An example of a critical system

- A personal insulin pump for people suffering from diabetes
- This will be used as an illustrative example throughout the course

Medical systems

- More and more medical instruments now include embedded control software.
- These software systems are often critical systems as a patient's life (or at least their health) may depend on the correct and timely functioning of these systems
- The systems themselves are often relatively small and are therefore understandable unlike, for example, industrial control systems

Many safety-critical systems such as the control system for a chemical plant or a nuclear reactor, the control software on aircraft, etc. are not price sensitive. That is, they are part of larger installations that are very expensive and that are produced in relatively small numbers. Therefore, adding to the cost through redundant hardware and software is not usually a problem.

Medical devices, on the other hand, are often mass-produced devices and so have to be price-sensitive. Furthermore, they are often portable devices and so are weight sensitive and power-sensitive. They are battery powered rather than mains powered.

All of this has implications for the hardware and software. The chip count must be minimised as chips add weight, cost and power drain. There is unlikely to be scope for hardware replication and software redundancy.

Diabetes

- People with diabetes cannot make their own insulin, a hormone that is normally secreted by the pancreas. Insulin is essential to metabolise sugar and hence generate energy
- Currently most diabetics inject insulin 2 or more times per day, with the dose injected based on readings of their blood sugar level
- However, this results in artificial blood sugar fluctuations as it does not reflect the on-demand insulin production of the pancreas

Current practice for diabetes control relies on the sufferer measuring the level of glucose (sugar) in their blood then using their experience to judge how much insulin they should inject. They have to make predictions of how their future level of blood glucose will be affected by planned meals, exercise, etc.

Failure to control blood sugar can result in a number of nasty side-effects such as blindness, kidney failure, heart disease and circulation problems.

For reasons that are almost certainly related to current lifestyles, the number of diabetics in the population has increased significantly over the past few years. It has been estimated by the World Health Organisatation that:

“Diabetes cases in adults will more than double globally from 143 million in 1997 to 300 million by 2025 largely because of dietary and other lifestyle factors. “

A personal insulin pump

- A personal insulin pump is an external device that mimics the function of the pancreas
- It uses an embedded sensor to measure the blood sugar level at periodic intervals and then injects insulin to maintain the blood sugar at a ‘normal’ level.
- I will draw on this example at various points in the course to illustrate aspects of critical systems engineering

Personal insulin pumps are currently beyond the ‘state of the art’ although I believe that larger-scale devices of this type have been developed for use in hospitals.

The key difficulty (I suspect) in developing such a system is that blood sugar sensors are invasive and there are probably problems with infections in developing such a system. In future, it may be possible to measure blood sugar level by looking at secretions on the skin and this would then make automated pumps possible.

Personal insulin pumps are available but these are not ‘smart’ systems and they rely on users to make decisions about how much insulin to inject and when to inject it. To read more about them, see:

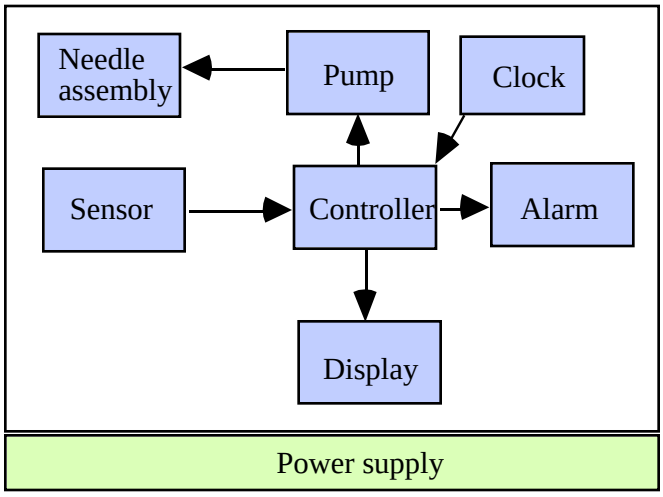
http://www.minimed.com/files/how.htm

Critical system attributes

- Availability
  - It is important that the system should be available to deliver insulin when required
- Reliability
  - It is important that the system performs reliably and delivers the correct amount of insulin to compensate for the current level of blood sugar
- Safety
  - A system failure that resulted in excessive doses of insulin being delivered could threaten the life of the user

You could also argue that security is an attribute as you wouldn't want someone apart from the individual sufferer using the machine. However, this is a fairly unlikely scenario so I haven't considered it in the example.

Insulin pump components



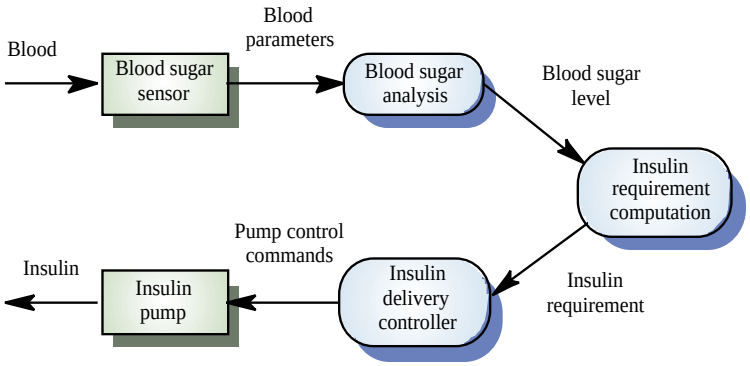
The arrows in this diagram means that there is some communication between these components. The controller is a software component.

In fact, as we shall see later, the system has two displays plus buttons that signal the controller to take certain actions.

The pump delivers a single increment of insulin on receipt of a signal pulse from the controller. Therefore, to deliver 6 insulin increments, 6 pulses are sent to the pump unit. The pump unit includes a pressure sensor so that if the needle assembly is blocked then insulin delivery will be halted

Insulin delivery system

- Data flow model of software-controlled insulin pump



Concept of operation

- Using readings from the embedded sensor, the system automatically measures the level of glucose in the sufferer's body
- Consecutive readings are compared and, if they indicate that the level of glucose is rising (see next slide) then insulin is injected to counteract this rise
- The ideal situation is a consistent level of sugar that is within some 'safe' band

Sugar levels

- Unsafe
  - A very low level of sugar (arbitrarily, we will call this 3 units) is dangerous and can result in hypoglaecemia which can result in a diabetic coma and ultimately death.
- Safe
  - Between 3 units and about 7 units, the levels of sugar are ‘safe’ and are comparable to those in people without diabetes. This is the ideal band
- Undesirable
  - Above 7 units of insulin is undesirable but high levels are not dangerous in the short-term. Continuous high-levels however can result in long-term side-effects

Insulin injection

- The decision when to apply insulin does NOT depend on the absolute level of glucose that is measured in the sufferer's blood.
- The reason for this is that insulin does not act instantaneously and the change in sugar level does not simply depend on a single injection but also on previous injections
- A more complex decision based on previous levels and rate of change of sugar level is used

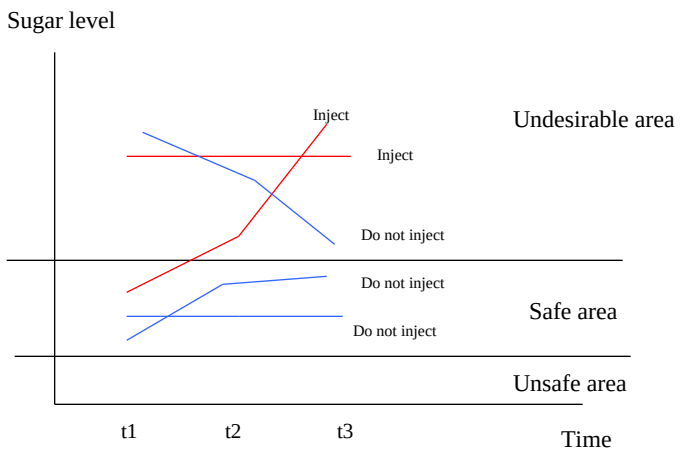
Injection scenarios

- Level of sugar is in the unsafe band
  - Do not inject insulin
  - Initiate warning for the sufferer
- Level of sugar is falling
  - Do not inject insulin if in safe band. Inject insulin if rate of change of level is decreasing
- Level of sugar is stable
  - Do not inject insulin if level is in the safe band
  - Inject insulin if level is in the undesirable band to bring down glucose level
  - Amount injected should be proportionate to the degree of undesirability ie inject more if level is 20 rather than 10

Injection scenarios

- Level of sugar is increasing
  - Reading in unsafe band
    - No injection
  - Reading in safe band
    - Inject only if the rate of increase is constant or increasing. If constant, inject standard amount; if increasing, compute amount based on increase
  - Reading in unsafe band
    - Inject constant amount if rate of increase is constant or decreasing
    - Inject computed amount if rate of increase is increasing

Glucose measurements



The decision on whether or not to inject is dependent on whether the rate of change of sugar level is increasing or decreasing and the current sugar level.

Insulin is injected if the rate of change of sugar level is increasing but not if the rate of change is decreasing and the level is in the safe zone. However, it is injected if the rate of change is decreasing and the level is in the undesirable zone.

If the level is falling and the rate of change is increasing, no injection. If however, the rate of change is decreasing then an injection is made if the level is in the undesirable zone

Key points

- The insulin pump software is a critical software system
  - Availability
  - Reliability
  - Safety
- The blood sugar level is measured and insulin injected if necessary
- The dose of insulin injected depends on the blood sugar level and the rate of change to the sugar levels