Socio-Technical Probabilistic Risk Assessment: Its Application to Aviation Maintenance

D.A. Marx, JD\textsuperscript{1} and J.E. Westphal\textsuperscript{2}

\textsuperscript{1}Outcome Engineering, LLC, 9805 Capilano Dr., Plano, TX, 75025 USA
\textsuperscript{2}Outcome Engineering, LLC, 9805 Capilano Dr., Plano, TX, 75025 USA

Contact author: D. Marx, dmarx@outcome-eng.com
Tel 972-359-0440

Abstract

This paper describes the process of socio-technical probabilistic risk assessment (ST-PRA). What makes ST-PRA an evolutionary step is the entire risk model is made up of human errors and at-risk behaviors – attempting to model the as-is state of a predominantly human process. Where traditional PRA will generally model a technical system with some input of human errors such as THERP or WASH 1400,\textsuperscript{1} The ST-PRA attempts to model human errors and human variations – where one task may be performed many different ways within one risk model.

Commercial aircraft maintenance operations are complex, with risks that vary from equipment failure to human error, at-risk behavior to environmental hazards. Risks within aircraft maintenance have long been managed on an event-by-event basis. Building a socio-technical risk model allows the maintenance organization to see risks in a manner previously unavailable. Even for those maintenance organizations that have collected human factors data, this data does not provide any visualization of the interconnectedness of events that might combine to lead to an aircraft accident. Additionally, many quality assurance systems today do not account for the presence of behavioral norms that are part of the socio-technical model. Building an aircraft maintenance fault tree will allow an organization to have a much more inclusive model of risk.

ST-PRA is still in its infancy. The unique techniques and rules required to effectively model human behavioral risks within a fault tree are still advancing. Given, however, that human errors and behaviors are major contributing factors to most accidents in high-risk industries; this is a development effort that must continue – despite the uncertainties in the socio-technical aspects of risk modeling.

The Un-Covering of ST-PRA

Taking a historical view, probabilistic risk assessment (PRA) has an extensive application in strictly mechanical systems, where engineering objects (devices, vehicles, systems, subsystems) have been structurally analyzed for risk possibilities using a variety of tools (e.g., fault trees, failure modes and effects analysis, hazards analysis). This approach has been particularly successful in providing design guidance.\textsuperscript{1} However, we know that these same objects are placed and used in operational environments in which many other risks can affect the risk of failure. For example, weather (such as a sea air environment) may significantly accelerate corrosion properties of an aircraft. Humans who work with mechanical objects may significantly accelerate the chance of failure due to mere handling or testing of systems as well as collateral damage due to human error.

In recent years, the PRA of mechanical systems has been augmented with some incorporation of human error models (e.g., organizational factors, ergonomic considerations), which included performance shaping factors. This enhancement has been difficult and slow primarily because of the lack of human error data precise enough for design engineers. Additionally, because operator environments and operator use of equipment will vary between operators it is also difficult for the design engineer to model operational risk.\textsuperscript{2} In contrast to PRA of mechanical systems with some limited modeling of human errors; socio-technical probabilistic risk assessment (ST-PRA) is the PRA of socio-technical systems with limited modeling of equipment failure. It is a structured process for building a risk model from probability estimates of individual human errors and at-risk behaviors.
The Basics of Fault Tree Analysis

Fault trees are the tools used in PRA for visualizing risk. Unlike FMEA or RCA, fault tree analysis begins with the identification of an undesirable top-level event. Additions to the fault tree contribute to supporting the estimated level of risk for the top-level event. Fault trees are populated by three principal elements: basic events, “AND” gates, and “OR” gates. Figure 1, a simple fault tree, models the undesirable outcome of an aircraft engine oil pressure drop during takeoff on one type of a aircraft engine.

Figure 1 – A simple fault tree depicting an Aircraft discrepancy on take off roll

This fault tree models three combinations of failures leading to the top-level event. Immediately below the top-level event is an “AND” gate, which indicates the two functional failures that must occur to create a drop in engine oil pressure. The engine oil cap must fail “AND” the pre-flight inspection must fail to capture the discrepancy in order for the top-level event to occur. Neither one of these events is sufficient, by itself, to cause the next higher failure state. Directly below the event “Engine oil cap fails” is an “OR” gate, meaning that any individual item below the gate is sufficient, by itself, to cause the next higher-level failure state. For example, a mis-installation of the cap, technician forgets to install cap and mechanical failure of oil cap are each independently associated with the engine oil pressure drop.

“Basic events” are the fundamental failures or conditions that can be combined either by “AND” or “OR” gates to create higher level states. These three components - “AND” gates, “OR” gates, and basic events - are the principal elements of any fault tree. Fault trees can illustrate both the robustness and the vulnerability of the system just by the very shape of the tree. In our example, the engine oil cap task and pre-flight inspection work together (i.e., robustness) requiring two independent failures to cause the top-level event.

Predicting Event Rates

Assignment of basic event probabilities is often the most difficult task in ST-PRA. Many socio-technical probabilistic risk assessments are developed purely through focus group data. In environments such as healthcare, events are so under-reported that the risk models developed through focus group data will vary significantly from those developed through reported event data. In other environments, such as aircraft ground damage, where the undesirable outcome is visible, the focus group model can be directly compared to a data-developed model.
The real power of fault trees is in performing probabilistic analyses, as shown in Figure 2 below. In probabilistic analysis, each basic event is given a probability or frequency of occurrence. In our sample tree, each event was given a probability of $1 \times 10^{-3}$. The gates in the tree then provide the mathematical basis for analyzing combinations of failures. For the “AND” gates, the probabilities of basic events are multiplied together. For the “OR” gates, the probabilities are added together, with the overlap then subtracted so as not to double-count for the condition where both failures may occur simultaneously. In our sample tree, the probability of engine oil pressure drop during take off is derived at $3 \times 10^{-6}$ (a low rate because two independent failures were required). (Fortunately, given the complexity of the mathematical computations in large trees, commercial fault tree software is available to perform the calculations.)

**Figure 2 – A simple fault tree with the probabilities of risk included for each level of event**

A socio-technical risk model can be both qualitative and quantitative; the qualitative model illustrates system design with the quantitative model a guide to actual practice. As a qualitative risk model, the model itself becomes a visual representation of basic events and how they combine to produce an aircraft maintenance discrepancy. A qualitative model shows the inter-relation between equipment failures, human error, and at-risk behaviors that can combine to produce the undesired result. With probability estimates included, the model provides a quantitative estimate of the relative risks, from one branch to another, and from one failure combination to another. Quantitative risk models are the higher value trees; however, they also face criticism associated with the uncertainty of their numbers.

Figures 3, 4, and 5 show three progressively enhanced risk models. The first model is simply a qualitative model of the risks associated with dispatch of an aircraft with circuit breakers not reset after aircraft maintenance. Essentially, the model suggests a very high level of reliability with the six events required for the aircraft to be dispatched with a circuit breaker pulled. Qualitatively, the model shows that this is a redundant maintenance process and suggests a high level of reliability.
In practice, there is little data inside an organization relating to the individual events comprising the risk model. The maintenance organization would likely have data on how many aircraft are dispatched with a circuit breaker pulled; however, they would not know the rate at which a pre-departure check does not catch that a circuit breaker is pulled. Most data systems today only capture the end result – with the rate of intermediate failures relatively unknown.

The evolution of the risk model at this point can take two paths – to insert probability estimates, or to add additional behavioral failures. If we add estimates, we might produce a risk tree that looks as follows:

This risk tree, with very uncertain error rates attached, now shows a predicted top level risk of 1 event in one billion flights. For a maintenance organization that tracks the outcomes, this risk model might be far from their reality. For a mid-size airline, this number would equate to one event every 1500 years. Again, this is likely far from the reality of multiple events each year.

The next evolution in the tree is to add behavioral risks – the at-risk behaviors that grow within an organization. These are not “human errors” in that they are intentional, rather than inadvertent deviations. For example, there is a rate of human error attached to a technician who tries to spot a pulled circuit breaker. Given the array of hundreds of breakers, we might predict a high level of human error. This is different, however, from the rate at which the technician simply does not perform the task. With the behavioral risks added, the tree might look as follows:
This model better represents the risk factors we might expect to see in a maintenance operation, including the contribution of at-risk behaviors. At this point, there are two paths to complete the model – 1) working back from the top level event, or 2) working up from the bottom level events. If we know the top-level risk, we might adjust the numbers below to obtain an approximation of what is happening in the actual system.

For example, if we knew that a maintenance organization was experiencing 5 events per year, we would have to drastically change the error rates (beyond the point of reasonableness) or add in rates to the at-risk behaviors to produce a model that predicts what is actually happening. This model is shown with the four behavioral norms set at p=.5. This model might now predict a rate that matches actual event occurrences, but are the underlying estimates reasonable, or accurate? While this model is quantitative, it is far from being considered the objective “truth”. This, however, is not the point. Does the model give us information that will guide further inquiry? Does the quantitative model provide us with more information than the merely qualitative model? The answer is “yes”. It provides a visual representation of risk that can guide decision-making around further inquiries into the sources of risks, along with giving the organization the ability to update probability estimates through specific data collection and event data to understand if norms or behaviors have changed.

Use of the Fault Tree Models

The purpose of building ST-PRA fault trees is to understand the sources of risk. In the case of aviation maintenance, this is achieved through the use of cut set reports, which is a rank ordering of paths within the PRA. The cut sets are a visual representation of the risk of an aircraft discrepancy created during aircraft maintenance, as seen through the eyes of aircraft technicians, inspectors, and engineers. After looking at a completed model, the maintenance organization might choose to add a verification task to the process, decreasing the risk in the model by requiring two errors rather than just a single error leading to the top level event. On the other hand, the maintenance organization might choose to look at this event and decide the process and risk are acceptable and allocate limited resources to more critical areas.

Clearly, where there is a lack of objective data, one can argue that any decisions made off of a predictive model are to be suspect. The estimation of human error rates in particular have been met with skepticism by equipment designers. One of the many challenges for an ST-PRA modeling team is the establishment of probability rates for at-risk behaviors within an aircraft maintenance environment. Is the at-risk behavior a norm within the organization or was this simply one individual taking a risk? Additionally, how robust are the capture opportunities within the maintenance organization: are the inspections performed to the appropriate level or is the maintenance organization’s defense in depth design a paper tiger?

Given the difficulties in performing ST-PRA modeling and uncertainties associated with the outcome, what then is the advantage of ST-PRA? The alternative to ST-PRA, is to assume the system is safe, wait for events to occur, investigate, and mitigate to remove the newly seen risk. The question for those looking to venture into
predictive modeling of socio-technical risk is not in its objective truth, but in its value to managers who must model system risk.

One US air carrier used the ST-PRA process to model risk of aircraft damage at one of its largest hubs. Prior to building the model, the principal strategy for managing ground damage risk was to investigate the ground damage events when they occurred and to make local point fixes. This strategy seemed unable to significantly drop the rate. The airline chose to build an ST-PRA model of ground damage using model building teams comprised of pilots, flight attendants, gate agents, ground crew, and maintenance crews. Over five weeks, the modeling team built an ST-PRA with 1500 events and over 500 cut-set combinations of principally human errors and at-risk behaviors. Through the analysis, the team identified roughly 20 strategies to reduce ground damage risk by a predicted 50%. Today, that one airport reports one half the rate of ground damage as the rest of the airline.2

Again, the value in ST-PRA modeling must be made by those who will use the model. As an operational tool within complex socio-technical systems, ST-PRA, even with its uncertainties, typically yields outcome improvements not achievable by an event-by-event risk management scheme.

Conclusion

This paper asserts that socio-technical fault trees have value when built by operational teams – and when used as an operational decision-making tool. While there are difficulties associated with predicting human error rates. It is the process, however, of building socio-technical fault trees that allows the operational organization to visualize the combination of failures designed into the system to prevent top-level events. The fault tree modelling allows the operational group to see where single path failures or probable combinations of failures (cut set) might exist. Additionally, the process of requiring focus group estimates of probability rates often results in a deeper operational understanding of defense-in-depth design, rate dependencies and other human reliability concepts that are not easy to visualize with failure modes and effects analysis or other qualitative tools. Through the NASA research effort, we have been able to continue to demonstrate the application of ST-PRA methods as a tool for visualising risk in extremely complex socio-technical settings. Development of socio-technical use of fault trees should continue as experience shows that the fault tree modeling techniques that have been applied in the equipment world can be transferred to the operational setting where human error and at-risk behaviors make up a majority of the model.2

Acknowledgements

Through research support from NASA Ames (Barbara Kanki, principal researcher), this technique has been used to model risks in healthcare medication safety, railway passenger egress, space shuttle tile installation, airspace mid-air collision assessment, as well as aircraft maintenance risk. This paper discusses the use of ST-PRA in aircraft maintenance, where the work has been funded through the internal R&D efforts of Outcome Engineering, and the research support of NASA’s Aviation Safety and Security Program.

References