1. **Giving reasons for your answers, suggest which dependability attributes are likely to be most critical for**

**the following systems:**

**\_1 An Internet server provided by an ISP with thousands of customers.**

**\_2 A computer-controlled scalpel used in keyhole surgery**

**\_3 A directional control system used in a satellite launch vehicle.**

**\_4 An Internet-based personal finance management system.**

Answer:

1. For the customers to be able to use the system they need to be able to connect to the server (Availability). As the system is connected to the internet its exposed to many threats (Security).

2. When using a scalpel it’s essential that the scalpel does not hurt the patient or the surgeon (Safety).

It’s also important that the scalpel follows the instructions of the surgeon precisely (Reliability).

3. When launching satellites it is crucial that all calculations are performed correctly (Reliability), and that the system is ready to perform its purpose without fault when needed (Reliability).

4. No unauthorized user may tamper with any of the data accessible in the system (Security). No errors may occour (Reliability). The system should be available as much as possible (Availability) but not at the expense of security and reliabilty.

**2. Giving reasons for your answer based on the type of system being developed, suggest the most appropriate generic software process model that might be used as a basis for managing the development of the following systems:**

**a)     A system to control anti-lock braking in a car**

**b)     A virtual reality system to support software maintenance**

**c)     A university accounting system that replaces an existing system**

**d)     An interactive travel planning system that helps users plan journey with the lowest environment impact**

*a)     Anti-lock braking system* This is a safety-critical system so requires a lot of up-front analysis before implementation. It certainly needs a plan-driven approach to development with the requirements carefully analysed. A waterfall model is therefore the most appropriate approach to use, perhaps with formal transformations between the different development stages.

*b)     Virtual reality system* This is a system where the requirements will change and there will be an extensive user interface components. Incremental development with, perhaps, some UI prototyping is the most appropriate model. An agile process may be used.

*c)     University accounting system* This is a system whose requirements are fairly well-known and which will be used in an environment in conjunction with lots of other systems such as a research grant management system. Therefore, a reuse-based approach is likely to be appropriate for this.

*d)     Interactive travel planning system* System with a complex user interface but which must be stable and reliable. An incremental development approach is the most appropriate as the system requirements will change as real user experience with the system is gained.

**3. Identify six consumer products that are likely to be controlled by safety-critical software**

**systems.**

Possible domestic appliances that may include safety-critical software include:

Microwave oven

Power tools such as a drill or electric saw

Lawnmower

Central heating furnace

Garbage disposal unit

Vacuum cleaner

Food processor or blender

**4. Reliability and safety are related but distinct dependability attributes. Describe the most important distinction between these attributes and explain why it is possible for a reliable system to be unsafe and vice versa.**

Ensuring system reliability does not necessarily lead to system safety as reliability is concerned with meeting the system specification (the system 'shall') whereas safety is concerned with excluding the possibility of dangerous behavior (the system 'shall not'). If the specification does not explicitly exclude dangerous behavior then a system can be reliable but unsafe.

Give an example

**5.     In a medical system that is designed for deliver radiation to treat tumors, suggest one hazard that may arise and propose one software feature that may be used to ensure that the identified hazard does not result in an accident.**

A possible hazard is delivery of too much radiation to a patient. This can arise because of a system failure where a dose greater than the specified dose is delivered or an operator failure where the dose to be delivered is wrongly input.

Software features that may be included to guard against system failure are the delivery of radiation in increments with a operator display showing the dose delivered and the requirement that the operator confirm the delivery of the next increment. To reduce the probability of operator error, there could be a feature that requires confirmation of the dose to be delivered and that compares this to previous doses delivered to that patient. Alternatively, two different operators could be required to independently input the dose before the machine could operate.

**6. Explain how both the waterfall model of software process and the prototyping model can be accommodated in the spiral process model.**

For spiral model, there are several loops, each loop in the spiral represents a phase in the process

, and for each loop it can be accommodated as waterfall model: it follow the same principle

as waterfall model in each loop.

Requirements->analysis->Software design ->Implementation ->Testing and integration.

And in the Software design stage and Implementation stage can use the prototyping model to do the risk analysis to choose the most appropriate approach for implementation.

**7.Explain why programs that are developed using evolutionary development are likely to be difficult to maintain**.

From an engineering and management perspective, the evolutionary approach has two problems:

1. *The process is not visible* Managers need regular deliverables to measure progress. If systems are developed quickly, it is not cost-effective to produce documents that reflect every version of the system.

2. *Systems are often poorly structured* Continual change tends to corrupt the software structure. Incorporating software changes becomes increasingly difficult and costly.

**8. What are the advantages of providing static and dynamic views of the software process as in the Rational Unified Process?**

With evolutionary development, many changes are made in the requirements and design, system has multiple versions, documenting is not cost-effective, and hence, documentation is poor. Maintenance of the poor documented system is difficult.

* An approach to process modeling which is simply based on static activities, such as requirements, implementation, etc. forces these activities to be set out in a sequence which may not reflect the actual way that these are enacted in any one organization.
* In most cases, the static activities shown in Figure are actually interleaved so a sequential process model does not accurately describe the process used. By separating these from the dynamic perspective i.e. the phases of development, you can then discuss how each of these static activities may be used at each phase of the process.
* Furthermore, some of the activities that are required during some of the system phases are in addition to the central static activities shown in Figure . These vary from one organization to another and it is not appropriate to impose a particular process in the model.