|  |  |
| --- | --- |
| opcetlogo ***CHEMICAL ENGINEERING TRANSACTIONS*** ***VOL. xxx, 2025*** | A publication ofaidiclogo_grande |
| The Italian Associationof Chemical EngineeringOnline at www.cetjournal.it |
| Guest Editors: Bruno Fabiano, Valerio CozzaniCopyright © 2025, AIDIC Servizi S.r.l.**ISBN** 979-12-81206-xx-y; **ISSN** 2283-9216 |

Importance of indications of deviations for preventing incidents at Seveso sites

Henk J. Manuel\*, Mark P.N. Spruijt, Jochem H.J. Wijten, Bert G. Wolting

\*RIVM, PO Box 1, 3720 BA Bilthoven, The Netherlands

henkjan.manuel@rivm.nl

Incidents over the past 20 years at Seveso sites in the Netherlands have been analysed with the Storybuilder MHCA (major hazard chemical accidents) model. The model assumes that deviations from process control barriers can be used to bring the process back to a safe envelope. For this, deviations need to be indicated (I), detected (D), diagnosed (D) and responded (R) to: the "IDDR" framework. This framework helps in determining how deviations were handled in incidents, which influencing factors played a role and how they were connected to flaws in the safety management system. Analysis of 375 incidents shows that in half the cases studied deviations were not properly indicated, either due to missing equipment or procedures or simply being inadequate, not fit for purpose. Influencing factors that can be used to improve on indicating deviations are given in this paper: periodic inspections and review of hazard assessments, leak testing, monitoring of process parameters and last minute risk assessment. Flaws in the safety management system can lead to deviations and the paper provides some thoughts on possible improvements with respect to the elements of operation control, management of change and identification and evaluation of major hazards. The paper gives a number of examples of incidents for clarification of elements of the model and helps with learning from incidents.

* 1. Introduction

In the Storybuilder model, barriers to prevent incidents or effects of these incidents are grouped in lines of defence (LoD's). The model and database were introduced earlier (Kooi et al, 2019 & 2020), where the six LoD’s were explained. For this paper only the first two LoD’s are relevant. In the first LoD, barriers are grouped that control the overall process by taking care of the integrity of the installations, the process parameters (such as temperature, pressure, flows etc.), safe startup and site/environment control. Deviations from this control that occur can be handled in the second LoD, according to the "IDDR" framework. An example of this is a blinking light (indication), that is seen by an operator (detection), who understands the need for an action (diagnose) after which that action is taken in a timely manner (response). In about half the incidents analysed with the MHCA model and recorded in the Storybuilder database, the indication of deviations failed.

In this paper the influencing factors surrounding failures in IDDR and possible ways to prevent such incidents is given, with a focus on indication failures. This analysis looks back at past incidents. Thus, it is complementary to recent research aimed at predicting incidents, for example by looking at process data or meta data such as watch reports with the help of artificial intelligence techniques (Goede and Middelaar, 2024).

* 1. Incidents

The Storybuilder database currently holds records for 375 incidents where failures to recover deviations occurred from 2004 through 2023. It is filled with data from incidents that were investigated by the Netherlands Labour Authority or the Dutch Safety Board.

* + 1. Recovery failure types

 Table 1 gives a breakdown into the percentage of different recovery failures recognized in the incidents.

Table 1: Percentages of incidents where recovery of deviations failed. Per incident the first failure in the IDDR chain is selected. Therefore each incident is represented once in these numbers.

|  |  |
| --- | --- |
| **Recovery failures** | **Percentage of occurrence for all incidents with known recovery failure** |
| Recovery of deviations failure | 100% |
|  Indication failure |  52% |
|  Detection failure |  16% |
|  Diagnosis failure |  12% |
|  Response failure |  11% |
|  Unknown failure |  9% |

Table 1 shows that the indication of deviations fails in more than half the incidents. It should be mentioned that there is a bias in the data, as the incident analysts are instructed to determine the failure class in the IDDR order. For example: if an indication failure is detected, the analyst stops looking for possible other failures. So, there might have been other failures as well, although in these cases there is usually little information in the investigation report on other types of failures. Examples of the different IDDR classes that explains them in more detail are given below:

* Indication failure. Nitric acid leaked from an installation due to erosion, caused by grit of ceramic rings. The installation was inspected according to the inspection plans. Despite of the fact that the risk of erosion was recognized by the company, this particular installation was not inspected for erosion even though parts of the installation were regularly removed. Therefore, there was no indication of the erosion until the leak finally occurred.
* Detection failure. Vinyl chloride escaped from a pipe, connected to a reactor vessel. In the pipe a rupture disc and a safety valve were installed. The rupture disc protects the safety valve from the corrosive vinyl chloride and is designed to break at a lower pressure than set for the safety valve. In the incident the rupture disc broke and instantly vinyl chloride was released, because several bolts of the safety valve were not properly tightened, possibly due to earlier maintenance work. The process control system gave an indication that the safety valve was no longer airtight, as the pressure gauge between the rupture disc and the safety valve showed a constant value of 0 mbar from nine weeks before the incident. Normally the signal showed fluctuations. Detection of this deviation from the normal fluctuating state was missed by the operators because they used the pressure gauge only to detect rupture of a rupture disc. It was not used to check whether the pipe system was leak tight, thus missing the opportunity to detect the deviation.
* Diagnosis failure. Liquid LNG escaped when the bolts of a flange were loosened during maintenance work. Before starting the maintenance work the section with the flange was locally insulated by closing a valve. However, the valve was leaking and LNG ended up in the section. The resulting rise in pressure was detected by an operator and written down in a work permit. The work planner and the person responsible for releasing the work permits both misinterpreted this, eventually leading to the release.
* Response failure. During an inspection round in the evening, a corroded flange that was leaking hydrogen chloride was detected and reported by an operator. The day shift checked this and diagnosed that a clamp should be placed on the flange until the next turnaround. The procedures stated that the flange should be packed in plastic and put under a protective nitrogen blanket to stop the corrosion. Due to a communication error this was neglected after which the flange started leaking badly. The installation then had to be shut down for maintenance work.
	+ 1. Management tasks of indication failures

Indication of deviation is of particular interest as proper indication can prevent over half the incidents and thus are considered for the remainder of this paper. The management system must make sure that indications work in practice via a number of tasks, the so-called PUMM’s (Provide/Use/Maintain/Monitor). Indications may fail if not present, not properly used by personnel, not maintained to work when needed or if they are not monitored for the way they are used in practice. The PUMM’s can be used to understand all the types of failures but here are used to answer the question ‘how’ the indication of a deviation failed as explained in more detail below:

* Provide. Firstly, the management system should provide an adequate indication. Failures may happen at this stage if the indication was not present at all, or if the indication was not sufficient to give an indication of a deviation.
* Use. If an indication mechanism was provided, it may fail if it is not used properly. The management system should make sure that operators know how to use equipment or procedures through training and instructions.
* Maintain. indication mechanisms must be maintained to make sure they will work when needed. In some incidents, alarms no longer worked properly due to lack of maintenance.
* Monitor. If the indication was not used properly due to insufficient supervision, the Storybuilder analysts categorises the failure under a monitor failure. It may be that operators are instructed initially to work according to a procedure, but deviate from the instruction in daily practice. The management system should provide for corrections of this by proper supervision.
* Unknown. If the incident reports are clear about a failure to indicate the deviation, but do not give enough information on the precise nature of the failure, it is classified as unknown

Table 2: Percentages of failing tasks where recovery of deviations failed due to inadequate or missing indication of a failure. Only one task allowed per indication failure: the total number of failing tasks adds up to 100%.

|  |  |
| --- | --- |
| **Recovery task** | **Percentage of incidents with indication failure** |
| How did indication of recovery fail | 100% |
|  Provide |  58% |
|  Use |  9% |
|  Maintain |  11% |
|  Monitor |  6% |
|  Unknown |  16% |

Table 2 shows that in more than half the incidents no accurate indication of a deviation (or no indication at all) was provided by the organization. This emphasizes the need for companies to give more thoughts on possible ways to get an indication of a deviation. The model can give more insight into where the failures originated, with influencing factors. Two influencing factors (periodic inspection and leak testing) were built in the model from the beginning. In 2021 this was expanded into five categories, that are now used for all of the IDDR categories. Since 2021, 38 incidents were recorded where indication failed. Table 3 gives percentages of incidents in which an influencing factor played a role.

Table 3: Percentages of incidents per influencing factor for the incidents since 2021 where an indication failure occurred. Multiple influencing factors can be chosen, but in these particular incidents they add up to 100%.

|  |  |
| --- | --- |
| **Influencing factor in indication failure**  | **Percentage of incidents with the influencing factor** |
| All influencing factors | 100% |
|  Regarding periodic inspection |  24% |
|  Regarding leak testing |  8% |
|  Regarding monitoring of process parameters |  34% |
|  Regarding last minute risk assessment (LMRA) |  5% |
|  Regarding periodic review of hazard assessments |  8% |
|  Unknown or other influencing factor |  21% |

Table 3 shows that the best opportunities to improve on indicating deviations lie in periodic inspections and monitoring of process parameters. Examples where the different factors were encountered in incidents are given below:

* Periodic inspection. In one incident 40 tons of hydrocarbons escaped from a heat exchanger, ended up in the cooling water and were released through the cooling tower. The risk of breakthrough of materials had been identified earlier. This knowledge had not been translated into inspection plans that could have given an indication to prevent the severe loss and dispersal of materials in the air.
* Leak testing. Failures regarding leak testing can be divided in two types for which it should be relatively easy to improve upon in practice. In four of the six incidents the leak test was forgotten or was not prescribed at all after maintenance jobs. These incidents could have been prevented with a relatively simple checklist. In the remaining incidents the leak tests were inadequate: soap bubbles were not detected as they were blown away due to large flow, or the leak test was performed on an installation part that was not yet filled with materials at the time of testing so that no leak could have been detected. Leak tests thus should be validated when installations are in operation to make sure they will actually work.
* Monitoring of process parameters. A cleaner became unwell after inhaling formic acid vapours. The vapours were released from a gas scrubber that should scrub the last remnants of formic acid formed in a reactor. The reaction in the reactor was monitored by a temperature meter. However, its position was inadequate for getting a good reading of the reaction phase. Due to a production method where reactants were fed instantaneously into the reactor, the temperature would rise to such a high level that the scrubber was working outside its design criteria.
* LMRA. After maintenance work on a reactor, a supply line had to be purged. For this purpose, a T-piece was attached to the pipeline. According to the procedures, a LMRA had to be performed, as this work deviated from standard maintenance work. This was not done and the operators working on the purging missed the risk of an open or partially open valve on the T-piece. When one operator emptied the pipe, the other operator got aniline on his trousers due to a partially opened valve. He had to be taken to hospital for overnight observation.
* Periodic review of hazard assessments. A contractor was working on a wastewater tank, which was placed in a lowered pit. When finishing the work and climbing out of the pit, he started coughing and became unwell. It appeared that chlorine gas had assembled in the pit, due to changes in wastewater streams. Wastewater from acid- and lye-scrubbers, formerly segregated, now were both collected in the wastewater tank and produced chlorine gas. This leaked from several small openings and accumulated in the pit. After the incident, the installation’s design and the process will be reviewed. Generally, companies will have a framework to decide if a MoC procedure is needed or not. This incident shows that small changes for which it was decided not to use the MoC procedure may ultimately lead to something for which a periodic review is needed.
* Unknown or other influencing factor. When information lacked in the reports or the influencing factor did not fall into one of the categories above, the analyst used this classification.
	+ 1. Safety management system elements of indication failures

The Storybuilder model also records the safety management system (SMS) elements for the recovery failures. As discussed above, the management system in the incidents often does not provide for an (adequate) indication of deviations. This is linked with the SMS elements in the first LoD, since the deviations occur here. In that first LoD, the SMS elements that occur the most in the different barriers are ‘operational control’ (in 65% of all barriers in LoD 1), ‘management of change’ (14%) and ‘identification and evaluation of major hazards’ (30%). Please note that this adds up to over 100%, as multiple barriers and multiple SMS elements per barrier can be entered in the database. This provides another insight into the underlying causes and a possibility to intervene and prevent incidents in the future:

* Operational control. This element is somewhat obvious as the incidents occurred, so a loss of (operational) control must have happened. However, when the hazard was not identified beforehand it is difficult to distinguish between failures happening in operational control or in identification of the hazard. The following example of an incident shows what can happen if you rely on procedures, but do not identify the need for testing of critical materials to pick up on a deviation:
	+ Nitric acid was released from a valve. Stainless steel was used for working with nitric acid, but a part of the valve was replaced with nickel-copper. According to the procurement system, the correct part had been ordered. As this is a safety-critical part, it should have been tested to determine whether the right material had been delivered. X-ray tests will now be conducted by the company to test incoming materials.

Apart from checking incoming material, in normal operational control the management system should make sure that the right material is used everywhere, as is shown in the following incident:

* + A mixture of formaldehyde and methanol was suddenly released form a tank when a coupling in a flexible line broke. The line was corroded and material analysis showed that the coupling was made of regular carbon steel instead of stainless steel. Tracking of materials could have prevented this. The company has taken measures by checking all other couplings at the site and adjusting internal instructions.

Operational control also means that personnel can rely on equipment to check for deviations:

* + The wrong sequence of instructions was followed prior to opening a valve and flammable materials accumulated before the valve. Upon opening the valve, flammable material was released. There were no means to check the pressure, as the activities were not thought to be safety critical.
* Management of change (MoC). The need to control changes in designs is generally acknowledged. However, in incidents regularly it can be seen that not all changes are thought to be as critical. It is difficult to envision what a particular change can cause in the future. The database with examples on how seemingly small changes can have big consequences, can be useful for that purpose. The incidents show that it pays to at least have a periodical evaluation to check whether the hazard assessment of the installation, such as HAZOP (Hazard operability study) and PHA, is still in line with the company standards and operations. Incidents occurred where the hazard assessment was no longer up to date. After some of the incidents companies have taken measures to ensure a stricter implementation of rules concerning management of change. Two examples of incidents concerning MoC are given below:
	+ Periodic review: Heat exchangers had been replaced because of regular leaks at flange connections. Although the new heat exchangers had been tested, strong temperature differences at start-up after maintenance had not been considered. In addition, there were no specific procedures for hot restart. The strong temperature differences now caused an undesired heat-stress on the flanges which resulted in leakage. A flammable mixture above the self-ignition temperature escaped and ignited immediately. The resulting fire was contained by filling the installation with nitrogen. The company is now drawing up procedures for a warm restart and will train staff. The company is also going to do Computational Fluid Dynamics calculations for new installations to properly predict stress in flanges.
	+ Strict implementation/following of MoC procedures: A leak occurred in a carbon steel pipeline and 250 kg of oleum was released. Almost 1700 workers had to take shelter from the resulting sulphuric acid mist at the site. The carbon steel together with oleum forms a protective layer of ferrous sulfate, which protects against corrosion. Due to increased capacity demands, the fluid velocity had been increased over time. Because of this, the flow through the pipes then changed from laminar to turbulent flow. The turbulent flow eroded the protective layer, causing a hole to occur. This seemingly small change had not been identified as a change to be handled by the MoC procedures. Five years earlier a similar incident had occurred at the site, but had not been recognized as being caused by the earlier change in flow.
* Identification and evaluation of major hazards. It is sometimes easy to point a finger at the cause of an incident when looking at incidents in retrospect. The incidents in general however show that it is difficult to predict upcoming hazards. They were either not foreseen, were not thought to be as hazardous as they turned out to be or were not given the right priority.

In general when plants, installations, processes etc. are designed, general engineering practices (OSHA, 2016) and fundamental safety principles (EPSC, 2021) are used to identify hazards and create a safe operational envelope. Techniques such as HAZOP are used to try and predict possible deviations from this safe space. Technical control loops are then introduced to deal with these deviations. A rising temperature of a reactor, for example, can be controlled by increasing the flow of cooling water. It appears that there are not a lot of incidents in the database where these mitigating technical measures failed. Possibly HAZOPs have a blind spot when it comes to human operations as a lot of incidents seem to occur on a procedural level. HAZOPs should also identify the need for workers to obtain indications of deviations to determine if they are working within a safe envelope. This includes actions to adjust or return the process to normal conditions, to start up processes, or actions during maintenance, inspection or cleaning. The organisation should then provide for indications of deviations, for example, by using gauges to monitor process parameters, a leak test, periodic hazard assessments and inspections or an LMRA. In 36% of the incidents with failures to indicate deviations, scenarios are involved regarding maintenance, inspection and cleaning and commissioning and decommissioning plants.

Two examples of incidents where identification of hazards was overlooked:

* + While unloading a tank truck filled with methyl methacrylate (MMA) a number of maintenance workers, busy with a storage tank, became unwell. No harmful emergency response concentrations were exceeded, but MMA is detected by smell much earlier than these concentrations and caused the work to be stopped. The company had not identified this risk and had no indication of being outside a safe working envelope. After the incident, procedures were implemented to avoid working near the unloading area during the unloading of MMA.
	+ The driver of a truck tanker filled with a sodium nitrite solution discharged the contents into a tank, aided by an operator. The contents of the truck tanker were meant for another company, situated at the same site. After transferring the sodium nitrite into a tank, filled with a sodium bisulphite solution, an exothermic reaction occurred. The rising temperature caused the automatic overpressure protection to activate. The direct cause of this incident was the mixing of incorrect raw materials. Driver and operator had communicated about the delivery of a ‘sodium solution’, but unfortunately it was the wrong one. As the driver showed up for unloading at an unexpected time for the operator, the incident could have been prevented by checking purchase orders. The company did not have a system for preventing unforeseen deliveries of goods and the general discharge procedure was not known to the operators. There was insufficient communication between the purchasing department and the operators. The establishment will now modify the unloading procedure and improve the information provided to employees about incoming materials.
	1. Conclusions

The Storybuilder database contains 375 incidents regarding failing recovery of deviations that can be used for learning purposes. Although each incident in itself is unique, the underlying causes have a lot in common. Unfortunately, there is not a single underlying cause that can be addressed to prevent all incidents. However, the paper shows that a lot can be gained by looking at the deviations that occur in all incidents and that were somehow not acted upon. There is in fact a great potential for improvements here, especially when looking at the indications of deviations. In over half the incidents the indication that a deviation had occurred was missing, either because the means to indicate it were absent or because they were inadequate. A number of possible influencing factors that can lead to improvements or possible interventions are given in this paper:

* Periodic inspections. Inspect safety critical installations or processes on a regular basis and make sure they are included in inspection plans once hazards are identified.
* Leak testing. Make sure leak tests are performed where prescribed e.g. by using simple checklists. The tests should be validated in practice to ensure they work when needed, under all conditions.
* Monitor process parameters. Not every plant has been designed according to the newest engineering techniques. There should be more emphasis on giving workers the means to monitor process parameters. This helps them to determine if they are working within a safe envelope.
* Last minute risk assessment (LMRA). Perform LMRA, especially for work with hazards deviating from normal operating procedures. Use guidelines, e.g. in the form of a quick reference card to help with this.
* Periodic review of hazard assessments. Make sure that hazard assessments are up to date. Individual modifications may not meet the criteria to be assessed with a MoC procedure, but put together may provide new hazards.

Regarding the safety management system three elements are of main importance for improvements:

* Operational control. Obviously the system should provide for a good operational control, not just with regard to deviations. Some improvements can be found in a better tracking of incoming and used materials, and making sure equipment to indicate deviations is provided where needed.
* Management of change. As stated above it is recommended to periodically review if hazard assessments still reflect the actual situation. Examples from the Storybuilder database can be used for this, as it is hard to envision what could happen with small modifications over time. Be aware that seemingly small changes can have big consequences and make sure to have a consistent framework for applying MoC procedures.
* Identification and evaluation of major hazards. More thought should be given to operations that depend on humans to perform actions. The safety management system should provide for adequate means to detect deviations and to be able to act upon them. This may be overlooked in HAZOPs as there are not a lot of incidents in the database with failing technical control loops.

Acknowledgments

The development of Storybuilder-MHCA and the analyses were financed by the Dutch Ministry of Social Affairs and Employment. The Netherlands Labour Authority provided access to relevant incident investigation reports.

References

EPSC, 2021, Process safety fundamentals, <epsc.be/Documents/PS+Fundamentals/\_/6\_EPSC%20PS%20 Fundamentals%20-%20English\_website.pdf> accessed 07.09.2024.

Goede E. de, Middelaar J. van, 2024, Guide BLIC ahead, Better Learning from Information in Chemistry (in Dutch), <brightsitecenter.nl/wp-content/uploads/2024/06/2024-1869\_Brightsite\_BLIC\_V4\_LR.pdf>, accesssed 07.09.2024.

Kooi E.S., Bellamy L.J., Manuel H.J., 2019, Presenting RIVM's publicly available database of Dutch Major Hazard Chemical Accidents: Storybuilder-MHCA, Chemical Engineering Transactions, 77, 403-408.

Kooi E.S., Manuel H.J., Mud M, Bellamy L.J., 2020, Fifteen years of incident analysis, <rivm.nl/bibliotheek/rapporten/2020-0115.pdf>, accessed 07.09.2024.

OSHA, 2016, RAGAGEP in Process Safety Management Enforcement 5/11/2016, <osha.gov/laws-regs/standardinterpretations/2016-05-11>, accessed 07.09.2024.