
ANTICIPATING ACCIDENTS THAT HAVE NOT HAPPENED YET A QUANTITATIVE APPROACH AND AIRLINE MAINTENANCE APPLICATION

**Elisabeth Paté-Cornell
Marc Sachon**

Professor and Chair
Department of Management Science and Engineering
Stanford University, Stanford, CA

References: Sachon, M, and M. E. Paté-Cornell. "Delays and Safety in Airline Maintenance", Reliability Engineering and Systems Safety, Vo. 67, pp. 301-309, March 2000.

Paté-Cornell, M.E. and D.M. Murphy, "Human and Management Factors in Probabilistic Risk Analysis: the SAM Approach and Observations from Recent Applications", Reliability Engineering and System Safety, Vol. 53, pp. 115-126, 1996.

**INFORMS
San Antonio, November 2000**

OUTLINE

- **PROACTIVE VS. REACTIVE RISK MANAGEMENT POLICIES**
- **A DIFFERENT INTERPRETATION OF THE PRINCIPLE OF PRECAUTION**
- **THE USE OF PROBABILISTIC RISK ANALYSIS TO IDENTIFY PROBLEMS THAT HAVE NOT HAPPENED YET**
- **EXTENSION OF PROBABILISTIC RISK ANALYSIS TO INCLUDE MANAGEMENT FACTORS**
- **THE TRADEOFF BETWEEN SAFETY AND DELAYS IN UNPLANNED AIRPLANE MAINTENANCE**
- **PROBABILISTIC MODELING FOR THE FLAPS AND SLATS OF THE LEADING EDGE OF AIRPLANE X (APX)**

PROACTIVE vs. REACTIVE POLICIES

- **RARE EVENTS THAT DO NOT APPEAR ON PAST STATISTICS CAN BE EITHER IGNORED OR OVEREMPHASIZED**
- **REACTIVE POLICIES: DO NOTHING UNTIL PROVEN NECESSARY BY SIGNIFICANT STATISTICS ABOUT THE EVENT ITSELF (MEDICAL EXAMPLE)**
- **PROACTIVE POLICIES: IDENTIFY SYSTEMS WEAKNESSES, ASSESS CHANCES OF FAILURES AND TAKE PROACTIVE MEASURES BASED ON PRIORITIES**

PRINCIPLE OF PRECAUTION

- **TWO DIFFERENT CASES:**

AN EXISTING ACTIVITY (EX: AIRLINE OPERATIONS) vs. A NEW ONE

1. DOES “PRUDENCE” MEAN ”STOP EVERYTHING UNTIL PROVEN SAFE”?

2. OR TRY TO ANTICIPATE *WHAT HAS NOT HAPPENED YET* AND BALANCE COSTS AND BENEFITS TO SET PRIORITIES?

3. NEED FOR A PROACTIVE APPROACH IN BOTH CASES BASED ON FUNDAMENTAL KNOWLEDGE

TWO EXAMPLES OF REACTIVE ATTITUDES

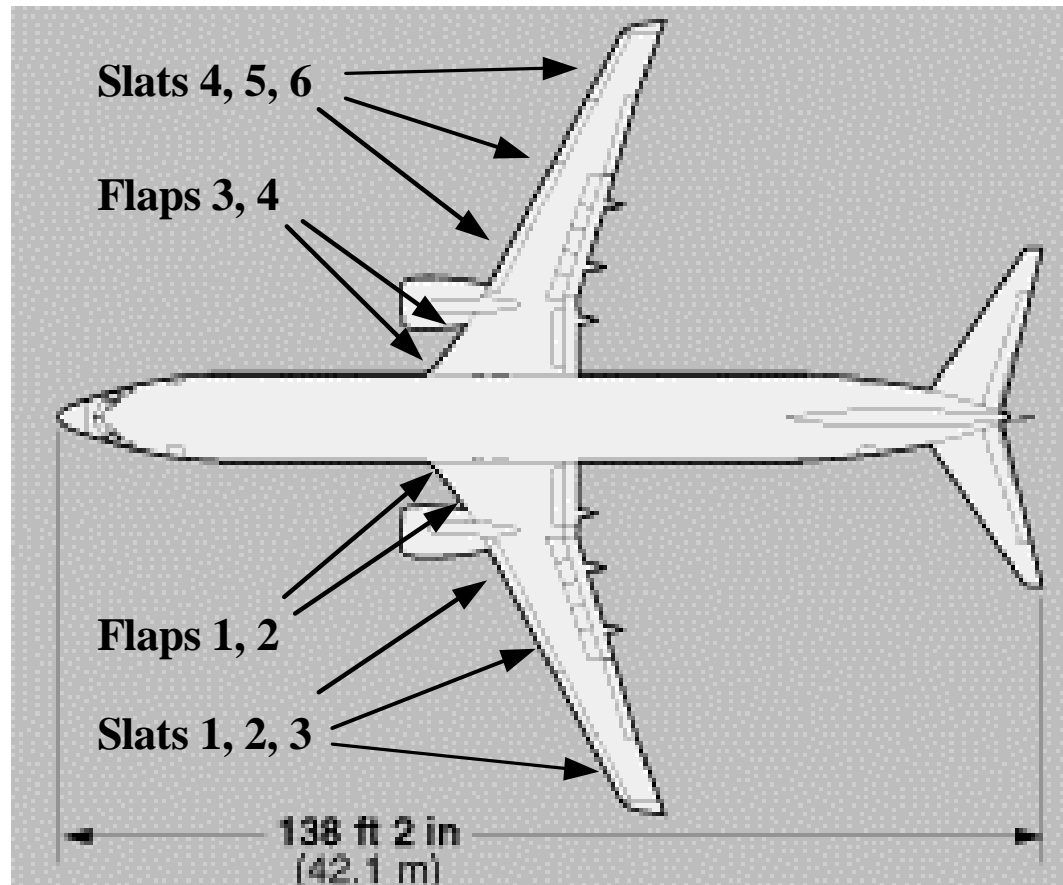
- **ANESTHESIA ACCIDENTS CAUSED BY MEDICAL ERRORS:**
**DOING NOTHING BECAUSE THERE ARE NOT “ENOUGH STATISTICS” TO
DETECT SOURCE AND TYPE OF ERRORS**

 - **AIRLINE ACCIDENTS:**
**VERY LOW RATE (10^{-7} PER TAKEOFF IN THE U.S. DOMESTIC MARKET).
TENDENCY TO BLAME “HUMAN ERRORS” AND TO WAIT UNTIL A
PROBLEM CAUSED AT LEAST ONE CRASH TO ADDRESS IT**
- THE ZILLION MILES ARGUMENT: “IT WON’T HAPPEN BECAUSE WE
HAVE FLOWN WITH IT FOR X MILLION MILES AND WE DID NOT CRASH
YET BECAUSE OF THIS”**

ALTERNATIVE: BAYESIAN METHOD

- **OBJECTIVE: IDENTIFY RARE FAILURE MODES (ACCIDENT SEQUENCES) AND THEIR PROBABILITIES, WEAK POINTS AND FIXES.**
- **QUANTITATIVE PROBABILISTIC ANALYSIS BASED ON BAYESIAN PROBABILITY.**
SOURCES OF DATA: FUNDAMENTAL MECHANISMS, STATISTICS, SURROGATE DATA ENGINEERING AND ORGANIZATIONAL MODELS, EXPERT OPINIONS, ETC.
ALLOW UPDATING OF PROBABILITIES “IN REAL TIME”.
- **USE OF INFLUENCE DIAGRAMS (BAYESIAN NETWORKS) EQUIVALENT TO DECISION TREES. INCLUDE:**
 - ⇒ **DECISION NODES**
 - ⇒ **STATE NODES (WITH PROBABILITY DISTRIBUTIONS)**
 - ⇒ **OUTCOME NODES****ARROWS REPRESENTING PROBABILISTIC DEPENDENCIES**
(*NOT A FLOW CHART*)

THE FLAPS AND SLATS OF THE “APX”



SLATS AND FLAPS OF THE LEADING EDGE OF THE “APX”

UNPLANNED MAINTENANCE BETWEEN FLIGHTS

- **PILOT WRITE-UP DURING FLIGHT**
- **“TROUBLE SHOOTING” AND VERIFICATION (PROBLEM EXISTS OR NOT)**
- **CLASSIFICATION OF PROBLEM AS DEFERRABLE OR NOT**
- **MAINTENANCE AND REPAIR IF NON DEFERRABLE**
- **CHECK BY FAA-CERTIFIED MECHANIC**
- **PILOT “WALK AROUND” AND DECISION TO TAKEOFF**

**ERRORS OF MAINTENANCE, LACK OF INFORMATION, CORNER CUTTING,
AND EFFECTS ON BOTH SAFETY AND DELAYS?**

LEADING EDGE FLAPS AND SLATS OF THE APX

FUNCTIONS AND MALFUNCTIONS

-
- **ALLOW AIRPLANE OPERATIONS ON SHORT RUNWAY**
 - **COMPONENTS: ELECTRONIC, HYDRAULIC, MECHANICAL**
(ELECTRONIC SENSORS OUTSIDE, SIGNALS IN THE COCKPIT)
 - **PLANE CAN STILL FLY WITHOUT F&S (NEEDS LONGER RUNWAY)**
 - **INCIDENT IN FLIGHT: F&S EXTEND ASYMMETRICALLY**
 - **PLANE TENDS TO ROLL; PILOT BALANCES THE PLANE USING THE**
RUDDER AND THE ELEVATION CONTROL (SHOULD BE NO
PROBLEM)

AIRPLANE ACCIDENTS CAN OCCUR (BUT HAVE NEVER HAPPENED YET)

- **IF F&S DROP AT TAKEOFF**
- **IF PILOT DOES NOT REACT PROPERLY IN FLIGHT**
- **IF ANOTHER FAILURE HAPPENS AT THE SAME TIME IN FLIGHT**

ANALYTICAL PROBLEM (RISK ANALYSIS):

⇒ **IDENTIFY CONJUNCTIONS OF EVENTS (INCLUDING
DEPENDENCIES) INVOLVING F&S MALFUNCTION THAT CAN LEAD TO
A CRASH**

⇒ **COMPUTE THEIR PROBABILITIES AND THEIR LINK TO
MAINTENANCE OPERATIONS**

EXCELLENCE IN MAINTENANCE

QUALITATIVE DESCRIPTION

- **CORRECT IDENTIFICATION OF PROBLEM BY PILOT (NO T. 1 OR T. 2 ERROR)**
- **INTERVENTION OF MAINTENANCE CREW IMMEDIATELY AFTER LANDING**
- **AVAILABILITY OF ALL NEEDED PARTS OR OF A SPARE PLANE**
- **COMPETENT CREW: CORRECTLY IDENTIFIES PROBLEM (NO TYPE I AND TYPE 2 ERRORS)**
- **PERFECT INSPECTION OF COMPLETED REPAIR WORK**
- **STRICT MANAGEMENT OF DEFERRABLE ITEM**

=> DELAY OCCURS IF MAINTENANCE TIME EXCEEDS LAYOVER TIME

=> ACCIDENTS CAN OCCUR IF MAINTENANCE ERROR CAUSES IN-FLIGHT

INCIDENT COMPOUNDED BY OTHER FACTORS => *TRADEOFF*

THE TRADEOFF

BETWEEN MAINTENANCE AND DELAYS

- **MAINTENANCE CAN START TOO LATE AFTER LANDING**
- **PROBLEM MAY NOT EXIST BUT VERIFICATION TAKES TIME**
- **PARTS MAY NOT BE AVAILABLE (E.G., BECAUSE OF LOCATION)**
- **NO SPARE PLANE => FLIGHT CANCELLED**
- **THE PROBLEM (S) MAY NOT HAVE BEEN PROPERLY IDENTIFIED**
=> FIXING TAKES TIME BUT DOES NOT ADDRESS REAL ISSUE
- **THE PILOT DOES NOT TRUST THAT THE PROBLEM WAS FIXED**

IDENTIFICATION OF TECHNICAL AND HUMAN WEAKNESSES IN ENGINEERED SYSTEMS

THE SAM MODEL: THREE TIERS

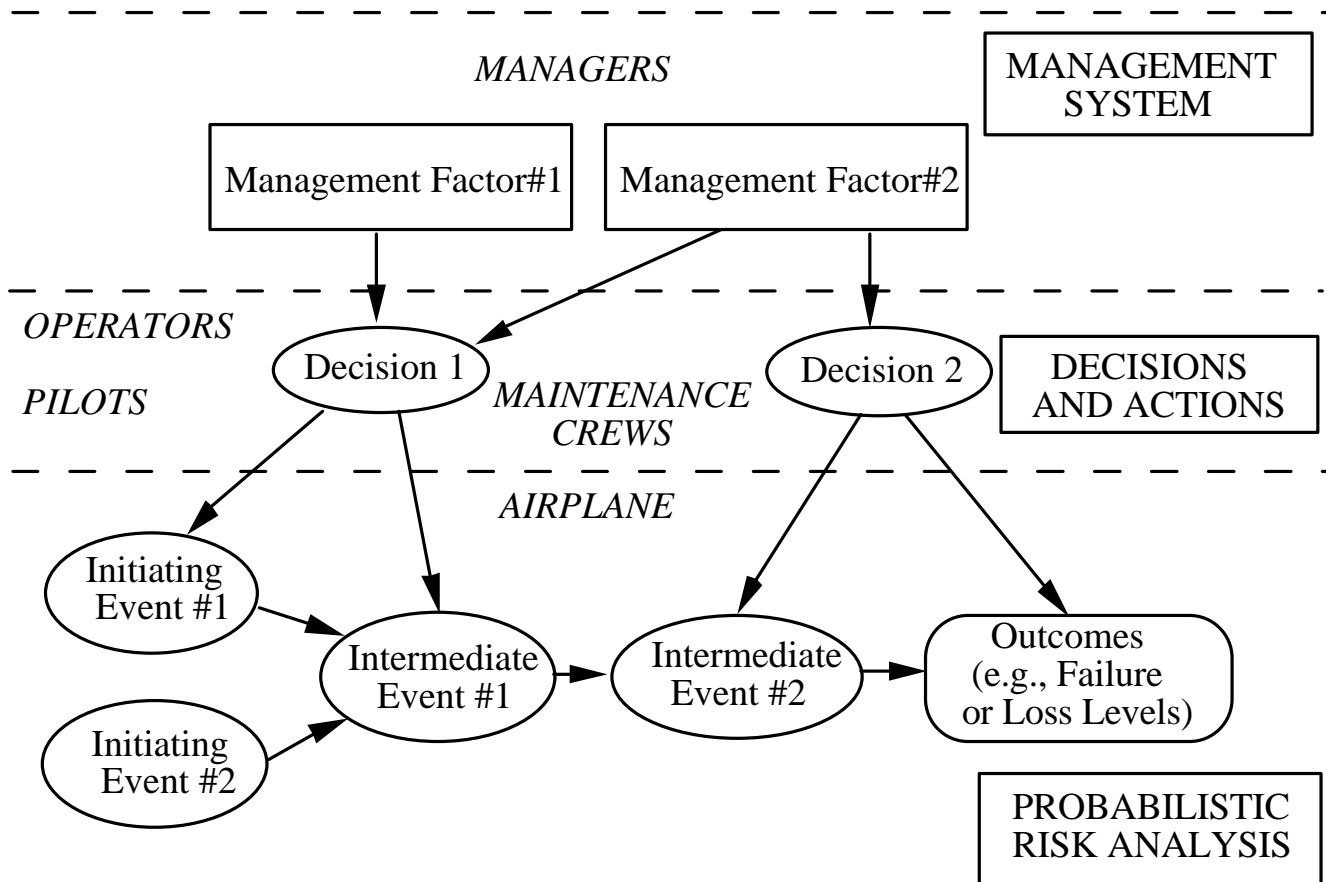
1. PROBABILISTIC RISK ANALYSIS OF THE SYSTEM

- FUNCTIONAL ANALYSIS**
- PROBABILISTIC ANALYSIS**

2. HUMAN DECISIONS AND ACTIONS

3. MANAGEMENT AND ORGANIZATIONAL FACTORS

THE S.A.M. MODEL



A THREE-TIER ANALYSIS:

TECHNICAL PRA, HUMAN DECISIONS AND ACTIONS, MANAGEMENT FACTORS THE ILLUSION OF PERFECTION

AND PROBLEMS WITH ACCIDENTS THAT HAVE NOT HAPPENED YET

- **SOMETIMES, WE DON'T KNOW THE SYSTEM'S WEAKNESSES**
 - => CAN'T SET PRIORITIES UNDER RESOURCE (E.G., TIME)**
 - CONSTRAINTS**
- **DEFERRAL SYSTEM ALLOWS DELAYING FIXING MINOR PROBLEMS**
- **DON'T KNOW WHERE TO FOCUS WORK INSPECTION**
- **DON'T KNOW HOW TO MONITOR SHORT CUTS AND ASSESS THE SAFETY EFFECTS OF DEFERRAL**
- **(DON'T) KEEP YOUR FINGERS CROSSED AND HOPE THAT NO ONE MESSES UP IN THE WRONG PLACE**

QUANTITATIVE MODEL OF THE RISK/DELAY TRADEOFF

REPRESENTATION: A THREE-TIER INFLUENCE DIAGRAM

(AN EXAMPLE OF THE S.A.M. FRAMEWORK)

1. MANAGEMENT DECISIONS

QUALIFICATION OF THE MAINTENANCE PERSONNEL

TIMING OF MAINTENANCE OPERATIONS

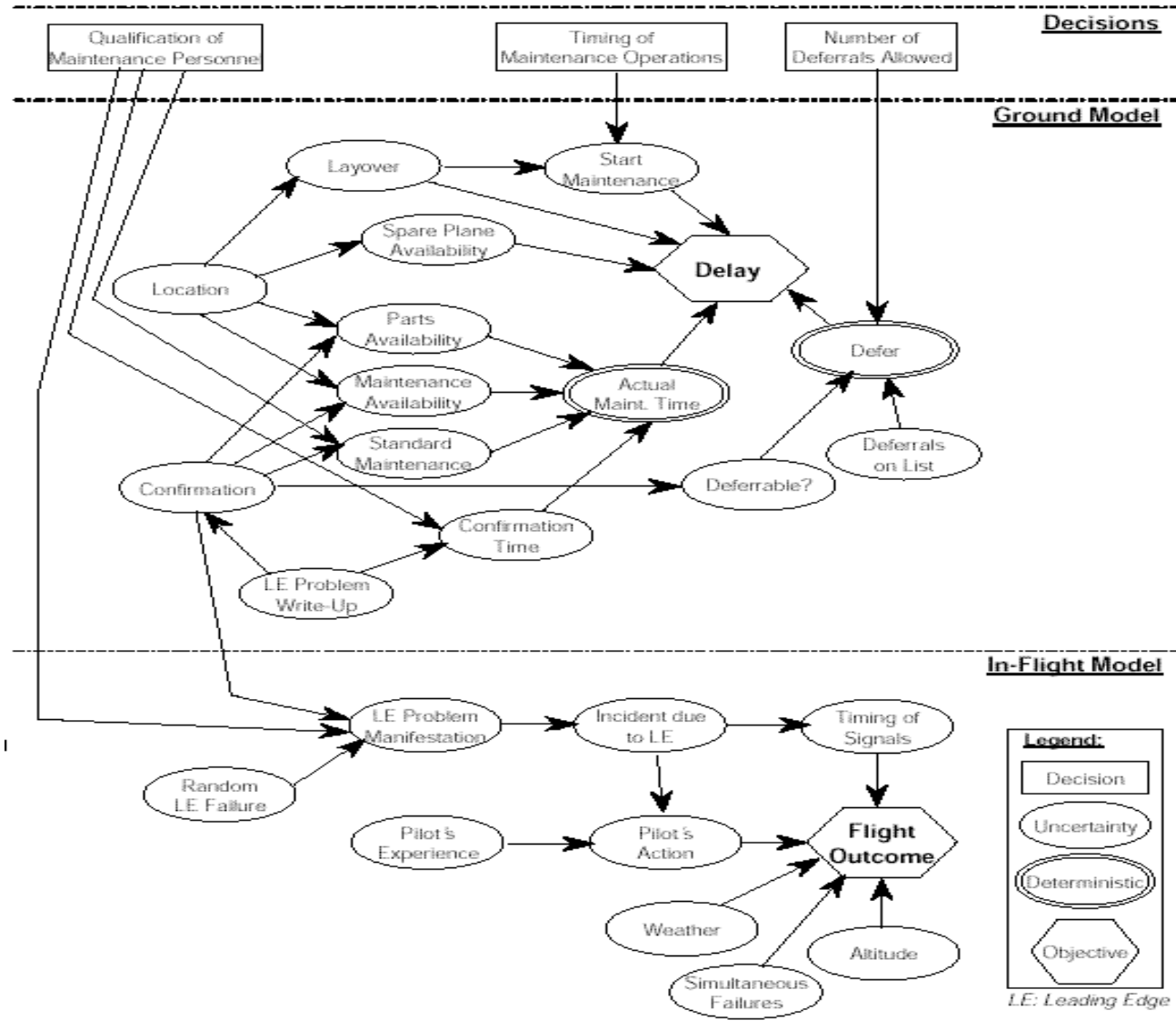
NUMBER OF DEFERRALS ALLOWED

THAT AFFECT

2. A GROUND MODEL AND

3. AN IN-FLIGHT MODEL

INFLUENCE DIAGRAM REPRESENTING THE PROBABILISTIC MODEL



MANAGEMENT DECISION VARIABLES

- **QUALIFICATION OF MAINTENANCE PERSONNEL**

ILLUSTRATION HERE: “STANDARD” VS “PERFECT” (AFFECTS COSTS AND PROBABILITY OF ERROR)

- **TIMING OF MAINTENANCE**

ILLUSTRATION HERE: “STRICT” POLICY = GATE-IN PRACTICE (START ASAP)

“TOLERANT” POLICY” = GATE-OUT PRACTICE (SCHEDULED DEPARTURE TIME MINUS STANDARD MAINTENANCE TIME) => NO SLACK

- **NUMBER OF DEFERRALS ALLOWED**

ILLUSTRATION HERE: FROM 2 TO 5

RESULTS

- **FROM THE MODELING PROCESS:**
SOFTWARE MAINTENANCE PROBLEMS. DATA COLLECTION AND STORAGE (COMPATIBILITY, TERMINOLOGY),
- **NUMERICAL INSIGHTS:**
(DATA MODIFIED FOR CONFIDENTIALITY REASONS) SIMULATION FOR 45,000 FLIGHTS.
ASSUME FLIGHT CANCELLATION IF DELAY > 3 HOURS
MOST IMPORTANT VARIABLE: QUALIFICATION OF MAINTENANCE PERSONNEL
- **SHIFT IN AIRLINE CULTURE: PROACTIVE VS REACTIVE POLICIES**

NUMERICAL RESULTS

EFFECTS OF MAINTENANCE ON PROBABILITY OF DELAYS

ASSUME: PROBABILITY(L.E. PROBLEM) = 10^{-3} /FLIGHT

BEST SITUATION

- FOR A MAXIMUM OF TWO DEFERRALS PER PLANE, (**BEST**)
- “STRICT” TIMING OF MAINTENANCE OPERATIONS
- AND “INCREASED” QUALIFICATION OF MAINTENANCE PERSONNEL

CONDITIONAL P(DELAY|LEPROBL.) 0.7 => MARGINAL P(DELAY/FLIGHT) 7×10^{-4}

CONDITIONAL P(CANCEL.|DELAY) = 0.75 => MARGINAL P(CANCEL.FLIGHT) 7.5×10^{-4}

CONDITIONAL MEAN OF DELAY LENGTH *GIVEN NO CANCELLATION* = 8 MINUTES

STANDARD SITUATION

- FOR A MAXIMUM OF FIVE DEFERRALS PER PLANE, (**STANDARD**)
- “TOLERANT” TIMING OF MAINTENANCE OPERATIONS AND
- AND “STANDARD” QUALIFICATION OF MAINTENANCE PERSONNEL

CONDITIONAL P(DELAY|LE PROBL.) 0.6 => MARGINAL P(DELAY/FLIGHT) 6×10^{-4}

CONDITIONAL P(CANCEL.|DELAY) = 0.28 => MARGINAL P(CANCEL.FLIGHT) 2.8×10^{-4}

CONDITIONAL MEAN OF DELAY LENGTH *GIVEN NO CANCELLATION* = 78 MINUTES

NUMERICAL RESULTS

EFFECTS OF MAINTENANCE ON FLIGHT SAFETY

- “STANDARD” MAINTENANCE POLICY (EVERYTHING STANDARD)
=> $P(\text{ACCIDENT} \mid \text{L.E. PROBLEM}) = 6.7 \text{ in } 45,000 \text{ FLIGHT CYCLES} = 1.48 \times 10^{-4}$
=> $P(\text{ACCIDENT}) = 1.48 \times 10^{-7}$

[OBVIOUSLY MUCH HIGHER THAN WHAT.

US EXPERIENCE SHOWS: $P(\text{ACCIDENT FROM ALL CAUSES}) = 10^{-7}/\text{FLIGHT}$]

- “STRICT” MAINTENANCE POLICY (EVERYTHING “BETTER”)
=> $P(\text{ACCIDENT} \mid \text{L.E. PROBLEM}) = 6.6 \text{ in } 45,000 \text{ FLIGHT CYCLES} = 1.46 \times 10^{-4}$
=> $P(\text{ACCIDENT}) = 1.46 \times 10^{-7} \Rightarrow \underline{2\% \text{ DIFFERENCE ONLY}}$

LIMITATIONS OF THE QUANTITATIVE APPROACH

- **INSUFFICIENT STATISTICAL DATA AND PROBLEM STRUCTURING**
- **SUBJECTIVITY OF SOME ESTIMATES (EXPERT OPINIONS)**
- **COMPLETENESS OF FAILURE SCENARIOS**
- **UNWARRANTED IMPLICATIONS OF RISK ACCEPTABILITY**
- **TREATMENT OF HUMAN ERRORS**
- **HIDDEN ASSUMPTIONS**

BUT:

- * **BEST USE OF PROBABILISTIC ANALYSIS IS FOR AN ORGANIZATION
THAT WANTS TO GENERATE AND USE THE RESULTS**
- * **PROACTIVE APPROACH BEATS THE “ZILLION MILES” ARGUMENT**

CONCLUSIONS

- **RESULTS ONLY AS GOOD AS THE MODEL AND THE DATA**
- **PROBABILISTIC ANALYSIS PARTICULARLY USEFUL WHEN AN ACCIDENT HAS NOT OCCURRED YET (PROACTIVE VS REACTIVE POLICIES)**
- **THE MORE COMPLEX THE SYSTEM, THE MORE USEFUL THE ANALYSIS**
- **QUALITATIVE SOLUTIONS DO NOT ALWAYS PERMIT IDENTIFICATION OF WEAK POINTS, DO NOT ALLOW SETTING PRIORITIES AND WORK BEST WHEN THE SYSTEM IS KNOWN AND SIMPLE (OR TOO COMPLEX FOR ANALYSIS)**