Chapter 2

MNR Safety Amplifier Subsystem Analysis

In this chapter we will complete the reliability analysis of the Safety Amplifier by analyzing its individual subsystems in more detail. These subsystems together with the reliability unit that represents an abstract model of all reliability units were introduced in Chapter One. The abstract reliability unit is depicted on Figure [1-12]. Our goal is now to connect precisely each unit presented in Table [1-1] to this abstract model. Hence, the whole Safety Amplifier will be decomposed in the smallest parts possible, and yet the reliability picture will be preserved. Somewhat less attention will be given to the analysis of the Safety Amplifier electrical circuitry. For a detailed electrical operation of the Safety Amplifier refer to [AMF Atomics, 1958].

2.1. UIC Subsystem

Uncompensated Ionizing Chamber Subsystem (UIC) has two identical active parallel units: UIC-1, and UIC-2. Term “parallel units” means “units that belong to concurrent threads” (see Figure [1-7]). Term “active” as opposed to “standby” means that both units are operational at the same time. UIC-1 unit is presented on Figure [2-1].

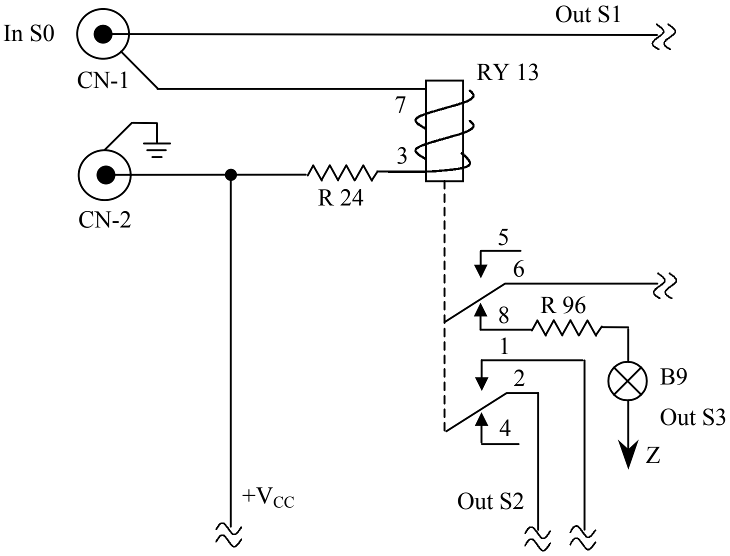


Figure 2-1. UIC-1 Unit

Each UIC unit provides its own error-condition detection line ("Out S2" on Figure [2-1]) and a signaling device for external supervision ("B9" on Figure [2-1]) that is also connected to the control board through the output line denoted by "Z". If the UIC cable is not properly grounded (i.e. the cable "fails") the relay RY13 activates (de-energizes). It is because the current cannot flow from $+V_{CC}$ through R24, then RY13, and then through the sheaths surrounding connectors CN-1 and CN-2, if the ground at CN-2 is lost (refer to Figure [2-1]). (Note that the default state of the input for all the figures in the report is the state of failure, S0=1). Connections 4 and 5 are not used. The device has one analog (S1) and two digital outputs (S2 and S3). Input signal S0 is analog and the cabling error signal is presumed to be digital since no current adjustment subsystem is provided to the unit. S2 and S3 are presumed to work synchronously, but the lines are physically separated to increase the probability of at least one line being operational. Thus, the redundancy has been implemented at the component level. An important theorem in reliability theory states that the redundancy at the component level is more effective than the redundancy at the system level, see Barlow-Prochan [1975]. The mode of operation of UIC units will be analyzed in Chapter 2.4 together with the rest of the SSS subsystem.

2.2. SDA Subsystem

Scram Level Definition and Activation Subsystem (SDA) is composed of four identical SDA units. SDA-1 unit (see Figure [2-2]) is a composite, two-module unit made of V1A and RY1 subsystems. The inputs and outputs to all three units on Figure [2-2], V1A, RY1, and SDA-1 itself, are all compliant to the abstract model from Figure [1-10]. The interface between V1A and RY1 units, presented with dotted line is located between points “Out S1A” and “In S0B”. The reason why we decided to analyze DCT[1-4] and MRY[1-4] together is because we wanted to discuss the presence of the current adjustment subsystem R18-R19. Also, the UIC chamber meter No1 sets the MTTR of V1A unit close to zero, making this unit rather simple to analyze. In other words, V1A cannot fail unnoticeably because of the continuous monitoring. Although the unavailability of V1A has been reduced greatly, this unit is not completely fail-safe, as its failure frequency remains the same as without the Chamber-meter No.1 supervision. Namely, this will alter the effective repair rate, or MTTR of the composite SDA-1 unit, comparing to the MTTR of the MRY-1 unit without DCT-1, since the new repair rate is weighted by the relative frequencies of the pure failures $\lambda(0\rightarrow\text{DCT-1})$ and

$\lambda(0 \rightarrow \text{MRY-1})$. ("Pure failure" means transition to a state that can not be reduced further and therefore is a singleton. This state is presented at the right of the arrow. A markov state is a mixture, or assemblage of pure states that have a specified number of failures.)

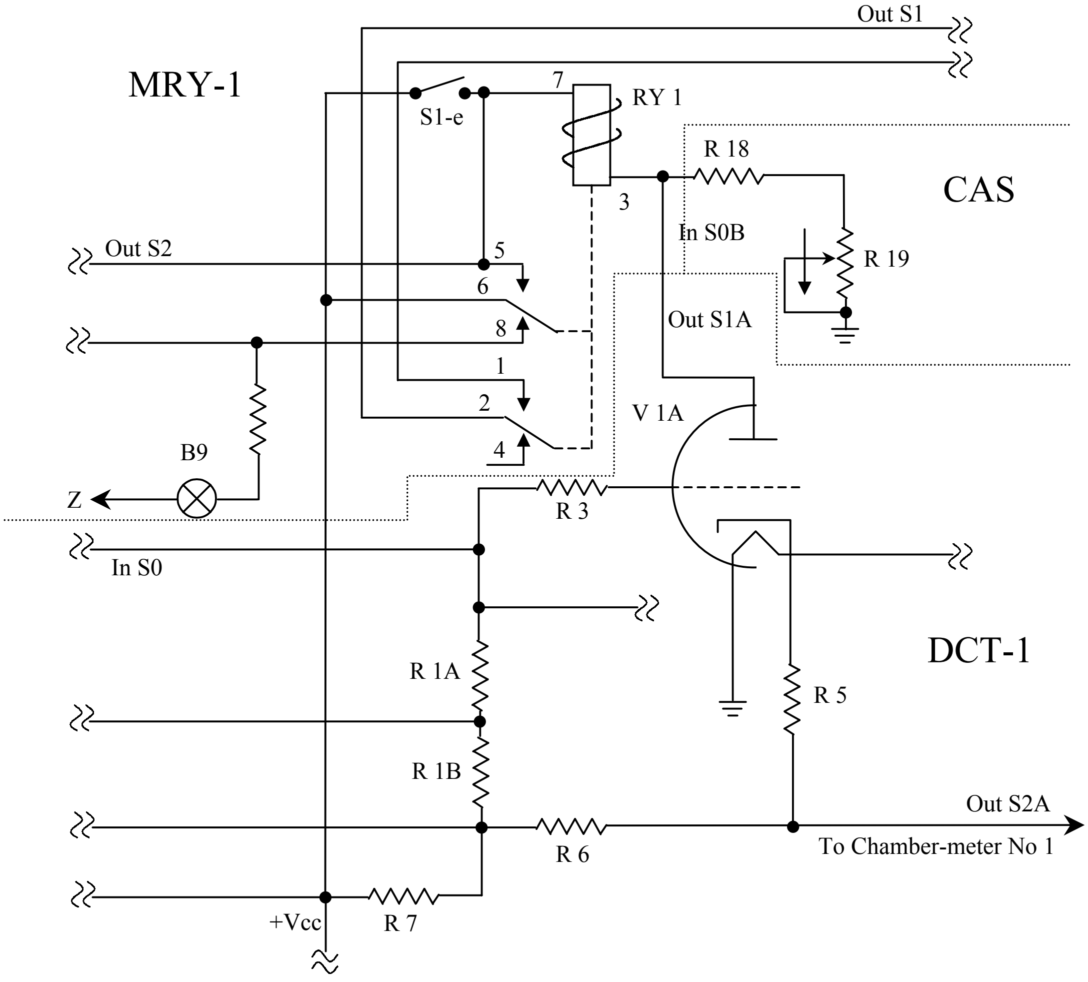


Figure 2-2. SDA-1 Unit

The following result represents the combined SDA unit reliability parameters in analytical terms (Barlow-Proschan, 1975, theorem 7.2.9.):

Model description:

Condition 1. The subsystem is assumed series, not an arbitrary coherent system. Thus the subsystem failure coincides with the failure of any of its unit.

Condition 2. While a failed unit is undergoing replacement, all other units remain in "suspended animation". When replacement of the failed unit is completed, the remaining units resume operation. At that instant, they are not "as good as new," but rather as good as they were when the system stopped operating.

Theorem: (Barlow-Proschan, 1975, theorem 7.2.9.)

(a) The average of system up times converges almost surely to

$$MTTF = (\sum_{j=1}^{n} (\frac{1}{MTTF_j}))^{-1} \tag{2.1}$$

(b) The average of system down times converges almost surely to

$$MTTR = MTTF \sum_{j=1}^{n} (\frac{MTTR_j}{MTTF_j}) \tag{2.2}$$

Convergence almost surely means that the probability of convergence is one. Our unit, for example unit SDA-1, consists of two prototypical units, DCT-1 (or V1A) and MRY-1 (or RY1), with their respective failure and repair rates λ_j and μ_j. Even without a proof it should be intuitively obvious that Equation 2.1 and Equation 2.2 must both hold, because (a’) MTTF for series system should be a harmonic mean of the units’ MTTFs, and because of the Condition 2 (see “model description”), MTTF does not, in fact, depend on MTTRs (Equation 2.1).

(b’) The system’s repair rate of the series system (Condition 1) is likely to be a weighted harmonic mean of the units’ repair rates. Equation 2.2 states that these weights are proportional to the units’ failure rates.

Recall that $MTTR(V1A) \approx 0$. According to the above theorem

$$\begin{aligned} MTTF(SDA-1) &= \frac{MTTF(V1A)\cdot MTTF(RY1)}{MTTF(V1A)+MTTF(RY1)} \\ &= \frac{1}{\lambda(0\to V1A)+\lambda(0\to RY1)} = \frac{1}{\lambda(0\to 1)} \end{aligned} \tag{2.3}$$

and

$$\begin{aligned} MTTR(SDA-1) &= \frac{MTTF(V1A)\cdot MTTF(RY1)}{MTTF(V1A)+MTTF(RY1)}\cdot\frac{MTTR(RY1)}{MTTF(RY1)} \\ &= \frac{1}{\mu(RY1\to 0)}\cdot\frac{\lambda(0\to RY1)}{\lambda(0\to V1A)+\lambda(0\to RY1)} \\ &= \frac{1}{\mu(RY1\to 0)}\cdot\frac{\lambda(0\to RY1)}{\lambda(0\to 1)} \end{aligned} \tag{2.4}$$

Here, $\lambda(0\to V1A)$ means “the failure rate for transition from the working state of SDA-1 to the state in which V1A unit has failed”. Using the convention used in Markov analysis, “0” denotes the state in which all units in SDA-1 are working, while “1” denotes that SDA-1 has failed, which is equivalent to a failure of either RY1 or V1A.

DCT-1 unit is the actual amplifier of the Safety Amplifier. The triode amplifies the voltage between the point where resistors R3 and R1A are joined and the point where resistors R5 and R6 are joined. As the signal InS0 increases the holding control grid current decreases until dropout occurs at a point determined by the amount of the by-pass current set by CAS. RY1 current drops because of the high voltage introduced to the V1A plate, which equals the voltage at the connector No.3 of the relay RY1. RY1 de-energizes and opens the fast scram circuit (see Figure 2-4) as well as the +300V supply to the slave relay RY6 (slow scram input SRY-1 InS0, see Figure 2-5).

Although the Current Adjustment Subsystem, represented by branch R18-R19 on Figure 2-2, can be considered either as a part of the V1A output or as a part of the RY1 input, it is strictly speaking not a part of any of the two subsystems but rather the interface between them. It serves to adjust the output resistance (impedance) of V1A to the input resistance (impedance) of RY1 in order to reach certain working point characteristics. Namely, any spontaneous change in characteristics of either V1A or RY1 alone would dislocate this point from the optimal position, thus affecting the operating characteristics of the combined system. Other current adjustment systems are: the CAS units at the end of the UIC chamber-meters, and a vector CAS unit set between SDA and FSP as a part of the divider DIV (see Figure 2-7). The principle of CAS operation in all cases is depicted on Figure 2-3 where the operating point of the system is presented as an intersection in working characteristics of two arbitrary systems, named A and B. Each system has one pair of connections. The same figure presents both: 1) first system as a source and the second system together with CAS as a load, and 2) the second system as a source and the first system together with CAS as a load. In case of V1A and RY1, the coarse position of the operating point is set by R18, and the fine adjustment needed for compensating the point migration due to, for example, different responses to temperature changes or aging, is made by R19. Note that the neon bulb indicator B9 (see Figure [2-2]) detects regular operating conditions (since S1=S2) as well as some error conditions. In case if error condition is tested, parallel information channel must be set by operator who must deliberately create a scram in order to perform a test. Note also that RY1 cuts off its own power supply in addition to that of the slave relay RY6. Operator must use switch S1-e (the “reset” button) in order to reverse the system into the previous, conditioning state. This is a safety feature. Namely, after RY1 is once de-activated the system cannot reach the previous operating state from any subsequent state automatically. Thus, the operator is forced to bring attention to the cause of the scram. In addition, a type of relay that has two sets of connections is chosen for RY1 (Sigma-22RJ). In comparison to

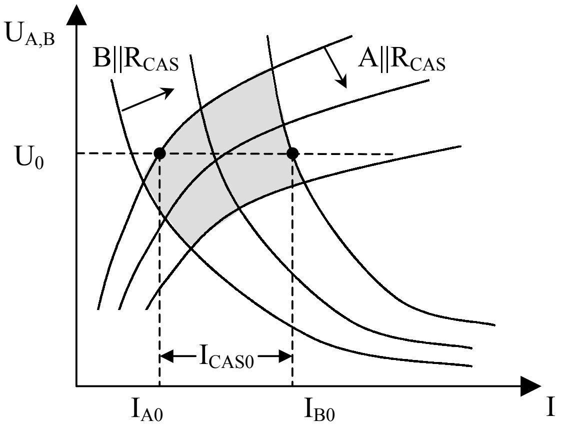


Figure 2-3. Operating U-I Characteristics with CAS on the Interface

connecting both S1 and S2 outputs to a single set, this choice has obvious advantage in increasing the survival probability of at least one output channel. In case of MRY unit these two channels split the signal propagation route into fast scram line and slow scram line. In the way they are used, all relays (there are three different types used in the Safety Amplifier) have two distinctive characteristics:

1. All relays are energized while they are in dormant state
2. The default response to the input scram signal S0=1 is always to open the active line, resulting in S1=1.

The first characteristic, as already mentioned, is a significant safety feature that greatly reduces the possibility of reaching the illegal state represented by (S0=1, S1=0, S2=0). The second characteristic is the result of optimizing the connections between the threads. The solution must be simple, because any additional (non-redundant) part in the circuitry will only increase the overall probability of failure due to existence of the additional cut sets. Two complementary solutions are presented on Figure 2-4, both in case of the "energized dormant state". The advantage of the dormant close line (DCL) solution over the open line is in reducing the delay of the output response by reducing the time constant of the system. By opening the closed line in case of scram, the first (left) solution suppresses the current below the operating threshold almost immediately, while by closing the opened line the second (right) solution might require much more time to surpass the operating threshold level. The threshold level can be made arbitrarily close to the operating point of the subsequent unit if energized (by using CAS, for instance), while it cannot be made arbitrarily close to the zero point necessary in the case if the subsequent unit is in de-energized dormant state.

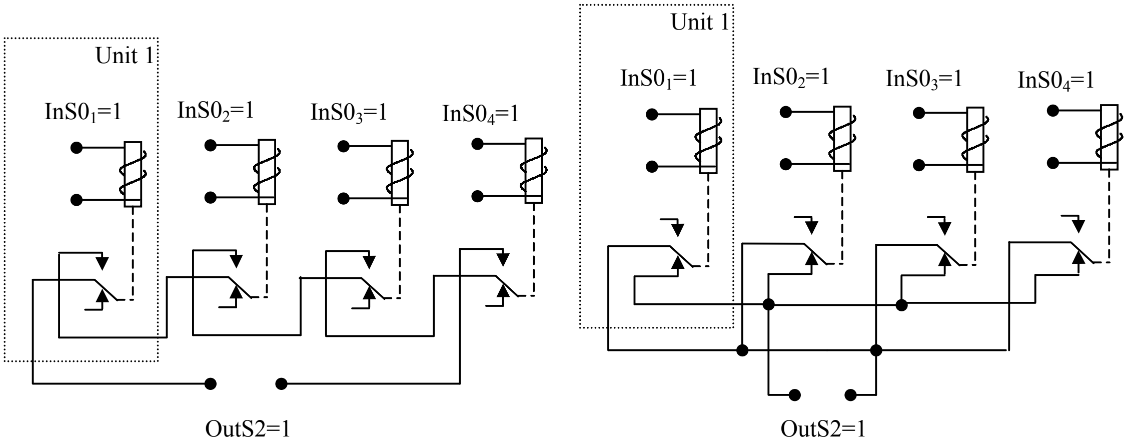


Figure 2-4. Parallel Thread Designed as: Dormant Closed Line (DCL, left), and Dormant Opened Line (DOL, right)

2.3. SRY Subsystem

Slow Scram Slave Relay Subsystem (SRY) has four units and it represents the simplest subsystem in the Safety Amplifier. SRY-1 unit is depicted on the Figure 2-5.

The input of the SRY unit (denoted as “In S0” in Figure 2-5) is connected to the output of the MRY unit (denoted as “Out S2” in Figure 2-2). When the scram signal reaches the output of the MRY unit, it is amplified and discretized, so that it can act as a switch. It is obvious that at this point the signal is ready to be delivered directly to the rod magnets without passing through any “parasitic” components that may only fail. This has been accomplished by means of disconnecting the power supply to the rod-magnets - the solution that is virtually fail-safe. However, since this “slow scram line” requires some time for the power supply current to die-off, another line, called “fast scram line” was introduced. This line requires additional hardware - fast switches, for which the pentodes were ideal candidates. The fast scram line compromises the reliability for performance. The designers also wanted the RY[1-4] to be able to cut off its own power supply for the reasons explained earlier. Because of the lack of sufficient connections, relay RY[5-8] was attached as a slave to RY[1-4] (in parallel with RY[1-4]) to provide the switch for the slow scram line. This relay alone constitutes SRY[1-4] unit (see Figure 2-5).

The characteristic feature of the SRY subsystem is that it can only be supervised as a system, and not per channel (unit-wise). Since SRY units are put in parallel, their long-term availability decreases with time if no appropriate inspection strategy is applied. Thus, the long-term “safety efficiency” of the unsupervised SRY unit is low. In order to include this fact into our calculations we may state that the distinction among the repair times

1) due to the supervising action failure
2) generated by a signaling device or Z-output failure, and
3) generated by tests or inspections

is necessary for more accurate reliability predictions. Hence, the complete set of different testing path sets (in the reliability graph) should be constructed, according to different testing times (weekly, monthly, etc.) Also some units, like SRY relays, can be tested against failures *only* by inspection, as these units do not have a signaling device at all.

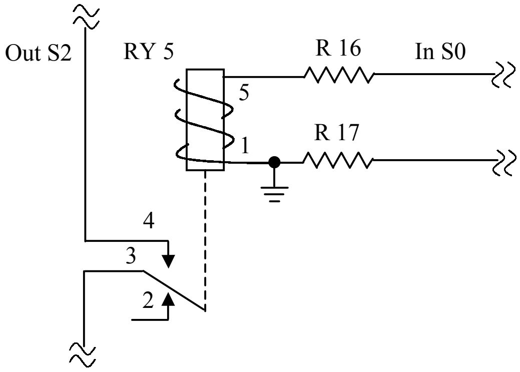


Figure 2-5. SRY-1 Unit

Note that all redundancy units are hidden from testing paths if they lack a signaling device. Hence, the reliability of the system over a long period can decrease significantly, because not even the failure of the entire system guaranties that these sub-failures would be detected and that the corresponding units would be repaired. Is it then possible that over the 40 years of operation some of the SRY relays are inoperable? The following calculation shows that even with arbitrarily large common cause failure rate λ^* this is highly unlikely. The initial reliability of an SRY[1-4] unit can be found as follows:

The unconditional probability that the relay is working after 40 years of operation is simply the reliability $e^{-\lambda t}e^{-\lambda^* t}$, where t = 40 [years], λ denotes the inherent failure rate of the relay, and λ^* denotes the common cause failure rate, i.e. the rate of all events combined that would cause all four relays to fail. These two failures, characterized by λ and λ^*, are connected in series, since if either one of them happens it would cause the relay to stop operating. However, we know for sure that at least one out of four relays is working, so that the true reliability is larger than $e^{-\lambda t}e^{-\lambda^* t}$, because otherwise the neon bulb

NE51 at Magnet Power would fail to activate in the case of scram (see Figure [1-7]). In other words, the whole slow scram line is supervised, but the individual relays are not. The mean time between scrams is much smaller than 40 years. Hence, the true reliability equals the conditional reliability given that at least one relay is working. The probability that at least one relay is working is

$$\Pr(\textit{after } 40y \textit{ at least one relay is working}) = \coprod_{i=1}^{4} R_i(t)e^{-\lambda^* t} = [1-(1-e^{-\lambda t})^4]e^{-\lambda^* t}$$

where the operator $\coprod$, defined as $\coprod_j R_j = 1 - \prod_j (1-R_j)$, denotes the "parallel product". Here, the inherent failures (λ) are connected in parallel, i.e. all relays should fail in order for the condition "after 40y at least one relay is working" to be false. The common cause failure (λ^*) is connected in series, just as in the case above. Therefore, the "modified" initial reliability of an SRY[1-4] unit equals the conditional probability that after 40 years the relay is working, and essentially equals the unconditional probability that after 40 years the relay is working without having common cause failures, i.e.

$$\begin{aligned} R(t=0) &= \frac{R(\textit{after } 40y \textit{ the relay is working, unconditionally})}{P(\textit{after } 40y \textit{ at least one relay is working})} \\ &= \frac{e^{-\lambda t}e^{-\lambda^* t}}{[1-(1-e^{-\lambda t})^4]e^{-\lambda^* t}} \cong e^{-\lambda t} = e^{-10^{-7}\times 40\times 4160} = 0.983 \end{aligned} \tag{2.5}$$

This simplified model did not include failures that may be common only to two, or three out of four SRY relays.

2.4. Slow Scram Subsystem Interdependencies

2.4.1. Calculation of Availabilities by Event Space Decomposition Method

Slow Scram Subsystem (SSS) consists of UIC, SDA, and SRY subsystems that are interconnected in such a way that their effective failure modes are mutually dependent. Dependencies usually make most methods, like cut-sets, rare event approximation, etc., useless. UIC-to-SDA dependencies are generated in the UIC units because of the different routes of signals S1 and S2. We will use the principle of total probability (see Appendix 1) in order to decompose the probability of the SSS signal propagation into terms. Each term shall correspond to the combination of values of error output signals S2 in UIC(1-2) units. Recall that the UIC(1-2) units' active components are cable connections. Each set of cable connections acts as a semaphore between the S1 and S2 output. Hence, the partition π of the event space in each of the two cases, UIC-1 and UIC-2, is simply π(UIC-1) = π(UIC-2) = {cable connections fail, cable connections do not fail}. Next, we will find the exact SSS structure function and corresponding reliability function using the partition method, and then we will show that in case when the dependencies are caused by the partition of the event space, the minimal cut-set method still provides acceptable results. In fact, it would provide more accurate results than in the case where events are assumed independent.

Since the signal propagation time is short comparing to the characteristic system times (λ_i, μ_i), we can directly calculate the reliability of SSS at each point of time. Time variable, therefore, will not be presented in the calculation to follow.

The UIC1-V1 line (henceforth denoted by subscript L1) would fail to deliver the scram signal from input to output if it falls in a state $S_{L1}=(X_1,X_2,\ldots)$ such that $\phi_{L1}(S0=1,S_{L1})=0$. Structure function ϕ_{L1}, state input S0, and the state vector S_{L1} are discrete random variables. Probability of being in such a state is $P(S_{L1}=\text{fail}) = P(\phi_{L1}=0 \mid S0=1)$, where the condition "S0=1" will be omitted in the following calculation for brevity:

$P(\phi_{L1}=0)$
$= P(\phi_{L1}=0$ | cable fails)·P(cable fails)
$+ P(\phi_{L1}=0$ | cable does not fail)·P(cable does not fail)
= P(RY5=0 "AND" RY6=0 "AND" RY13=0 | cable fails)·P(cable fails)
+ P(RY5=0 "AND" RY6=0 "AND" RY13=0 | cable does not fail)·P(cable does not fail)
= P(RY13=0 | RY5=0 "AND" RY6=0 "AND" cable fails)·P(RY5=0 "AND" RY6=0 | cable fails)·P(cable fails) + P(RY5=0 "AND" RY6=0 | RY13=0 "AND" cable does not fail)·P(RY13=0 | cable does not fail)·P(cable does not fail)
= P(RY13=0 | cable fails)·P(cable fails) + P(RY5=0 "AND" RY6=0 | cable does not fail)·P(cable does not fail)
= P(RY13=0 | cable fails)·P(cable fails) + P(RY5=0 | cable does not fail)·P(RY6=0 | cable does not fail)·P(cable does not fail)
= P(RY13 fails)·P(cable fails) + P(RY5 line fails)·P(RY6 line fails)·P(cable does not fail)
= P(RY13 fails)·P(cable fails) + P(V1A fails "OR" RY1 fails "OR" RY5 fails)·P(V1B fails "OR" RY2 fails "OR" RY6 fails)·P(cable does not fail)

Similar is true for UIC2-V2 line.

SSS subsystem will fail if and only if both of these lines fail. If we simplify the notification by substituting

A_1 = *RY5 line fails,* $a_1=P(A_1)$
A_2 = *RY6 line fails,* $a_2=P(A_2)$
A_3 = *RY7 line fails,* $a_3=P(A_3)$
A_4 = *RY8 line fails,* $a_4=P(A_4)$
B_1 = *RY13 fails,* $b_1=P(B_1)$
B_2 = *RY14 fails,* $b_2=P(B_2)$
Y_1 = *UIC1 cable fails,* $y_1=P(Y_1)$
Y_2 = *UIC2 cable fails,* $y_2=P(Y_2)$ $(A_1,A_2,\ldots\in\{0,1\};\ a_1,a_2,\ldots\in[0,1])$

then the SSS conditional failure probability, as well as its point-wise unavailability can be presented as

$$Q_{SSS} = (a_1a_2(1-y_1)+b_1y_1)\cdot(a_3a_4(1-y_2)+b_2y_2) \tag{2.6}$$

Likewise, the realized structure function of the SSS subsystem might be presented as

$$\phi_{SSS} = (A_1A_2\overline{Y_1} \oplus B_1Y_1)\cdot(A_3A_4\overline{Y_2} \oplus B_2Y_2) \tag{2.7}$$

where operator "⊕" emphasizes the fact that its operands must be mutually exclusive, since $P(\phi_{SSS}=0)$ must be equal to Q_{SSS} for every realized stochastic process ϕ_{SSS}. However, for all practical purposes "⊕" can be safely replaced by "+" since

$$\begin{aligned} A_1A_2\overline{Y_1} \oplus B_1Y_1 &= (A_1A_2\overline{Y_1})(\overline{B_1Y_1}) + (\overline{A_1A_2\overline{Y_1}})(B_1Y_1) \\ &= A_1A_2\overline{Y_1}(\overline{B}_1+\overline{Y}_1) + (\overline{A}_1+\overline{A}_2+Y_1)B_1Y_1 \\ &= A_1A_2\overline{Y_1} + B_1Y_1 \end{aligned} \tag{2.8}$$

The expression (2.7) is given in the irreducible form with respect to the ("AND", "OR", "NOT") representation. It is therefore suitable for fault tree calculations. Nevertheless, it is not in the spirit of our modular presentation of the Safety Amp reliability chart, and it also hides the hierarchical structure of the fault tree. Therefore, we shall transform the structure function ϕ_{L1} to fulfill the requirements of modularity

$$\begin{aligned} \phi_{L1} &= A_1 A_2 \overline{Y}_1 + B_1 Y_1 = A_1 A_2 \overline{Y}_1 + B_1 Y_1 + A_1 A_2 B_1 Y_1 \overline{Y}_1 + Y_1 \overline{Y}_1 \\ &= (Y_1 + A_1 A_2 \overline{Y}_1)(\overline{Y}_1 + B_1 Y_1) = (Y_1 + A_1 A_2)(\overline{Y}_1 + B_1) \\ &= \phi_{V1} \cdot \phi_{UIC1} \end{aligned} \tag{2.9}$$

Hence, the modular disjunctive normal form yields

$$\begin{aligned} \phi_{SSS} &= \phi_{L1} \cdot \phi_{L2} = (\phi_{V1} \cdot \phi_{UIC1}) \cdot (\phi_{V2} \cdot \phi_{UIC2}) \\ &= (\phi_{UIC1} \cdot \phi_{UIC2}) \cdot (\phi_{V1} \cdot \phi_{V2}) = \phi_{UIC} \cdot \phi_{V} \end{aligned} \tag{2.10}$$

or in expanded form

$$\phi_{SSS} = [(\overline{Y}_1 + B_1)(\overline{Y}_2 + B_2)][(Y_1 + A_1 A_2)(Y_2 + A_3 A_4)] \tag{2.11}$$

Probability that the signal at the SSS output is equal to one in the above case is the SSS(1,1,0) multi-input availability denoted as $A_{SSS}(1,1,0)$. That is the conditional availability given that both input-signals from UIC units are available at all times, while the slow scram signal from Log-N Amplifier is not available. Two separate UIC inputs, (1,0,0) and (0,1,0), send the signal via two independent but symmetrical signal propagation path-sets, or threads, that are connected in parallel. Hence

$$\begin{aligned} &A_{SSS}(1,1,0) = A_{SSS}(1,0,0) + A_{SSS}(0,1,0) - A_{SSS}(1,0,0) \cdot A_{SSS}(0,1,0) \\ &= 2 A_{SSS}(1,0,0) - A_{SSS}(1,0,0)^2 \end{aligned} \tag{2.12}$$

and therefore

$$A_{SSS}(1,0,0) = 1 - \sqrt{1 - A_{SSS}(1,1,0)} \tag{2.13}$$

Also, for $0 \le x_1 \le 1$, $0 \le x_2 \le 1$, when the slow scram Log-N Amplifier input signal x_3 is available we have

$$A_{SSS}(x_1, x_2, 1) = 1 \tag{2.14}$$

However, the slow scram input signal from the Log-N Amplifier is optional, and it will not be considered further. The x_3 argument in $A(x_1, x_2, x_3)$, hereafter, will actually represent the *fast* scram input from the Log-N Amplifier. Then, for the whole Safety Amp, the fast scram conditional availability $A_{FS}(x_1, x_2, 1)$, given that a fast scram signal from Log-N Amplifier is available, is not a function of the remaining inputs, i.e.

$$A_{FS}(x_1, x_2, 1) = A_{FS}(x_1', x_2', 1) \tag{2.15}$$

2.4.2. Calculation of Availabilities by Minimal Cut Set Approximation Method

Minimal cut set method is based on a notion that there is an exact lower bound formula for the reliability of the system (see Chapter 3.2.1)

$$R(t) \ge 1 - [\Pr(F_1) + \Pr(F_2) + \ldots + \Pr(F_j)] \tag{2.16}$$

where for small values of failure probabilities $\Pr(F_i)$ the right-hand side becomes a handy approximation of the left-hand side because it is light on computation. This approximation is ideal for practical reliability assessment of fail-safe equipment for two more reasons:

1. $F_i(t)$ represents the event "all subsystems in the corresponding cut set have failed before time t", so that $\Pr(F_i)$ in case of the fail-safe equipment is indeed very small, and
2. the true reliability, as Equation (2.16) indicates, is always greater or equal to the one found by this method, so that the reliability is never overestimated.

However, for dependent events, A and B, the conditional probability $\Pr(A|B)$ might become as large as unity, even in cases when the probabilities $\Pr(A)$ and $\Pr(B)$ are arbitrarily small, so that the rare event approximation is no longer valid. The minimal cut set method consists of replacing the "greater or equal" sign with "equal" sign in Equation (2.16). The minimal cut set method, therefore, may not be a suitable approximation for dependent events.

Nevertheless, in the case of UIC subsystem, where the dependencies are caused by the event set partitioning, the minimal cut set method is still valid. One can even argue that it provides better results than expected, essentially because the cut set events are now being shifted towards a formation of a mutually exclusive set rather than a set with large intersections. To demonstrate the validity of the minimal cut set method we will calculate the reliability of the UIC1-V1 unit whose signal graph is presented in Figure [2-6]. All the cut sets are also minimal, and they are: $\{Y_1, Y_1^c\}$, $\{A_1, A_2, Y_1^c\}$, $\{B_1, Y_1\}$, $\{A_1, A_2, B_1\}$. The minimal cut set method yields for the probability of failure

$$\begin{aligned}\Pr(F_{UIC1-V1}) &= \Pr(Y_1\overline{Y_1}) + \Pr(A_1A_2\overline{Y_1}) + \Pr(B_1Y_1) + \Pr(A_1A_2B_1) \\ &= a_1a_2(1-y_1) + b_1y_1 + a_1a_2b_1\end{aligned} \tag{2.17}$$

which is slightly greater than the true failure probability. Namely, the additional, third term on the right-hand side is of the third order (of smallness), while the rest of the terms are of the second order.

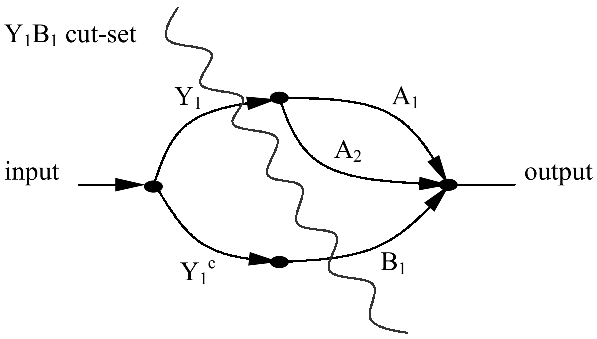


Figure 2-6. SSS-1 Reliability Graph and a Sample Cut Set

Note that the third term in the equation above would diminish in the exact minimal cut set expression for reliability that leads to the lower bound formula, which gives the true solution immediately, i.e.

$$\begin{aligned}\Pr(F_{UIC1-V1}) &= \Pr(Y_1\overline{Y_1} + A_1A_2\overline{Y_1} + B_1Y_1 + A_1A_2B_1) \\ &= \Pr(\varnothing + A_1A_2\overline{Y_1} + B_1Y_1 + A_1A_2B_1(Y_1 + \overline{Y_1})) \\ &= \Pr(A_1A_2\overline{Y_1}(\Omega + B_1Y_1) + B_1Y_1(\Omega + A_1A_2\overline{Y_1})) \\ &= \Pr(A_1A_2\overline{Y_1} + B_1Y_1) \\ &= \Pr(A_1A_2\overline{Y_1}) + \Pr(B_1Y_1) \\ &= a_1a_2(1-y_1) + b_1y_1\end{aligned} \tag{2.18}$$

2.5. Divider

Divider is a module with no active elements or relays. It consists solely of resistors: R49, R50, and CAS unit (see Figure 2-7). The purpose of the divider is to provide an appropriate bias for each pentode V[3-6] (see Figure 2.9). R49 is normally shunted (see Figure 2.7). If any of the following: RY1, RY2, RY3, RY4, or Log-N Amplifier activates (see Figure 1-7) the DCL line (see Figure 2.7) opens which is equivalent to "adding" R49 in series to R50. This results in the cut-off potentials being reached at the grids of V[3-6] which terminates the pentode currents. As mentioned earlier, R49 represents a bottleneck in the system. If it fails, the fast scram line fails too, since there are no input entries after this point. According to Table [2-1], 30% of all resistor failure modes can be associated to the failures resulting in open circuit. Next, as

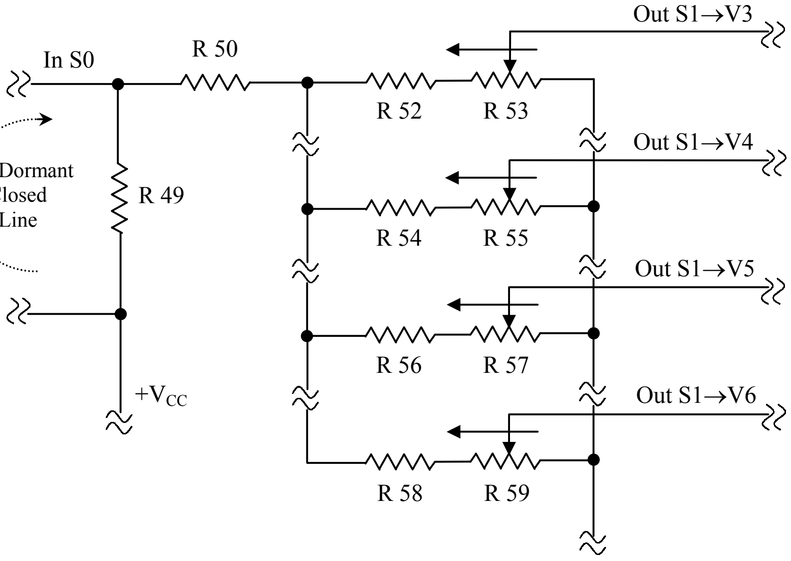


Figure 2-7. DIV Subsystem

Figure [2-7] indicates, only a parameter change resulting in a significant decrease of the resistance of the R49 will cause the divider failure. We will associate approximately half of the parameter changes from Table [2-1], or 30% of all failure modes to this case. Thus, from Figure [2-8], for ambient temperature of 30°C and operating/rated wattage ratio of 0.8, using the conversion factor of 4160 hr/yr we can calculate the divider failure rate as

$$\begin{aligned}\lambda_{DIV} &= (\text{fraction failure in open mode})\cdot(\text{failure rate per hour})\\ &\quad\cdot(\text{conversion factor: per hour} \rightarrow \text{per year})\\ &= (0.3)\cdot(0.07\cdot 10^{-2}\cdot 10^{-3}(hr^{-1}))\cdot(4160(hr/yr)) = 8.7\cdot 10^{-4}\,yr^{-1}\end{aligned} \tag{2.19}$$

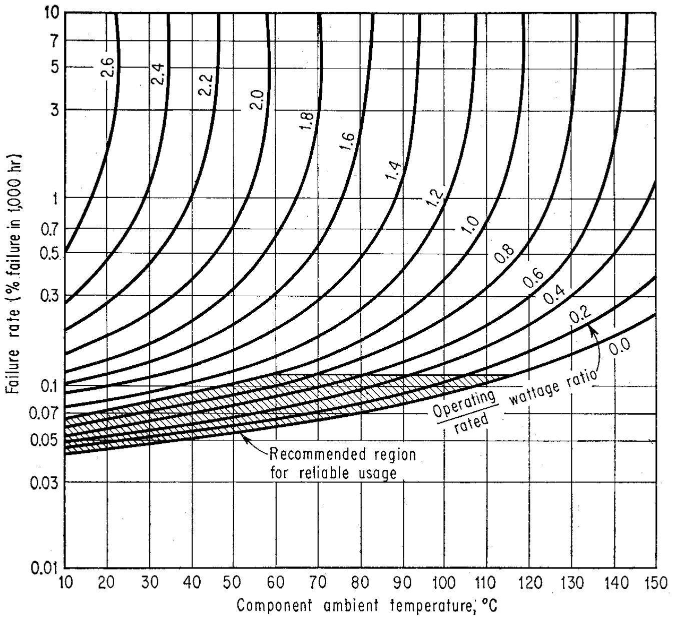


Figure 2-8. Predicted Failure Rates of Fixed Composition Resistors. From 'Resistance and Resistors', Charles L. Wellard, McGraw-Hill Inc., 1960.

Any failure of R49 will only be detected during a scram, since it is "hidden" otherwise by DCL (see Figure 2-7 and Figure 2-4). A failure of the resistor R50, which is not hidden, is much less likely to cause a failure of the divider during a scram. Namely, any parameter change of the resistor R50 will automatically be compensated by potentiometers R[53-59] during the process of calibration. In addition, since R49 is larger than R50 (15K vs. 12.5K), even if R50 is shorted, R49 should be able to deliver the scram signal through the divider by itself. Still, any parameter change of R49, caused by environmental conditions and aging, is expected to be accompanied by a similar parameter change of R50. The cumulative R49-R50 resistance drop, if the calibrations of the divider are omitted, may actually cause the divider to fail on demand, i.e. at the time of the scram.

	Failure modes	**Per cent proportions**
Resistors	Open-circuit	30
	Parameter change	70
Relays	No transfer	20
	Intermittent	70
	Short-circuit	10

Table 2-1. Electronic Systems Reliability. From 'Practical Reliability Engineering' by Patrick O'Connor, John Wiley & Sons Ltd., 1991.

The main standard database of failure rates for electronic components that is most commonly used for reliability assessment is US MIL-HDBK-217. However, the predictions from MIL-HDBK-217 method are a subject to a lot of criticism, and, for instance, NASA does not recommend using this method at all. The main disadvantage comes from the fact that experience shows that only 1 to 10 per cent of electronic failures is due to components failing owing to internal causes. Transient voltages are the main cause of failures of the components inside the Safety Amp. Since there are no semiconducting devices in it, except diodes, electrostatic discharge and radiation hardness are less likely to affect the reliability of the system.

Several environmental parameters can cause a resistor to fail by “external“ means. The most important parameters are as follows:

1. Moisture
2. Temperature
3. Vibration
4. Stress

The absorption of moisture during the years, for instance, may cause a shunting effect. A thermal shock, similarly, may cause a mechanical fracture of the resistor. For that reason, the operational conditions in the control room are maintained at level of maximum relative humidity of 60% and maximum temperature of 80^{o}F.

The divider is tested daily, so that the repair rate of the divider is

$$\mu_{DIV} = 2 day^{-1} = 5 \cdot 10^{2} yr^{-1} \tag{2.20}$$

2.6. FSP Subsystem

FSP subsystem has four parallel units that are connected to five shim rod magnets. FSP units V[3-6] are positioned at the end of the fast scram circuitry controlling the magnets MAG[1-5]. Unit V5 is connected to both MAG3 and MAG4, while other units are connected to one magnet each. Unit V3 is presented in Figure [2-9].

In terms of its output, FSP subsystem is described as “n out of m” system. It means that at least “n” units must *operate* in order to be $\phi=1$. Note that any series system is actually “m out of m”, and a parallel system is “1 out of m” system. For the system that has odd number of units, if $2n=m+1$ then the system is in “n out of m” mode in terms of both success and failure. For example, “2 out of 3” system can both be described as a) the system that operates if at least two (out of three) units operate, and b) the system that fails if at least two (out of three) units fail. Our system require at least two or at least three units (out of four) to operate/fail, depending on whether the unit V5 operates/fails. For example, both {V3, V5} and {V3, V4, V6} are minimal requirements for both operation and failure. Thus, just like the rod magnets, FSP is completely symmetrical in terms of success vs. failure representation, so that it can be decisively described as “2.5 out of 4” system. Recall that the rod-magnets form the “3 out of 5” system. The extension of $2n=m+1$ formula to even number of components is to be interpreted as follows: the minimum *expected* number of failures/successes in order for FSP system to fail/succeed if the FSP unit failures are equal and independent is 2.5.

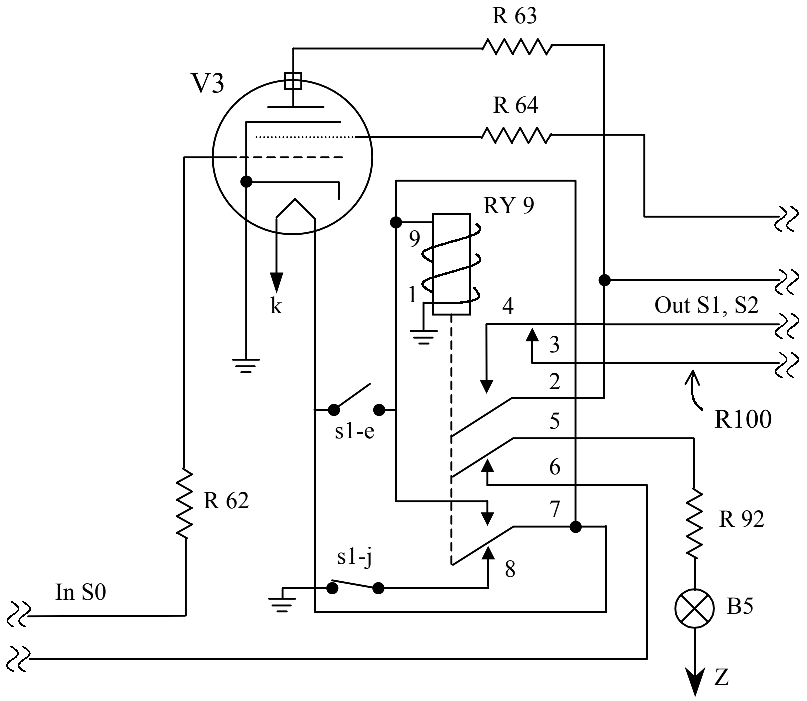


Figure 2-9. V3 (or FSP-1) Unit

Through the corresponding relays RY[9-12] energized by filament currents, the magnets were initially connected to a dummy load resistor R99. This feature was embedded to allow the replacement of a single tube whose filament had burned out during the reactor operation, since the electric current would still be able to flow through the corresponding magnet and a bypass circuit. If the second tube filament burns-out (while the first one has not yet been replaced) the electrical current through the first magnet would drop and as a result both first and second shim rods would be released. By removing R99, relay RY9 lost its purpose except for providing the signal B5. Whenever the filament of V[3-6] burns out the relay RY[9-12] deenergizes. Contacts 2 and 4 open, the circuit from the plate of the tube to the magnet is broken, and the corresponding rod(s) would be detached. This is also true for a plate-cathode or grid-cathode shorts. In addition, when RY[9-12] deenergizes contacts 5 and 6 close energizing the burn-out magnet lamp B[5-8]. The failure rate of the FSP[1-4] unit is at the order of magnitude of R62 failure, which gives λ_{FSP}~$1.5x10^{-3}yr^{-1}$. Regular inspection of the pentodes is performed semiannually, but the complete checkup of the FSP[1-4] unit is performed weekly via B[5-8], so that the repair rate yields μ_{FSP}~$10^{2}yr^{-1}$. If the filament in pentode V5 burns out both shim rod #3 and shim rod #4 are unavailable, and therefore if only one of the remaining rods, in addition, fails to drop for any reason, the scram can not be performed. The expected failure rate from this scenario dominates over the other ones, and hence determines the failure rate of the FSP subsystem itself.

2.7. Implementation of the Dual Filament Burn-Out Feature that has Acceptably Low Resulting Unavailability

As we already mentioned, pentodes V3, V4, V5, and V6 were initially supposed to control the currents of the magnets MAG1, MAG2, MAG3, and MAG4 respectively (see Figure 1-6). Through the corresponding relays RY9, RY10, RY11, and RY12 that are controlled by filament currents, the magnets were connected to dummy load resistor R99 forming the filament burn-out feature of the tubes. This feature allowed the replacement of the tube whose filament was burned-out while the reactor was still operating, since the current was still allowed to flow through the corresponding magnet.

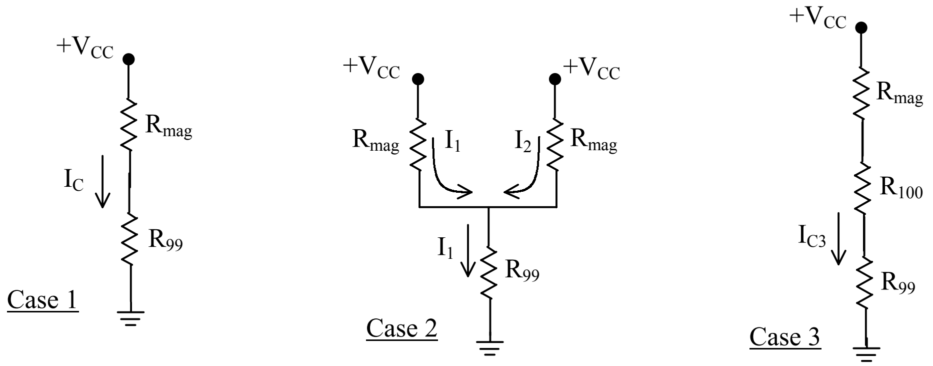
If the second tube filament was burned-out (and the first tube had not been replaced) the electrical current through the first magnet would drop and as a result both shim rods would be released. This additional feature was implemented because of the safety concerns. However, since there are five shim rods in the MNR, five magnets ought to be controlled by four pentodes. This resulted in magnets MAG3 and MAG4 being connected to a single pentode, V5. Since in this new arrangement a single defective pentode, V5, causes two shim rods to be inoperable, the dummy load resistor was being detached, so that V5 tube could not be replaced during operation. Nevertheless, none of the remaining tubes could be replaced during operation either. It is possible, however, to implement a solution that would preserve the functionality of the original design, with compromising the safety only in the case when V5 fails second. Figure 2-10 depicts the electric circuits for three cases of interest for further discussion: (1) single filament burn-out; (2) dual filament burn-out; and (3) equivalent single filament circuit for dual filament burn-out.

The calculation presented is rather straightforward, so that no additional comments are necessary. Calculation shows that the value of R_{100} equals R_{99}. Resistor R_{99} should be selected and installed in the circuit only after the characteristics of the magnets were once determined. Note that a shim rod magnet is not a part of the Safety Amplifier. The position of the resistor R100 is indicated in Figure 2-9.

The solution presented:

- is easy to implement

- is easy and safe to test (the removal of pentode V5 should cause rods #3 and #4 to drop, removal of V3, V4, or V6 alone should cause no change)
- is not affecting any other part of the equipment or its function
- will preserve the low overall unavailability of the Safety Amplifier with R99 attached



$$I_C = \frac{V_{CC}}{R_{mag} + R_{99}}$$

$$I_1 R_{mag} + I_3 R_{99} = V_{CC}$$
$$I_1 + I_2 = I_3$$
$$I_1 = I_2$$
$$\text{Hence, } I_1 = \frac{V_{CC}}{R_{mag} + 2R_{99}}$$

$$I_{C3} = \frac{V_{CC}}{R_{mag} + R_{100} + R_{99}}$$
$$\text{From condition } I_{C3} = I_1$$
$$\text{follows that } R_{100} = R_{99}$$

Figure 2-10. Equivalent Single Filament Circuit for Dual Filament Burn-out

2.8. Fast vs. Slow Scram: R49 Failure Case

The fast scram line in the Safety Amp has a reaction time of less than 10 millisecond, while the slow scram line has a reaction time of ~20 milliseconds. In the case when the reactor period is less than 4 seconds it is assumed that the fast scram line shall activate. The weak link of the Safety Amp, therefore, might become the divider (resistor R49) that separates MRY from FSP module, because it has no redundant parts. How often should R49 be tested depends not only on the possible failure rate of the unit, but also on the estimated severity of the consequence after the failure. The worst-case scenario taking into account the possible consequences is the following:

> The reactor is operating at *low* power. An inadvertent *increasing* reactivity insertion starts to change the power level. Long before the UIC chambers could activate, the period drops below 4 seconds. At exactly 4 seconds the Log-N amplifier activates, disconnecting through CN-6 the fast scram DCL line at the MRY output circuit. Because of the R49 failure, the potential at R49-R50 divider point is insufficient to overcome the necessary threshold of the pentode grids (of all of them). Thus, the magnets remain energized. Next, when the first UIC chamber power level reaches the first cut-off bias set by the corresponding SDA unit (adjustable via R19, R21, R41, and R43), both slow and fast scram lines activate. As the fast scram line is unavailable *after* the SDA subsystem, only the slow scram will persist. The period at this point, when the maximum allowable power is reached, is *significantly below* 4 seconds, and the Safety Amp still needs 20 milliseconds to release the rods.

Since the completion of the shutdown sequence requires the rods to be inserted in the core and not just released, we may question whether the role of the Safety Amp's inability to activate the fast scram circuitry in the possible core meltdown accident is essential regardless of the accident scenario:

> In time interval of 20 milliseconds required for slow scram the rod would drop
>
> $$\Delta h = a\frac{t^2}{2} = 4.9\frac{m}{s^2}\cdot\frac{(0.02s)^2}{2} = 0.00098m \qquad (2.21)$$
>
> i.e. less than one millimeter. The effective acceleration of 4.9[m/s^2] in Equation (2.21) is used as provided by "MNR Technical Report TR 1998-11, Revision 2, 1999". Given that the 5 millisecond fast scram failed, the UIC signal time delay of t_{del} = 20ms – 5ms = 15ms would have negligible effect on the combined shutdown delay time, i.e. the time from the UIC trip to the complete insertion of the absorbing rods. Nevertheless, after only ~50ms (see Butler [1995]), the inserted negative reactivity starts to affect the core kinetics significantly.

For the worst-case scenario mentioned earlier, the fast scram action is essential. This scenario assumes that a *small positive feedback* or an external *reactivity increase* on a *small initial positive reactivity* insertion under *low power* is in effect, which is a credible assumption. In this case the unavailability of the Log-N amplifier input can delay the time of the rod release for much more than 15ms since the reactor period would decrease slowly at the beginning, after breaking the 4 second limit while still under low power. The total response time delay caused can be several seconds, which is the time that is comparable to the 0.5 seconds gravitational delay, or full length rod drop time, and much more than the total delay time to rod release of 50ms. According to the scenario given above, we may conclude that the testing time interval for R49 should become more frequent only during the periods when the reactor is intended to run mainly at low power (100kW), or while a refueling is performed (zero power). The following simplified point kinetics model illustrates the point:

An inadvertent positive reactivity insertion is characterized by the multiplication factor

$$k(t) = k(0) + \frac{k'(t)|_{t=0}}{1!}(t-0) + \ldots \cong k(0) + c_1 t \cong 1 + \rho(0) + c_1 t \qquad (2.22)$$

where $c_1>0$ is some constant. If we shift the time-scale so that the reactor becomes prompt-critical at t=0 (i.e. $\rho(0)=\beta$), the reactor period for t>0 is

$$T(t) = \frac{\Lambda}{k(t) - 1 - \beta} = \frac{\Lambda}{c_1 t + (\rho(0) - \beta)} = \frac{\Lambda}{c_1 t} \qquad (t > 0) \qquad (2.23)$$

The power level scram, denoted further by P_{trip}, will occur at 125% of full power and can be considered constant. If the reactor is initially at power $P_0>0$, then

$$P_0 e^{\int_0^{t_{trip}} \frac{d\tau}{T(\tau)}} = P_0 e^{\frac{c_1 t_{trip}^2}{2\Lambda}} = P_0 e^{\frac{\Lambda}{2 c_1 T^2(t_{trip})}} = P_{trip} \qquad (2.24)$$

and hence the reactor period at the time of the high power trip is

$$T(t_{trip}) = \left(2\frac{c_1}{\Lambda}\ln\frac{P_{trip}}{P_0}\right)^{-\frac{1}{2}} = (c_2 - c_3 \ln P_0)^{-\frac{1}{2}} \qquad (2.25)$$

where we introduced new constants c_2 and c_3. Equation (2.25) shows that the reactor period at the time of the high power trip, $T(t_{trip})$, decreases as the power P_0

at which the reactor became prompt-critical decreases. The sensitivity of the reactor period $T(t_{trip})$ to the initial power level can be very high if the initial power is low. Namely, if $P_0 << P_{trip}$ then

$$\frac{\delta T(t_{trip})}{\delta P_0} \approx \frac{\frac{1}{2} c_2^{-\frac{3}{2}} c_3}{P_0} = \frac{c_4}{P_0} \tag{2.26}$$

On January 1994 a fuelling incident occurred in the MNR. This incident happened when the input to the Log-N Amplifier was disconnected from the Safety Amplifier during the fuelling. Regardless of the different initiator, this event and the R49 failure propagates through the Safety Amplifier alike, resulting in similar consequences.

Example (January 1994 fuelling incident):

$P_{init} = 13mW$
$P_{trip} = 2.5MW$
$\Delta k = 0.025$ inserted over 20 seconds
$k_{init} = 0.983$
$k_{final} = 1.008$
$\Lambda = 51\mu s$

Since k_{final} is provided, we can find $T(t_{trip})$ by using Equation (2.23), as

$$T(t_{trip}) = \frac{\Lambda}{k(t_{trip}) - 1 - \beta} = \frac{51 \times 10^{-6}}{1.008 - 1 - 0.007} = 51\, ms$$

As mentioned earlier, the total delay time to significant rod release is estimated at ~50ms, so that the lower bound of the maximum power achieved during the incident is

$$P_{\max} = P_{trip} e^{\frac{50ms}{T(t_{trip})}} = 6.66MW$$

which is close to the lower bound value of 6.32MW provided by Butler [1994]. Using Equation (2.24), we can find the power at which the reactor became prompt-critical

$$\begin{aligned} P_0 &= P_{trip} \exp\left[\frac{-\Lambda}{2(\Delta k/\Delta t)T^2(t_{trip})}\right] \\ &= 2.5\times 10^6 \exp\left[\frac{-51\times 10^{-6}}{2\times(0.025/20)\times 51^2\times 10^{-6}}\right] = 981W \end{aligned}$$

This relatively high power-level was achieved due to the initial power of the core prior to incident of 13mW. It can be noted that, had the incident occurred with a fresh core (theoretically at arbitrarily low power), according to the equations above, the reactor period at the time of the high power trip, $T(t_{trip})$, would be arbitrarily small. Thus, the maximum power, P_{max}, would become unbounded. In this case the fast negative feedback effects (e.g. the Doppler broadening) would limit the power rise. Recall that the feedback effects are proportional to the power, and not to the period. As we emphasized several times, the period can become rather small while the power is still low, thus causing a very rapid power excursion rate while the feedback mechanisms are not yet employed. Fortunately, because of the process of spontaneous fission, arbitrarily low powers cannot be achieved and thus the feedback effects may not be crucial. A credible worst-case scenario includes fresh low-enriched uranium core with the speed of the fuel insertion of ~4c_1. Equation (2.25) yields $T(t_{trip})\approx$20ms with an estimated peak power of ~50MW, or less. In case of R49 failure, the peak power can reach ~80MW, since the fast-scram line is disconnected from the UIC input, which increases the response delay time for ~10ms. This power overshoot increases the water pressure to the aluminum shields of the absorber rods, and may eventually bend the shields closing the passage to the rods. In the period from October, 1954 to June 1956 the U.S. Atomic Energy Commission conducted a series of safety experiments that involved five different reactor classes, including MNR class. The experiments were conducted in order to determine whether a significant core damage would occur in the case of a severe power excursion with shutdown rods removed (see Nyer [1956]). The experiments that included ramp-rate studies showed that such a damage is highly unlikely. Some theoretical models (Fush-Hansen model, Bethe-Tait model) are designed to deal with the similar type of situation and for some core configurations, reactor types, and accident scenarios, predict possible core blow-apart or partial meltdown (see Bell, Glastone [1970]).

For analyzing the process during the time interval before the prompt-critical stage, we need to include delayed precursors. If we shift the time-scale again, so that $\rho(0) = 0$, then the one-precursor group model for Equation (2.22) leads to the differential equation

$$\frac{d^2P}{dt^2} + \left(\lambda - \frac{\rho - \beta}{\Lambda}\right)\frac{dP}{dt} = \left(\frac{\lambda\rho}{\Lambda} + \frac{c_1}{\Lambda}\right)P \tag{2.27}$$

which has the exact solution (see Lewins, [1978])

$$P(t) = A_1 I_1(t) + A_2 I_2(t) \tag{2.28}$$

where

$$I_1(t) = \int_{-\infty}^{\lambda} g(\xi, t)d\xi, \quad I_2(t) = \int_{-\lambda}^{\infty} g(\xi, t)d\xi \tag{2.29}$$

and

$$g(\xi,t)=(\xi+\lambda)^{\frac{\beta}{c_1}}\exp\left(-\frac{\Lambda\xi^2}{2c_1}-\frac{\beta\xi}{c_1}+\xi t\right) \tag{2.30}$$

The two initial conditions for our system are

$$P(0)=13mW, \quad (dP/dt)|_{t=0}=0 \tag{2.31}$$

It should be noted that the ramp insertion approximation (Equation (2.22)), appropriate in the prompt-critical region (ρ>β), is not as nearly as good in the sub-prompt-critical region (ρ<β). If we rewrite Equation (2.22) with the third term added

$$k(t)=k(0)+\frac{k'(t)|_{t=0}}{1!}(t-0)+\frac{k''(t)|_{t=0}}{2!}(t-0)^2+\ldots \tag{2.32}$$

it is easily seen that this term becomes more important as *t* increases. The time interval covered in the sub-prompt-critical region is approximately 400 times larger than the time covered in the prompt-critical region. This “boosts up” the third term in Equation (2.32) 400 times in terms of its importance (i.e. the ratio of the third and the second term) for sub-prompt-critical vs. prompt-critical region. Thus, we may need to test the robustness of the solution provided by Equations (2.28-31) against the variation of c_1 in Equation (2.27) first.

For a complete analysis of the January 1994 fuelling incident see Garland [1997], Butler [1994], or Basha [1997].