Chapter 1

MNR Safety Amplifier Decomposition

1.1. Introduction to Fault Tree Analysis

Fault Tree Analysis is a comprehensive analytical tool developed for the safety analysis of reliable systems of moderate and high complexity. This tool is widely adopted in the aerospace and nuclear industries since markov processes and other exact analytical techniques cannot provide adequate results when the complexity of the system is high. Fault Tree Analysis uses logical gates to combine failure probabilities of components and systematically builds them up to the overall system failure probability. Two logical gates, OR and AND, are supported by many commercially available reliability software packages. However, they can only be applied to "coherent" systems. Coherent systems are systems in which a failure of a component cannot lead the system into a safer state.

Example:

Consider a parallel system consisting of two identical components in which the first component, A, is active, while the second one, B, is in a standby mode, as presented in Figure [1-1]. For the case of component A failing, switch S automatically switches to position '2', allowing the continuous operation of the system. A typical example of the standby operation can be found in any

uninterruptible power supply (UPS) unit. A standby unit is not a coherent system. Namely, the failure of component A can actually lead the system to a safer state, which will happen if the component B is more reliable than A. The switch can be modeled by

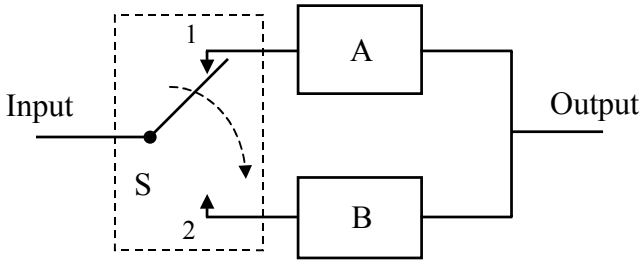

Figure 1-1. System in the standby 'parallel' mode

using the NOT gate. The events E_A = "a signal propagates through component A" and E_B = "a signal propagates through component B" are not independent any more, but rather mutually exclusive. Because of the strong dependencies between E_A and E_B, the rare event approximation cannot be applied. Although this system is often called "standby parallel", it cannot be presented as a serial system, a parallel system, or any of their combinations. For more on this, see Appendix 2.

The NOT gate, that characterize non-coherent systems, has also been supported by some of the recently developed reliability software. We will use one of them, called FaultTree+ 6.0 (see [Isograph Ltd., 1995]) for the calculations of the Safety Amplifier reliability parameters. For further discussion on non-coherent systems see [NATO, 1978]. NOT gates are necessary if logical dependencies between events exist, which is indeed the case in the Safety Amplifier, as we will soon see. For more information on Fault Tree

Analysis see [McCormick, 1981]. Figure [1-2] depicts the symbols most commonly used in the Fault Tree Analysis.

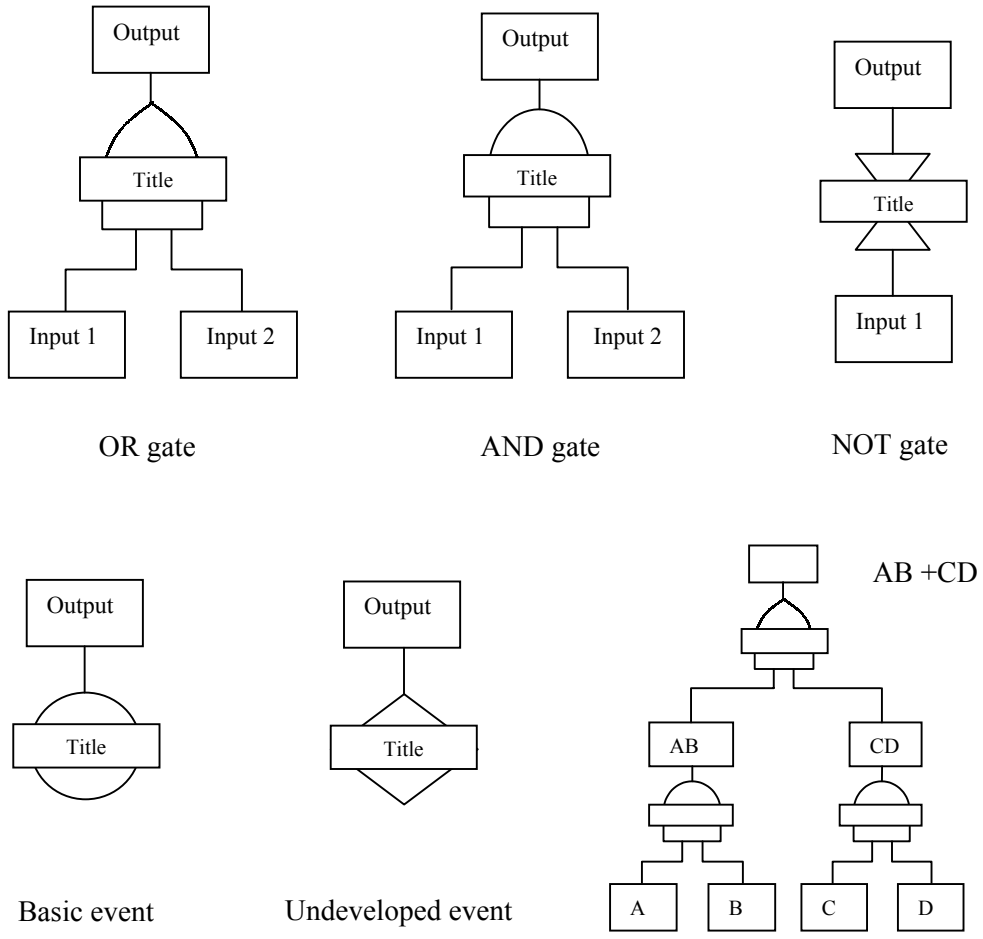

Figure 1-2. Fault Tree Symbols

1.2. Uncertainty Propagation in a Fault Tree

Any uncertainty in the SA system components propagates from a lower to a higher level ultimately reaching the top level of the Safety Amplifier fault tree.

In the case of an OR gate the output mean is given by

$$\mu_{OR} = \mu_1 + \mu_2 \ldots + \mu_n \tag{1.1}$$

and the standard deviation is

$$\sigma_{OR}{}^2 = \sigma_1{}^2 + \sigma_2{}^2 \ldots + \sigma_n{}^2 \tag{1.2}$$

Note that Equation (1.1) is a consequence of the fact that if the events A and B are both rare and independent, than the following rare approximation is in effect: $P(A \cup B) \cong P(A) + P(B)$. This is graphically depicted in Figure 1-3, for the case when $P(A) = P(B)$.

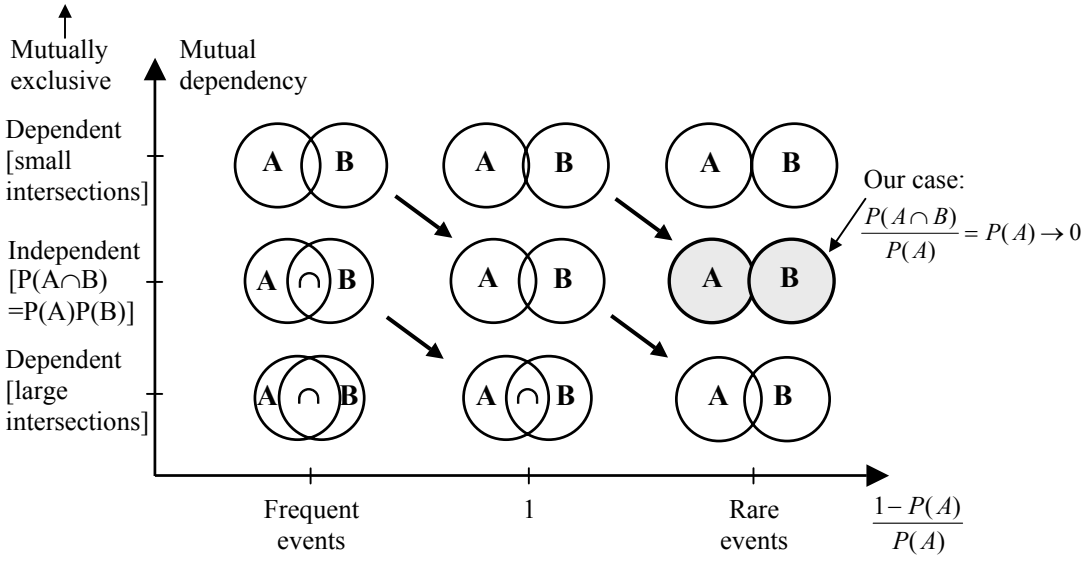

Figure 1-3. The comparison between absolute and relative sizes of intersections for various event-frequency pairs. Diagonal arrows indicate constant absolute intersections.

From Equation (1.1) and Equation (1.2) it follows that the coefficient of variation of the output, defined as $\kappa \equiv (\sigma/\mu)$, is lower than the largest coefficient of variation in input,

$$\kappa_{OR}^{\ 2} = \frac{\sigma_{OR}^2}{\mu_{OR}^2} = \frac{\sigma_1^{\ 2} + \sigma_2^{\ 2} \ldots + \sigma_n^{\ 2}}{(\mu_1 + \mu_2 \ldots + \mu_n)^2} < \frac{\sigma_1^{\ 2} + \sigma_2^{\ 2} \ldots + \sigma_n^{\ 2}}{\mu_1^{\ 2} + \mu_2^{\ 2} \ldots + \mu_n^{\ 2}} \leq \max \kappa_i^{\ 2} \tag{1.3}$$

Therefore, an OR gate decreases the uncertainty of failure. The uncertainty of failure is represented herein as a coefficient of variation of a failure rate. It is a normalized, or non-dimensional, value. Thus, uncertainties with different means may be compared.

In the case of an AND gate the mean is

$$\mu_{AND} = \mu_1 \cdot \mu_2 \ldots \cdot \mu_n \tag{1.4}$$

and the standard deviation in case of two inputs is

$$\sigma_{AND}^2 = \sigma_1^{\ 2}\sigma_2^{\ 2} + \mu_1^{\ 2}\sigma_2^{\ 2} + \mu_1^{\ 2}\sigma_2^{\ 2} \tag{1.5}$$

An AND gate increases the uncertainty of failure. The coefficient of variation of the output is greater than the largest coefficient of variation in the input, since from Equation (1.4) and Equation (1.5) it follows that

$$\kappa_{AND}^2 = \frac{\sigma_1^{\ 2}\sigma_2^{\ 2} + \mu_1^{\ 2}\sigma_2^{\ 2} + \mu_1^{\ 2}\sigma_2^{\ 2}}{\mu_1^{\ 2}\mu_2^{\ 2}} = \kappa_1^{\ 2}\kappa_2^{\ 2} + \kappa_1^{\ 2} + \kappa_2^{\ 2} > \max \kappa_i^{\ 2} \tag{1.6}$$

In the case of an AND gate with *n* equally distributed random failures with coefficient of variation κ the relationship between the input and output uncertainties is given by the following equation

$$\kappa_{AND}^2 + 1 = (\kappa^2 + 1)^n \qquad (1.7)$$

1.3. Modular Decomposition. Threads

For the purposes of reliability analysis the Safety Amplifier will be decomposed in several functional units or modules. These units are named as follows

1. Uncompensated Ionizing Chamber Subsystem (UIC)
2. Dual Coupled Triode Subsystem (DCT)
3. A/D Master Relay Subsystem (MRY)
4. Slow Scram Slave Relay Subsystem (SRY)
5. Divider (DIV)
6. Fast Scram Pentode Subsystem (FSP)

The name "module" will be reserved for these six units only. All modules will be presented individually during the ongoing analysis. The reader should refer to each unit's figure in Chapter 2 and to the Safety Amplifier schematic diagrams (Figures [1-6], [1-7], and [1-8]) frequently in order to understand how the signal flows through the system and how the units are connected. In order to avoid redundant explanations, the logic of the Safety Amp operation is not systematically portrayed in this report. It is covered in other MNR documents. The interested reader is urged to read internal MNR document 6147-A. For the purposes of our analysis we must use a level of abstraction that is appropriate for

reliability assessment and not for electrical circuit analysis. The signal that we follow is essentially an information flow signal and does not necessary represent any physical quantity like current, or voltage. Accordingly, we will build a fault tree systematically "from top to bottom", and not by following any physical signal flow from input to output. Determining the top portion of the fault tree requires a precise definition of the function of the system. We may say that:

- The function of the Safety Amp is to cutoff the current to at least three rod-magnets when: a) both UIC Chambers activate, or b) Log-N Amplifier activates.

We chose both chambers to activate (not necessary at the same time) instead of each single chamber separately, because they respond to the same demands, and their failures are not independent. Namely, since the chambers are: 1) located near to each other, 2) operate under same environmental conditions, and 3) are considered to be individually reliable, their failures are correlated due to common causes. Nevertheless, once the fault tree is developed, it is easy to run the program for the case where the two UIC inputs (not the chambers) are completely separated. However, these results can be meaningful only if the correlation between the chambers' failures is known. Note that we would still have to run the program both for both inputs and for each input individually, in order to find the correlations between the Safety Amplifier's unavailabilities that belong to the different inputs. It is important to note that, since the two UIC chambers and the two corresponding SA inputs are not correlated, as indicated in Figure 1-4, the chambers and inputs can be analytically disjointed. Let A_1, A_2, B_1, and B_2 (see Figure

1-4) be events, each denoting the failure of the corresponding unit. Then, the UIC chambers - Safety Amplifier pair (henceforth UIC-SA) fails to respond on high power trip if and only if (A_1 A_2) (B_1 B_2) happens. Hence, the probability of the failure of UIC-SA yields

$$\begin{aligned}
&\Pr((A_1 \cup A_2) \cap (B_1 \cup B_2)) = \Pr\bigcup_{i,j}(A_i \cap B_j) \\
&= \Pr\bigcup_{i}(A_i \cap B_i) + \Pr\bigcup_{i \neq j}(A_i \cap B_j) - \Pr(A_1 \cap A_2 \cap (B_1 \cup B_2) \\
&\cong \Pr\bigcup_{i}(A_i \cap B_i) = \Pr(A_1|B_1)\Pr(B_1) + \Pr(A_2 \cap B_2)
\end{aligned} \tag{1.8}$$

where the terms with negligible cross-dependencies are ignored. The result is analytically convenient, since the two remaining terms in Equation (1.8) separate the variables that belong to the UIC from those belonging to the SA. The last term in Equation (1.8) shows that we have to analyze only the simultaneous failures of UIC inputs.

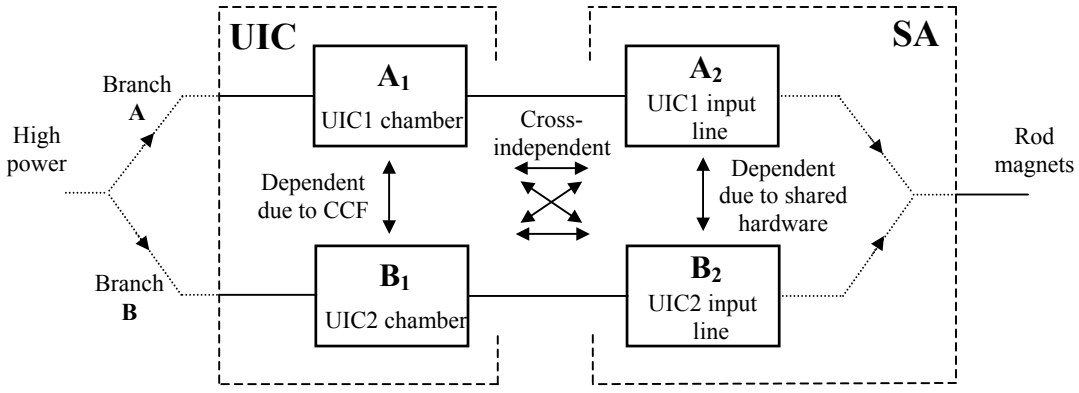

Figure 1-4. The connectivity between the UIC chambers and the Safety Amplifier

Note that the separation of variables would not be possible had the UIC-SA covariance not had the following Jordan canonical form

$$Cov(UIC-SA)=\begin{bmatrix} Cov(UIC) & \mathbf{0} \\ \mathbf{0} & Cov(SA) \end{bmatrix},\ where\ \ Cov(UIC)=\begin{bmatrix} \Pr(A_1) & \Pr(A_1 \cap B_1) \\ \Pr(B_1 \cap A_1) & \Pr(B_1) \end{bmatrix},\ etc.$$

Example:

Consider the following per-demand failure probabilities:

$$\Pr(A_1)=\Pr(B_1)=10^{-5}$$
$$\Pr(A_2)=\Pr(B_2)=10^{-7}$$
$$\text{No. of high - power occurences } = 1$$
$$\Pr(A_1|B_1)=0.02$$
$$\Pr(A_2|B_2)=0.9$$
$$\Pr(X_i|Y_j)=\Pr(X_i) \quad \text{if } i \neq j$$

Equation (1.8) immediately yields

$$\Pr(A_1|B_1)\Pr(B_1)+\Pr(A_2 \cap B_2)=0.02\times 10^{-5}+0.9\times 10^{-7}=2.9\times 10^{-7}$$

which is the UIC-SA failure probability per single demand. The reader might find it easier to think that this result must equal the probability that the branch A fails, and then the branch B fails given that A has failed, or

$$\begin{aligned}&\Pr(A)\times\Pr(B\mid A)\cong(\Pr(A_1)+\Pr(A_2))\\&\times\left(\frac{\Pr(A_1)}{\Pr(A_1)+\Pr(A_2)}\Pr(B_1\mid A_1)+\frac{\Pr(A_2)}{\Pr(A_1)+\Pr(A_2)}\Pr(B_2\mid A_2)\right)\\&=\Pr(A_1)\Pr(B_1\mid A_1)+\Pr(A_2)\Pr(B_2\mid A_2)=2.9\times 10^{-7}\end{aligned}$$

which yields the same result as above.

We will analyze each individual module of the Safety Amplifier by pursuing the fault trees presented in the Figure 1-5. The two fault trees presented belong to two different scenarios, or event sequences. These two scenarios exist because an initiating signal may come either from the Log-N Amplifier (short period signal), or from the UIC chambers (high-power signal).

Compound subsystems in the Safety Amplifier are

1. Slow Scram Subsystem (SSS)
2. Fast Scram Subsystem (FSS)

All subsystems, whether simple or compound, represent logical gates in a fault tree.

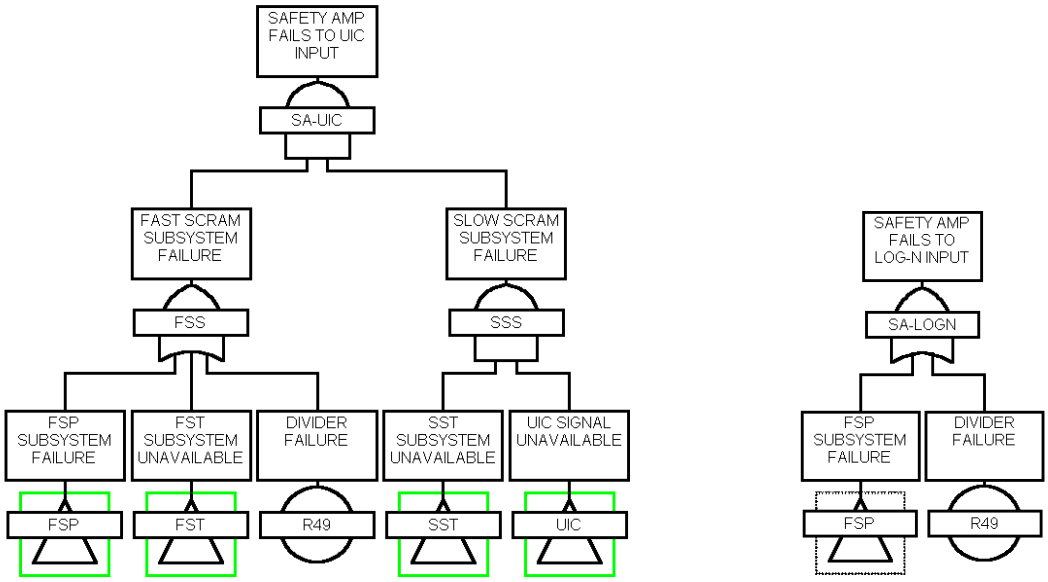

Figure 1-5. Fault trees of the Safety Amplifier

Units will be named by their order of appearance in a subsystem (i.e. DCT-1, DCT-2, etc.) or by the name of the characteristic component within the unit.

The complete list of units is as follows:

1. UIC: RY13 (UIC-1), RY14 (UIC-2)
2. DCT: V1A (DCT-1), V1B (DCT-2), V2A (DCT-3), V2B (DCT-4)
3. MRY: RY1 (MRY-1), RY2 (MRY-2), RY3 (MRY-3), RY4 (MRY-4)
4. SRY: RY5 (SRY-1), RY6 (SRY-2), RY7 (SRY-3), RY8 (SRY-4)
5. DIV: R49 (DIV-1), R53 (DIV-2), R55 (DIV-3), R57 (DIV-4), R59 (DIV-5)
6. FSP: V3 (FSP-1), V4 (FSP-2), V5 (FSP-3), V6 (FSP-4)

A collection of units will be denoted by parenthesis, e.g. MRY(1-4) means "all four units in MRY", and any single unit from the given collection of units by brackets, i.e. MRY[1-4] means "any one of the units MRY-1, MRY-2, MRY-3, MRY-4". Also, recursive expressions are allowed. Thus, SDA(1-2) means "both subsystems 'V1A and RY1' and 'V1B and RY2'", while SDA[1-2] means "any one of the subsystems 'V1A and RY1' or 'V1B and RY2'. Recursive names will be used only for subsystems composed of neighborhood units, i.e. when the signal within the subsystem flows uninterruptedly, thus preserving the physical meaning of the word "subsystem". However, these units may not belong to the same module.

Note finally that the modular decomposition presents an attempt to divide the system into parts along the direction of the signal flow. Signal flow is then presented as a vector with threads, or channels. The boundaries of the modules are assemblages of threads such that if one thread belongs to a minimal cut set then all threads from the assemblage must belong to that minimal cut set. Each unit within a module belongs to a distinct thread.

(Note: for Figure 1-6 see file “4a Figure 1-6”)

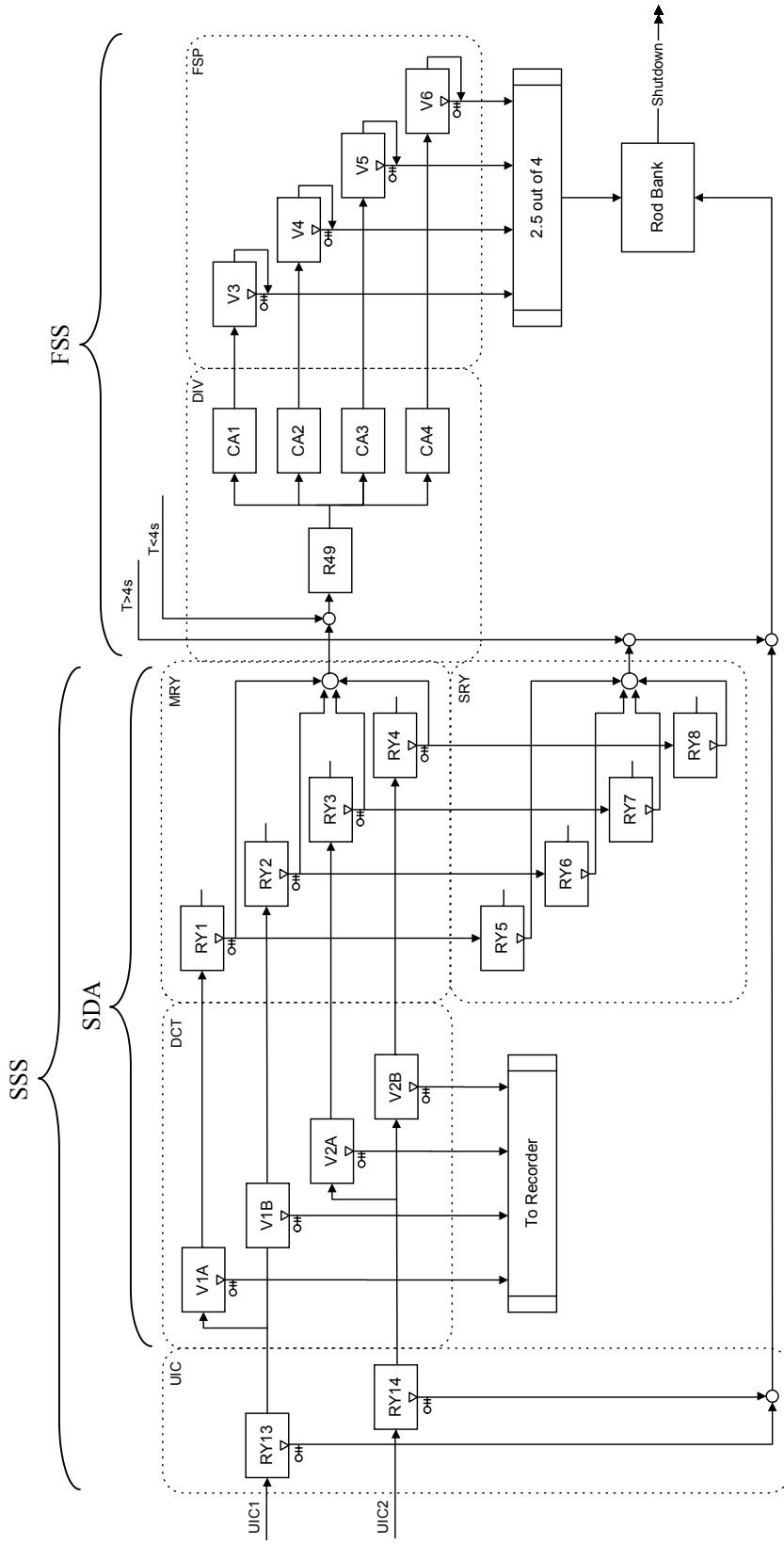

Figure 1-7. MNR Safety Amplifier Success-signal Propagation Chart

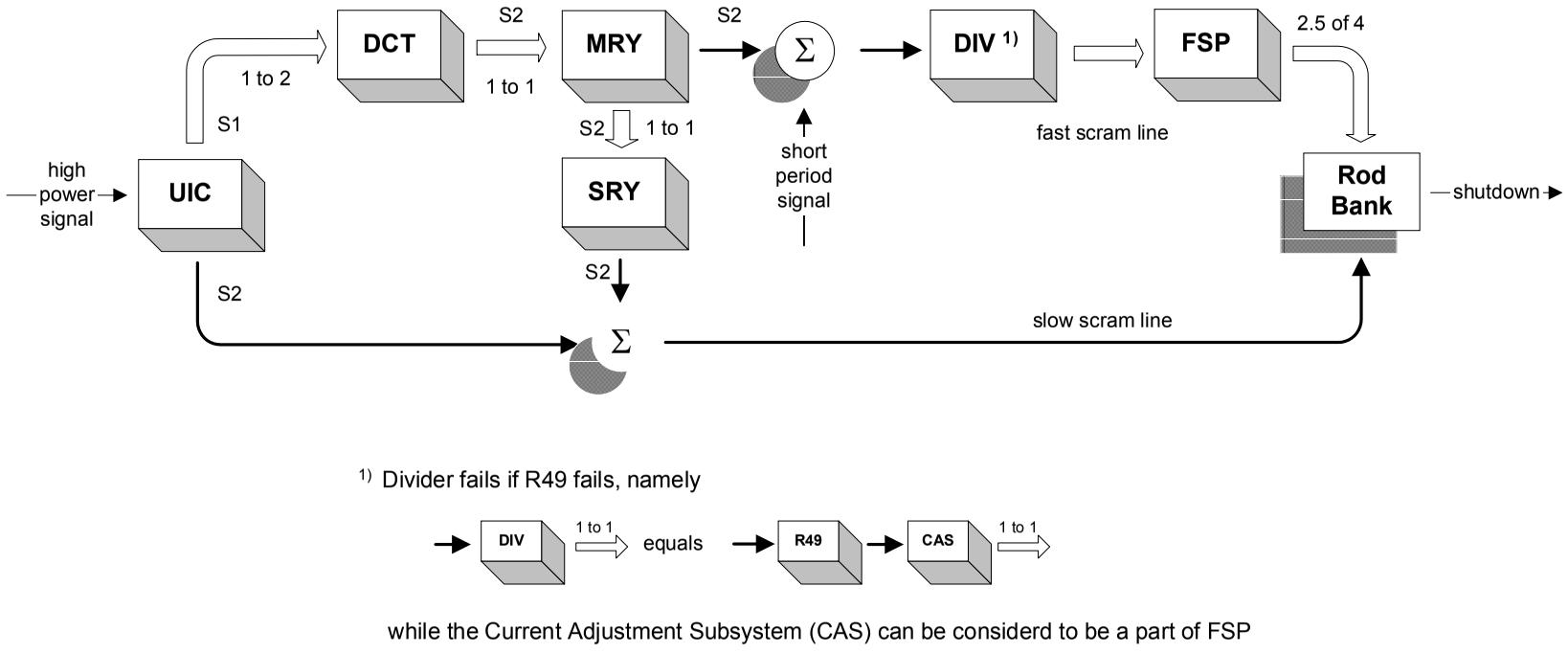

Figure 1-8. MNR Safety Amplifier Success-Signal Propagation Chart, Matrix Form

Figure 4. Success signal propagation chart - matrix form

1.4. Repairable Systems with Supervision

For purposes of availability analysis it is important that we make a distinction between the actual repair time and the failure detection time. ***Actual repair time*** represents the time for unit replacement or any other operator's repair action once the failure of the component has already been detected. ***Failure detection time*** is the time span from the time of failure to the moment when the actual repair is notified or begins. Thus, the ***total repair time*** equals failure detection time plus actual repair time. Consider the following case:

> The purpose of the resistor R99 (see Figure [1-6]) was to enable the replacement of any single defective pentode while under operation. After the resistor R99 had been removed from the circuitry, the actual repair time for each fast scram pentode unit was virtually brought to zero, because in a case of a failure either the rod(s) controlled by the defective pentode would be released, or else the operator would shutdown the reactor prior to repair, i.e. immediately after receiving the signal from the neon bulb B[5-8].

If the complete MNR maintenance and inspection policy had been designed following this case, the reactor would never operate under actual repair. This, however, increases the cost of operation and a certain risk of an accident that minimizes the cost/benefit ratio is allowed, leading to acceptance of the reactor operation under repair. However, the Safety Amplifier itself should not be put under repair while the reactor is operating. The

only time when the reactor is operating while the Safety Amplifier is not should be before its failure is detected.

The failure detection time itself consists of two parts. The first part is determined by the time window between the tests of the unit and the second part is determined by the unit's signaling device failure probability. An example of signaling device failure is the B[9-10] failure (bulb failure) in the RY[13-14] unit. In this case B[9-10] failure cuts off the cabling error signal from the UIC[1-2] making a RY[13-14] failure undetectable to the operator.

Figure 1-9 depicts a system consisting of two identical active parallel units, for example, triodes V1 and V2 (see Figure 1-6). λ represents the failure rate of one unit, and μ represents the repair rate of one unit. λ^* represents the rate of failure of both units simultaneously, and τ is the time between the tests. If the actual repair is performed while the system is in suspended state only, the repair rate μ remains finite only because there is a time delay time between the failure of a unit and the first subsequent scheduled test of the unit. Thus, the mean repair time is the time span between the actual failure and the

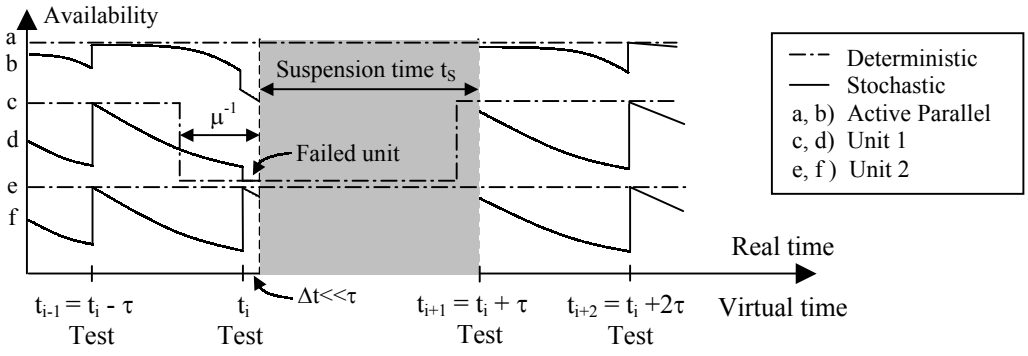

Figure 1-9. Timeline Diagram of a System with Two Active Parallel Units

detection of the failure. Without a loss of generality, we may assume no delay in the transition of the system from active to suspended state once the failure of any unit is detected. Hence, the 'effective' repair rate, μ, of any of unit becomes a function of both failure rates of the unit (λ, λ^*) and the rate at which the test of the unit is performed, τ^{-1}. Although we cannot change the failure rates, by increasing the test rate we can effectively alter the repair rate and thus increase the availability of the system. If we assume that the units cannot fail simultaneously, the availability of the redundant system can be brought arbitrarily close to unity. In this manner, we can incorporate the tests, which are essentially deterministic events, into the memoryless stochastic transition rates, and analyze the system transitions using the markov modeling techniques.

Finally, the Safety Amplifier should be tested as frequently as possible, taking into account the cost/benefit considerations. Although no recommendations towards maintenance policies are made by International Commission for Radiation Protection (ICRP), the national regulatory agencies (AECB) are likely to adopt their recommendations for stochastic limits on dose uptake, which converts to the risk and finally to the equipment reliability parameters. As outlined in ICRP documents, the cost/benefit criteria should include socio-economical factors, and not just corporate revenue or other internal interests (ALARA principle). According to maintenance policy, different parts of the Safety Amp are being tested in different time intervals – daily, weekly, monthly, semiannually, etc. By varying the importance parameters it can be shown whether or not these time intervals are appropriately chosen, and consequently

whether or not the resulting Safety Amplifier limiting unavailability is being kept within reasonable limits.

We should not disregard the fact that a supervising unit, which by definition undertakes an action when error conditions are met, is a vital part of a safety system. A supervising unit can be a part of the equipment, but it can also be supervised against failures by another unit. Eventually, the action that has to be undertaken by some of these units at some point will become complex enough - replacement of the electronic tube is a good example - or even unpredictable, so that the human intervention is needed. Inevitably, at the end of the supervising chain is always a human operator (who, by the way, is also supervised, but we disregard this fact herein).

As an example of a machine supervision one may think of the safety amp as a supervisor of the UIC chambers. When the chambers provide appropriate signals ($I>125\mu A$), the safety amp acts. The action in this case is always the same, namely "cut-off the current to the safety rod bank". The neon bulb, on the other hand, is not a supervising unit because it does not perform any action. It is just a signaling device, serving to open an information channel to a human supervisor who should perform an action that is apparently too complex for the machine to handle. The input signal to a supervisor is an "error condition signal" so that the supervisor is a component that is always in a standby mode during the normal operation.

1.5. Subsystems and the Unit Prototype

A typical unit with a supervising and signaling device is presented on the Figure 1-10. Units like this are put together to form logical subsystems of the Safety Amplifier.

A typical unit in safety amp has three outputs:

- output signal 1 (or S1) represents a default action signal that the host unit (active element) delivers to the subsequent unit. As a response function with zero delay, S1 depends only on the current input signal and the internal state of the host unit.

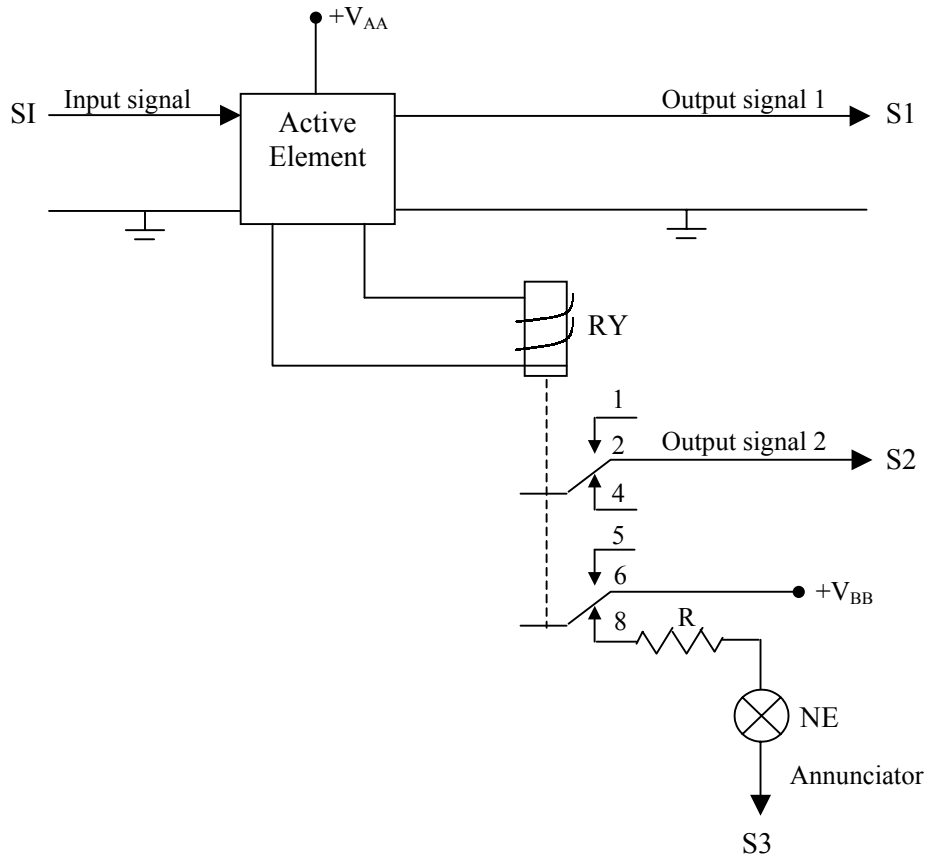

Figure 1-10. Typical Unit of the Safety Amplifier

- output signal 2 (or S2) can play the role of the output signal S1, in which case the signal S1 is omitted, but it can be also representing an error condition signal. This action signal is frequently coupled with a signaling device, and represents a no-delay response to the internal state of the host unit rather than the response to the input signal itself. Output signal S2 is often a part of the redundancy loop made by a serial connection of several identical units.
- state annunciator signal (S3) is often used to bring attention of the supervising unit that the error conditions were met. The supervising unit than acts either deterministically or by making a *decision*. Without this signal the unit, if put in parallel, would form a simple parallel connection with no repair capabilities. No repair is possible because no failure can be detected. In this case, regular inspections should be performed, but since they are expensive and therefore less frequent than tests, the failure detection time becomes much longer.

To illustrate the role of the signaling device in an arbitrary redundant system, two distinct signal propagation paths (path sets) are presented in Figure 1-11. The failure of the component 'D', for instance, cannot be detected clearly. Still, some information about the state of 'D' is delivered. Component 'G' is virtually undetectable. There are 256 different states of the system, and only 4 annunciating states. If the failure probabilities of all component, including bulbs B1 and B2, are small, the failure of the component 'C' can be detected with high confidence (i.e. with confidence $1-p \approx 1$, where 'p' is a "weighted" failure probability of a single component).

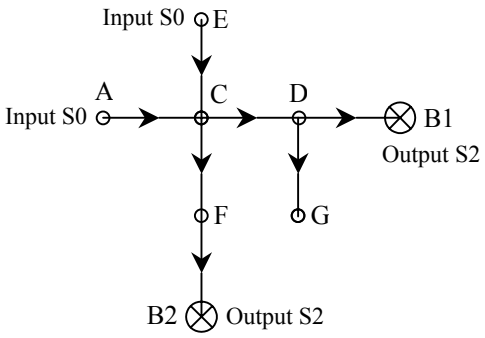

Figure 1-11. Signal Flow and Information Channels

Relay RY (see Figure 1-10) is normally *energized* (through V_{AA}) to enhance the system safety. If the power supply fails the relay activates. Recall that the signal we want to analyze is the failure signal, not the current or the voltage. Therefore, "to activate" means "to open a gate for the failure signal". This action is usually to disconnect the circuit in which the unit is connected to several other units in series. Let x_j represent the functioning state (x_j=1) or a failed state (x_j=0), (j=1,…n), of each component in the system. The system structure function $\phi(x_1,\ldots,x_n)$ is defined as a binary function of its arguments. It is assumed that the system is functioning if ϕ I and is failed if ϕ ĭ. The term "redundancy circuit" denotes a close loop of units that all have identical function, i.e. that are symmetrical in terms of permutation of the arguments in the system structure function. (For more about structure function see [Barlow-Prochan, 1975].) The unit x_j is loosely redundant if there is a state $(x_1,\ldots,0_j,\ldots,x_n)$ in which $\phi(x_1,\ldots 0_j,\ldots,x_n)$=1, i.e. if there is a state in which the system is working while x_j is failed. Note that the redundancy unit must not necessarily have an identical counterpart in the system. As we are about to

see, the reliability of a redundant system is greatly increased if the failures of its units are detected early.

The typical unit presented on Figure [1-10] has three components:

- Active Element (AE)
- Relay (RY)
- Neon Bulb (NE)

These components are responsible for creating three corresponding outputs that we will denote as

- Output Signal 1 (S1)
- Output Signal 2 (S2)
- Annunciating Signal (S3)

Note that some of the components or outputs may be missing in some modular units of the Safety Amplifier. This fact is presented in the Table [1-1].

	AE	RY	NE	S1	S2	S3
UIC		✓	✓	✓	✓	✓
DCT	✓		✓	✓	✓	✓
MRY		✓	✓		✓	✓
SRY		✓			✓	
DIV				✓		
FSP	✓	✓	✓	✓	✓	✓

Table 1-1. Components of the Typical Unit That Correspond to Different Modular Units

Note: Newark Electronics Catalog, 1997 edition gives the value of 15,000 operating hours for the average lifetime for the neon bulb NE51 used in the safety amp as a signaling device. For instance, each one of the neon bulbs B[5-8], if energized, indicates that the filament of the corresponding pentode V[3-6] had burned-out. The bulbs themselves have no filament and withstand considerable shock vibrations. They are rugged and long-lived, and are ideal for use on circuit boards. As a result, they are typically used as indicators in circuit control applications. While the Safety Amp is in dormant state, the neon bulb light is off. Hence, aging becomes the only contributor to the neon bulb's failure rate increase. Aging should be slow since the environmental conditions in the MNR control room are rather stable. Thus the neon bulb's real time lifetime is likely to be many times larger than 15,000 hours.

In the signal flow diagrams a functional unit will be represented by the symbol depicted on Figure [1-12]. Thus, by removing everything unnecessary from the electric circuit diagram we can draw a reliability diagram needed for cut set calculations (see Figure [1-7]).

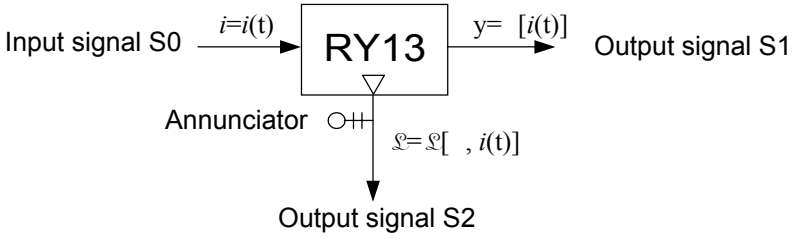

Figure 1-12. Symbol Denoting the Typical Unit in Signal Flow Charts

1.6. I/O Modes

As we already mentioned there are six logical modular subsystems. Each logical subsystem, according to the number of its inputs and required number of outputs, operates in one of four possible modes, as Figure [1-7] indicates. These modes are as follows:

- active quad-parallel mode (two inputs, four outputs)

  UIC subsystem - made of two UIC units
- active quad-quadruplet mode (four inputs, four outputs)

  DCT subsystem - made of four dual coupled triode units

  MRY subsystem - made of four supervised relay units

  SRY subsystem – made of four non-supervised relay units
- "2.5" out of 4 mode (four inputs, 2.5 outputs)

  FSP subsystem - made of four fast scram pentode units
- active quad-single mode (one input, four outputs)

  DIV subsystem – made of R49 and four non-supervised CAS units

SDA and FSP subsystems are connected through the divider DIV in series forming the Fast Scram Subsystem (FSS). SDA subsystem has two-component vector input from two UIC chambers and is supervised in cascade, first through the corresponding amp-meters M[1-2] (see Figure [1-6]), and then through the neon bulbs

B[1-4]. SDA and SRY subsystems are connected together in vector-series forming one part of the complete Slow Scram Subsystem (SSS), see Figure [1-7]. This has been established using the one-directional master-slave pull connection between the corresponding relays RY[1-4] and RY[5-8]. Each SRY[1-4] unit consists of a single relay that is not supervised. The second part of the SSS subsystem is made of two UIC connector error detection units that would activate if the connections between the corresponding UIC chamber and the amplifier fail due to the cable shorts, or if the power to chambers is cut off. UIC and SRY subsystems are connected together in parallel, forming a complete Slow Scram Subsystem (SSS) output. Finally, the output of the Safety Amplifier is a function of two input components: one component, a vector itself, comes from two UIC chambers, and another component, a scalar, comes from the Log-N Amplifier that detects short reactor periods. As each of the six modules has different unavailability and failure frequency characteristics, the next chapter will be dedicated to analyze the modular units separately.

1.7. Insufficiencies of the Traditional Reliability Theory

Traditional reliability theory is based on several assumptions that are too restrictive for applying to a wide variety of complex systems. In order to bring more light to the question of why we occasionally chose to employ a particular approach that may not be immediately obvious, a short retrospective of the basic definitions of the traditional theory together with some remarks about the heuristics behind it is given as follows:

1. A current *deterministic* state of the system, possibly not known to us, is described by the ***structure function*** $\phi(x_1,\ldots,x_n)$. A structure function is defined as a binary function of its arguments which represent the functioning state ($x_j=1$) or a failed state ($x_j=0$), (j=1,…n), of each component. The structure function completely determines the system's deterministic state from the reliability point of view, i.e. it is assumed that the system is functioning if ϕ I and is failed if ϕ ĭ.

2. The *j*th component is ***irrelevant*** to the structure function ϕ if ϕ is constant in x_j; that is if $\phi(1_j,\mathbf{x}) = \phi(0_j,\mathbf{x})$ for all $\mathbf{x} = (x_1,\ldots,x_{j-1},x_{j+1},\ldots,x_n)$. A component that is ***relevant*** to the structure function ϕ if there exists $\mathbf{x} = (x_1,\ldots,x_{j-1},x_{j+1},\ldots,x_n)$ such that $\phi(1_j,\mathbf{x}) \neq \phi(0_j,\mathbf{x})$.

3. A system is ***coherent*** if (a) its structure function ϕ is a non-decreasing function per each argument and (b) each component is relevant. A coherent system is arguably taken to present a "reasonably" designed system in which "a failure of a component cannot lead the system into a safer state".

4. The components' states and thus the system state are always assumed to be known at t=0. Even more restrictively, some fundamental theoretical results are known to be valid only under the assumption that all units are initially working, i.e. $x_j(t=0)=1$, (j=1,…n), and therefore $\phi(t=0) = \phi(x_1(t=0), \ldots,x_n(t=0)) = \phi(1,\ldots,1) = 1$. It can be easily shown that the latest identity is always true if the system is coherent and non-

trivial. A non-coherent system, however, may be in a failed state ($\phi = 0$) even if all its units are working.

5. If the arguments of the structure function are *statistically independent* random variables (processes) $X_1,\ldots,X_n$ then the ***reliability of the system*** is given by

$$P[\phi(\mathbf{X}(t)) = 1] = E\phi(\mathbf{X}(t)) = \phi\,(E\mathbf{X}(t)) \qquad (1.9)$$

Therefore, the reliability is the mathematical expectation of the structure function. Similarly, the entropy of the structure function represents our knowledge of the state of the system prior to some future time *t*. ("*E"* in Equation (1.9) stands for mathematical expectation.)

6. The structure function ϕ, and thus the reliability of the system in a traditional sense, essentially models the reliability, i.e. a survival probability, of a *single and specified output* y_0 of a system with a *single and specified input* i_0 that is always available, i.e. $y_0 \equiv \phi = \phi(i_0,x_1,\ldots,x_n) = \phi(1,x_1,\ldots,x_n)$. For that reason, the input and output of the structure function are usually not specified.

Next, we will show that the conditions [1-6] cannot prevail in the case of the Safety Amplifier.

First, we may say that the traditional theoretical assumptions insufficiently model the boundaries of a system both in time and space, thus making the system artificially

isolated from the surroundings (see conditions 1, 4, and 6 above). In addition, as opposed to conditions 2 and 3, most safety systems are deliberately designed to be non-coherent which, ironically, turns out to be an outcome of the very effort to increase the reliability of the system. In particular, the following conditions are violated in the case of Safety Amplifier:

1. Condition 3 violated: Safety Amplifier is not a coherent system. Given that relay RY13 is operational, UIC-1 (same as "RY13") unit outputs RY13-S1 and RY13-S2 are always in the opposite state, or succinctly RY13-S1⊕RY13-S2=1 (⊕ stands for exclusive OR, i.e. 'A⊕B' means A or B but not A and B). The structure function therefore cannot be a monotone function, since if it is increasing at relevant component RY13-S1 it is decreasing at RY13-S2. Recall that by the definition of the relevant component (see Condition 2), the structure function cannot be flat at all remaining variables.

2. Condition 4 violated: At no point of time after its commissioning forty years ago, except of course when a complete inspection is being undertaken, can we state that the Safety Amp is in "as good as new" state. Parallel connections without supervision are present, the most obvious one being the SRY module whose reliability at time t=0, i.e. immediately after *any* test, might be reduced to as low as one functioning unit RY[5-8] only.

3. Condition 5 violated: Component failures are not statistically independent. Beside the failure on demand "dependencies" there are other, more genuine dependencies that include:
   - effects that tend to increase the overall failure rate by increasing the events mutual dependencies. The most important effects belong to a group of "common mode failures"
   - effects that tend to decrease the overall failure rate by making some events mutually exclusive. This is the case with UIC module, and we will have to account for this effect separately.

4. Condition 6 violated: Safety Amplifier has several inputs (two from UIC chambers and one from the Log-N Amplifier), and several outputs (V3 to V6). Ordinary availability scalar functions therefore can not contain all information about the state of the system at any time.

1.8. Reliability Functions of the Multi-input Systems

Let $G_k=\{F^k_1,\ldots,F^k_{n(k)}\}$ be a family of all minimal cut sets of the system S given the input k=1,…,m, and let t be a mapping t: $\{1,\ldots,m\} \rightarrow \{0,1\}$. For each collection $t^{-1}(1)$ we denote by

$$\Gamma(t) = \{ \bigcup_{j \in t^{-1}(1)} F^j_{i(j)}, \quad 1 \le i(j) \le n(j)\} \tag{1.11}$$

a family of cut sets generated by the mapping t. Let $H(t)=\{H^t_p,\ p=1,..,q\}$ be a set of minimal cut sets in $\Gamma(t)$ and let $A(t)=\Pi A_k$, $k\in t^{-1}(1)$, be an availability of the input set $t^{-1}(1)$. Then, the availability A_M of the multi-input system $\{1,\ldots,m,S\}$ is given by the following minimal cut set approximation

$$A_M = \sum_{t\in\{0,1\}^m} A(t)[1-\sum_p \prod_j Q(H^t_{p,j})] \tag{1.12}$$

where $Q(H^t_{p,j})$ denotes the unavailability of the *j*th element in the minimal cut set H^t_p. Note that the mapping $t\rightarrow\Sigma\Pi Q(H^t_{p,j})$ is a monotone function of the lattice t.

Availability, mean time to failure (MTTF), and other reliability parameters that represent the output values of Safety Amp are multivariable linear forms. For example, the output availability depends on the unknown input availabilities from the uncompensated ionizing chambers and the Log-N amplifier. Besides, different signal propagation path-sets are available for different input nodes. Figure [1-13] represents a signal propagation graph with multiple inputs that is enclosed by the super-graph with one input that is always available. The unknown availabilities would appear in minimal cut-sets that would sum up to the resulting availability of the system. In case of identical components, the resulting availability is a multivariable polynomial transformation.

For the purposes of the fault tree calculation we would assume two simple scenarios: 1) both ionizing chambers available only (1,1,0), and 2) Log-N amplifier available only (0,0,1). These cases might appear in different places in the event trees

depending on the initiating events or other scenario related requirements. These two fault trees that corresponds to different initiators will be named SA-UIC and SA-LOGN respectively. By changing the parameters in a unique Safety Amplifier's fault tree that is suitably designed, however, the true availability and hazard rate might be calculated for each case of interest. For this reason we may include all input nodes into the fault tree as if they were basic events, giving them initially discrete failure probabilities (x_i=0 or x_i=1), although they are not exactly parts of the Safety Amplifier. By putting $x_1=x_2=\ldots=x_j=0$, we can also check the fault tree for consistency, because since Πx_i is a cut-set the output availability must become zero.

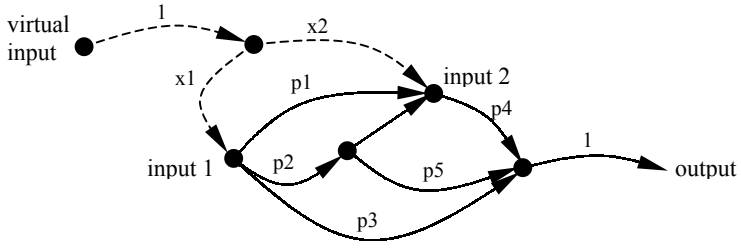

Figure 1-13. Multiple Inputs Enclosed in a Supergraph

A multiple input cannot be decomposed into a series of single case inputs, each one with its own reliability graph. It shouldn't be inferred that, assuming the rare event approximation, the final reliability could now be found as a simple linear combination of the single input reliabilities. Namely, the short time interval between different input signals implies that their responses are cross-correlated. In other words, if V3 fails after receiving the signal from UIC1, it would most probably also fail if the signal had come

from UIC2. This is because the inner state of V3, as a function of time, is the same in both cases, while the unit is unable to recognize where the input originated.

1.9 Initiating Events that may lead to Improbable Failures of the Safety Amplifier

In the probabilistic safety analysis of the MNR it is assumed that the initiating events for all relevant failures can be categorized into four different groups:

1. increased energy production
2. primary flow impairment
3. loss of pool inventory
4. loss of heat sink

Detailed analysis of the Safety Amplifier operation is required only for group one. As we tried to illustrate throughout this chapter, the Safety Amplifier is an integral and inseparable part of the bigger device that monitors and controls the power and power-rate in the core. On the other hand, monitors of the initiating events that belong to groups two, three, and four, are completely divided from the Safety Amplifier. They are put in series and connected, also in series, to the magnet power supply (look at Figure 1-6 for the SA magnet power line connector, CN-11). In case if any of these monitors activates, the power to the magnets that holds the shim-rods is disconnected. Therefore, the Safety Amplifier cannot fail with respect to these inputs.