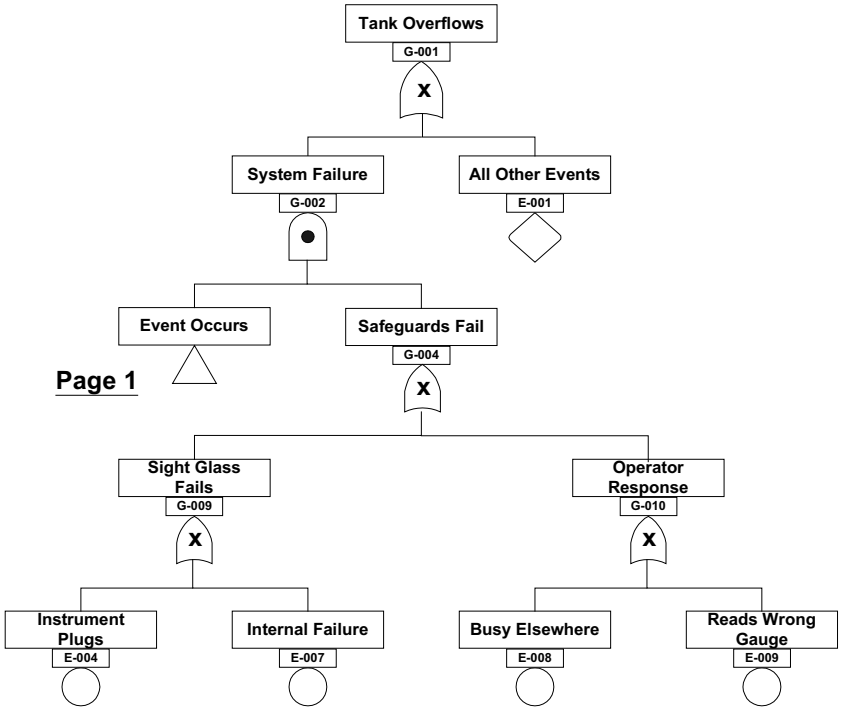
Figure 12
Final Fault Tree (Page 2)



Inspection of Figures 11 and 12 leads to the following comments.

Page 1 (Figure 11) — the System Fault — develops through a series of OR and AND Gates. The system can fail due to problems with the pumps or with the instruments. Eventually, this part of the Tree leads to the creation of six separate Base Events.

Page 2 (Figure 12) — the Safeguards Fail — has only OR Gates. There is no redundancy within the safeguard system. *A priori* this lack of AND Gates in Figure 12 may suggest that this is the area where improvements could be made, *i.e.,* it may make sense to have safeguards within the Safeguard system.

Figure 12 leads to the creation of four Base Events.

4. IDENTIFY THE CUT SETS

Developing a Fault Tree in the manner shown in the previous pages is very useful in that everyone is forced to think through logically ways in which events may interact with one another in a complex manner to create an unacceptable incident. However, it can be seen that a tree could quickly become difficult to follow and understand as more events and gates are added. Inspection of Figures 11 and 12 does not give any immediate insights, apart from the hint that AND Gates should be inserted into the Safeguards section.

In order to simplify and summarize the lessons to be learned from Fault Tree analysis, and in order to provide a basis for quantifying the Tree, the next step in the analysis is to develop Cut Sets, which are defined as follows:

> A Cut Set is a collection of Base Events such that, if all the Base Events in that Cut Set were to occur, the Top Event would occur.

The convention used in this eBook is to show Cut Sets within curly braces { }. The development of Cut Sets is illustrated by using the logic developed in the earlier part of this eBook. The first Cut Set, which is simply the Top Event by itself as shown in Figure 2, is:

{ G-001 }

Moving to Figure 10, two Cut Sets are created from G-001. They are:

{ G-002 } — System Fault
{ E-001 } — 'All Other Events'

Events which constitute an OR Gate are shown on separate lines, where each line represents a Cut Set. In other words, if the output from G-002 ('System Failure') is positive, or if the 'All Other' event occurs, then system failure will occur.

Being an AND Gate, G-002 is developed as follows:

{ G-003 G-004 }
{ E-001 }

AND Gates expand horizontally. All the events on that line must occur for the Cut Set to deliver a positive signal.

In words: for the first Cut Set to trigger the Top Event, the High Level Event has to occur, AND the Safeguards have to fail. These two events are placed on the same line (and the cut set { G-002 } has disappeared).

G-003 is an OR GATE that creates two new Cut Sets. The system is now:

{ G-005 G-004}
{ G-006 G-004 }
{ E-001 }

Mathematically, the three Cut Sets are equivalent to three events entering an OR GATE.

Repeating the above actions for all events, the full set of non-condensed Cut Sets for the final Tree of Figures 11 and 12 is: