SAFETY NEWSLETTER

No. 109

SOME ACCIDENTS CAUSED BY SIMPLE MISTAKES

The information in the following pages — some of which has appeared in earlier Newsletters — is based on the discussions held at Wilton from October 1977 to March 1978. Nearly every week a group of managers and engineers from the Design and Production Departments discussed the incidents and made the recommendations which follow. This Newsletter is therefore a record of those discussions and a reminder or souvenir for those who were present.

If you attended one of the discussions, may I remind you that the recommendations are **yours** , not mine (though I agree with them) and that it is up to you to see that they are followed, where appropriate, on the plants that you operate, maintain or design.

If you see the Newsletter on circulation but would like your own copy of this issue please let us know.

Other accidents, similar to those described, appeared in Newsletters 108/8, 1 03/3, 98/6, 97/3, 96/7, 93/4, 86, 74/3 and 66/3.

TREVOR A KLETZ

Division Safety Adviser

Petrochemicals Division Headquarters

March 1978

IMPERIAL CHEMICAL INDUSTRIES LIMITED

PETROCHEMICALS DIVISION

SOME ACCIDENTS CAUSED BY SIMPLE MISTAKES

“Man is a creature made at the end of the week …. when God was tired.”

Mark Twain

“I haven’t got a memory, only a forgettory.”

Small boy quoted on “Tuesday Call”,

BBC Radio 4, 6 December 1977

“I do feel we are rather too ready to relieve the operator of all responsibility. We seem to be developing a system of design whereby if the operator can conceivably get it wrong, then the design is unacceptable. These are not the conditions to encourage the design of the most economic, efficient and productive plant.”

A design engineer

“The Factories Acts would be quite unnecessary if all factory owners were to employ only those persons who were never stupid, careless, unreasonable or disobedient or never had moments of clumsiness, forgetfulness or aberration. Humanity was not made up of sweetly reasonable men; hence the necessity for legislation with the benevolent aim of enforcing precautions to prevent avoidable dangers in the interests of those subjected to risk (including those who do not help themselves by taking care not to be injured).”

Lord Pearce, in the Court of Appeal, quoted in the Financial Times, June 1 965.

“A person is not, of course, bound to anticipate folly in all its forms, but he is not entitled to put out of consideration the teachings of experience as to the forms those follies commonly take.”

A House of Lords 1 949 judgement, quoted in The Guardian, 7 February 1 966.

1 AN EXPLOSION WHILE FILLING A PLANT WITH OIL

What Happened?

Figure 1 shows a plant in which coke is made from hot oil. Light ends are removed in the dephlegmator and the bottoms recycled.

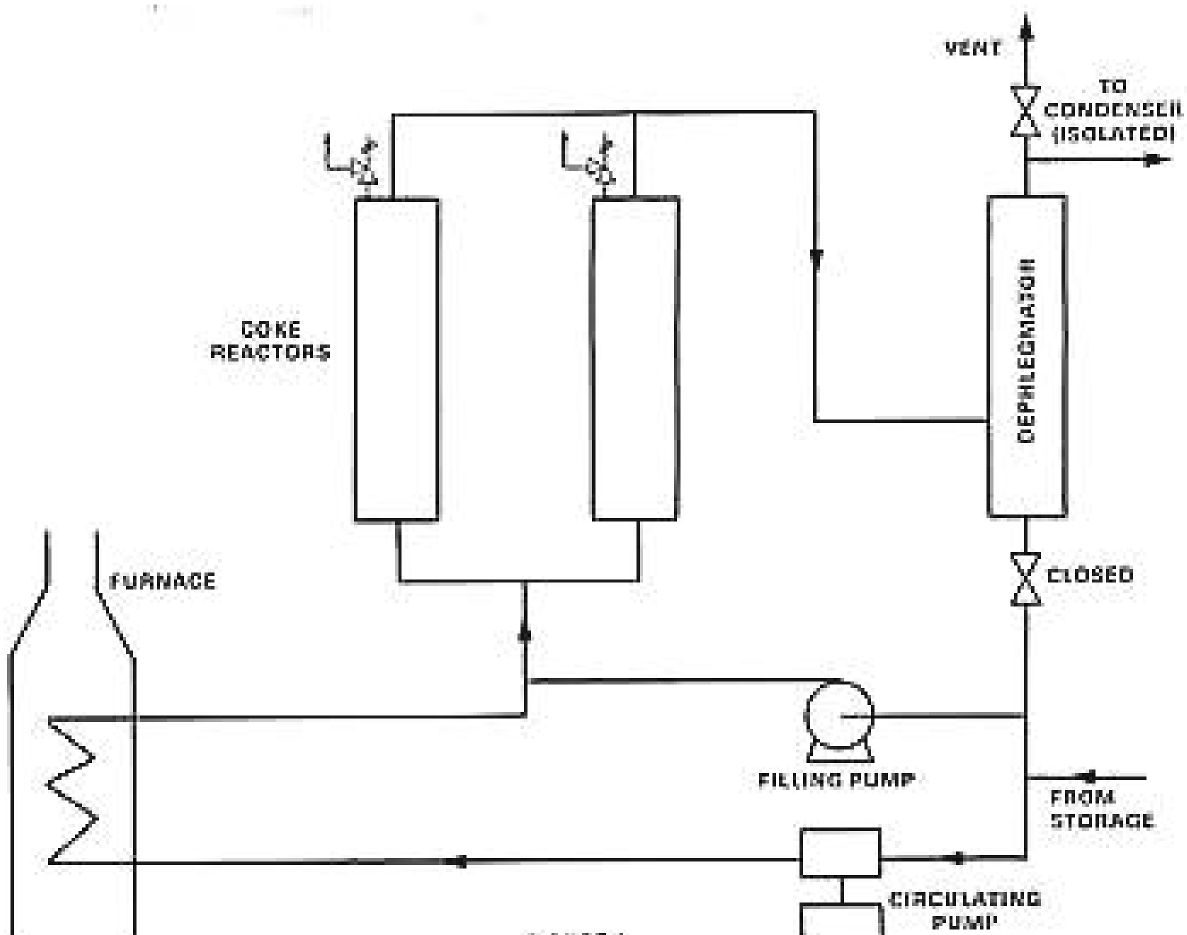


FIGURE 1

The unit is shut down every few days to remove the coke and afterwards it is filled with oil using the centrifugal filling pump as well as the positive displacement circulating pump. The vent is left open to expel air and closed when the oil overflows.

One night, soon after filling had started, the pressure on the delivery of the circulating pump was 90 psig, which was higher than usual. The operators decided that this was probably due to viscous oil, as it was a very cold night, and lit the furnace at a low rate. This had been done before.

However, the pressure did not fall and several hours later it reached 130 psig. The operators now realised that their theory might not be correct. Perhaps the previous shift had forgotten to open the vent valve. They went up to see and found it shut and too stiff to open. They came down to find a wheel-dog and, while they were looking, an explosion occurred. The top section of the dephlegmator landed in a field next to the plant and one of the operators was killed. During the last half-hour before the explosion, the pump delivery pressure had risen rapidly to 300 psig.

Why Did it Happen?

1 The immediate cause of the explosion was a diesel engine effect in the dephlegmator. The rising level of oil had compressed the air and oil vapour until the auto-ignition temperature was reached.

The plant was not swept out with nitrogen as the oil had a flashpoint above atmospheric temperature.

Lighting the furnace was wrong as it meant that warm oil was being pumped into a vessel containing air. However, the explosion could still have occurred if the oil had been cold. It would merely have taken a little longer.

2 In another sense the cause of the explosion was the operator forgetting to open the vent valve. This was not due to lack of knowledge, training or instructions. It was the sort of slip that we all make from time to time. If we had carried out an operability study we would have foreseen that the vent valve might be left shut, but would we have foreseen the diesel effect? We might have said that leaving the valve shut would not have been dangerous as it would merely result in a relief valve lifting.

On this and another similar unit there had been 6000 successful start-ups. What would the manager have said if someone had suggested, before the explosion, that the start-up procedure was unsafe?

We cannot say that a method is safe because it has been used 6000 times, unless we accept that an explosion on the 6001st occasion is acceptable.

Perhaps the valve had been left shut before but this was found out in time.

3 The explosion was due to a failure to heed warning signs. The high pump pressure gave an early warning but the operators had another theory to explain it — viscous oil. They stuck to their theory until the evidence against it was overwhelming (Don’t we all?).

The centrifugal filling pump had to be shut down as it was running hot. The operators assumed it was faulty. In fact it could not pump against the higher pressure developed by the positive circulation pump. How often do we say equipment is faulty instead of looking for faults in the process?

4 The explosion would not have occurred if the operators had stopped filling when the pressure reached 130 psi_9 or when they found the vent valve shut. It is hard to blame them. When we find shut a valve that should be open, the natural reaction is to carry on and get it open as soon as possible.

What Should We Do?

It is not sufficient to tell the operator to be more careful. An occasional mistake is inevitable. As the consequences are serious, a change in the design or method of operation is necessary. Some device is therefore needed to prevent the plant being filled with the vent shut — or at least to make it less likely. There are several ways of doing this:-

(a) The vent valve and filling pump could be interlocked, or

(b) The filling pump only could be used for filling and the delivery valves on the two pumps interlocked so that only one is on line at a time. (A way must be found to remove air from the furnace)

or

(c) A warning light on the panel could show the position of the vent valve.

It is doubtful if a check-list would have helped. The start-up was done so often that operators knew the procedure by heart and would not use the list.

Can you think of other locations where failure to open a valve can have such serious consequences? If so, what precautions do you take?

For more information see “Fire Protection Manual for Hydrocarbon Processing Plants”, edited by C H Vervalin, Gulf Publishing Co, 2nd Edition, 1973, p 66.

2 AN EXPLOSION IN A BATCH REACTOR

What happened?

Figure 2 shows a batch reaction system. A batch of glycerol is placed in the reactor and circulated through a heat-exchanger which can act as both a heater and a cooler. Initially it is used as a heater and when the temperature reaches 115°C addition of ethylene oxide is started. The reaction is exothermic and the exchanger is now used as a cooler.

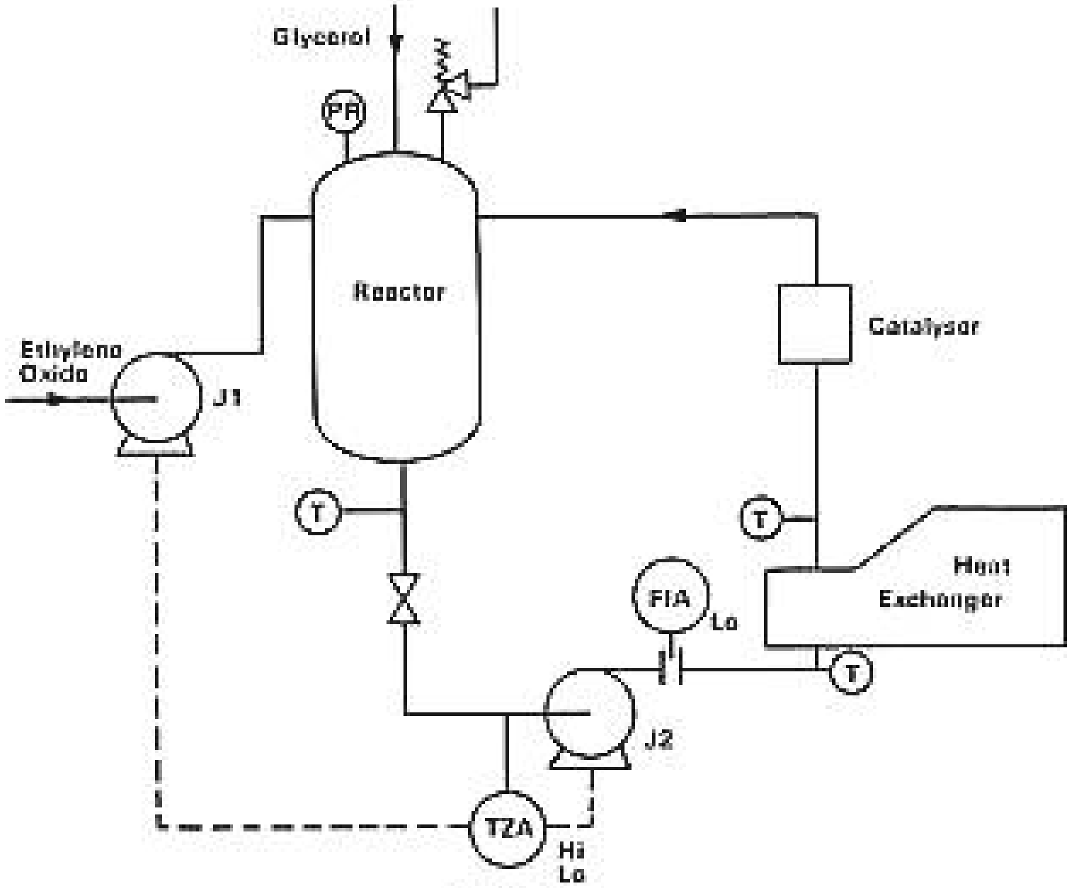


FIGURE 2

The ethylene oxide pump cannot be started unless:-

(a) The circulation pump is running.

(b) The temperature is above 115 °C, as otherwise the ethylene oxide will not react.

(c) The temperature is below 125 °C, as otherwise the reaction is too fast.

Despite these precautions an explosion occurred. One day, when ethylene oxide addition was started, the pressure in the reactor rose. This showed that the ethylene oxide was not reacting. The operator decided that perhaps the temperature point was reading low, perhaps a bit more heat was required to start the reaction, so he adjusted the trip setting and allowed the indicated temperature to rise to 200 °C. Still the pressure did not fall.

He then suspected that his theory might be wrong. Perhaps he had forgotten to open the valve at the base of the reactor? He found it shut and opened it. Three tons of unreacted ethylene oxide, together with the glycerol, passed through the heater and catalyser and a violent uncontrolled reaction occurred. The reactor burst and the escaping gases exploded. Two men were injured; one, 160 m away, was hit by flying debris and the other was blown off the top of a tanker.

The indicated rise in temperature had not been real. Pump J2, running with a closed suction valve, got hot and the heat affected the temperature point which was close to the pump.

Why did it happen?

1 As in the last example, the explosion was due to an operator forgetting to open a valve. It was not due to lack of knowledge, training or instructions, but was another of those errors that even well-trained, well-motivated, capable people make from time to time.

2 If the operator had not opened the valve when he found it shut, the explosion could have been avoided. However, it is hard to blame him. His action was instinctive. What would you do if you found undone something you should have done some time ago? (In the first incident the correct action was to open the valve as soon as possible).

3 As in the last incident, the explosion was due to a failure to heed warning signs. The high pressure in the reactor was an early warning but the operator had another theory to explain it. He stuck to this theory until the evidence against it was overwhelming.

The other temperature points would have helped the operator to diagnose the trouble but he did not look at them. He probably thought that there was no point in doing so, as all the temperature points were bound to read the same.

4 The explosion was due to a failure to measure directly the property we wish to know. The temperature point was not measuring the temperature in the reactor but the temperature near the pump. This got hot as the pump was running with a closed suction valve.

Similarly, the trip initiator on J2 showed that its motor was energized; it did not prove that there was a flow.

5 The explosion occurred because key instruments were not kept in working order. The flow indicator and low flow alarm (FIA) were out-of-order. They often were, and the operators had found that the plant could be operated without them. If there is no flow, they thought, J2 will have stopped and this will stop J1.

6 The operator should not have raised the trip setting, though doing so did not in itself cause the explosion. (However, he did try to use his intelligence and think of a reason why reaction was not occurring. Unfortunately, he was wrong).

What should we do?

It is no use telling the operator to be more careful. We have to recognise that the possibility of a mistake — forgetting to open the valve — is inherent in the woik situation — and if we want to prevent a mistake we must change the work situation, that is, the design and/or the method of operation —the hardware and/or the software.

The original report blamed the operator for the explosion, but his failure to open the valve might have been foreseen.

1 The temperature should be measured in the reactor or as close to it as possible. We should always try to measure the property we wish to know directly, rather than another property from which the property we wish to know can be inferred.

The designers assumed that the temperature near the pump would be the same as that in the reactor. It will not be if there is no circulation.

The designers assumed that if the pump is energised, then liquid is circulating, but this is not always the case.

If you were taking part in an operability study would you have picked up these points?

2 Operators should not be allowed to change trip settings at will. Different temperatures are needed for different batches, but even so the adjustment should be made only by someone who is given written permission to do so.

3 More effort might have been made to keep the flow indicator alarm in working order.

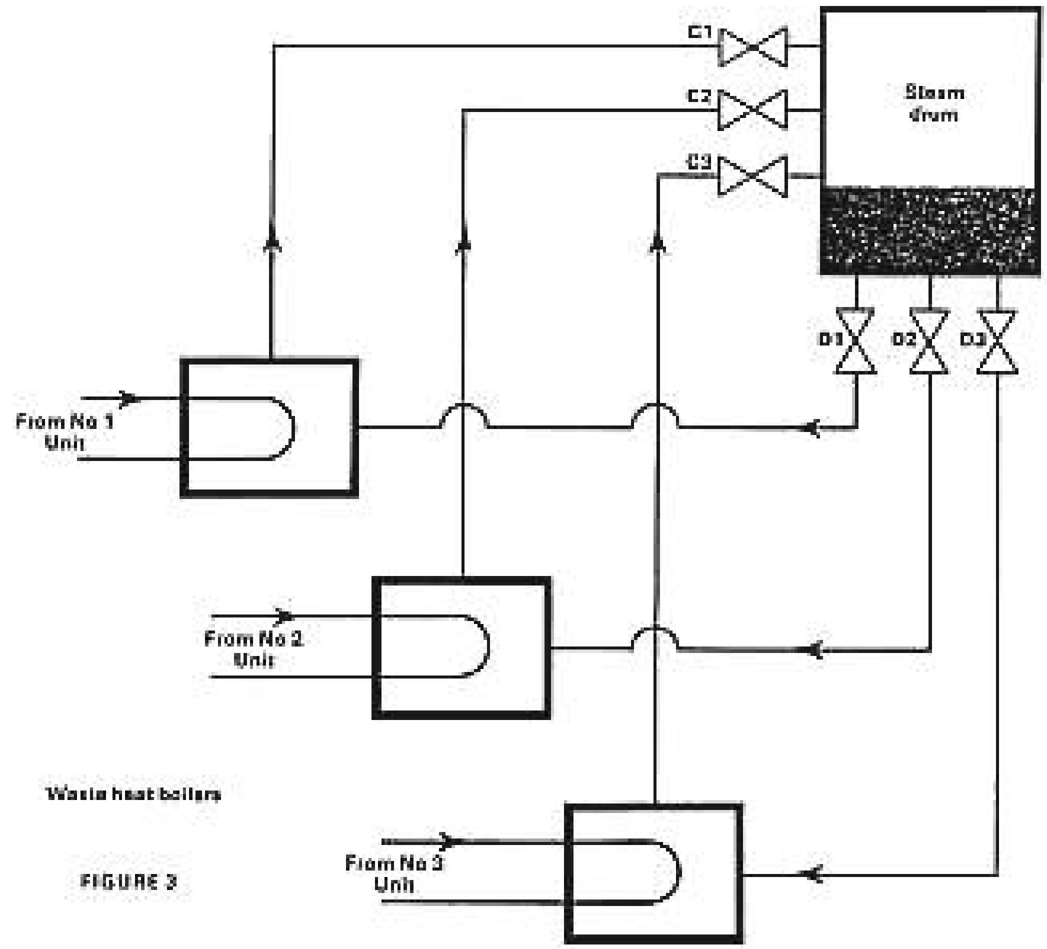
4 A high pressure trip should be installed on the reactor.

5 Operators should be trained to ‘look before they leap” when they find valves wrongly set.

3 DAMAGE TO A WASTE HEAT BOILER

What happened

Figure 3 illustrates a plant in which three waste heat boilers share a common steam drum.



Waste heat boilers

FIGURE 3

No 2 unit had been shut-down while Nos 1 and 3 units continued on line. An operator was asked to close valves C2 and D2 so that No 2 waste heat boiler could be cleaned.

Soon after he had closed the valves the high temperature alarm on No 3 boiler operated. It was then found that the operator had closed valve D3 instead of D2. By the time D3 had been opened the boiler had been overheated and some tubes damaged.

Why did it happen?

1 The damage was due to an operator closing the wrong valve. It was not due to lack of knowledge, training or instructions, but was another of those mistakes that well-trained, well-motivated people make from time to time.

2 There were no labels. This made a mistake more likely.

What should we do?

It is no use telling the operator to be more careful. We have either to accept an occasional mistake or change the work situation.

1 Labelling will make a mistake less likely. However, it is not as easy as it seems. Labels disappear after a while — they get broken or removed when a valve is changed.

Labels should be big and strong and fixed to the pipe rather than the valve and they should be inspected from time to time.

Labels are a sort of protective system and, like all such systems, have a failure rate. If they are never inspected their “fractional dead time” will be high.

2 On a new plant, each boiler could have its own steam drum. This would be expensive but simplicity is sometimes worth paying for. (Are we more willing to spend money on complexity than simplicity?).

3 The boiler valves could be interlocked so that they cannot be closed until the corresponding unit is shut down.

To shut C2 and D2, for example, we would need a key which is also used to open the fuel gas valve to No 2 unit furnace and which cannot be removed until the fuel gas valve is shut.

Would the cost of the interlocks be money well spent? It is unlikely that anyone would be injured by the overheating of the waste heat boiler, so we can compare the cost of the interlocks with the cost of the damage and loss of production.

If Cost of interlocks is < Damage x Probability of occurrence then the interlocks are a good investment.

The costs are known but what is the probability of another mistake?

Valve operations are carried out 135 times per year so, if the operators make one mistake in 1000 operations — quite a low error rate — a waste heat boiler will be damaged every 7 or 8 years. In fact, two mistakes had been made in the 7 years since the plant was started up. If the interlocks prevent one mistake in the next 7 years they will pay for themselves many times over, so they were installed.

4 A RAILWAY ACCIDENT

Many railway accidents have been blamed on human error, for example, Britain's worst railway disaster — at Quintinshill, just north of Gretna Green on the Carlisle-Glasgow line, in 1915. 226 people were killed, most of them soldiers.

Figure 4 shows the layout of the railway lines. (Lines to London are called up lines; lines from London are called down lines).

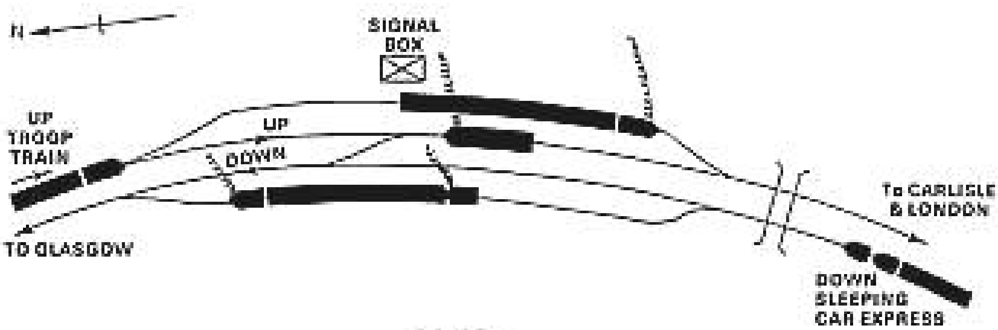


FIGURE 4

The two loop lines were occupied by goods trains and so a slow north-bound passenger train was backed on to the up-line in order to let a sleeping car express come past. The signalman, who had just come on duty, had had a lift from Gretna Green on the slow train and had jumped off the footplate as it was backing on to the up-line. He could see the slow train through the signal box window. Nevertheless, he completely forgot that it was there and accepted a south-bound troop train which ran into the slow train. A minute or so later the north-bound express train ran into the wreckage. The wooden coaches of the troop train caught fire and many of those who survived the first impact were burned to death.

Why did it happen?

1 The accident occurred because the signalman forgot that there was a train on the up line, though he could see it from his window and had just got off it, and accepted another train.

2 A contributory cause was the failure of the signalman who had just gone off duty to inform the signalman in the next signal box that the line was blocked and to put a reminder collar on the signal lever.

One signalman had a lapse of memory — and obviously it was not deliberate.

The other signalman was taking short cuts — omitting to carry out jobs which he may have regarded as unnecessary.

What should we do?

As in the other incidents discussed, there are three ways of preventing similar incidents happening again:

i) Change the hardware

ii) Persuade the operators to be more careful

iii) Accept the occasional accident (perhaps taking action to minimise the consequences).

i) Changing the hardware is, in this case, possible, but expensive. The presence of a train on a line can complete a “track circuit” which prevents the signal being cleared. At the time, track circuiting was just coming into operation and the Inspector who conducted the official enquiry wrote that Quintinshill, because of its simple layout, would be one of the last places where track circuiting would be introduced. It was not, in fact, installed there until the recent electrification of the London-Glasgow line and many main lines are still not track-circuited.

ii) Both signalmen were sent to prison — it was war-time and soldiers had been killed.

It is doubtful if prison, or the threat of it, will prevent anyone forgetting that there is a train outside their signalbox, especially if they have just got off it.

Prison, or the threat of it, might prevent people taking short cuts but a better way is management supervision. Did anyone check that the rules were followed? It would be surprising if the accident occurred on the first occasion on which a collar had been left off or another signalman not informed.

iii) In practice, since prison sentences were probably ineffective, society accepted that sooner or later other similar accidents will occur. They have done, though fortunately with much less serious consequences.

Sometimes accepting an occasional accident is the right solution, though we do not like to admit it. So we tell people to be more careful if the accident is trivial, punish them if the accident is serious and pretend we have done something to prevent the accident recurring. In fact, the accidents arise out of the work situation and, if we cannot accept an occasional accident, we must change the work situation.

Although a similar accident could happen today on the many miles of British Rail track which are not track-circuited, the consequences would be less serious as modern all-steel coaches and modern couplings withstand accidents much better than those in use in 1915.

For more details of the Quintinshill aCcident see “Britain’s Greatest Rail Disaster”, by J A B Hamilton, Allen & Unwin, 1969. Other accidents caused by signalmen’s errors are described in “Railway Accidents of Great Britain and Europe” by A Schneider and A Mase”, David & Charles, 1968 and “Red for Danger” by L T C Rot, Pan Books, 2nd edition, 1968.

5 A PITFALL

Suppose a hole 6 feet deep was dug outside a control room door and the operators were told to step over it.

We would never accept such a situation as we know that sooner or later someone would fall in. We would change the situation by covering the hole.

Are the incidents just described any different? Did not someone leave a trap for the operators into which they fell?

6 AN ANALOGY

A man went into a tailor’s shop for a ready-made suit. He tried on most of the stock, but could not find one to fit. Finally, in exasperation, the tailor said, “I’m sorry sir, you’re the wrong shape”.

Do designers, like the tailor, sometimes expect men to change their (mental) shape to fit the plant, instead of designing plants to fit the bumps of human nature, irritable though these are?

GENERAL CONCLUSIONS

1 Well-trained, well-motivated men, physically and mentally suited to the job they are doing, and properly instructed, make occasional mistakes while carrying out jobs that they have often done before.

2 We should either accept an occasional mistake (when the consequences are unlikely to be serious) or change the work situation. Telling people to be more careful or punishing them will not prevent mistakes of this sort.

3 We can change the work situation by changing the hardware or, sometimes, by changing the way a job is done.

If the consequences of a mistake are serious we may want to design out the possibility of error. On other occasions it may be sufficient to reduce the probability by installing an alarm or introducing a supervisory check.

4 We can often make a rough estimate of the probability of a mistake and this will help us to decide whether to change the work situation or whether to accept an occasional error.

For example, if when an alarm sounds, a man has to go outside and close a valve, most people think that he will forget to do so (or close the wrong valve)

1 in 10 times if he works in a busy control room

1 in 100 times if he works in a quiet control room.

Some more estimates of error rates are given in Safety Note 74/7A.

5 In carrying out operability studies we should not ask if a man will make an error but how often?

6 Men do not make errors in spite of the fact that they are well-trained but because they are well-trained. The operation becomes almost automatic; it is not monitored by the conscious mind and, if for any reason the normal pattern is interrupted, a step may be left out or performed wrongly.

7 All the incidents described occurred on jobs which are carried out frequently. If a job is done once a year it never becomes routine and mistakes of forgetfulness are less likely (though mistakes may occur because of lack of knowledge).

8 Talking over problems helps to solve them as we become more aware of them.

Would it help if you discussed these incidents (or others) with the people you work with?

TREVOR A KLETZ