

## **Advanced Risk Assessment Methods for Aircraft Electrical Wiring Interconnection Systems (EWIS)**

V.L. Press and A. M. Bruning  
*Lectromechanical Design Co.*  
*Dulles, Virginia*  
*703.481.1233*

D.C. Wood and R. L. Steinman  
*Advent Engineering Services, Inc.*  
Ann Arbor, Michigan  
*734.930.7500*

*Presented at the:*

*6<sup>th</sup> Joint FAA/DoD/NASA  
Conference on Aging Aircraft*

*San Francisco, CA, USA  
September 16, 2002*

## Background

An aircraft's electrical wiring interconnection system, (EWIS), is one of many critical systems that compose a modern day airplane. EWIS, however, has historically been treated as a "fit and forget" system. Recently, the aviation industry has directed more attention to EWIS by way of 1) Research & Development, 2) Policy Statements (e.g. DOT / FAA Policy St. ANM – 01-04), and 3) Proposed Rulemaking, recognizing it as a sub-system that has potentially hazardous failure modes, which may adversely affect other systems. The Federal Aviation Administration's ATSRAC (Aging Transport Systems Rulemaking Advisory Committee) working groups, which have been studying various aspects of aging wiring since 1998, have recently submitted recommendations which should enhance safety and address some of the longstanding EWIS concerns (*examples of proposed regulation changes pertinent to this paper include §25.1703 - Electrical Wiring Interconnection System Function & Installation and §25.1705 - Electrical Wiring Interconnection System Failures*).

FAA has also commissioned a multi-year study (among several other important FAA sponsored EWIS related efforts), to develop advanced EWIS risk assessment tools for aircraft supplemental type certification (STC) optimization and life-cycle management. The project will ultimately result in an easy to use software application that helps facilitate compliance with (the broad and sometimes ambiguous) paragraph §25.1309 of the Federal Aviation Regulations, and its associated Advisory Circular (AC 25.1309). Lectromec Design Co, co-authors of this paper, are currently under contract with the FAA to develop the aforementioned risk tools.

Presently, the Systems Safety Analyses and Functional Hazard Assessments (FHA) required under FAR §25.1309, do not address wires (harnesses) as separate, stand alone systems, that support other critical systems onboard an airplane. As a result, the SSA and FHA are seldom run for EWIS or its components. Rather, existing regulations are based on an overall aircraft-level quantitative safety goal ( $1 \times 10^{-9}$  catastrophic failure per flight hour). In practical terms, the safety goal is implemented through a combination of deterministic requirements (e.g., single-fault criterion, fail-safe design) and quantitative reliability requirements applied at a system or functional level (e.g., systems performing critical functions must be made redundant if its single system reliability is below a target value). Both crash investigation and destructive post-service testing of actual aircraft wiring indicate that the contribution of EWIS-related failures to aircraft risk may be dominated by failure modes that are not addressed in an integrated manner by the current certification process and related assessment tools. Examples include: failure to detect latent EWIS problems through certification check requirements (CCRs); failure of more than one function due to wire bundle or connector failures; consequential damage near localized electrical fires; and normal and accelerated aging effects due to exposure to mechanical, thermal, humidity, and chemical environments, many of which vary considerably in different aircraft zones. Aircraft safety can be improved by the application of risk assessment methods to the EWIS (particularly for aftermarket STC actions) and integrating the results into an "aircraft-level" risk assessment process.

## The Issue

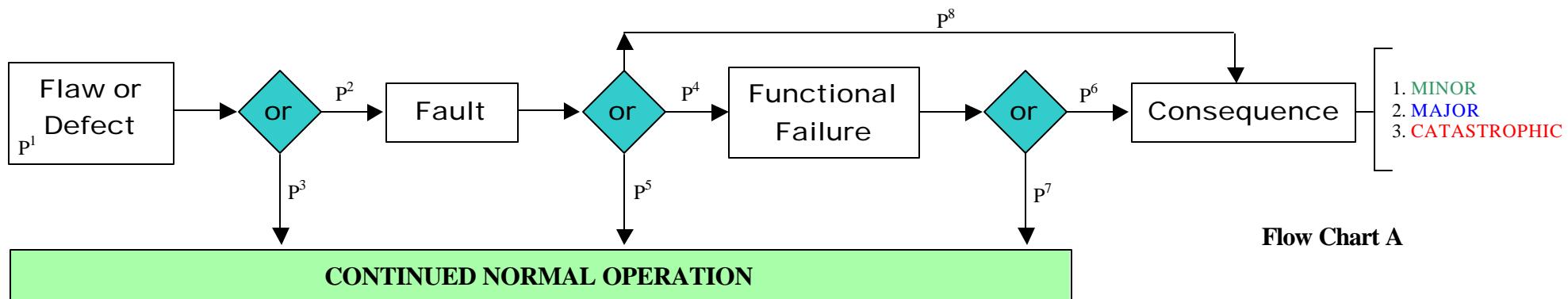
A wire (or its insulation) can become damaged in many different ways at any point throughout an aircraft's lifetime. Obviously, as an aircraft ages, the probability for the EWIS to become damaged increases. An instance of *damage (or defect)*, such as those shown in *Figures 1-3*, has a certain likelihood of occurring;  $p^1$  below, dependant upon numerous environmental, operational and human contributory factors. In fact, several high-profile, industry inspections uncovered multiple instances of insulation breaches per 1,000 feet of electric cable. Based upon these findings, several hundred such defects may exist within the wiring of a single aircraft, (often more prevalent in certain un-pressurized compartments, high traffic zones or swamp areas). After EWIS damage has happened, a fault directly attributable to that damage also has a certain probability of occurrence;  $p^2$ . The resulting *fault*, if one occurs at all, may take many forms including: a short circuit, series arcing or a high energy sustained arcing event. The result of the fault may be a non-event or it may lead to a (functional) *failure* such as an intermittent avionics interruptions or loss of a particular control device. The *consequence* of the failure can be grouped into three categories: Minor, Major and Catastrophic. Of course, the chain of events can terminate at any point in the progression (Flow Chart A). [This process is similar to the one identified in AC 25.1309 System Design & Analysis, that starts with a Functional Hazard Assessment (FHA) and then ends with a safety assessment whose initial objectives are defined by the FHA.] Again, EWIS is not necessarily addressed as an independent system / subsystem as part of this process.

**Flaw or Defect** – Breach in wire insulation , loose pin in connector, etc.

**Fault** – Spark to ground, series circuit spark, conduction from circuit to circuit, etc.

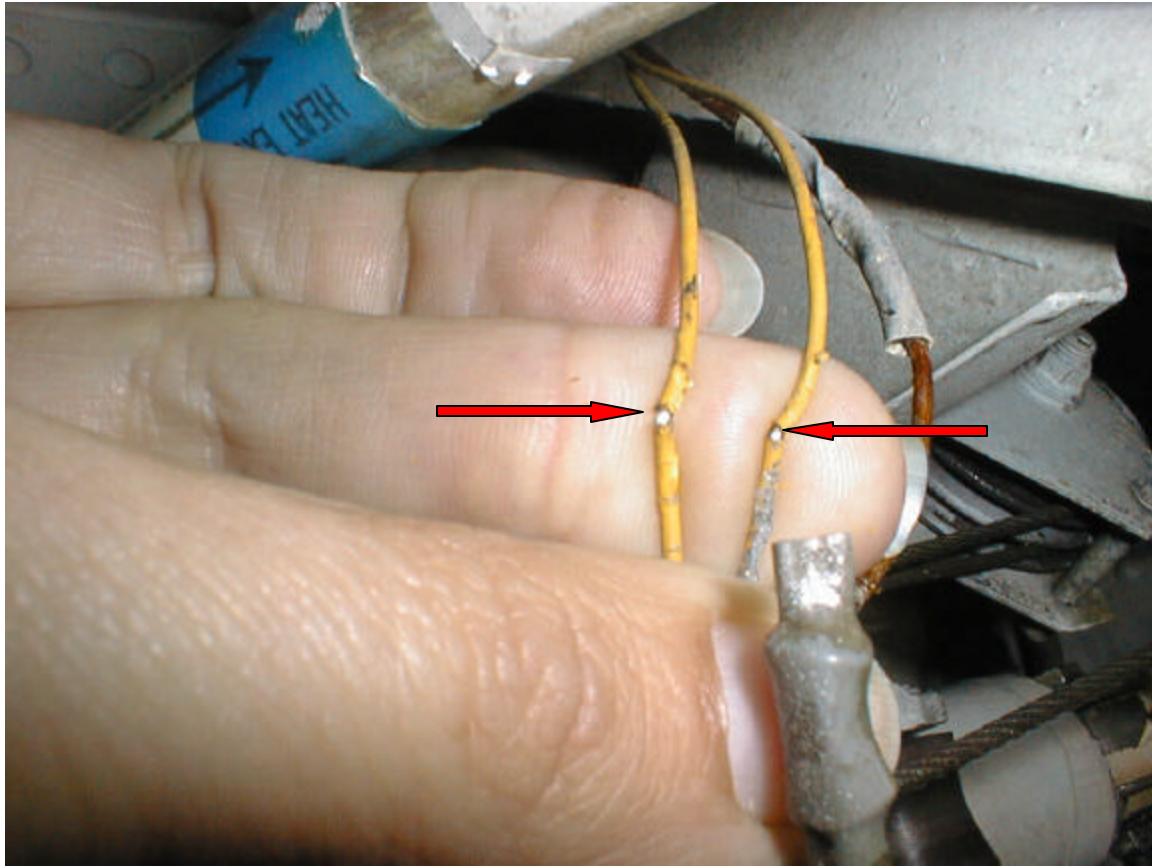
**Functional Failure** - intermittent LRU, avionics malfunction, inoperative landing gear, etc.

**Consequence** – minor, major, or catastrophic.



Past accident investigations indicate that very simple failure modes can cascade into rare but complex chains of events (consequences), which in-turn can result in operational problems, or worse case, a catastrophic event (TWA 800 being one well known likely illustration of this). Determining the significance of hazards, either individually or in the aggregate, requires the use of probabilistic risk assessment methods. The elements that are considered in probabilistic risk assessments ultimately suggest how certain maintenance actions should be conducted, how rigorous inspections should be, how wires should be routed and even what replacement wire types should be selected. Examples of questions that should be considered as part of an effective Probabilistic Risk Assessment (PRA) include:

- How will these outcomes affect the circuit that was damaged?
  - Measure severity of outcomes and function of circuit!
- How will these outcomes affect other systems in the airplane?
  - Measure arcing characteristics and criticality of the other systems!
- How will the more serious of these outcomes, effect the continued safe operation of the airplane?



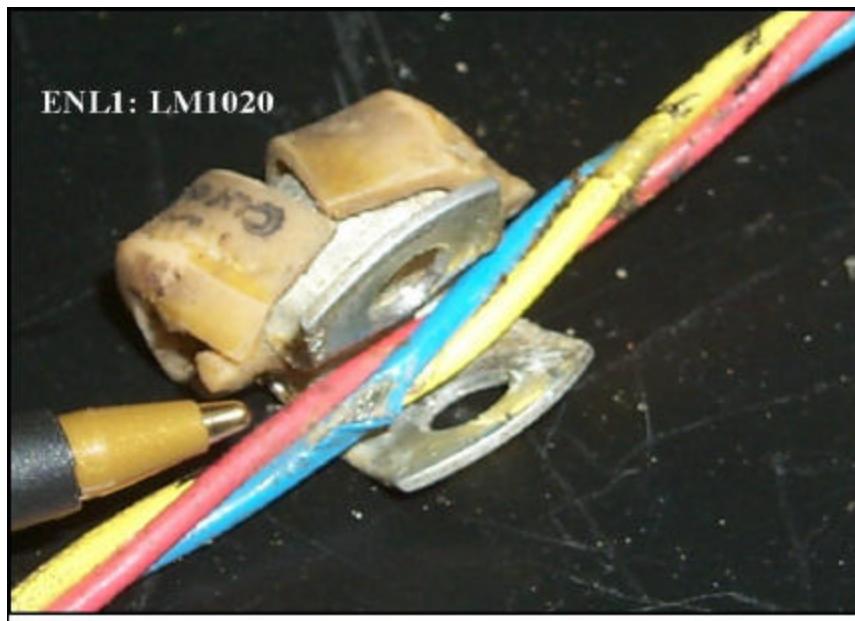
**Figure 1** – Insulation damage on a Fuel Quantity Circuit.

Multiple insulation breaches occurring adjacent to each other is actually more common than widespread convention would indicate. The forces, either environmental or physical, that act upon a wire or harness tend to affect a concentrated area. This results in an potentially hazardous condition where the necessary ingredients for an electrical fault become present.



**Figure 2** – Chafed insulation on Wing Tip Light Power Circuit.

“All of the needed ingredients”. A wire bundle, which chafes against structure (Figure 2) or under a clamp (Figure 3), presents a potential condition where multiple insulation breaches occur adjacent to one another *or* are close to a ground source.



**Figure 3** – Exposed conductor under clamp, discovered during the FAA ATSRAC intrusive inspections.

## Project Importance

For the above reasons, it is vital that end-users such as: STC applicants, maintenance facilities, designers, aircraft operators, manufacturers and certification professionals have the proper tools (software, hardware and equipment) to help identify, assess and mitigate EWIS threats as well as assure compliance with present and future reliability regulation. Lectromec's study began by reviewing present day certification requirements related to probabilistic safety analysis and reliability in several high consequence industries; nuclear, electrical utility and aviation. For each, the regulations which govern risk assessment and the methods of compliance were studied for possible crossover techniques which may be useful to the aviation industry. (two additional surveys are currently underway to gain insights into the *chemical* and *space* industries).

## Survey of High Consequence Industries

### Nuclear Power

Risk mitigation regulations and techniques have evolved over the past 30 years from simplistic qualitative risk assessment methods to the present “risk-informed” approach which integrates both traditional deterministic decision making with sophisticated quantitative risk models. This allows us to consider the quantitative risk benefit of proposed system design changes or maintenance practices at the plant level (or potentially aircraft level). The timeline in Figure 4 depicts the five risk assessment “eras” of the Nuclear Power industry. Key industry events that either affected or characterized changes in the use of risk technology are also shown on the right hand side of the timeline.

The following bullets summarize application of risk technology to the commercial nuclear power industry and the associated benefits it has provided:

(excerpted from Gaertner & True, *Safety Benefits of Risk Assessment at US Nuclear Power Plants*, June 2001)

- US nuclear power plants have improved safety and have evolved to a risk-informed safety culture through application of PRA. Nuclear plant PRA has matured from 1975 to date; every plant has models, expertise, and PRA application experience.
- Risk to the public from US nuclear power is very low relative to NRC safety goal policy and relative to other risks. Calculated risk has decreased threefold in the past decade, while trends of other performance indicators such as plant trip rate, capacity factor, and challenges to safety systems have shown marked improvement.

- Insights from PRAs have established which initiators, equipment, and human actions are risk-important and have helped to foster a new plant culture of risk management. Many detailed examples illustrate the scope and magnitude of changes that either reduce risk or simplify plant operations while maintaining a low level of risk. Some of these changes were enabled by risk-informed regulations, petitioned by owner/operators or initiated by the NRC.
- The above observations establish that the industry is positioned for more risk-informed improvements. Continuing change in regulations and attitudes about risk-informed and performance-based operations is necessary.

*Note:* A recent discovery of corrosion in the nuclear reactor vessel head at the Davis Besse Nuclear Power Station, Oak Harbor, Ohio, was implicitly included in the existing plant risk assessment as one of the possible mechanisms that could cause a large Loss of Coolant Accident (LOCA). The initiating event frequency assigned to such piping and pressure vessel failures in the risk assessment credits inspection and surveillance programs designed to detect and correct such deficiencies prior to catastrophic failure. This emphasizes that with the impressive and continued maturation of the following chart, initiative and human skill are indispensable.

**Figure 4**  
**PRA Timeline**

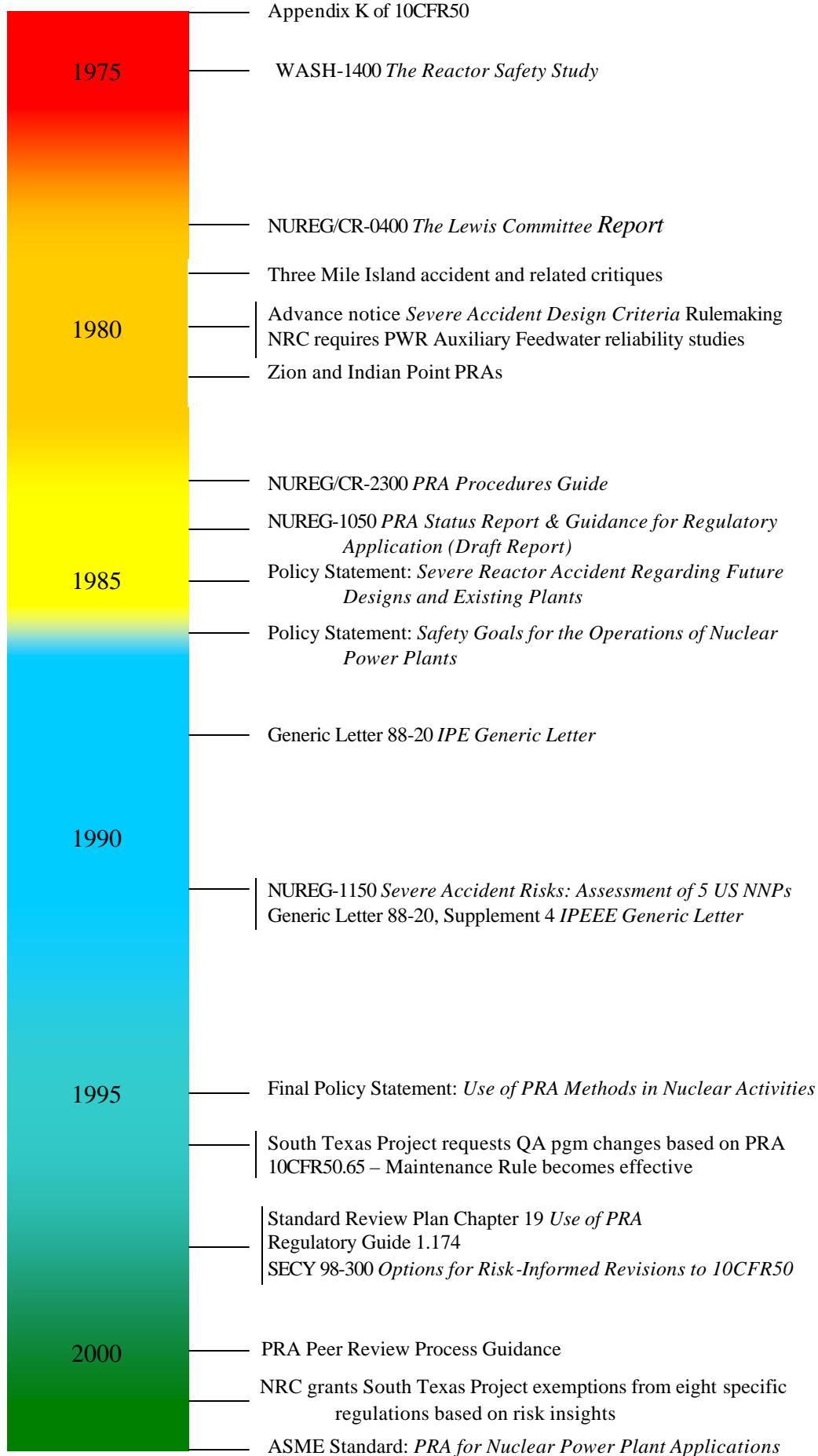
Qualitative use only in regulation

Licensee use for non-regulatory applications.  
Regulator use for justifying deterministic requirements

Proof of quantitative PRA capability & regulatory endorsement

Limited special applications within existing deterministic regulations

Risk-informed regulation challenges existing deterministic regulations



## Electric Utilities

The electric utility industry is not a "high-consequence" industry in regard to the potential for human loss but rather because of the widespread reliance on power, from a supply and distribution standpoint. This is evident in lessons learned from past power failures. Lectromec survey concentrated in the distribution and sub-transmission aspects of the industry.

A survey of seven utilities, suggested that most of the risk assessment and mitigation in the electric utility business is satisfied via multiple contingency planning and implementation. Risk assessment during the design phase is a fairly new concept to electric utilities. The driving philosophy being "install and forget" when it comes to wires and cables. Further, a prevalent sentiment seems to be "do not touch until it fails." The perceived risks lie in the inability to supply power to the customers after the network has been designed rather than during the design itself. Electric utilities, in this sense, are a good example where "best wiring practices" may be enough during design. The 'best practices' have been employed for a long time and they have worked. Further, as stated earlier, the failure of a distribution system rarely has any resulting human loss associated; the fall out is more political by nature, so there is no urgency in risk assessment during design.

Risk assessment approaches are 'diffused' through utilities internal organizations, with no single utility source responsible for all equipment. Generation, Transmission and Distribution divisions or companies interests are all handled separately and in different ways. Assessments in Distribution area seem to be some guesswork, a lot of dependence on history, and no software used to estimate risk. The same appears to be true for sub-transmission equipment.

One approach to substation maintenance is unique, and not the norm for most utilities. One company used two models at present and a third is in the prototype stage. The two working models are called "Contingency" and "Monitor." The term used for network shutdowns and failures is "Jeopardy." These two models help in identifying and avoiding jeopardy. These models are further explained below:

The *contingency* model identifies components most likely to contribute to jeopardy. This model looks at the components comprising the feeder: failure rates, operating temperature, load shifts, among others. This model predicts a trend by looking at a twenty year time frame. The modeling is taking place now to provide an outlook for the next twenty years. The types of information incorporated includes, among others:

- Cables - broad categories such as paper or extruded were mentioned without any distinction between them.
- Splices, Stop-joints that join paper and solid dielectric were mentioned
- Terminations
- Age
- Predicted operating temperature

The *monitor* model is analogous to the contingency modeling except that it provides a seven-day outlook. This modeling helps in a more day-to-day failure prediction. This modeling uses the same type of information that is used in the contingency modeling.

Most utilities are only now getting started on ‘asset management’ which is the terminology used in electric utility that comes closest to meaning some form of risk assessment and management.

In the generation area, there is more dependence on use of software and programs to estimate risk, but there is much dependence on history here too.

No group indicated any need to comply with uniform external standards. Cable suppliers must comply with an industry specification, developed by IOUs (thru AEIC), which builds on manufacturer’s inputs.

### Aviation

The aviation community is a multi tiered industry consisting of: original aircraft manufacturer (OAM), aircraft operators (airlines), maintenance organizations (MO), and third party maintenance, modification organizations and government regulators. Each of these organizations address risk assessment and mitigation in different ways (which can vary in effectiveness) even though standard regulations exist.

Aircraft Operators (Airlines): Airlines typically are more concerned with maintenance than design changes or modifications. In a situation where the airline is required to modify an aircraft, for a myriad of reasons including airline requirement, retrofit, upgrade, etc., quantitative risk analysis is rarely done. This is because, typically a vendor selling a system will already have the system and/or equipment certified as airworthy. The airline at most will conduct the installation. This current system does not always work well for various reasons.

A living example coming out of our Task 1 industry survey: A certified system (under an STC) was being installed in a commercial aircraft. The installation procedure called for the systems’ power wires to be routed within an existing bundle. An astute technician noted that the bundle in which the power wires were to be routed with, actually contained the automatic landing systems wires. This was brought to the attention of the maintenance engineers, whereupon the routing was changed. This is merely one example of how the EWIS may not be adequately considered under present regulation. Not all technicians might have been as concerned with the situation. Aftermarket modification actions such as this historically have not benefited from, specific guidance that take into account meaningful EWIS function, system redundancy and zonal flammability concerns. Consequently, there has been a lack of specific direction as to “red flag” issues or other important original aircraft manufacturer OAM or previous life cycle information (this is not the case for newer aircraft). Again, these concerns are presently being addressed through FAA ATSRAC recommendations and concepts like the ones outlined in this paper.

The requirements set in §25.1309 (b) also state that safety can be proven by using a predecessor analysis run on a similar system. This method is employed in most cases. Once again, the drawback is that the analysis will be on the system and its individual wires, but the effect of the added wires on an “aircraft level” system is not considered. Of the airlines surveyed, a unanimous opinion was that the requirements in 25.1309 (b) were very ambiguous and the airlines do not have clear instructions regarding compliance by quantitative methods. Most perceive the risk analysis as volumes of algebraic and numerical calculations and hence, attempt to avoid them.

Airlines typically categorize modifications into two categories: *Major* and *Minor*. The prevalent practice is to attempt to prove that modifications are *Minor* in nature, because a Supplemental Type Certificate (STC) or other approval exercise are then not required. In these situations the operator can use the authority they have under FAR Parts 121 or 145 to design the modification which then must be approved by a Principal Maintenance Inspector (PMI) or Principal Avionics Inspector (PAI). Field Authorizations (FA) and Engineering Change Orders (ECO) are also widely used because they are simpler to implement than a major modification, therefore, a risk analysis is not required. Further, for an FA or ECO, the approving authority is the Flight Standards District Office (FSDO), where review personnel may not be well versed in EWIS issues.

Maintenance and Modification Organizations: These organizations are generally responsible for modifications to a postproduction aircraft. These organizations are commonly conducting work for (or are) STC holders. Part of their responsibility is to conduct safety analysis of systems or any other modification action that will result in a change to the original configuration of the aircraft. Lectromec has met with a few select maintenance organizations and has found that they also follow the same process as the airlines, i.e., try to find an analogous predecessor system and pirate the safety analysis done for it. One main reason behind the reluctance in conducting any quantitative analysis, is lack of clear directions in the regulations.

Generally, the organizations are not opposed to conducting thorough analysis on any change but are again intimidated by the perceived notion that showing compliance equates to time consuming, rigorous calculations as well as investigating a paper trail of maintenance, modification and OAM document and records. In this regard, a tool that could help these organizations conduct a focused risk (safety) analysis would be highly valuable.

Phase 2 of the project concentrates on designing enhanced EWIS risk assessment methods or tools based upon findings of current industry practices and that consider: 1) functional failures (including cascading failure) 2) unintended consequences of failures (including collateral damage and fire) and 3) controlling EWIS hazards to acceptable levels by facilitating the evaluation of subsystem level trade-offs or other suitable control measures. Lectromec’s experience with arcing phenomena, modes of wire failure, empirical data, zonal characterizations and trends, etc., will also play a role in this Task. This is where electrical engineering knowledge, physics, chemistry, statistics, PRA, are melded with industry protocol and current practices. For instance, we must now consider existing experience data (in-flight smoke and fire events), integrate age related

degradation into system reliability models, evaluate design or design philosophy changes (routing wire within bundles, routing bundle within aircraft zones, arc-fault circuit breakers), and evaluate changes in maintenance practices (inspection, installation, testing). Emphasis is being placed on mechanistic models, testing, and data analysis to quantify the probabilities of discrete functional failure of EIS components, probabilities of collateral damage from arcing events and localized fires, and aging-dependent failures. Unlike the nuclear business, the aviation industry is rich in data and information regarding EWIS related events (the major reason being that there are simply very few nuclear plant incidents and accidents, and many more aircraft electrical events). “The failure data (regarding EWIS) is sitting there waiting for someone to mine it”. (Quote: Doug Wood, Advent Engineering Services, Inc.)

### Chemical and Space Vehicle Industries

The evaluation as to whether there are techniques and lessons that can be transferred to the commercial aviation industry, is ongoing as part of the work on which this paper is addressed.

## Best Practices

The remarkable aviation safety record of U.S. Flag carriers has been the result of contributions from a large community of interests. In the process of producing and caring for aircraft many viewpoints and techniques have been used and experience has accumulated as to “do’s and don’ts”. Skilled personnel with years of experience intuitively know what is a good design, analysis technique, etc. This knowledge is formalized for example in Boeing Chapter 20 for electrical systems as well as other design and standards manuals. This mass of procedures and drawings, establishes what is commonly referred to as “*Best Practices*”. Best Practices will continue to be the vast body of knowledge for industry that has afforded the outstanding safety performance to date.

Best Practices is however based upon many different sources of information (historical and new), and is regularly interpreted by many maintenance professionals. This leaves some room for error or ambiguity. In some cases, the original basis for a “best practice” recommendation may now be obsolete due to advancements in equipment and technique. For this reason, we must consider “Best Practices” when developing an enhanced method / tool for EWIS risk assessment. The challenge our work is to develop an easy to use tool from an amalgamation of elements –and perhaps other yet-to-be-discovered techniques.

While Best Practices are based on safety assessments, both formal and informal (experience), they are not themselves a safety assessment. They are by necessity general in nature and cannot foresee complex interaction that may occur in or between specific systems. An EWIS safety assessment for a specific system to be installed on an aircraft must use advanced analytical tools to supplement Best Practices but not replace them.

## **System vs. Zonal Failure**

Practitioners of risk analysis for aircraft, maintainers or inspectors essentially conduct their respective duties based a System and a Zonal viewpoint.

A significant distinction in assessing the probability of various consequences of the “defect-fault-failure-consequence chain” is the view the analyst takes of the proposed scenario. Classically, an analyst or design engineer examines his system to see what happens if an element in the system fails. For instance in the case of a simple system circuit, should the contacts of the relay weld shut, then despite the system’s various switches and breakers, a fire can still ensue. This is essentially an example of an unprotected failure mode and its possible effects. One related risk method, Failure Modes and Effects Analysis (FMEA), is one popular system of quantitative probability risk assessment practiced in the aviation industry that focuses on a system.

Zonal analysis is another viewpoint. This approach is particularly useful in assessing the condition of (EWIS) or the safety risk that it poses when it has been damaged. In regard to wiring for example, one foot is the characteristic length for generating a distribution curve for future failures (aromatic polyimide wire type). With many thousands of feet of wire in large commercial jet, attempts to run a probability fault tree calculation for a system that crosses many (irrelevant) zones, greatly complicates the analysis. To avoid this difficulty, one can instead calculate, and sometimes measure, the probability of failure in a zone. (Lectromec has been characterizing the condition of aircraft zones for more than fifteen years, to be discussed in a later section). Quantitative Probabilistic Risk Assessment becomes more feasible when a particular zone is studied. Certain characteristics within each zone such as flammability materials or flight critical systems, heavily influence the PRA consequences.

The following Risk Concepts should take into consideration both the system and zonal analysis.

## **Risk Concepts**

There are many different methods to assessing and ascertaining risk. SAE Aerospace Recommended Practices (ARP 4761) covers some of these in their *Guidelines and Methods for conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*:

- a. FMEA (Failure Mode & Effects Analysis)
- b. External Event PRA (Common Cause Analysis)
- c. Fault Tree Analysis (FTA)
- d. Markov Analysis
- e. Monte Carlo Method
- f. Fatality Curve Zonal Analysis
- g. Reliability Centered Maintenance (RCM)

The data for these methods can be derived through the following:

1. Visual Inspections
2. Best / Recommended Practices or Maintenance Manuals
3. Epidemiology
4. Sampling prognostics (laboratory testing)
5. Instrumented inspection

The challenge at hand is to apply a variation or combination of risk techniques to the assessment of EWIS, and the effects of STC actions on the EWIS. Lectromec and Advent Engineering are now focusing on this aspect of the Enhanced EWIS Risk Assessment Methods project.

### Failure Mode and Effects Analysis (FMEA)

This basic approach is occasionally used by the design engineer or as part of an STC application package if deemed necessary. Again, a cumbersome risk analysis can be avoided as part of an STC action, depending upon the somewhat subjective criticality judgment of the applicant and approving authority. An FMEA requires that one postulates a device failure and then traces out the probability of consequences. This is combined with the formal FHA (AC 25.1309 System Design & Analysis) to determine if change in approach design is required. One of the major limitations of the FMEA is that it is limited to looking at the effects of a single failure rather than combinations of multiple failures than can lead to an undesired outcome.

### The External Event PRA (Common Cause Analysis)

This PRA method is used for nuclear power plants and may have application in the aviation industry. One benefit to this approach is that it can usually be done on a zone and critical function level, and therefore may not require the use of a component or subcomponent risk models. In addition, if the analysis is conducted in a phased approach, time-consuming analyses can sometimes be avoided by simplified screening criteria that either assume total damage or assume no damage (with justification) in certain zones or conditions. Also, this approach may help quantify the benefits of improvements such as the introduction of the Arc Fault Circuit Interrupter (AFCI). In the nuclear business, an external event PRA calculates the risk (probability and consequences) from one or more external events such as fire, earthquake, flooding from sources inside or outside the plant, or severe weather conditions such as tornadoes and wind. All of these examples represent situations where a single cause has common widespread effects (across systems, structures, and components) and is thus called a common cause event.

The most recent industry-wide application of external event PRAs to address common causes was initiated by the IPEEE Generic Letter (NRC Generic Letter 88-20 Supplement4 dated June 28, 1991, *Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities, 10CFR50.54(f)*). The IPEEE program,

including background, objectives, general findings and perspectives for each of the major types of external events (seismic, fire, high winds, floods and other (HFO), as well as plant-specific summaries of findings is described in NUREG-1742 *Perspectives Gained from the Individual Plant Examination of External Events (IPEEE) Program* published in April 2002.

The fire IPEEE has been chosen due to its spatial effects within the plant and the resulting area-by area analysis approach to plant risk. This approach would also apply to spatially distributed risk contributors in aircraft such as fires or adverse environments.

Although the seismic external event risk analysis is not discussed as a specific example in this report, the approach used in the seismic external event risk analysis would be applicable to vibration-induced failures due to takeoff, landing, or in-flight turbulence.

The discussion of fire contribution to risk is limited the impact on core damage frequency (CDF). For a Level 2 or 3 PRA, the contribution of fires to the Large Early Release Fraction (LERF) or offsite consequences could be addressed, respectively.

Fire PRAs typically do not directly use the event trees and fault trees developed for the Level 1 internal events PRA for a number of reasons. First, few Level 1 PRAs model components down to the cable level, which would be needed to model system failures due to fire-induced cable damage. Second, key inputs to a fire PRA include the location of mitigating system cables and components relative to the redundant division and flammable hazards. These are also not modeled in the Level 1 internal events PRA.

Third, the criteria for electrical separation of components, cables, and circuits to demonstrate independence of redundant safe shutdown equipment in the Level 1 internal events PRA is not sufficient to demonstrate independence when they can both be exposed to a single fire. For these reasons and others, a separate analysis method is used to quantify the risk contribution (CDF) due to in-plant fires.

One of the commonly-used fire PRA analysis methodologies in the nuclear industry is the Fire-Induced Vulnerability Evaluation (FIVE) Methodology, developed by EPRI. The premise of FIVE and other fire PRA models is that because spatial analysis is time consuming, it is most cost effective to concentrate the analysis on plant areas *where ignition sources and safe shutdown cable and equipment are located* (This is a similar theory to that of ATSRAC's Task Group 9's Enhanced Zonal Analysis Program (EZAP) criteria). The FIVE methodology is a progressive screening technique based on conservative assumptions using both industry and plant-specific data for evaluating fire event sequences. In short, per the FIVE methodology, a fire area containing no risk-significant circuits or equipment, or with a calculated CDF less than or equal to  $1 \times 10^{-6}$  events per reactor year is considered insignificant and is screened from further analysis.

The FIVE methodology evaluates the areas in the following analytical phases:  
(these will not be expanded upon in this paper)

- Phase I - Fire Area Screen (Qualitative Analysis)
- Phase II - Critical Fire Compartment Screen (Quantitative Analysis)
- Phase III - Detailed Fire Propagation & Effects Analysis of Unscreened Compartments (Quantitative Analysis)

## Fault Tree Analysis

This process is a rigorous procedure for calculating the probability of a consequence for operation of an aircraft from a defect, fault, or failure or non-event. Using a Failure Hazard Analysis (AC 25.1309) procedure, one can develop the hazards that they are concerned about. (Conventional wisdom says there are three events about which a pilot is concerned: A structural failure, a fire, or a loss of control). Presumably any other category does not have catastrophic consequences.

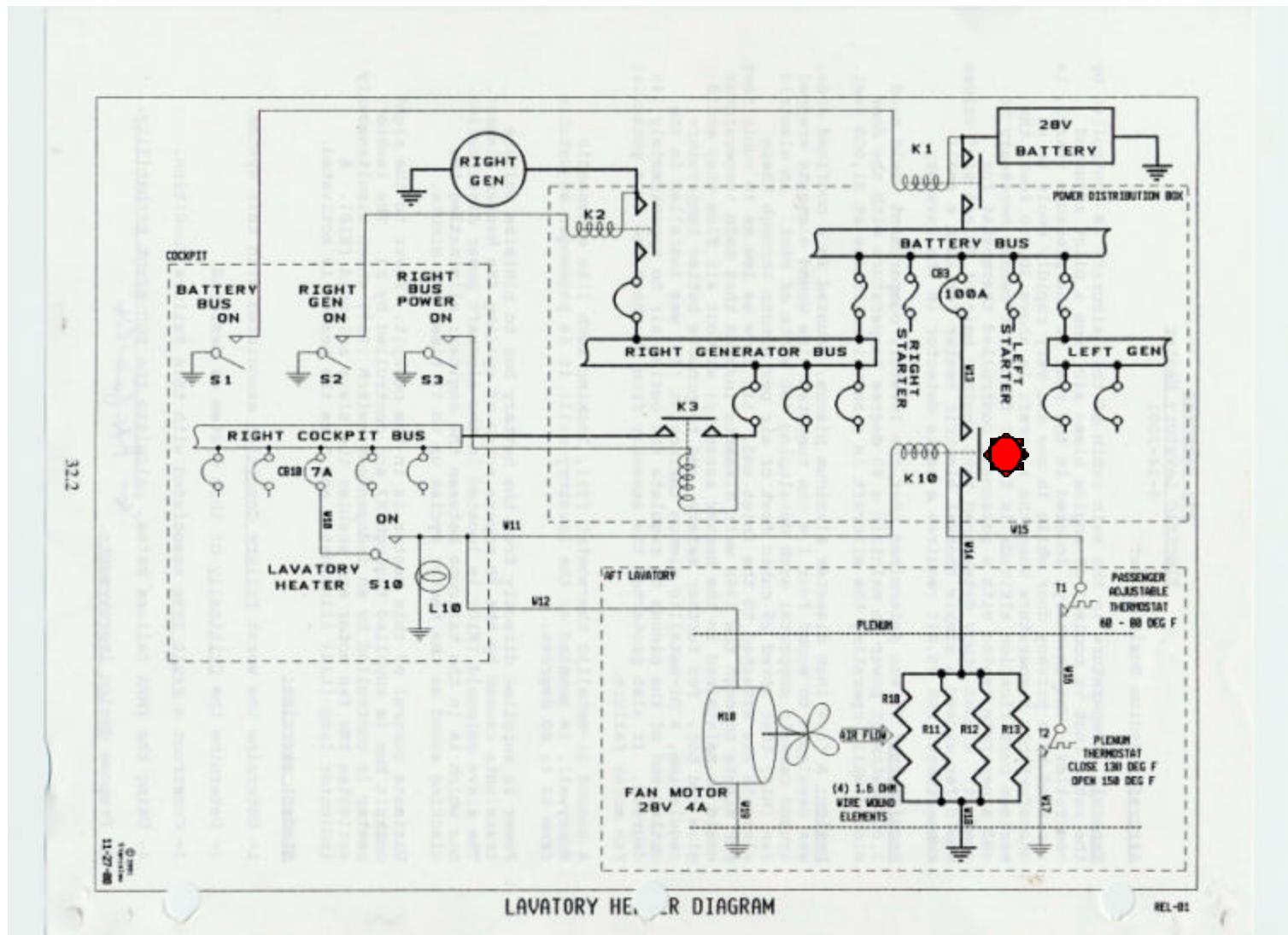
Figure 5 is the circuit diagram for an aircraft lavatory space heater. (provided courtesy of Mr. David Stanislaw, University of Kansas, from his Short Course; *Reliability & 25.309 Design Analysis for Aviation Systems*). A failed component (relay - K10) resulted in an in-flight fire during takeoff. Figure 6 is an example of a fault tree, or “top-down”, depiction of the chain of events leading to the fire. This analysis was backed into using post incident data, and indicated a probability well in excess of the classical  $10^{-9}$  threshold for a catastrophic event. In this case, the event, could have had catastrophic consequences but did not. The original safety analysis did not properly identify the possibility of a failed component leading to the event. By means of a fault tree analysis, in conformance with the calculational rules of Haasl, a unique and complete solution of the Boolean algebra equations, could have pre-identified possibility this event.

## Markov Analysis

Like fault tree analysis (FTA), Markov Analysis is a top down method. It uses a chain of states of the system and rates of transition between these states. A transition occurs due to component failure (or repair). For each state, the rates of transitions into and out of that state are used to write a differential equation for that state. The set of differential equations formed by all of the states describe the system and can be solved to obtain the time dependent probability of being in any one state including a final failure state.

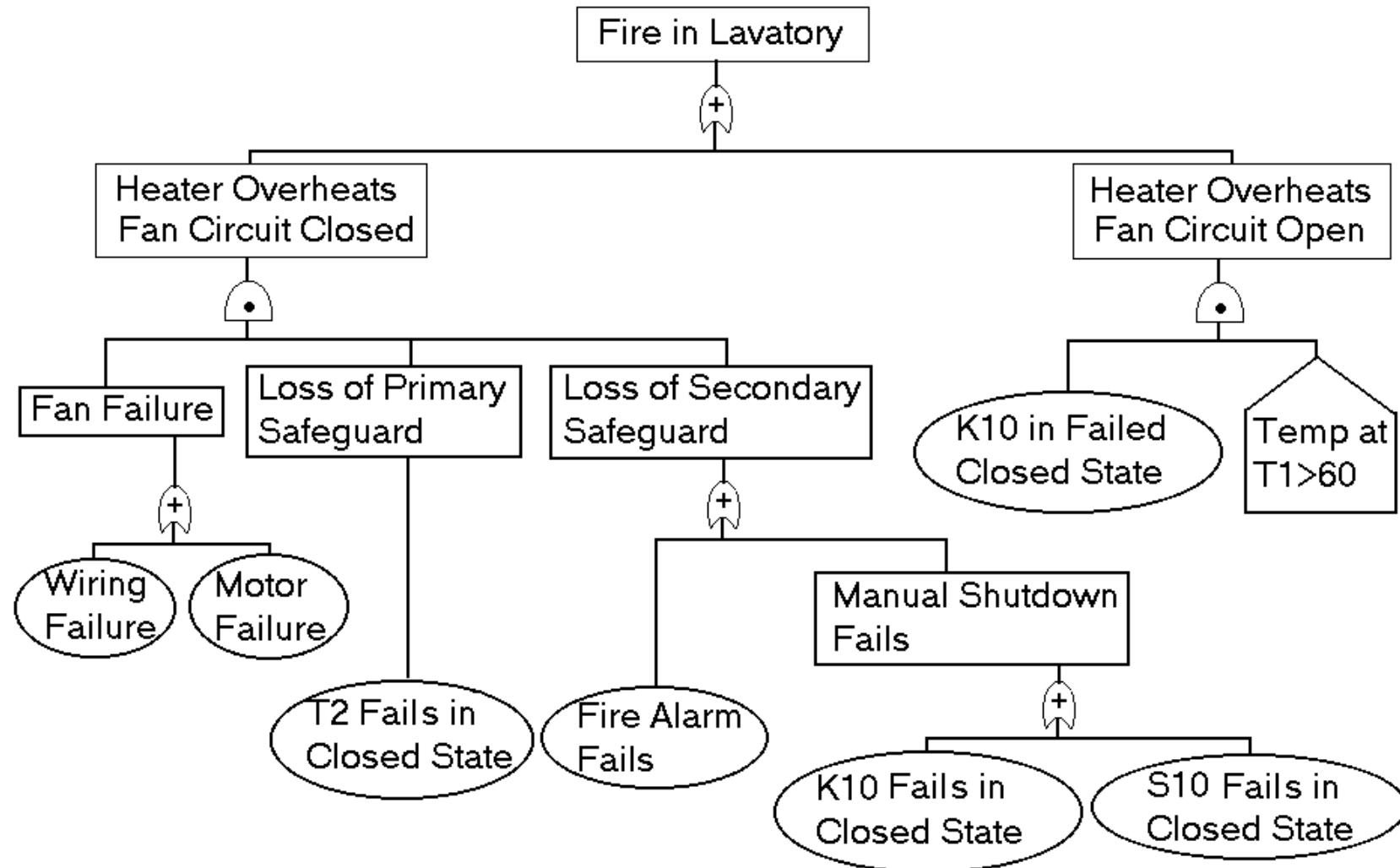
Markov Analysis is more complex than FTA but as a result it can take into account different conditions includes transient and intermittent faults, repairable systems, and latent failures among others. The price of this complexity is an increase in model size that may grow exponentially with the number of components.

Figure 5



Circuit diagram of lavatory heater which resulted in the in-flight fire from failed relay.

**Figure 6**



Post event Fault Tree analysis suggests that it could have prevented the in-flight fire had it been conducted prior to modification. (+ equals “or”, \* equals “and”).

### Monte Carlo Method

This sampling technique examines the probabilities of a “consequence” by sampling a portion of the scenario. As such it can ignore some of the undefined probabilities, and so is not used, to our knowledge, for PRA on aircraft. However, our work to date indicates a combination of this system with a Fault Tree Analysis may solve some of the challenges presented by the broadly distributed nature of EWIS throughout the aircraft.

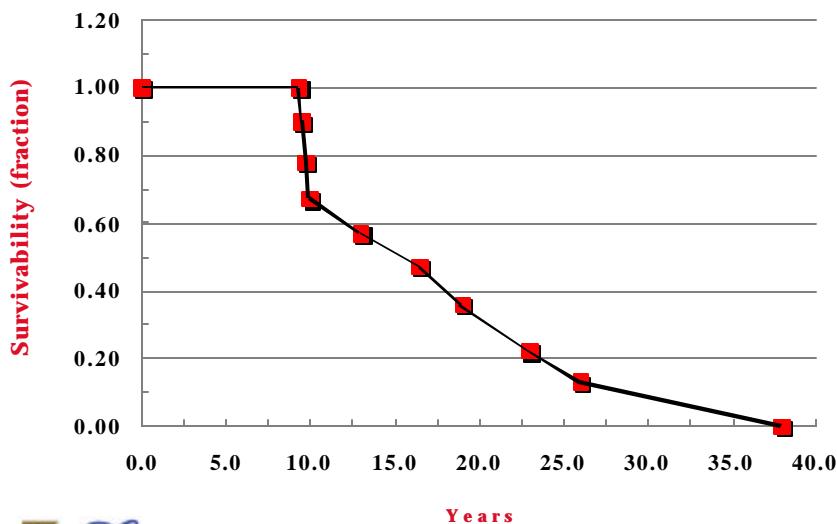
### Fatality Curve & Zonal Analysis

Figure 7 represents the experimental measurement of time versus the first wire insulation defect to appear in a zone based on sampling of aircraft (fatality curve). This fatality curve can then be applied to the fleet to better anticipate when and when EWIS failures may occur. The number of aircraft afflicted, by year is shown in Figure 8.

### Reliability Centered Maintenance (RCM)

This quantitative assessment process uses field data in the form of mean time between failures to calculate a time at which one can choose to take corrective action. It is the classical method used for maintenance action initiation. The use of epidemiological data is an aspect that can be incorporate into some of the other Probabilistic Risk Assessment techniques.

## Wire Aging & Life Testing



 **Lectromec**  
Lectromechanical Design Co.

10

**Figure 7**

## Wire Technology

% Probability of Failure of the Worst  
Polyimide Insulated Wire in each USN P -3  
"Aircraft Location vs. Time"  
As of 5/7/95

 **Lectromec**  
Lectromechanical Design Co.

Location	% Failures				
	1	2	5	10	20
Bomb Bay	0	0	0	24	33
Wing, Outboard Trailing Edge	0	0	0	28	53
Galley/Aft Cabin	0	0	0	41	61
Wing,Center Leading Edge	0	0	15	23	30
Forward Electrical Load Center	0	0	24	35	48
Avionics Bay C1	0	0	43	57	68
Wing, Inboard/Root, Leading Edge	15	20	32	46	60
Avionics Bay H1	21	23	40	46	78
Hydraulic Service Center, Under Deck	20	26	39	56	64
Main Wheel Well	38	42	50	72	100
Nose Wheel Well	31	57	89	100	100
Wing, Center, Trailing Edge	0	74	91	100	100

13

**Figure 8**

## Promising PRA Techniques for the Aviation Industry

Figure 9 shows a preliminary flow diagram of a Functional Hazard Assessment (FHA) and Preliminary System Safety Assessment (PSSA) module of a potential Enhanced Risk Assessment Tool for EWIS. The program will survey the end-user (i.e. technician), prompting him to enter the required input data. Data required include 1) information for the EWIS system being installed or modified (e.g. proposed routing, circuit protection, number of wires and available voltage and current on those wires etc.), 2) information on the other systems that will be routed with the new system to be installed (type of systems, available voltage and current, possible failure modes, etc., and 3) information about non-EWIS systems located near the proposed routing (failure modes etc.). It is realized that some of this information may not be available, especially for older aircraft.

Imbedded in the tool will be an EWIS fault and consequence matrix that describes all known EWIS failure modes and the resulting consequences. The matrix will be developed by conducting Fault Tree Analyses (FTA) and Failure Modes and Effects Analyses (FMEA) on generic EWIS systems. For example, a wire that becomes shorted to structure or a parallel arcing event are examples of faults. Possible consequences for an arcing fault are: the transfer of energy to other wires in the harness, the “opening” of wires in the harness and localized high temperature dispersion. The effect of mitigating factors on the consequences, such as arc fault circuit breakers, will also be contained in this matrix.

The input data will be compared with the fault and consequence matrix and possible failure modes will fall out. Depending upon the failure mode and the system that failed, the resulting hazard will be classified as minor, major or catastrophic. Any weak links of the system will be identified and possible mitigation techniques recommended. Based on the hazard classification and type of EWIS failure, recommendation will be made as to which quantitative analysis, if any, should be conducted next.

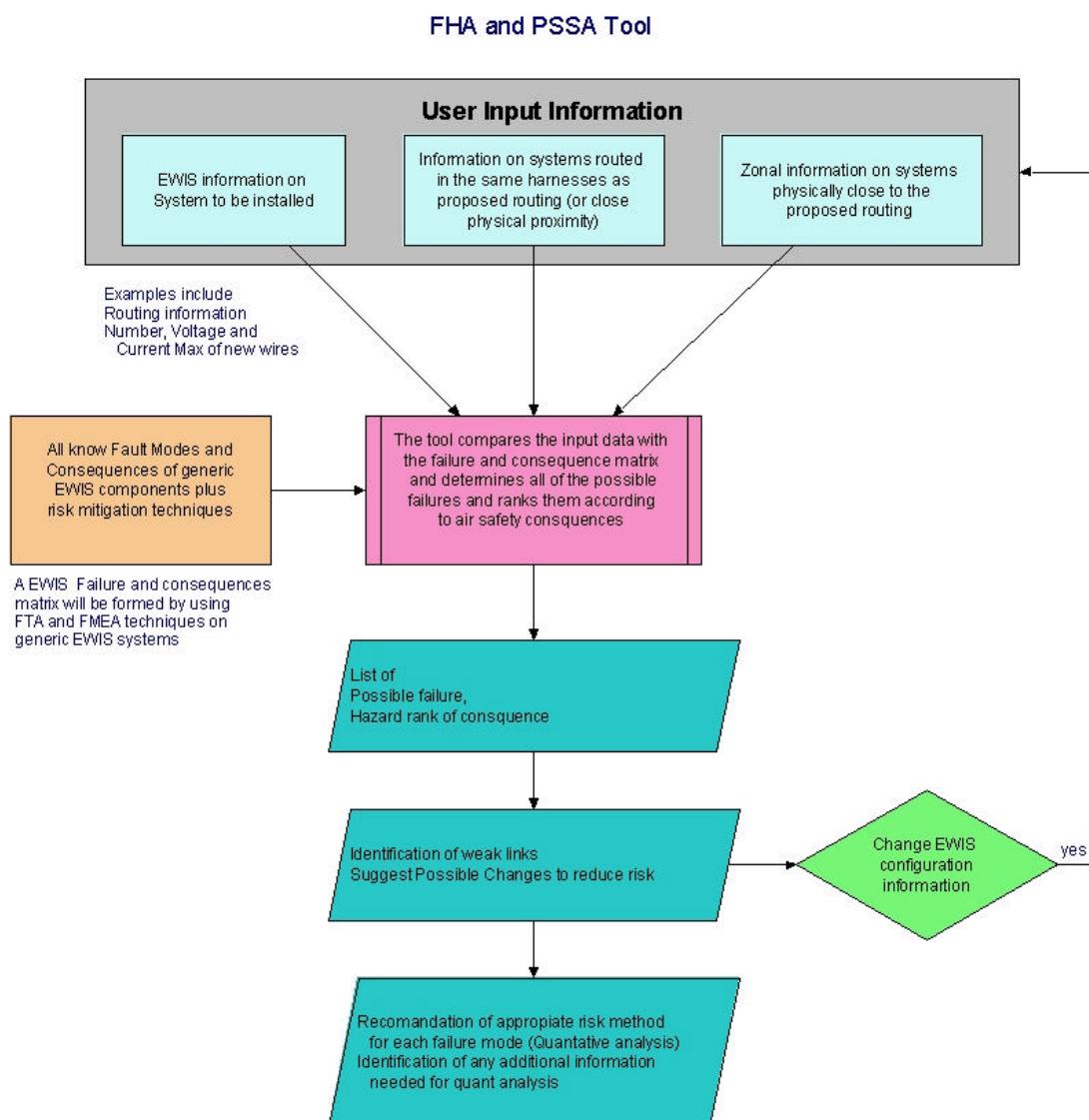
At this point, the methods of performing a quantitative assessment are still being evaluated in order to determine which ones, or which combination, are most applicable to the EWIS.

### External Event PRA (Common Cause Analysis)

Examples of “external” common causes applicable to aircraft risk analyses include wire arcing, wire bundle failures, compartment fires, projectile trajectories, and compartment exposures to adverse environments (temperature, humidity, chemical atmospheres, spray) and other aging stressors (vibration, maintenance-induced damage). These examples closely parallel the nuclear power plant IPEEE external events common cause analyses, and are expected, like in nuclear power plants, to represent a significant contribution to loss-of-aircraft risk.

## Combining Methods

At the time of publication for this paper, the Phase 1 effort of studying the risk techniques of various industries is almost complete. Phase 2, the development of an easy to use risk assessment tool or technique for EWIS is just beginning. Due to the extremely large number of EWIS elements –many hundreds of thousands, and its complexity, the use of a combination of multiple risk methods is the most likely alternative. One possible hybrid approach being explored is to use the Monte Carlo sampling calculations with the rigorous results from a hazard specific Fault Tree Analysis.



**Figure 9 – Preliminary Conceptual Flow Diagram of Functional Hazard Assessment (FHA) and Preliminary System Safety Assessment (PSSA) module.**

- end -