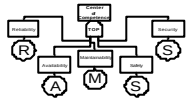
Towards a Hybrid Approach for Incident Root Cause Analysis

Jens Braband, Bernhard Evers, Ernesto de Stefano

Siemens Transportation Systems – Rail Automation
System Development Integrity

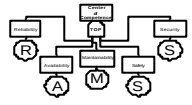
jens.braband@ts.siemens.de

Overview



- Introduction
- Necessary Aspects in Incident Analysis
- Case Study: Herald of Free Enterprise (HFE)
  - Story of the Accident in a Nutshell
  - Time-Actor Diagram
  - Why-Because Graph
  - STAMP Diagram
- Comparison and Relationships
- Conclusion and Way Forward

Introduction

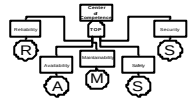


- Increased interest in causal analysis methods
  - IRIA2002
  - Bieleschweig workshops, 2002&2003
- Several new approaches available
  - Why-because analysis (WBA, Ladkin, University of Bielefeld)
  - Systems-Theoretic Accident Modeling and Processes (STAMP, Leveson, MIT, Boston)
  - Safety by Organizational Learning (SOL, Wilpert/Fahlbruch, TU Berlin)
  - Events and Causal Factors diagram (ECF, Johnson, U of Glasgow)
  - Etc.
- No standardised or commonly agreed way to analyse causes and present results of such an analysis
- Different investigators or different sectors have very different procedures and put emphasis on different issues.

Necessary Aspects in Incident Analysis

- Organisational factors play a major role in many incidents, but are they sufficient?
- What kinds of aspects are important in a root cause analysis?
- Experience gained from several case studies shows the importance of:
  - Time and sequence aspects of events
  - Causal relationships
  - Organisational factors
- There may be more aspects, but these are deemed necessary.

Case Study: HFE



- A formal report is available (Sheen, 1987), which is the only source used.
- It is a real case and the results from the various analyses fit almost entirely into a single paper. In many other cases, even the results of a single analysis will not fit into one paper.
- The authors were not familiar with the case before and the case does not come from their usual application domain. This could make it easier to concentrate on methodology issues and not get bogged down in the technical details of the case.
- Each coauthor was responsible for one particular analysis. Only the results underwent a peer review to ensure correctness.

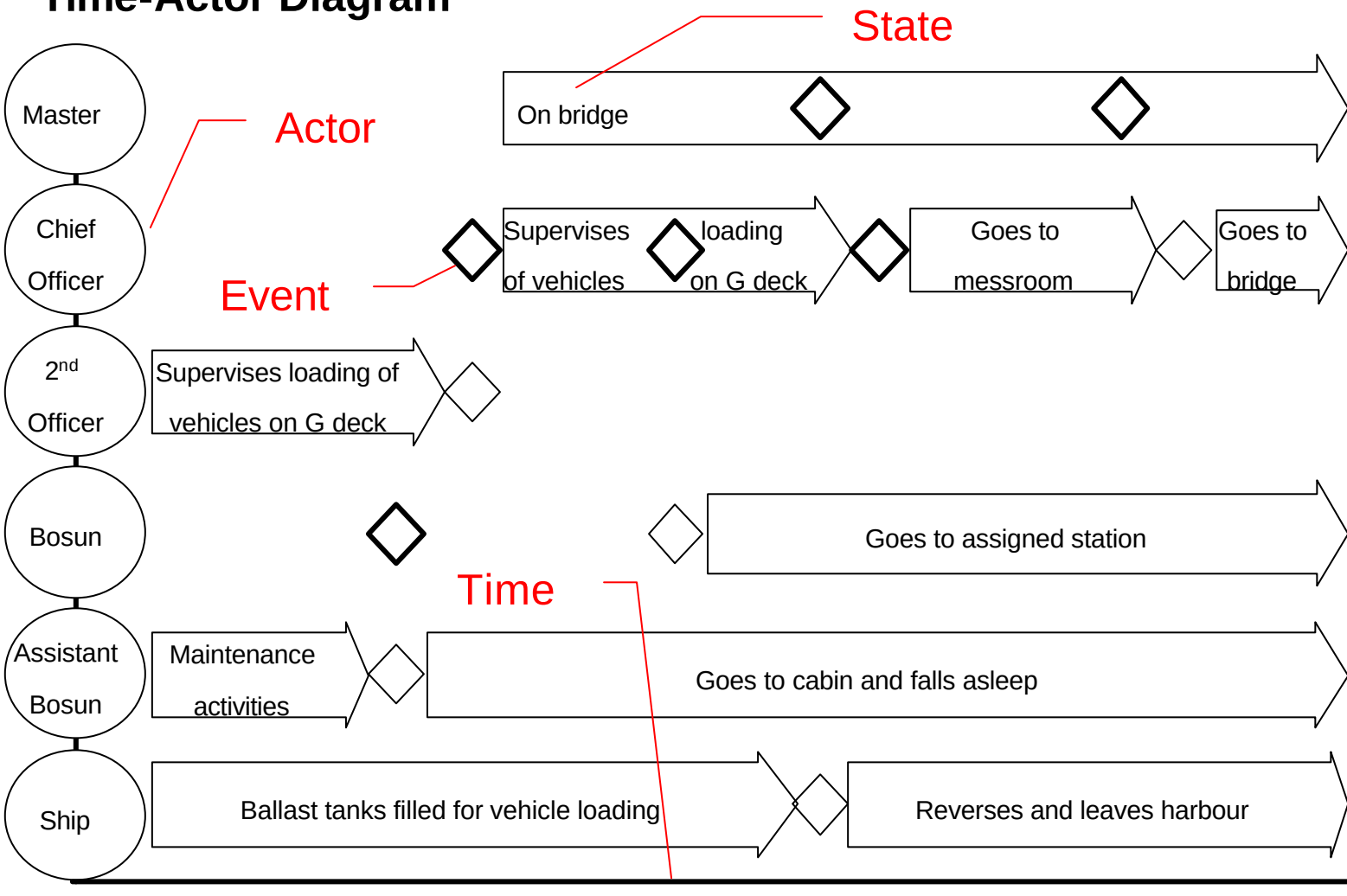
Story of the Accident in a Nutshell

- The HFE left Zebrugge harbour with her bow doors open.
- She passed the outer mole and increased speed.
- Water flooded onto the lower car deck.
- The ship became destabilised and capsized.
- Of the 459 on board, 189 died.

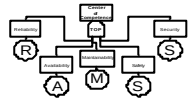
Some facts the investigation brought to light:

- The Assistant Bosun, whose immediate responsibility it was to close the bow doors upon departure, was asleep in his cabin.
- The Chief Officer, responsible for ensuring door closure, thought he saw the Assistant Bosun going to close the doors.
- The Captain always assumed that the doors were safely closed unless told otherwise.

Time-Actor Diagram

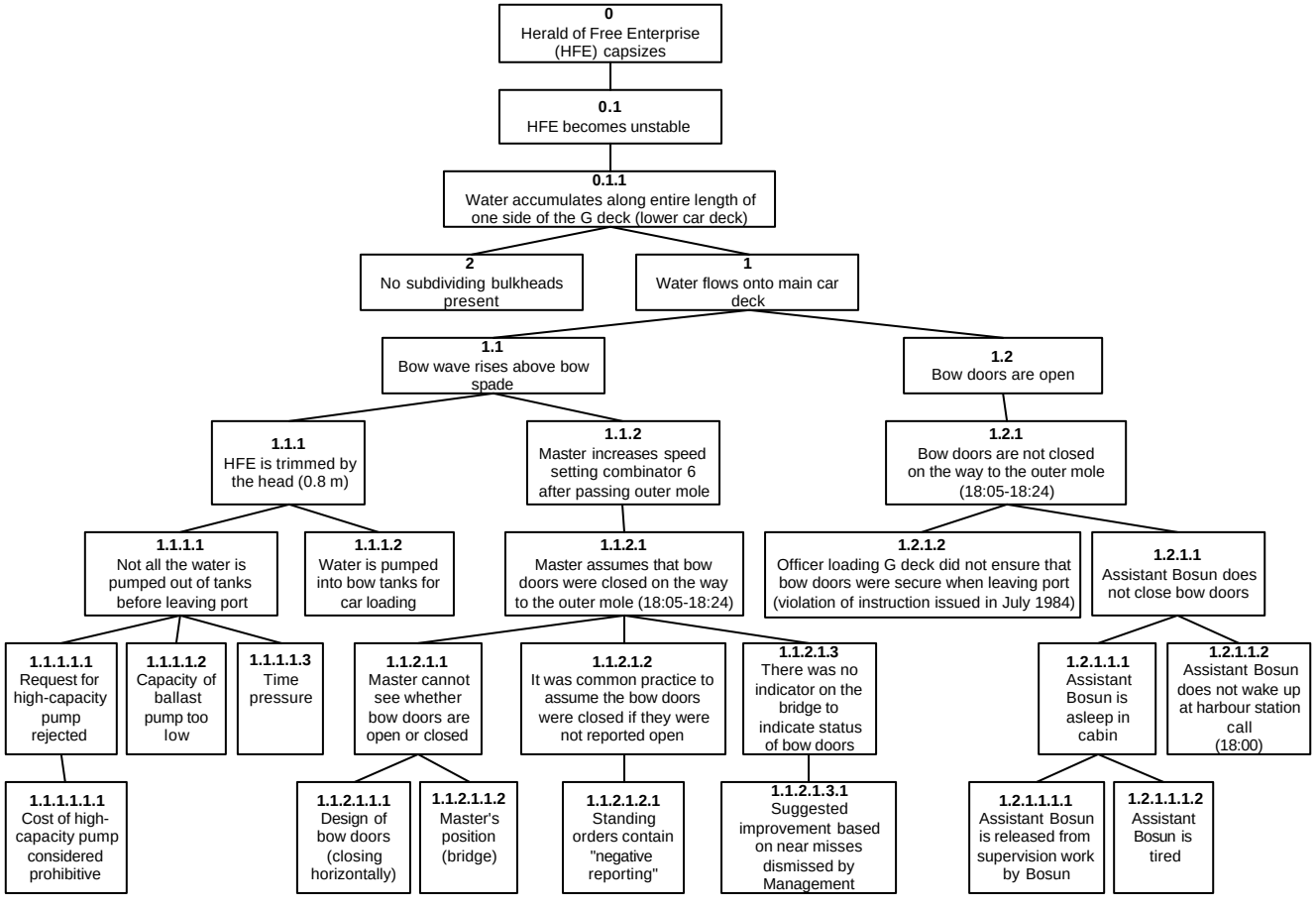


Why-Because Analysis

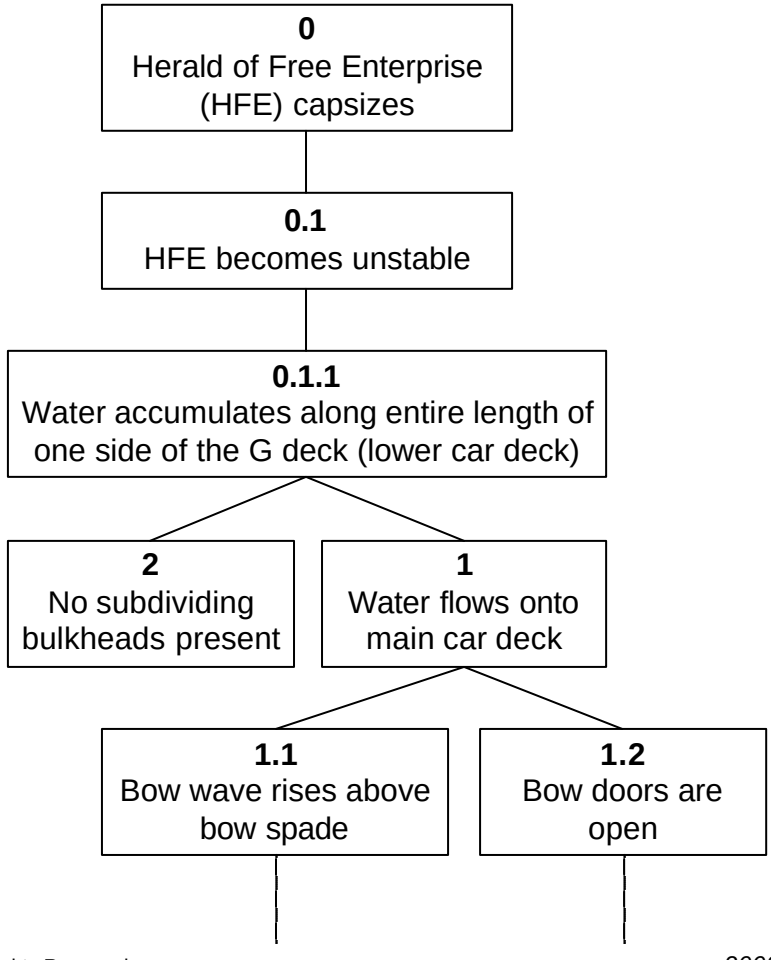


- Define an event as the starting point.
  In our case, we started with the capsizal of the Herald of Free Enterprise.
- Ask what the immediate causal factors were and repeat this step for each factor identified.
- Check if each causal factor is individually necessary for the event it is connected to.
  Based on Lewis's formal definition of causality, B is a necessary causal factor of A if: had B not happened, A would not have either.
- Check whether the causal factors connected to a particular event are jointly sufficient for it.

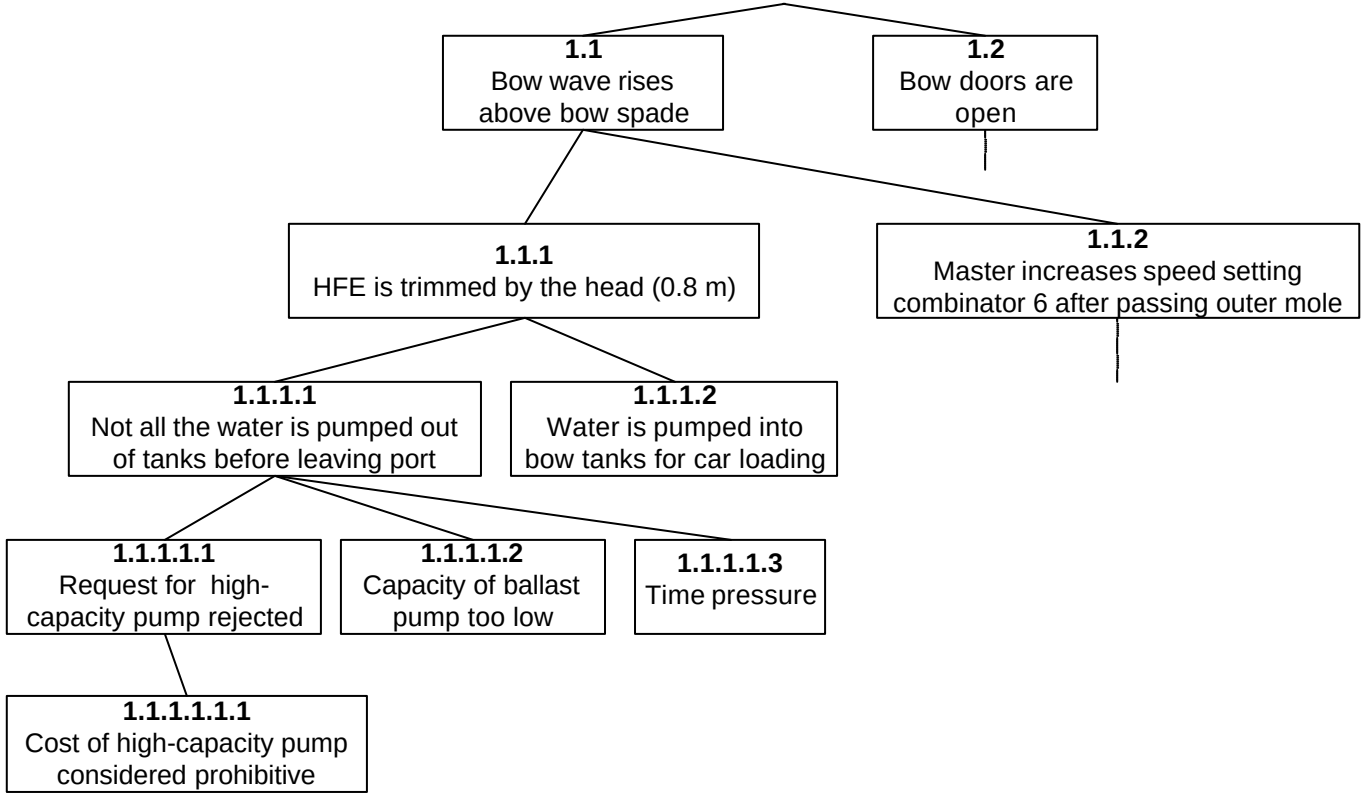
Why-Because Graph: Herald of Free Enterprise, 1987-03-06



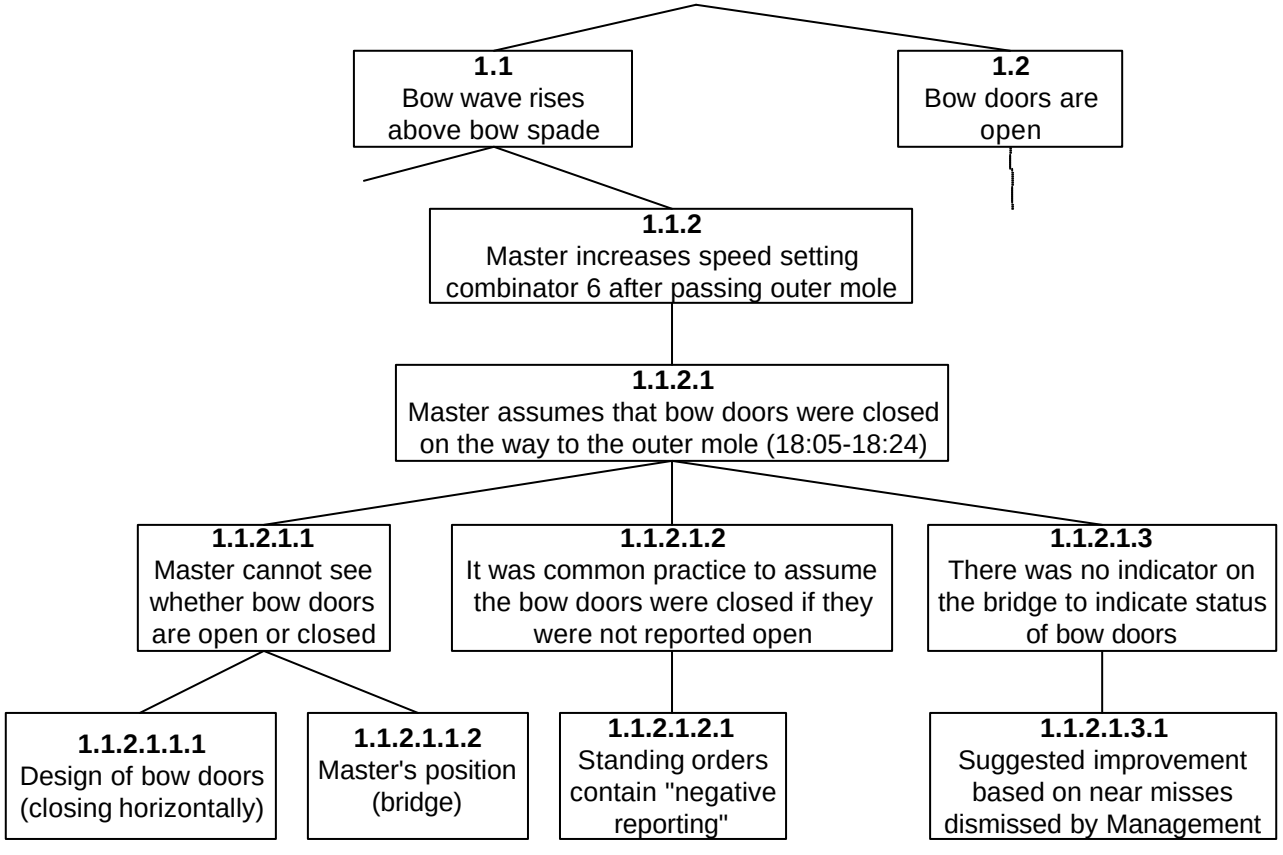
Why-Because Graph: Herald of Free Enterprise, 1987-03-06



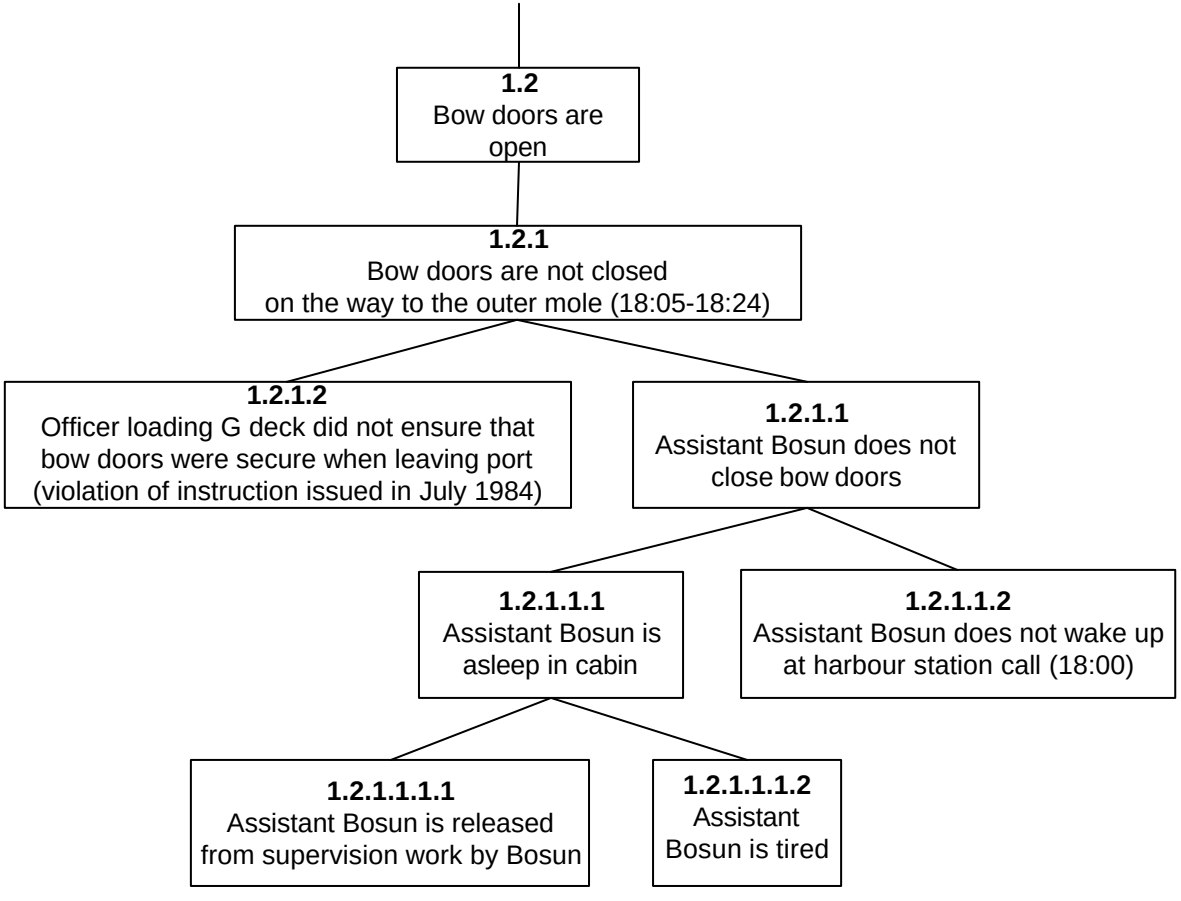
Why-Because Graph: Herald of Free Enterprise, 1987-03-06



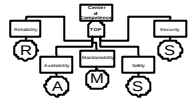
Why-Because Graph: Herald of Free Enterprise, 1987-03-06



Why-Because Graph: Herald of Free Enterprise, 1987-03-06

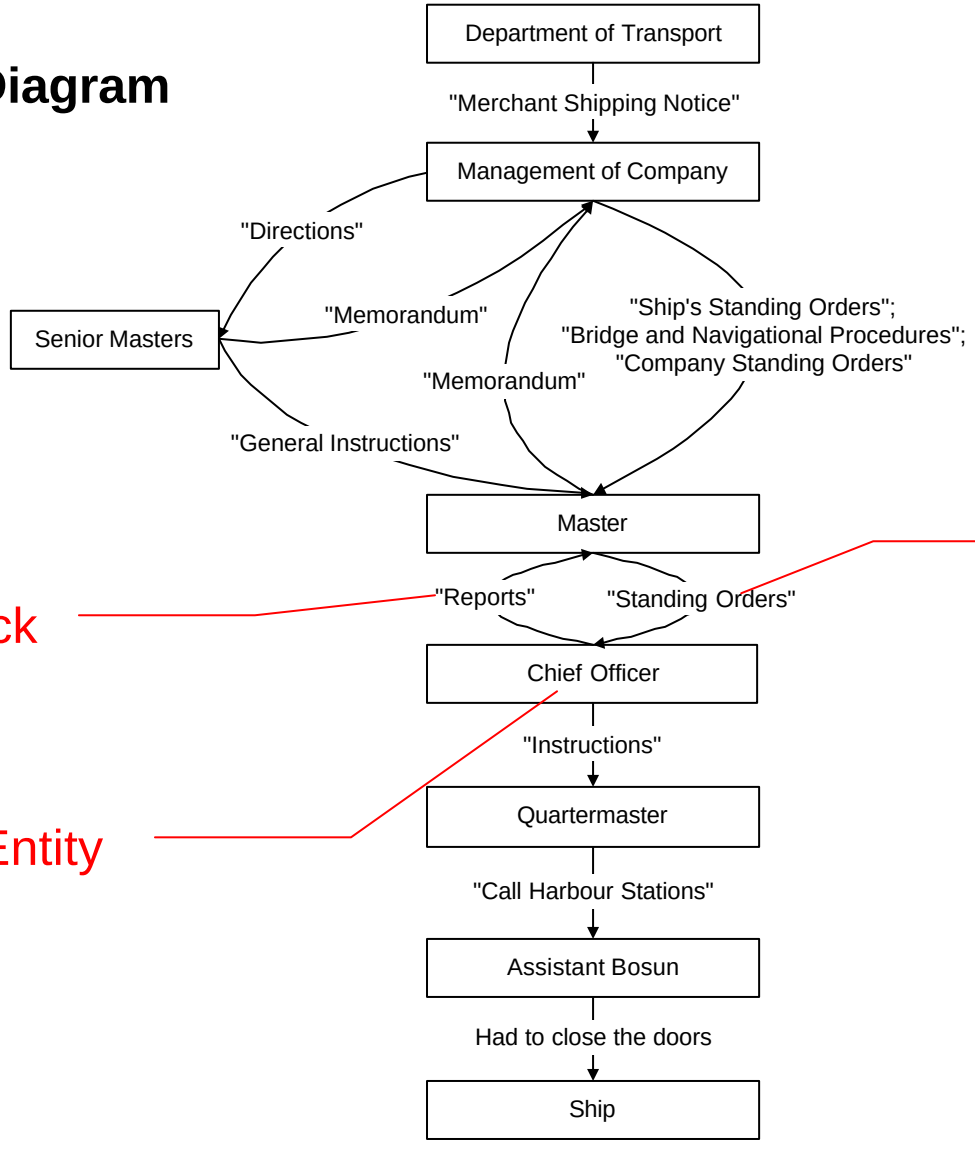


STAMP



- The basic concept is not an event, but a constraint.
- Systems are viewed as socio-technical control structures, with each level imposing constraints on the activities of the level beneath it.
- Accidents result from inadequate control of safety-related behaviour.
- STAMP provides a classification of control flaws leading to hazards:
  - Inadequate control actions
  - Inadequate execution of control actions
  - Inadequate or missing feedback

STAMP Diagram

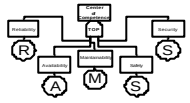


Feedback

Control action

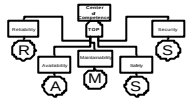
Entity

Comparison



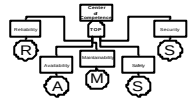
	Pros	Cons
TAD	■ Good overview of what happened	■ More abstract factors not represented
WBG	■ Clear structuring of the incident causes ■ Formal definition of causality	■ Strict definition of causality may be a hindrance when it comes to human or organisational factors

Comparison



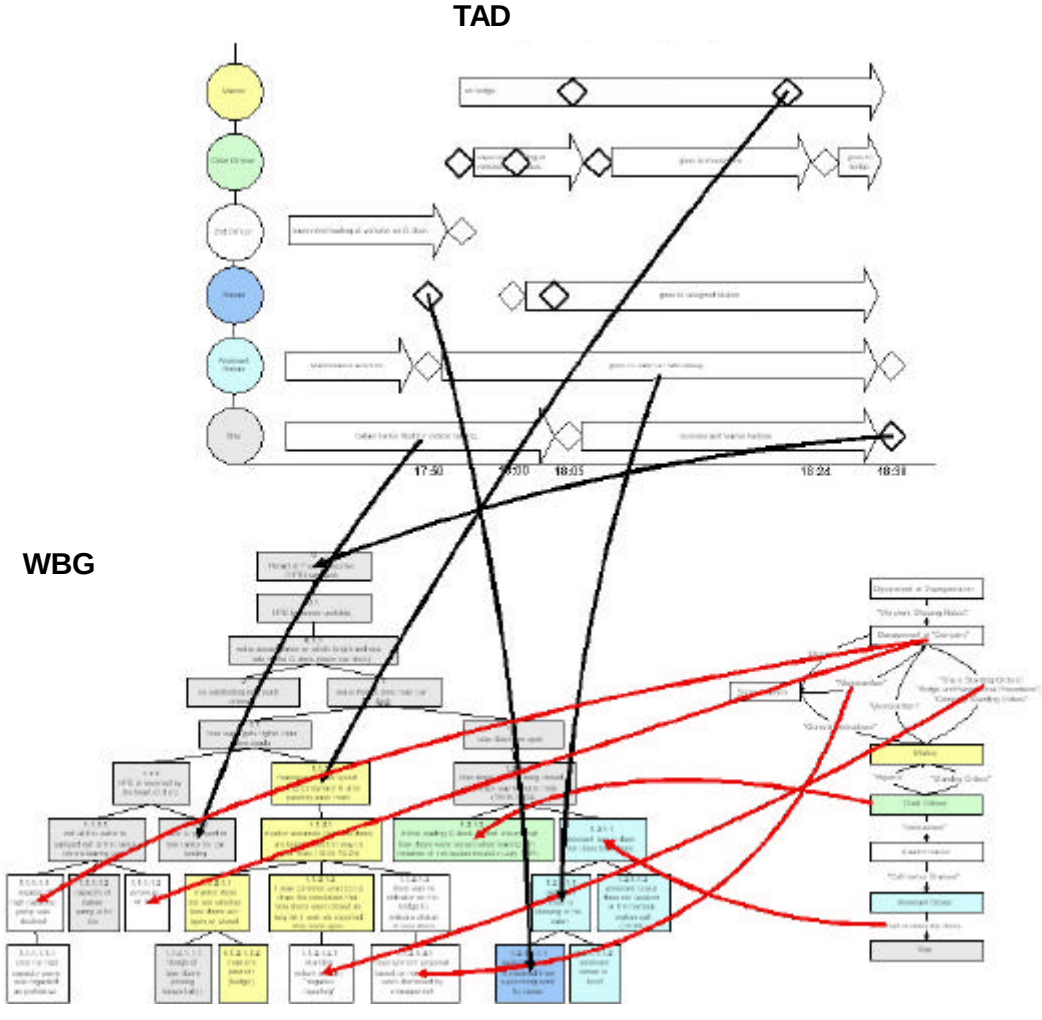
	Pros	Cons
STAMP	■ Systematic uncovering of organisational structures	■ A structured presentation of results was not available at the time of our analysis.
	■ Directs you to ask revealing questions	■ Retrospective application only useful if investigation report is excellent
	■ Can be used even before an incident or accident happens	■ Enormous effort required for analysis

Relationships

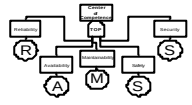


- The actors in the TAD are only a subset of the entities in the STAMP diagram.
- Events and states in the TAD do not appear in the WBG unless they are causal factors.
- Many of the causal factors in the WBG do not appear in the TAD.
- Not all causal factors in the WBG have a corresponding control flaw in the STAMP diagram and vice versa.

Relationships

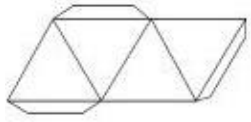


Conclusion



- No single analysis technique proposed so far covers all necessary aspects.
- A hybrid approach should be adopted which combines the best features of various techniques:
  - TAD diagram or similar representation of time and sequence properties
  - WBG, to acquire a clear overview of the causal factor landscape
  - STAMP or SOL, for the identification of contributory organisational or human factors
  - Extension of WBG, to include these factors even if they do not pass the strict causal factor test

Way Forward



- The "Bieleschweig workshops" will evaluate the methods for benchmark examples using a harmonised catalogue of criteria.
- The hybrid approach has to be scaled according to incident complexity.
- The cost of applying all methods as part of an industrial root cause analysis programme is prohibitive and justified only in exceptional cases.
- SOL and other techniques should be evaluated and adapted.
- A hybrid approach should be applied to real railway incidents.