Incident

Small or big changes, not managing them can be risky!

Bureau for Analysis of Industrial Risks and Pollutions (BARPI), France

All industrial activity can be expected to undergo changes, to varying degrees, throughout its life cycle, especially to maintain its efficiency. These changes often come with the development of new processes, an increase in the level of safety, regulatory modifications, etc., and although these factors may contribute to progress, they also represent a risk for the organisations involved. The ARIA database, which has been recording technological accidents in France and abroad since 1992, contains many examples resulting from such situations.

Involuntary changes

Before discussing events stemming from deliberate modifications, we note that some accidents result from unnoticed changes. A deviation, that may occur slowly or quickly, can lead to a different operating mode than expected. This may include undetected changes in the raw materials used such as an increase in the level of impurities that modifies the reaction kinetics, changes in packaging which lead to operational errors, increased flammability of the waste resulting in fires in treatment centres, etc.

The majority of accidents related to unidentified changes involve equipment such as use of supposedly interchangeable parts but which are in fact different and inappropriate (seals, piping elements, mechanical fittings, valves, electric cables, forklifts, pumps, actuators, sensors) or for which the supplier did not report the modification (rupture disc, hose, sensors).

A drop in the personnel's skill level if the installations have been taken over by a new operator, or when a rarely used piece of production line equipment is put back into service, can also generate deviations from procedures which then lead to accidents. Organisational changes may also be the cause, such as self-heating phenomena resulting from extended hold times of a synthetic intermediate over a holiday period, or storage of material in unusual conditions as a result of understaffing. Another example is slow variations in operating parameters which can affect effluent treatment plants during shutdown/restart phases of units or during periods of reduced activity.

Finally, climate change can lead to so-called NaTech events, including flooding of a site not currently considered vulnerable, soil instability due to excess precipitation, etc.

Voluntary changes

Unfortunately, conscious modifications of industrial systems have generated a long list of accidents. The introduction of new raw materials may be the cause of this — for example: decomposition and explosive characteristics which were not taken into account, incomplete reactivity tests (see insert, ARIA 50134), poorly evaluated combustible characteristics, or packaging modifications which induce a change in the material's stability.

Uncontrolled reaction in a synthesis reactor

ARIA 50134 — France, 2013

At a chemical site, a runaway reaction occurred during the production of aluminium orthophosphate by reacting phosphoric acid and aluminium hydroxide (ATH). A technician heard a noise just five minutes after having introduced the ATH into the reactor. Two tonnes of hot reagents were expelled from the reactor.

The thermal runaway was attributed to the use of a more reactive ATH that had been supplied by a new supplier. The facility operator had conducted tests on the new ATH. These tests, however, had focused mainly on the product's granulometry and did not include calorimetric measurements. During production at different concentrations, the technicians had already noticed an increase in the reactivity of this new ATH, although their observations had not been reported. In addition, the operator was unable to locate the risk analysis for this operation given the plant's recent takeover.

The facility operator conducted the risk analysis of its processes and reinforced the operating procedures. The approval procedures for new raw materials were completed. The management of process deviations was also modified. The technicians must evaluate the consequences of all deviations and record them in writing.

Changes in manufacturing processes can also be the source of accidents. Changes in operating parameters, such as temperature, pH alarm thresholds, the nature or stirring rate or concentration of certain reagents may lead to the loss of control of a reaction. Similarly, there are cases of runaway reactions caused by the increase of batch sizes without verification of the sizing of the cooling system.

Poorly planned equipment modifications have caused numerous events. For example:

- Replacement of equipment made of a new material without verification of its suitability for the operating conditions which led to unforeseen deterioration such as rupture as a result of thermal creep or mechanical wear, vacuum collapse, cracking as a result of corrosion, vibratory fatigue, shrinkage, etc.

knowledge and competence

engineering and design

systems and procedures

0260-9576/19/$17.63 + 0.00

IChemE

- Equipment additions without an evaluation of the consequences on overall functionality, such as branch connections added preventing a control action, modifying condensate flow conditions on a steam panel, modifying the loadings on a pipe, rendering the security instrumentation inefficient, and adding agitation resulting in an excess of foam, etc.
- The installation of inadequate sensors generating a high number of false alarms (see ARIA box 40584), resulting in operators installing permanent bypasses.

Overflow of a diesel tank in a refinery

ARIA 40584 — France, 2011

In a refinery, an employee noticed a diesel tank overflowing at around 5 a.m. The tank was isolated. One-thousand cubic-metres of hydrocarbons were recovered in the retention basin and then transferred to recycling tanks.

The tank in question was in fact already full when it was mistakenly configured to be filled at around 1:30 a.m. The technician in the control room had asked a colleague outside to close the tank's manual feed valve before starting a transfer from the production unit to another tank. The technician outside had requested the control room to confirm the number of the valve to be closed but the tag on the valve had been reversed on site during the previous maintenance operation. He thus closed the wrong valve. The tank began overflowing at around 4 a.m.

The transfer error was detected by the centralised alarm system but went undetected by the technicians in the control room. The radar type level sensor was in the process of being replaced. The new sensors were not yet fully operational, and many false alarms were being activated in the control room. The technicians did not identify the alarm indicating the overflow on the tank amongst the multitude of very high-level alarms which were continuously triggered in the control room.

There are also several accidents in the ARIA database related to changes in the equipment use conditions — a fire following the change of assignment of a tank of petroleum products or a pipeline, corrosion of a cooling circuit linked to the change of biocide in a cooling tower, etc. Putting old equipment back into service without checking its suitability can also generate incidents, such as an explosion during the commissioning of pressurised equipment resulting from a degraded safety level, loss of process control due to an inappropriate instrumentation operating range or the commissioning of components unnecessary or incompatible with the process (see insert, ARIA 43616), especially resulting from a failure of the lockout process.

Prolonged release of mercaptans from a chemical plant

ARIA 43616 — France, 2013

At around 8 a.m., a technician detected an odour of mercaptans in the alkylation unit of a chemical site. A sample of the product was taken pending transfer (two days) to a control tank when the high-temperature alarm was triggered. At around 9 a.m., analyses were able to confirm the product's breakdown. The gas treatment plant became saturated and an odorous cloud drifted off the site. The facility operator triggered the plant's emergency plan, alerted the Prefecture and the 33 communities likely to be affected. Several neutralisation tests were conducted during the day but were unsuccessful. Odours were detected throughout the entire region, Paris and into the south of England. Tens of thousands of people reported feeling ill, complaining of vertigo, vomiting, etc. Over the following three days, a new procedure was able to neutralise little by little the 36 t of decomposing product.

Several causes were identified, including:

- Inadvertent start-up of the tank's agitator three days earlier. The batch was transferred the following day at 94°C. It gradually heated up as a result of friction until it began to decompose thermally at around 110°C;
- The tank had been transferred from another unit 16 years earlier with an agitator and insulation that were unnecessary for the process — no change management process had taken place;
- The agitator, which had been locked out in 2006, was no longer locked out due to a poorly controlled maintenance intervention;
- The risk analysis did not identify the product's risk of decomposition at around 110°C.

The facility operator removed the thermal insulation from the tank, installed appropriate cooling facilities, modernised the operation of the unit and resized the gas treatment operation. The intervention procedures were improved, the technicians received training on how to deal with emergency situations, the changes made on the equipment that was installed 16 years ago were analysed and the inspection procedures were improved.

The phases during which these modifications take place also present risks. A large number of accidents occur during these periods of work — explosions and fires during hotspot work or resulting from the creation of an explosive atmosphere because of dust. Some are particularly linked to the mismanagement of parallel activities, especially during operations where some

0260-9576/19/$17.63 + 0.00

activities continue to operate. Shared networks, such as those for the treatment of effluents, are particularly affected.

When the work has been completed, commissioning of the modifications can also lead to accidents. Events occurring during the test phases have been recorded, including poorly defined protocol, discovery of nonconformities in relation to the specifications, tag-out or alignment errors (circuit positioning). Several accidents resulted from the lack of technician training on new equipment or processes. The failure to update operating procedures and instructions can also lead to dangerous situations. Finally, several post-accident investigations have revealed that technicians were forced to deal with systems that were not functioning satisfactorily, such as unstable control PLC operation, inappropriate sensors, need for bypass due to incorrect parameter settings or false alarms, etc.

It should also be noted that the modifications at the origin of the accidents may also be organisational. These may include changes, over time, in the activities performed without review of the site's hazard study, increase in potential hazard without risk analysis, lack of review after a series of small changes (see insert, ARIA 45737), etc. Accidents also occur when work reorganisation is decided without the measures to accompany the changes implemented, such as removal of a crew dedicated to certain tasks without training the technicians newly appointed to perform them (see insert, ARIA 47253), reduction in the number of technicians assigned to carrying out or monitoring activities without checking means-mission suitability, etc.

Collapse of a floating roof in an oil depot.

ARIA 45737 – France, 2014

During a period of exceptional rainfall, the floating roof on a tank in a petroleum storage facility began to sink. Numerous residents were complaining of the strong hydrocarbon smell, and some individuals felt ill. The facility operator, who also detected a 300-litre leak in the tank's retention basin, initiated the internal emergency plan. The 3,900 m^3 of petroleum present in the tank was emptied at a slow rate while being monitored with an explosimeter. The operation lasted 35 hours.

Under the accumulated weight of the rainwater on the floating roof, it began to sink and flex in the centre. As the roof was in the low position in the tank, the base of a valve present on the roof came into contact with the bottom of the tank, causing it to open. The open valve allowed the petrol to flow, thereby causing the roof to sink even faster. Also, the capacity to drain water from the roof was insufficient. The following are among the organisational failures that led to this event:

- Insufficient assessment of the modifications carried out during the 1990s:
  – the strut of the two additional valves, installed in the 1990s in the centre of the floating roof, was longer than the roof's support legs;
  – the drain's discharge capacity was not reassessed after the installation of the automatic closure systems.
- Poor design of the modifications and incomplete maintenance plans.

The facility operator conducted a series of verifications on the depot's vent valves, revised its inspection plans for floating roof tanks, and conducted studies on how to improve the drainage system.

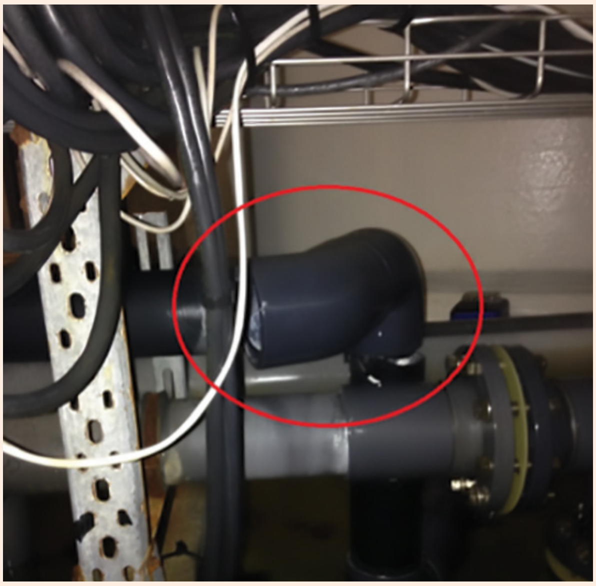
Leak of bleach in a detergent plant

ARIA 47253 — France, 2015

A technician conducting rounds in the storage facilities of a household detergent packaging plant discovered that the retention basin (for two tanks) in the storage facility was full of bleach. The retaining basin was not sealed, and 30 l of product was able to enter the rainwater network. The product contained in the retention basin was pumped into an empty tank. The rainwater network was pumped to an empty container. The container, having previously contained acid, released chlorine vapours and slightly intoxicated an employee. It was estimated that approximately 83.5 tonnes of 2.6% bleach was released.

Four months prior, the operator had done away with the night shift that was in charge of transfers between storage tanks and packaging lines. On the night of the accident, the production crew was to fill bleach containers. A technician went to the storage facility's control station at around 10 p.m. From the control desk, he was able to start the transfer pump and then opened the bottom valve on the corresponding tank. Water hammer began due to pumping with the valve closed. As a result, an elbow downstream from the valve became detached from its piping. The leak was discovered only two hours later. The level sensor on the retention basin was out of order.

The subsequent investigation revealed that insufficient instructions were provided regarding the transfer operations and that the production team was not trained in how to use the transfer control station.



0260-9576/19/$17.63 + 0.00

Lessons learned

Without claiming to provide a miracle solution, an analysis of the accidents related to poor change management highlights some recommendations:

- **Check** the essential, safety-related elements. To avoid accidents resulting from unplanned changes, it is important to identify parameters, equipment, processes, etc. that are critical to safety and to implement the means to ensure that there is no deviation concerning these elements (see insert, ARIA 46336).

Explosion in a chemical waste recovery plant

ARIA 46336 — Germany, 2014

A violent explosion occurred in a chemical waste recovery plant. An employee was badly burnt. Several plant buildings caught fire. Firefighters were able to gain control over the fire at around midnight. Nearby residents were confined to their homes. The employee died from his burns in hospital. Three people were slightly injured. Forty homes in the surrounding area suffered significant damage and property damage amounted to tens of millions of euros.

Although the cause of the explosion was not determined, several serious failures in the plant's operation were detected as well as the laxity of the control administration. The combustion plant was not allowed to incinerate chemical waste from external companies, but for a number of years, ten tonnes of such waste was burnt on a daily basis. The supervisory authority had been aware of this activity for 14 years. Furthermore, the power of the combustion plant, set at 1 MW per authorisation, was actually 3.5 MW. The supervisory authority did not require that risk analyses be conducted and did not consider the modification to be substantial.

In 2008, the company, having become insolvent, had replaced the facility operator. No thorough verification of the administrative status had been conducted at that time. Following the accident, the Ministry of Regional Environment verified the authorisations of 1,000 equivalent companies.

- **Analyse** the risks induced by modifications. The robustness of industrial systems is based on a set of components — the reliability of the installations, process stability, the know-how of the personnel, etc. The changes must be examined in terms of how they affect these points in order to eliminate the risks they represent in both the short and long-term.

- **Anticipate** the actions needed to accompany the implementation of changes. Whether they are technical, cultural, or organisational, changes cannot be improvised. Their implementation must be prepared, the boundaries defined by operational risk analysis, and the control of essential safety requirements must be planned for the long term.

Modifying an installation, in any form whatsoever, must be accompanied by an update of the applicable risk analysis. If no such analysis exists, this would be an opportune time to conduct one. This approach makes it possible to integrate all the above considerations.

0260-9576/19/$17.63 + 0.00