

## CHIST-ERA Proposal Template

Project Acronym

**SUCCESS**

Project Title

**SecUre aCCESSibility for the internet of things**

Addressed Call Topic (SPTIoT<sup>1</sup> or TMCS<sup>2</sup>):

**SPTIoT**

Coordinator contact point for the proposal

Name	Florian Kammüller
Institution/Department	Middlesex University – School of Science and Technology
Address	Hendon Campus – London
Country	UK
Phone	+447826293578
Fax	
E-mail	f.kammuller@mdx.ac.uk

Partners' people involved in the realisation of the project<sup>3</sup>

Partner Number	Country	Institution/Department	Name of the Principal Investigator (PI) <sup>3</sup>	Name of the co-Investigators <sup>4</sup>	Name of the other personnel participating in the project <sup>5</sup>
<b>1</b> Coordinator	UK	Middlesex University London – School of Science and Technology	Dr Florian Kammüller	Prof Juan Carlos Augusto	Prof R. Bayford Dr S. Jones Dr T. Chen Research Assistant (Ph.D.)
<b>2</b>	France	INRIA	Dr Axel Legay	Dr A. Cohen	Research Assistant (Ph.D.)
<b>3</b>	France	UGA - VERIMAG	Prof Saddek Bensalem	Dr M. Bozga	Research Assistant (Ph.D.)
<b>4</b>	Netherlands	U TWENTE	Prof Mariëlle Stoelinga	...	Research Assistant (Ph.D.)

<sup>1</sup> User-Centric Security, Trust and Privacy in the Internet of Things

<sup>2</sup> ~~Terahertz Band for Next-Generation Mobile Communication Systems~~

<sup>3</sup> The Principal Investigator (PI) is the point of contact of the partner for the corresponding National Funding Organisation.

<sup>4</sup> A co-investigator is a known scientist and/or group leader making a substantial contribution to the project

<sup>5</sup> If the name is for the moment unknown, specify the level of expertise sought (PhD, post-doc, engineer, professor...).



Duration: 36 months

**Summary of the project<sup>4</sup>** (*publishable abstract, max. 1/2 page*):

The IoT has a great potential to provide novel services to humans in critical areas for society. This innovation however requires updating our understanding of the risks associated with the new technology so that we can deploy it with confidence and society can trust it. Amongst the biggest problems for this vision to become a reality are security flaws due to technical restrictions, immaturity of software applications, intrusion threats through new challenges in complex usage scenarios, and mainly a lack of transparency. The IoT could become human centric computing that serves our society, but simultaneously amongst the main triggers for security problems is human behaviour, either unintentionally or maliciously. The core idea of SUCCESS is to use methods and tools with a proven track record to provide more transparency of security risks for people in given IoT scenarios. Our core scientific innovation will consist on the extension of well-known industry-strength methods in our priority areas. Our technological innovation will provide adequate tools to address risk assessment and adaptivity within IoT in healthcare environments and an open source repository to foster future reuse, extension and progress in this area. Our project will validate the scientific and technological innovation through pilots, one of which will be in collaboration with a hospital and will allow all stakeholders (e.g. physicians, hospital technicians, patients and relatives) to enjoy a safer system capable to appropriately handle highly sensitive information on vulnerable people while making security and privacy risks understandable and secure solutions accessible. This innovation will be achieved by a multi-disciplinary team of recognized experts in their fields which has significant experience in knowledge transfer to and from society. SUCCESS will have significant impact, strengthening the interdisciplinary approach to this important challenge at the crossroads between society and technology, creating new methods for increased security in healthcare, supporting the use of these robust methods by adequate open-source tools, and educating on the use of our products through real-life working prototypes.

**Relevance to the topic addressed in the call<sup>5</sup>** (*in particular specify here which part of the call text is concerned by your project, max. 1/2 page*):

Our team crosses boundaries between disciplines applying techniques from *hardware and software, user behaviour and human-computer interaction* applying them to a research pilot from the healthcare sector on supporting IoT monitoring techniques for patients that are human understandable and can be certified by automated techniques.

The research challenges we specifically target are  
*Dynamic security to allow systems to adapt to varying users and*  
*Empowering users with risk evaluation tool for their data and contacts.*

Our proposal also aims to have impact in the areas  
*Data visualisation for increasing user awareness of privacy issues and*  
*Assistive technology/techniques to encourage more secure behaviour and awareness of users.*

Florian KammueLLer 12/14/15 12:14 PM

**Comment [1]:** Deleted IoT definition „The Internet of Things (IoT) denotes the combination of physical objects with a virtual representation in the Internet. It consists not only of human participants but “Things” as well.“

Florian KammueLLer 12/4/15 1:34 PM

**Comment [2]:** Changed from „, to provide a more holistic consideration of security in relation to human factors within IoT“

Florian KammueLLer 12/4/15 1:49 PM

**Comment [3]:** Deleted „We also look at aspects of but only to the extent which they contribute to our two priority areas of concern.“

Florian KammueLLer 12/4/15 1:55 PM

**Comment [4]:** Replaced „trustworthiness“

Florian KammueLLer 12/4/15 2:00 PM

**Comment [5]:** New

<sup>4</sup> Be precise and concise. This summary will be used to select suited reviewers for the proposal.

<sup>5</sup> Be precise and concise. Relevance to the topic addressed in the call is an evaluation criterion.



## Detailed project information

### 1. S/T Quality

#### 1.1 Objectives of the project

The IoT enables using smart devices, like smart-watches, smart wristbands, and smartphones, to provide cost-effective services for humans, for example, for low-cost monitoring schemes in the health-care sector to provide early diagnosis of diseases.

From a security and privacy perspective, at this point the IoT could be described as a hopeless case since all prevention aspects of security (confidentiality, integrity, and availability) are inherently weak and unwanted tracking and monitoring throws the doors wide open to privacy attacks. To provide secure IoT solutions, modeling and analysis needs to be integrated in the planning and validation of application scenarios and smart-device architectures to address burning security issues like unintentional or intentional insider attacks. The more so, we need to look at how to represent humans and the ways they interact with systems, and make security risks understandable for humans and secure IoT solutions accessible.

Security assessment of IoT architectures that integrate human behaviour require advanced scientific methods and techniques in security, verification, component based software engineering, embedded system design and certification. The challenge lies in a secure and yet flexible combination of

- specification and verification techniques for secure IoT components and their composition,
- verification methods and risk assessment techniques for IoT scenarios with models of human behaviour, social interactions and human-system interactions,
- implementation and modeling languages with algorithms for the certification of safety, availability, secrecy, and trustworthiness across from the model to the platform.

To further develop existing advanced scientific methods and simultaneously show that they can be combined into feasible solutions, we need to rely on realistic scenarios and tools from the application domain.

SUCCESS has the following scientific and technological objectives:

**(S1)** to provide logical specification and analysis methods for organisational security and integrate them with risk and fault tree analysis,

**(S2)** to extend quantitative attack tree analysis and decentralized access control for IoT component systems by generalizing security models to include smart devices,

**(T1)** to design and prototypically implement certification methodology for IoT component frameworks,

**(T2)** to build and test the dynamic security of an IoT pilot scenario from the healthcare sector of a sensor based monitoring architecture for dementia patients with security critical data and actions.

SUCCESS extends the successful methods of fault tree analysis, attack tree modelling and quantitative analysis, and the Behaviour, Interaction, Priority (BIP) method to support secure IoT systems. The extension enables the transparent and dynamic risk assessment of IoT security architectures, i.e., it addresses the necessities and potential risks involved in an IoT environment for healthcare specifying when and where to apply security controls in an understandable and certified way. Stakeholders in this pilot are physicians, hospital technicians, patients and relatives.

#### 1.2 State of the art and expected progress beyond state of the art

(max. 2 pages)

Florian Kammueeller 11/25/15 2:37 PM

**Comment [6]:** The original instructions (deleted from form to save space):

**General recommendation:**

1. The same font and style should be used for the whole proposal (Arial, 11pt, single spaced).
2. Please complete all sections.
3. Please adhere to the given page limits.
4. For the evaluation criteria, please refer to the call announcement. Your proposal should include all details required.

Florian Kammueeller 11/25/15 2:36 PM

**Comment [7]:** The original instructions (deleted from form for space):

"(max. 1 page)

Describe the context, objectives and expected results. They should be clear, measurable, realistic and achievable within the duration of the project."

Florian Kammueeller 12/16/15 11:24 AM

**Comment [8]:** I rephrased/rewrote that whole paragraph towards IoT and new goals

Florian Kammueeller 12/5/15 6:25 PM

**Comment [9]:** Added „risk assessment“

Florian Kammueeller 12/5/15 6:18 PM

**Comment [10]:** Changed from synthesis to certification

Florian Kammueeller 12/16/15 11:23 AM

**Comment [11]:** Main change:

- Introduced fault trees and attack trees
- Extension of BIP not to human components but rather readymade smart devices for IoT

Florian Kammueeller 12/15/15 4:52 PM

**Comment [12]:** Added for the sake of IoT

Florian Kammueeller 12/5/15 6:30 PM

**Comment [13]:** Replaced „synthesis“ by certification

Florian Kammueeller 12/16/15 11:21 AM

**Comment [14]:** Replaced „change management“ because it is no longer a priority of the call.

Florian Kammueeller 12/5/15 9:08 PM

**Comment [15]:** Tweaked the whole paragraph from producing one verified reproducible security architecture to „risk assessment and certification of IoT architectures in an understandable way“

Florian Kammueeller 12/6/15 3:00 PM

**Comment [16]:** Leave this for now, needs to be updated later.



*Describe background, state of the art and expected progress beyond state of the art. Quantitative information must be provided and your answer should refer to the objectives, concepts involved, issues and problems to be addressed, and approaches and methods to be used.*

### 1.3 Scientific description of the project and research method

We propose a combination of successful techniques of security analysis and component specification and verification to provide accessible security for IoT. Starting from a model that integrates human behaviour with an infrastructure, we apply fault tree analysis to produce attack vectors. Using formal models of the security policy, the attack trees can identify security properties for a transparent explanation for the user and for verification. The resulting formal specification is the basis for certifying that a given IoT scenario represents a secure component architecture for IoT. We will extend the BIP methodology and techniques for automated construction of component architectures to make them amenable to support the certification of these IoT architectures that are flexibly composed from off-the-shelf components to guarantee the user-transparent security specification. The case study is a hospital room equipped with sensors for monitoring dementia patients, personnel and network-connected IoT devices running other IoT service components. The IoT sensor network recognises and monitors humans. Humans are physical entities but may also carry IoT devices (smart phones and watches) that communicate with the IoT sensor network. This scenario is going to be installed by MU and deployed for testing in Homerton University Hospital, London. In each layer of secure IoT system assessment, *SUCCESS* picks up scientific challenges from human centric IoT system modelling using fault tree analysis, attack tree modelling and quantitative analysis, and extending component based certification by integrating the human factor into the BIP technology.

**A. Organisational security:** security must be integrated at system analysis and design time. Security engineering (1-3) starts with quantification of the attacker and security requirements elicitation. Modeling human behaviour, infrastructure, and security policy in Isabelle/HOL (4-6) leads to security properties, access control policies, and allows high level verification to exhibit attack vectors. Results are use cases, attack trees and logically specified security properties as requirements specification for an IoT application design. As a **novelty** we enable that human behaviour and security can be expressed within IoT application designs. *The extensions 4, 5 and 6 allow the integration of humans into IoT models and support the risk analysis:* 1. Security policies (what users can do, how to treat data). 2. Identification of protection goals (confidentiality, integrity, availability, accountability). 3. Invalidation of security policy to identify attacks 4. Fault tree analysis to identify attack vectors 5. Formal modelling of agent/actor within an infrastructure with the Isabelle Insider framework. 6. Isabelle attack trees to refine attack vectors.

**B. Risk assessment and Accessibility for IoT scenarios:** to incorporate security requirements into an IoT architecture, the security specification from **A.** is transformed into an accessible security specification analysing probable risks and defining suitable access control (1,2). Data security and action security model and security verification are already partially available in BIP. As a **novelty** for secure IoT certification we include quantitative attack tree analysis for access control of IoT components (smart devices): 1. Quantitative attack tree analysis to evaluate the risks and produce a transparent visualisable security and privacy risk output for users. 2. Define access control (decentralized security classes for actors and data). 3. Security extended BIP (SecureBIP, Ben Salem et al 2014) already has decentralized access control model: add security classes for new IoT abstract components. 4. Verification of access control: use information flow control of SecureBIP to check access control on the BIP IoT model.

**C. Certification of secure IoT architectures:** certification of secure IoT scenarios necessitates mapping them to existing atomic components, like a small OS for network nodes and sensors (2), and integrating them into networked IoT scenarios (1). Our **novelty** is to extend the BIP to integrate smart devices. *Secure construction (3-4) lead to augmented certification and verification techniques (5). We explore scenarios in our human centric*

Florian Kammueßer 12/5/15 6:45 PM

**Comment [17]:** Requirements from form: (max. 3 pages)

*Description of the project, highlighting the novelty and originality of the approach, especially regarding novel ICT disciplines and future challenges (FET principles). Describe the scientific and technological methodology envisaged and how you will assess progress towards the objectives.*

Florian Kammueßer 12/5/15 6:57 PM

**Comment [18]:** At this point we need to integrate fault tree analysis and attack trees of Marielle.

*healthcare sensor network pilot enabling the assessment of progress made (6-8):* Build secure IoT systems by adding security components and extensions to IoT. For example, authentication protocols for access to network, encryption of data and communication, implementation on security extended operating systems, but also better interfaces facilitating usability or monitoring components to observe insider attackers. Verification of atomic BIP components for security (e.g., TinyOS, Basu2007) already possible with current BIP concepts for security. 3. Extend BIP component methods for sound-and-safe-by-construction to security properties. 4. Dynamic security: preservation of security properties by adding smart components to existing BIP IoT system. 5. Verification methods for certified IoT architectures, i.e., what auxiliary assumptions are necessary (and can be verified) on composed system. 6. **Scenario:** smart device, e.g. for self-tracking, comes into the range of a network; the resulting security risks need to be identified and quantitatively analysed, the extended attack tree and BIP methodology should be able to express these risks and re-verify security properties 7. **Scenario:** human behaviour changes: how dynamic is the quantitative security policy, what are boundaries to distinguish between technical glitches, unintentional or malicious behaviour? Figure 2 summarizes the proposed extended framework. It shows how the scientific and technological objectives and its associated advances to the state of the art are all feasible within the methods we have selected. Furthermore the table below provides details on how the progress towards the scientific and technological objectives is assessed. This provides a harmonic and coherent strategy which is at the core of our scientific approach.

**Pilot for Dementia patients:** What is already known about the problem that our project will address: Dementia is a common condition that affects about 800,000 people in the UK. Our focus is on Alzheimer's disease, the most common form of dementia with an estimated 37 million sufferers worldwide and expected to affect 115 million by 2050 (World Health Organization). The global cost is estimated to be over \$600 billion at present. However, Alzheimer's Disease is under-reported on death certificates, which often list the immediate cause of death, such as pneumonia, rather than the underlying cause. The risk of developing the disease increases with age and it usually occurs in people over the age of 65. It is a syndrome associated with an ongoing decline of the brain and its abilities. Due to the inability to diagnose the patient at an early stage of the disease or monitor its progression, drugs are given to the patient at a late stage. Current diagnosis of Alzheimer's can only be used to monitor progression and treatment of Alzheimer's in patients; they cannot predict the disease. Furthermore, neuroimaging techniques are only available in some hospitals and some patients are not able to undergo this technique. These tests may not always identify the condition in the early stages so that new approaches for early, specific recognition of Alzheimer's disease at the prodromal stages are of crucial importance. There is a clear need to produce an objective testing and monitoring method which is reliable and cost-effective, so that we are able to intervene to minimize the effect of Alzheimer's. This project will aim to produce a new low cost bioassay (investigative procedure in laboratory medicine) using multiple biosensors, each sensor will be tailored to identify a specific bio marker, which can be used in the home based on an array of electrical biosensors to provide objective data of the progression and possible causes of the Alzheimer's (Figure 2). Compared with other assays, biosensors offer the key advantages of low-cost, small size and ease of operation but create security and privacy issues for patients.

#### Assessment of progress towards scientific and technological objectives

Objectives (Section1.1)	Progress assessed in:
<b>S1</b>	<b>A.4-6:</b> security risks can be identified for given IoT scenarios
<b>S2</b>	<b>B.1 &amp; B.3-4 &amp; C.3-4:</b> attacks can be analysed for IoT and made transparent for humans; definition of security properties for IoT components
<b>T1</b>	<b>C.6-7:</b> IoT pilot can be modelled and analysed with extended methodology
<b>T2</b>	<b>Pilot:</b> works, is accepted by users, certification according to needs is possible while security properties are proved

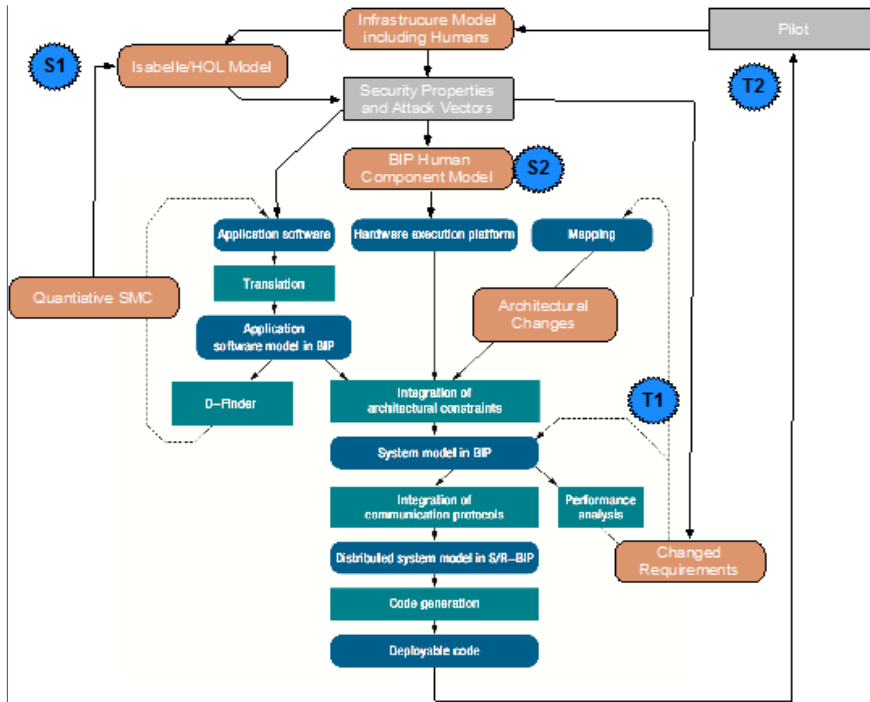


Figure 1. Illustration of workflow of the extended BIP method

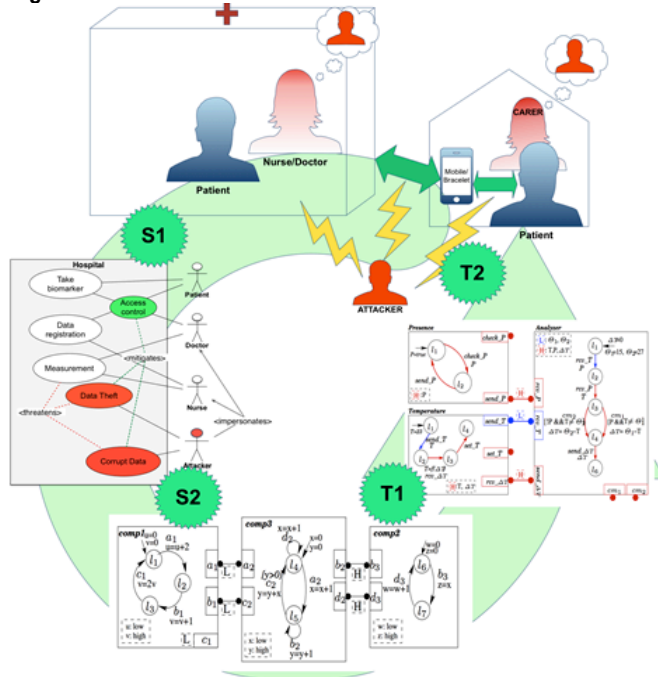


Figure 2. SUCCESS Pilot and Security architecture with Objectives S1-T2

Florian Kammüller 12/16/15 11:45 AM

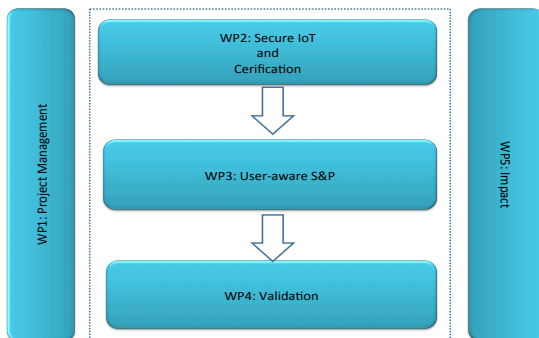
**Comment [19]:** Both illustrations need to be updated.



## 2. Implementation

### 2.1 Work plan

The SUCCESS workplan is simple and efficient, we design and implement our innovation in WP2 guided by stakeholders, we have a specific WP where the core scientific advances are produced and one WP focused on validation. We have also a WP focused on Impact. See **Figure 2** below.



WP1 (Management) will look after all aspects of running the project, making sure the project is a success for the stakeholders, for CHIST-ERA and for the partners of the consortium. This involves looking after administrative, technical, and communicative aspects of our SUCCESS project. This WP will be led by Middlesex University, a partner with extensive experience in developing innovation in the IoT area, and on participating of and coordinating projects.

WP2 (Secure IoT and Certification) will be the 'drawing board' for the whole consortium to inform the best way to materialize the proposed solution with input from the external stakeholders and internal experts. Continuing the analysis we have performed during proposal writing and complemented with strategic meetings we will be continuously assessing and revising our priorities to maximize the results and impact. Implementation of tools and core functions will also be achieved here. This WP will be led by Université Grenoble Alpes (UGA) who are recognized experts in the design of this type of systems.

WP3 (User-aware S&P) will produce the core of the scientific innovation. We will advance the state of the art in all four areas of interest by this call but with a strong emphasis on: Security and Human Aspects. The WP will be led by INRIA who has expertise in all these core technical areas and on their applications to innovation in industry.

WP4 (Validation) will exercise the platform and services developed at all stages of the project. This will include the building of the technological platform and the development of two types of prototypes: one in a lab and one for a real healthcare setting. This WP will be led by MU whose area of expertise is precisely the development of IoT architectures as part of real-life applications.

WP5 (Impact) will make sure the expected impact is achieved so that the results of the project are useful for the various stakeholders. This WP will be led by University of Twente (UT) with extensive experience on dissemination and exploitation activities through their continuous engagement with industry.

The following Gantt chart show how the activities of these WPs are scheduled in time.

Florian Kammüller 12/5/15 8:45 PM

**Comment [20]:** Proposal requirements:"  
(max. 2 pages)

*Provide a general overview of the work plan and a timing of the different work packages and their components (Gantt chart or similar) and a graphical presentation of the components showing how they inter-relate (Pert chart or similar).*

Year	YEAR 1 (Oct. 2015 - Sep. 2016)												YEAR 2 (Oct. 2016 - Sep. 2017)												YEAR 3 (Oct. 2017 - Sep. 2018)																									
	Month												Month												Month																									
Month Number (relative to project start)	O	N	D	J	F	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S		
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36														
WP1: Management	K												S																																					
Task 1.1: Communication																																																		
Task 1.2: Reporting																																																		
Task 1.3: Research quality assurance																																																		
Task 1.4: Finance and Legal aspects																																																		
WP2: System Design and Implementation																																																		
Task 2.1: Security requirements for CPS with human factors							A1						S2																																					
Task 2.2: Use case requirements																																																		
Task 2.3: Abstract model configuration with human factors																																																		
Task 2.4: Platform-independent tools to support																																																		
Task 2.5: Platform-dependent implementation with human factors																																																		
WP3: Resilience																																																		
Task 3.1: Information Confidentiality																																																		
Task 3.2: Security																																																		
Task 3.3: Change management																																																		
Task 3.4: Human factor																																																		
WP4: Validation																																																		
Task 4.1: CPS infrastructure																																																		
Task 4.2: Pilot 1																																																		
Task 4.3: Pilot 2																																																		
Task 4.4: Ethics Assurance																																																		
WP5: Impact																																																		
Task 5.1: Dissemination & Knowledge Transfer																																																		
Task 5.2: Exploitation Strategy																																																		
Main events during life-time of the project:																																																		

Main events during life-time of the project:

K: Kick-off meeting  
T: technical meeting with Steering Committee and Advisory Committee  
C: review meeting with CHIST-ERA  
A: Academic Workshop

S: Stakeholders Workshop  
P: Pilot active  
W: webpage  
E: exploitation plans

Our project will be done iteratively along three years. The first year will help to further specify the requirements of the system from the proposal submission stage, we will prepare a significant part of the basic infrastructure, including the first approaches to solutions for the conceptual challenges, the tools which will facilitate design and implementation in the next stages, and the equipment for the pilots. We will also start work in the fundamental science which will produce the advances to the state of the art. By the second year we will deploy the first pilot and will use it as a testing platform adding and refining the system through several versions. This pilot will remain always operational and will be a development testbed. Some of the most expensive data (biomarkers) will be fed directly from files of volunteers giving consent to share the data. The third year will see this escalated to the real-life scenario in a hospital in London. We will continue refining our strategies and increasing the quality of the impact requiring at this stage that all stakeholders perceive we are improving their experience of the security aspects of the system as a result of our innovation. This pilot in the healthcare service will not run continuously as the one set up at the university. Given we will interact with real patients we will run three one month long deployments. They will be based on a mix of data collected from different sensors: patients' activities in daily life and biomarkers collected in the hospital.

Other activities like dissemination and exploitation are permanent. We want to highlight our plans to engage with different stakeholders through several strategic workshops which will allow the system to be co-designed and foster exploitation.

Florian Kammueeller 12/6/15 2:33 PM  
Comment [21]: Attention: is not yet updated!



## 2.2 Work packages

WP 1		Management				Start: M1		End: M36	
Contribution of project partners									
Partner number		1	2	3	4				
Total effort per partner (Person*months)		4	1	1	1				
Aim of the WP: overall this WP takes care of administrative and strategic side of the project and it makes sure the deliverables are produced in good time and form and milestones are achieved as expected. It materializes and monitors several executive actions, including the distribution of the joint budget, compilation of reports, and cost statements for submission to the CHIST-ERA office, development of strategies and long-term project plans, chairing the Steering Committee and follow-up of their decisions, transfer of documents and information connected with our SUCCESS project to and between the partners concerned, ensuring that the exploitation strategy is achieved, coordination of the entry and exit of partners from the consortium, ensuring that work complies with national and EU Health and Safety regulations and Ethical Guidelines.									
Tasks									
T1.1		Communication (M1-M36; responsible: 1-MU) Provision of a project office with appropriate records and communications to support the management of the project and interaction between the partners. This task will be implemented under the responsibility of MU to keep all partners, the advisory committee and the EC informed at all times.							
T1.2		Reporting (M1-M36; responsible: 1-MU; involved: all partners) Monitoring progress of deliverables through the operation of the Steering committee and its two subgroups. In particular to conduct regular reviews of progress and to report to the Commission as appropriate. This task will be led by MU however all partners are expected to actively and permanently engage with it.							
T1.3		Research quality assurance (M1-M36; responsible: 1-MU) Monitoring quality of deliverables (technical infrastructure used and produced, software and services). Making sure requirements and outcomes are clear and match each other. Predicting and avoiding risks and deviations. This task will be led by MU however all partners are expected to actively and permanently engage with it.							
T1.4		Finances and Legal aspects (M1-M36; responsible: 1-MU) Provision of financial and legal management support to the project. Financial management will be carried out including the preparation of annual cost reports and the administration of payments according to the budget. Resource allocation will be monitored to ensure that activities remain within budget and transparency is achieved at all times. Other aspects included are: Consortium Agreement, contract amendments and audits. This task will be implemented under the responsibility of MU with support from its experienced Research and Knowledge Transfer Office.							
Deliverable	Month of delivery	Title of deliverable							
D1.1	M1	Consortium Agreement							
D1.2	M1	Webpage and platform for documents and software sharing							
D1.3	M1	Quality Assurance Plan							
D1.4	M12	First Project Management Review							
D1.5	M24	Second Project Management Review							
D1.6	M36	Third Project Management Review							

Florian Kammüller 12/5/15 8:57 PM

**Comment [22]:** Proposal requirement: „(max. 1 page per WP)

For the description of each work package, please use the template provided. Use as many templates as needed.

WP 2	Secure IoT and Certification				Start: M1	End: M36
Contribution of project partners						
Partner number	1	2	3	4		
Total effort per partner (Person*months)	7	3	20	8		
Aim of the WP: The goal of this work package is to develop a practical automated method for designing and certifying secure IoT systems using a model-based approach. Information flow security is established once on an abstract high-level model of the system. The abstract model is then further transformed into low-level IoT models and finally to distributed implementation including IoT devices, while preserving information flow security. This work package also includes the extension and creation of tools to support our development and the implementation of our innovative contributions from WP3.						
Tasks						
T2.1	Security requirements for IoT (M1–M30; responsible: 3-UGA; involved: all partners) The goal of this task is to find and specify the requirements which we have gathered so far. The requirements will provide the specific constraints and the problems that have to be solved in WP2, WP3 and WP4. The purpose is to formalize the security requirements and the context of the IoT scenario, covering the different architectural layers from applications design to the physical platform execution.					
T2.2	Use case requirements (M1–M30; responsible: 3-UGA; involved: 1-MU, 4-UT) Identification of the requirements which will drive and focus the scope of the analysis in WP3 and WP4. These requirements will be elicited to support the definition of the SUCCESS breakthrough methodology and associated tools against current methodology and best practice covering different design and implementation methods.					
T2.3	Abstract IoT model configuration (M1–M30; responsible: 3-UGA; involved: all partners) In this task we will use the existing BIP framework and its security extension SecureBIP as our underlying modelling language. We will work on the development and implementation of model transformations for automated decentralization and distributed implementation. These model transformations allow the transformation of high-level SecureBIP models with human behavior into IoT models while preserving information flow security. In this way, information flow security needs to be verified once, for the high-level model, and then it holds “by construction” on the distributed model and final implementation as an IoT system.					
T2.4	Platform-independent tools to support development (M1–M36; responsible: 3-UGA; involved: 1-MU, 4-UT) We will provide tools which help our team to develop and test our prototypes and also to support future development in this area. The outcome of this task will be open source code which can be reused by other researchers and developers to extend our framework and generate more innovation in this area. This will include special support to represent and track the relationship security-humans.					
T2.5	Platform-dependent implementation with human factors (M6–M36; responsible: 1-MU; involved: 2-INRIA, 3-UGA) Here we will consider a platform specific configuration where a system developer may select through a configuration file the security mechanisms to be used in generating secure code. Cryptographic methods are used to keep sensitive information confidential and guarantee integrity of exchanged messages between components. In this task we will generate automatically stand-alone processes for every abstract model configuration obtained by model transformation developed in T2.3.					
Deliverable	Month of delivery	Title of deliverable				
D2.1	M18	Design principles				
D2.2	M36	Tool set				
D2.3	M36	Final Prototype (partial prototypes delivered each year)				

Florian Kammüller 12/6/15 2:34 PM

**Comment [23]:** I've adapted this to the new IoT architecture design and certification idea rather than engineering and synthesis.

WP 3	User-aware S&P						Start: M1	End: M36
Contribution of project partners								
Partner number	1	2	3	4				
Total effort per partner (Person*months)	9	10	13	10				
Aim of the WP: We will build a taxonomy associated with the engineering and evolution of resilient IoT. It will anchor domain-specific elements from the healthcare pilots in WP4 within generic challenges, properties and requirements. The taxonomy will be based on quantitative and formal models, covering human behaviour and social interactions, environmental disturbances, secrecy, security and ethics. These models will first address the verification of single components, then be incrementally composed and integrated through the BIP extensions and tools defined in WP2. Four parallel tasks contribute to the design, integration and validation effort, aligned with the four elements of human-centric, secure IoT. Tasks report individually and through consolidated secure characterisations.								
Tasks								
T3.1	Information Confidentiality (M1 – M24: responsible: 2-INRIA; involved: 3-UGA, 4-UT) Formalizing confidentiality properties with an emphasis on transparency and human interaction, as captured by T2.1. Building on the existing model of SecureBIP, we will propose composition, model transformation for adaptation and certification methods to preserve information secrecy in T2.2.							
T3.2	Security (M1 – M24: responsible: 4-UT; involved: all partners) 2-INRIA, Formalizing security properties with an emphasis on security, adaptation, and the social context, as captured by T2.1. The existing model of SecureBIP will be enhanced with these perceptive properties before being applied to model transformations, verification and certification in T2.2.							
T3.3	Dynamic Security (M12 – M36: responsible: 2-INRIA; involved: 1-MU, 4-UT) IoT must adapt to a changing environment. BIP allows to model and certify runtime adaptation, but quantitative aspects of changing security requirements remain a challenge, especially in the context of governance changes, user-defined interaction, lifelong system evolution. We will also address the unobtrusive adaptation of mission-critical systems with heterogeneous components. The BIP model and flow will be updated to capture the quantitative evolution of IoT in time and its reactivity, from the model to the platform.							
T3.4	Human Factor (M1 – M36: responsible: 1-MU; involved: 2-INRIA, 3-UGA) A cross-cutting task involving all partners throughout the project, considering IoT-intrinsic as well as extrinsic (social, environmental) properties. These will include statistical and predictive interaction models, adoption, monitoring and maintenance, permanent risks (from infiltration and social engineering, through training and security awareness) as well as sporadic risks (attacks, theft). Data collection and validation take place in WP4.							
Deliverable	Month of delivery	Title of deliverable						
D3.1	M12	Formal and quantitative taxonomy of resilient IoT and human-IoT interactions						
D3.2	M24	Security certification and quantitative modeling of human-centric, secrecy and security properties						
D3.3	M36	Security certification and quantitative modeling of unobtrusive adaptation in human-IoT interactions						

Florian Kammüller 12/6/15 2:36 PM

**Comment [24]:** This is the only package where a title change might be meaningful. We could call it Security or Accessible Security or Dynamic S&P certification.

WP 4		Validation				Start: M1		End: M36	
Contribution of project partners									
Partner number		1	2	3	4				
Total effort per partner (Person*months)		9	4	5	3				
<b>Aim of the WP:</b> This work package will concentrate on the validation of the innovative concepts being developed in WP2 and WP3. This will involve all the processes required to materialize the pilots which will help to develop and revise the innovation we produce in our system. This work package includes two pilots of increasing complexity. These pilots are very important as they offer ways to more naturally discuss requirements with stakeholders and offer a specific context where we can more intuitively explain to potential future beneficiaries how the system works in practice. An important part of this work package activity will be the ethical considerations associated with the pilots.									
Tasks									
T4.1		<b>IoT infrastructure (M1-M36; responsible: 1-MU; involved: all partners)</b> This work package will lead the creation of the infrastructure which we need to run the pilots. Taking as an input the vision from Task 2.2, it will select, acquire and network the sensors and actuators. It will also have the responsibility to integrate this network with the software created in WP2 and WP3. Part of the software created in this task will be the interfaces which allow other partners from this project to remotely see, monitor and experiment with the system.							
T4.2		<b>Pilot 1 (M13-M36; responsible: 1-MU; involved: all partners)</b> This pilot will allow our team to build the system at early stages. For this reason it will be deployed in our university lab in London so that we can build and test the network and try different early versions of different components more easily. It will be based on role simulation and will be presented to the stakeholders of the second pilot so that when it is deployed at that stage it has higher chances of success.							
T4.3		<b>Pilot 2 (M25-M36; responsible: 1-MU; involved: all partners)</b> This pilot involves the deployment of the network in a real hospital setting (Homerton University Hospital, based in the east London Borough of Hackney). Our organization has had ongoing successful collaborations with this hospital and the hospital has explicitly manifested their interest in our project (see accompanying letter). Members of the MU team are currently developing one such collaborative project with the hospital focusing on early detection of Dementia signs. This project generates a wealth of sensitive information which has to be shared by different departments inside and outside the hospital and by people in very different roles (user, carers, healthcare staff, etc.). The more technical interactions with the hospital will take place across one year, with the system being fully functional 2-3 periods of approximately a month each, as we try different versions of the system and revise it with the different trials.							
T4.4		<b>Ethics Assurance (M1-M36; responsible: 1-MU)</b> Our pilots deal with sensitive data hence our team will take very seriously privacy, data integrity and ethics in general, applying the highest standards. All our SUCCESS teams are highly experienced in this. In particular, MU has a research group focused on Ethics in Computing and will coordinate all ethics-related actions. We have developed an ethical framework which has been specifically developed for Intelligent Environments and applied to an FP7 Inclusion project.							
Deliverable		Month of delivery		Title of deliverable					
D4.1		M24		Pilot 1 (software and documentation)					
D4.2		M36		Pilot 2 (software and documentation)					

WP 5		Impact						Start: M1	Start: M36
Contribution of project partners									
Partner number		1	2	3	4				
Total effort per partner (Person*months)		3	2	4	10				
Aim of the WP: This work package will aim at maximizing the visibility and impact of the SUCCESS project by raising awareness, especially within the EU, of the potential of adopting methods and tools that can reassure companies and consumers of the dependability of Intelligent Environments. This will include liaising with the CHIST-ERA office to agree on a plan that can maximize the visibility of the project, especially within the EU.									
Tasks									
T5.1		Dissemination & Knowledge Transfer (M1-M36; responsible: 1-MU; involved: all partners) This task will (1) raise awareness of the methods and tools developed through SUCCESS, (2) contribute to the scientific body of knowledge in the technical literature, (3) promote the project to relevant industry and business sectors to pave the way for market deployment, and (4) facilitate collaboration with related European initiatives. The project will achieve these objectives by: (a) participating in conferences and other relevant technical events (including annual and/or topical meetings organised by the Commission), (b) organising workshops, some of them in relevant conferences in the field, others with user groups and other strategic stakeholders, (c) disseminating the project results through demonstrations, interviews, videos, and participation in the media (social networks and traditional), (d) creating a web portal for the project which will explain the project and provide access to public documents, videos and other material, and (e) supporting an Open Source Repository which will provide all the material created by the project (including executables, tutorials and documentations).							
T5.2		Exploitation Strategy (M1-M36; responsible: 4-UT; involved: all partners) This task focuses on the exploitation of the project results and products by exploring different business models with the potential to promote the uptake of the methods and tools produced in SUCCESS and, in general, promote the increase of integration by similar initiatives. This will be accomplished through a properly developed exploitation plan, consistent with our IPR Plan. The exploitation plan will include an analysis of bottlenecks for adoption, economic consequences, and impact on the market. To this end our consortium will include in our Advisory Board a number of industry and EC representatives. All members of the consortium will actively participate in these activities with respect to their role, expertise and background.							
Deliverable	Month of delivery	Title of deliverable							
D5.1	M2	Project web-site (access to project information and progress)							
D5.2	M3	Initial Dissemination and Exploitation Plan							
D5.3	M12	Market Analysis							
D5.4	M36	Dissemination Report (Partial reports in months 12 and 24)							
D5.5	M36	Dissemination material (final material available for dissemination)							
D5.6	M36	Exploitation Plan (Initial Plan available at month 24)							
D5.7	M36	Open Source repository (contains: software/tutorials/ documents)							

As a summary, **Table 2** shows where the expected advances are generated.  
**Appendix C** provides additional WP tables with task distributions.

Florian Kammüller 12/6/15 2:40 PM

**Comment [25]:** Add updated table from previous proposal.

**Work package overview (total effort per WP and partner in person.months)**

Partner	WP1	WP2	WP3	WP4	WP5	Total
1-MU	4	7	9	9	3	32
2-INRIA	1	3	10	4	2	20
3-UGA	1	20	13	5	4	43
4-UT	1	8	10	3	10	32
Total	7	38	42	21	19	127



## 2.3 Management and Risk Assessment

### 2.3.1 Management Strategy

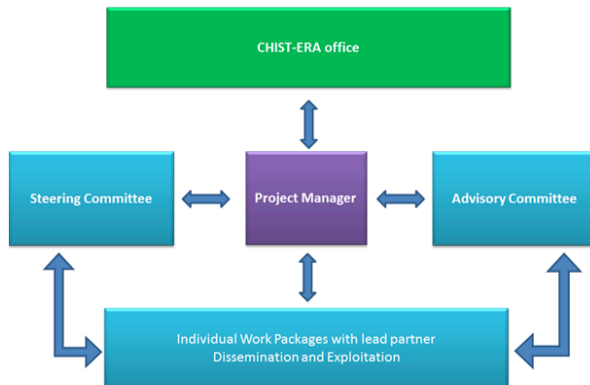


Table 2.3 a. Organizational Structure

Our Steering Committee is composed of one representative per partner, plus the ethics coordinator (Dr. S. Jones). The advisory committee will have experts in the four main technical areas (WP3) and also representatives of stakeholders. The Project Manager is responsible for risk management and contingency plans. The consortium will put in place procedures and work actively to reduce internal and external risks. See some examples in Appendix A.

#### List of milestones

Milestone	Delivery month	WP involved	Title
M1	1	1	(M1.1) Setting up and activating the project management structure
M2	6	2	(M2.1) Conceptual framework first draft
M3	12	1	(M1.2) Satisfactory completion of first project review with the Commission
M4	12	4	(M4.1) Basic IoT infrastructure operational
M5	12	5	(M5.1) Web page populated with initial design documents
M6	18	2	(M2.2) Detailed Conceptual framework first draft
M7	24	1	(M1.3) Satisfactory completion of Second project review with the Commission
M8	24	4	(M4.2) Successful Pilot 1
M9	24	5	(M5.2) Open Source Repository created
M10	36	1	(M1.4) Satisfactory completion of Third project review with the Commission
M11	36	2	(M2.3) Tool set fully functional
M12	36	2	(M2.4) Final prototype fully functional
M13	36	4	(M4.3) Successful Pilot 2
M14	36	5	(M5.3) Open Source Repository with final versions

Florian Kammueeller 12/6/15 2:38 PM

**Comment [26]:** Proposal spec: „(max. 1 page)

*Describe the organisational structure, the management structure and the decision-making including a list of milestones (template provided). A milestone is a major and visible achievement in the project. It should be SMART: Specific, Measurable, Attainable, Relevant, Time-bound.*

*Provide an assessment on the feasibility, and identification of possible risks and/or bottlenecks.”*


Juan Carlos Augusto 12/6/15 2:37 PM


**Comment [27]:** finalize


Juan Carlos Augusto 12/6/15 2:37 PM

**Comment [28]:** This table should take less space

## 1.4 Description of the Consortium

<b>Partner 1</b> (Project Coordinator)	<b>Organisation name / Department:</b>   <b>Middlesex University</b>  <b>Middlesex University London,</b> <b>School of Science and Technology</b>
<p><b>Expertise:</b> Middlesex University is a very dynamic emerging institution continuously growing its research expertise. Our Department of Computer Science is the 13<sup>th</sup> largest in size in the whole of the UK. This research project will be supported by the <i>Research Group on the Development of Intelligent Environments</i> (<a href="http://ie.cs.mdx.ac.uk/home/">http://ie.cs.mdx.ac.uk/home/</a>) with collaboration from the <i>Foundations of Computing Science Research Group</i>, the <i>Networks and Distributed Systems Laboratory</i> and the <i>Biophysics and Cancer lab</i>.</p> <p><b>Florian Kammüller</b>, holds a PhD from the University of Cambridge and a Habilitation from Technische Universität Berlin. He is an expert on applying formal techniques to security and software engineering. He has conducted various research projects with international collaborations exploring Security Engineering ranging from modelling of human behaviour over distributed active object programming to verifying secure protocols for the internet.</p> <p><b>Juan Carlos Augusto</b>, Head of the Research Group <i>Research Group on Development of Intelligent Environment</i>, has contributed 200+ publications, given more than a dozen invited talks and tutorials, chaired several conferences in the area and is Editor in Chief of one of its main journals. He participated in 14 research projects (P.I. for six of them), and advises the EU (including the ARTEMIS program for embedded systems) on a yearly basis as area expert and as external referee.</p> <p><b>Richard Bayford</b> is the Director of Biophysics at the Middlesex University Centre for Investigative Oncology, Professor of Bio-Modelling and Informatics and Honorary Senior Lecturer in the UCL Department of Electrical and Electronic Engineering. His expertise is in bio-modelling, tele-medical systems, instrumentation and biosensors. He is currently leading a research project on biosensors for detection of Alzheimer's.</p> <p><b>Simon Jones</b>, is a Senior Lecturer in the Department of Computer Science and an expert in ethical issues related to the use of computers in society. He led the creation of the eFRIEND ethical framework to guide development of Intelligent Environments (Jones et al 2015).</p> <p><b>Taolue Chen</b>, is a Senior Lecturer in the Department of Computer Science and an expert on quantitative model checking.</p> <ol style="list-style-type: none"> <li>1. F. Kammüller and C. W. Probst. Modeling and Verification of Insider Threats Using Logical Analysis. <i>IEEE Systems Journal</i>, <a href="#">Preprint online</a>, 2015.</li> <li>2. F. Kammüller, J. R. C. Nurse, and C. W. Probst. Attack Tree Analysis for Insider Threats on the IoT using Isabelle. <i>Human Computer Interaction International</i>, Invited paper, to appear in LNCS Springer, 2016.</li> <li>3. J. C. Augusto, and M. J. Hornos. Software Simulation and Verification to Increase the Reliability of Intelligent Environments, <i>Advances in Engineering Software</i>, Volume 58, Pages 18-34, April 2013, Elsevier.</li> <li>4. Diane J. Cook, Juan C. Augusto, and Vikramaditya R. Jakkula. Ambient Intelligence: applications in society and opportunities for AI. <i>Pervasive and Mobile Computing</i>. 5:277-298, 2009. Elsevier. Note: This is one of the highest cited papers on Ambient Intelligence.</li> <li>5. R. Bayford and A. Tizzard. Bioimpedance imaging: an overview of potential clinical applications. <i>Analyst</i>, 2012, 137, 4635-4643.</li> </ol>	
<p><b>Role in project:</b> We will manage the project (WP1) and also coordinate WP4 (including the deploying of the pilots), and coordinate ethics. We will also have important technical participation including on the design and implementation for WP2 and WP3 and on Impact (WP5).</p>	

Partner 2	<b>Organisation name / Department</b> <b>INRIA / ESTASYS and PARKAS</b> 
<p><b>Expertise:</b> ESTASYS is a team of Inria Rennes and Irisa Rennes. The team is leading research on Systems of Systems, variability management, and formal modelisation/validation via statistics. PARKAS is a joint team of INRIA and École Normale Supérieure (ENS) in Paris, the top-ranked University in France. It is leading research on data-flow and synchronous languages, synthesizable models of mixed-critical, multicore and distributed cyber physical systems.</p> <p><b>Axel Legay</b> is a permanent Research Scientist at Inria Rennes and a part-time Reader at Royal Holloway University of London. He received his PhD from the University of Liège (Belgium) in 2007 (awarded with the Belgian IBM prize in computer science). He has been a BAEF postdoc at Carnegie Melon (2008) and a visiting scholar at Urbana Champaign (2010). Axel was also invited professor at Aalborg University (2010) and research scholar at Oxford University (2006). He coauthored more than 170 papers in refereed journals and international conferences, and he is or has been the advisor for 3 PhD theses. He served as a PC or GC of major conferences including TACAS, FSE, DATE, and ASE.</p> <p><b>Albert Cohen</b> is a Senior Research Scientist at INRIA and part-time Associate Professor at École Polytechnique. He graduated from ENS Lyon and received a PhD from the University of Versailles in 1999 (awarded two national prizes). He has been a visiting scholar at the University of Illinois in 2000-2001 and an invited professor at Philips Research, Eindhoven in 2006-2007. He coauthored 110 papers in refereed journals and international conferences, and he is or has been the advisor for 22 PhD theses. He served as a PC or GC of major conferences including PLDI 2017, PPOPP 2015, DAC 2012-2014, CC 2014, HiPEAC 2012.</p> <ol style="list-style-type: none"> <li>1. Nouri, M. Bozga, A. Molnos, A. Legay and S. Bensalem. Building Faithful High-level Models and Performance Evaluation of Manycore Embedded Systems. In <i>MEMOCODE'14</i>.</li> <li>2. Fabrizio Biondi, Axel Legay, Pasquale Malacaria, Andrzej Wasowski: Quantifying Information Leakage of Randomized Protocols. In <i>VMCAI'13</i>.</li> <li>3. Kong et al. Compiler/run-time framework for dynamic data-flow parallelization of tiled programs. <i>ACM Transactions on Architecture and Code Optimization (TACO)</i>, 2014.</li> <li>4. Upadrasta et al. Sub-polyhedral scheduling using (Unit-)two-variable-per-inequality polyhedra. In ACM Symp. on <i>Principles of Programming Languages (POPL)</i>, January 2013.</li> <li>5. Cohen et al. Programming parallelism with futures in Lustre. In <i>ACM Conference on Embedded Software (EMSOFT)</i>, October 2012. Best paper award.</li> </ol>	
<p><b>Role in project:</b> Technical coordination of the project and Work package coordinator for WP3: Resilience. Also participation in various tasks from design to implementation.</p>	

<b>Partner 3</b>	<b>Organisation name / Department:</b>  <b>UGA-VERIMAG</b> 
<p><b>Expertise:</b> UGA-VERIMAG - Université Grenoble Alpes: UGA-VERIMAG is one of the main European labs in embedded systems. It develops theory, methods and tools for safety critical and embedded systems. It has been established in 1993. It is a research lab associated with the CNRS, Université Joseph Fourier, and the INPG Technical University. Currently, it has a total staff of 90 persons including 30 permanent researchers, 15 researchers under contract and 40 Ph.D. students. UGA-VERIMAG carries out research in the area of embedded systems design. It aims to produce theoretical and practical tools for the cost-effective development of embedded systems of guaranteed quality. Quality includes dependability properties such as security, safety, availability and performance.</p> <p>UGA-VERIMAG's results have given rise to transfer and to numerous contractual relations implying Verilog, Schneider Electric (nuclear plants), EADS for the development of safety critical systems in Airbus, Prover-Technology for a verification tool dedicated to Lustre, and Esterel-Technologies. Other industrial partners of UGA-VERIMAG are STMicroelectronics, Alcatel, CS-Transport, EDF, France Telecom, IBM, Intrasoftware, ISD, Leti/CEA, Prover Technology, RATP, Silicomp, Trusted Logic.</p> <p>UGA-VERIMAG has well-recognised competences in synchronous languages, validation and verification with focus on security and safety, modelling and temporal and hybrid systems analysis. It plays a significant role in real-time embedded systems. UGA-VERIMAG has been and is currently involved in many European projects: LTR VIRE (Verification of Real time systems), IST Crisys, IST Interval, IST SafeAir I &amp; II (Advanced Design Tools for Aircraft Systems and Airborne Software) and Agedis IST Next-TTA (01-03), RISE, AMETIST, ASSERT, SPEEDS, PRO3D, CERTAINTY, D-MILS, ASCENS, SMECY, CyPhERS, and ACROSS. VERIMAG coordinated the projects OMEGA (Correct Development of Real-Time Embedded Systems) CC, COMBEST. VERIMAG coordinated the IST-004527 ARTIST2 NoE on Embedded Systems (<a href="http://www.artist-embedded.org">http://www.artist-embedded.org</a>). The NoE includes 35 partners representing the top research teams in embedded systems design.</p> <p><b>Prof Saddek Bensalem</b> is Professor in Computer Science. His research is centered around the design of computer systems, notably embedded systems, with emphasis on the formalization of design processes and techniques that ensure correction by construction.</p> <p><b>Dr Marius Bozga</b> is research at VERIMAG laboratory. He has conducted research and tool development for modelling and verification of distributed real-time systems. His work focuses actually on modelling, analysis and efficient implementation of Embedded systems.</p> <ol style="list-style-type: none"> <li>1. N. Ben Said, T. Abdellatif, S. Bensalem, M. Bozga Model-driven Information Flow Security for Component-Based Systems In <i>FPS'14 ETAPS Workshop</i>.</li> <li>2. S. Bensalem, M. Bozga, J. Quilbeuf and J. Sifakis Optimized Distributed Implementation of Multiparty Interactions with Restriction In <i>Science of Computer Programming</i>, 2014.</li> <li>3. A. Basu, S. Bensalem, M. Bozga, J. Combaz, M. Jaber, T-H. Nguyen, J. Sifakis Rigorous Component-Based System Design Using the BIP Framework In <i>IEEE Software</i>, 28(3): 41-48 (2011).</li> <li>4. S. Bensalem, A. Legay, M. Bozga Rigorous embedded design: challenges and perspectives In <i>Software Tools for Technology Transfer (STTT)</i> 15(3):149-154(2013).</li> <li>5. A. Basu, S. Bensalem, M. Bozga, B. Delahaye, A. Legay Statistical abstraction and model-checking of large heterogeneous systems In <i>Software Tools for Technology Transfer (STTT)</i> 14(1):53-72(2012).</li> </ol>	
<p><b>Role in project:</b> UGA-VERIMAG will contribute across the full project and particularly we will coordinate WP2 System Design and Implementation which is at the core of the project, and will contribute to all other work packages.</p>	



<b>Partner 4</b>	<b>Organisation name / Department</b> <b>Formal Methods &amp; Tools</b> <b>University of Twente</b>	<b>UNIVERSITY OF TWENTE.</b>
<p><b>Expertise:</b></p> <p>The University of Twente is one of the technical universities in the Netherlands. Its research focus is High Tech, Human Touch; that is to connect innovative technical solutions work in a personal of societal context.</p> <p><b>Mariëlle Stoelinga</b>, is associate professor in the Formal Methods and Tools group at the University of Twente. She is an active and well-established researcher (60+ publications, H-index 24, 2100 citations) and leads a successful research line in the area of risk management for computer systems.</p> <p>Together with her team, she develops quantitative risk assessment methods to model, predict, and improve the risks of complex systems. These methods include fault tree analysis, attack tree analysis, architectural reliability and security modeling, and quantitative model checking. Stoelinga has developed compositional methods to simplify and improve attack fault tree analysis, which led to the tool sets DFTCalc and ATCalc.</p> <p>Stoelinga coordinated several national and international projects, and a WP in the EU FP7 project Quasimodo, on extra-functional system aspects. She is a key participant in the EU IP TREsPASS on quantitative security analysis for socio-technical systems. She (co-)supervised a number of PhD students and postdocs, and has been invited as a keynote speaker at several venues.</p> <ol style="list-style-type: none"> <li>1. Rajesh Kumar, Enno Ruijters, Mariëlle Stoelinga: Quantitative Attack Tree Analysis via Priced Timed Automata. FORMATS 2015: 156-171</li> <li>2. Florian Arnold, Holger Hermanns, Reza Pulungan, Mariëlle Stoelinga: Time-Dependent Analysis of Attacks. POST 2014: 285-305</li> <li>3. Enno Ruijters, Mariëlle Stoelinga: Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools. Computer Science Review 15: 29-62 (2015)</li> <li>4. Anne Remke, Mariëlle Stoelinga: Stochastic Model Checking. Advanced Lectures. Lecture Notes in Computer Science 8453, Springer 2014</li> <li>5. Tri Minh Ngo, Mariëlle Stoelinga, Marieke Huisman: Effective verification of confidentiality for multi-threaded programs. J. Computer Security 22(2): 269-300 (2014)</li> </ol>		
<p><b>Role in project:</b> UT will participate in the Modelling (WP2), Information Secrecy and Change management (WP3) activities. We will coordinate WP5 (Impact). In particular, through the interaction with partners in two European projects, UT will contribute to the exploitation of the project results.</p>		

## 2.4 Added value of the collaboration, including multidisciplinary and European dimension

SUCCESS is supported by expert teams in applying the BIP methodology, teams that have extensive experience in the area of developing methods and tools for safety and security verification. We also have experts in the synthesis of IoT systems and on developing sensor based technology. See table below:

Teams	Areas of Expertise					
	IoT	Risk Assessment	Security	Dynamic Security	Human Factors	Healthcare
MU	√		√		√	√
INRIA				√	√	
UGA	√		√			
UT		√	√	√		

The focus of SUCCESS is to provide secure accessible IoT for the healthcare sector. We secure the impact through the activities outlined in table below:

Contribution to Impact	Where is produced
Build and strengthen an interdisciplinary community of researchers working across the different domains of cyber-physical systems.	Our activities in SUCCESS bring together professionals from bio-engineering, healthcare and from different technical areas of Computer Science (security, human-centred computing, IoT). This is materialized through the scoping activities in WP2, our validation in WP4 and our dissemination in WP5.
Create new methods for specific emerging application domains with a concrete use case and concept for scientific empirical evaluation.	We will significantly expand methods and tools which have proved to be effective in embedded systems to incorporate a more dynamic and transparent interaction with humans (WP3). We validate this innovation in a hospital (WP5).
Create new technologies, methods and prototypes that address a business-related perspective.	Our innovation in WP3 will directly improve practice in healthcare environments (WP4) and, with revision, in other domains where human interaction and security are paramount (we will explore these alternatives in Task 5.2).

## 2.5 Consortium agreement principles (partner's rights and duties, IPR management)

The Project Manager will take the initiative to make a consortium agreement, together with partners in the project, which will contain the following information about IPR issues:

- Consortium members will undertake to keep confidential information disclosed to them by other members.
- The law applicable to IP protection will be defined.
- Any IP generated during the project will be owned by the partner or partners who have generated that IP.
- Results will not be published until their IP value has been assessed and agreed. Rights for objecting to publication will be defined.
- Access rights to pre-existing IP shall be granted where necessary, but a partner may exclude specific pre-existing IP from this obligation.
- Each party may continue to use the knowledge generated in their own research.

The Project Manager, in discussions with the Steering Committee, will determine if there are suitable opportunities for IP development and protection, whether within one partner's work or in work between several partners, and a decision will be made as to whether to seek appropriate IP protection or place the results in the public domain.

Florian Kammüller 12/6/15 7:45 PM

**Comment [29]:** Proposal requirement: „(max. ½ page)

*Describe the added value of the consortium as a whole (including complementarity, balance). Indicate the contribution of the project, at the European and/or international level, to the expected impacts."*

Florian Kammüller 12/6/15 7:51 PM

**Comment [30]:** (max. ½ page)



## 2.6 Description of significant facilities and large equipment available to the consortium to perform the project

(Only Middlesex University described as it is hosting the Pilots)

Our school is hosting a number of resources which are ideal for this project:

- The SensoLab is a laboratory for research on networks of sensors and will be in charge of the infrastructure supporting the pilots.
- Another key partner in this project will be the *Research Group on the Development of Intelligent Environments* which specializes in the processing of sensor-based systems and has a long experience developing systems related to healthcare and well-being in the UK and Europe.
- The lab led by Professor Bayford in the Natural Sciences Department where biomarkers for Alzheimer are developed and tested will be again used in connection with the Alzheimer's disease project which will be used for the second pilot. We have extensive facilities and equipment for ELISA, mass spectrometry analysis including UPLC hyphenated to API3000 triple quadrupole mass spectrometer, MALDI-Tof/Tof and LC-ion-trap-time of flight mass spectrometer for accurate mass measurement so this will incur no additional cost apart from consumables.

The first pilot will be deployed on a permanent basis in our Living Lab Smart Home where the system can be built and tested continuously during the first year until we enter the phase where we deploy it in the healthcare setting.

The second pilot will be hosted in Homerton University Hospital, based in the east London Borough of Hackney. This is an NHS (National Health Service) authorized fully functional hospital which has agreed to interface with patients and to help with the setting up of the experiments, which will gather information through sensors from daily life activities (smart phone and bracelet) as well as more specialized clinical information (biomarkers) sensed at the hospital with special equipment.

## 2.7 Link with ongoing projects

**Middlesex University** is the technical director of the POSEIDON project funded by the program "ICT for smart and personalised inclusion" (Objective ICT-2013.5.3). The project is developing a PersOnalized Smart Environments to increase Inclusion of people with DOWn's syNdrome. This is a network of mobile and stationary devices based on context-awareness. POSEIDON is not focused on resilience and trustworthiness, however given it is dealing with vulnerable adults security issues and robustness of the system are a core concern.

Professor Bayford taking part in this proposal is leading a research project on Early Detection of Dementia Through Biomarkers, which uses a combination of sensing equipment and is being developed in collaboration with Homerton University Hospital. This project will be directly related to the second pilot of SUCCESS.

Another project which is available to the group is NOCTURNAL (Night Optimised Care Technology for UseRs Needing Assisted Lifestyles), which the coordinator of this project developed from 2009 until 2012 and was a national UK project jointly funded by most prestigious funding bodies for Computer Science and ICT in the UK: TSB and EPSRC. This project used a networked sensing devices to increase safety and understanding of needs for elderly people living independently.

Florian Kammueeller 12/6/15 7:55 PM

**Comment [31]:** (max. ½ page)

Florian Kammueeller 12/6/15 7:56 PM

**Comment [32]:** proposal requirement: "(max. ½ page per project partner)"

For each partner indicate (if applicable) the ongoing projects linked to the proposal topic, and their funding sources."



**INRIA** is currently running an Inria-Microsoft co-funded grant on **PRIVACY** (Privacy-Friendly Services and Apps). This is a project whose main objective is to develop new techniques to quantify privacy and changes. It involves several companies linked to INRIA. The objective of this project is to re-imagine how modern on-line services and applications may be engineered to provide a higher degree of technical privacy protection. Supporting stronger privacy and user control involves a serious redesign of key protocols and architectures that underlie these services, as well as the development of principled definitions of privacy, tools to realize them, and methods to evaluate the quality of protection afforded. The following type of sensitive data is considered: Location data, Health related data, and Financial related data. One of the fundamental objectives of this project is to develop principled and robust definitions of privacy, as well as methods for evaluating the quality of protection offered by different proposed mechanisms. The project intends to prototype high quality software tools for developing and evaluating privacy-friendly services. These include tools and libraries that implement high value computations in a privacy preserving manner; language based tools, such as compilers and runtimes, to support building higher level services; and platforms and API that support privacy features out of the box.

**UGA** is leading the EU FP7 STREP **D-MILS** (where INRIA is also a partner): This project develops an environment for the design, analysis, verification, implementation and certification of scalable, interoperable, and affordable trustworthy architectures. D-MILS uses an advanced time-triggered network architecture for communication among its nodes, providing, predictable, deterministic behaviour for safety-, security-, and enterprise-critical operation. D-MILS provides an end-to-end and top-to-bottom solution for certifiable highly-dependable systems that starts from a high-level, declarative (and graphical) language, the Architecture Analysis and Design Language (AADL), and provides a complete machine-processable chain of representations (BIP), usable within a verification framework providing verification of probabilistic and non-probabilistic properties, all the way down to the automated compilation of the detailed resource, schedule, and policy configurations of a distributed collection of single- and multi-processor MILS platform nodes. Moreover, D-MILS establishes a concrete linkage between the assurance activities performed at various levels of the system specification, design and implementation, and the high-level claims (and derivative sub-claims) made for the complete D-MILS system, using another declarative language, Goal Structuring Notation (GSN), to represent the assurance case for the system, with an automated connection to the component- and composition-centric verification framework.

**UT** leads a WP in the EU FP7 project Quasimodo, on extra-functional system aspects and is a key participant in the EU IP TRESPASS on quantitative security analysis for socio-technical systems.

## 2.8 Financial plan

We have negotiated with our partners a carefully planned budget which we are confident will allow us to produce all the innovation and impact we are committing to.

All our partners will engage on active planning, development and validation of the framework hence all four partners of the project will be involved in all WPs, including each country represented leading one stakeholder's workshop and actively engaged with several activities of dissemination which will require their travelling to meet with partners of the consortium, with officers of the CHIST-ERA program and to technical events.

The budget includes the cost of the two pilots which will be hosted by MU. This cost is entirely within MU's budget. The other partners will visit these facilities and will access the facilities remotely to upload upgrades and to test specific versions.

Florian KammueLLer 12/6/15 7:59 PM

**Comment [33]:** Copied from Partner description. Please expand.

Florian KammueLLer 12/6/15 8:00 PM

**Comment [34]:** Proposal requirement: „(max. 1 page)

*The resources to be committed for each project partner have to be described in the Electronic Submission System (ESS) by the coordinator. These resources include: Personnel, Consumables, Equipment, Travel, Subcontracting, Provisions, Licensing fees, other. Justify them here.“*



Another cost which has been included in the budget for partners MU, INRIA and UT is the cost for the stakeholder's workshops. We have explained in section "Dissemination and Exploitation of Results" we have planned these events in a way to make it financially efficient by aligning them with the steering/advisory committees meetings.

Our team is willing to use technologies like teleconferencing, all the partners have important infrastructure in this regard in each campus, so that we will minimize the cost of meetings. At the same time we all understand the importance of fluent and frequent communication amongst the teams so this will be secured and given priority.

The summary of our budget is below showing our project has a proportional cost per effort, is aligned with the commitments of the partners and represents good value for money overall:

Florian KammueUer 12/6/15 8:02 PM

**Comment [35]:** Updated Financial Plan Tabell to be added (compare previous proposal).

### 3. Impact

#### 3.1 Expected Impacts

Florian KammueUer 12/6/15 8:03 PM

**Comment [36]: Proposal requirement:**  
„(max. 1 page)

*Describe the scientific impact of the research project and if applicable, the foreseen societal impact, and the potential markets. Provide only information that applies to the project and its objectives. Wherever possible, use quantified indicators and targets.*

Florian KammueUer 12/6/15 8:05 PM

**Comment [37]:** Insert here ½ page of detailed analysis to what extent and how the call's principles are met by the project (See also previous proposal).

**Scientific community impact:** *SUCCESS* will push the importance of security and transparency of IoT higher in the agenda of research groups and companies. Our consortium wants to equip teams with a solution, an IoT security architecture which is reproducible for the community, and above this, to install in the community awareness the importance of developing IoT with dynamic security higher up in their agendas.

The **economic and social impact** of *SUCCESS*: a) *Economic Impact*: the overall cost for dementia care in Europe is an expected 600 billion Euro, b) *Impact on Healthcare*: at the present time, the expenditures on health care in the member countries of the European community account for an estimated 8.5% of the GDP and could rise up to 11.8% in 2030. *SUCCESS* will help this sector by facilitating the creation of automated monitoring of dementia patients, releasing time for nurses and doctors who can focus on more important tasks, c) *Impact for Dementia patients*: *SUCCESS* improves privacy for dementia patients from first diagnosis to care. It mitigates problems with insurance companies and employers of dementia patients.

### 3.2 Dissemination and Exploitation of Results

Work package 5 is entitled “Impact” to ensure that the reproducible security architecture produced in *SUCCESS* can fulfil its potential and brings the benefits of highest security standards into critical areas of the health care sector. ||

We will aim to disseminate our results continuously, starting with the development of a webpage devoted to the project where we are going to make available the documents we produce and link up with social media and the wider community in general. We will also create our open source repository which will be kept during our

We expect to submit several contributions to conferences and journals since the project's ambitious application goals bring together various related research fields: security and privacy, socio-technical aspects of security and trust, automated verification, formal methods for software engineering, component based software engineering, and embedded systems amongst others. Therefore, we will aim to publish in various conferences: S&P, CSF, CCS for security and privacy POST, DPM, STAST for socio-technical aspects of security, CAV, TACAS, ITP for automated verification, SEFM, FASE for formal methods for software engineering, ICSE, CBSE for component based software engineering, EMSOFT, MEMOCODE for embedded systems.

We will give importance to the interaction with several types of stakeholders. For our project we see our impact more specifically connected with the research community and with the professionals in healthcare, which is our selected area of application. Therefore we will have two types of workshops with both communities: (A) the goal of the academic workshops will be to provide a venue for (a) rapid dissemination of scientific innovation; (b) realigning with the progress of other researchers and practitioners and (c) identifying new exploitation opportunities. We are planning two academic workshops in years 1 and 2. Academic workshops will take place co-located with high quality conferences. The rationale being that clearly marked public events guarantee project visibility, thus increasing the impact and the chances of project results being adopted by a wider community. The workshop will consist of invited presentations—both by members of the consortium and by researchers and practitioners not involved in the project, and (B) the stakeholders' workshops will be held as part of our annual meeting with the Steering and Advisory committees. We plan three such workshops, one will be held in London, one in Paris and another one in Lausanne. For this workshop we will invite professionals (e.g., technicians and managers) from the healthcare sector which are based within the region where we held the workshop. In this way the stakeholders' workshop will not require a large extra financial investment. Given our pilot is in the healthcare sector and based on a UK hospital, the workshops in France and Switzerland will be very helpful to make sure we equally hear and consider the concerns of professionals in those countries adding generality and acceptability to our solution.

These workshops will also help us to implement our exploitation plan as they will provide excellent opportunities to assess, agree, and outline more precisely the potential market and potential opportunities for the teams involved in *SUCCESS*. After the initial workshop we will draw an initial exploitation plan which we will present and update in subsequent workshops.

Each partner will have a clear gain doing internal knowledge transfer in teaching and research activities to feed the cycle of innovation

The *SUCCESS* team will also engage with professional bodies and with the CHIST-ERA team to identify other opportunities and maximize the opportunities for exploitation by considering ways to transfer this innovation to the companies our organizations interact with.

Florian Kammüller 12/6/15 8:08 PM

**Comment [38]:** Proposal requirement:

„(max. 1 page)

Provide a plan for disseminating and exploiting the project results.

Juan Carlos Augusto 12/6/15 8:06 PM

**Comment [39]:** Not sure we can fit it in ...

“We consider impact as extremely important as something that goes beyond the fundamental science we can create. We need to show this project will improve things for industry and citizens.”

## 4. Ethical issues

### **Foreseeable ethical issues arising during the project:**

- Conducting research with vulnerable participants raises issues of consent competence due to reduced cognitive functions and intellectual disabilities.
- Sensor-based, automated monitoring systems raise privacy and confidentiality issues, particularly when related to the gathering and processing of sensitive personal information, including diagnostic and therapeutic medical data.
- Data protection issues will be involved where personal data needs to be collected and shared.
- The security and integrity of critical data collection, transmission and storage highlights the need for resilient and trustworthy security and access controls.
- The risk of replacing human emotional care and social interaction with automated, computer-based monitoring systems raises potential issues around dignity and social inclusion.

**Mitigation strategies to reduce ethical risks:** Respect for the dignity of all participants will be prioritised by establishing a supportive research environment throughout all phases of the project. Established guidelines for research involving people with reduced consent competence will be adhered to. The aims of the project, and how the system works, will be clearly explained, in understandable terms, to different beneficiaries. The system will support healthcare professionals in a way that does not replace the emotional dimension of human care, or increase social isolation amongst dementia patients. Privacy and confidentiality of data will be preserved through compliance with data protection laws regarding the collection, use and dissemination of personal data, secondary uses of that data, and access to it by third parties. Data protection principles will be adhered to, regarding data retention, anonymity and secure data handling. A framework of guiding ethical principles will be developed and embedded throughout the project. This framework will draw on established, practice-based medical ethics, ethical guidelines for research with human participants from the field of psychology, and an ethical framework for intelligent environment development produced by project team members. The project will be monitored by Middlesex University's Ethics Committee, and relevant committees in the partner institutions.

**Justification of research methodology with respect to ethical issues:** The project will pursue a user-centric research methodology with a high a level of stakeholder input to ensure needs and requirements are appropriately identified and modelled. A broad range of stakeholders will be consulted, including primary users, and secondary and tertiary users, such as social and health care professionals, and representatives of relevant professional and voluntary associations with specialist medical knowledge. This user-centric approach will inform the building and testing of Pilots 1 and especially Pilot 2 which will be deployed in close collaboration with hospital staff in a healthcare setting.

Florian Kammüller 12/6/15 8:12 PM

**Comment [40]:** Proposal requirement:  
"(max. ½ page)"

*Describe any foreseeable ethical issue that may arise during the course of the research project. Describe all mitigation strategies employed to reduce ethical risk, and justify the research methodology with respect to ethical issues."*

## 5. References

*(max. 30 references)*





## Appendix A

Examples of Internal risks: Nature and associated action
The web page is delayed and this deteriorates the visibility of the project and also the mechanisms for data sharing between the partners. <b>Action:</b> the Webpage will be considered as another document deliverable and subject to the mechanisms of peer review and Advisory Board review.
There is a risk that the cooperation of the partners within a WP does not work. <b>Action:</b> This risk will be handled through a prior agreement of responsibilities for each team which will be officially stated in the consortium agreement.
There is a risk that cross WP cooperation does not work. <b>Action:</b> The cooperation between work packages will be overseen at a local level by WP coordinators and at a project level by the project coordinator. Discrepancies and misalignments will be considered first by the WP leaders and if needed by the Steering Committee.
A partner does not comply with the promised services at a level that jeopardizes the whole project. <b>Action:</b> if unanimous consensus is achieved in the Steering Committee emergency meeting then the partner is separated and the money is used to sub-contract services as close as possible to those that should have been delivered.

## Examples of WP-specific technical risks

WP affected	Nature and associated action
WP1 <u>Status:</u> Low <u>Impact:</u> High	<b>Problem:</b> Some aspects of management do not work efficiently. <b>Action:</b> the team leading the project (Middlesex University London - UK) has been selected for his experience in running projects of different dimensions to minimize the chances of this risk happening. Also the oversight of the overall management and direction of the project has been shared with different partners within the project (through the Steering Committee and the Advisory Committee) so that there are different people with capacity to spot and warn of potential dangers so that strategies can be put in place to avoid problems from occurring.
WP2 <u>Status:</u> low <u>Impact:</u> High	<b>Problem:</b> It is difficult to attract stakeholders to the workshops, which then adversely affects the gathering of requirements and validation. <b>Action:</b> given the partners leading the project are used to user-centred activities and they understand the logistical difficulties behind this, the task will be started as early as the project starts and equally will be planned with anticipation for each yearly cycle. We will also broaden the search to each partner and CHIST-ERA to make sure the situation is one of having choices to select from.
WP3 <u>Status:</u> Medium <u>Impact:</u> Medium	<b>Problem:</b> The solution of a technical problem takes longer than anticipated affecting achievements in other tasks, integration into the overall architecture and validation. <b>Action:</b> the problem will be fragmented trying to maximize the situations which can be used with confidence and a contingency plan will be designed on how to proceed with the remaining aspects of that challenge.
WP4 <u>Status:</u> Medium <u>Impact:</u> Medium	<b>Problem:</b> Creating the basic CPS and Integration with WP2 and WP3 takes more time than expected. <b>Action:</b> we will be approaching these through several incremental steps instead of awaiting for big parts of the system to be ready.
WP4 <u>Status:</u> Low <u>Impact:</u> Medium	<b>Problem:</b> Validation takes more time than expected. As this task grows on importance towards the last part of the project it may jeopardize the overall outcome at the end of the project. <b>Action:</b> This task will be given high priority, protected and followed carefully to make sure this does not happen. MU is an experience partner in running projects and on validation. The project will have more effort deployed on the third year for both Pilots.
WP5 <u>Status:</u> Low <u>Impact:</u> High	<b>Problem:</b> Technology perceived as not needed by the market. <b>Action:</b> the team has developed a community-centred approach precisely to make sure the product of this project is relevant to our colleagues in academy and industry. Stakeholders will be consulted and invited to co-design the project during all its lifetime.



Appendix B: Letter of Support

Florian Kammüller 12/6/15 9:04 PM

**Comment [41]:** Will be updated by a more recent letter.

Homerton University Hospital **NHS**  
NHS Foundation Trust

Homerton University Hospital NHS Trust  
Department of Chemical Pathology  
Homerton Row  
London  
E9 6SR

Tel: 020 8510 7886  
Fax: 020 8510 5795  
Web site: [www.homerton.nhs.uk](http://www.homerton.nhs.uk)

Homerton University Hospital NHS foundation Trust has been conducting collaborative research with Professor Richard Bayford in the area of Alzheimer's disease and through Prof. Bayford we have learnt about the SUCCESS project which is proposing to investigate how to improve security in relation to human data in healthcare settings.

I support the SUCCESS project because as our research develops with Richard we intend contacting carers of patients with Alzheimer's disease, some of whom may be in the prodromal phase, in order to assess changes in cognitive development. The development of apps with robust and secure data is essential. We agree to interact with the consortium of SUCCESS to support research into this area and their pilots.

We understand that all expenses incurred in this collaboration will be covered by the SUCCESS project.

Dr. Peter M Timms BSc., MCB., FRCPath., CSI., PhD.

Dr Manish Sharma  
Consultant Chemical Pathologist

Dr Peter Timms  
Consultant Clinical Biochemist

*Incorporating hospital and community health services, teaching and research*

## Appendix C: Detailed PM effort spread through WPs

WP1	1-MU	2-INRIA	3-UGA	4-UT	Total
T1.1	1				1
T1.2	1	1	1	1	4
T1.3	1				1
T1.4	1				1
Total	4	1	1	1	7

WP2	1-MU	2-INRIA	3-UGA	4-UT	Total
T2.1	1	1	2	1	5
T2.2	1		2	1	4
T2.3	1	1	4	2	8
T2.4	2		3	4	9
T2.5	2	1	9		12
Total	7	3	20	8	38

WP3	1-MU	2-INRIA	3-UGA	4-UT	Total
T3.1		1	6	1	7 <sup>8</sup>
T3.2	5	1	2	5	13
T3.3		5	2	5 <sup>2</sup>	7 <sup>9</sup>
T3.4	4	8 <sup>3</sup>	3	2	15 <sup>12</sup>
Total	9	10	13	10	42

WP4	1-MU	2-INRIA	3-UGA	4-UT	Total
T4.1	1	1	1	1	4
T4.2	3	1	2	1	7
T4.3	4	2	2	1	9
T4.4	1				1
Total	9	4	5	3	21

WP5	MU	INRIA	UGA	UT	Total
T5.1	2	1	2	5	10
T5.2	1	1	2	5	9
Total	3	2	4	10	19

Partner	WP1	WP2	WP3	WP4	WP5	Total
1-MU	4	7	9	9	3	32
2-INRIA	1	3	10	4	2	20
3-UGA	1	20	13	5	4	43
4-UT	1	8	10	3	10	32
Total	7	38	42	21	19	127