IAC-13.D6.1.9

DETERMINING APPROPRIATE FAILURE PROBABILITIES FOR PROBABILISTIC ANALYSIS OF NEW COMMERCIAL SPACEFLIGHT VEHICLES

Chris Butt, Dan Padilha, Michael Brett, James Tisato & Shaun Wilson
Aerospace Concepts Pty Ltd
Australia
support@concepts.aero

This paper details the approach employed by Aerospace Concepts in determining Failure Response Mode (FRM) probabilities in aerospace vehicles in applying Australia's Range Safety Template Toolkit (RSTT). Special reference is made to the application of these probabilities of new commercial spaceflight vehicles. The approach is well suited to determining FRM probabilities in situations when manufacturer data on vehicle failure characteristics is not available. It employs relative probabilities of failure, along with a system level failure probability derived from historical data, to determine the absolute probability of failure of each FRM. The methodology behind failure response modes is also discussed, along with the process used in identifying them from a list of vehicle failure possibilities.

1. INTRODUCTION

In range safety analysis, the behaviour of the vehicle under failure conditions is just as important as its behaviour under nominal conditions. However, due to the inherent complexity of aerospace vehicles, the list of potential failures is typically extensive. Directly simulating each of these failures individually would not only impose a considerable effort in simulation model development but also likely make a comprehensive analysis computationally expensive or even infeasible.

RSTT is Australia's flight safety analysis system for space launch and re-entry Risk Hazard Analysis (RHA), to which this paper refers. Aerospace Concepts has presented work over several years ([1],[2],[3],[4],[5],[6]) describing the broad RSTT capability, theoretical underpinnings, operational user and regulatory needs and development approach.

RSTT offers rapid generation of mission-specific safety templates which comply with common standards for range risk criteria such as the US Range Commanders' Council (RCC) STD-321-10 [7]. This is done through the use of high-fidelity nominal and failure vehicle modelling in conjunction with massive Monte Carlo simulation.

The result is a significant amount of data across a wide range of flight behaviours, allowing potentially unknown vehicle failure characteristics to emerge, and eventually produce a comprehensive and defensible RHA.

Vehicle failure modelling in RSTT employs Failure Response Modes (FRM) to simplify an otherwise unmanageably complex (and unaffordable) task. Safety template production requires application of the respective FRM probabilities. Hence both the FRMs themselves and the probabilities must be determined through a credible and systematic approach such as the one given in this paper in order to create credible risk products for safety decision-making.

2. APPLICATION TO NEW SPACE VEHICLES

As the number of commercial organisations seeking to test and operate new space vehicles increases, the need for robust safety analysis to protect the uninvolved public becomes increasingly important, particularly to build and maintain public confidence in commercial spaceflight.

Despite the best efforts of designers and operators, there will always be failures and some of these will have a major impact on the operator concerned or even the wider industry. Based on the author' own experience, the potential impact of failure will be particularly severe when highly unexpected ('black swan' events) and catastrophic loss of life or property occurs or is only narrowly avoided.

Working outside the military system for development and test of new vehicles brings additional challenges, in particular meeting the regulatory requirements in a civil jurisdiction. This paper presents a model for appropriately defining and quantifying potentially unknown vehicle failure characteristics. This is particularly challenging for new vehicles and vehicle classes as a flight history is yet to be established.

A simple sounding rocket is used as a proxy example, but can readily applied to larger programs such as Orbital Sciences Corporation's Antares light launch vehicle or Arianespace's new Vega launch vehicle.

Figure 1. Overview of range safety template generation process using RSTT

3. RSTT SAFETY ANALYSIS PROCEDURE

The generic RSTT process for generating or verifying range safety templates is shown in Figure 1. The template production method involves creation of a six degrees-of-freedom (6DOF) model of the vehicle of interest from available technical data. This model includes both nominal and off-nominal (failure) behaviours. The failure behaviours modelled are the FRMs. The model is simulated across a range of conditions using Monte Carlo analysis, where many runs are executed with random draws for each of the defined inputs.

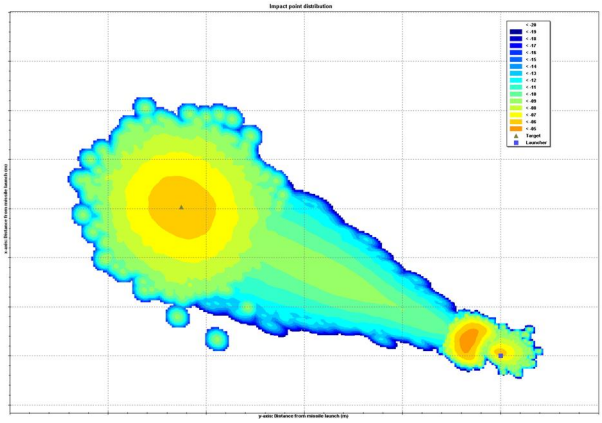

Figure 2. PDF generated from ground impacts

The outputs of those simulations, commonly called Ground Impact Points (GIPs), are statistically processed to create Probability Density Functions (PDFs), as shown in Figure 2, and hence range safety templates. Importantly, RSTT does not assume any underlying distribution of impacts, and lets the shape of the PDF emerge from the numerous Monte Carlo simulations.

4. FAILURE RESPONSE MODES

The key to making the failure analysis process tractable, and computation times acceptably short, is the FRM concept which recognises that many failures often result in the same overall system behaviour. An FRM identifies the immediate response of the vehicle to a given failure or group of failures, which can then be modelled in the 6DOF simulator. For example, in a liquid rocket engine, a failure in the igniter, or a valve, or the turbo pump assembly can all cause the engine ignition process to fail, with potentially catastrophic results. Rather than modelling each of these failures individually, they are grouped together into a 'motor ignition failure' FRM, such that all three failures result in the same or very similar vehicle behaviour.

The modelling of these responses is used to produce an RHA, which reflects the outcomes of the vehicle trajectory based on both the nominal and failure behaviour. It is necessary to determine a comprehensive list of FRMs in order to adequately cover the range of potential outcomes of the vehicle trajectory; thereby producing a credible assessment of risk to the general public, mission personnel and assets on the range.

5. PROBABILITY DETERMINATION

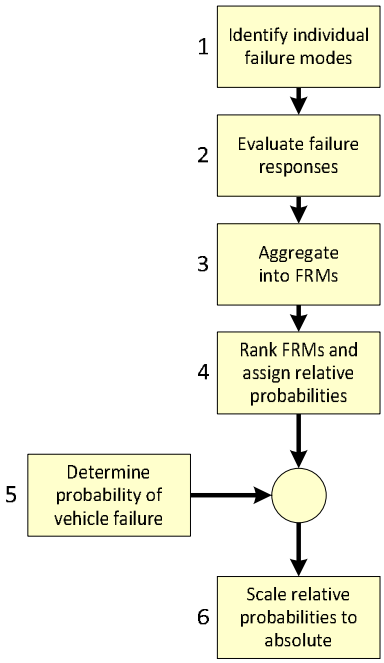

Figure 3. FRM probability development process

RSTT uses a 'top-down' process for probability determination as illustrated in Figure 3 and expanded in Sections 6 through 11:

1. Individual modes of failure of the vehicle are identified using known or derived data.
2. Each failure is analysed and the expected immediate response of the vehicle is determined.
3. Similar failure immediate responses are combined to produce a set of unique FRMs.
4. These FRMs are ranked and a relative probability value is assigned to each.

5. The probability of an overall vehicle failure is determined from historical performance or by other means.
6. The overall vehicle failure probability is then used to scale the relative probabilities to produce an absolute probability for each FRM.

This process is an iterative one where refinements at each stage improve accuracy and/or efficiency. Furthermore, given that the process relies heavily on engineering judgement, there is considerable scope for the introduction of supporting analyses and flight data.

6. STEP 1 – FAILURE MODE IDENTIFICATION

The list of potential failures for most aerospace vehicles is extensive. To determine a suitable FRM set for a vehicle, individual sub-system and component failures must be analysed in order to determine their effect on the overall vehicle. As the analysis progresses, trends emerge in the overall system behaviour that are associated with different failures.

Identification of credible failure modes is best done using Original Equipment Manufacturer (OEM) data. For expensive and/or complex systems manufactured in quantity, such as guided missiles, the method is usually straightforward (if laborious) as the OEM will have already performed detailed testing and failure analysis from which credible failure modes can be derived.

However, sounding rockets and other lower-cost vehicles do not typically undergo rigorous failure testing due to the associated impracticality and cost. In such cases a detailed analysis must be performed in order to determine the likely failure modes of such a vehicle. This is a difficult and costly procedure and requires specialist knowledge in conjunction with vehicle design information. In such circumstances, reference can be made to vehicles of similar classes and the failure modes applicable to them.

Failures will only be considered if they pose a hazard to personnel, property or areas of concern. Failures must be 'credible and foreseeable' and have a contribution to the eventual safety template (i.e. sufficiently unlikely failures are ignored). Making these choices is guided by experience and the risk thresholds defined in standards such as RCC STD-321-10. The exact causes and details of failures are unimportant, only the general nature of the failure and the vehicle response; hence, only unique failure modes need to be identified.

7. STEP 2 – EVALUATION OF FAILURE RESPONSES

The response of the vehicle to the failure mode and the characteristics of the failure are then analysed. This is initially done using knowledge and experience from area specialists and as much OEM data as can be obtained. Failure Mode, Effects, and Criticality Analysis (FMECA), in particular the effects data, is also used where available, for a more accurate evaluation.

As a part of the iterative process, the evaluation of failure modes can also involve simulation runs, whereby any similar failure behaviours that emerge can be observed and aggregated. For example, we might find that two seemingly different immediate vehicle responses actually give an almost identical behaviour when simulated, in which case we might aggregate them together to save computer run time.

8. STEP 3 – AGGREGATION INTO FRMS

Similar responses of the vehicle to individual failures are classified into unique FRMs. This aggregation process requires a balance of minimising workload through combining sufficient failure modes, while at the same time not over-aggregating so that the FRM becomes difficult to model without making significant assumptions.

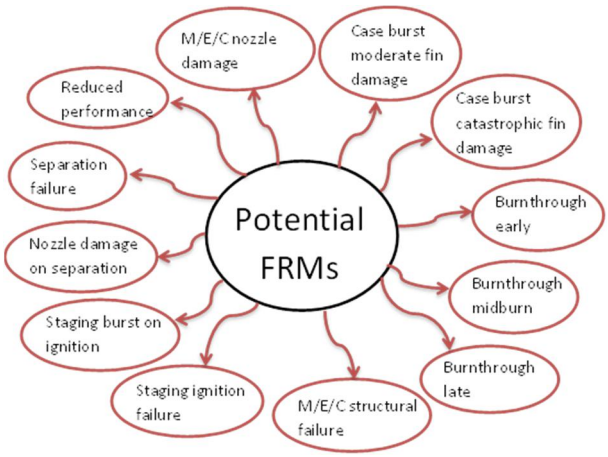

Figure 4. Potential FRMs for a high-altitude sounding rocket

The potential FRM set resulting from failure of a high-altitude sounding rocket is shown in Figure 4. Note that in the figure 'M/E/C' denotes '*Moderate* / *Extreme* / *Catastrophic*' where the three cases are individual FRMs in the actual analysis.

Once the full list of FRMs has been compiled, it should be reviewed and any FRMs which are unlikely to affect the eventual safety template be removed.

9. STEP 4 – DETERMINING RELATIVE FRM PROBABILITIES

Once all applicable failure behaviours have been accounted for in their respective FRMs, probabilities need to be assigned accordingly. Ultimately each FRM is assigned an absolute probability of failure which defines the likelihood of the failure occurring during the mission. The RHA is based upon Monte Carlo simulations of all possible vehicle behaviours including nominal and failure modes, whose impact is

driven by these failure probabilities. To satisfy application of the RCC STD-321-10 standard for risk analysis, the failure probabilities applied must be demonstrably conservative.

There are two primary sources of information used to determine the probability of occurrence for each FRM, which are the same as in determining each FRM as above. They are; using OEM data or through in-house derivation. Again, it is preferable to use any available OEM data or data from similar vehicle classes, as the latter procedure is a costly one.

Naturally, the probability of occurrence for any given FRM is the sum of the absolute probabilities for all the individual failure modes that produce that unique response. Thus the probability of vehicle failure would ideally be found be summing all the individual failure probabilities (all the FRMs) up to give a vehicle level failure probability, in a 'bottom-up' approach. These individual probabilities can be found from OEM data or through a quantitative FMECA approach. However as stated previously, such data is generally not available for one-off vehicles, so a different approach is required.

In RSTT, the approach taken is to examine the final list of FRMs and, using OEM data and/or specialist knowledge, assign a relative probability value to each. For example 'stage one reduced performance' may have a relative probability of failure of 100, compared to 'stage two ignition failure' which only has a relative probability of 10. This means that it is 10 times more likely that stage one will exhibit reduced performance than stage two is to fail in ignition.

The determination of relative probabilities, if OEM data is unavailable, relies almost entirely upon specialist engineering judgement. This is one of the weaker points of the approach, and a more rigorous method is desired, however none are known to be available. Nevertheless, the overall approach is sufficiently robust given the conservative nature of the overall RHA and each successive application helps to further consolidate the process.

10. STEP 5 – DETERMINING THE OVERALL VEHICLE PROBABILITY OF FAILURE

In order to scale the relative probabilities to an absolute value able to be used in risk analysis, an overall probability of vehicle failure is required.

For existing vehicle models which have flown numerous times (common with sounding rockets), previous flight data is used to determine this overall probability of failure. This is done by assessing the historical performance of that vehicle, including previous number of flights made and the outcomes of those flights. If the vehicle is slightly different to previously flown configurations, then global historical data for a similar class or classes of vehicles is used.

If a new vehicle with no analogous launch history is being analysed then determining a reasonable probability of failure becomes much more subjective. Wilde [8] provides an evidence-based approach for making an assessment of failure probabilities for new expendable launch vehicles based on operator experience. We have adopted this as the basis of overall probability of vehicle failure where applicable and unless the operator can provide an appropriate alternative.

In either approach used, the final system value chosen should be conservative and defensible.

11. STEP 6 – SCALING RELATIVE PROBABILITIES TO ABSOLUTE

Once the overall system failure probability of a vehicle is known, it can be applied to the relative probabilities via a scaling method to determine the absolute probability of failure of each FRM. The use of scaling to a known global historical value ensures that the failure modes end up producing a realistic system failure probability.

This scaling is done by dividing the system probability of failure by the sum of the relative probabilities of failure, which gives a 'scaling factor'. Each FRM probability is then multiplied by this scaling factor to produce its absolute probability. It can be seen that when the absolute probabilities of all the FRMs are summed, the result is the probability of failure of the system as determined in the previous step. This is the desired result, as now each FRM, which has been defined to be credible and significant, has been allocated an absolute probability of failure which is both realistic and defensible.

As an example, consider a vehicle with a system probability of failure of 10% and two FRMs each with relative probabilities of failure 10 and 100 respectively. The 'scaling factor' is found as 0.1 (10%) divided by the total relative probability of 110 (10+100), giving 0.00091. By applying this scaling factor, the absolute probability of failure for the two FRMs is thus found to be 0.0091 and 0.091 respectively. The sum of these probabilities is 0.1, verifying that the system probability of failure is equal to 10%.

12. APPLYING PROBABILITIES OF FAILURE FOR RISK HAZARD ANALYSIS

Once the absolute probabilities of failure have been determined for each FRM, they need to be applied to simulation outputs to generate a number of risk products.

Each FRM is simulated X times to produce Y Ground Impact Points (GIPs) (Y > X due to staging and debris impacts). X is chosen to be as large as possible while still achieving reasonable total simulation runtime. Monte Carlo simulation ensures that each time an

FRM is simulated it produces a slightly different set of GIPs.

The GIPs are statistically processed to generate an unweighted PDF for debris impact on the ground, an example of which is given in Figure 2. No standard distribution type is assumed; rather, the shape of the GIP distribution emerges from massive Monte Carlo simulation of each FRM, and the PDF is calculated using Kernel Density Estimation (KDE) across a discrete grid of cells. The size of the cells defines the resolution of the PDF. In each cell, a Gaussian distribution of appropriate bandwidth is applied to each GIP that exceeds the user-defined kinetic energy threshold.

These distributions are summed by superposition and appropriately normalised to form an overall probability density of impact in that cell, as shown below in Figure 5. The PDF created is therefore measured 'per unit area', and gives the probability density of a piece of debris impacting within that area.

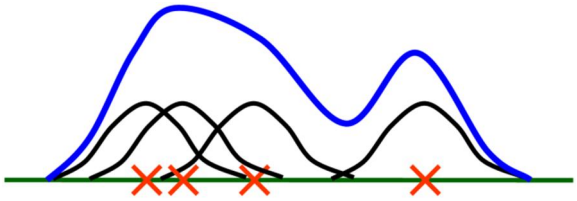

Figure 5. Kernel Density Estimation

The resulting PDF is then scaled to the absolute probability of failure for that FRM, as determined in Section 11. This is done for each FRM PDF, noting that the nominal flight of the vehicle is modelled in much the same way as a FRM. These PDFs are then combined through superposition to give the overall mission PDF – considering the nominal flight and all included FRMs.

13. 3-STAGE SOUNDING ROCKET EXAMPLE

Table 1 below describes a number of the FRMs that would be used for a generic three-stage sounding rocket. Also included are the behavioural response of the vehicle for the given FRM, and both the relative and absolute probabilities of the failure occurring.

The overall probability of failure for the vehicle was set to 10%, a value derived from extensive US and European flight histories of particular sounding rocket types. This is therefore considered appropriate for an experienced operator using this generic class of well-proven sounding rockets.

The resulting scaling factor (K_{Scale}) is:

$$K_{Scale} = \frac{System\ Failure\ Probability}{\sum Relative\ Probabilities}$$

$$K_{Scale} = \frac{0.1}{560.5} = 0.000178$$

Table 1. FRM data for a 3-stage sounding rocket

Affected component		Failure Response Mode	Relative $p_{failure}$	Absolute $P_{failure}$	Behaviour response
Stage 1 motor	Propellant	Reduced performance	100	0.01784	Reduction in thrust
	Nozzle	Nozzle damage (moderate)	6	0.00107	Increased dispersion
		Nozzle damage (extreme)	3	0.00054	
		Nozzle damage (catastrophic)	1	0.00018	
	Casing	Burst (moderate fin damage)	1.4	0.00025	Stage 2 fin damage
		Burst (catastrophic fin damage)	0.6	0.00011	
		Burn-through (early)	14.2	0.00254	Randomised time of flight
		Burn-through (late)	5.77	0.00103	
Stage 1 fin can	Fins	Structural failure (moderate)	30	0.00535	Randomised failure time
		Structural failure (extreme)	15	0.00268	
		Structural failure (catastrophic)	5	0.00089	
Stage 2 motor	Initiator	Ignition Failure	10	0.00178	No stage 2 ignition
	Propellant	Reduced performance	100	0.01784	Reduction in thrust
	Nozzle	Nozzle damage (moderate)	1.2	0.00021	Increased dispersion
		Nozzle damage (extreme)	0.6	0.00011	
		Nozzle damage (catastrophic)	0.2	0.00004	

Affected component		Failure Response Mode	Relative $p_{failure}$	Absolute $P_{failure}$	Behaviour response
		Nozzle damage (on separation)	10	0.00178	Increased dispersion at separation point
	Casing	Burst (early)	0.364	0.00006	Randomised failure time
		Burst (late)	1.14	0.00020	
		Burst (on ignition)	1	0.00018	
		Burn-though (early)	2.43	0.00043	Randomised time of flight
		Burn-though (mid-burn)	4.70	0.00084	
		Burn-though (late)	2.87	0.00051	
Stage 2 fin can	Fins	Structural failure (moderate)	60	0.01070	Randomised time of flight
		Structural failure (extreme)	30	0.00535	
		Structural failure (catastrophic)	10	0.00178	
Inter-stage	Separation	Mechanism failure	10	0.00178	Randomised flight time
Stage 3 motor	Initiator	Ignition Failure	10	0.00178	No stage 3 ignition
	Propellant	Reduced performance	100	0.01784	Reduction in thrust
	Nozzle	Nozzle damage (moderate)	1.2	0.00021	Increased dispersion
		Nozzle damage (extreme)	0.6	0.00011	
		Nozzle damage (catastrophic)	0.2	0.00004	
		Nozzle damage (on separation)	10	0.00178	Increased dispersion
	Casing	Burst (early)	0.5	0.00009	Randomised failure time
		Burst (late)	0.5	0.00009	
		Burst (on ignition)	1	0.00018	
		Burn-through (early)	2.75	0.00049	Randomised time of flight
		Burn-through (mid-burn)	4.59	0.00082	
		Burn-through (late)	2.66	0.00047	
Vehicle	**All**	**All**	**560.5**	**0.09997**	**All**

14. FUTURE DEVELOPMENT

As with many similar toolkits, RSTT is continually being revised and improved with each application that reveals an aspect not previously considered or accounted for.

As mentioned previously, one area of ongoing concern is the assignment of relative probabilities. For launch vehicles in RSTT so far, this process has relied almost entirely on experts with specialist technical knowledge of the vehicles, their design and behavioural characteristics. Ideally, this database would be expanded to include directly more assessments from vehicles manufacturers. This would add confidence and help to improve the fidelity of the procedure.

The approach used in RSTT to determine the system level failure rate of a vehicle, described in Section 10, draws on reliable historical data sources in conjunction with FAA and ACTA methodologies; however, the process in not yet mature. Benefit would come from having a well-structured, formalised approach to determining an overall vehicle failure rate, which could be applied to all possible cases.

15. CONCLUSIONS

The need for robust safety analysis of commercial spaceflight vehicles to protect the uninvolved public is becoming increasingly important, particularly to build and maintain public confidence in commercial spaceflight.

The RSTT approach to making an estimate of failure probabilities offers a reasonable and defensible basis for determining risk when OEM or FMECA data is unavailable or cost-prohibitive to acquire. This is done by applying relative probabilities to each FRM, and scaling them with a system level failure probability, determined using historical data for that type of vehicle. Thus the FRMs and their respective probabilities can be determined for individual use in RHA, while still giving an appropriate system level failure rate.

Some aspects of the approach rely upon specialist vehicle knowledge, and more OEM data in these areas would help improve fidelity. Also a more formalised approach to system failure rate probabilities is another area that will continue to develop over time.

16. REFERENCES

1. Tisato, J.T., Vuletich, I.J., Brett, M.S., Williams, W.R. & Wilson, S.A. (2011). *Improved Range Safety Analysis for Space Vehicles Using Range Safety Template Toolkit*, 5th IAASS Conference, Versailles, France.
2. Wilson, S.A., Vuletich, I.J., Bryce I.R., Brett, M.S., Williams, W.R., Fletcher, D.J., Jokic, M.D. & Cooper, N. (2009). *Space Launch & Re-entry Risk Hazard Analysis – A New Capability*, 60th International Astronautical Congress (IAC), Daejeon, Korea.
3. Wilson, S.A., Vuletich, I.J., Fletcher, D.J., Jokic, M.D., Brett, M.S., Boyd, C.S., Williams, W.R. & Bryce, I.R. (2008). *Guided Weapon Danger Area & Safety Template Generation – A New Capability*, AIAA Atmospheric Flight Mechanics Conference, Honolulu, Hawaii, USA.
4. Jokic, M.D, White, T., Fletcher, D.J., Wilson, S.A. & Vuletich, I.J. (2007). *Guided Weapon Danger Area Generation – Australian Capability Development*, International Range Safety Advisory Group, Amsterdam, The Netherlands.
5. Fletcher, D.J., Jokic, M.D. & Graham, R.F. (2007). *DSTO Approach to Standoff Weapon Danger Area Generation*, International Range Safety Advisory Group, Amsterdam, The Netherlands.
6. Fletcher, D.J., Wilson, S.A., Jokic, M.D. & Vuletich, I.J. (2006). *Guided Weapon Safety Trace Generation – Implementing a Probabilistic Approach*, AIAA Atmospheric Flight Mechanics Conference, Keystone, Colorado, USA.
7. United States Range Commanders Council (2010). *Common Risk Criteria Standards for National Test Ranges*, RCC Standard 321-10, Secretariat Range Commanders Council, White Sands Missile Range, New Mexico, USA. [and associated supplement]
8. Wilde, P.D., (2011), *Probability of Failure Analysis for new Expendable Launch Vehicles*, 3rd IAASS Workshop on Launch and Re-entry Safety, Paris, France.