1. **Critical Software** [2013 Paper 3 Question 9]

Google have spent several years developing self-driving cars which rely on a range of sensors and stored data and are now claimed to have covered hundreds of thousands of miles with a good safety record.

A Google executive has now asked to meet the Transport Secretary, who has in turn asked your company for advice. What sort of safety case should the government demand from vendors and service providers if autonomous vehicles are to be allowed on Britain’s roads?


   (a) Describe the following two methodologies as they are used in building safety-critical systems:

   (i) failure modes and effects analysis;

   (ii) fault tree analysis.

   (b) Describe three cognitive factors that can lead to operator errors in safety-critical systems.

   (c) If the safety of a system depends on correct operator actions, then under what circumstances is fault tree analysis likely to be more or less effective?

3. **Software Life Cycle** [2011 Paper 3 Question 9]

   (a) Describe the waterfall model for software development and list three of its advantages for software development.

   (b) When discussing system development Fred Brooks says, “plan to throw one away – you will anyway”. What disadvantages of the waterfall model is he referring to? Outline an alternative software development model that deals with these disadvantages.

   (c) You work for a large “social networking” company which has recently introduced a one-to-one chat mechanism, promising that they will never censor conversations. Users are now reporting that their friends’ computers are being compromised by malicious software. When users click on links within messages sent by this malicious software, their machine is also compromised, and spreads the infection still further. A crisis meeting has decided that the chat software must be modified to block this “worm” behavior.

   As manager of this project, how will you approach the development, how will you estimate how long the task will take, and how will you establish that your solution is safe to deploy?
4. Software Projects [2010 Paper 3 Question 8]

(a) Discuss the lessons learned from the London Ambulance Service disaster from the following viewpoints.
   (i) Requirements engineering.
   (ii) Human factors.
   (iii) Testing.
   (iv) Project management.

(b) You have been hired by the Department of Energy and Climate Change (DECC) to manage a project to replace Britain’s 47 million gas and electricity meters with “smart” meters that report energy use every 30 minutes. These reports go to a central service, and energy companies have access to their customers’ readings. The goals of the system are to facilitate more flexible pricing, so customer demand can be brought more into line with supply; to make it simpler for customers to switch energy companies; and to help DECC predict and manage energy demand.

Describe what measures you would take to reduce the likelihood of a project disaster.

5. Reliability and Safety

Discuss what is meant for a software to provide reliability vs safety. Give an example (ideally not discussed in the lectures) to demonstrate how confusing between the two could lead to disastrous consequences.