ASSIGNMENT 1 - TREE DIAGRAMS, CONDITIONAL PROBABILITY, AND INDEPENDENCE

1. Reliability

1.1. **Background.** The concept of reliability of a system can be quantified as one minus the probability of a catastrophic system failure.

If a system has n components, with probabilities of failure $P(F_i)$, $i = 1, 2, \ldots, n$, then the law of total probability says that the probability $P(C)$ of a catastrophic system failure C is:

$$P(C) = P(C|F_1) \cdot P(F_1) + P(C|F_2) \cdot P(F_2) + \cdots + P(C|F_n) \cdot P(F_n)$$

A component for which $P(C|F_i) = 1$ is considered a critical component, because its failure guarantees a catastrophic system failure. In this case, the unconditional probability of a catastrophic failure $P(C)$ is always greater than or equal to the sum of the probabilities of failure of the critical components.

A principle of safety engineering is *redundancy*, which means every critical component has one or more backup components capable of taking over the function should the primary unit fail.

In other words, the system has no components for which

$$P(C|F_i) = 1$$

Through redundancy, a system can in theory be made more reliable than any of its components.

1.2. **Problem 1.** Suppose failure of a certain component increases the probability of a catastrophic failure of the system, but does not guarantee it.

Assume the component has a probability of failure $P(F)$ of 1/10000 each time it is activated. Assume also that the conditional probabilities of a catastrophic system failure (C) are:

$P(C|F) = \frac{1}{100}$ the probability of C given that the component failed

$P(C|F') = \frac{1}{8000}$ the probability of C given that the component did not fail

eLearn Question 1: What is the *unconditional* probability $P(C)$ of a catastrophic failure in this system? (hint: draw a tree diagram)

1.3. **Three Mile Island.** The Three Mile Island nuclear power station is located near Harrisburg, PA. Two nuclear reactors designed and built by the Babcock and Wilcox corporation were located on the site.

While a nuclear detonation of the type produced by nuclear bombs is believed to be impossible in a pressurized water reactor, a breach of the reactor vessel and containment building could result in a Chernobyl-type accident that might render a sizeable portion of the state of Pennsylvania uninhabitable for thousands of years - dire consequences indeed.

To evaluate the risks involved, during the design phase the safety of these reactors, which depend on constant circulation of cooling water through the reactor core, was evaluated in a study known as WASH-1400. WASH used techniques similar to tree diagrams to estimate the probability of certain events, and also made assumptions about the indepencence of certain events. It has been criticized for being too optimistic.

On the operator's console there are two levers that shut off the emergency feedwater pumps for the steam generators. Suppose the probability that each of them is closed by mistake on a certain day at 1/1000, and they are opened and closed independently.

eLearn Question 2: What is the probability $P(C_1 \cap C_2)$ that both events occur on a given day?

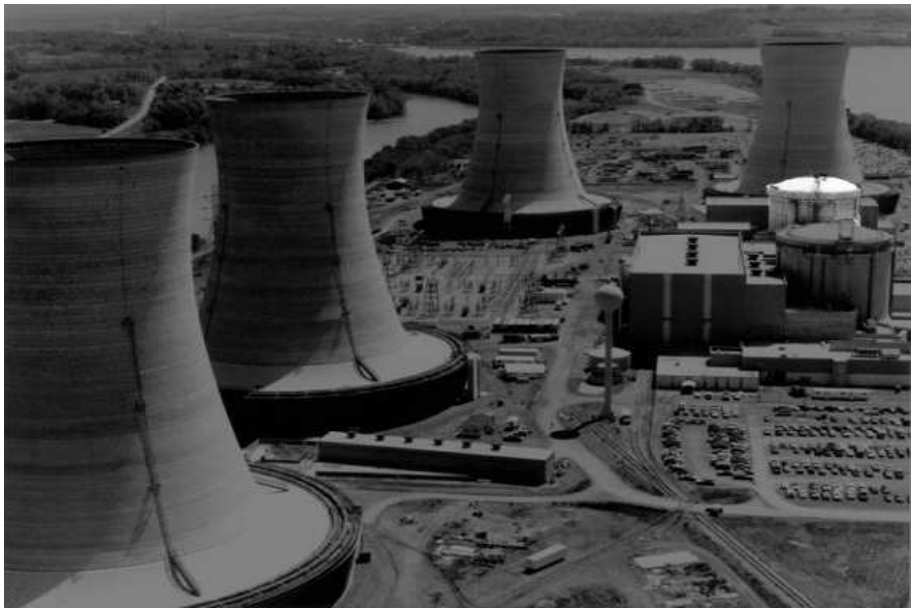
The likelihood of events with very low probabilities is difficult to comprehend. In risk analysis, a common way to make them more understandable is to convert them to frequencies of occurrence, usually of the form "once in x years".

eLearn Question 3: Assuming the law of large numbers applies, meaning the *proportion* of days the event $C_1 \cap C_2$ occurs approaches $P(C_1 \cap C_2)$ as the number of days increases, how many times do we expect both valves to be closed by accident in 100 years (approximately $36,500$ days) of operation?

eLearn Question 4: How many days do we need to operate before the number of times we expect accidental closure of both valves reaches 1?

Question 5: How many years does this represent (The risk would often be stated as "one event in this many years of normal operation")?

On March 28, 1979, a pump shutdown set off a chain of events that led operators to believe that there was too much water in the system, and they took a series of actions to reduce the flow of cooling water. A partial meltdown of the reactor core followed, as well as a hydrogen explosion in the containment building. Several days passed before the reactor could be stabilized and it was not declared completely shut down until May. During that time, then President Jimmy Carter (a trained nuclear engineer) visited the site to reassure the public, but the situation was far more serious than anyone realized. Analysis of the damaged reactor revealed that much of the 100 tons of fuel in the reactor had melted, *drained to the bottom of the reactor*, and was minutes away from melting through the steel reactor vessel (See http://americanhistory.si.edu/TMI/index.htm). No nuclear power plants have been built in the U.S. since this accident.



Department of Energy photograph of the Three Mile Island site. The reactors are located in the two small cylindrical containment buildings at the right center of the photo. Reactor 2 is highlighted. The four large hourglass shapes are cooling towers.

During the investigation, it was determined that both emergency feedwater valves for the steam generators had been mistakenly left closed the day before. Operators testified that they never closed one valve and not the other, that they always either opened both or closed both (the levers are right next to each other on the console).

eLearn Question 6: What is the probability that both valves are accidentally closed under this scenario?

eLearn Question 7: How many years of normal operation have to pass before we expect this to happen once?

1.4. **UA232.** The McDonnell-Douglas DC-10 was a first generation wide-body jet designed to compete with the Boeing 747. At the time of its design, control systems on commercial aircraft were mostly mechanical (hydraulic). Pressure on the controls in the cockpit was amplified and transmitted to other parts of the plane through hydraulic fluid contained in a system of high-pressure tubing, much like the power brake system of an automobile. And, like the brake system of a car, a leak in the tubing that causes loss of fluid quickly results in a failure of the system.

To reduce the probability of this occuring to an acceptable level, the DC-10 was designed with three independent hydraulic systems. In the event of even a double failure, the remaining system would allow the pilots to control the plane.

Assume that on any given flight the probability of failure of each individual hydraulic system is 1/1000, and that the systems are independent: failure of one does not change the probability of failure in the others.

$$P(F_2|F_1) = P(F_2) \quad P(F_3|F_1) = P(F_3) \quad \text{and so on}$$

Hint: draw a tree diagram. The first stage should represent the two events F_1 and F_1', representing the failure or non-failure of the first hydraulic system, the second should represent F_2 and F_2', and so on. The final stage should represent te event catastrophic failure C or no catastrophic failure C'. Assume that all conditional probabilities of catastrophic failure given zero, one, or two hydraulic system failures are zero, but the conditional probability of C given that all three hydraulic systems failed is one.

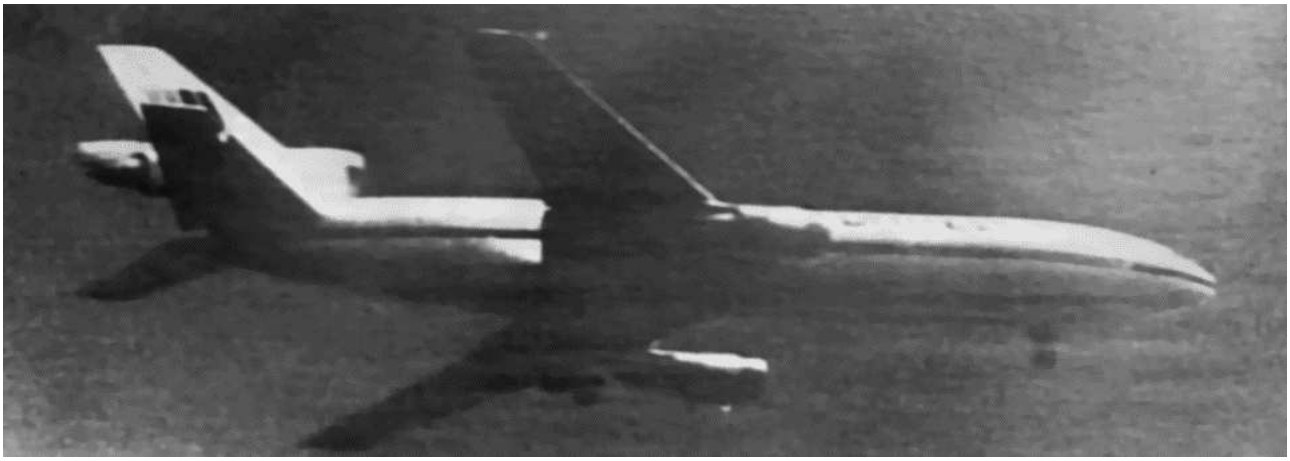
eLearn Question 8: What is the unconditional probability $P(C)$ of a catastrophic failure?

eLearn Question 9: Assuming the law of large numbers applies, meaning the *proportion* of catastrophic failures approaches $P(C)$ as the sample size increases, how many catastrophic failures do we expect in $1,000,000$ flights?

eLearn Question 10: How many flights do we need to make before the number of catastrophic failures we expect reaches 1?

eLearn Question 11: If there are 500 planes of this type each making three flights per day, how many years would it take to accumulate this number of flights? (The risk would often be stated as "one event in this many years of normal operation".)

On July 19th, 1989, an undetected metallurgical flaw caused the fan disk on the rear engine of a DC-10 to disintegrate in flight, resulting in the loss of all three hydraulic systems. Investigation revealed that there was a section of the tail near the engine where the lines of all three systems were located in close proximity. Why would this change the probability of catastrophic failure $P(C)$? What would the effect be?



NTSB photograph of flight UA232 taken before the crash landing. The apparent white dot on the right horizontal stabilizer is damage caused when the fan disk in the tail-mounted engine disintegrated. Like the recent landing in the Hudson river, the exceptional skill and professionalism of the pilots is credited with greatly reducing the loss of life.

On newer commercial aircraft, hydraulic systems have been replaced by electromechanical devices controlled by computers ("fly by wire"), but the need for reduncancy still exists.