

# Pervasive Adaptation

## *background document*

### ***Introduction and Motivation***

Prospective advances in microprocessor-, communication- and sensor-/actuator technologies envision a whole new era of computing systems, woven into the “fabric of everyday life”. Information and communication technologies will seamlessly pervade into everyday objects as well as larger systems and infrastructures in our environment, delivering services adapted to the person and the context of their use. Each object will be in contact with larger networks, forming “anyware technologies”, and information on any such object will be available anywhere on planet. Such technologies, which are increasingly intertwined with our daily activities, are becoming ever more distributed, heterogeneous, decentralised and inter-dependent, and are operating more and more in dynamic and often unpredictable environments.

The applications and services that are created with these technologies will need to evolve towards a more implicit and proactive interaction with humans, interacting with the physical world via a variety of sensors and actuators. Instead of developing computer-oriented systems where people have to adapt to the computer we have to develop human-oriented systems into which computers integrate seamlessly. They will have to cope with highly dynamic environments and changing resources. However, while our expectations of the quality of these systems are increasing dramatically, our current methods are not sufficient to deal with adaptive software in a dynamic environment, especially not for large systems with complex interactions.

In the next ten to fifteen years we will have to create human-oriented systems that can cope with the new level of complexity arising from the fact that systems have to operate in large, open and non-deterministic environments: the complexity of interaction and adaptation. Behaviour will often emerge from interactions between independently designed components and not from a single, well-specified entity. Influencing the behaviour of the system and obtaining information will in many cases only be possible by interacting with other systems that may not even exist when the system is designed.

In such foreseeable technology rich environments, the role of content providers and content consumers is being reshaped due to their immense and unprecedented number, and the way they generate, preserve, discover, communicate, trade?, use and abandon information. Consequently, also future pervasive communication systems will have to go beyond the fixed end-to-end connectivity paradigm, considering situations where devices cooperate friction-free and spontaneously in the absence of centralized authentication or name services. There is a need for new communication architectures based on device autonomy, fragmented connectivity, spatial awareness and the data harnessing inside each node that takes part in complex networks.

Besides technology related issues, this will also raise human and social issues. How can security mechanisms be designed so that they cope with dynamic contexts in which threats and user expectations are constantly changing? What kind of systems should be considered to support human life and values, and how should they be designed to fit people's abilities, desires and demands? The

place of the technology-society link in the research agenda is a prerequisite for fruitful technological developments and, moreover, an opportunity for a European approach which is not purely technology driven, but targeted to the goal of improving quality of life.

## ***Vision and Grand Challenges***

Systems developed in the next decades will increasingly have to face a new challenge: a constantly changing networked environment that can no longer be centrally controlled, or even completely understood, by the developer or user. To be successful in such highly dynamic environments, systems have to adapt themselves, taking into account the emergent behaviour of the system. They will have to consider the reaction of the system to their actions, and to achieve their goals they will have to adapt their own behaviour to induce the desired system behaviour. Yet in spite of this adaptation of individual components, the system should still provide guarantees about its behaviour, such as minimal requirements or quality of service.

Instead of users being located at the system boundaries, we will increasingly see *collaborative systems*, i.e., systems that feature complex interactions between people, intelligent objects and computers. Collaborative systems will have to take into account the non-deterministic and often non-predictable behaviour of people. The system cannot simply stop working if a human actor takes some action that the system does not expect or understand. Instead it has to adapt to the new situation.

This leads to an intuitive, unobtrusive and distraction free interaction with technology-rich environments. In an attempt of bringing interaction “back to the real world” after an era of keyboard and screen interaction, computers are being understood as secondary artefacts, embedded and operating in the background, whereas the set of all physical objects present in the environment are understood as the primary artefacts, the “interface”.

Furthermore, this vision involves a ubiquity of heterogeneous, small, embedded and mobile devices, all enabled to communicate in a seamless way with heterogeneous technologies. Their population can self-organise, evolve and interoperate, is able to perceive and interpret their situation locally or via distributed communications, and can overcome the traditional end-to-end paradigm for connections. They take advantage of communication opportunities, use autonomicity in their goal-oriented behaviour, offer services in a dynamic and context-adaptive way, and provide ad-hoc interoperability of services and different modes of user interaction upon those services.

The pervasiveness and adaptiveness of systems that are envisioned pose specific problems for trust, dependability and security. Systems should react to new threats that emerge and to new user expectancies in changed environments. Trust should be established in changing configurations of actors. Lastly, security mechanisms have to be developed for tiny devices that have different needs for trust, dependability and security due to their large numbers, low cost and limited resources.

The following focal points reflect the challenges and milestones that were identified as steps that must be solved towards achieving this vision.

***Networked Societies of Artefacts:*** Future Pervasive Computing landscapes will be manifested by technology rich artefacts and environments, cooperatively attempting goals with society-like behaviour in a highly dynamic context. Going beyond their capability to localize and recognize other artefacts as well as humans and their intentions, societal artefacts will have to form up to “goal tribes”, i.e. ensembles of possibly complementing competencies, to act in a sensitive, proactive, and responsive way according to the perceived and anticipated needs, habits, and emotions of the users. While the social ability of self-managing artefacts is just the demanding prerequisite, the ability to form goal driven interest communities according to societal models is the

potential approach to harness an ever increasing complexity of technology rich living environments. Coordinated goal oriented artefact communities are supposed to be the “interface”, via which humans will ultimately be served.

***Evolve-able Pervasive Systems:*** Pervasive Computing and Communications environments require the systems to grow from their origin driven by their goals. The idea of evolvable systems originated from early research in cybernetics, where evolve-ability is known as “the ability of a population to produce variants fitter than any yet existing” (here it is used for describing a system’s ability to adapt to all possible futures). It has recently experienced a significant upturn through advances in bio-inspired systems and evolvable hardware. The ability to evolve is a key feature as it ensures a seamless integration of future emerging technologies, which might by nature constitute a revolutionary change or radical innovation, but which still has to be able to interface with existing environments to fully exploit the available infrastructures. In order to cope with the continuously changing contexts, conditions, and purpose of their use, systems must become self-configuring, self-healing, self-optimizing and self-protecting, from a hardware and software point of view.

***Adaptive Software Systems:*** The ubiquity of software raises new problems for the maintenance and evolution of programs. The authors of a program cannot foresee all circumstances and every environment in which the software will be deployed or used if the software is part of a large system or interacts with an open environment. Therefore we have to design software that can adapt to different circumstances with limited, or even without, intervention by a developer. Furthermore, we cannot shut down critical infrastructure to perform software upgrades, so we have to find engineering methods that allow us to guarantee that programs can be upgraded or enhanced while retaining their particular adaptations. It is not sufficient for software modifications to be “locally correct”: the whole system has to continue working correctly after some of its components have been modified — even if the environment of the program is so large that we cannot completely understand it, and even if the environment is largely not under the control of the software developer or user. It is currently possible to design and analyse individual components, however there is no reliable way to predict the behaviour of the complete system from the behaviour of the components. Software and system engineering do not offer the theories, methodologies and tools to reliably engineer these systems.

***Adaptive security and dependability:*** Future ICT systems will have to cope with greater complexity, new networking architectures, higher levels of interconnectedness, device heterogeneity, incremental development and mobility of users and devices. The scale, complexity and ever-expanding scope of human activity within this new ecosystem present enormous technical challenges for system security, resilience, dependability and privacy. We currently lack both a conceptual framework and adequate tools to resolve these problems. Traditional security models based on a rigid perimeter defence have failed as they are based on assumptions of closed tightly controlled networks that no longer apply.

There is a need to model and understand the multiple interactions and interconnections among systems, when they all depend on each other. The ecology of these interactions and interconnections needs to be addressed through analysis and techniques for security, dependability and privacy. This includes understanding new risks and threats arising from the dynamic and evolutionary nature of the systems and their environments, and developing self-healing and self-organising capabilities.

This should achieve theories, techniques and architectures, able to cope with the volatile landscape of risks, threats, attacks and context dependent user expectations for privacy and security in evolving and heterogeneous pervasive systems.

***Dynamicity of trust:*** The lack of trust is one of the main barriers for the establishment of a secure and dependable Information Society. Current ICT systems lack a capability for managing and negotiating trust relationships, adapted to the level of security required in a given situation.

The challenge is to obtain a greater understanding of partial trust, security-based trust (where trust follows from security), and trust-based security (where security is achieved through a trusted partnership), and to use this understanding to realise a high level of trust of the citizen in the deployment, economic viability and social acceptance of systems and services.

Based on this understanding, the trust management and access control and policy systems should be created that are flexible enough to understand and accommodate the dynamic nature of trust, allowing for establishing trust relationships between humans and/or machines that jointly act and interact within ad-hoc and changing configurations.

***Tiny and massively networked devices:*** Tiny and massively networked devices will have specific requirements such as energy consumption, and computation power. Current security systems and cryptographic mechanisms require too many resources to be suitable in such devices.

Low-footprint and scalable building blocks should be developed, but also mechanisms and methodologies for assembling these building blocks so that security and privacy properties emerge at the system level; allowing systems to prevail even if some elements are compromised. This includes hardware-based mechanisms, as well as biologically or socially inspired ones.

## ***Source Documents***

Further details can be found in the following documents, several of which were created as part of the "Beyond the Horizon" project, and which together formed a basis for this vision. They are available from <http://cordis.europa.eu/ist/fet/id.htm> (See FET FP7 CLOSED CONSULTATIONS). Please note however that most documents have a wider scope, and not all of the visions and challenges they identify relate to the pervasive adaptation initiative.

***Pervasive Computing and Communication***

***Software Intensive Systems***

***Security, Dependability and Trust***

***Complexity Research***