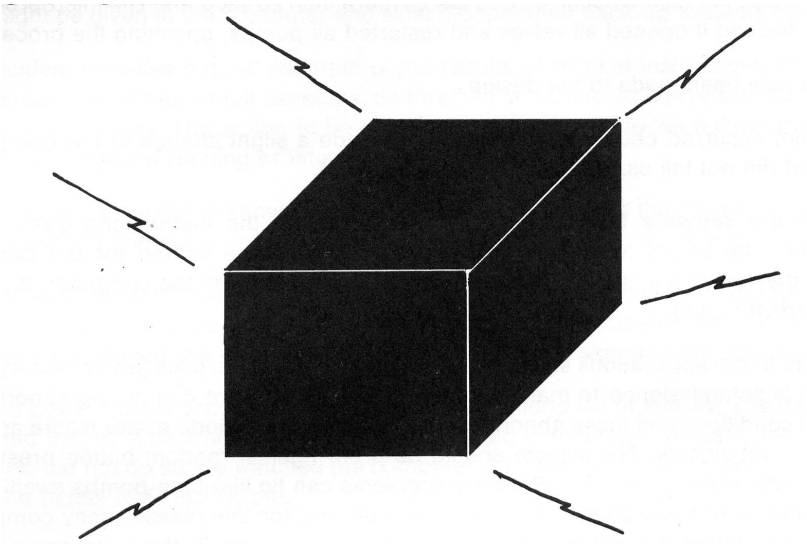
# SAFETY NEWSLETTER

## No. 152
## BLACK BOXES AND ACCIDENT INVESTIGATIONS



**152/1** Some of the hazards of microprocessors

**152/2** An explosion in a pit

**152/3** Sampling — a hazardous task

**152/4** Accident investigation is like peeling an onion — or the dance of the seven veils

**152/5** Operator neglect or design error?

**An Engineer's Casebook — Project specifications**

**This wxxk's safxty mxssagx**

IMPERIAL CHEMICAL INDUSTRIES LIMITED

PETROCHEMICALS DIVISION

## 152/1 BEWARE OF THE BLACK BOX

We try to foresee the hazards introduced by new technology, but we may not foresee them all. If we do not foresee them, at least let us learn from them when they occur.

What hazards have been introduced along with microprocessors and computers?

First, there are **hardware faults**. The equipment may not perform as expected.

For example, on one plant in the Company the microprocessor was supposed to switch off all output signals if a power failure occurred and lasted more than 20 seconds. The microprocessor did not do so. Instead it opened all valves and restarted all pumps, upsetting the process.

Changes have now been made to the design.

Another incident occurred because a manufacturer made a slight change to the design of a component and did not tell us. (See Safety Note 80/11, p4).

Second, there are **software faults**. There may be errors in the instructions given to the microprocessor. The errors may be in the applications software written for the particular application or they may be in the systems software that is bought with the computer: these are usually the hardest to find.

To detect errors in the applications software detailed and meticulous tests are necessary when the equipment is commissioned to make sure it behaves as we want it to during abnormal as well as normal conditions and these abnormal conditions should include power failure and loss of input and output signals. The system should be proof against random button pressing; it should accept only valid commands. Software problems can lie like time-bombs awaiting the correct combination of freak conditions to set them off and for this reason many companies consider that computers are not suitable for trip systems for which they use conventional hardware. For the same reason some companies are reluctant to use computers for front-end (direct digital) control and use them only as supervisory controllers.

To avoid errors in the systems software only well proven systems software from reputable sources should be used.

However the most serious hazards are, I suspect, not the result of faults in the equipment or programme but faults of analysis, **the result of treating the computer as a 'black box'** — something that will do what we want it to do without the need to understand what goes on inside it.

This is illustrated by an incident in a computer-controlled batch reactor in another Company.

The computer was programmed so that, if a fault occurs on the plant, all controlled variables would be left as they were and an alarm sounded. One day the computer received a signal telling it that there was a low oil level in a gearbox. The computer did as it had been told; it sounded an alarm and left the controls as they were.

By coincidence, catalyst had just been added to the reactor and the computer had just started to increase the cooling water flow to the reflux condenser. The flow was therefore kept at a low value. The reactor overheated, the relief valve lifted and the contents of the reactor were discharged to atmosphere.

The operators responded to the alarm by looking for the cause of the low oil level. They established that the level was normal and that the low level signal was false, but by this time the reactor had overheated.

A hazard and operability type study had been done on the plant but those concerned did not understand what went on inside the computer and treated it as a ‘black box’. Clearly what they should have done (and what we should do) is:

Query precisely what the computer will do for **all possible deviations** (back flow, more flow, more temperature, more pressure, less flow, less temperature, loss of power, loss of input or output signal, etc.)

Ask what the consequences will be.

If they are hazardous or prevent efficient operation, consider what alternative instructions might be given to the computer and what independent back-up systems may be required.

The incident provides a good example of the results of blanket instructions (to computers or people) such as “When a fault develops, do this.” All faults should be considered separately, for all operating modes. The action to be taken during start-up may be different from that to be taken during normal running or later in a batch.

As technologists we like to know how things work and like to take things to bits. We must extend this curiosity to computer programmes and not treat them as ‘black boxes’.

The incident just described occurred because the design team did not understand the working of the computer and treated it as a ‘black box’. Other incidents have occurred because **designers misjudged the way operators would handle the signals from the computer.**

When a power failure occurred a computer printed a long list of alarms. The design team had assumed that in such a situation the operator would immediately press a button and trip the plant. He did not do so. He watched the computer print the list of alarms and wondered what to do. (See Safety Note 80/11, p4).

We cannot blame the operator. If we overload any man with too much information, he may do nothing. He probably won’t say, “I don’t know what’s happening, so I’ll assume the worst and shut down”.

Unfortunately computers can easily produce too much information.

**To sum up** — the hazards produced by microprocessors and computers and the ways to avoid them are:

| Fault | Avoiding action |
|---|---|
| Hardware faults<br>Faults in applications software. | Exhaustive testing covering normal and abnormal conditions. |
| Faults in systems software. | Use well-proven systems. |
| Faults in analysis —<br>not understanding what goes on inside the computer. | Ask what the computer will do in all circumstances. |
| Human factors —<br>wrong assumptions about the operator’s actions | A better knowledge of how men react to computers. In time more of this information may be codified in standards. |

Remember: A man can do what you **want** him to do but a computer can do only what you **tell** it to do.

I shall be grateful for information about other incidents involving computers and microprocessors.

*"To err is human. To really foul things up needs a computer"*

## 152/2 AN EXPLOSION IN A PIT

About ten years ago fires and explosions in flare stacks and their drums and in storm water and drainage sumps were quite common in the Division and in the industry as a whole. (See Newsletters 72/3, 69/1, 60/4, 47/5d, 45/6, 40/8, 21/3, 14/5, 10/2, 7/2 & 3, 5/3 and 3/3 and an article by J L Kilby in Chemical Engineering Progress, June 1968, p 49).

Today such explosions are rare, mainly as the result of nitrogen blanketing, but one occurred recently in the Division in a pit which collects drainage from two drums. The explosion was a mild one, lifting the concrete pit cover and damaging some cable trays and their supports. (Newsletters 60/4 and 21/3 described fires in sumps).

The pit was not provided with nitrogen blanketing at the design stage as it was intended to collect water only. Inevitably, however, some oil gets into the pit with the water. The source of ignition was a fault on the pump in the pit — a pin in the drive shaft was displaced and contacted the casing of the shaft in which it was located.

The pit has now been nitrogen blanketed.

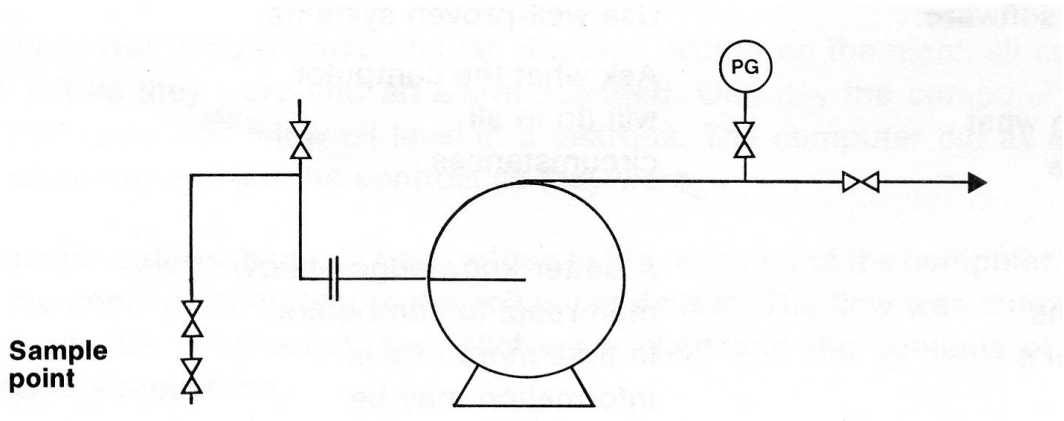
Newsletter 93 (and an article in Loss Prevention, Vol 13, 1980, p1) described a number of serious incidents which were repeated after ten or more years — staff had changed and the earlier incidents had been forgotten. Perhaps it is time to check that your flare stacks, vent stacks and drainage sumps are provided with nitrogen blanketing, that the system is in good order and that the oxygen content is checked continuously or frequently.

An alternative to nitrogen blanketing used on a pit some way from the nearest nitrogen supply is to fit a light cover which will not hurt anyone if it blows off. If you use this system make sure no one can stand on the cover. (See Newsletter 7/2).

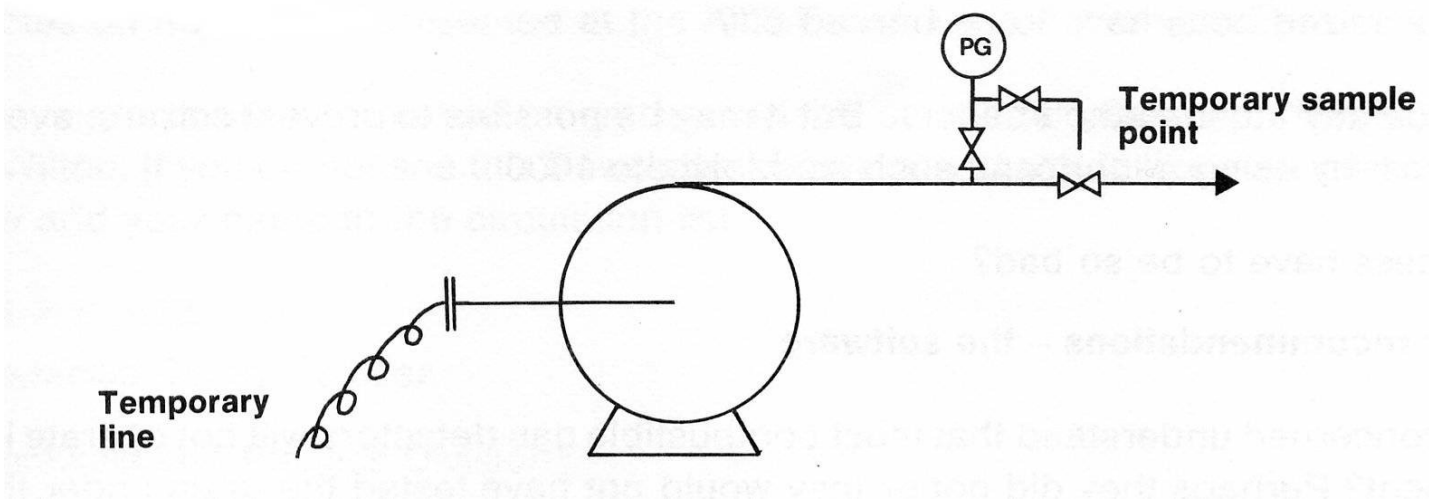
## 152/3 SAMPLING

Sampling used to be a common cause of accidents in ICI and the chemical industry generally. Accidents have been few in recent years as the result of better design of sampling points, but accidents can still occur as the following incident shows.

A pump was fitted with a sample point on its suction line, where the pressure was low.



Because another pump was out-of-use, a temporary line was run to the pump. The sample point could no longer be used so a temporary sample point was fitted to the pressure gauge connection on the delivery line. The valve used was not a fine control valve and was not really suitable for sampling.




When the temporary line was removed, the temporary sample point was left and continued in use. Why? Because the original sample point was choked with rust and no one had reported this.

Finally the operator was splashed while taking a sample.

**Is it time to check your sample points as well as your stacks and sumps?**

Since this item was written a man has received chemical burns to the eyes face and neck while sampling. He was not wearing goggles but the design of the sample point fell far short of the Division Standard (See Specification IN 0578).

**152/4 ACCIDENT INVESTIGATION IS LIKE PEELING AN ONION - OR THE DANCE OF THE SEVEN VEILS**

In a paper in Hydrocarbon Processing, Nov 1979, p 373 I likened accident investigation to peeling onions. I did not mean that it makes us weep (though the way the same accidents recur is enough to make one weep) but that the more we consider the facts, the more recommendations we make.

While the first layer of recommendations is usually concerned with the obvious ways of preventing the accident, the inner layers look at ways of avoiding the hazard and at the weaknesses in the management system. This layered approach is illustrated by a recent small fire in the Division.

While some seized bolts on a pump were being burned off, a spark set alight to a drain about 1 m away. The work area had been surrounded by flameproof sheets and the drain had been covered with a polythene sheet. Either the polythene sheet did not fully cover the drain or the sparks burned a hole in it.

The fire was soon extinguished and there was no damage.

The atmosphere in the drain had been tested with a combustible gas detector before welding started. No gas was detected, possibly because the atmosphere under the sheet was too rich in hydrocarbon and there was not enough air present for the gas detector to work.

**First layer recommendations**

1. Cover drains more thoroughly during welding. Use flameproof sheets and make sure they are sealed round the edges.

2. Test the atmosphere **outside** the sheet. This is more important than the atmosphere below the sheet.

3. As conditions may change during welding use a portable gas detector alarm such as the Dalek, (See Newsletters 36/1, 51/1 and 90, page 13.)

**Second layer recommendations — avoiding the hazard**

Why did the seized bolts have to be burned off?

Access made any other method difficult. But it may be possible to prevent seizure, even at high temperatures, by using a lubricant, such as 'Molycote 1000'.

Did the access have to be so bad?

**Third layer recommendations — the software**

Did those concerned understand that most combustible gas detectors will not operate if there is no air present? Perhaps they did not or they would not have tested the drain under the cover.

The Works instructions call for drains to be covered by flameproof sheets when welding takes place nearby. Over the years everyone had got into the habit of using polythene sheets —cheaper but flammable. Did the managers and supervisors notice this and approve the change? Or did they notice and turn a blind eye? Or did they simply not notice? To prevent the fire it needed only one manager to keep his eyes open, notice that polythene was being used and ask why?

Finally, a more poetic metaphor than peeling an onion is suggested by Danny Abse.

*Below, distant, the roaring courtiers*
*rise to their feet — less shocked than irate.*
*Salome has dropped the seventh veil*
*and they've discovered there are eight.*

## 152/5 OPERATOR NEGLECT OR DESIGN ERROR?

Another Company reports that a large tank, 43 m diameter, was sucked in because the three vents were never cleaned.

The vents were covered with wire mesh, to keep birds out, but a waxy deposit had almost sealed the mesh.

It is not surprising that the vents were never cleaned or inspected because there was no handrail round the roof of the tank and the conical roof had quite a steep slope!

## 152/6 A LOOK BACK AT NEWSLETTER 52 (May 1973)

**A spillage comes to light in an unusual way**

An operator started to fill a road tank wagon with a chemical. He forgot to check that the exit valves were shut and that there was a cap on the exit branch.

Later the operator found the contents running out of the tanker. He closed the exit valves and washed away the spillage. As the loss was small — or so he thought — he did not bother to report it immediately.

The chemical is a good foam-maker and the incident came to light when foam was seen in the river.

## 152/7 UNUSUAL ACCIDENTS No 111

A four year old Worcester boy was knocked unconscious by an electric shock when he stepped onto the metal steps of his parents' caravan. A nest of beetles in an electric box under the caravan had caused a short, making the metal steps live.

*Care in the Home, October 1980, p 9*

## 152/8 RECENT PUBLICATION

Some notes on the papers presented at the AIChE 15th Loss Prevention Symposium

For a copy or for more information on any item in this newsletter please 'phone P.2845 or write to us at Wilton. If you do not see this Newsletter regularly and would like your own copy, please ask us to add your name to the circulation list.

October 1981

**An Engineer's Casebook No 52**
**PROJECT SPECIFICATIONS**

A recurring theme of these Newsletters is the problem of large organisations remembering the lessons of the past. The organisation's 'memory' is widely dispersed, but one useful source is Project Specifications.

The Petrochemicals Division specifications were the subject of a thorough review in 1980. This review was carried out by a team of six engineers of widely differing backgrounds. Their remit was to:

1 Simplify

2 Make the specifications self-consistent and consistent with each other

3 Reduce costs

4 Write specimens where standardisation was not possible

5 Make them instructional rather than discussive

6 Cut out alternatives

and

7 Incorporate our latest experience

The method of working was to allocate several specifications to each engineer who would present his proposals to the whole team in a series of reviews in committee. The number of reviews for each specification ranged from one to eight. Between reviews, the drafts were offered to engineers outside the team for their comments. The approved specifications were then printed and issued.

There is now available an index of project specifications, summarising the main changes that were made and giving the name of the 'lead engineer' during the review. Copies can be obtained from the writer at Olefine Works, Wilton (Extension W.1632).

The specifications themselves can be obtained from Standards section, Chilton House, Billingham.

J M Glanville

**THIS WXXK'S SAFXTY MXSSAGX**

**Xvxn though my typxwritxr is an old modxl it works quitx wxll xxcxpt for onx of thx kxys. I havx wishxd many timxs that it workxd pxrfxctly.**

**Thxrx arx forty-thrxx kxys that opxratx vxry wxll but just onx kxy not working makxs all thx diffxrxncx.**

**Somxtimxs it sxxms to mx that our safxty programmx is likx my typxwritxr — nxarly all thx pxoplx and xquipmxnt arx working propxrly but onx or two may not bx.**

**You may fxxl "I am only onx pxrson, I won't makx a safxty programmx".**

**But it doxs makx a diffxrxncx, bxcausx a safxty programmx, to bx xffxctivx, nxxds thx co-opxration of xvxry pxrson and pixcx of xquipmxnt. Onx pxrmit-to-work madx out incorrxctly, onx trip not txstxd, onx short-cut could causx an accidxnt.**

**So thx nxxt timx you think you arx only onx pxrson and that your xfforts arx not nxxdxd, rxmxmbxr my typxwritxr and say to yoursxlf, "I am a kxy pxrson in our safxty programmx and nxxdxd vxry much.**

**Trxvor Klxtz**

**(With thanks to thx unknown writxr from which this has bxxn adaptxd).**