AN ADVANCED RISK ANALYSIS FRAMEWORK. D. G. Robinson, Sandia National Laboratories, Information and Cognitive Sciences, PO Box 5800, MS 1327, Albuquerque, NM 87185 drobin@sandia.gov

Introduction: This presentation provides a summary of the risk analysis framework developed to support the launch safety analysis of the Mars Science Laboratory (MSL).

A risk assessment answers three questions: *Scenario*: What can happen? *Probability*: How likely is it to happen? *Consequences*: What are the consequences if it happens? Examining the latter two elements over the entire space of possible scenarios results in a probabilistic description of the consequences.

In addition, there are three fundamental characteristics that we require of a solid risk analysis framework:

- Disparate sources of data
- Multi-scale failure modes
- Tractability from bottom-to-top-to-bottom

Notice that there is no requirement that our methodology track epistemic and aleatory uncertainties. In the new framework we are less concerned with the type of uncertainty, and we avoid introducing errors by focusing on identifying the source of the uncertainty. Hence the emphasis on tractability. We need the capability to roll-up uncertainties from lower to successively higher level analyses, and then relate the uncertainty in the final launch risk statement down to specific uncertainties at the lower levels. Figure 1 depicts a *typical* breakout of different possible uncertainty types used in the risk analysis.

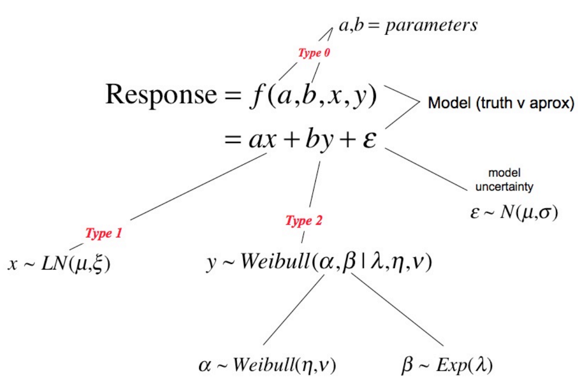

Figure 1. Typical Uncertainty Types

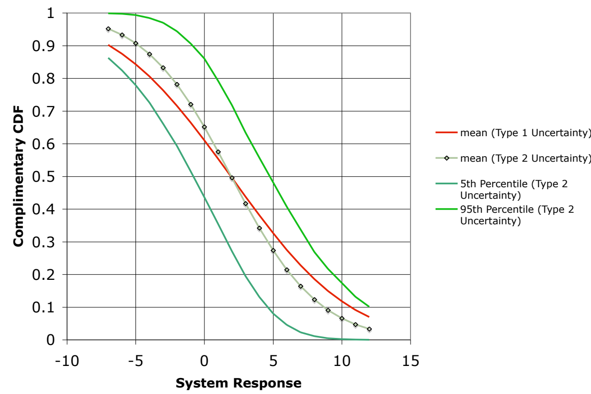

Figure 2. Typical Uncertainty Combination

Test and operational data are extremely limited and it is necessary to combine results from computer models, laboratory testing, and expert opinion. This integration must be done carefully with an appreciation of the limitations of each data source. Figure 2. depicts how each of the different uncertainty types manifest themselves on a CCDF.

Alternative Frameworks: The MSL rover design uses a Radioisotope Thermoelectric Generator (RTG) to provide continuous power on the Martian surface. A number of different approaches to estimating uncertainty in launch safety risk assessment have been proposed or applied in the past. These include the convolution-deconvolution methodology developed for the Cassini risk analysis [1] and the nested/shell Monte Carlo method utilized for the Pluto New Horizons risk analysis.

At various points in the analysis, risk characterization involves continuum mechanics modeling, thermal response modeling, reentry response modeling, accident analysis, atmospheric transport and dispersion modeling, and modeling of radiological consequences.

Risk Analysis: A discrete set of possible accident initiating events is identified, along with estimates for probabilities of those events, and the uncertainty in the event probabilities.

Accident Definition: Event information includes a time history and flight profile. For example, the range of times during the flight profile during which a particular accident scenario is possible, the component(s) in the launch vehicle that fail, and a statistical description of the characteristics of the environment that the payload might see during such an accident. These accidents are identified as a Representative Accident Scenario (RAS).

Source Term Generation: Given each of these discrete initiating events, Sandia analysts run a computer simulation (LASEP) to propagate the initiating event through the launch system and capture the response of the system to the event. Repeated Monte Carlo simulations are performed over possible accident environments and resulting system configurations, e.g. development of a fire pool, attitude of the vehicle at impact, etc. Each simulation collects data on the state of the RTG to determine if the RTG is breached, and, if so, the mass, location, and particle size distribution of material released.

Each accident scenario may lead to various combinations of air and ground-based fuel releases and fireball conditions. The characteristics of each release are tracked (air, air/fireball, ground, ground/fireball) for mass, particle size distribution, and other important characteristics. The various data are used to construct uncertainty distributions for the system state at the conclusion of the accident scenario.

Consequence Evaluation: These probability distributions of the system state are then sampled, and coupled with a random sample of possible weather conditions that might exist at the launch site. This information is then passed to the consequence analysis for input to the Space Accident Radiological Release and Consequences (SPARRC) code. The SPARRC system consists of a suite of codes to evaluate the consequences of different classes of release scenarios.

The SPARRC code system is deterministic in nature. A source term input is sampled from the LASEP output distributions (mass of fuel released in each particle size category, altitude, etc.). Coupled with a random sample of weather conditions, the SPARRC consequence suite calculates doses and health effects to exposed populations based on population density, land usage, and food production and consumption patterns. Consequence uncertainty is constructed via repeated sampling of the input variables provided as output by LASEP and possible weather conditions.

Risk Integration: In summary, an accident scenario is chosen, the results from that that scenario are simulated many times using LASEP, and the resulting consequences for that accident scenario are estimated by repeatedly sampling LASEP output, coupled with possible weather conditions at the time of the accident, and assessing the resulting population exposure health effects. This culminates in a complimentary cumulative distribution function (CCDF) for the health effects for a particular accident scenario. In addition, due to the manner in which uncertainty is modeled, credibility intervals about the CCDF are also available. These CCDFs provide the probability that any particular level of 50 year health effects will be exceeded.

Under some minor conditions, we can then construct an estimate of the CCDF for the entire launch.

Launch Risk: The goal of risk analysis is to characterize the underlying probability of specific consequences in terms of the CCDF including uncertainty bands about the CCDF at 5%, 50%, and 95%. We do not want our analysis to be dominated by assumptions regarding the underlying distribution functions: non-parametric Bayesian analysis is therefore preferred.

If the accident scenarios are mutually exclusive such that for scenarios $i \neq j$: $C_i \cap C_j = \emptyset$, then we can add the consequence risk for each scenario: $P(C_i \cup C_j) = P(C_i) + P(C_j)$. Since the risk is characterized using credibility intervals then the CCDF for the for each phase of the launch is given by:

$$CCDF\left(c_i, Phase\ j\right) = \sum_{RAS \in Phase\ j} CCDF(c_i)$$

Finally, a Dirichlet Process Prior is used to combine the CCDFs for each phase.

As a result of the MCMC analysis, we have a full characterization of the probability density function of the risk for each RAS at specific values of health consequences. Finally, since we employed a Bayesian methodology, we can roll-up the risk uncertainties for each Phase to characterize the uncertainty in the overall Mission Risk.

Acknowledgements Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. This work was supported by the DOE Office of Space and Defense Power Systems.

References:

[1] Wyss, G., 2002. "Uncertainty Analysis for the Cassini Space Mission," 6th International Conference on Probabilistic Safety Assessment and Management, San Juan, Puerto Rico, June, 2002 (SAND2002-2135).