



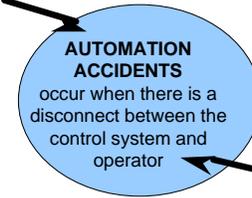
Automation in Transportation Accidents

Deborah Bruce
National Transportation Safety Board
Washington, DC



Automation Accidents

Control
System
Design



Person

- Monitoring
- Task overload
- Expectancy
- Inattention
- Complacency
- etc....



The Role of Automation

- Transportation databases focus on fatalities
- Automation-related mistakes difficult to analyze
- Varied and inconsistent taxonomies

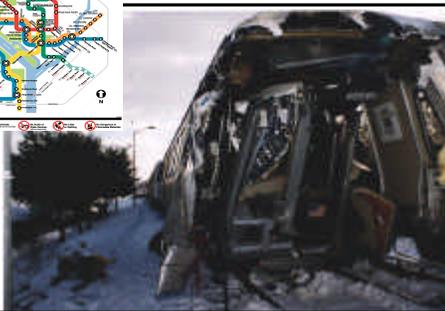


Accident Examples

- Washington Metro Train Collision
 - Shady Grove MD on Jan 6, 1996
- Grounding of the Royal Majesty
 - Near Nantucket on June 10, 1995
- Pipeline release of hazardous liquid
 - Near Gramercy LA on May 23, 1996
- A300 Inflight Upset
 - Near West Palm Beach FL on May 12, 1997



Metro train



Pre-Accident Events

- Severe snow storm track conditions worsening.
- All Metrorail trains were functioning in Automatic train operation as opposed to Manual operations.
- Computerized system at Metro's Operations Control Center controls train acceleration, speed, and braking.
- Train operator responsible primarily for monitoring train functions and ensuring safe operations.



Metrorail Operations Control Center

- Controllers monitor and direct operations throughout the system.
- Controllers set parameters for trains by assigning the train's "performance levels" (train's acceleration and top speed).
- Under new Metro policy, controllers were not permitted to authorize train operators to change from automatic to manual mode except in emergencies.



Metro Operating Practices

- High number of wheel flats on Metro train . . . because of braking slides in manual mode.
- The November 17, 1995, notice instructing controllers *not* to permit train operators to change to manual mode (except in emergencies).
- The Jan. 6, 1996 storm was the first serious snow storm after change - - first real test of the new policy.



Accident Sequence

- Controllers instructed the train to continue Automatic mode, set speed at lower performance level (59 mph).
- Train overruns Twinbrook Station (told by controllers not to service station go to next in Automatic mode).
- The train then overran Rockville Station by one car. Results in *performance level* loss because the train was not within platform limits.
- Thus, the train departed to Shady Grove Station at 75 mph (rather than 59 mph). Train overran station by 470 ft, struck and telescoped 21 feet into standing train.



NTSB Findings

- Safety Board found over reliance on system automation to ensure safe train operations.
- Controllers had responsibility for day-to-day train operations, but lacked authority.
- For the 20 year history of Metrorail, controllers routinely gave permission for train operators to change to manual operation during periods of inclement weather.
- Controllers felt that train operator could do a better job of controlling the trains manually in slippery track conditions.



NTSB Conclusions

- Metro management practices were inconsistent with complex automated rail system.
- Decisions for highly technical automated systems usually affect other activities (and sometimes produce unanticipated hazards).
- Metrorail management failed to fully understand the design features and limitations of the automatic train control system--
- Which led to unjustified management confidence that the system could ensure safe train operation under all operating conditions.



Royal Majesty





Navigational Track



Integrated Control Bridge



Chartroom



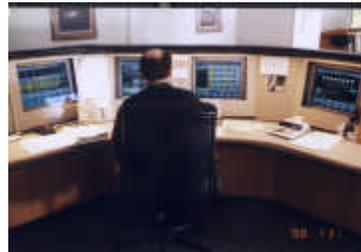
GPS Display



Pipeline Control System



SCADA System





Process Control Screen



A300-600 Inflight Upset

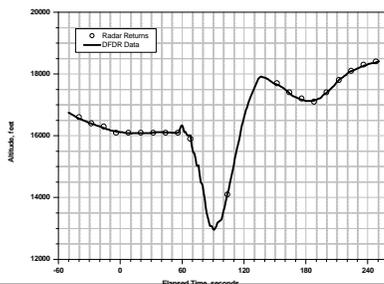


Event Sequence

- Autothrottle set to hold 210 knots
- Engaged at start of descent from FL240
 - During descent - power reduced from idle to mechanical stops
- Not engaged at level off at FL160
- Airspeed decreased
- About 170 knots flightcrew advanced throttles
- Stall warning activated and upset occurred
- No evidence of autothrottle malfunction



AA 903 Altitude Plot

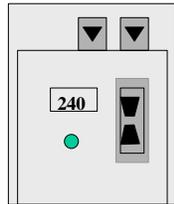


Cockpit





Instrument Diagram



Autothrottle Controls

- Engaged via button on glareshield
- Disengage - depress disconnect button on throttle, FMA to amber "MAN THR", green bars on FCU out
- Other airplanes have warning systems requiring additional flightcrew action
- A300 - passive and persistent indications
- More typical of information display, does not command attention, possible delay between inadvertent disconnect and recognition



A300 Upset Loss of Displays

- Primary flight controls went out momentarily during upset
- Replaced by indication that computers driving the displays were undergoing automatic reset and self-test
- Function designed to detect unreliable data - monitors flight parameters



A300 Upset Loss of Displays

- Reset threshold for roll rate - greater than 40 degrees per second
- Airbus first time reset reported during upset
- Recommendation issued to FAA asking that Airbus modify this software on A300 because of the potential for loss of information during unusual attitude recovery



What do these accidents tell us?

- Role of defaults in adaptive automation
- Effects of high false alarm rates
- Dangers of passive monitoring
- Unanticipated failure modes

and, that training just won't cover everything