NUCLEAR SAFETY AND RELIABILITY

WEEK 5

TABLE OF CONTENTS – WEEK 5

1. Construction and Evaluation of Fault Trees

This material is presented in Sections 8-1 to 8-3 of McCormick. The Fault Tree Guide from the Darlington Probabilistic Safety Evaluation can be used to supplement these sections.

Definition: A fault tree is a graphical model of the various parallel and sequential combinations of various "primary" system faults which might result in the TOP EVENT -- normally the failure of a mitigating function.

The top event is a success/ failure node in the event tree; the purpose of the fault tree is to determine the failure branch probability at such a node. The success-or-failure criterion of the system is defined by the function of the system in the accident sequence being analyzed.

2. Simple Fault Tree Examples

See Sections 8-4 to 8-6 in McCormick. Self-study is required to become familiar with the principles of fault tree logic.

A simple fault tree example can be constructed from the emergency coolant injection logic of Figure 5.1, taken from the book authored by Fullwood and Hall:

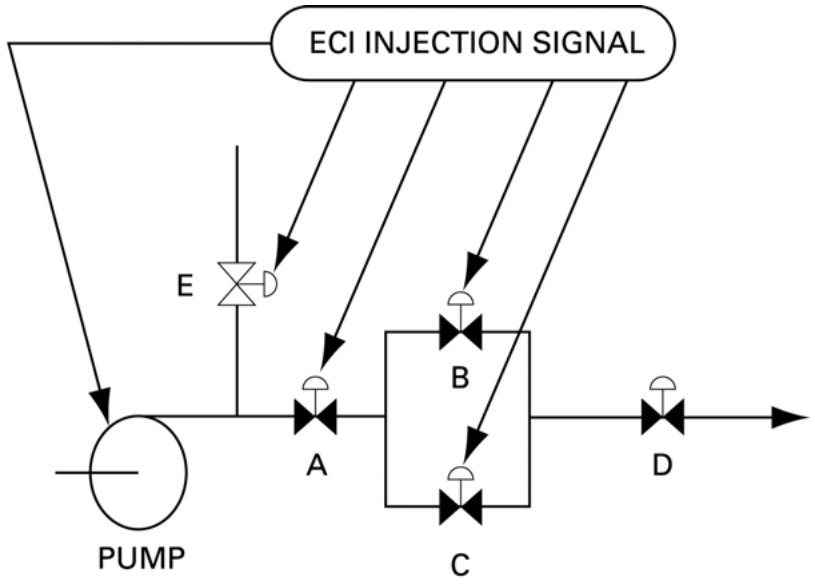

FIGURE 5.1 – A SIMPLE EMERGENCY COOLANT INJECTION SYSTEM

For injection to be successful the pump must be started, valve 'E' must be closed, valves 'A' and 'D' must be opened, and either valve 'B' or 'C' must be opened. The initial fault tree for this system is shown in Figure 5.2

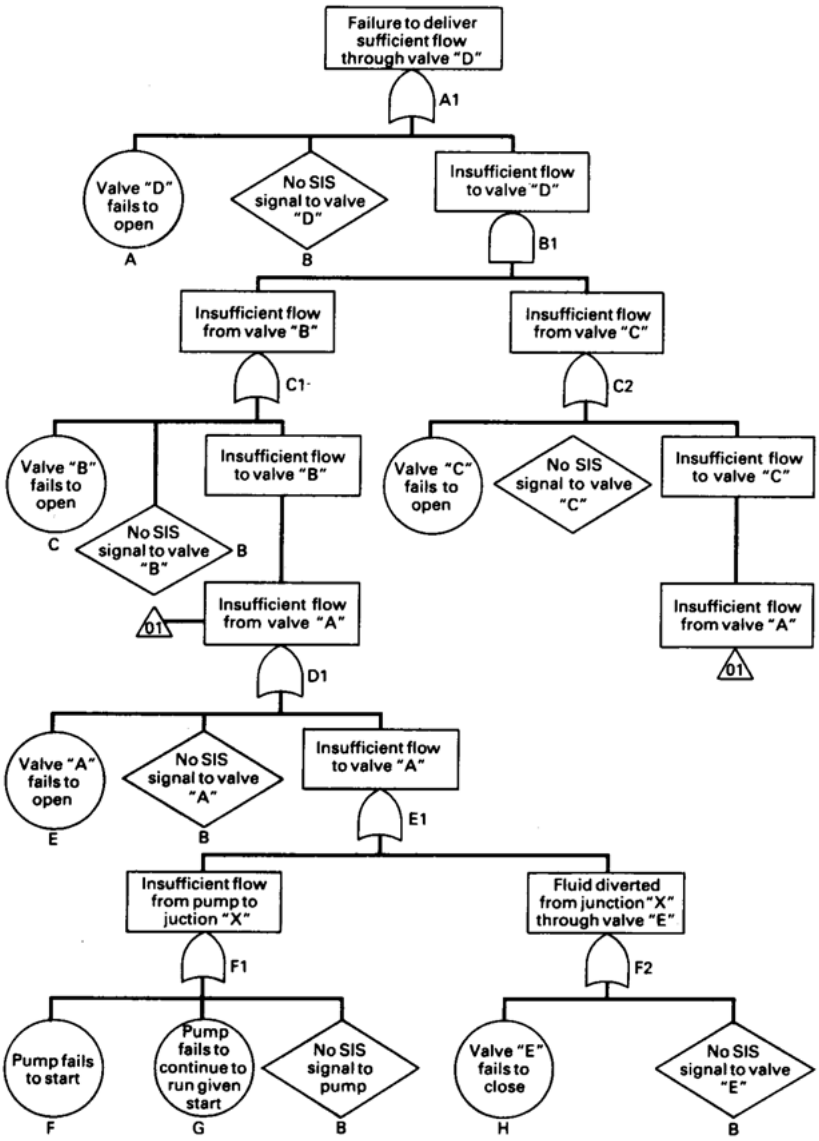

Figure 5.2 -- "Failure to Inject" fault tree, labelled for Boolean reduction

Boolean reduction for this fault tree is shown in Figure 5.3.

$A1 = A = B = B1$
$B1 = C1 \cdot C2$
$C1 = C + B + D1$
$C2 = D + B + D1$
$D1 = E + B + E1$
$E1 = F1 + F2$
$F1 = F + G + B$
$F2 = H + B$

By substitution,

$E1 = (F + G + B) + (H + B)$
$D1 = E + B + (F + G + B) + (H + B)$
$C2 = D + B + E + B + (F + G + B) + (H + B)$
$C1 = C + B + E + B + (F + G + B) + (H + B)$
$B1 = (C + B + E + B + (F + G + B) + (H + B) \cdot (D + B + E + B + (F + G + B) + (H + B)$
$A1 = (C + B + E + B + (F + G + B) + (H + B) \cdot (D + B + E + B + (F + G + B) + (H + B)$

Simplifying,

$A1 = A + B + (C + B + E + B + F + G + H + B) \cdot (D + B + E + B + F + G + B + H + B)$
$= A + B + (C + B + E + B + F + G + H + B) \cdot (D + B + E + F + G + H)$

Multiplying,

$A1 = A + B + CD + CB + CE + CF + CG + CH + BD + BB + BE + BF + BG + BH + ED + EB + EE +$
$EF + EG + EH + FC + FB + FE + FG + FH + GD + GB + GE + GF + GG + GH + HD + HB + HE +$
$HF + HG + HH$

Using identity "X·X=X",

$A1 = A + B + CD + CB + CE + CF + CG + CH + BD + B + BE + BF + BG + BH + ED + EB + E + EF +$
$EG + EH + FD + FB + FE + F + FG + FH + GD + GB + GE + GF + G + GH + HD + HB + HE +$
$HF + HG + H$

Using identity "X+(X·Y)=X",

$A1 = A + B + E + F + G + H + CD$

Figure 5.3 -- Boolean Reduction of "Failure to Inject" fault tree

Fault trees and "success trees" for this system are shown in Fig's 5.4 and 5.5.

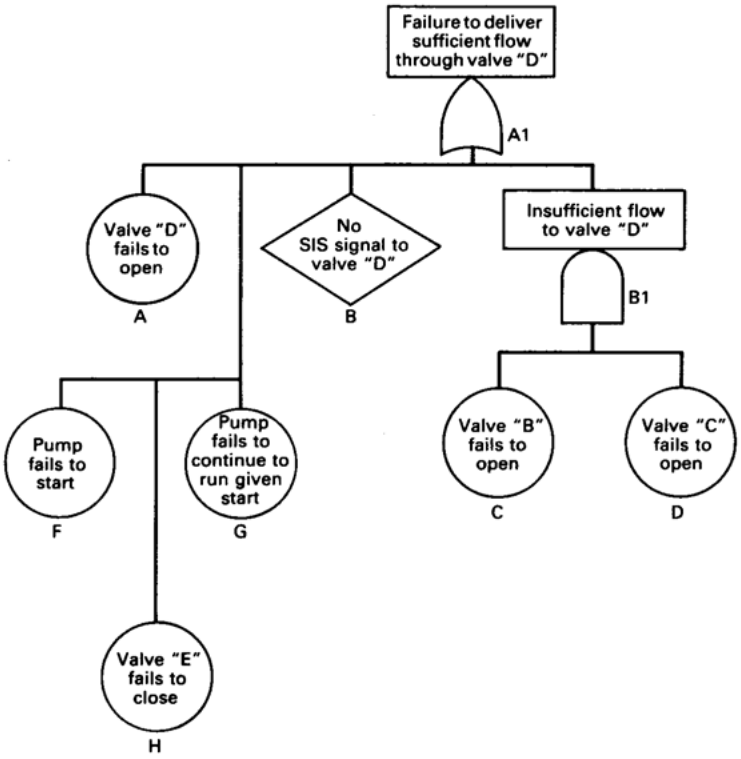

Figure 5.4 -- Injection system mincut fault tree equivalent to fault tree shown in Figure 5.2

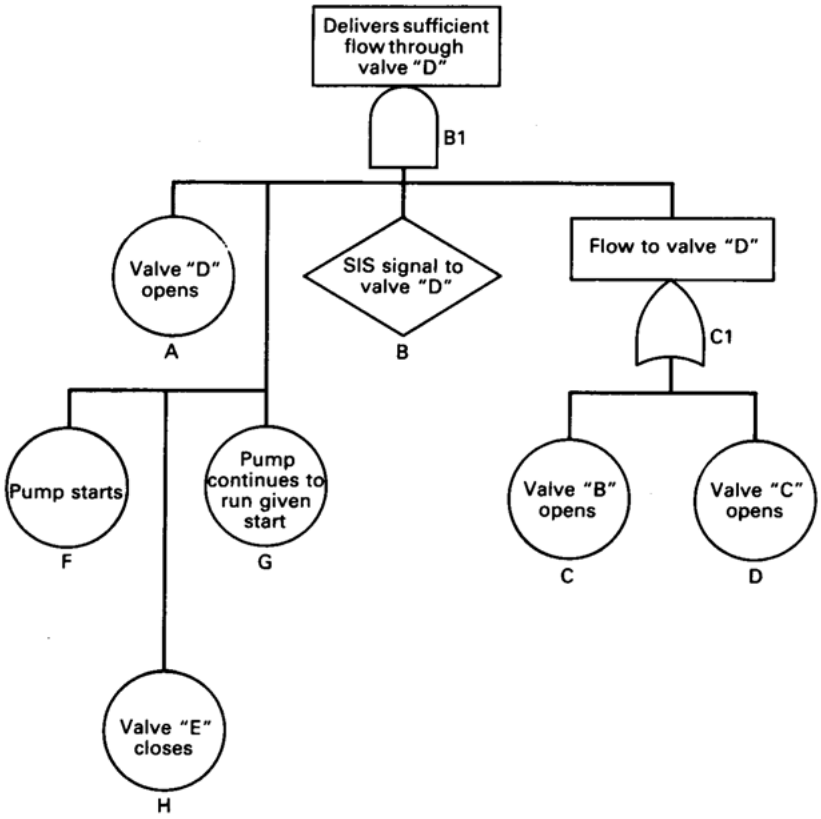

Figure 5.5 -- Success tree form of Figure 5.4

Note the error in this fault tree. Also, there is a simplification of the injection signal failure; these all are assumed to be due to one common cause.

3. Common Cause Failures

Common cause failures are those in which two or more components fail as a consequence of the failure of a third component. A simple example is failure of multiple electrical panels due to failure of a sump pump to keep the water level down in a room, following a piping failure. In such a case the common cause would be the pump, since it was put in place to deal with the pipe failure.

Common cause events generally reduce the overall reliability of a system. Therefore, a significant part of design for high reliability is the process of discovering potential common-cause failures and eliminating them.

An example of linking of the fault trees of multicomponent systems with both independent and common-cause failures (from "PRA Procedures Guide", NUREG/CR-2300, Vol.1). The following shows a fault tree for a three-component system with independent and common causes.

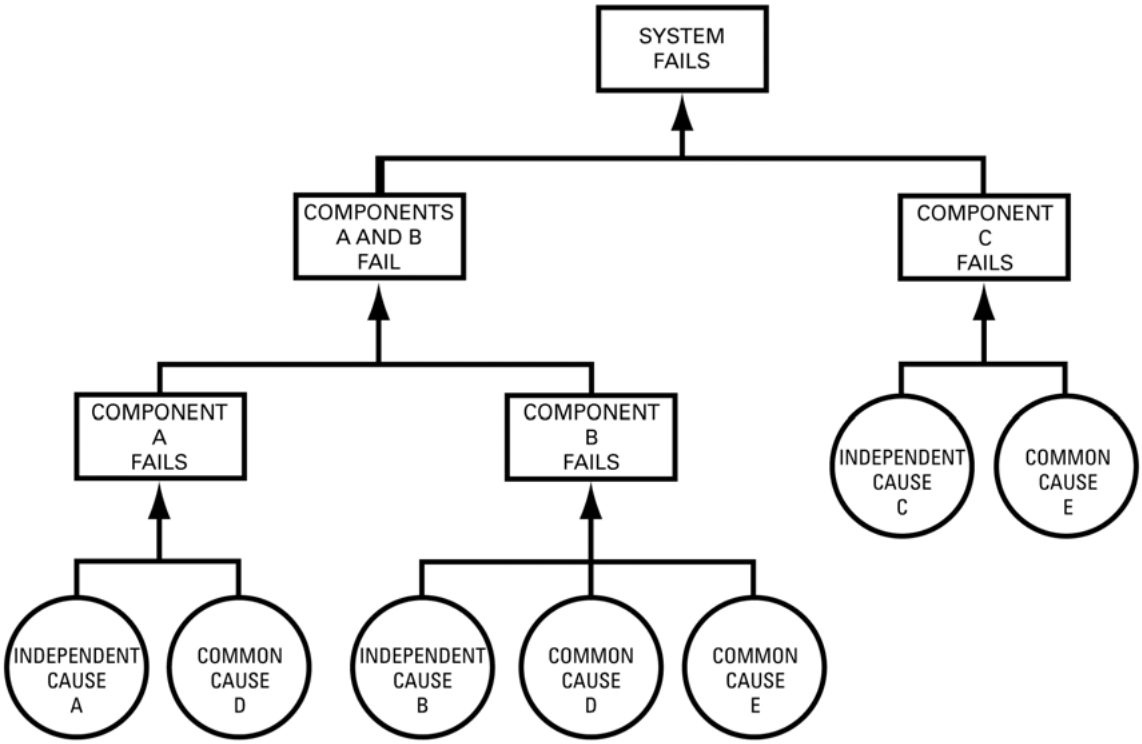

FIGURE 5.6 – COMMON - CAUSE FAILURE ANALYSIS

Minimal cutsets: Without common causes -- A,B,C
With common causes -- A'B', C',D,E

The TOP EVENT (system fails) is

F = A*B+C

A = A' + D
B = B' + D + E
C = C' + E

Using A + AB =A, one gets

F = (A' + D) * (B' + D + E) + C' + E = A'B' + D + C' + E

--- which correctly identifies the (4) minimal cutsets.

4. Darlington Probabilistic Safety Evaluation

A Probabilistic Safety Evaluation (DPSE) was conducted on the Darlington station (first unit in-service date 1989) with the prime purpose of evaluating the design with regard to the full set of potential failure mechanisms which might lead to fission product release and health consequences. Economic risks to the operating utility also were analyzed. The study included fault tree and event sequence analysis down to the component level; it integrated the major systems (civil, electrical, mechanical, instrumentation/control, etc.) into one overall package. Human failure, internal common cause failure, and cross-linked failure analysis were included; external common cause events (earthquake, tornado, external explosion, etc.) were excluded.

The first results of the study were directly useful in correcting design errors. Some 100 design faults were uncovered. Over 25 of these were judged by plant operating staff to be such that they would not have been revealed during commissioning and so would have been present in the plant after startup. An error that was not picked up in this study, but was detected separately, was a series of bugs in the computerized safety system logic. (Darlington is the first plant in the world in which relay trip systems have been completely replaced by digital logic.)

Only one major design mistake was found during the DPSE study which could have seriously compromised plant safety. This would have been detected and corrected during station commissioning. It is likely that the most serious impact of these errors, had they been left in the design, would have been extension of the commissioning period at a very high cost.

The overall findings were that the most exposed individual will be subject to a risk of 9×10^{-6} Sv/yr during station operation (compared with about 1×10^{-3} Sv/yr from natural background). The economic risk of station operation was found to be $10,000,000 per unit per year -- dominated by loss of coolant accidents without any release of fission products, but which require emergency coolant injection. The cost is incurred through shutdown of all units while this water is recovered from the fueling machine duct and pumped into the ECIS storage tank.

An indication of the appreciated value of this kind of study is that Ontario Hydro Operations have commissioned similar studies of all other stations. The basic worry is that design errors of the kind found in the DPSE study might be present in the operating plants - several of these already have been found and corrected over the years. A secondary concern is that the accident coverage existing in the plants may not be as good as expected. This work will not be quite as extensive as was the DPSE study, but still will require of the order of 50 man-years ($6,000,000) per station.

Some aspects of the DPSE summary report will be discussed in class. It is a good example of a full-scale probabilistic safety evaluation as carried out in many plants around the world. The first requirement of any study such as this is detailed knowledge of the plant; the second is strict discipline in forming the fault trees and event-sequence diagrams. The third requirement is for a high-quality computer package for processing the large quantities of data.

One common weakness of all risk assessments like DPSE is the unknown initiating event (the Unidentified Failure Mode) as illustrated in the following copy of Figure 1.2.

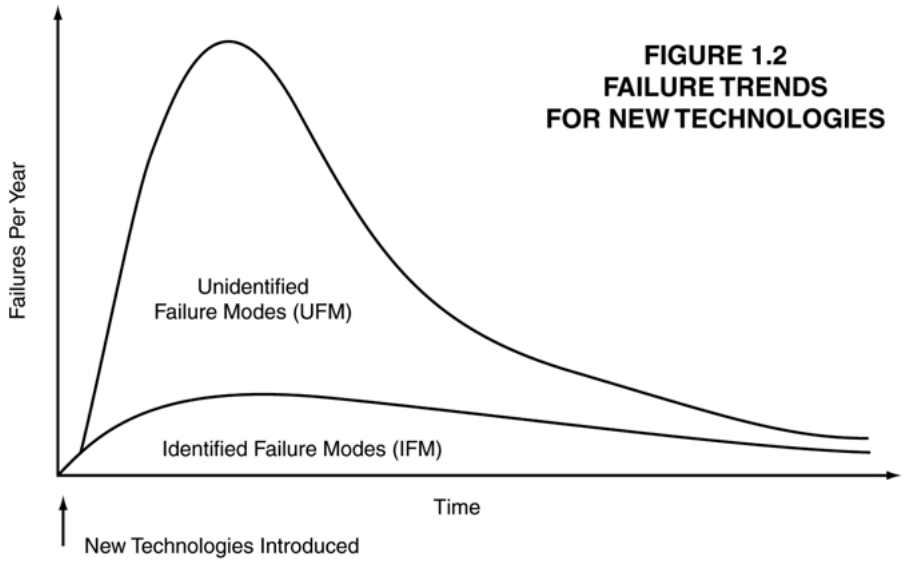

FIGURE 1.2
FAILURE TRENDS
FOR NEW TECHNOLOGIES

The UFM category of accident has two sources - first the completeness uncertainty for the plant as defined in the study, and second the completeness uncertainty for the pre-accident plant states. In general, UFM failures result from ignorance of the sum total of failure modes.