Introduction: Risk assessment techniques identify the probability that a hazard will lead to an incident or accident. They also help analysts to identify the consequences that a hazard may have for the safety of a complex system. During this course, you will be introduced to a number of risk assessment techniques including Fault Trees, Failure Modes, Effects and Criticality Analysis, HAZOPS Probabilistic Risk Assessment etc. As you will have seen, some of these approaches are quantitative – they provide numerical estimates for probability and consequence typically measures in failures per operating hour and financial losses. Other approaches are qualitative; probabilities are given as ‘likely’ or ‘rare’ and consequences are described using words like ‘very bad’ or ‘trivial’.

Unfortunately, there are some areas where these techniques do not work so well. In particular, it can be difficult to quantify the probability of human error – this is influenced by hundreds of factors including fatigue, stress, workload. Similarly, software failures do not reflect normal probability distributions, for instance they may cluster around upgrades. Bugs may also stay in a program for many years before they are triggered by a particular sequence of execution.

Introduction to Unmanned Airborne Systems: Unmanned Airborne Systems (UAS) have been developed for a host of applications. Here we focus on their civil use in maritime search and rescue, the aircraft will not carry any weapons. You are being asked to assess the risks of operating a small UAS that is launched from a coast guard vessel to find mariners, eg fishermen and sailors, who have been lost at sea. Each UAS consists of a Ground Control System (GCS) which helps the crew to pilot the vehicle. These include the software interfaces used to control the aircraft and also to monitor the images and other signals sent from the UAS. The system also includes radio and communications links from the GCS to the vehicle. The aircraft has an array of on-board software systems to monitor the health of the aircraft and also to collect signals, such as video images, from the area being monitored.

Your Task: You have been asked by the China Coast Guard (中国海警) to assess the risks of operating a UAS for search and rescue. You can use any of the techniques that have been introduced during the course. However, if you choose to use a quantitative approach then you must explain where you will obtain the data that supports your assessment. It is also important to carefully consider the risks created by both human error and also by software bugs.

Hint: One good way of starting any risk assessment is to identify the ways in which previous systems have failed because this gives you an idea of the hazards that we have seen in the past – there are several reports into UAV failures on http://www.dcs.gla.ac.uk/~johnson/papers.html, especially the reports into the loss of the Predator over Nogales, in the USA.

Submission: Please show your solution to one of the tutors during the afternoon session for the safety-critical systems course. This will form one of the four pieces of coursework that will be assessed in Safety-Critical Systems.