'organisation au cours du temps. Il existe des systèmes où l'organisation évolue au fil du temps, par exemple dans les réseaux informatiques [55, 56].

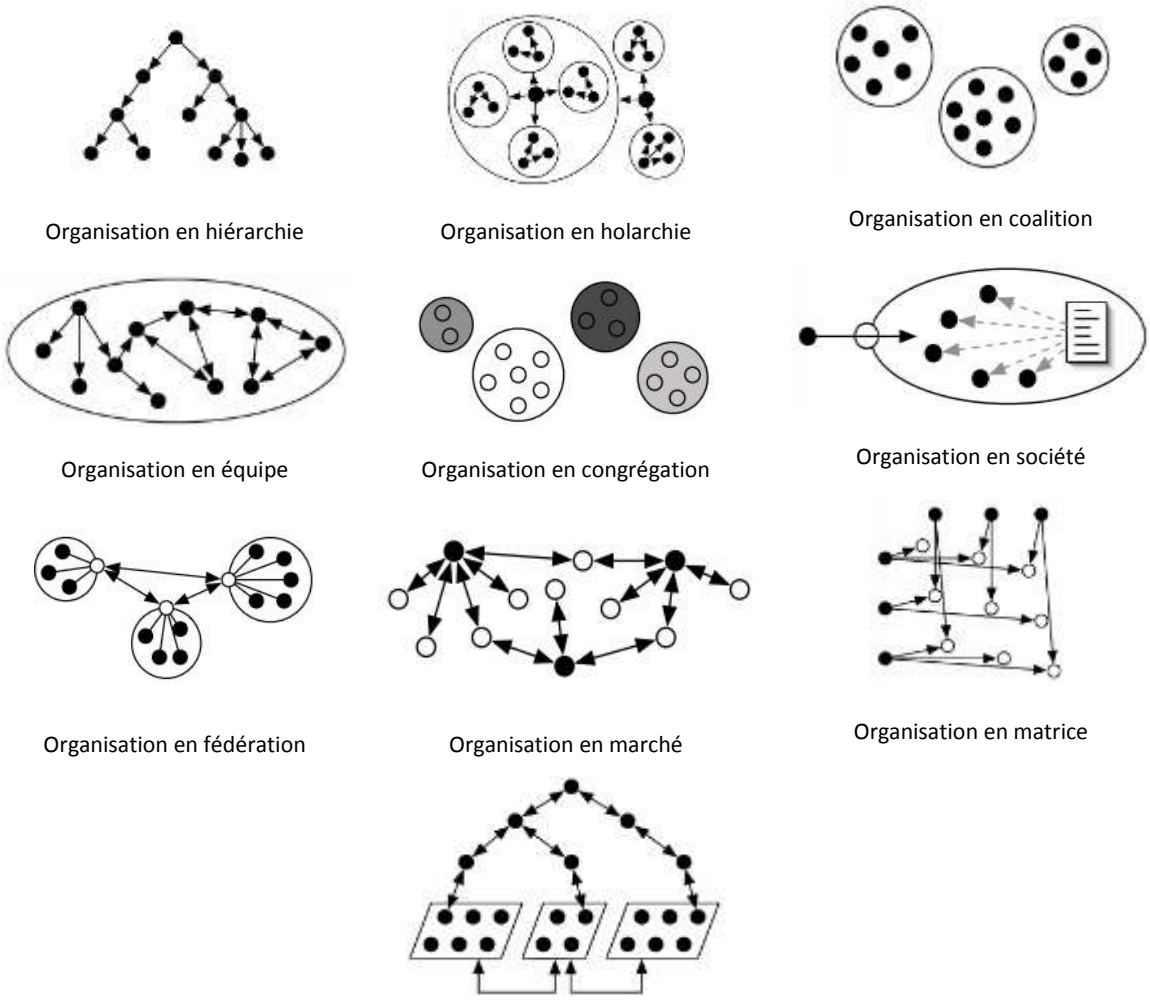



Figure 6 - Les différentes organisations d'agents

Le Tableau 1 récapitule les points forts et les inconvénients des différentes organisations présentées. La Figure 6 présente ces organisations sous forme de schéma permettant de les comprendre de manière visuelle.

Tableau 1 - Récapitulatif des différentes organisations des systèmes multi agents [37].

| Paradigme | Caractéristique clef | Avantages | Inconvénients |
|---|---|---|---|
| Hiérarchie | Décomposition | S'adapte facilement aux différents domaines; compatible avec les petites et grandes structures | Potentiellement fragile; peut être source de goulots d'étranglement |
| Holarchie | Décomposition et autonomie | Exploite l'autonomie des entités fonctionnelles | Les holons doivent être organisés; difficile de prévoir la performance |
| Coalition | Dynamique; dirigé par les objectifs | La force réside dans le nombre d'agents | Les bénéfices sur le court terme peuvent être annulés par les coûts de la mise en place de l'organisation |
| Équipe | Cohésion au niveau du groupe | Peut adresser des problèmes plus grands; centré sur les tâches | Communications plus nombreuses |
| Congrégation | Durée de vie longue; dirigé par les services | Facilite la découverte d'agents | L'organisation peut être trop restrictive |
| Société | Système ouvert | Des services publics; des conventions bien définies | Les agents potentiellement complexes peuvent avoir recours à des capacités additionnelles |
| Fédération | Agent représentant | Transactions, jumelage, services de traduction; | Les agents intermédiaires deviennent les goulots d'étranglement |
| Marché | Compétition via l'établissement des prix | Bon pour l'allocation; utilité accrue grâce à la centralisation; augmentation de l'équité dans les offres | Peut potentiellement être malveillant; la complexité de décision peut être élevée |
| Matrice | Plusieurs gestionnaires | Partage de ressources; les agents sont influençables par plusieurs autres agents | Potentiel de conflits; nécessaire de sophistiquer davantage les agents |
| Composé | Organisations concurrentes | Exploite l'avantage des organisations utilisées | Augmentation de la sophistication; Cumule les inconvénients des organisations utilisées |

Pour nos travaux, l'organisation doit être de longue durée, avec des objectifs variés (identifier l'utilisateur, surveiller les risques, etc.) mais garder un savoir commun (les informations contextuelles). Pour ces raisons, l'organisation retenue pour nos travaux est la congrégation. Ce type d'organisation groupe les agents qui ont les mêmes objectifs ensemble, ici les objectifs sont de rendre les services à la personne dans le même espace. De plus, la découverte de nouveaux agents est un aspect très utile qu'offrent les congrégations et répond à l'aspect dynamique et flexible que ces travaux demandent.

## 2.6 La sécurité dans les habitats intelligents pour la santé

Pour des personnes âgées atteintes de déficiences cognitives telles que la maladie d'Alzheimer, utiliser les équipements de la cuisine est un défi en soi. Pour cela, l'assistance lors de la préparation d'un repas est importante.

Dans la littérature, beaucoup d'articles concernent l'assistance à la personne pour l'élaboration des repas. Par exemple, Kranz [57] élaborent une planche à découper intelligente permettant de détecter le type d'aliment à découper. Pour cela, il utilise des capteurs de pression et des caméras pour détecter et identifier l'aliment. Une autre forme d'assistance pour l'élaboration de repas est proposée par Tsuji [58]. Dans ses travaux, la personne est en communication avec une autre personne distante. Ainsi, cette personne peut guider la personne dans l'élaboration de son repas au fur et à mesure. Certains travaux [59, 60] permettent de proposer des recettes sur une interface. Ces recettes sont disponibles sous forme de vidéos ou d'images. Dans la même voie, Mou [61] propose un catalogue de recettes, mais propose également une plateforme de partage sur laquelle les personnes peuvent partager des recettes. Certains travaux vont encore plus loin et traitent en plus l'aspect santé dans le choix des recettes [62]. Ce dernier indique lorsque la personne ajoute trop d'ingrédients gras ou caloriques dans sa recette. Chaque plaque chauffante est équipée d'un capteur de pression permettant de détecter l'ajout d'un ingrédient. La détection du type d'ingrédient se fait par caméra. D'autres travaux traitent l'aspect santé grâce à l'emballage du produit [63]. Plus spécifiquement, le système est intégré

dans un four à micro-ondes et permet d'identifier les produits via les codes-barres présents sur la plupart des produits alimentaires. Ce système récupère ensuite en ligne le type de cuisson adaptée et les risques allergènes associés à ce produit. Cependant, ces travaux ne correspondent pas au cadre de nos recherches. En effet, ces travaux se focalisent sur l'élaboration d'un repas en soi, et non sur les dangers liés à leur réalisation. Différents outils sont nécessaires et représentent des dangers. Par ailleurs, tous ces travaux ne sont pas axés sur des usagers ayant des déficiences cognitives.

Le public visé par nos travaux est constitué des personnes âgées atteintes de la maladie d'Alzheimer. Dans cette voie, des travaux comme Cook's Collage [64] ont été réalisés pour rappeler à la personne où elle en est resté dans l'élaboration de son repas. Cook's Collage affiche sur un écran les dernières activités de la personne dans la cuisine. De cette manière, une personne qui réalise plusieurs activités en même temps (faire à manger, répondre au téléphone etc.) garde trace de sa recette et a moins de risques d'oublier des ingrédients. Cette solution peut être utilisée pour l'élaboration d'un repas par une personne atteinte de la maladie d'Alzheimer, mais elle ne donne pas d'indications sur l'étape suivante de la recette à réaliser. De plus, la reconnaissance d'activités se fait à l'aide de caméras, qui sont des équipements intrusifs. Certains travaux [65] ont été réalisés pour assister la personne lors de la réalisation des AVQ simples comme par exemple préparer du café. Ces travaux sont axés sur une personne ayant des troubles de mémoire. La personne est guidée par un système vidéo qui capture l'avancement de l'activité.

Des études plus récentes sur la sécurité dans les habitats intelligents se focalisent plutôt sur la sécurité des données personnelles, notamment vis-à-vis des systèmes connectés à internet. Par exemple, Fernandes [66] a étudié plusieurs plateformes permettant de contrôler des équipements à domicile, en particulier SmartThings de Samsung [67]. Cette plateforme dispose de plusieurs centaines d'applications téléchargeables qui chacun peut contrôler un équipement. Un grand nombre de ces applications sont évènementiels, c'est-à-dire qu'ils réagissent selon des évènements produits dans l'environnement. Ces évènements peuvent être générés par des

sources externes malveillantes et compromettre l'usage et la sécurité de ces applications. La grande variété et hétérogénéité des appareils intelligents dans un habitat intelligent permettent à ces applications malveillantes d'attaquer de façons différentes. Ces attaques peuvent également venir de l'intérieur du domicile via des applications mobiles malveillantes installées à l'insu de la personne [68].

On peut remarquer que beaucoup de travaux assistent la personne lors de l'élaboration de son repas, mais rares sont les travaux traitant l'aspect de sécurité lors de la réalisation du repas. Peu de travaux intègrent la sécurité lors de la préparation du repas [69]. De plus, nous nous situons dans le cadre d'usagers âgés, atteints de déficiences cognitives, qui sont d'autant plus concernés par ces risques. Pour concrétiser ce que nous entendons par risques de sécurité, dans la partie suivante nous développons les règles de sécurité.

### 2.6.1 Les règles de sécurité

Les règles de sécurité permettent d'interrompre l'utilisation des appareils en cas de mauvaise utilisation [70]. Leur but premier est de protéger et d'assurer la sécurité des personnes. Nous choisissons d'utiliser des règles de sécurité par leur facilité de création et d'interprétation. Dans le cadre de nos travaux, nous reprenons quelques règles de sécurité élaborés par [70] car elles correspondent à nos objectifs. Voici la liste des conditions dangereuses qu'on considère :

1) Si une personne utilise le four et quitte l'environnement, quatre cas de figures se présentent. (1) Le four est à une température inférieure à 300°F, (2) le four est à une température comprise entre 300°F et 400°F, (3) le four est à une température supérieure à 400°F, (4) le mode grill est activé. La personne peut s'absenter pendant X minutes, avec X variable selon le cas de figure et selon le profil médical de la personne.

2) Si une personne quitte l'environnement pendant plus de X minutes lorsqu'un appareil est toujours actif.

3) Si une personne utilise le four mais laisse la porte ouverte pendant plus de X minutes.

4) Si le four est activé mais vide pendant plus de X minutes.

5) Si un foyer des plaques chauffantes est allumé mais qu'aucun ustensile ne se trouve dessus.

6) Si une personne utilise les plaques chauffantes mais qu'aucune personne n'est présente pendant plus de X minutes.

Si un des cas ci-dessus se présente, le système doit dans un premier temps avertir la personne qu'une condition est enfreinte et qu'il doit y remédier. S'il ne remédie pas dans le délai prévu, le système verrouille l'appareil pour réduire les risques envers les personnes. Ces conditions dangereuses sont prévues pour des personnes atteintes de TCC. Nous considérons que les symptômes de la maladie d'Alzheimer et TCC sont proches et que les règles de sécurité sont également valables pour le public visé par nos travaux. Pour faciliter la lecture de ces situations à risque, elles sont également dressées sous forme de schémas fonctionnels (Annexe A). L'objectif de ces travaux est de traduire ces situations dangereuses en règles de sécurité et de les appliquer.

## 2.7 Objectifs

Pour s'adresser aux défis sociétaux présentés à la fin du chapitre précédent, différents objectifs ont été dressés et adressés dans les parties suivantes. Pour rappel, les défis sociétaux sont :

- Fournir une assistance adaptée à des personnes, qui vivent dans un habitat intelligent pour la santé, atteintes de la maladie d'Alzheimer ou non, de façon continue et autonome, tout en tenant compte de leur profil médical.

- Tenir compte de l'arrivée et de la disparition des équipements dans un habitat intelligent pour la santé et les utiliser pour mieux assister les habitants. Gérer les défaillances qui peuvent surgir à tout moment et continuellement proposer une qualité de service élevée.

- Tenir compte des risques liés à l'utilisation de certains équipements et assurer la sécurité.

- Assurer le fonctionnement et le déploiement du système sur des équipements hétérogènes présents chez les résidents.

### 2.7.1 Le domicile multi-usager

L'étude de la personnalisation des services a permis de connaitre à quels niveaux le système peut s'adapter pour pallier aux handicaps des usagers. Nous allons développer un système capable de se personnaliser en fonction les trois axes proposées: 1) selon le profil médical de la personne, 2) ses préférences ainsi que 3) le contexte. L'identification de plusieurs personnes proches est une difficulté, mais nécessaire dans le cadre de nos travaux où plusieurs personnes peuvent préparer un repas ensemble. Pour surmonter cette difficulté, nous utiliserons des étiquettes RFID uniques représentant chaque personne. Ainsi, l'identification de plusieurs personnes proches est possible. Les profils utilisateur des usagers sont différents, le système doit être en mesure de pallier aux handicaps des uns sans contraindre l'usage du système pour les autres. Les objectifs pour ce défi sont :

- Réaliser un système personnalisable selon : le profil médical de la personne, ses préférences ainsi que le contexte.

- Pouvoir identifier plusieurs personnes.

- Dans le cas d'un usage multi-utilisateur, pallier aux handicaps des uns sans contraindre l'usage du système des autres.

### 2.7.2 L'évolution de l'environnement

Le système devra être dynamique en s'adaptant à son contexte, c'est-à-dire utiliser les différents capteurs disponibles à sa portée, y compris les équipements mobiles, pour pouvoir améliorer sa connaissance du contexte et adapter au mieux la sécurité. L'informatique omniprésente, la sensibilité au contexte et l'auto-configuration s'adaptent parfaitement pour cette problématique. Pour s'adapter à son contexte, le système utilisera une boucle MAPE-K. Cette boucle permet également, en plus de l'autoréparation, au système de s'adapter lorsque des capteurs tombent en panne. Pour limiter l'utilisation de la bande passante, nous choisissons d'utiliser seulement les capteurs présents dans les équipements et ceux présents dans les appareils mobiles. Ces derniers doivent s'intégrer automatiquement. Les appareils mobiles ont deux rôles : Enrichir la connaissance du contexte du système et permettre au système de communiquer via de nouvelles interfaces homme/machine. Les objectifs pour ce défi sont :

- Obtenir des informations contextuelles grâce à un réseau de capteurs.
- Intégrer automatiquement les capteurs venant d'appareils mobiles.
- S'adapter à son contexte en utilisant la boucle MAPE-K.
- Gérer les défaillances des capteurs.

### 2.7.3 La sécurité dans la cuisinière

Le système doit assurer la sécurité des usagers en tout temps en adoptant des règles de sécurité. Ces règles doivent s'adapter à la personne et à son profil médical. Pour ce défi, un ensemble de règles de sécurité a été défini. Les limites de ces règles de sécurité sont qu'ils ne considèrent pas tous les dangers liés à l'activité de la préparation d'un repas. Cependant, l'élaboration de ces règles simples constitue une première étape pour la sécurité. Par la suite, d'autres règles peuvent être ajoutées au système pour réduire davantage les risques. Les objectifs pour ce défi sont :

- Analyser l'activité de haut niveau et appliquer les règles de sécurité.
- Personnaliser les règles de sécurité selon les usagers.

### 2.7.4 Déploiement du système sur du matériel existant

Le système doit être adaptable et déployable sur du matériel existant dans le domicile des résidents. L'informatique autonome répond parfaitement à ce défi. L'aspect auto-configuration et auto-optimisation permettent au système d'être déployé dans un environnement variable. La flexibilité que propose l'organisation de la congrégation dans les SMA permet une adaptabilité facile sur n'importe quelle application. L'objectif lié à ce défi est :

- Déployer le système sur des applications différentes en utilisant une congrégation dans un SMA.

### 2.7.5 Conclusion

Pour réaliser les différents objectifs, une base nécessaire est la réalisation d'un intergiciel (ou *middleware*) permettant de faire le lien entre les équipements de la cuisinière et le verrouillage/déverrouillage de la cuisinière en passant par l'application des règles de sécurité. La personnalisation dépend de plusieurs paramètres : le profil médical de la personne, ses préférences et son contexte mais aussi l'utilisation de la cuisinière. Plusieurs personnes peuvent préparer un repas en même temps, le système doit être capable de gérer cet ensemble d'usagers. Ensuite, le système doit pouvoir s'adapter aux évolutions de l'environnement, qu'il s'agisse de la découverte de nouveaux capteurs ou au contraire de capteurs qui tombent en panne. Cette adaptation permet de fournir une surveillance personnalisée des risques de sécurité en tout temps lors de l'activité de la préparation d'un repas. Finalement, le système a pour vocation d'être déployé sur les appareils de cuisine dans les domiciles domotisés chez les résidents, dans ce cadre, le système doit être flexible et facilement déployable. Dans le chapitre suivant, nous allons présenter des modèles théoriques pour s'adresser à ces objectifs.

# Chapitre 3

# Modélisation du système de sécurité autonome

Dans ce chapitre, nous allons essayer d'apporter des réponses aux objectifs et questions scientifiques posés auparavant. Pour rappel, ces objectifs sont :

- Domicile multi-usager :
  - ♦ Réaliser un système personnalisable selon : le profil médical de la personne, ses préférences ainsi que le contexte.
  - ♦ Pouvoir identifier plusieurs personnes.
  - ♦ Dans le cas d'un usage multi-utilisateur, pallier aux handicaps des uns sans contraindre l'usage du système des autres.
- L'évolution de l'environnement
  - ♦ Obtenir des informations contextuelles grâce à un réseau de capteurs.
  - ♦ Intégrer automatiquement les capteurs venant d'appareils mobiles.
  - ♦ S'adapter à son contexte en utilisant la boucle MAPE-K.
  - ♦ Gérer les défaillances des capteurs.
- La sécurité dans la cuisinière :
  - ♦ Analyser l'activité de haut niveau et appliquer les règles de sécurité.

- ♦ Personnaliser les règles de sécurité selon les usagers.

- Déploiement :

  - ♦ Déployer le système sur des applications différentes en utilisant une congrégation dans un SMA.

Dans un premier temps, une solution est proposée permettant au système d'être utilisé par plusieurs personnes en simultané (3.1). Ensuite, les besoins de perception du système de l'environnement sont brièvement présentés (3.2). Ces connaissances du contexte permettent ensuite au système de superviser et réagir aux risques et dangers qui peuvent survenir lors de la préparation d'un repas (3.3). Finalement, une architecture est proposée pour structurer les composantes du système (3.4) et nous proposons une solution permettant d'homogénéiser la coopération homme/machine qui est présente dans nos travaux (3.5).

## 3.1 Le domicile multi-usager

Un habitat intelligent pour la santé peut être occupé par un ensemble de personnes différentes, ayant leur propre situation médicale. Ces personnes ont chacune des attentes et des utilisations des équipements qui leur sont propres. Pour cela, chaque personne qui souhaite utiliser les équipements se voit attribuer un profil utilisateur. La structure de chaque profil varie en fonction du rôle attribué à la personne (Figure 7) :

- Les personnes avec le déficit cognitif : Les personnes atteintes de la maladie d'Alzheimer.

- Les aidants professionnels : Les personnes qui assistent la personne ayant des déficits cognitifs au cours de sa maladie.

- Les membres de la famille qui vivent avec la personne déficiente. Les aidants naturels font partie de cette catégorie.

- Les techniciens d'entretiens qui viennent réparer ou mettre à jour l'installation du système dans la résidence.

- Toute autre personne pouvant rendre visite et aider la personne déficiente (voisin, amis, autres aidants naturels, etc.).

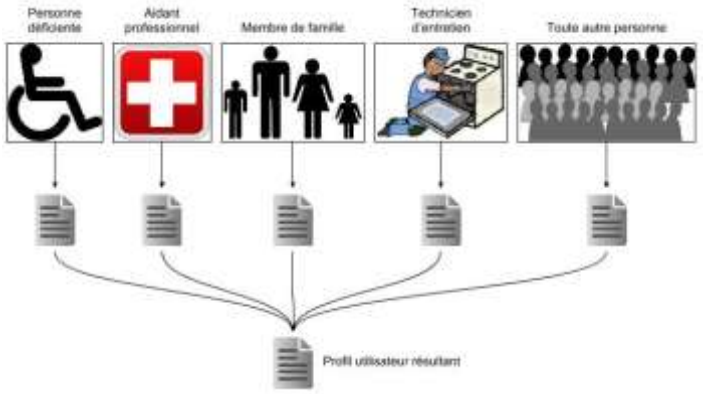



Figure 7 - Catégories de personnes considérées par nos travaux et leurs profils utilisateurs.

Les maladies cognitives ont un impact sur les fonctions exécutives. Par exemple, elles peuvent entraîner des déficits d'attention, les personnes ayant alors de la difficulté à se concentrer sur plusieurs tâches à la fois. De telles informations sont cruciales pour déterminer sur quoi l'assistance devrait se concentrer, quels comportements superviser et quelles règles de sécurité mettre en place. Le profil utilisateur devra contenir ces informations et bien d'autres. Voici un échantillon des informations qu'il devrait contenir :

- Des informations personnelles de l'utilisateur : son nom, son identifiant unique (adresse email), la capacité d'encadrement (détaillé un peu plus loin dans cette section) et une autorisation à déverrouiller les équipements.

- Des informations liées à l'utilisation du système : la durée que l'utilisateur peut s'absenter de l'environnement proche du four (par exemple répondre à un appel téléphonique), laisser la porte du four ouverte, laisser le four vide mais allumé, etc.

- Les paramètres de contraintes d'utilisation. Ces paramètres permettent de limiter l'usage des équipements par l'utilisateur sur deux volets : en capacité d'usage (les fonctionnalités des équipements que l'usager peut utiliser) et en temps (les créneaux horaires sur lesquels l'utilisateur a le droit d'utiliser les équipements).

Lorsque le système est utilisé par plusieurs personnes en simultané, c'est-à-dire lorsque plusieurs personnes préparent un repas, il garde en mémoire l'ensemble des personnes identifiées sur le système. Les profils utilisateurs de l'ensemble des personnes connectés sont fondus pour créer un profil utilisateur résultant (Figure 7). La génération de ce profil résultant relève plusieurs problématiques :

1) Cas de figure 1 : A et B ont des déficits cognitifs. Comment générer ce profil résultant ? Faut-il considérer le pire des cas pour chaque attribut des profils (Figure 8) ? Le meilleur des cas (Figure 9) ? Considérer le pire des cas signifie que l'ensemble des personnes sont un frein à l'activité pour chaque individu, que chaque personne est une source de distraction pour l'autre. Dans ce cas, on veut s'assurer qu'aucune situation dangereuse ne puisse survenir. Il se peut que dans certains cas de figure, aucun équipement n'est disponible pour les personnes identifiées. Si l'on considère le meilleur des cas, on considère que les personnes peuvent s'entraider pendant la préparation du repas.

2) Cas de figure 2 : A a des déficits cognitifs et B n'en a pas. Quel profil privilégier lorsqu'une personne non déficiente s'identifie au système ? Doit-t-elle subir les contraintes d'utilisation de la personne déficiente ?

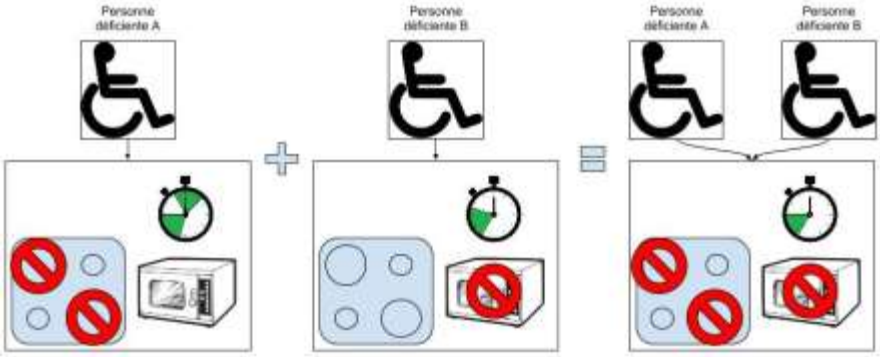



Figure 8 - Profil utilisateur résultant en prenant le pire des cas des contraintes d'utilisation. L'accès aux plaques chauffants, au four ainsi que les créneaux horaires y figurent.

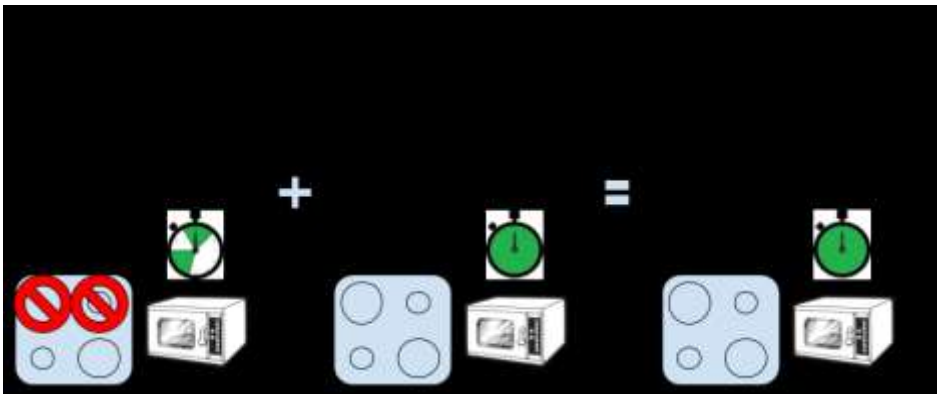


Figure 9 - Profil utilisateur résultant en prenant le meilleur des cas des contraintes d'utilisation. L'accès aux plaques chauffants, au four ainsi que les créneaux horaires y figurent.

On choisit de considérer pour ces deux cas : (1) Dans le cas où plusieurs personnes déficientes sont connectées au système, le profil résultant de l'ensemble de leurs profils représente le pire des cas (cas à gauche de la Figure 10). Ce choix a été retenu car elle est plus sécuritaire pour les usagers. (2) Lorsqu'une personne non-déficiente se connecte au système en plus d'une personne déficiente, elle n'a pas envie de subir les contraintes d'utilisation de la personne déficiente. Pour cela, nous introduisons le paramètre « capacité d'encadrement » dans les profils utilisateurs. Cette capacité est représentée par une valeur numérique entière et indique si la personne peut encadrer (signe positif) ou doit être encadrée par d'autres personnes (signe

négatif). La valeur numérique indique le nombre de personnes que la personne peut encadrer ou qui doivent être présentes pour encadrer. Par exemple, une valeur de « -1 » indique que la personne a besoin d'une personne accompagnatrice. Si la somme des capacités d'encadrement des personnes connectées est strictement négative, le système considère seulement les profils des personnes déficientes et génère un profil résultant sur le pire des cas. Si la somme des capacités d'encadrement est positive ou nulle, cela signifie qu'il y a suffisamment de personnes encadrantes pour les personnes déficientes, le système peut alors générer un profil résultant correspondant à un profil d'un encadrant (qui a généralement accès à l'ensemble des équipements) (cas de droite de la Figure 10).

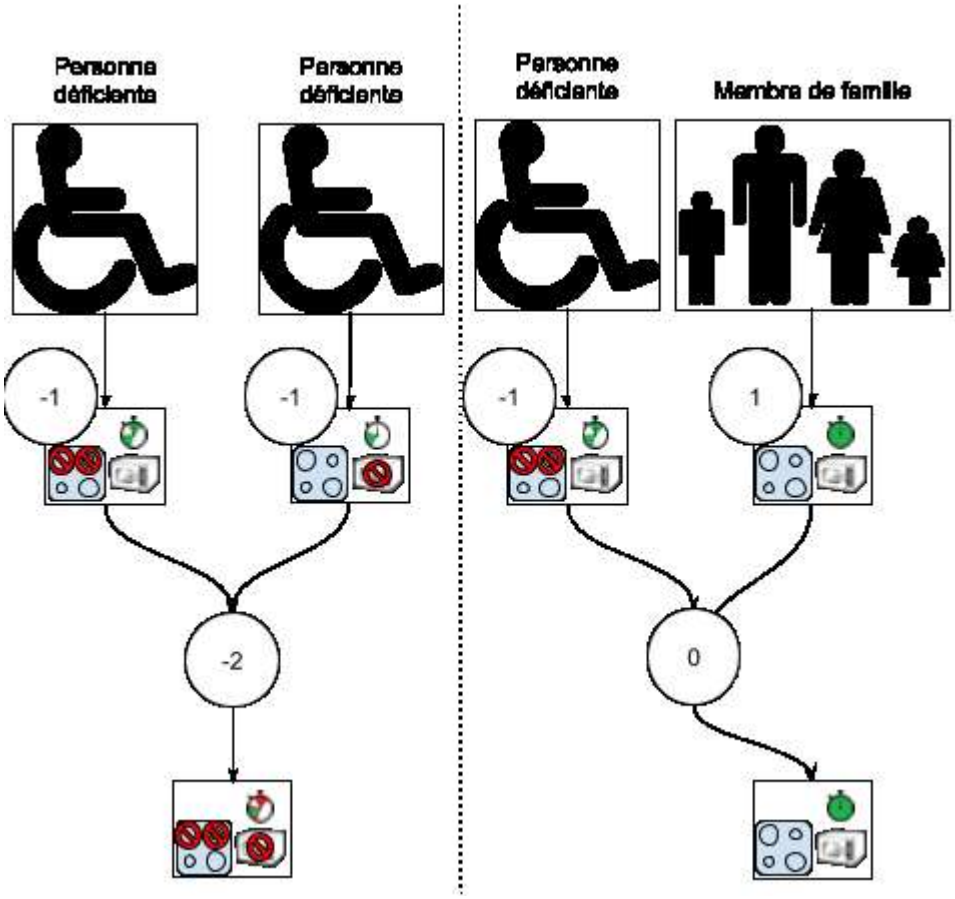



Figure 10 - Choix du profil résultant selon la catégorie de personnes connectées en utilisant la capacité d'encadrement.

## 3.2 L'environnement

Pour la réalisation de l'activité de la préparation d'un repas, ces personnes vont interagir avec des équipements dans un environnement communément appelé cuisine. Dans cet environnement, on considère deux types d'équipements. D'une part on retrouve les équipements de cuisine tels que la cuisinière et les plaques chauffantes. D'autre part, on considère les équipements mobiles comme une tablette tactile ou un téléphone intelligent dont la personne peut disposer. C'est à partir ces deux types d'équipements que notre système pourra fonctionner.

Dans cette section, nous allons développer les différentes parties constituant l'environnement du système : Les différents équipements sur lesquels il peut être implanté, les besoins du système en termes de capteurs et la hiérarchisation des données de ces capteurs.

### 3.2.1 Instrumentation

Les appareils sur lesquels le système peut être implanté sont typiquement les appareils permettant de préparer un repas. Sur ces équipements doivent être installés un ensemble de capteurs permettant au système d'avoir des informations contextuelles concernant les appareils et l'utilisateur.

- Un ensemble de capteurs doivent être enfouis dans l'environnement pour détecter et identifier des personnes dans la cuisine. Ces informations sont pertinentes pour personnaliser le système vis-à-vis du profil utilisateur. L'information de présence d'une personne est pertinente vis-à-vis des règles de sécurité.

- Le système doit avoir connaissance de l'activité des équipements. Un ensemble de capteurs permettent d'observer la température, l'activité électrique, la présence d'objets, la masse et l'état des différentes pièces mobiles des équipements (portes, tiroirs etc.).

Le système doit pouvoir interagir avec les utilisateurs pour être en mesure de les notifier de l'état de sécurité des équipements. Si l'état de sécurité l'exige, le système doit être capable de couper l'appareil en coupant son circuit électrique d'alimentation.

### 3.2.2 L'historisation des données

L'ensemble des données de capteurs recueillies doivent être stockées pendant un certain laps de temps pour être analysées. Ces données sont stockées par modules (Figure 11). Ces modules représentent des modules physiques sur lesquels les capteurs sont branchés. Un capteur peut appartenir à un seul module. Ce choix a été fait pour faciliter la recherche des capteurs en panne. Ainsi, si un capteur tombe en panne, le système est capable de localiser le branchement physique du capteur défaillant. Cela permet un remplacement aisé de ce capteur par un technicien.

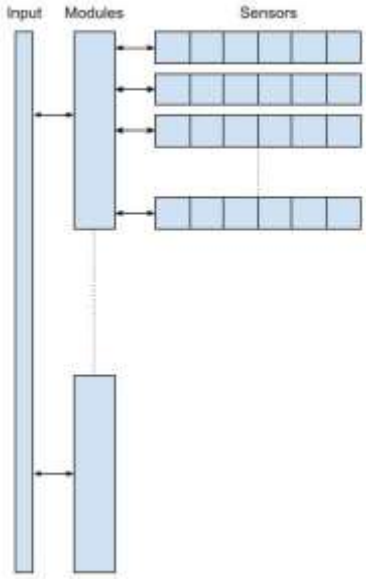



Figure 11 - Organisation des données des capteurs.

Chaque capteur dispose de plusieurs propriétés : un nom, un type, sa valeur etc. La valeur du capteur est enregistrée dans un tableau qui est mis à jour à chaque nouvelle lecture à la valeur du capteur. À chaque mise à jour, l'horodatage est accolé à cette valeur pour garder une trace de l'évolution des données du capteur. Une fois que ce tableau est rempli, une nouvelle donnée

remplace la donnée la plus ancienne. Ainsi on garde en mémoire la plus récente évolution du capteur. La longueur de ce tableau, et donc indirectement la durée de l'historique en mémoire, est variable et dépend des besoins pour analyser l'activité des équipements.

## 3.3 La sécurité pour les habitants et pour le domicile

L'activité de la préparation d'un repas nécessite généralement des équipements qui peuvent être dangereux ; chaleur, feu, éclaboussures peuvent, par manque d'attention et de précautions, blesser une personne.

En analysant l'activité des appareils et l'activité des utilisateurs, des situations à risque peuvent se présenter. Une manière d'exprimer ces risques est par la définition de règles de sécurité [70]. Ainsi, en observant les origines des risques, une règle de sécurité peut être associée à ce risque. Le système peut alors via cette règle observer les éléments déclencheurs et avertir les personnes avant qu'un danger ne surgisse.

Le public visé par ces travaux est les personnes âgées atteintes de déficiences cognitives. Les personnes qui souhaitent installer notre système de sécurité chez elles souhaitent continuer à utiliser leurs appareils dans leur cuisine. Dans cette optique, le système a été pensé de façon à ce qu'il s'adapte aux équipements déjà présents dans l'environnement de la personne, sans avoir besoin de les modifier. De la même manière, si la personne ne souhaite plus utiliser notre système, il pourra être ôté sans modifier les équipements existants. Ceci est fait pour que l'environnement de la personne reste identique après l'installation. Changer son environnement pourrait nuire à l'autonomie de la personne (elle pourrait se sentir égarée) et c'est aussi une solution beaucoup plus coûteuse.

## 3.4 Une architecture répartie pour assurer la sécurité lors de la préparation d'un repas

Une architecture de notre système, appelé StoveMAS, permet de lier les éléments ensemble (Figure 12). L'analyse de l'activité de l'utilisateur dans cette architecture est basée sur les différents profils utilisateurs. Dans l'ensemble, tout public peut utiliser le système, mais des profils particuliers ont été érigés pour correspondre aux mieux aux besoins des personnes atteintes de déficiences, des membres de famille qui cohabitent avec la personne atteinte, des aidants professionnels qui, entre-autres, suivent l'évolution de la personne atteinte ainsi que des techniciens qui font l'entretien du matériel. L'activité de l'utilisateur (mouvements) est analysée via les informations issues de différents capteurs et du profil utilisateur.

L'analyse de l'activité des équipements de cuisine et l'historisation se font par l'intermédiaire de l'acquisition des données qui elle-même repose sur l'instrumentation. L'analyse de l'activité matérielle correspond à une connaissance de haut niveau (états, utilisation) du système des équipements que le système surveille.

Ces deux activités (matérielle et usager) permettent au système d'être sensible au contexte et fournir les éléments nécessaires pour assurer la sécurité des personnes lors de la préparation du repas.

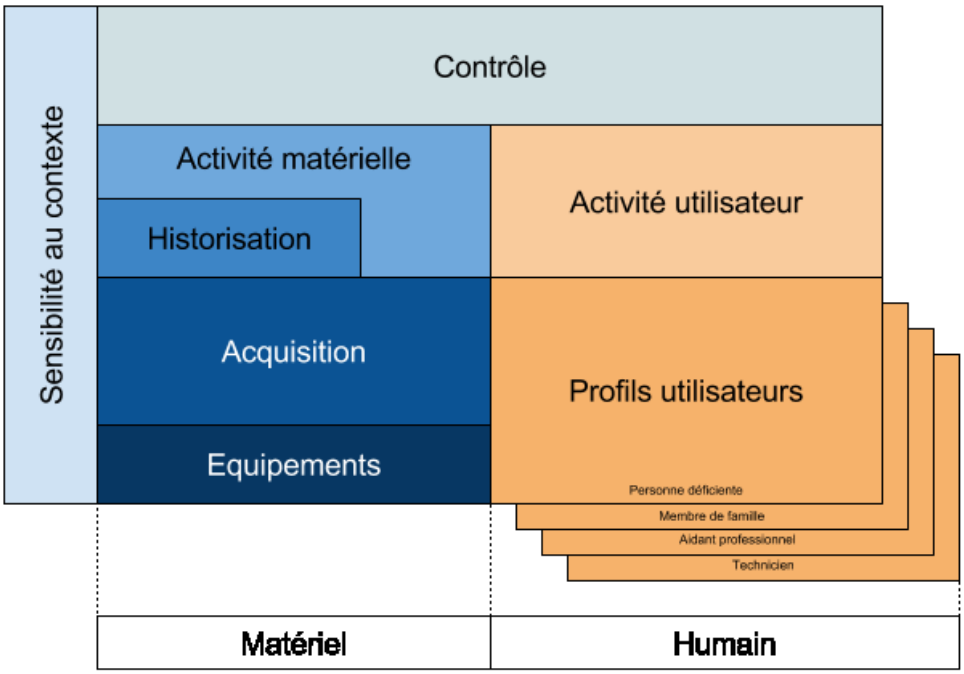



Figure 12 - Architecture de StoveMAS.

## 3.5 La collaboration entre l'homme et la machine

Afin de donner vie à ce modèle, un système multi-agents (SMA) est utilisé pour représenter le système. Un SMA est composé d'entités autonomes appelés agents. Les propriétés autonomes des agents sont des propriétés qu'on recherche pour représenter les fonctionnalités de notre système. Par conséquent, chaque agent de notre SMA a une tâche bien précise. Ce système multi-agents doit être inter-opérationnel pour accroitre la flexibilité et la portabilité. Dans cette section nous allons développer les agents d'acquisition qui permettent d'acquérir les informations issues des capteurs, les agents de haut niveau qui analysent l'activité des appareils

de cuisine et des utilisateurs, les agents qui ont la tâche de s'occuper des risques de sécurité et les agents qui gèrent la sécurité de StoveMAS.

### 3.5.1 Organisation

La nature dynamique et les interactions de haut niveau des agents s'adaptent parfaitement pour les besoins de nos travaux. L'organisation retenue pour notre SMA est la congrégation. Les congrégations sont des groupements d'agents dans lesquels les membres du groupe ont des buts différents (gestion des risques de sécurité, l'acquisition des données, gestion des utilisateurs, etc.). Les agents peuvent entrer et sortir librement d'une congrégation. Dans le cadre de nos travaux, une seule congrégation est mise en place, permettant une connaissance globale à tous les agents dans ce groupe. Les arrivées et départs d'agents correspondent à l'évolution de l'environnement, c'est-à-dire l'arrivée de nouveau matériel ou des risques supplémentaires. Chaque agent a un rôle et des buts bien définis dans la congrégation, mais ils partagent une connaissance commune.

### 3.5.2 Les agents pour l'acquisition des données

L'installation de StoveMAS chez les résidents implique une adaptation du système vis-à-vis des équipements de cuisine présents (cuisinière tout en un, four, four à micro-ondes, plaques de cuisson, etc.). De multiples technologies de capteurs peuvent ainsi être utilisées pour faire l'acquisition des données. Pour homogénéiser ces différences d'acquisition, un SMA s'adapte parfaitement. Un ou plusieurs agents spécifiques peuvent être mandataires de la fonctionnalité d'acquisition des données selon la nature de l'installation des capteurs. Ensuite, des agents de haut niveau permettent de traiter les données indépendamment du matériel d'acquisition. Cela permet d'avoir des agents de haut niveau identiques pour toutes les installations.

### 3.5.3 Les agents pour représenter le matériel de cuisine

Pour analyser l'activité des équipements à haut niveau, nous définissons des *DeviceAgents*. Ces agents permettent de représenter ces appareils de cuisine (cuisinière tout en un, four, four à micro-ondes, plaques de cuisson, etc.). Ils récupèrent les informations des capteurs des

différents agents d'acquisition des données. Ces informations permettent aux *DeviceAgents* de déduire l'état des différents équipements et leur activité de haut niveau. Par activité, on entend l'état intrinsèque de l'appareil (allumé, chargé, chaud etc..). Les *DeviceAgents* peuvent représenter les équipements selon trois niveaux de granularité (Tableau 2). Ces trois niveaux de granularité peuvent coexister ensemble :

1. Un *DeviceAgent* pour l'ensemble des équipements : Tous les équipements sont représentés par un seul *DeviceAgent*. Cet agent détient toutes les informations concernant l'état de l'ensemble des appareils et réduit ainsi le nombre de communications. Par contre, si une panne informatique surgit au sein de cet agent, l'ensemble du système est paralysé.

2. Un *DeviceAgent* pour chaque équipement : Cette solution représente au mieux la correspondance entre un *DeviceAgent* et un équipement. Chaque *DeviceAgent* est mandataire d'un équipement et observe son activité. Il devient aisé de faire la correspondance entre l'analyse de l'activité de l'équipement et les capteurs nécessaires pour faire cette analyse. La complexité du *DeviceAgent* pour cette granularité est proportionnelle à la complexité de l'équipement dont cet agent est mandataire.

3. Un *DeviceAgent* pour chaque fonctionnalité d'un équipement : Lorsque l'équipement est complexe et que l'analyse de son activité devient tout aussi complexe, il est possible d'associer un *DeviceAgent* à chaque fonctionnalité d'un équipement pour garder une bonne visibilité de l'activité de l'équipement.

Tableau 2 - Comparaison entre les différentes solutions de granularité pour les *DeviceAgents*.

| | 1 DA pour n équipements | 1 DA pour 1 équipement | 1 DA pour chaque fonctionnalité d'un équipement |
|---|---|---|---|
| Avantages | • Centralisation des données | • Optimisation du placement des capteurs<br>• Robustesse<br>• Association agent/équipement | • Des agents très spécifiques<br>• Facilité à intégrer pour des appareils complexes |
| Inconvénients | • Robustesse<br>• Fiabilité | • Agents complexes si l'équipement est complexe | • Grand nombre d'agents<br>• Plus de communications |

Tous les *DeviceAgents* suivent le même modèle (Figure 13) :

1. Se configurer selon l'équipement dont il est mandataire en chargeant le fichier de configuration correspondant (Annexe E). Ce fichier de configuration contient une liste de capteurs dont l'agent a besoin pour fonctionner correctement. Accompagné de cette liste, un ensemble de valeurs de tarage permet de paramétrer les capteurs au fonctionnement propre de l'équipement.

2. Analyser l'activité de l'équipement en permanence. Si un changement de l'activité a lieu, l'agent diffuse cette information aux agents mandataires des risques par message et enregistre un changement d'état s'il y a lieu. Cet évènement est également enregistré dans un fichier log pour garder une trace de l'activité de l'appareil sur une longue durée.

3. La configuration de l'agent. Cette partie de l'agent contient toutes les variables nécessaires à l'agent pour fonctionner correctement, notamment les noms des autres

agents dans la congrégation pour la communication et l'état de l'équipement dont il est mandataire. Ces données sont internes à l'agent.

Ces trois fonctionnalités sont identiques pour chaque *DeviceAgent* dans notre système. Là où chaque *DeviceAgent* se différencie des autres est dans la partie configuration. Chaque *DeviceAgent* charge un fichier de configuration différent (car mandataire d'un équipement différent) et analyse selon les fonctionnalités de cet appareil. L'activité de ces agents est historiée et permet de garder une trace sur l'activité d'un équipement sur le long terme, elle permet également d'adapter au mieux le profil de l'appareil au fonctionnement de celui-ci.

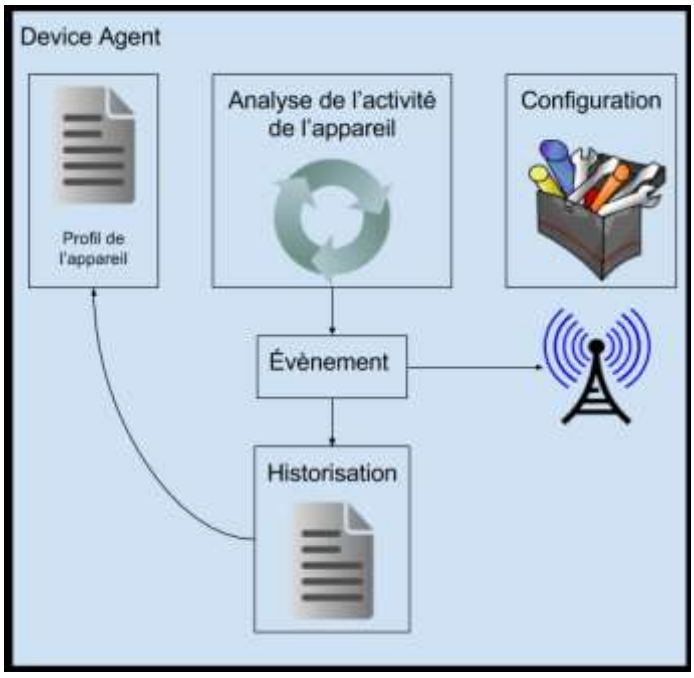



Figure 13 - Modèle des agents *DeviceAgents*.

Les équipements dont ces agents sont mandataires peuvent se trouver dans des états différents (Figure 14). Les équipements transitent entre ces états en permanence. Lors du démarrage de StoveMAS, il n'a aucune connaissance des équipements, ils se trouvent par conséquent dans un état « inconnu ». StoveMAS vérifie pour chaque équipement s'il dispose de tous les capteurs nécessaires pour fonctionner correctement. Si oui, l'équipement se trouve en état « éteint »

(l'équipement ne peut être allumé à ce moment car le système doit verrouiller tous les équipements au démarrage par mesure de sécurité). Sinon, si StoveMAS dispose d'un nombre minimal de capteurs pour assurer la sécurité, l'équipement peut malgré tout fonctionner, mais en mode « dégradé ». Sinon on considère qu'il est en panne et qu'une intervention est nécessaire afin de le réparer. Lorsqu'un utilisateur s'identifie auprès du système, les équipements peuvent se déverrouiller et par conséquent être en état « allumé ». Les actions venant des usagers peuvent garder l'équipement dans le même état (par exemple allumer un deuxième rond, augmenter la température, etc.), ou le faire revenir dans état « éteint ». Une incompatibilité entre le profil utilisateur et l'usage de la personne peuvent provoquer un risque et ainsi mettre l'équipement dans l'état « verrouillé ». De la même manière, une panne peut survenir et amener l'équipement dans un état « dégradé » ou « en panne ». Une panne peut survenir à n'importe quel moment au cours du fonctionnement de l'appareil. Le passage entre un fonctionnement normal et un fonctionnement en mode « dégradé » peut alors se passer aussi à n'importe quel moment. Si un tel passage a lieu, l'état de l'appareil sera le même après qu'avant. Par exemple, si l'appareil était en mode « allumé » avant la panne et que l'appareil peut fonctionner en mode dégradé malgré cette panne, l'appareil se retrouve en mode « allumé dégradé » suite à cette panne.

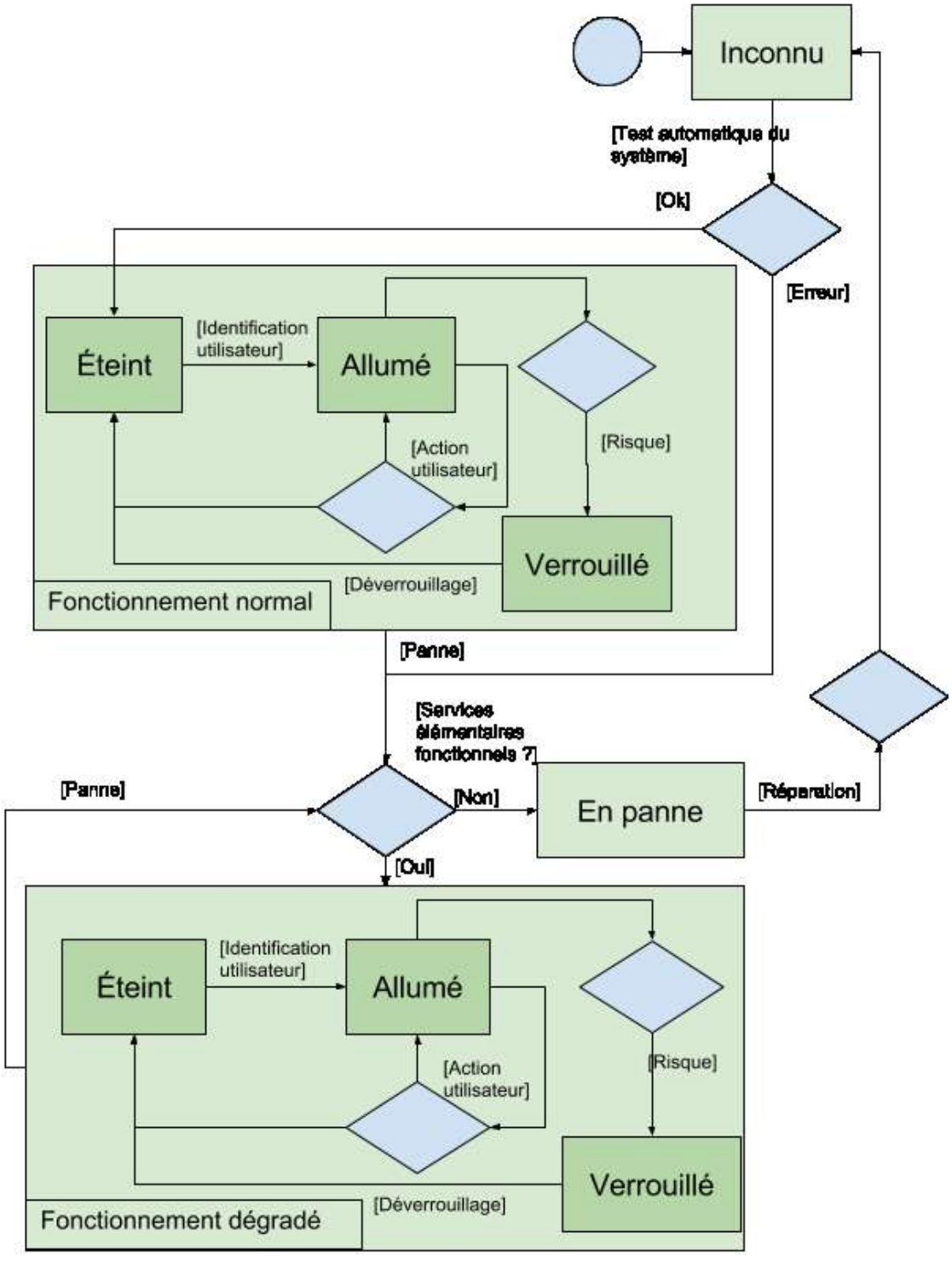



Figure 14 - États des équipements.

### 3.5.4 L'utilisateur en tant que part entière du système

De la même manière que pour les appareils de cuisine, il est nécessaire de représenter les utilisateurs. Pour cela, nous définissions un *UserAgent* qui est mandataire de la gestion de tous les utilisateurs et de leurs profils. Au vu de leurs buts assez similaires, le modèle du *UserAgent* est très proche du modèle des *DeviceAgents* (Figure 15). Dans la partie d'identification de la personne, le *UserAgent* identifie la ou les personnes qui se connectent au système. Lorsque le *UserAgent* est sollicité pour indiquer la connexion d'un nouvel utilisateur, ce dernier charge le profil de l'utilisateur en question et génère le profil utilisateur résultant. Ensuite, il déverrouille les appareils de cuisine si les utilisateurs y sont autorisés et que les conditions contextuelles le permettent. Finalement, ce profil résultant est transmis aux *RiskAgents*. Parallèlement à la gestion des profils utilisateurs, le *UserAgent* gère également les capteurs de détection de présence des personnes dans l'environnement. Le *UserAgent* gère ces capteurs car ils ne dépendent d'aucun appareil, mais détectent la présence d'usagers dans l'environnement. L'historisation permet de garder une trace à longue durée sur l'activité de la personne. Elle permet également aux aidants professionnels d'avoir une information sur l'évolution de l'activité de la personne déficiente (nombre de risques enclenchés lors de l'AVQ, décalage chronologique de l'activité), qui ensuite, adaptent le profil au mieux à l'évolution de la maladie de la personne atteinte.

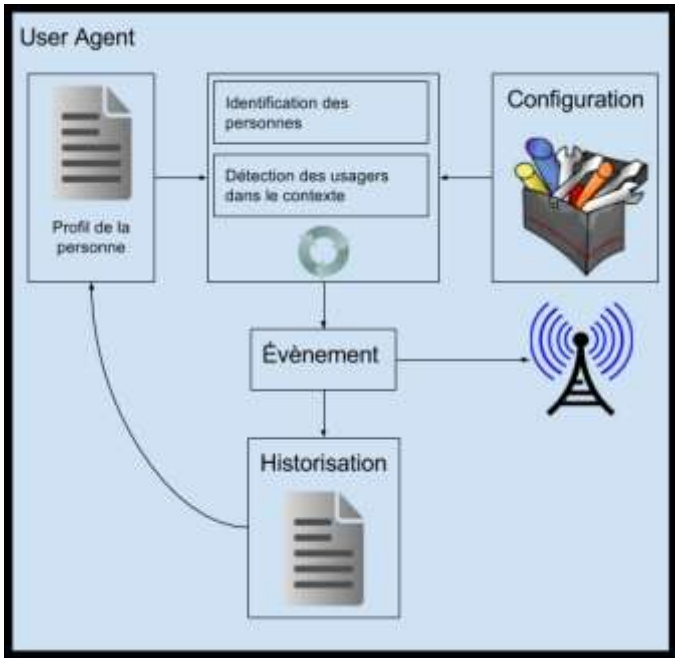



Figure 15 - Modèle de l'agent *UserAgent*.

### 3.5.5 La sécurité pour tous

Pour que le système soit sensible au contexte, il est nécessaire que les entités représentant les règles de sécurité soient suffisamment flexibles et intelligentes. Pour cela, on choisit de représenter les règles de sécurité par des agents. Les *RiskAgents* (RA) sont des agents qui représentent les règles de sécurité dans notre système (Chapitre 2.6.1). Ces agents reçoivent les données des équipements et des utilisateurs, respectivement des *DeviceAgents* et du *UserAgent*. On peut représenter les *RiskAgents* selon deux niveaux de granularité (Tableau 3) :

- Si on choisit de représenter toutes les règles de sécurité par un seul *RiskAgent*, toutes les données des règles de sécurité sont centralisées. Les *DeviceAgents* et *UserAgent* ont seulement besoin de communiquer avec ce *RiskAgent*, simplifiant ainsi les communications. Cependant, si une erreur se produit au sein de cet agent, toutes les règles de sécurité seront défaillantes et tout le système sera paralysé.

- Si on choisit de représenter chaque règle de sécurité par un *RiskAgent* individuel, le système devient plus robuste en cas de panne d'un *RiskAgent* individuel. Avec cette modélisation, un *RiskAgent* peut être facilement ajouté ou ôté de la plateforme. Cependant, lorsqu'il y a plusieurs *RiskAgents*, les communications entre *DeviceAgents*, *UserAgent* et les *RiskAgents* deviennent plus complexes à gérer.

Tableau 3 - Comparaison entre les différentes granularités pour les *RiskAgents*.

| | 1 RA pour n règles | 1 RA pour 1 règle |
|---|---|---|
| Avantages | • Centralisation des données<br>• Peu de communications | • Robustesse<br>• Flexibilité |
| Inconvénients | • Robustesse<br>• Flexibilité (difficile à rajouter ou ôter des règles) | • Plus grand nombre d'agents<br>• Plus difficile d'assurer la cohérence entre les décisions<br>• Plus difficile de gérer les interrelations entre les règles |

Nous choisissons de représenter chaque règle de sécurité par un *RiskAgent* individuel car on souhaite préserver un maximum de flexibilité. On souhaite également garder des *RiskAgents* assez simples pour qu'un technicien, ne connaissant pas le système dans sa totalité, puisse intégrer ses propres règles de sécurité dans StoveMAS. Il devra cependant s'assurer de la cohérence entre les règles.

Pour faciliter les communications entre les *DeviceAgents*, *UserAgent* et les *RiskAgents*, les deux premiers diffusent leurs messages à l'ensemble des *RiskAgents* (Figure 16). Les *RiskAgents* font ensuite le tri des messages qui les intéressent ou non. Ces messages permettent aux *RiskAgents* de mettre à jour leur connaissance de l'environnement. L'analyse du risque se fait en comparant la configuration de l'environnement (informations issues des *DeviceAgents*), avec la configuration des utilisateurs (informations issues du *UserAgent*) pour une règle de sécurité donnée. L'analyse du risque est présentée plus en détail dans la section 4.3.3. Si un risque se déclare, le ou les utilisateurs sont notifiés et sont alors invités à résoudre le problème

qui est survenu dans un délai prédéterminé. Si le risque disparait, le *RiskAgent* n'émet plus de notifications. Par contre, si le risque n'a pas été traité dans le délai approprié, le *RiskAgent* demande le verrouillage des équipements pour éviter tout danger pour le ou les utilisateurs. L'ensemble des *RiskAgents* fonctionnent de manière indépendante, c'est-à-dire que lorsqu'un *RiskAgent* détecte un risque, les autres *RiskAgents* continuent de fonctionner normalement. Il se peut même que certaines actions peuvent enfreindre plusieurs règles de sécurité simultanément, les utilisateurs doivent alors « réparer » individuellement chaque risque. Les évènements qui ont eu lieu (notifications, verrouillages et divers) sont historiés et permettent de connaitre les erreurs et oublis fréquents des utilisateurs.

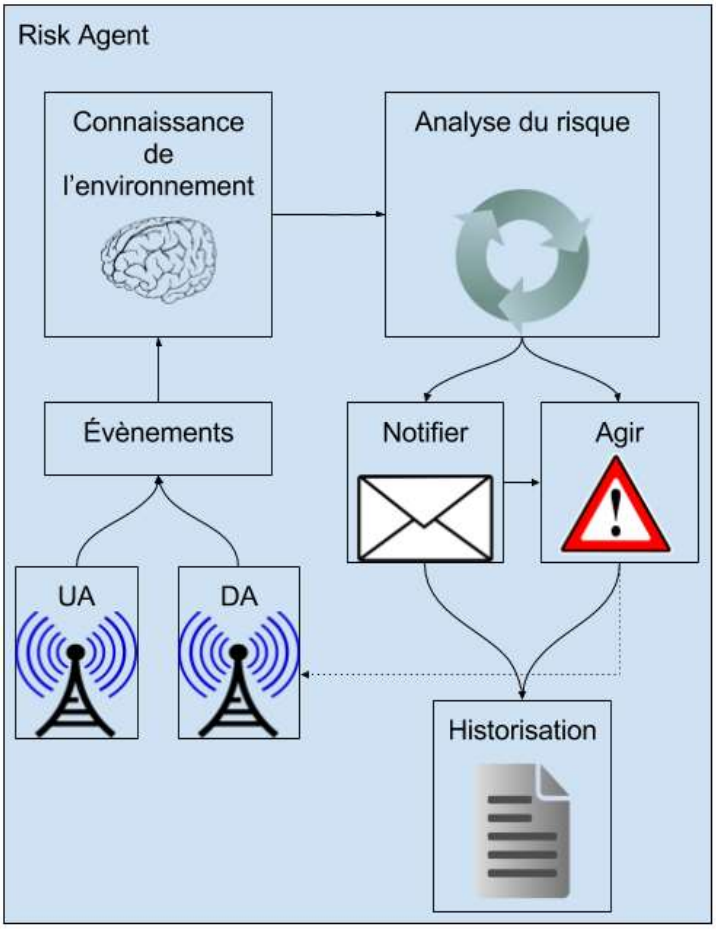



Figure 16 - Modèle de l'agent *RiskAgent*.

### 3.5.6 System Agent

Pour que StoveMAS soit fiable et fournisse une qualité de service élevée, une partie de ce dernier doit, en plus d'être sensible au contexte, être sensible aux évolutions du système en lui-même (pannes au sein des agents, ajout/retrait d'agents). Dans cette optique, le *SystemAgent* est un agent qui s'occupe de vérifier l'intégrité du système, gère les fonctions périodiques planifiées et envoie un message périodiquement à l'agent *WatchdogAgent* (Figure 17) permettant de garder le système actif.


Figure 17 - Modèle de l'agent *SystemAgent*.

Pour vérifier l'intégrité du système, l'agent *SystemAgent* vérifie si tous les agents présents sont correctement enregistrés dans l'annuaire de la plateforme multi-agents. Pour cela, l'agent contacte l'annuaire pour connaitre la liste des agents enregistrés. Le *SystemAgent* a également connaissance des agents présents dans le système. En comparant ces deux listes, deux cas de figure peuvent se présenter :

- Le cas où un ou plusieurs agents sont présents mais ne sont pas enregistrés. Dans ce cas le *SystemAgent* contacte les agents en question et leur demande de s'enregistrer. Si après un délai les agents en question ne se sont pas enregistrés, ils sont tués par le *SystemAgent* et un message de notification indiquant un problème au sein du système est envoyé aux utilisateurs.

- Le cas où un ou plusieurs agents sont enregistrés, mais pas présents sur la plateforme. Ce cas peut se présenter lorsqu'un agent externe malveillant cherche à nuire au système. L'agent *SystemAgent* récolte des informations concernant cet agent malveillant et le désenregistre des pages.

Le *SystemAgent* gère également l'exécution des fonctions planifiées. Ces fonctions peuvent être exécutées à heures fixes durant la journée ou la semaine. L'intérêt de ces fonctionnalités est typiquement la recherche de pannes dans les capteurs, de faire des tarages des capteurs pour mieux adapter les données des capteurs à la réalité.

La dernière fonction, l'envoi d'un message à l'agent *WatchdogAgent*, est détaillée dans la partie suivante.

### 3.5.7 Watchdog Agent

L'agent *WatchdogAgent* permet de verrouiller les équipements si un problème majeur se produit dans le système. Cet agent fonctionne comme un compte à rebours, qui, lorsqu'il arrive à terme, verrouille les équipements (tel un fonctionnement de heart-beat). Pour éviter que le système se retrouve verrouillé en permanence, cet agent doit voir son compte à rebours remis en état initial. Ce sont les messages envoyés par le *SystemAgent* qui ont cette tâche. Ces messages indiquent que le système est dans un état fonctionnel et que le verrouillage n'a pas lieu d'être.

L'agent *WatchdogAgent* se comporte comme étant l'ultime recours pour verrouiller les équipements en cas de danger. Dans cette optique, l'agent a été implémenté de façon à agir directement sur le matériel physique. L'agent doit cependant être adapté au matériel qu'il commande. Ce choix a été fait pour pouvoir contrôler le matériel physique avec le moins d'agents intermédiaires possible.

## 3.6 Réalisation des boucles MAPE-K

Les agents mentionnés dans la section précédente ont chacun un rôle important dans la mise en place des boucles de rétroaction. Nous avons identifiés deux boucles MAPE-K à travers l'élaboration de nos agents.

### 3.6.1 À travers les RiskAgents

Grâce à l'ensemble des agents *DeviceAgents*, *UserAgent* et *RiskAgents* qu'on retrouve une boucle MAPE-K (Figure 18). Les agents *DeviceAgents* et *UserAgent* s'occupent de monitorer et analyser l'activité dans l'environnement. Les *RiskAgents* s'occupent de planifier et d'exécuter si nécessaire. L'historisation des données de ces agents permet d'améliorer la connaissance du système.

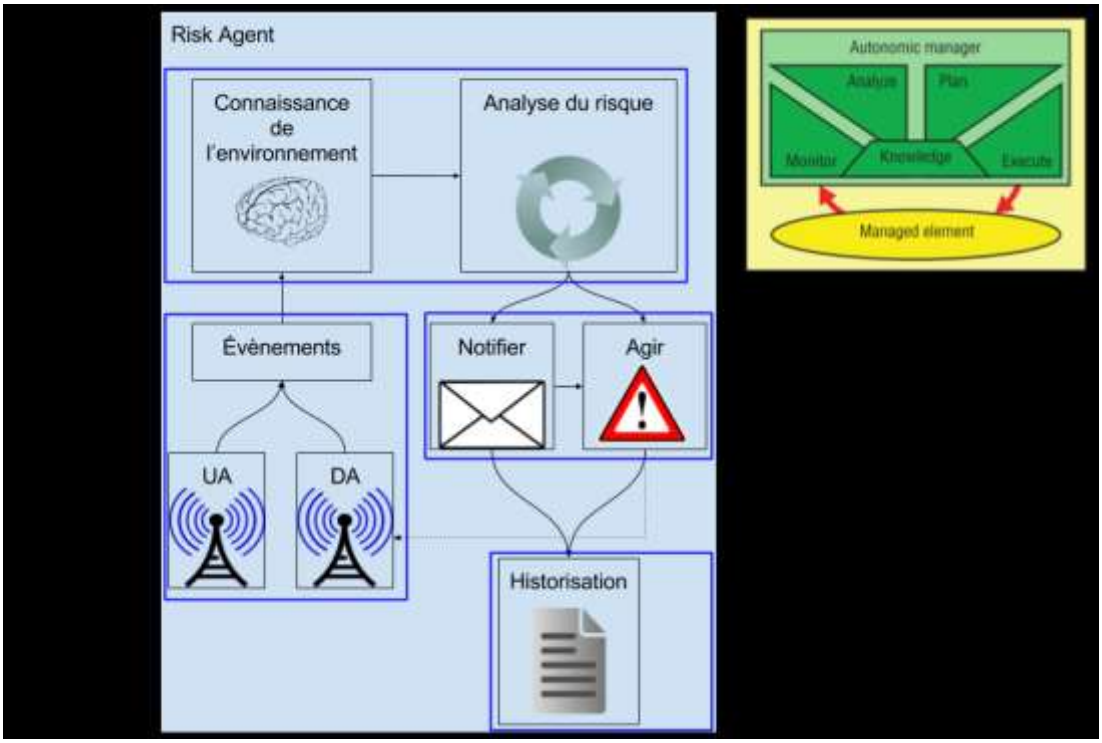



Figure 18 - Boucle MAPE-K présent dans les *RiskAgents*.

### 3.6.2 À travers le WatchdogAgent

Les agents *SystemAgent* et *WatchdogAgent* constituent une boucle MAPE-K court bio inspiré permettant de verrouiller les appareils par mesure de sécurité si un problème se produit dans le système. On retrouve ce mécanisme dans le monde animal et humain avec les battements de cœur. Tant que le cœur bat, l'organisme vit. Le cœur cesse de battre lorsque l'organisme subit des problèmes majeurs. Nous avons mis en place ce fonctionnement dans StoveMAS. Par analogie, l'agent *WatchdogAgent* incarne le cœur et le *SystemAgent* incarne l'organisme. La Figure 19 présente les boucles de rétroaction présentes dans notre système via les agents.

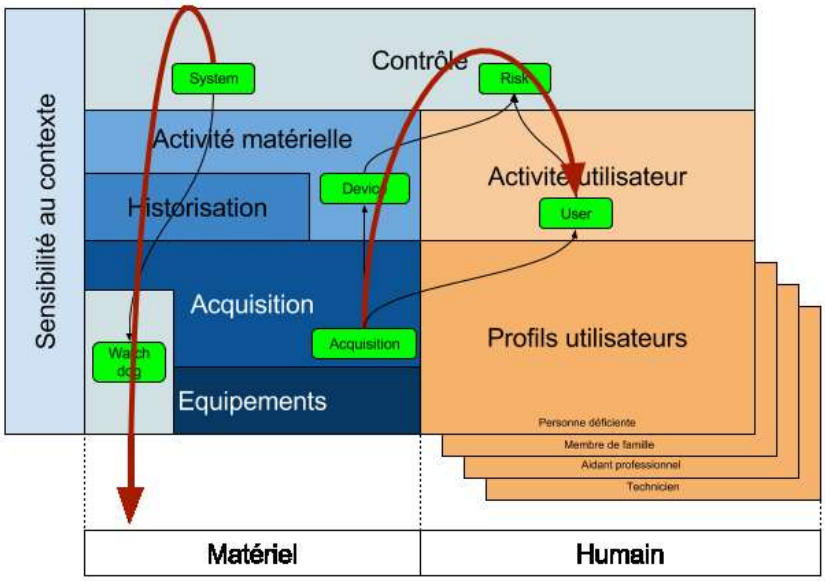



Figure 19 - Boucles de rétroactions présentes dans StoveMAS (en rouge).

## 3.7 Conclusion

Via l'ensemble de ces agents, StoveMAS est capable de répondre aux besoins des utilisateurs en termes de sécurité. La Figure 20 illustre l'architecture du système et y fait figurer les différents agents.

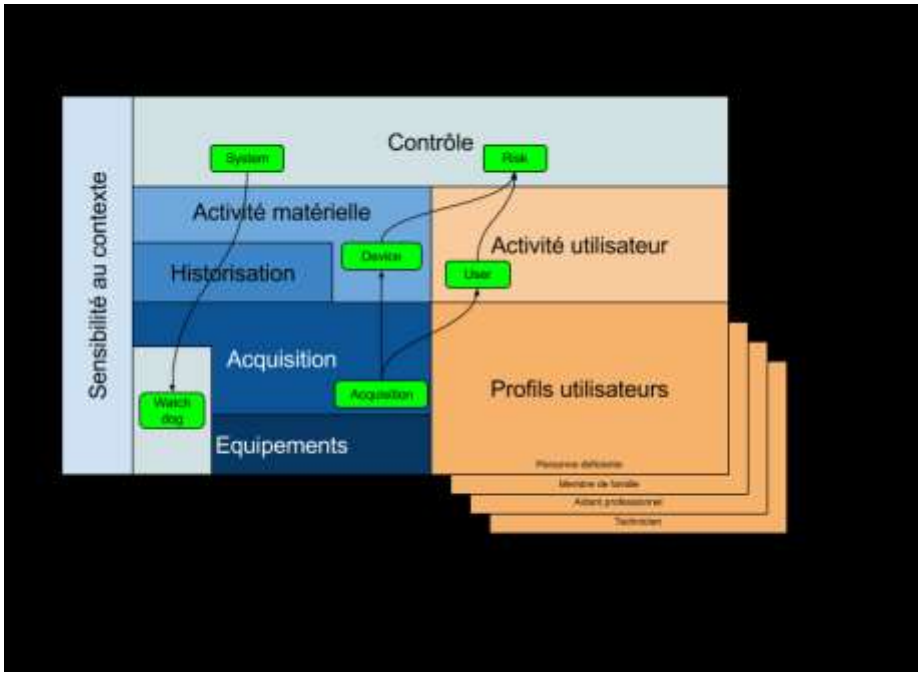



Figure 20 - Architecture de StoveMAS comportant les agents (en vert).

Via le profil utilisateur, il est possible de fournir à une clientèle une assistance adaptée à leur situation médicale et leurs préférences. Les différents agents disposent de fonctionnalités de détection d'erreurs, ce qui permet au système une fiabilité accrue. De plus, les agents *SystemAgent* et *WatchdogAgent* sont un dernier recours lorsque le système rencontre des pannes majeures. L'organisation en congrégation de ces agents rend la plateforme flexible pour l'intégration de nouveaux agents. Dans cette congrégation, les risques de sécurité, représentées par des agents permettent une sécurité adaptée au profil des utilisateurs. De plus, on retrouve cette flexibilité au niveau des *DeviceAgents* permettant une adaptation sur des équipements hétérogènes. Dans le chapitre suivant, nous allons développer cette architecture sur deux supports physiques et implémenter les différents agents mentionnés.

# Chapitre 4

# Implémentation

Dans le chapitre précédent, les modèles généraux de StoveMAS ont été présentés. Dans ce chapitre, nous allons appliquer ces modèles dans deux environnements distincts avec des équipements concrets.

D'une part, on retrouve le laboratoire Lab-STICC, situé à Lorient, en France. Au sein du bâtiment ENSIBS (École Nationale Supérieure d'Ingénieurs de Bretagne-Sud), un appartement domotique est mis à disposition pour les expérimentations du laboratoire. Cet appartement est composé de deux étages. Au rez-de-chaussée, on retrouve une entrée, une cuisine, un salon et une salle de bain. À l'étage, on retrouve une cuisine, une chambre ainsi qu'une salle de bains. Cet appartement est seulement équipé d'un réseau EIB (European Installation Bus) actuellement. Cet appartement domotique constitue une étape de transition de déploiement entre un concept et la mise en place en milieu réel d'un système. Des personnes ayant des déficiences cognitives et physiques seront accueillies au sein de cet appartement lors des expérimentations pour ces systèmes.

D'autre part, le laboratoire DOMUS, à Sherbrooke au Canada, dispose d'un appartement domotique composé d'un hall d'entrée, d'un salon, d'une salle à manger, d'une cuisine, d'une salle de bain et d'une chambre (Figure 21). L'appartement accueille régulièrement des personnes ayant des traumatismes cranio-cérébraux ou atteintes de la maladie d'Alzheimer. Cet appartement est aussi utilisé afin de mener des études cliniques et pour mettre au point des systèmes avant de les déployer en milieu réel, en particulier dans une résidence pour TCC, qui agit comme laboratoire vivant.

Figure 21 - L'appartement du laboratoire DOMUS.

Ce chapitre s'articule autour de 4 parties. Dans un premier temps, une présentation des choix des supports technologiques est faite. Ensuite, nous détaillerons l'interfaçage de ces supports technologiques avec notre système : SPI (Serial Peripheral Interface), ADAM et sans fil. Puis, nous montrons comment les agents de haut niveau exploitent ces données. Enfin, une présentation des interfaces entre l'homme et la machine est faite.

## 4.1 Les choix technologiques

StoveMAS est un système qui doit être flexible pour s'adapter à son environnement. Ses composants doivent être facilement déployables selon les équipements présents et l'interfaçage des capteurs.

Un système multi-agent (SMA) répond à ce critère et est utilisé pour représenter les différentes fonctionnalités de StoveMAS. Chaque agent du SMA représente une fonctionnalité. On utilise la plateforme open source JADE (*Java Agent DEvelopment framework*). Comme son nom l'indique, il s'agit d'une plateforme en langage Java, ce qui permet la portabilité du programme sur des machines différentes. JADE propose une implémentation conforme aux spécifications FIPA (*Foundation for Intelligent Physical Agents*) permettant une certaine interopérabilité avec d'autres systèmes basés sur les systèmes multi-agents.

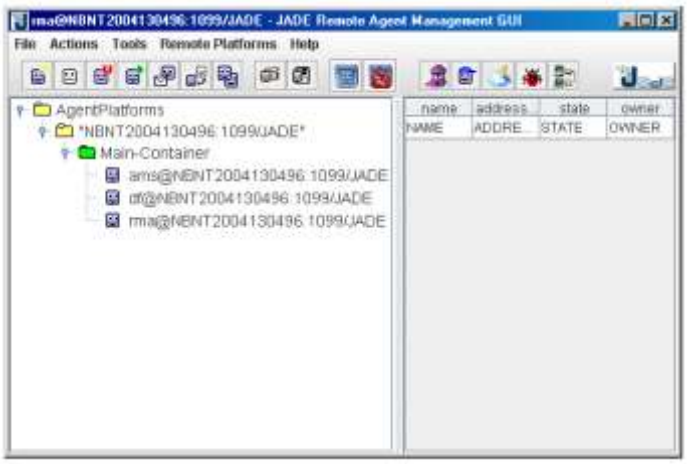



Figure 22 - Interface graphique de JADE.

JADE est fournie avec une interface graphique qui permet de visualiser les différents agents [71] (Figure 22). On peut remarquer que par défaut on y retrouve trois agents dans un conteneur. L'agent *AMS* (*Agent Management System*) permet de garder une trace de toutes les instances JADE sur l'ordinateur. Cet agent est particulièrement intéressant lorsque le système multi-agents contient plusieurs conteneurs[1]. L'agent *RMA* (*Remote Management Agent*) propose plusieurs outils et fonctionnalités dont l'interface graphique. L'agent *DF* (*Directory Facility*) est en quelque sorte un service d'annuaire, contenant une liste des services que proposent les agents connectés à la plateforme JADE. Les agents contenus dans le container peuvent s'enregistrer auprès de l'agent *DF* et déclarer les services qu'ils proposent. Le développement du code a été fait en utilisant Eclipse Néon (version 4.6.1).

Nous avons aussi développé une application Android. L'application mobile constitue une partie importante du système car elle permet l'interaction entre ce dernier et les occupants. Le développement s'est fait avec le logiciel Android Studio en version 2.2.2.0.

[1] Groupe d'agents sur un même ordinateur physique

## 4.2 La communication entre les capteurs et les agents

Dans cette section, nous allons développer la communication entre les capteurs et les agents. Dans un premier temps, l'instrumentation des deux laboratoires est présentée, puis l'interfaçage des capteurs avec StoveMAS est développé.

### 4.2.1 Instrumentation au laboratoire Lab-STICC

Au laboratoire Lab-STICC, notre système est implanté sur une Raspberry Pi 3 modèle B. Cette carte possède un processeur ARMv8 quadricoeur cadencés à 1.2 GHz, d'une mémoire vive de 1 Go, de 4 ports USB et des connexions sans fil telles que le Wi-Fi et le Bluetooth. Un lecteur de carte mémoire au format SD permet de stocker le système d'exploitation ainsi que notre programme. Le système d'exploitation installé sur la Raspberry Pi est une variante Linux Debian : Raspbian Jessie (version 4.4). Cette carte dispose également de 40 ports GPIO (General Purpose Input/Output) que nous utilisons pour récolter les données issues des capteurs (Figure 23). Les équipements de cuisine sont composés de deux appareils électriques distincts : un four à micro-ondes ainsi qu'une plaque vitrocéramique.

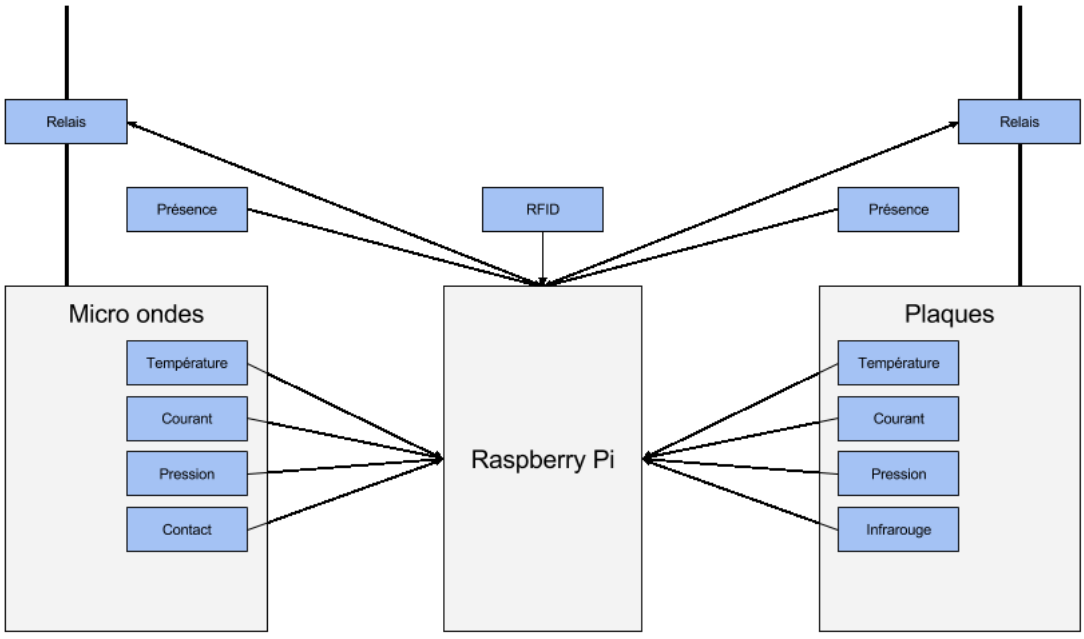



Figure 23 - Topologie des capteurs au laboratoire Lab-STICC.

Le four à micro-ondes de marque *Samsung Smart Oven mc28h5125ak* (Figure 24), dispose de plusieurs fonctions de cuisson :

- Micro-ondes (d'une puissance allant de 100W à 900W)
- Fonction grill (1500W)
- Four à convection (2100W)

Figure 24 - Le four à micro-ondes *Samsung Smart Oven*.

La plaque chauffante utilisée au laboratoire Lab-STICC est de marque *Brandt tv1000b*. Cet appareil dispose de deux foyers chauffants (1200W et 1800W de puissance) réglables par des boutons tournants sur 9 positions.

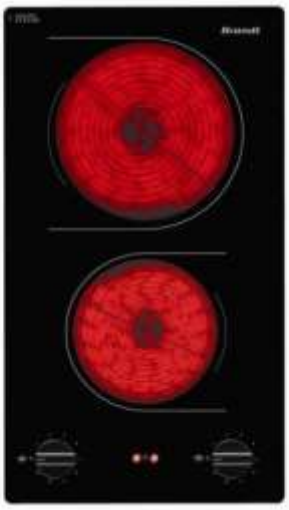


Figure 25 - La plaque vitrocéramique *Brandt tv1000b*.

Les deux appareils ne disposent que de quelques fonctions de base de sécurité, empêchant par exemple d'activer le four à micro-ondes lorsque la porte de l'appareil demeure ouverte. Cependant, aucun mécanisme n'avertit la personne de ne pas toucher des parties brulantes (par exemple l'arrière de l'appareil) ou les ronds chauds vides lorsque les appareils sont activés (seul un voyant rouge indique que la surface est chaude). Dans nos travaux, nous allons les équiper avec les capteurs suivants :

- Un capteur de contact. Ce capteur de contact permet de connaître l'état de la porte du four à micro-ondes. Bien que l'appareil dont nous disposons soit déjà équipé de capteurs de ce type qui ont cet objectif, il n'est pas possible de connaitre leur état sans avoir à modifier le circuit électrique de l'appareil. Le capteur que nous utilisons à la place est un capteur de contact magnétique, il n'y a pas de pièce mécanique qui ferme le contact lorsque la porte est fermée. Ainsi, il est plus difficile pour l'utilisateur de tromper le système en fermant le contact si la porte est ouverte (Annexe C.3).

- Quatre capteurs de pression sous chaque appareil. Ces capteurs sont situés en dessous des pieds des appareils. Ils sont de type *Flexiforce A201-25* et ont une

épaisseur très fine, ce qui les rend quasi invisibles une fois positionnés. Ces capteurs peuvent chacun mesurer une masse de 11.2kg. Sachant que le four à micro-ondes pèse à lui seul 17.8kg et la plaque un peu plus de 7kg, il reste une plage d'utilisation importante pour les produits alimentaires. Ces capteurs permettent de détecter si un objet est présent dans l'appareil au moment de l'allumage (Annexe C.1).

- Trois capteurs de température. Pour la mesure de la température, nous utilisons un thermocouple de type K permettant une mesure allant de 0°C à 800°C (Annexe C.5). Ces capteurs informent le système sur l'activité des appareils. Un de ces capteurs est placé proche de l'élément chauffant du four à micro-ondes pour avoir une information la plus précise possible. Les deux autres, situés proches des ronds sur la plaque vitrocéramique, permettent de relever la température de chacun des foyers. Bien que l'un des objectifs soit de ne pas modifier les équipements existants, il est impossible d'obtenir l'information de la température au sein du four à micro-ondes sans y installer un capteur de température à l'intérieur. On ne peut donc pas respecter cet objectif car l'information de la température est essentielle pour que StoveMAS fonctionne correctement.

- Deux capteurs de présence. Ces capteurs de présence sont installés dans l'entourage des appareils pour détecter la présence d'une personne à proximité. En effet, certaines règles de sécurité nécessitent que la personne reste à proximité lors de la préparation du repas. Les capteurs utilisés sont de marque *Sharp GP2Y0A710K*, elles détectent une présence entre 1 et 5 mètres de distance (Annexe C.4).

- Six capteurs de courant. Trois capteurs de courant sont nécessaires afin de détecter le fonctionnement de chacun des fonctions de chauffe du four à micro-ondes. Les capteurs de courant sont des pinces ampérométriques qui fournissent une tension, image du courant, qui traverse le fil mesuré. Les pinces sont de marque *YHDC SCT 013-030* et permettent de mesurer un courant alternatif jusqu'à 30A et fournissent une tension alternative de 1V d'amplitude. Les trois capteurs de courant restants

permettent de détecter le fonctionnement de chacun des foyers de la plaque de cuisson. Le troisième permet d'être en redondance sur l'entrée de la plaque vitrocéramique. De la même manière que pour le capteur de température, il est impossible de connaitre l'état électrique de chaque fonctionnalité de la plaque de cuisson et du four à micro-ondes sans installer un capteur à l'intérieur (Annexe C.2).

- Un lecteur de carte RFID. Ce lecteur permet l'identification des personnes qui souhaitent utiliser le système. Le déverrouillage des appareils se fait également via la lecture d'une carte RFID, cependant seules certaines cartes permettent le déverrouillage suite à un verrouillage causé par l'enfreinte d'une règle de sécurité. L'antenne RFID est de marque *Innovations ID-12LA* et contient un convertisseur USB.

- Deux relais. Les relais permettent au système d'agir sur le matériel. C'est via ces composants que le système peut couper l'alimentation des équipements de cuisine. Les relais utilisés sont de marque *Crouzet Series 84137000*. Ces relais peuvent être commandés en 3-32V. Un relai est utilisé par appareil et permet de couper le circuit électrique d'alimentation de ce dernier.

- Trois capteurs infrarouges. Ces capteurs sont de marque *Sharp GP2Y0A02YK* et permettent de détecter la présence ou non d'ustensiles sur la plaque vitrocéramique. Deux de ces capteurs (PSHh et PSHl) sont positionnés face à chaque foyer, le troisième (PSH2), est situé sur l'axe de l'entraxe permettant de détecter une présence sur un foyer sur deux (Figure 26). Ainsi, les deux capteurs peuvent détecter la présence d'un ustensile sur chaque rond, et le capteur positionné sur l'entraxe fait office de redondance (Annexe C.4).

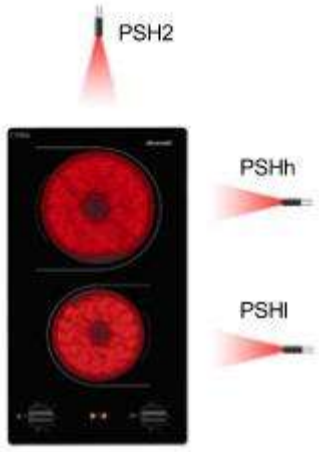



Figure 26 - Positionnement des capteurs infrarouges autour de la plaque vitrocéramique.

### 4.2.2 Instrumentation au laboratoire DOMUS

Au laboratoire DOMUS, la cuisinière est de marque *Frigidaire CFEF3048LSM*, cet appareil dispose de deux équipements distincts : un four et quatre plaques électriques (Figure 27).

Figure 27 - La cuisinière *Frigidaire CFEF3048LSM*.

Les plaques sont commandées individuellement par 4 boutons tournants. Le four, quant à lui, est commandé par les boutons tournants au centre de la console. Ce four dispose de deux modes

de cuisson : cuire (bake) et griller (broil). Les capteurs utilisés sur cet équipement sont de nature similaire à ceux utilisés au laboratoire Lab-STICC, à savoir :

- Six capteurs de courant permettant de détecter l'activité du four et des plaques. Ces capteurs sont installés à l'arrière de l'appareil, proche des boutons pour commander les différents éléments chauffants. On retrouve ainsi un capteur de courant pour chaque plaque chauffante, ainsi que deux capteurs de courant pour chaque mode de cuisson du four. Les capteurs de courant sont de type *CR Magnetics 3110 3000 c1* et peuvent mesurer une intensité allant jusqu'à 100A.

- Quatre capteurs de pression (jauges de contrainte) disposés en dessous de la cuisinière ainsi que quatre capteurs de pression situés sous la plaque des ronds. Les capteurs de pression utilisés sont des *Flexiforce A201-100*, pouvant mesurer une masse jusqu'à 100 livres (45.35 kg).

- Cinq thermocouples permettant d'obtenir l'information de la température des quatre plaques de cuisson et du four.

- Un capteur de contact installé sur la porte du four.

- Quatre capteurs infrarouges installés dans la hotte permettant de détecter si les ronds de la plaque rayonnent de la chaleur.

- Deux capteurs ultrasons installés dans l'environnement proche de la cuisinière permettant la détection de la présence des personnes.

- Un lecteur de d'étiquettes RFID, placé au-dessus des boutons tournants des plaques à gauche de l'appareil. Ce lecteur permet l'identification des utilisateurs.

- Les relais de sécurité sont de marque *Carlo Gavazzi CC40*. Ce relais dispose d'une entrée permettant de valider l'état du relais.

### 4.2.3 Interface Capteurs/Agents

Pour que la communication entre les agents et les capteurs se fasse correctement, nous proposons trois interfaces différentes. Ces trois interfaces sont représentées par des agents de bas niveau. Ces agents récoltent les informations des capteurs et les transmettent aux *DeviceAgents*.

#### 4.2.3.1 L'interface SPI

L'interface SPI est utilisée dans le cadre du laboratoire Lab-STICC. Les capteurs que nous utilisons donnent un signal analogique, or la Raspberry Pi gère seulement les signaux numériques. Ce changement de type de signal est assuré par un convertisseur analogique vers numérique (CAN) (Figure 28). Le composant *MCP3008* est un convertisseur qui permet de transformer le signal analogique issu des capteurs directement en un message sur un bus SPI (Serial Pheripheral Interface), bus qui est nativement géré par le Raspberry Pi (Annexe CC).

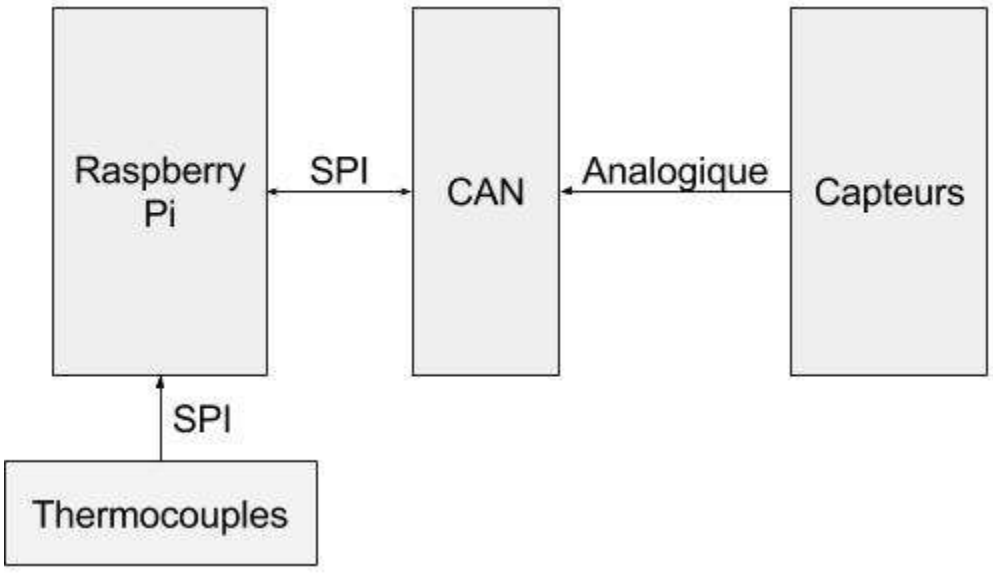



Figure 28 - Interfaçage des capteurs avec la Raspberry Pi.

#### 4.2.3.2 L'interface ADAM

L'acquisition des données au laboratoire DOMUS se fait par l'intermédiaire d'un programme serveur en langage C# dans un automate industriel de marque *Advantech UNO-2174*. Ce

programme écoute l'activité provenant du boitier ADAM (Annexe DD) et transmet cette activité sous forme d'évènements aux clients connectés à ce serveur. StoveMAS est un client de ce programme. StoveMAS dispose d'un agent *ADAMAgent* qui se connecte au serveur. Il récupère les informations des capteurs issues du serveur et enrichit la base de données de StoveMAS. Ces informations dans le message sont hiérarchisées dans un *JSONObject* et contient les informations de tous les capteurs connectés au boitier *ADAM* à un instant donné.

#### 4.2.3.3 L'interface sans fil

Différents protocoles de communication sans fil existent en domotique : Wi-Fi, Bluetooth, Zigbee, Z-Wave, EnOcean, C-Bus, KNX, X10, etc. L'agent *WirelessAgent* établit une connexion sans fil Wi-Fi avec des équipements mobiles tels que des tablettes ou des smartphones. Pour les autres protocoles de communication sans fil, d'autres agents doivent être implémentés. Dans le cadre de nos travaux, une tablette *Asus Nexus 7 version 2013* est utilisée. Ces appareils mobiles, en plus de proposer une interface graphique, embarquent un ensemble de capteurs tels que des accéléromètres, gyroscopes, capteurs de luminosité etc. L'agent *WireLessAgent* permet d'établir une connexion sans fil avec un appareil Android et de récolter les informations des capteurs embarqués.

## 4.3 Les agents au sein de la plateforme JADE

Les agents de haut niveau (*DeviceAgents*, *UserAgent* et *RiskAgents*) permettent d'analyser l'activité des équipements et de les adapter en fonction des usagers qui souhaitent réaliser l'activité de la préparation d'un repas. Ces agents communiquent avec des agents de plus bas niveau, qui eux, dépendent de l'architecture matérielle qui est présente chez le résident (Figure 29).

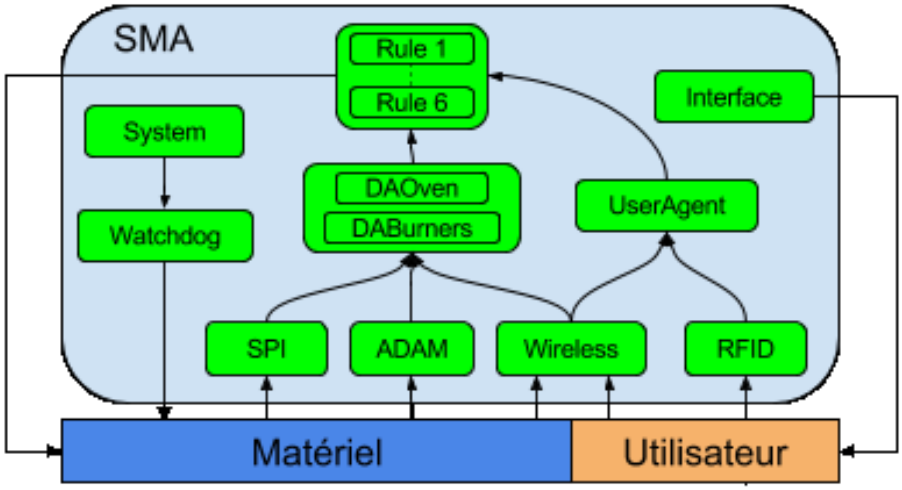



Figure 29 - Dépendances des agents dans StoveMAS.

### 4.3.1 La représentation des équipements

Les appareils sont représentés par des *DeviceAgents*. Pour les équipements du laboratoire Lab-STICC, nous représentons les deux appareils par deux *DeviceAgents* (micro-ondes et plaques électriques). Les deux *DeviceAgents* implémentés s'appellent *DAOven* et *DABurners*. Ils s'occupent respectivement du four et des plaques électriques. Ces deux agents chargent le fichier de configuration de l'équipement de cuisine dont ils sont mandataires. Ces fichiers contiennent des informations concernant les capteurs nécessaires pour analyser l'activité de l'appareil ainsi que des paramètres de configuration de l'agent (Annexe E).

L'agent *DAOven* s'occupe de l'activité du four à micro-ondes et relève l'activité des trois fonctionnalités de l'équipement, à savoir la fonction micro-ondes, grill et convection. Pour cela, il utilise les informations issues des capteurs de pression, de température, de courant ainsi que le capteur de contact installés sur le four à micro-ondes. L'agent *DABurners*, surveille l'activité des deux plaques chauffantes et la présence d'ustensiles. Pour cela, il utilise les informations issues des capteurs de pression, température, de présence et courant (Tableau 4).

Tableau 4 - Capteurs utilisés par les *DeviceAgents* au laboratoire Lab-STICC.

| DAOven | |
|---|---|
| Type | Nom |
| Capteur de pression | FSMfl |
| | FSMrl |
| | FSMrr |
| | FSMfr |
| Capteur de courant | AMPOm |
| | AMPOg |
| | AMPOc |
| Capteur de température | TCO |
| Capteur de contact | BTN1 |

| DABurners | |
|---|---|
| Type | Nom |
| Capteur de pression | FSHfl |
| | FSHrl |
| | FSHrr |
| | FSHfr |
| Capteur de courant | AMPHl |
| | AMPHh |
| | AMPH2 |
| Capteur de température | TCHl |
| | TCHh |
| Capteur de présence | PSHl |
| | PSHh |
| | PSH2 |

Au sein des *DeviceAgents*, il est intéressant de détecter un mauvais fonctionnement ou une panne probable de capteurs. Cette détection est possible lorsqu'il y a une redondance entre certains capteurs. Par exemple, au laboratoire Lab-STICC, les trois capteurs de présence sur la plaque électrique sont en redondance (Figure 26). Si le capteur de la plaque du dessus (PSHh) détecte une présence, mais que le capteur sur l'entraxe (PSH2) ne détecte rien, il y a probablement un problème au niveau de ces deux capteurs.

Tableau 5 - Capteurs utilisés par les *DeviceAgents* au laboratoire DOMUS.

| DAOven | |
|---|---|
| Type | Nom |
| Capteur de pression | FSOfl |
| | FSOrl |
| | FSOrr |
| | FSOfr |
| Capteur de courant | AMPOBroil |
| | AMPOBake |
| Capteur de température | TCO |
| Capteur de contact | BTN1 |

| DABurners | |
|---|---|
| Type | Nom |
| Capteur de pression | FSHfl |
| | FSHrl |
| | FSHrr |
| | FSHfr |
| Capteur de courant | AMPHfl |
| | AMPHrl |
| | AMPHrr |
| | AMPHfr |
| Capteur de température | TCHfl |
| | TCHrl |
| | TCHrr |
| | TCHfr |
| Capteur de présence | PSHfl |
| | PSHrl |
| | PSHrr |
| | PSHfr |

Au laboratoire DOMUS, nous représentons l'appareil par un *DeviceAgent* par fonctionnalité de l'appareil, c'est-à-dire deux agents. La cuisinière est composée d'un four et des plaques électriques au sein d'un même appareil physique. On a jugé plus judicieux de séparer la

cuisinière en deux appareils virtuels, représentés par deux *DeviceAgents,* pour rendre ces agents plus lisibles. Cette séparation est possible car les deux appareils virtuels sont indépendants. Les deux *DeviceAgents* implémentés s'appellent également *DAOven* et *DABurners* et s'occupent respectivement du four et des plaques électriques. L'agent *DAOven* utilise les capteurs de force, de courant, de température et de contact. L'agent *DABurners* surveille l'activité des quatre plaques électriques et la présence d'ustensiles via les informations issues des capteurs de pression, température, de courant et de présence (Tableau 5).

### 4.3.2 L'identification des utilisateurs

Le *UserAgent* est l'équivalent des *DeviceAgents,* mais pour l'ensemble des utilisateurs du système. Le *UserAgent* s'occupe de l'ensemble des utilisateurs connectés. Pour cela, le *UserAgent* fait appel à une interface RFID.

Le choix retenu pour identifier les utilisateurs est via l'association d'une étiquette RFID pour chaque personne. La lecture se fait via une antenne RFID connectée en USB à l'automate industriel ou à la Raspberry Pi. L'agent *RFIDAgent* écoute les messages sur le port USB correspondant. L'écoute se fait avec une lecture série. Le message transmis par l'antenne est une chaine de caractères de 12 caractères hexadécimaux. Cette chaine de caractères correspond au code unique inscrit dans chaque carte RFID. Cette carte RFID permet ensuite d'identifier la personne qui souhaite utiliser le système en associant le code RFID avec son profil. Cette information est contenue dans le fichier Profiles.json (Annexe B.1). L'agent *RFIDAgent* tri les codes RFID contenant une information connue (profil utilisateur) et les codes inconnus. En cas de succès, le code est envoyé vers le *UserAgent*.

Les personnes peuvent également s'identifier au système en utilisant leur application mobile. Cette solution remplace l'identification utilisant le tag RFID. L'application mobile reconnait automatiquement l'utilisateur courant de l'appareil mobile et connecte la personne au système au lancement de l'application. Les profils utilisateurs se présentent sous forme de fichiers de configuration. Lorsqu'un utilisateur souhaite se connecter au système, le système charge le

fichier de configuration correspondant à l'utilisateur (Annexe B). Ces fichiers de configuration contiennent un ensemble de paramètres permettant au système de se configurer pour cet usager précis. Lorsque l'agent *RFIDAgent* contacte le *UserAgent* pour indiquer la connexion d'un nouvel utilisateur, ce dernier charge le fichier de configuration de l'utilisateur en question et génère le profil utilisateur résultant. Ensuite, l'agent *UserAgent* déverrouille les équipements en vérifiant la capacité de déverrouillage et les plages horaires d'utilisation du profil. Finalement, ce profil résultant est transmis aux *RiskAgents*.

Parallèlement à la gestion des profils utilisateurs, le *UserAgent* gère également les capteurs de détection de présence des personnes dans l'environnement (PSu1 et PSu2). L'historisation permet de garder une trace à longue durée sur l'activité de la personne. Elle permet également aux aidants professionnels d'avoir de l'information sur l'évolution de l'activité de la personne atteinte (décalage chronologique de l'activité). Les aidants professionnels peuvent ensuite adapter le profil en fonction de l'évolution de la maladie de la personne atteinte.

### 4.3.3 Les RiskAgents

Nous choisissons de représenter les règles de sécurité élaborées [70] dans le Chapitre 2 par des *RiskAgents*. Ces agents ont pour nom le numéro de la règle de sécurité qu'ils surveillent (Tableau 6).

Tableau 6 - Liste des *RiskAgents* implémentés.

| N° de règle | Nom de l'agent RiskAgent associé | Description brève |
|---|---|---|
| 1 | Rule1 | Four activé et absence utilisateur pendant X minutes |
| 2 | Rule2 | Porte du four ouverte depuis X minutes |
| 3 | Rule3 | Four vide et activé depuis X minutes |
| 4 | Rule4 | Inactivité des appareils depuis X minutes |
| 5 | Rule5 | Rond activé mais vide pendant X minutes |
| 6 | Rule6 | Rond activé et absence utilisateur pendant X minutes |

Les *RiskAgents* se configurent en fonction du profil utilisateur résultant qu'ils reçoivent de la part du *UserAgent*. Cette configuration concerne les délais de passage entre les différents états des *RiskAgents* si un risque s'avère et qu'aucune action n'est menée par les utilisateurs pour y remédier (section 3.5.5).

Les messages issus des *DeviceAgents* et du *UserAgent* sont triés selon leur importance pour la règle. Pour cela, les messages transmis entre agents dans JADE ont des propriétés comme : Un expéditeur, un contenu, un identifiant de conversation, une langue et une ontologie. Dans le cadre de nos travaux, le tri sur l'expéditeur et l'identifiant de conversation est suffisant. L'information de l'expéditeur permet de connaitre l'origine du message, autrement dit, s'il s'agit d'une information concernant l'utilisateur ou le matériel si l'expéditeur est respectivement le *UserAgent* ou un *DeviceAgent*. Ensuite, connaissant l'expéditeur, les messages sont triés selon leur identifiant de conversation. L'identifiant de conversation

correspond à l'évènement qui s'est produit et qui a généré l'envoi de message. Le contenu quant à lui, contient la valeur de l'évènement, c'est-à-dire l'état de l'activité surveillé. Le *RiskAgent* connait alors l'état des éléments de l'appareil qu'il surveille. Si l'état des éléments est jugé dangereux l'agent diffuse une notification. Si aucun changement n'est observé par le *RiskAgent*, l'appareil est verrouillé par mesure de sécurité. Par exemple, l'agent *Rule1* reçoit les messages d'activité électrique avec l'identifiant de conversation *isDeviceActive* de la part de *DAOven*. Le contenu de ce message est une valeur booléenne indiquant si l'appareil vient d'être activé (valeur à 1) ou désactivée (valeur à 0). *Rule1* reçoit de la part de *UserAgent* un message avec l'identifiant de conversation *UserProfile* contenant le profil résultant des usagers. Ce message est reçu lorsqu'il y a une modification dans les personnes identifiées à StoveMAS. Ce profil résultant des usagers contient les variables de configuration de l'agent *Rule1* (délais de notification et verrouillage, heures d'accès aux appareils, etc.). *Rule1* reçoit également de *UserAgent* l'information de présence des usagers dans l'environnement proche des appareils. Avec ces informations, *Rule1* est capable de connaitre la présence ou l'absence des usagers et depuis combien de temps. De la même manière, il est capable de connaitre l'activité électrique du four et depuis combien de temps ce dernier est activé ou non. S'il n'y a pas d'usagers dans l'environnement et que le four est activé depuis trop longtemps, *Rule1* diffuse une notification. Si la situation n'évolue pas, *Rule1* verrouille le four. Les autres *RuleAgents* fonctionnent de la même manière.

## 4.4 La communication entre l'homme et la machine

La communication entre l'homme et la machine se fait via deux interfaces usagers. Le premier est un agent qui gère l'interface par défaut de StoveMAS. La deuxième est l'interface dont l'utilisateur dispose en se connectant au système depuis un appareil mobile.

### 4.4.1 L'agent de l'interface

L'agent de l'interface est un agent à part entière de StoveMAS et est constitué de trois éléments :

- La console d'exécution
- L'interface de contrôle
- L'interface des agents

Ces trois éléments permettent l'interaction avec les utilisateurs et sont détaillés dans les parties suivantes.

#### 4.4.1.1 La console d'exécution

La console d'exécution est la console dans laquelle StoveMAS a été exécutée (Figure 30). Elle s'affiche sur l'automate industriel ou la Raspberry Pi. Lorsque le système a été lancé, les différents agents sont compilés et exécutés dans la plateforme multi-agents JADE. Une fois que tous les agents s'exécutent, ils s'enregistrent auprès de l'agent DF : le système fonctionne. Dans cette console sont affichés tous les messages importants tels que les notifications de sécurité, les erreurs et les connexions des usagers sur toute la durée d'exécution de StoveMAS.

```
janv. 31, 2017 10:19:48 AM jade.core.messaging.MessagingService boot
INFOS: MTP addresses:
http://DINF-D60015-23A.DInf.FSCI.USherbrooke.ca:7778/acc
janv. 31, 2017 10:19:48 AM jade.core.AgentContainerImpl joinPlatform
INFOS: ----------------------------------------
Agent container Main-Container@10.44.160.9 is ready.
------------------------------------------------
------------------------
-      STOVEMAS        -
-     2013 -2016       -
- SYSTEM RUNNING ON PC -
------------------------
031:10:19:48.194 Rule3: correctly registered with DF
031:10:19:48.194 Rule3: correctly started
031:10:19:48.196 UserAgent: correctly registered with DF
031:10:19:48.197 UserAgent: correctly started
031:10:19:48.199 Rule1: correctly registered with DF
031:10:19:48.201 Interface: correctly registered with DF
031:10:19:48.203 WatchDogRule: correctly registered with DF
031:10:19:48.201 Rule1: correctly started
031:10:19:48.207 SecurityAgent: correctly registered with DF
031:10:19:48.205 WatchDogRule: correctly started
031:10:19:48.203 Interface: correctly started
031:10:19:48.213 Rule2: correctly registered with DF
031:10:19:48.212 WirelessAgent: correctly registered with DF
031:10:19:48.210 SecurityAgent: correctly started
031:10:19:48.210 DAOven: correctly registered with DF
031:10:19:48.208 DABurners: correctly registered with DF
031:10:19:48.223 DAOven: correctly started
031:10:19:48.219 WirelessAgent: correctly started
031:10:19:48.218 ADAMAgent: correctly registered with DF
031:10:19:48.217 Rule2: correctly started
031:10:19:48.216 Rule4: correctly registered with DF
031:10:19:48.233 ADAMAgent: correctly started
031:10:19:48.225 DABurners: correctly started
031:10:19:48.238 Rule4: correctly started
```

Figure 30 - La console d'exécution de StoveMAS.

#### 4.4.1.2 L'interface de contrôle

L'interface de contrôle permet de gérer l'affichage de StoveMAS et l'acquisition des données (Figure 31). Cette interface s'affiche également sur l'automate industriel ou la Raspberry Pi. Elle a été réalisée avec *Java Swing*. Les différentes fonctionnalités de cette interface sont expliquées dans l'ordre de haut en bas visible sur l'interface.

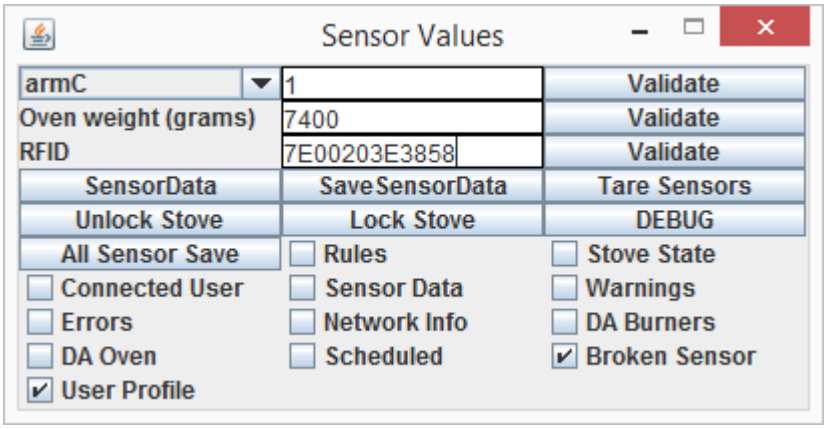



Figure 31 - Interface de contrôle de StoveMAS.

- A l'aide de la première ligne de l'interface, on peut manuellement entrer une valeur pour un capteur pour en simuler son fonctionnement. C'est une fonctionnalité pratique lorsqu'un capteur ne répond pas ou lorsqu'on souhaite tester une nouvelle fonctionnalité du programme. Pour cela, on sélectionne le capteur dans la liste déroulante à gauche, on entre une valeur dans la zone de texte du centre et on clique le bouton valider à droite.

- La deuxième ligne permet de définir la masse de l'équipement (en grammes) et de faire des calculs de masse sur les produits placés sur la plaque de cuisson et dans le four. Aujourd'hui, cette fonctionnalité reste à améliorer car les résultats sont très imprécis.

- Ensuite, à la troisième ligne, il est possible de manuellement entrer un code RFID dans le système. Ajouter manuellement des codes RFID permet de tester des fonctionnalités et simuler l'arrivée et le départ d'utilisateurs lorsqu'on ne dispose pas des cartes RFID physiques.

- La quatrième ligne propose 3 boutons.

    - Le bouton *SensorData*, à gauche, permet d'afficher sur la console d'exécution l'historique des valeurs du capteur sélectionné dans la liste déroulante à la première ligne. Ces valeurs sont affichées dans une liste de paires <*valeur, date de mise à jour*>.

    - Le bouton *SaveSensorData* permet d'enregistrer dans un fichier, au nom de la date de l'enregistrement et du capteur, les valeurs d'historique du capteur sélectionné dans la liste déroulante à la première ligne. Ce fichier se retrouve dans le dossier actif dans lequel StoveMAS a été exécuté. Le contenu de ce fichier contient trois colonnes : (1) La date de la donnée, (2) l'intervalle de temps entre l'heure d'enregistrement du fichier et l'heure d'enregistrement de la

donnée et (3) la valeur de la donnée. L'intervalle de temps entre l'heure d'enregistrement du fichier et l'heure d'enregistrement de la donnée permet de facilement afficher les données sur un graphique. Le bouton *All Sensor Save* a la même fonction, mais permet d'enregistrer les informations de l'ensemble des capteurs et génère un fichier par capteur.

- ♦ *TareSensors* permet, comme son nom l'indique, de faire un tarage des capteurs. Le tarage est un simple calcul de la moyenne de valeurs relevées dans l'historique. Cela permet, lorsque l'appareil demeure vide pendant ce laps de temps, de connaitre la valeur moyenne relevée par les capteurs. Il est possible de comparer cette valeur de tarage à des valeurs relevées lorsque l'appareil est en charge pour calculer la masse. Cette valeur est enregistrée dans une variable *sensortarevalue* propre à chaque capteur.

- La ligne suivante propose également 3 boutons avec les fonctionnalités suivantes :
  - ♦ Un bouton *Unlock Stove* pour déverrouiller les équipements.
  - ♦ Un bouton *Lock Stove* pour verrouiller les équipements.
  - ♦ Un bouton *DEBUG* qui n'a aucune action associée pour le moment. Des fonctions peuvent être attribuées à ce bouton lors de l'élaboration de nouvelles fonctionnalités.

- Les cases à cocher suivantes permettent l'affichage d'informations diverses sur la console d'exécution.
  - ♦ *Rules* : affiche l'état des différentes règles de sécurité dans le système.
  - ♦ *StoveState* : donne périodiquement (réglé à 1 seconde) l'information de l'état des différents équipements.

- *Connected User* : affiche les noms des personnes connectées sur le système.
- *SensorData* : fournit les données brutes des capteurs lues par l'agent d'acquisition.
- *Warnings* : affiche les différents messages liés au verrouillage du système et autres notifications.
- *Errors* : affiche les différents messages liés aux erreurs dans le système.
- *NetworkInfo* : permet de connaitre si StoveMAS peut communiquer avec une adresse distante, ce qui peut être pratique pour vérifier si StoveMAS a accès à des données capteurs distants par exemple.
- *DABurners* et *DAOven* : dans la même philosophie que la case à cocher *Rules*, permet d'afficher les données liées à l'activité d'un équipement en particulier. En cochant, l'interface affiche des données sur l'état de l'équipement en question et les différents évènements qui ont lieu.
- *Scheduled* : permet d'afficher les messages en rapport avec les vérifications périodiques. Les vérifications périodiques sont des vérifications qui ont lieu à heure fixe dans une journée ou dans la semaine. Ces vérifications permettent de faire un autodiagnostic du système ou d'autres tâches longues pendant la nuit par exemple.
- *Broken Sensor* : Ce bouton permet d'activer ou non l'affichage des capteurs en panne.
- *User Profile* : Ce bouton permet d'afficher le profil utilisateur résultant des utilisateurs connectés au système.

#### 4.4.1.3 L'interface des agents

L'interface des agents est l'interface graphique de JADE (Figure 22). Cette interface présente les agents qui fonctionnent dans StoveMAS. Elle présente les fonctionnalités de déverminage, comme par exemple l'affichage des messages entre agents (Sniffer Agent, par défaut dans JADE), l'ajout et le retrait manuel des agents ou encore l'envoi manuel de messages. Cette interface est optionnelle car elle n'apporte rien pour le fonctionnement nominal du système.

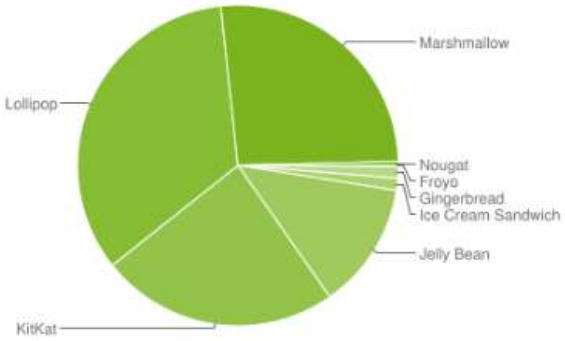
### 4.4.2 L'application mobile

L'application mobile propose une interface mobile utilisable pour les usagers pour l'affichage des notifications. Cette interface affiche les mêmes informations que celles affichés sur la console d'exécution. Cette application communique avec le système par le biais de l'agent *WirelessAgent*.

#### 4.4.2.1 Introduction

En 2015, la plateforme Android détient 82.8% du marché des smartphones [72]. A cause de cette popularité et de l'évolution des technologies modernes, des nouvelles versions apparaissent régulièrement. Il faut alors faire un compromis entre les fonctions embarquées par l'application et l'étendue des appareils compatibles. Plus l'appareil mobile est ancien, moins il contient de fonctionnalités et moins la dernière version d'Android compatible est élevée. 84.7% des appareils Android sur le marché utilisent une version d'Android 4.4 ou plus récente (Figure 32) [73]. Dans nos travaux, on se limitera à une rétrocompatibilité jusqu'à la version 4.4, qui semble un bon compromis entre les fonctionnalités disponibles et le nombre d'appareils compatibles. Les appareils mobiles qui sont utilisés lors du développement sont des Nexus 7 (modèle 2013) du fabricant Asus. Ces appareils fonctionnent avec la version 6.0 du système d'exploitation.

| Version | Codename | API | Distribution |
|---|---|---|---|
| 2.2 | Froyo | 8 | 0.1% |
| 2.3.3 - 2.3.7 | Gingerbread | 10 | 1.2% |
| 4.0.3 - 4.0.4 | Ice Cream Sandwich | 15 | 1.2% |
| 4.1.x | Jelly Bean | 16 | 4.5% |
| 4.2.x | | 17 | 6.4% |
| 4.3 | | 18 | 1.9% |
| 4.4 | KitKat | 19 | 24.0% |
| 5.0 | Lollipop | 21 | 10.8% |
| 5.1 | | 22 | 23.2% |
| 6.0 | Marshmallow | 23 | 26.3% |
| 7.0 | Nougat | 24 | 0.4% |




*Data collected during a 7-day period ending on December 5, 2016.*

Figure 32 - Les différentes distributions d'Android utilisées dans le monde (décembre 2016).

#### 4.4.2.2 Mécanismes d'identification

Dans le cadre de nos travaux, il est essentiel d'identifier les usagers. On souhaite, par facilité d'usage pour les utilisateurs, qu'ils soient capables de s'identifier au système par le biais de leur appareil mobile. D'une part, on a besoin d'une faible portée pour qu'il n'y ait pas des confusions de détection des usagers par le système. D'autre part, nous avons besoin d'une technologie existante dans l'appareil mobile pour que le plus grand nombre d'appareils mobiles soient compatibles. Nous avons identifiés 3 technologies qui pourraient répondre à ce besoin : La technologie Bluetooth, la lecture de codes-barres et la technologie NFC.

La technologie Bluetooth est déjà existante dans les appareils mobiles. L'identification de l'usager peut se faire via une connexion entre son appareil mobile et StoveMAS. Un identifiant unique par appareil mobile permettrait d'identifier alors l'usager. Cependant, la technologie

Bluetooth a une grande portée qui pourrait fausser la détection des usagers dans l'environnement. Des usagers localisés dans d'autres pièces de l'habitat pourraient, à leur insu, se connecter à StoveMAS. De plus, cette technologie permet seulement la connexion entre deux appareils à la fois, ce qui n'est pas compatible avec une identification de plusieurs usagers.

La lecture par code-barres (QR code) est une alternative peu couteuse et possible avec des appareils mobiles disposant d'une caméra. Cependant, cette technologie est contraignante pour des personnes atteintes de la maladie d'Alzheimer.

La technologie NFC (Near Field Communication) est une technologie très répandue sur les appareils mobiles. Cette technologie est semblable à la technologie RFID, mais pour des distances de détection plus faibles. Dans le cadre des travaux, la portée de détection et la démocratisation du NFC dans les appareils mobiles sont un atout. La démocratisation de cette technologie la rend facile d'accès et pour un faible coût.

Dans le cadre de ces travaux, nous avons confrontés ces technologies et nous avons retenu la technologie NFC pour l'identification des usagers (Tableau 7).

Tableau 7 - Comparaison des technologies d'identification sur les appareils mobiles.

| Technologie | Avantages | Inconvénients |
|---|---|---|
| Bluetooth | • Technologie déjà existante sur les appareils mobiles | • Grande portée<br>• Une connexion seulement entre deux appareils |
| Code barres | • Peu couteux | • Difficile d'usage pour le public visé |
| NFC | • Technologie répandue sur les appareils mobiles<br>• Peu cher | • L'étiquette peut être égarée |

La technologie NFC permet, comme son nom l'indique, de communiquer avec des appareils à faible distance, de l'ordre de quelques centimètres. Cette technologie est en plein essor et compte de plus en plus d'appareils compatibles : proche de 600 millions d'appareils estimés compatibles en 2015 [74]. Sur les appareils Android, cette technologie est compatible à partir de la version 2.3, c'est-à-dire que les équipements visés par nos travaux sont compatibles. Cette technologie est utilisée pour avoir des informations ponctuelles telles que l'horaire des bus, la composition d'un produit au supermarché etc. Dans le commerce, on peut retrouver des étiquettes NFC sous forme de porte-clés, de cartes plastiques ou d'autocollants. Des étiquettes NFC passives sont utilisées dans nos travaux pour identifier l'utilisateur qui souhaite utiliser le système. Le type d'étiquettes NFC utilisés dans nos travaux respectent la norme NTAG203 et répondent à une fréquence de 13.56MHz. Ils se présentent sous forme d'un autocollant ou d'une carte en plastique. Il existe plusieurs types d'étiquettes et de normes différentes, mais la norme NTAG203 est adaptée pour une utilisation avec des smartphones et des tablettes tactiles. Pour nos travaux, une étiquette NFC est disponible proche de la cuisinière et permet l'identification de la personne auprès du système. La tablette tactile Nexus 7 possède un lecteur d'étiquettes NFC. Pour s'identifier, la personne approche son appareil mobile, avec l'application préalablement exécutée, devant l'étiquette NFC et l'application enverra automatiquement l'identifiant de l'utilisateur à StoveMAS. Cette procédure est identique que l'identification en utilisant les étiquettes RFID. Lorsque l'application mobile est exécutée, elle allume automatiquement l'antenne NFC de l'appareil via une permission dans le fichier *AndroidManifest.xml*. La détection d'une étiquette NFC exécute une méthode dans l'application qui va identifier le code unique contenu dans l'étiquette et le transmettre au *WirelessAgent*.

#### 4.4.2.3 L'interface mobile

L'interface sur la tablette tactile doit être facile d'usage et facilement compréhensible pour des personnes ayant des troubles cognitifs. La tablette a l'avantage d'être emportée avec la personne. L'interface doit rester la plus simple possible. Lorsque la personne lance l'application, cette dernière recherche les informations concernant la session d'utilisateur

ouverte. Avec Android, il existe un patron permettant de récupérer l'adresse courriel de l'utilisateur actif (Figure 33).

```
1.  Pattern emailPattern = Patterns.EMAIL_ADDRESS;
2.  Account[] accounts = AccountManager.get(this).getAccounts();
3.  for (Account account : accounts) {
4.      if (emailPattern.matcher(account.name).matches()) {
5.          accountName = account.name;
6.      }
7.  }
```

Figure 33 - Algorithme permettant l'obtention de l'adresse courriel de l'utilisateur courant.

Ce code parcourt la liste d'utilisateurs de l'appareil mobile et récupère l'adresse courriel de l'utilisateur actif. On utilise cette information pour identifier l'utilisateur courant et configurer le système pour s'adapter au profil médical de la personne. Nous disposons alors de deux manières d'identifier les personnes via l'appareil mobile : via les étiquettes NFC et via l'adresse courriel de la personne.

Sur l'interface de l'application mobile, l'utilisateur a accès à des informations sur l'état des risques de sécurité et l'état des appareils de cuisine. Lorsqu'un risque de danger a été détecté par un des agents de risques du système, il envoie un message sur l'interface de l'appareil mobile pour prévenir l'utilisateur qu'un risque potentiel est présent. Cette notification est accompagnée d'une explication des tâches à réaliser afin de rendre l'activité de préparation de repas sécuritaire à nouveau. Lorsque la personne a accompli ces taches et que les agents de risque ne détectent plus de risque, les notifications ne sont plus transmises à l'interface. Dans le cas contraire, les agents de risque verrouillent l'appareil de cuisine et notifient l'utilisateur de la raison pour laquelle le système aura été verrouillé.

#### 4.4.2.4 Les capteurs embarqués

Chaque appareil mobile embarque un ensemble de capteurs différents. L'application récolte des informations concernant tous les capteurs embarqués dans l'appareil tels que leur nom, leur valeur ainsi que la valeur maximale que peut atteindre le capteur. Ces différentes informations

sont récoltées lorsque l'application mobile est lancée et fonctionnera en tâche de fond tout au long de l'exécution de l'application. Ces informations sont directement disponibles via le *Sensor framework* dans Android. Lorsque la valeur d'un capteur change, un évènement est produit et la méthode *onSensorChanged* est exécutée (Figure 34).

```
1.  public void onSensorChanged(SensorEvent event) {
2.      Sensor sensor = event.sensor;
3.
4.      // Send to server
5.      sensor.getName();
6.      sensorType = sensor.getStringType(); // Android API 19 (4.4) and higher
7.      event.values[0];
8.      sensor.getMaximumRange();
9.  }
```

Figure 34 - Code permettant d'obtenir les informations des capteurs embarqués.

Dans cet exemple de code, on récupère le nom, le type, la portée, ainsi que la valeur du capteur. La valeur est sous forme de tableau car certains capteurs donnent des informations composées. Par exemple, un accéléromètre fournit des informations sur l'accélération sur les trois axes dans l'espace. On ajoute à ces données capteurs l'identifiant de la personne afin de garder une trace de l'origine de ces capteurs. Ces données sont ensuite envoyées vers le système et intégrées dans la base de données afin d'enrichir la connaissance du système de son environnement. La tablette tactile que nous utilisons, dispose des capteurs suivants (Tableau 8) :

Tableau 8 - Liste des capteurs embarqués dans l'Asus Nexus 7 (modèle 2013).

| Capteurs | |
|---|---|
| MPL Accelerator | Linear Acceleration |
| AKM Magnetic Field | Rotation Vector |
| Orientation | Significant Motion |
| Lite-On Ambient Light Sensor | Game Rotation Vector |
| MPL Gyroscope | Gravity |

Lorsque la connexion entre l'appareil mobile et le serveur est rompue, comme par exemple lorsque l'utilisateur quitte l'application, que l'appareil mobile est éteint ou que l'appareil mobile quitte l'habitat intelligent, toutes les données concernant les capteurs embarqués sont effacées de la base de données et l'utilisateur est déconnecté du système. Ces données sont effacées car elles ne sont plus représentatives.

#### 4.4.2.5 La gestion multi-utilisateurs

Depuis la version 4.2 d'Android, il est possible, sur un même appareil mobile, de gérer plusieurs utilisateurs. Chaque compte d'utilisateur a ses propres applications auxquelles les autres utilisateurs n'ont pas accès. Le changement d'utilisateur se fait au niveau de l'écran de déverrouillage de l'appareil mobile. Pour accéder à son compte, un utilisateur doit d'abord sélectionner son compte sur l'écran de déverrouillage, puis déverrouiller l'appareil. Le compte de l'appareil et l'identifiant de StoveMAS utilisent ensemble un identifiant identique : l'adresse courriel de la personne. Ainsi, lorsque la personne accède son compte sur son appareil mobile, l'application récupère l'adresse courriel de la personne active.

## 4.5 Conclusion

Dans ce chapitre, une description détaillée de StoveMAS a été présentée. Deux implémentations différentes du système montrent sa flexibilité vis-à-vis du matériel sur lequel il est déployé. Le système a été décrit en détail en deux parties : D'une part, la description du fonctionnement des différents équipements au sein des deux laboratoires et d'autre part, la description des utilisateurs. La description de l'instrumentation dans les différents laboratoires met en avant les parties fixes et les parties variables du système. En effet, la partie d'analyse des utilisateurs et du matériel reste inchangée quel que soient les équipements disponibles. Cependant, l'acquisition des données dépend des équipements et de l'interfaçage des capteurs. L'identification des utilisateurs se fait de la même manière pour les deux implémentations, c'est-à-dire soit en présentant un tag RFID au système, soit en s'y connectant depuis un terminal mobile. L'analyse des risques ne dépend pas du matériel non plus, cependant elle

dépend des usagers connectés. La Figure 35 synthétise l'ensemble des communications présentes dans notre système. L'usager se connecte au système soit via les étiquettes RFID, soit en exécutant l'application mobile qui peut identifier la personne soit via son adresse courriel soit via des étiquettes NFC. L'usager agit sur les appareils de cuisine pour préparer son repas. Son activité est observé par des capteurs dans les appareils et dont les informations sont transmises vers le système multi-agents. Ce dernier permet, dans un premier temps, de notifier l'usager via différentes interfaces de l'état de sécurité de son activité. Dans un second temps, le système multi-agents peut agir, par mesure de sécurité, sur le matériel.

Dans le chapitre suivant, le fonctionnement du système sera mis à l'épreuve avec les différents scénarios de tests.

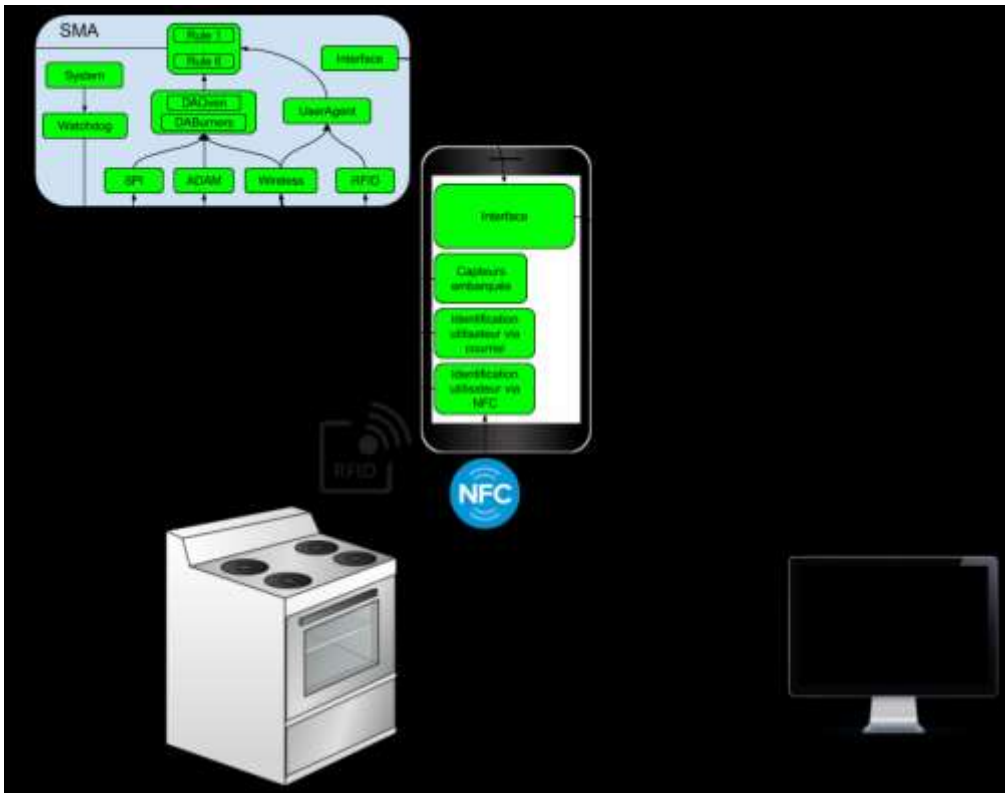



Figure 35 - Communications entre l'homme et StoveMAS.

# Chapitre 5

# Résultats

Lors de ces travaux, des expérimentations en lieux réels sont réalisés. Ces expérimentations permettent de valider l'acceptabilité de StoveMAS vis-à-vis des personnes qui vont utiliser ce système. Pour cela deux scénarios ont été élaborés : un scénario par lieu d'expérimentation. Les expérimentations se feront d'une part au laboratoire Lab-STICC, en partenariat avec le CMRRF (Centre Mutualiste de Rééducation et de Réadaptation Fonctionnelles) de Kerpape et d'autre part au laboratoire DOMUS (DOmotique et informatique Mobile à l'Université de Sherbrooke).

## 5.1 Les scénarios

Pour tester les fonctionnalités de notre système, plusieurs scénarios ont été érigés. Ces scénarios ont été inspirés par les scénarios du projet de l'assistant culinaire au laboratoire DOMUS pour leur déroulement et format, et des scénarios présents dans les travaux de M. Castebrunet [75] pour les noms des figurants. Les scénarios présentent plusieurs personnes fictives qui représentent des archétypes d'utilisateurs appelés persona [76]. Les personas réalisés dans le cadre de ces travaux sont les suivants.

- René, une personne âgée atteinte de la maladie d'Alzheimer en stade modéré.
- Jeanne, la compagne de René, est une personne saine qui vit dans le même habitat.
- Claude, une personne âgée atteinte de la même maladie que René (pas présent dans les scénarios, mais présent dans les autres tests). Ce persona permet de tester le

fonctionnement de StoveMAS lorsque les usagers sont plusieurs personnes atteintes de déficiences.

- Georges, un aidant professionnel, qui suit la maladie de René et de Claude. (pas présent lors des scénarios, mais permet de faire des tests avec la connexion multi-usager).

Ces scénarios permettent de valider les objectifs posés pour nos travaux. Pour cela, différents scénarios d'usage (scénario 1 à 3) ont été élaborés. Ces scénarios d'usage présentent des personas qui sont incarnés par des étudiants bénévoles de l'université et permettent de tester le système lors d'un usage normal. Les scénarios 4 et 5 permettent de tester le fonctionnement du système à un plus bas niveau. Le premier scénario se déroule comme suivant (Les autres scénarios se trouvent en Annexe F) :

### 5.1.1 Scénario 1 : Rond vide

Conditions initiales :

- Se déroule au laboratoire DOMUS.
- Seul René est présent.
- La cuisinière est fonctionnelle et verrouillée.
- StoveMAS est installé et fonctionnel sur la cuisinière.

Déroulement :

1) René s'identifie au système.
2) Il remplit une casserole d'eau, la place sur le rond avant gauche de la cuisinière.
3) Il active le deuxième bouton en partant de la gauche de la cuisinière.

4) Il s'assoit dans le canapé pour écouter la télévision.

Résultat attendu :

Le bouton activé ne correspond pas au rond sur lequel la casserole d'eau a été placée, le système doit observer une présence sur le rond avant gauche, mais une activité sur le rond arrière gauche est détectée. Une notification doit être transmise à René au bout de 15 secondes et lui indiquer l'erreur. René ignore la notification et le système verrouille la cuisinière par mesure de sécurité au bout de 15 secondes supplémentaires.

Variables d'observation :

Pour valider le fonctionnement de ce scénario, on doit observer l'activité qu'enregistre l'agent *DABurners* via l'interface de contrôle. Cet agent doit détecter la présence de la casserole d'eau sur le rond avant gauche et l'activité électrique sur le rond arrière gauche. Ensuite, l'erreur de René est relevée par l'agent *Rule5* (Tableau 6). Pour vérifier l'envoi de la notification, on observe dans la console d'exécution la notification horodatée qui doit s'afficher. Il en est de même pour le message indiquant le verrouillage de l'appareil. Les délais pour la notification et le verrouillage de l'appareil peuvent être vérifiés avec les paramètres de l'agent *Rule5* et du profil utilisateur de René.

Les scénarios permettent de tester plusieurs fonctionnalités du système. Le premier scénario met en avant l'utilisation du système par une personne ayant des déficiences cognitives et l'adaptation des règles de sécurité par son profil médical. Le deuxième scénario met en avant l'utilisation d'autres règles de sécurité sur une fonctionnalité différente de la cuisinière. Le troisième scénario met en avant l'utilisation multi-usager du système et l'adaptabilité des règles vis-à-vis des utilisateurs connectés. Les scénarios 4 et 5 ne sont pas des scénarios d'usage, mais plutôt des scénarios de test permettant de valider le fonctionnement du système à bas niveau (Tableau 9). Le dernier objectif (section 2.7.4), concernant le déploiement du système sur des équipements hétérogènes (plaques de cuisson et four à micro-ondes), n'est pas adressé par un

scénario en particulier, mais plutôt à travers le fonctionnement de StoveMAS sur les équipements dans les deux laboratoires.

Tableau 9 - Objectifs adressés par les scénarios.

| N° de scénario | Section de l'objectif associé |
|---|---|
| 1 | 2.7.1 et 2.7.3 |
| 2 | 2.7.1 et 2.7.3 |
| 3 | 2.7.1, 2.7.2 et 2.7.3 |
| 4 | 2.7.1 et 2.7.2 |
| 5 | 2.7.1 et 2.7.2 |

## 5.2 Le domicile multi-usager

Lors du développement de StoveMAS, les différentes fonctionnalités ont été testées et validées lors d'une session d'expérimentations. Dans le cadre de ces vérifications, l'interface graphique de contrôle constitue un outil pratique pour rapidement analyser les résultats.

Une première étape constitue à identifier les utilisateurs. Pour cela, ils disposent chacun d'un tag RFID propre :

- René : 7E00203E3858
- Jeanne : 7E002051C2CD
- Claude : 7E00203E3859 (persona non présente lors des scénarios)
- Georges : 7E00203E3860 (persona non présente lors des scénarios)

Pour les expérimentations, nous avions seulement deux étiquettes RFID à notre disposition. Initialement, aucun utilisateur n'est connecté au système. Lorsque René s'identifie, on s'attend

qu'en retour, le système charge le profil associé à René : *Rene.json*, et on lui demande d'afficher le profil résultant sur la console (Figure 36). Dans cette figure, on remarque à la première ligne que l'agent *UserAgent* détecte un changement d'utilisateurs. Initialement, aucun usager n'était connecté à StoveMAS. Ensuite, lorsque René se connecte, un évènement se produit et l'agent détecte un changement dans les utilisateurs connectés et affiche le profil résultant. Dans ce cas, le profil résultant correspond au profil médical de René (Annexe B.2). Ce même exercice est répété avec le profil et l'étiquette RFID de Jeanne (Figure 37). L'identification de ces deux personas est également concluante lorsqu'on entre les étiquettes RFID directement dans l'interface graphique de contrôle.

```
315:10:52:00.574 UserAgent: Connected users have changed, new profile:
{
  "coaching_ability": -1,
  "oven": [
    {
      "id": "bake",
      "activated": "true"
    },
    {
      "id": "broil",
      "activated": "true"
    }
  ],
  "device_lockdown_time_before_use": 200000,
  "unlock_times": [
    {"format": "HH:mm:ss"},
    {
      "start": "11:30:00",
      "end": "13:00:00"
    },
    {
      "start": "19:00:00",
      "end": "21:00:00"
    }
  ],
  "name": "Rene ",
  "device_lockdown_time_after_use": 240000,
  "user_absence_time": 300000,
  "oven_door_open_time": "20000",
  "empty_oven_active_time": "15000",
  "unlock_capable": "false",
  "email": "labdomus.rene@gmail.com ",
  "surface_burner": [
    {
      "id": "fl",
      "activated": "true"
    },
    {
      "id": "rl",
      "activated": "false"
    },
    {
      "id": "rr",
      "activated": "false"
    },
    {
      "id": "fr",
      "activated": "true"
    }
  ]
}
```

Figure 36 - Chargement du profil médical de René. On retrouve notamment René dans le champ *name* et la nécessité d'être encadré par une personne (*coaching ability*) pour profiter pleinement des appareils.


Figure 37 - Chargement du profil médical de Jeanne. On y retrouve notamment Jeanne dans le champ *name* et sa capacité à encadrer une personne (*coaching ability*).

Pour réaliser un test complet d'identification des utilisateurs on doit tester l'identification de plusieurs personnes en simultané. Dans ces tests, la clé « *coaching_ability* » (capacité d'encadrement) est mise en avant, car, elle permet au système de savoir s'il faut charger le profil de la personne déficiente ou le profil de la personne encadrante (ici Jeanne) comme indiqué dans la Figure 10. Deux cas de figure se présentent :

- Lorsqu'une ou plusieurs personnes déficientes s'identifient avec une personne encadrante (mais que la capacité d'encadrement reste nulle ou positive).

- Lorsque plusieurs personnes déficientes s'identifient (capacité d'encadrement strictement négative).

Dans le premier cas, le profil résultant doit correspondre au profil de la personne encadrante (ici Jeanne). Peu importe l'ordre dans lequel les utilisateurs se connectent (René puis Jeanne, ou Jeanne puis René), le profil résultant correspond au profil de Jeanne (Figure 37). Dans cette figure, seulement le nom de Jeanne parait dans le profil résultant, car c'est son profil qui est chargé lorsque ces deux usagers s'identifient.

Dans le deuxième cas de figure, le profil résultant correspond au pire des cas pour chaque caractéristique de l'ensemble des profils individuels. Pour tester cette fonctionnalité, les deux personas déficientes René et Claude se connectent au système. Également dans ce cas, le profil résultant ne dépend pas de l'ordre dans lequel les profils s'identifient. Le profil médical de René, le contraignait seulement à utiliser les deux ronds du devant de l'appareil car il risque de se brûler le bras avec le rond à l'avant s'il fait chauffer un rond à l'arrière. Son profil permet une utilisation de toutes les fonctionnalités du four. Cependant, Claude, n'a accès seulement qu'au rond avant gauche et ne peut utiliser que le mode cuisson du four. Si René et Claude s'identifient ensemble, et que le système est configuré à ne considérer seulement que le pire des cas, le profil résultant ressemble à ce qui figure à la Figure 38. Les plages horaires d'utilisation du midi pour René lui permettent d'utiliser le système entre 11h30 et 13h00, pour Claude, cette plage horaire se limite à une utilisation entre 12h30 et 14h00. La plage d'utilisation résultante dans le cadre du pire cas, correspond à une utilisation entre 12h30 et 13h00. Malgré que cette solution ne soit pas retenue dans nos travaux, ce même test est effectué en prenant les mêmes personas mais en prenant le meilleur des cas (Figure 39). Les résultats

illustrés dans la Figure 38 et la Figure 39 peuvent être comparés par les informations contenus dans les profils individuels de René et Claude dans l'Annexe B.


Figure 38 - Profil résultant de l'identification de René et Claude en prenant le pire des cas.


Figure 39 - Profil résultant de l'identification de René et Claude en prenant le meilleur des cas.

On remarque, par le biais de ces tests, que le système charge correctement le profil correspondant. Dans le cas de plusieurs utilisateurs, le système génère correctement un profil correspondant à l'ensemble des utilisateurs connectés. Pour rappel, ces tests permettent de

valider la preuve de concept et ne correspondent en aucun cas à une utilisation réelle et pratique par des personnes réelles.

Au vu de la réponse du système vis-à-vis de la connexion des utilisateurs, on peut considérer que ce dernier répond correctement aux trois objectifs imposés concernant le domicile multi-usagers (section 2.7.1), à savoir :

- Réaliser un système personnalisable selon : le profil médical de la personne, ses préférences ainsi que le contexte.
- Pouvoir identifier plusieurs personnes.
- Dans le cas d'un usage multi-utilisateur, pallier aux handicaps des uns sans contraindre l'utilisation du système des autres.

## 5.3 L'évolution de l'environnement

Dans chaque laboratoire, le système acquiert ses données issues des capteurs d'une manière différente. Ces différences sont homogénéisées au niveau de la couche d'historisation dans le système. Lors du lancement du système, l'historique de chaque capteur est vide et se remplit au fur et à mesure que le flux de données entre dans le système.

### 5.3.1 Campagnes de mesures

Au laboratoire Lab-STICC, plusieurs campagnes de mesures ont été effectuées pour étudier l'évolution des données capteurs selon l'activité du matériel. Lors du scénario 4 : Réchauffer un plat (Annexe F.3), les données capteurs ont été enregistrées à l'aide de l'interface graphique de contrôle. Pour une meilleure compréhension, ces données sont affichées sur un graphique (Figure 40). Sur ce graphique, on a les informations concernant les capteurs de force, les ampèremètres, ainsi que le capteur de contact de la porte du four à micro-ondes.

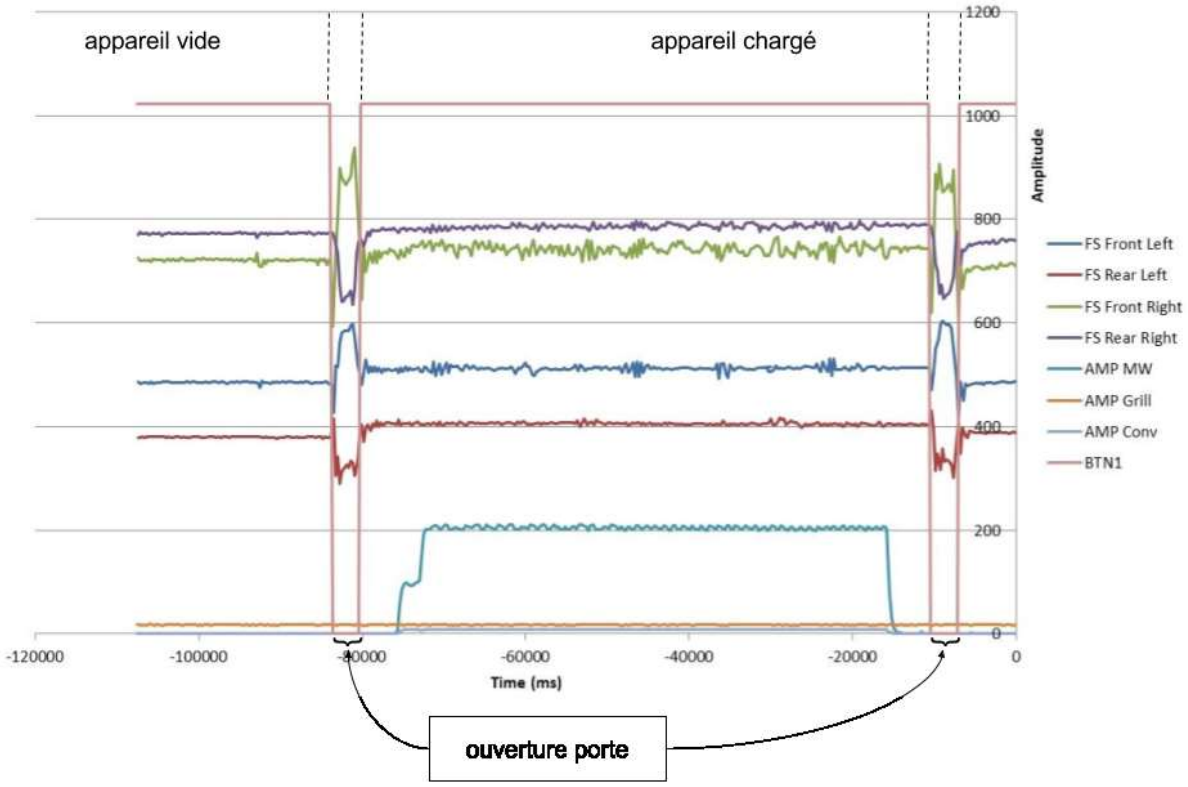



Figure 40 - Données de différents capteurs (pression, courant et contact) recueillis lors du scénario 4 : Réchauffer un plat. Données de l'appareil vide (à gauche) et activé et chargé (à droite)

La chronologie de ce graphique va de gauche à droite. Lorsque le four à micro-ondes est vide, on ne constate aucune activité électrique au sein de l'appareil. Cependant, les capteurs de force *FS* mesurent le poids à vide de l'équipement. Lorsque René ouvre la porte du four à micro-ondes, le capteur de contact *BTN1* passe en état logique bas et du bruit est mesuré au niveau des capteurs de force *FS*. Ce bruit est généré par l'ouverture de la porte qui déséquilibre l'appareil vers l'avant. Les capteurs de force à l'avant (*FS Front Left* et *FS Front Right*) de l'appareil mesurent une masse plus grande, les capteurs de force à l'arrière (*FS Rear Left* et *FS Rear Right*) mesurent une masse moindre. Lorsque René a placé son repas et referme la porte, le capteur de contact *BTN1* détecte la fermeture et les capteurs de force mesurent le poids de

l'appareil et son contenu. Lors de la troisième étape du scénario, chauffer le plat à 900W, l'ampèremètre situé sur le circuit électrique du four à micro-ondes *AMP MW* détecte une activité. On peut constater du bruit au niveau des capteurs de force *FS* lorsque l'appareil est en fonctionnement, Ce bruit vient des vibrations du transformateur haute tension du magnétron ainsi que du plateau tournant dans l'espace chauffant. L'appareil émet un signal sonore indiquant la fin de la cuisson des aliments. René ouvre la porte du four à micro-ondes et enlève son repas.

Durant ce scénario, il est possible d'estimer la masse du contenu dans le four à micro-ondes. Pour cela, lorsque les équipements sont inactifs, le système apprend les valeurs par défaut des capteurs et fait un tarage (actuellement une action manuelle de la part de l'utilisateur via l'interface de contrôle). Le calcul de la masse se fait ensuite lorsque le système détecte une activité électrique au sein de l'appareil. Le calcul de la masse se fait à l'aide l'équation suivante (Équation 1):

$$m_{produit} = \sum_{i=1}^{n} \left( FS_i - FS_{i_{moyen_{vide}}} \right) \frac{m_{FS_{MAX}}}{FS_{i_{MAX}}}$$

Équation 1 - Calcul de la masse d'un produit dans le four à micro-ondes en utilisant les valeurs maximales mesurables.

Dans cette équation, on retrouve :

- $m_{produit}$ : la masse estimée du produit à un instant donné, en grammes.
- $n$ : le nombre de capteurs de pression utilisés. Dans notre cas, nous utilisons 4 capteurs.
- $FS_i$ : la valeur que le système lit pour ce capteur de force.

- $FS_{i_{moyen_{vide}}}$ : la valeur de tarage du capteur déterminée par le système lorsque l'appareil est vide (actuellement obtenu manuellement via l'interface de contrôle).

- $m_{FS_{MAX}}$ : la masse maximale mesurable par ce capteur en grammes. Cette valeur dépend du type de capteur utilisé. Dans notre cas, nous utilisons des capteurs de type Flexiforce A201-25 qui peuvent mesurer au maximum une masse de 25 lb. (11.2kg). La valeur associée à cette variable est donc 11200 g.

- $FS_{i_{MAX}}$ : la valeur maximale lue par le système lorsque le capteur est en pleine charge. Cette valeur dépend de la résolution de l'acquisition des données. Dans notre cas, avec les composants MCP3008, la valeur maximale correspondante à cette variable est 1023 (encodage sur 10 bits). Cette valeur ainsi que $m_{FS_{MAX}}$ sont fixes et leur rapport vaut $\frac{11200}{1023} = 10.948$. C'est cette valeur qui est enregistrée dans StoveMAS pour faire le calcul de la masse.

Lorsque l'appareil est vide, $FS_i = FS_{i_{moyen_{vide}}}$ et par conséquent on retrouve une masse de produit nulle. Lors du scénario, la mesure de la masse du produit correspond à ce qui figure sur la Figure 41. On y retrouve les deux phases d'ouverture de porte de l'appareil où du bruit sur les signaux se produit. Lorsque l'appareil est actif, le bruit généré par le transformateur et le plateau tournant est cumulé.

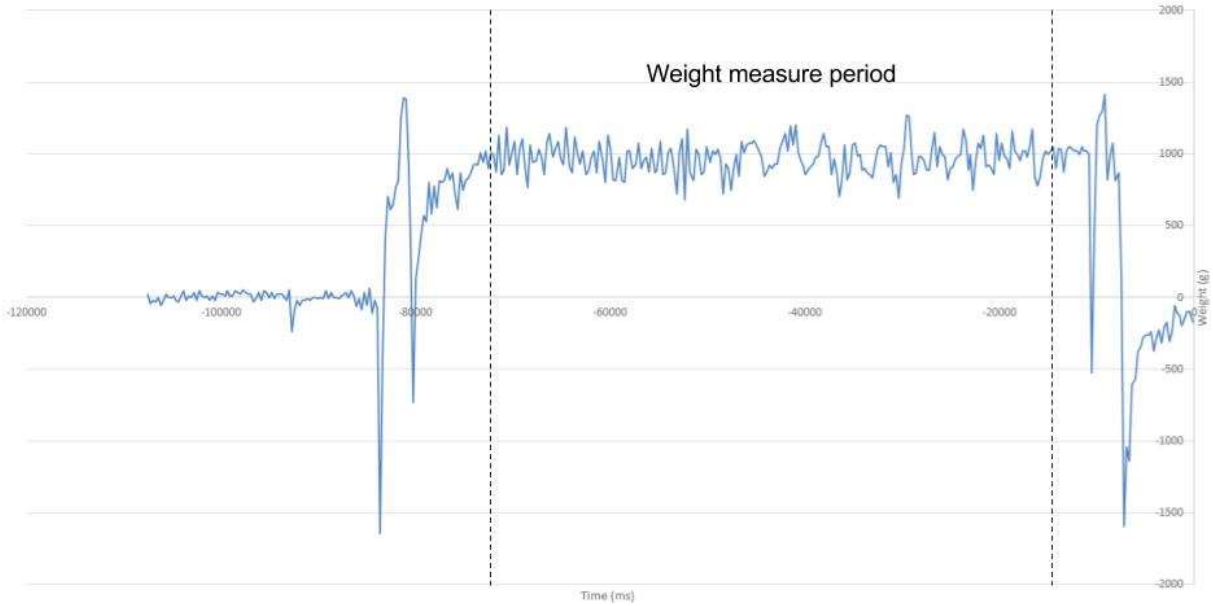



Figure 41 - Estimation de la masse du contenu dans le four à micro-ondes lors du scénario 4 : Réchauffer un plat en utilisant l'Équation 1.

La tasse utilisée était remplie pour avoir une masse exacte de 700 grammes. En faisant la moyenne de la mesure de la masse sur la période d'activité électrique de l'appareil, on mesure une masse moyenne de 966.48 grammes, soit une erreur de mesure de 38.07%. Cette erreur dépend de plusieurs facteurs.

- Le rapport $\frac{m_{FS_{MAX}}}{FS_{i_{MAX}}} = 10.948$ qui semble bon, mais les valeurs prises pour ces variables sont théoriques et jamais atteintes. Par exemple, la valeur maximale lue par le système ne peut atteindre la valeur de 1023, car la tension fournie par le montage électrique en entrée du convertisseur ne dépasse pas 4.2V (valeur maximale lue de 860) en utilisant le montage en Annexe C.1.

- Les erreurs de mesure propres aux capteurs.

Pour améliorer la précision du calcul du poids, on peut, au lieu de se baser sur le rapport $\frac{m_{FS_{MAX}}}{FS_{i_{MAX}}}$, se baser sur le rapport de la masse mesurée et la masse à vide de l'appareil qui est fixe et connue (Équation 2).

$$m_{produit} = \frac{m_{Equipement}}{FS_{moyen_{vide}}} \sum_{i=1}^{n} (FS_i) - m_{Equipement}$$

Équation 2 - Calcul de la masse d'un produit dans le four à micro-ondes en utilisant la masse de l'équipement.

Dans cette équation, on retrouve.

- $m_{produit}$ : la masse estimée du produit à un instant donnée, en grammes.
- $n$ : le nombre de capteurs de pression utilisés. Dans notre cas, nous utilisons 4 capteurs.
- $FS_i$ : la valeur que le système lit pour ce capteur de force.
- $FS_{moyen_{vide}}$ : la valeur moyenne de tarage de l'ensemble des capteurs de force lorsque l'appareil est vide.
- $m_{Equipement}$ : la masse de l'équipement à vide posé sur les capteurs de force. Dans notre cas, le four à micro-ondes a une masse de 17300 grammes (données constructeur).

En utilisant cette formule, on s'affranchit des variables liées à acquisition et aux capteurs. Cependant, il faut connaitre la masse de l'appareil pour disposer d'un étalon comparatif. En

utilisant cette formule sur les mêmes données que précédemment, on obtient la courbe suivante (Figure 42).

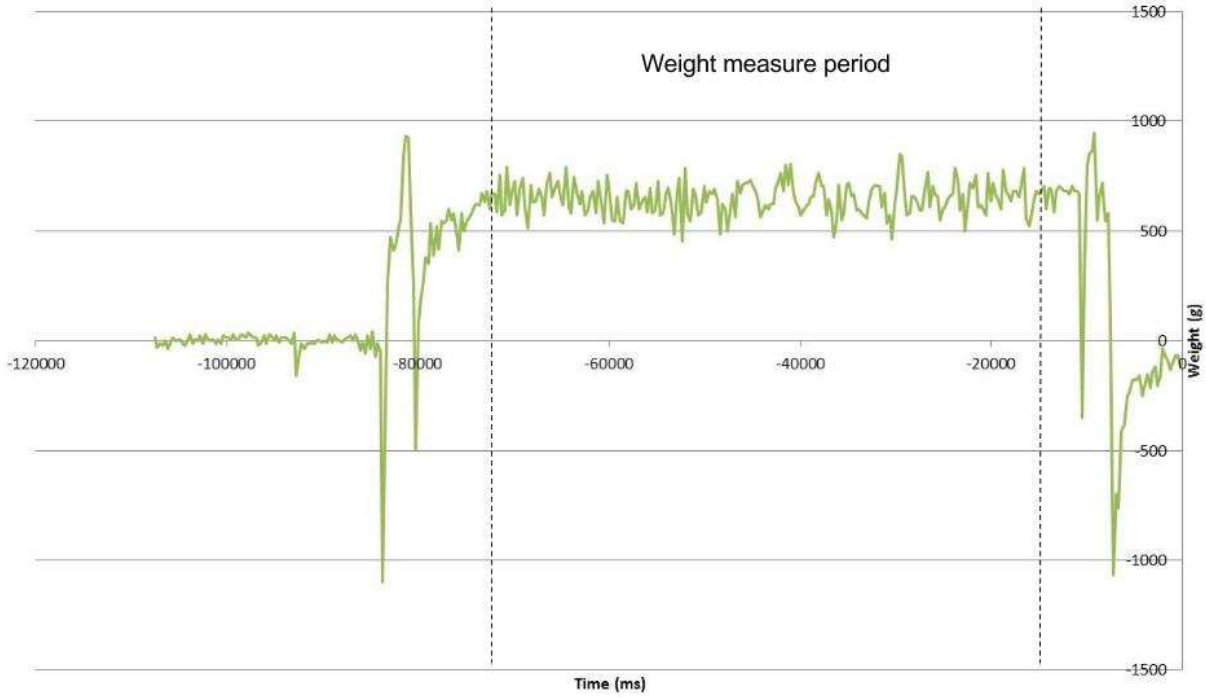



Figure 42 - Estimation de la masse des aliments dans le four à micro-ondes lors du scénario 4 : Réchauffer un plat en utilisant l'Équation 2.

En faisant la moyenne de la mesure de la masse sur la période d'activité électrique de l'appareil, on mesure une masse moyenne de 647.67 grammes, soit une erreur de mesure de 7.67%. On remarque qu'il est possible via l'étude des données issues de ces capteurs de connaitre l'activité du matériel et de calculer avec une précision plutôt bonne une masse au sein de l'équipement.

Grâce à ces tests, on a pu montrer qu'il est possible d'obtenir des informations contextuelles grâce à un réseau de capteurs. On considère que le premier objectif de la section 2.7.2 est atteint : Obtenir des informations contextuelles grâce à d'un réseau de capteurs.

### 5.3.2 Capteurs dynamiques

Lors du fonctionnement du système, les personnes peuvent s'identifier via leur appareil mobile au système. Lorsque la personne exécute l'application mobile et qu'elle se connecte à StoveMAS, elle transmet les informations des capteurs embarqués.

L'appareil mobile utilisé lors du développement est une tablette Asus Nexus 7 (2013). Cette tablette embarque 10 capteurs (Tableau 8). Lorsque la tablette se connecte au serveur, elle envoie à chaque évènement généré par un capteur les nouvelles informations du capteur source de l'évènement. On remarque que la plupart des capteurs embarqués sont reconnus. Trois capteurs n'apparaissent pas dans les données du système :

- *Linear Acceleration* : L'information du capteur *Linear Acceleration* est comprise dans la donnée de l'accéléromètre par la relation suivante (Équation 3)[77] :

$$acceleration_{axis} = gravity_{axis} + linear\_acceleration_{axis}$$

Équation 3 - Composition de l'accélération dans Android.

- *Significant Motion* : Ce capteur est particulier, il permet de réveiller une application lorsqu'un mouvement significatif a été détecté. Par conséquent, il n'envoie pas de données au système.

- *Orientation* : Ce capteur permet de connaitre l'orientation de l'appareil selon le système de coordonnées utilisé par Android (Figure 43). Le capteur *Orientation* utilise les rotations d'Euler, qui peuvent être inexploitables dans certaines conditions. L'utilisation du capteur *Rotation Vector* lui a été préféré car il utilise les quaternions. Les informations fournies par le *Rotation Vector* sont plus précises et demandent moins de ressources matérielles pour être calculées.

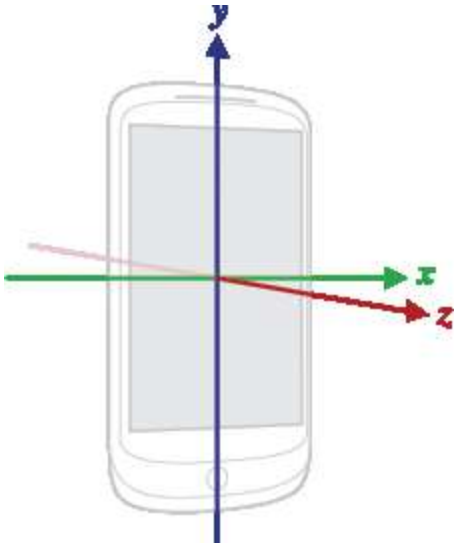



Figure 43 - Système de coordonnées utilisé dans Android.

Les informations issues du capteur de gravité peuvent être bien pratiques, car elles permettent de connaitre l'orientation de la tablette. Par exemple, si les composantes X et Z du capteur de gravité sont très proches de 0 $m.s^{-2}$, tandis que la composante Y est très proche de la valeur -9.81 $m.s^{-2}$. La valeur de 9.81 $m.s^{-2}$ correspond à l'accélération terrestre et nous indique que l'appareil ne se déplace pas selon cet axe. De cette manière, en utilisant le système de coordonnées utilisé par Android, on peut savoir que la tablette est placée verticalement de façon immobile, comme dans une poche de pantalon par exemple. Les variations sur les axes X et Z du capteur de gravité, associé à l'accéléromètre, nous informent sur un mouvement probable de la personne.

Bien que l'ensemble des capteurs s'intègre correctement dans le système, la mise à jour des informations dépend des évènements en provenance des capteurs qui surgissent au sein de l'appareil mobile. Cette période peut être définie dans le programme Android via la variable SENSOR_DELAY, mais ce n'est qu'une suggestion que l'on peut faire dans le programme. C'est à dire que le système d'exploitation Android garde la main sur cette période. Il se peut alors que les informations de certains capteurs soient mises à jour régulièrement et pour d'autres beaucoup moins souvent. Par exemple, les informations concernant le capteur de

luminosité ainsi que de l'accéléromètre sont mises à jour environ une fois par seconde, tandis que les informations concernant la rotation de l'appareil et le gyroscope sont mises à jour une fois par minute environ. Cette mise à jour lente rend l'utilisation et la pertinence de ces capteurs quasiment nulle.

Cependant, ces tests ont permis de montrer que le système est bien capable d'intégrer des données capteurs issues de capteurs d'un appareil initialement méconnu du système. L'objectif associé à cette partie (deuxième objectif dans la section 2.7.2 : intégrer les capteurs issus d'appareils mobiles) est considéré partiellement atteint.

### 5.3.3 Informatique autonome

Pour tester que StoveMAS réponde bien aux critères de l'informatique autonome (auto-configuration, auto-optimisation, autoréparation et autoprotection) différents tests ont été menés :

L'auto configuration des capteurs :

L'auto configuration de l'informatique autonome permet à la cuisinière de détecter et d'utiliser automatiquement de nouveaux capteurs qui pourraient être connectés au système. Comme les capteurs filaires sont branchés sur les modules d'acquisition et que les équipements de cuisine comportent des hautes tensions électriques, il est préférable de mettre hors tension les appareils et le système afin d'y installer un nouveau capteur. Pour rajouter des capteurs de la même manière que les capteurs déjà présents, il y a besoin d'intervenir physiquement sur le système pour rajouter le câblage nécessaire. Il y aura ensuite une configuration à faire sur le module ADAM (au laboratoire DOMUS), ou adapter le signal pour l'acquisition avec les convertisseurs *MCP3008* (au laboratoire Lab-STICC) pour exploiter les informations fournies par ces nouveaux capteurs. Ensuite, il faut déclarer dans StoveMAS de quel type de capteurs il s'agit (via le profil de l'équipement). Il est actuellement impossible à un système de reconnaitre la grandeur mesurée par un capteur automatiquement. Lorsque les nouveaux capteurs sont

branchés et identifiés dans le système, ces nouveaux capteurs sont automatiquement utilisés par les différents agents.

Dans le cadre de capteurs sans fil, l'intégration de ces derniers se fait automatiquement à condition d'avoir des informations complètes par rapport aux capteurs (nom, type), ce qui est le cas des capteurs embarqués de la tablette Nexus 7. Grâce aux informations du capteur comme le nom et le type, StoveMAS peut déduire la grandeur de l'information donnée par ce capteur.

L'arrivée d'un nouvel équipement peut se faire à tout moment lors du fonctionnement du système. Mais lors du démarrage du système, l'ensemble des capteurs branchés sont considérés comme nouveaux. On doit alors se poser la question s'il y a une importance sur l'ordre de démarrage du système. Car, si le système n'a pas accès à certaines informations, il verrouille la cuisinière. Mais vu que le système verrouille les équipements par défaut, l'ordre de démarrage des différents composants n'a pas beaucoup d'importance. Le verrouillage par défaut se fait via les relais qui sont installés. Tant que ces relais ne sont pas alimentés, les appareils de cuisine ne sont pas alimentés. Les relais peuvent seulement être alimentés via StoveMAS. Ce dernier déverrouillera la cuisinière lorsqu'il aura accès à toutes les informations nécessaires, c'est-à-dire lorsque le *DeviceAgent* mandataire de cet appareil ne le considère pas en mode « en panne ».

L'auto optimisation :

L'auto optimisation concerne l'optimisation automatique du système par rapport à son environnement. Les *DeviceAgents* choisissent les capteurs dont ils ont besoin via le profil du matériel disponible et adaptent leurs variables en permanence (tarage, seuils) pour connaitre l'activité des appareils avec la plus grande précision.

L'auto optimisation se fait également au niveau des règles de sécurité qui optimisent leurs variables par rapport aux profils utilisateur connectés. Ces variables changent de valeur à

chaque fois qu'il y a une modification dans les usagers identifiés. Cette personnalisation est mise en avant lors du scénario 1 : Rond vide et du scénario 3 : Préparation d'un oeuf.

L'autoréparation :

L'autoréparation permet de trouver des sources de pannes, de les notifier et de les compenser le cas échéant. L'autoréparation se fait à 2 niveaux : les capteurs et l'organisation des agents.

Au niveau des capteurs, les agents *DeviceAgents* permettent de détecter de sources éventuelles d'erreurs lorsque des capteurs en redondance donnent des informations incompatibles, par exemple lorsque l'agent *DABurners* alerte lorsqu'un ustensile est détecté sur un rond alors qu'aucune masse n'est observée pour ce rond. Un essai a été mené dans lequel une poêle a été placée à la main 2 cm au-dessus du rond. Ainsi, le système détecte la présence de la poêle, mais pas sa masse. L'agent *DABurners* envoie une notification d'une erreur possible entre le capteur de pression et le capteur de présence associé à ce rond. Actuellement, le système est incapable de déduire lequel de ces deux capteurs est fautif. Lorsqu'une telle erreur se produit, l'agent met l'équipement dont il est mandataire en mode dégradé. Le mode dégradé indique à l'utilisateur qu'il y a une panne au niveau des capteurs, mais il est toujours en mesure de se servir de l'appareil pour préparer son repas. Si l'utilisateur décide d'allumer ce rond, StoveMAS considère que le rond n'est pas chargé mais activé, il y a donc un risque potentiel que l'agent *Rule5* doit surveiller.

L'objectif lié à la gestion des défaillances des capteurs est considéré partiellement résolu (dernier objectif dans la partie 2.7.2 : Gérer les défaillances des capteurs). En effet le système est capable de gérer les défaillances des capteurs et s'adapter en fonction de ces défaillances. Cependant il n'est actuellement pas capable d'isoler le capteur défaillant.

Au niveau des agents, l'autoréparation se fait au niveau de l'enregistrement des agents. L'agent *SystemAgent* permet une surveillance de haut niveau en vérifiant l'état d'enregistrement des agents. Si un agent n'est pas connecté auprès des pages jaunes, le *SystemAgent* le contacte et

l'incite à s'enregistrer (Figure 44). Ce cas peut se produire lorsqu'il y a eu une erreur lors du démarrage de StoveMAS par exemple.

```
025:11:47:29.799 SecurityAgent: Non registered agent: [DABurners]
025:11:47:29.799 SecurityAgent: Attempt to register agents
025:11:47:29.815 DABurners: correctly registered with DF
025:11:47:34.810 SecurityAgent: agent: DABurners SUCCESS
```

Figure 44 - Enregistrement auprès des pages jaunes par le *SystemAgent*.

L'autoprotection :

L'auto protection permet de protéger le système contre des menaces malveillantes externes. La sécurité est un aspect très important pour préserver les données sensibles des résidents. Même si la sécurité des communications et des données ne fait pas partie du fil conducteur de nos travaux, quelques notions de sécurité ont malgré tout été implémentées.

Nous avons testé ce cas à l'aide d'un scénario simple, l'agent *SystemAgent* surveille si les agents sont correctement enregistrés auprès des pages jaunes. Dans ce cadre, un agent simple, appelé *DummyAgent*, a été élaboré pour être présent sur la plateforme sans s'enregistrer. Dans ce cas, le *SystemAgent* le détecte et demande aux agents non enregistrés de s'enregistrer. Si après un délai de 5 secondes l'agent n'est toujours pas enregistré, le *SystemAgent* tue l'agent en question (Figure 45).

```
322:10:54:44.849 SecurityAgent: Non registered agent: [DummyAgent]
322:10:54:44.849 SecurityAgent: Attempt to register agents
322:10:54:49.854 SecurityAgent: agent: DummyAgent FAILED
322:10:54:49.854 SecurityAgent: agent: DummyAgent got killed
322:10:54:50.187 DummyAgent: Terminated
```

Figure 45 - Vérification de l'enregistrement auprès des pages jaunes par le *SystemAgent*. Si un agent refuse de s'enregistrer, il est tué.

Cette solution bien que simple, permet d'éliminer les agents ne respectant pas des procédures d'identification simples.

## 5.4 La sécurité dans la cuisinière

La sécurité dans la cuisinière est mesurée par la capacité de StoveMAS d'avertir et de verrouiller les équipements en cas de danger. Pour cela, les scénarios d'usage (scénarios 1 à 3) permettent de représenter des situations où la personne se met face à un danger potentiel. Ces expérimentations ont été réalisées par deux étudiants bénévoles du laboratoire. Lors de ces scénarios, chaque étudiant incarne un persona présent dans le scénario. A l'issue des scénarios, les données récoltées par StoveMAS ont été observées et confrontées par rapport aux observations visuelles des participants lors du déroulement des scénarios. Pour ces scénarios, les étudiants incarnant les différents personas devaient exécuter dans l'ordre les étapes proposées.

### 5.4.1 Identification des participants

L'identification de la personne s'est déroulée correctement lors de l'ensemble des scénarios. Les étudiants disposaient des cartes RFID correspondants aux personas et les profils utilisateurs résultants étaient générés correctement.

De la même manière, l'identification via la tablette tactile (scénario 3) se faisait correctement. Lors du lancement de l'application mobile l'identifiant de la personne était automatiquement envoyé vers StoveMAS.

La composition des profils utilisateurs restait assez basique lors des scénarios proposés (maximum 2 personas de connectés). Cette limitation était justifiée pour simplifier le déroulement des scénarios, où seulement deux tags RFID étaient disponibles. Il est possible via l'interface de contrôle d'identifier davantage de personnes en y entrant manuellement une code RFID pour simuler l'arrivée d'une nouvelle personne, mais cette procédure est plus contraignante pour des usagers novices du système. De plus, généralement, le nombre de personnes préparant un repas en simultané est rarement au-delà de deux dans un usage quotidien. Lors des scénarios, il n'y a pas eu recours à l'identification par l'interface de contrôle

pour des personnes supplémentaires, mais lors des tests préliminaires les personas s'identifient via cette interface. Lors des scénarios 2 et 3, l'ordre d'identification entre René et Jeanne a été alterné permettant la vérification de la cohérence du profil utilisateur résultant indifféremment de l'ordre d'identification.

### 5.4.2 Premier scénario d'usage : Rond vide

Lors du premier scénario, l'étudiant était invité à placer une casserole d'eau sur le rond avant gauche de la cuisinière. Dans ce scénario, on souhaite vérifier que StoveMAS détecte correctement l'absence d'ustensile sur le rond qui est activé. Ce scénario a été déroulé une seule fois.

L'agent *DABurners* a détecté dans un premier temps l'apparition d'une présence sur le rond avant gauche sans que le rond soit activé. Ensuite, cet agent détecte l'activité électrique sur le rond arrière gauche. Les données relevées montrent que l'agent *Rule5* estime qu'un danger est présent et avertit au bout de 15 secondes environ via la console l'information sur la nature du danger. Étant donné que l'étudiant était en dehors de l'environnement de la cuisinière au moment de l'envoi des notifications d'alerte et que ces notifications n'apparaissaient que sur l'écran, l'étudiant n'était pas en mesure de corriger l'erreur produite. L'agent *Rule5* a, au bout de 15 secondes supplémentaires, verrouillé la cuisinière, ce qui pouvait être constaté à partir de la console sur l'écran ainsi que sur la cuisinière qui a cessé de fonctionner. On peut également noter qu'à ce stade d'avancement dans le scénario, l'agent *Rule6* détectait également un risque d'usage avec l'appareil de cuisine allumé mais sans présence de personnes dans l'environnement. Cependant, le temps entre le début de la détection de ce danger et le début d'envoi des notifications d'alerte était trop long (5 minutes) pour que cet agent commence à se manifester.

Ce scénario est présenté sous forme de chronogramme permettant d'illustrer les évènements produits dans StoveMAS durant le scénario (Figure 46).

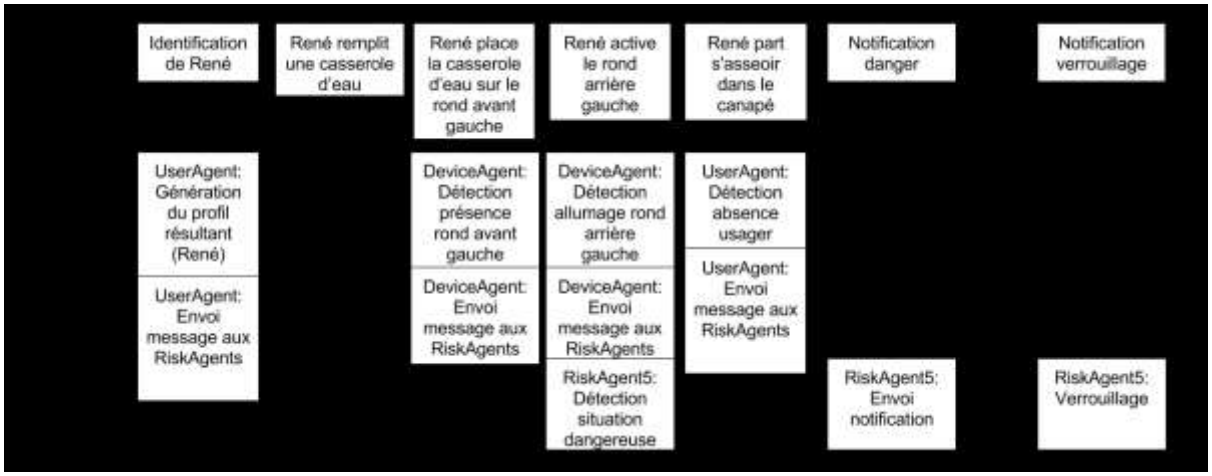



Figure 46 - Chronogramme du scénario 1 : Rond vide.

### 5.4.3 Deuxième scénario d'usage : Four ouvert

Lors de ce scénario, le four est chargé mais la porte du four demeure ouverte. On souhaite vérifier que StoveMAS détecte correctement que le four a été activé mais qu'il reste vide (agent *Rule2*). Ce scénario a été déroulé une seule fois.

L'agent *DAOven* détecte que le four a été activé mais reste vide (préchauffage). Pendant ce préchauffage, il était nécessaire d'adapter l'agent *Rule3* (four vide mais actif) pour ne pas verrouiller l'appareil avant qu'il ait terminé de préchauffer. Ainsi, cette règle de sécurité a été modifiée afin de ne se déclencher seulement lorsque le four est vide, actif mais également au-delà de 400°F.

Ensuite, lorsque le four était chaud, au moment où la personne ouvrait la porte du four pour y placer l'aliment, elle était interrompue par une autre personne. L'agent *DAOven* détectait la présence de l'aliment dans le four et la porte demeurant ouverte. L'agent *Rule2* observe le risque lié à la porte ouverte et envoie une notification au bout de 10 secondes. Cela a laissé 10 secondes à la personne pour fermer la porte du four. En fermant la porte l'agent *Rule2* a cessé de notifier.

Ce scénario est présenté sous forme de chronogramme permettant d'illustrer les évènements produits dans StoveMAS durant le scénario (Figure 47).

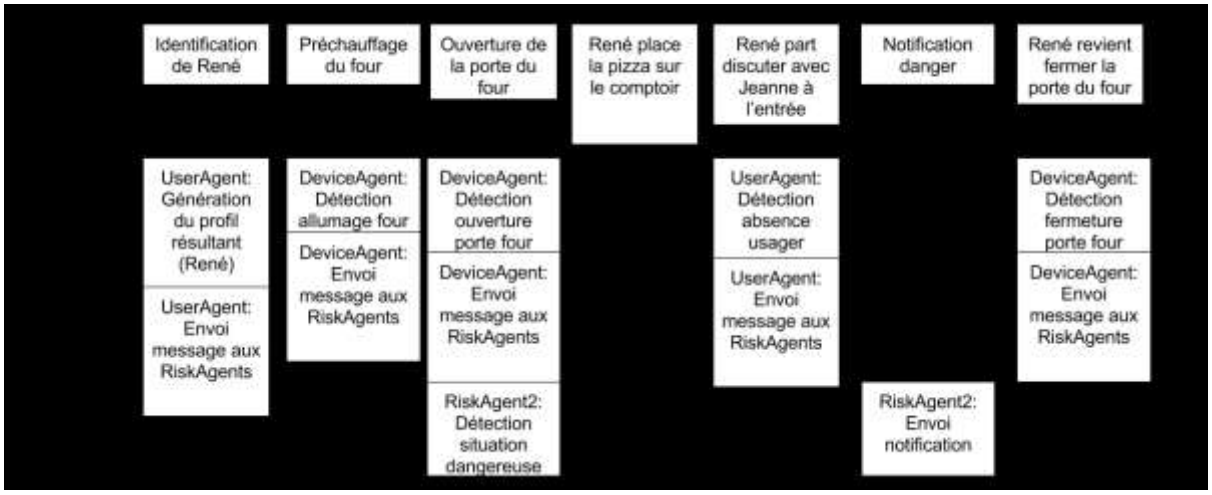



Figure 47 - Chronogramme du scénario 2 : Four ouvert.

### 5.4.4 Troisième scénario d'usage : Préparation d'un oeuf

Lors de ce scénario, le rond activé ne correspond pas au rond sur lequel l'ustensile a été placé. Lors du troisième scénario, le placement de la casserole d'eau sur le mauvais rond a généré les mêmes symptômes que lors du premier scénario. Le troisième scénario met l'accent sur la connexion de Jeanne, qui, par le biais de sa présence, change les délais des notifications dans StoveMAS. Ce scénario a été fait deux fois, en alternant l'incarnation des personas.

Ainsi, lors du déroulement de ce scénario, la notification issue de l'agent *Rule5* apparaissait seulement au bout de 30 secondes. Sachant que les étudiants restaient dans l'environnement de la cuisinière, l'agent *Rule6* ne s'est pas manifesté. Les étudiants ont pu par ailleurs prendre connaissance des notifications émises par l'agent *Rule5* et allumer le rond avant gauche et éteindre le rond arrière gauche. On a pu constater que l'agent *Rule5* a cessé d'émettre des notifications et que la cuisinière restait déverrouillée.

Ce scénario est présenté sous forme de chronogramme permettant d'illustrer les évènements produits dans StoveMAS durant le scénario (Figure 48).

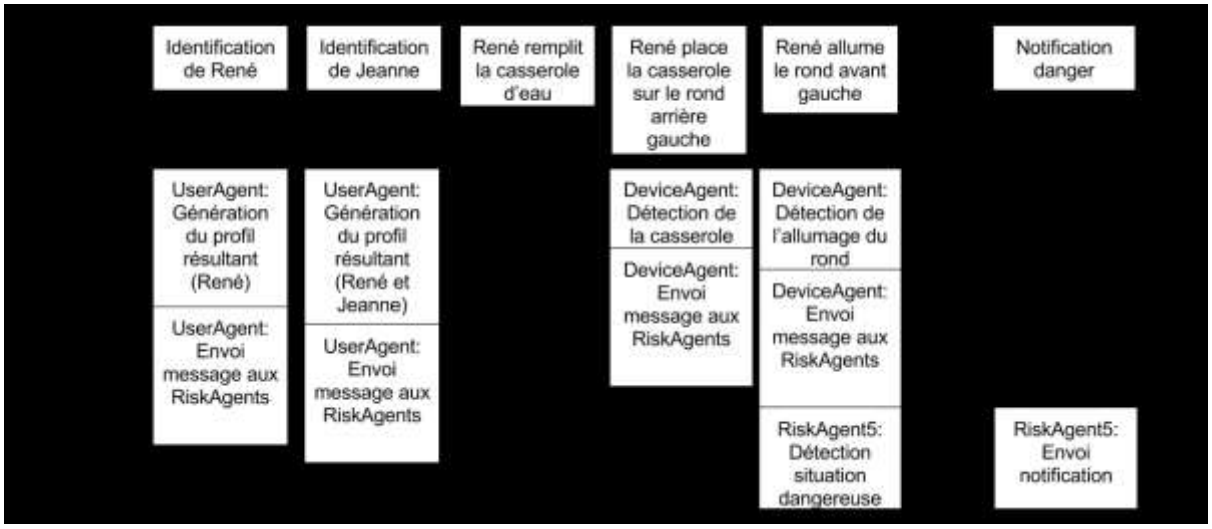



Figure 48 - Chronogramme du scénario 3 : Préparation d'un œuf.

### 5.4.5 Conclusion

Dans cette partie, nous allons analyser les résultats pour l'ensemble de ces trois scénarios. Cette analyse se fait selon deux dimensions : Les notifications et verrouillage de la cuisinière ainsi que la régulation des horaires.

#### 5.4.5.1 Notifications et verrouillage de la cuisinière

Les expérimentations se sont montrées concluantes. StoveMAS était en mesure de détecter les risques d'usage qui se sont manifestés lors des différents scénarios et fournissait des informations pertinentes permettant de rapidement définir la source des erreurs. Les notifications d'alerte ainsi que le verrouillage se font globalement dans les délais imposés. Lors du premier scénario, le délai de la notification d'alerte a été rallongé de quelques secondes pour deux raisons : d'une part, la cuisinière met un certain temps à chauffer une fois que le bouton a été activé. D'autre part, l'obtention des données capteurs ainsi que leurs traitements au sein

des différents agents rallongent ce délai. Pour des risques de sécurité critique, il est important de tenir compte de ces délais supplémentaires afin que le délai imposé par la règle soit adéquat.

#### 5.4.5.2 Régulation des horaires

Le déroulement des expérimentations a eu lieu le matin, les horaires d'utilisation des équipements de cuisine par René ont été adaptés. Par conséquent, René pouvait utiliser les équipements de 9h à 11h. Lors des expérimentations, une notification est apparue indiquant que la disponibilité des équipements allait prendre fin. Cette notification permet de prévenir René que la cuisinière peut se verrouiller sans qu'il y ait un risque de sécurité.

## 5.5 Déploiement du système sur du matériel existant

StoveMAS a pour vocation d'être installé au domicile des usagers. Au laboratoire Lab-STICC, StoveMAS est implanté sur une Raspberry Pi (Figure 49). Avec les cartes d'acquisition, l'ensemble reste assez compact (120 x 60mm environ) si on les superpose. Ces cartes peuvent être intégrées dans un petit boitier et être facilement dissimulées dans l'environnement.

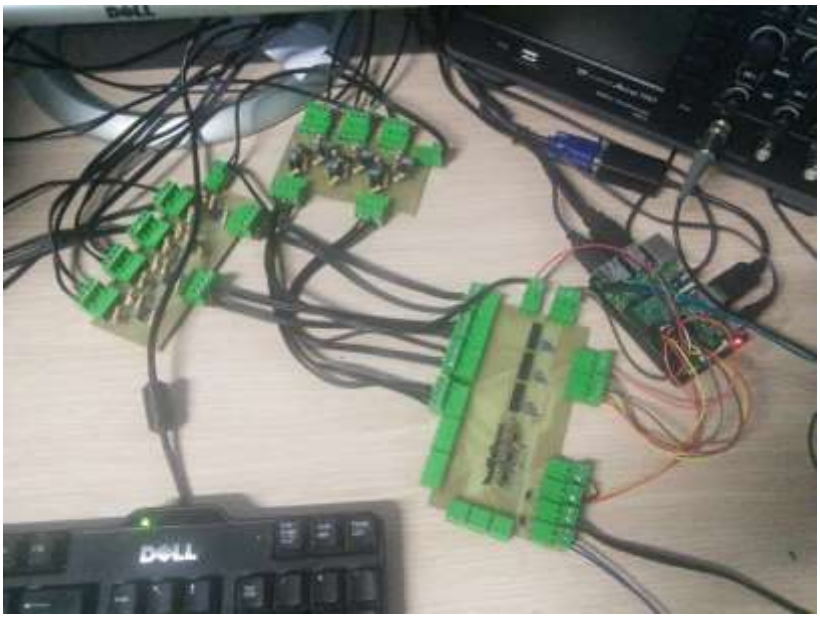



Figure 49 - StoveMAS installé sur la Raspberry Pi avec les cartes d'acquisition au laboratoire Lab-STICC.

Les différents capteurs utilisés s'implantent sur ou à l'intérieur des appareils électroménagers. Par exemple, les capteurs de force sont collés en dessous de chaque pied du four à micro-ondes. Les seuls capteurs intrusifs dans l'équipement sont les capteurs de courant et les capteurs de température. Les deux inconvénients de ces capteurs sont la nécessité d'une personne compétente pour l'ouverture de l'équipement pour l'installation et l'annulation de la garantie constructeur de cet équipement à cause de cette intervention si elle a lieu.

Au laboratoire DOMUS, l'installation est un peu plus complexe. L'intelligence se trouve dans le tiroir inférieur de la cuisinière (Figure 50). L'ensemble des composants au sein de ce tiroir sont interconnectés (Figure 51). Les capteurs de la cuisinière sont également interconnectés avec le boitier d'acquisition ADAM (en bleu à droite sur la Figure 50). Par conséquent, pour installer un capteur sur la cuisinière, il est nécessaire d'ouvrir le tiroir et de câbler les fils du capteur au bon endroit sur le module d'acquisition. Les câbles d'alimentation de l'intelligence, de la cuisinière et les câbles des capteurs étant directement fixés sur le tiroir, ceci implique une ouverture difficile du tiroir et empêche sa séparation avec la cuisinière. Pour installer ce matériel dans le tiroir de cuisinière chez le résident, il faut fortement modifier le tiroir pour fixer chaque composant. Lors de cette installation, la cuisinière au complet est indisponible. Cette installation doit se faire chez le résident et est coûteuse en temps.

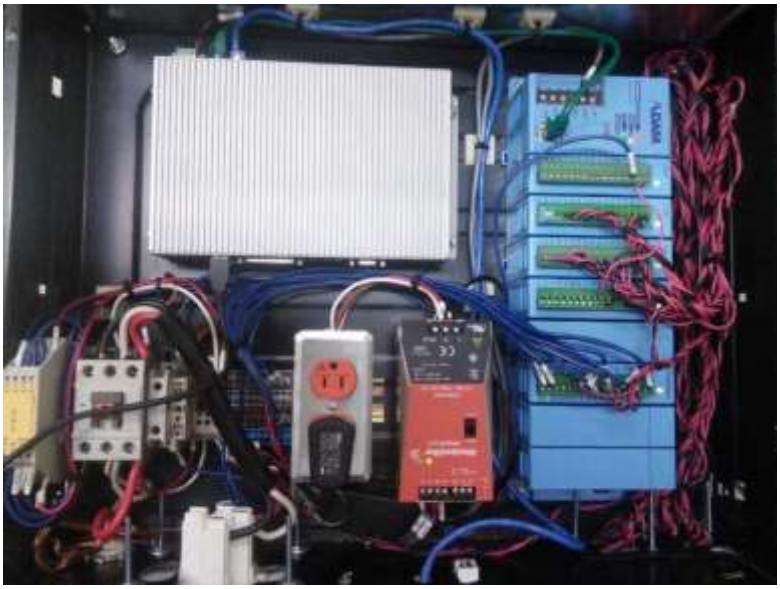


Figure 50 - StoveMAS installé sur l'ordinateur embarqué dans le tiroir de la cuisinière au laboratoire DOMUS.

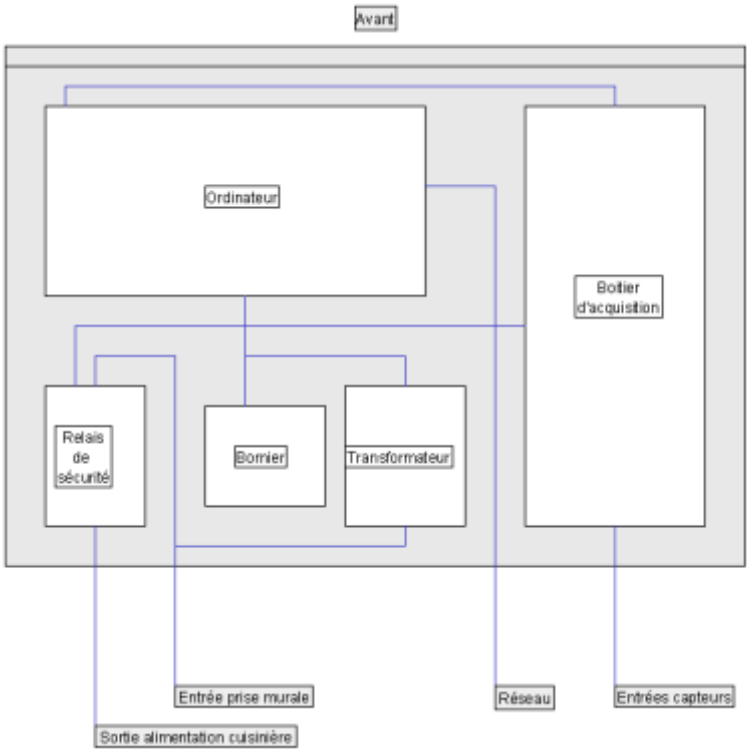



Figure 51 - Modélisation du contenu du tiroir de la cuisinière.

Pour faciliter le déploiement sur des équipements disponibles chez les résidents, on installe des connecteurs à l'arrière du tiroir permettant de désolidariser le tiroir de la cuisinière (Figure 52 et Figure 53). De cette manière, l'installation et les tests des composants au sein du tiroir peuvent se faire au laboratoire. La seule intervention à faire chez le résident est l'installation des capteurs sur les équipements et leur branchement sur le bornier à l'arrière du tiroir.

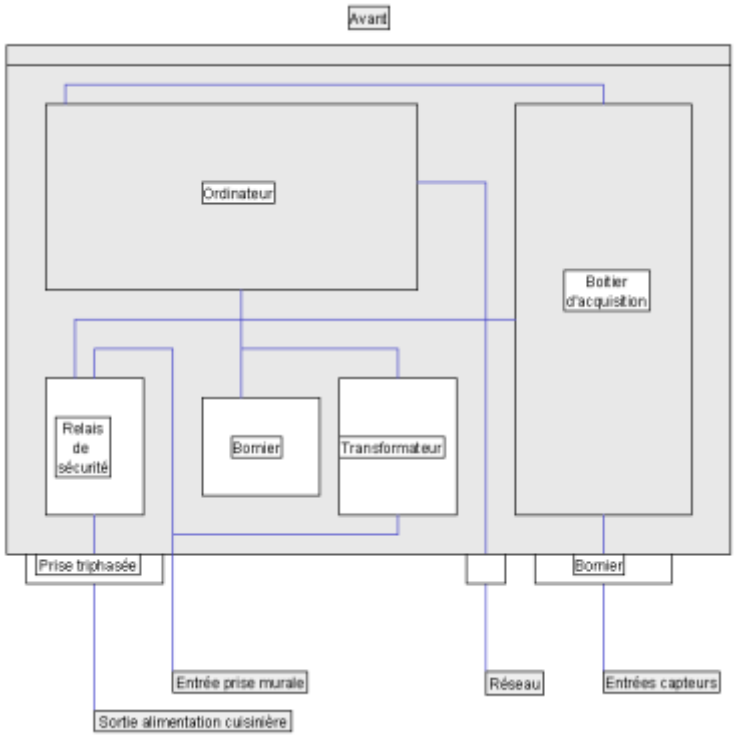



Figure 52 - Modélisation du contenu du tiroir de la cuisinière avec les borniers.

Figure 53 - Photo de l'arrière du tiroir avec (de gauche à droite) la prise triphasée, un bornier pour le câble réseau, deux ports USB et les borniers des capteurs.

Cette solution présente également l'avantage d'être facilement remplaçable en cas de panne. Si l'ordinateur ou le boitier d'acquisition viennent à tomber en panne chez le résident, le tiroir au complet peut être échangé pour que le résident garde une cuisinière fonctionnelle au plus vite. Le tiroir en panne peut ensuite être réparé au laboratoire.

L'inconvénient de cette solution réside dans le fait que chaque constructeur de cuisinière dispose d'un tiroir aux dimensions différentes. Il faut disposer d'un second tiroir pour le modèle de cuisinière en question pour l'installation du matériel informatique. Dans certains cas, la cuisinière ne dispose d'aucun tiroir. Dans ces cas-là, il peut être possible d'implanter le système sur la Raspberry Pi pour avoir un encombrement minimal.

## 5.6 Conclusion

Lors de ce chapitre, les quatre objectifs définis au début de ce document ont été adressés. Pour chaque objectif, le moyen de vérification a été montré et les résultats ont été discutés (Tableau 10). Différents scénarios ont été mis en œuvre permettant de mettre en avant la validation du système par rapport à ces objectifs. Ces différents scénarios avaient deux objectifs ; tester le

système vis-à-vis des différents aléas qui peuvent se produire dans l'environnement et tester le système vis-à-vis de l'utilisation par des personnes. Les différents tests dans ce chapitre ont pu montrer la validité de notre solution vis-à-vis des défis scientifiques posés.

Tableau 10 - Validation des objectifs.

| Section | Objectif | Validation |
|---|---|---|
| 2.7.1 | Réaliser un système personnalisable selon le profil médical de la personne, ses préférences ainsi que le contexte | Oui |
| | Identifier plusieurs personnes | Oui |
| | Pallier aux handicaps des uns sans contraindre l'usage du système des autres | Oui |
| 2.7.2 | Obtenir des informations contextuelles grâce à un réseau de capteurs | Oui |
| | Intégrer automatiquement les capteurs venant d'appareils mobiles | Partiel |
| | S'adapter à son contexte en utilisant la boucle MAPE-K | Oui |
| | Gérer les défaillances des capteurs | Partiel |
| 2.7.3 | Analyser l'activité de haut niveau et appliquer les règles de sécurité | Oui |
| | Personnaliser les règles de sécurité selon les usagers | Oui |
| 2.7.4 | Déployer le système sur des applications différentes en utilisant une congrégation dans un SMA | Oui |

Le domicile est un lieu où généralement plusieurs personnes vivent. Via l'élaboration de profils utilisateurs, StoveMAS est capable de fonctionner pour un ensemble d'usagers différents et s'adapter au mieux à leurs besoins. Les scénarios ont montré que StoveMAS élabore un profil utilisateur résultant correspondant aux usagers connectés et à leurs capacités individuelles.

Lors du scénario 3, un appareil mobile s'est connecté à StoveMAS. Malgré la faible pertinence de ces données capteurs pour StoveMAS, ce dernier était malgré tout capable d'intégrer correctement ces données. On peut considérer que StoveMAS est capable de récolter des données de capteurs pour enrichir ses connaissances dans un environnement évolutif.

StoveMAS assure la sécurité des usagers via l'utilisation des règles de sécurité prédéfinies. Lors du scénario 2 : Four ouvert, on a pu constater que certaines de ces règles (*Rule2* et *Rule3*) se recouvraient en partie et qu'il fallait trouver une solution pour que *Rule3* ne verrouille pas les équipements lors d'un fonctionnement voulu et autorisé. Malgré tout, StoveMAS était capable de verrouiller les équipements lorsque ces risques étaient mis en évidence lors des scénarios.

Enfin, le système a été déployé dans deux environnements différents, le premier constitué d'un four à micro-ondes associé à une plaque vitrocéramique, le deuxième d'une cuisinière tout en un. Ces équipements sont des équipements grand public et représentent les équipements types des résidents. L'adaptation de StoveMAS sur ces deux plateformes fut aisée et montre qu'il peut être déployé sur du matériel existant dans le domicile des usagers, répondant ainsi au dernier objectif (section 2.7.4). La congrégation facilite le déploiement de certains agents en fonction des besoins de la plateforme, notamment au niveau des *DeviceAgents* et des agents d'acquisition *SPIAgent* et *ADAMAgent*.

Les thèmes scientifiques initialement choisis pour ces travaux ont permis de répondre aux défis scientifiques. L'informatique omniprésente, la personnalisation des services et la sensibilité au contexte sont des thèmes scientifiques bien connus dans le domaine de la domotique.

L’informatique autonome est un thème scientifique plutôt connu dans le domaine des serveurs et réseaux, mais ce thème a également son importance en domotique. Dans ce sens, StoveMAS a été élaboré pour correspondre au mieux des critères de l’autogestion.

Les objectifs posés ont tous été adressés. Le système y répond correctement. Seuls les objectifs liés à la gestion des défaillances et l’intégration automatique des capteurs sont partiellement résolus. En effet, le système est actuellement incapable, lors d’une défaillance d’un capteur, d’identifier le capteur défaillant. Le système détecte seulement une incohérence entre les capteurs en redondance et notifie une erreur possible entre ces capteurs. L’objectif lié à l’intégration automatique des capteurs est adressé par le système pour les capteurs d’une tablette tactile. Cependant, la mise à jour lente pour certains de ces capteurs rend l’usage de ces capteurs non pertinents. Cette problématique provient à première vue du matériel et du système d’exploitation Android et non de StoveMAS.

# Conclusion

## Contributions

Les personnes âgées deviennent de plus en plus nombreuses dans les pays développés tels que la France ou le Canada. Les démences cognitives et motrices liées à l'âge évoluent aussi dans ce sens. Nos travaux visent les personnes atteintes de déficiences cognitives comme la maladie d'Alzheimer. Cette maladie est une maladie où la mémoire est atteinte, les personnes qui en sont atteintes sont continuellement confrontées à des oublis. Ces oublis peuvent engendrer des situations dangereuses lors d'activités de la vie quotidienne telle que la préparation d'un repas. L'objectif de nos travaux est la réalisation d'un système autonome permettant d'améliorer la sécurité lors de la préparation d'un repas pour des personnes atteintes de déficiences cognitives. Par le biais du renforcement de la sécurité lors de cette activité, ces personnes peuvent en toute sécurité réaliser un repas. Nous avons identifiés des problématiques sur quatre aspects :

- Le domicile multi-usagers. Adapter le système pour pallier aux handicaps des usagers, tout en prenant compte que le domicile peut être habité par plusieurs personnes, atteintes de déficiences ou non.
- L'évolution de l'environnement. Adapter le système en fonction de son contexte, des appareils et équipements disponibles.
- La sécurité. Assurer la sécurité pour les habitants atteints de troubles cognitifs lors de la préparation d'un repas.
- Le déploiement. Développer un système qui peut être installé sur du matériel déjà existant chez les résidents.

Pour répondre à ces problématiques, le système développé se base sur différents thèmes scientifiques tels que l'informatique omniprésente, la personnalisation, la sensibilité au contexte, l'informatique autonome ainsi que la sécurité lors de la préparation d'un repas. Dans le Chapitre 2, la solution présentée dans nos travaux utilise l'informatique omniprésente pour déployer des capteurs discrets et qui permettent d'avoir une bonne connaissance du contexte. La personnalisation permet de personnaliser l'usage du système en fonction des besoins individuels des personnes atteintes et à leur situation. La sensibilité au contexte permet une adaptation du système également en fonction de la situation contextuelle, c'est-à-dire en fonction des capteurs, interfaces, équipements disponibles dans l'environnement. L'ensemble du système est plongé dans un environnement où il n'y a pas de techniciens. L'informatique autonome permet l'évolution du système de manière autonome, permettant le moins d'interventions de maintenance possible. La sécurité lors de la préparation d'un repas permet de rendre plus sécuritaire l'activité de préparation d'un repas. Dans ce sens, six règles de sécurité ont été dressées.

Le chapitre 3 présente notre système sous forme de modèles. Ces modèles ont pour vocation d'être génériques et être adaptables. L'architecture, basée sur un système multi-agents, sous forme de congrégation, présente les avantages de la flexibilité et l'interopérabilité. Des agents ont chacun un rôle au sein de la plateforme. On retrouve des agents de bas niveau tel que *SPIAgent*, *ADAMAgent* ou *WirelessAgent* qui permettent l'acquisition des informations issues des capteurs dans l'environnement. Ces informations sont ensuite transmises aux *DeviceAgents* qui sont mandataires d'équipements physiques, tels qu'un four à micro-ondes ou des plaques de cuisson. Ces agents définissent l'activité de haut niveau de l'appareil dont ils sont mandataires. Parallèlement, l'agent *UserAgent* s'occupe de la détection et de l'identification des usagers et dresse le profil résultant qui synthétise les profils des usagers connectés. Les *RiskAgents* sont chacun mandataires d'une règle de sécurité et collectent les données issues des *DeviceAgents* et du *UserAgent* et surveillent les situations à risque. Cette architecture est déployée sur deux applications distinctes, leurs besoins en termes de matériels et leur fonctionnement sur ces applications ont été développés.

Cinq scénarios ont été élaborés permettant de tester chaque partie du système. Deux de ces scénarios, au laboratoire Lab-STICC, permettaient de tester l'aspect technique de StoveMAS, c'est-à-dire l'étude des données capteurs et son fonctionnement vis-à-vis de plusieurs pannes. Les trois scénarios restants se sont déroulés au laboratoire DOMUS et ont permis de confronter StoveMAS dans un cadre d'usage type. Ces deux laboratoires d'expérimentations sont complémentaires et ont permis de tester le développement pour les personnes avec des déficiences sur des équipements et dans des environnements variés. Ces scénarios ont pu valider le fonctionnement du système vis-à-vis des objectifs posés. Les situations à risque mises en avant lors des scénarios ont montrés le fonctionnement des règles de sécurité pour un public varié (personas atteints de déficiences cognitives et personas sains).

Ces travaux ont fait l'objet d'articles scientifiques. Le premier article concerne l'application d'un système multi-agent dans un habitat domotisé [78]. Ce SMA a la particularité d'être composé de plusieurs groupes : un par pièce de l'habitat. Ainsi, des agents mandataires de services disponibles, peuvent suivre les déplacements des usagers de pièce en pièce en se déplaçant de groupe en groupe. Cet article couvre un sujet plus large que le sujet actuel nos travaux. Depuis cet article, nos travaux se sont centrés sur l'activité de la préparation d'un repas sur des équipements de cuisine. Cet article a été accepté et présenté lors de la 30$^{e}$ *Conference of Artificial Intelligence* (AAAI) *Applied to Assistive Technologies and Smart Environments* en février 2016 à Phoenix, États-Unis. Le deuxième article présente l'application StoveMAS, et plus particulièrement l'étude des données des capteurs issues des scénarios 4 et 5. Cet article a été accepté pour la *Conference of Pratical Applications of Agents and Multi-Agent Systems* (PAAMS) qui aura lieu en juin 2017 à Porto, Portugal.

# Critique du travail

Cette thèse a développé un système de sécurité qui permettra à des personnes atteintes de déficiences cognitives d'être plus autonomes lors des tâches quotidiennes complexes telles que la préparation d'un repas. Cependant, le système réalisé reste au niveau de la preuve de concept, testé en laboratoire par des personnes saines.

Des règles de sécurité ont été élaborées et implémentés pour tester le fonctionnement du système. Ces règles, au nombre de six, bien que fonctionnelles, ne couvrent pas tous les dangers possibles. Ils ont été testés lors des trois scénarios d'usage au laboratoire DOMUS. Ces règles de sécurité sont issues d'une étude clinique par des ergothérapeutes et répondent par conséquent à un danger réel. Des tests en milieu réel du système devraient être réalisés.

Nos travaux visent en première place les personnes atteintes de troubles cognitifs, en particulier celles qui souffrent de la maladie d'Alzheimer. Ces personnes sont continuellement concernées par des oublis et des manques d'attention. Dans ce cadre, l'identification de la personne auprès de notre système, via des étiquettes RFID peut représenter une difficulté d'usage pour ces personnes. Il suffit que la personne atteinte de la maladie d'Alzheimer égare son étiquette RFID pour que les équipements de cuisines gérées par StoveMAS soient rendus inutilisables. Cette solution, malgré qu'elle soit simple et peu coûteuse, reste malgré tout complexe à utiliser pour ces personnes. De plus, les personnes extérieures, comme par exemple les voisins ou autres membres de famille, n'ont pas forcément une étiquette RFID à leur disposition. L'utilisation des appareils mobiles pour identifier les usagers solutionne le problème de la carte égarée. De plus, les personnes extérieures peuvent plus facilement utiliser StoveMAS. Cependant, l'utilisation d'appareils mobiles apporte la contrainte des batteries. Il peut être envisagé d'utiliser d'autres méthodes d'identification, tels que la technologie NFC sur les appareils mobiles, ou encore via des empreintes digitales. L'identification de plusieurs personnes dans un espace restreint de façon fiable et non intrusive, reste à ce jour, une voie de recherche ouverte.

L'utilisation d'un système multi-agents pour représenter StoveMAS est une bonne approche. La représentation des différentes fonctionnalités de StoveMAS (représentation du matériel, des usagers, des risques, etc.) se font aisément par des agents. Les concepts d'une organisation par congrégation (durée de vie longue, agents avec des buts précis, savoir commun, etc.) et les besoins de StoveMAS sont similaires. La congrégation est la meilleure représentation de l'organisation des agents dans StoveMAS.

Les résultats des expérimentations ont montrés que deux sous-objectifs (utilisation des capteurs issus d'appareils mobiles, gestion des défaillances des capteurs) ont été partiellement atteints. En effet, lors des tests, certaines données de capteurs de la tablette ne se mettaient pas à jour de façon régulière. Des tests avec des appareils mobiles différents, embarquant d'autres capteurs pourraient montrer si le problème est matériel ou logiciel. La gestion des défaillances des capteurs reste également à améliorer dans StoveMAS. Actuellement il est capable d'identifier une incohérence entre les données de capteurs dont les informations sont redondantes ou complémentaires, mais n'est pas en mesure d'identifier exactement quel capteur est défaillant.

Nos travaux ont fait l'objet de deux réalisations physiques. D'une part, le tiroir inférieur de la cuisinière au laboratoire DOMUS s'est vu ajouter des connecteurs. Ces connecteurs permettent de facilement désolidariser le tiroir du reste de la cuisinière pour son remplacement en cas de panne matérielle, mises à jour ou autre. D'autre part, la réalisation de cartes électroniques au laboratoire Lab-STICC a permis de réaliser un prototype compact et peu coûteux de StoveMAS.

StoveMAS est un système qui se rajoute sur des appareils de cuisine existants. Son installation permet aux résidents d'être notifiés lorsque des situations à risque se présentent. Les usagers peuvent avoir une sensation de sécurité et de confort lors de la préparation de repas avec StoveMAS. L'inconvénient de StoveMAS est qu'il rend l'usage des appareils de cuisine impossible en dehors des plages d'utilisation prévue dans le profil utilisateur. Il se peut que pour certaines personnes StoveMAS produise de la frustration. Les usagers peuvent également

se déresponsabiliser vis-à-vis des risques de sécurité en considérant que StoveMAS les surveille. Par exemple, les usagers peuvent laisser le four ou une plaque de cuisson activé à la fin de la préparation d'un repas en se disant que de toute manière StoveMAS va s'occuper de couper l'appareil.

## Travaux futurs de recherche

À l'issue de cette thèse, un ensemble de règles ont été élaborées. Une perspective de ces travaux est de réaliser davantage de règles de sécurité, permettant d'avoir un système plus performant pour d'avantage de situations et environnements. Outre le nombre de règles de sécurité, la qualité, la complexité et la granularité des règles peuvent également être améliorées. C'est-à-dire que dans certains cas il peut être possible que des règles de sécurité soient contraires, auquel cas les agents mandataires de ces règles de sécurité doivent communiquer et négocier une solution.

L'aspect autoprotection de l'informatique autonome n'a pas vraiment été adressé. Étant donné que de plus en plus de systèmes informatiques dans un habitat domotique sont connectés à Internet, l'autoprotection ajouterait une couche de sécurité supplémentaire de sécurité pour protéger les données personnelles des résidents. Le cyber sécurité peut être une réponse à ces problématiques.

Les capteurs embarqués dans les appareils mobiles sont recueillis dans StoveMAS, ils ne sont cependant pas utilisés car leurs informations ne sont pas représentatives par rapport aux règles de sécurité implémentées. Ces données peuvent renforcer la localisation des différents utilisateurs et éventuellement remplacer l'identification des personnes via des cartes RFID. L'appareil mobile peut également servir pour localiser la personne dans l'environnement, en utilisant la triangulation par Wi-Fi (WPS : Wi-Fi Positioning System). L'intégration des données de capteurs issues d'appareils mobiles a permis de montrer qu'il était possible d'intégrer des capteurs inconnus au départ dans StoveMAS. Cette intégration peut être élargie

au niveau de capteurs dans l'environnement (détecteurs de mouvement sans fil au plafond, capteurs de contact sur les portes, etc.)

## Perspectives

Au vu de la flexibilité du système, il peut être envisagé de l'utiliser sur d'autres équipements de la cuisine, comme par exemple une cafetière, un réfrigérateur ou encore un robot de cuisine. La cafetière peut représenter un danger car il contient des liquides chauds, donc risque potentiel de brûlures. Pour le réfrigérateur, la notion de sécurité peut être élargie et vue comme des risques de sécurité d'un point de vue péremption des aliments. La notion de sécurité peut être également élargie jusqu'à l'échelle de l'habitat au complet, chaque pièce de l'habitat comporte son lot de risques et dangers pour une personne atteinte.

Au vu des réalisations matérielles lors de nos travaux, en particulier l'implantation de StoveMAS sur la Raspberry Pi et les cartes d'acquisition, StoveMAS est un prototype qui peut être commercialisé et installé par des personnes compétentes chez les résidents.

StoveMAS évolue dans un environnement dans lequel une multitude d'autres systèmes évoluent. De la coopération entre systèmes peut être envisagé pour que l'ensemble des systèmes ait une connaissance plus grande de l'activité des utilisateurs dans l'environnement. Ainsi, en plus d'être sensible au contexte, l'ensemble des systèmes formera l'intelligence ambiante du domicile. StoveMAS peut être vu comme étant un système dans une congrégation de plusieurs autres systèmes. Chaque système a ses propres buts, mais partagent une connaissance commune. Pour intégrer StoveMAS dans une telle congrégation, la connaissance commune dans StoveMAS doit être disponible pour les autres systèmes dans cette congrégation. Un agent dans StoveMAS aurait le rôle de faire la communication avec les autres systèmes et le partage des connaissances. De cette manière, des services pourraient littéralement suivre la personne dans ses déplacements dans son domicile, assurer sa sécurité

selon son profil, les personnes qui l'entourent, son environnement et l'activité qu'il souhaite réaliser.

# Bibliographie


[1] INSEE, “Population par âge Population par âge,” *Tableaux de l’Économie Française*, pp. 34 – 35, 2010.

[2] ISQ, *Le vieillissement démographique : de nombreux enjeux à déchiffrer*. 2012.

[3] Fougeyrollas Patrick, *La funambule, le fil et la toile. Transformations réciproques du sens du handicap*. 2011.

[4] OMS, “Rapport mondial sur le handicap,” 2011.

[5] M. Wortmann, “Dementia: a global health priority-highlights from an ADI and World Health Organization report,” *Alzheimers Res. Ther.*, vol. 4, no. 5, p. 40, 2012.

[6] A. Martin Prince *et al.*, “World Alzheimer Report 2015 The Global Impact of Dementia An analysis of prevalence, incidence, cost and trends,” *Alzheimer’s Dis. Int.*, 2015.

[7] P. P. Amouyel, “La perte de mémoire, première manifestation,” pp. 1–6, 2014.

[8] B. Reisberg, S. H. Ferris, M. J. De Leon, and T. Crook, “The global deterioration scale for assessment of primary degenerative dementia,” *Am. J. Psychiatry*, vol. 139, no. 9, pp. 1136–1139, 1982.

[9] Société Alzheimer du Canada, “Stade léger,” *Mal. d’Alzheimer Stade Léger*, 2013.

[10] Société Alzheimer du Canada, “Stade modéré,” *Mal. d’Alzheimer Stade Modéré*, 2013.

[11] Société Alzheimer du Canada, “Stade avancé,” *Mal. d’Alzheimer Stade Avancé*, 2013.

[12] ISQ, “Données sociales du Québec,” 2009.

[13] J. B. Waldner, *Nanocomputers and Swarm Intelligence*. 2013.

[14] M. Satyanarayanan, “Pervasive computing: Vision and challenges,” *IEEE Pers. Commun.*, vol. 8, no. 4, pp. 10–17, 2001.

[15] T. Dujardin and J. Rouillard, “Gestion intelligente d ’ un contexte domotique par un Système Multi-Agents,” *Actes Journées Francoph. sur les Systèmes Multi-Agents*, p. -– , 2011.

[16] M. Weiser, “Some computer science issues in ubiquitous computing,” *Commun. ACM*, vol. 36, no. 7, pp. 75 – 84, 1993.

[17] M. W. Musa, M. Mokhtari, B. M. Ali, M. F. a. Rasid, and M. Ghorbel, “Seamless semantic service provisioning mechanism for ambient assisted living,” *Proc. 8th Int. Conf. Adv. Mob. Comput. Multimed. - MoMM ’10*, pp. 119–125, 2010.

[18] A. Harter, A. Hopper, P. Steggles, A. Ward, and P. Webster, “The Anatomy of a Context-Aware Application,” *Wirel. Networks*, vol. 8, pp. 187–197, 2002.

[19] M. D. Addlesee, A. Jones, F. Livesey, and F. Samaria, “The ORL active floor,” *IEEE Pers. Commun.*, vol. 4, no. 5, pp. 35–41, 1997.

[20] R. J. Orr and G. D. Abowd, “The Smart Floor : A Mechanism for Natural User Identification and Tracking,” *Conf. Hum. Factors Comput. Syst.*, pp. 275–276, 2000.

[21] C. R. Yu, C. L. Wu, C. H. Lu, and L. C. Fu, “Human localization via multi-cameras and floor sensors in smart home,” *Conf. Proc. - IEEE Int. Conf. Syst. Man Cybern.*, vol. 5, pp. 3822–3827, 2007.

[22] C. Piechnick, S. Richly, T. Kühn, S. Götz, G. Püschel, and U. Aßmann, “ContextPoint: An Architecture for Extrinsic Meta-Adaptation in Smart Environments,” *Adapt. 2014, Sixth Int. Conf. Adapt. Self-Adaptive Syst. Appl.*, pp. 121–128, 2014.

[23] J. O. Kephart and D. M. Chess, “The Vision of Autonomic Computing,” *Computer (Long. Beach. Calif).*, vol. 36, pp. 41–50, 2003.

[24] M. E. Hoque, F. Rahman, S. I. Ahamed, and L. Liu, “Trust based security auto-configuration for smart assisted living environments,” *Proc. 2nd ACM Work. Assur. usable Secur. Config. - SafeConfig ’09*, p. 7, 2009.

[25] R. Iyengar, K. Kar, and S. Banerjee, “Low-coordination topologies for redundancy in sensor networks,” *Proc. 6th ACM Int. Symp. Mob. ad hoc Netw. Comput. - MobiHoc ’05*, p. 332, 2005.

[26] J. Byun, B. Jeon, J. Noh, Y. Kim, and S. Park, “An intelligent self-adjusting sensor for smart home services based on ZigBee communications,” *IEEE Trans. Consum. Electron.*, vol. 58, no. 3, pp. 794–802, 2012.

[27] F. Corno and F. Razzak, “Intelligent energy optimization for user intelligible goals in smart home environments,” *IEEE Trans. Smart Grid*, vol. 3, no. 4, pp. 2128–2135, 2012.

[28] H. Psaier and S. Dustdar, “A survey on self-healing systems: Approaches and systems,” *Computing*, vol. 91, no. 1, pp. 43–73, 2011.

[29] A. Ray and R. Luck, “An introduction to sensor signal validation in redundant measurement systems,” *Control Syst. IEEE*, vol. 11, no. 2, pp. 44–49, 1991.

[30] J. O. Kephart, “Research challenges of autonomic computing,” *Proc. 27th Int. Conf. Softw. Eng. 2005 ICSE 2005*, pp. 15–22, 2005.

[31] C. F. Liao, Y. W. Jong, and L. C. Fu, “PSMP: A fast self-healing and self-organizing pervasive service management protocol for smart home environments,” *Proc. 3rd IEEE Asia-Pacific Serv. Comput. Conf. APSCC 2008*, pp. 574–579, 2008.

[32] A. Arabo, I. Brown, and F. El-Moussa, “Privacy in the age of mobility and smart devices

in smart homes," *Proc. - 2012 ASE/IEEE Int. Conf. Privacy, Secur. Risk Trust 2012 ASE/IEEE Int. Conf. Soc. Comput. Soc. 2012*, pp. 819–826, 2012.

[33] J. Buford, G. Jakobson, and L. Lewis, "Extending BDI multi-agent systems with situation management," *2006 9th Int. Conf. Inf. Fusion, FUSION*, pp. 1–7, 2006.

[34] M. Wooldridge, *An introduction to multi-agent systems*. 2009.

[35] S. Poslad, "Specifying protocols for multi-agent systems interaction," *ACM Trans. Auton. Adapt. Syst.*, vol. 2, no. 4, p. 15, 2007.

[36] "FIPA Communicative Act Library Specification," *Architecture*, vol. 2000, no. SC00037J, 2002.

[37] B. Horling and V. Lesser, "A survey of multi-agent organizational paradigms," *Knowl. Eng. Rev.*, vol. 19, no. 04, p. 281, 2005.

[38] D. J. Cook *et al.*, "MavHome: an agent-based smart home," *Proc. First IEEE Int. Conf. Pervasive Comput. Commun. 2003. (PerCom 2003).*, pp. 1–4, 2003.

[39] D. Kotak, S. Wu, M. Fleetwood, and H. Tamoto, "Agent-based holonic design and operations environment for distributed manufacturing," *Comput. Ind.*, vol. 52, no. 2, pp. 95–108, 2003.

[40] L. Vig, J. A. Adams, and S. Member, "Multi-Robot Coalition Formation," vol. 22, no. 4, pp. 637–649, 2006.

[41] T. Pinto, H. Morais, P. Oliveira, Z. Vale, I. Praça, and C. Ramos, "A new approach for multi-agent coalition formation and management in the scope of electricity markets," *Energy*, vol. 36, no. 8, pp. 5004–5015, 2011.

[42] J. Yen, Y. H. Yan, B. J. Wang, P. K. H. Sin, and F. F. Wu, "Multi-agent Coalition Formation in Power Transmission Planning," *Syst. Sci. 1998., Proc. Thirty-First Hawaii*

*Int. Conf.*, vol. 4, pp. 433–443, 1998.

[43] J. Yang and Z. Luo, “Coalition formation mechanism in multi-agent systems based on genetic algorithms §,” vol. 7, pp. 561–568, 2007.

[44] H. Kitano *et al.*, “The RoboCup synthetic agent challenge 97,” *IJCAI Int. Jt. Conf. Artif. Intell.*, vol. 1, pp. 24–29, 1997.

[45] C. Candea, H. Hu, L. Iocchi, D. Nardi, and M. Piaggio, “Coordination in multi-agent RoboCup teams,” *Rob. Auton. Syst.*, vol. 36, no. 2–3, pp. 67–86, 2001.

[46] S. T. Gal A. Kaminka, Manuela M. Veloso, Steve Schaffer, Chris Sollitto, Rogelio Adobbati, Andrew N. Marshall, Andrew Scholer, “GameBots: A Flexible Test Bed for Multiagent Team Research,” *Commun. ACM*, vol. 45, no. 7, pp. 43–45, 2002.

[47] C. H. Brooks and E. H. Durfee, “Congregation Formation in Multiagent Systems,” *Auton. Agent. Multi. Agent. Syst.*, vol. 7, no. 1–2, pp. 145–170, 2003.

[48] N. Griffiths, “Supporting Cooperation Through Clans,” *Proc. IEEE Syst. Man Cybern. 2nd UK&RI Chapter Conf.*, no. September, pp. 87–96, 2003.

[49] Y. Moses and M. Tennenholtz, “Artificial social systems,” *Comput. AI*, vol. 4, no. 14, pp. 533–562, 1995.

[50] Z. Zhang and X. Zhang, “Realization of open cloud computing federation based on mobile agent,” *Proc. - 2009 IEEE Int. Conf. Intell. Comput. Intell. Syst. ICIS 2009*, vol. 3, pp. 642–646, 2009.

[51] M. P. Wellman, W. E. Walsh, P. R. Wurman, and J. K. MacKie-Mason, “Auction Protocols for Decentralized Scheduling,” *Games Econ. Behav.*, vol. 35, no. 1–2, pp. 271–303, 2001.

[52] B. Horling, R. Mailler, J. Shen, R. Vincent, and V. Lesser, “Using Autonomy,

Organizational Design and Negotiation in a Distributed Sensor Network," in *Distributed Sensor Networks*, vol. 9, V. Lesser, C. L. Ortiz, and M. Tambe, Eds. Boston, MA: Springer US, 2003, pp. 139–183.

[53] C. H. Brooks and E. H. Durfee, "Congregating and market formation," *Proc. first Int. Jt. Conf. Auton. agents multiagent Syst. part 1 - AAMAS '02*, p. 96, 2002.

[54] S. Abdallah and V. Lesser, "Organization-based cooperative coalition formation," in *Proceedings - IEEE/WIC/ACM International Conference on Intelligent Agent Technology. IAT 2004*, 2004, pp. 162–168.

[55] M. Mamei and F. Zambonelli, "Self-organization in multi agent systems: A middleware approach," in *Engineering Self-Organising Systems*, 2004, pp. 233–248.

[56] D. Ye, M. Zhang, and D. Sutanto, "Self-organization in an agent network: A mechanism and a potential application," *Decis. Support Syst.*, vol. 53, no. 3, pp. 406–417, 2012.

[57] M. Kranz, a Schmidt, A. Maldonado, and R. B. Rusu, "Context-aware kitchen utilities," *Proc. Int. Conf. Tangible Embed. Interact.*, pp. 213–214, 2007.

[58] H. Tsuji, Y. Yamakata, T. Furiatomi, H. Hiramatsu, and S. Mori, "IwaCam: A multimedia processing platform for supporting video-based cooking communication," *1st Int. Conf. Futur. Gener. Commun. Technol. FGCT 2012*, pp. 109–116, 2012.

[59] W. Ju, R. Hurwitz, T. Judd, and B. Lee, "CounterActive: an interactive cookbook for the kitchen counter," *Proc. ACM Conf. Hum. Factors Comput. Syst.*, pp. 269–270, 2001.

[60] J. Bradbury and E. Al, "Hands on cooking: towards an atentive kitchen," *CHI 03 Ext. Abstr. Hum. factors Comput. Syst.*, pp. 996–997, 2003.

[61] T. Y. Mou, T. S. Jeng, and C. H. Ho, "Sociable kitchen: Interactive recipe system in kitchen island," *Int. J. Smart Home*, vol. 3, no. 2, pp. 27–38, 2009.

[62] P. Y. Chi, J. H. Chen, H. H. Chu, and J. L. Lo, “Enabling calorie-aware cooking in a smart kitchen,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2008, vol. 5033 LNCS, pp. 116–127.

[63] K. L. Yam, “Intelligent packaging for the future smart kitchen,” *Packag. Technol. Sci.*, vol. 13, no. 2, pp. 83–85, 2000.

[64] Q. T. Tran and G. Calcaterra, “Cook ’ S Collage,” *Access*, 2005.

[65] Y. Li, M. Asghar, and P. Pulii, “Visually-aided smart kitchen environment for senior citizens suffering from dementia,” *Aware. Sci. Technol. ...*, pp. 584–590, 2013.

[66] E. Fernandes, J. Jung, and A. Prakash, “Security Analysis of Emerging Smart Home Applications,” *Symp. Secur. Priv.*, pp. 636–654, 2016.

[67] Samsung, “SmartThings,” 2017. [Online]. Available: https://www.smartthings.com/.

[68] V. Sivaraman, D. Chan, D. Earl, and R. Boreli, “Smart-Phones Attacking Smart-Homes.,” *Wisec*, pp. 195–200, 2016.

[69] T. De Champs, B. Abdulrazak, H. Pigot, M. Ouenzar, M. Frappier, and B. Fraikin, “Pervasive safety application with model checking in smart houses: The INOVUS intelligent oven,” in *2011 IEEE International Conference on Pervasive Computing and Communications Workshops, PERCOM Workshops 2011*, 2011, pp. 630–635.

[70] S. Pinard *et al.*, “Maximizing safety during meal preparation in persons with TBI,” in *Canadian Association of Occupational Therapists*, 2016.

[71] David Grimshaw, “JADE Administration Tutorial,” 2010. [Online]. Available: http://jade.tilab.com/doc/tutorials/JADEAdmin/index.html.

[72] IDC, “Smartphone OS Market Share, 2015 Q2,” 2015. [Online]. Available:

http://www.idc.com/prodserv/smartphone-os-market-share.jsp.

[73] Android, “Platform Versions,” 2016. [Online]. Available: https://developer.android.com/about/dashboards/index.html. [Accessed: 05-Jan-2017].

[74] S. Clark, “Two in three phones to come with NFC in 2018,” 2014. [Online]. Available: http://www.nfcworld.com/2014/02/12/327790/two-three-phones-come-nfc-2018/.

[75] M. Castebrunet, “Etude et conception d’un système de personnalisation et d‘ aide fonctionnelle multi-agents permettant d’assister simultanément de manière transparent les activités de vie quotidienne de multiples personnes dans un Habitat Intelligent pour la Santé,” 2011.

[76] A. Cooper, *The Inmates Are Running the Asylum: Why High Tech Products Drive Us Crazy and How to Restore the Sanity*. 1999.

[77] Android, “Android Sensor Event,” 2016. [Online]. Available: http://developer.android.com/reference/android/hardware/SensorEvent.html#values.

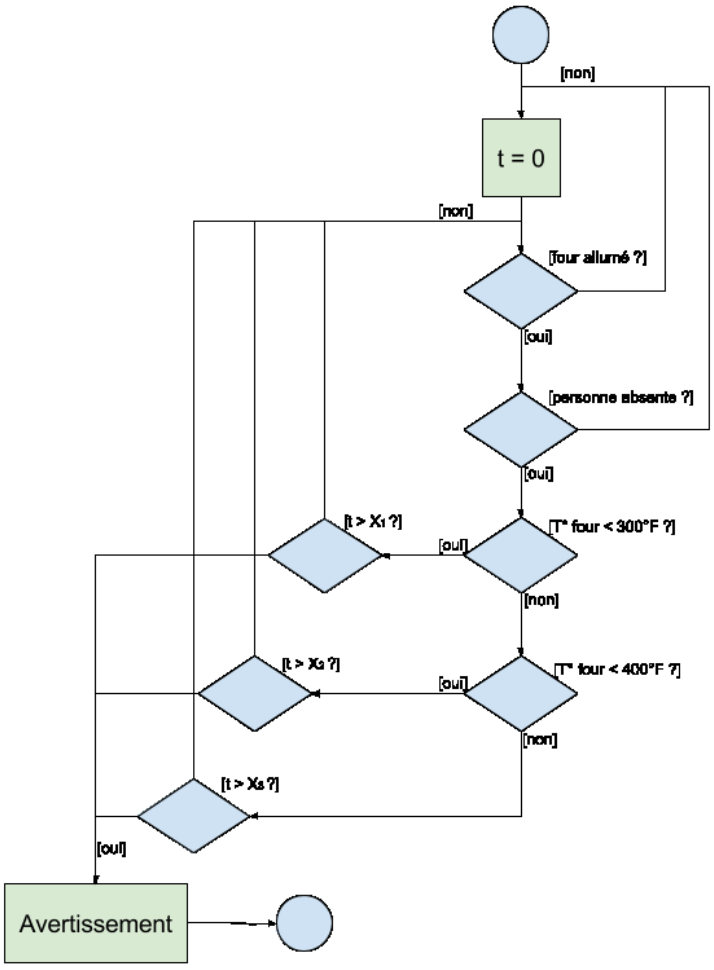
[78] N. Kuijpers, S. Giroux, F. De Lamotte, and J. Philippe, “Proposal of an adaptive service providing system for a multi-user smart home,” *Work. Thirtieth AAAI Conf. Artif. Intell. - Artif. Intell. Appl. to Assist. Technol. Smart Environ. Tech. Rep. WS-16-01*, no. 1, pp. 41 – 46, 2016.

# Annexe A

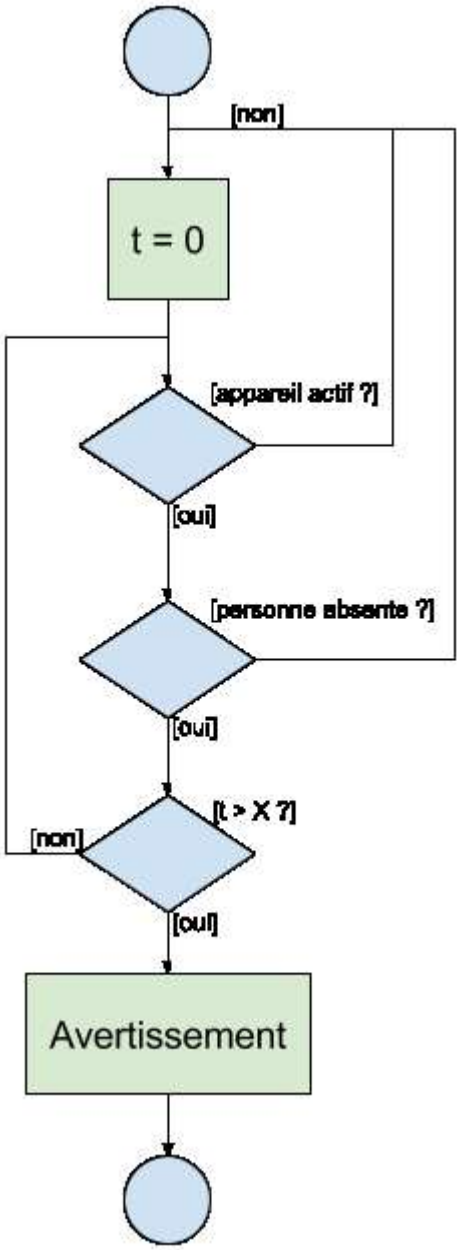
# Situations à risque

Cette annexe présente les différentes situations à risque (2.6.1) sous forme de schémas fonctionnels.

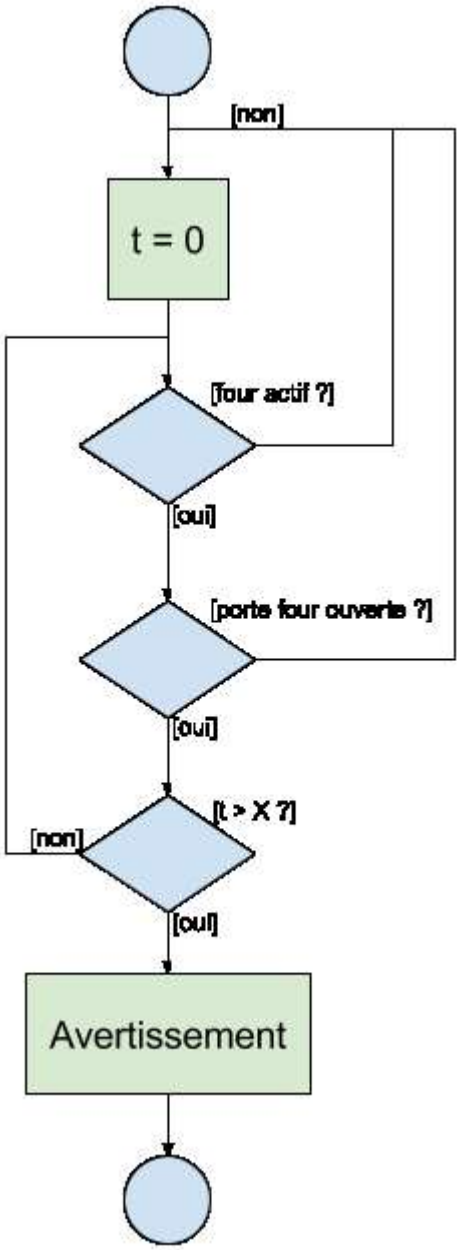
## A.1 La situation à risque 1 : Four activé et absence usager pendant X minutes



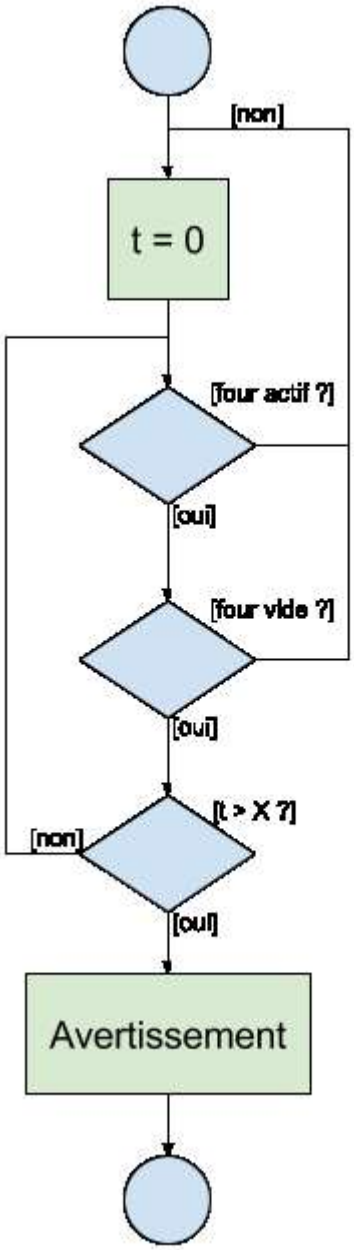
## A.2 La situation à risque 2 : Porte du four ouverte depuis X minutes



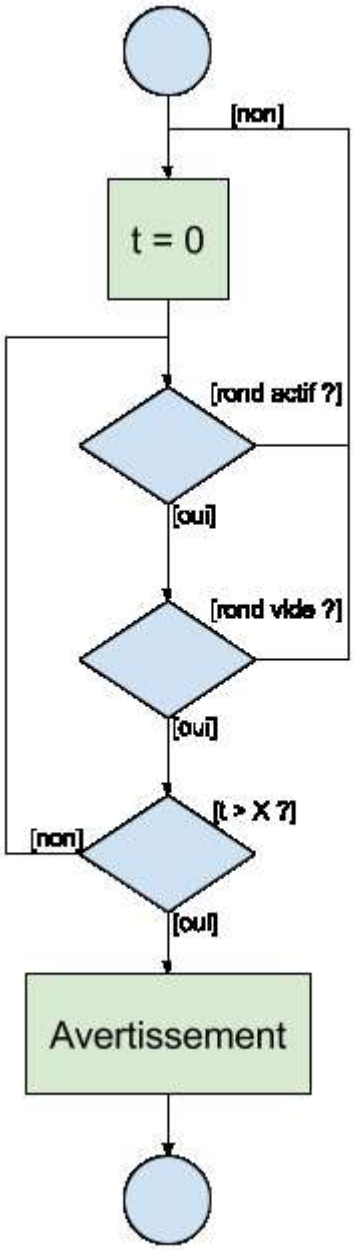
## A.3 La situation à risque 3 : Four vide et activé depuis X minutes



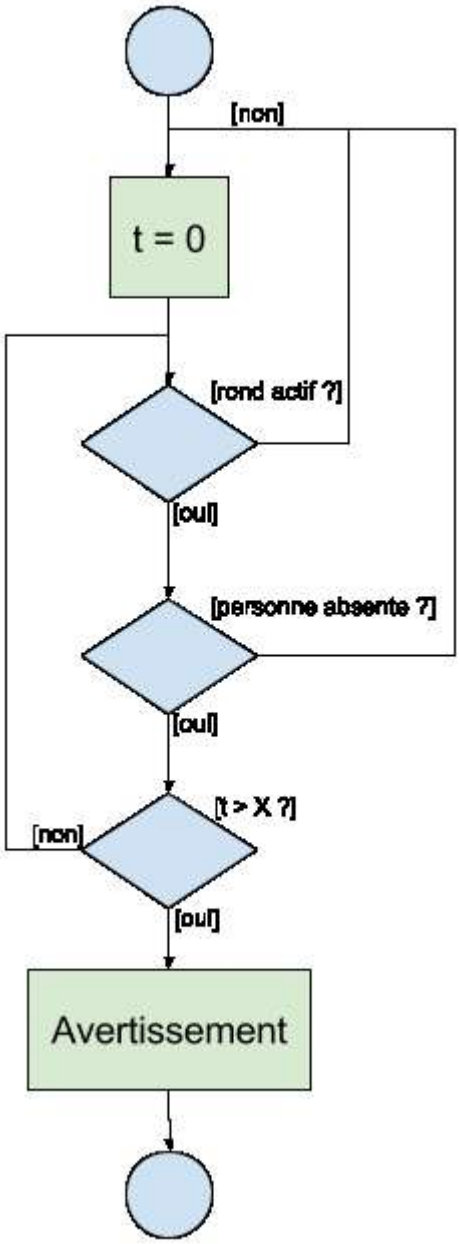
## A.4 La situation à risque 4 : Inactivité des appareils depuis X minutes



## A.5 La situation à risque 5 : Rond activé mais vide pendant X minutes



## A.6 La situation à risque 6 : Rond activé et absence utilisateur pendant X minutes



# Annexe B

# Profils utilisateurs

Cette annexe présente les différents profils utilisateurs utilisés lors du développement et expérimentations. Ces profils utilisateurs se présentent comme des fichiers aux noms de *NOM_PERSONNE.json*, où le nom de personne est défini dans un fichier *PROFILES.json*. Ces fichiers se trouvent dans le dossier */json/userprofiles/* du programme.

## B.1 Le fichier Profiles.json

```
// Profiles.json
{
    "profiles": [
        {
            "name": "Rene",
            "rfidcode": "7E00203E3858",
            "email": "labdomus.rene@gmail.com"
        },
            {
            "name": "Claude",
            "rfidcode": "7E00203E3859",
            "email": "labdomus.claude@gmail.com"
        },
        {
            "name": "Jeanne",
            "rfidcode": "7E002051C2CD",
            "email": "labdomus.jeanne@gmail.com"
        },
        {
            "name": "Georges",
            "rfidcode": "7E00203E3860",
            "email": "labdomus.georges@gmail.com"
        }
    ]
}
```

## B.2 Le profil utilisateur de René

```
// Rene.json
{
    "name": "Rene",
    "email": "labdomus.rene@gmail.com",
    "coaching_ability": "-1",
    "device_lockdown_time_before_use": "200000",
    "device_lockdown_time_after_use": "240000",
    "user_absence_time": "300000",
    "oven_door_open_time": "20000",
    "empty_oven_active_time": "15000",
    "empty_hob_active_time": "15000",
    "unlock_capable": "false",

    "surface_burner": [
        {
            "id": "fl",
            "activated": "false"
        },
        {
            "id": "rl",
            "activated": "true"
        },
        {
            "id": "rr",
            "activated": "false"
        },
        {
            "id": "fr",
            "activated": "true"
        }
    ],
    "oven": [
        {
            "id": "bake",
            "activated": "true"
        },
        {
            "id": "broil",
            "activated": "true"
        }
    ],
    "microwave": [
        {
            "id": "microwave",
            "activated": "true"
        },
        {
            "id": "grill",
            "activated": "true"
        },
        {
            "id": "convection",
```

```
            "activated": "true"
        }
    ],
    "unlock_times": [
        {
            "format": "HH:mm:ss"
        },
        {
            "start": "11:30:00",
            "end":  "13:00:00"
        },
        {
            "start": "19:00:00",
            "end":  "21:00:00"
        }
    ]
}
```

## B.3 Le profil utilisateur de Jeanne

```
// Jeanne.json
{
    "name": "Jeanne",
    "email": "labdomus.jeanne@gmail.com",
    "coaching_ability": "1",
    "device_lockdown_time_before_use": "180000",
    "device_lockdown_time_after_use": "180000",
    "user_absence_time": "600000",
    "oven_door_open_time": "30000",
    "empty_oven_active_time": "30000",
    "empty_hob_active_time": "15000",
    "unlock_capable": "true",

    "surface_burner": [
        {
            "id": "fl",
            "activated": "true"
        },
        {
            "id": "rl",
            "activated": "true"
        },
        {
            "id": "rr",
            "activated": "true"
        },
        {
            "id": "fr",
            "activated": "true"
        }
    ],
    "oven": [
```

```
        {
            "id": "bake",
            "activated": "true"
        },
        {
            "id": "broil",
            "activated": "true"
        }
    ],
    "microwave": [
        {
            "id": "microwave",
            "activated": "true"
        },
        {
            "id": "grill",
            "activated": "true"
        },
        {
            "id": "convection",
            "activated": "true"
        }
    ],
    "unlock_times": [
        {
            "format": "HH:mm:ss"
        },
        {
            "start": "00:00:00",
            "end":  "23:59:59"
        }
    ]
}
```

## B.4 Le profil utilisateur de Claude

```
// Claude.json
{
    "name": "Claude",
    "email": "labdomus.claude@gmail.com",
    "coaching_ability": "-1",
    "device_lockdown_time_before_use": "180000",
    "device_lockdown_time_after_use": "180000",
    "user_absence_time": "180000",
    "oven_door_open_time": "15000",
    "empty_oven_active_time": "15000",
    "empty_hob_active_time": "15000",
    "unlock_capable": "false",

    "surface_burner": [
        {
            "id": "fl",
```

```
            "activated": "true"
        },
        {
            "id": "rl",
            "activated": "false"
        },
        {
            "id": "rr",
            "activated": "false"
        },
        {
            "id": "fr",
            "activated": "false"
        }
    ],
    "oven": [
        {
            "id": "bake",
            "activated": "true"
        },
        {
            "id": "broil",
            "activated": "false"
        }
    ],
    "microwave": [
        {
            "id": "microwave",
            "activated": "true"
        },
        {
            "id": "grill",
            "activated": "true"
        },
        {
            "id": "convection",
            "activated": "false"
        }
    ],
    "unlock_times": [
        {
            "format": "HH:mm:ss"
        },
        {
            "start": "12:30:00",
            "end":  "14:00:00"
        },
        {
            "start": "20:00:00",
            "end":  "22:00:00"
        }
    ]
}
```

# Annexe C

# Branchements des modules au laboratoire Lab-STICC

Ce composant gère 8 entrées analogiques. Au vu du nombre de capteurs à gérer, nous avons besoin de 3 CAN. L'alimentation électrique du *MCP3008* se fait en 5V, il peut alors être directement alimenté par la Raspberry Pi. Les signaux en entrée du CAN doivent être des tensions analogiques entre 0V et 5V représentatives de la grandeur qu'on souhaite mesurer. La partie logicielle de l'acquisition est assurée par l'agent *SPIAgent*. Cet agent communique avec les CAN via le bus SPI. Une liaison SPI est réalisée entre un maître et un ou plusieurs esclaves. Dans notre cas, le maître est la Raspberry Pi et les esclaves sont les CAN (Figure 54).

- Une liaison MISO (Master In / Slave Out) permet aux CAN d'envoyer des données au maitre. Cette liaison est faite entre tous les composants SPI.

- Une liaison MOSI (Master Out / Slave In) permet au maitre d'envoyer des données aux esclaves. Cette liaison a été mise en place mais n'est pas utilisée dans notre cas, car actuellement ce bus permet seulement de connaitre l'état des capteurs. Seulement les CAN disposent d'une entrée MOSI.

- Une liaison CLK (Clock) permet de définir la vitesse à laquelle notre bus fonctionne, par conséquent tous les composants SPI sont reliés par cette liaison.

- Plusieurs liaisons CS (Chip Select) permettent au maitre de sélectionner l'esclave qu'il souhaite écouter. Nous disposons en tout de six esclaves (3 CAN et 3 modules d'acquisition pour thermocouples).

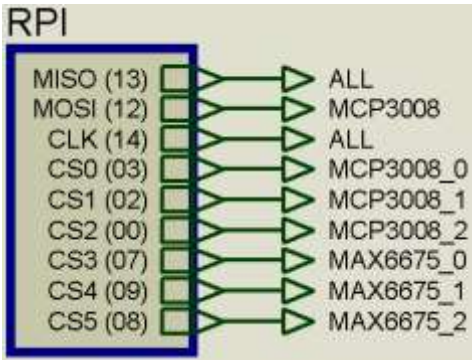



Figure 54 - Liaison SPI entre la Raspberry Pi et les composants.

On utilise les librairies *Pi4j* permettant à l'agent *SPIAgent* de communiquer avec le GPIO de la Raspberry Pi. Ces librairies disposent d'un ensemble de fonctionnalités facilitant l'usage de la carte et le contrôle des différents GPIO nécessaires (Figure 55). Dans l'agent, il faut associer chaque pin à la fonction dont on a besoin. Ensuite, l'agent écoute, à tour de rôle, sur chaque entrée analogique des CAN et des modules d'acquisition des thermocouples pour obtenir les données. A chaque lecture d'entrée, l'agent donne une impulsion d'horloge. La vitesse d'horloge dépend donc de la vitesse d'exécution de la boucle de lecture. Par exemple, des tests en utilisant une Raspberry Pi 2 nous donne environ 2 lectures par seconde par capteur, tandis que la Raspberry Pi 3 nous donne environ 4 lectures par seconde. A chaque écoute de capteur, l'agent met à jour la base de données des capteurs dans le SMA.


Figure 55 - Numérotation des pins du GPIO sur la Raspberry Pi en utilisant *Pi4j*.

## C.1 Les capteurs de pression

Les capteurs de pression que nous utilisons sont des résistances variables selon la pression exercée sur celles-ci. Cette résistance varie entre environ 40kΩ et >5MΩ. Ainsi, la résistance variable du capteur ainsi que la résistance R4 se comportent comme un pont diviseur de tension, avec une tension variable entre 0V et 1.4V (Figure 56). L'amplificateur opérationnel *MCP602* est alimenté en 0-5V et est utilisé dans un montage amplificateur de signal non inverseur. La tension de sortie de ce montage est donnée par l'Équation 4 et donne une tension variable entre 0V et 4.2V :

$$U_s = \left(1 + \frac{R_2}{R_1}\right) U_e$$

Équation 4 - Relation de tensions dans un montage amplificateur non inverseur.

Le couple R3 et C2 forment un filtre passe bas pour supprimer le bruit dans le signal. Ce filtre induit une constante de temps caractérisant la rapidité de l'évolution du signal. Dans le cas ci présent, cette constante de temps est représentée par le produit $\tau = RC$ et vaut $\tau = 0.22$ secondes. C'est-à-dire qu'il faut un temps de 0.22 secondes au signal pour atteindre 63% de sa valeur finale. On considère qu'il faut un temps $3\tau$, soit un peu plus d'une demi-seconde, pour atteindre sa valeur totale. La valeur de la résistance R3 a été choisie en fonction du courant de sortie maximal de l'amplificateur opérationnel. Ensuite, la valeur du condensateur C1 a été choisie pour correspondre à une constante de temps équivalente à la vitesse de lecture sur le bus SPI de la Raspberry Pi, qui est d'environ deux lectures par seconde. Ce montage est utilisé pour tous les capteurs de pression que nous utilisons, indépendamment de l'appareil sur lequel ils sont installés.

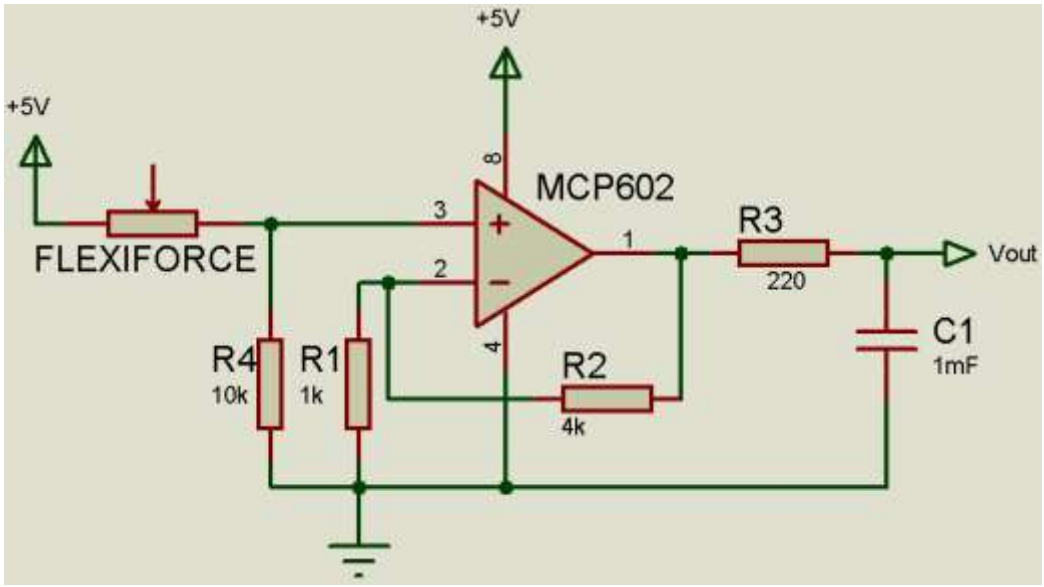



Figure 56 - Montage de l'acquisition des données issues des capteurs de pression.

## C.2 Les capteurs de courant

Les capteurs de courant fournissent une tension image du courant qu'on souhaite mesurer. Les appareils dont nous disposons fonctionnent avec l'électricité du réseau électrique, à savoir une tension sinusoïdale 230V à 50Hz. Par conséquent, la tension fournie par le capteur de courant est une tension sinusoïdale 1V à 50Hz. Lorsqu'on branche ce capteur sur la plaque vitrocéramique et qu'on allume le petit foyer (1200W), on observe à l'oscilloscope la courbe illustrée en Figure 57. La puissance consommée par l'appareil peut être retrouvée avec l'Équation 5 :

$$P = U_{eff} I_{eff} \cos(\varphi) = U_{eff} \frac{U_{max} * \Delta_{AMP}}{\sqrt{2}} \cos(\varphi)$$

$$P = 230 * \frac{0{,}256 * 30}{\sqrt{2}} * 1 = 1249\ W$$

Équation 5 - Calcul de la puissance consommée par un appareil électrique.

Dans cette formule on voit apparaitre le facteur $\Delta_{AMP}$ qui représente le rapport de réduction de l'amplitude du signal. La valeur du $\cos(\varphi)$ est bien égale à 1 car nous disposons d'un appareil purement résistif.

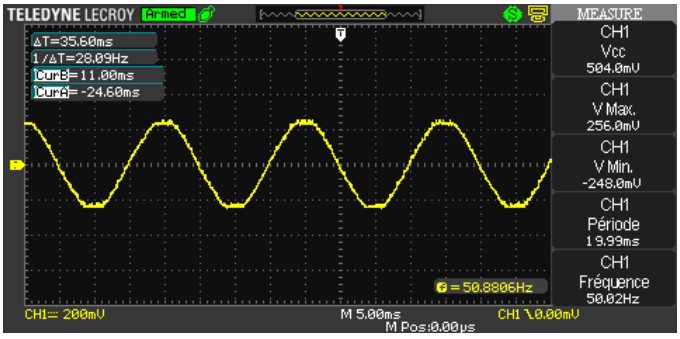



Figure 57 - Courbe issue du capteur de courant sur la plaque vitrocéramique.

Le CAN a besoin d'une tension continue 0-5V, le signal doit être redressé. Un pont de diodes permet de redresser un signal sinusoïdal (Figure 58) en double alternance. C'est-à-dire que la

partie négative du signal sinusoïdal est transformée en signal positif. Cependant, l'utilisation des diodes implique une chute de tension d'environ 1.4V (0.7V par diode). Le redressement, en utilisant un pont de diode, n'est donc pas envisageable compte tenu de l'amplitude du signal que fournit le capteur.

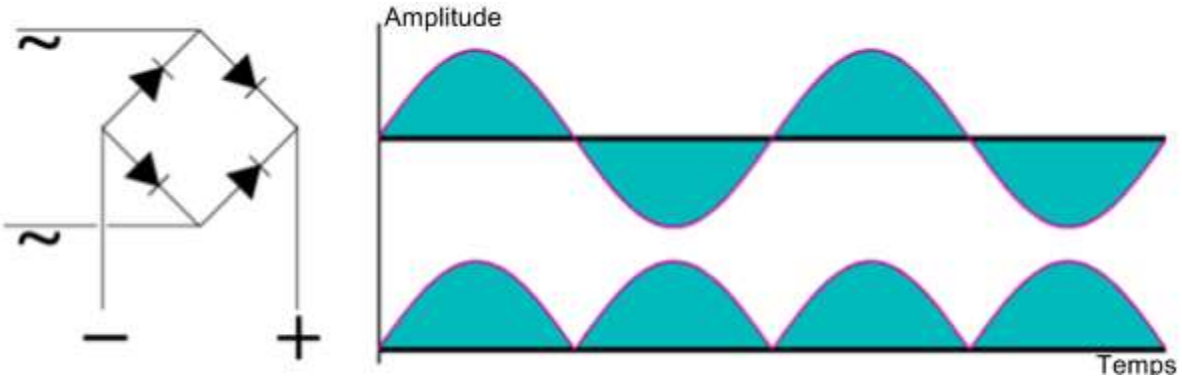



Figure 58 - Fonctionnement d'un pont de diodes double alternance.

Le redressement peut également se faire via un amplificateur opérationnel. On combine le redressement et l'amplification dans une seule opération (Figure 60). Le redressement est possible car l'amplificateur opérationnel est alimenté en 0-5V. Cependant, ce redressement est à simple alternance. Ceci implique que la partie négative du signal sinusoïdal est transformé en signal nul (Figure 59).

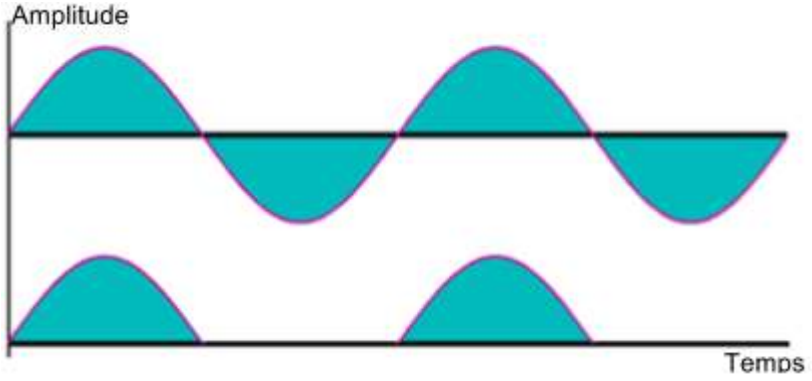



Figure 59 - Fonctionnement d'un redressement simple alternance.

Le montage amplificateur non inverseur (R5 et R6) est identique au montage proposé pour les capteurs de force, aux valeurs des résistances près. Une telle amplification est nécessaire ; (1)

d'une part pour atteindre les 5V d'amplitude nécessaire afin de bénéficier de la pleine échelle du CAN. (2) Le capteur est surdimensionné par rapport aux besoins, la valeur de sortie de 1V n'est jamais atteinte. En sortie de l'amplificateur opérationnel, on retrouve un filtre passe bas identique au montage pour les capteurs de pression. Une résistance de pull-down (R8) est nécessaire afin de faire une mise à zéro du signal lorsque l'appareil est éteint. En effet, les capteurs de courant utilisent le champ magnétique produit par le fil que l'on mesure, mais des champs magnétiques parasites peuvent se produire et fausser les données lorsque l'élément qu'on souhaite contrôler est éteint.

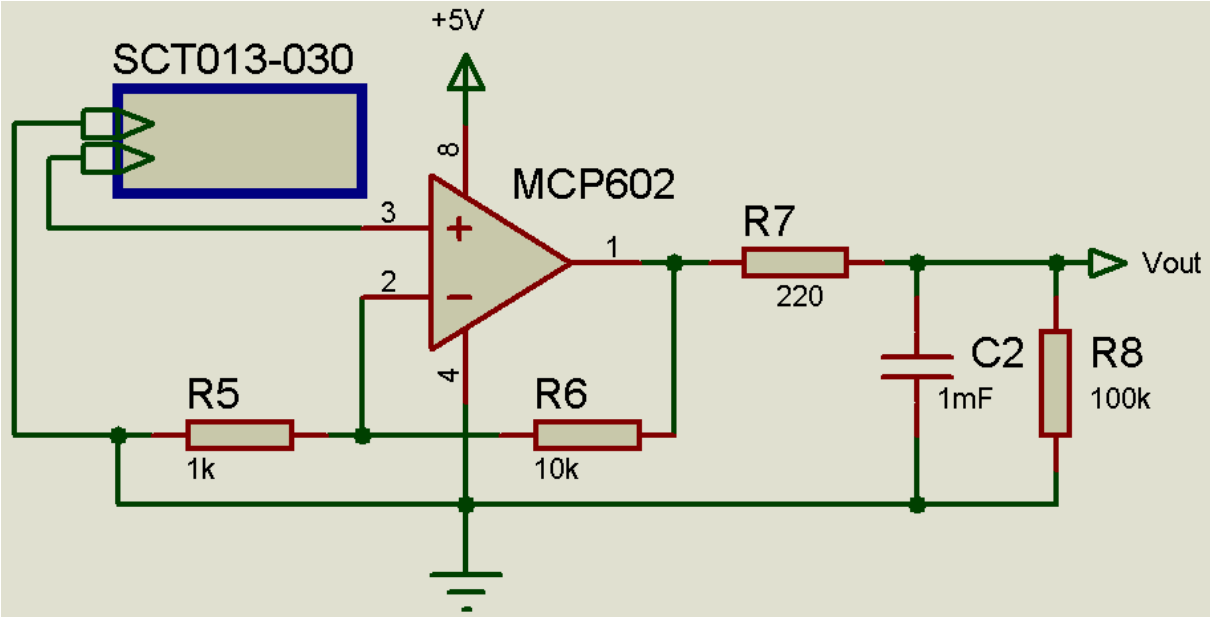



Figure 60 - Montage de l'acquisition des données issues des capteurs de courant.

## C.3 Le capteur de contact

Le capteur de contact est également connecté sur les modules CAN, cependant son fonctionnement est binaire. On associe à ces deux états deux tensions correspondantes, à savoir 0 et 5V respectivement à l'état ouvert et fermé. Une résistance de pull-down permet de se rassurer que la tension soit effectivement à 0V lorsque l'interrupteur est ouvert.

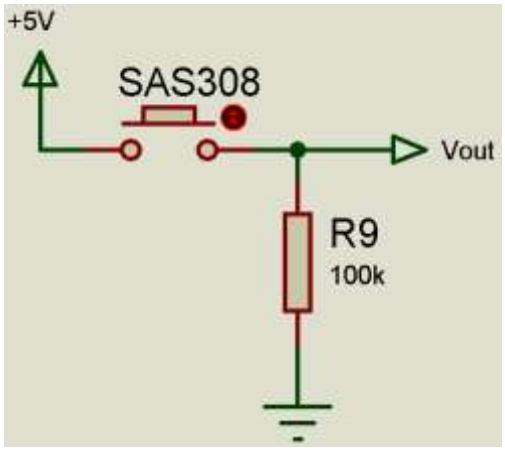



Figure 61 - Montage de l'acquisition des données issues du contact.

## C.4 Les capteurs de présence

Les capteurs de présence et infrarouge fournissent nativement une tension variable entre 0V et 5V. Leur montage est aisé et correspond au montage illustré en Figure 62.

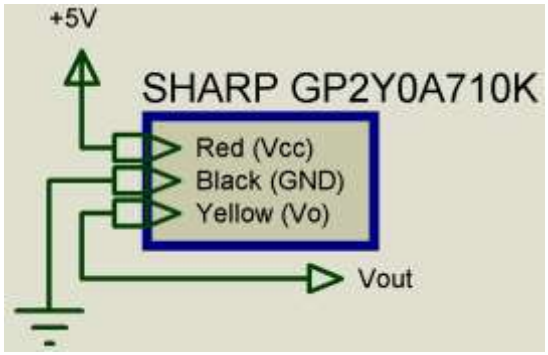



Figure 62 - Montage des capteurs de présence.

## C.5 Les capteurs de température

Les capteurs de température sont des thermocouples de type K. Il est nécessaire d'utiliser un convertisseur qui permet de transformer le signal issu du thermocouple en un signal exploitable pour le système. Les composants *MAX6675* permettent de transformer un signal issu d'un

thermocouple de type K en un signal SPI sur 12 bits (Figure 63). Il est alors possible de mesurer des températures allant jusqu'à 1024°C avec une précision de 0.25°C.

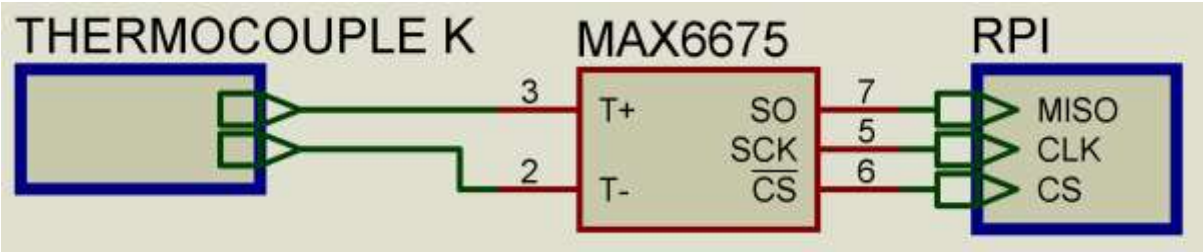



Figure 63 - Montage des capteurs de température.

# Annexe D

# Branchements des modules ADAM au laboratoire DOMUS

Au laboratoire DOMUS, le système est implanté sur un ordinateur industriel qui se situe à l'intérieur du tiroir en bas de la cuisinière. L'acquisition des données se fait par l'intermédiaire d'un boitier ADAM-5000/TCP. Ce boitier est un boitier d'acquisition modulaire sur lequel jusqu'à huit modules différents, selon la nature de l'acquisition, peuvent se greffer. Contrairement à l'acquisition des données au laboratoire Lab-STICC, le boitier ADAM fait automatiquement la mise en forme du signal. Ce boitier communique par réseau à l'ordinateur industriel. Dans la cuisinière, les modules suivants sont installés (Figure 64) :

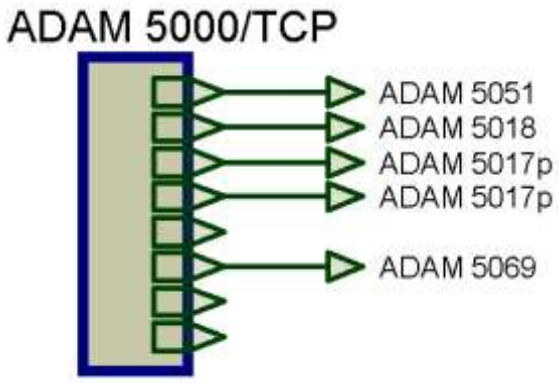



Figure 64 - Modules d'acquisition sur le boitier ADAM-5000/TCP.

Un module 5051. Ce module propose 16 entrées tout ou rien. L'état logique bas se trouve entre 0 et 2V, tandis que l'état logique haut se trouve entre 4 et 30V. En tout, 8 capteurs peuvent être connectés sur ce module (en borne + et -). Ce module est utilisé pour connaitre l'état de la sécurité, l'armement de la cuisinière ainsi que l'état de la porte du four.

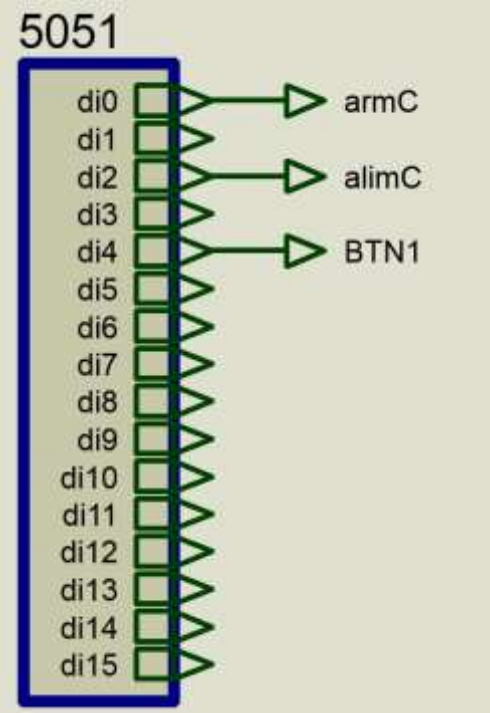



Figure 65 - Branchements du module ADAM-5051.

Un module 5018. Ce module est composé de 7 entrées différentielles. Ces entrées ont une résolution 16 bits et acceptent une mesure en tension jusqu'à ±2.5 V ou une mesure en intensité jusqu'à ±20 mA. Ce module a un taux d'échantillonnage de 10 échantillons par seconde. Actuellement, les cinq thermocouples (TC) correspondant à chacun des ronds et un thermocouple du four y est connecté (Figure 66).

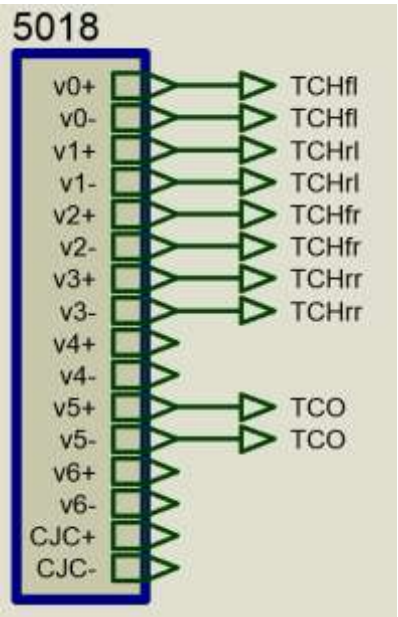



Figure 66 - Branchements du module ADAM-5018.

Deux modules 5017p. Le module ADAM 5017p est composé de 8 entrées analogiques différentielles d'une résolution 16 bits et acceptent une mesure en tension jusqu'à ±10 V ou une mesure en intensité jusqu'à ±20 mA. Ce module a un taux d'échantillonnage de 10 échantillons par seconde. La différence entre le module ADAM 5017p et le module ADAM 5018 est que le second dispose d'une entrée thermocouple qui est usuellement utilisée pour mesurer une température. Le premier module ADAM 5017p est configuré pour recevoir des mesures en courant. Les capteurs ultrason y sont branchés (Figure 67). Le second, en mesure de tension, permet l'acquisition des données issues des capteurs de pression (Figure 68).

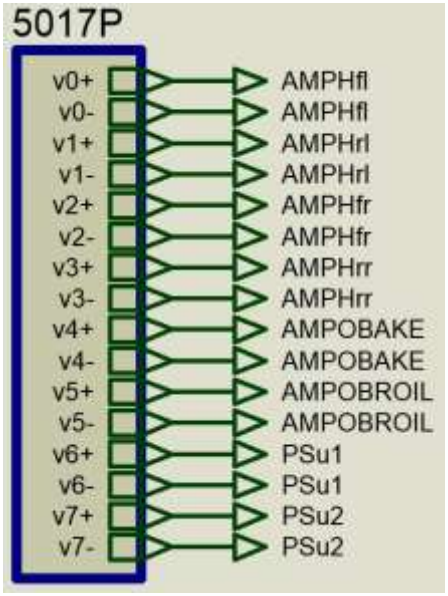



Figure 67 - Branchements du module ADAM-5017p (en courant).

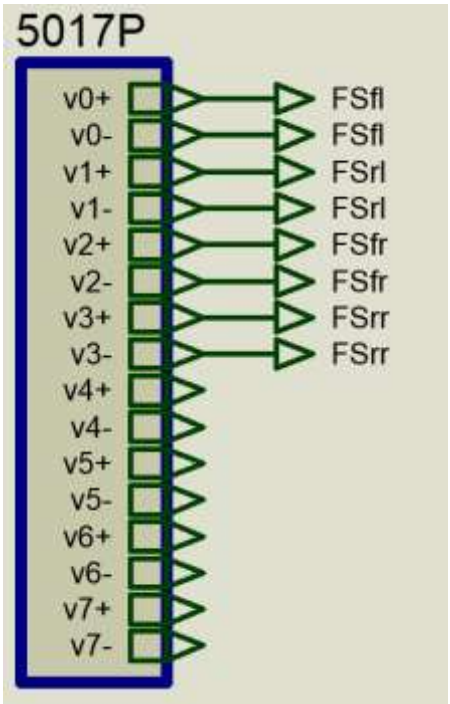



Figure 68 - Branchements du module ADAM-5017p (en tension).

Un module 5069. Ce module n'est pas un module d'acquisition, mais un module de commande. En effet, ce module permet de commander les relais pour verrouiller la cuisinière (Figure 69). Dans le cadre du verrouillage de la cuisinière, seulement les relais RLY4 et RLY7 nous intéressent.

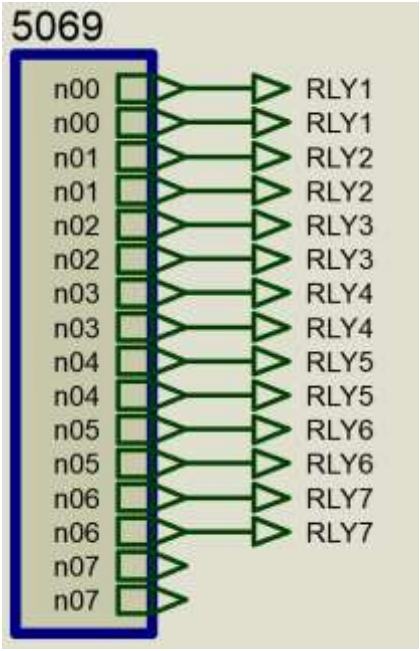



Figure 69 - Branchements du module ADAM-5069.

# Annexe E

# Profils des appareils

Cette annexe présente les différents profils des appareils utilisés lors du développement et expérimentations. Ces profils se présentent comme des fichiers aux noms de *NOM_APPAREIL.json*. Les fichiers de configuration en Annexe E1 et E2 sont utilisés au laboratoire DOMUS, tandis que les fichiers de configuration en Annexe E3 et E4 sont utilisés au laboratoire Lab-STICC. Ces fichiers se trouvent dans le dossier */json/deviceprofiles/* du programme

## E.1 Le fichier Frigidaire_CFEF3048LSM_Hobs.json

```
1.  {
2.      "thresholds": [
3.          {
4.              "id": "current",
5.              "function": "hobfl",
6.              "value": "-0.01"
7.          },
8.          {
9.              "id": "current",
10.             "function": "hobrl",
11.             "value": "-0.01"
12.         },
13.         {
14.             "id": "current",
15.             "function": "hobfr",
16.             "value": "-0.01"
17.         },
18.         {
19.             "id": "current",
20.             "function": "hobrr",
21.             "value": "-0.01"
22.         },
23.         {
24.             "id": "temperature",
25.             "function": "temperature",
26.             "value": "75"
27.         },
28.         {
29.             "id": "presence",
30.             "function": "presence",
```

```
            "value": "100"
        },
        {
            "id": "weight",
            "function": "weight",
            "value": "100"
        }
    ],

    "sensors": [
        {
            "current": [
                {
                    "id": "AMPHfl"
                },
                {
                    "id": "AMPHrl"
                },
                {
                    "id": "AMPHfr"
                },
                {
                    "id": "AMPHrr"
                }
            ]
        },
        {
            "temperature": [
                {
                    "id": "TCHfl"
                },
                {
                    "id": "TCHrl"
                },
                {
                    "id": "TCHfr"
                },
                {
                    "id": "TCHrr"
                }
            ]
        },
        {
            "weight": [
                {
                    "id": "FSHfl"
                },
                {
                    "id": "FSHrl"
                },
                {
                    "id": "FSHfr"
                },
                {
                    "id": "FSHrr"
                }
```

```
            ]
        },
        {
            "presence": [
                {
                    "id": "PSHfl"
                },
                {
                    "id": "PSHrl"
                },
                {
                    "id": "PSHfr"
                },
                        {
                            "id": "PSHrr"
                        }
                    ]
                },
                {
                    "activation": [
                        {
                            "id": "lock"
                        }
                    ]
                }
            ],

            "weight": [
                        {
                          "resolution": "10.96",
                          "deviceweight": "7000",
                          "fixedweightresolution": "false",
                          "dynamictare": "false"
                    }
            ]
      }
```

## E.2 Le fichier Frigidaire_CFEF3048LSM_Oven.json

```
{
    "thresholds": [
        {
            "id": "current",
            "function": "bake",
            "value": "50"
        },
        {
            "id": "current",
            "function": "broil",
            "value": "50"
        },
        {
            "id": "temperature",
```

```
            "function": "oven",
            "value": "75"
        },
        {
            "id": "weight",
            "function": "weight",
            "value": "100"
        }
    ],

    "sensors": [
        {
            "current": [
                {
                    "id": "AMPOBake"
                },
                {
                    "id": "AMPOBroil"
                }
            ]
        },
        {
            "temperature": [
                {
                    "id": "TCO"
                }
            ]
        },
        {
            "weight": [
                {
                    "id": "FSOfl"
                },
                {
                    "id": "FSOrl"
                },
                {
                    "id": "FSOfr"
                },
                {
                    "id": "FSOrr"
                }
            ]
        }
    ],

    "weight": [
        {
            "resolution": "10.96",
            "deviceweight": "7000",
            "fixedweightresolution": "false",
            "dynamictare": "false"
        }
    ]
}
```

## E.3 Le fichier Brandt_tv1000b.json

```
{
    "tresholds": [
        {
            "id": "current",
            "name": "hobhigh",
            "value": "50"
        },
        {
            "id": "current",
            "name": "hoblow",
            "value": "50"
        },
        {
            "id": "current",
            "name": "hobboth",
            "value": "50"
        },
        {
            "id": "temperature",
            "name": "hobhigh",
            "value": "75"
        },
        {
            "id": "temperature",
            "function": "hoblow",
            "value": "75"
        },
        {
            "id": "weight",
            "function": "weight",
            "value": "100"
        }
    ],

    "sensors": [
        {
            "current": [
                {
                    "id": "AMPHh"
                },
                {
                    "id": "AMPHl"
                },
                {
                    "id": "AMPH2"
                }
            ],
        };
        {
```

```
            "temperature": [
                {
                    "id": "TCHh"
                },
                {
                    "id": "TCHl"
                }
            ],
        },
        {
            "weight": [
                {
                    "id": "FSHfl"
                },
                {
                    "id": "FSHrl"
                },
                {
                    "id": "FSHfr"
                },
                {
                    "id": "FSHrr"
                }
            ]
        }
    ],

    "weight": [
        {
            "resolution": "10.96",
            "deviceweight": "7000",
            "fixedweightresolution": "false",
            "dynamictare": "false"
        }
    ]
}
```

## E.4 Le fichier Samsumg-mc28h5125ak.json

```
{
    "tresholds": [
        {
            "id": "current",
            "function": "microwave",
            "value": "50"
        },
        {
            "id": "current",
            "function": "grill",
            "value": "50"
        },
        {
            "id": "current",
```

```
            "function": "convection",
            "value": "50"
        },
        {
            "id": "temperature",
            "function": "temperature",
            "value": "75"
        },
        {
            "id": "weight",
            "function": "weight",
            "value": "100"
        }
    ],

    "sensors": [
        {
            "current": [
                {
                    "id": "AMPOm"
                },
                {
                    "id": "AMPOg"
                },
                {
                    "id": "AMPOc"
                }
            ],
        };
        {
            "temperature": [
                {
                    "id": "TCO"
                }
            ],
        },
        {
            "weight": [
                {
                    "id": "FSMfl"
                },
                {
                    "id": "FSMrl"
                },
                {
                    "id": "FSMfr"
                },
                {
                    "id": "FSMrr"
                }
            ]
        }
    ],

    "weight": [
        {
```

```
71.             "resolution": "10.96",
72.             "deviceweight": "17300",
73.             "fixedweightresolution": "false",
74.             "dynamictare": "false"
75.         }
76.     ]
77. }
```

# Annexe F

# Scénarios d'expérimentation

Ces scénarios permettent de tester différents critères de notre système. Le premier scénario figure en tant qu'exemple dans le Chapitre 5.

## F.1 Le scénario 2 : Four ouvert

Conditions initiales :

- Se déroule au laboratoire DOMUS.
- René et Jeanne sont présents.
- La cuisinière est fonctionnelle et verrouillée.
- StoveMAS est installé et fonctionnel sur la cuisinière.

Déroulement :

1) René s'identifie au système.
2) Il met le four à préchauffer à 425°F.
3) Il ouvre la porte du four.
4) Il va aller chercher une pizza et la poser sur le comptoir.
5) Il va aller à la porte d'entrée de l'appartement pour discuter avec Jeanne pendant au moins 20 secondes (sans avoir mis la pizza au four et fermé la porte).

6) Il revient et ferme la porte du four.

Résultat attendu :

Le système observe l'oubli de fermer la porte du four allumé. Ce cas de figure présente un danger d'une part parce que les éléments chauffants du four sont atteignables pour une personne, d'autre part la porte ouverte du four est un risque potentiel de basculement du four si une personne ou un animal appuie dessus. Le système notifie René au bout de 10 secondes et indique l'erreur. René en prend connaissance et corrige son oubli en fermant la porte. Le système revient alors en fonctionnement nominal.

Variables d'observation :

Dans ce scénario, on observe l'activité enregistrée par l'agent *DAOven* en affichant les détails de cet agent via l'interface de contrôle. Cet agent doit détecter l'activité du four via l'activité électrique et la température qui augmente. Il doit également détecter que la porte du four est restée ouverte par le biais du capteur de contact. L'agent *Rule2* (Tableau 6) reçoit les informations transmises par *DAOven* et observe un danger. Pour vérifier que l'agent *Rule2* réagit correctement, on peut observer l'envoi de la notification sur la console d'exécution. Lorsque René corrige son erreur, *DAOven* détecte la fermeture de la porte et *Rule2* ne doit plus observer de danger. On peut observer que la notification cesse de paraitre sur la console d'exécution et que l'agent *Rule2* s'est remis en fonctionnement nominal. Les délais pour la notification et le verrouillage de l'appareil peuvent être vérifiés avec les paramètres de l'agent *Rule2* et du profil utilisateur de René.

## F.2 Le scénario 3 : Préparation d'un œuf

Conditions initiales :

- Se déroule au laboratoire DOMUS.
- René et Jeanne sont présents.
- La cuisinière est fonctionnelle et verrouillée.
- StoveMAS est installé et fonctionnel sur la cuisinière.
- Une tablette tactile Asus Nexus 7 est disponible avec l'application Android_StoveMAS installée et configuré pour se connecter à StoveMAS.

Déroulement :

1) Jeanne s'identifie au système avec un tag RFID.
2) René s'identifie au système via la tablette tactile.
3) René remplit une casserole d'eau et la place sur le rond avant gauche de la cuisinière.
4) René active le deuxième bouton en partant de la gauche de la cuisinière.
5) René et Jeanne discutent à propos de l'activité de la soirée qu'ils ont prévue.

Résultat attendu :

Le bouton activé ne correspond pas au rond sur lequel la casserole d'eau a été placée, le système doit observer une présence sur le rond avant gauche mais une activité sur le rond arrière gauche. Ce scénario est identique au scénario 1, mise à part l'identification de Jeanne, cette identification induit une modification des règles de sécurité. Une notification doit être transmise à René et Jeanne au bout de 30 secondes et indique l'erreur. Si René et Jeanne

ignorent la notification, le système verrouille les équipements au bout de 30 secondes supplémentaires. Ces notifications doivent également apparaitre sur la tablette tactile utilisée par René. Les capteurs embarqués de la tablette tactile améliorent la connaissance du système.

Variables d'observation :

L'observation se fait de la même manière que pour le scénario 1. L'observation du profil résultant retenu par le système se fait en activant l'affichage des informations du *UserAgent* via l'interface de contrôle. Ainsi, le profil résultant s'affichera dans la console d'exécution après la connexion des deux personas. L'affichage des notifications sur la tablette tactile validera et l'affichage des données des capteurs sur la console d'exécution de StoveMAS indiquera le fonctionnement des équipements mobiles dans le système.

## F.3 Le scénario 4 : Réchauffer un plat

Conditions initiales :

- Se déroule au laboratoire Lab-STICC.
- Seul René est présent.
- Les équipements sont fonctionnels et verrouillés.
- StoveMAS est installé et fonctionnel.

Déroulement :

1) René s'identifie au système.
2) Il prend un plat dans le frigidaire.
3) Il fait chauffer le plat dans le four à micro-ondes à 900W pendant une minute.
4) Il enlève le plat chaud du four à micro-ondes et se met à table.

Résultat attendu :
Ce scénario permet d'étudier le fonctionnement des capteurs lors de l'utilisation d'un équipement. StoveMAS doit fonctionner correctement et n'émettre aucune notification.

Variables d'observation :
L'observation se fait via l'étude des données capteurs issues de ce scénario. Ces données sont disponibles en enregistrant les logs de données à l'issue du scénario. L'étude de l'évolution des données des capteurs permet d'affiner le comportement des *DeviceAgents*.

## F.4 Le scénario 5 : Réchauffer un plat, variante

Conditions initiales :

- Se déroule au laboratoire Lab-STICC.
- Seul René est présent.
- Les équipements sont fonctionnels et verrouillés.
- StoveMAS est installé et fonctionnel.

Déroulement :

1) René s'identifie au système.

2) Il prend un plat dans le frigidaire.

3) Il fait chauffer le plat dans le four à micro-ondes à 900W pendant une minute.

4) Une erreur au sein du système se présente.

4.1) Un agent d'acquisition plante.

4.2) Un *RiskAgent* plante.

4.3) Un *DeviceAgent* plante.

4.4) Le *SystemAgent* plante.

4.5) Un capteur en redondance se déconnecte.

4.6) La connexion entre l'ordinateur et l'acquisition est rompue.

4.7) La tablette perd la connexion avec le système (Appareil éteint).

Résultat attendu :

Ce scénario permet d'étudier le fonctionnement du système vis-à-vis des pannes qui peuvent surgir. Dans les 3 premiers cas, le système doit reconnaitre que l'agent a planté via l'agent *SystemAgent*. Ce dernier essaye de relancer l'agent planté. Dans le cas échéant, (4.1 et 4.3) le système verrouille les équipements par mesure de sécurité et envoie une notification aux utilisateurs. (4.2) Le système se met en mode dégradé et notifie l'utilisateur. (4.4) Le système se verrouille automatiquement via le *WatchdogAgent*. (4.5) Le *DeviceAgent* qui s'occupe de ce capteur détecte une incohérence dans la lecture d'un des capteurs en redondance et notifie. (4.6) Les relais ne sont plus armés par le système et les équipements se verrouilleront automatiquement (relais normalement ouverts). (4.7) Les capteurs embarqués s'arrêteront de se mettre à jour dans StoveMAS, les notifications et alertes continuent à être affichées sur la console d'exécution.

Variables d'observation :

Pour les cas (4.1) à (4.4), l'interface des agents permet de tuer un agent au choix au moment voulu, permettant de générer la panne. On peut, via cette même interface, constater directement la disparition de l'agent en question. Ensuite, dans la console d'exécution les messages du *SystemAgent* seront visibles indiquant l'état et l'avancement dans la relance des agents. Dans le cas (4.4), aucun message ne sera affiché sur la console d'exécution, seulement un message de verrouillage de la part du *WatchdogAgent*. Lorsqu'un capteur en redondance se déconnecte (manipulation à faire par une personne compétente), il est possible de relever les données d'historique de ces capteurs via l'interface de contrôle et de constater l'activité du *DeviceAgent* en question à ce même moment. Lorsque la connexion entre l'ordinateur et le boitier d'acquisition est rompue (4.6), aucune donnée de capteur ne se rend jusqu'au système. Par conséquent, on peut constater une absence de données dans la console d'exécution. Il faudra alors constater le verrouillage de l'équipement en essayant de l'utiliser (en vain). Enfin, si la tablette perd la connexion avec le système (4.7), les données des capteurs embarqués ne sont

plus mises à jour dans StoveMAS, ce résultat peut être observé en regardant les logs de données des capteurs embarqués. StoveMAS continuera à fonctionner correctement sans les données de capteurs embarqués.