Accident Analysis
What to do… What not to do…

Quote for the day

- “*Experience* is waiting until we have had an accident ourselves.”
  Lee Hung-Kwong

Accidents presented…

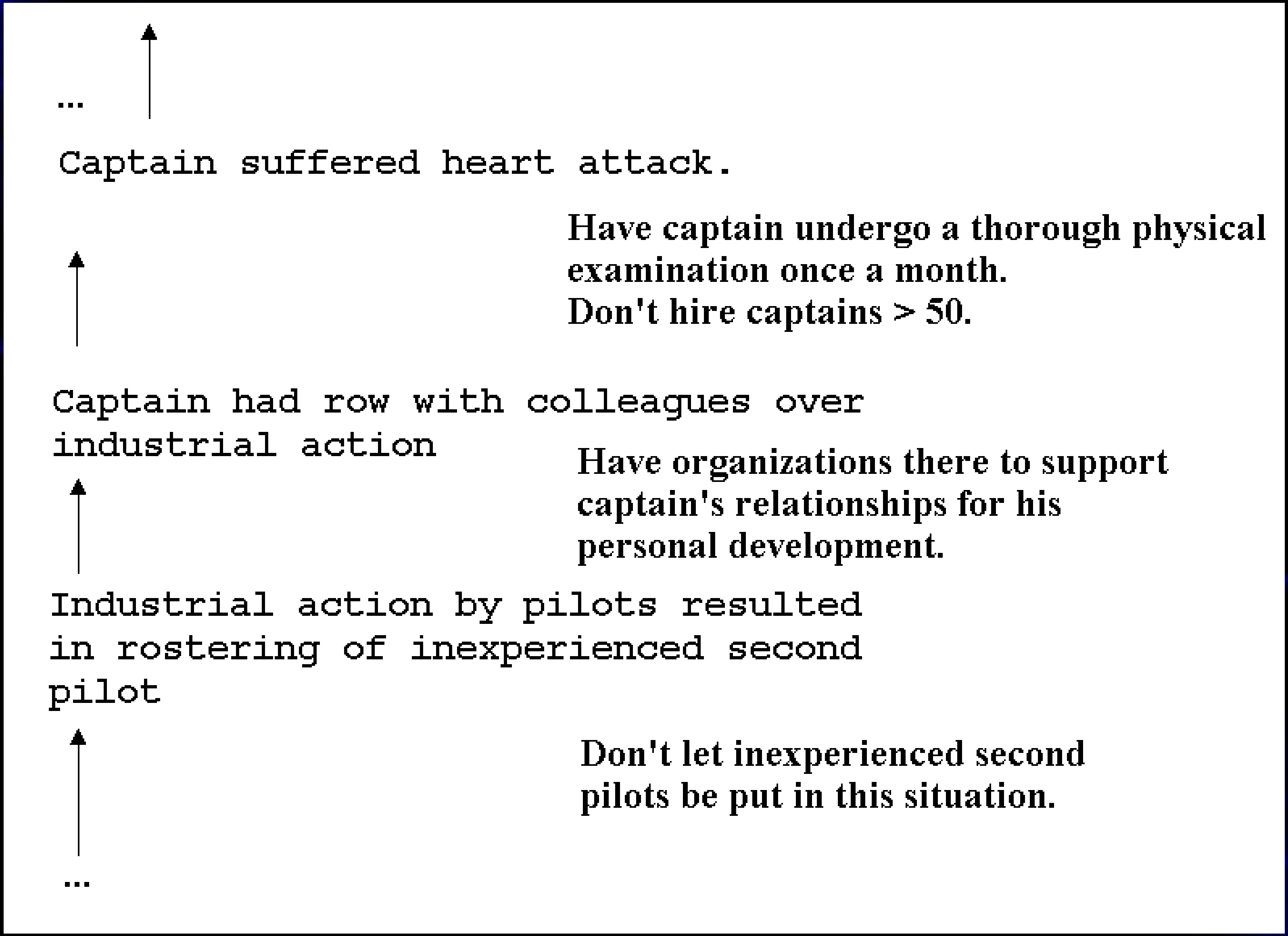
- R101 Airship (leaking hydrogen)
- Comet crashes (fuselage)
- Munich crash (de-icing and slush)
- 1972 Trident crash at Heathrow (stall)
- …

Goals

- Common factors in aviation accidents
- Apply findings to accident analysis and software

Errors in Aviation

- Kletz’ model
  - 3 layer classification
    - Technical
    - Avoidance
    - Improve management
  - Not very good but better than nothing
  - Let’s take a look at Trident crash at Heathrow of ‘72



...

Captain suffered heart attack.

Have captain undergo a thorough physical examination once a month.
Don't hire captains > 50.

Captain had row with colleagues over industrial action

Have organizations there to support captain's relationships for his personal development.

Industrial action by pilots resulted in rostering of inexperienced second pilot

Don't let inexperienced second pilots be put in this situation.

...

Kletz Model

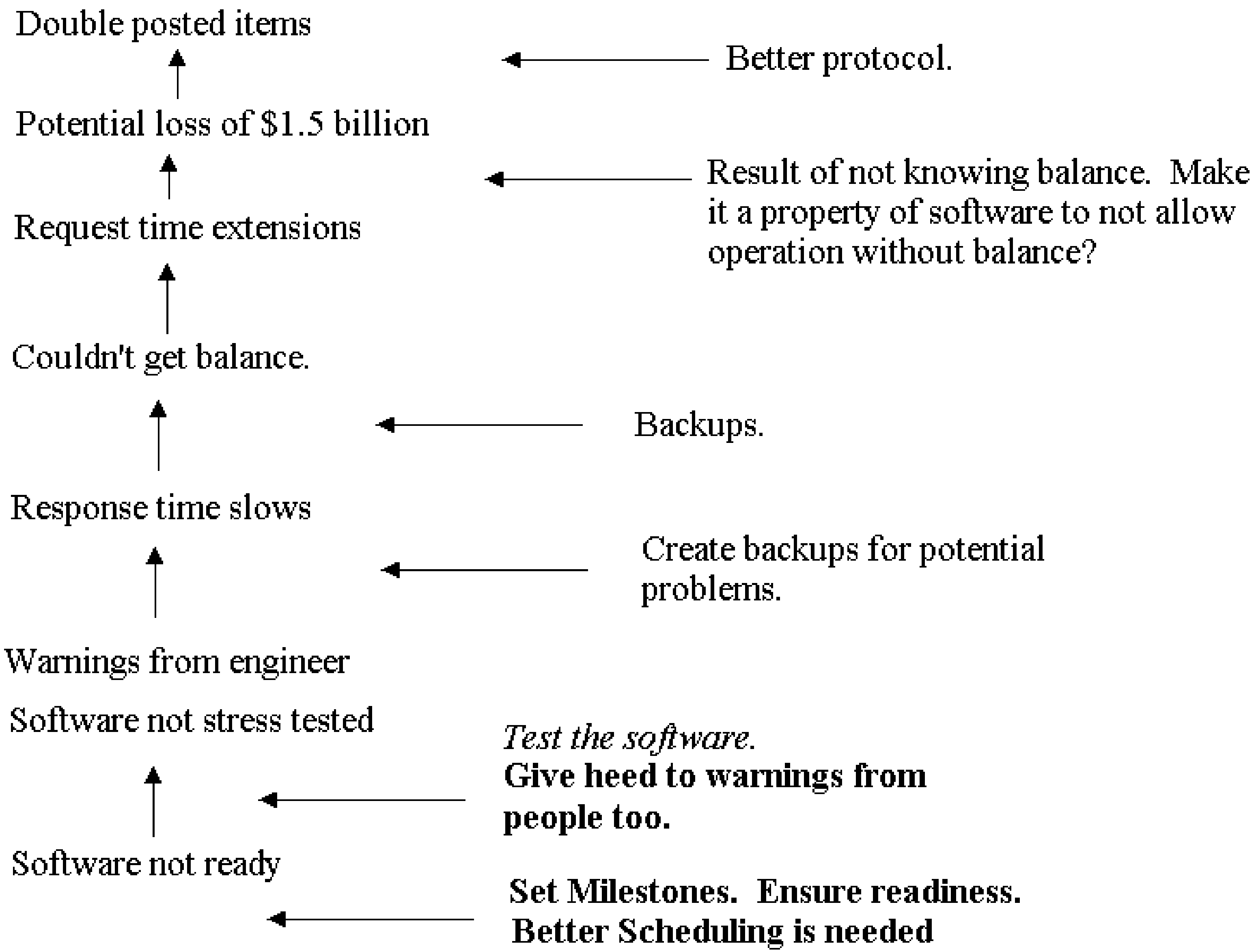
- “Recommendations”
  - **Learn from experience**
  - Do not take unnecessary risks in high-risk areas.
  - **Follow up known weaknesses…**

Simon says…

- Many recurring “recommendations”
  - Provide better training
  - “You get what you pay for.”
  - Learn lessons of the past… of incidents (not just accidents).
  - Don’t rush.
  - Error on side of safety.
  - Don’t ignore warnings. Turning them off?
  - Politics’ involvement

A software accident…

- Federal Reserve’s funds transfer system
  - “Bankwire”
  - Upgrade to help protect against overdrafts
  - Software not ready. Ok for production 2 days later? No, not “stress tested.” Whatever…
  - Fine on first day. By end of 2nd day, main file in new software heavily fragmented, consuming system resources
  - Response time slowed
  - Transactions of “double posted” items



Double posted items

Better protocol.

Potential loss of $1.5 billion

Result of not knowing balance. Make it a property of software to not allow operation without balance?

Request time extensions

Couldn't get balance.

Backups.

Response time slows

Create backups for potential problems.

Warnings from engineer

Software not stress tested

Test the software.

Give heed to warnings from people too.

Software not ready

Set Milestones. Ensure readiness.

Better Scheduling is needed

Comments on Kletz’ applied model

- Hard to find proper recommendations
- How many recommendations are necessary?
- Are some of these accident issues unique to software?
- Some of the same problems in the Bankwire accident as in aviation accidents

Appendix 1 – Questions to ask during accident investigation

- WHAT equipment failed?
- HOW can we prevent failure or make it less likely?
- HOW can we detect failure or approaching failure?
- Apply these questions in using model for accident analysis
- Not what is the cause, but how can this accident be prevented from happening again?

Classification of errors

- Identify a trend
- Need good categorizations of errors
- Extended to software
  - Common errors
    - Index out of bounds
    - Bad input (e.g. null input, tainted user input)
    - Timing issues
    - What classifications in software could help reduce accidents?

Accident Investigation Myths

- Many popular beliefs about technology, management, and the environment are not wholly true, although they may have a measure of truth
- These ideas hinder, rather than help, the process of accident investigation and (future accident) prevention
- Consider this a list of pitfalls to avoid…

Myths About Accidents

- Most accidents are due to human error
- Natural accidents are “Acts of God” and are unavoidable
- We have reached the limit of what can be done by engineering to reduce accidents. We must now concentrate on human factors.

Myths About People

- Most industrial accidents occur because:
  - managers put costs and output before safety
  - workers fail to follow instructions
  - workers are unaware of the hazards
- If someone’s action has resulted in an accident, the extent of the damage or injuries is a measure of his or her guilt

Myths About Organizations

- Warnings don’t travel up
  - “If I had known that was happening I would have stopped it…”
- Long periods of “smooth sailing,” with few accidents, indicate that everything is under control

Myths About Investigation

- Two competent and experienced investigating teams will find the same causes for an accident.
- The purpose of accident reports is to establish blame

DOGBERT IS HIRED AS A BLAME CONSULTANT.
THE COMPANY'S WOES ARE YOUR FAULT, NOT SENIOR MANAGEMENT'S!
9-16
E-Mail: SCOTTADAMS@AOL.COM
S. Adams
DO YOU REALIZE HOW MUCH YOU COULD GAIN PERSONALLY BY MAKING THE COMPANY A SUCCESS?
© 1993 United Feature Syndicate, Inc
I WOULD GET A NICE PLAQUE IN A PLASTIC FRAME.
YEAH... I WAS HOPING YOU DIDN'T KNOW.

Clapham Junction: Fast Track to Disaster

- Crowded commuter train rear-ended another (stationary) train, then veered right to strike a third train head-on.
- Stationary train had stopped to report a faulty “wrong side” track signal
- The faulty signal failed to indicate the track was occupied, leading to the first collision

On 12 December 1988, Death: 35, Serious injuries: 69, minor : 415

Human Error at Clapham

- Errors by the technician:
  - Failure to cut back old wire
  - Failure to tie old wire out of the way
  - Old insulating tape used instead of new
  - Disconnection of only one end of a wire
  - Failure to insulate bare end of wire
- The last two are genuine lapses, but the rest were the result of habit and poor training
- None are really the result of failure to follow instructions, or ignorance of the hazards
- What are the software equivalents?

Organizational Failures

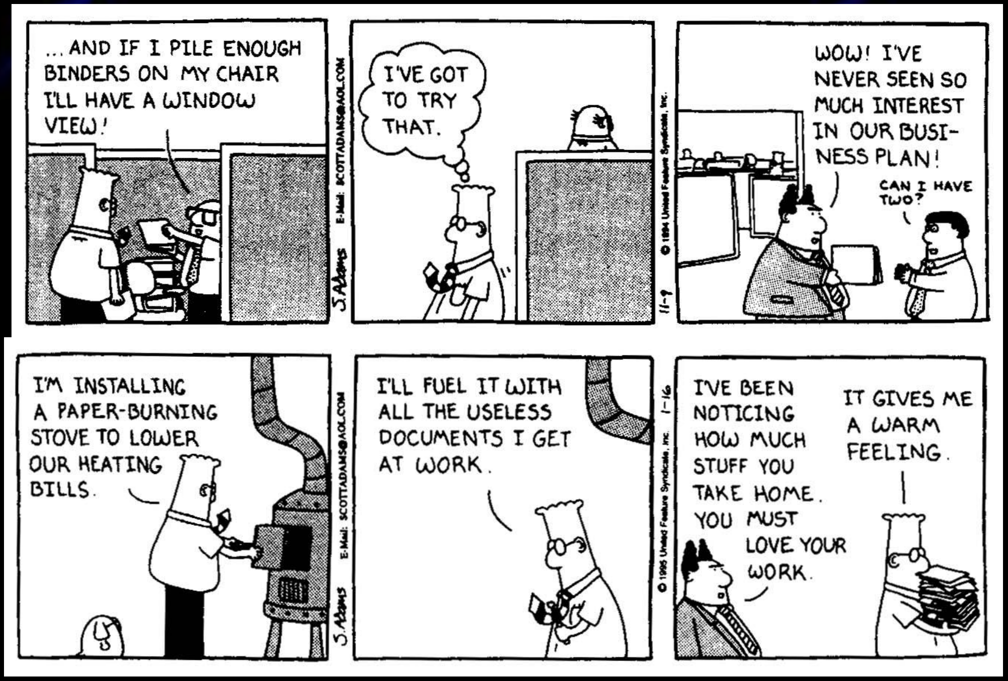
- The supervisor was doing manual work himself
  - – Failure to perform supervisory role
  - – Unaware of new instructions
- Job dissatisfaction
- Failure to follow up
- Supervisors “allowed *an originally sensible… system* to degenerate into *an incompetent, inept and potentially dangerous way of working.*”

✈ Redundant checkers encourage(d) negligence

- What does this say about processes like code review?

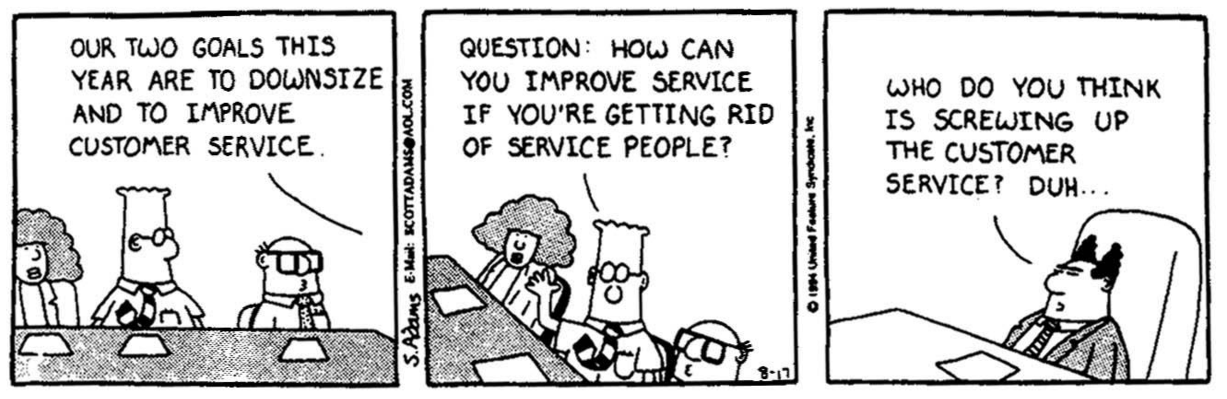
Communication Failures

- People don’t read documentation
  - “[He] had no time to…study [a provisional instruction]… He…*filed it and carried on*…”


…AND IF I PILE ENOUGH BINDERS ON MY CHAIR I'LL HAVE A WINDOW VIEW!
E-Mail: SCOTTADAMS@AOL.COM
S. Adams
I'VE GOT TO TRY THAT.
© 1994 United Feature Syndicate, Inc.
11-9
WOW! I'VE NEVER SEEN SO MUCH INTEREST IN OUR BUSINESS PLAN!
CAN I HAVE TWO?
I'M INSTALLING A PAPER-BURNING STOVE TO LOWER OUR HEATING BILLS.
E-Mail: SCOTTADAMS@AOL.COM
S. Adams
I'LL FUEL IT WITH ALL THE USELESS DOCUMENTS I GET AT WORK.
1-16
© 1995 United Feature Syndicate, Inc.
I'VE BEEN NOTICING HOW MUCH STUFF YOU TAKE HOME. YOU MUST LOVE YOUR WORK.
IT GIVES ME A WARM FEELING.

Communication Failures, cont’d

- People don’t (or can’t) learn from past accidents
  - Five(!) previous wiring failures produced a new provisional instruction “which was *never to be properly understood* or implemented…”
  - “[T]he [British Rail] rules are written [in semi-legalese] to protect the writer *rather than help the reader*.”


OUR TWO GOALS THIS YEAR ARE TO DOWNSIZE AND TO IMPROVE CUSTOMER SERVICE.
S. Adams E-Mail: SCOTTADAMS@AOL.COM
QUESTION: HOW CAN YOU IMPROVE SERVICE IF YOU'RE GETTING RID OF SERVICE PEOPLE?
8-17
© 1996 United Feature Syndicate, Inc
WHO DO YOU THINK IS SCREWING UP THE CUSTOMER SERVICE? DUH...

Management Failures

- “As in many other organisations, [the senior management of British Rail] had not realised… that *saying that safety was important and urging people to do better was not enough*…”
- Microsoft recently announced a new emphasis on “security?” Do you know how much training was actually provided?
  - Does this make you feel more “secure?”

Where Does This Leave Us?

- “Progress, far from consisting in change, depends on retentiveness… Those who cannot remember the past are condemned to fulfil it.”
    - George Santayana, *Life of Reason*

- How do we:
    - design safer work processes?
    - create documentation that people will read?
    - create a culture of accident-prevention?