In-Class Activity

***2.1.* Your colleague Joe argues that since reliability is the probability that the product operates free of failure for some unit of time and safety is the probability that the product operates free of catastrophic failures, and since catastrophic failures are failures, then a reliable system is necessarily safe. Do you agree with Joe? Why or why not?**

***Answer*:**

No, I do not agree with Joe because a reliable software means there is no violation of specification while a safe software means a software running without causing a catastrophic failure. A Safe system means no failure related to Safety.

In brief, if one of the specification of a software/system failed than also the software/system will work safely but it won't be reliable anymore.

For example, an aeroplane needs to be available to fly. It could be quite safe if it never took off, but that wouldn't be considered reliable. Alternatively, it could reliably transport passengers from place to place, but kill one or two every flight. That would be reliable but not safe.

***2.2.* Can a system be reliable but not secure? Can a system be secure but not reliable?**

Answer:

Yes, a system may be reliable but unsafe and a system may be safe but unreliable. A reliable system means there is no violation of specification while a safe system means a software running without causing a catastrophic failure. A Safe system means no failure related to Safety.

Example of an unreliable but safe system.

A word processing system may not be very reliable but is safe. A failure of the software does not usually cause any significant damage or financial loss. It is therefore an example of an unreliable but safe system.

Example of an unsafe but reliable system.

A hand gun can be unsafe but is reliable. A hand gun rarely fails. A hand gun is an unsafe system because if it fails for some reason, it can misfire or even explode and cause significant damage. It is an example of an unsafe but reliable system.

***2.3.* Can a system have high reliability but low availability? Can a system have high availability but low reliability?**

Answer:

Reliability the probability that the software product operates for a given amount of time without violating its specification.

Availability refers to a system's ability to continue delivering service to its user community

Yes, a system can have high reliability but low availability. For example, the space shuttle. When they were in use, at any given time, they were not available for launch. However, when they were launched, in general they would not fail for the following 14 days. This kind of reliability is common in aviation. Helicopters, for example, need many hours of maintenance for every hour they spend in the air.

Conversely, a system may be highly available but not very reliable. For example, Microsoft DOS was very fast to boot. It was also very easy to crash, and so had poor reliability. Because you could reboot quickly, the poor reliability was not a problem. Modern data centers take this approach by focusing on rapid recovery rather than high reliability. Thus, it is better to have a server crash quickly and cleanly, and provision a replacement quickly than it is to try to keep the server up and running.