Part C

BASIC MANAGEMENT SYSTEMS (SMS & EMS)

C 1 Introduction

The Safety and The Environment must have "*Systems*" by which they can be "managed". This is a convoluted statement but in simple terms it means that if there is no management, the safety and environmental controls will disintegrate. This part is an attempt to illustrate some of the Safety (Environment) Management Systems (S/EMS) and how they operate. This Part was put after that on Hazard Identification as it is, almost, a stand-alone which is best dealt with early before the more "*technical items*" are introduced. These "*Systems*" are the "software" part of Defence in Depth. More advanced systems are given in part F which is possibly more appropriate to a Masters Course.

In part A the general principals of HASWA were explained. The change that HASWA introduced was a move from "***prescription***" to "***self-regulation***". In simple terms prior to HASWA (and some of the Regulations set up by the Factories Acts are still in operation) the approach changed from:

> "You will fit guards wherever necessary"
>
> To:
>
> "You will protect your employees – so far as is reasonably practicable".

This was the intent but the Guidance Notes are becoming more and more prescriptive such that there is a drift back to the pre-HASWA approach.

In the older Factories Act there was a requirement to fit handrails on all structures over 6 feet above the ground (1.83 m). So, if it structure was 5 foot 11 inches high (1.80 m) it would not be necessary to fit handrails. HASWA removes the definition of height and leaves the duty on the employee to prove that the protection was appropriate "*so far as was reasonably practicable*". This would indicate that a rail would be required for any height. Likewise a pump coupling installed with a poorly fitted guard might satisfy the spirit of the old Factories Acts but would fail the duty of "*so far as was reasonably practicable*" layed down in HASWA.

Management Systems are central to the Safety Cases required for Major Hazard Processes.

C 2 Systems

The following is a simple approach to what is a complex study and only some of the more common S/EMS are outlined. It would be wrong to differentiate between Safety and Environmental Systems. Many are similar and have only minor differences, for example a release of a toxic material has an impact on both Safety and Environment. The result is that they will only refer to ***Management Systems***.

Annual Appraisals

At first you might think that Appraisals are totally for managing people, this would be a mistake. Consider what can be done within that appraisal. The appraisal is a dialogue where the strengths are praised and areas of weakness are pointed out with suggestions for improvements using **C**ontinuous **P**rofessional **D**evelopment (**CPD**). There is also the opportunity to review the "Skills Matrix" against possible promotions. If the employee is due for promotion is there a need for certain skills to be enhanced and new ones added? In this manner the employee is being groomed for promotion and "hits the ground running!" to use the modern idiom. This is good management and avoids the mistakes that might result from inexperience.

Management of Change (MoC) Procedure or Hardware

Changes are one of the major causes of incidents. The classic example is Flixborough (1974) but equally it was a **change** that created the "steam explosion" at Chernobyl in 1984. (See incident Studies Part H)

The rule is that if the change is not "**like – for - like**" it is a real change and that change has to be managed! This rule may appear to be dogmatic but it has to be so for good reasons. Some years ago the replacement of a valve, which had identical dimensions, but had a slightly different internal construction, resulted in the release of materials and the injury of a Fitter Figure F 13.1 (See also incident Studies Part H). Could this have been predicted? Most definitely YES!

The MoC applies not only to hardware but also equally to procedures and management structures and personnel. Remember what I said about Appraisals. If the new Manager does not have the skills there is the potential for a problem. The MoC must manage the change from the state "A" with the original Manager in place to state "B" with a new Manager in place.

The MoC System will vary between companies and processes. This is outlined later. An assessment form which has been imitated by many companies is shown in Part F. It is historic but to date no-one has devised a better one!

Procedure Change (see Part F later)

Think about a change in a procedure. This could be a Design Guide, which is the record of "best practice based on the experience of the company in that sphere of endeavour", or an Operating Procedure called by different names such as a ***Works General Order*** (WGO), ***Standing Instruction*** (SI) or a ***Permanent Instruction*** (PI). (The names may differ but the Procedure has the same intent.) (Note that there is a slight conflict in the contraction with "Statutory Instruments" and "Standing Instructions") The original procedure probably worked well but in the light of new circumstances or experience it might require to be changed. The approach would be very much as outlined in the introduction.

What requires to be changed?

What are the implications of this change?

Are all of the best people there to review the change?

If the change is an operating procedure the Operations Staff must be in the discussions and of course there will be the need for training. How will it be implemented and verified?

When the new procedure is to be put into place how do you manage the distribution of the new procedures and the removal and destruction of the old procedures?

Is the timing and announcement of the change sufficiently clear?

How do you ensure that ALL old copies are recovered? This is not a silly question as Engineers and Operators have their own copies. There is only one way of ensuring that there are no rogue copies and that is to ensure that the Master Copies are marked with a **RED** stencil. This will copy **BLACK** and will be clearly visible as an illicit copy. This is yet another Management System.

Hardware Change

In the case of a piece of Hardware there is usually a detailed "checklist" (taken from an ICI Safety Newsletter and shown in Part F) which has to be filled in and reviewed by an independent person. In the ultimate the review could become as shown in Part B on "Identification of Hazards". The checklist covers questions that must be answered such as:

What physical changes will take place?

If it is an operating procedure – what changes will be made to the operating parameters –

Flow,
Temperature,
Pressure,
Level
Composition?

What effects might these changes have on?

Corrosion,
Wear,
Reaction kinetics

What might these changes and effects have on?

Pressure Protection (Pressure Relief Valves)
Controls
Instrumented protective systems – Shut Downs - ESD

What impact might the change have on the access to safety equipment or means of escape?

What improvements are required for illumination or maintenance access?

In the case of a hardware change not like-for-like the questions may be as follows:

What internal and external changes will take place?

Can the integrity of the item be violated during maintenance?

Are there any potential traps for fluids?

This listing is only illustrative and is not complete - See Part F for more detail

Following the completion of the check-list it will be reviewed by an independent assessor and the **change** will be accepted, rejected or accepted with conditions, one of which may be that all or part of the **Hazards Study Review** are carried out (see part B).

C 3 Permit to Work (See Part F Advanced Management Systems for more detail and an illustration)

All work that is not routine day to day operations require to be carried out under a Permit to Work (PtW). These have different names in different companies. They could be called a Works Clearance. Whatever the name they are a requirement for "***safe systems of work***" are required by HASWA.

It is appropriate to describe PtW at this point. This Management System requires that the full assessment of the risks is carried out (qualitatively in most cases) and that the appropriate risk reduction features are put into place to reduce the risks ***so far as is reasonably practicable.*** These risk reduction features will be detailed on the Permit with the task to be carried out, the scope and the other conditions that **must** be adhered to.

Essentially it is a written record of the ***HAZARD IDENTIFICATION*** carried out PRIOR to any form of maintenance. For the most part this will be non-quantitative and based on experience. It will record those tasks that require to be done (and those that may not be done) and the tools by which it may be done. It will then record the perceived risks and the precautions required to mitigate those risks. These will include isolation (Design Part D) and personal protective equipment (Part G). Finally there will be a written and signed contract between the operations group and the maintenance group were the equipment is "handed over" from one to the other. At the end it will be handed back under signature once again. The names of this document have changed over the years from "Hand Over Certificate" to "Clearance Certificate" but PtW is far more descriptive.

There are a number of PtWs with reducing risk potential. At the very top is the Entry permit and at the bottom is the Isolation Certificate.

These are:

Entry Permit* - to a Confined Spaces. Risk of fumes, asphyxiation or worse.

Hot Work Permit* – Open Flame. High potential for a fire

Hot Work Permit – Drilling or grinding but spark producing. Low potential for a fire. See also sources of ignition in Part D

Maintenance Permit to Work – Specification of appropriate site preparation (including isolation) and use of Personal Protective Equipment (PPE) (Part G)

Electrical Isolation Permit – Potential for electrocution

Nucleonic Isolation Permit – Potential for nuclear radiation

Isolation Permit (process valves) – Wrong valve may be closed resulting in a process upset

There are other PtWs, which include:

Under-pressure Break-in* - Potential to lose containment

Roof Access Permit – Falling through the roof

Excavation Permit – Potential to dig into underground piping or cables

In general those permits with the highest risk potential (shown as *) are only authorised by the Senior Supervisors or even Managers. In some companies there is a unifying permit which contains sections for all of these activities in other companies they are single permits for each operation and it is obvious that there could be a Permit to Work, an Entry Permit PLUS a Hot Work Permit if a welding repair is required on the inside of a vessel.

Too many incident reports which resulted in fatalities were caused by poor use of Permits. The Epitaphs could have read:

"Did not follow the permit ….."
"Did not have an appropriate permit ….."
"The permit was inadequate"
"He was only an innocent bystander!"

C 4 PIs or SIs or WGOs

PIs, SIs or WGOs (as indicated above) are different names for the same system and cover a whole raft of objectives. At one end they may cover the detailed procedure for plant operation – operating instructions. At the other end they may be simple statement of "Policy" - it is a statement to the effect, "This is what **YOU** should do!" In the final analysis they are the Management Systems put in place for whenever the Manager is not present. Illustrations are to be found in Part F.

Some examples would include:

"All personnel will wear eye protection while still on company property and when outside the office"

"All visitors will be escorted, at all time, by a Company Employee!"

Ultimately there are the detailed and thought out Procedures for operation and also for maintenance.

The following is a tabular approach which is an attempt to illustrate the preparation of a SI, PI, WGO or a Design Guide.

SYSTEM	COULD IT BE DONE PROPERLY?	WAS IT DONE PROPERLY?
Operating Instruction SI/ PI/WGO	**Did it consider and give guidance on the following:** Preplanning 1 Are valves Accessible? 2 Hazard Identification complete?	1 Was the sequence followed – if not why? 2 Was a different parameter or value

	Procedure 1 Hazards that may be encountered 2 Line of Command 3 The line of Communication 4 The Responsibilities of each person in the group 5 The EXACT sequence of events which MUST occur 6 The clear objectives and the "window" of the operation 7 The "abort" condition of the operation 8 Verification of the attainment of the objective	used? 3 Could the valve be accessed easily?
Design Guide	Did it consider: 1 Start up 2 Shut Down 3 Operation 4 Failure of Services 5 Operators well meant but ill-advised operation 6 Were all protective systems specified?	1 Was the HAZOP carried out? 2 Were the operators asked to review the guide?

Ask the two questions – "Could it be done safely?" and "Was it done safely?" to show how far reaching Management Systems can be!

Have you thought out the problem?

Consider:

Design Guides/Codes
Hazard Studies
HAZOP Studies
Operating Instructions
Emergency Procedures
PtW
MoC

Was it carried out correctly?

Do managers carry out "walk-about" tours round the work place be it office or Plant?
Are checks carried out on PtW?
Are operating procedures checked on routine?
Are checks carried out on a design as it is being developed?
Are audits carried out?
Are there rrecording and follow-up systems in place?
Are quality checks carried out?

Trip testing
Performance testing after Maintenance
Environmental checks

All of these a Management Systems!

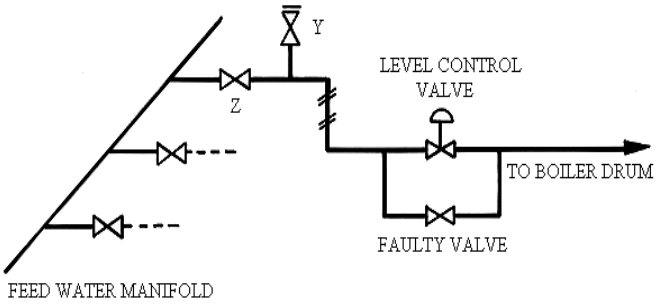
Finally, this is an article written for the IChemE Loss Prevention Bulletin 104 after an incident that occurred Offshore. The article was “sanitised” and was written “incognito” so as to protect the guilty!!

C 5 What is more important - the permit to work or the execution of the plan? Extract from LPB

The incident is used to illustrate and to discuss the significance of this question. It looks at the task, the execution and the potential consequences and then uses this to answer the question.

The Task

The task was to replace a boiler drum level control bypass valve. This valve was welded in. Unfortunately the feed water manifold isolation valve "z" was leaking and some other positive isolation was required (See Figure below).



Sketch of piping isometric of boiler feed system

The Plan

The plan, as devised, was to install an ice plug using a nitrogen bath in a VERTICAL section of pipe line (shown “hatched” above). As a back up the plug would be pressure tested by injecting water at "Y" with valve Z closed so as to achieve a pressure equal to the line rating. After this the level control valve was to be removed and a stopple fitted in the line. With this arrangement there would be a “double block” with one proven isolation.

Execution 1

The execution was not totally according to plan. First the main isolation valve (Z) was leaking so badly that no pressure test could be achieved. Second the stopple could not be installed due to difficulty with access.

Whatever the rights and wrongs the task was completed successfully and the ice plug thawed out. The boiler was put on line and as all the tools were on site it was decided to do the same task on an adjacent boiler drum level control valve bypass.

Execution 2

The piping configuration on the adjacent boiler was different and the only suitable section of piping was oriented horizontally. As a result a different nitrogen bath had to be fitted. Once again the pressure test could not be achieved and the stopple could not be fitted. The plan had now been violated on three accounts but the task had started and no-one thought any more about it.

Early in the execution of this task the Nitrogen Dewar Flask level indicator malfunctioned, however it was decided that the flask could be weighted and thereby the weight of the remaining nitrogen could be determined. As the task proceeded it was evident that a second Dewar flask of liquid nitrogen would have to be used, unfortunately, for some reason, the hose did not fit onto the Flask. (It is possible the coupling on the second flask had been damaged in transit).

At this point the work site was only protected by a single isolation which is only effective as long as the flow of nitrogen was maintained to the nitrogen bath and that flow was not guaranteed.

The inevitable occurred, whether it was due to premature loss of nitrogen or low nitrogen flow matters little, the ice plug blew out and hot feed water sprayed out of the line. The levels in the on-line boilers started to fall and by means of reduced throughput and putting on extra feed pumps, boiler levels were maintained during a controlled shutdown.

Analysis of this Incident

The analysis of this incident illustrates one of the major misunderstandings and application of the Permit to Work system. Too often there is heated debate about the niceties of the layout of the Permit itself. The Permit to Work should be written record of:

1. The Work Planning (including calculations of loads, forces, stresses or other physical engineering limitations).

2. The preparation of the work itself (Isolation, draining, purging etc).

3. The preparation of the work site (sand bagging drains, isolation of local equipment).

4. Limitation of incompatible practices (such as draining flammables during hot work).

5. The exact scope and limitations of the work to be carried out.

6. The exact method and tools to be used to carry out that work.

7. The monitoring and supervision of the work site.

8. The physical protection to be adopted by the person doing the work.

9. The precautions to be adopted by the person doing the work.

10. The possible process and physical hazards associated with the work site.

11. The contingency plans to be adopted should anything untoward develop, including **how** and **when** the work should stop.

12. The agreement in the form of signature, that all parties visited the work site, inspected it and agree that the work will be done as described, without deviation and that all possible precautions have been carried out in order to make the work and the site safe (*sfairp*) for the operation.

Where appropriate this should include testing the tools and associated equipment to ensure they will work as required, when required.

Far too often, steps 1, 4, 7, 11 and particularly 12 are omitted. In this case in question:

1. The plan was not devised properly nor was it followed.

2. The site was poorly supervised and monitored.

3. Contingency plans were not developed and the work should have been aborted on a number of occasions.

4. The equipment had not been tested.

What would have happened if the fluids had been toxic or flammable or corrosive - the consequences could have been quite unthinkable.

What is more important - the permit to work or the execution of the plan? Surely it is the execution of the detailed plan which is embodied in written format in the permit to work.

Postscript

As time has passed it is possible to say that this incident was sanitised, in reality, and it was the failure of a process isolation on an offshore platform and could have resulted in a major loss of life - some three or four years before Piper Alpha. The fluids were **not** boiler feed water but were hydrocarbons. These flooded onto the installation – but did not ignite.