

NATIONAL TRANSPORTATION SAFETY BOARD
Office of Aviation Safety
Washington, D.C. 20594

May 19, 2000

Systems Group Chairman's Factual Report Addendum for Fault Tree Data

DCA-96-MA-070

A. ACCIDENT

Location : East Moriches, New York
Date : July 17, 1996
Time : 2031 Eastern Daylight Time
Airplane : Boeing 747-131, N93119

B. SYSTEMS GROUP

Chairman : Robert Swaim
NTSB
Washington, DC
Assistant : Scott Warren
NTSB
Washington, DC

C. SUMMARY

On July 19, 1996, at 2031 eastern daylight time, a Boeing 747-131, N93119, crashed into the Atlantic Ocean, about 8 miles south of East Moriches, New York, shortly after takeoff from John F. Kennedy International Airport (JFK). The airplane was being operated under an instrument flight rules (IFR) flight plan under the provisions of Title 14, Code of Federal Regulations (CFR), Part 121, as a regularly scheduled flight to Charles De Gaulle International Airport (CDG), Paris, France, as Trans World Airlines (TWA) flight 800. The airplane was destroyed, and all 230 people on board were killed.

As part of the accident investigation, Boeing submitted a center wing tank (CWT) ignition fault tree report on November 25, 1996 followed by the first revision on December 20, 1996. The fault tree considers the ignition of the CWT to be the top level

failure mode, and the impact of all lower level elements which compose the tree are evaluated using mathematical probability relationships. On June 4, 1998, the Safety Board requested that Boeing review and further revise the fault tree. Boeing declined this request citing a preference to utilize its resources to continue the various inspection and modification programs already underway.

D. DETAILS OF THE INVESTIGATION

Current FAA regulations governing the certification of new airplanes require that a quantitative evaluation be conducted to determine the probability levels for systems failures. These probability levels are required to fall between various levels depending on the severity of the consequences for a given failure. When 747-136, N93119 was certified, there were no requirements for the quantitative evaluation of probability levels for catastrophic failures. The Boeing 747-100 series airplanes were certificated on December 30, 1969. The regulatory guidelines that covered quantitative evaluation of failure modes were adopted in April, 1970 as amendment 25-23 to 14 CFR Part 25. Amendment 25-23 included Section 25.1309 to which AC 25.1309-1A is applicable. The quantitative evaluation procedures are detailed in AC 25.1309-1A. The allowable probability levels are quoted for different failure consequence levels (minor, major, and catastrophic). Section 25.1309 states that airplane systems must be designed so that the occurrence of any catastrophic failure (a failure condition which would prevent the continued safe flight and landing of the airplane) is extremely improbable. Advisory circular AC 25.1309-1A defines the term "extremely improbable" as failure conditions that are "so unlikely that they are not anticipated to occur during the entire operational life of all airplanes of one type". These conditions are further defined as having a probability on the order of $1e-09$ or less.

As part of the National Transportation Safety Board investigation into TWA flight 800, Boeing submitted a center wing tank (CWT) ignition fault tree report on November 25, 1996 followed by the first revision on December 20, 1996.

According to Boeing, the fault tree includes ignition sources that come from three different sources. The first source includes external events (meaning external to the CWT) such as lightning, fires in other parts of the airplane, and induced voltage transients. The second source includes electrically generated faults such as wiring faults in the various systems connected to the CWT. The third source includes mechanical faults such as metal parts striking one another to create a spark and mechanical pump failures. The fault tree consists of 167 basic elements (basic elements are those elements which have no predecessors in the tree) which are combined to generate the top level probability of failure.

The CWT ignition fault tree considers the ignition of the CWT to be the top level failure mode, and the impact of all lower level elements which compose the tree are evaluated using mathematical probability relationships. The fault tree builds down from the top level event by determining the conditions required for each event. Eventually, the

tree reaches a level where an event has no preceding events. These lowest level events are called basic elements. According to Boeing, each basic element is assigned a failure rate and exposure time based on either in-service data or engineering estimates. These are combined to produce a probability of failure for each element. The formula used for determining the probability is:

$$\text{Probability of failure} = 1 - e^{(-\text{failure rate} * \text{exposure time})}$$

The failure probabilities for each element are combined mathematically to generate the top level failure mode probability. The probabilities are combined using “and” and “or” logic gates. The “and” gate is used when two (or more) elements are required to have a given condition be true. The “or” gate is used when the resulting condition can be reached with either of the two lower level elements being true.

The Boeing fault tree report explicitly states the assumptions used by Boeing to generate their report. The assumptions are listed below:

1. Configuration of the aircraft is as originally delivered plus pertinent airworthiness directives and known incorporated service bulletins.
2. Only events considered germane to the TWA event have been quantified.
3. Aircraft is assumed to be in climb/cruise configuration.
4. Service bulletin to de-activate water injection was incorporated but wiring was still in (the fuel tank) dry bay.
5. The CWT FQIS worked normally on the previous flight.
6. Override/jettison and scavenge transfer pumps are not GFI protected.
7. The delivery schedule of this report requires that many of the failure rates developed for events in this report be subjectively established. Using the qualitative criteria contained in FAA AC 1309-1A as shown below, best engineering judgement used qualitative risk assessment and then assigned quantitative values.
 - a. Probable 1e-05
 - b. Improbable 1e-06 to 1e-08
 - c. Extremely Improbable 1e-09

8. Quantitative rates assigned were the result of experience with system and discussion with subject matter specialists.
9. Failure rates will be reviewed for refinement as the final fault tree analysis is constructed.¹
10. Air cycle machines were determined to be intact at impact.
11. Override/jettison pumps were determined to be intact at impact.
12. There were no failures of equipment in the wheel well.
13. Lightning was not a factor in this scenario.
14. A combustible fuel/air mixture existed in all fuel tank air spaces as modeled.
15. A combustible fuel/air mixture existed in all non-fuel tank air spaces when fuel leakage was present.
16. Fire did not originate in the forward cargo compartment.
17. Scavenge pump switch was turned off at the time of the event.

Examples of basic elements included in the Boeing fault tree report are shown in Table 1.

¹ (Note: Other than the first revision already noted in this report, no further fault tree analysis was ever delivered).

Table 1
EXAMPLES OF BASIC ELEMENTS

Number	Description	Event Failure Rate (events/hour)	Event Exposure Time (hours)	Event Probability
1	Assume Fuel/Air Mixture Exists in CWT Sufficient to Support Explosion	n/a	n/a	1e00
2	Metallic Object Capable of Creating Spark Resides in CWT	1e-06	8.0	8e-06
3	Tank Sealant Decays and Second Metallic Striking Surface Becomes Available	1e-07	8.0	8e-07
4	Electrical Faults in Surge Tank Create Ignition Source	1e-07	8.0	8e-07
5	Fire Propagates from Surge Tank to CWT	1e-06	8.0	8e-06
6	Conductive Material Bridging Hi-Z and Lo-Z Terminals	3.55e-07	8.0	2.84e-06
7	Unique Wire to Wire Faults (Power on Wire) Route to FQIS Leads in Right Wing	2.44e-07	8	1.95e-06
8	Fuel Probe Contacts Structure	3.55e-07	8	2.84e-06
9	Unique Wire to Wire Faults (Power on Wire) Route to FQIS Leads in Left Wing	2.44e-07	8	1.95e-06
10	Fire Propagates from Center Dry Bay to CWT (Autoignition)	1e-05	8	8e-05
11	Combustible Fuel/Air Mixture Exists in Air Conditioner Bay	n/a	n/a	1e00
12	Explosion Proofed Equipment does not Failsafe as Designed	1e-08	60000	6e-04
13	Fire Propagates from Air Conditioner Bay to Dry Bay	1e-05	8.0	8e-05
14	Fuel Leak to Air Conditioner Bay	1e-05	8.0	8e-05
15	Volumetric Shutoff Unit Internal Fault Results in Power on FQIS Lead	1.4e-07	8.0	1.12e-06
16	FQIS Wiring Fault Produces Ignition Source in Main Tank	1e-06	8.0	8e-06

The fault tree report, as provided by Boeing, contains a graphical representation of the fault tree as well as a table containing the failure rate and exposure time information for the fault tree's basic elements. For some elements, the information in the graphical presentation of the fault tree and the information in the table did not agree. For some elements, the disagreements were of several orders of magnitude. The elements with disagreements between the graphical data and the table data are presented in table 2. Using the graphical representation data for the fault tree, the probability of the top level failure mode was 8.45e-11.

Table 2
ELEMENTS WITH DISAGREEMENTS BETWEEN THE TABLE AND GRAPHICAL
VALUES

Event Name	Description	Failure Rate (graphical)	Failure Rate (table)	Exposure time (graphical)	Exposure time (table)	Probability of Failure (graphical)	Probability of Failure (table)
WAH14533	Optimum Air Gap Exists	4.00E-07	4.00E-07	0.22	8	8.80E-08	3.20E-06
AH14533	Optimum Air Gap Exists	4.00E-07	4.00E-07	0.22	0.2	8.00E-08	8.00E-08
FUEL_LK8	Leak Through Sob Rib From Web Fatigue Crack	7.69E-07	1.00E-05	8	8	6.15E-06	8.00E-05
AJ1453	Air Gap To Ground Exists	4.00E-07	N/A	0.22	N/A	8.80E-08	1.00E+00
AA153S	Scavenge Pump Deterioration Or Pump Wear Results In Loss Of Protection	3.40E-08	6.90E-07	8	8	2.72E-07	5.52E-06
G37	Foreign Object Provides Ground In Cwt	N/A	N/A	N/A	N/A	1.00E-06	1.00E+00
G5	Current Limit Circuit Failure (No Current Limit In Indicator)	1.10E-07	8.00E-07	8	8	8.80E-07	6.40E-06
CF211	Circuit Breaker Fails Closed	4.76E-06	4.76E-06	60000	60000	2.86E-01	2.48E-01
CF212	Short To Power On Lo-Z Lead In Wire Bundle	2.44E-08	4.07E-08	8	8	1.95E-07	3.26E-07

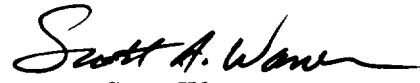
Table 2 (Continued)

Event Name	Description	Failure Rate (graphical)	Failure Rate (table)	Exposure time (graphical)	Exposure time (table)	Probability of Failure (graphical)	Probability of Failure (table)
8	Wire To Wire (Comp Lo-Z Short Inside Press Hull (Power On Wire) W985	4.07E-09	2.44E-07	8	8	3.26E-08	1.95E-06
AA1512	Sufficient Energy Created To Ignite Fuel/Air Mixture	1.00E-07	1.00E-05	8	8	8.00E-07	8.00E-05
AE152	Tank Sealant Decays And Second Metallic Striking Surface Becomes Available	1.00E-07	1.00E-06	8	8	8.00E-07	8.00E-06
AA1521	Scavenge Pump Burn Through Results In Ignition Source In Pump	1.15E-08	1.00E-07	8	8	9.20E-08	8.00E-07
AA1524	Scavenge Pump Internal Friction Faults Result In Ignition Source In Pump	3.45E-07	2.00E-06	8	8	2.76E-06	1.60E-05

On June 4, 1998, the Safety Board, after reviewing the December 20, 1996 revision, requested that Boeing review and further revise the fault tree. The Safety Board had several questions regarding the detailed information that was used to construct the fault tree and had determined that some of the information in the fault tree did not reflect the results of the ongoing investigation. In a letter dated July 29, 1998, Boeing responded that they would not revise the fault tree. Boeing agreed that some of the details pointed out by the Safety Board were correct, but stated:

“We do not believe that revising the FTA (fault tree analysis) by incorporating new data or changing the probability numbers will help identify new areas to inspect or help identify the cause of the accident. We believe it would be more productive to continue the various inspection and modification programs that are presently underway.”

Both the Safety Board's letter (minus proprietary attachments) and the Boeing response are included as Appendix A.



Scott Warren
Aerospace Engineer



APPENDIX A

- 1) National Transportation Safety Board Letter, Scott Warren to Dennis Rodrigues, "Systems Group Chairman's Request For Revision of TWA Flight 800 Center Wing Tank Ignition Fault Tree", dated June 4, 1998
- 2) Boeing Commercial Airplane Group Letter, John Purvis to Robert Swaim, "Fault Tree Analysis, TWA 747-100 N93119, Accident Near Long Island, NY - 17 July 1996", dated July 29, 1998



National Transportation Safety Board

Date : June 4, 1998

To : Dennis Rodrigues, Air Safety Investigation, Boeing Aircraft Company

From : Scott Warren

Subject : **SYSTEMS GROUP CHAIRMAN'S REQUEST FOR REVISION OF
TWA FLIGHT 800 CENTER WING TANK IGNITION FAULT
TREE**

This memorandum is to request that Boeing review and revise the Center Wing Tank (CWT) Ignition Fault Tree.

Boeing submitted the original CWT Ignition Fault Tree on 25 November, 1996 followed by the first revision on 20 December, 1996 in response to NTSB requests. The first revision included quantitative estimates for basic events required for a specific risk analysis and will be referred to as the "fault tree" in the remainder of this document. The fault tree, as submitted, provided a good starting point to estimate the basic probabilities of both the top level event (conditions for explosion exist in the CWT) as well as intermediary and basic events. Since the original submission of the fault tree, many tests have been performed as part of the TWA Flight 800 accident investigation. These tests have generated results which may affect the original basic event failure rate estimates as well as the structure of the fault tree itself. With the assistance of the Safety and Risk Management Branch at NASA Headquarters, the NTSB has concluded that both the exposure times and failure rates used for many basic events needs to be revised.

The fault tree, as submitted, contained exposure times which were considered to be too low by the NTSB/NASA review. The exposure times should reflect the amount of time that a given item is exposed to the potential of a fault occurring. In particular, the exposure time should equal the flight time incurred by the aircraft unless the item has been inspected for that particular fault. Most of the exposure times used in the fault tree were 8 hours. These times should be revised to reflect the time since the last inspection (e.g. time since last D check was 13,036 hours, time since last C check was 2,219 hours, etc.) whenever it may have occurred.

In the course of the TWA Flight 800 accident investigation, numerous inspections of high time aircraft have been conducted. These inspections have found a consistent pattern of contamination and adverse aging characteristics of electrical components. For example, the inspections have found conductive lint and chemical contamination of wire surfaces, cracked wires, drill shavings on top of and within wire bundles, and copper sulfide contamination of fuel system electrical components. The consistent pattern of these inspection results should be reflected in the failure rates used by the fault tree.

I have included, as a sample, a portion of the fault tree which includes comments made by Bob Swaim and myself. While the included pages are only a portion of the complete fault tree, please use these comments as examples of the types of revisions which the NSTB considers to be required throughout the entire document.

This request is an extension of the comments generated during the recent systems group meetings in Washington, but if you have any questions regarding the nature of the revisions or the scope of the work requested, please do not hesitate to call me. I can be reached at 202-314-6399 or at warrens@ntsb.gov. If at all possible, the Systems Group Chairman would like for the final revisions to be complete by 1 July, 1998.



Scott Warren
Aerospace Engineer (Systems)



Robert Swaim
Systems Group Chairman
TWA Flight 800 Investigation

Enclosure:

1. Partial copy of fault tree

29 July 1998
B-B600-15462-AS

Mr. R. Swaim, AS-40
National Transportation Safety Board
490 L'Entant Plaza East, S.W.
Washington D.C. 20594-2000



Subject: Fault Tree Analysis, TWA 747-100 N93119, Accident Near Long Island, NY - 17 July 1996

Reference: Your letter dated June 4, 1998

Dear Mr. Swaim:

In your reference letter, you suggested changes and raised some questions regarding the Fault Tree Analysis (FTA) and requested that Boeing review and revise the FTA. The comments in your letter can be broadly categorized as follows:

- Comments regarding how the investigation results would influence the existing FTA,
- Comments regarding how the FTA would change for a "Generic" fleet FTA,
- Comments regarding the mechanics for construction of the FTA,

Boeing developed the TWA 800 Fault Tree as a tool for guiding the TWA 800 investigation. The objective was to identify all the possible scenarios that could have led to the Center Wing Tank (CWT) explosion on the TWA 800 aircraft. Boeing believes that the evaluation of the data gained from the investigation and airplane inspections confirms that the FTA served its intended purpose in providing this guidance. The FTA, along with the data from the investigation, substantiated possible scenarios and eliminated others.

With regards as to how the investigation results would influence the FTA, most or all of the areas of interest identified through the information gathered during the investigation, particularly during inspections of older, retired and scrapped airplanes, are already addressed in the existing FTA. These identified areas have been pursued in the investigation. Areas of interest not identified in the FTA that are considered to be issues, need to be investigated as well. In the absence of an identified cause of the accident, all items identified on the FTA that are of potential interest, regardless of the probability numbers, should be investigated. Information learned from the "generic" fleet inspections should be pursued as well, again regardless of any affect on the FTA.



The question of exposure times and failure rates all deal with the mechanics of constructing the FTA. The use of the 8 hour exposure time identifies any event that becomes apparent to the crew at each flight. This requires some type of inspection or test, or equipment interaction which makes the occurrence of the event apparent. For instance, the existence of a "short" in an electrical circuit almost always adversely affects the output of a gage or other electronic equipment to the point where the "short" becomes apparent. Leaks in the fuel system become apparent to the crew during ground inspections. There are some instances where the NTSB has correctly pointed out that events with an 8 hour exposure time are only inspected during scheduled "C" or "D" checks.

The data gained from the investigation and from the fleet inspections are being dealt with through several avenues such as service bulletin inspections and modifications to the system to further raise the level of safety already built into the system. We do not believe that revising the FTA by incorporating new data or changing the probability numbers will help identify new areas to inspect or help identify the cause of the accident. We believe it would be more productive to continue the various inspection and modification programs that are presently underway.

If you have any questions, please do not hesitate to call.

Very truly yours,

A handwritten signature in black ink, appearing to read 'John W. Purvis', written over the typed name.

John W. Purvis
Director, Air Safety Investigation
Org. B-B600, M/S 67-PR
Telex 32-9430, STA DIR PURVIS
Phone (425) 237-8525
Fax (425) 237-8188

cc: Mr. A. Dickinson, IIC
Mr. S. Warren