ICST Transactions
on Ambient Systems

Position Paper ICST.ORG

Living without a safety net in an Intelligent Environment

Juan Carlos Augusto[1,*], Paul J. McCullagh[1], Julie-Ann Augusto-Walkden[2]

[1]University of Ulster, School of Computing and Mathematics, Jordanstown, UK; [2]South Eastern Health and Social Care Trust, Newtownards, UK

Abstract

Computing systems comprise a surreptitious and intrinsic part of our daily life activities. Applications that support humans in daily life facilitate the development of the so-called Intelligent Environments. Like any technology Intelligent Environments can fail. This paper examines potential negative consequences of such systems if they are too naively or optimistically developed and used. The aim of this work is to encourage those contributing to the technical area to reflect on these issues and to provide symbiotic solutions which make such a powerful technical development safer for humans so that it can unfold all its potential to empower future citizens, especially the vulnerable.

Keywords: Ambient Intelligence, Intelligent Environments, safety critical

Received on 20 September 2011; accepted on 20 September 2011

doi: 10.4108/trans.amsys.2011.e6

1. Introduction

Building computing systems that operate safely in the real world is very difficult. Compounded by commercial pressure unreliable systems are sometimes expedited and deployed in the marketplace. Even with the best intentions and state-of-the-art resources it is almost unavoidable that systems contain weaknesses that will lead to failure; evidence has demonstrated that it is not a matter of 'if' but 'when'.

Intelligent Environment systems [1, 2] are inherently complex, because of the need for a symbiotic interaction of hardware, software, human processes. Here we use the term Intelligent Environment to refer as a whole to the infrastructure (Smart Environments [3]) and the software that governs their behaviour (Ambient Intelligence [4]). By their very definition, '... digital environments that proactively, but sensibly, support people in their daily lives'. [5], these systems are conceived to be deployed in the real world to support humans in a variety of supervisory contexts. Some examples of such systems are 'smart' homes, classrooms, cars, offices, manufacturing plants, etc. In some of those applications the artificial system is given an enormous responsibility (e.g. related to safety or well-being).

The magnitude of practical problems to be solved has often concentrated designers' efforts on what to do to get these systems working. Little or no attention is paid to what happens when systems do not behave as anticipated. Nobody wants to announce that their system at some point will fail to deliver as expected, but it is an unavoidable circumstance that will eventually happen. Power cuts occur, sensors sometimes malfunction, sensors can be displaced and hence the quality of the input to the software taking decisions is degraded. Software can contain bugs, software and hardware updates can introduce errors, or rare, unanticipated and potentially unsafe scenarios can occur. Interoperability issues in complex computing and communication environments can lead to unintended consequences. As humans start to experience and benefit from the first successful Ambient Intelligence (AmI) systems supporting their daily activities, it may be unavoidable that the human (traditional) circle of care (family, friends, healthcare professionals) relaxes, invests trust in the system and may not be there when the artificial system fails.

*Corresponding author. Email: jc.augusto@ulster.ac.uk

Consider the requirement of the role of AmI in smart homes [6], in particular providing care for vulnerable people [7]. In the UK for the first time there are more people over the age of 65 years than are under the age of 18 years. More elders have care and support needs, which highlight the need for an affordable system. In England in 2010 £80m was invested in technologies to support preventative care and assist older people to remain in their own homes. In 2011, the Scottish government also has invested significantly in home care. It will spend £10m on a 4-year scheme designed to deploy telehealth systems, which aid treatment of health conditions within patients' homes. The Scottish Assisted Living Demonstrator programme will involve about 10000 people, both the elderly and those with disabilities[1]. This is in spite of a lack of agreement for the cost-effectiveness of such an intervention [8]. However, Gaikwad and Warren [9] demonstrated that home-based interventions applied to chronic disease management improved functional and cognitive patient outcomes and reduced healthcare spending.

Local authorities work with partners in housing, health, voluntary and independent sectors, and with service users and carers, to implement a telecare-based approach. However, technology-based intervention should not be seen as a substitute for meaningful human interactions and interventions, but as a means of enhancing them. Fisk [10] points out that technology is a tool and on its own is neither empowering nor disabling.

Researchers involved in the development of Intelligent Environments have a responsibility to start the discussion on how to design holistically safer systems. Systems (in the broader sense, i.e. the combination of hardware, software, humans and procedures being introduced) should have a responsible attitude towards the environment they serve when they cannot deliver appropriately, and disclose such information in a timely fashion. The AmI community cannot adopt the concept of an 'accident waiting to happen'. A thread of discussion should be opened within our community on the different ways this can be achieved.

However, we begin this debate from a far from perfect human-centric baseline. In the US it has been estimated that up to 98000 people currently die in hospitals each year as a result of preventable medical errors. This exceeds deaths caused by motor-vehicle accidents, breast cancer and AIDS. It is not acceptable for patients to be harmed by the healthcare system whose overarching goal is, 'First, do no harm'. [11]. In the UK approximately 20000–30000 people die as a result of medical errors every year, according to Dr Richard Smith, editor of the British Medical Journal[2]. A rethink of healthcare systems is required to cut the number of mistakes made by medical personnel [12] to the low levels of errors among other safety critical industries such as pilots or nuclear plant workers. According to the chief medical officer, Sir Liam Donaldson, clinical misjudgements or mistakes mean that the odds of dying as a result of being treated in hospital are 33000 times higher than those of dying in an air crash [13]. 'In an airline industry, the evidence ... from scheduled airlines is the risk of death is one in 10 million. If you go into a hospital in the developed world, the risk of death from a medical error is one in 300', he said.

Home healthcare is not without risk, of course. Roback and Herzog [14] considered risks that are encountered when placing electronic equipment in this environment. They found that adverse events could stem from technology itself, from human–technology interaction or from the environment in which the technology is placed. Guidelines aimed at performance improvement complement the more general guidelines on tele-homecare adopted by the American Telemedicine Association. Concerns on the safe development and deployment of these technologies were also clearly raised in [15].

Thus a major new question arises: Will AmI systems make this form of care safer or potentially dangerous?

2. The argument

This section explains why systems can and will most probably fail at some point and exposes the potential negative consequences for the people these systems are supposed to help.

2.1. Hypothesis 1: 'Computing systems DO fail!'

As software practitioners and consumers, we all experience minor faults on a daily basis, due to faulty or poorly developed software. However, the history of Software Engineering is plagued with examples of catastrophic failure made by organizations that have exceptional resources and powerful development teams. For example:

- A Computer-Aided Despatch system for London's Ambulance Service was introduced in 1992. It handled approximately 5000 patients, with over a thousand '999' emergency calls per day. If the position of vehicles was incorrectly recorded, multiple vehicles were sent to the same location; it has been claimed that the occurrence of such an error leads to the death of between 20 and 30 people.
- Intel Pentium processor, released in 1994, was designed to be three times faster for floating point computation than the 486DX chip. However, an error in the lookup table resulted in a component, which was not fit for the purpose. For example, the calculation of ratio 4195835/3145727 yielded 1.3337 and not 1.3338, an error in the 5th significant digit.

[1] www.guardian.co.uk/healthcare-network/2011/mar/16/scotland-spends-10m-transfer-telehealth-techology (accessed September 2011).
[2] http://news.bbc.co.uk/1/hi/uk/682000.stm (accessed September 2011).

- The Ariane 5 rocket, ESA (European Space Agency) was launched on 4 June 1996. Thirty-seven seconds later it self-destructed. An uncaught exception: numerical overflow in a conversion routine resulted in incorrect altitude computed by the on-board computer.
- The Mars Polar Lander was launched 3 January 1999 and lost 3 December 1999. Engine shutdown due to spurious signals gave false indication that spacecraft had landed. Subsequently NASA's Mars Rover freezes (21 January 2004) due to too many open files in flash memory.
- The BMW 3 Series, with 100s of embedded components, was extensively tested but in 1999 a safety recall of over 16000 cars was required due to faults with air-bag control unit—in certain conditions the airbag inflated for no reason. More recently Toyota was forced to recall 180000 vehicles in the UK, due to a failure of the controlled servo braking mechanism. Toyota reported that its biggest-ever safety scare cost the company $2bn worldwide. Honda and Renault also issued recalls recently due to software failures.

The list, of course, is not exhaustive. An open approach where legitimate safety concerns can be raised is required. There is evidence that this is beginning to happen [16] in the health system, allowing safety concerns to be raised by humans. AmI systems require a similar culture of transparency.

2.2. Hypothesis 2: 'The more complex the system the more prone to failure'

Modern computer systems are built as a complex interconnection of specialized modules (Figure 1). As systems become more complex, the potential for failure increases [17]. Therefore Software Engineering has provided important methods and tools in an attempt to increase the reliability in software and computing systems. These include testing, verification and validation as steps that can help developers and users ensure that the right system has been built in the right way. The reader can find a good summary on these approaches in [18, 19]. Even when big companies have specialized teams this is still insufficient to provide 'bullet proof' systems.

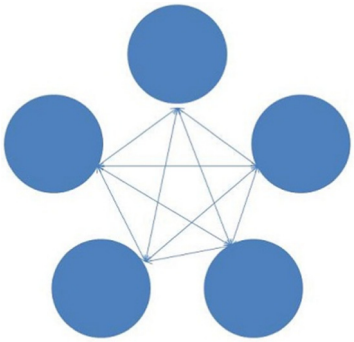


Figure 1. Modern computing systems are constructed as a set of autonomous modules that can interact with each other in various sophisticated ways.

The impact of complexity on reliability can be recognized in all fields. For example, Richard Cook [20] cites 18 reasons why complexity in the medical system can lead to failure. He discusses: '*How failure is evaluated; how failure is attributed to proximate cause; and the resulting new understanding of patient safety*'.

A complex system of relevance is The UK's National Programme for Information Technology, described as 'The Biggest Computer Programme in the World ... Ever!'. Brennan [21] points out that '*apart from the spine, the central repository of electronic health records, there is no single deadline or point of failure, just thousands of local implementations of systems of a type that we really should have got the hang of by now*'. An audit by the House of Commons Public Accounts Committee (14 January 2009) concluded [22]: '*Some systems are being deployed across the NHS. The Care Records Service, however, is at least four years behind schedule, with the Department's latest forecasts putting completion at 2014–15. At 31 August 2008, new care records systems had been deployed in 133 of the 380 Trusts*'. ... '*The estimated cost of the Programme is £12.7 billion, including £3.6 billion of local costs, although this figure remains uncertain*'. By 18 July 2011, a further report from Public Accounts Committee recommended that the DoH consider scrapping the project altogether, rather than continue with the remaining multi-billion pound investment. 'The [DoH] should review whether to continue the programme and consider whether the remaining £4.3bn would be better spent elsewhere'. The complexity of systems that work well in isolation caused delay and uncertainty. The interaction and acceptance of new systems with the people intended to use them was also underestimated.

2.3. Hypothesis 3: Intelligent Environment systems are inherently complex

Intelligent Environments can be developed in any environment where technology can be deployed to assist humans. That infrastructure is supported by a so-called Ambient Intelligence that relates software specifically designed to make decisions based on a sensed reality to the technical infrastructure. This creates a complex interdependence and a reliance on several well-established areas (Figure 2). For example, the system needs *sensors* to gather information from the monitored environment and *actuators* to intervene upon that environment. These sensors are interconnected through a (wired or wireless) network that provides information flows. For an environment to be useful to humans as they move along different

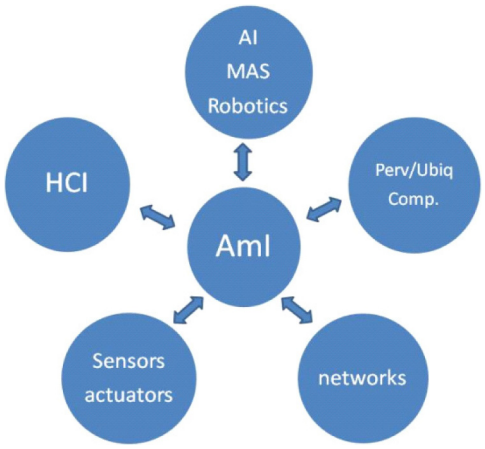


Figure 2. AmI is a multidisciplinary area, each of them highly complex in itself.

areas in their daily living routines, services have to be ubiquitous, i.e. be accessible everywhere and provide services transparently and according to the place and circumstance. These systems require sophisticated algorithms which can adapt to the user and provide appropriate interventions consistent with the user needs and preferences. For a system of this type to be successful it has to provide a subtle interaction with the user so that all the complexity is hidden within the system and the users enjoy the benefits with minimal effort, thanks to a natural interaction (e.g. everyday natural language).

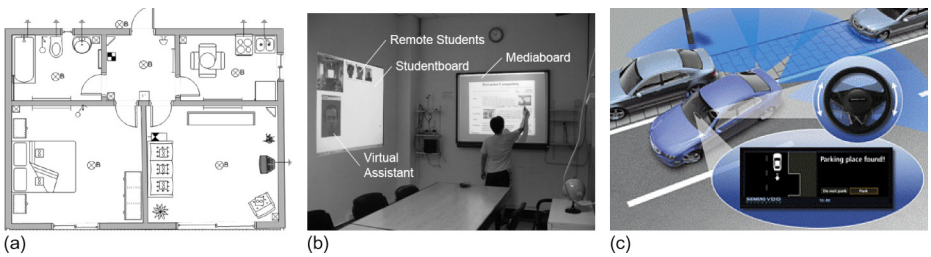
Sensors and actuators can sometimes be occluded, transmit noisy signals or be moved (intentionally or by accident). Networks can sometimes be unreliable and are vulnerable to changes in the infrastructure and to security attacks. Ubiquitous systems can be altered according to changes in the infrastructure or in the tasks the user performs in different places. Artificial Intelligence software can sometimes fail to provide an acceptable answer to some of the difficult problems that it faces. Different users interact differently with machines due to cultural, physical or intellectual differences, therefore there is no 'size that fit all' and it is also very difficult to have very flexible and human-level intelligent interfaces.

2.4. Hypothesis 4: AmI systems support people. Some of this support is critical (there is a potential for human harm or life loss if the AmI system fails)

We can potentially consider a wide range of Intelligent Environments. Some that have been started to be explored are: Smart Homes, Smart Classrooms, Smart Cars, health-related applications in hospitals, public transportation in cities, emergency services, industry, decision support for business and public surveillance. Let us exemplify this step with the first three as exemplars.

Smart Homes. A prominent example of an environment enriched with AmI is a Smart Home; that is a house equipped to bring advanced services to its users. Examples of such technology include movement sensors (Passive Infrared detectors), pull chord switch, thermostat, smoke detector, doorbell indicator, pressure pads, on-off switch detectors, phone and medical devices (e.g. blood pressure monitor, heart monitor, etc.). Examples of enriched devices are electro-domestics (e.g. cooker and refrigerator), household items (e.g. taps, bed and sofa) and temperature handling devices (e.g. air conditioning and radiators). Expected benefits of the application of this technology can be: (a) increased safety (e.g. by monitoring lifestyle patterns or the latest activities and providing assistance when a potentially harmful situation is developing), (b) enhanced comfort (e.g. by adjusting temperature automatically) and (c) better economy (e.g. controlling the use of lights). There is a plethora of sensing/acting technology: stand-alone devices (e.g. smoke or movement detectors), sensors embedded in household objects (e.g. a microwave controller or a bed occupancy sensor) and body-worn devices (e.g. shirts manufactured with electrodes that monitor heart beat, and potentially unsafe conditions). Figure 3(a) illustrates a plan of a house with a typical distribution of sensors.

Recent applications include the use of Smart Homes to provide a safe environment where people with special needs can enjoy a better quality of life. For example, in the case of people at early stages of dementia (the most frequent case being elderly people suffering from Alzheimer's disease) the system can be tailored to mini-



(a) (b) (c)

Figure 3. Intelligent Environments, from left to right: (a) Smart Homes [23], (b) Smart Classrooms [24], (c) Smart Cars (Courtesy of Siemens).

mize risks and ensure appropriate care at critical times by monitoring activities, diagnosing interesting situations and possibly advising the carer when intervention is required. This is a further example of AmI, whereby a message can be generated automatically and sent to carer (who may live remotely) by appropriate technology, such as mobile phone or digital television; the carer's environment of course having sensed the most appropriate delivery channel. Failing to detect an unsafe situation or to deliver a call for help through an appropriate channel at the right time can be critical for the person being cared by the system.

Education services. Universities and higher education institutions are starting to consider the concept of Smart Classrooms [25] where technology such as smart boards, smart sound system capable to recognize and process verbal instructions, and smart cameras which can capture images autonomously are to be shown to students attending a lecture remotely (Figure 3(b)). Twenty years ago lecturers went to the classroom to write the content of the lecture on a board and to explain it. Nowadays lecturers deliver a lecture with the help of slides, the Internet and simulation software. Students can actively participate using interactive boards, and express their response to queries by "voting" on an answer, hence empowering the lecturer and student with information on whether the knowledge has been transferred as intended, all in near real time. If the technology fails then the lecturer will strive to achieve the objectives of that lecture but students may lose significant content (e.g. for those attending remotely it may simply mean they do not have a class that day).

Intelligent cars. Modern cars have dozens of sensors to provide fuel efficiency, improved stability in the vehicle (e.g. better grip at high speed or in difficult weather conditions). More recently some manufacturers started to use sensors that can assist the driver in parking the vehicle by detecting proximity to cars at the front and back of the parking vehicle (Figure 3(c)). These sensors are starting to be used to prevent collisions. A more sophisticated recent development [26] has built a system that allows the car to 'observe' the driver, continuously estimating the driver's internal state and responding appropriately. Observations are focused on hand and leg motions and associated actions (e.g. passing, turning, stopping, car following, lane change or speeding up). This allowed the car to recognize and warn the driver about possible dangers. Other systems are under study that will recognize from the facial gestures and body movements of potentially dangerous situations, for example, the driver falling asleep while driving. Microsoft, among others, employ AmI technologies for driver assistance by providing route planners and customized dynamic route suggestions to bypass congestion [27, 28]. As one of the authors of this article

Figure 4. Current state of the art highlights success while often denying problems.

painfully experienced, a damaged car can easily be the direct result of a malfunctioning sensor during parking. Other failures can have severe consequences (e.g. injury or death).

Having explored the broader scope of AmI in an Intelligent Environment, we will emphasize health–social care applications like the use of Smart Homes for care of the elderly (Ambient Assisted Living).

2.5. Hypothesis 5: The current state of the art on developing AmI systems is not well organized. In particular, it does not contemplate as a standard that the system may/will fail

Marketing focuses on what an intelligent system can do and not so much on its limitations and never on its pitfalls (Figure 4). It is not good advertisement for a company to highlight the potential faults systems may have. Still companies should face this topic unashamedly and show genuine interest on offering good and reliable service. Hence, the concepts of 'mean time before failure' and 'service level agreement' should be considered mandatory for AmI components and systems.

2.6. Hypothesis 6: As humans start to experience the first successful AmI systems supporting their lives the human caring circle relaxes and is not there when the artificial system fails

Current caring systems are human based and rely on professionals from the health system, relatives and friends to care for another human being (Figure 5(a)). Imagine the scenario where an Ambient Assisted Living system is deployed and it works acceptably most of the time to the point that the human carers accept the system and get used to it. As this happens they will feel confident enough to be absent more often (Figure 5(b)); in some extreme cases they may withdraw completely (Figure 5(c)). However, people with dementia, for example, will continue to deteriorate, often challenging the requirements of the original system. This provides the ethical dilemma—living without a safety net in an Intelligent Environment.

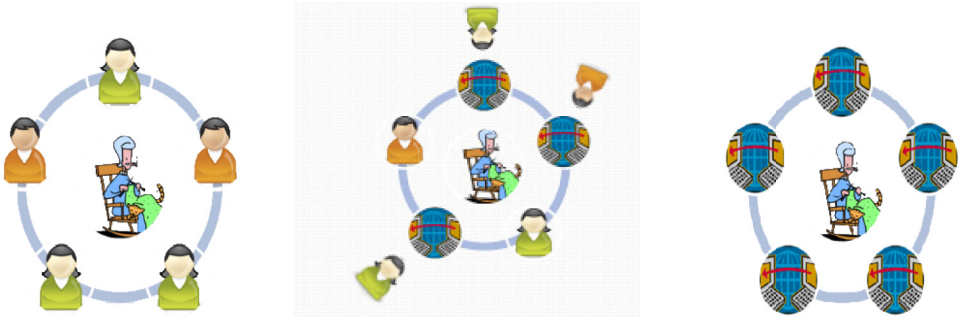


Figure 5. Potential deterioration of human circle of care.

3. Proposed solutions

The obvious and easy thing to say in these circumstances is: '*Systems should not be built to operate alone*', a sort of 'bury your head in the sand' strategy. The problem is people do not necessarily use systems in the ideal form. If a system has been designed to monitor whether an elderly person may have fallen and the system does not work properly, failing to detect or alert to such an occurrence then regardless of the fact that other carers may or not be available is irrelevant and does not exculpate the responsibility of the system; it is still failing to detect or achieve its main objective.

We have already experienced examples from other areas. McLaren recalled baby push chairs in the US during 2009 as some children had their fingers injured in the folding mechanism. McLaren could have claimed that it was not an intended use or they could have applied a warning sticker in an attempt to absolve themselves of responsibility. This solution would not have ameliorated the problem, reduced litigation or built a credible public reputation. For the same reasons car manufacturers (Toyota, Honda and Renault) recalled cars during 2010 because of the suspicion of faulty mechanisms.

There is a need for the community developing Intelligent Environments to adopt a more mature approach to the problem than simply passing the responsibility of problems to the final user. Below there are some suggestions which may be helpful to initiate a much needed discussion on this topic. We recognize that this is not a definitive solution but a starting point for further debate.

3.1. A formal software engineering approach to AmI systems design

Software Engineering uses systematic methods to increase reliability of software. 'Testing' has been used, but testing is limited to probing a system on a few of the many possible situations that can face. Research conducted for decades has matured to produce efficient tools based on Formal Methods which allow the automated analysis of the behaviour of a system in a more rigorous way.

These methods and tools allow for the Verification of Software and Hardware Systems. The most common strategy used is Model Checking which provides tools that development teams can use to increase the reliability and robustness of their software system [17, 18, 29]. This process is time consuming and therefore is mostly applied in the development of high-integrity systems where safety or security is important. Formal methods have been used in industrial applications to address the following:

- Safety, which is a measure of the continuous delivery of service free from occurrences of catastrophic failures.
- Reliability, which is a measure of the continuous delivery of proper service (where service is delivered according to specified conditions) or equivalently of the time to failure.
- Availability, which is a measure of the delivery of proper service with respect to the alternation of proper and improper service.

These criteria are equally relevant to AmI in healthcare. For example, Somerville [19] provides a formal specification to provide a state schema for an insulin pump, which is a safety critical application. Software Engineering Methods used for verification of Intelligent Environments are described in [23, 30, 31].

3.2. The need for enhanced understanding of human–computer (AmI) interaction

Further ethnographic research is required to understand how people interact with these systems and use the information they provide, particularly with regard to safety issues. This is required for the person being monitored, the carer and the healthcare professional. Data may be collected through participant observation, interviews and questionnaires. Human–computer interaction experts can contribute to the knowledge base. For previous work that has highlighted the need for methods of validation by users that combine scientific objectiveness with the

need of allowing the subjective opinion of the final user of AmI systems, see [32].

3.3. A partnership between AmI and human

In a systematic review of the benefits of home telecare for elderly people and those with long-term conditions, James Barlow *et al.* [8] concluded that, the most effective interventions appear to be automated vital signs monitoring (for reducing health service use) and telephone follow-up by nurses (for improving clinical indicators and reducing health service use). There was insufficient evidence about the effects of home safety and security alert systems. However, Barlow concluded that because there was insufficient evidence, this did not mean that those interventions have no effect. However, a key point is the relationship between systems and humans.

Hardware and software should have monitors and reporting built-in. A system of triage may be appropriate. For the most serious errors, the system should conclude that it could cause more harm than good and remove the appearance of a safety net. However for minor errors, it may be possible for the system to work safely with reduced sensors or a faulty software process and continue to work with a reduced capacity. This should be clearly signalled to the users (cared for person, carer and healthcare professional). Where a clean bill of health is given, the system must still monitor the occurrence of unanticipated event that could jeopardize safety.

3.4. The ethical dimension

The British Computer Society (BCS) has drawn up seven general principles of informatics ethics [33], which we

Table 1. Informatics ethics and AmI [33].

Ethical principles	Definition (BCS)	Factors relating to AmI Systems
Information privacy and disposition	All persons have a fundamental right to privacy, and hence to control over the collection, storage, access, use, communication, manipulation and disposition of data about themselves.	The cared for person, where appropriate, should have control over the information that is collected and made available to carers and relatives. Otherwise, a carer should have appropriate access.
Openness	The collection, storage, access, use, communication, manipulation and disposition of personal data must be disclosed in an appropriate and timely fashion to the subject of those data.	The AmI system must be open (so that its decisions can be evaluated), and the information must be made available to the cared for person or their carer.
Security	Data that have been legitimately collected about a person should be protected by all reasonable and appropriate measures against loss, degradation, unauthorized destruction, access, use, manipulation, modification or communication.	Data must be kept securely, particularly as they may be stored for trend analysis and communicated to remote locations.
Access	The subject of an electronic record has the right of access to that record and the right to correct the record with respect to its accurateness, completeness and relevance.	The data collected should be considered no different to other information in the electronic health record.
Legitimate infringement	The fundamental right of control over the collection, storage, access, use, manipulation, communication and disposition of personal data is conditioned only by the legitimate, appropriate and relevant data needs of a free, responsible and democratic society, and by the equal and competing rights of other persons.	Competing rights of other persons must be respected in AmI systems.
Least intrusive alternative	Any infringement of the privacy rights of the individual person, and of the individual's right to control over person-relative data as mandated under Principle 1, may only occur in the least intrusive fashion and with a minimum of interference with the rights of the affected person.	The least intrusive principle applies in AmI systems. This may have particular relevance to the recording (and communication) of images and multimedia data within an Intelligent Environment.
Accountability	Any infringement of the privacy rights of the individual person, and of the right to control over person-relative data, must be justified to the affected person in good time and in an appropriate fashion.	AmI system must be open and accountable for any infringement of the privacy rights of the individual person, e.g. alerting a call centre to wandering behaviour.

believe should be tested in any AmI system. These fundamental principles are evaluated in Table 1 and have added relevance where data are collected and processed by complex algorithms; on vulnerable people, some of whom may be dependent on carers or relatives. In particular, AmI systems should also be accountable for any infringement of the privacy rights of the individual person.

4. Conclusions

AmI researchers have a responsibility to design safer systems, with a high level of transparency. This includes systems that have a responsible attitude towards the environment they serve when they cannot deliver appropriately. Formal specification may provide a means of designing many unsafe conditions out of software. This is time consuming and expensive for normal software, but is important for safety critical AmI applications, and should not be discounted.

It is evident that the hardware and software should be reliable in an AmI system. Thus monitoring is a requirement that is self-testing, periodic checking processes with self-report of possible underperformance, e.g. due to a faulty, misplaced sensor or sensor whose battery may need replacement. It may be possible to provide a system which can continue to reason under uncertainty, but this condition must be identified so that periodic human triage can attend to maintenance issues.

We should strive to ensure that AmI used within an assistive environment should *improve* quality of life. Hence AmI can not only detect alarms, but can become proactive, for example to anticipate abnormal situations and provide guidance for a person under its care. For example, the AmI system could be used to guide a person with dementia back to bed during the night-time, if inappropriate or frequent wandering was detected by location sensors. Context, of course, is important to ensure a proper and sensible decision is made. However, built into this service model, there should always be a human backup. If the AmI system fails to achieve its objective, then a human carer or friend can be alerted (e.g. via a call centre), and appropriate care restored. This means we should not design a system equivalent to Figure 5(c), where the human 'safety net' is eliminated, even by stealth or overconfidence in the system.

The sensitivity and specificity of the AmI system then is a key quality metric. If the number of alerts to the users is reduced then the AmI system will add value. However, they should not be reduced to a point where external human help is needed and not signalled by the system, or beyond which the humans become disengaged.

As the capacity of AmI systems increases, and they become interconnected then Web 2.0 technologies (and beyond) may provide human contact with virtual neighbours, and contact with other AmI systems, to build a community feeling and thus enhance the safety net. This of course raises many societal questions with an ethical dimension. What information should be shared and with whom, and will this always benefit the individual being cared for? AmI, like other services, must adhere to the highest ethical principles in support of the human.

References

[1] Nakashima, H., Aghajan, H. and Augusto, J.C. [eds.] (2009) *Handbook on Ambient Intelligence and Smart Environments* (Springer Verlag).

[2] Cook, D.J., Augusto, J.C. and Jakkula, V.R. (2009) Ambient Intelligence: applications in society and opportunities for AI. *Pervasive Mob. Comput.* **5**: 277–298.

[3] Cook, D.J. and Das, S.K. (2004) *Smart Environments: Technology, Protocols, and Applications* (Wiley).

[4] IST Advisory Group (2001) *The european union report, scenarios for ambient intelligence in 2010*, ftp://ftp.cordis.lu/pub/ist/docs/istagscenarios2010.pdf.

[5] Augusto, J.C. (2007) Ambient Intelligence: the confluence of pervasive computing and artificial intelligence. In Schuster, A. [ed.] *Intelligent Computing Everywhere* (Springer Verlag), 213–234.

[6] Friedewald, M., Da Costa, O., Punie, Y., Alahuhta, P. and Heinonen, S. (August2005) Perspectives of ambient intelligence in the home environment. *Telematics and Informatics* **22**(3): 221–238.

[7] Orpwood, R., Gibbs, C., Adlam, T., Faulkner, R. and Meegahawatte, D. (2005) The design of smart homes for people with dementia—user interface aspects. *Univ. Access Inf. Soc.* **4**: 156–164.

[8] Barlow, J., Singh, D., Bayer, S. and Curry, R. (2007) A systematic review of the benefits of home telecare for frail elderly people and those with long-term conditions. *J. Telemed. Telecare* **13**(4): 172–179.

[9] Gaikwad, R. and Warren, J. (June 2009) The role of home-based information and communications technology interventions in chronic disease management: a systematic literature review. *Health Inf. J.* **15**(2): 122–146.

[10] Fisk, M. Elderly people and independent living: the implications of SMART house technologies. In *Proceedings of British Society of Gerontology Annual Conference.*

[11] Kohn, L.T., Corrigan, J.M. and Donaldson, M.S. [eds.] (2000) *To Err Is Human: Building a Safer Health System.* Published by the Committee on Quality of Health Care in America, Institute of Medicine.

[12] Leape, L., Lawthers, A.G. and Brennan, T.A. (1993) Preventing medical injury. *Qual Rev Bull.* **19**(5): 144–149.

[13] Hall, S. (November 2006) Medical error death risk 1 in 300. *The Guardian*, www.guardian.co.uk/society/2006/nov/07/health.lifeandhealth.

[14] Roback, K. and Herzog, A. (2003) Home informatics in healthcare: Assessment guidelines to keep up quality of care and avoid adverse effects. *Technol. Health Care* **11**: 195–206.

[15] Roberts, J. (2006) Pervasive health management and health management utilizing pervasive technologies: synergy and issues. *J. Universal Comput. Sci.* **12**(1): 4–15.
[16] Dyer, C. (2010) Doctor who was excluded for raising patient safety concerns is entitled to substantial damages. *BMJ* **340**: c739.
[17] Holzmann, G. (2003) *The Spin Model Checker—Primer and Reference Manual* (Addison-Wesley Publishing).
[18] Berard, B., Bidoit, M., Finkel, A., Laroussinie, F., Petit, A., Petrucci, L., Schnoebelen, Ph. *et al. Systems and Software Verification* (Springer Verlag).
[19] Somerville, I. (2007) *Software Engineering* (Addison Wesley).
[20] Cook, R.I. *How Complex Systems Fail* (Cognitive technologies Laboratory, University of Chicago), www.ctlab.org/documents/How%20Complex%20Systems%20Fail.pdf.
[21] Brennan, S. (2005) *The NHS IT Project: The Biggest Computer Programme in the World—Ever!* (Radcliffe Publishing).
[22] House of Commons Public Accounts Committee *The National Programme for IT in the NHS: Progress since 2006. 2nd Report of Session 2008–09 HC 153.* Published by authority of House of Commons: Stationery Office Ltd.
[23] Augusto, J.C. and McCullagh, P. (2007) Ambient Intelligence: Concepts and Applications. *Int. J. Comput. Sci. Inf. Syst.* **4**(1): 1–28.
[24] Shi, Y., Xie, W., Xu, G., Xiang, P. and Zhang, B. (July–September 2003) Project smart remote classroom—providing novel real-time interactive distance learning technologies. *J. Distance Edu. Technol.* **1**(3): 28–45.
[25] Augusto, J.C. (June 2009) Ambient Intelligence: opportunities and consequences of its use in smart classrooms. *Italics* **8**(2): 53–63.
[26] Pentland, A. (2005) Perceptual environments. In Cook, D. and Das, S. [eds.] *Smart Environments: Technologies, Protocols and Applications* (Wiley).
[27] Krumm, J. and Horvitz, E. (2006) Predestination: inferring destinations from partial trajectories. In *Proceedings of 8th International Conference on Ubiquitous Computing*, 243–260.
[28] Letchner, J., Krumm, J. and Horvitz, E. (2006) Trip router with individualized preferences: incorporating personalization into route planning. In *Proceedings of IAAI'06*, 1795–1800.
[29] Abdallah, A.E., Bowen, J.P. and Nissanke, N. (2005) Dependable computing systems: paradigms, performance issues, and applications, part I: models and paradigms, Chapter 9. In Diab, H.B. and Zomaya, A.Y. [eds.] *Wiley Series on Parallel and Distributed Computing* (Chichester: John Wiley & Sons).
[30] Augusto, J.C. Increasing reliability in the development of intelligent environments. In *Proceedings of 5th International Conference on Intelligent Environments (IE09)*, Barcelona, Spain, 20–21 July 2009, 134–141.
[31] Augusto, J.C., Zheng, H., Mulvenna, M., Wang, H., Carswell, W. and Jeffers, P. Design and Modelling of the Nocturnal AAL Care System. In *Proceedings of 2nd Int. Symposium on Ambient Intelligence (ISAmI 2011)*, Springer Verlag, 109–116.
[32] Augusto, J.C., Bohlen, M., Cook, D., Flentge, F., Marreiros, G., Ramos, C., Qin, W. *et al.* (2009) The Darmstadt Challenge (the Turing Test Revisited). In *Proceedings of the 1st International Conference on Agents and Artificial Intelligence (ICAART)*, Porto, Portugal.
[33] BCS Health Informatics Committee *A Handbook of Ethics for Health Informatics Professionals*, http://www.bcs.org/upload/pdf/handbookethics.pdf (accessed September 2011).