The WBA Workbook

Causalis in der IIT GmbH

info@causalis.com

October 13, 2005

Contents

Chapter 1

About this Workbook

This book provides five case descriptions for use in learning the Why-Besause-Analysis. The cases are breifly described and some sample WB-Graphs are given. The cases differ in length, complexity and domain.

- The first case is a so called "friendly fire" accident that occurred during Operation Enduring Freedom in Afghanistan. Its an easy case and a good point to start learning Why-Because-Analysis.
- The second case is a railway accident that happened near Warngau, Germany in 1975. Two trains collided head on. The case has been stripped to the accident description itself. The original case deals with many issues of German railroad operation bureaucracy, these have been omitted here.
- The third case is the capsize of a car ferry outside the port of Zeebrugge. It is an easy case and the graph produced is actually a tree.
- The fourth case is taken from the aviation domain. During a flights simulator test pilots experienced mode confusion. Automation facilities changed state without operators noticing.
- The fifth case deals with a runway miss by approximately 300 miles. A DC-10 landed in Brussels airport expecting it to be their designated destination, Frankfurt.
- The sixth case is the grounding of a cruise ship on a shoal off the coast of Massachusetts. The case involves the failure of human and technical protection mechanisms and interaction between them.

Chapter 2

Performing a WBA Analysis The WBA Process

This guide to the Why-Because Analysis (WBA) method concentrates on the detailed steps necessary to perform a WBA. The data to create this guide and the flow charts were determined by Hierarchical Task Analysis [Paul-Stüve 05]. The flow charts follow the IBM Flowcharting Techniques guide, which complies with the requirements of the ISO standard [IBM 69].

2.1 Process Overview

A Why-Because Analysis (WBA) [Ladkin 01, Ladkin 02] starts with gathering information about the incident (Figure 2.1). This information is then used to construct either a *List of Facts* (facts listed alone) or a *Why-Because List*.

The construction of the *Why-Because Graph* (WB Graph, WBG) starts with determining the mishap (the "top node"). Then the necessary causal factors (NCF) that finally led to the mishap are determined, using the Why-Because List, until a chosen level of detail is reached. Finally, the quality (correctness and explanatory completeness) of the WBG is assured by detecting and correcting errors. A report can then be written using the WBG.

The WBA process is factored here into eight subprocesses, explained using flowchart notation.

2.2 Gather Information

As shown in Figure 2.2, the first step is information gathering. First, the sources of information must be identified. These can be, for example, witness reports, responsible authorities, or applicable documentation. (It has proven useful to get printed copies of the material.)

The quality of the information must be assessed. Checking the sources and doing some background research helps. If a team is performing the WBA, the information material can be discussed. Finally, the useful information material is selected.

2.3 Determine the Facts

The selected information material is read again in-depth to identify the statements that concern the course of events. These statements are split into single events. Presumptions must also explicitly be identified in order to extract the facts! (Figure 2.3) There are at least two ways to arrange the facts, both shown in Figure 2.4: one may apply the Counterfactual Test earlier (to form a Why-Because List) or later (one creates then a List of Facts).

2.4 Create a List of Facts

A List of Facts is a collection of all the facts that might be relevant to the incident. Every fact determined is written down with (at least) a serial number, a brief description suitable for a title, and a reference to its origin.

2.5 Create a Why-Because List

A Why-Because List incorporates information about the facts and their relations to each other. These relations are expressed in Why-Because pairs of facts. First, every fact is noted with a serial number, a description, and its reference. When all facts have been recorded this way, the **Counterfactual Test** is applied to every pair. If there are any discrepancies, the Why-Because List has to be corrected. Finally the List is checked for completeness and consistency and again corrected if necessary.

2.6 Create an Auxiliary List of Facts

An Auxiliary List of Facts is optional, but often helpful to an understanding of the incident (see Figure 2.5). After having created a List of Facts or a Why-Because List, a classification system, such as selection according to time (to create later a *Timeline*) or according to the actors involved (to create later a *Time-Actor Diagram*, or TAD), is chosen. Then every fact is filed under its class. Again, every fact is noted with a serial number, a description, and its reference. If there are facts that do not fit the classification system, the classification must be adapted.

2.7 Determine the Mishap / Top Node

The first task in creating a WB Graph is to determine the unwanted event that constitutes the incident, the mishap. This will be the top node of the WB Graph. To determine the mishap, the facts collected in the List of Facts or Why-Because List are reviewed and assessed (Figure 2.6). Often, the mishap will be obvious, especially in transportation system accidents. But in some cases, for example in computer security incidents in which many interests are involved, it may not be so easy to identify the mishap event.

The mishap is the event or circumstance that most directly caused the loss of resources, e.g., lives or money, that constitute the accident. These facts can be as obvious as "AC impacts mountain", but it can often become difficult to tell what makes up the accident. If working in a team, discussing the facts in the group is helpful.

The mishap is inserted as the top node in the WB Graph with a descriptive label and a reference to the List of Facts or Why-Because List.

2.8 Determine the Necessary Causal Factors

Determining the Necessary Causal Factors (NCFs) is an iterative process starting with the mishap, the top node of the WBG (see Figure 2.7).

The following procedure is iterated until done. For every fact that is represented by a node **N** already in the WB Graph, the "child nodes", the *necessary causal factors* (NCFs) are determined either from the facts found in the List of Facts or from the pairs of facts found in the Why-Because List, as follows:

- the List of Facts is reviewed and the Counterfactual Test is applied between **N** and each other node in the List of Facts; or

- all pairs in the Why-Because List are selected which have **N** as the first item. The second item of the pair is then an NCF of **N**.

When working in a team, discussing the selection in the group is helpful.

The NCFs are added as child nodes of the node representing the examined fact with a descriptive label and a reference to the List of Facts or Why-Because List.

This procedure is iterated until the desired level of detail is reached, or until every node appears in the graph.

2.9 Quality Assurance and Correction of the WB Graph

After having determined all NCFs to reach the desired level of detail, the *Causal Completeness Test* is applied. The graph is thoroughly inspected to ensure that the incident is described sufficiently, and that there are no errors. This step is most successful if carried out in a face-to-face team meeting (see Figure 2.8).

If inadequacies or errors are found, they are corrected by changing or adding causal relations, removing nodes, or adding nodes. Adding nodes requires carefully extending the List of Facts / Why-Because List and then returning to the process of determining NCFs (Figure 2.9).

If it is determined that the quality of the WBG must be improved, the Counterfactual Test should be applied once again to check the causal relations. When the entire WB Graph has been checked in this manner, it is finished.

2.10 Glossary

Auxiliary List of Facts (auxLoF) Auxiliary List of Facts are optional. The facts are arranged according to a classification system, such as *timestamp* or *actor involved*. Auxiliary List of Facts help to gain a better understanding of an incident. The facts are notated with a serial number, a short description, their class, and a reference to their source.

Causal Completeness Test (CCT) A technical criterion for determining sufficiency of causal explanation. The CCT applies between a collection $A_1, A_2, ..., A_n$ of facts and a fact **B**. The CCT is satisfied when (a) each A_k is an NCF of **B**; and (b) the Causal Sufficiency Criterion holds between the set $A_1, A_2, ..., A_n$ and **B**. The technical definition may be found in [Ladkin 01].

Causal Sufficiency Criterion The Causal Sufficiency Criterion between a set of facts $A_1, A_2, ..., A_n$ and a fact **B** is that, given the world as it more or less is, it is impossible for **B** not to have happened if all of the A_k have happened. That is, had the world been just sufficiently different that **B** did not happen, then at least one of the A_k (not necessarily the same one for each different circumstance) would not have happened either. The technical definition may be found in [Ladkin 01].

Counterfactual Test (CT) The criterion for determining a *Necessary Causal Factor*.

Given two facts, **A** and **B**, CT asks whether, if the world had been just sufficiently different that **A** had not happened, whether **B** would have happened anyway. If **B** would not have happened in this situation in which **A** did not happen, the Counterfactual Test is passed, and **A** is a *Necessary Causal Factor* of **B**.

List of Facts (LoF) The List of Facts contains the significant facts that are causal factors of the incident. The facts are notated with a serial number, a short description, and a reference to their source.

Necessary Causal Factor (NCF) A fact that causally affects the occurrence of another fact in the course of events of the incident. This is determined by applying the Counterfactual Test. In Why-Because Graphs, NCFs are represented by child nodes.

Topnode The top node of the Why-Because Graph represents the failure of the examined system (mishap).

Why-Because Graph (WB Graph, WBG) The Why-Because Graph shows as edges the causal relations between the facts, shown as nodes, that led to the failure of a system.

Why-Because List (WB List) The Why-Because List contains the facts that are causal factors of the incident, arranged in pairs consisting of a necessary causal factor and its effect. Every single fact is notated with a serial number, a short description, and a reference to its source.

Bibliography

[IBM 69] IBM. *Flowcharting Techniques*, GC20-8152-1 edition, 1969. Available from *http://www.fh-jena.de/˜kleine/history/*, accessed 20 September 2005.

[Ladkin 01] Peter B. Ladkin. Causal system analysis, volume RVS-Bk-05-01. RVS Group, University of Bielefeld, 2001. Available at *www.rvs.uni-bielefeld.de* → *Why-Because Analysis*.

[Ladkin 02] Peter B. Ladkin. *WBA Home Page*. Available at *www.rvs.uni-bielefeld.de* → *Why-Because Analysis*, June 2002.

[Paul-Stüve 05] Thilo Paul-Stüve. *Formal Task Analysis of Graphical System Engineering Software Use*. Rapport technique, RVS Group, Faculty of Technology, University of Bielefeld, March 2005. Available at *www.rvs.uni-bielefeld.de* → *Publications* → *Theses Written in the Group*.

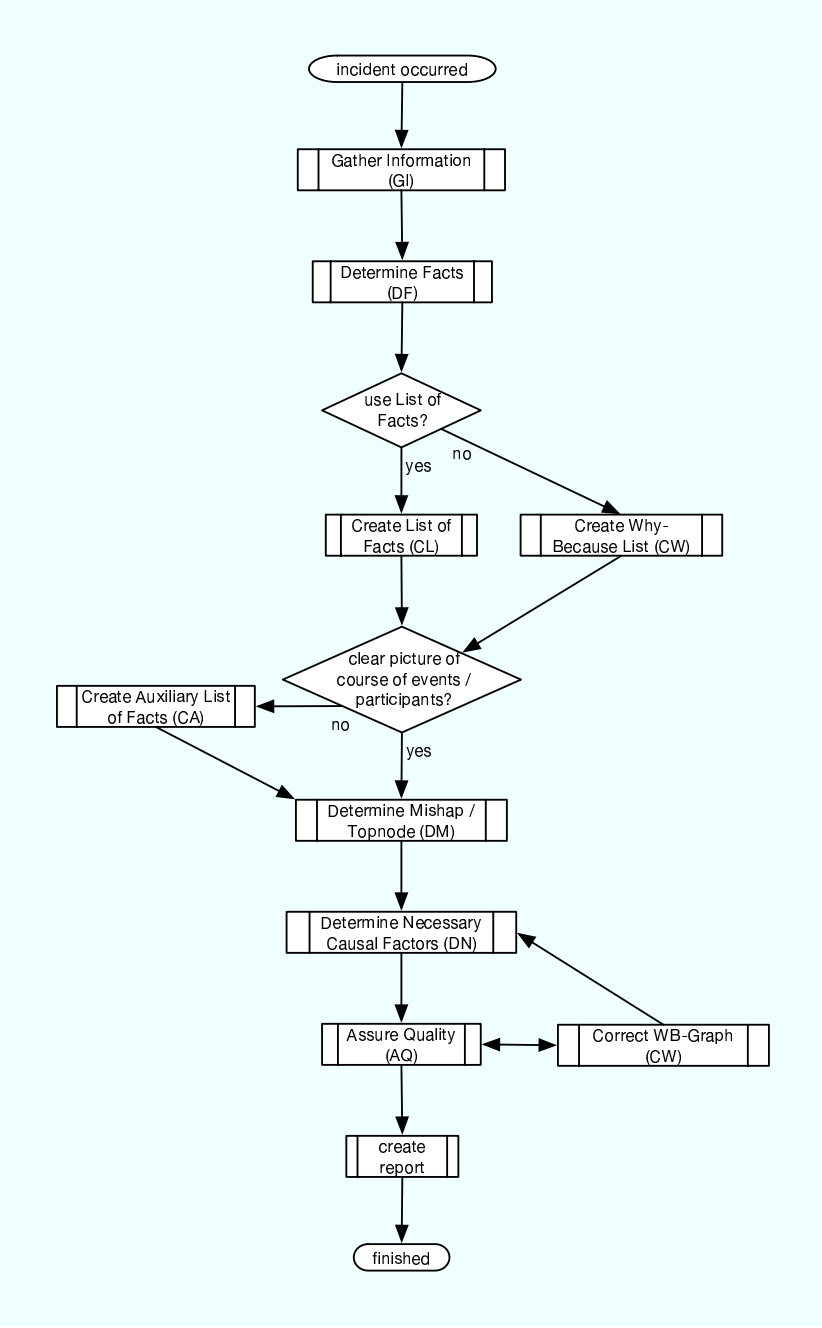


Figure 2.1: Why-Because Analysis Overview

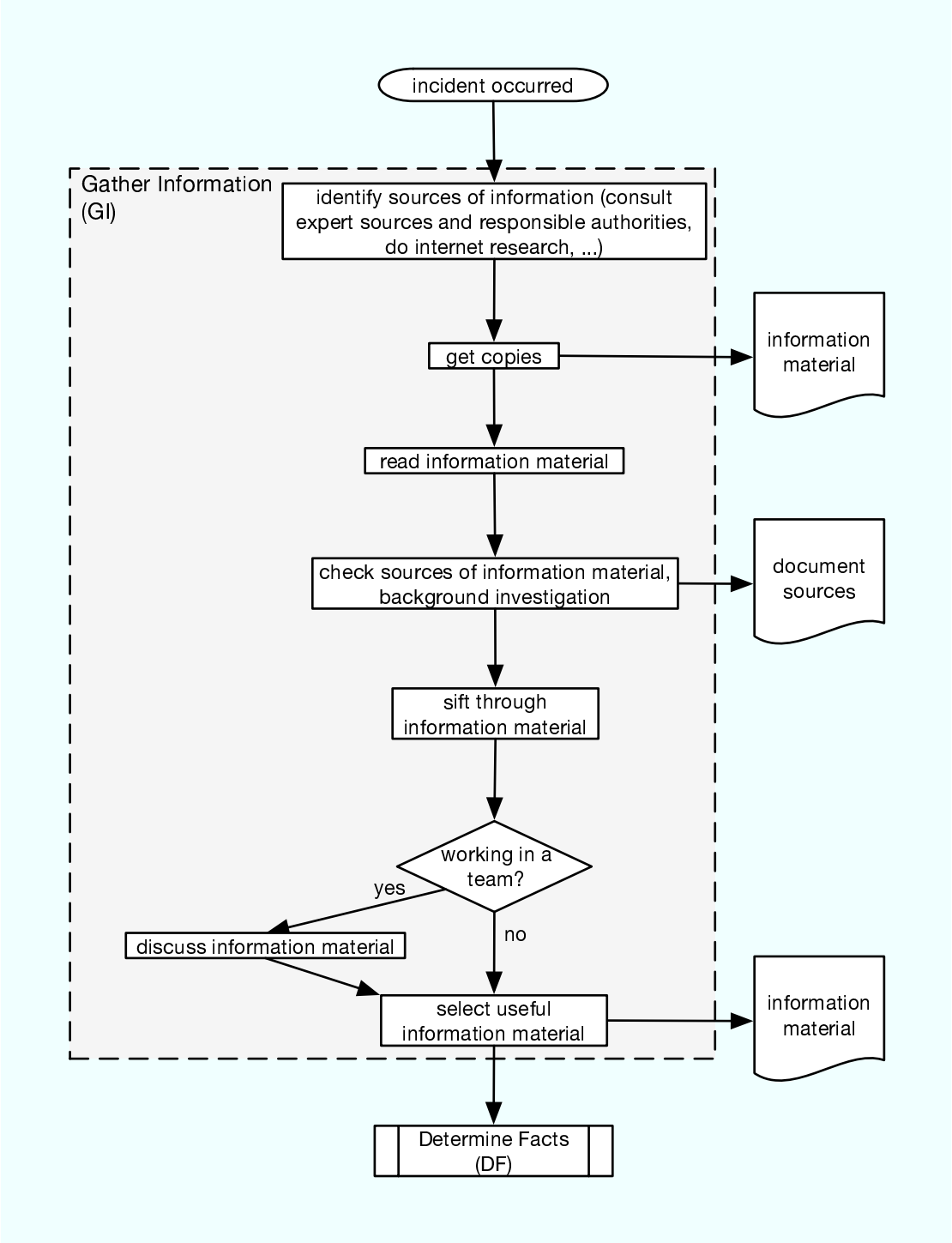


Figure 2.2: Gather Information

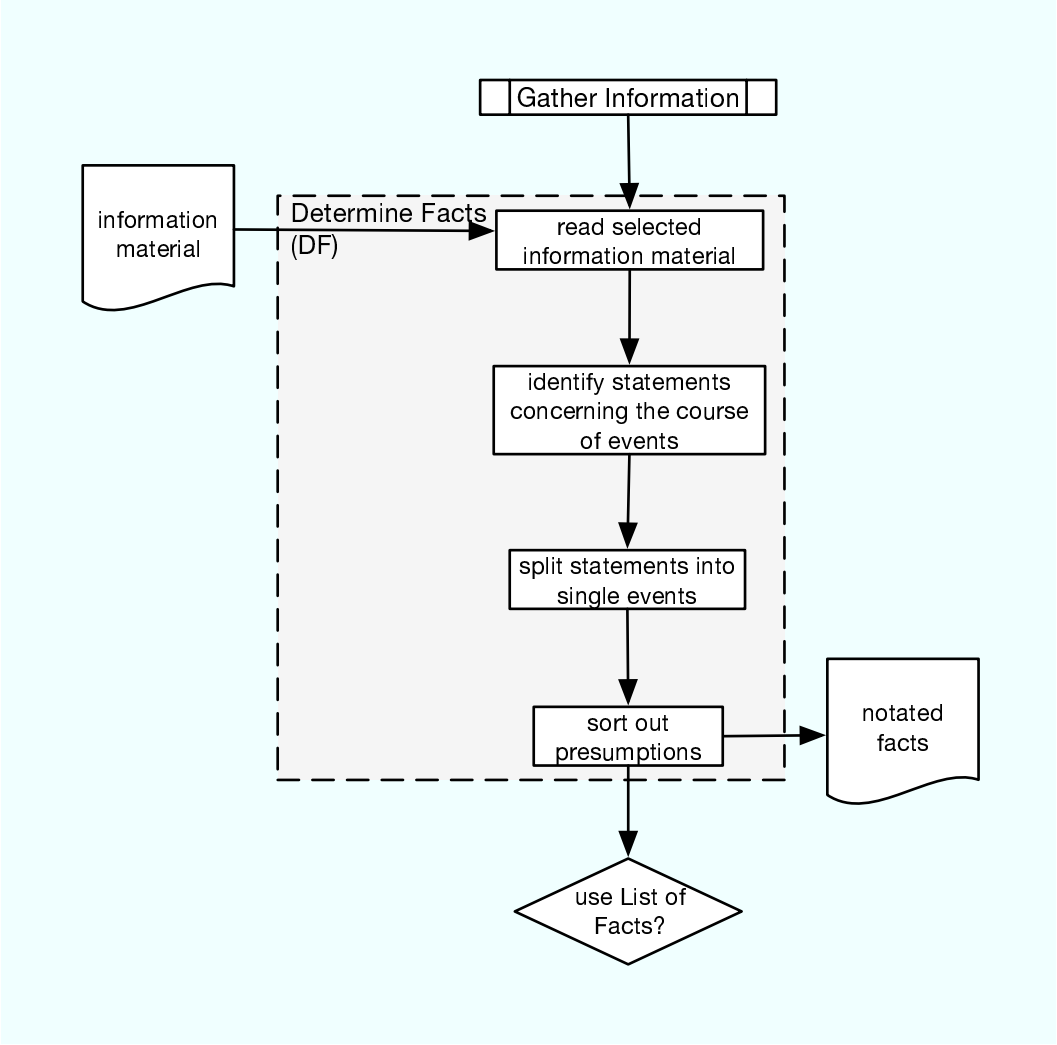


Figure 2.3: Determine the Facts

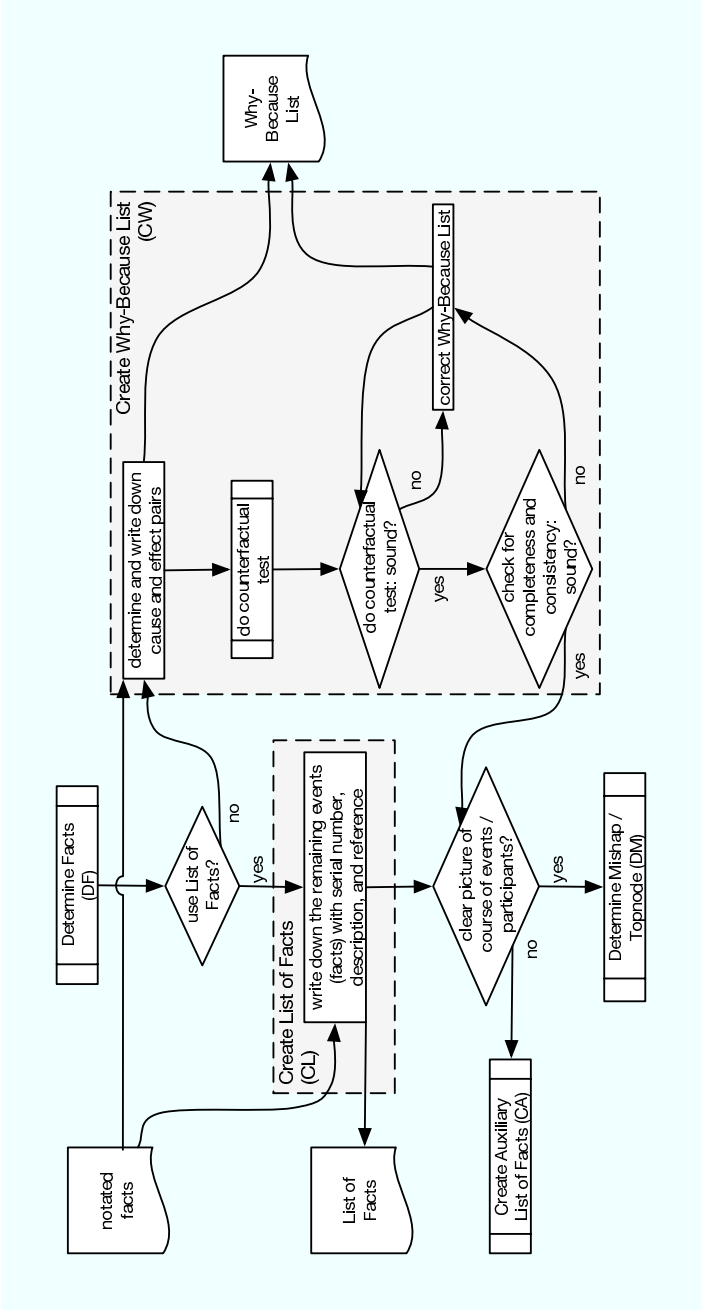


Figure 2.4: Create List of Facts / Why-Because List

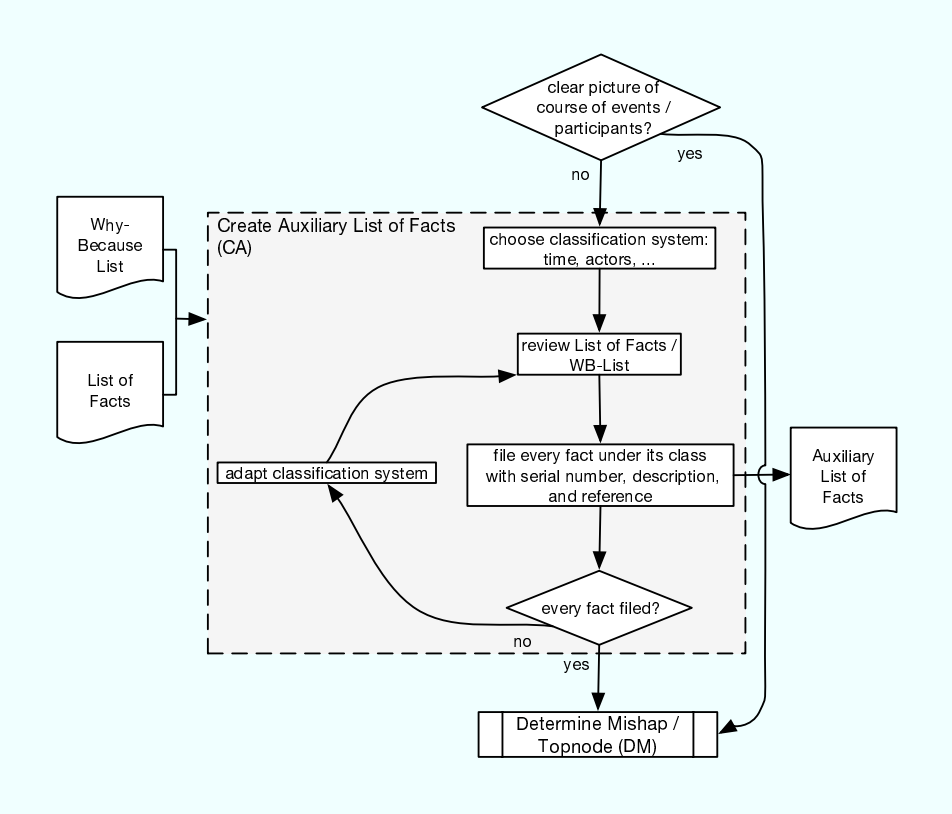


Figure 2.5: Create auxiliary List of Facts

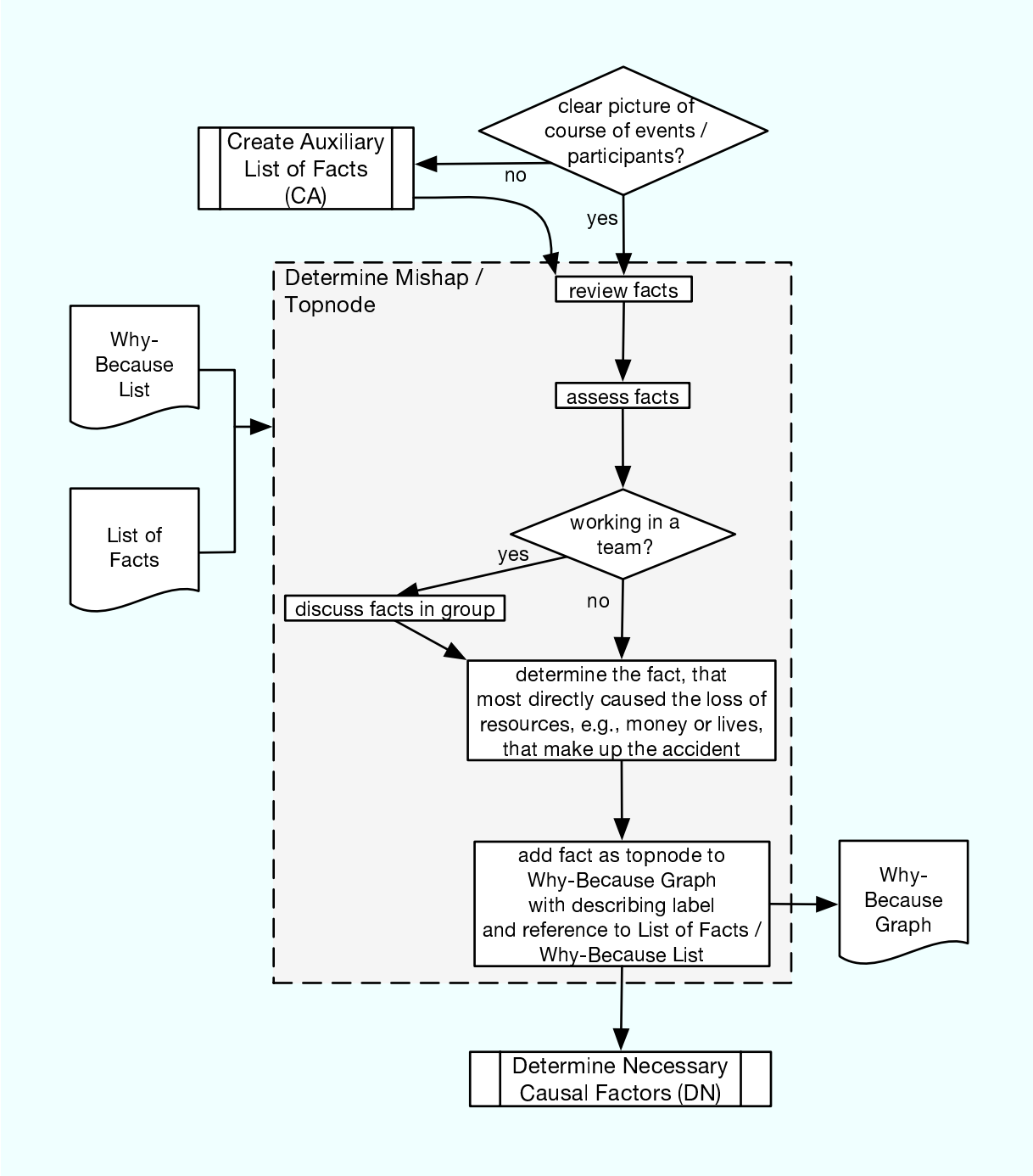


Figure 2.6: Determine the Mishap / Top node

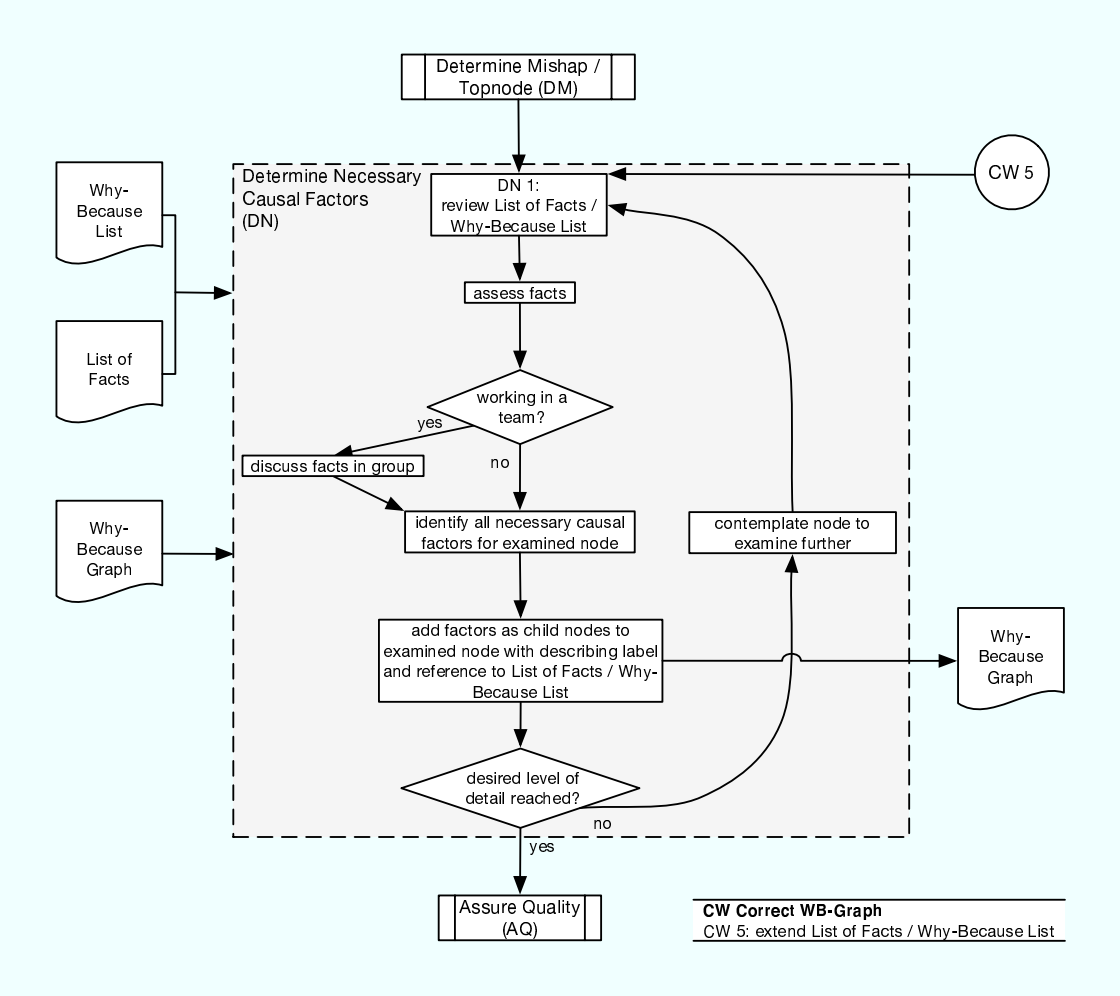


Figure 2.7: Determine the Necessary Causal Factors

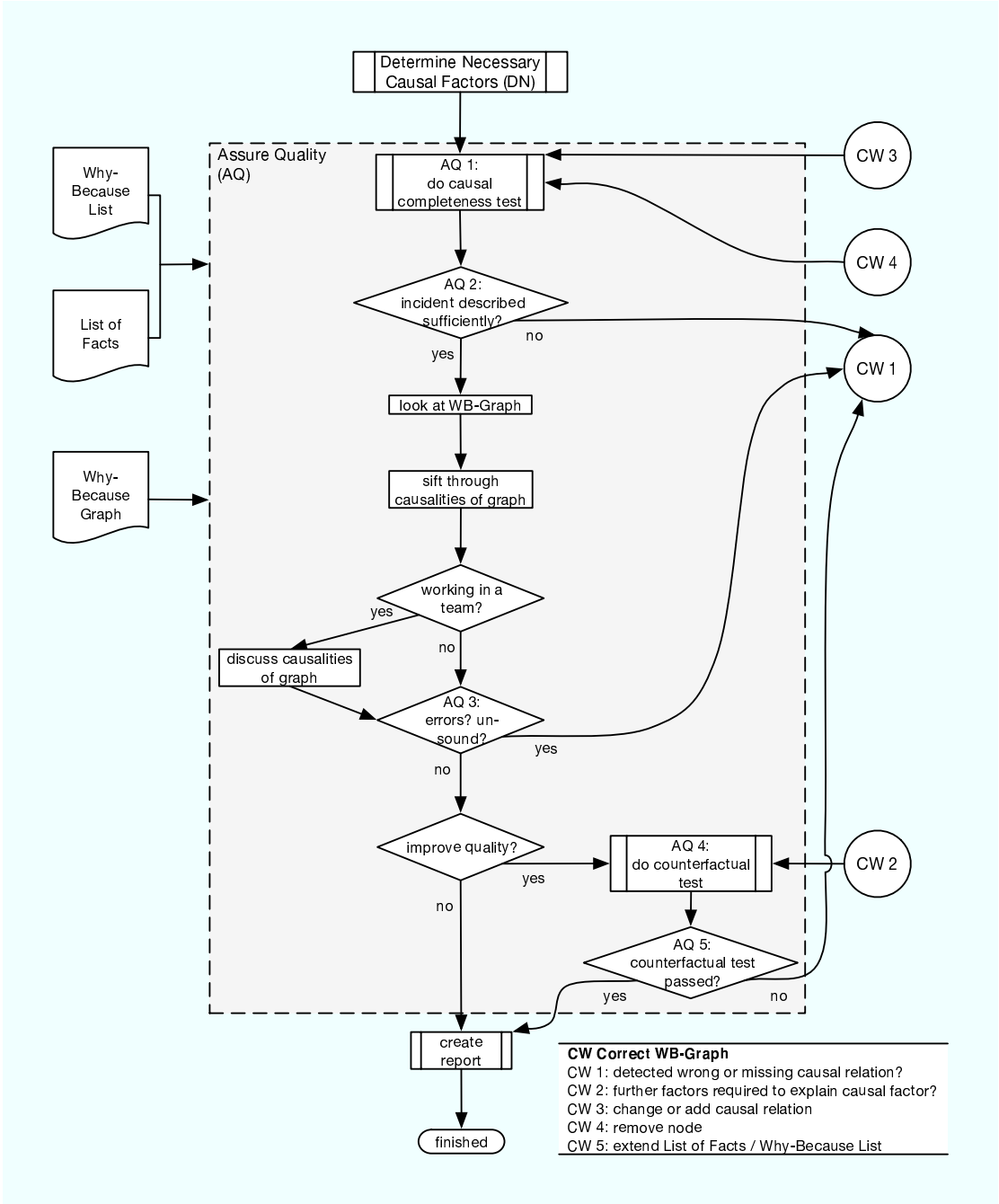


Figure 2.8: Assure the Quality

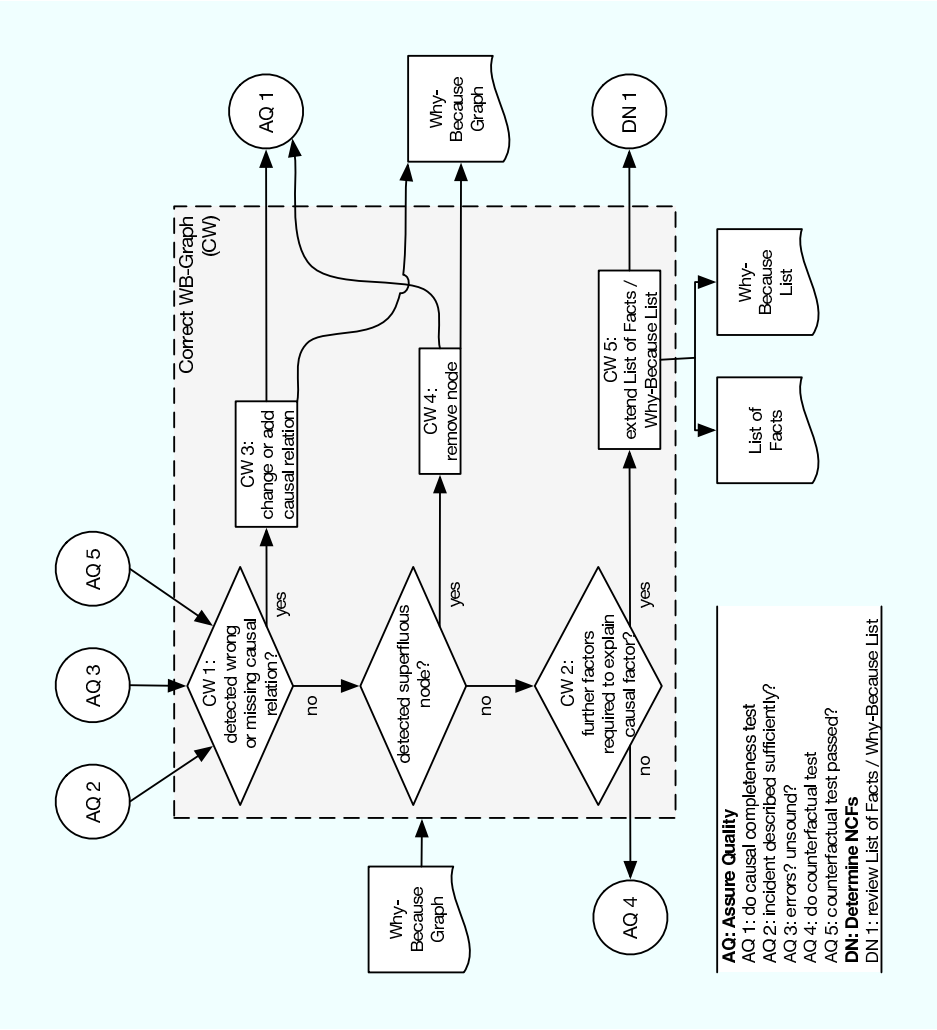


Figure 2.9: Correct the WB Graph

Chapter 3

Friendly Fire GPS Accident During Operation Enduring Freedom, Afghanistan

The following is an online news article by Vernon Loeb. The article was published in the Washington Post, where Loeb is a Staff Writer, on March 24th, 2002.

The incident happened during the US led Operation Enduring Freedom.

3.1 The Incident

"The deadliest 'friendly fire' incident of the war in Afghanistan was triggered in December by the simple act of a U.S. Special Forces air controller changing the battery on a Global Positioning System device he was using to target a Taliban outpost north of Kandahar, a senior defense official said yesterday.

Three Special Forces soldiers were killed and 20 were injured when a 2,000-pound, satellite-guided bomb landed, not on the Taliban outpost, but on a battalion command post occupied by American forces and a group of Afghan allies, including Hamid Karzai, now the interim prime minister.

The U.S. Central Command, which runs the Afghan war, has never explained how the coordinates got mixed up or who was responsible for relaying the U.S. position to a B-52 bomber, which fired a Joint Direct Attack Munition (JDAM[1]) at the Americans.

[1]JDAM is a US Air Force and US Navy program to enhance general purpose bombs by

But the senior defense official explained yesterday that the Air Force combat controller was using a Precision Lightweight GPS Receiver, known to soldiers as a 'plugger'[2], to calculate the Taliban's coordinates for a B-52 attack. The controller did not realize that after he changed the device's battery, the machine was programmed to automatically come back on displaying coordinates for its own location, the official said.

Minutes before the fatal B-52 strike, which also killed five Afghan opposition soldiers and injured 18 others, the controller had used the GPS receiver to calculate the latitude and longitude of the Taliban position in minutes and seconds for an airstrike by a Navy F/A-18, the official said.

Then, with the B-52 approaching the target, the air controller did a second calculation in 'degree decimals' required by the bomber crew. The controller had performed the calculation and recorded the position, the official said, when the receiver battery died.

Without realizing the machine was programmed to come back on showing the coordinates of its own location, the controller mistakenly called in the American position to the B-52. The JDAM landed with devastating precision.

The official said he did not know how the Air Force would treat the incident and whether disciplinary action would be taken. But the official, a combat veteran, said he considered the incident 'an understandable mistake under the stress of operations.'

'I don't think they've made any judgments yet, but the way I would react to something like that – it is not a flagrant error, a violation of a procedure,' the official said. 'Stuff like that, truth be known, happens to all of us every day – it's just that the stakes in battle are so enormously high.'

Nonetheless, the official said the incident shows that the Air Force and Army have a serious training problem that needs to be corrected. 'We need to know how our equipment works; when the battery is changed, it defaults to his own location,' the official said. 'We've got to make sure our people understand this.'

Navy Cmdr. Ernest Duplessis, a spokesman for the U.S. Central Command, declined to comment on the friendly fire incident, saying an investigation 'has not cleared our review yet.'

---

integrating a guidance kit consisting of an inertial navigation system/global positioning system guidance kit

[2]The official military abbreviation of the Precision Lightweight GPS Receiver is PLGR; thus the name 'plugger'

In another matter, Duplessis said that U.S. forces have found within the past week a possible al Qaeda biological weapons research site that had been abandoned near Kandahar.

'There was no evidence of any chemical or biological weapons production going on there,' Duplessis said. 'But there was equipment found – it had medical supplies, commonly available laboratory equipment suitable for growing biological samples, as well as a variety of other supplies like that. But I have to stress that this lab was still under construction and no samples of biological agents were found at the site."

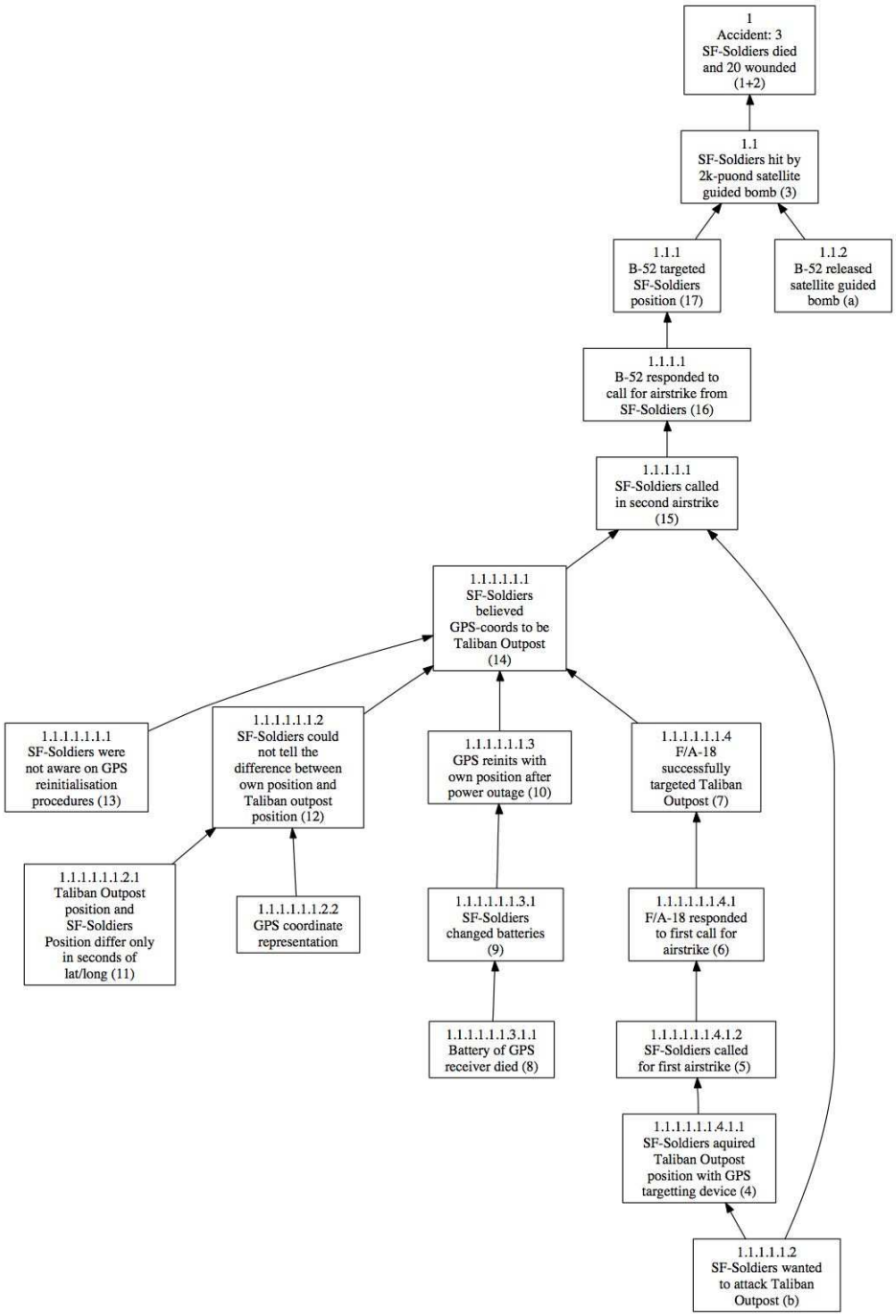


Figure 3.1: The Friendly-Fire WB-Graph

Chapter 4

Herald of Free Enterprise Capsizes after Leaving the Port of Zeebrugge

Narrative compiled by Peter B. Ladkin after a presentation by Enesto deStefano

The Herald of Free Enterprise was a roll-on/roll-off (RoRo) road-vehicle ferry used for scheduled crossings of the English Channel by road traffic. Such ships have bow doors and stern doors that open to allow drive-on and drive-off loading. These doors are closed before sailing, to prevent ingress of water.

The Herald of Free Enterprise left the harbour of Zeebrugge on 6 March 1987 with the bow doors still open. She passed the outer mole, and the Master increased speed (to setting combinator 6). The bow wave rose above the level of the bow spade. Water entered the main deck and flooded onto the lower car deck (G deck). There were no subdividing bulkheads on the G deck, and the water accumulating along the entire length of one side of the G deck. The ship became unstable and capsized in shallow water. Nevertheless,

189 people died of the 459 people on board.

The investigation brought to light that the Assistant Bosun, whose immediate responsibility it was to close the bow doors before departure, was asleep in his cabin, and had not woken up at the "harbor station" call. He was tired, and had been released from supervision work by the Bosun. The Chief Officer, whose responsibility it was to ensure that the doors were closed, thought he had seen the Assistant Bosum going to close the doors. The officer loading the G deck had not ensured that the bow doors were secure when leaving port, which was a violation of an instruction issued in July 1984.

It turned out that the Captain always assumed that the doors were safely closed, unless he was told otherwise. It was apparently common practice to make this assumption. The Master assumed that the bow doors were closed on the way to the outer mole. He could not see them or their closing sequence from the bridge (they closed horizontally), and there was no indicator on the bridge to indicate the status of the bow doors.

The sit of the ship in the water is affected by ballast tanks. Water was pumped into the ballast tanks to depress the bow for road vehicle loading. Not all the ballast water had been pumped out again before leaving port, partly because the capacity of the pump was too low and partly because the crew were under time pressure to depart. A request for a high-capacity pump had been rejected by management as the cost was considered prohibitive.

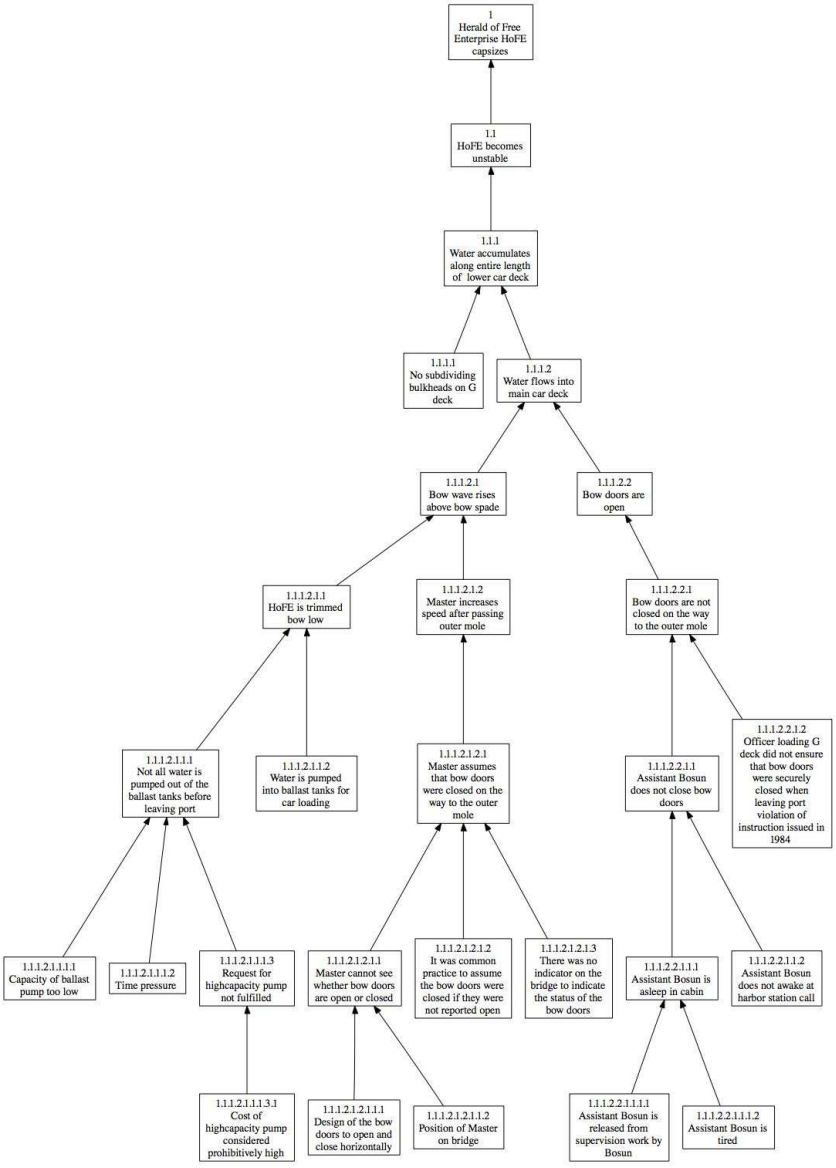


Figure 4.1: The Herald of Free Enterprise WB-Graph

Chapter 5

Train Crash near Warngau, Germany

5.1 Overview

On Sunday the 8th of June 1975 18:32h two passenger trains crashed into each other near Warngau, Germany. The passenger trains both entered the single track line between Warngau and Schaftlach after receiving permission to continue. One train was lifted off the track and fell to the side. The accident killed 44 people, the engine drivers among them, and injured 122. Damages amounted to 4 million Deutsche Mark. The accident was the most severe in German railroad history at that time.

5.2 Situation

The track length between Warngau and Schaftlach is 4.8 km. It is a single track line. It belongs to the main line between München and Lenggries, both in Bavaria. Train protection, automatic braking on passing a signal at danger, is performed by inductive train protection facilities (indusi). The track between Warngau and Schaftlach was not compartmentalized into track blocks. It contained only one section (a block, German Blockabschnitt). Schaftlach station and Warngau station both met the operational demands of the German railroad operation regulations (German: Eisenbahnbetriebsordnung, EBO). According to EBO, indusi was required for the track because it was designed for trains traveling faster than 100 kph. Compartmentalization was not required because traffic density was sufficiently low. Access to the track was controlled by station inspectors (Fahrdienstleiter) in Warngau and in Schaftlach, both coordinating using verbal procedures known as Train Announcement Procedures (TAP, German: Zugmeldeverfahren, see below).

5.3 Train Announcement Procedures (TAP, german, Zugmeldeverfahren)

EBO (Eisenbahnbetriebsordnung, German railroad regulations) requires that railroad operators follow the principle of Spatial Train Separation (Raumabstandsprinzip). The principle demands that there can only be one train in a block. Blocks are defined between stations or other operating facilities. Access to blocks is controlled by the station inspectors in charge of the block. If there is more than one station inspector in charge there is always a protocol for coordination of the parties involved. In the case of the track block between Warngau and Schaftlach the protocol was the TAP.

TAP protects trains from collision head-on-head and head-on-tail. No train is to enter a block while another train is still inside this block, even if both trains are assumed to travel in the same direction at the same speed.

Every time a train is about to leave one block to move into another, the train needs explicit permission. Permission is granted by station inspectors (or other operational personnel) in charge of the block. Communication between station inspectors is performed verbally over the phone. Communication between station inspector and engine driver is performed verbally over the radio.

On a single track line (as was the case between Warngau and Schaftlach) trains have to be

1. offered (OFF),
2. accepted (ACC),
3. checked out (PERM) and
4. reported back (ACK).

between station inspectors.

With OFF, station inspector A tells station inspector B that he has a train ready to enter a specific block. With ACC, station inspector B acknowledges that the train can enter and that the block is occupied until the train arrives at the B side of the block and leaves. This protects trains from colliding head-on-head. With PERM, station inspector A notifies the train to enter the block and notes the trains time of departure. With ACK, station inspector B notifies station inspector A that the train has cleared the block. This protects the other trains against colliding head-on-tail.

On many single track lines, TAP is the only protection mechanism. There are strict rules governing what and how to communicate. TAP require the use of fixed phrases for information exchange between station inspectors.

5.4 Schedule

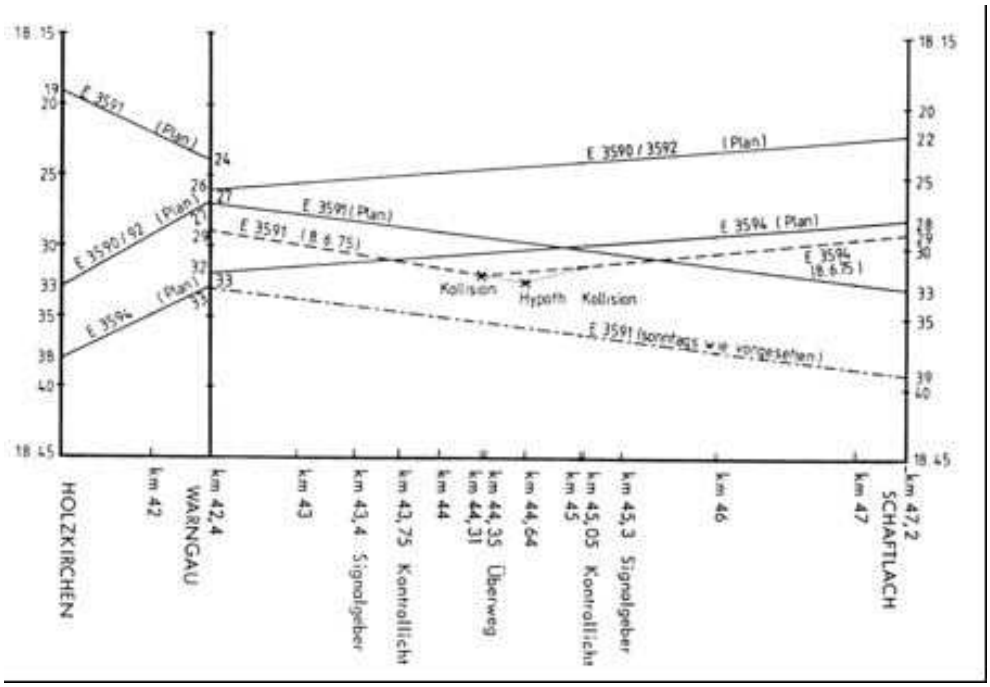
On the day of the accident train #3591 was waiting at Warngau, ready for departure. Train # 3594 S (scheduled sunday only) was waiting at Schaftlach, ready for departure. Both station inspectors offered their trains (OFF) and both interpreted the conversation for their respective train as if ACC. Both cleared the trains to depart. The misunderstanding was a result of not using the fixed phrases. They conversed using a bavarian dialect and cut corners where possible.

According to the schedule written, train #3591 had to wait for 2 trains coming from Schaftlach: trains #3592 and #3594 S. Station inspector Warngau had to handle 3 trains in a short time (9 minutes) and also had to sell tickets and answer passengers' questions. He was the only person in the station Warngau.

5.5 Timetable

The Deutsche Bundesbahn (DB, German Federal Railroad) provides two types of timetables. A picture timetable and a book timetable.

For station inspectors there is also the picture timetable. It shows a graphical representation of scheduled trains, when they depart, arrive, and the presence of "Luftkreuzungen" ("air intersection").



The timetable for Warngau contained such a Luftkreuzung. A Luftkreuzung describes a point on the line where two trains would meet if they went strictly by the timetable. Station inspectors have to control access to line blocks and a Luftkreuzung will give them greater flexibility in case of a deviation from the timetable. Indeed the trains' positions will intersect only at a station at the end of the block with the Luftkreuzung. Such a station has at least two different tracks with points. In the picture timetable a Luftkreuzung is highlighted.

EBO regulations explicitly disallowed "Luftkreuzung" in time table construction. It was nevertheless common practice at this time, as here.

5.6 Blinking Train-Signal

Between Warngau and Schaftlach there were two signals guarding a level crossing (grade crossing). The signal is composed of two lights. The first light (indicator light) blinks if the red lights, holding the road traffic at the level crossing, are on. The second light (control light) blinks to indicate that the signal is working properly. The signal indicator lights start to blink when a train's first axle passes a contact point on the track. If a train from the

opposite direction passes the respective contact point then the control light does not blink. In that case the engine driver must come to a full stop before the crossing.

The purpose of the signal is to feed back information about the state of a railway level crossing ahead of the train.

Train #3591 passed the contact point first. Train #3594 S passed its respective contact point after #3591 passed his. The driver of train #3594 S did not react on the signal guarding the level crossing, which should have indicated to him that he should commence an an emergency stop.The trains were in a blind curving section of track, so visual contact was not possible until late in the convergence.

Either visual contact or braking of train #3394 S would have reduced the severity of the collision.

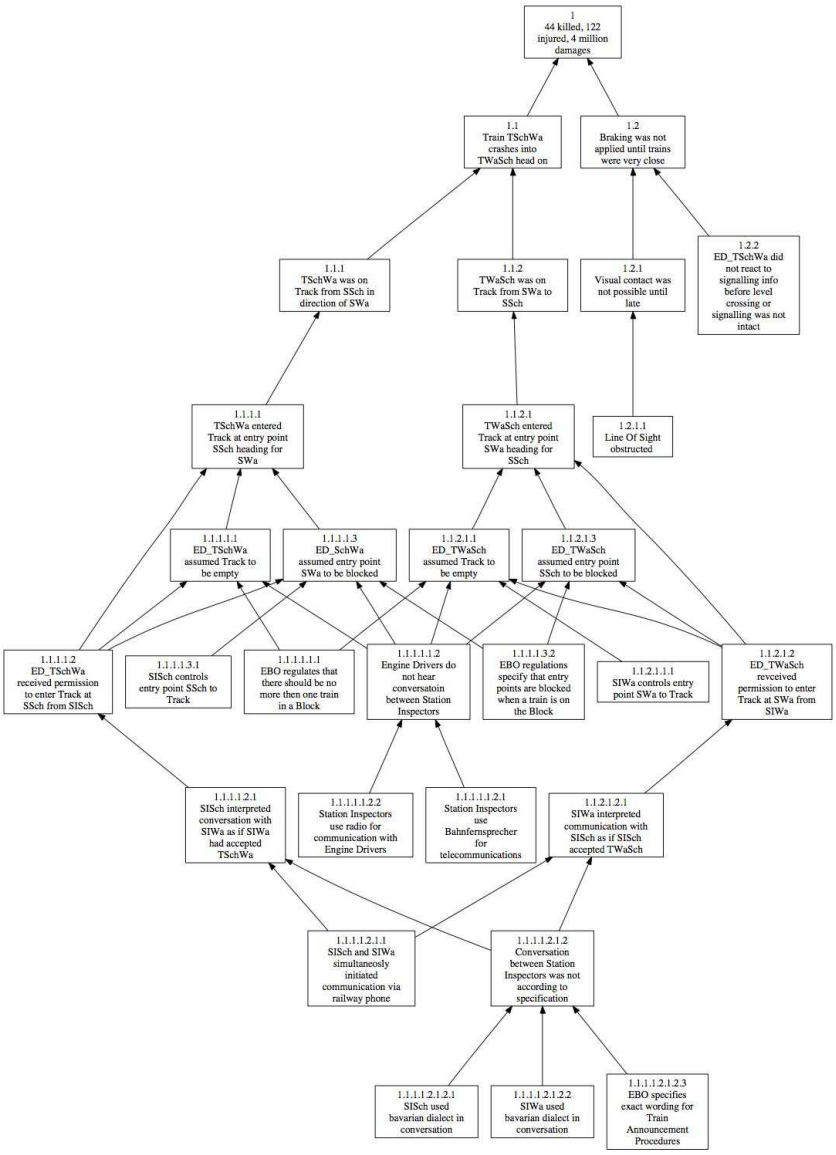


Figure 5.1: The Warngau WB-Graph

Chapter 6

The Altitude-Bust Simulator Incident

The following is an excerpt from "Using Model Checking to Help Discover Mode Confusions and Other Automation Surprises" by John Rushby.

The example is one of five altitude deviation scenarios observed during a NASA study in which twenty-two airline crews flew realistic two hour missions in DC-9 and MD-88 aircraft simulators.

To follow the scenario, it is sufficient to understand that the autopilot can be instructed to cause the aircraft to climb or to hold a certain altitude through the setting of its "pitch mode."

In VERT SPD (Vertical Speed) mode the aircraft climbs at the rate set by the corresponding dial (e.g., 2,000 feet per minute); in I AS (Indicated Air Speed) mode, it climbs at whatever rate is consistent with holding the air speed set by another dial (e.g., 256 knots); in ALT HLD (Altitude Hold) mode, it holds the current altitude. In addition, certain "capture modes" may be armed. If ALT (Altitude) capture is armed, the aircraft will only climb as far as the altitude set by the corresponding dial, at which point the pitch mode will change to ALT HLD; if the capture mode is not armed, however, and the pitch mode is VERT SPD or I AS, then the aircraft will continue climbing indefinitely.

The behavior of this system is complicated by the existence of an ALT CAP (Altitude Capture) pitch mode, which is intended to provide smooth leveling off at the desired altitude.

The ALT CAP pitch mode is entered automatically when the aircraft gets close to the desired altitude and the ALT capture mode is armed (do

not confuse the ALT CAP pitch mode with the ALT capture mode).

The ALT CAP pitch mode disarms the ALT capture mode and causes the plane to level off at the desired altitude, at which point it enters ALT HLD pitch mode.

6.1 The Incident

The following is the description of the incident by Peter B. Ladkin, based on a description by Evertt Palmer.

The crew had just made a missed approach and had climbed to and leveled at 2,100 feet. They received the clearance to ". . . climb now and maintain 5,000 feet. . . " The Captain set the MCP (Master Control Panel) altitude window to 5,000 feet (causing ALT capture mode to become armed), set the autopilot pitch mode to VERT SPD with a value of approximately 2,000 ft. per minute and the autothrottle to SPD mode with a value of 256 knots. Climbing through 3,500 feet the Captain called for flaps up and at 4,000 feet he called for slats retract. Passing through 4000 feet, the Captain pushed the I AS button on the MCP. The pitch mode became I AS and the autothrottles went to CLAMP mode. The ALT capture mode was still armed. Three seconds later the autopilot automatically switched pitch mode to ALT CAP. The FMA (Flight Mode Annunciator) ARM window went from ALT to blank and the PITCH window showed ALT CAP. A tenth of a second later, the Captain adjusted the vertical speed wheel to a value of about 4,000 feet a minute. This caused the pitch autopilot to switch modes from ALT CAP to VERT SPD. As the altitude passed through 5,000 feet at a vertical velocity of about 4,000 feet per minute, the Captain remarked, "Five thousand. Oops, it didn't arm." He pushed the MCP ALT HLD button and switched off the autothrottle. The aircraft then leveled off at about 5,500 feet as the "altitude-altitude" voice warning sounded repeatedly.

6.2 Identifiable Events and States

1. Missed approach procedure
2. maintaining 2,100 ft
3. clearance received to climb and maintain 5,000 ft

4. communication confusion
5. PF sets MCP.Alt ← 5,000
6. PF sets AP.Pitch ← <VERT/SPD, 2,000 fpm>
7. PF sets ATh ← <SPD, 256 kt >
8. Climb thru 3,500 ft & PF commands "Flaps up"
9. Climb thru 4,000 ft & FMA = <SPD/255,ALT,VOR/TRK,VERT/SPD> & PF commands "Slats retract"
10. PF sets MCP.Mode ← IAS
11. AP.PitchMode ← IAS & ATh ? CLAMP
12. <AP.Arm ← ALT/CAP>
13. Y: [Time = time(X) + 3 sec & AP.PitchMode ← ALT/CAP & FMA.Arm ← blank & FMA.Pitch ← ALT/CAP]
14. [Time = time(Y) + 0.1 sec & PF sets AP.VertSpd ← 4,000 fpm]
15. [AP.Pitch: ALT/CAP ← VERT/SPD]
16. [climbing thru 4,500 ft & FMA = <SPD/255,blank,VOR/TRK,VERT/SPD> & ApproachingAltitude light ← ON]
17. [climbing thru 5,000 ft & VertSpd = 4,000 fpm & PF says "Oops, it didn't arm"]
18. At altitude = 4,000 ft Until altitude = 5,000 ft: PNF copying holding clearance

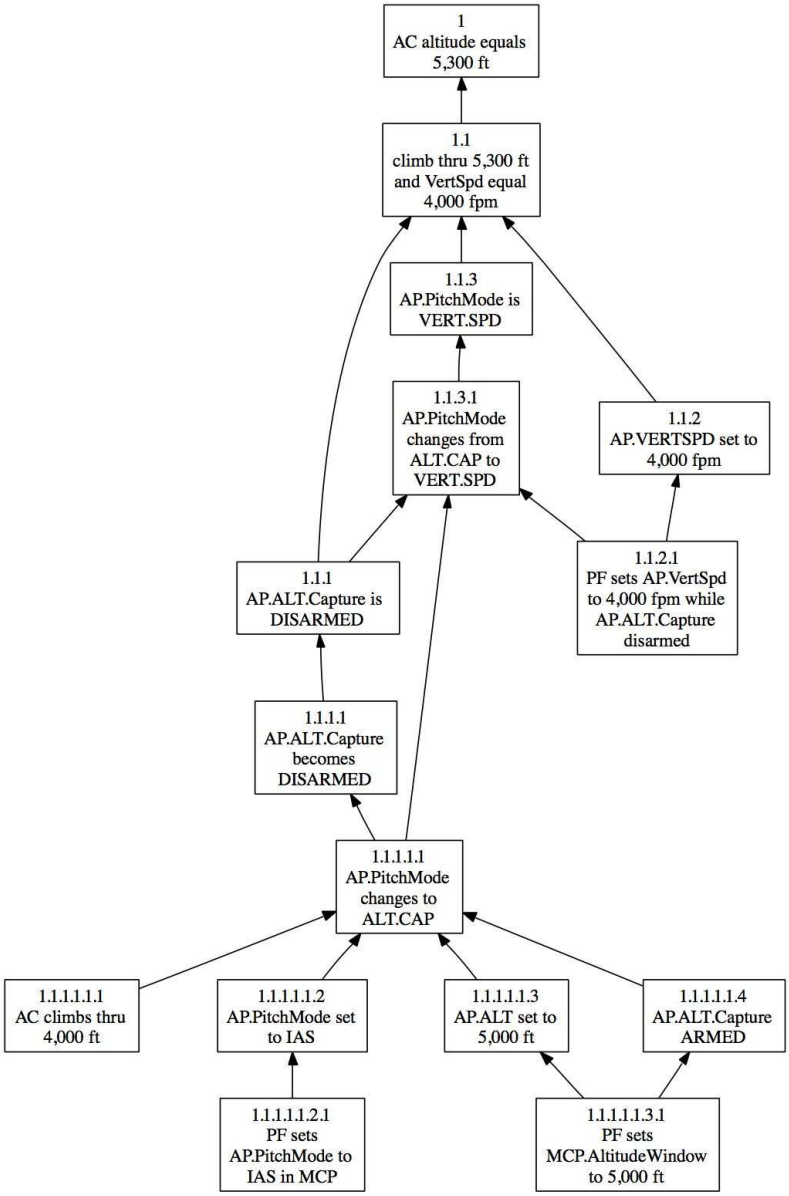


Figure 6.1: The Oops WB-Graph

Chapter 7

DC-10 misses Frankfurt runway – by 300km

A Northwest Airlines McDonnell Douglas DC-10-40 carrying 241 passengers from Detroit to Frankfurt missed its intended destination by 300km (160nm), landing at Brussels Airport by mistake on 5 September.

The pilots of Flight 52 only realised their error when they lined the aircraft up for the approach at Brussels. In spite of that, they decided to land anyway. [...]

Early reports from Brussels air traffic control (ATC) attributed the original error to Shannon ATC, alleging that an incorrect code had been entered into the aircraft's ARC flight-plan data, redesignating the aircraft's destination to Brussels.

The Irish Aviation Authority denies this, saying that the crew had acknowledged its destination as Frankfurt, and that the correct data was passed to the London Air Traffic Control Center, the last such center before Brussels.

By the time the aircraft entered the Brussels control region, however, its destination has been redesignated, Brussels ATC maintains. [...]

The aircraft's planned track for Frankfurt would normally have taken it over Belgium at its cruising altitude of 37,000ft (11,300m), according to ATC conditions. The upper-airspace (above 24,500ft) over Belgium, however, is handeled by the Maastricht ATCC in the Netherlands.

A senior Brussels ATC official confirms that the aircraft was cleared by the LATCC as it left the London control region to descend to 24,000ft and contact Brussels. The crew started the descent and called Brussels on the assigned frequency, addressing the controller as "Frankfurt" and announcing

its intention to land.

Brussels did not question the addressing error which, Northwest says, occurred more than once in subsequent transmissions.

Brussels approach instructed the crew to descend in-bound via Bruno, a VOR navigation beacon on one of the standard approaches to Brussels Airport. The crew had to ask ATC for the VOR's frequency. The aircraft was subsequently cleared for an instrument-landing system (ILS) approach to Brussels's runway 25L, which is the same runway orientation as at Frankfurt, but with different ILS frequencies.

At some point the crew finally realised they were landing at the wrong airport and opted to continue the landing for safety reasons, says Northwest. The airline has said that, whatever errors ATC may have made, if any, the crew must "share responsibility" for what happened.

7.1 Fly NorthWest Airlines to unknown destinations

Report *Fly Northwest Airlines to Unknown Destinations*, Peter B. Ladkin, RISKS Forum Volume 17 Issue 38, 8 October 1995.

The International Herald Tribune for Monday Oct 2, p1, has a report on a DC10, NorthWest Flight 52, on its way to Frankfurt from Detroit. They landed in Brussels, much to everyone's surprise except for the passengers, cabin crew and air traffic control.

A controller in Shannon changed the destination in the en-route computers for some reason no-one has fathomed. So everyone after that sent NW52 merrily on the way to Brussels. The cabin crew and passengers noticed, because the cabin flight-path display was showing them going to Brussels rather than to Frankfurt (the cities are 200miles=325km away from each other). The flight crew first noticed when they broke out under the clouds on approach to Brussels, and noticed that the layout of the airport was not similar to Frankfurt. Sensibly, they decided to continue the landing. And will remain landed until the investigation figures everything out. A spokesman for NorthWest pointed out that the crew *should* have known where they were.....

That reminds me of the time I was flying Chicago to SFO and following the ground on my WAC (World Aeronautical Chart). The routing went south of the Colorado/Wyoming boundary, past Aspen, and then over the Green river canyon, which is some 250km past Aspen. Just then, the captain announced "We're just passing Aspen, Colorado, out of the left window." But we got there OK. Even United pilots can recognise the Mina and Coaldale transitions to the Modesto arrival when it hits them ;-)

Peter Ladkin.

7.2 Re: Fly NorthWest Airlines to unknown destinations

Peter B. Ladkin, Risks Forum Volume 17 Issue 40, 19 October 1995

An article in Flight International, 11-17 October 1995, p8, entitled 'DC-10 misses Frankfurt runway–by 300km', considers the aftermath.

Brussels ATC attributed the original error to the Shannon ATC controller entering an incorrect code to the ATC flight-plan data. The Irish Aviation Authority denies this, saying the correct code was passed to London ATCC, the last such ATCC before Brussels. Brussels maintains that when the aircraft got to them, the destination data had been changed. 'A senior Brussels ATC official' confirms that NW52 was cleared by London ATCC as it left the London control region to descend to 24,000 ft (I think they mean Flight Level 240 but I'm not sure – I'll use FL's anyway). The aircraft's planned track for Frankfurt would have taken it over Belgium at FL370 under control of Maastricht ATCC in the Netherlands, which handles traffic over FL245 across Belgium.

NW52 also addressed Brussels as 'Frankfurt' on contact, and numerous times thereafter. Brussels ATC didn't question the 'addressing error', apparently. They were also cleared to a VOR, Bruno, that they didn't recognise, and asked for the frequency. They were cleared for an ILS RWY 25L approach, which is the same runway orientation as at Frankfurt, but with a different ILS frequency. NW says that the crew must share responsibility, no matter what happened with ATC (this is in any case what aviation law

requires).

It looks like there is a lot for them to discuss.

Peter Ladkin

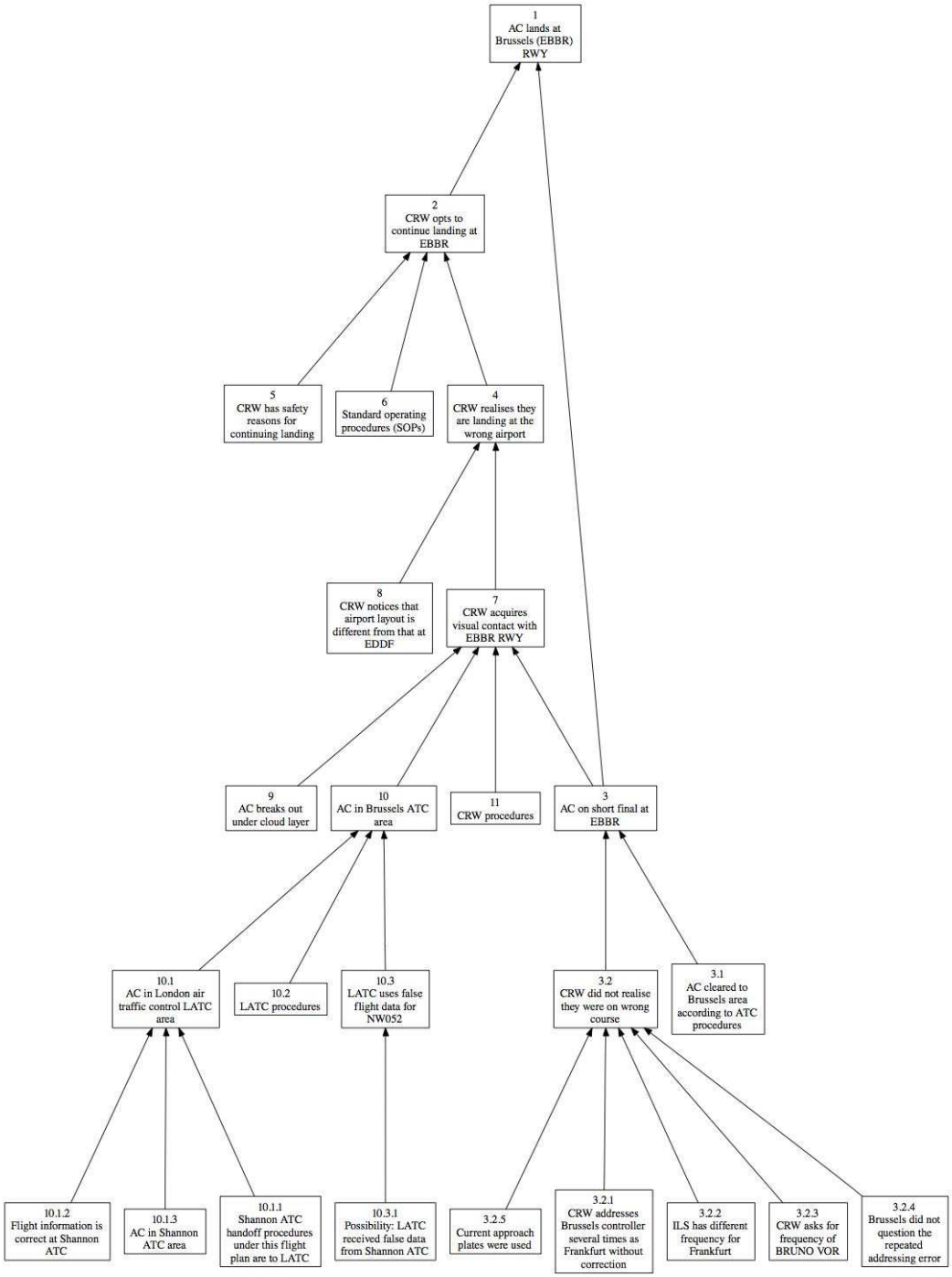


Figure 7.1: The North-West 052 WB-Graph

Chapter 8

The Grounding of the Royal Majesty on the Nantucket Shoals, USA

The Royal Majesty, a passenger ship registered in Panama, ran ashore on the Rose and Crown Shoal near Nantucket, Mas. This led to the vessel being structurally damaged. It had to be hauled from the shoal.

Although neither deaths or injuries, nor environmental damage resulted from the grounding of the vessel, the accident cost the shipping company an overall of $7m. The structural damage of the Royal Majesty accounted for $2m. Salvage and lost revenue, caused by the delayed disembarking of the ship's passengers, the vessel being moored in Boston, and the delayed resume of passenger service, accounted for $5m.

8.1 Cruise of the Royal Majesty

The Royal Majesty was on a 7-day voyage from Boston, Mas. to St. George's, Bermuda, back to Boston with 1509 persons on board. The ship departed St. George's, Bermuda, on June 9 1995 for the return trip to Boston where it was scheduled to arrive on June 11.

The vessel left pier in St. George's at 1203 and left port at 1252. The fathometer alarm, set to 0 meters when entering the harbour to avoid the alarm being falsely triggered, was not changed back to 3 meters, standard for open sea.

The bell log, logging technical information such as propeller pitch setting, the bearing, and the speed of the vessel, showed normal information up until 1245:37, 42 minutes after the ship left pier. After this time the vessel's course was recorded alternating with a bearing of 197.0 or 0.0. This indicates that at some point after 1245 the GPS device stopped functioning properly. Post-accident investigation found that the GPS antenna cable had separated from the antenna. The antenna itself showed no sign of physical damage.

The cruise back to Boston was divided into two legs. The first leg extended from St. George's to the entrance of the Boston traffic lanes. The second leg would have taken the vessel in a northerly direction through the traffic lanes along the eastern edge of Nantucket Shoals and around the eastern shores of Cape Cod. Estimated time for the cruise was about 41 hours.

Figure 8.1: Course of the Royal Majesty

The first leg was uneventful during the first 24 hours. The watch officers stated that the Royal Majesty followed its programmed track, as indicated on the display of the automatic radar plotting aid (ARPA) maintaining a course of about 336°.

Between 1200 and 1600, June 10, the navigator was on watch. He testified that the ship was heading 336° with an over-ground speed of 14.1 knots. The

weather was cloudy with winds out of east-northeast at 8 knots and seas between 1 and 3 feet. Visibility was greater than 10 miles. He stated that although he frequently checked the position data displayed by the Loran-C, all of the fixes he plotted during the voyage from Bermuda were derived from position data taken from the GPS and not the Loran-C. In addition he stated that the positions indicated by Loran-C and GPS would be expected to be within a half to one mile of each other in the open sea near Bermuda and within about 500 meters of each other in waters closer to the United States.

At 1600 the watch changed, and the vessel's chief officer relieved the navigator. He testified that he relied on the position data from the GPS to plot hourly fixes during his watches. The Loran-C was used as a backup system in case the GPS malfunctioned. He stated, however, that for the 1700 and 1800 hourly fixes he compared the data from the GPS with the data from the Loran-C and that in both instances the Loran-C indicated a position about 1 mile to the southeast of the GPS position.

At the beginning of the traffic lanes to Boston lies the "Precautionary Area" with buoys indicating the beginning of the traffic lanes. The BA buoy indicates the entry to the traffic lane from Nantucket to Boston. The Chief Officer testified that at about 1645 the master telephoned the bridge and asked him when he expected to see the BA buoy. The chief officer responded that the vessel was about 2.5 hours away (35.25 miles at 14.1 knots) from the buoy. The master then asked the chief officer to call him when he saw the buoy. About 45 minutes later (1730) the master visited the bridge, checked the vessel's progress by looking at the positions plotted on the chart and at the map overlay presented on the ARPA/radar display, and asked a second time whether the chief officer had seen the BA buoy. The chief officer responded that he had not. Shortly thereafter, the master left the bridge.

According to the chief officer, at about 1845, he detected a target on radar off the port bow at a range of about 7 miles and concluded that the target was the BA buoy. He stated that his conclusion had been based on the GPS position data, which indicated that the Royal Majesty was following its intended track, and on the fact that the target had been detected about the time, bearing, and distance that he had anticipated detecting the BA buoy. He further testified that on radar the location of the target coincided with the plotted position of the buoy on the ARPA/radar display. He said that about 1920, the radar target that he believed to be the BA buoy passed down the Royal Majesty's port side at a distance of 1.5 miles. He stated that he could not visually confirm the target's identity because of the glare on the

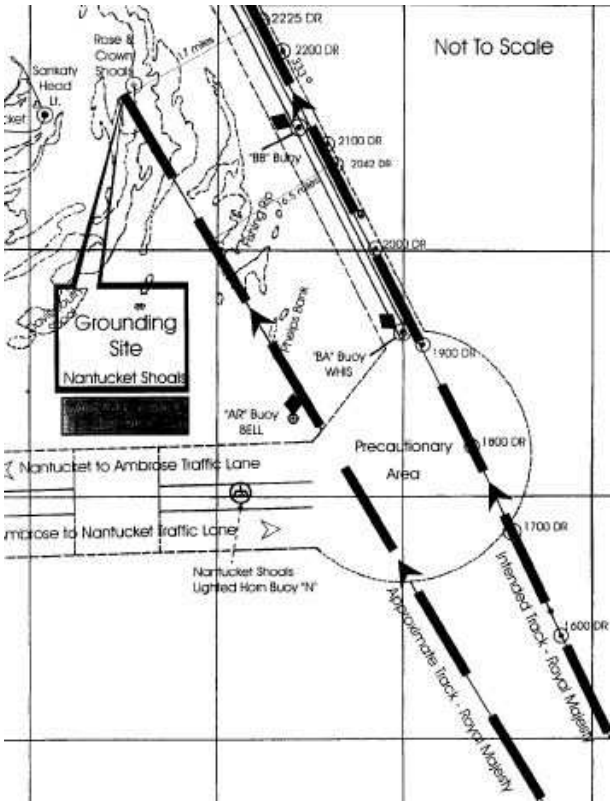


Figure 8.2: Precautionary Area and Shoals

ocean surface caused by the rays of the setting sun.

The reconstruction of the Royal Majesty's actual track suggests that the AR buoy marking the entrance to the Nantucket to Ambrose traffic lane was mistaken for the BA buoy.

The chief officer testified that about 1930, the master telephoned the bridge and asked him for the third time whether he had seen the BA buoy. According to the chief officer, he responded that the ship had passed the BA buoy about 10 minutes earlier. The master then asked whether the chief officer had detected the buoy on radar; the chief officer replied that he had. According to the testimony of the chief officer and the master, the chief officer did not tell the master that he had been unable to visually confirm the identify of the BA buoy, and the master did not ask whether the buoy had been visually confirmed.

The second safety officer (second officer) arrived on the bridge about

1955 and prepared to assume the watch from the chief officer. According to the testimony of both officers, during the change-of-the-watch briefing (2000), they discussed the traffic conditions and the vessel's course, speed, and position. According to the testimony, the chief officer did not discuss with his relief the circumstances surrounding his identification of the BA buoy. The second officer assumed the watch at 2000 and the chief officer left the bridge. Shortly after assuming the watch, the second officer reduced the range setting on the port radar from the 12-mile range to the 6-mile range. For plotting hourly fixes during his watches, he relied on the position data from GPS. He considered Loran-C to be a backup system. The second officer also stated that it was not his practice to use Loran-C to verify the accuracy of GPS.

The quartermaster standing lookout on the port bridge wing (port lookout) stated that about 2030 he saw a yellow light off the vessel's port side and reported the sighting to the second officer. The second officer acknowledged the report, but took no further action. Shortly after the sighting of the yellow light, both starboard and port lookouts reported the sighting of several high red lights off the vessel's port side. Again the second officer acknowledged the report, but took no further action.

Were the ship to have been on course it would have been about 17 miles east of its actual position. This would have made it difficult if not impossible to see these lights.

Shortly after the sightings of the yellow and red lights, the master came to the bridge. The master spent several minutes talking with the second officer and checking the vessel's progress by looking at the plotted fixes on the chart and the map overlay on the ARPA/radar display. According to the master, the GPS and ARPA/radar displays were showing that the vessel was within 200 meters of its intended track. The master then left the bridge. According to the testimony of both the master and the second officer, no one told the master about the yellow and red lights that the lookouts had sighted earlier.

About 2145 the master telephoned the bridge and asked the second officer whether he had seen the BB buoy. The second officer told him that he had seen it.

The master arrived about 2200 on the bridge for the second time during that watch. After talking with the second officer for several minutes, he checked the vessel's progress by looking at the positions plotted on the chart and at the map overlay on the ARPA/radar display. He again asked the second officer whether he had seen the BB buoy and the second officer replied

that he had. Satisfied that the positions plotted on the chart and that the map displayed on the radar continued to show the vessel to be following its intended track, the master left the bridge about 2210. He stated that he did not verify the vessel's position using either the GPS or the Loran-C as his officers had reported that the BA and BB buoys had been sighted, and he had observed that the map overlay on the ARPA/radar display showed that the vessel was following its intended track.

The second officer testified that he had not seen the BB buoy but had informed the master otherwise because he had "checked the GPS and was on track" and because "perhaps the radar did not reflect the buoy." On previous transits of the traffic lanes, he said he had sighted buoys both visually and by radar.

A few minutes after the master left the bridge, the port lookout reported to the second officer the sighting of blue and white water dead ahead. The second officer acknowledged receiving the information, but did not discuss it or take action. The port lookout stated that the vessel later passed through the area where the blue and white water had been sighted.

About 2220, the Royal Majesty unexpectedly veered to port and then sharply to starboard and heeled to port. The second officer stated that because he was alarmed and did not know why the vessel was sheering off course, he immediately switched from autopilot to manual steering. The master, who was working at his desk in his office, felt the vessel heel to port and ran to the bridge. He stated that when he arrived on the bridge, he saw the second officer steering the ship manually and instructed one of the lookouts to take over the helm. The master then turned on the starboard radar, set it on the 12-mile range, and observed that Nantucket was less than 10 miles away. According to the master, he immediately went into the chart room to verify his position. He stated that he immediately ordered the helmsman to apply hard right rudder. However, before the helmsman could respond, the vessel grounded, at 2225. The master stated that he then had the vessel's GPS and Loran-C checked and realized for the first time that the GPS position data was in error by at least 15 miles. The Loran-C position data showed the vessel where it had grounded, about 1 mile south of Rose and Crown Shoal.

8.2 The Integrated Bridge System

To aid with the steering of the vessel, the Royal Majesty was equipped with an integrated bridge system. Main component of this system was a NACOS 25 navigation system from STN Atlas Electronic.

This system provided the functionality to create maps which were presented on the ARPA/radar displays. Reference points such as way points, turning points or navigation marks could be defined on basis of these maps. The NACOS 25 provided an autopilot system, that steered the vessel according to the preprogrammed way-points and manoeuvring characteristics.

The information used as input for the NACOS 25 was Loran-C or GPS positioning information as well as gyro and speed data. The navigation system presented radar information, map, position and course on two ARPA/radar displays. Each display used radar input from a seperate Atlas 8600 ARPA radar. The starboard radar was only used in case of bad weather. On the day of the grounding it was only switched on by the master directly before the grounding.

Although both the GPS and Loran-C simultaneously sent position data to the NACOS 25, the system only used position data from one external position receiver at a time, as selected by the crew. The NACOS 25 was not designed to compare the GPS and the Loran-C position inputs, nor was it designed to display both sets of position data to the bridge officers simultaneously so that they could compare the data. On June 9 and throughout the voyage, the autopilot was set by the crew to accept and display position data from the GPS receiver, which was the position receiver normally selected by the crew during the 3 years the vessel had been in service.

8.2.1 Autopilot

The autopilot continuously calculated a dead reckoning (DR) position in order to provide a comparison with the position data provided by the external position receiver (GPS or Loran-C).

The autopilot compared its computed DR position with the position provided by an external position receiver. If the distance between these positions lay within a specified distance the autopilot made necessary course corrections and used the external position receiver's position as initial point for its DR calculations.

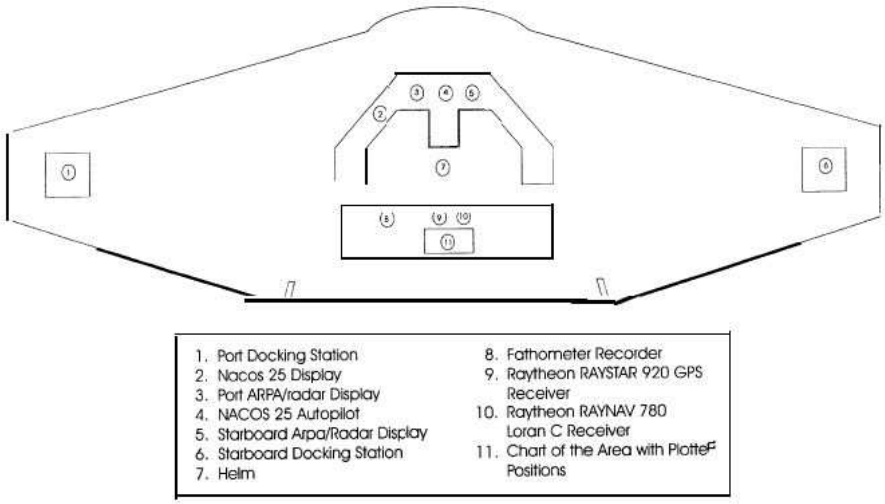


Figure 8.3: Layout of the Royal Majesty's Bridge

If the distance between DR and external position was greater than a specified distance the autopilot generated a *warning position fix* by sounding an alarm and presenting visual indication on all NACOS displays. This position fix indicated that the watch officer's immediate attention was required.

If the lateral distance between the external position and the preprogrammed track line exceeded a specified distance, the autopilot generated a *warning track limit exceeded* alarm indicating that the vessel is off course.

8.2.2 The Raytheon GPS System

The Raytheon GPS unit installed on the Royal Majesty had been designed as a stand-alone navigation device in the mid- to late 1980s, when navigating by dead reckoning was common and before the GPS satellite system was fully operational. This means that the GPS unit calculated a likely position based on course and speed input, in case of unavailable positioning information, e.g. not enough satellites in sight. Course and speed input could be provided manually or via an interface box. In case of the Royal Majesty the interface box was used as STN Atlas was told that the GPS would be backed up by a Loran-C system during periods of GPS data loss. STN Atlas stated that they were not told that the GPS receiver would default to the DR mode.

When the GPS unit (RAYSTAR 920 GPS) switched to DR mode, it

announced this change of mode with a 1 second aural alarm and continuously displayed SOL and DR on the unit's display. Additionally it was possible to connect an external alarm to a switch. To announce the mode change to connected systems a status field in the NMEA 0183 communication protocol was changed from valid to invalid, indicating that valid position data was no longer transmitted.

All the watch officers testified that they did not see SOL and DR displayed on the GPS unit during their watches before the grounding. Their testimony indicated that they understood the meaning of these symbols and had seen them on previous occasions.

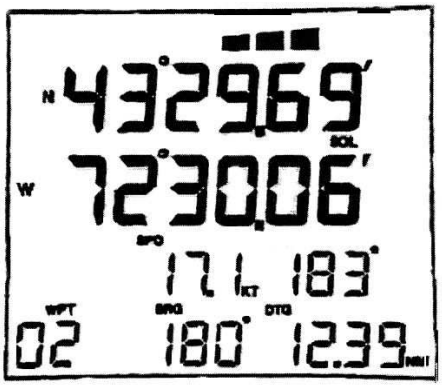


Figure 8.4: RAYSTAR 920 GPS Display

The navigator stated that during the 11 months he had been aboard the vessel, he had observed a phenomenon he called "chopping." Other deck officers too had witnessed this phenomenon. Chopping occurred when the position data displayed by the GPS was unreliable. Majesty Cruise Line's electronics technician and the Raytheon staff indicated that chopping could have been the result of atmospheric interference with GPS signals or the obstruction of the GPS antenna's view of the satellites. This could be caused by the vessel's superstructure and/or tall buildings or other structures while the vessel was in port. According to Majesty Cruise Line, the GPS antenna, originally installed on the radar mast, had been moved in February 1995, as part of an effort to eliminate the chopping. Majesty Cruise Line's electronics technician indicated, that as a result of the move, the antenna's view of the satellites was less obstructed and the crew complained much less about chopping.

8.3 Communication Protocol

The NACOS 25 System used for the Royal Majesty was sold in May 1988 to the Royal Majesty's shipyard. It was the last NACOS 25 unit sold by STN Atlas. Because of construction delays it was held in stock until it was installed in 1992 on board the ship.

It uses NMEA 0183 for the transmission of information between devices. This protocol provides three methods to indicate whether the transmitted data is inaccurate or unavailable:

- null fields where the sentence is transmitted but no data is inserted in the fields in question;
- using system-specific status sentences (available only for Loran-C);
- use of "status" or "quality indicator" characters in specific sentences.

With NMEA 0183 version 1.5, released in December 1987, the use of null fields is the most common method, as most sentences do not have status fields. According to STN Atlas's interpretation of this specification, when a position receiver with a GPS talker identifier has no GPS position data available, it must transmit null fields instead.

The Raytheon 920 GPS unit used a status field in the NMEA 0183 communication protocol from valid to invalid indicating that valid position data is no longer transmitted while transmitting its computed DR positioning information.

8.4 The Royal Majesty WB-Graphs

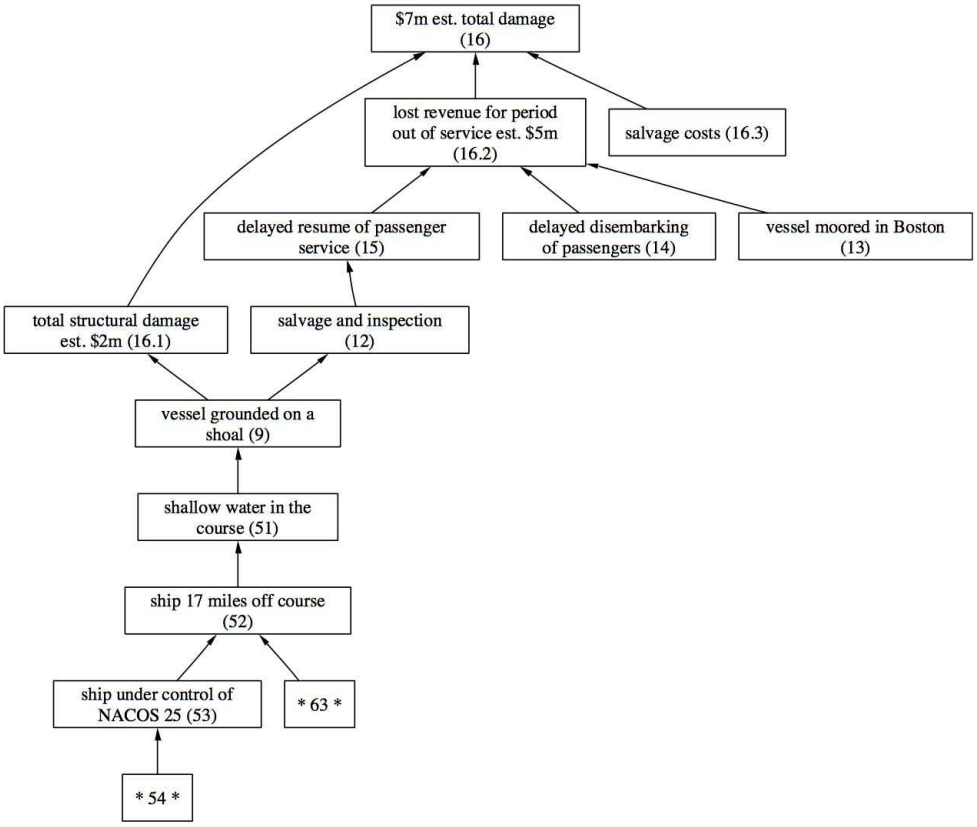


Figure 8.5: Royal Majesty WB-Graph (Part 1)

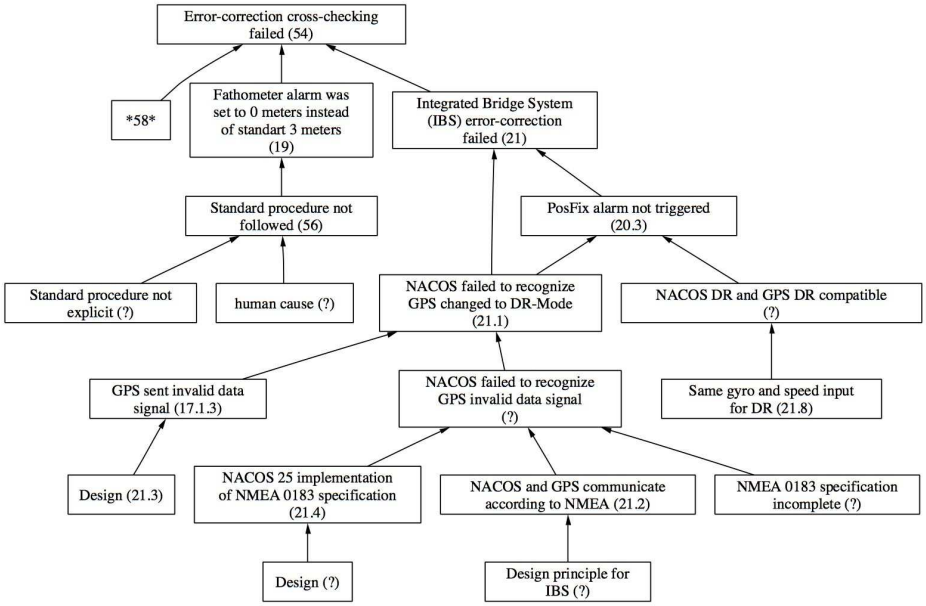


Figure 8.6: Royal Majesty WB-Graph (Part 2)

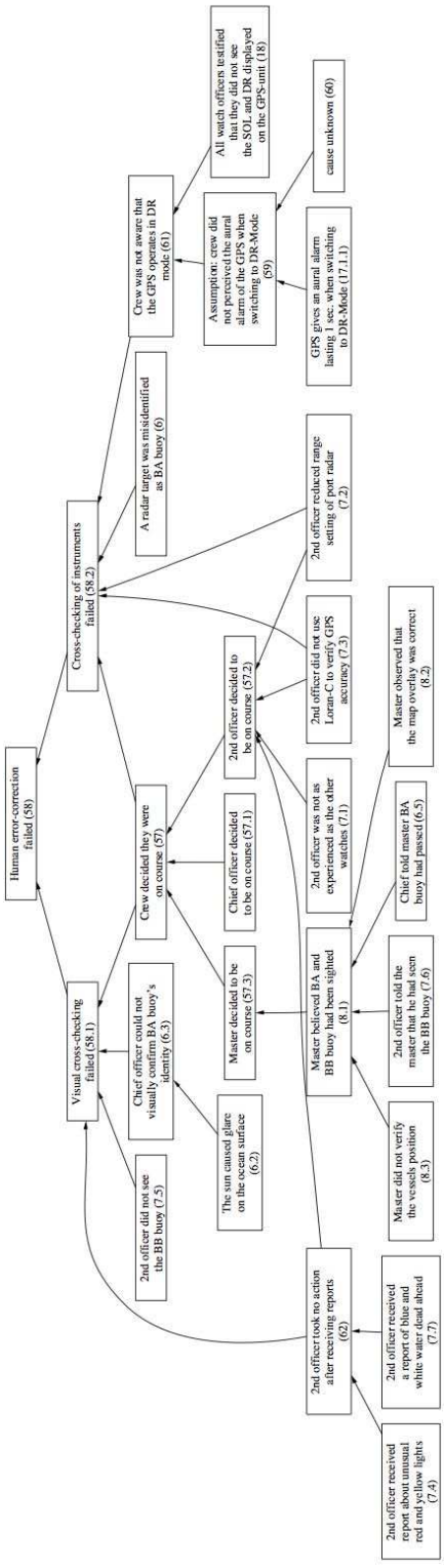


Figure 8.7: Royal Majesty WB-Graph (Part 3)

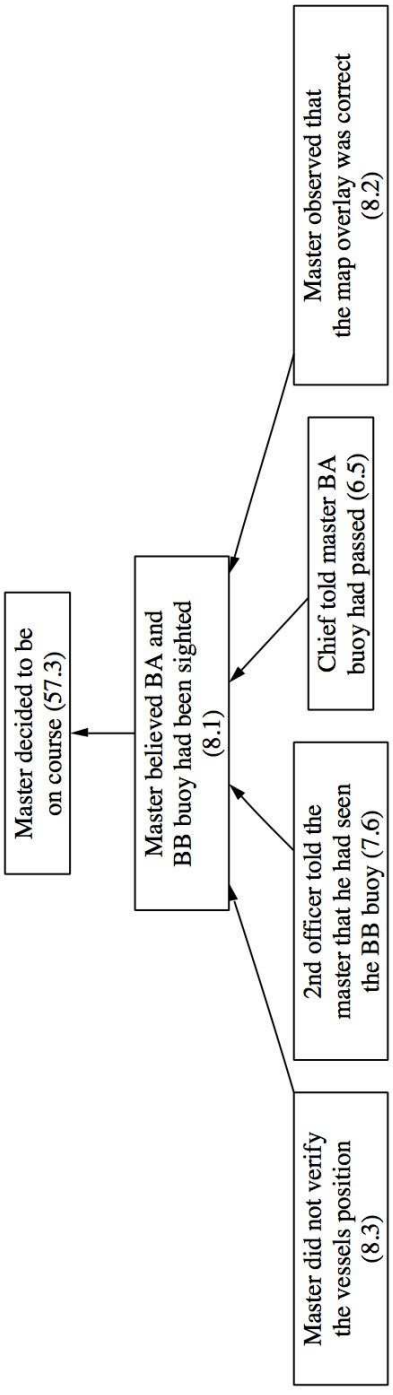


Figure 8.8: Royal Majesty WB-Graph (Part 4)

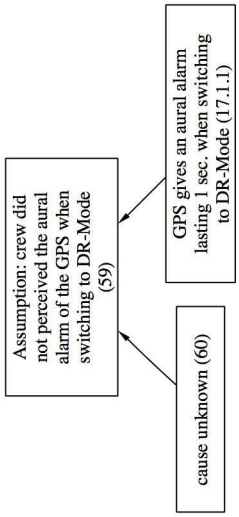


Figure 8.9: Royal Majesty WB-Graph (Part 5)

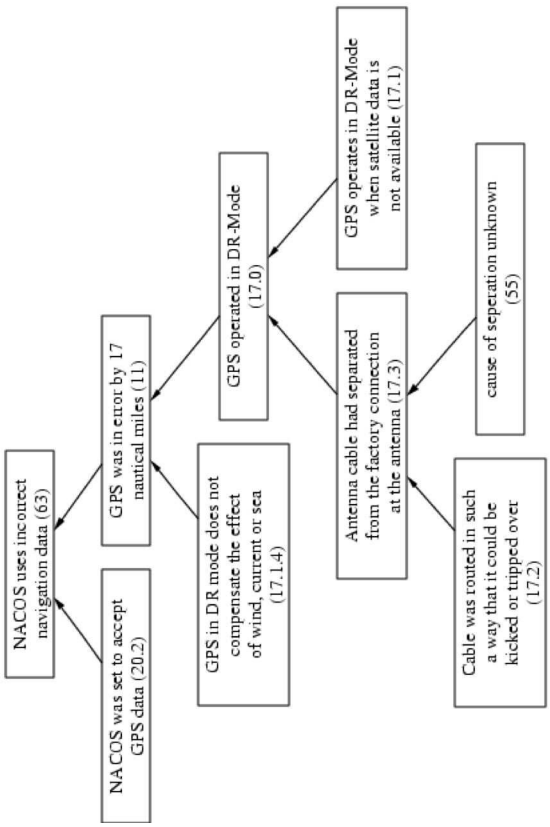


Figure 8.10: Royal Majesty WB-Graph (Part 6)

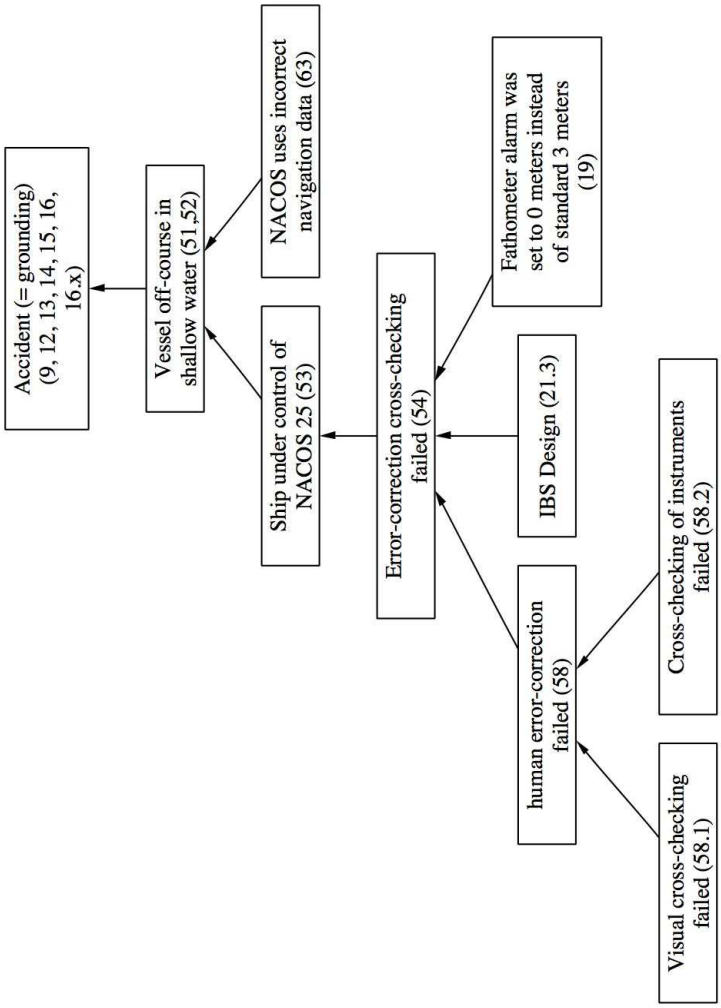


Figure 8.11: Royal Majesty WB-Graph (Part 7)

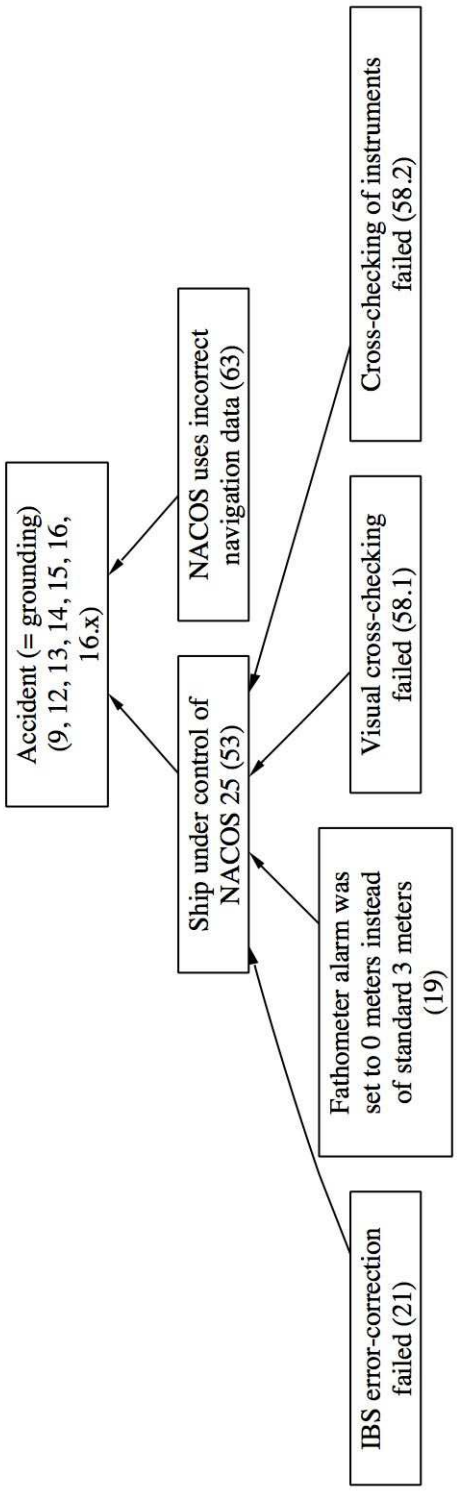


Figure 8.12: Royal Majesty WB-Graph (Part 8)

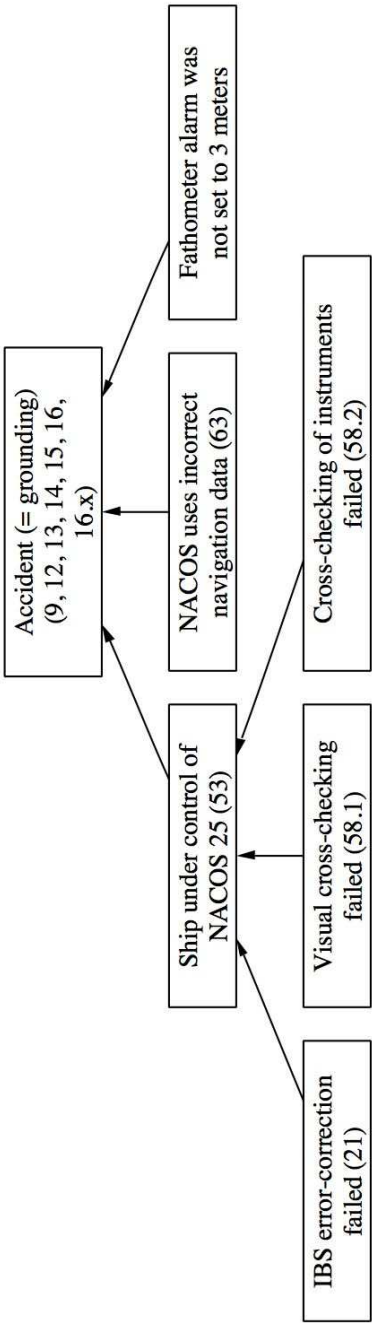


Figure 8.13: Royal Majesty WB-Graph (Part 9)