The Interaction Between Safety Culture and Uncertainty Over Device Behaviour: The Limitations and Hazards of Telemedicine

C.W. Johnson; Dept of Computing Science, Univ. of Glasgow, Scotland, G12 9QQ.

Keywords: Human Factors, Healthcare, Incident Reporting, Accident Analysis.

Abstract

The introduction of new technology carries with it a degree of uncertainty on the part of system operators. They must match device behaviour to the operating characteristics described during training sessions or within supporting documentation. When operators are uncertain about what their system is actually doing then they frequently resort to coping strategies. This threatens patient safety in many healthcare applications. For example, clinicians often reboot monitoring systems in order to return to a recognized state. This creates problems if the device is left in an inconsistent state on power-up or if critical data is lost when the device is restarted. Conversely, when manufacturers receive reports about adverse events, they often find it difficult to reproduce the error conditions that are described by clinicians and healthcare technicians. These problems are exacerbated when end-users do not fully understand the technologies that they are using. This paper argues that such uncertainty threatens the introduction of 'telemedicine'. We are interested in this class of applications because incident reporting systems are beginning to document a growing number of adverse events that stem from the distributed monitoring and treatment of large numbers of patients. The following pages illustrate this argument using reports submitted to the Food and Drugs Administration (FDA) Manufacturer and User Facility Device Experience (MAUDE) database over the last twelve months. These incidents show that uncertainty about device behaviour can undermine attempts to establish a new 'safety culture' based on communication between clinicians, technician and device manufacturers.

Introduction

The healthcare industries are experiencing rapid change. The deployment and integration of complex, software-controlled systems have revolutionized patient monitoring. For example, new technology has enabled relatively small teams of nurses to monitor larger numbers of patients within adult intensive care units (ICUs). This trend will continue. A chain of medical centres in southeastern Virginia has recently installed a monitoring system that provides a single nurse with a remote overview of up to 49 intensive care patients in 5 ICUs at 3 different centres (Ref. 1). Such developments have immense practical significance given that staff costs account for 50-80% of an ICU budget (Ref. 2).

The introduction of safety-critical technology extends beyond patient monitoring to more active intervention, including programmable infusion systems and surgical robots (Ref. 3). For instance, interim results were recently presented for the first robotic aid approved by the US FDA. Surgeons from the New York Presbyterian Hospital used the da Vinci Surgical System to operate on patients with atrial septal defects. This technology implements a similar relationship between the surgeon and the patient as a pilot has to a fly-by-wire aircraft. There need not be any one-to-one correspondence between the surgeon's gestures and the actions performed by the robot. The device may interpret control actions and perform them in a manner that is tailored to particular procedures, for example in terms of the force used. The surgeon can also access an enhanced 3D 'virtual' display of the site of the operation. The preliminary evaluation of the system found that the average length of hospital stay for the 17 patients involved was reduced from the 7-10 days associated with 'traditional' surgery to only 3 days. It has been argued that these systems will ultimately be combined with network support to enable complex interventions by clinicians who need not be in the same physical location as their patient (Ref. 1).

These innovative applications of new technology must be balanced by an increasing awareness of adverse medical incidents. Observational studies have found that 45% of patients experienced some medical mismanagement and 17% suffered events that led to a longer hospital stay (Ref. 4). It has been estimated that approximately 850,000 adverse events occur within the UK National Health Service (NHS) each year (Ref. 5). A similar study in the United States arrived at an annual estimate of 45,000-100,000 fatalities. This compares with 43,000 fatalities from road traffic accidents and 16,000 from Aids (Ref. 6). The additional care associated with these adverse medical events is estimated at $15 billion. These statistics are typically extrapolations from relatively small samples. They do, however, illustrate the 'headlines' that are being used by politicians to drive new initiatives to improve the safety of national healthcare systems.

The Chief Medical Officer for England, Liam Donaldson, has recently established a centralized reporting facility for adverse incidents across the NHS. The UK Health Secretary Alan Milburn said; "Patients, staff and the public have the right to expect the NHS to learn from its mistakes so we can ensure the alarm bells ring when there are genuine concerns so they can be nipped in the bud" (Ref. 7). Tommy Thompson, the Secretary at the US Department of Health and Human Services, launched a similar initiative in May 2001. He told the Senate Health, Education, Labor and Pensions Committee**: "**(We have) highlighted the need to establish a national focus to create leadership, research, and tools to enhance the knowledge base about safety; to identify and learn from medical errors through mandatory and voluntary reporting systems; to raise standards and expectations for improvements in safety through the actions of oversight bodies, group purchasers, and professional organizations; and to implement safe practices at the delivery level" (Ref. 8).

Both the UK and the US reporting systems are currently under development. In the meantime, precursors of these schemes can provide insights into the problems that are created by the introduction of innovative healthcare technology. This paper focuses on incidents reported to the Manufacturer and User Facility Device Experience database (MAUDE), maintained by the Centre for Devices and Radiological Health (CDRH) within the US FDA. MAUDE is updated every quarter with voluntary reports of adverse events involving medical devices. In particular, the following pages focus on the degree of uncertainty that is being created for the operators of advanced healthcare technologies. This uncertainty has a number of adverse consequences. Many clinicians exploit a range of coping strategies to support their operation of new healthcare technologies (Ref. 9). Users will reboot safety-critical systems in order to return to an initial state that they recognize. This creates problems if the device is left in an inconsistent state on power-up or if critical data is lost when the device is restarted. Device uncertainty also extends beyond clinical end users. The following pages will show how uncertainty about device behaviour also affects medical technicians, manufacturers and device sub-contractors who must all cooperate to support the successful application of these new systems.

Uncertainty over device behaviour also undermines important features of the 'safety culture' that many are trying to establish in modern healthcare systems. For instance, the Institute of Medicine Report 'To Err is Human' argues that "Setting standards, convening and communicating with members about safety, incorporating attention to patient safety into training programs, and collaborating across disciplines are all mechanisms that will contribute to creating a culture of safety. As patient advocates, health care professionals owe their patients nothing less" (Ref. 6). Unfortunately, many of the telemedicine incidents reported to MAUDE demonstrate that healthcare staff and manufacturers experience great difficulty in communicating information about the causes of incidents and accidents. Clinicians often have only a limited understanding of the distinction between normal and abnormal behaviors. In consequence, manufacturers argue that many incident reports have no relevance to patient safety. Healthcare technicians are often confused about the correct way in which to configure complex telemedicine networks. This creates problems when they are themselves called upon to debug network problems by clinical end users. The complexity of these systems coupled with their own confusion can limit the flow of incident information back to device suppliers. Further uncertainty stems from the market structure that has developed in many areas of telemedicine. Incident reports reveal that some manufacturers are uncertain about the intended behavior of the system components that they acquire from third-party vendors.

The incidents in this paper illustrate a paradox. On the one hand, the existence of these reports illustrates significant improvements in the safety culture of many healthcare organizations. On the other hand, many reports reveal the depth of confusion that exists over how complex medical devices should function. All too often end-users, technicians and manufacturers fail to address these uncertainties until after an incident occurs.

Existing Technologies and Past Certainties

Voluntary incident reports do not focus exclusively on the complex, technological systems that we have described in the opening sections. Many adverse events involve more ‘mundane’ devices. The following narrative from the MAUDE system provides an example. A Nurse anaesthetist was working to insert a tube in a patient when the head section of an operating table fell off. The patient was injured but the reporter was unsure of the precise consequences of the adverse event. The following reports preserve the upper case used by the FDA. Lower case is used to denote text that we have introduced to preserve the anonymity of manufacturers, technical support staff and clinicians:

> A TECHNICIAN WAS DISPATCHED… TO INSPECT THE TABLE. THE EVALUATION DETERMINED THAT THE TABLE WAS WORKING ACCORDING TO SPECIFICATIONS, NO COMPONENTS WERE BROKEN…THE CAUSE OF THE EVENT APPEARS TO BE USE OR USER ERROR IN THE FORM OF IMPROPERLY TIGHTENING THE HEAD SECTION THUMB SCREWS. TECHNICIAN DISCUSSED THE IMPORTANCE OF PROPERLY TIGHTENING THE THUMB SCREWS WITH HOSPITAL BIOMEDICAL DEPARTMENT.
>
> **(MDR TEXT KEY: 1506987)**

This report is typical of many incidents where direct forensic checks can be made to identify the causes of any problem. It also illustrates how human ‘error’ is, typically diagnosed if those checks cannot identify any obvious system failures. There is, however, a growing appreciation that analysts must consider the precursors or performance shaping factors that make operator ‘error’ more likely rather than viewing it as a root cause in itself. In this case, attention might focus on the difficulty of ensuring that the head unit was properly secured or the visibility of the mechanism so that clinicians can check it is correctly assembled. It is insufficient to show simply that a device can perform the function that it was designed for. Manufacturers must also show that operators can use the device to perform this function as well. The following report provides an example of this new attitude. The users of a computer controlled infusion device can be confused by a change in the units displayed from micrograms (MCG) to milligrams (MG).

> WHEN USING THE DOSE CALCULATOR FUNCTION FOR A NITROGLYCERIN DRIP, THE PROGRAM CHANGES FROM MCG ON ONE SCREEN TO MG ON THE NEXT SCREEN. A PROVIDER TRYING TO START AN IV INFUSION QUICKLY MAY NOT NOTICE THE CHANGE AND CONTINUE ON PROGRAMMING THE INFUSION. AT THE END THE

> DECIMAL POINT IS NOT EASY TO READ AND THE DOSING ERROR MAY NOT BE NOTICED. THE ERROR DESCRIBED ALLOWS FOR ONLY 10% OF THE DESIRED DOSE TO BE DELIVERED. The Supplier is MAKING SOFTWARE CHANGES TO BE RELEASED THIS SUMMER. (**MDR TEXT KEY: 1128586)**

The previous incident represents a relatively benign problem in the sense that it is easy to detect and relatively easy to rectify. Members of staff were warned about the potential problem and steps were taken to avoid any adverse events before the upgrade was introduced. Many recent healthcare incidents pose more 'wicked' problems. In particular, the introduction of software has complicated both the operation of many clinical devices and the task of identifying the likely causes of adverse events. These issues are illustrated by the following MAUDE incident involving a radiotherapy device. As in previous reports, the incident was detected by vigilant staff but there was considerable difficulty in understanding precisely what had happened and why. A manufacturer provided the following summary after working with the end users to understand what might have happened:

> SINCE THE PLACEBO TREATMENT IS STILL ACTIVE IN THIS VERSION OF SOFTWARE (REVISION 9), IT IS POSSIBLE TO UNINTENTIONALLY DELIVER A PLACEBO TREATMENT. THIS SITE WAS NOT INVOLVED IN ANY OF THE PAST CLINICAL TRIALS … AND IT APPEARS COINCIDENTAL THAT THE reporter USED THIS PARTICULAR PASSWORD… ONE POSSIBLE SCENARIO DICUSSED WAS THE X-RAY TECH OPERATING THE UNIT DURING THIS TIME SOMEHOW MISTOOK THE DEFAULT PHYSICS PASSWORD "9999" FOR "4444", WHICH MEANS THE OPERATOR WOULD HAVE ALSO CONFUSED THE TREATMENT PASSWORD WITH THE PHYSICS PASSWORD. HOWEVER, THIS IS SPECULATION AND COULD NOT BE CONFIRMED. **(MDR TEXT KEY: 1490034)**

There were no long-term consequences for the patient in the previous incident. A series of displays warned the operator of the potential problem. If the placebo password was used to deliver a treatment then the word 'PLACEBO' appeared on the delivery screen. 'PLACEBO TREATMENT – No Radiation delivered' also appeared on an associated treatment summary screen. The operator observed these warnings and the procedure was repeated as normal. Further investigations could not identify any other similar incidents of password confusion at other sites. This incident illustrates the complexity and uncertainty surrounding many adverse events involving healthcare technology. We do not know exactly what caused this incident. Even if we could be clear about the precise sequence of events, it can be difficult to know who was responsible for the mishap. We could argue that this incident stemmed from operator error. They should have been more careful when entering the required password. Additional training might be used to remind operators of the importance of selecting and using appropriate passwords before starting any radiotherapy. It could equally be argued that the development company is responsible. The previous incident provides yet another example of an adverse event caused by the retention of legacy code in production software. Not only were there problems with legacy code. The use of such a simple numeric password for a placebo was likely to lead to problems in the future. This is illustrated by the potential conflict with the default physics password. The physics department might, in turn, also be criticised for their choice of '9999'. This cannot easily be justified as a secure password. A number of commentators have use these complex incidents to argue for a safety culture that looks beyond the association of blame with the various parties involved in healthcare incidents. Instead, each of the previous criticisms should be regarded as an opportunity for learning (Ref. 6). There is a danger, however, that such arguments encourage a retrospective approach to safety. Greater encouragement may be necessary if individuals and teams are to take a more proactive responsibility for identifying potential weaknesses before an incident occurs.

Telemedicine and The Uncertainties of New Technologies

The introduction to this paper has described a vision of future ICU's in which a single nurse can monitor and intervene to support many more patients than is possible in conventional wards. Similarly, we have described moves towards robotic surgery by clinicians who may be many miles away from their patient. This proposed use of software monitoring and control forms part of wider moves towards the introduction of 'telemedicine'. While many people have written about the potential use of these techniques, very few have considered the new hazards that this creates. This is worrying given that many of the recent incidents reported to the FDA are related to the failure of remote monitoring devices in hospital settings. For instance, the following incident is typical of mishaps in which it is difficult to determine why a monitor has failed. Ventricular-Tachycardia (V-Tach) is a dysrhythmia in which the lower chambers of the heart, the ventricles, beat unusually fast. QRS waves are used to monitor ventricular contraction on an ECG machine:

> PATIENT HAD A HEART RATE OF 71 WITH A VERY CONSISTENT, TYPICAL QRS. HOWEVER, BEDSIDE AND CENTRAL MONITORS INDICATED A V-TACH ALARM. ALARM WOULD EXTINGUISH WHEN BEDSIDE MONITOR WAS DISCONNECTED FROM CENTRAL, INDICATING THE ERROR WAS GENERATED FROM THE CENTRAL MONITOR. CYCLING POWER ON THE CENTRAL STATION MONITOR RESTORED PROPER OPERATION. BIOMEDICAL TECHNICIAN ADDS THAT MANUFACTURE HAS ACKNOWLEDGED THAT THIS CAN OCCUR AFTER A PERIOD OF CONSTANT OPERATION AND WITHOUT ANY POWER DOWN TIME. IT CANNOT BE VERIFIED HOW MANY OF THE BEDSIDE MONITORS WERE ON AT THE TIME OF THE DEVICE FAILURE. IT IS THE REPORTER'S UNDERSTANDING THAT THIS TYPE OF DEVICE FAILURE ACTUALLY HAPPENED IN TWO (2) OF THE ICUs AT DIFFERENT TIMES. (**MDR TEXT KEY: 1505404)**

This incident illustrates the problem solving and diagnostic skills that support staff must use in order to identify the potential causes of technical failures in complex, healthcare applications. Only by selectively disconnecting monitors were they able to determine that the problem stemmed from the centralised control system because the local V-Tach alarm on the individual patient monitor disappeared. The reporter's uncertainty over the conditions that might trigger this problem are illustrated by their attempts to describe how many monitors are used throughout the ICUs at any particular time. Further analysis determined that the problem was caused when a V-Tach alarm is suspended at the bedside rather than first being reset. The alarm is then placed in a loop at the central monitor that cannot be cleared. The MAUDE account explains that there was no reference to this problem in the operators' manual but that it was subsequently corrected by an upgrade in the manufacturers' software.

The previous incident illustrates a number of further safety issues that complicate the development of telemedicine. One consequence of the proposed reduction in clinical staff is that there may have to be a corresponding increase in the number of support technicians who must maintain these increasingly complex systems. The following incident illustrates the sorts of problems that these support staff can face when they configure clinical devices. Zymed's EASI^{TM} software provides the data of a traditional, 12-lead ECG with only 5-leads connected to the patient instead of the standard 10-leads. By reducing the number of electrodes and cables it is possible also to reduce the workload for nurses and to improve patient comfort:

> A TELEMETRY TECH NOTED EASI (DERIVED 12-LEAD) DISPLAY ON A CENTRAL STATION FROM A TELEMETRY TRANSMITTER THAT WAS NOT EASI CAPABLE. THE CUSTOMER'S SYSTEM WAS EVALUATED BY THE FIELD ENGINEER AND IT WAS CONFIRMED THAT A TRANSMITTED SIGNAL WAS BEING LABELED AS EASI AT THE

> CENTRAL STATION WHEN IT SHOULD HAVE BEEN LABELED AS A STANDARD ECG. IN ORDER TO TROUBLE SHOOT THE CUSTOMER'S SYSTEM, THE CUSTOMER ENGINEER REPLACED THE TRANSMITTER WITH A NEW ONE AND THEN RELOADED THE SOFTWARE ON THE CENTRAL STATION AND CONFIRMED THAT ALL SIGNALS WERE CORRECTLY TRANSMITTED AND LABELED. THE CUSTOMER DID NOT HAVE A CLEAR UNDERSTANDING OF THE DIFFERENCE BETWEEN STANDARD ECG AND EASI. THE CUSTOMER WAS RETRAINED TO FURTHER THEIR UNDERSTANDING OF THIS DIFFERENCE. AS PART OF THE INVESTIGATION, THE ENGINEERING TEAM CONFIGURED A SYSTEM IN THE SAME SETUP AS IDENTIFIED BY THE CUSTOMER. IT APPEARED THAT THE MAINFRAME RECEIVERS CAN RECEIVE AN INCORRECT BIT THAT MISIDENTIFIED THE TRANSMITTER AS AN EASI CAPABLE TRANSMITTER…
>
> (**MDR TEXT KEY: 1379795)**

This incident again illustrates the uncertainty that faces the users of many healthcare devices. In this case, the 'customer' is reported not to have had a clear understanding of the difference between a standard electrocardiogram and those devices that support Zymed's EASI standard. As mentioned, conventional 12-lead ECGs require 10 electrodes. EASI compatible systems use only five. However, centralised monitors must be equipped with appropriate decoding software to interpret the different formats used by EASI and 'standard' ECG devices. In this case, an apparently rare set of circumstances led to a non-EASI device being recognised as one equipped to run the reduced cable set. It is important to recognise the social implications of such adverse events. In this case, clinicians and their technical support staff must rely on the suppliers' engineering team to explain the technical issues that led to the problem. This seems to be an increasingly common situation in which healthcare providers must rely upon information that is provided by vendors and manufacturers.

Retraining is proposed as a solution to this incident. This shows that the need to move away from individual blame has not been universally accepted across the healthcare industries. The recommended retraining also reveals little appreciation of the systemic causes of human 'error'. The report does not propose more direct measures to prevent the 'rare' circumstances that led to the miss-configuration. This incident also illustrates a key determinant of the successful introduction of telemedicine. Many of the adverse events that we have studied stem from inappropriate 'mental models' of the underlying technology. The integration of heterogeneous systems places new demands on system operators. In particular, they must grasp the many different ways in which their knowledge of existing applications can be changed through integration. In this example, knowledge about how to connect ECG devices through the telemetry system was insufficient to enable technical staff to diagnose EASI incompatibility. More work is required to identify situations in which existing knowledge is insufficient for the installation and operation of new telemedicine applications. Further research must also determine the best ways to help staff gain appropriate mental models to support the operation and maintenance of these systems (Ref. 10).

The previous incident provided a glimpse of the increasingly complex relationships that are emerging between medical device suppliers and the clinicians and technical support staff who must operate them. The following mishap report provides further insights. In this case, end-users made repeated attempts to fix problems that were created by the inadequate cooling of a patient monitor. The account of the problem clearly illustrates the end-user's sense of frustration both with the unreliability of the device and with the manufacturers' response:

> MONITORS LOSE FUNCTIONS DUE TO INTERNAL HEAT…NOTE: SEVERAL OF THE UNITS RETURNED FOR REPAIR HAVE HAD "FAN UPGRADES TO ALLEVIATE THE TEMP PROBLEMS". HOWEVER, THEY HAVE FAILED WHILE IN USE AGAIN AND BEEN

> RETURNED FOR REPAIR…AGAIN SALESMAN HAS STATED IT IS NOT A THERMAL PROBLEM IT IS A PROBLEM WITH X's Circuit Board. SPOKE WITH X ENGINEER…SHE STATED THAT Device HAS ALWAYS BEEN HOT INSIDE, RUNNING ABOUT 68C AND THE X product HAS BEEN RATED AT ONLY 70C…. THIRD DEVICE TRANSPONDER STARTED TO BURN…SENT FOR REPAIR. SHORTLY AFTER THE MONITOR BEGAN RESETTING ITSELF FOR NO REASON…FOURTH DEVICE MONITOR, SPO2 FAILED AND FACTORY REPAIRED 10/01, 3/02. ALSO REPAIRED BROKEN WIRE INSIDE UNIT 12/01. TECH 3/02 SAID THE SYMPTOMS REQUIRED FACTORY REPAIR... (**MDR TEXT KEY: 1370547)**

This incident resulted in a series of follow-up reports. However, the manufacturers felt that the events described by the user could not be classified as safety-related; "None of the complaints reported by the user were described as incidents or even near incidents. The recent report sent to the FDA appears to be related to frustration by the end user regarding the product reliability". Such a response reopens some of the long-running controversy within the software engineering community about the relationship between safety and reliability (Ref. 10).

The manufacturer further responded by describing the evaluation and test procedures that had been used for each of the faulty units. The first had involved the customer replacing a circuit board. This did not fix the problem and the unit was sent back to the factory. The power supply was replaced but no temperature related failure was reproduced under testing by the manufacturers. A second device was also examined after a nurse had complained that the monitor had 'spontaneously' been reset. The hospital biomedical technicians and manufacturers representatives were unable to reproduce the failure mode and all functions were tested to conform to the manufacturers' specifications. The key point here is that end users are not the only people who are uncertain about the causes of device failures and adverse healthcare incidents. Manufacturers and suppliers are also often unable to determine the particular causes of reported mishaps. An important aspect of this confusion is that many telemedicine applications are being developed by groups of suppliers. The marketing of the device may be done by an equipment integrator who out-sources components to sub-contractors. For example, one company might provide the patient monitoring systems while another supplies network technology. This market structure offers considerable flexibility and cost savings during development and manufacture. However, problems arise when incidents stem from sub-components that are not directly manufactured by the companies that integrate the product. Complaints and incident reports must be propagated back along the supply chain to the organisations that are responsible for particular sub-systems. In the previous incident, the integrator/manufacturer believed that some of the problems might have stemmed from a printed circuit board made by another company. This issue was followed up in subsequent investigations. Tests determined that a board malfunction resulted in a failure to display patient pulse oxymetry waveforms on the monitoring system. The problems did not end when the integrator replaced the faulty board. The customer again returned the unit with further complaints that the device would not change monitoring modes. The integrator determined that that the connectors to the printed circuit board were not properly seated. However, the board must have been properly placed prior to dispatch in order for the unit to pass its quality acceptance test. It is possible that the connector was not seated completely during the initial repair and gradually became loose over time.

This previous incident is typical of many recent healthcare incidents. Device repairs and upgrades not only rectify known problems, they can also introduce entirely new hazards. This is further illustrated by the following report. The problem was discovered by the manufacturers' in-house testing programme and affected a version of their central patient monitoring system. As we have seen, these systems are an important feature of telemedicine applications and a source of many recent incident reports:

> IN SOFTWARE RELEASE VF2, IF AN INDIVIDUAL PATIENT IS SET UP IN "AUTOADMIT" MODE, PATIENT PARAMETER DATA IS AUTOMATICALLY COLLECTED OVER TIME AND STORED IN THE SYSTEMS FULL DISCLOSURE DATABASE, IF THE PATIENT IS LATER REMOVED (BUT NOT DISCHARGED) FROM THE ORIGINAL ADMISSION BED/NETWORK LOCATION, DATA COLLECTION IS TEMPORARILY DEACTIVATED (FOR EXAMPLE DURING RELOCATION OR TRANSPORT TO THE LAB). THE PATIENT MAY IN FACT BE DISCHARGED AFTER DISCONNECTING THE MONITOR FROM THE NETWORK. IT IS AT THIS POINT IN TIME; THE PATIENT DATA IS AUTOMATICALLY MOVED FROM FULL DISCLOSURE TO THE COMPANY'S IQUEUE DATABASE FEATURE (AS THIS WOULD ALSO OCCUR WHEN A PATIENT IS DISCHARGED). THE PROBLEM PRESENTS ITSELF WHEN A NEW PATIENT IS ADMITTED TO THIS SAME BED/NETWORK LOCATION, BUT THE ORIGINAL PATIENT WAS NEVER DISCHARGED WHILE CONNECTED TO THAT LOCATION. THE NEW PATIENT ADMISSION BEGINS STORING DATA IN THE FULL DISCLOSURE DATABASE APPROPRIATELY. HOWEVER, IN PARALLEL, THE DATABASE INCORRECTLY BEGINS APPENDING THE NEW PATIENT DATA ON TOP OF THE OLD PATIENT'S DATA RECORD… (**MDR TEXT KEY: 1340560)**

This incident is typical of a growing number of 'wicked' problems that stem from the use of complex system software in telemedicine. This is illustrated by the difficulty of recreating the conditions in which the problem would occur. New data would only be appended if the original patient information were entered in 'AUTOADMIT' mode. The MANUAL ADMIT mode did not exhibit the problem. Similarly, the problem did not occur if the original patient was returned to the same monitoring point, for example after treatment elsewhere in the hospital, providing that no new patient had been entered for that point in the meantime. If the original patient were reconnected to another monitoring point then normal data collection would occur. None of this affected the real-time monitoring alarm system. Even once the company had identified the context in which the incident occurred, further work was required to trace the root causes of the problem. These were identified as a software design problem. In previous versions, all patients were auto discharged and no further data collection could be performed until they were re-connected to another monitoring point. The introduction of the distributed monitoring functionality created significant end-user benefits but at the same time created the opportunity for this relatively complex hazard to arise. The company successfully developed a software patch and has recently begun an update programme to correct all deployed versions of the centralised monitoring system.

Conclusion

This paper has reviewed a series of incidents submitted to the US FDA's Manufacturer and Use Facility Device Experience database (MAUDE) over the last twelve months. This database provides an important source of information about diverse technological failures across the healthcare industries. In the past, many incidents have been relatively simple. For example, we have described ergonomic problems that affect some operating tables. The introduction of software-controlled devices has created additional complexity. This was illustrated by an incident involving the inconsistent use of MCG and MG values on a microprocessor controlled infusion device. Recent initiatives to exploit 'telemedicine' techniques have increased this complexity even further. End-users are uncertain about whether or not particular devices are functioning in the manner intended. Medical technicians are uncertain about some of the distinctions between device protocols that hold between different forms of monitoring equipment. This was illustrated by an incident involving the incorrect configuration of standard ECG devices using EASI protocols. Finally, manufacturers are finding increasing difficulty in replicating the conditions that lead to particular incidents. This is due partly to the inherent complexity and coupling of the devices that they are producing. It is also due to structural characteristics of medical product development where incidents can arise from sub-components that are manufactured by other companies. We would argue that the current drive to create novel system functionality through telemedicine techniques has not been matched by similar initiatives to predict and address the new forms of hazard that are being created by this technology.

A number of caveats can be made about our conclusions. Uncertainty over device behaviour is not restricted to telemedicine. It affects the more general class of healthcare systems. We have, however, been deliberately broad in our interpretation of telemedicine. Some of the incidents that we have cited stem from relatively well-established technology. The irony is that the uncertainties expressed over the behaviour of these systems are likely to be exacerbated by more complex architectures. A more optimistic analysis might argue that many of the problems with existing distributed monitoring and treatment systems will be resolved by future developments. Incident reporting systems, including MAUDE and the systems proposed by the US and UK governments should provide early indications of whether or not this more positive interpretation is correct. In the meantime, however, the relatively few investigations that have been conducted into the hazards of telemedicine are outnumbered by the many proposals for new forms of integrated and distributed functionality.

The title of this paper explicitly linked uncertainty to safety culture. Recent studies have argued that many adverse healthcare events can be avoided through the improved management of safety-critical systems (Ref. 5 and 6). Our work has confirmed this argument. The incidents that we have described show how manufacturers and end-users can cooperate to share information about incidents and accidents. However, our work also points to the inadequacy of safety-culture as a panacea for iatrogenic incidents. For example, most of the adverse events reported in this paper come from large hospitals. These institutions have the resources and staff motivation to encourage voluntary reporting. In contrast, MAUDE receives relatively few submissions from residential care homes even though these institutions operate many of the devices that we know to have failed in other settings (Ref. 10). Further problems remain even if incident reporting and improved safety management can be sustained across the diverse healthcare industries. The previous incidents have shown that end-user uncertainty about device behaviour can prevent them from adequately diagnosing or even describing the context in which an incident occurred. This, in turn, can prevent manufacturers from recreating the causes of an adverse event. Our conclusions, therefore, point to the compounding effect of mutual uncertainty as manufacturers and clinicians attempt to address the causes of those adverse events that follow the deployment of new telemedicine technologies.

References

1. L. Childers, Instant Messengers, NurseWeek, October 2002.

2. Henning, RJ, McClish D, Daly B, Nearman J, Franklin C, and Jackson D. “Clinical characteristics and resource utilization of ICU patients: implications of organization of intensive care.” Critical Care Medicine, 15: 264-269, 1987.

3. M. Argenziano, Robotically Assisted, Minimally Invasive Cardiac Surgery. Technical report from the Minimal Access Surgery Centre, New York Presbyterian Hospital.

4. L.B. Andrews, C. Stocking, T. Krizek, L. Gottlieb, C. Krizek, and T. Vargish. An alternative strategy for studying adverse events in medical care. Lancet, (349):309-313, 1997.

5. NHS Expert Group on Learning from Adverse Events in the NHS. An organisation with a memory. Technical report, National Health Service, London, United Kingdom, 2000. www.doh.gov.uk/orgmemreport/index.htm.

6. L. Kohn, J. Corrigan, and M. Donaldson. To Err Is Human: Building a Safer Health System. Institute of Medicine, National Academy Press, Washington DC, United States of America, 1999. Committee on Quality of Health Care in America.

7. British Broadcasting Corporation (2000). Plan to stop dangerous doctors. News Staff, BBC, London, UK, 13 June 2000. Available at:
http://news.bbc.co.uk/hi/english/health/newsid 788000/788805.stm.

8. T. Thompson (2001), Secretary at the US Department of Health and Human Services statement to the Senate Health, Education, Labor and Pensions Committee, May 24, 2001. Available at:
http://www.os.dhhs.gov/asl/testify/t010524.html

9. R. Randell, An Observational Study of Tailoring in Medical Devices, PhD thesis, Department of Computing Science, University of Glasgow, Scotland, 2003 (forthcoming).

10. C.W. Johnson, The Failure of Safety-Critical Systems: A Handbook of Accident and Incident Reporting, Springer Verlag, London, in press and to appear 2003.

Biography

Prof. C.W. Johnson, MA, MSc, DPhil, CEng, Glasgow Accident Analysis Group, Dept. of Computing Science, University of Glasgow, Glasgow, G12 9QQ, Scotland, UK, telephone - +44 141 330 6053, facsimile - +44 141 330 4913, e-mail – johnson@dcs.gla.ac.uk, URL - http://www.dcs.gla.ac.uk/~johnson

Chris Johnson is Professor of Computing Science at the University of Glasgow. He heads one of the largest research teams specifically devoted to new generations of accident analysis techniques. He helped to author European guidelines for mishap reporting in Air Traffic Management. He has developed an incident analysis scheme for the UK Health and Safety Executive that is specifically designed to support the investigation of adverse events involving programmable systems across the process industries. In 2002, he held a NASA/ICASE fellowship analysing a series of mishaps, including the SOHO mission interruption.