

THE IMPACT OF UNCERTAINTIES ON THE PERFORMANCE OF PASSIVE SYSTEMS

REACTOR SAFETY

KEYWORDS: *passive systems, reliability, gas-cooled fast reactor*

LORENZO P. PAGANI, GEORGE E. APOSTOLAKIS,* and PAVEL HEJZLAR
*Massachusetts Institute of Technology, Nuclear Engineering Department
Cambridge, Massachusetts 02139-4307*

Received June 14, 2004

Accepted for Publication August 3, 2004

Passive safety systems are commonly considered to be more reliable than active systems. The lack of mechanical moving parts or other active components drastically reduces the probabilities of hardware failure. For passive systems, it is necessary to introduce the concept of functional failure, i.e., the possibility that the loads will exceed the capacity in a reliability physics framework. In this paper we analyze the passive cooling of a gas-cooled fast reactor, and we use an importance-sampling Monte Carlo technique to propagate the epistemic uncertainties and to calculate the probabilities of functional failures. The results show that functional failures are an important contributor to the overall failure probability of the system and, therefore, should be included in probabilistic risk assessments. A comparison with an alternative active design is considered also. The results show that the active system can have, for this particular application, better reliability than the passive one.

I. INTRODUCTION

The nuclear industry has relied on the concept of defense in depth (DID) and safety margins to deal with the uncertainties associated with the design and operation of nuclear facilities.¹ This approach uses redundancy, diversity, and large safety margins to ensure that the probability of undesired events is small. The development of probabilistic risk assessments (PRAs) has improved our understanding of the safety of nuclear facilities by quantifying the risk due to hardware failures, human actions, and natural phenomena and by determining its

main contributors. Through the use of PRAs, it has been possible to identify accident sequences and components important to safety. Although the risk impact of redundancy has been explicitly modeled and quantified, the role of safety margins is not taken into account.

Safety margins are used to deal with uncertainties related to the concept of functional failures. A functional failure is defined as the inability of a system to perform its mission due to deviations from its expected behavior.² Within a reliability physics framework,³ a functional failure occurs whenever the applied "load" exceeds the component "capacity." Sufficient safety margins are, therefore, defined as the margins that guarantee a negligible probability of functional failure. The role of functional failures is simplified in PRA practice by assuming that their probability is equal to zero whenever deterministic acceptance criteria are met and is equal to unity otherwise. In current-generation reactors, which rely on active safety systems, the impact of this simplification is minimal, because existing margins are indeed sufficient to guarantee negligible probabilities of functional failures.

In view of the important role that passive systems may play in future reactors, the quantification of functional failures and their explicit inclusion in PRAs may be necessary. Concerns arise because of the uncertainties involved in the operation of passive systems. In addition, the quantification of functional failures may help in addressing the concerns that have been raised regarding margin erosion in current reactors due to power uprates or license renewal.⁴

In this paper, we analyze a case study involving natural convection cooling in a gas-cooled fast reactor (GFR) under a post-loss-of-coolant accident (LOCA) condition to quantify the role of functional failures. First, we highlight the difference between hardware and functional failures. The model used in the case study is presented in Sec. III, and the numerical results are shown in Sec. IV. These results are obtained by propagating the uncertainties through Monte Carlo methods with importance

*E-mail: apostola@mit.edu

sampling. We provide a discussion of the results in Sec. V, highlighting some characteristics of functional failures. Conclusions are offered in Sec. VI.

II. HARDWARE FAILURES AND FUNCTIONAL FAILURES

Recent analyses by Burgazzi^{2,5} and Jafari et al.⁶ have shown that particular care has to be given to the quantification of uncertainties and their role when dealing with passive safety systems.

In passive systems, because of their design, mechanical failures, e.g., pipe failures, are very unlikely to happen. Thus, the probability of failure of the overall system calculated as a function of hardware failures of its components is very low. However, the uncertainties involved are usually larger than in active components, and it is possible that the loads will exceed the capacities, even if margins are present, thus causing the system to fail. The latter type of failure has been referred to by Burgazzi² as *functional failure*.

To clarify the distinction between a functional failure and a traditional hardware failure, let us define the two concepts considering the example of a pump whose mission is to provide a specified flow rate. The pump is supposed to work in a given environment, defined by the temperature and pressure of the fluid. Hardware failure of a component or system is said to occur when one or more subcomponents physically breaks, disabling the component. In the example of the pump, a mechanical failure of the rotor shaft would be classified as hardware failure. This type of failure^a is included explicitly in the PRA.

If there are no uncertainties regarding the model describing the system and the numerical values of its important parameters, then only hardware failures have to be considered. The only epistemic uncertainties in such a case are those associated with the numerical values of failure rates.⁷ However, because of the existence of these uncertainties, it is possible that even if no hardware failure occurs, the system may not be able to accomplish its mission. In this case, a functional failure is said to have occurred. In the example of the pump, a failure to accomplish the mission due to uncertainties in the temperature and pressure of the fluid would be classified as a functional failure.

III. THE CASE STUDY

III.A. System Description and Operating Conditions

The reactor used in the case study is a 600-MW GFR cooled by helium flowing through separate channels in a silicon carbide matrix core. This design has been the

^aWhile we focus only on hardware failure throughout the paper, human action failures are also to be considered in this category.

subject of study in the past several years at the Massachusetts Institute of Technology within the framework of the I-NERI project Development of GEN IV Advanced Gas-Cooled Reactors with Hardened/Fast Neutron Spectrum. The studies by Okano et al.,⁸ Eapen et al.,⁹ and Williams et al.¹⁰ have confirmed the possibility of using natural circulation to remove the decay heat in case of an accident. A number of identical loops have been considered in the analysis. In addition to the passive system, which operates in natural convection at 1.65 MPa, an active version with blowers providing the necessary flow rate and operating at atmospheric pressure has also been considered.

In case of a LOCA, long-term heat removal is ensured by forced (in the active system) or natural (in the passive system) circulation in each loop. To achieve the high pressure necessary for natural circulation, the primary system is contained in a guard containment designed to maintain the necessary pressure.

A GFR decay heat removal configuration is shown schematically in Fig. 1, where only one loop out of N is shown. The hot gas (helium) from the reactor core proceeds through a top reflector and chimney to the inner coaxial duct and then upward to the hot plenum of the emergency cooling system (ECS) heat exchanger (HX), where it transfers heat to naturally circulating water on the secondary side. Cold gas from the HX flows down through a check valve to the outer coaxial duct, which brings it back to the reactor vessel, where it proceeds through the downcomer back to the core, as indicated by arrows. A check valve is installed (item 15 in the figure) to prevent backflow through the ECS HX during normal operation. A blower is mounted in the downcomer below the HX to provide cooling during shutdown since the safety grade ECS HX is used for both shutdown cooling and post-LOCA heat removal. The blower can also be used for forced circulation in post-LOCA scenarios but is not credited for passive decay heat removal.

To achieve a sufficient decay heat removal rate by natural circulation, it is necessary to maintain an elevated pressure even after the LOCA. This is accomplished by a guard containment, which surrounds the reactor vessel and power conversion unit and holds the pressure at a level that is reached after the depressurization of the system.

The average core power to be removed is assumed to be 12 MW, equivalent to 2% of full reactor power (600 MW). Thus, significant reduction in decay heat would have to happen before reaching this scenario.^b To guarantee natural circulation cooling at this power level, a pressure of 1650 kPa is required.^c

^bThis reduction will be due to heat storage in core materials, helium from accumulators, and a short-time cooling safety system, before natural circulation can be established.

^cDuring normal operations, there is atmospheric pressure inside the guard containment.

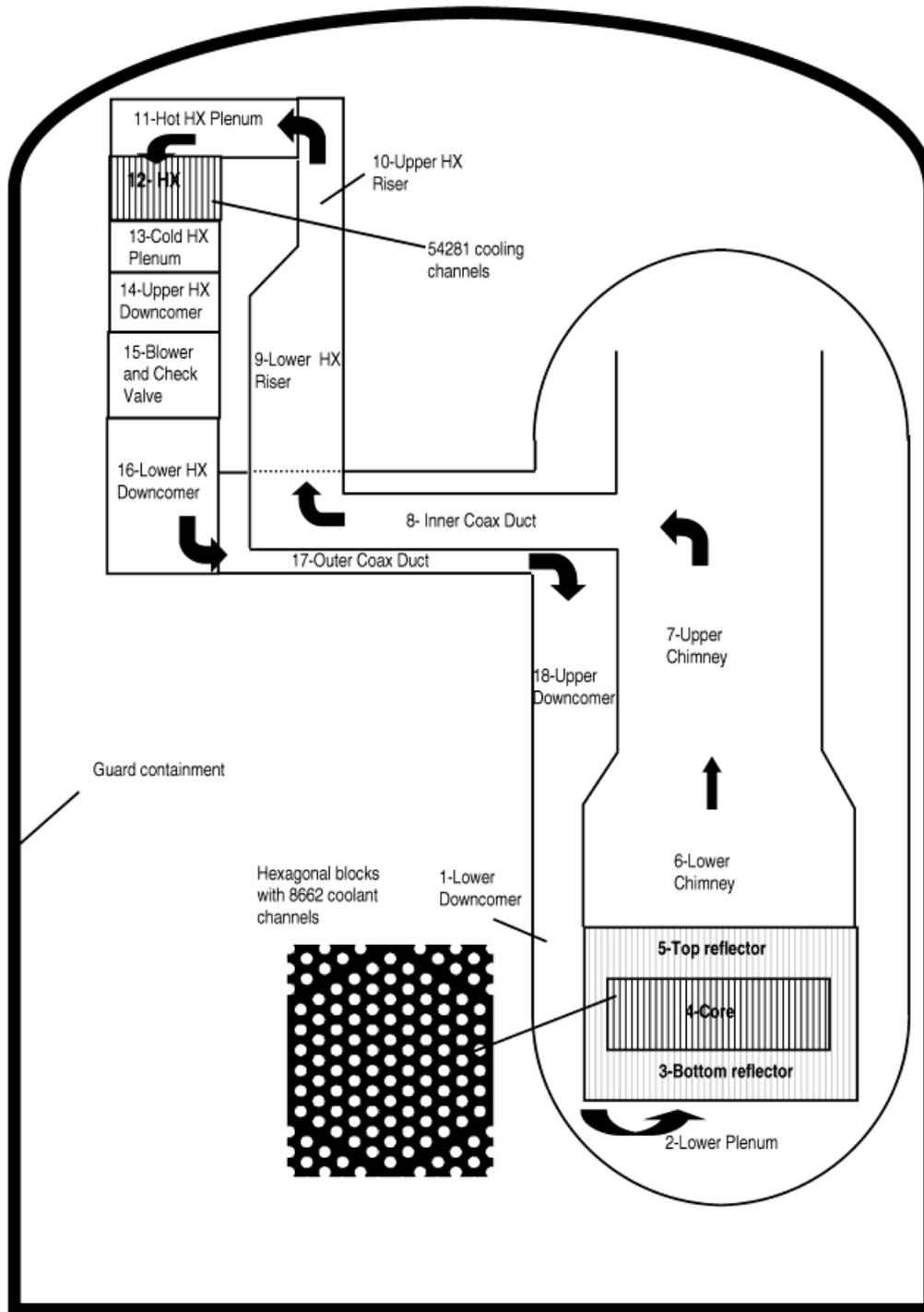


Fig. 1. Schematic of GFR decay heat removal loop.

The multiple loops are identical in geometry and characteristics. The secondary side of the cooler is assumed to have a constant wall temperature of 90°C.

The design is dimensioned so that only two loops will be sufficient to cool the core (50% loops). The

loop dimensions have been selected so that the design satisfies the requirements to keep the calculated outlet temperature below 1200°C in the hot channel and 850°C in the average channel. The geometry of the design is reported in Table I, where the section numbers in the

TABLE I
Geometry of the System

Section	Hydraulic Diameter (m)	Flow Area (m ²)	Length (m)	Height (m)	K Loss Coefficient	Roughness (m)
1	0.6	7.2571	7.7	-5.3	1	4.50E-05 ^a
2	7.4	43.008	1	0.5	0	4.50E-05
3	0.0145	1.65E-04	1	1	0.5	1.00E-05
4	0.0145	1.65E-04	1.7	1.7	0.25	1.00E-05
5	0.0145	1.65E-04	1	1	1	1.00E-05
6	7.4	4.30E+01	3	3	0	4.50E-05
7 ^b	5.4	2.29E+01	6	6	0.1	4.50E-05
8	0.8	5.03E-01	4	0	1.23	4.50E-05
9	1	2.24E+00	2	2	0	4.50E-05
10	1.6364	5.40E+00	1.5	1.5	0.1	4.50E-05
11	0.15	1.35E+00	1.25	-0.5	0.23	4.50E-05
12	0.003055	9.81E-06	0.3	-0.3	1.23	1.00E-05
13	0.15	1.35E+00	1.25	-0.2	1	4.50E-05
14	1.526	8.20E+00	1	-1	0	4.50E-05
15	1	3.76E+00	3	-3	13.23	4.50E-05
16	1.526	8.20E+00	1	-1	0	4.50E-05
17	0.25	3.63E-01	3	0	1	4.50E-05
18	2.0253	2.29E+00	5.4	-5.4	0.5	4.50E-05

^aRead as 4.50×10^{-5} .

^bThe loop geometry begins at section 7 and ends at section 18.

first column correspond to the flow path numbers on Fig. 1.

It is important to note that the subject of our analysis will be the quasi-steady-state natural convection cooling (or active if blowers are used) that takes place after the LOCA transient has occurred. The measures we calculate in the following sections refer to this steady-state period and are conditional on the successful inception of natural convection. Therefore, the analysis does not take into account the failure probability of not starting natural convection or the probability of failure to build up and maintain a high pressure level in the guard containment.

III.B. Thermal-Hydraulic Model

To simulate the steady-state behavior of the system, a thermal-hydraulic code developed at MIT (Ref. 10) has been used. This code treats all multiple loops as identical. The whole loop is subdivided in sections that are defined by their length, hydraulic diameter, area, height, form loss coefficient, and roughness. The heater (reactor core) and cooler (heat exchanger) sections have been further subdivided into separate nodes to calculate the temperature and flow gradient with sufficient detail (40 nodes have been used for this analysis). Both the average and hot channel are modeled in the core so that the increase in temperature in the hot channel due to the radial peaking factor can be calculated.

To obtain a steady-state solution, the code balances the pressure losses around the loop so that friction and form losses are compensated by the buoyancy term, while at the same time maintaining the heat balance in the heater and cooler. The heat balance between the inlet and outlet of every node is calculated through Eq. (1):

$$\dot{Q}_i = \dot{m}_i c_{p,i} (T_{out,i} - T_{in,i}) = S_i h_i (T_{wall,i} - T_{bulk,i}) \quad (1)$$

where \dot{Q}_i is the heat flux (kW), \dot{m}_i is the mass flow rate (kg/s), $c_{p,i}$ is the specific heat at constant pressure (kJ/kg K), T_i is the temperature in degrees Kelvin (measured at the outlet, the inlet, the wall channel, and the coolant bulk), S_i is the heat-exchanging surface (m²), and h_i is the heat transfer coefficient (kW/m² K). The index i refers to the different sections.

Equation (1) states the equality between the enthalpy increase between the flow at the inlet and the flow at the outlet in any section (first equality) and the heat exchange between the channel wall and the bulk of the coolant (second equality).

The heat transfer coefficient h is a function of fluid characteristics and geometry and is calculated through appropriate correlations covering forced-, mixed-, and free-convection regimes in both turbulent and laminar flow, including transitions between individual regimes and flows, as reported in Williams et al.^{10,11} Different

Nusselt number correlations are used in the different regimes to obtain a value for the heat transfer coefficient.

The mass flow rate is determined by a balance between buoyancy and pressure losses following Eq. (2)^d:

$$\sum_i \left[\rho_i g H_i + f_i \frac{L_i}{D_i} \frac{\dot{m}^2}{2 \rho_i A_i^2} + K_i \frac{\dot{m}^2}{2 \rho_i A_i^2} \right] = 0 \quad (2)$$

The index i refers to the different sections, ρ is the coolant density (kg/m³), H is the height of the section (m), f is the friction factor, L is the length of the section (m), D is the hydraulic diameter of the section (m), \dot{m} is the mass flow rate (kg/s), A is the flow area of the section (m²), and K is the form loss coefficient.

Equation (2) states that the sum of buoyancy (first term), friction losses (second term), and form losses (third term) should be equal to zero along the closed loop.

The summation is carried over all sections and over individual nodes for the heater and cooler. The friction factor f is a function of the fluid characteristics and geometry and is calculated using appropriate correlations.^{10,11} An iterative algorithm is used to find a solution that satisfies simultaneously the heat balance and pressure loss equations.

III.C. Uncertainties

The thermal-hydraulic model that we use to find the steady-state solution is a simplified description of what happens in reality. The correlations it uses are subject to prediction errors. That is, the results of the correlations are subject to errors:

$$y = f(x)\varepsilon \quad (3)$$

where y is the real value of the quantity to be predicted (h or f), $f(x)$ is the result of the correlation, and ε is the prediction error. This error is modeled as being normally distributed with mean value equal to unity and standard deviation to be determined below. This error represented in Eq. (3) is commonly classified as *model uncertainty*.¹² It is present because the correlations are approximate.

Also, some uncertainty exists regarding the value of parameters, such as the power level, the pressure in the guard containment, and the wall temperature in the cooler. Both model and parameter uncertainties are called epistemic (or state-of-knowledge) uncertainties and are meant to describe our current state of knowledge through probability distributions.^{7,12-14} The epistemic probability distributions used in our study are normal distributions whose mean value corresponds to the nominal value and whose

^dAcceleration losses are not considered in the equation because they cancel out over a closed loop. They are considered only to determine the flow split between the hot and the average channel.

standard deviation is proportional to the estimated uncertainty.^e

The uncertainties regarding parameter values are the following:

1. power, with an estimated standard deviation of 1%
2. pressure, with an estimated standard deviation of 7.5%
3. cooler wall temperature, with an estimated standard deviation of 5%.

The factor ε that represents model uncertainties is assumed to be normally distributed with mean value equal to unity (as stated above) and standard deviation as follows:

1. *Nusselt number in forced convection*: 5%
2. *Nusselt number in mixed convection*: 15%
3. *Nusselt number in free convection*: 7.5%
4. *friction factor in forced convection*: 1%
5. *friction factor in mixed convection*: 10%
6. *friction factor in free convection*: 1.5%.

The choices are elaborated on below.

III.C.1. Power

According to industry practice and experience, an error of 2% is usually considered in the determination of the power level, due to uncertainties in the measurements. Assuming that this error defines the 95% confidence interval,^f we have accordingly set the standard deviation equal to 1%.

III.C.2. Pressure

The system pressure before the accident is kept by the control system within a small percentage of the nominal value. However, the post-LOCA conditions are determined not only by the pressure level in the primary

^eThe choice of normal distributions is mainly driven by the fact that the calculations involved in the particular Monte Carlo algorithm we use are simplified using normal distributions. However, one problem of using normal distributions is that negative values of the parameters are possible. We overcome this difficulty by cutting off the tail of the distribution so that only positive values are considered. This trick does not affect the results because negative values are at least 10 standard deviations far from the mean.

^fFor a normal distribution, the two-sided 95% confidence interval lies at ± 1.96 standard deviations from the mean value; therefore an error of $\pm 2\%$ corresponds roughly to a standard deviation of 1%.

system and guard containment before the accident but also by the energy stored before the accident, the energy absorbed by surrounding materials, the dynamics of the accident, and the leakage rate of the gas from the guard containment. All these uncertainties accumulate in the final pressure value in the guard containment. Therefore, its uncertainty in post-LOCA conditions should be relatively large, and the 95% confidence interval has been set to $\pm 15\%$.

III.C.3. Cooler Wall Temperature

The model uses the inner wall temperature in the cooler as a boundary condition. Water with inlet and outlet temperatures of 25°C and 85°C, respectively, is proposed as the secondary cooling medium. The design of the secondary cooling system has not been finalized; hence, a uniform inner wall temperature of 90°C was used in the model as a first approximation. Independently of the detailed design of the water cooling system, this wall temperature will carry uncertainties stemming from fouling of heat transfer surfaces and from the heat transfer coefficient on the water side, as well as uncertainties in the inlet water temperature, which arrives from the water storage tank outside the guard containment and is affected by ambient conditions in the reactor building. Considering the secondary system uncertainties, a 95% confidence interval of $\pm 10\%$ on this value has been considered.

III.C.4. Nusselt Number and Friction Factor

Correlations used to calculate values for the Nusselt number and friction factor are obtained from experimental databases. They have different functional forms depending on the geometry, fluid characteristics, boundary conditions (uniform heat or uniform temperature), and regime (forced, natural, or mixed convection). Heating in vertical piping and the forced-flow regime has been extensively studied because of its practical importance in power production, and the correlations involved are quite precise. On the other hand, natural and especially mixed-convection correlations are not supported by extensive experimental results, and the resulting correlations suffer from larger uncertainty. The uncertainty distributions that we have used represent the current state of knowledge. It is conceivable that they may be reduced in the future as more experimental data are obtained and better correlations are developed.

Starting from correlation errors available in the open literature^{15,16} and depending on the applicability of the correlation used, we have estimated the error on the Nusselt number to range from a minimum of 10% (forced convection) to a maximum of 30% (mixed convection). Similarly, the error on the friction factor ranges from a minimum of 2% (forced convection) to a maximum of 20% (mixed convection).

IV. RESULTS

IV.A. Nominal Conditions

IV.A.1. Failure Limits

By using nominal values^g for all parameters, the outlet temperatures under nominal conditions can be calculated. The limits imposed on the coolant outlet temperature are 850°C for the average channel and 1200°C for the hot channel. “Failure” occurs whenever the calculated temperature value is larger than the limit. The limit of 850°C on the core-average outlet temperature is driven by concerns of unacceptably high thermal stresses in the cooler and in the stainless steel cross ducts connecting the reactor vessel and the cooler. This limit is rather arbitrary and is based on designers’ concerns. No stress calculations have been performed to support its value at this feasibility study level. Future mechanistic analyses could show that the 850°C limit may have to be corrected. The rationale for the hot-channel limit derives from the need to limit the fuel temperature to avoid excessive release of fission gases. A limit of 1600°C is commonly accepted for SiC-coated fuel pellets in modular high-temperature gas reactors (MHTGRs). However, the type of fuel in the GFR differs from that of the MHTGR, and a 1200°C limit on the coolant outlet temperature for the hot channel has been imposed conservatively.^h An additional rationale behind the hot-channel limit is given by the limit on thermal stresses on above-core structures due to non-mixed flow.

IV.A.2. Results

In Table II, the calculated nominal values for different numbers of loops are reported. Safety margins defined as the difference between the limit and the outlet temperature are reported in parentheses. With the exclusion of the single-loop case,ⁱ all other designs provide a positive safety margin for both the hot and the average channel. For comparison, the margins of the actively cooled system (with blowers) are shown. The active system has an identical design for each loop but uses

^gIn our example, given the choice of normal uncertainty distributions, nominal values happen to be both mean values and median values.

^hThe 1200°C has been imposed as a conservative limit believed to lie below the real failure point for the fuel. A complete probabilistic risk assessment should also quantify the uncertainties on the limits and propagate them in a way similar to that done for the calculated maximum temperatures. However, data about the relevant uncertainties are quite difficult to obtain, and in the present study we limit ourselves to the propagation of uncertainties in the calculated maximum temperatures and use as limits conservative values.

ⁱUnsatisfactory performance of the single-loop case is expected, since the system is designed to satisfy the limits for $2 \times 50\%$ loops in operation.

TABLE II
Calculated Outlet Temperature for Nominal Conditions*

	One Loop	Two Loops	Three Loops	Four Loops	Five Loops
Passive design					
Average channel	1085 (N/A)	616 (234)	489 (361)	438 (412)	413 (437)
Hot channel	1226 (N/A)	871 (329)	620 (580)	529 (671)	492 (708)
Active design					
Average channel	1158 (N/A)	562 (288)	428 (422)	390 (460)	371 (479)
Hot channel	1227 (N/A)	870 (330)	520 (680)	457 (743)	432 (768)

*Safety margins are in parentheses.

blowers placed in the cold leg (section 15 in Fig. 1). The active system operates at atmospheric pressure so that there is no need for backup pressure, and the blower power has been chosen to have the same margin for the hot channel as the passive system in the two-loop design.

IV.B. Probabilistic Calculations

Even if the nominal calculations show that the multiple-loop designs are capable of performing their cooling function, the uncertainties associated with both the model and the parameters do not rule out the possibility that the system will behave differently from the simulated one and will possibly fail to cool the reactor core. This event will lead to a functional failure of the system.

To calculate the probability of functional failures (as defined by the limits given in Sec. IV.A), we have performed 10 000 Monte Carlo simulations for each design.^j The calculated failure probabilities and their errors (corresponding to a 95% confidence level) are reported in Table III.

As previously stated, the values in Table III are conditional on the fact that natural (or forced in the active design) convection has already been established and do not take into account the initial transient phase. For instance, the two-loop design steady state in its passive

^j By performing Monte Carlo simulations, it is possible to propagate model and parameter uncertainties and calculate the distribution of the outlet temperatures and thus the probability of observing a temperature value above the defined limit. The application of a simple sampling Monte Carlo algorithm would require a prohibitively large number of simulations to obtain low errors for estimated values, on the order of 10^{-5} or even lower. Therefore, it was necessary to use a variance-reducing technique such as importance sampling to obtain small errors in the results with a limited number of simulations.

configuration has a probability of 4.76% to have temperatures above the limits. This failure event is due to epistemic uncertainties on the values of parameters and correlation results.

The failure probabilities for the passive design, although lower than the estimates provided in the examples by Burgazzi² and Jafari et al.,⁶ are far from being negligible. These results show that together with hardware failures, functional failures should be explicitly considered in evaluating the reliability of the overall system. On the other hand, the results for the active system show that for multiple-loop designs, the functional failure probabilities are negligible and can be ignored. Very low values for the active design are due to the fact that the system is less sensitive to uncertainties, as the results from a one-way sensitivity analysis show (Table IV). The table shows the relative variations of the maximum temperatures for a 1% variation in parameter value. For example, a 1% change in the pressure will change the maximum temperature by a factor of 0.011245 to 881°C.

The active design is not subjected to pressure uncertainty^k (because it operates at atmospheric pressure) or to uncertainties associated with mixed convection (because it operates in the forced regime); therefore, the total uncertainty on the outlet temperature and correspondingly the functional failure probability are smaller.

The single most important uncertainty is the one on the pressure value, which affects the final result both because of the large sensitivity (Table IV) and because of the associated standard deviation. For the hot channel the effect of this uncertainty is about 7% larger than for the average channel, and, in fact, the observed failure mode

^k We note that uncertainties on the pressure head provided by the blower could also be modeled and taken into account. However, we have assumed the blower to be conservatively designed, and we have not modeled the uncertainty on the pressure head.

TABLE III
Probabilities of Functional Failure

	Probability of Failure				
	One Loop	Two Loops	Three Loops	Four Loops	Five Loops
Passive design	9.93E-1 ^a ±3.39E-2	4.76E-2 ±2.24E-3	4.05E-4 ±4.02E-5	7.19E-6 ±8.72E-7	9.58E-7 ±8.40E-8
Active design	9.92E-1 ±2.95E-2	<1E-11	<1E-11	<1E-11	<1E-11

^aRead as 9.93×10^{-1} .

TABLE IV
One-Way Sensitivity Analysis for the Two-Loop Design: Relative Variation of the Outlet Temperature for a 1% Variation of the Uncertain Parameter

Parameter	Passive Design		Active Design	
	Hot Channel	Average Channel	Hot Channel	Average Channel
Power	0.011763	0.008732	0.02333	0.011279
Pressure	0.011245	0.010583	—	—
Cooler temperature	0.003594	0.003807	0.004362	0.00289
Nusselt number				
Free convection	—	—	—	—
Mixed convection	0.002055	0.002057	—	—
Forced convection	0.000236	0.000273	0.003979	0.002374
Friction factor				
Free convection	—	—	—	—
Mixed convection	0.00541	0.002565	—	—
Forced convection	6.96E-05 ^a	0.000356	0.010267	0.003633

^aRead as 6.96×10^{-5} .

is due exclusively to a hot-channel outlet temperature above the limit. This behavior is observed even if the safety margin for the hot channel actually appears to be larger than that for the average channel (Table II). This is because of the large sensitivity of hot-channel flow rate to kinematic viscosity. Due to small helium flow rates under natural circulation, the flow in the core channels is in the laminar regime, where the friction factor is inversely proportional to the Reynolds number and thus strongly dependent on kinematic viscosity. Kinematic viscosity ($\nu = \mu/\rho$) increases strongly with temperature (roughly as $T^{3/2}$), and because temperature in the hot channel is higher than in the average channel, the friction factor in the hot channel is increased, reducing the flow. The smaller the flow in the hot channel, the higher the coolant temperature rise will be, leading to an earlier attainment of the hot-channel temperature limit.

V. DISCUSSION OF RESULTS

V.A. Safety Margins as Reliability Measures of System Performance

Large safety margins are commonly used to enhance safety. Their importance lies in the fact that they are simple and measurable. They are often interpreted as an indirect measure of the unquantified system performance; i.e., the larger the margin, the safer the system is considered to be. However, this interpretation is not always accurate. It is possible to have two systems with the same safety margin but different probabilities of failure, and vice versa. The results from Table III show that indeed the probability of failure for the two-loop active design and the two-loop passive design are completely different, even if the hot-channel margins

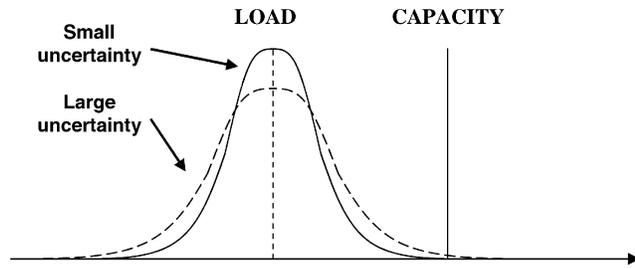


Fig. 2. Uncertainty on load. In the case study only uncertainty on the load is considered; the capacity is described by a point-estimate value.

are the same.¹ Also, despite the fact that for all designs the margins for the average channel are smaller than those for the hot channel, the hot channel is the cause of failure in all designs.

While the above observation is fairly well known in reliability physics,³ it is useful to highlight the fact that safety margins are a measure of the “distance” between the load and the capacity (Fig. 2). While this measure provides a first approximation of functional reliability, ranking different systems on safety margins alone can lead to erroneous results. The knowledge of the distance from failure in terms of safety margins is not sufficient to evaluate the risk of a system; the capability to cover that distance (the breadth of the uncertain distribution) is the other important part of the assessment.

V.B. Effects of Redundancy on Functional Failures

Employing redundancy is a common way to reduce the probability of system failure. The effect of redundancy on hardware failures can be modeled using analytical tools such as fault trees. The dependence among component failures is taken into account using appropriate common cause failure (CCF) models.¹⁷ On the other hand, functional failures are due to uncertainties that can affect different components at the same time and depend on the overall system sensitivity to these uncertainties. Uncertainties that affect all loops in the same way (such as power and pressure levels) reduce the benefits due to redundancy,^m while changes in system sensitivity could both improve or reduce them. The gain in functional reliability due to redundancy follows completely different rules and can be substantially different from the corresponding gain in hardware reliability.

¹As discussed in Sec. IV.B, the failure mode is the hot-channel temperature being above the limit; thus, the margin on this value is to be considered an appropriate measure of the safety margin.

^mA discussion on the correlations that epistemic uncertainties introduce in the analysis of redundant components can be found in Apostolakis and Kaplan.¹⁸

In the case of hardware failures, the larger reduction in failure probability can be achieved with ideal independence among components. In this special case, the reduction of the failure probability with the number of redundant components is

$$P_{n,i} = p^n, \quad (4)$$

where $P_{n,i}$ is the probability of failure of the system with n independent components and p is the probability of failure of a single component. This value constitutes a lower bound to the failure probability of a redundant system. However, this lower bound for reduction in failure probability does not apply to functional failures. Let us consider the results of Table III. For the case of a single loop, the probability of failure is 0.993, while for the redundant system with two loops the probability of failure is 4.76E-2. The decrease in failure probability due to the additional loop is larger than in the ideal case of perfect independence; in fact, $p^2 = 0.993^2 = 0.986 > 4.76E-2 = P_2$.ⁿ In Table V the results for all the configurations are compared with the theoretical results calculated assuming perfect independence and treating functional failures as if they were hardware failures. For the one-, two-, and three-loop configurations, the decrease in failure probability obtained by adding an additional loop is larger than the gain that would have resulted assuming independence.

V.C. Inclusion of Functional Failures in PRAs

The objective of a PRA is to identify all possible accident scenarios and quantify their frequencies. To achieve this result, a logic model of the system is developed, in the form of event trees and fault trees, that describes the system as a function of its components. By assigning frequencies to accident initiators (initiating events) and failure probabilities to components, it is possible to quantify the failure frequency of the overall system. While hardware failures are naturally included in the model as probabilities of failure of the individual components, functional failures should be dealt with at the success criteria level.

Success criteria are normally defined on the basis of deterministic analyses that rely on the concept of sufficient safety margins. Satisfying these requirements can theoretically imply a small functional failure probability; however, they are usually treated as full successes in PRAs, assuming implicitly a negligible probability of functional failure. The reason for this assumption is that active redundant safety systems, such as the ones

ⁿThis result should not be unexpected; in fact, the system has been designed so that a single 50% loop is expected to fail its mission, while two or more loops will be able to accomplish it. This example is intended to stress the fact that probabilities associated with functional failures cannot be treated in the same fashion as probabilities of hardware failures.

TABLE V

Comparison of Failure Probabilities Obtained from Simulations and Calculated Assuming Independence

	Probability of Failure				
	One Loop	Two Loops	Three Loops	Four Loops	Five Loops
From simulations	9.93E-1 ^a (P_1)	4.76E-2 (P_2)	4.05E-4 (P_3)	7.19E-6 (P_4)	9.58E-7 (P_5)
Assuming independence	—	9.86E-1 (P_1^i)	1.04E-2 ($P_2^{3/2}$)	2.99E-5 ($P_3^{4/3}$)	3.72E-7 ($P_4^{5/4}$)

^aRead as 9.93×10^{-1} .

installed in nuclear plants, are not sensitive to uncertainties to such a degree as to worry about functional failures. The results of Table III show that indeed functional failure probabilities for the active system (blowers operating) are negligible (below 10^{-11}).

A completely different approach should be taken for passive systems. Recent studies by Burgazzi^{2,5} and Jafari et al.⁶ have shown that functional failures can be important in risk assessment involving passive systems.

To show how much functional failure can affect the risk assessment of a passive system, let us quantify the risk of two-, three-, and four-loop designs considering functional failures. The passive system design has no hardware components that can fail^o; therefore, only functional failures due to epistemic uncertainty contribute to its unreliability.

For each configuration, there is a probability of functional failure F_i , given by the results of Table III. F_i is the conditional failure probability given that natural convection has occurred and is due to epistemic uncertainty. Including these functional failures, we can write the total failure probabilities of the systems as

$$P_{2,F} = F_2 = 4.76 \times 10^{-2} ,$$

$$P_{3,F} = F_3 = 4.05 \times 10^{-4} ,$$

and

$$P_{4,F} = F_4 = 7.19 \times 10^{-6} ,$$

where $P_{2,F}$, $P_{3,F}$, and $P_{4,F}$ are the total failure probabilities of the two-, three-, and four-loop designs, respectively.

^oThe check valves are the only hardware components that can fail. However, the check valve failure probability should be considered during the transient leading to natural convection (failure to open the check valve). During the steady-state operation, once the check valve has opened, it cannot fail. We also note that one of the loops of the passive system could be the location in which the LOCA occurs. In this case, that loop would be unavailable. Thus, a four-loop system would become a three-loop system, which is analyzed in the paper.

Given the previous estimates, it is possible to make a comparison with the actively cooled system (with blowers operating). In this case blower failures have to be included, while functional failures are negligible.

We assume a mission time of 72 h and a failure to run frequency ranging from 10^{-5} to 10^{-4} per hour.^p To take into account common-cause failures, the multiple Greek letter (MGL) model has been used. Realistic values for the parameters have been estimated from Marshall and Rasmuson¹⁷ and are the following^q:

$$\beta = 0.035 ,$$

$$\gamma = 0.65 ,$$

and

$$\delta = 0.7 .$$

Using the rare-event approximation, the total probability of failure of the three- and four-loop systems is given by the formulae

$$P_{2,A} = 2(1 - \beta)q + \beta q ,$$

$$P_{3,A} = 3[(1 - \beta)q]^2 + \frac{3}{2}\beta(1 - \gamma)q + \beta\gamma q ,$$

and

$$P_{4,A} = 4[(1 - \beta)q]^3 + 4\beta(1 - \beta)(1 - \gamma)q^2 + \frac{4}{3}\beta\gamma(1 - \delta)q + \beta\gamma\delta q , \tag{5}$$

where q is the probability of failure of the blower, β , γ , and δ are the MGL factors for the blowers, and $P_{2,A}$, $P_{3,A}$, and $P_{4,A}$ are the total failure probabilities of the two-, three-, and four-loop active designs, respectively.

^pThese values are assumed to be the 5th and 95th percentiles of the parameter epistemic distribution. The distribution used is lognormal.

^qEpistemic uncertainty has been modeled with lognormal-truncated distributions with error factor equal to 3. The truncation is necessary to avoid parameter values above unity.

TABLE VI
Probability of Failure Results for the Passive
and Active Systems

	Two Loops	Three Loops	Four Loops
Passive design	4.76E-2 ^a	4.05E-4	7.19E-6
Active design			
Mean	5.70E-3	1.58E-4	7.85E-5
Median	3.00E-2	1.82E-3	1.14E-3
5th percentile	3.00E-3	1.68E-4	1.06E-5
95th percentile	5.70E-2	3.48E-3	2.18E-3

^aRead as 4.76×10^{-2} .

The epistemic uncertainties have been distributed through Monte Carlo algorithms, and the results are summarized in Table VI. The failure probability of the active system is dominated by the common-cause failures of the blowers. In fact, an increase in redundancy from three to four loops does not improve the reliability of the system significantly.

The reliability results are summarized in Table VI. While the passive system is always more reliable than the active one when functional failures are not considered, this is not the case if their impact is included in the analysis. Comparing the mean values^r shows that the active system is actually more reliable than the passive one for the two- and three-loop designs. An increase in redundancy, as discussed in Sec. V.B, is more effective for functional reliability (affecting the passive system) than for hardware reliability (affecting the active system); therefore, for the highly redundant four-loop design the passive system seems to be better than the active one.

It should finally be stressed that the calculated failure probability refers to the 72-h steady-state period after the initial transient. The results are conditional on the successful inception of natural (or forced) convection.

VI. CONCLUSIONS

Functional failures are not taken into account in risk assessments explicitly. By satisfying deterministic criteria such as large safety margins, we presume that the

^rMean values have to be compared to assess the more reliable system because uncertainty is present. Uncertainty on the hardware reliability value is described by the 5th and 95th percentile values, while uncertainty on the functional reliability comes from the fact that the only possible outcomes are success (corresponding to a functional failure realization of zero) and failure (corresponding to a functional failure realization equal to unity).

probability of functional failures is sufficiently low. We have performed an analysis of the role and characteristics of functional failures in the case of passive cooling in a gas-cooled fast reactor using a simplified steady-state model to perform the necessary calculations. The results can be summarized in the following points:

1. Deterministic safety measures alone such as safety margins can provide a misleading evaluation of the failure probability of a passive system. Systems with the same safety margin can have different probabilities of functional failure. Additional information should be used together with safety margins to determine the safety of a system.

2. The analysis of multiple-loop systems has shown that redundancies impact hardware and functional failures in different ways. Functional failures depend on the behavior of the system with respect to uncertainties, and a change in the system such as the addition of a redundant loop can decrease the functional failure probability in a different way than the corresponding change in hardware failure probability.

3. The combination of large uncertainties and high hardware reliability, typical of passive safety systems, makes it necessary to include functional failures in the PRA explicitly. Failure to do this would lead to optimistic results. Also, due to the functional failure effect, passive systems are not necessarily more reliable than active systems, as is commonly believed.

Some simplifications have been assumed in the paper.

1. The model considers only steady-state behavior. A detailed analysis should include a transient analysis to understand the dynamics of inception of natural convection.

2. The estimates of uncertainties, i.e., standard deviations, were based on the authors' experience and are rough estimates for the real values. Also, the shape of the epistemic distributions has been chosen so that the calculations could be simplified. The functional failure probability is very sensitive to the tails of the epistemic distributions; therefore, the values of the standard deviations and the shape of the distributions can affect the final results. A detailed study of a real system should focus on the determination of epistemic uncertainties.

Finally, it should be noted that the GFR design is still in its early stages of development, with the potential for further improvement, and our results should be viewed as part of the process that will ultimately lead to a final design. Furthermore, it needs to be noted that in addition to PRA outcomes, the economic aspects will play an important role in the final selection of the design. Although the PRA results indicate that passive decay heat removal having more than three loops could achieve substantial reduction in failure probability, it

would be more costly because of the large size of the heat exchangers required to compensate for low heat transfer rates associated with natural convection and the need for a guard containment to maintain relatively high backup pressure. Considering both the PRA results and economics, for this particular example, the 3(\times 50%)-loop active emergency cooling system appears to be the preferred choice because it exhibits smaller failure probability than the three-loop passive system and is expected to have appreciably lower capital cost than the 4(\times 50%)-loop passive system with a high-pressure guard containment. Moreover, the active system can function safely in a passive mode should sufficiently high pressure be maintained in non-LOCAs. Thus, a passive system that does not require safety-grade power trains may not necessarily be more economical than an active system, as commonly believed.

ACKNOWLEDGMENTS

We thank Michael Driscoll of the Massachusetts Institute of Technology for his useful comments. We also appreciate the support and comments we have received from Hossein Hamzheh and Prasad Kadambi of the Office of Nuclear Regulatory Research of the U.S. Nuclear Regulatory Commission (NRC). Robert Youngblood of ISL, Inc., provided useful insights also. This work is part of a project on the quantification of safety margins that is supported by the NRC under a cooperative agreement with the MIT Department of Nuclear Engineering. The views expressed in the paper are the authors' and do not necessarily reflect the views of the NRC.

REFERENCES

1. J. N. SORENSEN, G. E. APOSTOLAKIS, T. S. KRESS, and D. A. POWERS, "On the Role of Defense in Depth in Risk-Informed Regulation," *Proc. Int. Topl. Mtg. Probabilistic Safety Assessment (PSA '99)*, Washington, D.C., August 22–26, 1999, pp. 408–413, American Nuclear Society, La Grange Park, Illinois (1999).
2. L. BURGAZZI, "Reliability Evaluation of Passive Systems through Functional Reliability Assessment," *Nucl. Technol.*, **144**, 145 (2003).
3. S. S. RAO, *Reliability-Based Design*, McGraw-Hill, New York (1992).
4. A. W. CRONENBERG, M. V. BONACA, and G. B. WALLIS, "Margin Reductions for Re-Licensing/Uprated Plants and Risk Implications," *Proc. Int. Topl. Mtg. Probabilistic Safety Assessment (PSA '02)*, Detroit, Michigan, October 6–9, 2002, American Nuclear Society, La Grange Park, Illinois (2002).
5. L. BURGAZZI, "Evaluation of Uncertainties Related to Passive Systems Performance," *Nucl. Eng. Design*, **230**, 93 (2004).
6. J. JAFARI, F. D'AURIA, H. KAZEMINEJAD, and H. DAVILU, "Reliability Evaluation of a Natural Circulation System," *Nucl. Eng. Design*, **224**, 79 (2003).
7. G. E. APOSTOLAKIS, "A Commentary on Model Uncertainty," *Proc. Workshop on Model Uncertainty: Its Characterization and Quantification*, pp. 13–22, A. MOSLEH, N. SIU, C. SMIDTS, and C. LUI, Eds., Center for Reliability Engineering, University of Maryland, College Park, Maryland (1995); also published as NUREG/CP-0138, U.S. Nuclear Regulatory Commission, Washington, D.C. (1994).
8. Y. OKANO, P. HEJZLAR, and M. J. DRISCOLL, "Thermal Hydraulics and Shutdown Cooling of Supercritical CO₂ GT-GCFRs," MIT-ANP-TR-088, MIT, Department of Nuclear Engineering (2002).
9. J. EAPEN, P. HEJZLAR, and M. J. DRISCOLL, "Analysis of a Natural Convection Loop for Post-LOCA GCFR Decay-Heat Removal," MIT-GCFR-002, MIT, Department of Nuclear Engineering (2002).
10. W. WILLIAMS, P. HEJZLAR, M. J. DRISCOLL, W. J. LEE, and P. SAHA, "Analysis of a Convection Loop for GFR Post-LOCA Decay Heat Removal from a Block-Type Core," MIT-ANP-TR-095, MIT, Department of Nuclear Engineering (2003).
11. W. WILLIAMS, P. HEJZLAR, and P. SAHA, "Analysis of a Convective Loop for GFR Post-LOCA Decay Heat Removal," *Proc. 12th Int. Conf. Nuclear Engineering (ICONE 12)*, Arlington, Virginia, April 25–29, 2004.
12. G. E. APOSTOLAKIS, "The Distinction Between Aleatory and Epistemic Uncertainties Is Important: An Example from the Inclusion of Aging Effects into PSA," *Proc. Int. Topl. Mtg. Probabilistic Safety Assessment (PSA '99)*, Washington, D.C., August 22–26, 1999, pp. 135–142, American Nuclear Society, La Grange Park, Illinois (1999).
13. G. E. APOSTOLAKIS, "The Concept of Probability in Safety Assessments of Technological Systems," *Science*, **250**, 1359 (1990).
14. R. L. WINKLER, "Uncertainty in Probabilistic Risk Assessment," *Reliabil. Eng. Syst. Safety*, **54**, 127 (1996).
15. S. W. CHURCHILL, "Combined Free and Forced Convection in Channels," *Heat Exchanger Design Handbook*, Sec. 2.5.10, G. F. HEWITT, Ed., Begell House, New York (1998).
16. V. GNIELISNIKI, "New Equations for Heat and Mass Transfer in Turbulent Pipe and Channel Flow," *Int. Chem. Eng.*, **16**, 2, 359 (1976).
17. F. M. MARSHALL and D. M. RASMUSON, "Common-Cause Failure Data Collection and Analysis System, Vol. 6: Common-Cause Failure Parameter Estimations," INEL-94/0064, Idaho National Engineering Laboratory (1995).
18. G. E. APOSTOLAKIS and S. KAPLAN, "Pitfalls in Risk Calculations," *Reliabil. Eng.*, **2**, 135 (1981).