

## CHISTERA CALL - RTCPS - SecUre Component Composition Enhances cyber phySical Systems (SUCCESS)

2015-01-13 04:56

### Consortium Partners

C/P	Institution	Contact	Other	Country	Legal Status	Ind.Eff
C	Middlesex University Higher Education Corporation/School of Science and Technology, Department of Computer Science	Juan Augusto	Florian Kammüller, Richard Bayford, Purav Shah and Simon Jones	United Kingdom	Public research organisation	42
P	Institut National de Recherche en Informatique et en Automatique	Axel Legay	Albert Cohen	France	Public research organisation	41
P	Université Joseph Fourier/VERIMAG	Saddek Bensalem	Marius Bozga and Jacques Combaz	France	Public research organisation	25
P	École Polytechnique Fédérale de Lausanne/School of Computer and Communication Sciences	Joseph Sifakis	Dr Simon Bliudze	Switzerland	Public research organisation	33

### Coordinator contact

Institution/Department	Middlesex University Higher Education Corporation/School of Science and Technology, Department of Computer Science
Principal Investigator	Juan Augusto
Address	The Burroughs, Hendon, London, NW4 4BT.
Telephone	+4407426999393
E-mail	J.Augusto@mdx.ac.uk
Names of other personals	Florian Kammüller, Richard Bayford, Purav Shah and Simon Jones
Country	United Kingdom
Legal status	Public research organisation
Individual effort (PM)	42
Funding agency	EPSRC

### Partners contact

Institution/Department	Institut National de Recherche en Informatique et en Automatique
Principal Investigator	Axel Legay
Address	Domaine de Voluceau, Rocquencourt - BP 105, 78153 LE CHESNAY Cedex
Telephone	+33 635434985
E-mail	axel.legay@inria.fr
Names of other personals	Albert Cohen

Country	France
Legal status	Public research organisation
Individual effort (PM)	41
Funding agency	ANR

Institution/Department	Université Joseph Fourier/VERIMAG
Principal Investigator	Saddek Bensalem
Address	Centre Équation - 2, avenue de Vignate, 38610 GIÈRES
Telephone	+33 (0)4 38 78 28 06
E-mail	Saddek.Bensalem@imag.fr
Names of other personals	Marius Bozga and Jacques Combaz
Country	France
Legal status	Public research organisation
Individual effort (PM)	25
Funding agency	ANR

Institution/Department	École Polytechnique Fédérale de Lausanne/School of Computer and Communication Sciences
Principal Investigator	Joseph Sifakis
Address	Rigorous System Design Laboratory, INJ 341 (Building INJ), Station 14, CH-1015 Lausanne
Telephone	+41216931398
E-mail	joseph.sifakis@epfl.ch
Names of other personals	Dr Simon Bliudze
Country	Switzerland
Legal status	Public research organisation
Individual effort (PM)	33
Funding agency	SNSF

## Financial Plan

Type	Middlesex University Higher Education Corporation/School of Science and Technology, Department of Computer Science	Institut National de Recherche en Informatique et en Automatique	Université Joseph Fourier/VERIMAG	École Polytechnique Fédérale de Lausanne/School of Computer and Communication Sciences	Project total
Personnel	200278	319700	303835	274006	1097819
Consumables	2700	0	12355	0	15055
Equipment	21539	3000	0	0	24539
Travel	38718	18000	30000	5833	92551
Commissions	0	0	0	0	0
Other	4645	1000	3000	4000	12645
Overheads	212890	0	5769	0	218659
Total costs	480770	341700	354960	283840	1461270
Requested	384616	150942	150000	170106	855665

**Middlesex University Higher Education Corporation/School of Science and Technology,  
Department of Computer Science**

Type	Item	Year 1		Year 2		Year 3	
		Total cost	Requested	Total cost	Requested	Total cost	Requested
Personnel	PI: Juan Augusto (2.52PM); Co-I: Florian KammueLLer (2.52PM); Co-I: Richard Bayford (1.08PM); Co-I: Simon Jones (0.36PM); graduate research assistant (36PM)	65379	52303	66745	53396	68153	54522
Consumables	pilot study consumables	2700	2160	0	0	0	0
Equipment	laptops; pilot study costs	21539	17231	0	0	0	0
Travel	annual review meetings; consortium workshops; conferences	14877	11901	14877	11901	8964	7171
Commissions		0	0	0	0	0	0
Other	meeting hosting costs	4645	3716	0	0	0	0
Overheads	estates, indirect costs	70963	56770	70963	56770	70963	56770

### Institut National de Recherche en Informatique et en Automatique

Type	Item	Year 1		Year 2		Year 3	
		Total cost	Requested	Total cost	Requested	Total cost	Requested
Personnel	24 PM of postdoc or expert engineer, 17 PM of senior INRIA researcher (not funded)	82640	31640	151165	64465	85895	32837
Consumables		0	0	0	0	0	0
Equipment	3 laptops for co-PIs and for postdocs working on the project	3000	3000	0	0	0	0
Travel	p.y.: 2 confs	6000	6000	6000	6000	6000	6000

(1500), 3\*2  
proj. meetings  
(500)

Commissions		0	0	0	0	0	0
Other	Organisation of workshop	0	0	1000	1000	0	0
Overheads		0	0	0	0	0	0

### Université Joseph Fourier/VERIMAG

Type	Item	Year 1		Year 2		Year 3	
		Total cost	Requested	Total cost	Requested	Total cost	Requested
Personnel	Post-doc: 25PM; IP: 9.6PM; IR: 9.6PM; IR: 9.6PM. Only 25 pms for the Post-doc are being funded.	72275	3955	115780	47460	115780	47460
Consumables	small computer equipment, software licences	4118	4118	4118	4118	4118	4118
Equipment		0	0	0	0	0	0
Travel	travels for meetings for 2 people and 3 conferences	10000	10000	10000	10000	10000	10000
Commissions		0	0	0	0	0	0
Other	Open Access Publishing	1000	1000	1000	1000	1000	1000
Overheads	Indirect costs attributed to the project	1923	1923	1923	1923	1923	1923

### École Polytechnique Fédérale de Lausanne/School of Computer and Communication Sciences

Type	Item	Year 1		Year 2		Year 3	
		Total cost	Requested	Total cost	Requested	Total cost	Requested
Personnel	Post-doc research assistant 24 PM; Scientific collaborator 6 PM; Full professor at	85793	39343	100970	80136	87243	40793

25kFr/year (3 pms)							
Consumables		0	0	0	0	0	0
Equipment		0	0	0	0	0	0
Travel	Travel to meetings and conferences	2500	2500	1666	1666	1666	1666
Commissions		0	0	0	0	0	0
Other	Open access publication and organisation of workshop	1000	1000	1000	1000	2000	2000
Overheads		0	0	0	0	0	0

## CHIST-ERA Proposal Template

*Project Acronym*

**SUCCESS**

*Project Title*

**SecUre Component Composition Enhances cyber phySical Systems**

**Addressed Call Topic (RTCPs<sup>1</sup> or HLU<sup>2</sup>):**

**RTCPs**

*Coordinator contact point for the proposal*

Name	Juan Carlos Augusto
Institution/Department	Middlesex University – School of Science and Technology
Address	Hendon Campus – London
Country	UK
Phone	+4407426999393
Fax	
E-mail	j.augusto@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> <i>Coordinator</i>	UK	Middlesex University London – School of Science and Technology	Prof Juan Carlos Augusto	Dr Florian Kammüller	Prof R. Bayford Dr S. Jones Dr P. Shah Research Assistant (Ph.D.)
<b>2</b>	France	INRIA	Dr Axel Legay	Dr A. Cohen	Research Assistant (Ph.D.)
<b>3</b>	France	UJF - VERIMAG	Prof Saddek Bensalem	Dr M. Bozga	Research Assistant (Ph.D.)
<b>4</b>	Switzerland	EPFL	Prof Joseph Sifakis	Dr S. Bludze	Research Assistant (Ph.D.)

<sup>1</sup> Resilient Trustworthy Cyber-Physical Systems

<sup>2</sup> Human Language Understanding: Grounding Language Learning

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

Cyber-Physical Systems are enabling a new generation of systems which have a great potential to provide novel services to humans in critical areas for society. This innovation however requires updating our understanding of the new risks associated with the new technology so that we can deploy it with confidence and society can trust it.

Amongst the biggest threats to the trustworthiness of new technology are security issues and amongst the main triggers for security problems is human behaviour, either through genuine errors or though malicious intent. The core idea of SUCCESS is to upgrade methods and tools with a proven track record to provide a more holistic consideration of security in relation to human factors within CPS. We also look at aspects of Information Confidentiality and Change management but only to the extent which they contribute to our two priority areas of concern.

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 trustworthiness within CPS 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.

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*):

We address "Resilient Trustworthy Cyber-Physical Systems"

We address mainly the combination between "Security" and "Human Factors" although we also take consideration of "Information Confidentiality" and of "Change Management" as this is all inter-related.

Our proposal aims to have impact in all the expected areas:

"Build and strengthen an interdisciplinary community of researchers working across the different domains of CPS", "Create new methods for specific emerging application domains (in our case we focus on smart health care)" and "Create new technologies, methods and prototypes that address a business-related perspective".

<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

Cyber Physical Systems (CPS) are made to benefit humans in their daily activities. So far, Computer Science produced methods and tools, which consider hardware and software systems, as they are mostly mechanical and predictable. However, the more we consider the complexity introduced by humans the less help we have. The focus of CPS and its subcategories (ubiquitous computing, pervasive systems, intelligent environments, AAL, etc.) must be on humans. Engineering secure CPS must make human behaviour a central element of modeling and analysis to address burning security issues like social engineering and insider attacks. The more so, we need to look at how to represent humans and the ways they interact with systems, or how humans and their ways of interactions are considered in a system.

Resilient trustworthy CPS that integrate humans require advanced scientific methods and techniques in security, verification, component based software engineering, embedded system design and implementation. The challenge lies in a secure and yet flexible combination of

- specification and verification techniques for secure CPS components and their composition,
- verification methods and techniques for component systems with humans with models of human behaviour, social interactions and human-system interactions,
- implementation and modeling languages with synthesis algorithms preserving 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 rigorous CPS development methods,

**(S2)** to extend decentralized access control for CPS component system by generalizing security models to include the human factor,

**(T1)** to design and prototypically implement synthesis and code generation methodology for CPS component frameworks,

**(T2)** to build and test the change management of a secure CPS pilot system from the healthcare sector of a sensor based monitoring system for dementia patients with security critical data and actions.

*SUCCESS* extends the successful Behaviour, Interaction, Priority (BIP) method to support development of secure CPS and at the same time creates a security architecture, i.e., a unified security design that addresses the necessities and potential risks involved in a CPS environment for healthcare specifying when and where to apply security controls while this design process will be reproducible. 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

Security cuts across all aspects of systems from an organisation's policy through to the physical layer of networks. Thus techniques from sociology via formally verified component system development through to network security need to be applied. Security is a valid application domain for formal techniques, specification, and verification. The idea of *SUCCESS* is to use a CPS integrating humans as a case study to show how far these techniques can be applied for accompanying the high quality formally founded development of a secure human centric CPS throughout all layers and support change management.

Information flow control (IFC) (Denning and Denning 1977) is a technique that allows specifying secure information flows for IT systems. Security means that only allowed flows are possible in a system, a generally undecidable property. IFC has received a lot of attention in recent research initiatives, see for example, the German network of excellence of the DFG Reliably Secure Software systems RS3, (Mantel 2014). Security of distributed component systems extensions to more complex access control models necessitates decentralized information flow control (DIFC, Myers et al. 97). DIFC models have been practically applied in distributed Java with security annotations (JifSplit, Zdancewic et al., 2002) but can also be transferred to distributed actor based programming languages (Kammüller, 2012). Security is generally not a compositional property, i.e., composition of two secure systems does not necessarily produce a secure system (Mantel, 2002). Component based systems for CPS need to address this problem. SecureBIP (Bensalem, Bozga et al. 2014) is an extension of the BIP methodology for information flow security for component based systems. It combines event flow and data flow non-interference to provide a method for secure by construction component systems. Starting from a security policy defined at the centralized level, the SecureBIP framework allows building distributed systems and generating secure code that implements the desired security policy defined at the centralized level (Bensalem, Bozga et al., 2015). Security for CPS not only needs consideration of distribution at the component level but also for CPS networks integrating human factors.

Quantifying privacy has been the subject of a series of recent work, motivated by the statement that having a pure Boolean notion for privacy does not make sense: there is no perfect zero-leaking information algorithm. Most of existing work on quantifying privacy rely on strong mathematical frameworks (Biondi et al., 2013), which limits their applicability for the case of very large state-space. In a series of recent work, several authors proposed to use simulation and statistics to estimate the privacy. In this project, we will lift those techniques to a compositional design reasoning in the spirit of (Palamidessi 2013).

Cyber security is the extension of security to organisational issues and society. Insider threats, privacy awareness, and whistleblowers demand additional means beyond computer security to assure protection of assets including data, desktops, servers, buildings, and most importantly, humans. Higher Order Logic enables modeling security scenarios that include human behaviour and infrastructures (Boender et al., 2014). This technique allows rigorous analysis of security policies including physical aspects of organisations like rooms and keys, organisational measures as well as psychological dispositions of humans to identify malicious insider attacks (Kammüller et al., 2014). Systematic exploration of the policies can identify attack vectors. Modeling and analysis are supported by a framework in the interactive theorem prover Isabelle/HOL. Such formal modeling facilitates the transfer of system model security policies to formal specification of properties for component-based design for a security architecture of CPS with humans.

There are numerous approaches to component development but BIP is a well established one integrating verification and code synthesis for CPS. BIP – Behaviour, Interaction, Priority - is a component framework consisting of a language for modelling component-based systems and associated execution, simulation, and verification tools, in particular Symbolic

Model Checking (SMC). To express behaviour at system architecture level, Glue-operators (Bliudze et al., 2008) are defined for BIP to preserve behavioural equivalence when composing systems. They enforce global security properties by characterisation of coordination between components at the architecture and design flow level (Basu et al. 2011). *SUCCESS* extends the secure-by-construction methodology of SecureBIP to CPS with human factors and provides a security architecture, i.e., a reproducible CPS design enforcing global security properties characterizing the coordination between components. The scenario is dementia patient care in the healthcare sector addressing mission-critical security issues for monitoring and clinical care for dementia patients while preserving confidentiality of their diagnosis and therapeutic data.

Table 1 gives a summary of the state of the art in relevant scientific areas and the progress we envisage for *SUCCESS*.

**Table 1.** Advances in the state of the art to be achieved by *SUCCESS*.

Area	State of the Art	Proposed Advances
Information Secrecy for Components	Numerous approaches to Information Flow Security but no pragmatic approach for human centred component systems	A1) We extend SecureBIP to accommodate security classes for humans and enhance the foundations to security by composition and preservation properties.
Security for CPS with Human factors	Cyber security is an active research area. Integration of human behaviour into CPS is a challenge.	A2) We use system models with human agents as decentralized security models to specify access control for CPS with human components, security properties, and attack vectors.
Security Verification of CPS	Numerous isolated approaches in specific areas. Extending verification of component CPS to include human factors is a hot topic.	A3) Challenges for verification are probabilistic verification to include human behaviour; verification for change management of component CPS; verification of information flow control for CPS with extended access control for humans.
Synthesis of Secure CPS	Security extended programming languages, operating systems, and network protocols are well understood: how to synthesize code for embedded systems for secure is a challenge	A4) Verification of small operating systems is possible, safe system synthesis from component specifications can be done. We extend these methods to security, i.e. how to ensure access control, how to ensure the requirements of human components, how to accommodate change management using BIP as a framework.
Change Management	Preservation of security properties of CPS components with humans is a quest: how to deal with components at different security levels, dynamic change of system architecture through movements etc.	A5) We support human centric CPS security by extending secure by construction CPS component systems to human factors. We advance in change management by extending security modelling, verification and synthesis for BIP component models with humans.

Quantification of the advances over the state of the art: our project will aim to produce

- New scientific methods or extensionextensions of existing ones in the areas A1-A5..
- A pilot case from dementia patient health care integrating areas A1-A5 to validate the success of the extensions.extensions The next section explains how we tackle the advances; The work plan in Section 2.1 and work package descriptions in Section 2.2 detail the concrete steps with **Table 2** finally indicating how we measure their achievement.

### 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 resilient and trustworthy CPS that include human behaviour. Starting from a model that integrates human behaviour with an infrastructure, we check for attack vectors to define a security policy and identify security properties for verification. The resulting formal specification is the basis for engineering a secure component architecture for a CPS. We will extend the BIP methodology and techniques for automated construction for component architectures to make them amenable to support the implementation of these component architectures as CPS that are flexibly composed from off-the-shelf components while simultaneously guaranteeing the security specification. The case study is a hospital room equipped with sensors for monitoring dementia patients, personnel and network-connected devices running other service components. The sensor network recognises and monitors humans. Humans are physical entities but may also carry devices (mobile phones, watches) that communicate with the 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 CPS system development, *SUCCESS* picks up scientific challenges from human centric development and extends BIP's component based technology by integrating the human factor into BIP.

**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) leads to security properties, access control model, and allows high level verification to exhibit attack vectors. Results are use cases, attack trees and logically specified security properties as requirements specification of component CPS design. As a **novelty** we enable that humans and their behaviour can be expressed within component designs. *The BIP extensions 5 and 6 allow the integration of human components into CPS models and support their verification:* 1. Security policies (what users can do, how to treat data). 2. Attacker model (who is the attacker, what power do we assume). 3. Identification of protection goals (confidentiality, integrity, availability, accountability). 4. Mechanical analysis of Isabelle/HOL model to find attack vectors. 5. Notion of agent/actor as a BIP component without a definitive behaviour: abstract BIP component whose behaviour can be replaced later with quantitative/probabilistic behaviour description that has to come from external sources and from empirical studies. 6. Quantitative model checking for BIP models with human components (e.g. probabilistic SMC with PRISM).

**B. Access control for distributed CPS with human actors:** to incorporate security requirements into a CPS, the security specification from **A.** must be enforced by access control in the design phase (1,2). Data security and action security model and security verification are already partially available in BIP. As a **novelty** for secure component design we include access control for human actors: 1. Modeling of infrastructure and actors (graphs where nodes have properties attached). 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 BIP human components. 4. Map access control (3) to BIP components. 5. Verification of access control: use information flow control of SecureBIP to check access control on the BIP CPS model.

**C. Synthesis of secure systems for humans:** synthesis of secure CPS for humans necessitates not just code generation from component models but mapping CPS component architectures to existing atomic components, like a small OS for network nodes and sensors (2), integrating them into networked CPS (1). Our **novelty** is to extend this to human components. *Secure construction (3-4) and extension (5) in the presence of human factors, lead to augmented synthesis and verification techniques (6). We explore scenarios in our human centric healthcare sensor network pilot enabling the assessment of progress made (7-9):* Build secure systems for humans by adding security components and extensions to CPS. 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. Meta-theoretical results on (subsets of) BIP components that allow compositional security. 5. Change management: security preservation or even emerging security properties by adding components to existing BIP CPS system. 6. Verification methods for change management, i.e., what auxiliary assumptions are necessary (and can be verified) on composed system. 7. **Scenario:** component comes into a secure network; the distributed access control needs to be expressive enough to specify components at different security levels, the extended BIP methodology should be able to analyse risks introduced, re-verify security properties, and manage the change on the synthesized code. 8. **Scenario** human changes behaviour (e.g. vulnerable human, or insider attacker). 9. For Scenarios 7&8: What happens to security and other properties?

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.5 &amp; A.6:</b> human behaviour can be verified for CPS specification
<b>S2</b>	<b>B.3-5 &amp; C.3-4:</b> access control can be expressed and verified for CPS with human components; definition and proof of security for compositions
<b>T1</b>	<b>C.6-9:</b> code can be generated and verified for CPS pilot
<b>T2</b>	<b>Pilot:</b> works, is accepted by users, change management according to needs is possible while security properties are (provably) preserved

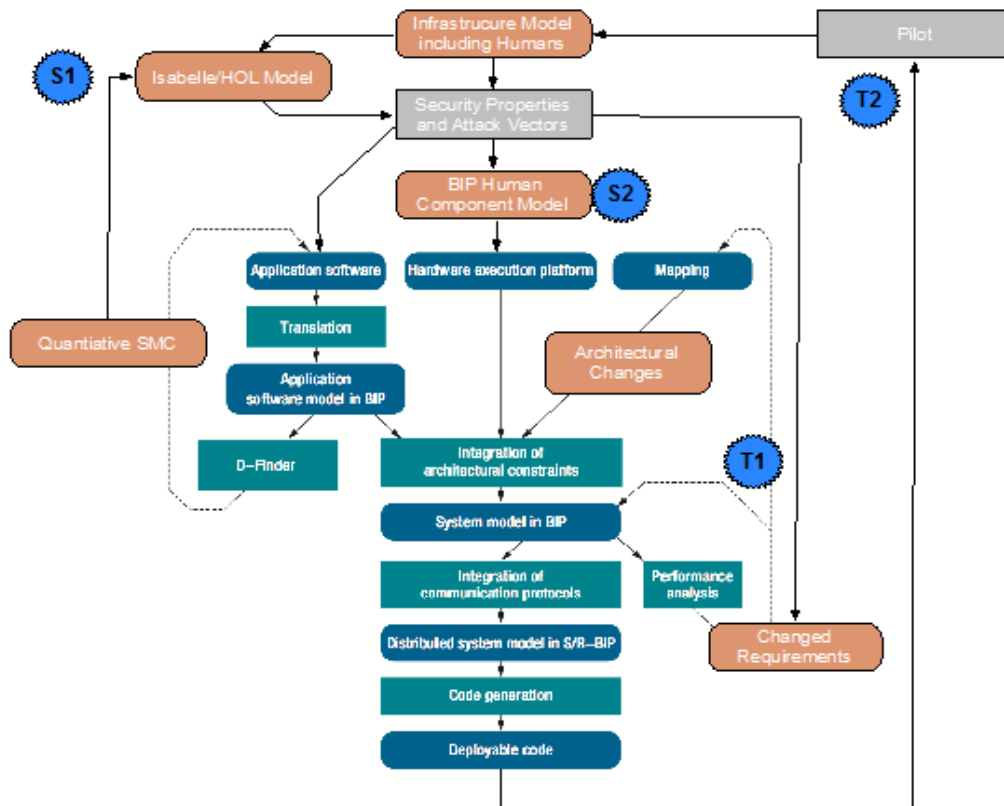


Figure 1. Illustration of workflow of the extended BIP method

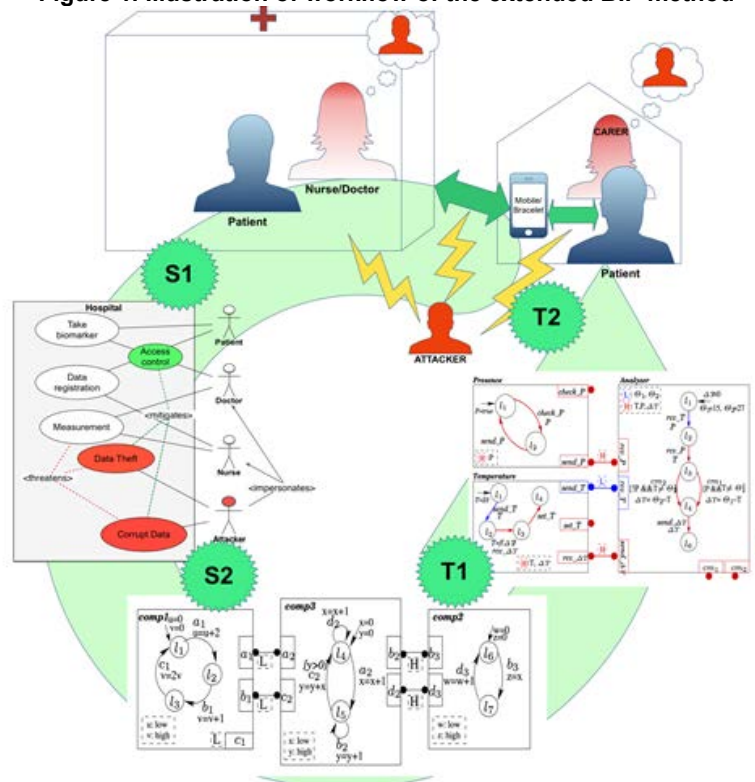


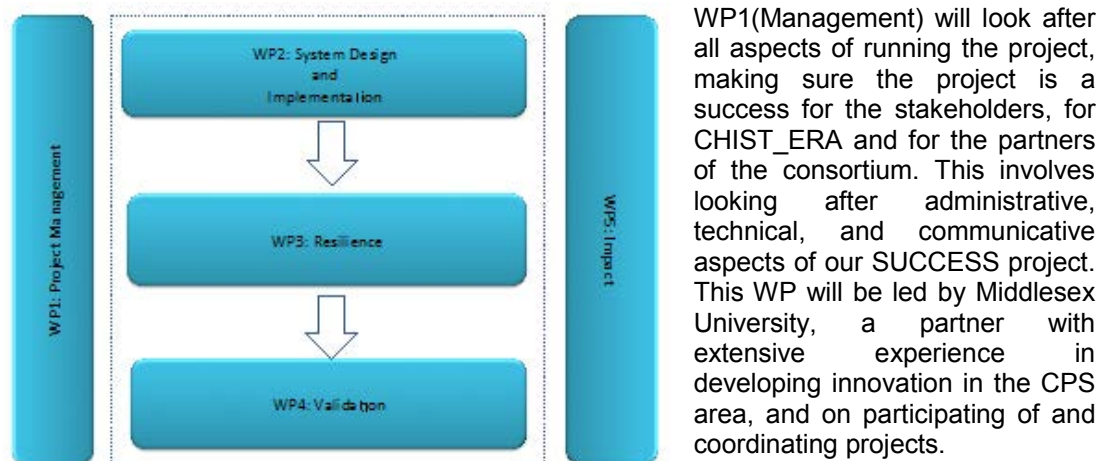
Figure 2. SUCCESS Pilot and Security architecture with Objectives S1-T2



## 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.



**Fig. 2.** Work packages organization

WP2 (System Design and Implementation) 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 UJF who are recognized experts in design of these type of systems.

WP3 (Resilience) 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 CPSs 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 EPFL 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.

Main events during life-time of the project:

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.

## 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)		6	1	1	1				
<b>Aim of the WP:</b> 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		<b>Communication (M1-M36; Responsible partner: 1-MU)</b> 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		<b>Reporting (M1-M36; Responsible partner: 1-MU, Involved: all partners)</b> 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		<b>Research quality assurance (M1-M36; Responsible partner: 1-MU)</b> 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		<b>Finances and Legal aspects (M1-M36; Responsible partner: 1-MU)</b> 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					



WP 2	System Design and Implementation					Start: M1	End: M36
Contribution of project partners							
Partner number	1	2	3	4			
Total effort per partner (Person*months)	15	11	12	10			
<b>Aim of the WP:</b> The goal of this work package is to develop a practical automated method for designing secure-by-construction distributed systems using a model-based approach integrating human factors. 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 distributed models and finally to distributed implementation, 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 in from WP3.							
<b>Tasks</b>							
T2.1	<b>Security requirements for CPS with human factors (M1–M30; responsible: 3-UJF; involved: all partners)</b> The goal of this task is to further 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 identify the security requirements and compositional context, covering the different architectural layers from applications design to the physical platform execution.						
T2.2	<b>Use case requirements (M1–M30: responsible: 3-UJF; involved: 1-MU, 4-EPFL)</b> 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 the different design and implementation.						
T2.3	<b>Abstract model configuration with human factors (M1–M30: responsible:3-UJF; involved: all partners)</b> 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 distributed 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.						
T2.4	<b>Platform-independent tools to support development (M1–M36; responsible: 3-UJF; involved: 1-MU, 4-EPFL)</b> 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	<b>Platform-dependent implementation with human factors (M6–M36; responsible: 1-MU; involved: 2-INRIA, 3-UJF)</b> Here we will consider a platform specific configuration where 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 confidentiality and integrity of exchanged messages between components. In this task we will generate automatically stand-alone processes for every abstract model configuration obtain 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)					

WP 3	Resilience						Start: M1	End: M36
Contribution of project partners								
Partner number	1	2	3	4				
Total effort per partner (Person*months)	10	27	6	10				
<b>Aim of the WP:</b> We will build a taxonomy associated with the engineering and evolution of resilient CPS. 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, resilient CPS. Tasks report individually and through consolidated resilience characterisations.								
Tasks								
T3.1	<b>Information Confidentiality (M1 – M24: responsible: 2-INRIA; involved: 3-UJF, 4-EPFL)</b> Formalizing confidentiality properties with an emphasis on trustworthiness and human interaction, as captured by T2.1. Building on the existing model of SecureBIP, we will propose composition, model transformation and synthesis methods to preserve information secrecy in T2.2.							
T3.2	<b>Security (M1 – M24: responsible: 2-EPFL; involved: all partners) 2-INRIA,</b> Formalizing security properties with an emphasis on resilience, 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 synthesis in T2.2.							
T3.3	<b>Change Management (M12 – M36: responsible: 2-INRIA; involved: 1-MU, 4-EPFL)</b> CPS must adapt to a changing environment. BIP allows to model and synthesize runtime adaptation, but quantitative aspects of change management 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 CPS in time and its reactivity, from the model to the platform.							
T3.4	<b>Human Factor (M1 – M36: responsible: 1-MU; involved: 2-INRIA, 3-UJF)</b> A cross-cutting task involving all partners throughout the project, considering CPS-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 CPS and human-CPS interactions						
D3.2	M24	Resilient synthesis and quantitative modeling of human-centric, secrecy and security properties						
D3.3	M36	Resilient synthesis and quantitative modeling of unobtrusive change management in human-CPS interactions						

WP 4		Validation				Start: M1		End: M36	
Contribution of project partners									
Partner number		1	2	3	4				
Total effort per partner (Person*months)		12	3	3	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>CPS infrastructure (M1-M36; Responsible: partner: MU Involved: partner(s): 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: 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: 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: 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)	6	4	4	9					
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: 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-EPFL, 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.

**Table 2:** State of the art advances are balanced amongst work packages.

<b>Advance #1:</b> extension of SecureBIP with security classes for humans and with security by composition and preservation properties.	Concept: 2.1 and 3.2 Implemented: 2.5 Validated: 4.2 and 4.3.
<b>Advance #2:</b> using system models with human agents as decentralized security models to specify access control for CPS with human components, security properties, and attack vectors.	Concept: 2.1, 2.3 and 3.3 Implemented: 2.5 Validated: 4.2 and 4.3.
<b>Advance #3:</b> enhancements to verification (probabilistic, change management, and information flow control for CPS with extended access control for humans).	Concept: 2.1, 2.3, 3.3 and 3.4 Implemented: 2.5 Validated: 4.2 and 4.3.
<b>Advance #4:</b> extending the BIP framework to ensure access control, to ensure the requirements of human components, and to accommodate change management.	Concept: 2.1, 2.3, 3.3 and 3.4 Implemented: 2.5 Validated: 4.2 and 4.3.
<b>Advance #5:</b> extending secure by construction CPS component systems to human factors, in particular advancing change management by extending security modelling, verification and synthesis for BIP component models with humans.	Concept: 2.1, 2.3, 3.3 and 3.4 Implemented: 2.5 Validated: 4.2 and 4.3.

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

Partner	WP1	WP2	WP3	WP4	WP5	Total
<b>1-MU</b>	6	15	10	12	6	<b>49</b>
<b>2-INRIA</b>	1	11	27	3	4	<b>46</b>
<b>3-UJF</b>	1	12	6	3	4	<b>26</b>
<b>4-EPFL</b>	1	9	10	3	9	<b>32</b>
<b>Total</b>	<b>9</b>	<b>47</b>	<b>53</b>	<b>21</b>	<b>23</b>	<b>153</b>

## 2.3 Management and Risk Assessment

### 2.3.1 Management Strategy



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.


Table 2.3 a. Organizational Structure


#### List of milestones

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





## 1.4 Description of the Consortium

<b>Partner 1</b> (Project Coordinator)	<b>Organisation name / Department:</b> <b>Middlesex University London,</b> <b>School of Science and Technology</b>  <b>Middlesex University</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>Prof. 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>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>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>Purav Shah</b> is a Senior Lecturer in the Design, Engineering and Mathematics Department at Middlesex University London. His expertise is in the field of wireless sensor networks, Internet of Things, and Intelligent Transportation.</p> <ol style="list-style-type: none"> <li>1. 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>2. 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>3. J. Boender, M. Georgieva Ivanova, F. Kammüller and G. Primiero. Modeling Human Behaviour with Higher Order Logic: Insider Threats. <i>Socio-Technical Aspects of Security and Trust, STAST2014, co-located with CSF'14 in the Vienna Summer of Logic, IEEE 2014</i>.</li> <li>4. F. Kammüller and C. W. Probst. Combining Generated Data Models with Formal Invalidation for Insider Threat Analysis, <i>IEEE Security and Privacy Workshops, SPW, WRIT'14</i>. 2014. An extended version has been accepted for a Special Issue of the IEEE Systems Journal on Insider Threats.</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>	

<b>Partner 2</b>	<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 <i>ACM Symp. on 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>UJF-VERIMAG</b> 
<p><b>Expertise:</b> UJF-VERIMAG - Université Joseph Fourier Grenoble 1: UJF-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. UJF-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>UJF-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 UJF-VERIMAG are STMicroelectronics, Alcatel, CS-Transport, EDF, France Telecom, IBM, Intrisoft, ISD, Leti/CEA, Prover Technology, RATP, Silicomp, Trusted Logic.</p> <p>UJF-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. UJF- VERIMAG has been and is currently involved in many European projects: LTR VIREs (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> UJF-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>	

Partner 4	<b>Organisation name / Department</b> <b>EPFL, Rigorous System Design</b> <b>laboratory (RiSD)</b>	 ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE
<p><b>Expertise:</b> Current research at RiSD focuses on rigorous system design and correct-by-construction techniques. Based on the BIP framework, RiSD is developing an <i>architecture-based</i> design flow. Architectures depict design principles; they enforce global properties characterizing the coordination between components. We showed that safety and liveness properties can be addressed by the architecture-based approach. Integrating security properties into this framework remains a challenge to be addressed in this project.</p> <p><b>Prof. Joseph Sifakis</b> is a laureate of the 2007 Turing Award—for his contribution to the emergence of model-checking—and a number of other academic and societal distinctions. He is recognized for his pioneering work on embedded system design and verification.</p> <p><b>Dr. Simon Bliudze</b> received his PhD degree at Ecole Polytechnique (France) in 2006. Before joining RiSD in 2011, he was a post-doctoral researcher with Joseph Sifakis at Verimag (Grenoble, France; 2006–2009), working on formal semantics for the BIP component framework, and a research engineer at CEA Saclay (France; 2008–2011).</p> <ol style="list-style-type: none"> <li>1. P. Attie, E. Baranov, Simon Bliudze, M. Jaber and Joseph Sifakis. A General Framework for Architecture Composability. <i>SEFM</i>. 2014.</li> <li>2. Simon Bliudze, M. Bozga, M. Jaber and Joseph Sifakis. Architecture Internalisation in BIP. <i>CBSE</i>. 2014.</li> <li>3. Simon Bliudze, A. Mavridou, R. Szymanek and A. Zolotukhina. Coordination of software components with BIP: Application to OSGi. <i>MiSE</i>. 2014.</li> <li>4. T. Abdellatif, J. Combaz and Joseph Sifakis. Rigorous implementation of real-time systems—from theory to application. In <i>Mathematical Structures in Computer Science</i>. 2013.</li> <li>5. Joseph Sifakis. Rigorous System Design. In <i>Foundations and Trends® in Electronic Design Automation</i>. 2012.</li> </ol>		
<p><b>Role in project:</b> RiSD 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 Swiss national projects, RiSD will contribute to the exploitation of the project results.</p>		

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

*SUCCESS* is supported by expert teams amongst which are the designers of 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 CPS systems and on developing sensor based technology. See table below:

Teams	Areas of Expertise					
	CPS	Information Confidentiality	Security	Change Management	Human Factors	Healthcare
MU	√		√		√	√
INRIA		√		√	√	
UJF			√			
EPFL	√		√	√		

The focus of *SUCCESS* is to provide resilient trustworthy CPS 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 <i>SUCCESS</i> bring together professionals from bio-engineering, healthcare and from different teachical areas of Computer Science (security, human-centred computing, CPS). 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 complex 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).

## 2.6 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.

## 2.7 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.

## 2.8 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.

**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.

**UJF** 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.

The **RiSD lab at EPFL** is involved in the following two on-going projects related to SUCCESS. In both projects, RiSD is working on BIP-based design flows for the development of software applications and control of the targeted platforms. UltrasoundToGo ([www.nano-tera.ch/projects/359.php](http://www.nano-tera.ch/projects/359.php); funded by Nano-Tera.ch) is another EPFL project. This project intends to develop a high-performance, low-power signal processing platform for ultrasound imaging applications, targeting future 3D portable ultrasound systems. Such imaging devices would be much easier to use also by non-specifically-trained personnel. As for all medical applications, security and privacy are highly important for such systems. Making ultrasound devices operable by non-specifically-trained personnel, brings humans into the centre of such concerns, following precisely the *SUCCESS* scenario. Commelec ([smartgrid.epfl.ch/?q=prn70Commelec](http://smartgrid.epfl.ch/?q=prn70Commelec); funded by SNSF) is also a project at EPFL. This project intends to develop a scalable methodology and reliable tools for real-time control of power flows, integrating intermittent widespread energy sources in distribution networks (smart grids). Commelec distribution networks will be structured hierarchically, with national and/or continental networks at the top level and house sub-networks at the bottom level. Malicious operation of sub-network controllers at any level of the hierarchy could lead to significant breach of security and/or privacy, again closely corresponding to the scenarios considered in *SUCCESS*.

## 2.9 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.

Another cost which has been included in the budget for partners MU, INRIA and EPFL 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:

### Financial Plan

Type	Middlesex University Higher Education Corporation/School of Science and Technology, Department of Computer Science	Institut National de Recherche en Informatique et en Automatique	Université Joseph Fourier/VERIMAG	École Polytechnique Fédérale de Lausanne/School of Computer and Communication Sciences	Project total
Personnel	200278	319700	303835	274006	1097819
Consumables	2700	0	12355	0	15055
Equipment	21539	3000	0	0	24539
Travel	38718	18000	30000	5833	92551
Commissions	0	0	0	0	0
Other	4645	1000	3000	4000	12645
Overheads	212890	0	5769	0	218659
Total costs	480770	341700	354960	283840	1461270
Requested	384616	150942	150000	170106	855665

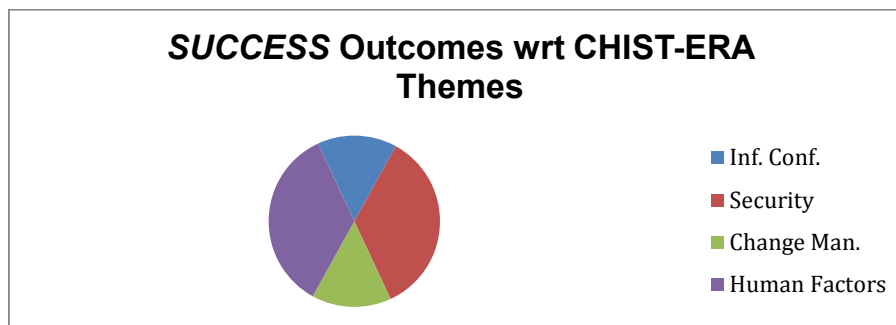


### 3. Impact

#### 3.1 Expected Impacts

Scientifically, the project *SUCCESS* will produce extensions to the BIP methodology to further improve security and integrate human factors, connecting the BIP methodology with modelling of human behaviour for security analysis in Isabelle/HOL. The application of the extended methodology to the scenario of dementia patient monitoring provides a security architecture, a reproducible scientific result in itself.

The impact of the scientific and technological objectives of *SUCCESS* is perfectly aligned with the expected impact of this call and addresses all four themes: Information Confidentiality (15%), Security (35%), Change Management (15%), and Human Factors (35%).



Using formal specification and verification from design through to verification, *SUCCESS* conforms to “highest requirements to quality in terms of resilience, safety, security and privacy.” *SUCCESS* specifically target the themes security and privacy since we start from a human centric security specification of a healthcare infrastructure where privacy interests for vulnerable humans, for example, dementia patients, can be specified. To accommodate “the heterogeneous, evolving and distributed nature of CPS” we extend the “state of the art methods and technology” by extending the successful component methodology BIP including Symbolic Model Checking and code synthesis. *SUCCESS* “copes efficiently with external and internal changes” by considering component technologies suitable for adaptation. We “integrate management, design and deployment aspects” by considering a Pilot security architecture from health care. The pilot is a “well defined use case” that will allow to “quantitatively measure performance”.

**Scientific community impact:** *SUCCESS* will push the importance of resilience of trustworthiness of CPS higher in the agenda of research groups and companies. Our consortium wants to equip teams with a solution, a security architecture which is reproducible for the community, and above this, to install in the community awareness the importance of developing CPS with resilience and trustworthiness 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 PET, 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.



## 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.

## 5 References

- Basu A, Bensalem S, Bozga M, Combaz J, Jaber M, Nguyen T-H, and Sifakis J. Rigorous Component-Based System Design Using the BIP Framework. *IEEE Software*, Vol. 28, No. 3, 2011.
- Basu A, Mounnier L, Poulhies M, Poulu J, Sifakis J. Using BIP and Verification of Networked Systems – A Case Study on TinyOS-based Networks. Sixth *IEEE International Symposium on Network Computing and Applications. NCA, IEEE*, 2007.
- Ben Said N, Abdellatif T, Bensalem S, Bozga M: Model-driven Information Flow Security for Component-Based Systems. In *Proceedings of the ETAPS Workshop 'From Programs to Systems', FPS@ETAPS 2014*: 1-20, 2014.
- Ben Said N, Abdellatif T, Bensalem S, Bozga M: Building Secure by Construction Distributed Component-Based Systems. *Annals of telecommunications*, to appear, 2015.
- Biondi F, Legay A, Malacaria P, Wasowski A. Quantifying Information Leakage of Randomized Protocols. *VMCAI 2013*: 68-87.
- Bludze S, Sifakis J. A Notion of Glue Expressiveness for Component-Based Systems. In: van Breugel F, Chechik M (eds.) *CONCUR 2008*. LNCS, vol. 5201, pp. 508-522. Springer, 2008.
- Boender J, Georgieva Ivanova M, Kammüller F, and Primiero G. Modeling Human Behaviour with Higher Order Logic: Insider Threats. *Socio-Technical Aspects of Security and Trust, STAST2014, co-located with CSF'14 in the Vienna Summer of Logic, IEEE* 2014.
- Evans C, Brodie L, Augusto JC. Requirements Engineering for Intelligent Environments. In *Proceedings The 10th International Conference on Intelligent Environments (IE'14)*, pp. 154-161. Shanghai, 29th of June to 4th of July, 2014. IEEE Press.
- Hutter D, Mantel H, Schaefer I, and Schairer A. Security of Multiagent Systems: A Case Study on Comparison Shopping. In *Journal of Applied Logic*, 2007.
- Jones S, Hara S, Augusto JC. eFRIEND: an Ethical Framework for Intelligent Environment Development. Accepted in *Ethics and Information Technology* by Springer. DOI: 10.1007/s10676-014-9358-1, 2015.
- Kammüller F and Probst C W. Combining Generated Data Models with Formal Invalidation for Insider Threat Analysis, *IEEE Security and Privacy Workshops, SPW, WRIT'14*. 2014. An extended version has been accepted for a Special Issue of the IEEE Systems Journal on Insider Threats.
- Kammüller, F. A semi-lattice model for multi-lateral security, in: *Data Privacy Management, DPM'12, Seventh International Workshop*. Co-located with ESORICS'12, volume 7731 of LNCS, *Security and Cryptology*, Springer, 2013.
- Lüth C, Autexier S; Hutter D; Soeken M; Wille R; Drechsler R. SPECifIC - A New Design Flow for Cyber-Physical Systems. In: *CPS20: CPS 20 years from now - visions and challenges - CyPhERS 2nd Experts Workshop. CyPhERS Experts Workshop*, April 14, Berlin, Germany, 2014.

Mantel H. On the Composition of Secure Systems. In *Proceedings of the 2002 IEEE Symposium on Security and Privacy*, Oakland, CA, USA, pp. 88–101, May 12-15, 2002. IEEE Computer Society.

Mantel H. Reliably Secure Software Systems (RS3) – DFG Priority Programme 1496. <http://www.spp-rs3.de>, accessed December 2014.

Myers A C and Liskov B, Protecting Privacy Using the Decentralized Label Model. *ACM Transactions on Software Engineering Methodology*, Volume 9, No 4, p. 410-442, 2000.

Palamidessi C. Quantitative Approaches to Information Protection. *WoLLIC 2013*: 31-32

Zdancewic S, Zheng L, Nystrom N, Myers A C. Secure Program Partitioning. *ACM Transactions on Computer Systems*. pp. 328-328, 2002.

## 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

### Homerton University Hospital 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 careers 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 Manisha 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-UJF	4-EPFL	Total
T1.1	1				1
T1.2	1	1	1	1	4
T1.3	1				1
T1.4	1				1
<b>Total</b>	<b>4</b>	<b>1</b>	<b>1</b>	<b>1</b>	<b>7</b>

WP2	1-MU	2-INRIA	3-UJF	4-EPFL	Total
T2.1	1	1	2	1	5
T2.2	1		2	1	4
T2.3	1	3	2	2	8
T2.4	2		3	6	11
T2.5	6	7	3		16
<b>Total</b>	<b>11</b>	<b>11</b>	<b>12</b>	<b>10</b>	<b>44</b>

WP3	1-MU	2-INRIA	3-UJF	4-EPFL	Total
T3.1		6	1		7
T3.2	6	4	3	5	18
T3.3		4		5	9
T3.4	6	8	1		15
<b>Total</b>	<b>12</b>	<b>22</b>	<b>5</b>	<b>10</b>	<b>49</b>

WP4	1-MU	2-INRIA	3-UJF	4-EPFL	Total
T4.1	1	1	1	1	4
T4.2	4	1	1	1	7
T4.3	5	1	1	1	8
T4.4	1				1
<b>Total</b>	<b>11</b>	<b>3</b>	<b>3</b>	<b>3</b>	<b>20</b>

WP5	MU	INRIA	UJF	EPFL	Total
T5.1	2	2	2	4	10
T5.2	2	2	2	5	11
<b>Total</b>	<b>4</b>	<b>4</b>	<b>4</b>	<b>9</b>	<b>21</b>

Partner	WP1	WP2	WP3	WP4	WP5	Total
1-MU	4	11	12	11	4	42
2-INRIA	1	11	20	3	4	41
3-UJF	1	12	5	3	4	25
4-EPFL	1	10	10	3	9	33
<b>Total</b>	<b>6</b>	<b>44</b>	<b>49</b>	<b>20</b>	<b>21</b>	<b>141</b>