Operating Experiences

Edited by William R. Casto

A Review of Safety-Related Occurrences in Nuclear Power Plants as Reported in 1976

By R. L. Scott and R. B. Gallaher

Abstract: *This article reviews the "Reportable Occurrences" submitted in 1976 to the U. S. Nuclear Regulatory Commission concerning light-water-reactor nuclear power plants. The review covers 1253 reports from boiling-water-reactor facilities and 1264 reports from pressurized-water-reactor facilities. Information is presented in tables listing instrument failures, equipment failures, systems involved, causes, deficiencies, and times of occurrence (i.e., refueling, testing, operation, or construction.) The tables give the number of reports concerned with each listed item and therefore indicate the frequencies of events and those events which should receive more attention in the form of maintenance and testing to improve plant reliability and safety.*

This review is based on information obtained from the Nuclear Safety Information Center (NSIC) computer file. The file contains 100-word abstracts of reports to the U. S. Nuclear Regulatory Commission (NRC) submitted by nuclear power-plant licensees. The requirements for submitting operating information to the NRC is described in Regulatory Guide 1.16, *Reporting of Operating Information, Appendix A: Technical Specifications,* Rev. 4, August 1975. Requirements for reporting design or construction deficiencies of facilities that have construction permits are given in *Title 10, Code of Federal Regulations, Part 50, Section 55, Paragraph e.*

For over a decade, NSIC has devoted a portion of its computer file to the storage of information concerning safety-related occurrences at nuclear power plants, and each year the information is retrieved so that a bibliography can be published. The first bibliography contained both 1967 and 1968 reported occurrences, and this has been followed with annual publications.[1-9]

For the reported occurrences in 1976 (as in 1975), two bibliographies were prepared, one for boiling-water-reactor (BWR) plants[10] and one for pressurized-water-reactor (PWR) plants.[11] In preparing the bibliographies, NSIC reviewed more than 2500 abstracts and then prepared tables listing the number of reports associated with a component failure, the system involved, the cause of the incident, etc. Thus the tables indicate the frequencies of component failures and those items which should receive more attention in the form of maintenance or testing. The information obtained is presented here in two parts: first for BWR plants and then for PWR plants.

SUMMARY OF OCCURRENCE DATA FOR BWRs

In 1976, 1253 reports concerned safety-related occurrences at BWRs. Table 1 lists the number of reports concerned with the various systems. In the same order as in 1975, the three systems most frequently reported on were containment isolation, main cooling, and reactor protection. One reason that the containment isolation system was reported on more may be because it encompasses many of the other systems listed, such as main cooling, high-pressure coolant injection (HPCI), reactor core isolation cooling (RCIC), and core spray. The containment isolation system consists of valves and controls

Table 1 Number of Reports Concerned with the Listed Systems for BWRs

System	Percent of total number of reports	Number of reports
Containment isolation	10	130
Main cooling	9	116
Reactor protection	7	82
HPCI*	7	74
RCIC*	5	60
Shutdown cooling	5	60
Pressure relief	4	51
Emergency power	4	49
Core spray	3	38
LPCI	3	36
Ventilation	2	30
Condenser cooling	2	29
Waste disposal	2	29
Emergency cooling	2	26
Electric power	2	22
Radiation monitoring	2	21
Coolant purification	1	18
Service water	1	17
Feedwater	1	16
Secondary shutdown	1	15
Containment purge	1	14
Cooling tower	1	13
Pneumatic	1	13
Standby gas treatment	1	13
Containment spray	1	11
Auxiliary cooling	<1	6
Hydraulic	<1	4
Component cooling	<1	3

*HPCI = high-pressure coolant injection; RCIC = reactor core isolation cooling; LPCI = low-pressure coolant injection.

required to isolate the many lines penetrating the containment, and it follows that most of the reports on this system involve malfunctioning valves and controls—approximately 61% of the reports are concerned with valves and approximately 26% with instrument switches. It should also be pointed out that the major or critical systems were reported on more often than the less important systems; however, this only reflects the attention given to these major systems by the utilities in the form of surveillance testing, etc., and the emphasis given them in the Nuclear Regulatory Commission's reporting requirements.

Table 2 lists the number of reports concerned with the various items of equipment. Again in 1976 as in previous years, valves, piping, and pumps were the equipment items that experienced problems most frequently. These three items accounted for over one-third of the reports. Diesel generators, seals, and valve operators accounted for another 15% of the reports; thus the first six items in the list accounted for 50% of the reports.

Table 3 lists various kinds of instrumentation that presented problems during 1976 and the number of

Table 2 Number of Reports Concerned with the Listed Equipment for BWRs

Equipment	Percent of total number of reports	Number of reports
Valves	20	246
Pipes and fittings	9	110
Pumps	6	80
Diesel generator	6	74
Seals	5	68
Valve operators	4	51
Cables and connectors	4	46
Support structures	4	44
Turbines	3	41
Shock absorbers	3	37
Breakers	2	29
Control-rod drives	2	27
Solenoids	2	27
Filters, screens	2	26
Check valves	2	26
Fasteners	2	22
Storage containers	2	20
Bearings	2	19
Pressure vessels	2	19
Control rods	1	16
Batteries and chargers	1	15
Containment vacuum breakers	1	15
Motors	1	15
Blowers	1	14
Tubing	1	10
Filters	1	9
Generators	1	8
Transformers	1	7
Fuel elements	<1	6
Heat exchangers	<1	6
Heaters	<1	6
Nozzles	<1	6
Accumulators	<1	5
Flanges	<1	4
Cranes	<1	3
Demineralizers	<1	3
Insulation	<1	3
Jet pumps	<1	3
Air driers	<1	2
Digital computer	<1	2
Recombiners	<1	2

Table 3 Number of Reports Concerned with the Listed Instrumentation for BWRs

Instrumentation	Percent of total number of reports	Number of reports
Switch	22	271
Pressure sensor	10	128
Radiation monitors	5	68
Level sensor	4	56
Relays	3	43
Flow sensor	2	28
Electronic function unit	2	23
Temperature sensor	2	23
Position sensor	2	20
Recorders	2	20
Power range instrument	1	17
Stack monitor	1	13
Air monitor	1	11
In-core instrument	1	10
Intermediate range instrument	1	7
Annunciators	<1	6
Solid-state device	<1	6
Containment leak monitor	<1	5
Indicators	<1	5
Startup range instrument	<1	5
Thermocouple	<1	5
Alarms	<1	3

Table 4 Number of Reports Concerned with the Listed Cause of Safety-Related Occurrences for BWRs

Cause of occurrence	Percent of total number of reports	Number of reports
Inherent failure	32	395
Maintenance error	12	153
Design error	10	128
Administrative error	9	113
Operator error	7	90
Installation error	4	54
Fabrication error	2	23
Weather	1	11

Table 5 Number of Reports for the Listed Time of Occurrence of Off-Normal Events for BWRs

Time of occurrence	Percent of total number of reports	Number of reports
Operation	42	528
Testing	45	559
Refueling	10	131
Construction	3	35

reports concerned with each item. Since 1971, when similar tables were first prepared, switches have been at the top of the list, accounting for more malfunctions than other instruments. Apparently the reason for this is the large number of switches in safety-related systems and their delicacy and sensitivity. As shown in Table 6, at least 167 of these reports involved set-point drift, which has been a problem for years. Various monitors and sensors account for most of the remaining reports on instrumentation problems.

Table 4 lists the identified causes of the safety-related occurrences and the number of reports concerned with each cause. Inherent failures were involved in 32% of the occurrences. Examples of items considered to be inherent include (1) excessive fish impingement on intake screens, (2) instrument set-point drift, and (3) spurious trips of instruments or equipment. Approximately 23% of the reports did not give a cause of failure, and in most of these cases an investigation was continuing.

Table 5 lists the various time periods in which the events took place and the associated number of reports. The 559 events that were discovered (or occurred) during testing could be remedied with little or no effect on operation.

Table 6 is a list of items considered to be of interest and the associated number of reports. In 1976 as in previous years, instrument calibration and set-point drift were the most frequently reported items, followed closely by piping and seal leaks. Procedural deficiencies most frequently involved inadequate procedures, but failure of operators to follow procedures is included. "Communication" is a new item that has been added, and it represents primarily those events involving a misunderstanding between personnel.

Table 7 is an alphabetical listing of the nuclear reactor units and the associated number of reports. Those nuclear units which were in commercial operation all year are listed first, followed by those which were in the power-ascension phase part of the year, and then by those which were under construction all year. There are 35 nuclear reactor units listed in Table 7. For the 22 nuclear units that were operable all year, there are 1157 reports, an average of 52 reports per unit. For the 3 units in the power-ascension phase, there are 134 reports, an average of 44 reports per unit. For the 10 units that were under construction all year, there are 34 reports, an average of 3 reports per year. The total number of reports listed in Table 7 is 1325, whereas

Table 6 Number of Reports Concerned with the Listed Deficiency for BWRs

Deficiency	Percent of total number of reports	Number of reports
Instrument calibration	14	181
Set-point drift	13	167
Leakage	9	114
Procedures	6	78
Crud	4	55
Cracks	3	35
Welds	3	32
Flow blockage	2	29
Vibration	2	24
Airborne release	2	23
Communication	2	22
Response time	2	22
Fish or crab mortality	2	21
Wear	2	21
Lubrication	1	16
Liquid radioactivity release	1	15
Corrosion	1	14
Fire	1	12
Age effect	1	7
Erosion	<1	5
Personnel exposure	<1	4
Lightning	<1	2

the bibliography contains abstracts of 1253 reports. The reason for this discrepancy is that a few of the reports involved more than one unit of a multiple-unit plant, and this is particularly true of those units which were under construction.

Tables 8a and 8b tabulate the number of reports for the listed units that were commercially operable all year. In Table 8a the tabulation is by plant age, and in Table 8b the tabulation is by power, design electrical rating (DER) in electrical megawatts [MW(e)]. These tables were prepared to see if age or power level was a factor in the number of occurrences reported by a nuclear unit. Both age and power level appear to be factors, although it may not be readily apparent from just looking at the tables.

The total number of reports for the 11 oldest reactors is 379. The number of reports for the 11 most recently built reactors is 778, more than twice the number of reports as for the older reactors. This tends to indicate that there will be fewer failures or malfunctions of safety-related equipment as the unit ages and experience is gained in operation.

The same type of count was made based on power level. The number of reports for the 11 smallest units is 410. The number of reports for the 11 largest units is 747, almost double the number for the smaller units. This seems to indicate that fewer problems can be expected with smaller units.

It should be recognized that the data presented are not absolute, especially when you consider that the reporting habits throughout the industry may not be uniform, but the tables and data do seem to indicate that a low-powered older reactor will probably have fewer problems than a high-powered newly built reactor. However, one factor to be considered with this conclusion is that the newly built reactors are the larger units, and thus far the feedback of operating information from operators to designers of these larger units has been limited.

The final bit of information gleaned from reviewing the reports of occurrences at BWRs in 1976 is that 48 of the 1253 reports indicated that a reactor shutdown occurred or was required because of equipment failure or malfunction.

SUMMARY OF OCCURRENCE DATA FOR PWRs

In 1976, 1264 reports concerned safety-related occurrences at PWRs. Table 9 lists the number of reports concerned with the various systems. As in 1975, the same four systems were involved in more occurrences than any of the others; these four systems are reactor protection, main cooling, feedwater, and containment isolation. Combined, these systems accounted for 31% of the total number of reports in 1976. The condenser cooling system was also involved in a substantial number of reports, accounting for 7% of the total number.

Table 10 lists the number of reports concerned with the various items of equipment. Whereas in 1975 the pipes, pumps, and valves were involved in about the same number of occurrences, in 1976 the valves accounted for nearly twice as many reports as for pipes and more than twice as many reports as for pumps. Valves accounted for 16% of the total number of reports, pipes accounted for 9%, and pumps accounted for 8%.

Table 11 lists the number of reports concerned with the listed instrumentation. Again in 1976 as in every year since 1972, switches accounted for more occurrence reports than other instruments. In 1976, switches were reported 166 times, accounting for 13% of the total number of reports. Lagging far behind were relays, pressure sensors, and electronic function units,

Table 7 Number of Reports Involving the Alphabetically Listed BWR Units

Plant	Percent of total number of reports	Number of reports	Plant age, years	Design electrical rating, net MW(e)
In Commercial Operation All Year				
Arnold	8	98	2.6	538
Big Rock Point	3	40	14.1	72
Browns Ferry 1	2	26	3.2	1065
Browns Ferry 2	2	23	2.3	1065
Brunswick 2	16	197	1.7	821
Cooper	4	56	2.6	778
Dresden 1	1	18	16.7	200
Dresden 2	6	70	6.7	809
Dresden 3	3	40	5.4	809
FitzPatrick	7	93	1.9	821
Humboldt Bay	1	12	13.7	63
La Crosse	1	17	8.7	50
Millstone 1	5	58	6.1	650
Monticello	2	24	5.8	545
Nine Mile Point 1	3	32	7.2	610
Oyster Creek	2	29	7.3	650
Peach Bottom 2	8	99	2.9	1065
Peach Bottom 3	7	83	2.3	1065
Pilgrim 1	3	33	4.5	655
Quad Cities 1	3	39	4.7	789
Quad Cities 2	2	21	4.6	789
Vermont Yankee	4	49	4.3	514
In Power Ascension for Part of the Year				
Browns Ferry 3	2	31		
Brunswick 1	1	8		
Hatch 1	8	95		
Under Construction All Year				
Grand Gulf 1	1	9		
Grand Gulf 2	1	10		
Hanford 2	<1	1		
Hartsville 1	<1	2		
Hartsville 2	<1	2		
Hartsville 3	<1	2		
Hartsville 4	<1	2		
La Salle 1	<1	2		
La Salle 2	<1	2		
Shoreham	<1	2		

with each accounting for about 50 reports, or 4% of the total.

Table 12 lists the number of reports for which a cause of failure was identified. Inherent failures were involved in 26% of the reports. The causes listed accounted for 85% of the reports; the remaining 15% of the reports did not state a reason for failure, and most indicated that further investigation was required.

Table 13 lists the times of occurrence of the various events and the number of reports associated with the time periods.

Table 14 lists additional items considered of interest, with the indicated number of reports associated with each item.

Tables 15a and 15b present an alphabetical listing of the pressurized-water-reactor units and the

Table 8a Number of Reports for the Listed BWR Units That Were Commercially Operable All Year

Plant	Plant age, years	Percent of total number of reports	Number of reports
By Age Since First Electrical Generation, years*			
Dresden 1	16.7	1	18
Big Rock Point	14.1	3	40
Humboldt Bay	13.7	1	12
La Crosse	8.7	1	17
Oyster Creek	7.3	2	29
Nine Mile Point 1	7.2	3	32
Dresden 2	6.7	6	70
Millstone 1	6.1	5	58
Monticello	5.8	2	24
Dresden 3	5.4	3	40
Quad Cities 1	4.7	3	39
Quad Cities 2	4.6	2	21
Pilgrim 1	4.5	3	33
Vermont Yankee	4.3	4	49
Browns Ferry 1	3.2	2	26
Peach Bottom 2	2.9	8	99
Arnold	2.6	8	98
Cooper	2.6	4	56
Browns Ferry 2	2.3	2	23
Peach Bottom 3	2.3	7	83
FitzPatrick	1.9	7	93
Brunswick 2	1.7	16	197

*Average age, 5.9 years; median age, 4.7 years.

ciated number of reports. Those reactors which were in commercial operation all year are listed in Table 15a. Table 15b lists those which were in the power-ascension phase part of the year and those which were under construction all year. Counting Indian Point 1, which was shut down all year, 64 nuclear reactor units are listed in Tables 15a and 15b. For the 30 nuclear units that were operational all year, there are 1036 reports, an average of 34 reports per unit. For the 6 units in the power-ascension stage, there are 167 reports, an average of 28 reports per unit. For the 27 units that were under construction, there are 157 reports, an average of 6 reports per unit. It should be pointed out that Table 15b indicates that there are 1363 reports, whereas the bibliography contains abstracts of 1264 reports. The reason for this discrepancy is that a few of the reports involved more than one unit of a multiple-unit plant, and this is particularly true of those units which were under construction.

Tables 16a and 16b tabulate the number of reports for the listed units that were commercially operable all year. In Table 16a the tabulation is by plant age, and in Table 16b the tabulation is by power, design electrical rating (DER) in megawatts electrical [MW(e)]. These tables were prepared to see if age or power level was a factor in the number of occurrences reported by a nuclear unit. Both age and power level appear to be factors, although it may not be readily apparent from just looking at the tables.

The total number of reports for the 15 oldest reactors is 343. The number of reports for the 15 most recently built reactors is 693, more than twice as many reports as for the older reactors. This tends to indicate that there will be fewer failures or malfunctions of safety-related equipment as the unit ages and experience is gained in operation.

The same type of count was made based on power level. The number of reports for the 15 smallest units is 376. The number of reports for the 15 largest units is 660, almost double the number for the smaller units. This seems to indicate that fewer problems can be expected with smaller units.

Table 8b Number of Reports for the Listed BWR Units That Were Commercially Operable All Year

Plant	Design electrical rating, net MW(e)	Percent of total number of reports	Number of reports
By Design Electrical Rating, net MW(e)*			
Browns Ferry 1	1065	2	26
Browns Ferry 2	1065	2	23
Peach Bottom 2	1065	8	99
Peach Bottom 3	1065	7	83
Brunswick 2	821	16	197
FitzPatrick	821	7	93
Dresden 2	809	6	70
Dresden 3	809	3	40
Quad Cities 1	789	3	39
Quad Cities 2	789	2	21
Cooper	778	4	56
Pilgrim 1	655	3	33
Millstone 1	650	5	58
Oyster Creek	650	2	29
Nine Mile Point 1	610	3	32
Monticello	545	2	24
Arnold	538	8	98
Vermont Yankee	514	4	49
Dresden 1	200	1	18
Big Rock Point	72	3	40
Humboldt Bay	63	1	12
La Crosse	50	1	17

*Average DER, 656 MW(e); median DER, ~717 MW(e).

Table 9 Number of Reports Concerned with the Listed Systems for PWRs

System	Percent of total number of reports	Number of reports
Reactor protection	9	112
Main cooling	8	105
Feedwater	7	93
Containment isolation	7	92
Condenser cooling	7	91
Secondary cooling	6	71
Electric power	5	69
Safety injection	3	44
Emergency power	3	40
Chemical and volume control	3	34
Engineered safety feature	2	29
Waste disposal	2	28
Ventilation	2	26
Containment purge	2	24
Shutdown cooling	2	22
Containment air cooling	2	21
Pneumatic	2	20
Containment spray	1	16
Emergency cooling	1	16
Service water	1	16
Coolant purification	1	14
Cooling tower	1	14
Component cooling	1	13
Radiation monitoring	1	13
Reactor control	<1	10
Spent-fuel storage	<1	7
Waste storage	<1	6

It should be recognized that the data presented are not absolute, especially since the reporting habits throughout the industry may not be uniform, but the tables and data do seem to indicate that a low-powered older reactor will probably have fewer problems than a high-powered newly built reactor. Yankee Rowe and Trojan seem to bear this out. However, as with the BWR data, one factor to be considered in this conclusion is that the newly built reactors are the larger units, and thus far the feedback of operating information from operators to designers of these units has been limited.

The final bit of information gleaned from reviewing the reports of occurrences at PWRs in 1976 is that 41 of the 1264 reports indicated that a reactor shutdown occurred or was required because of equipment failure or malfunction.

A review of the units that were operational all year indicates that 1157 reports were received from the 22 BWR units, or an average of 52 reports per unit. From the 30 PWR units, 1036 reports were received, or an average of 34 reports per unit. A review based on plant age indicates that 379 reports were received from the 11 oldest BWRs, and 343 reports were received from the 15 oldest PWRs; whereas 778 reports were received from the 11 most recently built BWRs, and 693 reports were received from the 15 most recently built PWRs.

Table 10 Number of Reports Concerned with the Listed Equipment for PWRs

Equipment	Percent of total number of reports	Number of reports
Valves	16	208
Pipes and pipe fittings	9	109
Pumps	8	103
Steam generators	6	71
Diesel generators	5	67
Storage container	5	62
Breakers	5	57
Cables and connectors	4	54
Seals	4	50
Support structures	4	45
Intake screens	3	41
Tubing	3	36
Valve operators	3	31
Shock absorbers	2	25
Accumulators	2	21
Control rods	2	21
Heat exchangers	2	21
Bearings	2	20
Control-rod drives	2	20
Heaters	1	17
Blowers	1	16
Solenoids	1	14
Cranes	1	13
Fasteners	1	13
Pressure vessels	1	13
Batteries and chargers	1	12
Insulation	1	12
Turbines	1	12
Fuel	<1	11
Generators	<1	11
Check valves	<1	11
Motors	<1	10
Filters	<1	9
Digital computer	<1	7
Condenser	<1	7
Nozzle	<1	7
Transformers	<1	7
Containment ice condenser	<1	6
Flanges	<1	4
Containment vacuum breakers	<1	3
Air driers	<1	2

Table 11 Number of Reports Concerned with the Listed Instrumentation for PWRs

Instrumentation	Percent of total number of reports	Number of reports
Switch	13	166
Relays	4	54
Pressure sensor	4	50
Electronic function unit	4	49
Level sensor	3	36
Power range instrument	3	35
Flow sensor	2	27
Temperature sensor	2	26
Position instrument	1	12
Solid-state device	1	12
Annunciators	<1	7
Containment leak monitor	<1	7
Indicators	<1	4
Intermediate range instrument	<1	4
Startup range instrument	<1	4
Area monitor	<1	3
Stack monitor	<1	3

Table 12 Number of Reports Concerned with the Listed Cause for PWRs

Cause of occurrence	Percent of total number of reports	Number of reports
Inherent failure	26	324
Design error	16	199
Maintenance error	10	129
Administrative error	10	121
Operator error	9	117
Installation error	7	87
Fabrication error	5	68
Weather	2	26

This indicates that age is a factor for both BWRs and PWRs, and a unit with more years of operation and experience can expect to have fewer difficulties.

The review based on the design electrical rating of the units indicates that 410 reports were submitted for the 11 smallest BWRs, and 747 reports were submitted for the 11 largest BWRs; 376 reports were submitted for the 15 smallest PWRs, and 660 reports were submitted for the 15 largest PWRs. This indicates that the power level is a factor for both BWRs and PWRs, and a unit with a low power level can expect to have fewer difficulties. Therefore the most trouble-free unit should be a low-powered older reactor.

There were 48 shutdowns at BWRs and 41 shutdowns at PWRs discussed in the reports. These shutdowns were either direct results of the occurrences reported or were required subsequent to the occurrences.

The review indicates that there was considerable similarity between the PWRs and BWRs, especially with respect to systems, components, and causes of the safety-related occurrences. The only significant difference noted was that the average number of occurrences at an operating BWR unit was 50% greater than the number at a PWR unit. A review of both types of plants indicates that age and size are factors in the

Table 13 Number of Reports for the Listed Time of Occurrence of Off-Normal Events for PWRs

Time of occurrence	Percent of total number of reports	Number of reports
Operation	51	641
Testing	30	378
Construction	12	156
Refueling	7	89

Table 14 Number of Reports Concerned with the Listed Deficiency for PWRs

Deficiency	Percent of total number of reports	Number of reports
Leakage	11	140
Set-point drift	7	92
Instrument calibration	7	88
Procedures	6	74
Welds	5	63
Crud	3	41
Fish or crab mortality	3	37
Quality assurance	2	29
Corrosion	2	28
Vibration	2	28
Wear	2	25
Communication	2	23
Lubrication	2	23
Airborne release	2	21
Fatigue	2	21
Response time	1	17
Records	1	14
Liquid activity release	1	13
Personnel exposure	<1	9
Fire	<1	5
Stress corrosion	<1	5
Erosion	<1	4

Table 15a Number of Reports Involving the Alphabetically Listed PWR Units That Were Commercially Operable All Year

Plant	Percent of total number of reports	Number of reports	Plant age, years	Design electrical rating, net MW(e)
Arkansas Nuclear 1	3	40	2.4	850
Calvert Cliffs 1	4	50	2.0	845
Connecticut Yankee	2	21	9.4	575
Cook 1	5	64	1.9	1054
Fort Calhoun	3	46	3.4	457
Ginna	2	27	7.1	490
Indian Point 2	2	28	3.5	873
Kewaunee	2	32	2.7	535
Maine Yankee	1	17	4.1	790
Millstone 2	6	81	1.1	828
Oconee 1	2	34	3.7	887
Oconee 2	2	30	3.1	887
Oconee 3	2	33	2.3	887
Palisades	3	36	5.0	668
Point Beach 1	1	9	6.2	497
Point Beach 2	1	16	4.4	497
Prairie Island 1	3	47	3.1	530
Prairie Island 2	3	41	2.0	530
Rancho Seco	1	19	2.2	913
Robinson 2	2	26	6.3	712
San Onofre 1	2	27	9.5	430
Surry 1	3	36	4.5	822
Surry 2	3	35	3.8	822
Three Mile Island 1	3	43	2.5	819
Trojan	4	59	1.0	1130
Turkey Point 3	1	10	4.2	693
Turkey Point 4	1	7	3.5	693
Yankee Rowe	1	14	16.1	175
Zion 1	5	66	3.5	1040
Zion 2	3	42	3.0	1040

Table 15b Number of Reports Involving the Alphabetically Listed PWR Units*

Plant	Percent of total number of reports	Number of reports
In Power Ascension for Part of the Year		
Beaver Valley 1	1	15
Calvert Cliffs 2	1	13
Crystal River 3	1	9
Indian Point 3	4	48
St. Lucie 1	4	54
Salem 1	2	28
Under Construction All Year		
Arkansas Nuclear 2	<1	4
Beaver Valley 2	<1	2
Bellefonte 1	<1	6
Callaway 2	<1	1
Catawba 2	<1	1
Comanche 1	<1	2
Comanche 2	<1	1
Davis Besse 1	1	16
Diablo Canyon 1	<1	1
Farley 1	1	7
Farley 2	<1	1
McGuire 1	1	9
McGuire 2	1	7
Midland 1	<1	2
Midland 2	<1	2
Millstone 3	<1	2
North Anna 1	2	23
North Anna 2	2	22
Salem 2	<1	1
San Onofre 2	<1	6
San Onofre 3	<1	6
Summer 1	<1	4
Surry 3	<1	2
Surry 4	<1	2
Waterford 3	<1	3
Watts Bar 1	1	12
Watts Bar 2	1	12

*Three reports involved Indian Point 1, which was shut down all year with no decision on its future.

Table 16a Number of Reports for the Listed PWR Units That Were Commercially Operable All Year

Plant	Plant age, years	Percent of total number of reports	Number of reports
By Age Since First Electrical Generation, Years*			
Yankee Rowe	16.1	1	14
San Onofre 1	9.5	2	27
Connecticut Yankee	9.4	2	21
Ginna	7.1	2	27
Robinson 2	6.3	2	26
Point Beach 1	6.2	1	9
Palisades	5.0	3	36
Surry 1	4.5	3	36
Point Beach 2	4.4	1	16
Turkey Point 3	4.2	1	10
Maine Yankee	4.1	1	17
Surry 2	3.8	3	35
Oconee 1	3.7	3	34
Indian Point 2	3.5	2	28
Turkey Point 4	3.5	1	7
Zion 1	3.5	5	66
Fort Calhoun	3.4	3	46
Oconee 2	3.1	2	30
Prairie Island 1	3.1	3	47
Zion 2	3.0	3	42
Kewaunee	2.7	2	32
Three Mile Island 1	2.5	3	43
Arkansas Nuclear 1	2.4	3	40
Oconee 3	2.3	2	33
Rancho Seco	2.2	1	19
Calvert Cliffs 1	2.0	4	50
Prairie Island 2	2.0	3	41
Cook 1	1.9	5	64
Millstone 2	1.1	6	81
Trojan	1.0	4	59

*Average age, 4.3 years; median age, 3.5 years.

Table 16b Number of Reports for the Listed PWR Units That Were Commercially Operable All Year

Plant	Design electrical rating, net MW(e)	Percent of total number of reports	Number of reports
By Design Electrical Rating, Net MW(e)*			
Trojan	1130	4	59
Cook 1	1054	5	64
Zion 1	1040	5	66
Zion 2	1040	3	42
Rancho Seco	913	1	19
Oconee 1	887	2	34
Oconee 2	887	2	30
Oconee 3	887	2	33
Indian Point 2	873	2	28
Arkansas Nuclear 1	850	3	40
Calvert Cliffs 1	845	4	50
Millstone 2	828	6	81
Surry 1	822	3	36
Surry 2	822	3	35
Three Mile Island 1	819	3	43
Maine Yankee	790	1	17
Robinson 2	712	2	26
Turkey Point 3	693	1	10
Turkey Point 4	693	1	7
Palisades	668	3	36
Connecticut Yankee	575	2	21
Kewaunee	535	2	32
Prairie Island 1	530	3	47
Prairie Island 2	530	3	41
Point Beach 1	497	1	9
Point Beach 2	497	1	16
Ginna	490	2	27
Fort Calhoun	457	3	46
San Onofre 1	430	2	27
Yankee Rowe	175	1	14

*Average DER, 732 MW(e); median DER, ~805 MW(e).

number of difficulties that will be experienced, with the smaller and older units experiencing fewer malfunctions. However, in evaluating this conclusion, one should consider the fact that the newly built plants are the larger plants, and to date the feedback of operating experience information to designers has been limited.

The data presented here have conveyed only negative impressions of plant operations, and it should be remembered that other, more favorable types of information are also used to evaluate the overall performance of a plant. Because of the multiple levels of protection, or defense in depth, including the provision of redundant safety systems and components, such events as have been considered in this review generally do not have an actual impact or consequence on the health and safety of the public. However, the information can be used to improve safety, plant reliability, and plant availability, and this is the purpose for which the review was intended.

REFERENCES

1. E. N. Cramer and W. R. Casto, *Safety-Related Occurrences in Nuclear Facilities as Reported in 1967 and 1968*, USAEC Report ORNL/NSIC-69, Oak Ridge National Laboratory, NTIS, 1970.
2. R. L. Scott and W. R. Casto, *Safety-Related Occurrences in Nuclear Facilities as Reported in 1969*, USAEC Report ORNL/NSIC-87, Oak Ridge National Laboratory, NTIS, 1971.
3. R. L. Scott, *Safety-Related Occurrences in Nuclear Facilities as Reported in 1970*, USAEC Report ORNL/NSIC-91, Oak Ridge National Laboratory, NTIS, 1971.
4. R. L. Scott and R. B. Gallaher, *Safety-Related Occurrences in Nuclear Facilities as Reported in 1971*, USAEC Report ORNL/NSIC-106, Oak Ridge National Laboratory, NTIS, 1972.
5. R. L. Scott and R. B. Gallaher, *Safety-Related Occurrences in Nuclear Facilities as Reported in 1972*, USAEC Report ORNL/NSIC-109, Oak Ridge National Laboratory, NTIS, 1973.
6. R. L. Scott and R. B. Gallaher, *Annotated Bibliography of Safety-Related Occurrences in Nuclear Power Plants as Reported in 1973*, USAEC Report ORNL/NSIC-114, Oak Ridge National Laboratory, NTIS, 1974.
7. R. L. Scott and R. B. Gallaher, *Annotated Bibliography of Safety-Related Occurrences in Nuclear Power Plants as Reported in 1974*, ERDA Report ORNL/NSIC-122, Oak Ridge National Laboratory, NTIS, 1975.
8. R. L. Scott and R. B. Gallaher, *Annotated Bibliography of Safety-Related Occurrences in Boiling-Water Nuclear Power Plants as Reported in 1975*, NRC Report ORNL/NUREG/NSIC-126, Oak Ridge National Laboratory, NTIS, 1976.
9. R. L. Scott and R. B. Gallaher, *Annotated Bibliography of Safety-Related Occurrences in Pressurized-Water Nuclear Power Plants as Reported in 1975*, NRC Report ORNL/NUREG/NSIC-127, Oak Ridge National Laboratory, NTIS, 1976.
10. R. L. Scott and R. B. Gallaher, *Annotated Bibliography of Safety-Related Occurrences in Boiling-Water Nuclear Power Plants as Reported in 1976*, NRC Report ORNL/NUREG/NSIC-137, Oak Ridge National Laboratory, NTIS, 1977.
11. R. L. Scott and R. B. Gallaher, *Annotated Bibliography of Safety-Related Occurrences in Pressurized-Water Nuclear Power Plants as Reported in 1976*, NRC Report ORNL/NUREG/NSIC-138, Oak Ridge National Laboratory, NTIS, 1977.

It may also be possible to apply the safety functions listed in the body of this Safety Guide to develop classification systems in the areas of quality assurance, in-service inspection, seismic classification, etc. These additional potential applications are not provided in this version of the Safety Guide but may be subjects of future revisions and extensions of this Safety Guide or may be part of other IAEA Safety Guides.

2. SAFETY FUNCTIONS

2.1 INTRODUCTION

Safety in this document refers to the need to limit to acceptable levels the radiation exposure of the public and site personnel for all operational states and accident conditions of the nuclear power plant.

To ensure adequate nuclear safety, the following general safety criteria, derived from the Code of Practice - Design, shall be met by the plant design:

1. Means shall be provided to shut down the reactor safely and maintain it in the safe shutdown condition following all plant operational states and accident conditions.
2. Means shall be provided to remove residual heat from the core following reactor shutdown under all circumstances.
3. Means shall be provided to reduce the potential for, and to limit, the release of radioactive material to the acceptable limits during all operational states and accident conditions.

The safety functions listed in the following section enable the design to meet these general criteria. These safety functions include those necessary to prevent an accident as well as those necessary to mitigate the consequences of an accident. They can be accomplished, as appropriate, using systems, components or structures provided for normal operation or provided to prevent anticipated operational occurrences from leading to accidents or provided to mitigate the consequences of an accident.

2.2 LIST OF SAFETY FUNCTIONS

The safety functions are:

GE -12/21/71

(a) To control the reactor ~~during normal operation and~~ during those anticipated operational occurrences not requiring shutdown.

(b) To maintain the reactor in a safe shutdown condition following all shutdown actions.

(c) To shut down the reactor as required to mitigate the consequences of anticipated operational occurrences and accident conditions. (See also [d]).

(d) To shut down the reactor following a loss-of-coolant accident where such shutdown action is necessary to permit acceptable cooling of the reactor core. *

(e) To maintain sufficient reactor-coolant inventory for core cooling during all operational states and accident conditions.

(f) To remove heat from the core** following a failure of the reactor coolant pressure boundary in order to limit fuel damage.

(g) To remove residual heat** during appropriate operational states and accident conditions with the reactor coolant pressure boundary intact.

(h) To transfer heat from other safety systems to the ultimate heat sink(s). This is a support function for those other safety systems when they are required to perform their safety functions.

(i) To ensure necessary power (electric, pneumatic, hydraulic, etc.) as a support function for a safety system.

---

* Note that this safety function is a special case of safety function (c) and applies to reactor designs wherein the loss of the coolant medium from the reactor core does not provide an adequate inherent shutdown mechanism.

** These safety functions apply to the first step of the heat removal system(s). The remaining step(s) are encompassed in safety function (h).

(j) To maintain acceptable integrity of the cladding of the fuel in the reactor core.

(k) To maintain the integrity of the reactor coolant pressure boundary.

(l) To limit the release of radioactive material from the reactor containment following an accident that releases radioactive material within the reactor containment.

(m) To keep the exposure of the public and site personnel within the appropriate acceptable limits following an accident that releases radioactive materials from sources outside the reactor containment.

(n) To limit the discharge or release of radioactive waste and airborne radioactive material below acceptable levels during all operational states.

(o) To maintain environmental control within the nuclear power plant for the operation of safety systems and for personnel habitability necessary to allow performance of operations important to safety.

(p) To maintain control of radioactive releases for irradiated fuel transported or stored outside the reactor coolant system.

(q) To remove decay heat from irradiated fuel stored outside the reactor coolant system.

(r) To maintain sufficient subcriticality of fuel stored outside the reactor coolant system.

(s) To prevent the failure or limit the consequences of failure of a component or structure whose failure would cause the impairment of a safety function.

2.3 APPLICATIONS OF SAFETY FUNCTIONS

The list of Safety Functions provided in Section 2.2 may be utilized to satisfy one or both of the following objectives:

1. To provide a reference list to serve as a basis for determining if a system, component or structure performs or contributes to one or more safety functions.

2. To group safety functions, as appropriate, to serve particular end usages. For certain purposes, this selection may be done in such a way as to establish an appropriate order of importance to safety of the safety function.

   Such groupings of safety functions in accordance with their relative importance to safety are termed safety classes. The general methodology for ranking of safety functions is discussed in Section 3 which follows. One purpose of establishing safety classes is to provide a basis for assigning an appropriate gradation in design requirements. This is discussed in more detail in Section 4.

An example of the establishment of safety classes to determine particular design requirements for fluid retaining boundaries of components is given in Appendix A.

It is possible that the establishment of safety classes may prove useful with regard to classifying other types of components and for other considerations such as seismic requirements, quality assurance, etc.

3. RANKING OF SAFETY FUNCTIONS

3.1 INTRODUCTION

Safety functions are those functions necessary to achieve the general safety criteria given in Section 2.1. It follows that failure to accomplish a safety function could lead to a reduction in safety in terms

of the possible increase in radiation exposure. In Section 3.2 a methodology is given for ranking safety functions.

As stated in the Introduction (Section 1) to this Guide and in Section 2.3 various subjects such as quality assurance, in-service inspection, and seismic classification etc. may be classified in future extensions of this guide. It is expected that the number of safety classes used would depend on the subject that is being classified, the number of safety functions affected by component failure and other factors (See Section 4.1).

Regardless of the subject that is classified, or the number of safety classes used, the system is generally applicable. The same 19 safety functions would be considered and the same general methodology would be used to rank the safety functions. However, the distribution of the safety functions among the safety classes could differ in other appendices added to future editions of this Safety Guide.

The requirements assigned to each safety class would also depend on the subject being classified. If the subject being classified were in-service inspection, there would be in-service inspection requirements for each safety class. Appropriate to the appendix issued with the present version of this guide, structural integrity requirements are given for fluid retaining components.

As stated earlier, a mixture of deterministic and probabilistic methods have been used in various Member States to assign graduated requirements to systems, components, and structures important to safety. The deterministic method may differ from one appendix of this Guide to another. The general probabilistic method, outlined below, should be applicable to all appendices.

3.2 METHODOLOGY

The ranking of a safety function in order of its importance by the probabilistic method considers the combination of:

1. The consequence of failure of that safety function and;
2. The probability that the safety function would be required.

The first point considers only the magnitude of the potential increase in radiation exposure upon failure of that safety function. In general when these analyses show that the consequences of failure are large for a postulated accident the safety function will usually get a high ranking. For example, the consequences of failure of Safety Function (k) can be quite large. By contrast, the consequences of failure of Safety Function (n), is small. In the appendix we find that Safety Function (k) is ranked higher than Safety Function (n).

The second point considers only the probability that the safety function will be required. To illustrate this it is useful to compare Safety Functions (k) and (f). The consequences of failure of Safety Function (k), as stated above, can be quite large. Similarly the consequences of failure of Safety Function (f) are also quite large. However, Safety Function (f) is only required after an accident. Failure of Safety Function (f) independent of an accident would not lead to a potential increase in radiation exposure. In the appendix we find that Safety Function (f) is ranked lower than Safety Function (k).

Thus any ranking of safety functions should include considerations of probability as well as consequences of failure. The judgements used in the appendix of this Safety Guide for the ranking of the safety functions reflect the analyses performed in various Member States of numerous postulated accidents for the various reactor types. These analyses have directly and/or indirectly evaluated the probability that a safety function would be required and the consequences of failure to accomplish this safety function where there is an assumed failure of a fluid retaining boundary. The same general methodology could be used to rank safety functions for other applications.

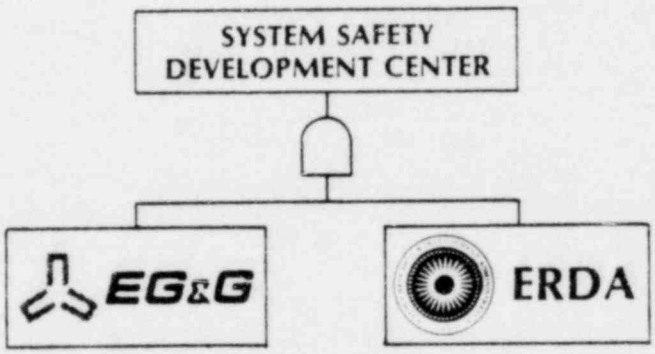
4. ASSIGNMENT OF SAFETY CLASS REQUIREMENTS

4.1 INTRODUCTION

Since there are currently 19 different safety functions as listed in Section 2.2 it is theoretically possible to establish 19 different design requirements. As discussed in more detail in Section A.2.1 for fluid retaining components this has not proven to be practical. It has been found

ERDA 76-45/8
SSDC-8

STANDARDIZATION GUIDE FOR CONSTRUCTION AND USE OF MORT-TYPE ANALYTIC TREES



EG&G Idaho, Inc.

P.O. Box 1625
Idaho Falls, Idaho 83401

FEBRUARY 1977

UNITED STATES
ENERGY RESEARCH AND DEVELOPMENT ADMINISTRATION
DIVISION OF SAFETY, STANDARDS, AND COMPLIANCE

DISCLAIMER

Available from:

National Technical Information Service (NTIS)
U.S. Department of Commerce
5285 Port Royal Road
Springfield, Virginia 22161

Price: Printed Copy: $ 4.00
Microfiche: $ 3.00

ERDA 76-45/8
SSDC-8
UC-41

STANDARDIZATION GUIDE FOR CONSTRUCTION AND USE OF MORT-TYPE ANALYTIC TREES

Prepared By

J. R. Buys

Work Performed At
EG&G IDAHO, INC.
IDAHO OPERATIONS OFFICE
Under Contract No. EY-76-C-07-1570

February 1977

(Second Printing - April 1977)

ACKNOWLEDGMENT

Special acknowledgment is extended to the staff of the System Safety Development Center and to reviewers throughout the ERDA complex for their helpful suggestions and guidance, and to Della T. Kellogg for her editorial assistance.

CONTENTS

INTRODUCTION

Since the introduction of MORT (Management Oversight and Risk Tree) technology as a tool for evaluating the success or failure of safety management systems, there has been a proliferation of analytic trees throughout ERDA and its contractor organizations. Standard "fault tree" symbols have generally been used in logic diagram or tree construction, but new or revised symbols have also been adopted by various analysts. Additionally, a variety of numbering systems have been used for event identification. The consequent lack of standardization has caused some difficulties in interpreting the trees and following their logic.

This guide seeks to correct this problem by providing a standardized system for construction and use of analytic trees. Future publications of the ERDA System Safety Development Center (SSDC) will adhere to this guide. It is recommended that other ERDA organizations and contractors also adopt this system to achieve intra-ERDA uniformity in analytic tree construction.

The proposed system is the outgrowth of the SSDC's experience in developing and teaching the use and construction of MORT diagrams and other analytic trees. It is equally applicable to both "success" or "positive" trees and "failure", "fault", or "negative" trees.

ANALYTIC TREES

The use of analytic trees originated as "fault tree analysis" in the early 1960's in the aerospace industry, as an attempt to prevent oversights, particularly at system interfaces, which had previously resulted in costly retrofits or inordinately short operational lifetimes for promising systems. Fault tree analysis was strongly hardware-oriented, but also showed promise as an analytic tool for evaluation of systems involving a great deal of human performance. Development of the MORT concept a decade later, and its acceptance by AEC (ERDA) for agency-wide use, made application of the fault tree analysis techniques to management systems a reality.

An analytic tree is simply a graphical display of information to aid the user in conducting a deductive analysis of any system (human, hardware, or environmental) to determine critical paths to success or failure. It identifies the details and interrelationships that must be considered to prevent oversights or omissions that lead to failures. It enables the analyst to:

1. Systematically identify the possible paths from base events to predicted outcome.

2. Display a clear visual record of the analytical process.

3. Identify management system weaknesses and strengths.

4. Provide a basis for rational decision making by management.

In an analytic tree, a top or major event or outcome is stated. It may be either a desired objective or goal, or an unwanted or injurious occurrence. On the next lower tier are listed those events required to achieve the top event. Each of these is subsequently broken down into its constituents to reveal the events, causes, and sources that contribute to the occurrence of the top event. Construction of an analytic tree, therefore, constitutes a deductive analysis of a management system or safety system, proceeding from general to specific, or outcome to source, and answering the question, "How could this happen?".

Once an analytic tree has been developed, it can be used as a tool to aid in achievement of "first-time-safe" operations; assurance of successful completion of a desired objective; prevention of significant accidents by foreseeing and avoiding managerial and operational oversights and omissions; and maintenance of effective total loss control. It can also be used after-the-fact in investigation of injuries, property damage, programmatic degradation, etc., to identify not just the symptoms, but also the root causes and sources of these accidents and the management system weaknesses that permitted them to occur.

SUMMARY

In the following sections of this monograph, analytic tree analysis steps and construction principles will be discussed. Both are summarized here to provide the user with a tool for rapid preview and a checklist for analytic tree-based system analysis.

A. Analysis Steps for Analytic Tree Use

1. Define the top event.
2. Acquire a working knowledge of the system to be analyzed.
3. Construct the analytic tree.
4. Validate the analytic tree.
5. Evaluate the analytic tree.
6. Conduct trade-off studies (risk/benefit studies).
7. Provide management with the recommendations and alternatives needed for informed decisions.

B. Analytic Tree Construction Principles

1. Use common and accepted graphic symbols for events, logic gates, and transfers. (See Figures 1, 2, 3, and 4. Figure 1 compares the "modified MORT" symbols recommended in this guide with "initial MORT" and Fault Tree Analysis symbols.)
2. Keep the analytic tree as simple as the complexity of the system allows (see Figures 5 and 6).

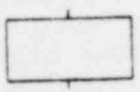
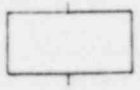
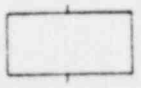
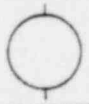
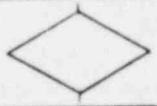
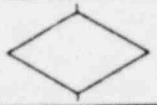
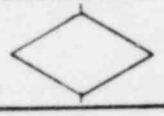
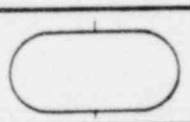
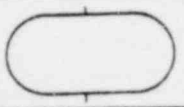
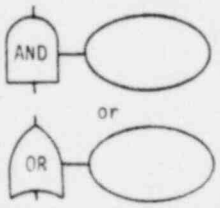
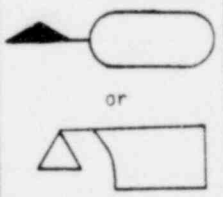
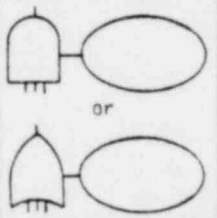
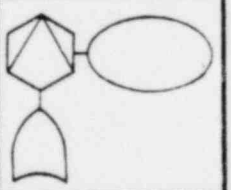
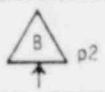
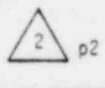
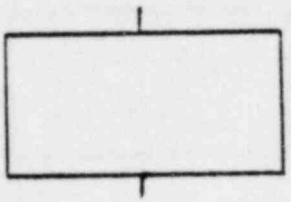
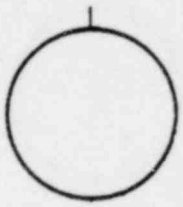
SYMBOL \ SOURCE	MODIFIED MORT	INITIAL MORT	FAULT TREE ANALYSIS
Gate Output or General Event			
Base Event			
Undeveloped Terminal Event			
Normally Expected Event			
Satisfactory Event			NONE
AND Gate			
OR Gate			
Conditional Gate			
Summation Gate		NONE	
Basic Transfer			
Transfer from Another Page			
Assumed Risk Transfer			NONE

Figure 1. Cross Index of Logic Symbols



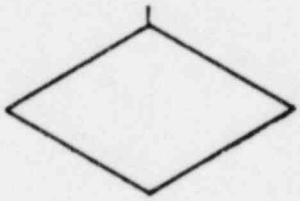
RECTANGLE

A general event or a gate output event resulting from the logical combination of contributory events acting through a logic gate.



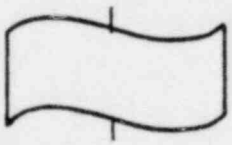
CIRCLE

A base event requiring no further development. It is an independent event used only as a logic gate input.



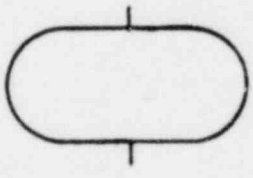
DIAMOND

An undeveloped terminal event not developed to its cause. Terminated for lack of information, resources or risks, or to avoid redundancy of analysis.



SCROLL

A normally expected event that should occur naturally during normal functioning of the system.



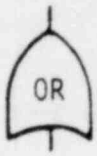
STRETCHED CIRCLE

A satisfactory event that exists noncommittally in the system as a logic gate output and is used to show completion of a logical analysis.

Figure 2. Analytic Tree EVENT Symbols

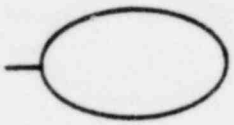
AND Gate

A logic gate that produces an output only when all input events occur. Contains the identifying word "AND".



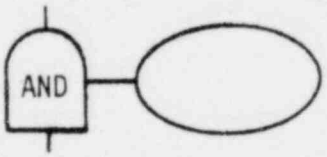
OR Gate

A logic gate that produces an output when one or more of the input events occur. Contains the identifying word "OR".



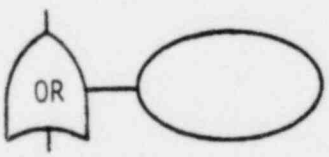
CONSTRAINT

A conditional event that applies conditions or constraints to a basic logic gate or output event. Imposed condition is written in the ELLIPSE.



CONDITIONAL AND Gate

Input produces the output provided the conditions written in the ELLIPSE are satisfied. (Example: PRIORITY AND gate specifying order of input event occurrence.)



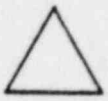
CONDITIONAL OR Gate

Input produces output provided the constraint conditions are met. (Example: EXCLUSIVE OR gate enabling an output to occur only if a single input is present.)

SUMMATION Gate

A special logic gate which requires that an acceptable combination of input events be present to produce an output. Inputs can be present in varying proportions, as long as the sum of the inputs is adequate to generate an output.

Figure 3. Analytic Tree LOGIC GATE Symbols



TRIANGLE

The basic transfer operator represents the exact repetition of a tree section found elsewhere on the tree below an identical triangle.

Intrabranch TRANSFER

Transfers substructure within a branch. Has identifying lower case letter.

Interbranch/Interpage TRANSFER

Transfers substructure from another branch or another page. Has an identifying capital letter.

OUT-TRANSFER, Same Page

Horizontal arrow away from symbol shows transfer of substructure to another location on the same page in the direction the arrow points.

IN-TRANSFER, Same Page

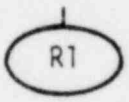
Horizontal arrow toward symbol shows transfer from direction of arrow on the same page.

IN-TRANSFER, Other Page

Vertical arrow toward base of symbol indicates transfer from branch on designated page.

OUT-TRANSFER, Other Page

"Recipient events" from other pages in broken lines above oversized triangle indicate transfer of substructure to recipient event locations on designated pages.



SMALL OVAL

Assumed risk transfer is used to transfer an assumed risk from any tree location to the assumed risk event (a SCROLL). The number of the assumed risk is indicated inside the symbol as shown. It normally originates at a DIAMOND (undeveloped terminal event).

Figure 4. Analytic Tree TRANSFER Symbols

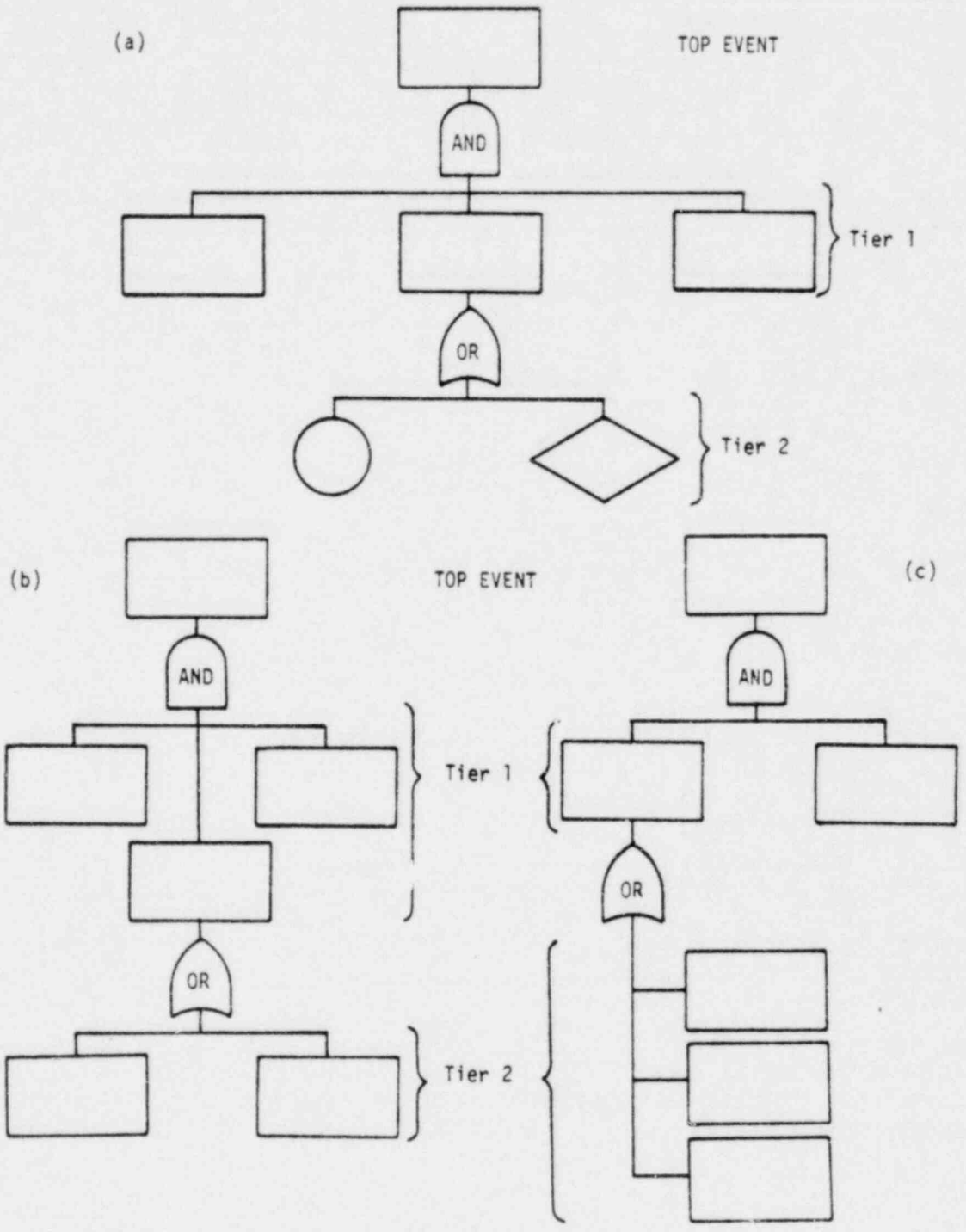
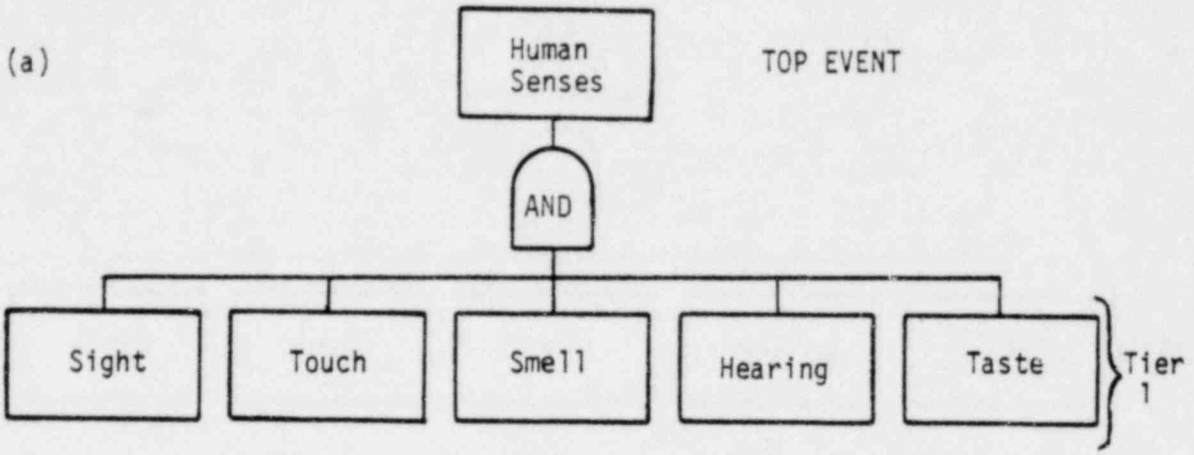


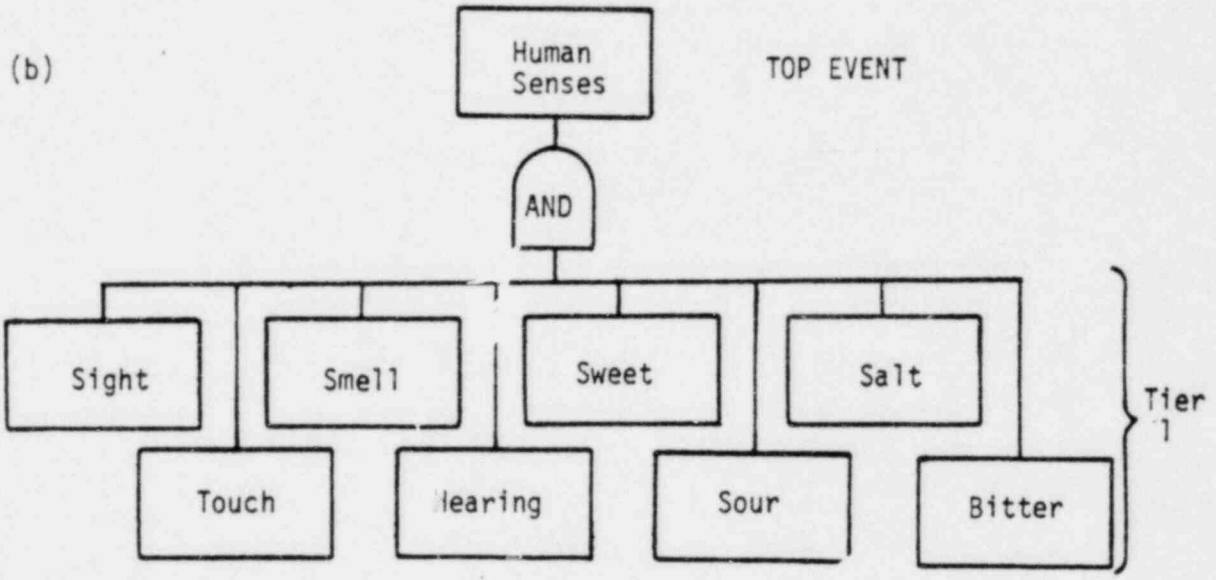
Figure 5. Acceptable Tier Arrangements

(a)



This example exhibits good logic because all of the recognized senses are listed, but no extraneous detail is included on Tier 1.

(b)



Poor logic has been used here, for detailed constituents of taste are listed on the same tier as the other four senses. If this level of detail is desired, the contributory events should be listed on Tier 2 under the appropriate sense.

Figure 6. Examples of Good and Poor Logic[3][4]

3. Keep the analytic tree logical and expect no miraculous occurrences. Use only those contributory events which are "necessary and sufficient" to produce the output event.

4. Select the logic gates and constraints (conditional events) which best describe true system functioning.

5. Select event titles or descriptions which are simple, clear, and concise. Avoid those which are abstract or are not readily understood by the intended users.

6. When constructing complex trees, limit the number of tiers on a single page to nominally four or five tiers (see Figure 7).

7. Use the Dewey decimal system for numbering events below the top event on the first page of the analytic tree. Locate the event identification above the upper right corner of the event symbol (see Figure 7).

8. Use a modified decimal system for identifying events below transfer symbols beginning with the letter designation of the transfer (see Figure 8).

9. Use transfers to avoid duplication of identical branches or segments of the tree, and to reduce single-page-tree complexity (see Figures 7 and 8).

   a. Identify "intrabranch" transfers by lower case letter designations and "interbranch" or "inter-page" transfers by capital letter designations, i.e.,  and  , respectively.

   b. Show transfers into a branch of the analytic tree by an arrow pointing toward the transfer symbol from the general direction of transfer; horizontal for transfers on the same page and vertical for those from another page (see Figures 7 and 8).

   c. Show transfers out of a branch to another location on the same page by an arrow pointing away from the transfer symbol in the direction of transfer (see Figures 7 and 8).

   d. For transfer of a branch to another page, list the "recipient events" in broken lines above an "over-sized" transfer symbol on the page where the transfer originates. The page to which the substructure is to be transferred is specified below the lower right corner of the recipient event. A similar notation at the transfer symbol on the receiving page shows the origin page of the transferred branch (see Figures 7 and 8, transfer "A").

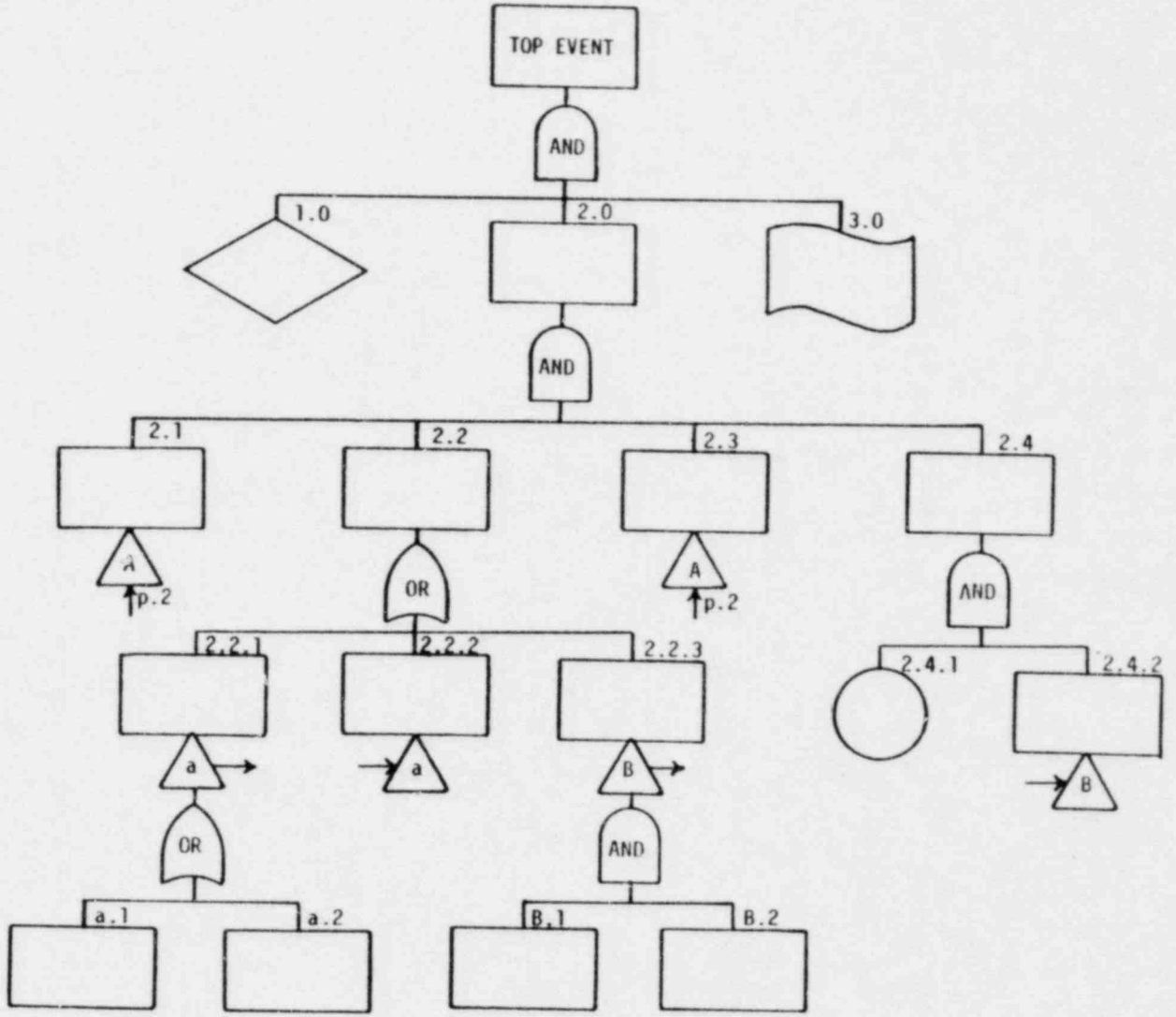


Figure 7. Sample Analytic Tree - Sheet 1

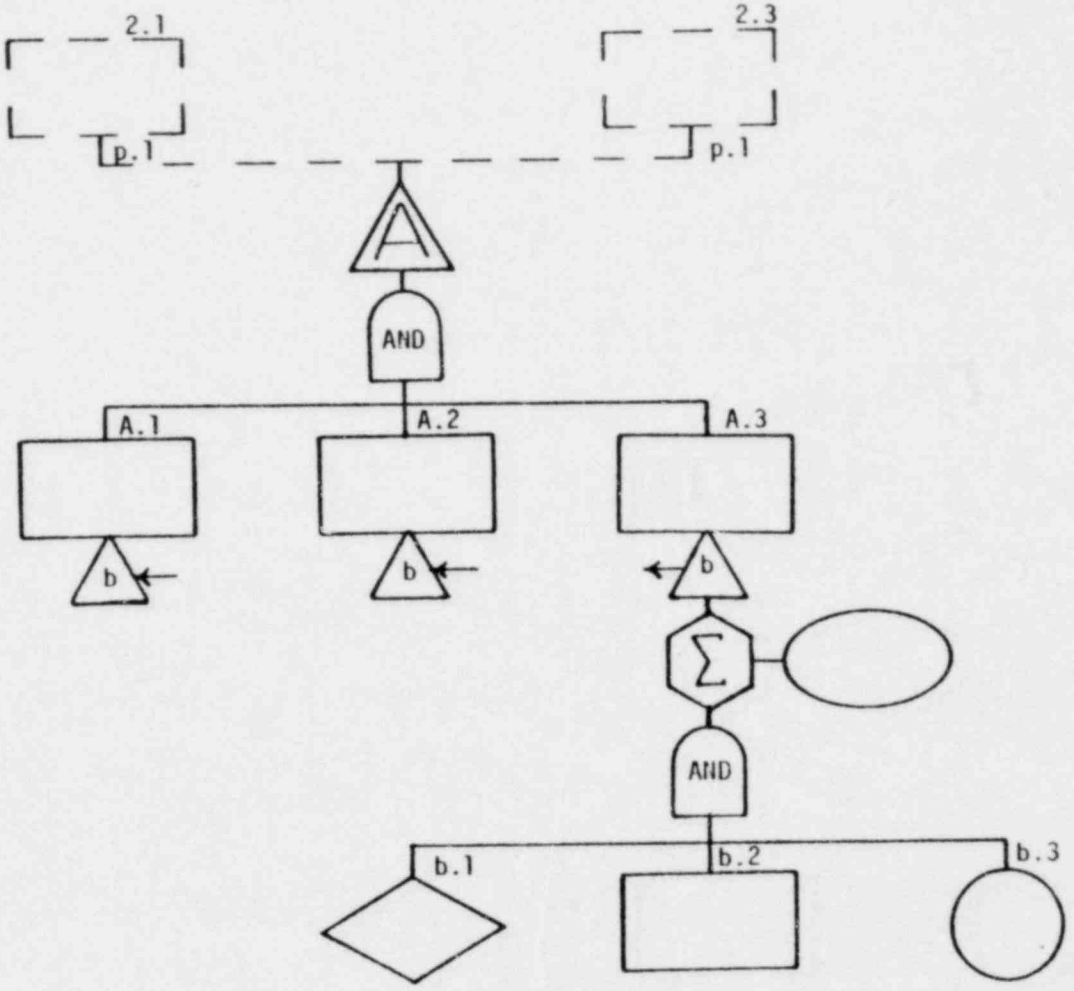


Figure 8. Sample Analytic Tree - Sheet 2

10. Do not number or letter logic gates. They are adequately identified by the input events which operate through them and the resulting output events.

11. Follow the convention of indicating order of performance or time sequencing from left-to-right, for related events on a single tier.

ANALYSIS STEPS

The basic steps in analyzing any system through use of an analytic tree are:

1. Define the top event. That which you desire to achieve, or which you desire to prevent from happening is the top event. Make it as specific as you can so that contributory events can be clearly and accurately recognized and defined.

2. Acquire a comprehensive understanding of the management system or safety system to be analyzed. Only by fully understanding the system, its constituents and details, and their interrelationships and interfaces can a logical and complete analysis be performed, which identifies and considers all those events which are necessary and sufficient to produce the top event or outcome. It is often necessary and desirable, particularly with success trees, to:

    - Define the "ideal" management system or safety system.
    - Compare the existing system with it.
    - Incorporate those events and logic gates in the analytic tree that are required to bring the present system up to the ideal.

3. Construct the analytic tree. With the top event defined and a thorough understanding of the system acquired, the analyst then constructs the analytic tree, using appropriate logic gates and standardized event symbols and transfers. Specifics of tree construction will be discussed later.

Proper logic is followed to assure that all events meet the "necessary and sufficient" criterion, i.e., those events are specified which are the minimum necessary, and no more than is sufficient, to immediately produce the logic gate output event. Each event is essential to the tree logic (necessary) and no other information is needed (sufficient) to achieve the stated output. All other events are either excluded as being extraneous, or are relegated to a supportive and more detailed lower tier.

Steps 2 and 3 ordinarily are not separate and distinct as suggested here, but rather more about the system is often discovered and applied as tree construction develops.

4. Validate the analytic tree. Once construction of the analytic tree has been completed, one or more knowledgeable persons should review the tree events and logic for accuracy and completeness - for omissions and oversights. The purpose of this validation review is to confirm that:

   - The tree meets its intended objectives.
   - The system and its functioning are fully and clearly described.
   - Inputs to logic gates are necessary and sufficient to logically produce the stated output events.

   Validation by other persons has proven time and again to be essential to produce useful, error-free analytic trees, which identify system weaknesses and strengths and lead to proper assessment of identifiable risks. Often, consultation with others to validate the tree begins before construction is complete, so steps 3 and 4 sometimes overlap.

5. Evaluate the analytic tree. Following validation of the tree, it is evaluated to identify critical paths to achievement of the top event. Thorough study of the elements and interrelationships in the tree will enable the analyst to identify oversights and omissions in the safety/management system, and to assure that identifiable risks are presented to the proper management levels for acceptance or resolution. As the analyst evaluates the failure or success paths from base events to the top event, paths or chains of varying importance and system impact will emerge. The relevance to system output of these paths, and the events of which they are comprised, must be carefully weighed and major emphasis placed on those of greatest significance. (This, of course, will require value judgments by the analyst, but they should be based realistically on what the analysis reveals.) Management must not only be informed of the risks involved, but also of their relative significance, if they are to make the best risk-related decisions.

6. Conduct trade-off studies. Trade-off, cost-benefit, or risk-benefit studies are needed to determine which risks should be assumed, which risks cannot be assumed, and where controls can most effectively be applied to achieve the desired objective or prevent the undesired occurrence.

7. Management makes rational and informed decisions concerning the safety/management system. The results of analytic tree evaluation and subsequent trade-off studies lead logically to recommendations and alternative solutions, from which management can select in making knowledgeable and informed decisions on system control and repair, and risk assumption.

TREE CONSTRUCTION

Analytic tree construction is a logical development of the top event, using deductive reasoning to progress through successively more specific events to basic events or causes, from which sequential chains of success or failure begin. The various levels of tree development are tiers and branches of contributory events that are sequentially linked by logic gates. Each tier of tree development contains those events which, when processed through the logic gate, are necessary and sufficient to lead directly to the success or failure of the event on the next higher tier. Branching occurs when any of the multiple events, which may operate through a logic gate to produce a common higher event, have substructures of their own.

Use of the standardized approach for analytic tree construction and identification requires adherence to eleven basic principles:

1. Use common and accepted graphic symbols. Analytic tree symbols may be categorized into three groups: (a) events, (b) logic gates, and (c) transfers. Although an ERDA-approved MORT template currently does not exist, logic symbol templates that can aid the analyst in tree construction are available from several commercial sources.

   a. Events

      An event is a possible condition or state of a system element or function. It may be a long-lived condition, or it may arise spontaneously or gradually from a dynamic change of state. If it results in a desirable or intended occurrence, it is a success or normal event. If it results in system degradation or failure, or an abnormal occurrence, it is a failure or fault event. The same common symbols are used as components of both success trees and fault trees.

Event symbols are of five basic types, each of which represents a different kind of event (see Figure 2).

(1) The RECTANGLE is the general event symbol and is used extensively in all trees, but particularly in success trees. It is also used to represent a gate output event, resulting from the logical operation of contributory events acting through a logic gate.

(2) The CIRCLE represents a base event that requires no further development. It is an independent event that defines an inherent system element fault or a base-level success, and is used only as an input to a logic gate.

(3) The DIAMOND represents an undeveloped terminal event, which is not developed further because of:

(a) Low relevance or low risk, i.e., a JSA (Job Safety Analysis) is not performed on a particular task, because it has a low potential for accident, and the low risk is assumed.

(b) Lack of adequate information or resources for solution, i.e., the nearest hospital is 40 miles from the work site, and cost is prohibitive to move nearer, therefore, event development is terminated and the distance risk is assumed.

(c) Redundancy avoidance when another analytic tree gives the needed information, i.e., in developing a detailed use readiness tree for a new complex facility, the safety criteria event should be a DIAMOND, and reference made to the "Occupancy-Use Readiness Manual - Safety Considerations"[3], where the safety criteria tree is already developed.

(d) Influence on the scope of the tree, but not necessary to the development of the analytical logic, i.e., safety considerations only are analyzed in the Occupancy-Use Readiness Tree[3], but undeveloped interfacing events with other organizations are shown because they influence tree scope, even though they are not necessary to logic development.

In cases (a) and (b), the event logically becomes an "assumed risk". In case (c), a footnoted reference identifies the supplementary analysis. In case (d), "fringe area" events are identified which do not contribute significantly to development of the final system outcome, but which should be included on the tree to indicate that their influence on the extent or depth of system analysis has been considered.

Like base event circles, terminal event diamonds represent base-level events which are used only as logic gate inputs.

(4) The SCROLL represents a normally expected event, which is expected to occur naturally during normal functioning of the system. It has the same meaning as the "house" in Fault Tree Analysis symbolism. Assumption of some risks in any major operation is normally expected, so the "assumed risk" event would be a SCROLL. Likewise, in assessing deviations in personnel performance, normal variability among workers would be expected and should be depicted as a SCROLL.

(5) The STRETCHED CIRCLE is a satisfactory event, which simply exists in the system but is neither fault-oriented nor success-oriented. It is a logic gate output event which is most often used to show completion of logical analysis. It covers such events as the presence of personnel or objects in an energy channel because they are needed there to perform a functional task.

b. Logic Gates

A logic gate performs a discrete operation upon contributory events to produce a logical output event. The fundamental logic gates for analytic tree construction are the AND gate and the OR gate. Many analytic trees can be constructed using only these basic logic gates. If a CONSTRAINT symbol is added to a basic logic gate to modify it or impose special conditions on its operation, greater flexibility is added. Further addition of a SUMMATION gate should provide the analyst with all the logic gates he needs for thorough analysis of the system (see Figure 3). The AND gate produces an output only if all required input events coexist.

In other words, all contributory events must occur for an AND gate to produce an output event. The OR gate produces an output event when one or more of the contributory events occur.

The addition of a CONSTRAINT symbol (an ELLIPSE) to the side of a basic logic gate applies conditions or constraints to the basic gate to create a CONDITIONAL gate, which inhibits or prevents an output until the specified condition is met. Typical of a CONDITIONAL gate are the PRIORITY AND gate, which requires a particular input event sequence to cause occurrence of the output event, and the EXCLUSIVE OR gate, which enables the output event to occur if one, and only one, of the input events is present.

The SUMMATION gate is a special logic gate which requires that an acceptable combination of the input events occur to produce an output. This allows for contributory events to be present in varying proportions, as long as the composite contribution is sufficient to produce occurrence of the output event; that is, a deficiency in one or more input events can be compensated by greater contributions by the other input events. Unlike the Fault Tree Analysis "basic and/or" gate logic, which requires each input event to be either present or absent (a strict binary logic), the SUMMATION gate allows any contributory event to be present to any degree from 0 to 100%, as long as the total input from all events can generate the output event. For example, in the Behavioral Change Tree[1], four input events operate through a SUMMATION gate to produce the output event, "Select Means for Introducing Behavioral Change". Deficiencies in input 1, "Control Selection and Placement", can be compensated by improved performance on input events 2, 3, and 4, "Control Training", "Control Factors That Influence Attitudes", and "Control Organizational Psychology Factors", respectively. This provides a satisfactory combination of events for introducing the desired behavioral change.

c. Transfers

A TRANSFER symbol indicates that an event, a series of events, or a complete branch of the analytic tree is transferred from one location on the tree to another. Rather than duplicating that portion of the tree in the second location, a transfer TRIANGLE is used to indicate an exact repetition of that tree section at the second, third, etc., location. Use of a special SMALL OVAL to represent transfer of an "assumed risk"

event is peculiar to MORT[2]. Both TRANSFER symbols, the tree-section transfer TRIANGLE, and the "assumed risk" transfer SMALL OVAL are used to avoid repetition, conserve space, and simplify tree construction (see Figure 4). Additional information on use of TRANSFER symbols will be provided as other tree construction principles are discussed.

2. Keep the analytic tree as simple as the complexity of the system allows. When the analyst has gained a thorough understanding of the system to be analyzed, he begins to lay down its logical progression from the top event to base events. He should be ready to get additional system information as the tree reveals that need. However, he should be selective in determining the depth of analysis, and should use the undeveloped termination event DIAMOND when further development is clearly not justified. This usually occurs when all the relevant dependencies and the necessary and sufficient input events have been identified. Normally, the analyst will clean up and further simplify the analytic tree that he has used as an analysis tool, before presenting it to management for their use in making risk assumption and risk resolution decisions.

3. Keep the tree logical and expect no miraculous occurrences. Deductive analysis, using an analytic tree as a logic aid, should proceed logically from the top event to base events. Related events at the same level of logic and detail are entered on a single tier and are joined by a line before being processed through a logic gate. A vertical line and a logic gate join a gate output event on one tier with its more detailed contributory events on the next lower tier. Ideally, all events on the same tier will be on the same horizontal level [Figure 5(a)], however, because of space limitations and page-fitting problems during tree construction, they are often joined to a common horizontal line by vertical extensions of varying lengths [Figure 5(b)], or they are joined to a single vertical line and listed ladder-like, one below the other [Figure 5(c)]. Any of the tier arrangements in Figure 5 are acceptable. Figure 6 displays examples of good and poor logic in placement of events in analytic tree tiers.

   Expect no miracles, either good or bad. The analytic tree cannot do the work for the analyst. It is simply a tool for his use in organizing and systematizing his thinking to help him find right answers. Its output can be no better than the quality and organization of its inputs. Be reasonable, logical, and practical, and expect logical and rational sequences to develop through logic gates, as identifiable events interrelate and interact. Lower tier input events should be only those which are necessary and sufficient to produce the gate output event.

Do not struggle to develop outlandish or irrational events which would require a miracle for occurrence, such as postulating simultaneous occurrence of a building fire, bomb threat, severe winter storm, tornado, earthquake, and an impending nuclear attack in analyzing an Emergency Response System.

4. Select the logic gates and constraints (conditional events) which best describe true system functioning. The basic AND, OR, and SUMMATION logic gates, modified as necessary by CONSTRAINTS, provide sufficient flexibility to accurately describe the logical processing of contributory input events, and produce the defined output events at each level of the analytic tree. Proper selection and use of logic gates will establish a logical progression of identifiable event interactions through the tree to tie the top event to its root contributors at the base event level, and to accurately describe the way the system really works.

5. Select event descriptions that are simple, clear, and concise. Event descriptions should be sufficiently descriptive and understandable that the analytic tree user can grasp their meaning and follow the analytic process without having to refer to explanatory data found somewhere else. Analysts should particularly avoid event descriptions which are abstract, or which contain terms with which the intended user is unfamiliar. Additionally, event descriptions for systems with considerable people-involvement should include active verbs ("do" verbs), such as "plan", "prepare", "control", "implement", etc., to convey the precise nature of input events which are necessary and sufficient to generate the output events and, ultimately, the top event.

6. When constructing complex trees, limit the number of tiers on a single page to nominally four or five tiers. There are two basic reasons for imposing such a limitation:

   a. Most trees are reproduced on 8-1/2"x11" or 11"x17" sheets for inclusion in a document or for convenient use on the job. The complexity of branches of the analytic tree will cause some variance in the number of tiers that may appear on a single page, but normally more than four or five tiers cannot be reproduced legibly or read without magnification.

   b. Use of the Dewey decimal system for event identification (discussed in principle 7) becomes cumbersome and difficult to manage beyond five digits (five tiers). A modified decimal system restores the simplicity of event identification below TRANSFER symbols (see principle 8).

7. Use the Dewey decimal system for numbering events below the top event on the first page of the analytic tree. Each event is uniquely identified by a Dewey decimal number located above the upper right corner of the event symbol. The number of nonzero digits in the Dewey decimal event numbering system corresponds to the tier on which the event is located, i.e, the third tier contains 3 digit event numbers. Table I gives representative Dewey decimal numbers for various tiers.

   A Dewey decimal event identification number not only uniquely describes an event, but it also systematically traces its development through subbranches and branches to its progenitor event on the first tier. Each successively higher level event can be identified by dropping the last digit from the number as shown below:

Top Event	
1.0	First Tier
1.1	Second Tier
1.1.1	Third Tier
1.1.1.1	Fourth Tier
1.1.1.1.1	Fifth Tier

   Example 1 shows another numeric progression in tree format.

8. Use a modified decimal system for numbering events below transfer symbols beginning with the letter designation of the transfer, i.e., A.1.3.2 or a.1.3. Numbering progresses through succeeding subtiers in the same way as the pure numerical Dewey decimal system, as shown in Table II and the accompanying examples.

   Alphanumeric progression from the fourth subtier to the TRANSFER is shown below:

D	TRANSFER
D.2	First Subtier
D.2.2	Second Subtier
D.2.2.1	Third Subtier
D.2.2.1.2	Fourth Subtier

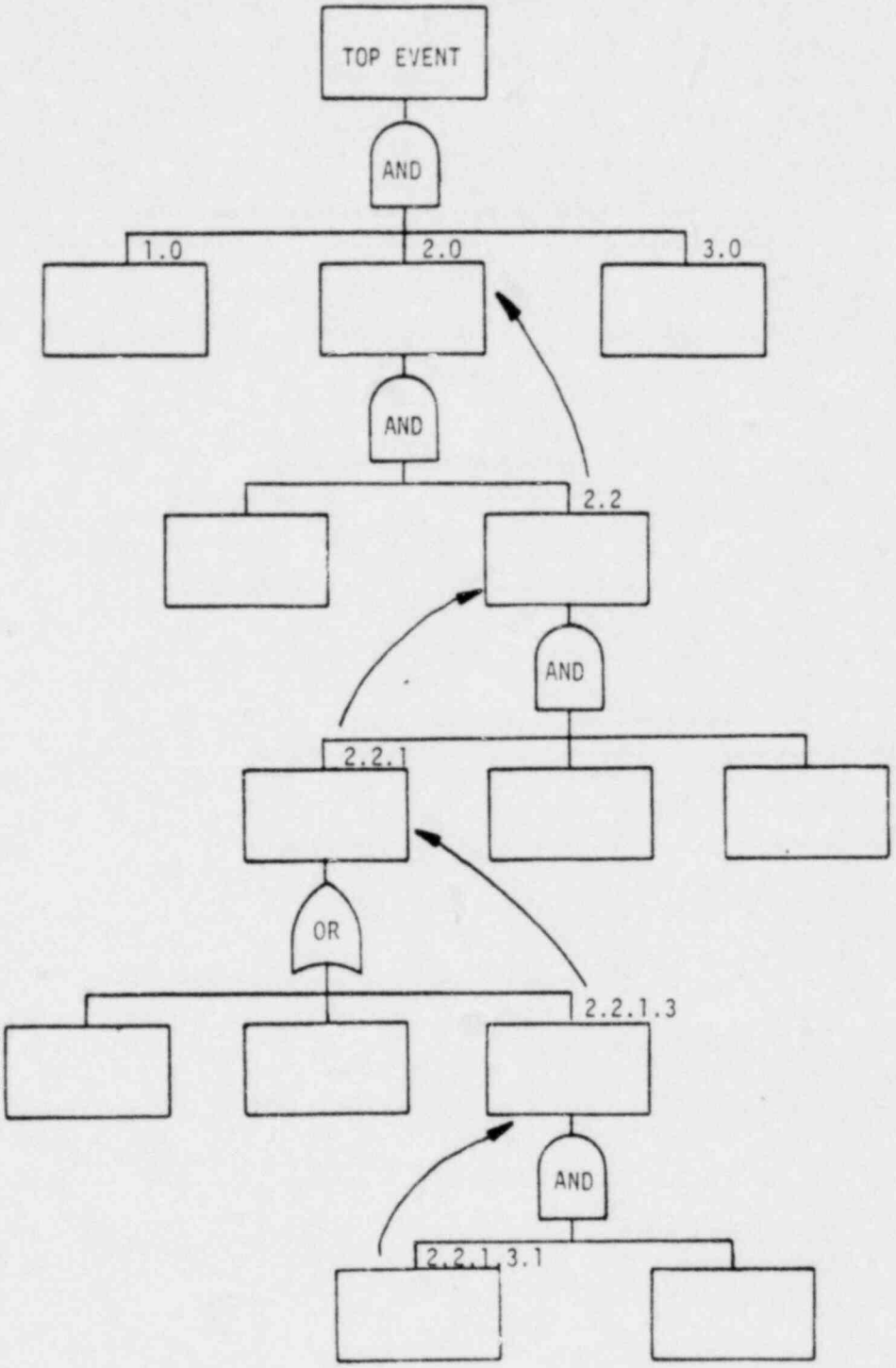
   Example 2 shows the same progression in tree format.

9. Use transfers to avoid duplication of identical branches or segments of the tree and to reduce single page tree complexity. Whenever two or more gate output events have identical details in the substructures contributing to their occurrence, that substructure should be constructed under only one of the output events, and then transferred to the others through the use of TRANSFER symbols (see Figure 7, TRANSFERS "a" and "B"). Be careful to avoid the inclination to force a

TABLE I

DEWEY DECIMAL EVENT IDENTIFICATION NUMBERS

Tier	Number Designation
Top Event	Unnumbered
First	1.0, 2.0, 3.0, 4.0...n.0
Second	1.1, 1.2, 1.3...2.1, 2.2, 2.3...n.m
Third	1.1.1, 1.1.2, 1.1.3...2.1.1, 2.1.2...n.m.p
Fourth	1.1.1.1, 1.1.1.2...2.1.3.1, 2.1.3.2...n.m.p.q
Fifth	1.1.3.2.1, 1.1.3.2.2...2.1.4.2.1...n.m.p.q.r



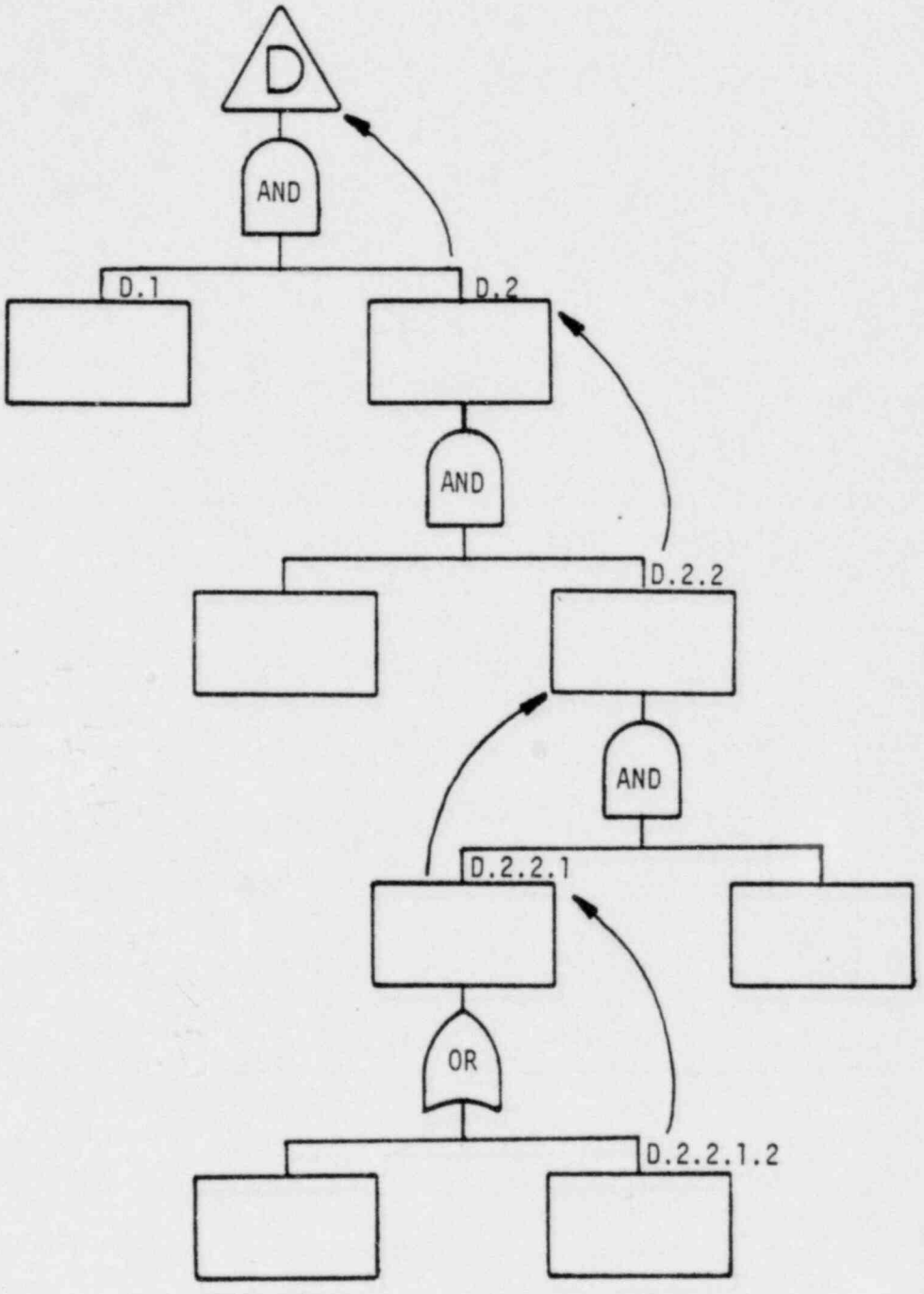
EXAMPLE 2

(Also See Figure 7)

TABLE II

MODIFIED DEWEY DECIMAL EVENT
IDENTIFICATION NUMBERS

Transfer Subtier	Number Designation
Transfer	A, B, C...N
First	A.1, A.2, A.3...N.m
Second	A.1.1, A.1.2...A.2.1, A.2.2...N.m.p
Third	A.1.1.1, A.1.1.2, A.1.1.3...N.m.p.q
Etc.	



EXAMPLE 2

(Also See Figure 8)

substructure that "almost fits", but has basic differences, into a "transferable" structure. TRANSFERS should be used also below the bottom tier events on a page to indicate continuance of subbranches of those events on other pages. Additionally, whenever there is insufficient space on a page to develop a branch below an event at any level, a TRANSFER immediately below that event indicates that the branch is developed on another page (see Figures 7 and 8, TRANSFER "A").

a. Identify "intrabranch" transfers by lower case letter designations, and "interbranch" or "interpage" transfers by capital letter designations, i.e.,  and  , beginning with "a" and "A", respectively, and proceeding logically. Refer to Figures 6 and 7 where TRANSFERS "a" and "b" transfer substructures within a branch (are intrabranch transfers); TRANSFER "A" is the transfer of a branch between pages (interpage transfer), and TRANSFER "B" is a substructure transfer from one branch to another (interbranch transfer).

b. Show transfers into a branch of the analytic tree by an arrow pointing toward the transfer symbol. For transfers from a branch on the same page, the arrow points to the side of the TRANSFER symbol from the direction in which the transfer is made, i.e.,  (see Figures 7 and 8, TRANSFERS "a", "b", and "B"). For transfers from another page, the arrow points to the base of the TRANSFER triangle, and the source page is listed adjacent to the arrow, i.e.,  (see Figure 7, TRANSFER "A").

c. Show transfers out of a branch to another location on the same page by an arrow pointing away from the transfer symbol in the direction of the transfer, i.e.,  . (See Figures 7 and 8, TRANSFERS "a", "b", and "B".) Remember, transfers out are away from the symbol and transfers in are toward the symbol; also, arrows point in the general direction of the transfer, horizontal for transfers on the same page and vertical for transfers from another page.

d. For transfer of a branch to another page, list the "recipient events" in "broken" lines above an "oversized" transfer symbol on the page where the transfer originates. Also, specify the page or pages to which the branch will be transferred by listing the appropriate page number below the lower right corner of the recipient event. (See Figure 8, TRANSFER "A". Note that the "A" structure transfers to two locations on page 1, event 2.1 and event 2.3.) On a multipage tree, it is conceivable that there could be several recipient events fed by a single transfer structure, and that they might be located on different pages, i.e., one recipient event on page 3, another on page 4, still another on page 6, etc. In such a case, all the recipient events should be identified by "broken lines" (dashed lines) above the TRANSFER triangle on the transfer originating page, and each recipient event be further identified by its page location, i.e., p.3, p.4, p.6, etc. When a multipage analytic tree with many transfers is compiled onto a single, oversized "fold sheet", such as the universal MORT diagram, the page designations of transfer and recipient event locations can be replaced by coordinate area designations. The coordinate system could be based on an unlined cartesian grid with a numbered ordinate (vertical) and a lettered abscissa (horizontal) to give such event locations as 1a, 4c, 7f, etc.

10. Do not number or letter logic gates, use numeric and alphanumeric decimal identification designations only for events. Logic gates are defined by the input events that operate through them and the specific output events that occur. Therefore, it is not necessary to assign specific identification numbers to logic gates, for they are fully defined by the events they serve.

11. Follow the convention of indicating time sequencing or order of performance from left-to-right for related events on a single tier. It should also be apparent that a higher tier event has greater significance (more impact on the top event) and occurs later than the more detailed contributory events located on lower tiers within its branch.

Construction and use of an analytic tree involves deductive analysis beginning with a stated top event, and then proceeding through the immediate causal events, intermediate events, and detailed events to the base events, which originate the sequential chains that lead to top event occurrence. If the analyst has done his job well, the

* U. S. GOVERNMENT PRINTING OFFICE : 1977 240-979/16

events will occur in the logical sequence displayed on the analytic tree. Critical paths to success or failure can then be discerned by the user, and appropriate fixes applied at the proper event level to assure the desired success or prevent the predicted failure.

The user's task will be made simpler, more logical, and more orderly if he knows that the analytic tree author has also established a left-to-right sequencing of occurrence among events on a single tier. The analytic tree is a tool for use in system analysis; anything that contributes greater simplicity, order, and logic to it enhances its usefulness.

REFERENCES

[1] Nertney, R. J. and Buys, J. R., Training As Related to Behavioral Change, ERDA-76-45-6, SSDC-6, June 1976

[2] Johnson, W. G., MORT - The Management Oversight and Risk Tree, SAN 821-2, February 12, 1973

[3] Nertney, R. J., Clark, J. L., and Eicher, R. W., Occupancy-Use Readiness Manual - Safety Considerations, ERDA-76-45-1, SSDC-1, September 1975

[4] Knox, N. W. and Eicher, R. W., MORT User's Manual, ERDA-76/45-4, SSDC-4 (Rev. 1), March 1976

[5] Lambert, H. E., System Safety Analysis and Fault Tree Analysis, UCID-16238, May 9, 1973

Other SSDC Publications in This Series

SSDC-1	Occupancy-Use Readiness Manual
SSDC-2	Human Factors in Design
SSDC-3	A Contractor Guide to Advance Preparation for Accident Investigation
SSDC-4	MORT User's Manual
SSDC-5	Reported Significant Observation (RSO) Studies
SSDC-6	Training as Related to Behavioral Change
SSDC-7	ERDA Guide to the Classification of Occupational Injuries and Illnesses