Introduction

The McMaster Nuclear Reactor (MNR) is a five-megawatt swimming pool type research reactor located at McMaster University. Since McMaster University is located in a highly populated area, the city of Hamilton, MNR imposes a concern from the public safety standpoint. The atomic regulatory agency (AECB) requires that the MNR safety report be periodically updated for the purposes of the operating license renewal. The Safety Amplifier is studied herein since it is a key component in the reactor's safety system. Hence, it is an important element in the safety report.

MNR is a light-water moderated, heterogeneous, solid fuel reactor in which the water is also used for cooling and shielding. The reactor currently operates at a maximum thermal power of two megawatts. Control of the reactor is accomplished by the insertion or removal of neutron-absorbing rods suspended from control drives mounted on the reactor core bridge. Five shim-safety rods are attached to the drive mechanism via an aluminum tube and an electromagnet. If the scram conditions are met, the electromagnets are de-energized, and as a result, the safety rods would drop into the core performing an immediate shutdown. No alternative scram mechanism, such as boron injection for example, is present. Current to energize the electromagnets is obtained from the Safety Amplifier.

The Safety Amplifier itself receives the scram signal from three different input channels. Two of these channels are attached to two Uncompensated Ionizing Chambers

(UIC) located in the reactor core - each channel to one chamber. The purpose of each UIC chamber is to monitor the power level in the core. An appropriate amount of the bypass current from a UIC chamber can generate the scram signal that will propagate through the Safety Amplifier. Once the signal passes the Safety Amplifier's triodes it becomes highly non-linear and can be presented by one out of two values: 'no-scram', and 'scram'. The UIC threshold current is adjustable by potentiometers. Normally, this threshold is reached when the core power exceeds 125% of its maximum operating power. Although one chamber is sufficient, two chambers are used to increase the probability that at least one of them is operational at any given time. The third input channel to the Safety Amplifier is connected to the Log-N Amplifier. Log-N Amplifier is an electronic device that generates a scram signal if the reactor period is too short. In this case, prompt action is necessary, since the power is rising too fast and accelerates. At the time when it reaches the Safety Amplifier, the input signal from the Log-N Amplifier is already discretized and amplified. Therefore, unlike the signal from the UIC chamber, it does not need to go through the triodes. The Log-N Amplifier input channel of the Safety Amplifier is positioned in such a way that the scram signal, which propagates only through one part of the Safety Amplifier is able to reach the rod bank in a shortest time possible. This channel is called "the fast-scram line". The signals from the UIC chambers, on the other hand, are first split in two, and then, in the form of parallel threads, transferred through the fast-scram line and another channel called "the slow-scram line". The slow-scram line alone will also activate if the power supply to the Safety Amplifier fails. Nevertheless, the power supply failure does not initiate a genuine trip signal because it is not correlated to either the core power or the core power-rate. However, since the power supply failure may lead to an illegal state of operation of the Safety Amplifier, and can indicate a more general power failure that may affect the rest of the MNR, it should be followed by the reactor shutdown. Once in an illegal state, the Safety Amplifier can not go back to the operational state without the assistance of an operator.

The rationale behind the ability of the Safety Amplifier to shutdown the reactor after receiving signals not correlated to the power in the core is twofold. Firstly, some signals may indicate a trouble in vital MNR functions that are likely to affect the core integrity during an event sequence that may or may not include an increase in core power. These scram signals are valid event tree initiators. Some examples include low primary flow, low pool level, or flapper open. Secondly, as a safety device, the Safety Amplifier is capable of detecting some of its own failures. This adds a whole new dimension to the reliability analysis because the signal flow graph is not a constant anymore. In the approach we used, these internal failures are not considered to be initiators. All scram signals except for those from the UIC chambers, the Log-N Amplifier, and internal Safety Amplifier failures are connected in series to the magnet power supply. If any one of these signals eventuate, the magnet power supply will be disconnected from the Safety Amplifier. This will cut off the current to the rod-magnets. Although the rod-magnets are not a part of the Safety Amplifier, the mission of the Safety Amplifier does not end here. It is also partially responsible for a rod drop because it checks whether the rods are attached to the magnets or not. *The Safety Amplifier cannot fail with regard to these* *inputs*. For that reason, the safety analysis of the Safety Amplifier will only be concerned with cases of an inadvertent excursion of the power in the core.

To formulate the operating conditions of the Safety Amplifier with respect to the MNR as a whole, we need the following events (A-H):

1) Safety Amplifier is operational with respect to:
    A) UIC-1 input
    B) UIC-2 input
    C) Log-N Amplifier input
2) The following input device to the Safety Amplifier is operating:
    D) UIC-1
    E) UIC-2
    F) Log-N Amplifier
3) The following condition is met:
    G) High neutron flux is present in the core (current power exceeds 125% of the operating power)
    H) Excessively fast rate of increase of neutron flux has been achieved (reactor period less than 4 seconds).

The Safety Amplifier will de-energize the magnets if the condition presented by the Boolean expression (AD+BE)G+CFH is satisfied. In the case of a power excursion the converse is also true. This logical expression allows us to construct a simple fault tree that can be used in the event tree in which the increased energy production is an initiating event.

Each of the conditions G and H can initiate the sequence of events that may lead to the core meltdown, and therefore to the significant release of radiation to the environment. In addition, any potential core meltdown caused by the loss of regulation must at one point reach the condition G, and is more than likely to reach the condition H. Core meltdowns related to coolant problems (e.g. loss of coolant inventory, some cases of flow impairment, etc.) are not included in this scheme, as they would initiate the scram signal through the magnet power supply. If the conditions D, E, and F are satisfied, then, regardless of the accident scenario, the Safety Amplifier remains solely responsible for transferring the scram signal to the rod magnets. The reliable operation of the Safety Amplifier is therefore essential in order to keep the probability rate of the core-meltdown caused by the loss of neutron flux regulation below the prescribed limit. This limit is currently set to $\omega=10^{-6}$ accidents per reactor-year, which includes all types of failure to trip (and possible subsequent core damage). As the above discussion may suggest, the probability rate of the core damage caused by the loss of regulation is considered to be proportional to the fraction of time during which the Safety Amplifier is unable to respond to a scram signal. This relative time fraction is called the unavailability of the Safety Amplifier. Having in mind that there are two inputs that represent two independent variables (despite the fact that they are correlated), we may note that two respective availabilities ought to be calculated – one for the power (UIC), and another for its first derivative (Log-N).

The goal of this investigation can thus be stated in one sentence: calculate the unavailability of the McMaster Nuclear Reactor shutdown control unit, the Safety

Amplifier, and show whether or not this unavailability is in agreement with the acceptable limits for reactor accidents. However, the methods to achieve this goal are by no means as simple as the goal itself.

If not explicitly stated otherwise we will always assume that the reliability parameters between the Safety Amplifier and any other part of the MNR system are statistically independent. By assuming that events are independent we automatically have excluded common mode failures. However, common mode failures play an important role in virtually any *system* failure. As experience shows, common mode failures can increase the failure probability of a system by several orders of magnitude. We do not intend to disregard this fact. It should be inferred that, in order to complete the work, a separate analysis of common mode failures should be performed. None of the major common mode failures will be analyzed herein. These events should be accounted for when the whole system is analyzed, and when correlation between events, i.e. their consequences, is explicitly taken into account. Major common mode failures include earthquakes, fires, sabotages, and other events that would likely produce significant physical damage to the rest of the system, including damage to the reactor core itself.

Some insufficiencies of the traditional reliability theory are examined in Chapter One. Most serious of them includes a multi-input feature. Namely, as we mentioned before, the Safety Amplifier has more than one input (or initiator) that cannot be easily analyzed by the theory at hand. Another problem includes the existence of mutually exclusive signal propagation paths throughout the system that, again, is not encompassed by the traditional theory. We will discuss these and related issues in more detail in subsequent chapters.

We will keep the framework of our analysis as simple as possible. This means that we do not intend to calculate the reliability parameters precisely, but only within some established bounds of confidence. Using a conservative approach will be our major guideline. For instance, it is desirable that the true unavailability of the Safety Amplifier be smaller than the unavailability calculated. For this reason, the cut-set analysis methodology was chosen since it matches the conservative approach. It is also true that the calculated unavailability will hence be biased, and we will, in fact, calculate this bias. Only the reliability data with established bounds of confidence will be used. In particular, the component failure data were adopted from IAEA technical documents or more reliable sources when available.

Chapter One is dedicated to the Safety Amplifier reliability model design. The Safety Amplifier is decomposed into modules most appropriate for purposes of following the information flow signal throughout the device. An abstract component is defined which was used later on to depict the Safety Amplifier reliability diagram. In Chapter Two the Safety Amplifier subsystems are studied in greater detail. In Chapter Three the uncertainty propagation, confidence, sensitivity, and importance of the fault trees have been examined. This chapter also contains some basic introduction to the reliability theory, such as the minimal cut set method and fault tree analysis. In Chapter Four we will give a closer look to the analysis of the common cause failures (CCF). We will explain the significance of the CCF calculation together with the enormous difficulties that this calculation imposes – both from the probabilistic and the statistical point of view. Next, the importance of the failures on demand in redundant systems will be discussed. Finally, a simple approximation of CCF used in the fault tree calculations, called Beta Factor Method, is explained. Next, treated as a system of moderate complexity, the Safety Amplifier is analyzed in Chapter Five utilizing a fault tree technique. This technique is recommended by IAEA and widely adopted by nuclear engineers as the main route for performing probabilistic risk assessment [McCormick, 1981]. The basic events, i.e. those that represent the leaves of the fault tree, have been determined. The Safety Amplifier fault tree was developed and reliability parameters of the root event were calculated using a commercial software application 'FaultTree+' [Isograph Ltd., 1995]. The main reliability parameters of the root event to be calculated are unavailability, failure frequency, and the corresponding uncertainties.

In particular, this work is a part of the undergoing probabilistic safety analysis of the McMaster Nuclear Reactor. Although the measure of risk imposed to the general public will not be established herein, as that requires a consequence analysis, the resulting importance parameters can readily be used for improving the safety design or performance of the facility. Furthermore, the methodology used in this thesis was kept as broad as possible, so that with minimal changes it could be adopted to cover the estimation of occurrences of other natural or manmade events that are rare but have catastrophic or otherwise important consequences. These events may not necessarily be related to the area of nuclear engineering. Some examples may include complex technologies such as aviation (e.g. airplane crashes), or chemical process plants, where highly toxic chemicals may be released. One such accident was the Bhopal chemical-plant accident of 1984. Accidents in national defense, involving nuclear weapons, for example, would be even worse, probably causing a nationwide catastrophe.

Finally, the work herein can be extended in many ways, some of which are hinted at above. It barely scratches the surface of the complexity of the probabilistic theory of safety, a theory that is presumably yet to come.

In order to prevent the volume of the thesis to exceed all reasonable limits, neither the basic reliability theory nor the principle of the MNR Safety Amplifier operation is discussed in detail in the chapters to follow. An interested reader is urged to consult the documents referenced at the end of the thesis, or other suitable papers, in order to become fully familiar with the terminology used herein. Some previous knowledge of the reliability theory, although not necessary, is beneficial for further reading.