Book Questions
Chapters 12
Devayan Mandal

12.3 In the insulin pump system, the user has to change the needle and insulin supply at regular intervals and may also change the maximum single dose and the maximum daily dose that may be administered. Suggest three user errors that might occur and propose safety requirements that would avoid these errors resulting in an accident.

Ans: Three user errors which may arise in the insulin pump system scenario and safety requirements to address the respective errors:

1. **Error**: The user does not correctly attach the needle to the insulin pump.

   Safety Requirement: The design of the insulin pump will equip the system to have a sensor which will alert the user of a needle which is incorrectly attached. An error message will light up on the insulin pump's display screen.

2. **Error**: The user does not correctly set the maximum single dose of insulin in accordance to the instructions given by the healthcare professional.

   Safety Requirement: The insulin pump system will display the confirmatory message screen before the user sets the single dose:

   "Correct max single dose: Y (↑) or N (↓)"

   The user will press ↑ to select Yes and ↓to select No on the system's keypad.

   'Yes', will allow the user to proceed whereas 'No' will redirect the user to the beginning screen.

3. **Error**: The user does not correctly set the maximum daily dose of insulin in accordance to the instructions provided by the healthcare professional.
   Safety Requirement: The insulin pump system will have preprogrammed default maximum daily dosage information. In addition, the user will be prompted to enter expected maximum daily dosage before the user first uses the system.

   If the user exceeds the maximum daily dose, the system will display the following alert:

   "Exceeds max daily dose. Continue: ↑, Reset: ↓"

12.4 A safety-critical software system for treating cancer patients has two main components:

- A radiation therapy machine that delivers controlled doses of radiation to tumor sites. This machine is controlled by an embedded software system.
- A treatment database that includes details of the treatment given to each patient. Treatment requirements are entered in this database and are automatically downloaded to the radiation therapy machine.

Identify three hazards that may arise in this system. For each hazard, suggest a defensive requirement that will reduce the probability that these hazards will result in an accident. Explain why your suggested defense is likely to reduce the risk associated with the hazard.

Ans: Three hazards which may arise during the operation of the safety-critical software system used for treating cancer patients and the defensive requirements which may prevent the risk of accidents for each respective hazard are as follows:

1. **Hazard**: Incorrect patient information used to provide treatment.
   Defensive Requirement: The healthcare professional will be required to verify the patient’s details such as name, date of birth and other medical records for identification purposes as the first step before administering treatment.

   The system will prompt the healthcare professional to download and view the radiation dosage information directly sent from the prescribing physician/oncologist. The healthcare professional will verify the patient’s details from the physician’s records as a second confirmatory step.

2. **Hazard**: Inability to transfer treatment requirements from the treatment database.
   Defensive Requirement: The system will prevent the administration of treatment until the healthcare professional is allowed complete access to the patient’s information from the treatment database.

   Also, the case may arise that emergency radiation treatment is required. For this, backup wiring, backup battery reserve and a backup software system display will be provided to connect the software system to the database server in case of hardware malfunctioning.

3. **Hazard**: Incorrect treatment administration.
   Defensive Requirement: The system will ensure that the healthcare professional provides the prescribed amount of treatment to the correct location in the patient’s body. This will be ensured by having the software system display the treatment dosage,

treatment duration and anatomical location for treatment with the patient’s identifying information as the last confirmatory screen before the system authorizes treatment administration.

12.6 Explain when it may be cost-effective to use formal specification and verification in the development of safety-critical software systems. Why do you think that some critical systems engineers are against the use of formal methods?

Ans: It is cost-effective and advisable to observe formal techniques during the specification requirements gathering and process verification stages while developing safety-critical software systems. Nearly all safety critical systems are required to undergo detailed inspection by the respective industry's safety regulatory organization. Only when the system meets the organization's minimum requirements can the system be made commercially available or ready for purchase.

By developing the safety-critical system in accordance to the guidelines set out by the respective industry's safety regulatory organization, the development team increases the probability of approval and can release the system sooner to its respective industry.

Critical system engineers may not be in favor or formal methods because it may be more time consuming to learn, abide and document the steps of developing the critical system formally. Also, it may be more time consuming to communicate the requirements to other subdivisions of the development as the later would be required to learn the rules and regulations of formally documenting processes.

12.8 List four types of systems that may require software safety cases, explaining why safety cases are required.

Ans: Four types of systems that may require software safety cases are:

1. **Vehicle braking system**: Many modern cars use a software system centralized to control important automotive functions, one of which being measured braking to halt the vehicle. The system will ensure precise responsiveness when the vehicle operator uses the brakes. Safety cases are crucial because delayed or unresponsive signaling from the system could lead to an accident.

2. **Flight navigation software**: This provides safety cases such as allowing the airplane pilot to connect to the air traffic control in real time with as minimum time delay as possible. Another case which is important for the safety-critical

system is allowing the pilot to provide accurate GPS information to air traffic control.

3. **Law enforcement's response to crime**: Police officer's cars are equipped with state-of-the-art safety critical software systems to help respond to criminal activity. Safety cases may include acquainting the officer with the location of the crime as relayed over by the law enforcement dispatcher. Another case may include providing the officer with a database which displays information about past criminal activity for a given location.

4. **Release of chemical industry by-products**: Safety critical systems are used by the chemical industry to monitor the release of chemical by-products. Cases include following local and state environmental regulatory guidelines, measuring the present atmospheric concentration of chemical by-products to ensure that additional by-products are not released in an uncontrolled manner.