white queen

Safety Strategies

Reducing the chance of information failures in the control room

Better prevention management through lessons from the past

Linda J. Bellamy

White Queen BV, Postbus 712, 2130 AS Hoofddorp, The Netherlands
Tel/fax +31 (0) 23 56 51353
e-mail: linda.bellamy@whitequeen.nl

prism ***Managing high-demand situations, Brussels, Belgium, 13-14 Nov 2003***

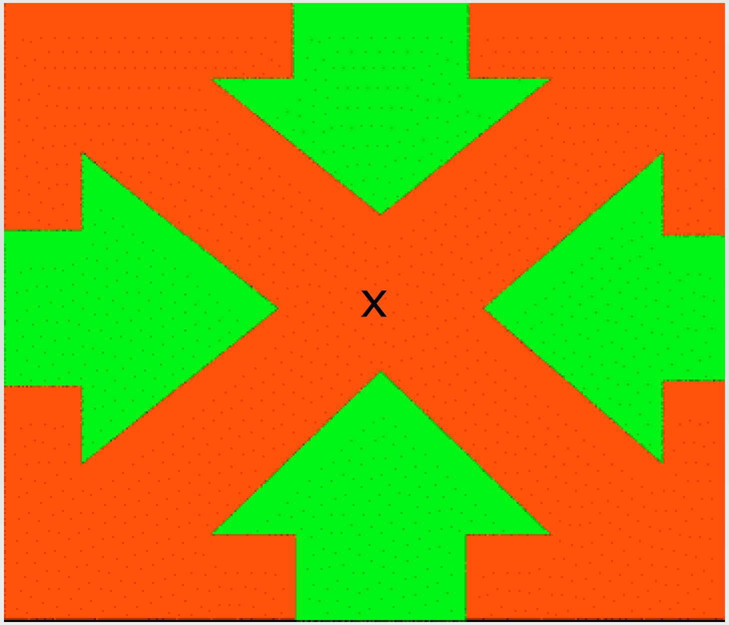
Issues

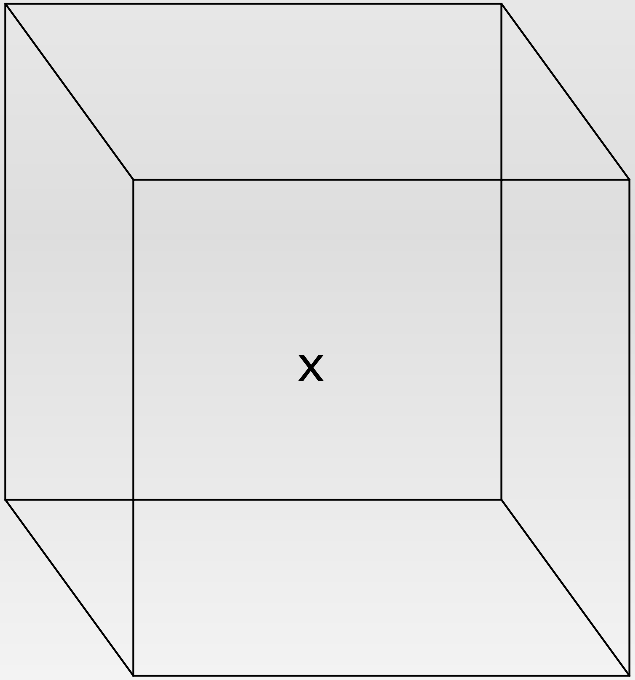
- Control room failures
- Causes
- Lessons learned
- Safety management solutions

Some things about humans

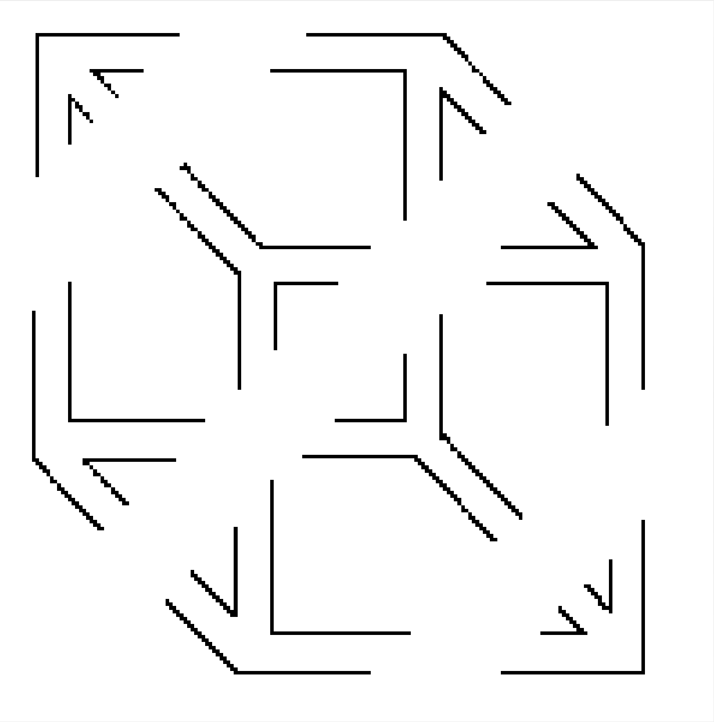
....

Attention fluctuates

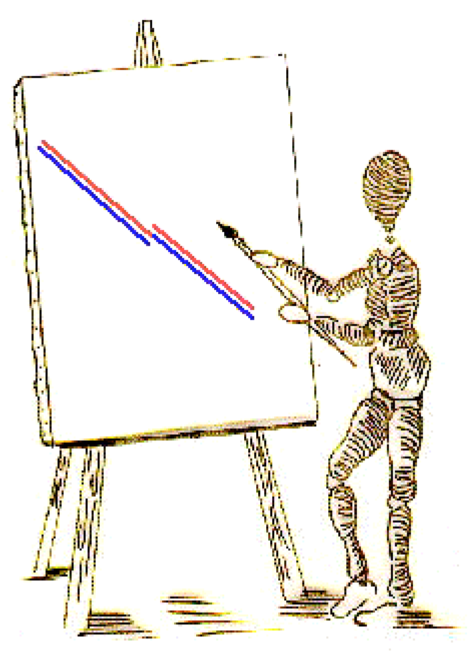


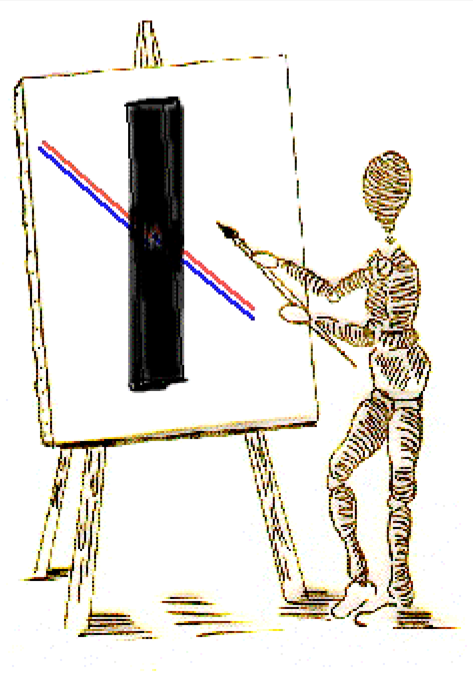


We fill in missing information



We make assumptions about hidden information





We make assumptions in order to resolve conflicting information

Mid air collision

A Swiss controller realised what was about to happen and told the pilot to descend

But at almost exactly the same time the Russian plane's TCAS, also registered that a collision was possible. A computerised voice advised the pilot to climb.

He decided to obey air traffic control, and descend. It was probably the wrong decision.

1988 study about computer controlled processes

Of 17 accidents supplied by companies:

- **Human errors** occurred in
- **59% of cases** which were primarily caused by
- **poor information**

Contribution to failure to recover from abnormal conditions

- □ Incorrect information
- □ No information
- □ Missed information
- □ Allocation of function problems

CAUSE CONTRIBUTOR	
Interface does not display actual status of plant or process	WRONG INFO
Installation error leads to incorrect information	
Alarm set incorrectly	
No alarm (maintenance)	
No alarm (design)	
Operator misses information (overload)	
No independent means of cross checking provided	NO REDUNDANCY
Operator fails to cross check	
Trip disabled/manual override	SAFETY SYSTEM DISABLED
Over-reliance on computer	
Inadequate knowledge	
Failure to update operators information	
Incorrect control signal (maintenance)	

	ACCIDENT NUMBER																
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
CAUSE CONTRIBUTOR																	
Interface does not display actual status of plant or process	x				x		x									x	
Installation error leads to incorrect information		x					x										
Alarm set incorrectly			x														
No alarm (maintenance)			x	x													
No alarm (design)			x	x													
Operator misses information (overload)												x		x	x		x
No independent means of cross checking provided	x	x			x											x	
Operator fails to cross check							x										
Trip disabled/manual override	x						x			x							
Over-reliance on computer								x		x			x				
Inadequate knowledge										x							
Failure to update operators information											x						x
Incorrect control signal (maintenance)									x								
Design error: plant			x	x			x										x
Design error computer controlled system						x											
Software error						x		x									
Equipment hardware				x								x	x	x	x		
Computer hardware						x										x	
Connection hardware: electronic					x												

Accident 1: Forgotten

- Final error
  - Bottom discharge valve of reactor not closed when batch job started resulting in a release of a toxic gas
- Causes:
  - System was originally software interlocked
  - **Operator disabled the switch because it was oversensitive**
  - By disabling the switch the valve was taken out of the interlock
  - As a result **the interface did not display the actual valve status**
  - No facilities for cross checking existed
  - At the moment that the batch job was started the wrong valve status was displayed
  - The operators **forgot that a special case applied** to this operation.

Accident 12: Not expected

- Due to a compressor failure a unit was shut down according to a standard procedure.

- **During the shutdown a compressor on another unit nearby tripped** and, as with the first unit, a manual valve needed to be opened.

- **This trip however was overlooked** resulting in a release of a flammable chemical to the atmosphere.

- The operator received **so much information at once** from the process computer because of the shutdown operation that he missed the second compressor trip.

Accident 15: Blinkered

- Damage occurred in a chemical plant due to exposure of equipment to extremely high temperatures.
- An operator failed to recognize a low level alarm in the cooling system because his attention was focused elsewhere.
- **Only a restricted part of the process could be monitored on the screen and the operator was only watching what was happening in the furnace.**
- Alarms were shown on a scrolling display such that only the last 12 alarms were indicated.
- For a big event with lots of alarms being triggered this meant that the operator lost control of what went wrong and where.

Unanticiapted problems

Not only is their poor information. Often other accident ingredients present:

- .....unusual nature of the circumstances
- ……the failure to anticipate what might go wrong

SOLUTION:

- Anticipate:
  - look at the past
  - look at what is similar now
  - implement solutions
  - test for the future
  - monitor the process

Consider rare events and their effects on the system e.g. The weather on the night of the Titanic disaster

- Sir Ernest Shackleton (being questioned on his iceberg expertise): “Of course, that particular night was an abnormal night at sea in being a flat calm; it is a thing that might never occur again.”
- Attorney General: You say apparently it is very rare to get such a flat calm as there was that night?
- Shackleton: “I only remember it once or twice in about 20 years' experience - the sea absolutely calm, without a swell, as it was recorded to have been.”
- A.G.: And if I followed correctly what you said earlier it would make it more difficult to pick up an iceberg with the eyes?
- Shackleton: “Decidedly.”
- A.G: If you had this calm sea?
- Shackleton: “Yes, decidedly so”.
- A.G: Although it was a clear night?
- Shackleton:”Yes.”

Ask important HF questions like: Does man and computer work as a team/designed as a team? Apollo 11 about to land on the moon 1969 one man’s story

- “ As the vehicle approached the target, one of the astronauts, Buzz Aldrin I believe, announced that the on-board computer just displayed a 1202 alarm.
- They were confused by the alarm and appealed to the Houston controllers for help.
- The computer alarms were buried deep within the executive software and really weren't meant for user recognition…..
- We could not figure out, in real time, the immediate danger, the consequences for the mission, nor how in the world such a remote alarm could have been caused in the first place. I had never seen one or heard of one in all of our pre-flight testing.”

Apollo 11 cont…The man-computer team

The man: “We worked all night and time was running short. I remember bumping into one of our M.I.T. engineers. He asked "the Switch isn't on, is it?" "Why would it be on for Descent, it's meant for Ascent?" ... yikes!!!, the bit was ON. Why was it on? It had to be set in that position by an astronaut. We looked at the 4 inch thick book of astronaut procedures and there it was -- *they were supposed to put in on* (in the AUTO position) prior to Descent.”

So…??
“The computer: had been looking for radar data” (which it couldn’t find)

The man and the computer: “If the astronauts were trained this way, why had this effort never shown during training sessions?
I later found out that *such training was for procedures only and the Switch was never connected to a real computer*.”

Luckily the computer system was well designed:
“Had we demanded computer time for every scheduled task, then time would have run out, tasks would have overlapped, data would be confused and out of sync, and the flight would have been lost.”

Recently…

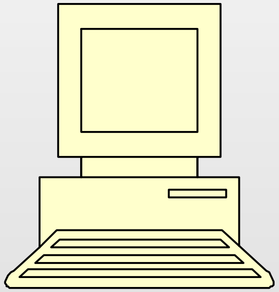
- On a top tier Seveso site:
  - 3700 alarms went off in the control room without any prioritisation (the initiator occurred during start-up).
  - A video link to the equipment which had failed was not looked at by operators for 20 minutes
  - By this time a big cloud of flammable gas was floating over the site.

Haven’t we learnt any basic principles?

Safety Critical Information should be…

- □ attention grabbing
- □ complete but only what is needed
- □ grouped together for the task
- □ not violating operators’ expectations
- □ reliable
- □ accurate
- □ within capacities of the operator

Company human factors and control room philosophy and standards (do they exist?)



- □ Centralised or local HF standards
- □ Control room philosophy
- □ Recording of design decisions and reasons
- □ Reviewing <u>for safety </u>(eg. Use foreseeable and unusual scenarios)
- □ Review of the overall management system for Human Factors (of CRs)
  - Standards
  - Implement
  - Monitor
  - Review
  - *<u>Improve</u>*

Conclusion: Safety Management System needed

- The SMS should include
  - □ reviewing lessons from the history of own and similar plants
  - □ monitoring the reviewing
  - □ striving to avoid repetition of accidents
  - □ monitoring the striving
  - □ follow-up/adjustment
  - □ monitoring the adjustments