Beating Luck: A breakthrough in Major Accident Hazard Prevention

Konstantia Kalabaliki – ENERGIA Engineering

The Objective of this Paper is to investigate and analyse the cause/s of Major accidents in the Oil and Gas industry, onshore and offshore. There will be an attempt to quantify the factor of "luck" and based on that, propose a structured way forward on how Major Accidents could be prevented.

The paper investigates the reasons behind the fact that there have been numerous major accidents over the years and despite many studies and Lessons Learned, things still go wrong. In reality, "full compliance" is almost non-existent, but, if this is the case, maybe we need to approach operations and process safety of Oil and Gas plants in a different way.

We will reveal the importance of accepting and moving on with long running non-compliance in standards and procedures, with the help of "Bow-tie" and "Swiss Cheese" models.

The result will reveal that it is the non-acceptance of Standards' and Procedures' non-compliance that is the hidden risk for Major Accident Hazards. This way the majority of facilities in the world depend on "competent people", which in essence equates to luck.

Competence may not be the only driver for the person-in-charge to shut down a facility. There is a large phycological factor that has to do with the pressure to continue operations, albeit the flow of cash for the Owner/ Boss. This will always vary from person to person and cannot be quantified. Therefore, we can still have Major Accidents.

The paper presents practical and feasible ways to overcome the "Bad Luck" factor which could lead to Major Accident Hazards for each facility.

Investigating and trying to quantify luck as a component for Major Accident Hazards is definitely a novel way of approaching Process and Operator Safety. This paper may be very interesting for all Operators and their facilities as it will break the taboo of Standard non-compliance, by presenting ways to overcome the Hazards associated with that.

1. Introduction

The paper will investigate current operation practices in Oil and Gas plants and what can be done so that Major Accident Hazards (MAH) will be avoided as far as practicable.

The factor of luck will be introduced and it will be given a definition suited for the Oil and Gas industry. An attempt will be made to quantify luck, by using examples of common causes of Major Accidents.

Moreover, the study will look into individual examples of non-compliance to Standards and Procedures, in order to present easy fixes, which could reduce the chance of Major Accidents.

The study will conclude with a combination of findings involving the use of "Bow-tie" and "Swiss Cheese" models and suggestions on what causes "Bad Luck" and how to beat it with a series of practical steps.

2. Quantifying Luck

2.1 Definition

What is Luck?

According to Oxford Dictionaries "Luck" is: "success or failure apparently brought by chance rather than one's own actions".

Adopting the meaning of "Luck" in the Oil and Gas industry could be: "**safe or unsafe plant operation is brought by chance rather than by controlled means**".

This definition implies that a plant might be operating in a way that appears either "safe" or "unsafe", but since there are no procedures and standards (**controlled means**) clearly followed, its "safe" or "unsafe" status depends on luck.

2.2. Quantification attempt – Eliminating "Bad Luck"

The last few decades, the industry has worked intensively to identify, design, install and operate the "controlled means" that would ensure "safe operation". However, accidents still happen. Some of those accidents that have "Slight", "Minor" or "Moderate"[1] effect, are appropriately recorded within the Operator's premises and most probably the public never learns of them. Some other accidents have "Major" or "Massive" impact and depending where they happen in the world and the spread of the environmental and societal impact, the public might be informed about them or not.

---

[1] Common Terms used by Oil and Gas Operators in their Risk Matrices to identify Consequence Severity.

In the Oil and Gas industry's definition of luck (section 2.1 of this Study), the word "chance" is the one that is very difficult to be quantified. We will therefore attempt to instigate patterns through accident scenarios that have been triggered by similar cause/s.

Ignition of Gas Leak from a Vehicle

Ignition of a gas leak due to the presence of a vehicle in the area of the gas cloud is a relatively common cause of "Minor" to "Major" accident hazards.

We might have a gas leak in an onshore plant and a vehicle might not enter the affected area, detection would shut down the plant and all would be recorded as a minor incident (lucky). Alternatively, the vehicle might pass by the area just after the leak is detected and cause explosion (unlucky).

The chance of a gas leak may be small but the chance of a vehicle igniting the gas cloud may not be small. If any vehicle is inside the premises for half day the chance is actually 50%. Reducing the time of the vehicle inside the premises, would drop the chance significantly: if the vehicle was in the premises only ¼ of the day, the chances of ignition would fall to 25%, this is a significant reduction from the previous case. Eliminating the presence of vehicles for the majority of time of operations would significantly decrease the chance of the gas leak igniting. Also, the use of other measures such as flame arrestors, could also minimise the chances of gas leak ignition.

Leak Detection after Misinterpreting of Transmitter Reading

The misinterpretation of -mainly pressure- transmitter readings have been another common cause of accidents in our industry. Pressure might be rising in a piece of equipment and the failure to take action when reading the transmitter by the operators has caused in a number of cases Major accidents. Subsequently from pressure rise we could have a leak that is detected and isolated (lucky) or we might have a leak that leads to an explosion (unlucky).

In this case the chance that the leak is detected and isolated could be up to 99% if shutdown is activated automatically on detection. In case that the shutdown is manual the chance is significantly reduced due to the Human Factor element. The chance in this case could be anything from 90% to 0%. The 90% comes a common reliability number used for operators. At 0% is the time that there is no timely shutdown. Human factors are recognised as one of the most complex issues causing Major Accident hazards and it is very difficult to quantify them. The Human factors models depend on a large number of factors that will always vary from facility to facility and even shift to shift within a plant.

By looking at the two examples above, we can see that by minimising the factor that can lead you to a MAH (see the vehicle presence or the Human Factor) we can easily say that this would be an ideal method to eliminate the "Bad Luck" i.e. the chances for a MAH.

When reviewing the overall design of a plant, there are a number of barriers that would need to be overcome for a Major Accident to happen. Multiple Failures, especially failure of Hardware Barriers such as detection systems and shutdown systems, are considered highly unlikely and are usually placed in the "Acceptable" or the "ALARP" region.

In fact, the majority of Operators when investigating potential MAH, they do not take into account double jeopardy. Unfortunately, the reality is quite different and there is usually a number of failed barriers before a Major Accident happens.

There is, therefore, a clear omission in the syntax of design methods against Major Accident potential, so they still happen. Furthermore, the actual implementation of the design in reality may not be as ideal as the engineering drawings and documents present it to be.

Eliminating by design the "Bad Luck" is of course an ideal situation, but as we don't live in an ideal world or experiencing an ideal industry, the study will investigate some "real" examples of challenges that operations face, in order to give some guidance on how to deal with situations where Hardware Barriers have failed and the chances for a Major Accident is high.

3. Beating Luck

In this chapter the study will investigate "real life" examples of unnamed oil and gas facilities. Experience shows that the majority of facilities across the globe do not follow design rules and standards to the letter. With time, this omission becomes the norm in the operation of a facility. We will often hear from operators on site:

"This accident is impossible, it can't happen",

"We've never done it this [a certain safe practice/operation] before",

"We have been operating safely and without a lost time incident for a million man-hours".

Unfortunately, this sort of attitude results in operating a plant where an accident is more probable rather than improbable.

Making an Oil and Gas facility strictly follow rules and standards may be difficult as in the majority of the countries around the world the legislation (if any) is not enforced. In order to improve things though and for the benefit of Operator production continuity -without unnecessary fatalities- and protection of the environment, the study will use each of the examples to show that there is a way to recognise and propose immediate and ideally inexpensive fixes which could reduce the likelihood of a Major Accident taking place.

Well pad area

The subject -fully operating- well pad area, consists of a number of Xmas trees connected to temporary piping, on temporary “supports”. Despite temporarily started-up to boost production, the subject wells have been operating in such a condition for over two years.

Although well designed and ordered, the Wellhead Control Panel has not been connected at this stage. In case of fire there is a single manual valve on the Xmas tree. The Sub-Surface Shutdown valve (SSSDV) and Surface Shutdown Valve (SSDV) are not yet connected to the I&C system therefore are not able to be operated).

Well Absolute Open Flow (AOF) is 4500m^3/day. The main river suppling with water half of the country’s population is only a couple of kilometres away.

There is normal vehicle movement and construction in the area. There are hundreds of meters drop on the hole around the Xmas tree area.

Figure 1: Operating well pad area.

Figure 2: Flowlines leading to the main manifold.

Figures 3a and 3b: Pipe supports

This case is one of the most challenging to beat "Bad Luck" due to the large number of inconsistencies observed. The Operator has approved the risk to operate the wells in such a manner in order to boost production. In reality, a simple presentation of the potential risk in case of fire and explosion and furthermore a leak to the nearby river, as well as a basic cost benefit analysis, could actually be enough to persuade the management that maybe such risk is not worth it as it is really pushing its luck and a Major Accident could happen and even escalate to a "Massive" scale.

In case that there is still the need to operate under such conditions:

- The wellhead control panel would need to be connected as soon as possible in order to allow for the SSSDV and SSDV to operate in case of an emergency.
- The pipe supports could be improved locally and without great expense.
- Firefighting means could be made available: i.e. a firefighting vehicle could be on standby constantly during this period of construction. Also, large fire extinguishers could be strategically positioned.
- For the Construction, Site managers should ensure the importance of avoiding, or staying at a distance from the temporarily operating areas.

Simple fixes could improve significantly the chances of something going wrong in this well pad.

Pipeline Line Block Valve (LBV) Station

In this scenario, the study will investigate a pipeline LBV station electricity and housekeeping issues.

The overhead power line which was supposed to be supplying electricity to the LBV station has not been installed. It was therefore essential that alternative means of electrical supply should be seek and as such temporary diesel generators have been placed within the perimeter of the LBV Station.

The Operators Procedure called for minimum distances for the temporary generators. However, the location of the proposed diesel generators – which are in poor maintenance condition-, were a concern to the site team. The team examined the diesel generator sitting between the transformer (not connected) and the Satellite Instrument House (not on line) –see Figure 1. The generator was in close proximity with the topside valves and instrumentation of the pipeline –towards the direction of the prevailing wind (Figure 5).

Figure 4: Current location of temporary power supply diesel generator.

Figure 5: Proximity of temporary power supply diesel generator with pipeline topside valves and instrumentation

The site team unanimously agreed that the diesel generators currently on site were in very poor condition and pose a fire hazard – see Figure 6.

Potential fire could easily spread and damage the adjacent equipment (Transformer and Instrument Satellite House). The Major Accident scenario could be the damage the topside valves and instruments of the pipeline, causing fire and explosion and major oil leak potentially to the local river.

Figure 6: Diesel generator in poor condition.

The LBV the site was also found to be in poor housekeeping condition with no firefighting means available (the only extinguishers on site were damaged and dropped on the ground – see Figure 7

Figure 7: Damaged fire extinguishers /poor housekeeping.

The simple fixes proposed in order to improve the safety of this site were the following:

- The diesel generators should be located outside the perimeter fence (and not adjacent) as there are concerns on their integrity.
- The diesel generators –wherever located should be supplied with 50-100 kg extinguisher with wheels –given the lack of firefighting means in the area.
- Housekeeping should be improved.

These simple fixes could significantly improve the chances of a Major Accident avoidance in this LBV area.

Deluge system

During a deluge test a plug was blown from a deluge valve (Figure 8) causing water to shoot out of the line in high pressure (potentially dangerous to personnel).

Figure 8: Water jet cause by blown plug on Deluge Valve during a Firewater test.

Investigation showed that the deluge valve was fully clogged (Figure 9).

Figure 9: Fully Clogged Deluge Valve (mainly by sea shells)

At the same time a large number of deluge nozzles were also clogged (Figure 10).

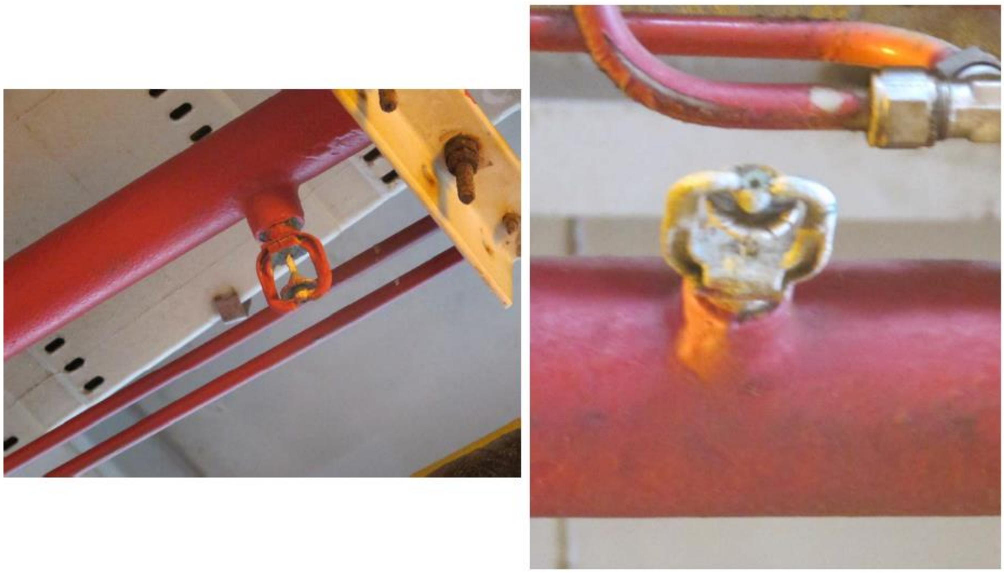

Figure 10: Clogged deluge nozzles (mainly by sea shells)

The deluge test on this offshore platform showed that there was significant ingress of sea debris such as sea shells to the fire water system, proving it not fit-for-service. Further investigation showed that the firewater pumps were temporarily used as utility pumps due to for the permanent utility pumps being under maintenance. However, for such unavailability of Safety Critical Elements (SCE) and subsequently Hardware Barriers, there was no Management of Change procedure produced or signed no permit and many of the operators on the platform were not even aware of such change.

The easy fix was to:

- Accept the non-compliance and produce a plan of action during the maintenance period of the utility pumps.
- Enhance the protection of the platform using nearby firewater/foam monitors and mobile fire extinguishers. This easy fix reduced the chance of complete lack of firewater, due to relying only on the -clogged- deluge system.

- Communicate clearly to the operations team that the deluge system is not available and have competent personnel on stand-by in case of an accident.

In this specific case, as soon as the utility pumps were available, the firewater pump filters were replaced completely and firewater pump performance test was carried out. The system nozzles were removed to flush the system, then cleaned and reinstated. The Hardware Barrier was therefore again in place and “luckily” nothing happened in the meantime. Easy fixes though, would mean that they would not need to increase their chance of not being able to respond to an emergency.

4. Conclusions

The examples presented in this study are just a small representation of the large number of non-compliance in Oil and Gas facilities, causing the unavailability of the facility’s Safety Critical Elements (SCE) and Hardware Barriers (which would prevent or limit the consequences of a major incident).

In many cases there can be an easy fix in order to reduce the chances that would cause a Major Accident.

In reality, the main issue within Operators’ culture is the non-acceptance of Standards’ and Procedures’ non-compliance. The non -acceptance leads to a culture of hidden information and also non-openness to easy fixes, as dealing with easy fixes could “expose” the wider problem.

Furthermore, long term non-acceptance of non-compliance, makes operators non-trusting their system alarms and warnings thinking that they might be erroneous. The false perception of “this can’t happen in this facility” or “such an explosion is impossible”, makes them also psychologically unprepared for an emergency.

At the same time when we are looking at examples of common causes of Major Accident Hazards we recognise that the failed safety barriers, were not identified in safety studies mainly because there is a clear omission in the syntax of design methods, as in the majority of cases double jeopardy is not investigated. Although, this study is not suggesting additional Hardware Barriers, which would add in the cost of the design, it is suggested for all plants to have a basic Swiss Cheese model (Figure 11) created in order for the operators to be able to appreciate that there may be possibility of Major Accident in case of one, two, three or more hardware barrier failures. Ideally, it would be very effective if they are able to add and or remove barriers according to their availability or even a possible non-compliance (Figure 12). Visually removing a safety barrier from a Facility’s Swiss Cheese model could have a more positive phycological effect, as it is recognised and whether compliant or not, it could provide the necessary recognition of the missing element.

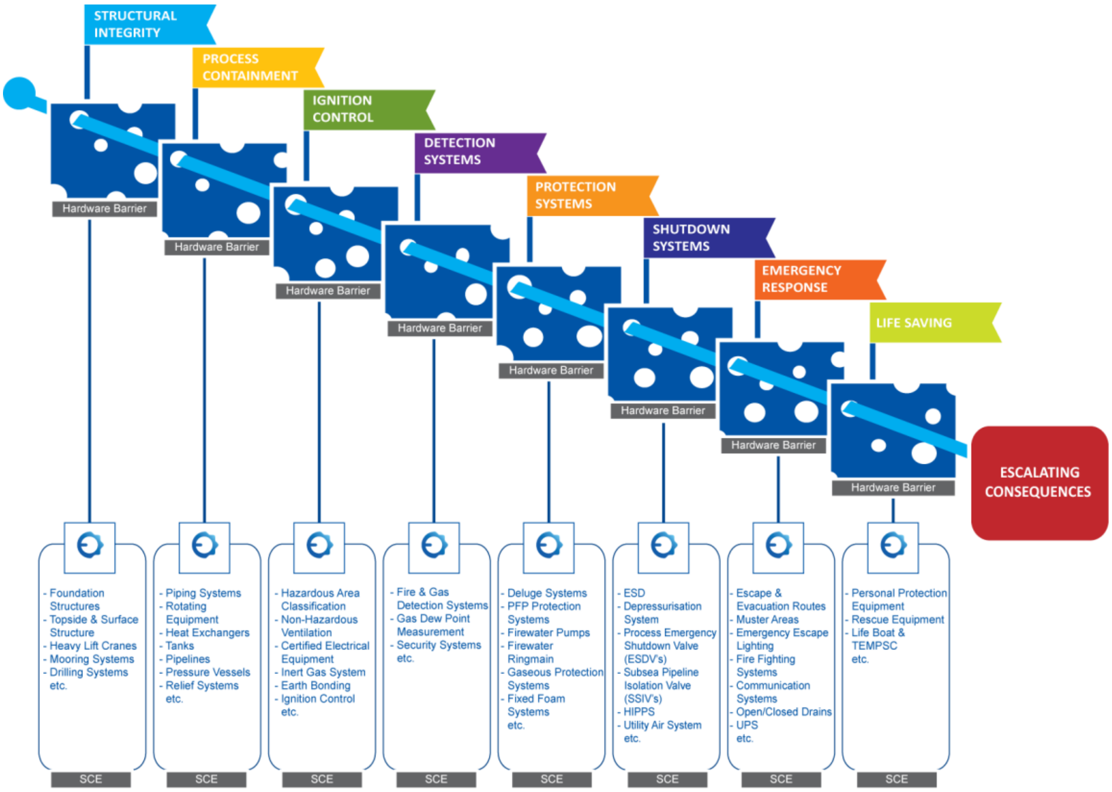

Figure 11: Swiss Cheese model with hardware barriers

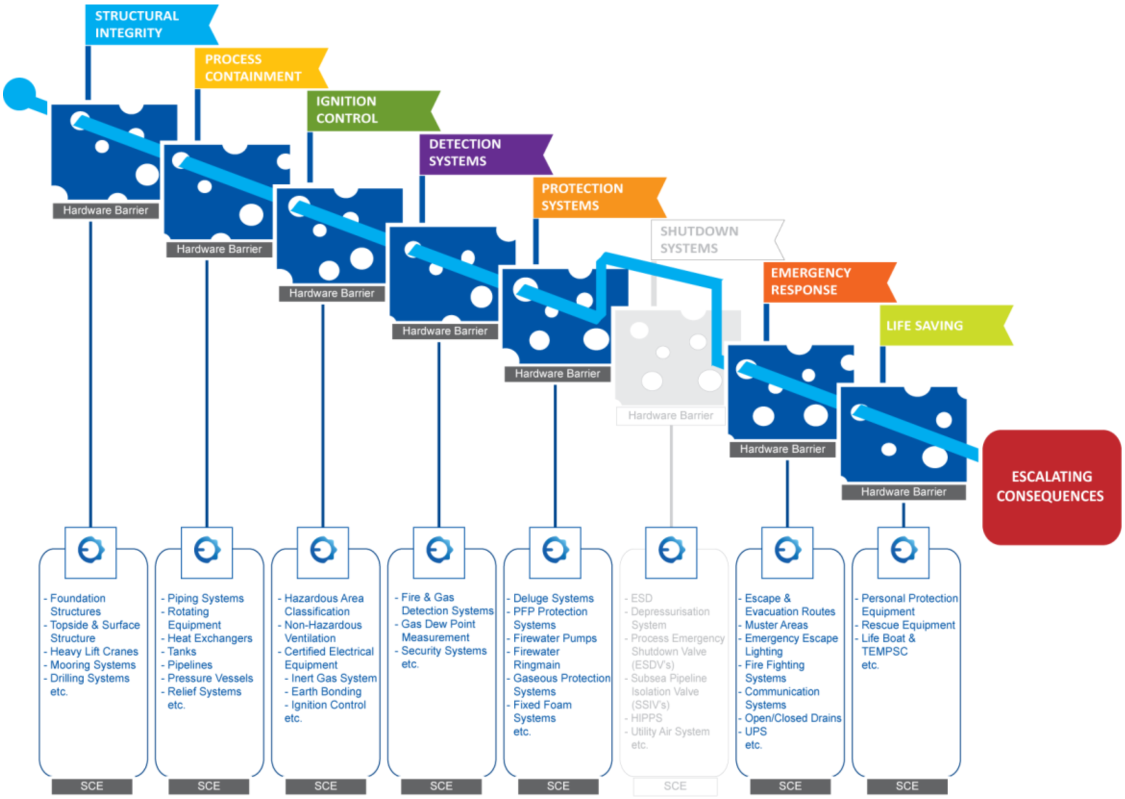

Figure 12: Swiss Cheese model with removed hardware barrier

At the same time, the bow-tie model (Figure 13) could be used as reference when more detail is need on a threats, barriers and consequences of a Top Event (Major Accident).

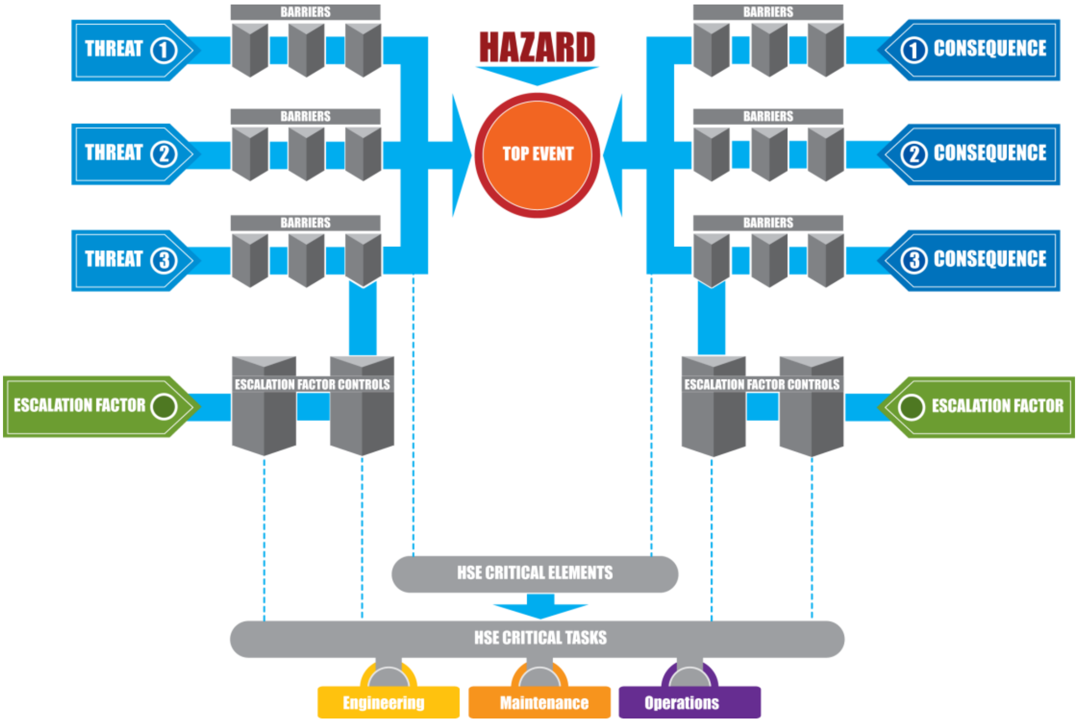

Figure 13: Bow-tie

To conclude, beating “Bad Luck” equates to:

- Mature recognition of Standards’ and Procedures’ non-compliance.
- Easy-fix improvements. Conscious, inexpensive decisions that are documented and shared on each operator shift.
- Phycological recognition factor of any missing safety barriers (with the help of visual removal of SCE and Hardware Barriers). This would subsequently result in overcoming potential misinterpretation of instrument and alarm readings. Furthermore, acting during a Major Accident emergency would be calm and composed.
- The recognition of non-compliance becoming part of the short-term or long-term plans of the improvement of a facility, reducing even further the chances of Major Accidents.

Following those steps, Operators would benefit immensely in terms of reducing their facility overall risk profile, especially when operating in areas where government regulations do not exist or are not enforced.

References

[1] All photos and graphic representations belong to the author and ENERGIA Engineering in-house procedures.