REQUIREMENTS SPECIFICATION

The control software for an automated insulin pump

CSc 365 Critical Systems Engineering 2002

1. Introduction

This specification defines the operation of control software for a portable, automated insulin pump which is used by diabetics to administer insulin as required. In simulates the action of part of the pancreas, an internal organ that manufactures insulin.

Diabetes is a medical condition where the body does not manufacture its own insulin. Insulin is used to metabolise sugar and, if it is not available, the person suffering from diabetes will eventually be poisoned by the build-up of sugar. It is important to maintain blood sugar levels within a safe range as high levels of blood sugar have long-term complications such as kidney damage and eye damage. These are not however, normally dangerous in the short-term. Very low levels of blood sugar (hypoglaecemia) are potentially very dangerous in the short-term. They result in a shortage of sugar to the brain which causes confusion and ultimately a diabetic coma and death. In such circumstances, it is important for the diabetic to eat something to increase their blood sugar level.

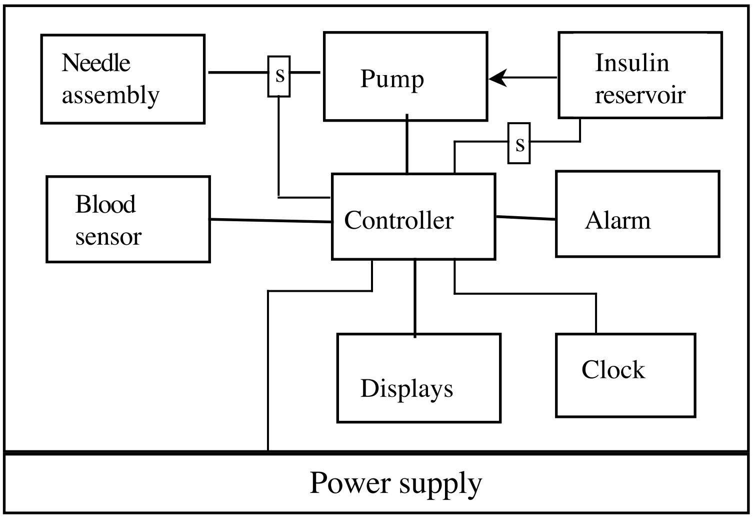
Most diabetics are currently treated by injections of insulin 2 or 3 times a day but this leads to peaks and troughs in their level of insulin. A portable insulin pump measures the level of blood sugar at regular intervals and delivers doses of insulin depending on the actual level of sugar in the blood. This will lead to a situation where the sufferer’s blood sugar levels are much closer to those of people without diabetes. The complications and long-term effects of diabetes can therefore be reduced.

The system measures the level of blood sugar every 10 minutes and if this level is above a certain value and is increasing then the dose of insulin to counteract the increase is computed and injected into the diabetic. The system can also detect abnormally low levels of blood sugar and, if these occur, an alarm is sounded to warn the diabetic that they should take some action.

2. The insulin pump hardware organisation

An insulin pump is a safety-critical system which is used to deliver regular doses of insulin to diabetics.

A block diagram of the insulin pump assembly is shown below. Note that the small boxes marked *s* indicate a sensor.



Needle assembly
Connected to pump. Component used to deliver insulin into diabetic's body.

Sensor
Measures the level of sugar in the patient's blood. The input from the sensor is represented by *Reading?* in the following specification.

Pump
Pumps insulin from a reservoir to the needle assembly. The value representing the number of increments of insulin to be administered is represented by *dose!* in the following specification.

Controller
Controls the entire system. This has a three position switch (off/auto/manual) plus a button to set the number of units of insulin to be delivered (1 unit per press). Moving the switch to the manual position causes the blood sugar measurement and automated insulin delivery to be disabled but information is maintained about the amount of insulin delivered and the reservoir capacity.

Alarm
Sounded if there is some problem. The value sent to the alarm is represented *alarm!* in the following specification.

Displays
There are 3 displays. These displays are represented by *display1*!, *display2*! and *clock!* in the following specification. *display1!* displays system messages, *display2!* shows the last dose of insulin delivered and *clock!* shows the current clock time.

Clock
Provides the controller with the current time. The system clock is initialised when the machine is installed and the start time of each 24-hour period is set at midnight each day using a hardware interface on the machine. For safety reasons, the clock cannot be altered by system users.

3. Requirements for the insulin pump

This specification is a specification of the requirements for the control software for the insulin pump. It is NOT a complete system requirements specification for the pump itself or even all of the software associated with the pump. In particular, it does not include a specification of the self-testing operations or a specification of the hardware interfacing.

The requirements for the insulin pump are specified in natural language and partially in the Z specification language. Z is not ideal to express all requirements but is useful when precise descriptions are required. In all cases, the Z specification should be considered as an annotation that provides detailed information which augments the natural language specification.

3.1. The dose of insulin to be delivered shall be computed by measuring the current level of blood sugar, comparing this to a previous measured level and computing the required dose as described in 3.3 below.

3.2. The system shall measure the level of blood sugar and deliver insulin if required every 10 minutes.

3.3. The amount of insulin to be delivered shall be computed according to the current sugar reading as measured by the sensor:

3.3.1 If the reading is below the safe minimum, no insulin shall be delivered. See schema SUGAR_LOW.

3.3.2 If the reading is within the safe zone, then insulin is only delivered if the level of sugar is rising and the rate of increase of sugar level is increasing. The amount of insulin required is defined in the schema SUGAR_OK.

3.3.3 If the reading is above the recommended level, insulin is delivered unless the level of blood sugar is falling and the rate of decrease of the blood sugar level is increasing. The amount of insulin required in this case is defined in the schema SUGAR_HIGH.

3.3.4 The amount of insulin actually delivered may be different from the computed dose as various safety constraints are included in the system as defined in the schema RUN. There is a limit on the maximum dose to be delivered in a single injection and a limit on the total cumulative dose in a single day.

3.4. Under normal operating conditions, the system is defined by the schema RUN.

3.5. When operating in manual mode, the system is defined by the schema MANUAL.

3.6. The controller shall run a self-test program every 30 seconds. This shall test for the conditions shown in Table 1 below. The self-testing of the system is defined by the schema TEST.

3.7. When switched on, the system is initialised as defined in the schema STARTUP.

3.8. The system shall maintain three displays:
display1! is a text display that shows system messages. It has an associated hardware buffer that can hold several messages. When there is more than 1 message in this buffer, each message is displayed for 5 seconds until all messages have been displayed. The display sequence then restarts with the first message. Hence, several messages may be specified for display on *display1!*.
display2! shows the last dose of insulin that was computed.
clock! displays the current clock time.

Alarm condition	**Explanation**
Battery low	The voltage of the battery has fallen to less than 0.5V
Sensor failure	The self-test of the sugar sensor has resulted in an error
Pump failure	The self-test of the pump has resulted in an error
Delivery failure	It has not been possible to deliver the specified amount of insulin (e.g. the needle may be blocked or incorrectly inserted)
Needle assembly removed	The user has removed the needle assembly
Insulin reservoir removed	The user has removed the insulin reservoir
Low insulin level	The level of insulin is low (indicating that the reservoir should be changed).

Table 1: Error conditions for the insulin pump.

3.9. The user may replace the insulin reservoir with a new reservoir at any time. The design of the reservoir compartment is such that only full reservoirs holding 100 ml of insulin may be inserted. When a new insulin reservoir has been inserted, the system is reset according the RESET schema.

3.10. At the beginning of each 24 hour period (indicated by clock =00:00:00), the cumulative dose of insulin delivered is reset to 0.

3.11. The error conditions that should be detected and indicated by the system are shown in Table 1.