Medical Informatics Europe '96
J. Brender et al. (Eds.)
IOS Press, 1996

A Rigorous Approach To Assessing Medical Device Communication Standards

Phil Curran[†], Kate Norrie[‡] and Mike Spicer[§]

[†]Medical Computing & Informatics,
Royal Free Hospital School Of Medicine,
London NW3 2PF, UK
email:philc@rfhsm.ac.uk
[‡]Computer Science & Electronic Systems,
Kingston University,
Kingston, Surrey KT1 2EE, UK
email: K.Norrie@kingston.ac.uk
[§]Biomedical Engineering,
Royal Brompton Hospital
London

Abstract. In this paper we report on our experience of using formal methods to analyse aspects of a national standard for open systems medical device communications. Mathematical techniques are used to specify aspects of the standard and modal logic is used to validate certain safety-related properties. We discuss how these techniques can increase the confidence of developers and users in specific safety related aspects of a standard prior to testing prototypes. This work has informed comments to the balloting process of the standards committee.

1. Introduction

In this paper we consider real time data acquisition and control in the acute bedside environment. We concentrate on the emerging standards for medical device communications.

In the modern intensive care setting the patient will be connected to a variety of life support and monitoring equipment. Traditionally charting and setting of this equipment has been the responsibility of nursing staff. As the number and complexity of bedside devices increases, IT systems are being introduced to perform charting and control functions.

Integrating different devices into a comprehensive clinical information system requires standardisation of communications protocols between these devices. To extend the integration to devices from various suppliers necessitates an open international standard.

The need for standardisation has been the motivation behind the work of various standards making bodies including the European CEN and the American IEEE. The IEEE have approved several documents, informally known as the Medical Information Bus (MIB) [10,11] of a family of documents comprising a standard for medical device communications. The remaining documents are awaiting ballot approval. CEN is also involved in a similar standards making process which has not yet reached the approval stage.

In order for a standard to be adopted, the clinical community must have confidence that it will fulfil the requirements of the acute care setting. In this paper we describe the use of mathematical techniques, often called formal methods, to rigorously analyse key aspects of standards. The results of this analysis can be used as a criteria to make judgements on the quality of standards and as an objective means of comparison between standards.

2. Medical Information Bus

The distinctive requirements for a system conforming to the MIB are that it should be "plug and play" and that it must be able to cope with frequent re-configuration. Therefore the connection establishment procedures defined by the standard, which deal with these aspects, are of central importance.

The configuration of such a system is shown in figure 1 below. Each patient has at least one bedside communications controller (BCC) and no patient shares a BCC. Numerous devices can be connected to a BCC in a star topology. Each device has its own device communications controller (DCC).

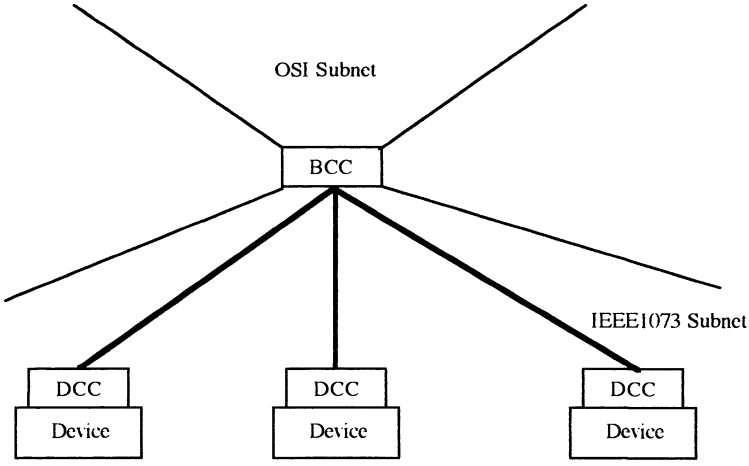

Figure 1 - The MIB Bedside Topology

3. Research Objectives

There is an increasing awareness of the contribution that software can make to safety, or otherwise, of embedded computer systems [2]. This concern has prompted the International Electrotechnical Committee (IEC) to suggest a taxonomy of integrity levels for computer based systems according to their safety critical nature [8,7]. The IEC define five levels of integrity required for systems, ranging from level 0 for non-safety related systems to level 4 for systems at the very high risk end of the safety spectrum. For each integrity level the IEC recommends suitable methodologies and design techniques for system developers. At level 4 formal methods are highly recommended, indeed at this level a system developer would have to make a special case for not using formal methods. Computer based systems for use in intensive care are at the high end of this spectrum.

The primary goal of our research was to investigate the suitability of state of the art formal methods for the critical analysis of standards for medical device communications. We chose to study the MIB because it is the only standard in this area to reach approval by a recognised national body, but our results are applicable to medical device communications standards in general. In the work reported here we have focused on safety critical aspects of the crucial connection establishment phase and applied rigorous techniques to their specification and subsequent analysis.

A secondary goal of this work was to evaluate the effectiveness of formal specification as a means of communicating design concepts within a multi-disciplinary research team.

4. Presentation of Methods

In software engineering the demonstration that a system satisfies certain requirements is usually achieved through a process of testing the final product. The complexity of concurrent systems, such as those defined by the MIB standard, is such that exhaustive

testing is impossible. In this situation mathematical proof becomes extremely valuable. With a formal specification of the system in question, proof techniques can be used to determine the behaviour defined by the specification. Of course, whether or not the final implementation of the software has the desired properties depends on it being consistent with the original specification.

We have formally specified connection establishment services of the Data Link layer as described in the standards documents. The specification was generated directly from the state tables and accompanying text of the standard. We have used the formal specification language LOTOS, a Formal Description Technique (FDT) which is itself an ISO standard [9]. The Language of Temporal Ordering Specification (LOTOS) was developed for the formal description of OSI standards. Although its design grew out of the requirements and experience of work on OSI standard protocols, LOTOS has become widely used as a general specification language for concurrent or distributed systems. Our LOTOS specification may be found in [3].

Having produced the formal specification we are able to prove that it has certain properties. We now give an example of the type of properties that we are able to demonstrate.

Many medical devices are programmed to raise an alarm if the physiological data that they monitor passes some defined threshold. These alarms are intended to attract the attention of nursing or other clinical staff to what is deemed to be a state of the patient that requires urgent management. For the MIB these alarms will rely on the establishment of a connection between the medical device and the patient care system via the bedside communications controller. To communicate any data, including alarms, in its simplest form the medical device is dependent on the BCC polling the device DCC at regular intervals. An alarm will be communicated in the same manner as other data. If an alarm is not communicated or there is an extreme delay in communicating an alarm, then a hazardous situation for the patient ensues. Therefore we wish to ensure that the system cannot reach a state in which the above dangerous scenario can ensue. In order to express this condition, i.e. that the system can never be in such a state, as a safety-related property, we need to identify the relevant states and sequences of events or actions of the MIB system. These events will include message exchanges between BCC and DCC protocol entities.

The MIB standard defines events and actions such as the following:

- *connection confirm*, to indicate the establishment of a connection between a BCC and DCC;
- *disconnect confirm*, to indicate the loss of connection between a BCC and DCC;
- *data request*, to indicate the sending of a frame of data by a BCC or DCC;
- *data indication*, to indicate the receipt of a frame of data from a BCC or DCC;
- *poll timer*, to indicate the passing of a fixed time period since a BCC last communicated with a DCC.

Using these actions we may formulate a safety-related property that captures the requirement that the system will be live, and providing a connection is maintained between a BCC and DCC, then if a device has data to send then within a fixed duration of time the bedside controller will be in a state where it is waiting to receive it. Here it is in English:

> The system has the enduring property that; some action is possible, and also whenever a connection confirm to a medical device happens, and subsequently whenever the poll timer expires and the device executes a data request (in either order) then the following property holds; the bedside controller may receive information from the device via a data indication action and no action other than this or a disconnect indication is possible.

To express the above safety property we need to use a meta logic. We have used the modal-mu calculus described in [6]. This requirement is then expressed in the modal-mu calculus as shown in figure 2 below. The use of a modal and temporal logic allows us to reason about the LOTOS specification, and in particular to automate the proof.

$$\nu Z.\left|\begin{array}{l}\langle Act\rangle Z \wedge [dsap!\,DL\_Cconfirm] \\ \left|\begin{array}{l}[poll][dsap!\,DL\_DATArequest]\left(\begin{array}{l}\langle bsap!\,DL\_DATAindication\rangle tt \wedge \\ [K]ff\end{array}\right) \\ \wedge [dsap!\,DL\_DATArequest][poll]\left(\begin{array}{l}\langle bsap!\,DL\_DATAindication\rangle tt \wedge \\ [K]ff\end{array}\right)\end{array}\right.\end{array}\right.$$

where $K = Act \quad \{bsap!\,DL\_DATAindication, dsap!\,DL\_Dindication\}$

Figure 2 - Modal-Mu Calculus Expression Of Above Safety Property

We have also constructed proofs that show internal consistency of aspects of the protocol. Specifically we have shown that high level descriptions of the intended services to be offered to higher layers of the protocol are consistent with the more detailed descriptions of how these services are implemented by the lower layers. An example of such a verification is given in [5].

All of the analysis that we have undertaken is too complex to be performed by hand, and so we have used automated tool support. There are two major techniques underlying computer based tools capable of such tasks: term rewriting and model checking. Each approach has its advantages and we have found that a mixture of the two techniques provides the most efficient method of automated analysis. The specific tools that we have used are; the Larch Theorem Prover [4], the Edinburgh Concurrency Workbench [12] and the LOTOSPHERE Lite tools [1]. All of these tools are in the public domain and are available for a wide range of computer hardware and operating systems.

5. Results and Discussion

In this paper we have discussed how formal description techniques and modal and temporal logic can be used to analyse a standard for medical device communications. We have shown how important safety-related properties hold for a formal specification developed from the original non-formal standard document. The insights of this work have informed comments on draft proposals made both to the standards committee and the balloting process for the MIB standard.

Our experience has been that at the very least the use of rigorous techniques has increased our understanding, and therefore our confidence in the standard. Of course there are many aspects of this type of standard that are not easily captured using these techniques, such as timing considerations. We are therefore also actively involved in developing MIB compliant prototypes. The clarity of the formal specification has assisted greatly in building these prototypes. The prototypes are being implemented in Standard ML of New Jersey (SML) on UNIX workstations, and this approach is proving to be complimentary to the formal one.

We have also found that the LOTOS specifications are comprehensible by our entire team, including the people who are not experts in these mathematical techniques.

So far only basic aspects of the standard have been analysed. We have chosen to concentrate initially on some of the unique and safety-critical features of the MIB. We are currently extending our work to include elements of the protocol which relate to data error detection, flow control and other management issues. There is much scope for further analysis, for instance to cover other aspects of alarm monitoring and interrupt driven devices.

We believe that the adoption of an international standard for medical device communications will bring about significant benefits for intensive care treatment. The higher the quality of such a standard the greater will be the resulting benefits for the provision of intensive care. It is vital therefore that all possible measures are taken to ensure the highest possible confidence in systems conforming to such standards. For the reasons outlined in this paper the authors believe that the application of formal methods to the rigorous assessment of standards is one important measure which can contribute towards achieving this confidence.

6. References

[1]. Caneve, M. and Salvatori, E., *Lite User Manual*, LOTOSPHERE Consortium, v3.0, March, 1992.

[2]. Leveson, N.G. Software safety in embedded computer systems. *Communications of the ACM 34*, 2 (February 1991), 34-46.

[3]. Norrie, K. and Curran, P. Using Formal Methods To Enhance The Quality Of A Standard For Medical Device Communications. In *FORMAL METHODS IN SOFTWARE PRACTICE*, ACM, ACM SIGSOFT, Jan. 1996, pp. 132- 140.

[4]. Garland, S.J. and Guttag, J.V. Proc. Rewriting Techniques and Applications, 3rd International Conference. *Lecture Notes In Computer Science 355*(1989), 137-151.

[5]. Curran, P. and Norrie, K. An Approach to Verifying Concurrent Systems - A Medical Information Bus (MIB) Case Study. In *Computer- Based Medical Systems*, IEEE, IEEE Computer Society Press, 1992, pp. 74-83.

[6]. Stirling, C. *Modal and temporal logics*, Oxford University Press, Vol. 2, Handbook of Logic in Computer Science (1992)pp. , 478--551, Chapter 5.

[7]. *Functional safety of Programmable Electronic systems; generic aspects - Part 1:General requirements (IEC SC65A/WG10/216(A)*, International Electrotechnical Commission, .

[8]. *Software for Computers in the Application of Industrial Safety related Systems (IEC SC65A/WG9)*, International Electrotechnical Commission, .

[9]. *Information Processing Systems - Open Systems Interconnection - LOTOS - A formal Description Technique Based on the Temporal Ordering of Observable Behaviour*, ISO/IEC JTC 1/SC 21, August 1988, .

[10]. *Standard for Medical Device Communications -Transport Profile - Connection Mode*, IEEE Standards Department, Dec. 1994, .

[11]. *IEEE Standard For Medical Device Communications - Physical Layer Interface - Cable Connected*, IEEE Std 1073.4.1-1994, Dec. 1994, .

[12]. Moller, F., "The Edinburgh Concurrency Workbench (Version 6.1)," , Technical Note, no. LFCS-TN-10, October 1992.