Title: Standards and the dependability of electronic assistive technology

Authors: Gordon Baxter, Andrew Monk, Kevin Doughty, Mark Blythe and Guy Dewsbury

Affiliation/address:

Gordon Baxter, Andrew Monk, Kevin Doughty, Mark Blythe
CUHTec
Department of Psychology
University of York
Heslington
York YO10 5DD
Guy Dewsbury
Department of Computer Science
University of Lancaster
Lancaster LA1 4YR

Phone: +44 (0)1904 433170
Fax: +44 (0)1904 433181

E-mail:

g.baxter@psych.york.ac.uk
a.monk@psych.york.ac.uk
dr.k.doughty@btinternet.com
m.blythe@psych.york.ac.uk
g.dewsbury@lancaster.ac.uk

Submission type: Formal paper

Filename: BaxterMonkDoughty.doc

Version of Word used: vX.

Chapter 1

Standards and the Dependability of Electronic Assistive Technology

G.D. Baxter, A.F. Monk, K. Doughty, M. Blythe and G. Dewsbury

1.1 Electronic assistive technologies as critical systems

Electronic Assistive Technology (AT) includes both technology to help people with their daily activities, such as a door entry, and sensors that can raise alarms on detecting a fall or some other incident in the home i.e. home telehealthcare (usually abbreviated to Telecare). Electronic AT is of great economic and social value as it allows people to remain in normal homes when otherwise they would be forced to move to some sort of institutional setting.

Electronic ATs are critical systems in the sense that if they fail there may be resulting injury or distress. A door entry system that locks an older person into their home, or opens the door at random times when interfering radio signals are received will cause considerable distress. A social alarm system that leads someone who has had a fall to believe help is on the way, when it is not, is a danger to life. Given the critical nature of these systems one would expect them to be covered by extensive legislation to enforce high standards of design and manufacture. This paper examines the measures that can be taken in this respect. It can be viewed as preparatory to a survey of current practice which has yet to be carried out and as the beginning of a campaign to encourage more visible evaluation of the dependability of electronic ATs.

1.2 Legislation, standards, codes of conduct and guidelines

It is well established practice in engineering to record guidelines and standard procedures to ensure good design practice and in most companies these are formalised as part of the quality assurance process for a product. Where this is true staff are expected to be able to demonstrate that they comply with these procedures. A company that invests significantly in developing the required knowledge and procedures to ensure dependability of their products will want to demonstrate this to their customers. It is thus in their interest to join with other companies and professional bodies to develop public standards that they can sign up to. Eventually, these standards may become legal requirements upon all manufacturers. EC directives, for example, are implemented as national legislation by individual member countries of the EC. Manufacturers can show compliance with the legislation (where required) by conforming to the appropriate standards which have been developed as a way of promoting perceived wisdom and best practice. Compliant equipment carries a CE marking.

The process of developing and publishing a standard is the business of a standards agency. There are specialist standards organisations, which are national or international such as the British Standards Institute (BSI), and the International Standards Organisation (ISO). Within individual industries, professional organisations also develop their own standards, such as the Institution of Electrical Engineers (IEE) in the UK and the Institute of Electrical and Electronic Engineers in the USA. Trade organisations also exist, such as the Association of Social Alarm Providers (ASAP), who have developed their own code of conduct for the operation of a call centre, with which all of its members should comply. However, these codes of practice tend to be very much less formal in their definition and in measures of compliance. Also, membership of professional and trade organisations is generally not mandatory.

Some standards have been very influential. The ISO 9000 series, for example, are very widely used to demonstrate a systematic quality assurance process. The US military standards (DEF STAN) set the gold standard for risk analysis

In this paper we will examine two approaches to providing standards in the area of electronic AT. One is to develop an overarching standard specifically for this purpose and the next section examines medical devices legislation as a way of doing this. The alternative is to use a variety of standards as they apply to different components of the system. This is examined in section 1.4.

1.3 Medical Devices Legislation and Electronic AT

The Medical Devices Agency (MDA) in the UK was recently made part of the Medicines and Healthcare Products Regulatory Agency. The MDA is largely responsible for implementing the three medical devices directives (The Active Implantable Devices Directive (90/385/EEC), The Medical Devices Directive (93/42/EEC), and The In Vitro Diagnostic Medical Devices Directive (98/79/EC)) under the auspices of the Secretary of State for Health. These were recently implemented in the UK by the Medical Devices Regulations 2002 (SI 2002 No. 618). One of the latest updates (EN60601-1-2:2002) provides an international standard for EMC testing of Medical Electrical Equipment. This is important both because medical devices need to operate correctly in hospital environments that can be quite hostile in terms of interference from other equipment, and because they need to provide very limited electronic 'noise' so that other sensitive equipment may not be disturbed.

If a *manufacturer*, makes a *medical device* and intends *placing (it) on the market*, then the Medical Devices Regulations apply. Each of the italicised terms are defined by the regulations.

> *Manufacturers* are defined in a fairly broad sense. The term includes people who build systems from existing components, with the intention of placing the resultant system on the market. There is one key exception, which is the person who assembles or adapts devices already on the market to their intended purpose for an individual person.
>
> A *Medical Device* is defined as "an instrument, apparatus, appliance, material or other article, whether used alone or in combination, including software necessary for its proper application , which —
>
> a. is intended by the manufacturer to be used for human beings for the purpose of:
>
> i diagnosis, prevention, monitoring, treatment or alleviation of disease,
>
> ii diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap,
>
> iii investigation, replacement or modification of the anatomy or of a physiological process, or
>
> iv control of conception;
>
> and does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, even if it is assisted in its function by such means."

This is a very broad based definition. In its literature the MDA provides an incomplete list of examples of medical devices that includes walking aids, prescribable footwear and "equipment for disabled people". The latter term would seem to embody what many people would describe as assistive technology.

Medical devices are divided into three classes by the Directive. These classes directly relate to the level of risk associated with the device, so Class I devices are those generally regarded as low risk, and Class III devices are those generally regarded as high risk; medium risk devices are divided into two subclasses of Class II. Classification of the devices is determined using a set of rules that form part of the regulations, and there is a fee for obtaining compliance which is about £3,000 for a Class I device. Of course, this fee is but a small part of the cost of employing an engineer to perform a risk analysis, document the risk management applied and submit the application for compliance. There are interesting differences between Europe and the USA where the Food and Drug Administration (FDA) enforces the equivalent legislation, however, in both cases obtaining compliance with this standard is expensive and can be a problem for small start-ups with a single product or large companies with families of devices to register (Mackenzie, 2002). For these reasons companies will look for exceptions that allow them to bypass this legislation. There are also some problems with the associated standard, ISO 14971 – Application of risk management to medical devices. These include a lack of definition of risk management as part of the system quality assurance process, and uncertainties in the ways that risk scoring is performed (MacKenzie, 2002).

As noted above a person "who assembles or adapts devices already on the market to their intended purpose for an individual person" is exempt. This excludes individual installations that may differ from home to home. Devices that are developed within one organisation for use within that same organisation are considered to be exempt, because they are not placed on the market. This means, for example, that systems developed by the medical physics department in an NHS trust hospital for use on patients elsewhere in the hospital are exempt. In addition, to the explicit exemptions, there are grey areas in the regulations. If a person buys a device of their

own volition as an aid to daily living, for example, then it is not normally considered as a medical device. Similarly, there are some devices that can be considered as having a medical role when they are used by disabled people, but can also be used by able bodied people. Such devices are not considered as medical devices. A door entry system, for example, which allows the person in the home to see who is at the door, and remotely open it is obviously very useful for someone with mobility problems. Such systems are also sold to people without mobility problems, so it would not normally be considered as a medical device. More generally, one can claim that if the technology is sometimes used by people without "disease", "injury" or "handicap" then it is not primarily for "diagnosis, prevention, monitoring, treatment or alleviation" of those afflictions and so the regulations do not apply.

Given the major grey areas and exceptions that are embodied within the legislation, the meaning of a CE marking on electronic AT is not at all clear. If the relevant legislation and standards are not easily defined what does it mean to say that the device meets all relevant European legislation. It is thus very difficult for the standards to do their job and demonstrate to customers that a product meets high standards of dependability.

1.4 Alternative Standards for electronic AT

In trying to identify the current standards that apply to electronic AT, the MDA was contacted directly. They indicated that they do not keep a list of the relevant standards. A similar response was also received from the Health and Safety Executive: they do not have any ongoing work relating to the use of electronic AT in the home. There are, however a number of standards that could be applied to different system components.

Figure 1 is a block diagram representation of a typical telecare system. The sensors and the client are shown in a box that represents the home. In addition to the client, the system will normally have at least one other type of user: the person who monitors the client's status through a computer system in a call centre, and may interact with the carer network (social worker, informal carer, GP and so on).

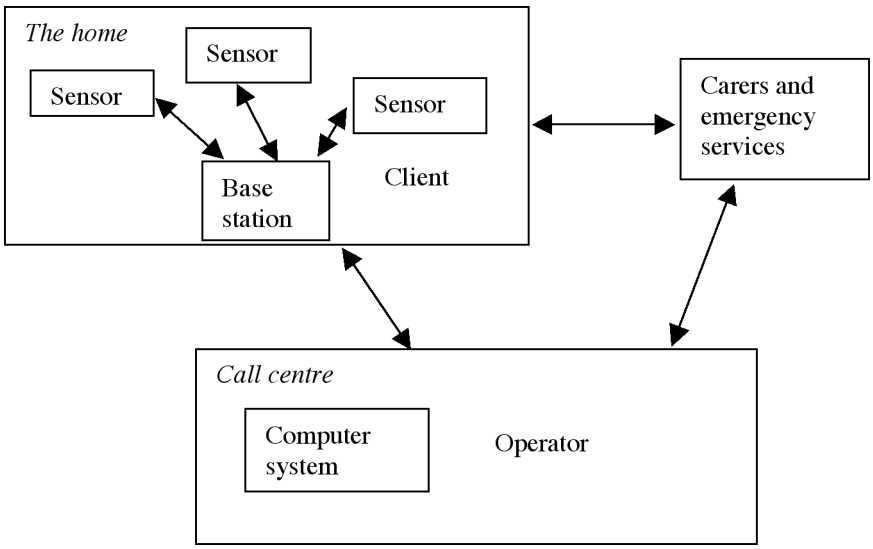

Figure 1.1. Typical telecare system, see text for explanation.

Based on Figure 1, there are three obvious areas where standards exist that could be useful in assessing how good an electronic AT system is: computer systems (the base station in the home and the computer system in the call centre); people (operator, professional carers and emergency services), and infrastructure. There is a plethora of standards available that apply to systems development. The situation has been described as "The Frameworks Quagmire" (Sheard, 1997), since there are at least seven identifiable frameworks, each of which has several associated standards. Fortunately, there does seem to be a gradual evolution towards new frameworks which encompass the best bits from the old frameworks. Sheard's assessment of the situation only addresses systems development in the most general sense. In other words, Sheard does not consider the particular standards associated with the development of safety critical systems.

Given the impetus for a move towards more care being carried out in the home, and the use of various monitoring technologies for medical purposes, it is fairly easy to see that electronic AT systems will take on an increasingly critical role in individual health care. There are some natural parallels here with existing industrial safety critical systems where a culture has evolved which has identified the unique features of such systems, and standards have been introduced to help to assure the quality of such systems (Hone et al, submitted). There are costs associated with the development of critical systems to ensure that they meet the extra, more stringent requirements, although these can normally be justified in a cost-benefit analysis.

The clients will normally be the main users of the system however they are not open to regulation (Dewsbury et al., 2003). There are other identifiable users, however. In some electronic AT systems, there is a monitoring station that allows a carer, for example, to monitor multiple clients. The interface required for the carer will be different to that required by the user. There are existing standards that apply to the selection of people who work as carers. These are beyond the scope of this paper. Similarly, although there are various building standards, these are not discussed here. Neither are the available network cabling and communication standards.

Table 1.1 shows the relationship between the components of dependability and the system components in Figure 1, and where the various standards fit in. It is not intended to be exhaustive, but does give a reasonable picture. A longer list of standards that are (potentially) applicable to the development of an electronic AT system is given in Appendix A. Note that the issue of network communication standards has not been addressed, and basic electrical standards (wiring regulations, radio interference, and so on) are assumed.

It may be apparent that some components of a telecare system (such as the pendant trigger or an automatic sensor (e.g. a bed occupancy device) that has been built on the infra-structure of a social alarm system might also be used in an Environmental Control System used by a disabled and, hence, vulnerable person. Different standards will apply in the two cases. On the one hand, environmental control systems, which are used by little over 4000 people in the UK, must comply with MDA regulations. Social alarms, and extended systems based on them (i.e. 1st generation telecare) need to comply only with the relevant sections of EN50134 which are far less stringent but extremely pertinent to the industry in which they are used. It follows that a manufacturer of components of Assistive Technology devices may need to apply different standards according to the end application. This would be practically impossible and would give manufacturers of the lowest cost elements of AT an administrative burden that cannot be justified. The responsibility for ensuring compliance with the relevant standards should therefore lie with the system integrators, commissioners and installers.

Individual sub-categories of dependability of importance in home technologies in general, and electronic AT in particular, have been enumerated by Dewsbury et al. (2003). A selection of these attributes that are particularly relevant to Telecare are given below, expressed from the end user's point of view:

- Safety: Can I injure myself when using it?
- Reliability and availability: Will it always work when I need it?
- Maintainability: Can it be changed when my needs change without introducing new faults?
- Confidentiality and Integrity: Will it make my data publicly available?
- Usability and learnability: Will I be able to work it?
- Fitness for purpose: Does it meet my real needs?

The categories of systems shown above the thick line in Table 1.1 can be considered as physical systems, in that they can all exist independently of any users and an environmental context. Those systems below the line are socio-technical systems, in which there is at least one set of users, and the systems are all embedded into some context. These systems are essentially the result of installing a physical system into a particular setting. What is clear that maintainability and fitness for purpose are not catered for at all.

Maintainability, being able to modify components or the system as a whole as the client's abilities and needs change, is partly covered in the ASAP code of conduct but the advice given is very informal. Similarly, fitness for purpose, by which we mean "Is the system appropriate to the real needs of the user?" is not covered. Consumer protection law will ensure that a device performs the function specified but is this really the function that the client needs? There is no real advice on how one assesses the real needs of a client in these engineering standards. While their are duties of care for health professionals there is little agreement as to how this should work more generally and little concern with the detailed specification of the equipment prescribed. In general, assessment of clients for electronic AT has been criticised as having a very narrow notion of client need (Hone et al., submitted).

Physical systems	Safety	Reliability and availability	Maintain-ability	Confidentiality and integrity	Usability and learnability	Fitness For Purpose
Component devices (e.g., sensors such as a fall detector, the base station, call centre software and computer)	ISO 13485 ISO 13488 ISO 14971 *IEC 61508?*			IEC 61508 Data Protection Act	ISO 9241 ISO 13407	Not applicable to single device
Communicating components	*IEC 61508?*			IEC 61508 Data Protection Act	ISO 9241 ISO 13407	Not applicable to single device
Socio-technical systems						
Home system + call centre (incl. Operators and Procedures)	BSI EN 50134 *IEC 61508?* ASAP COP Part 1	*BSI EN 50134?* ASAP COP Part 1	ASAP COP Part 1	IEC 61508 Data Protection Act ASAP COP Part 1	ISO 9241 ISO 13407	
Home system + call centre + care support network	BSI EN 50134 ASAP COP Part 1 BS 5979 *IEC 61508?*	BSI EN50134 ASAP COP Part 1		IEC 61508 Data Protection Act ASAP COP Part 1	ISO 9241 *ISO 13407?*	

Table 1.1. Dependability-related standards as they apply to Telecare Monitoring System

The future will undoubtedly see the introduction of more advanced telecare systems, many of which will include physiological alarm sensors such as hypoglycaemia detectors and epileptic fit detectors. These will need to be approved medical devices. Will the remainder of the telecare system i.e. the care phone, the call centre and the telecoms arrangement also need to be MDA approved in order to provide the same level of quality throughout? Second generation telecare involved the data mining of lifestyle information gathered through a variety of sensors, most of which will have been designed and manufactured for security applications rather than for care purposes. This will mean that the entirety of the data set will not be reliable. Should this limit the use of and belief in the outputs of the system? Clearly, a new set of standards will be needed to ensure that errors in measurement do not result in wrong assessments which, in turn, lead to inappropriate levels of care provision being offered.

1.6 Conclusions

As things currently stand, there is no simple way for a system purchaser to easily determine the dependability of an electronic AT system as there is no appropriate single standard it may demonstrate compliance with. One solution would be to modify the Medical Devices Regulations to make them more applicable, either by creating a subcategory within it or a completely new standard. Such a standard has to shut the various loop holes by which manufacturers currently avoid providing a full risk analysis, but at the same time, reduce the costs and practical difficulties that make them seek these loop holes in the first place. For some suggestions about alternative risk analysis procedures see Williams et al. (2000) and Hone et al. (submitted).

Another way round the problem would be for the people who purchase the electronic AT to insist on compliance with multiple standards. This document has shown that, even though coverage is patchy, there are existing standards that can be applied to electronic AT. The drawbacks with this approach, however is that unless a manufacturer is already working to some of these standards, there may be a high cost involved in attaining compliance. It is likely that at least some of this extra cost will be passed on by the manufacturer to the people who purchase the systems or that valuable ideas will not come to market. There may again also be problems of clearly defining what standards are applicable.

Whatever route is taken the need to report failures to a central authority is an important requirement. This authority can then record and track these problems, and where appropriate issue safety bulletins, as the MDA does for other devices at the moment. This probably means establishing a similar reporting scheme for electronic AT, outside of the MDA. Such systems exist in other domains, although there are obvious logistical problems—such as who would run the system, and who would pay for it—none of which appear

insurmountable. Such a system would provide another useful source of data for the designers of electronic AT systems and for those updating the standard.

1.7 References

Dewsbury, G., Sommerville, I., Clarke, K., & Rouncefield, M. (2003). A dependability model for domestic systems. *In proceedings of Safecomp, LNCS*, Springer Verlag.

Hone, K., Monk, A.F., Lines, L., Dowdall, A., Baxter, G., Blythe, M. and Wright, P. (submitted) Risk analysis in the home: enabling people with disabilities and the elderly to live independently.

MacKenzie, D. M. (2002). Medical device risk management, *Proceedings of the 20th International System Safety Conference* . Unionville, VA: The System Safety Society.

Sheard, S. A. (1997). The frameworks quagmire: A brief look, *Proceedings of INCOSE, 1997* .

Williams, G., Doughty, K., and Bradley, D.A. (2000) Safety and risk issues in using telecare. Journal of telemedicine and telecare, 6, 249-262.

Acknowledgements:

Baxter, Monk, Blythe and Dewsbury were supported by the Dependability Interdisciplinary Research Collaboration ("DIRC") funded by UK, EPSRC.

Appendix A

Year	Reference	Title
2001	ISO 13485	Quality systems -- Medical devices -- Particular requirements for the application of ISO 9001
1996	ISO 13488	Quality systems -- Medical devices -- Particular requirements for the application of ISO 9002
2001	ISO 14971	Medical Devices: Application of Risk Management
2002	BS EN 50134-1	Alarm systems. Social alarm systems. System requirements
2000	BS EN 50134-2	Alarm systems. Social alarm systems. Trigger devices
2001	BS EN 50134-3	Alarm systems. Social alarm systems. Local unit and controller
1996	BS EN 50134-7	Alarm systems. Social alarm systems. Application guidelines
2002	ASAP COP	Association of Social Alarm Providers Code of Practice: A Management framework for best practice. Part 1 – Call handling operations
2000	BS 5979	Code of practice for remote centres receiving signals from security systems
1997	DEF-STAN 00-42	Software reliability. Reliability and maintainability (R&M) assurance guides. Part 2: Software.
1997	DEF STAN 00-55	Requirements for safety related software in defence equipment
1997	DEF STAN 00-56	Safety management requirements for defence systems
2000	DEF STAN 00-58	Hazop studies on systems containing programmable electronics
2000	ISO 9001	Quality Management Systems – Requirements
1995	ISO/IEC 12207	Software Life Cycle Processes
1998	ISO 15504	Software Process Assessment (9 parts)
2001	ISO/IEC 9126-1	Software Engineering – Product Quality. Part 1: Quality Model.
1999	IEC 61508	Functional safety of electrical/electronic/programmable electronic safety related systems
1992	RTCA DO-178B/ED-12B	Software considerations in airborne systems and equipment certification
1995	AECL CE-1001-STD	Standard for software engineering of safety critical software
1996-2000	ISO 9241	Ergonomics requirements for office work with visual display terminals (VDTs).
1999	ISO 13407	Human centred design process for interactive systems
1998	DPA	Data Protection Act