1

The Risk of Core Damage in Risk-Informed Decision Making: The Original Sin and the Road to Redemption

Yuri Orechwa
NRR/DSS/SFNB
May 3, 2021

Introduction: The Original Sin

The foundational paper on the formulation of risk in the context of nuclear reactor operation by Kaplan and Garrick (Ref.6),when first published, drew some serious critique in the subsequent issues. See "Some Misconceptions About the Foundations of Risk Analysis", Ref. 9, "Some Misconceptions About Misconceptions: A Response to Abramson", (Ref.10), and "A Rejoinder to Kaplan and Garrick", (Ref. 11). Ref. 11 states " I leave it to the reader to judge how responsive Kaplan and Garrick have been to my comments." We agree with Abramson! In particular, from today's perspective Abramson's critique, with regard to Kaplan and Garrick's introduction of 'subjective probability' or 'degrees of belief' for assessing the likelihood of events in the real world. In our view the confusion introduced by 'subjective probability' and/or 'degree of belief' is based, as Abramson points out, on the relationship between *their* notions of frequency, probability density, and the probability of an event. With regard to their definition of risk, Kaplan and Garrick state; "One often hears it said that 'risk' is probability *times* consequence. We find this definition misleading and prefer instead, in keeping with the set of triples idea, to say that 'risk' is probability *and* consequence." Their argument is based on the fact that "In case of a single scenario the probability *times* consequence viewpoint would equate a low-probability high-damage scenario with a high-probability low-damage scenario - clearly not the same thing at all." (Ref. 6) The observation, in principle, is *mathematically* true *for point estimates*, but irrelevant in risk analysis *of events*. Risk is associated with the *event* in the tail of the probability density function of the figure of merit, where the damage is greatest. (see Ref. 12) We believe that their methodology, based on the triplet formulation formally contains the correct ingredients, while the word '*and*' is the wrong recipe.This has has relegated, the result of a Level 1 PRA of the CD to risk transformation, to a purgatory as two end states - 0 and 1. (Ref. 7)

We note in passing, with regard to the issue of correct recipe for risk (+/×,?), a 'slip of the tongue' in Ref. 7 (p. C-105). "The other definition of risk is aggregate risk , [25] which is defined as the sum of the ***products*** of the scenario frequencies and the scenario consequences:

$R = \sum_{i=1}^{n} [F_i]x[C_i]$, where F_i is events/time and C_i is consequences/event."

Footnote 25 says "This term is not commonly recognized nomenclature but is used here

to *discus the concept.*" We find this curious, since FxC ~ [# events/time]x[consequence/event] = consequence/time a recognized measure of risk, while F + C has no clear interpretation. (See Ref. 16 for an example)

It is time to atone for not taking into account Abramson's critique!

The Road to Redemption

Let us recall the three sequential levels of analysis into which current risk assessments of light - water reactors are broken . (Refs 7 and 13) This allows us to identify the necessary ingredients of the CD for the analytic form of the risk transformation for a PRA reactor analysis (Ref. 7) .

A. Heuristic Probabilistic Structure of PRA Reactor Analysis

Level 1(L1). System analysis - An assessment of plant design and operation consisting of the definition and quantification of accident sequences, component data, and human reliability **that could lead to core melt.** (Ref. 14)

Level 2 (L2). Containment analysis - An analysis, **conditional on** L1, of the response of the reactor containment to core damage.

Level 3 (L3). System consequence analysis - An assessment, **conditional on** L1 **and** L2, of the transport of radio-nuclides through the environment and the public-health consequences.

Let us consider a simple L1 PRA based on the elements in Fig. 1.

Initiating Event Safety System 1 Safety System 2 Event Sequence i Consequence

IE SS1 SS2 ESi PRA & LBA

Fig. 1 Generic Linked Structural Elements of a L1 PRA

The unifying structure for the simple PRA of Fig. 1 is depicted for our discussion in Fig.2 by an event tree that orders the safety functional responses (SS1 and SS2) that mitigate the initiating event. A function event tree is, in general, developed for each postulated initiating event, since each initiator may require a unique plant response. Similarly all LBAs also have the same basic formal postulated initiating event and safety system structure. There are 4 end states in Fig. 2 for the particular initiating event.

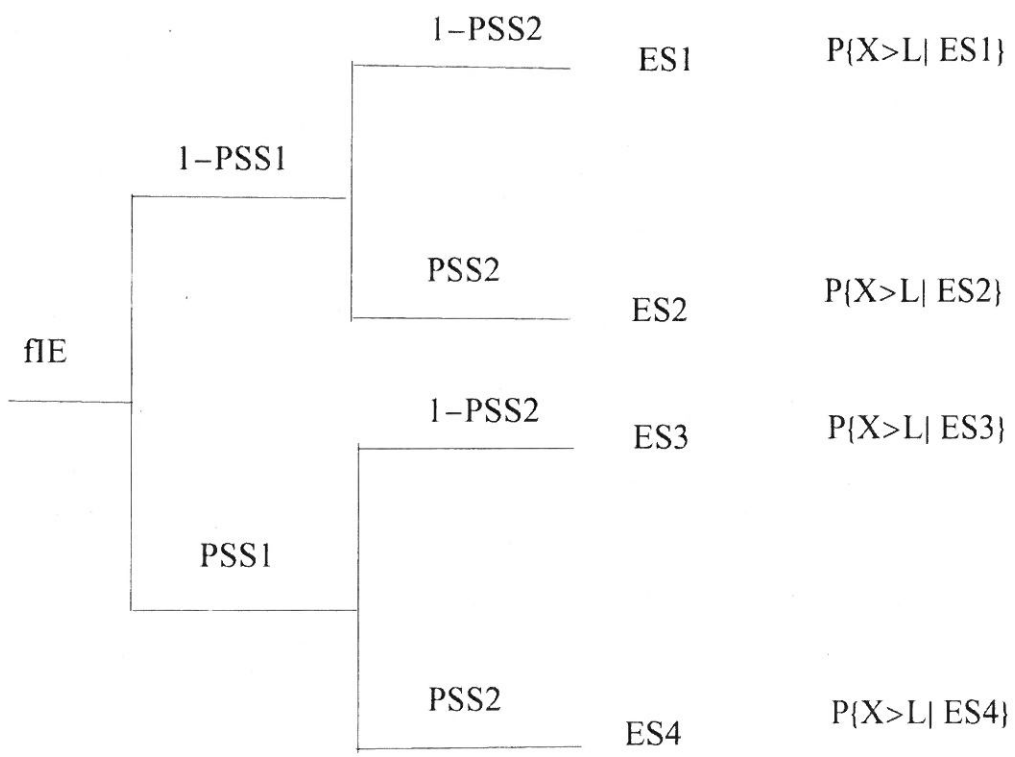

Fig. 2. Generic Simple Event Tree for PRA and LBA Analysis for L1

We define:

fIE - Initiating Event frequency

PSS1 - Conditional Probability of SS1 failure

PSS2 - Conditional Probability of SS2 failure

PES1 = (1-PSS1)*(1-PSS2) -Conditional Probability of Event Sequence 1
PES2 = (1-PSS1)*PSS2 - Conditional Probability of Event Sequence 2
PES3 = PSS1*(1-PSS2) - Conditional Probability of Event Sequence 3
PES4 = PSS1*PSS2 - Conditional Probability of Event Sequence 4

P{X>L| ES1} - Probability of a damage surrogate X exceeding limit L given ES1,

etc.

Note: The computation of the point estimates of the conditional branching probabilities of the event tree are assumed to have been derived for each safety system by a separate fault tree analysis and are not at issue in our argument.

The guidance for NRC staff uses of probabilistic risk assessment proffered in NUREG – 1489 (Ref. 7) is as follows: "Regardless of the method that is chosen to perform a *transformation* from a core damage frequency estimate to a risk estimate, the NRC staff must be fully aware of the constituents of the PRA (i.e. scope, models, and assumptions) yielding the *numerical quantities* used in a transformation from core damage frequency to risk." The current state of Level 1 PRA end–state success criteria is given in NUREG/CR–7177 (Ref. 14) as Table 4.1 page 45. It lists 13 different CD surrogates! These are based on experience with MELCOR models and "informed" by regulatory guidance such as NUREG–1465 and the 2012 revision of 10 CFR 50.46.

We put forward *one criterion* as the numerical quantity of interest in the estimation of CD: *The number of failed fuel elements* in the core. The failure of each element is based on the *local* thermal–hydraulic state variables at the pin cell level. (Ref. 8) Thus, from our perspective, core damage (CD) is functionally related to the *number* of failed fuel elements and is estimate via methods such as those presented in Ref. 2.

B. Representations of Probabilistic Structure of Risk

The basic expression for Risk consists of three terms. (Ref.7) For an L1 analysis as shown in Fig. 2, the three terms are:

fIE - the frequency per year of an initiating event, (for example one from a set IE≡{LBLOCA, SBLOCA, SBO, ATWS, etc.})

ES - an event scenario (i.e. a sequence of safety system actions (failure/non-failure))

X>L - an outcome, generally a surrogate for core damage (CD) where the surrogate value X has exceeded the acceptance limit L.

Based on the notation of the event tree in Fig. 2, we can formulate the Risk R_{ij} of an adverse event (X_{ij}>L) due to an initiating event IE_i and an activation of a sequence of safety systems resulting in an event sequence ES_{ij}, that occurs with frequency fIE_i, which can be expressed as a joint probability distribution function

$$R_{ij} = fIE_i * P\{ ES_{ij}, X_{ij} > L\}. \tag{1}$$

The total risk for the reactor, therefore, is given as

$$R = \sum_{i=1}^{N} fIE_i * \sum_{j=1}^{M} R_{ij}, \tag{2}$$

where N is the number of postulated initiating events and M the number of safety systems.

The joint probability distribution function for the contribution to the total risk R by a specified initiating event IE_i and event sequence ES_{ij} can be decomposed into the product of three terms,

$$R_{ij} = fIE_i * P\{ ES_{ij} \mid IE_i\} * P\{ X_{ij} > L \mid IE_i, ES_{ij} \}. \tag{3}$$

This expression can be viewed in the context of Fig. 2 as having two components:

First, we can consider fIE analogous to a multiplicative constant and drop its contribution to risk from further analysis without loss of the *probabilistic* content of our argument.

$R^{PRA} = P\{ ES_{ij} \mid IE_i\}$ - probabilistic methods that focus on the probabiity of *operation of the plant safety systems* that define the event sequences.

R^{LBA} = P{ X_{ij}>L |IE_i, $ES_{ij,}$ } - deterministic methods concerned with the probability of the t*ransient behavior of the reactor core* exceeding a specified limit for a particular sequence of events.

Thus, in the expression for the plant risk (Eq. 3), the link between the PRA analysis component and the LBA analysis component is through the event sequence ES for a given initiating event IE. That is, the probability of the event {X>L}, i.e. core damage, is dependent on the probability of the event {ES}, which is specified by a particular safety system failure sequence. Here an important dichotomy between L1 PRA risk analysis and a best-estimate plus uncertainty LBA is revealed. Two distinct analyses are performed that exhibit a clear symmetry. (Ref. 16)

In a traditional PRA analysis we have:

P{ES| IE} = a probability density function of the failure of the safety systems in ES.
P{X~L|ES,IE} = 0/1 (indicating no-CD/CD, based on events {X≤L}/{X>L}.

On the other hand, in a best-estimate plus uncertainty LBA analysis we have:

P{ES| IE} = 1 (failure of only the limiting safety system)
P{X>L|ES,IE} = a probability density function of core damage.

We, therefore, have four ways of expressing risk of CD dependent on the level of information content:

1. (P{ES| IE} = 1)*(P{X<L|ES,IE} =1) which would imply no CD for a bounding ES and bounding calculate mechanistic result. That is Appendix K like analysis.

2. (P{ES| IE} = 1)*P{X>L|ES,IE} which is a best-estimate plus uncertainty result of CD for the limiting ES.

3. P{ES| IE} *(P{X>L|ES,IE} =1) which is the traditional PRA result of CD frequency where the uncertainty is based on the failure probabilities of the safety systems ES.

4. P{ES| IE}*P{X>L|ES,IE} which is a risk based PRA, where both the probability of failure of the ES and the best-estimate plus uncertainty of CD form a quantified joint uncertainty probability function P{IE,ES,X>L}.

It is the fourth representation we shall address. For discussions and examples see Refs. 16 and 4.

C. Consistency of Information for the Exit from Purgatory

Let us consider the information content of the above four expressions of risk at level L1 as follows: The first is a deterministic bounding statement of the risk. The fourth a more realistic probabilistic statement of the risk; and two as an improvement over one, and three as an approximation to four.

We previously indicated, that the integrated overall risk analysis of a plant is based on three separate but coupled analyses L1, L2 and L3, and, thereby, requires well defined interfaces of the damage states between the three parts. Our focus is limited to the 1st interface between L1 and L2. Clearly any decision with regard to a consistent analysis with regard to the safety of the reactor that takes all available information (such as defense-in-depth) into account is critically dependent on the probability of the estimate of CD at L1.

The guidance for NRC staff uses of probabilistic risk assessment proffered in NUREG – 1489 (Ref. 7) is as follows "Regardless of the method that is chosen to perform a *transformation* from a core damage frequency estimate to a risk estimate, the NRC staff must be fully aware of the constituents of the PRA (i.e. scope, models, and assumptions) yielding the *numerical quantities* used in a transformation from core damage frequency to risk." We put forward as the numerical quantity of interest *the number of failed fuel elements* in the core as a measure of CD. The failure of each element is based on the *local* thermal–hydraulic state variables at the pin cell. (Ref. 8) Thus, from our perspective, core damage (CD) is functionally related to the *number* of failed fuel elements, the 'sine qua non' for a reacctor accident, irrespective of frequency.

Let us deconstruct the statement of the risk of CD as a function of the number of failed fuel elements. It may be instructive for this discussion, with nuclear engineers in mind, as an analogy to first recall the computation and interpretation of multi-group parameters in neutron transport calculations. To this end, let us consider the computational analogy

with risk analysis.

In the analysis of nuclear reactor cores, the key information of the economic and safety performance is contained in the calculated neutron flux ϕ(r,E,t). This term is not a point function, but rather a density function. Thus, it only makes physical sense as a differential ϕ(r,E,t)dVdEdt and gives the number of neutrons in volume dV at point r, with energies in energy interval dE at E, during time period dt. Due to the complicated analytic forms of the coefficients of the governing neutron transport equation, the equation is discretize in neutron energy via the multi-group formalism. To this end, we define for example, a group cross section $\sigma_g$in the energy interval $[E_g, E_{g-1}]$ as

$$\sigma_g = \int_{E_g}^{E_{g-1}} \sigma(E)\, \phi(E)\, dE \Big/ \int_{E_g}^{E_{g-1}} \phi(E)\, dE \qquad (4)$$

where σ(E) is the extent to which a neutron interacts with a nucleus *at* energy E. Whereas ϕ(E) is the neutron density *in* the energy interval *d*E. Thus, σ_g is the mean number of reactions that occur due to neutrons *in* the energy interval $[E_g, E_{g-1}]$; in probability theory parlance the "event".

In nuclear reactors with cores consisting of fuel pins, that are not only the source of the power generated, but also the first and primary barrier to the radioactive material generated in the operation of the reactor of reaching the environment. The risk of a breach of this barrier, during accident conditions, is central to decision making with regard to the safety of operating such an energy source. The key figure of merit in assessing this risk is the estimate of the pin cladding temperature (PCT). (REf. 4)

We can apply a similar approach, as in multi-group theory, to computing the *level* of core damage (CD) due a reactor transient, as follows. Let the role played by the neutron energy be the peak cladding temperature T. (It is recognized that PCT is not the only variable that comes into play. However, the required multivariate analysis is a straightforward extension.) Then, given an estimated clad failure probability *density* f(T) of cladding temperature in temperature interval dT. We can define f(T)dT as the probabiity of clad failure at clad temperature T *in* the interval dT of a fuel element. Furthermore, let CD(T) be the function of the number failed fuel elements *in the core* at T. (For the logic in the construction of this function see Ref. 12.) The the mean number of failed fuel elements in the peak clad temperature interval [T_L, ∞) is then given as

$$\mathrm{CD}_L = \int_{T_L}^{\infty} \mathrm{CD}(T)\, f(T)\, dT \,/\, \int_{T_L}^{\infty} f(T)\, dT \qquad (5)$$

The peak fuel cladding temperature density function f(T) is a property of the fuel pin design, and estimated via a BEPU computation of the fuel pin. The damage is a function of peak cladding temperature and is a property of the core; and reflects the number of fuel pins with peak cladding temperature T or higher, and is computed by the core calculation.

D. Consistency of Information Content with the Risk Triplet

Recall the definition of risk R_i at NRC as defined by the risk triplet (Refs.6 and 7):

$R_{ij} = < S_{ij}, f_{ij}, x_{ij} >$, where S_i is the i-th scenario (sequence, progression) associated with the j-th initiating event, f_{ij} the associated frequency, and x_{ij} the resulting consequence.

In our notation (Eq. 3) in the analysis, we define the three terms in the risk triplet as follows:

$$S_{ij} \longleftrightarrow \mathrm{P}(\, \mathrm{ES}_j \mid \mathrm{IE}_i \,)$$

$$f_i \longleftrightarrow \mathrm{P}(\mathrm{IE}_i)$$

$$x_{ij} \longleftrightarrow \int_L^{\infty} \mathrm{CD}(T)\, P\big(T \geq L\,,\ \mathrm{ES}_j, \mathrm{IE}_i\big)\, dT =$$
$$\int_L^{\infty} \mathrm{CD}(T)\, P\big(T \geq L \mid \mathrm{ES}_j, \mathrm{IE}_i\big)\, P\big(T, \mathrm{ES}_j \mid \mathrm{IE}_i\big)\, P(\mathrm{IE}_i)\, dT$$

In terms of our analogy with the energy group formalism, we have:

$$\mathrm{CD(T)} \longleftrightarrow \sigma(\mathrm{T})$$

$$\mathrm{P}\big(\mathrm{T} \geq \mathrm{L}\,,\ \mathrm{ES_j}, \mathrm{IE_i}\big)\, d\mathrm{T} \longleftrightarrow \mathrm{f(T)}d\mathrm{T}$$

Thus, the risk of event [T≥ L], is given by the expression

$$\mathrm{R}[T \geq L] \equiv \int_L^{\infty} \mathrm{CD}(T)\, P\big(T \geq L \mid \mathrm{ES}_j, \mathrm{IE}_i\big)\, P\big(T, \mathrm{ES}_j \mid \mathrm{IE}_i\big)\, P(\mathrm{IE}_i)\, dT. \qquad (6)$$

E. Computational Sources of Inputs to the Risk Estimate

The calculational machinery for the input to Eq. 6 is exemplified to a great extent by approach to reactor safety analysis as exemplified Ref. 1 and applied in Ref. 8. This machinery is illustrated by an analysis of the OECD-NEA Multi-Physics Pellet Cladding Mechanical Iteration Validation (MPCMIV) benchmark using coupled codes: rector physics (MOLTRES+SERPENT), thermal-hydraulics (SAM) and fuel performance (BISON) on the MOOSE framework.This type of multi-physics calculational framework, together with uncertainty propagation and quantification, would generate all the necessary ingredients to compute the risk as presented in Eq. 6.

References

1) Carlo Parisi, et al. "Risk - Informed Safety Analysis for Accident Tolerant Fuels," Nuclear Science and Engineering, Vol. 194, p748 - 770, August - September 2020.

2) Maria Avramova, et al. "Innovation in Multi-Physics Methods Development, Validation, and Uncertainty Quantification,", J. Nucl. Eng. 2021, 2, p44-36.

3) U. S. Nuclear Regulatory Commission, "Guidance on the Treatment on Uncertainties Associated with PRA's in Risk-Informed Decision-making: Final Report,"NUREG-1855, Revision 1 (March 2017).

4) Y. Orechwa, "Some Formal Considerations in the Application of Best_Estimate Plus Uncertainty Results in Licensing Basis Analysis to Risk "Informed" Decision Making for Reactor Safety," Internal NRC/NRR/DSS White Paper, June 14, 2018.

5) Y. Orechwa, "Best-Estimate Analysis and Decision Making Under Uncertainty," Proc. Int. Mtg. Updates in Best-Estimate Methods in Nuclear Installations Safety Analysis (BE-2004), November 14-18, Washington D. C., American Nuclear society (2004).

6) Stanley Kaplan and B. John Garrick, "On the Quantitative Definition of Risk," Risk Analysis, Vol 1, no. 1 (1981).

7) A Review of NRC Staff Uses of Probabilistic Risk Assessment, NUREG - 1489, March 1994.

8) Travis Mui, Tomasz Koslowski, "Preliminary Fuel Performance and Thermal Hydraulic Modeling of the MPCMIV Benchmark," Trans. of the ANS, Vol 123, Nov. 16-19, 2020.

9) Letter Lee R. Abramson to Editor, "Some Misconceptions About the Foundations of Risk Analysis," Risk Analysis, Vol 1, no. 4 (1981).

10) Letter Stanley Kaplan and B. John Garrick to Editor, "Some Misconceptions About the Foundations of Risk Analysis," Risk Analysis, Vol 1, no. 4 (1981).

11) Letter Lee R. Abramson to Editor, "A Rejoinder to Kaplan and Garrick" Risk Analysis, Vol 1, no. 4 (1981).

12) Y. Orechwa, "The 95/95 Acceptance Criterion in Risk-Informed Regulation: The 95/95 Delusion," Internal NRC/NRR/DSS White Paper, September 15, 2019.

13) U.S. Nuclear Regulatory Commission, "PRA Procedures Guide,"NUREG/CR-2300, Vol. I (January 1983).

14) U.S. Nuclear Regulatory Commission, "Compendium of Analyses to Investigate Level1 Probabilistic Risk Assessment End-State Definition and Success criteria Modelling Issues," NUREG/CR-7177 (May2014).

15) U.S. "Confirmatory Thermal-Hydraulic Analysis to Support Specific Success Criteria in the Standardized Plant Analysis Risk Models - Byron Unit 1," NUREG_2187 (January 2016).

16) H. F. Martz, et al.,"Combining mechanistic best-estimate analysis and Level 1 probabilistic risk assessment." Reliability Engineering and System Safety, Vol. 39 (1993).