M2 3/5

Application of Goal Trees for Nuclear Power Plant Hardware Protection

M. Modarres, M.L. Roush
University of Maryland, Dept. of Chemical & Nuclear Engineering, College Park, Maryland 20742, U.S.A.
R.N.M. Hunt
Baltimore Gas and Electric Co., Fort Smallwood Road Complex,
P.O. Box 1475, Baltimore, Maryland 21203, U.S.A.

ABSTRACT

A brief discussion of the Goal Tree Methodology is presented. The Goal Tree for protection of hardware (Protection Tree) concept is discussed. Utilization of the Protection Tree for determination and assessment of conventional failure mechanisms is discussed. To demonstrate the application of these methods, an example of an equipment protection goal tree is provided together with the analysis for which it was used. In this and other recently performed analyses, the goal tree approach has been shown to be a very powerful and comprehensive method for understanding problems and pointing the way toward a technically sound program for their solution.

1. Introduction

Economic risks associated with ownership and operation of a commercial nuclear power plant can be strongly influenced by the ways in which it is protected from the occurrence of various potentially significant failures. This influence of equipment protection on economics results from the impact that successful protection can have in reducing the average time to restore equipment to operation following a failure (i.e., parameter τ in the unavailability function $U=\lambda\tau$). An analytic method which can be used to evaluate the needs for an equipment protection program which will minimize the impact of all critical equipment failures, no matter their origin, will be described in the remainder of this paper.

The method to be applied in this evaluation requires the development of a goal tree for "Equipment Protection ." The general approach to goal tree development described by N. Hunt and M. Modarres in reference (1) will be utilized in this paper. This goal tree, using descriptive deduction to show the logical structure of the tree, provides the conceptual visualization of all linking factors which influence the overall objective of equipment protection.

The paper will go on to detail how this developed tree can be utilized to evaluate the goals and functions of protection associated with conventional failure mechanisms, but, additionally provide insights into the nature of the information which could be used to both allow an operator to prevent failure and to take action in limiting the damage to the equipment, should failure or degradation occur.

2. Goal Tree Development

To develop a goal tree, the first step involves definition of the top event or "objective" for the tree. This top event,which for a nuclear plant must reflect the economic objective, (equipment protection here) should be explicitly defined in terms which make it a single unambiguous statement. It is from this definition that the analyst will identify and relate all the different plant goals and subgoals which must be achieved to attain the overall economic objective. Typically the objective and its supporting goals are displayed in tree format so that their interrelationships can be clearly represented and easily recognized, as demonstrated graphically in figure 1.

The goal tree is built vertically downward from the objective in levels, wherein the analyst subsequently decomposes each identified goal to its necessary and sufficient set of dependent subgoals. The prime attribute required of the analyst during this task is that he have a broad and expert understanding of the physical processes involved, since it is the achievement of these physical processes by the hardware that will allow their optimal performance and maximization of the objective function. It is this composition of fundamental processes which will be represented in graphical form by the goal trees.

As the vertical detailed development of the tree increases, it is necessary that tests be applied to ensure its accuracy and completeness, and that hierarchy between goals and subgoals is rigorously maintained. This latter requirement is crucial to the tree's being capable of providing the needed framework for future cause-consequence analyses.

The rules or tests which are to be applied at every level of the developed tree to ensure adequacy are:

- o Upon looking <u>upward</u> from any subgoal towards the objective or tree-top, it is possible to explicitly define <u>why</u> the specific goal or subgoal must be satisfied.

- o Upon looking <u>downward</u> from any goal towards the bottom of the tree, it is possible to explicitly define <u>how</u> the specific goal or subgoal is satisfied.

Failure of the tree to pass either of these tests at any level implies that:

- o There is a lack of completeness, and intermediate subgoals have been omitted, or

- o the hierarchy of goals or their interdependencies have neither been rigorously nor completely defined.

The process of downward development of the tree continues until the analyst is unable to further define subgoals without recourse to using references to actual hardware. As soon as hardware is explicitly mentioned, the tree becomes one which describes "success paths", not goals. It is important that this boundary between goals and success paths be recognized because this is the point at which the logical structure of the tree changes. Within the goal tree, all goals must be connected by logical 'AND' gates, whereas the success paths must be connected to the goals they serve by logical 'OR' gate will be used if there is only one success path for any specific goal.

Use of the fact that all connectors in the goal tree are logical 'AND's' can be made in a convention which allows the analyst to provide a means for easy distinction between the goal tree and the hardware success paths. The goal tree is drawn with no gates explicitly defined. If a gate is shown, success paths are being described.

A complete goal tree would provide the analyst with the foundation for a cause-consequence model which can be used to seek information to help the operator to take actions to:

- Prevent failures
- Detect incipient failures and prevent any damage propagation
- Detect failures quickly to limit or minimize consequential damage that would otherwise occur.

3. Reactor Coolant Pump Motor Protection Goal Tree

To demonstrate the practical application of these methods in solving operating plant problems, an example of the use of an equipment protection goal tree will be provided in figure 2 together with a description of the analysis in which it was used. The problem posed, and for which a solution was sought, was whether in an operating nuclear power generating station, there was exposure to a significant level of economic risk originating with the possibility that multiple reactor coolant pump motor failures could occur and result in extended plant shutdown during the replenishment cycle for the single on-hand spare motor. To produce and understand the optimal plan of corrective actions to be followed, a goal tree was developed and used as a foundation for the risk analysis. This analysis provided the means for defining programmatic changes which could be shown to provide cost effective economic risk reduction measures. This goal tree which has an economic equipment protective objective of "Reactor Coolant Pump Motor Damage Prevented" is shown in fig. 2. Since application of industry actuarial data showed that multiple independent failures of reactor coolant pumps presented little economic risk, the source of any significant risk contributors would likely be:

- Common cause failures,
- Aging phenomena which cause time dependent failure rates

The tree in figure 2 was used to identify sources of common cause failures between seemingly independent operating pump motors which occur as a result of activities which involve:

- Maintenance,
- Operations,
- Test,
- Design and construction.

In a similar way, use of the tree allowes the analyst to identify the causes and effects of the various activities and mechanisms associated with aging, so that it is not only possible to establish the need for remedial action, but also to provide the basis for a cost justified and technically sound program of corrective measures for the reactor coolant pumps.

From figure 2,in which all concerns associated with RCP motor protection are shown, it is possible to startidentifying areas of potential common cause/mode interactions which are germane to the RCP motor parts by asking the following questions:

- If a goal or sub-goal is not achieved, will damage lead to a need for motor rewind or repairs of similar magnitude?
- Can the lack of goal or subgoal achievement lead to similar effects or results in more than one motor within the same general time frame?
- Does the lack of goal or subgoal achievement lead to aging phenomena which invalidate the constant failure rate model and lead to consideration of a time-dependent model, which can significantly increase the risk of multiple failures as the plant approaches its expected design life?

When these answers have been addressed with regard to the germane issues of potential common cause/mode, it is possible to determine whether:

- Existing programs address the common cause/mode issues adequately and eliminate the need for additional goals or sub-goals.
- Enhanced information can allow plant personnel to adequately address the common cause/mode issues and remove them as items of concern.
- Additional hardware is needed to provide adequate protection.
- Additional inspections, tear-downs, or active preventive programs are required to provide adequate protection.
- The economic risk is sufficient to justify a second spare motor.

An analysis which employs the method just described above, provides identification of several areas of potential common cause/mode failure mechanisms and causes which are significant to the RCP motor, because they lead to:

1. Bearing failure.
2. Bearing failure which progresses to catastrophic failure of rotor/stator.
3. Catastrophic failures of stator/rotor which originates with component mechanical failure.
4. Winding or core iron failures which originate with failure or deterioration of the RCP motor electrical insulation.

Each identified mechanism which leads to failures such as those listed above could be examined to determine if there were common initiating actions originating from operation, design, or maintenance. As an example let us consider the "RCP Motor Electrical Insulation Failures." From the tree, the following failures among others could be identified:

1. "Failure to Maintain Conductor Location or Orientation".

If the conductors are not adequately constrained, fretting or vibration damage to the insulation can occur. Analgously, if the tightness of connections between conductors is not maintained, there is the possibility of local resistive heating which could lead to failure of insulation. The potential consequences of these failures would be evidenced by damage to the windings or the core iron.

Prevention of this failure mechanism lies with control in the original construction and with subsequent inspection and maintenance activities - any potential contribution to failure rate could be common to each motor, and since the effects would presumably take some time to show themselves, would result in a time-dependent failure

2. "Electrical Properties of the Insulation are Maintained". This sub-goal has several contributions of somewhat different character.

   a. Deterioration of the insulation as a result of aging mechanisms due to the motor, environment, or surface contamination.

   b. Deterioration of the motor insulation as a result of mechanical stress.

   c. Premature aging of the motor insulation resulting from high temperatures.

In all cases, the failure of winding integrity or insulation properties can lead to damage from local arcing. Such damage, if undetected, could progress to severe damage of the windings or the core iron.

Use of the tree by an analyst allowed assessment of the needs for performance of careful examination of mechanical connections and highlighted the need for periodic monitoring to infer the condition of the conductors. Additionally, the benefit of the installation of RF arc detectors and vibration monitoring techniques, in concert with periodic inspection were easily recognized as important contributors to protection, or limitation of the damage to the motors should a failure occur.

Prevention of motor failure can be enchanced to a degree by recognizing how the human can contribute to potential insulation degradation, as a result of his failure to prevent ingress of harmful chemicals (cleaning materials) or moisture. As a result of this recognition of the causes of insulation damage and the coupling between actions at separate pumps, programmatic changes can be implemented to prevent multiple failures.

3. REFERENCE

/1/ Hunt, N., M. Modarres, "Integrated Economic Risk Management in a Nuclear Power Plant," 1984 Annual Meeting, The Society For Risk Analysis, Knoxville, TN., U.S.A., October, 1984.

Fig. 1

A Typical Goal Tree

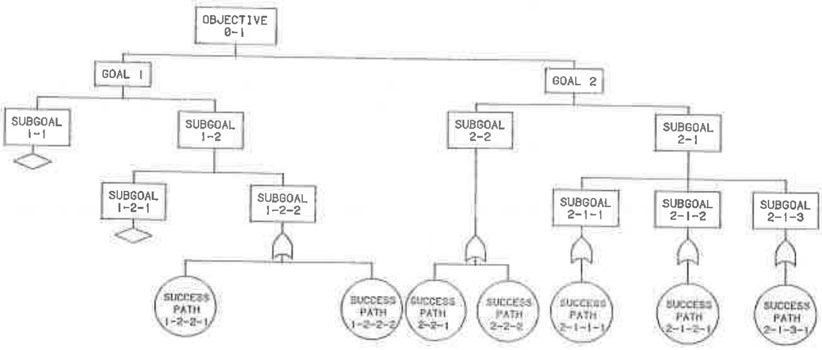

Fig. 2

A Simplified Goal Tree for RCP Motor Protection