Effectively evaluating risks under degraded operating conditions

A degraded situation is merely an initial phase that could lead to an accident with serious consequences.

"Operating in a degraded mode" refers to a condition during which operations are ongoing despite there being no access to all necessary or normally expected functional resources upon completion of the corresponding risk analysis, whether such resources are organisational or technical.

It is essential for a facility operator to identify "deviations" that serve to degrade a situation in order to respond, by means of a well-informed risk analysis, in a way that makes it possible to implement appropriate compensatory measures.

In some cases however, this deviation becomes "acceptable" for the operator or for the various actors, who exhibit what experts in technological risks call the normalisation of deviation, which means accepting a relatively severe risk that is perceived to be highly unlikely to occur when compared with the immediate benefits of this normalisation (e.g. smaller investments in safety, less disturbance to production schedules, no time lost treating this risk).

Below are the main lessons learnt in pursuit of effectively evaluating risks under degraded operating conditions.

1. Never ignore or overlook the deviation

Many examples show that poor communication among actors, ambiguous instructions, the assignment of multiple tasks, a lack of controls or inability to treat deviations expeditiously can all lead to omitting a deviation either voluntarily or involuntarily.

• ARIA 42163: Around 10:30 pm at a Seveso-rated chemical plant, a sensor detected a rapid rise in conductivity inside a heat exchanger. Upon tripping the sensor alarm (at a 50 µS level), the automated safety controller isolated the circuit. A 2nd conductivity-meter, which had been idled and scheduled for replacement by the maintenance unit, showed a value of 0 µS. Not informed that this device was inoperable, technicians proceeded with sampling to remove any doubt and notified the duty manager, who analysed the situation, did not wait for the laboratory results, bypassed the conductivity-meter whose alarm had triggered, and restarted manufacturing. Ultimately, only a limited discharge of phosgene into the environment was observed, thanks to an effective 2nd safety barrier.

ARIA 42163 © Site Operator

• ARIA 14693: Mix of incompatible products during a transfer operation due to the fact that the technician had not been informed of a change in chemical product, resulting in 3 injuries.

• ARIA 13917: Overflow of a tank and pollution entering a river subsequent to the launch of a fuel oil transfer operation between 2 tanks by a technician who had left his station in forgetting about the ongoing transfer.

• ARIA 30486: A 60 m^3 leak of orthoxylene into the OISE River caused by neglecting to replace the buffer on an inspection flange.

2. Avoid normalising the deviation

Normalising the deviation entails considering that the degraded situation, which in theory should be treated as exceptional, becomes normal out of short-sightedness. The multitude of reasons for this tendency are often correlated with burdensome constraints, like maintaining production levels, avoiding heavy capital expenditures, etc.

The most infamous accident is undoubtedly Bhopal (ARIA 7022) with at least 3,780 fatalities. Operators incurring debt at a site were interested in saving money: refrigeration down for several months at a time; defective temperature, pressure and level indicators in the tank; inoperable gas washer; idled flare; no more inerted storage; etc.

The installation of permanent shunts is a frequent cause of accidents stemming from normalised deviations.

A deep-rooted cause of this normalisation process is related to ergonomics (e.g. constraints generated by repeated alarm activation, poorly designed tanks):

• ARIA 17531: High level and very high level alarms bypassed on gasoline tanks. Consequence: overflow into the retention basins.

• ARIA 38674: Delayed operations upon restarting a fungicide production unit in order to avoid reliance on 2 successive work shifts. Consequence: explosion in the spray tower.

• ARIA 49246: Bypassing a security feature that normally requires technicians to remain during a transfer operation. Consequence: fuel spill.

Another situation often encountered when the initial deviation is "normalised" consists of introducing a second deviation, which then offers a streamlined solution when coping with a degraded situation:

• ARIA 47892: Installation of a shunt in order to maintain a float in the upper position given that it was defective and responsible for untimely and frequent outages. Consequence: fire outbreak quickly brought under control.

3. Do not neglect warnings or public and media sensitivity

As a situation worsens and becomes more seriously degraded, the operator might hope to control the situation, in addition to being tempted to avoid spreading panic in the neighbourhood or disturbing the authorities.

In the case of accidents involving rapid kinetic reactions, it is essential to quickly inform authorities so as to provide them with the maximum amount of time to protect the local population.

Some accidents reveal that the operator's decision not to comply with this principle (ARIA 47277) caused a tremendous ethylene cloud (100 m long by 4 m high) to be released from a chemical site. The smallest spark would have unleashed a UVCE (Unconfined Vapour Cloud Explosion) event. Despite the presence of this hazard, the operator still decided not to activate the Internal Emergency Plan and authorities were not notified until 2 days after.

In the case of degraded operations with slower kinetics (ARIA 48764, 48766), neighbours may feel anxious about the situation, especially when nuisances are readily perceptible outdoors (odours, smoke, noise). The operator must not overlook the benefit of real-time communication regarding these events in order to explain the type of deviations involved and thereby reassure the local population (ARIA 43616).

For public authorities, the primary difficulty raised is the decision to be made in the aim of protecting both the population and the environment. The balancing act required is based on the risk of accident occurrence and its consequences, plus the unintended consequences of measures adopted (e.g. evacuation, confinement, road closures).

As an example, in February 2017, American authorities were fearing collapse of the backup spillway at the Oroville Dam. They requested 200,000 residents evacuate the affected zone. Three days later, following a sizeable drop in the dam water level, the population evacuation order was transformed into a simple alert.

This recent positive example (ARIA 49207) demonstrates that potential consequences in the event of a dam break received greater consideration than the logistics difficulties inherent in any such decision.

4. Areas for improvement

The aforementioned event analysis reveals that lines of organisational defence serve to guarantee control over maximum risks, even under degraded conditions. This defence entails at least the following:

- identifying the deviations from normal operations;
- tracking these deviations and conducting regular reviews to monitor their resolution and/or the effectiveness of compensatory measures;
- performing an in-depth risk analysis that takes into account this unique set of operating conditions by determining not only the stable process phases, but also the means by which a degraded state arises. Such an analysis constitutes a key element in accidental mechanisms featuring rapid kinetics, which leave little margin to react if the degraded situation has not been properly examined ahead of time;
- anticipating deviations by introducing response guidelines, i.e. procedures describing how to return to a normal situation and the relevant set of compensatory measures devised in a stress-free setting;
- addressing operational anomalies, like deficient emergency response resources (electric generating set, inverter, cooling, fire protection, etc.);
- assessing degraded situations from the perspective of worst-case consequences and not best-case consequences, then programming the alarm on this basis, even if in the end the major accident could be averted;
- reworking the risk/benefit calculation, which may lead to refusing expenditures in order to avoid a risk that seems highly unlikely or even acceptable;
- resisting the temptation to minimize the seriousness of an unlikely hazard when coping with multiple productivity constraints;
- tuning in to weak signs: personnel warnings, drift in production indicators, increased rate of equipment down time;
- communicating in real time on events, for the purpose of reassuring the local population.

A critical and attentive approach to safety in day-to-day activities, along with calculation of the risk/benefit objective and an awareness of weak signs, constitutes a state of mind to be displayed by senior management. This mindset must be nurtured day in day out to allow the safety “pointer” to indicate the appropriate direction among the various activity constraints.