University of Bielefeld
Faculty of Technology

RVS
Rechnernetze und
Verteilte Systeme

CAUSALIS

Negotiating Accidents

Analysis and Blame

Prof. Peter B. Ladkin PhD
ladkin@causalis.com

Derailment at Brühl, 06.02.2000

Derailment at Brühl

- Train driver (Triebfahrzeugführer) went through a set of points at the passenger station at about 122 kph
- The points, posted for 40 kph, diverted the train temporarily onto an adjacent track, on which there was an exit signal (required by regulations)
- This after a sequence of line works and speed modifications, partly described in the route plan, partly by temporary and permanent trackside signalling.

- Driver prosecuted. He could not say much, it seems
- His evidence is **crucial** to understanding the accident
- Information on the accident is thus incomplete

Brühl Accident: Analysis

- Accident partially analysed by IfEV, T.U. Braunschweig (Gayen, Lemke) using WBA
  - *www.rvs.uni-bielefeld.de → Bieleschweig → First*
- Reanalysed using STAMP for comparison (Brinkmann)
  - *www.rvs.uni-bielefeld.de → Bieleschweig → Second*
- Lessons to be learned depend heavily on sequence of information available to driver
- Especially visibility and sequence of trackside signalling
  - **the operator's view:** Michael Mandelartz, Mandelartz Bahntechnik *www.online-club.de/~feba/br0.htm*

Singapore Airlines SQ006, Taipei, 31 Oct 2000

SQ 006 Events

- On take-off from Taipei for Los Angeles
- Approaching typhoon
  - heavy rain
  - quartering crosswind with gusts
  - reduced visibility
- Attempted takeoff from closed Rwy 05 Right rather than cleared Rwy 05L
- Hit construction equipment shortly after V1
- Returned to earth, burned, 82 died
- First (and only) fatal accident to Singapore Airlines

SQ 006 Analysis – Official Report

- Final Report Findings: Factors
  - Weather
  - Closed rwy with construction equipment
  - CRW did not review their taxi procedures and location sufficiently
  - CAP focused on green centerline lights (white edge-marker lights may have been on or off)
  - Moderate time pressure led to narrow focus and loss of situational awareness
  - Loss of situational awareness

SQ 006 Analysis - Dissent

- Singapore Ministry of Transport
  - Systems, procedures and facilities at the airport „*seriously inadequate*“
  - The accident could have been avoided if „*internationally-accepted precautionary measures had been in place*“ at the airport

- Aviation Safety Network (a service of the Flight Safety Foundation)
  - *aviation-safety.net/database/record.php?id=20001031-0*

SQ 006 Associated Events

- CRW taken into custody
- Released after international outcry
- Allowed to return to Singapore on condition that they held themselves ready to return for trial to Taiwan

SQ 006 Expert Analysis

- Sidney Dekker, Tuesday Luncheon talk, International System Safety Conference, Ottawa, August 2003
  - Sequence of still photographs, showing what the crew would have seen
- Overwhelmingly persuasive that one would have performed similarly to the SQ 006 crew
- Ladkin, *Proper Understanding of the Human Factor*, Risks Digest 23.08, 22 Dec 2003:
  - *catless.ncl.ac.uk/Risks/23.08.html*

Operator's Cognitive State

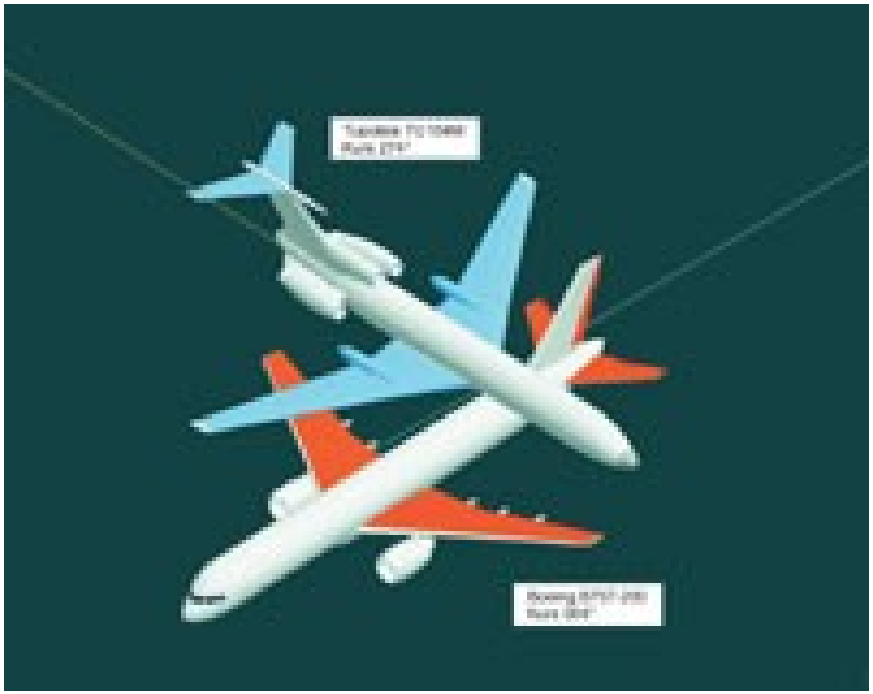
- Sidney Dekker, *Field Guide to Understanding Human Error* (Ashgate, 2002, New Edition 2006)
  - „*the old view of human error is that it is the cause of accidents whereas the new view is that it is a symptom of trouble deeper inside the system*“ (Don Norman on Dekker, Risks Digest 23.07, 18 Dec 2003 *catless.ncl.ac.uk/Risks/23.07.html*)
  - *„Alas, the „old view“ is .. the current view, whereas the „new view“ is still seldom understood. ([It] has only been around for 50 years, so I suppose we need to give it more time.)*“ (Don Norman, *op.cit.*)

Cognitive State and Error

- Don Norman
  - *„it is far too easy to blame people when systems fail. The result is that over 75% of all accidents are blamed on human error. ... When the percentage is that high, it is a signal that something else is at fault, namely [that] the systems are poorly designed from a human point of view.... If a valve failed 75% of the time, would you get angry with the valve and simply continue to replace it? No, ... you would try to figure out why the valve failed, and solve the root cause of the problem*“ (Don Norman, *op.cit.*)

The Überlingen Midair Collision, 1 July 2002

The Überlingen Midair Collision



Überlingen Analysis

- Flight controller's verbal error (visual cognitive error)
- Ladkin speculated that the Russian crew had thought that there was a third, unseen, aircraft above them (*ACAS and the South German Midair, Tech Report RVS-Occ-02-02, 12 August 2002*)
- This supposition confirmed by official report (BFU, May 2004, available from *www.bfu-web.de/berichte/index.htm*)

- The Russian crew's actions were rational in the light of what they thought they knew (Ladkin, *Causal Analysis of the ACAS/TCAS Sociotechnical System*, in Cant, ed., *Safety Critical Systems and Software 2004*, available from *crpit.com/vol47.html*)

Überlingen Consequences

- All participants dead
  - Passengers and crew of the aircraft
  - Air traffic controller Peter Nielsen murdered by relative of victim
- Eight former and current air traffic controllers at Skyguide (Swiss ATC) charged in August 2006 with involuntary manslaughter
  - „*Yet none were present the night of the crash*“ (Don Phillips, *If blame is assigned, what would be gained?* International Herald Tribune, August 17, 2006)

Phillips on the Swiss Prosecution

- *„The charges highlight a stark difference in the way Europe and the United States pursue responsibility.... Attempts by U.S. prosecutors to bring a felony charge are typically stopped by the Justice Department.... Canada has gone one step further, adopting a long list of possible causes in its investigative reports rather than concentrating on one or two factors. The idea ... is ... that it is far more important to make certain that the aviation industry learns from crashes than to assign culpability, unless there is clear criminal intent. If employees understand that they will not be prosecuted ... they are likely to be far more open and honest in crash investigations, according to this thinking*.“ (Don Phillips, *op.cit.*)

Aviation Week's Pierre Sparaco

- Longtime European editor for the trade journal Aviation Week and Space Technology
- Writes regular one-page column „*A European Perspective*“
- Three columns in 2006 on blame and understanding:
  - 22 May 2006, „*Investigative Errors*“, on France's way of conducting aviation accident investigations with parallel technical and judicial inquiries, in which the jurists have priority over custody of evidence; „*continues to stun the international flight safety community*“. Why so strong words? Because he is commenting on the trial in Colmar of then-principals of Airbus, Air Inter (the carrier), and DGAC (the regulatory authority), *fourteen years after* the accident. He asked what purpose the trial can serve.

Two Further Sparaco Comments

- 3 July 2006, „*Missed Opportunity*“, also on the Colmar trial, quotes Jean Pinet, a former Concorde test pilot who also devised Airbus's training: „*it would be more useful to review the lessons of experience than to devise sentences*.“
- Sparaco, 3 July 2006: „*Safety experts were hoping that the chain of catastrophic events would be revisited with fresh eyes, in an attempt to reconcile the needs of technical investigators, the judicial world, and the travelling public. But no such outcome is in sight .....*“

- 13 Nov 2006 „*Unwarranted Criminalisation*“, about the midair collision of an executive jet with a commercial transport over the Amazonian jungle, 29 September 2006 and the legal events surrounding it

GOL 1907 / Embraer Legacy Collision

GOL 1907 / Embraer Legacy Collision

Amazonas Collision Events 1

- Legacy was on a delivery flight from the factory to its U.S. owner. A New York Times journalist, Joe Sharkey, was on board. The Legacy felt the collision, the pilots determined they had hit something, and made a precautionary landing at a nearby military airfield.
- The wreckage of GOL 1907 was found some time later
- Both airplanes flying IFR under control of Brazilia Cindacta-1 and Manaus Cindacta-4 centers.
  - Note: same airspace, different control centers
- Secondary radar (transponder returns) on Legacy lost 54 minutes before collision; primary radar lost 19 minutes before
- No TCAS Resolution Advisories to either aircraft

Amazonas Collision Events 2

- Contact between Brazilia Center and the Legacy was lost from about ½ hour before collision, despite attempts by both to communicate.
- Brazilia had an altitude change for the Legacy, to descend and maintain Flight Level 360 (36,000 ft pressure altitude), which was not received (and known by Center not to have been received)

- According to the U.S. NTSB, „*there is evidence that the flight display warning [„TCAS OFF“ in small white lettering on the flight display] was available to the crew but not noticed and acted upon until after impact.*“ The NTSB recommends such warnings be enhanced (Recommendations A-07-35/6).

Amazonas Legal & Political Events

- Legacy pilots' passports withheld immediately by Brazilian authorities, and pilots were detained
  - Prosecutors said publically that the crew might have turned off the transponder, and could therefore be charged with involuntary manslaughter
  - TCAS requires an operating transponder
  - Secondary radar returns (that is, returns from an operating transponder) were not observed from some while before the collision until shortly thereafter

Amazonas Legal & Political Events 2

- The Flight Safety Foundation president William Voss said „*We call on the Brazilian government to ... continue to respect the integrity of the investigation and not rush to judge the various players in this accident*“.
  - Concerning the suggestion that the pilots might have turned off the transponder to be able to continue to fly at Flight Level 370, „*from a common-sense perspective, that's a lot of trouble to go [to] for 1,000 feet*.“ (Paulo Prada and Matthew L. Wald, International Herald Tribune, 9 October 2006)
- The Allied Pilots Association, representing 13,000 American Airlines pilots, requested (Aviation Week, 27 Nov. 2006)
  - the investigation be conducted according to ICAO Annex 13 guidelines and not as a „*criminal proceeding*“
  - release of the pilots and the return of their passports.

Amazonas Legal & Political Events 3

- International Federation of Air Line Pilots' Associations (IFALPA) said there is „*no valid reason for the continued detention of the two Excelaire pilots*“ and called on the Brazilian authorities to return their passports immediately (Flihgt International, 21-27 Nov. 2006)
- President and CEO of the U.S. National Business Aircraft Association (NBAA), Ed Bolen, requested President da Silva intervene to resolve „*an unacceptable situation that must not continue*.“ (Aviation Week, 27 Nov. 2006)
- President da Silva changed the organisation of Brazil's military-run air traffic control organisation on 25 Nov. 2006 (Aviation Week, 4 Dec. 2006)
-

Amazonas Legal & Political Events 4

- A Brazilian federal court ruled on 5 Dec. 2006 that there were „*no grounds*“ for the passports to be withheld.
- Brazilian federal police charged the pilots on 8 Dec. 2006
  - They were questioned for 6 hours
  - Their passports were returned
  - They were allowed to leave the country, but are required to return for their trial
- (Associated Press, 8 Dec. 2006, in International Herald Tribune WWW site *iht.com*)

Amazonas Legal & Political Events 6

- Lead investigator Renato Sayo was reported to have told „local media“ that „*air traffic controllers shared some of the blame*“ (*Avoiding the Blame Game*, Flight International, 30 Jan. - 5 Feb. 2007)
- FSF President Voss said the „*rush to punish must be balanced against the need for openness and reporting that is essential to avoid the next tragedy*.“ (*op.cit.*)

Amazonas Investigative Events 1

- It is procedurally required in the U.S. under conditions of communication loss for pilots operating under IFR to fly at the highest of the altitudes
  - assigned in the last ATC clearance received
  - [other conditions that do not pertain here]
  - Federal Aviation Regulations: 14 CFR 91 § 91.185 (2)

Amazonas Investigative Events 2

- Brazilian ATC representatives (IFATCA) visited Cindacta-1 days after the collision
  - the display software automatically updates the cleared flight level to that in the flight plan, without direct involvement of the controller and without prominent indication that this occurred
  - it would follow that the display software updated the FL to 360 at the Brazilia VOR (BRS), since that was in the flight plan (FL 370 on UW2 to BRS; change to UZ6 to Manaus and FL 360; to FL380 at TERES. NTSB Factual Report, October 2006)
  - hence the controller would see the Legacy at FL 360 after BRS, although it was flying at last cleared altitude, FL 370
- Loss of secondary surveillance info entails that any mismatch of flown/cleared Flight Level was not displayed
- (David Kaminski-Morrow, Flight International, 5-11 Dec 2006)

Opinion (Sparaco)

- Pierre Sparaco, Column „*Unwarranted Criminalisation*“ in Aviation Week, 13 Nov. 2006
- Quotes William Voss, President and CEO of the Flight Safety Foundation: „*We are increasingly alarmed that the focus of governments in the wake of accidents is to conduct lengthy, expensive and highly disruptive criminal investigations in an attempt to exact punishment, instead of ensuring the free flow of information to understand what happened and why, and prevent recurrence of the tragedy*.“
- Reports a joint resolution of the Flight Safety Foundation, the U.K. Royal Aeronautical Society, the French Academie Nationale de l'Air and the Civil Air Navigation Services Organisation (umbrella org of air traffic service providers)

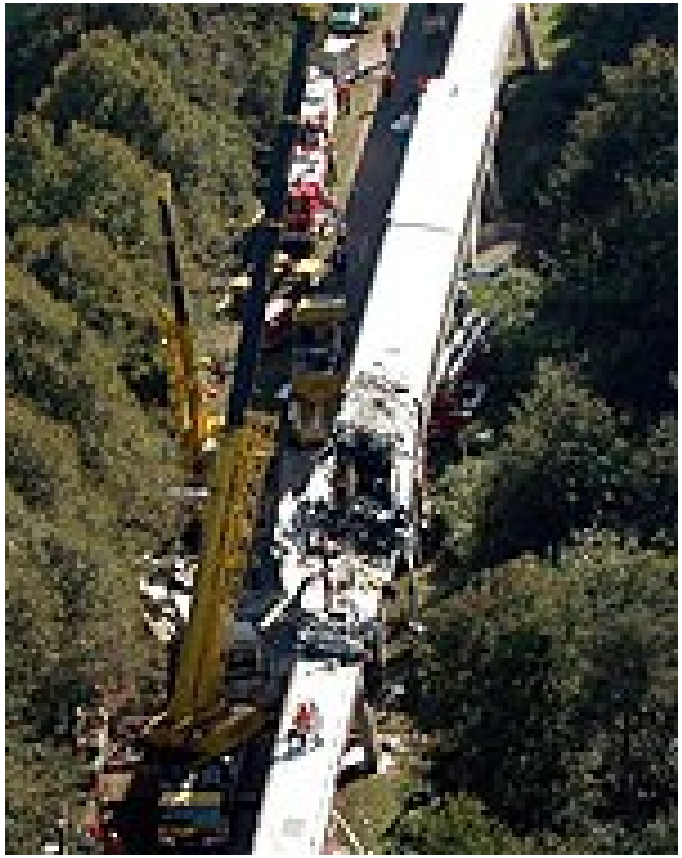
Opinion 2

- The four independent organisations jointly urge governments „*to exercise far greater restraint and adopt stricter guidelines before officials initiate investigations or bring criminal prosecutions in the wake of aviation disasters*.“
- Sparaco: „*we all agree with the resolution when it stresses that the predominant risk of accident criminalization is the refusal of witnesses and other parties to cooperate with investigators to protect themselves from criminal prosecution*.“
- Sparaco: „*The resolution also urges governments to refrain from „premature disclosure“ of probable causes or factors believed to have contributed to an accident*.“

Opinion 3

- *„Of course, aviators and technical investigators are not suggesting that judicial immunity should prevail. Criminal investigations can be appropriate under specific circumstances, but accident criminalization is certainly not an effective deterrent.“*

Transrapid Accident, Lathen, 22 Sept 2006



Transrapid Accident, Lathen, Sep 2006

- The Transrapid was accelerating through 180 kph when it collided with a stationary service wagon on the elevated track
- State prosecutor Alexander Retemeyer, on the evening of the accident: „*Vermutlich ist von menschlichem Versagen auszugehen*.“ (Neue Westfälische Zeitung, 23-4.09.2006)
- **But**: „*At this point, we believe the main reason is that the maintenance vehicle was not integrated into the train security system*“ (Retemeyer, Associated Press report, 22.09.2006)
- „*Menschlisches Versagen deutet sich somit für die Ermittler als Auslöser der Katastrophe an, aber es werden auch Lücken in System sichtbar*“ (NW, 25.09.2006)

Transrapid Accident, Lathen

- Note:
  - On the evening of the accident, when he proposed that human error was the cause of the accident, Herr Retemeyer had not had the time at that point even to look into the safety system descriptions and definitions
  - What Retemeyer said to AP contradicts what he said to NW.
  - It is accepted amongst researchers into causal explanations of accidents that there is no generally-agreed way of prioritising some causal factors over others (Leveson, Knight, Ladkin, personal communications, April 2007). Some (e.g., Leveson) believe there can be no objective prioritisation, and that prioritisation stems largely from political decisions, not objective technical criteria.

Transrapid Accident, Lathen

- Rudolph Schwarz, IABG: „*[It] is the result of human error*“ (AP, 22.09.2006, on the International Herald Tribune WWW site)
  - The same applies to Herr Schwarz. He has not had the time to analyse many of the circumstances. Besides, he works for the operating company. The operating company may be presumed to have a legal and business interest that their systems are not judged to be failure-prone.
- Kevin Coates, a „former spokesman for Transrapid“: „*I have to believe that this is not a malfunction of technology but a communications breakdown [between operators and maintenance personnel]*“ (*op.cit.*)
  - These are not the only two possibilities. Poor system safety design and poor system safety assessment are two others

Transrapid Accident, Lathen

- One to two years previously, employees had asked that the service vehicles be integrated into the „technical safety system“, according to the CEO of the operating consortium. This request was declined (Neue Westfälische Zeitung, 27.09.2006. Statement from Joachim Schwarz, Chairman (Vorsitzender) of the Executive (Geschäftsführung)).
  - The „technical safety system“ uses trackside sensors; the service vehicle has voice radio-communications and a GPS locator only (NW, 25.09.2006)
  - That this was explicitly considered and rejected fulfils the criterion for this to be a technical „non-event“ in a WBA List of Facts

Transrapid Accident, Lathen

- Although parts of the system are monitored through video cameras, the service wagon was stopped at a location that was outside video surveillance (NW, 25.09.2006). This location, Post 120, is its „*normal daily halting point*“ (AP, 23.09.2006, from IHT WWW site)
  - Lack of video surveillance thus fulfils the formal criterion for a „non-event“ in a WBA List of Facts
  - *Had there been* full video surveillance of the test track, the position of the service wagon *would have been* visually observed (in the „*nearest possible world*“)
  - *Had* the position of the service wagon been visually observed on a video monitor, the start clearance for the Transrapid *would not have been* given

Transrapid Accident, Lathen

- Conclusion: that the „*normal daily halting point*“ of the service wagon, Post 120, was outside the video surveillance area satisfies the Counterfactual Test to be a necessary causal factor (NCF) for the start clearance to have been given to the Transrapid.

Transrapid Accident, Lathen

- There were two separate radio communication systems: one for the Transrapid train, and one for the service wagon (Reuters, 10 Jan 2007, citing the Neue Osnabrücker Zeitung)
  - The GOL 1907 / Legacy collision also involved two different communication systems for the same airspace
  - The Royal Commision investigating the rail collision in Glenbrook, near Sydney, 2 Dec 1999, cited the different communication systems as a causal factor in the accident (Ladkin, *Why-Because Analysis of the Glenbrook, NSW Rail Accident and Comparison with Hopkins's Accimap,* Research Report RVS-RR-05-05, Uni Bielefeld 2005)

Transrapid Accident, Lathen

- *Had* there been one radio communication system for both vehicles, there *would have been* one controller handling both positions and states.
  - That this controller would have known both positions and states, and thus observed the conflict, is highly likely, provided heshe was not handicapped in some way – drugs, sudden illness.
  - The „*no handicap*“ proviso is assured through the „*nearest possible world*“ interpretation of the counterfactual.
  - *Had* the controller observed the conflict, heshe *would have resolved it* through instruction or through not switching the power on

Transrapid Accident, Lathen

- Conclusion:
  - That there was not one communication system is a non-state in the List of Facts
  - That there was not one communication system satisfies the Counterfactual Test as NCF for the Transrapid start clearance to have been issued

Transrapid Accident: Further Questions

- For systems with safety-critical features .....
  - such as a very-high-speed train
- .....it is standard practice to perform
  - a hazard analysis
  - a risk analysis on the identified hazards
  - identify mitigations that reduce the actual risk of a hazard to the „socially acceptable“ risk
- This „standard practice“ has been formulated in the International Standard IEC 61508 for functional safety of systems incorporating electrical, electronic, or programmable electronic (E/E/PE) components, which came into force in 1997
- Let's see .....

Transrapid Accident: Further Questions

- 1. Was the hazard of having an obstruction on the track during a run explicitly considered in the hazard analysis?
  - This is a routinely recognised hazard for trains
- Was the possibility that this obstruction could be a service vehicle considered?
  - Collision with another object-under-control (train) is a routinely recognised hazard for trains
- Two answers
  - 1Y: Yes. Then was there a risk analysis of the control setup?
    - Go to 1Y.1
  - 1N: No. Then faulty hazard analysis
    - Moral question: Should we prosecute the hazard analysts?

Transrapid Accident: Further Questions

- 1Y.1: Was there a risk analysis performed of having another vehicle on the track during a run?
  - 1Y.1Y: Yes. Then how great was that assessed risk?
    - See 1Y.1Y.1
  - 1Y.1N: No. Then risk analysis faulty because absent.
    - Moral question: Should we prosecute the risk analysts?
- 1Y.1Y.1: How great was that assessed risk?
  - 1Y.1Y.1Negl: Negligible: Then faulty risk analysis
    - Moral question: Should we prosecute the risk analysts?
  - 1Y.1Y.1L: Low. Then were mitigations undertaken?
    - See 1Y.1Y.1L.1
  - I presume the risk was assessed as neither high nor very high

Transrapid Accident: Further Questions

- 1Y.1Y.1L.1: What mitigations were undertaken?
  - No technical mitigation (so it appears)
    - This was explicitly requested two years ago
    - Moral quesion: Should we prosecute the management who decided „no“?
  - Just human-operational mitigation
    - How is it that we give operators distributed information sources, expect them to integrate it all, and threaten them with prosecution when (not „if“, but „when“) they fail?
    - Why is it that the people „at the pointy end“ are the first to be suspected of being „responsible“ for an accident, although they are the last in terms of time who contributed to the flow of events?

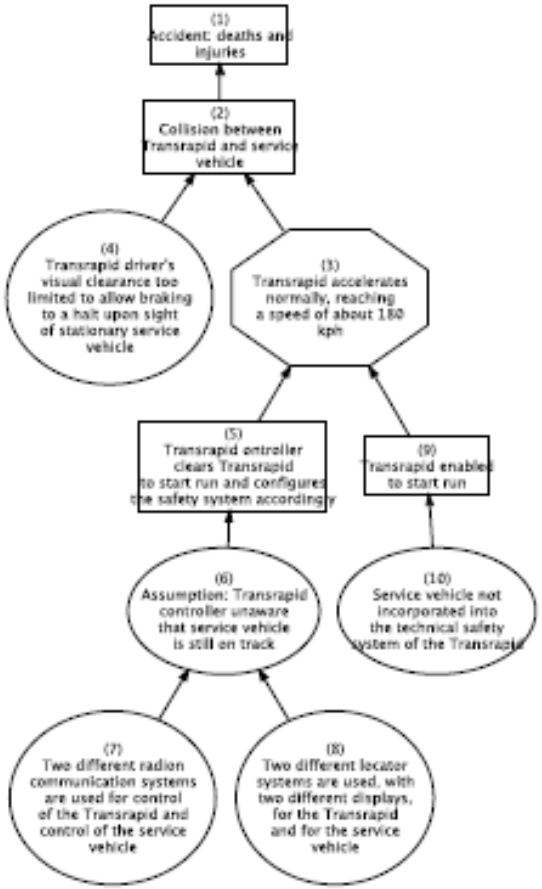
Transrapid Accident: Further Questions

- What management oversight ensured the correctness of the hazard analysis, the risk analysis, and the mitigation?
  - If we don't get to 1Y.1Y.1L.1, we have a failure of the standard assessment procedures for safety of critical systems
  - If we do get to 1Y.1Y.1L.1, it could be argued that failure to undertake specific mitigation when asked to do so is a decision failure of management
  - It follows there was in any case **a failure of a standard process in safety-critical system management**
  - Senior management is conventionally „responsible“ for the correct execution of these standard critical-system management processes. Moral question: Should we prosecute them also?

Transrapid Accident: Observations So Far

- The different visual location systems were overseen by two different people, who were to coordinate procedurally
- The two different communication systems were overseen by two different controllers, who were to coordinate procedurally
- There was no video surveillance of a regular halt point for service vehicles
- The service vehicle was not incorporated into the technical safety system used for the Transrapid itself
- I have also argued towards a failure of analysis or oversight. Let's leave this for now.

Lathen, the Partial WB-Graph



Lathen, Possible Countermeasures

- Incorporate all vehicles into the technical safety system
- Use one display for location of all vehicles
- Use one radio communication channel for communication with all vehicles on the demo track
- Have one controller for all vehicles on the demo track (technically supported as necessary)

- Note: none of these are measures which one takes to avoid human error („menschliches Versagen“)
- That is because they work by allowing fewer possibilities for operations personnel to make errors with dangerous consequences

Human Error

- Human error is unavoidable
- Human Reliability Assessments conventionally assign a general error rate to a generic task of one in one thousand
- One must design systems such that such errors result much less frequently in dangerous overall system failures
- This said, I regard it as morally inappropriate to try to assign blame to operations personnel for making errors which result in a dangerous system failure, when ALARP-based mitigation of the causal connection between such errors and dangerous system failures has not been undertaken

- But don't just take my word for it .....

Menschliches Versagen

- „*Nicht das menschliche Versagen sollte uns beschäftigen, sondern wir sollten mit unserer menschlichen Kreativität nach Lösungen suchen, die gefährliche Auswirkungen des menschlichen Irrtums bis zur Unwahrscheinlichkeit minimieren*“
- Jochen Trinckauf, Professor für Verkehrssicherungstechnik, Fakultät Verkehrswissenschaften „Friedrich List“, Technische Universität Dresden, in *Menschliches Versagen?*, Signal+Draht, März 2007

First Lesson

- The examples here show that the technical causal investigation of accidents is way in advance of society's ability to handle the social issues arising from accidents (e.g., blame, reparations, mitigation)
  - Technical causal investigation generally produces results that assign root causes across a wide spectrum
  - There is no identified and well-accepted method for prioritising root causes across this spectrum
  - It should follow that there is no identified and well-accepted method for assigning liability to the proponents of/participants in those root causes
    - In particular, to the people at the „pointy end“ rather than to hazard analysts, risk analysts, or senior management „responsible“ for accepting those analyses and making appropriate decisions

Second Lesson

- Blaming the operators is not helpful for prophylaxis
  - The Brühl driver could „remember“ nothing, although understanding his cognitive sequence would have been crucial to identifying weaknesses in signalling and other procedures
  - Blaming the crew of SQ006 deflected attention from the contributory features (even „affordances“) of the airport environment
  - Blaming the Russian crew for manoeuvring contrary to the RA deflected attention from those features of TCAS procedures that would have led them to do this rationally
  - Detaining the Legacy crew accomplished nothing for the investigation into the Brazilian midair collision
- **So what will happen about Lathen?**

Thanks for listening!