STI 10-027

An Accident Precursor Analysis Process Tailored for NASA Space Systems

Frank Groen[a], Michael Stamatelatos[a], Homayoon Dezfuli[a] and Gaspare Maggio[b*]
[a]Office of Safety & Mission Assurance, NASA, Washington, D.C.
[b]Technology Risk Management Operations, ISL, New York, NY

Abstract: Accident Precursor Analysis (APA) serves as the bridge between existing risk modeling activities, which are often based on historical or generic failure statistics, and system anomalies, which provide crucial information about the failure mechanisms that are actually operative in the system and which may differ in frequency or type from those in the various models. These discrepancies between the models (perceived risk) and the system (actual risk) provide the leading indication of an under-appreciated risk. This paper presents an APA process developed specifically for NASA Earth-to-Orbit space systems. The purpose of the process is to identify and characterize potential sources of system risk as evidenced by anomalous events which, although not necessarily presenting an immediate safety impact, may indicate that an unknown or insufficiently understood risk-significant condition exists in the system. Such anomalous events are considered accident precursors because they signal the potential for severe consequences that may occur in the future, due to causes that are discernible from their occurrence today. Their early identification allows them to be integrated into the overall system risk model used to inform decisions relating to safety.

Keywords: Anomalous Conditions, Accident Precursor Analysis, Anomaly Risk Significance

1. INTRODUCTION

The Accident Precursor Analysis (APA) process presented herein provides a systematic means of meeting the relevant requirements within NASA Procedural Requirement (NPR) 8715.3C, *NASA General Safety Program Requirements* [1] by evaluating anomaly occurrences for their system safety implications and, through both analytical and deliberative methods, identifying those that portend more serious consequences to come if effective corrective action is not taken. APA builds upon existing safety analysis processes currently in practice within NASA, leveraging their results to provide an improved understanding of overall system risk. As such, APA represents an important dimension of safety evaluation; as operational experience is acquired, precursor information is generated such that it can be fed back into system safety analyses to risk-inform safety improvements.

The purpose of the APA process is to identify and characterize potential sources of system risk for which indications are received in the form of anomalous events which, although not necessarily presenting an immediate safety impact, may indicate that an unknown or insufficiently understood risk-significant condition exists in the system. Such anomalous events are considered accident precursors because they signal the potential for more severe consequences that may occur in the future, due to causes that are discernible from their occurrence today. Their early identification allows them to be fully scrutinized and the results to be used to inform decisions relating to safety. In addition to a systematic analysis of the anomalous event that was actually observed (a hallmark of all APA processes including the NRC process used as a point-of-departure), the NASA process also invokes an "imaginative" aspect to the process using a structured brainstorming session to identify similar anomalous conditions which could have more severe consequences than the observed anomalous event. In the context of NASA systems, the term severe consequences typically refers to loss of crew (LOC), loss of vehicle (LOV), or loss of mission (LOM). It is up to the particular project employing the approach to define severe consequences appropriate to its objectives and apply the technical approach accordingly. For instance, science missions may consider loss of science (LOS) to be a severe consequence.

*Email address for contact author: gaspare.maggio@islinc.com

The APA process presented in this document is specifically tailored to Earth-to-Orbit Space Transportation Systems, although the fundamental process steps are valid for other mission classes (e.g., manned and unmanned orbital platforms, manned lunar and planetary outposts, deep-space robotic missions, and other human space exploration missions), and may be tailored to the specific needs of each class. Current programs at NASA that can benefit from the APA process presented in this document include the Space Shuttle, certain Constellation systems, and (with appropriate tailoring) the International Space Station. In addition, NASA is continuing to exercise a robust terrestrial and solar system satellite and robotic based science agenda that would benefit from a systematic accident precursor analysis process. In this case, an accident precursor process could provide valuable information to guide the design of future scientific missions as well as indicate when corrective actions are required during the mission to preclude potential mission-ending failures. APA guidance focusing on these other mission classes is expected to be produced in the near-future.

2. FUNDAMENTALS OF ACCIDENT PRECURSOR ANALYSIS

The Swiss Cheese model of accident causation, originally proposed by James Reason [2], likens a system's defenses against severe failure as a series of slices of randomly-holed Swiss Cheese arranged vertically and parallel to each other with gaps in between each slice. Each slice could represent a safety process, preventative maintenance, a subsystem, adverse environmental condition, etc. The holes represent latent conditions, possible severe stresses, opportunities for human error, or simply specific subsystem failures. Essentially, the holes in the cheese slices represent individual weaknesses in the system to various events and conditions, and are continually varying in size and position in all slices. Using the Swiss Cheese model, an accident can be represented as a trajectory through a momentary alignment in a set of holes (as shown by the red line in Figure 1). In other words, a failure mechanism can sequentially negotiate these holes thus compromising a barrier meant to obviate catastrophe and snowball to a full-blown accident. Whenever a failure mechanism manages to make it through one or more holes, but not all, it is effectively deflected from continuing to a severe consequence (as shown by the blue line in Figure 1) and it is cataloged as an *anomaly*.

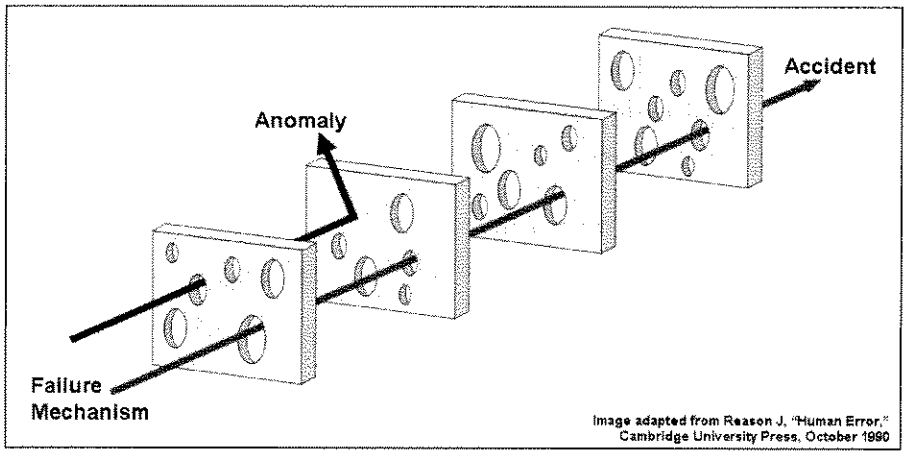

Figure 1: "Swiss Cheese" Model to Accident Causation

Therefore an *anomalous event* makes an organization aware of weaknesses in the system that may, in combination with other potential weaknesses, lead to a severe consequence. If there is indeed potential for more weaknesses to align with the observed weaknesses in such a way to lead to an accident, then the event can be called an *accident precursor* since it portends the potential for more severe consequences if the failure mechanism were to recur.

Some examples of accident precursor types are:

- A near-miss because of chance or an opportune mitigation
- Faults that can become failure conditions without correction
- Unexpected trend in test or operation
- Reduced maintenance effectiveness
- Unexpected effects from aging of equipment
- Common causes of faults or deteriorations

Three well-known examples of accident precursors are:

- O-ring blow-by at Space Shuttle Solid Rocket Booster (SRB) joint locations, prior to the loss of the Challenger;
- Foam loss from the Space Shuttle External Tank (ET) and Space Shuttle Thermal Protection System (TPS) debris damage, prior to the loss of Columbia;
- Increased containment air filter flow-rate deterioration, prior to the discovery of significant vessel head erosion at the Davis-Besse nuclear power plant.

Accident precursor analysis (APA) is the process by which an organization evaluates observed anomalies and determines if their risk significance is indicative of a potential accident precursor. There is no one way to conduct APA, but all APA processes should evaluate operational and/or test experience to identify unrecognized accident potential or underappreciated vulnerabilities, so that something can be done about them *in a timely manner*[†].

3. NASA ACCIDENT PRECURSOR ANALYSIS PROCESS OVERVIEW

APA establishes a systematic process for risk significance-based evaluation of operational and test anomalies by:

- Screening observed anomalies for the need to perform an evaluation
- Postulation of anomalous conditions related to the original anomalous event
- Evaluating and grading anomalous conditions for further analysis
- Performing detailed analysis of selected anomalous conditions

The NASA APA process may be applied as soon as there are anomalous events that will impinge upon the current or impending operation of a particular system. In some cases this may be as early as the preliminary design review (PDR) in the development portion of the system life cycle. For instance, if the design solution at PDR includes heritage equipment from previous NASA programs/projects or even external applications of that equipment, the anomalies that have historically occurred on that

[†] "In a timely manner" is a matter to be determined by the organization overseeing the system (as will be discussed in subsequent sections) but basically is defined by the end result – which is the avoidance of an accident due to a recurring failure mechanism.

equipment can be evaluated to determine what, if any, risks they portend for the system being designed. Once prototype subsystems begin testing, usually between PDR and the critical design review (CDR), test anomalies can be evaluated to both inform the Failure Modes & Effects Analysis (FMEA) as well as integrating the results of the APA into any nascent system risk models. The combined findings can, of course, be utilized to effect design changes that may eliminate or mitigate unacceptable risks early in the design process when the cost of making those changes is relatively low. After the system begins operation, it is prudent to continue applying the APA process to root out under-appreciated risks and to identify new risks that crop up as the system processes, missions, and operating environments change, or in the case of reusable systems, as they simply begin to show signs of degradation due to aging.

Figure 2 presents a high-level view of the conceptual framework of NASA's APA approach. The process begins with a review of anomalous events as reported in existing databases [e.g., Problem Reporting and Corrective Action (PRACA) database], and a screening out of those events that can be judged by either manual or automated inspection as having no practical relationship to any potentially risk-significant condition existing in the system of interest. This is necessary because almost any such database will tend to include many reports of no real interest to an APA, and it is important not to spend too much effort on such reports.

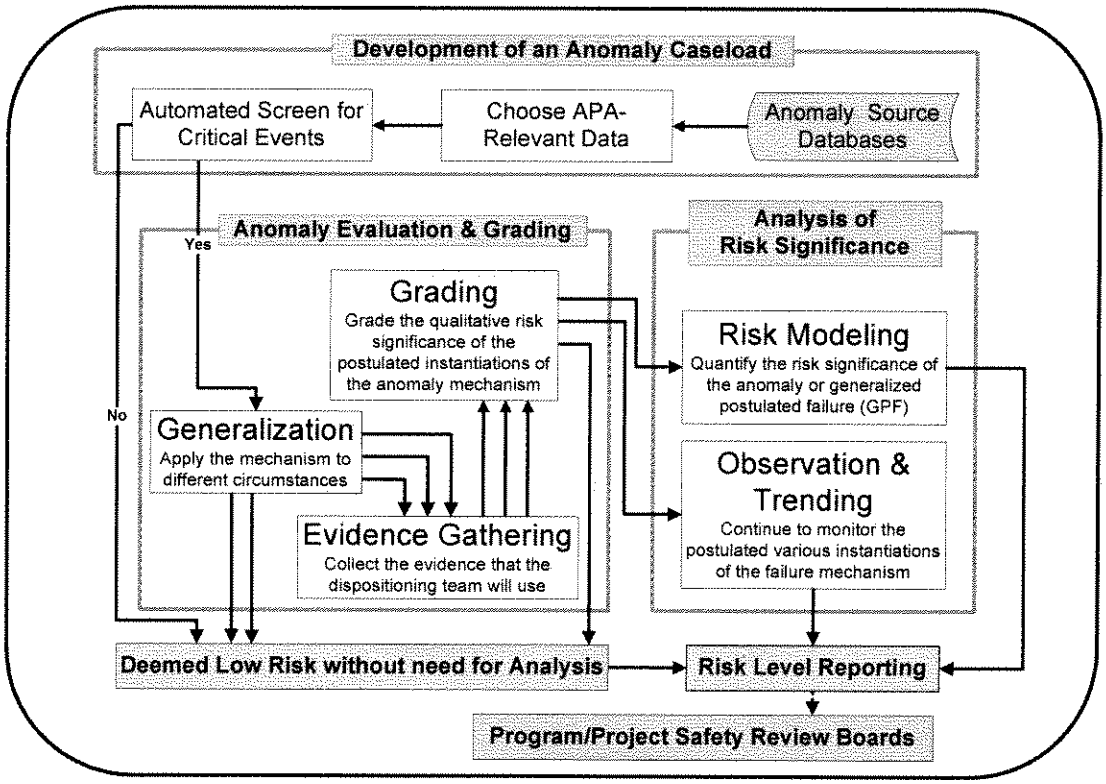

Figure 2: NASA Accident Precursor Analysis Process Overview Diagram

3.1. Generalization

Events surviving this preliminary screen, meant to include all but the most clearly non-risk significant events (to minimize false negatives), are assessed for their causal failure mechanisms. These mechanisms are then generalized to different circumstances under which they might recur in the system, including the possibility of recurrence in different subsystems, at different times, or with different fault magnitudes. These generalized, postulated occurrences of the failure mechanism are referred to as *generalized potential failures (GPFs)*, and characterize the potential for the failure

mechanism that caused the observed anomaly to occur elsewhere in the system, with potentially more severe results.

Generalization instills within the APA process the ability to go beyond the circumstantial aspects of the anomaly *as it occurred*, to the spectrum of possible instantiations of the causal failure mechanism, i.e., *what might occur*. The scope of generalization goes beyond the immediate issue of assessing and mitigating the anomaly itself. Instead, generalization is focused on the anomaly's causal failure mechanism as it might arise in other circumstances, in order to identify design or operational vulnerabilities to the failure mechanism in a broader sense. Generalization produces a set of GPFs which, together with the anomaly itself, comprise the anomalous conditions that characterize the potential for the underlying failure mechanism to occur in the system as a whole. Anomaly generalization is illustrated in Figure 3, with the expanding cone representing the increasing number of GPFs originating from the initial anomaly review.

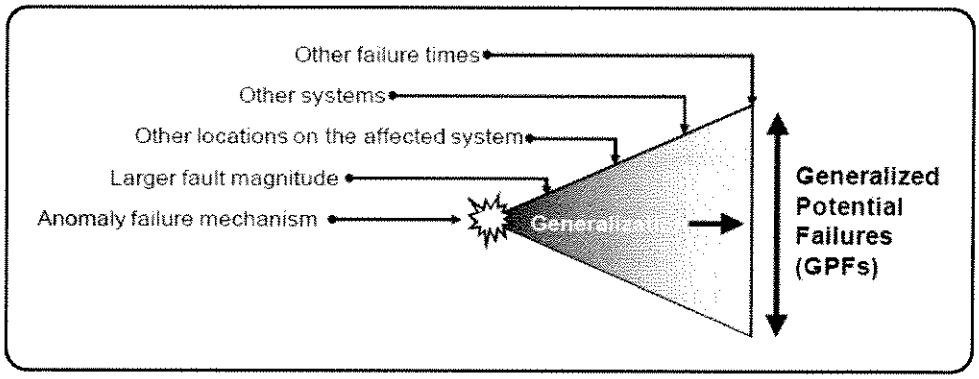

Figure 3: Anomaly Generalization Illustration

The output of generalization is a set of anomalous conditions deemed worthy of further evaluation and grading. Subsequent grading of these anomalous conditions involves an evaluation of their potential to produce severe consequences. This potential depends on the physical locations and functional roles of the affected components.

3.2. Data Gathering & Rule-Based Screening

Following generalization, data on each of the anomalous conditions is collected, as well as sufficient system-level data to evaluate the potential for actual system failure to occur, given the presence of the failure mechanism, and the potential for the failure to propagate to severe consequences. Since both anomalies and GPFs are subsumed under the general heading of anomalous conditions, the individuals or teams gathering the data treat each equally without regard to whether it is an actual anomaly or a postulated GPF. This is important since the data collectors may be swayed by the rigor they put into searching for relevant information based on whether they perceive the anomalous condition to be a "real anomaly". The data collected in this step are in addition to the anomaly-related data that have already been collected and used for purposes such as indentifying the anomaly failure mechanism.

Anomalies and identified GPFs (herein simply jointly referred to as *anomalous conditions*) are then screened using "rule-based" criteria, to eliminate those for which deterministic information can be brought to bear to demonstrate their lack of risk significance. This rule-based step is comparable to that used in the NRC precursor analysis process [3], with the significant difference that the NRC criteria have been developed over years of application.

3.2. Deliberative Grading

Since the NASA APA process is in its infancy, for those anomalous conditions that cannot be screened out as potential precursors based solely on a rule-based approach, a metric called the Potential

Problem Index (PPI) is assigned via a deliberative evaluation process, as discussed below. With time and experience, useful system-specific grading patterns may emerge that allow the evaluation process to become progressively more rule-based, but there will always be a need for eliciting expert knowledge within a structured deliberation format.

The PPI is formulated so that anomalous conditions with a high PPI warrant further investigation of the causal failure mechanism and its effect on system risk; those with a moderate PPI warrant a recommendation for continued monitoring and trending of related anomalies that share the underlying failure mechanism; and those with a low PPI are graded out of the process as being insignificant to the risk metrics being addressed.

Once an anomaly's causal mechanism has been generalized into a set of anomalous conditions and the requisite evidence has been collected, the deliberation-based grading process can be conducted. To do this, the failure condition index (FCI); and the conditional consequence index (CCI) are assigned after the underlying evidence garnered from the data collection exercise is reviewed and documented for each index assignment.

The two indices (FCI and CCI) hinge upon what is defined as the *failure condition of concern*. The failure condition of concern is a postulated failure state that could be caused by a failure mechanism acting at a susceptible location, which has the potential to propagate to severe consequences. A failure condition of concern:

- Typically corresponds to a genuine functional failure in a particular item, as opposed to that item being merely out of spec
- May vary from one susceptible location to another, even for the same failure mechanism, due to the different functions and system interactions associated with different components.
- Structures the assessment of susceptibility (and subsequent evaluation) by providing an anchor point for consideration of propagation pathways from the failure mechanism to severe consequences.

In some cases, one or both of the indices will indicate very high likelihood or even certitude (i.e., cases where the failure condition of concern did happen, or where severe consequences are certain, given the failure condition of concern). In other cases, the situation is less than certain, and needs to be evaluated. It is important to keep a scenario-based perspective in mind when assigning FCI and CCI values to make sure that they are consistent with the definition of the failure condition of concern: the failure condition of concern upon which the CCI is conditioned should be the same as that used to assign the FCI.

3.3. Evidence Caliber & Grading Results

If the data type caliber of all the data used to evaluate FCI and CCI were 100%, and all the data were strongly applicable to their respective evaluations, then the PPI could be determined directly from FCI and CCI, and in fact would simply be the sum of FCI and CCI. In reality, there is no such thing as perfect and completely applicable evidence, so PPI also takes into account the *evidence caliber* of the data set used to support FCI and CCI assignments. For decreasing evidence calibers, progressively larger positive adjustments are made, resulting in correspondingly higher PPI values for the same FCI and CCI values.

The evidence caliber itself is a function of the baseline data type calibers and assigned applicabilities of the supporting data used by the evaluation team when assigning FCI and CCI. For each piece of data, its applicability (expressed as a percentage) is multiplied by the baseline data type caliber to produce a *Data Caliber, DC*. Then, the *DC* metrics are aggregated together to produce an overall *Evidence Caliber, EC*, in the following manner:

$$EC_{FCI} = 1 - [\,(1-DC_1) * (1-DC_2) * \ldots * (1-DC_M)\,] \quad (1)$$

$$EC_{CCI} = 1 - [\,(1-DC_{M+1}) * (1-DC_{M+2}) * \ldots * (1-DC_N)\,] \quad (2)$$

$$EC_{PPI} = EC_{FCI} * EC_{CCI} \quad (3)$$

In the above equations, M pieces of data support FCI assignment (Eq. 1) and N - M pieces support CCI assignment (Eq. 2).

Equations (1) through (3) define the data caliber aggregation within a single index (EC_{FCI} and EC_{CCI}, respectively), and for the two indices combined (EC_{PPI}). Aggregation within an index is treated as a coproduct, under the principle that multiple sources of evidence contribute to an increasing confidence in the assigned value. Aggregation across the indices is treated as a product, under the principle that each index is separately supported by its evidence, so that the evidentiary support for PPI as a whole is no stronger than its weakest link. If EC_{PPI} is low then one can conclude that there is some uncertainty in PPI, and therefore the grading should be correspondingly conservative in this case.

The PPI is the grading metric for each anomalous condition which is the basis for the recommended further action as shown in Figure The grading result specifies:

- Explicit analysis, in the case of a high PPI;
- Observation and trending, in the case of a moderate PPI; and
- No further analysis, in the case of a low PPI.

For high values of evidence caliber, PPI closely matches the sum of FCI and CCI. For low values of evidence caliber, PPI is higher than the sum of FCI and CCI, indicating an upward adjustment to account for the higher uncertainty inherent in the FCI and CCI assignments.

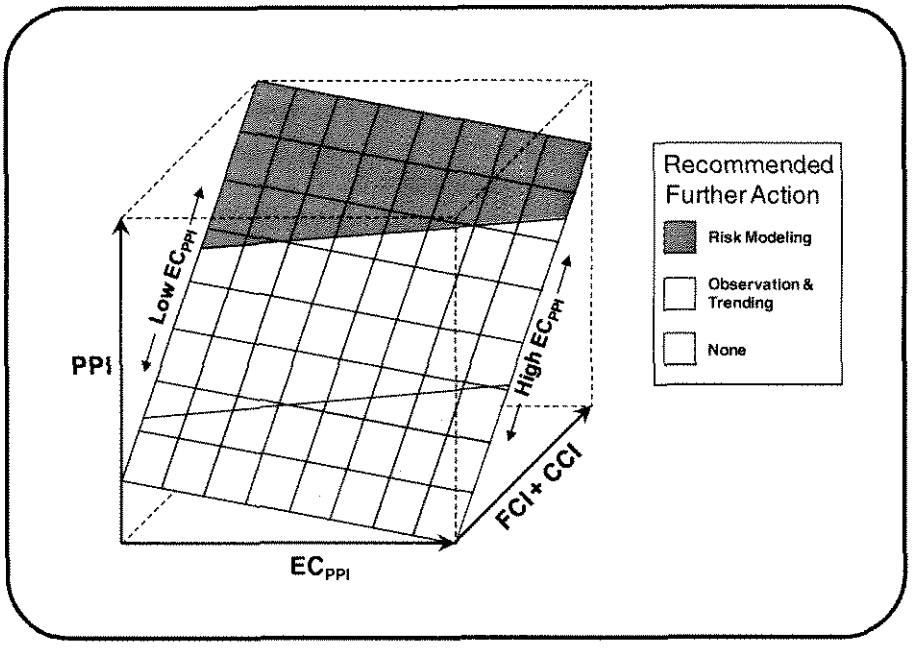

Figure 4: Notional Graph of Recommended Further Action

The lowest possible graded result simply indicates that the anomalous condition is not risk significant. The anomalous condition passed all prior screening attempts; however, upon evaluation, the assessed PPI indicates that the anomalous condition is within the safety envelope of the system and does not warrant further analysis.

If the PPI of an anomalous condition is judged not to be high enough to warrant explicit risk modeling, but also is non-negligible, then an intermediate grading recommends observation and trending of the failure mechanism to ensure (1) that the full history of the failure mechanism is brought to bear on the characterization of the spectrum of fault magnitudes; (2) that parameters correlating to anomaly occurrence and fault magnitude are identified; (3) that multiple occurrences of related anomalies (unexpected anomaly recurrence) do not pose an undue risk to the system; and (4) that adverse trends in frequency or fault magnitude are identified before they penetrate the safety envelope of the system. Once the finding is made, if the recurring problem analysis determines that the anomaly is not part of a recurring set of events, it is possible that the failure mechanism is deemed to be a low risk, or in other words "not risk significant." However, if there is anomaly trend that raises questions then additional modeling may be necessary to understand the trending pattern to ensure that the failure mechanism poses no significant risk to the system, or to redesign the system to preclude recurrence.

The highest grading possible, risk modeling, is prescribed for those circumstances where the potential for severe consequences is too high to simply continue observation and trending. Risk modeling is discussed further in the following section.

3.4. Risk Modeling

Risk modeling is prescribed for all anomalous conditions above the upper threshold for observation and trending. The rationale is that a high PPI for a failure mechanism that has received the elevated PPI warrants an understanding of its risk implications. In accordance with the graded approach to system safety modeling specified in NPR 8715.3C [1], the level of detail of the model should be commensurate with the magnitude of the risk. For example, if it is found that a risk model already exists for the anomalous condition, then the upshot of the risk modeling activity should be a potential change in the predicted frequency, reflecting the fact that elements of the affected scenarios have been observed, rather than a complete replacement of the existing risk model.

As the previous paragraph implies, the risk modeling activity is meant to leverage existing analyses wherever possible, filling in any gaps that are found. These gaps may consist of scenarios that are not currently represented, or assumptions about scenario progression that are insufficiently substantiated by evidence to be confidently relied on. Sources of analysis information include Hazard Analyses, FMEAs, Critical Items Lists (CILs), and Probabilistic Risk Assessments (PRAs).

The risk models developed as part of the APA process should be phenomenological, in that they simulate the physical phenomena involved in the progression from failure mechanism to consequence. They should also be probabilistic, in that the uncertain parameters of the model are characterized by probability density functions (pdfs) as opposed to point values. This enables explicit calculation of the probability of severe consequences in terms of the fundamental uncertainties in the phenomenology of the system. Simulation of physical phenomena under uncertainty is a known discipline, as described in references such as [4], [5] and [6], and such models are referred to in the APA process as *Parametric Probabilistic Models (PPMs).*

Parametric probabilistic modeling combines statistical inference, logic-based modeling, and parametric functions to model not only how an initiating event can propagate in a time-dependent manner to a severe consequence but also how the likelihood of transitioning from one system state to another is governed by the underlying physical parameters involved in that propagation. PPM development can be complex and challenging, but is justified in the case of APA because (1) we are focusing on specific anomalous conditions graded for risk modeling rather than attempting to build a risk model of an entire system, (2) we must understand what physical parameters are driving the risk

in order to implement effective corrective actions, and (3) if we don't understand how some of the key parameters are driving the potential accident propagation then testing/engineering analyses needs to be focused on gaining this knowledge and should be focused on characterizing the driving physical parameters.

The example in Figure 5, which presents a portion of a notional PPM, illustrates the fundamental attributes of a parametric probabilistic model. The anomaly failure mechanism (the initiating event in the sequence) produces a leak in a pipe containing flammable fluid. The functions associated with each event in the PPM, as well as the parametric connections between the events, are illustrated above the event tree. Note that the actual leak rate is uncertain, and is defined in the PPM as a pdf, *representing the distribution of leak rates, given the anomalous condition.* Combustion of the leaked fluid depends on the leak rate (e.g., a certain amount of pooling may be required, or a combustible mixture is achievable only under a certain range of leak rates). The occurrence or non-occurrence of combustion is characterized by a "fluid combusts" pivotal event, whose probability of occurrence is a function of the leak rate. If combustion occurs, the resulting temperature rise might defeat the insulation protecting a needed backup system, resulting in system failure. To model this in the PPM, an "insulation fails" pivotal event is defined whose probability of occurrence depends on temperature. Thus, within the scope of this notional example, the possible sequences of events are defined by the pivotal events, "fluid combusts" and "insulation fails."

In order to clearly indicate the significance of temperature rise in the sequence, an "insulation temperature increases" functional event is defined between "fluid combusts" and "insulation fails." This functional event takes the fluid leak rate as input and produces the insulation temperature, which is a function of leak rate, as output. Thus the probability of insulation failure is ultimately a function of the leak rate, and is therefore correlated with the anomaly fault magnitude.

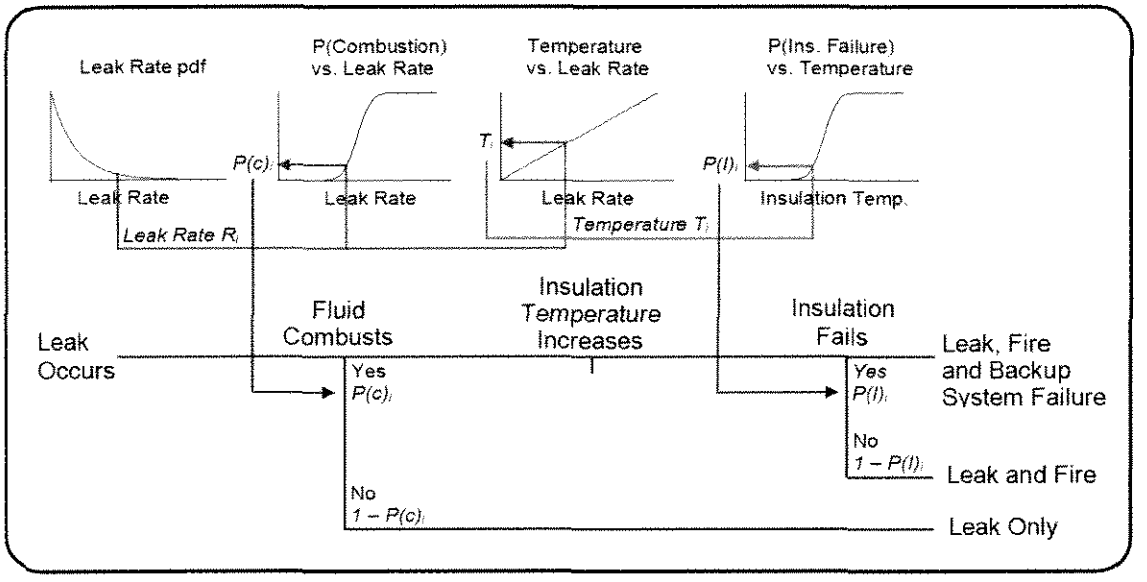

Figure 5: Parametric Probabilistic Modeling of Pivotal and Functional Events

In the APA process, the PPM is exercised to generate a number of precursor risk measures [7]. These measures are designed to assist the program/project in identifying specific system configurations, in terms of risk model parameter values, that might represent risk-significant vulnerabilities in the design, operation, or condition of the system, so that specific recommendations can be made that have the greatest potential to reduce risk. Such recommendations might take the form of additional analysis and/or testing, *in order to reduce uncertainties to the point where the anomalous condition is* adequately controlled, or they might take the form of design or operational modifications, in cases where the presence of a vulnerability is substantiated by the PPM.

The APA risk modeling process is illustrated in Figure 6.

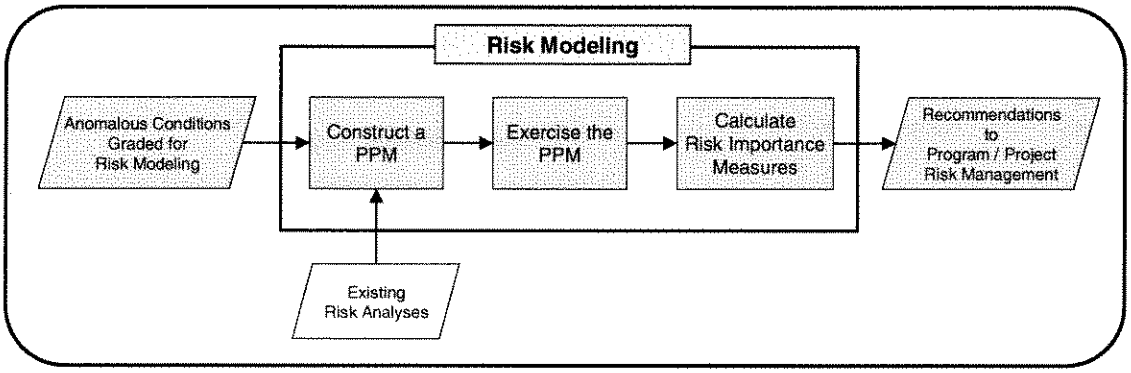

Figure 6: Risk Modeling Process Flow Diagram

4. PRECURSOR DESIGNATION

Up to this point methods and processes for evaluating and grading anomalous conditions, as well as modeling and quantifying their risk significance, have been presented, but in the end the process, by its very name, promises the identification of accident precursors. Unfortunately, you may be dismayed to learn that the process, in and of its self, cannot designate an anomalous condition as an accident precursor. This is because an accident precursor is defined not so much by the absolute values of the risk significance measures but instead by the way that those risk significance measures are interpreted by a program.

The bottom-line is that the program must define criteria by which to designate an anomalous condition (whether actually observed or postulated) as an accident precursor. It is important that once the criteria are defined, they be adhered to, since not doing so relegates the program to the subjective type of attention given to anomalies that APA is attempting to remedy. Once an anomalous condition has been designated as an accident precursor, the information garnered from the risk modeling activity provides a means of focusing program resources upon the parameters and system states that either require more information or are explicitly driving the failure propagation to severe consequences.

5. CONCLUSION

In summary, the basic principles of the NASA APA process are:

- Anomaly data may point to failure mechanisms that, under different circumstances, could result in severe consequences. The prudent response to such anomalies is to assess this potential to assure that no unknown or underappreciated risks exist in the system. The APA process generalizes from the particulars of the observed anomaly to the spectrum of potential failures that share the same failure mechanism but which may occur in more severe form, at different times, or in different subsystems.

- Given that anomaly data sources contain a significant number of events having negligible risk implications, an efficient screening method is used to eliminate these events from further consideration while minimizing false negatives to ensure potential accident precursors are not missed. Anomalies which are retained are then qualitatively graded for continued observation and trending of the failure mechanism, or explicit scenario-based risk modeling.

- An effective APA process depends on a graded approach to anomaly assessment that includes rule-based screening, qualitative assessment and quantitative modeling. Quantitative modeling is used only as needed to understand the system risk attributable to the failure mechanism.

- Evidentiary support is a key element of the process. Failure mechanism generalization involves the postulation of fault magnitudes, propagation pathways and system stresses that may not have occurred within the operational experience base of the system. Thus, uncertainties are potentially large and care must be taken to avoid mischaracterization. The APA process explicitly weighs the evidence that is used to support the characterization of risk, implying where additional testing or analysis may be beneficial.

- Anomalies are significant to the extent that they either imply performance degradation of well-understood elements or reveal risks that were underappreciated or misunderstood prior to the anomaly occurrence. APA makes use of existing risk models to ascertain the risk significance of the failure mechanism, and entails additional risk modeling as needed to understand the physical drivers of that risk.

The APA process is designed to produce actionable findings. It is expected that the findings will be available to the risk management system to support the development of risk-informed recommendations for system operation and testing, as well as assessing the adequacy of any corrective actions that may already have been taken in response to the original anomaly. Therefore, top-level metrics that measure the risk importance of the underlying failure mechanism, as well as the associated physical parameters that may contribute to a catastrophic exacerbation of that mechanism, are key to the process.

Acknowledgements

The authors would like to acknowledge the significant contributions made to this effort by Dr. William Vesely from NASA's OSMA and Christopher Everett and Anthony Hall of ISL's Technology Risk Management Operations. Their ideas in the development and implementation of the process were invaluable in bringing it to fruition.

The development of the process was also in a large part made possible by the exercises held at the Johnson Space Flight Center, which were hosted and supported by the Space Shuttle SR&QA organization managed by Roger Boyer. The authors would like to thank all of the working session participants, and in particular M. Trent Kite, Mark Veile, Mark Bigler, Bruce Reistle and Mark Valentine of NASA and Robert Bobola, William Stockton, Wallace Tuthill, Eric Thigpen, Tieva De Koninck, and Aisha Garel of SAIC. All of these individuals not only supported the detailed technical discussions, but also helped to improve the application of the approach itself, including both the format and the technical flow of the discussions. The authors would like to extend a very special thanks to Teri Hamlin in particular, not only for coordinating the exercises from NASA's side, but also for making numerous key technical and process contributions, as well as serving as discussion facilitator on numerous occasions.

The authors would also like to mention the U.S. Nuclear Regulatory Commission staff, specifically Pat Baranowsky, Gary DeMoss, and Don Marksberry, for sharing lessons learned from USNRC's application of precursor analysis to nuclear plant safety. Also included in this acknowledgement are ISL staff James Meyer, Bruce Mrowca, and Ali Azarm for assisting in formulation of the technical approach, based on ISL's history of support to the US Nuclear Regulatory Commission in precursor analysis and related areas.

Lastly, but certainly not least, the authors would like to express their appreciation to Clay Smith of APL for his comments and insights throughout the methodology development stages and for his continuing efforts to expand the application of this process. In addition, Scott Insley, is acknowledged for his editorial contributions to this document.

References

[1] NPR 8715.3C, "*NASA General Safety Program Requirements*", NASA, March 2008.

[2] Reason J, "Human Error," Cambridge University Press, October 1990.

[3] Sattison M.B., "Nuclear Accident Precursor Assessment: The Accident Sequence Precursor Program," appearing in J.R. Phimister, V.M. Bier, and H.C. Kunreuther, eds., "Accident Precursor Analysis and Management: Reducing Technological Risk Through Diligence," National Academy of Engineering of the National Academies (The National Academies Press, Washington, DC, 2003).

[4] Geisser S, Johnson W, "Modes of Parametric Statistical Inference," John Wiley & Sons, 2006.

[5] NASA Office of Safety and Mission Assurance, "Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners," Washington, DC. 20546. August, 2002.

[6] NIST (National Institute of Standards and Technology), "*NIST/SEMATECH e-Handbook of Statistical Methods*," http://www.itl.nist.gov/div898/handbook/

[7] Everett C, Maggio G, Groen F, "An Extreme-Value Approach to Anomaly Vulnerability Identification," 10th International Probabilistic Safety Assessment and Management Conference, PSAM-10, Seattle, WA. June 2010.