A WBA of the Royal Majesty Accident

Peter Husemann, Peter B. Ladkin, Jan Sanders, Jörn Stuphorn
RVS Group, Faculty of Technology, University of Bielefeld

DRAFT VERSION of July 7, 2003

1 Reference Document

This accident is reported in NTSB Accident Report [NTSB97]. We worked from this document while preparing the WBA.

2 Short History

The cruise ship *Royal Majesty* left St. George's, Bernmuda bound for Boston at about midday on June 9, 1995. The ship was equipped with an Integrated Bridge System (IBS) consisting of a STN Atlas Elektronik NACOS 25 autopilot obtaining position data from a Raytheon RAYSTAR 920 GPS and a Raytheon RAYNAV 780 Loran-C navigation units. Shortly after departure, the GPS switched to dead-reckoning mode because it was no longer receiving satellite signals. The GPS antenna was later found to have separated from its cable. The autopilot tracked the GPS "data" until the ship grounded on the Nantucket shoals, some of the most dangerous waters to general shipping in the world, at about 22.25 on June 10, some 34 hours later and some 17 miles west of course. The Loran-C was serviceable; however, no one had noticed the large discrepancy between the GPS reading and the Loran-C reading despite it being procedure to cross-check hourly. Two buoys, BA and BB, identified the shipping lane. The first buoy was "identified" against the glare of sunset; it seems likely that another buoy, positioned west of BA, was seen instead. The second buoy was reported identified, but reconstruction of the ship's track shows no buoy remotely in the area. "Blue and white water", a seafarer's indication of shallow water, was reported by watch. Some shore lights were seen, presumed to be inter alia the indentification lights of radio towers, in an area which should have been sea had the ship been on track. No action was taken and the ship ran aground on Rose and Crown Shoal. No one was injured. The cost of salvage and the cost in lost revenue was substantial.

There is a fathometer on board, independent of the IBS, which alarms when a preset depth is sounded. The fathometer alarm is normally set to 0m in port, to avoid nuisance alarms during harbor manoeuvring, and reset to a standard 3m depth under way. The fathometer alarm had remained at its in-port setting of 0m and did not alarm as the ship entered shallow water in the Nantucket shoals.

The GPS was taken to have been reporting that its data was "*invalid*". It reports this by setting the international standard (NMEA 0183) *valid/invalid* status bits to *invalid*. The designers of the autopilot "expected inaccurate or failed GPS position data to be recognizable by nulled position data fields or by no change in the position latitude/longitude.... STN Atlas therefore chose not to program the NACOS 25 to check the *valid/invalid* bits in the NMEA 0183 data stream as a means of detecting invalid GPS data" (NTSB).

3 List of Facts

The nodes numbered 1-21, with their subnodes, were obtained directly from the NTSB report. The nodes numbered 51 and upwards were inserted by us as necessary statements of causal factors, which we needed to construct the WBG

1. Navigator found the navigation equipment in "perfect" operating condition before scheduled departure at 1200, June 9. *(Page 1)*
2. June 9, 1203: Departure from St. George's according to the Bell-log. *(Pages 19,20)*
3. June 10, 1200: The Navigator had the watch. *(Page 4)* He
   - 3.1 frequently checked the position data of the Loran-C. *(Page 4)*
   - 3.2 used the GPS only for the hourly fixes. *(Page 4)*
4. June 10, 1600: The chief officer relieved the navigator for watch. *(Page 4)* He
   - 4.1 stated that he compared the position data of GPS and Loran-C, which showed a difference of 1 nautical mile at 1700. *(Page 4)*
   - 4.2 stated that he compared the position data of GPS and Loran-C, which showed a difference of 1 nautical mile at 1800. *(Page 4)*
   - 4.3 said that he relied on the position data of the GPS to plot hourly fixes. *(Page 4)*
   - 4.4 generally used the Loran-C only as a backup when he thought the GPS was malfunctioning. *(Page 4)*
5. Weather was good and the visibility was clear. East-northeasterly wind and sea. *(Page 4)*
6. A radar target was misidentified as BA buoy, which is an important waypoint *(Page 4)*
   - 6.1 1920: The radar target that the chief officer believed to be the BA buoy passed down at a distance of 1.5 miles. *(Page 4)*
   - 6.2 The rays of the setting sun caused glare on the ocean surface in the direction of the buoy. *(Page 4)*
   - 6.3 The chief officer could not visually confirm the target's identity. *(Page 4)*
   - 6.4 June 10, 1845: A radar target coincided with the plotted position of the BA buoy at a range of about 7 miles. *(Page 4)*
   - 6.5 The chief officer told the master at 1930 that the BA buoy had passed 10 minutes earlier. *(Pages 4,8)*
     - 6.5.1 The chief officer did not tell the master that he had been unable to confirm the identity of the BA buoy. *(Page 8)*
     - 6.5.2 The master did not ask whether the buoy had been visually confirmed. *(Page 8)*
7. June 10, 2000: the second safety officer assumed the watch from the chief officer. *(Page 8)* He
   - 7.1 was not as experienced as the other navigation watches. *(Page 13)*
   - 7.2 reduced the range setting of the port radar from 12 to 6-mile-range. *(Page 8)*
   - 7.3 did not use the Loran-C to verify the accuracy of the GPS. *(Page 8)*
   - 7.4 received a report of an unusual yellow light at 2030 and several red lights on the port side shortly after. *(Page 8)*
     - 7.4.1 took no action after receiving the reports. *(Page 8)*
   - 7.5 did not see the BB buoy. *(Page 9)*
   - 7.6 told the master that he had seen the second (BB) buoy. *(Pages 8,9)*
     - 7.6.1 He said he had "checked the GPS and was on track". *(Page 9)*
     - 7.6.2 He said "perhaps the radar did not reflect the buoy". *(Page 9)*
   - 7.7 received a report of blue and white water dead ahead. *(Page 9)*
     - 7.7.1 took no action after receiving the report. *(Page 9)*
8. The master checked the vessel's progress twice between 2030 and 2210. *(Page 8)* He
   - 8.1 believed that the BA and BB buoy had been sighted. *(Page 8)*
   - 8.2 observed that the map overlay on the ARPA display showed the planned and plotted track. *(Page 8)*
   - 8.3 did not verify the vessel's position. *(Page 8)*
9. June 10, 2225: The vessel grounded on a shoal. *(Page 9)*
10. The master checked the GPS and Loran-C after the grounding and realized that the GPS was in error by at least 15 nautical miles. *(Page 9)*
11. GPS was in error by 17 nautical miles. *(Page 7)*

12. June 11, 2154: Salvage and first inspection of damage of the Royal Majesty *(Page 11)*
    - 12.1 Majesty Cruise Line, the owner of the vessel, made arrangements to hire tugboats to pull the vessel off the shoal. *(Pages 9,11)*
    - 12.2 The Vessel was refloated with the help of five tug boats*(Page 11)* and
    - 12.3 escorted to a save anchorage near Chartham *(Page 11)* where
    - 12.4 the damage was surveyed by the U.S. Coast Guard. *(Page 11)*
13. June 12, 1535: The vessel was moored in Boston. *(Page 11)*
    - 13.1 Scheduled arrival was 0530 on June 11. *(Page 1)*
14. June 12, 1710: Passengers began disembarking. *(Page 11)*
15. June 24: The vessel resumed passenger service. *(Page 12)*
16. $7 million estimated total damage. *(Page 12)*
    - 16.1 Total structural damage: estimated $ 2 million. *(Page 12)*
    - 16.2 Lost revenue for the period out of service: estimated $ 5 million. *(Page 12)*
    - 16.3 Salvage costs are not mentioned in the report.
17. Postaccident testing of the Raytheon 920 GPS indicated that the GPS transmitted unreliable DR-derived position data *(Page 24)*
    - 17.0 GPS operated in DR mode
    - 17.1 The GPS unit operates in DR (dead reckoning) mode when satellite data is not available. *(Page 14)* When switching to this mode it
        - 17.1.1 gives an aural alarm lasting 1 second. *(Page 14)*
        - 17.1.2 continously displays SOL (solution) and DR on the LCDisplay. *(Page 14)*
        - 17.1.3 changes NMEA 0183 status field bits from *valid* to *invalid* to indicate that valid position data is no longer being transmitted. *(Page 14)*
        - 17.1.4 does not compensate for the effect of wind, current or sea. *(Page 14)*
    - 17.2 GPS cable was routed in such a way that it could be kicked or tripped over. *(Page 24)*
    - 17.3 Postaccidental examination of the GPS found the antenna cable of the GPS had separated from the factory connection at the antenna. *(Page 24)*
        - 17.3.1 Bell logs indicate the separation happened at 1252 on June 9. *(Pages 19,20)*
18. All the watch officers testified that they did not *see* the SOL and DR displayed on the GPS unit. *(Page 17)*
    - 18.1 Their testimony indicated that they understood the meaning of these symbols and had seen them on previous occasions. *(Page 17)*
19. The Fathometer alarm was set at 0 meters instead of a standard of 3 meters. *(Page 21)*
20. The NACOS 25 autopilot from STN Atlas
    - 20.1 was designed to use position data from only one external position receiver at a time although both GPS and Loran-C simultaneously sent data to it. *(Page 17)*
    - 20.2 was set to accept GPS data. *(Page 17)*
    - 20.3 has a *position fix* alarm which visually and aurally informs the watch officer about discrepancies between track and intended track if the own DR position and the external position are more than a specified distance apart. *(Page 18)*
    - 20.4 has DR capability. *(Page 17)*
21. There were incompatibilities in the communication between devices of the Integrated Bridge System (IBS).
    - 21.1 The autopilot did not "understand" when the GPS switched to DR mode and accepted the data as valid.
    - 21.2 The IBS uses NMEA 0183 for the communication between the devices. *(Page 17)*
    - 21.3 The Raytheon 920 GPS uses NMEA *valid/invalid* bits to indicate the invalid data derived from DR mode, as listed in 17.1.3. *(Page 17)*

- 21.4 STN Atlas NACOS 25 expected invalid GPS position data to be recognizable by
  - 21.4.1 nulled position data fields *(Page 17)*, or
  - 21.4.2 halted transmission *(Page 17)*, or
  - 21.4.3 no changes in the position latitude/longitude. *(Page 17)*
- 21.5 No changes in the position latitude/longitude would trigger *position fix* alarm. *(Page 17)*
- 21.6 Nulled data fields or halted transmission cause the NACOS 25 to switch its position input to *estimated* (own DR mode). *(Page 17)*
  - 21.6.1 If NACOS 25 is in estimated input mode this information is highlighted on all NACOS and radar displays. *(Page 17)*
- 21.7 NMEA 0183 has three methods to indicate inaccurate or unavailable data. *(Page 17)*
  - 21.7.1 null fields where the sentence is transmitted but no data is inserted in the fields in question, which is the most common method. *(Page 17)*
  - 21.7.2 by using system-specific status sentences (available only for Loran-C). *(Page 17)*
  - 21.7.3 by the use of “status” or “quality indicator” characters in specific sentences. *(Page 17)*
- 21.8 NACOS and GPS get and use the same gyro and speed input for DR. *(Page 32)*

51. Shoals and shallow water were in the course. *(Page 17)*
52. Ship was 17 nautical miles off the planned and plotted course. *(Pages 7,17)*
53. Ship was under control of NACOS 25 autopilot.
    - 53.1 The Navigator set the NACOS 25 to NAV mode shortly after departure. *(Page 1)*
    - 53.2 When engaged and operating in NAV mode, the NACOS steers the ship in accordance with the programmed track while automatically compensating for the effect of gyro error, wind, current, and sea. *(Page 14)*
54. Error-correction cross-checking failed.
55. Cause of separation of cable from GPS-antenna (unknown).
56. Cause of 19 : standard procedure not followed.
57. Crew decided they were on course
    - 57.1 The chief officer decided they were on course
    - 57.2 The second officer decided they were on course
    - 57.3 The master decided they were on course
58. Human error-correction failed.
    - 58.1 Visual cross-checking failed.
    - 58.2 Cross-checking of instruments failed.
59. Assumption: Crew did not perceived the aural alarm of the GPS when switching to DR-Mode.
60. Cause of 59 (unknown)
61. Crew is not aware of the fact that the GPS operates in DR-Mode.
62. Second Officer took no action after receiving visual reports. (7.4, 7.7)
63. NACOS uses incorrect navigation data.

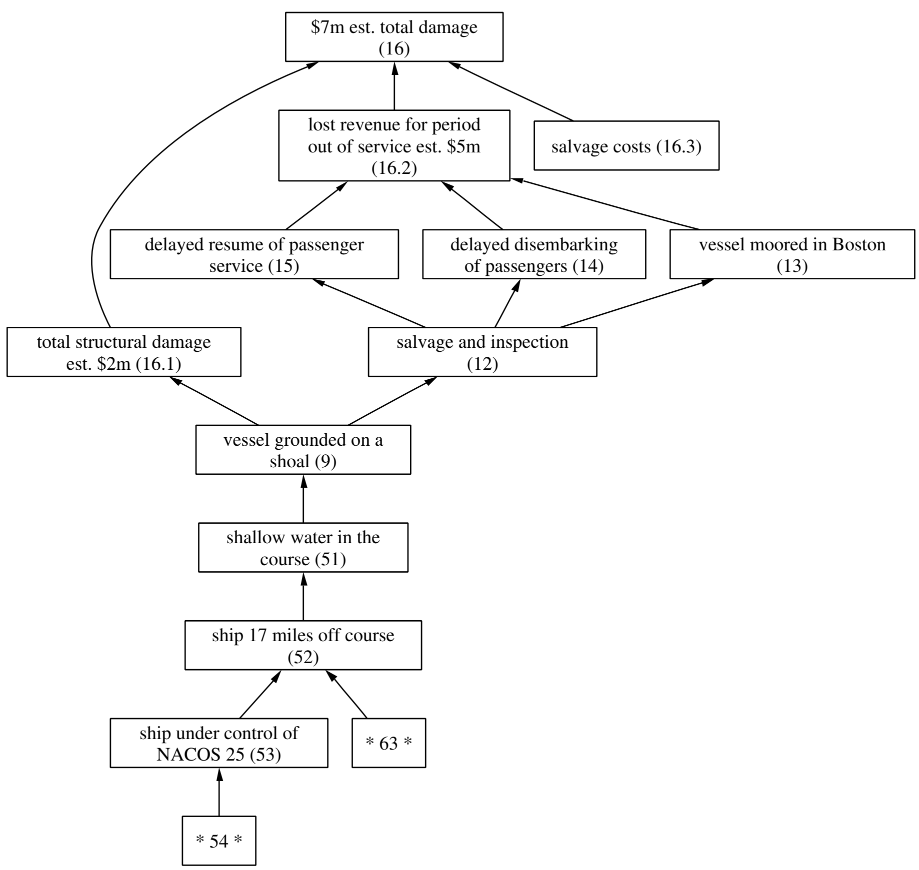
Acknowledgements

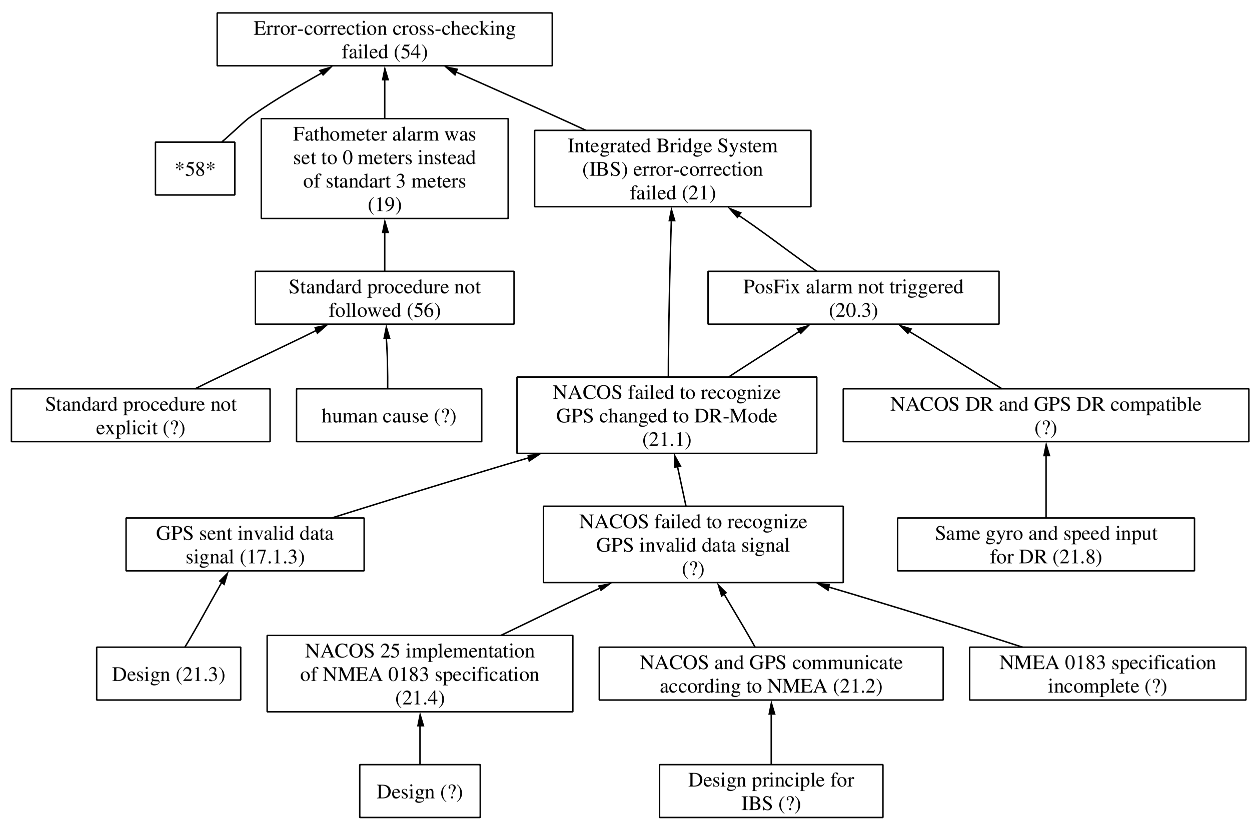
The List of Facts was developed in seven versions by a team including the authors as well as Lars Heidieker, Nils Hoffmann, Jan Paller and Andreas Vangerow. We started from a seed document prepared by Husemann and Hoffmann. Given this seed document, the total time spent in meeting devising the List of Facts, excluding the time spent writing it up, was of the order of 12 person-hours, comprising in this case 2-3 hours per person, with between 4 and 6 people per meeting, over 2 meetings. The List of Facts was supplemented during construction of the WB-Graph; the additional time was counted as time spent developing the WB-Graph.

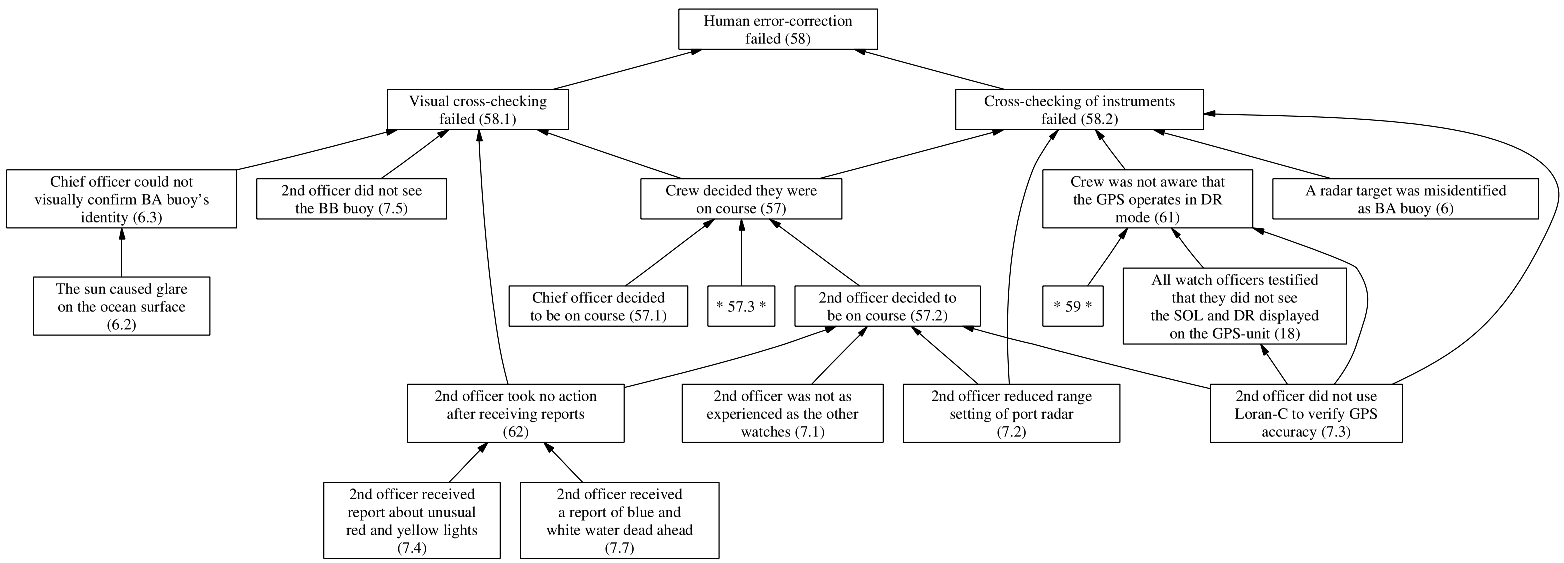
4 WB-Graphs

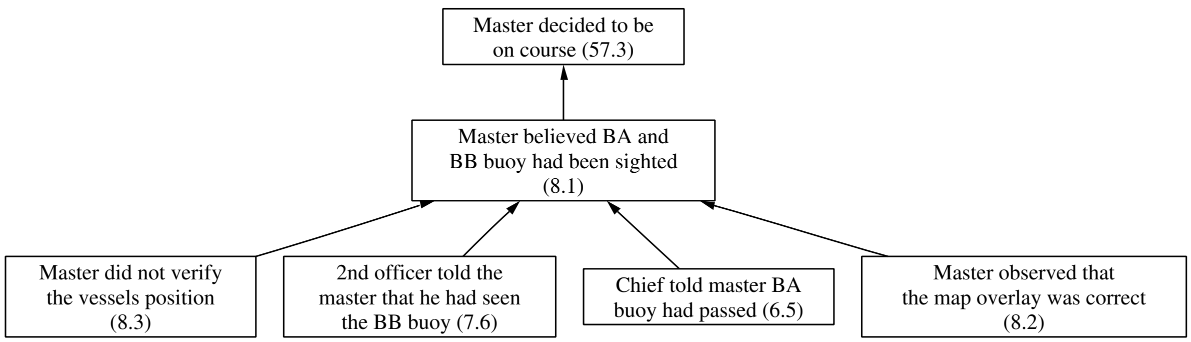
The Why-Because Graph (WBG) is constructed by applying the Counterfactual Test to the List of Facts taken two at a time. The Counterfactual Test asks the question of Events, States or Processes A and B, which both happened, whether B would have happened had A not happened. If the answer is yes, the Test is passed and an edge drawn between the nodes in the WBG; if the answer is no, the Test is failed and no edge is drawn. The Counterfactual Test is underlain by a rigorous semantics. A formal logic exists for the semantics, and also for demonstrating whether a WBG is correct and complete according to certain precise criteria. Details may be found in the references [Lad01, LadLoe98]. We did not apply these additional formal criteria yet to check the graph we constructed.

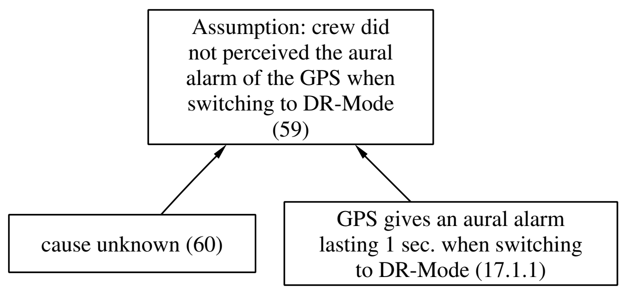
The WBG shown here is divided into a number of subgraphs using a "connector" notation which is not yet described in other documents on WBA. A *connector* is a node whose label consists entirely in the number from the List of Facts, surrounded by "*" symbols, as in the nodes labelled "* 54 *" and "* 63 *" in the main graph. These connector symbols indicate that the subgraph rooted at node 54 appears as a separate graph (in this case, the next graph). Using this method, we have split the WBG of the accident into 6 graphs.

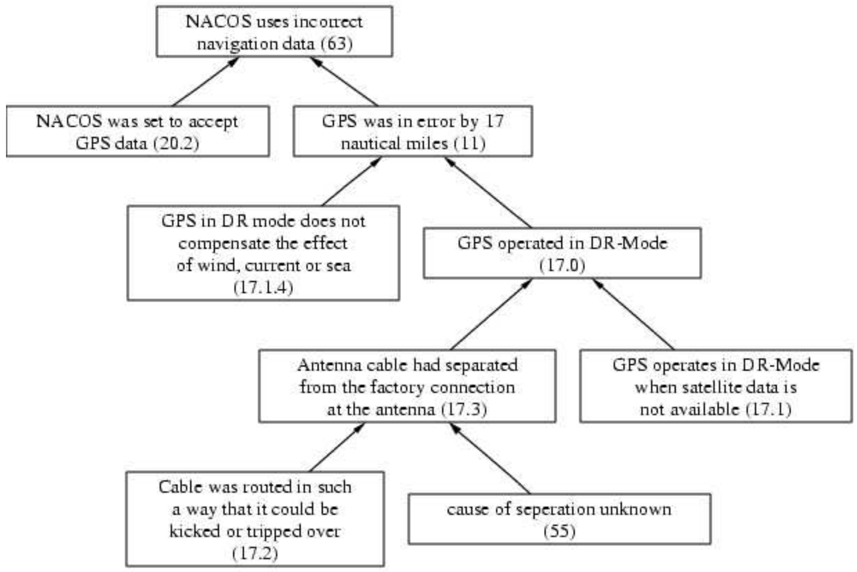



Error-correction cross-checking failed (54)
58
Fathometer alarm was set to 0 meters instead of standart 3 meters (19)
Integrated Bridge System (IBS) error-correction failed (21)
Standard procedure not followed (56)
PosFix alarm not triggered (20.3)
Standard procedure not explicit (?)
human cause (?)
NACOS failed to recognize GPS changed to DR-Mode (21.1)
NACOS DR and GPS DR compatible (?)
GPS sent invalid data signal (17.1.3)
NACOS failed to recognize GPS invalid data signal (?)
Same gyro and speed input for DR (21.8)
Design (21.3)
NACOS 25 implementation of NMEA 0183 specification (21.4)
NACOS and GPS communicate according to NMEA (21.2)
NMEA 0183 specification incomplete (?)
Design (?)
Design principle for IBS (?)


Human error-correction failed (58)
Visual cross-checking failed (58.1)
Cross-checking of instruments failed (58.2)
Chief officer could not visually confirm BA buoy's identity (6.3)
2nd officer did not see the BB buoy (7.5)
Crew decided they were on course (57)
Crew was not aware that the GPS operates in DR mode (61)
A radar target was misidentified as BA buoy (6)
The sun caused glare on the ocean surface (6.2)
Chief officer decided to be on course (57.1)
* 57.3 *
2nd officer decided to be on course (57.2)
* 59 *
All watch officers testified that they did not see the SOL and DR displayed on the GPS-unit (18)
2nd officer took no action after receiving reports (62)
2nd officer was not as experienced as the other watches (7.1)
2nd officer reduced range setting of port radar (7.2)
2nd officer did not use Loran-C to verify GPS accuracy (7.3)
2nd officer received report about unusual red and yellow lights (7.4)
2nd officer received a report of blue and white water dead ahead (7.7)


Master decided to be on course (57.3)
Master believed BA and BB buoy had been sighted (8.1)
Master did not verify the vessels position (8.3)
2nd officer told the master that he had seen the BB buoy (7.6)
Chief told master BA buoy had passed (6.5)
Master observed that the map overlay was correct (8.2)


Assumption: crew did not perceived the aural alarm of the GPS when switching to DR-Mode (59)
cause unknown (60)
GPS gives an aural alarm lasting 1 sec. when switching to DR-Mode (17.1.1)



Acknowledgments

The WBG was developed by a team led by Husemann, including the authors and other developers of the LoF, excluding Ladkin. The graphs were implemented in *ciedit* by Husemann, Stuphorn and Ladkin. Six participants developed the WBGs over meetings totalling 3.5 hours; total time spent developing the WBG was 21 person-hours. The team comprised novices as well as more experienced WBA users. We felt that four participants was probably an optimal size for a group developing a WBG. The time spent implementing the graphs (drawn on a blackboard) with ciedit, our on-line WBG-drawing tool, included three people and some debugging time (we were working with a rough version of ciedit). We estimate the resources for drawing the graphs with ciedit at 2 person-hours and have verified this on another roughly equally-complex case.

5 Conclusions (NTSB Quotation)

1. The weather, the mechanical condition of the *Royal Majesty*, except for the global positioning system receiver, the officers' certifications, drugs, and fatigue were not factors in the accident.

2. Although Coast Guard personnel observed no indications that the officers had been under the influence of alcohol, alcohol could not be conclusively ruled out as a factor in the accident because of the delay in collecting the blood and urine specimens.

3. About 52 minutes after the *Royal Majesty* left St. George's, Bermuda, the global positioning system receiver antenna cable connection had separated enough that the global positioning system switched to dead-reckoning mode, and the autopilot, not programmed to detect the mode change and invalid status bits, no longer corrected for the effects of wind, current, or sea.

4. Openly routing the global positioning system antenna cable in an aread where someone occasionally walked increased the risk of damage to the cable and related connectors.

5. Had the fathometer alarm been set to 3 meters, as was the stated practice, or had the second officer chosen to display the fathometer data on the control console, he would have been alerted that the *Royal Majesty* was in far shallower water thatn expected and, thus, was off course. He would have been alerted perhaps as long as 40 minutes before the grounding, and the situation could have been corrected.

6. The watch officers' monitoring of the status of the vessel's global positioning system was deficient throughout the voyage from St. George's.

7. Deliberated cross checking between the global positioning system and the Loran-C to verify the *Royal Majesty*'s position was not being performed and should have been on the voyage from St. George's.

8. Even though it is likely that the watch officers were not aware of the limitation inherent in using the position-fix alarm to monitor the accuracy of GPS position data, it was inappropriate for them to rely solely on the alarm to warn them of any problems with the GPS data.

9. The sighting of lights not normally observed in the traffic lanes, the second officer's inability to confirm the presence of the BB buoy, and the sighting of blue and white water should have taken precedence over the automation display on the central console and compelled the second officer to promptly use all available means to verify his position.

10. The chief officer and the second officer did not observe good watchkeeping practices or act with heightened awareness of the precautions that are needed when a vessel approaches the Boston traffic lanes and landfall.

11. The master's methods for monitoring the progress of the voyage did not account for the technical capabilities and limitations of the automated equipment.

12. The watch officers on the *Royal Majesty* may have believed that because the global positioning system had demonstrated sufficient reliability over 3 1/2 years, the traditional practice of using at least two independent sources of position information was not necessary.

13. All the watchstanding officers were overly reliant on the automated position display of the navigation and command system 25 and were, for all intents and purposes, sailing the map display instead of using navigation aids or lookout information.

14. Because the industry standard 0183 data protocol did not provide a documented or standardized means of communicating or recognizing that a dead-reckoning positioning mode was in use by a hybrid, dead-reckoning capable position receiver, Raytheon and

STN Atlas adopted different design philosophies about the communication of position-receiver mode changes for the Raytheon 920 global positioning system and the navigation and command system 25.

15. STN Atlas should have, in order to help ensure safety and compatibility with different National Marine Electronics Association (NMEA) 0183 position receivers, programmed the *Royal Majesty*'s navigation and command system 25 to recognize the *valid/invalid* status bits in the NMEA 0183 data, including those specified in the NMEA 0183 v1.5 *RMC* recommended minimum global positioning system data sentence.

16. Had the navigation and command system 25 autopilot been configured to compare position data from multiple independent position receivers and had a corresponding alarm been installed that activated when discrepancies were detected, the grounding of the *Royal Majesty* may have been avoided.

17. Because watch officers must verify proper equipment operation frequently, alternative sources of critical equipment status should have been displayed directly on the console or on repeaters located where they could be seen from the central console.

18. The brief aural alarm of the Raytheon 920 global positioning system receiver, the remoteness of the receiver's location, and the failure of the installer to connect the global positioning system external alarm resulted in the inadequacy of the aural warning sent to the crew when the global positioning system defaulted to the dead-reckoning mode.

19. Failure modes and effects analyses of the *Royal Majesty*'s integrated bridge system would probably have disclosed the shortcomings of the system's components.

20. The on-the-job training program employed by Majesty Cruise Line to train the *Royal Majesty*'s watch officers in the operation of the integrated bridge system did not adequately prepare these officers to identify and respond to system malfunctions.

21. The *Royal Majesty*'s integrated bridge system did not adequately incorporate human-factors engineering.

22. There is a need to have performance standards for integrated bridge systems, and to required that the systems be inspected and certified.

6 Comments on NTSB Conclusions

1. The weather *was* in part a factor. See LoF 6.2: *The rays of the setting sun caused glare on the ocean surface in the direction of the buoy (BA).* Otherwise, this conclusion is a conjunction of observations derivable from the WBG using a checklist (weather, equipment status, human operator status, human operator common natural/induced physiological factors).

2. This cannot be concluded from the graph. The effects of alcohol as induced physiological factor cannot generally be identified from use of the counterfactual test. Human operator natural/induced physiological factors do not in general enter in via use of the Counterfactual Test. They enter in through direct testing or inference (testing for drugs, determination of the statistically known precursors or other indications of fatigue) and

their possible effects, as known from medical research, are hypothesised. This form of causal influence derives more from Pearl's methods (confirming causal models through experiments and statistics using generally Bayesian methods) than from the Counterfactual Test.

3. This conclusion appears to be a conjunction of different causal subgraphs (specifically involved LoF 17.0, 17.1.4, 17.3, 21.1, and the hypothesised cause of 21.1)

4. This conclusion joins LoF 17.2 with a statement of likelihood. LoF 55 says that the cause of separation is unknown. It substantiates directly Recommendation M-97-4.

5. This is a statement of causality using the Counterfactual Test, corresponding to the connection LoF 56 →LoF 19 in the WBG. The rest of the statement gives a time constraint. Notice that the assertion that the fathometer alarm was not displayed on the central console is not in the body of the report, and hence not in the LoF above.

6. This is a statement of causality corresponding to LoF 61 → 58.2 as well as LoF 7.3 → 58.2, and LoF 57.1 →57 → 58.2 in the WBG. But it also includes a deontic judgement of deficiency. Note also that LoF 57.1 has no specific causal factor, but it connects with Conclusion 7 below.

7. This is a statement of causality corresponding to LoF 7.3 →LoF 58.2 in the WBG. It contradicts some statements of the second officer (as expressed in LoF 7.3). The statement may also invoke a causal factor for LoF 57.1. The chief officer decided that they were on course; he could not have decided that, had he been cross-checking GPS against Loran-C. Ergo he did not perform the cross-check. The NTSB (Rob Molloy, personal communication) confirmed that they could not reconcile any assertion that GPS-Loran cross-checking was being performed with the continuing decisions that the vessel was on course (LoF 57) given the actual course of the vessel and the known behavior of the equipment. Neither could we. The statement also includes a deontic judgement.

8. This appears to be a statement concerning LoF 61 and its related causal factors LoF 59 and 18. LoF 59 is an assumption: the crew did not hear the alarm. It is assumed that the alarm must have sounded. The statement includes a deontic judgement about procedures.

9. This is an iteration of standard procedures, along with the observation that they had low priority in the crew's "input data", and the deontic judgement that they should have had high priority. It related to LoF 58.1, 7.5, 6.3 and 62.

10. This is a statement corresponding roughly to LoF 58.1, along with a deontic judgement.

11. This follows from the observation that the master relied on verbal reports only, along with a technical assessment of the equipment.

12. This conclusion is an assumption, introduced perhaps to account for the violation of standard procedure.

13. This appears to be a restatement of Conclusion 9, or to be closely related to it.

14. This conclusion is an assertion of partial causality, consisting of precursors of the unnumbered node *NACOS failed to recognize GPS invalid data signal*, along with its causal factors LoF 21.4, 21.2, and the unnumbered design causes of those. It also includes the node LoF 21.3. Notice that it is incomplete - the fact that the NMEA specification was incomplete also played a causal role, but is not included here. Conclusion 14 ubstantiates recommendations M-97-14, M-97-16, M-97-19 and M-97-20.

15. This is LoF 21.4, along with a deontic judgement that things should have been otherwise.

16. This is a proposal for better design. It grounds Recommendation M-97-12.

17. This is a proposal for better human-factor design: better location of indicators, better annunciation. It is a reiteration of a standard problem in HF design, that critical annunciators are not collocated with the operator in a position in which heshe can be expected to perceive them.

18. This asserts that the design of the warning signal was a general causal factor for LoF 61.

19. This an assertion along with a counterfactual which can be considered a causal statement. That FMEA was not performed on the IBS was a general causal factor in its behaving the way it did. In other words, a summary of LoF 21.

20. This appears to be an inference from the facts that a training program was used, and the trained behavior failed. It can be regarded as a formal inference.

21. This appears to be an inference from, *inter alia*, Conclusion 17.

22. This appears to be an inference from Conclusions 17, 18, 19, 21.

Acknowledgements

The conclusions were commented by a team including the authors and Lars Heidieker.

7 Classification of NTSB Conclusions

We classify the kinds of statements in the Conclusions as follows. Nodes may appear in more than one category - indeed, about half of them do. Of these classification items, only *design recommendation* and *deontic assertion* are not in some form or another derivable from the WBG. There are quite a few deontic assertions.

Conjunction of nodes in WBG: 1, 6, 10, 15, 20, 22

Causality assertion, consisting of a fragment of the WBG: 3, 5, 6, 7, 14, 16, 17, 18, 19, 21, 22

Inference from LoF or WBG: 6, 11, 7

Procedures either faulty or faultily executed: 9

Assumption: 12

Design recommendation: 14, 4

Deontic assertion: 5, 6, 7, 8, 15, 17, 20, 22

Epistemic assertion: 2, 4

8 Analysis of NTSB Deontic Conclusions

The general requirements for an NTSB report are to identify and formulate recommendations for procedures, regulation, and so forth which the NTSB believes would alleviate in the future certain safety deficiencies which it has identified during the course of the causal investigation of the accident. Since this includes considerations of design principles and operator behavior, the process of formulation of recommendations can have a strongly deontic flavor, as in some of the NTSB Conclusions.

Some of the conclusions of the NTSB can be reformulated:

6: The statement is equivalent to the following conjunction

$\wedge$ **Chief officer did not perceive that GPS was in DR mode**
$\wedge$ **Second officer did not perceive that GPS was in DR mode**
$\wedge$ **Chief officer should have perceived GPS in DR mode**
$\wedge$ **Second officer should have perceived GPS in DR mode**

Commentary: The first two conjuncts are LoF 61. The second conjuncts may follow from procedural precepts that say that the status of the GPS and other items of the IBS are required to be known at all times.

7: The statement is equivalent to the following conjunction

$\wedge$ **Chief officer did not monitor GPS-Loran status effectively**
$\wedge$ **Second officer did not monitor GPS-Loran status effectively**
$\wedge$ **Chief officer should have monitored this status effectively**
$\wedge$ **Second officer should have monitored this status effectively**

Commentary Here, the word "effectively" means: according to some norm. The first two assertions follow from comparing LoF 4.1, 4.2 with the charted course of the ship. The conclusion must be that the chief officer is mistaken in his assertions LoF 4.1, 4.2, unless the Loran-C has an undetermined sporadic failure mode, since it is not possible to reconcile a 1-mile discrepancy between Loran and dead-reckoning GPS with the position and heading of the ship (which did not suddenly track almost due west after 18:00). The second officer did not cross-check Loran with GPS (LoF 7.3). The last two conjuncts form a deontic statement: the statement that monitoring was deficient is to say that monitoring was thus-and-such and thus-and-such did not suffice. In form, the statement is similar to that of Conclusion 6.

8: The statement is equivalent to the following conjunction

$\wedge$ **Watch officers did not know of inherent limitations of relying on position-fix alarm**
$\wedge$ **It is inappropriate to rely on position-fix alarm**
$\wedge$ **Watch officers did rely on position-fix alarm**

Commentary: The first and third conjuncts are technically assumptions; they occur nowhere in the report body itself. The second conjunct is the deontic assertion; it relies on analysis of the technical situation including the human operator.

15: The statement is equivalent to the following conjunction

$\wedge$ **STN didn't program the NACOS 25 to use *valid/invalid* bits**
$\wedge$ **NACOS 25 didn't use *valid/invalid* bits to determine invalid data**
$\wedge$ **STN should have programmed the NACOS 25 to use these bits**
$\wedge$ **Reasons why STN "should have"**
$\wedge$ **STN was the supplier of the NACOS 25**

Commentary: Observe that there are important items for the logic that are implicit in the report. For example, say, IBM didn't program the NACOS to recognise the bits either. But then, since IBM had nothing to do with the development of this piece of equipment, it does not follow that they should have so programmed it. However, it does follow that STN, as the equipment provider, should have so programmed it. The inference may be obvious in this case, but in cases of "diffusion of responsibility", this may not be so clear. Other reasoning here does not derive directly from statements in the report. The second statement follows from

$\wedge$ **LoF 21.4: NACOS 25 used *nulled fields/no transmission* to determine invalid data**
$\wedge$ **This criterion is all that NACOS 25 used**
$\wedge$ **Using *nulled fields/no transmission* alone implies that *valid/invalid* bits were not used**
$\Rightarrow$ **NACOS 25 didn't use *valid/invalid* bits to determine invalid data**

Commentary to this part: The second conjunct of the antecedent is implicit, but obvious, as is the third. We may suppose that the logic is technical, but the inference is obvious.

17: The structure of this assertion appears to be as follows

$\wedge$ **Watch officers must check proper functioning of equipment frequently**
$\wedge$ **Critical equipment status should be displayed on central console**
$\wedge$ **The second conjunct is true because the first is true**

Commentary: It is not clear what status the "because" has in the third conjunct. If critical equipment status were to be displayed on the central console, it would indeed make checking of its functioning somewhat easier. This seems to be a general principle of human-factors-oriented design. One may imagine that there is a principle that principles of human-factors-oriented design should be followed. A reconstruction of the argument yields the following possibility.

Displaying data on central console
$\Rightarrow$
$\wedge$ **Status of GPS is apparent to watch officer**
$\wedge$ **GPS-Loran discrepancies are apparent to watch officer**
$\wedge$ **Position display is not cognitively dominant**

Commentary: From this inference it appears to follow that the Conclusions 6, 7,13 would not have pertained had the relevant data been displayed on the central console. This is an assumption, but a reasonable one, and it is a counterfactual, and thus it follows that the fact that the data were not displayed on the central console was a single causal factor of three untoward conditions. The argument appears to be that displaying the data on the central console is a single prophylaxis that copes with three phenomena at once. The phenomena, though, are selected, and one can multiply entities through careful selection.

20: We define the following terms:

OTJT-IBS	**On-the-job training in IBS operation**
MIBS	**Malfunction of the IBS**
X	**Identification and reaction of operators to MIBS**

Commentary: Conclusion 20 says that OTJT-IBS is insufficient for X. However, the components of Conclusion 20 appear nowhere in the WBG. It appears to be related to an inference of the following kind:

$\wedge$	**Problems should be recognised and dealt with**
$\wedge$	**This function is accomplished by training**
$\wedge$	**Problems were not recognised and dealt with**
$\Rightarrow$	**Training was insufficient to accomplish the function**

Commentary: The first conjunct is deontic. The consequent follows from the second and third conjuncts. So the argument appears to have two parts: a deontic part, and a standard procedural - self-fulfilling - part, that if trained personnel were able to perform according to training, and demonstrably did not perform satisfactorily, it is taken to entail that the training was inadequate.

9 Probable Cause According to the NTSB (Quotation)

> The National Transportation Safety Board determines that the probable cause of the grounding of the *Royal Majesty* was the watch officers' overreliance on the automated features of the integrated bridge system and in the implications of this automation for bridge resource management, the deficiencies in the design and implementation of the integrated bridge system and in the procedures for its operation, and the second officer's failure to take corrective action after several cues indicated the vessel was off course.
>
> Contributing factors were the inadequacy of international training standards for watchstanders aboard vessels equipped with electronic navigation systems and integrated bridge systems and the inadequacy of international standards for the design, installation, and testing of integrated bridge systems aboard vessels.

10 Analysis of the Statement of Probable Cause

1. The first factor, *overreliance on the automated features of the integrated bridge system*, includes information in the following nodes:

1.1 LoF 53: Ship under control of NACOS 25

1.2 LoF 21: IBS error-correction failed

2. In addition to nodes LoF 21 and 53, there is a claim that the crew were responsible for part of this state of affairs. The crew cannot have been responsible for LoF 21; it is clear that they were responsible for LoF 53 under standard interpretations of "responsibility", for the decision and action to use the NACOS 25 was theirs: LoF 53.1 *The Navigator set the NACOS 25 to NAV mode shortly after departure*

3. However, LoF 53 is a node constructed by us. It neither appears in the body of the report nor in the conclusions. So the statement of probable cause includes an assertion that appears nowhere else in the report. One could consider here introducing a formal principle that items may only appear in the Probable Cause statement if they previously appear in the report body or in the conclusions. For a derivation of probable cause must identify some set of facts which are taken to be causative, and it is reasonable to require this to be a selection from amongst those facts previously listed.

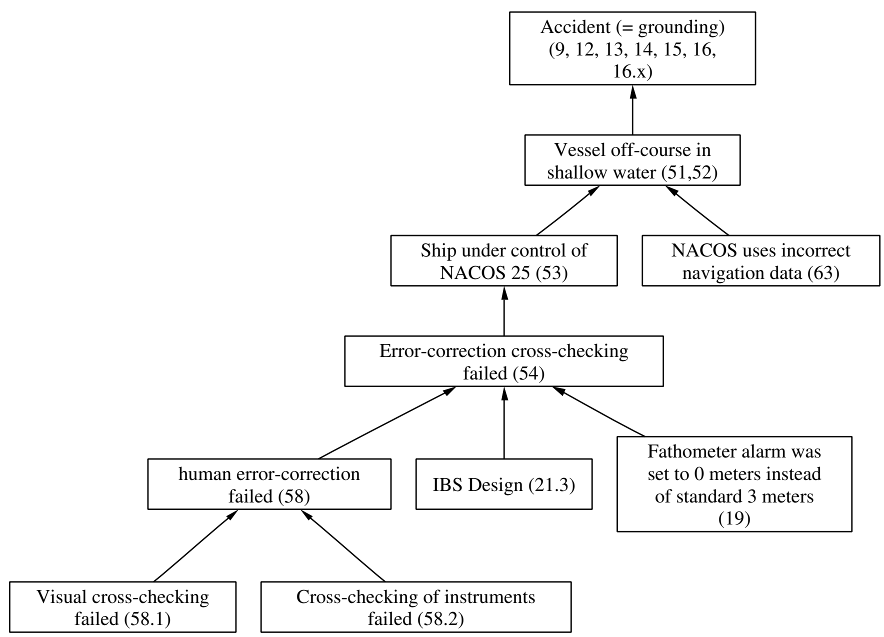
4. There are three types of constructed items in the WBG and NTSB report:

   4.1 Constructed through inference from other items (*ConsInf*)

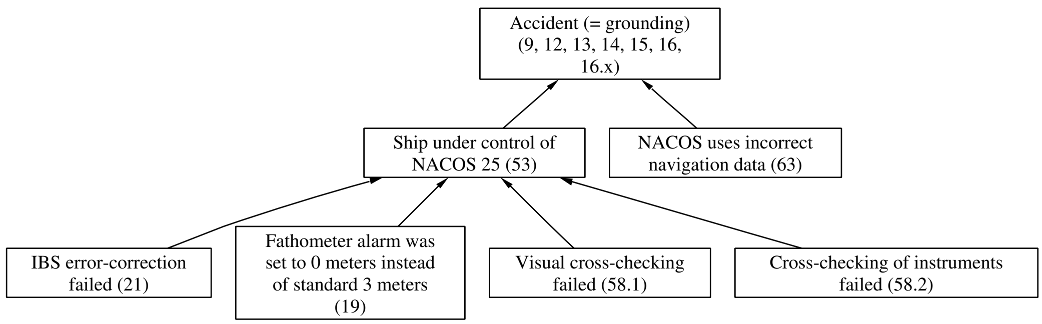
   4.2 Structural construction, as in a classification (*ConsStruct*). We used such a classification in dividing LoF 58 *Human error-correction failed* into LoF 58.1 *Visual cross-checking failed* and LoF 58.2 *Cross-checking of instruments failed.*

   4.3 Epistemic construction, as in Conclusion 2 (*ConsEp*)

5. It is possible to obtain a reduction of the WBG which corresponds as far as possible to the NTSB statement of Probable Cause. This reduction is obtained by eliminating intermediate nodes and reducing paths passing through those intermediate nodes to direct edges between the remaining nodes to retain causal continuity. Lewis has suggested that causality is the transitive closure of the causal-factor relation; this operation corresponds to indicating causal factors or causality. Note that the nodes retained do not construe a *sufficient* set of causes, since that would require retaining a partition of the nodes below a given node. Neither Node LoF 63 *NACOS uses incorrect navigation data*, nor any partition below this node, is included in the causes of node LoF (9,12,....). Similarly, Nodes LoF 58 and LoF 19 are explicitly present, as is *part* of a partition below Node LoF 21 (provided that Node *IBS Design* is taken to include the three design-aspect nodes together, as well as the Node 21.8 *Same gyro and speed input for DR*. It may also be argued that Node LoF 63 could be included under *deficiencies in the design and implementation of the [IBS] and in the procedures for its operation*). However, that is not a partition of Node LoF 21, since nothing covers *NMEA 0183 specification incomplete.* It follows that a complete statement of causes has not been given in the NTSB statement of Probable Cause.



6. An abstraction of the WBG which includes a partition of the nodes, and which includes as far as possible the NTSB causes and contributing factors and minimal other material is given below. It requires some interpretation. Edges here represent *causes,* namely paths in the WBG between the indicated nodes. We regard Node LoF 53 *Ship under control of NACOS 25* as part of the "*overreliance*" causal assertion, and the Nodes LoF 63 *NACOS uses incorrect navigation data* and LoF 21 *IBS error-correction failed* as part of the "*deficiencies in ... [IBS]*" assertion, even though they occur in two different places in the causal display. Node LoF 58.2 *Cross-checking of instruments failed* we regard as part of the "*training in ... implications of this automation for bridge resource management", and Node LoF 5*8.1 *Visual cross-checking failed* we regard as encompassing "*second officer's failure to take corrective action after ... cues".* Although this interpretation is liberal, it does provide a partition of the WBG. However, it includes Node LoF 19 *Fathometer alarm was set to 0 meters instead of standard 3 meters*, which cannot be subsumed, even liberally, under any of the categories of the NTSB's statement of Probable Cause. We conclude that the NTSB statement of Probable Cause is incomplete, even under a liberal interpretation.

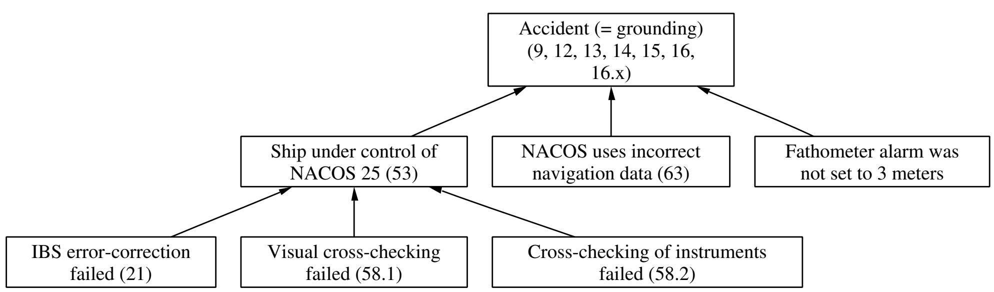


7. It is unclear to us, though, whether the fathometer and its alarm is regarded as part of the IBS. It is a separate entity from the other components, hardly "integrated" with them. The NTSB report describes the IBS on pp13-19, and deals exclusively with the STN Atlas NACOS 25, the Raytheon RAYSTAR 920 GPS unit, and the Raytheon RAYNAV 780 Loran-C unit. If the fathometer is indeed regarded as part of the IBS, then its inadequate setting could be regarded with some stretch of the imagination under *"overreliance..."* as well as "*[inadequate training] in... the implications of the automation for bridge resource management"*. Our inclination is not to take it as part of the IBS, since it is not apparently integrated with the other components, and indeed not setting the alarm to 3 meters when under way appears to us to be a failure to follow basic procedures, only peripherally connected with the focus on the IBS explicated in the statement of Probable Cause.

8. The WBG abstraction, then, while technically an explanation of cause (since it includes a partition of the WBG) contains a cause not contained in the NTSB statement of Probable Cause. That statement also includes further items not mentioned in the body of the report, but in the conclusions, namely the training program of Majesty Cruise Lines, and the lack of adequate performance standards for IBSs. However, the inadequacy of international watchkeeping standards for IBS-equipped vessels appears in the statement of Probable Cause for the first time.

9. The Node LoF 19 *Fathometer alarm .. set to 0 meters instead of .. 3 meters* appears where situated above because of a classification we introduced into the WBA, a *ConsStruct*. NTSB Conclusion 5 states counterfactually that the grounding would have

been avoided had the alarm been set to standard 3m. If so, this would suggest that the negative formulation *Fathometer alarm not set to 3m* is a causal factor of the grounding, by the WBA principle that an absent factor (something was *not* the case) is reifiable if it states a violation of procedure, and by the Counterfactual Test applies to this reified absent factor. The resultant WBG with this negative factor is shown below. This brings out the curious feature that a negative factor (created by the absence of procedure-following) and its positive formulation (what in fact happened, instead of what the procedure dictates) may have causal influence in quite different places. Although it is not guaranteed that the Counterfactual Test applied to causes (a node at the end of a chain of causal-factor relations) will succeed (the notion of causal factor is notoriously not transitive), it may well be that it might in certain cases. This suggests that a statement of causality as in the WBG-abstraction above may be suitably reformulated by considering whether subsidiary nodes are indeed direct causal factors of the accident. This suggests that essentially the same analysis may be presented in more than one way.



10. The question remains whether the partition above represents the neatest statement of probable cause of the accident. Intuitively, it seems to us that the reason the ship ran aground was that it was under control of the NACOS 25 (LoF 53), which was using incorrect navigation data (LoF 63) because the GPS antenna cable separated and neither standards nor design enforced uniform IBS notification methods for incorrect data. In addition to this, there was a massive failure of traditional seamanship (watchkeeping, setting the fathometer alarm), as well as of cross-checking the IBS equipment. The abstraction above does not mention the GPS cable separation, but (again under the negative formulation) the Counterfactual Test shows its importance: *had the cable not*

separated, the IBS would have obtained correct nav data and been on course and would not have run aground. The separation of the cable was a necessary causal factor in the grounding.

References

[NTSB97] National Transportation Safety Board, Marine Accident Report, Grounding of the Panamanian Passenger Ship *Royal Majesty* on Rose and Crown Shoal near Nantucket, Massachusetts, June 10, 1995. Report Number NTSB/MAR-97/01 available from *http://www.ntsb.gov*

[Lad01] Peter B. Ladkin, Causal Systems Analysis, manuscript available from author, to be published, Springer-Verlag, London, 2003.

[LadLoe98] Peter B. Ladkin and Karsten Loer, Why-Because Analysis: Formal Reasoning about Incidents, RVS-Bk-98-01, available from http://www.rvs.uni-bielefeld.de →Publications →Books.