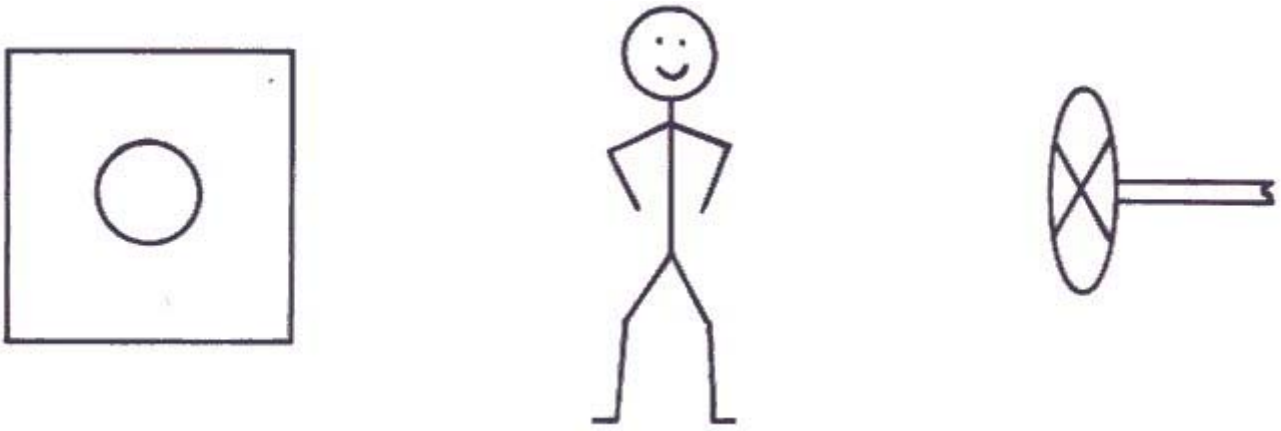
SAFETY NEWSLETTER

No. 123

THE MAN IN THE MIDDLE



123/1 When the alarm sounds, the man is expected to close the valve. Should we assume he will always do so — or should we assume he will never do so?

123/2 If we fit a lot of trips, will we turn operators into zombies?

123/3 Some simple changes in design which will make errors less likely.

123/4 A difference between men and machines.

123/5 How a man fell down a deep hole.

Who's Who in Safety — IRIS

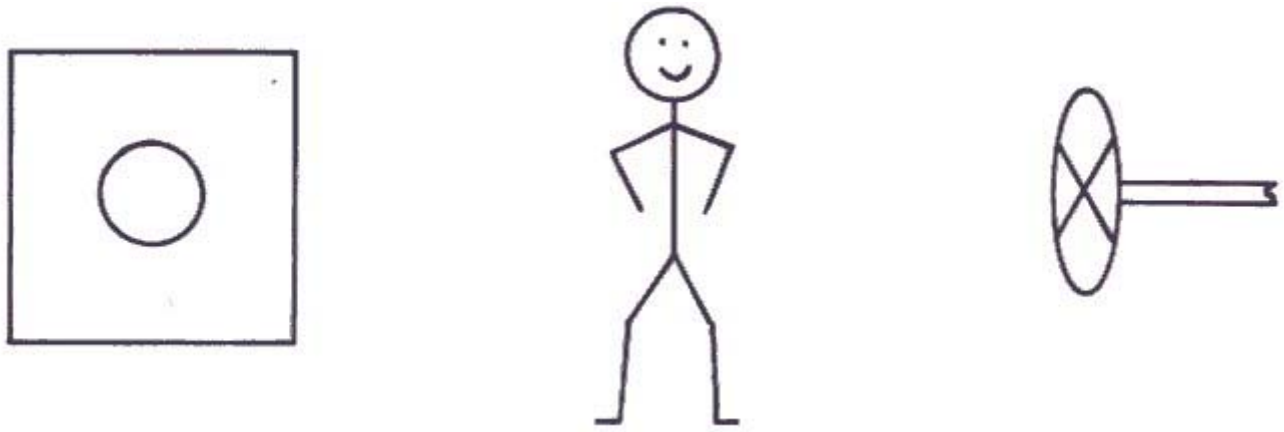
An Engineer's Casebook — Fatigue failure of small branches.

IMPERIAL CHEMICAL INDUSTRIES LIMITED

PETROCHEMICALS DIVISION

We are interested in knowing more about machinery and materials and processes and instruments and the way they work, but perhaps less interested in knowing more about men and the way they work. This Newsletter (like 86 and 109) attempts to redress the balance.

123/1 THE MAN IN THE MIDDLE



The diagram illustrates a common situation on our plants.

When the alarm sounds and lights up, a man is expected to close a valve. For example, the alarm might be a high level alarm on a tank and when it sounds a man is expected to close the tank inlet valve.

We know the reliability of the alarm fairly accurately. If it is tested regularly, and sounds once/year “in anger”, then about every 50th time that it should sound, it will fail to do so. If we are dissatisfied with this performance, it is easy to make the alarm more reliable.

We have a rough idea of the reliability of the valve. We know that on a typical duty turning the handle will not stop the flow about once in 50 years, though the figure will vary a good deal between different duties. Again, if we are not satisfied we can, at a cost, improve the reliability.

What about the man in the middle? How reliable is he? In the past our views have swung between two extremes.

At times we have assumed that he would always do what he was expected, and if he did not he ought to be reprimanded, or at least given extra training.

At other times we have assumed that he could not be relied on and that we ought to have an automatic system: The rise in tank level should close the inlet valve automatically.

Both these views are equally unscientific. What we should say is, “How often will the man close the valve?”

Before we try to answer this question, let us list some of the reasons why the man may fail to close the valve when the alarm sounds.

1 Lack of training or instructions — he may not know what to do.

2 Lack of physical or mental ability — the valve may be too stiff or out of reach or he may be unable to understand his instructions.

3 Lack of motivation — he may not appreciate the importance of closing the valve or cannot be bothered to do so.

Let us suppose that we have eliminated all these causes of failure by suitable training, instructions, design and so on. The man knows what he should do when the alarm sounds and is willing to do it and capable of doing it. Will he always do it?

The answer is No, as there is a fourth reason for failure which is harder to remove: Particularly if people are busy or under stress or if they are distracted by other people, they will occasionally forget to carry out a routine task or carry it out wrongly — they may forget to close the valve or close the wrong valve. How often?

We usually assume the following when designing our plants:

(a) If rapid and complex actions by an operator are necessary to avoid a serious incident, such as an explosion, his failure rate may be high and we prefer not to rely on the operator but to install a fully automatic system.

(b) In a busy control room we assume that perhaps once in ten times a man will fail to close the valve within, say, 10 minutes or will close the wrong valve. This seems a high failure rate but remember that other alarms may be sounding and the operator has to decide which to deal with first, the phone may be ringing, people may be demanding permits-to-work, and so on. If the operator knows that responding to a particular alarm is very important he will be more reliable, but not all alarms can be labelled “Important”.

(c) In a quiet control room we assume that a man will fail to close the valve, or close the wrong valve once in a hundred times. In other cases we choose a value between one in 10 and one in 100.

(d) If, when an alarm sounds, a man has to press a button next to it, his failure rate will be lower than if he has to go outside and select the right valve out of many. Even in this simple case there may be occasional failures, but perhaps as infrequent as one in 1000.

Safety Note 74/7A (available on request), gives some more information on human failure rates.

You may not agree with the figures I have quoted and your own estimates may be better. The point I want to make is that we should never say, “A man always will” or “A man never will”, but we should ask ourselves, “How often will an average man do what we expect him to do?” (We do not say, “Steel always corrodes” or “Steel never corrodes”, we ask “How much will it corrode on this duty?” and design accordingly. Our data on human reliability is as good as our data on corrosion).

Designers should not assume that men are fools. Neither should they assume that men never make errors. They should assume that they continue to behave as men have behaved in the past. It is easier to change plants than human nature.

Men are actually very reliable but in a normal day’s work a man has hundreds, sometimes thousands, of opportunities for error so it is not surprising that mistakes are occasionally made.

Earlier Newsletters (109, 86, 108/8, 103/3, 98/6, 97/3, 96/7, 93/4,74/3 and 66/3) have described many accidents which occurred because men forgot to close or open a valve, or closed or opened the wrong valve or made a similar slip. These accidents arose as a result of the work situation and could not be prevented merely by telling men to be more careful. We should either change the work situation or accept an occasional mistake.

How does this view of human reliability affect personal responsibility? Each of us tries to make as few mistakes as possible, but when attempting to forecast the behaviour of a group of people we have to assume that mistakes are possible. To quote B Inglis,

"Personal responsibility is a noble ideal, a necessary individual aim, but it is no use basing social expectations on it, they wi//prove to be illusions".

From "Private Conscience — Public Morality", Deutsch, 1964, p 138.

123/2 SOME QUESTIONS I AM OFTEN ASKED No 37

IF WE INSTALL A LOT OF AUTOMATIC TRIPS AND CONTROLS ON OUR PLANTS, WILL WE TURN OPERATORS INTO ZOMBIES?

No. First, operators have still got plenty to do even though some actions take place automatically. Second, automatic equipment is rarely 100% automatic and requires more skilful supervision by the operator than manual controls.

When should we use men and when should we use automatic equipment?

We should employ machines to do what machines do best and men to do what men do best.

Machines are better than men at control, for example at adjusting a steam flow in order to keep a temperature constant.

Machines are better than men at taking rapid, accurate action in an emergency, provided the action required can be prescribed in advance. For example, machines are usually better if a valve has to be closed when a level or temperature reaches a dangerous level.

Men are better than machines when judgement has to be used. If the high level has several possible causes, and the action to be taken is different in every case, the best system is to install an alarm and let the operator decide what to do. But operators need a little time. If the operators do not have time to think, decide and act, and automatic action is impossible, then there is something wrong with the system — we have an accident waiting to happen.

When a plant approaches a dangerous condition, we usually assume that 9 times out of 10 the operator will spot the dangerous condition and take action and that only on about one occasion in 10 will the trip have to operate. Sometimes the operator notices a change in the readings; sometimes an alarm warns him that the trip condition is being approached.

Suppose a high temperature or pressure is caused by a controller failing. Then typical figures might be:-

Controller fails	**Readings change or alarm sounds and operator takes action**	**Trip operates**
Once in 2 years	9 times out of 10	Once in 20 years

We say that the demand rate on the operator is once in 2 years and the demand rate on the trip is once in 20 years.

Of course, this is just an example. Some controllers fail more often; some demands occur for other reasons

123/3 SOME SIMPLE CHANGES IN DESIGN WHICH WILL MAKE ERROR LESS LIKELY

We can often reduce the probability of human failure by simple changes in design. Here are some examples:

(a) Another Division decided to fit a small disc to every ladder, giving the date on which it is due for inspection. They decided to fit the discs to the top rungs.

Someone suggested that the discs should be fixed to the sixth rung from the bottom, so that they will be at eye level and more easily seen.

(b) On a nuclear power station, two similar levers in the centre of the panel had quite different functions; operation of the wrong one could be serious.

An operator jammed a beer can over one of the levers. The two levers now look and feel different and are less likely to be confused.

The operator who put the beer can over the lever knew more about human reliability than the designer of the panel.

Should we employ experts in human factors to help us design plants so that errors are less likely?

(c) Early railway engines often blew up because the driver screwed down the safety valve on the boiler. As early as 1829 the Liverpool and Manchester railway laid down:

'There must be two safety valves, one of which must be completely out of reach or control of the engine-man

123/4 A DIFFERENCE BETWEEN MEN AND MACHINES

If a machine or an instrument is not as reliable as we would like it to be, then we duplicate it. For example, suppose that when a pressure or a level reaches a pre-set value it has to operate a trip. Suppose that the trip fails to operate when required on one occasion in 100, and that this is considered to be too often. We might then install two trips and if they are really independent they will fail to operate when required once in 10,000 occasions. (It is not really quite as simple as this and the true figure is usually rather more frequent). This duplication of equipment to ensure reliability is called redundancy. It might be thought that the same principles would apply with men. If a man fails to take the correct action once in 100 times, can we reduce the failure rate to 1 in 10,000 by getting a second man to check him? Unfortunately it never works out like this. The first man knows he is being checked and tends to be less careful, because he knows the checker will pick up his mistakes. The checker knows that the first man is usually reliable and relaxes. Sometimes the failure rate of a man and a checker is actually greater than that of one man alone.

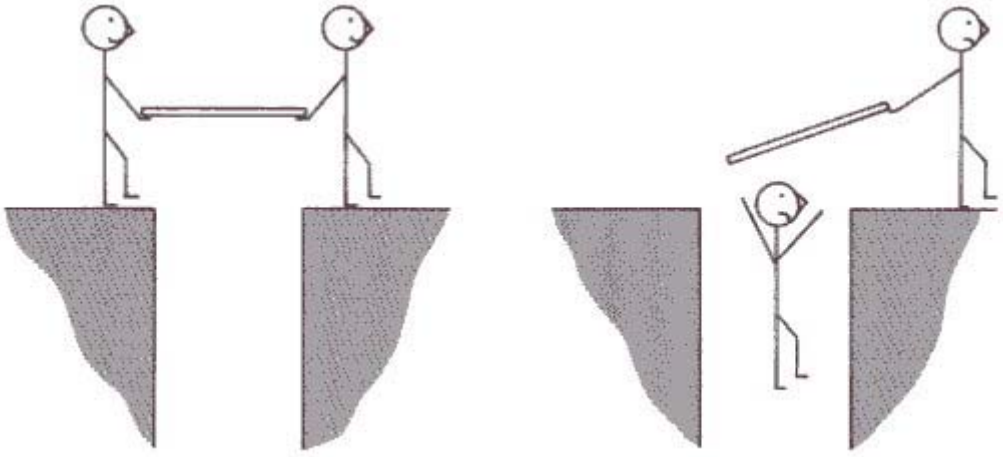
Failures by a "checker" have caused some railway accidents. One of the reasons put forward for providing a second man in the driving cab of a diesel locomotive is to alert the driver to any mistakes that he makes.

A derailment at Dorchester in 1974 was caused by a driver passing a signal at danger. The second man saw the signal when it was 300 yards away and reminded the driver to put the brakes on. The driver did not reply and took no action and the second man did nothing more until the engine actually passed the signal, when he shouted at the driver, but by this time it was too late. (See "Report on the Derailment that occurred on 25th August 1970 at Dorchester West Station", HMSO, 1975).

Many similar incidents have occurred in both the UK and the US.

123/5 UNUSUAL ACCIDENTS NO 86

A supervisor at a nuclear testing area asked two men to remove the sheet of plywood that covered a hole 1,000 feet deep. The two men went to opposite sides of the sheet and bent down to pick it up. One faced the hole and the other had his back to it so that he could hold the sheet behind his back. They picked up the cover and walked forward. The man in front felt the other end of the plywood drop and looking round saw his companion disappearing down the hole.



123/6 A LOOK BACK AT NEWSLETTER 23 (OCTOBER 1970)

"It is not the complete answer to call on design sections to remove the risk by the excellence of their design". This quotation from a letter from Engineering Dept. to a Works is quoted at the front of Report No 0.21,200/B, "Prevention of Loss through Fire, Explosion, and other Accidents: The Part to be Played by Better Training, Auditing, Operating Methods Etc.", available from Division Reports Centres. The report points out that perfect hardware would prevent only half our fires and explosions; to prevent the other half we need better "software". The action taken in recent years or recommended to improve the software is described.

123/7 RECENT PUBLICATIONS

(a) Report No PC.21,,877/B contains the papers and discussion at a symposium on simpler plants (See Newsletter 117/1) and includes many comments on operator reliability.

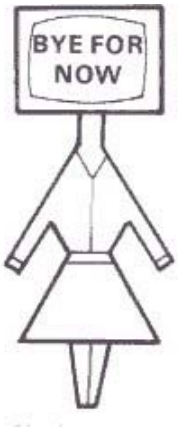
(b) In his inaugural lecture, "Too Important to be Left to the Engineer", Richard Booth, Professor of Safety and Hygiene at the University of Aston, comments that "Engineers lack knowledge of human behaviour" and suggests that they "should be required to have a greater knowledge of the limitations of human reliability" (Occupational Safety and Health, April 1979, p 10).

(c) National Centre of Systems Reliability Report No NCSR R1 7 by B K Daniels contains estimates of failure rates in process control computer systems.

For more information on any item in this Newsletter please 'phone ET (Ext. P.2845) or write to her at Wilton. If you do not see this Newsletter regularly and would like your own copy, please ask Mrs. T to add your name to the circulation list.

May 1979

WHO'S WHO IN SAFETY



No 31 — IRIS

IRIS is a young lady who can help you find information on safety (and engineering and business as well). Her full name is Information Retrieval by Interactive Search.

To converse with her all you need is a computer terminal connected to a telephone line. IRIS will type her replies to your questions or display them on a TV screen.

IRIS is very knowledgeable, quick, hardworking and friendly. But she is a bit stupid and so your requests must be very clear. If you ask her for information on "blasts", for example, she may tell you about the blast freezing of peas!

Like all young ladies, IRIS is much more willing to oblige if you take a little trouble to learn how to talk to her. The following notes will help you start. For more information ask SB at Wilton (P.2891) or TF at Millbank (4161).

[The following descrition of an early database is long out-of date. Twenty years after it was written I asked if the data was still available. I was told that the files could not be found and that, if they could be found they could no longer be opened. – Trevor Kletz]

Suppose you are looking for information on fires in air compressors. This is what you should do.

What you say or do	**What IRIS will say**	**Notes**
(After each item you must press the 'Return' button and, on some terminals 'Line Feed' as well).	(She'll add ? when it's your turn to speak).	
Set the terminal to: Half Duplex 30 characters per second Non-parity		
Dial IRIS's telephone		
No (0606) 76758	ICI MOND CICS. ID=	
ZXØ1	DFH 1025 READY	Ø is used to distinguish

		zero from the letter 0
ZAIB	IRIS SEARCH SYSTEM — DATE	
	ENTER PASSWORD	
Enter password	ENTER NAME	Sorry, IRIS will talk only to lCI staff
Enter your name	ADDRESS	
Enter your address	TITLE OF SEARCH (OPTIONAL)	
Enter title	START SEARCH	
LØØ/I/SOURCE=Ø9	SET OO OLOO/I/SOURCE=O9	This limits the search so that it includes (I) only the safety information (Ø9**)**
or LØØ/E/SOURCE=Ø8	SET OO O LOO/E/SOURCE=08	This limits the search so that it excludes (E) the business information (Ø8)
S AIR?	SET 01 62 S AIR	As the first task (SET 01) IRIS was asked to select (S) all items containing AIR as a keyword. The answer is 62 items.
S COMPRESSOR?	SET 02 20 S COMPRESSOR	IRIS knows of 20 items containing COMPRESSOR as a keyword. By adding the ? after COMPRESSOR we ensure that COMPRESSORS is also included. If we asked IRIS for COMPRESS? she would also include COMPRESSED, etc.
S FIRE?	SET O3 2 1O S FIRE	
CO1 AND O2 AND O3	SET O4 3 CO1 AND O2 AND O3	
		We asked IRIS to combine (C) the 3 sets and tell us how many contain the 3 words. The answer is 3 items.
T 04/5/01-03	See below	We asked IRIS to Type (T) set 04 in format 5 (that is, in full) items 01 to 03 (that is, all three items). If we had asked for format 2 we would have got the titles only.
END	ENDOFSEARCH YOU WERE CONNECTED TO IRIS FOR 05.32 MINS	
	BYE FOR NOW	
Press “Control” and D		
Buttons simultaneously		
ZAIB		If no response, you know you are disconnected

Here are the three abstracts that IRIS found for us:

0001
09001344
0777A SAFETY NEWSLETTER 47/9B AND 45/1
SECURITY CODE = A
FIRES AND EXPLOSIONS IN RECIPROCATING AIR COMPRESSORS.
GIVES PRECAUTIONS NECESSARY TO PREVENT FIRE OR EXPLOSION IN AIR COMPRESSORS. REPORT NO. 0.21,425/B DESCRIBES A RECENT FIRE IN DETAIL.

09001415
0777A SAFETY NEWSLETTER 55/2
SECURITY CODE = A
A FILTER IS PLACED BETWEEN A COMPRESSOR AND THE LOW SUCTION PRESSURE TRIP - RESULT, A FIRE.
BEFORE START UP OF A NEW PLANT A TEMPORARY FILTER, LOCATED BETE: EEN A COMPRESSOR AND LOW SUCTION PRESSURE TRIP, WAS INSTALLED. THE FILTER BECAME CHOKED AND AIR WAS SUCKED INTO THE COMPRESSOR THR0UGH LEAKING GLANDS OR JOINTS. THIS CAUSED AN EXPLOSION IN THE COMPRESSED GAS= SEVERAL JOINTS LEAKED AND THE LEAKING GAS CAUGHT FIRE. DURING THE FIRE, PIPES PROTECTED BY “CALCIUM SILICATE= INSULATION SURVIVED BU’1[1] A CONCRETE WALL MADE FROM PEBBLES WAS DAMAGED. LIMESTONE OR “BLAST FURNACE SLAG= WOULD HAVE BEEN BETTER.

0003
09001577
SECURITY CODE=A NEWSLETTER 54/12D
PRECAUTIONS AGAINST FIRES AND EXPLOSIONS IN LUBRICATED RECIPROCATING AIR COMPRESSORS - MACHINE PANEL GUIDANCE NOTE 3 AND REPORT EDN 1342.
NEWSLETTER 45/1 SUMMARISED PRECAUTIONS WHICH SHOULD BE TAKEN TO PREVENT FIRES OR EXPLOSIONS IN AIR COMPRESSORS. THESE PAPERS GIVE MORE DETAILS.

Note that all these abstracts contain the keywords AIR, COMPRESSOR and FIRE but that only two refer to fires on air compressors. We told you that IRIS is not too bright.

For more information you can consult the Safety Newsletters and Reports listed.

IRIS can do other things as well as those illustrated. If you want a lot of abstracts you ask her to print them (PR). She will do so overnight and post them to you. If you cannot find the words and phrases you want, IRIS will read the original abstracts and look for them. This is called a freetext search (F).

At present IRIS has memorised:

241 items on engineering	(Source code 01)
303 items on design procedures	(Source code 06)
114 items on materials handling	(Source code 07)
484 items on business information	(Source code 08)
256 items on safety	(Source code 09)

IRIS does not realise that petrol and gasoline are the same thing. So if you cannot find what you want under petrol, look under gasoline. Similarly, for hose and flex, tanker and tank wagon and so on. But she can be a big help if you ask her nicely.

An Engineer's Casebook

FATIGUE FAILURE OF SMALL BRANCHES

Unscheduled plant shut downs occur from time to time to repair cracked or broken branch connections. ¾ inch and 1 inch branches fitted with a valve on the branch are particularly prone to failure by fatigue even though the pipe wall thickness may be many times that required to withstand the pressure stress. The apparent handsome factor of safety against failure can be illusory under fatigue conditions.

How are the branches fatigued? The usual mechanism is by vibration arising from running machinery though vibration from high velocity gas flow in pipes and through control and let down valves can also give rise to causes of excitation.

The origins of vibration may be conveniently divided into two. Low frequency, high amplitude associated with reciprocating machinery and much higher frequencies related to high speed rotating equipment and/or high velocity gas streams.

Reciprocating compressors give rise to fluctuating pressures and flows in the suction and delivery piping in the immediate vicinity of the machine even if pulsation dampeners are fitted. The resulting reactions at bends and changes of section in the piping system cause the piping to sway to and fro, often with substantial amplitude, at frequencies in the region of 5-10 Hz, the machine speed or twice it. Even the stoutest piping support for the main piping cannot prevent some movement and this can be beneficial in absorbing the energy put into the system in a safe way. Small branches attached to the main pipe should have a reinforced or otherwise strong enough attachment to it so that there is little or no relative movement between the branch and the pipe over each vibration cycle. It may be necessary to clip or fasten small bore piping running from branches at more frequent intervals than the main piping. This should be done in such a way that the small piping does not restrain movement of the main pipe.

High frequency excitation of the order of 50-80 Hz can induce resonant vibration of branch connections whereby high amplitudes of vibration occur when the branch is 'tuned in'. The bandwidth of excitation is usually quite narrow and when outside the resonant frequency there is no problem. Valved branches with no piping connected or pressure gauge points are particularly sensitive to fatigue arising from resonant vibration since they provide virtually no damping. Once in resonance a high vibration amplitude and velocity build up, raising the stress level with consequent risk of a fatigue induced failure.

Small branches in both situations described above should be inspected whilst plant is running for signs of undue excitation and cracking. Branches more likely to be affected by fatigue should be crack detected from time to time.

E H Frank