1. Writing a Dependability Case

1. Revisit the four module case studies. Rank the four case study systems in terms of the extent to which the system described is a safety critical system.

1: Insulin

2: Patient Information System for Mental Health

3. Wilderness Weather Station

4. Digital Learning environment

1. Create a dependability case for the system you have ranked as the most critical. This should include the following:

The insulin system will be used for people who have been diagnosed with type 1 diabetes. The device is attached to the person and will provide insulin for the user. The system performs blood sugar checks at regular time intervals the system must be worn by the user at all times.

Reliability is the most important dependability requirement. The system has to be reliable at all times, as the system is required to work without interruption at regular time intervals. Failure to work as expected can result in serious injury or death. As the device is worn by the user 24/7, maintenance cannot be performed easily in an emergency.

Safety which is considered an extension of reliability is therefore very important in this system. It is vital that when the system is not functioning correctly that this be made very clear to the user in the form of a warning, a fail-unsafe failure is very dangerous. Also, just as important is the ability to when not working correctly to shut down in a safe way. For example, if the system was malfunctioning and made this clear to the user but was somehow issuing higher doses of insulin due to the malfunction this would cause great harm. The system must be able to show a warning to user and “terminate” its function in a safe way.

The user is also able to manually get a shot of insulin if needed. Therefore, the availability to do this is important. If the user decides that they need an extra dose, it would not be viable to have delays.

As this system is worn by the user at all times, the need for resilience is important and the physical device should be designed to be very robust. The user will not be sitting idle all day and as such the system should have a failsafe if the needle is disconnected form the user.

As long as the system is not connected to any external device i.e., Bluetooth or Wi-Fi and doesn’t allow access to its internal working via the input on the device, the system will be quite secure from external penetration. However, care must be taken as the user of the device could potentially alter the device by opening it and programming it that way. So there needs to be a failsafe for that possibility i.e., device stops working when alter in a significant way that could allow access to the inner workings.

2. Faults, errors and failures

1. Error
2. Fault
3. Failure
4. Fault
5. Error
6. Failure
7. Error
8. Failure

3. Redundancy and Diversity

The Airbus 340 Flight Control System employs extensive redundancy and diversity measures to ensure dependability. Use the internet to research the Airbus 340 FCS. Describe the redundancy and diversity measures used by Airbus in the A340aircraft.

When an aircraft is in operation there is no failsafe state so therefore the system must be designed to operate with faults.

Some of the diversity is achieved by replicating sensors and computers. When you duplicate some of the critical system components, it allows for a degradation in the case of a failure. What this means it that if the primary component of a critical system or the system has a failure then the secondary component/system will activate. This design allows for a robust system as your chances of having a critical failure is reduced due to the fact you have back up systems. i.e., the chances of an error occurring in both components is less than an error occurring in just 1.

This is done in the Airbus by having 3 primary flight control computers and 2 secondary computers. They divert this further by having the primary and secondary computer designed and supplied by different companies, also, they both use different components i.e., processors. This decreases an error in the hardware. As only 1 computer is needed for flight control this allows for quintuple redundancy.

Also, in a degraded state the essential facilities remain available to the pilots, so they can control the system in the event of a failure.