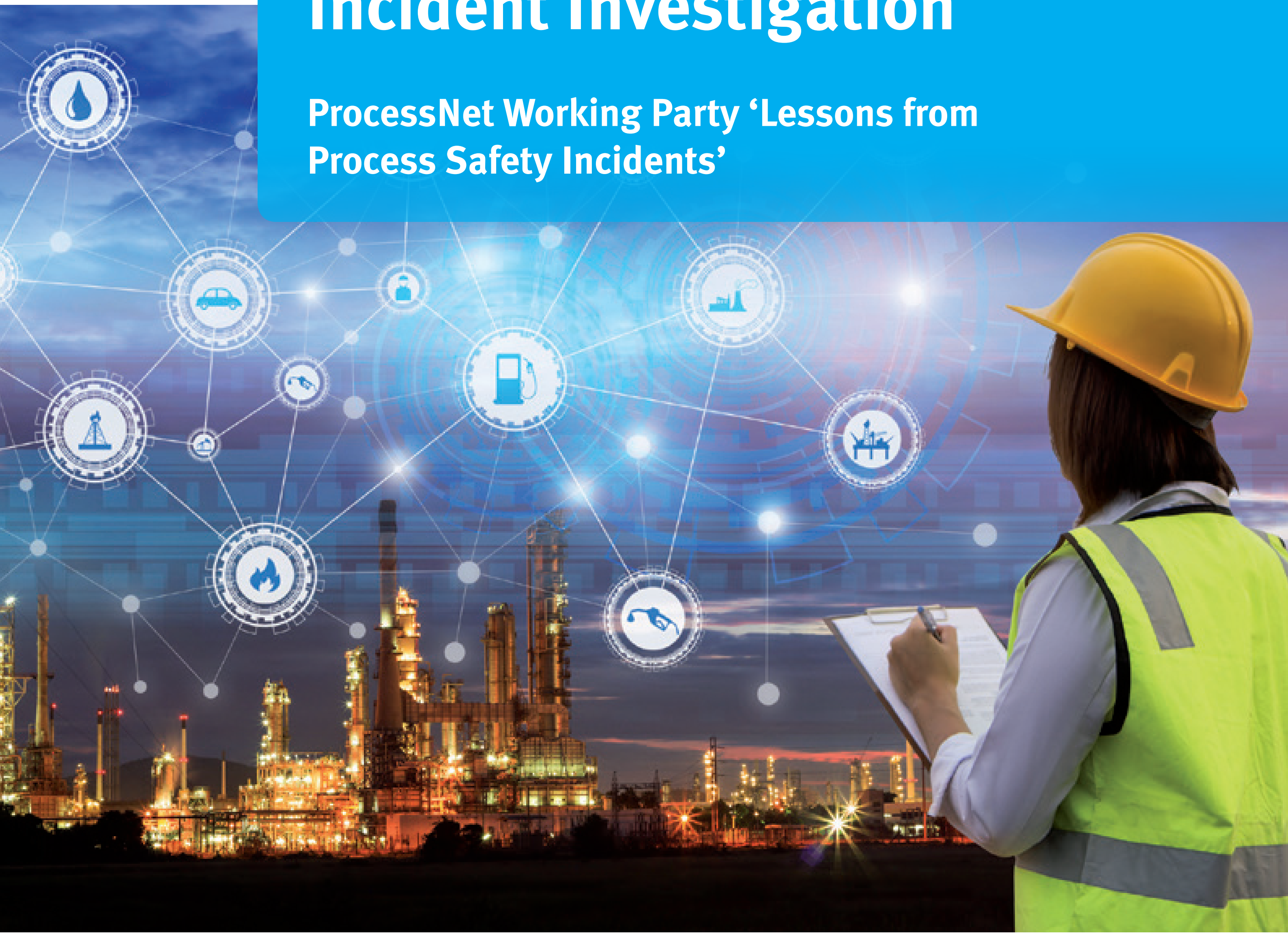
DECHEMA VDI

GUIDELINE

Incident Investigation

ProcessNet Working Party ‘Lessons from Process Safety Incidents’



PROCESSNET
EINE INITIATIVE VON DECHEMA UND VDI-GVC

LEGAL NOTICE

Publisher
ProcessNet Working Party Lessons from Process Safety Incidents

Responsible person according to the German Press Law (V.i.S.d.P):
DECHEMA e.V.
Dr. Andreas Förster
Theodor-Heuss-Allee 25
60486 Frankfurt am Main
Germany

ISBN: 978-3-89746-209-0

Although great care has been taken in preparing this Guideline no claim is made with regard to completeness or accuracy. It should be regarded as a checklist and is solely intended to offer ideas on how a typical incident investigation should proceed. This does not, however, exempt the user from the responsibility for carrying out a thorough assessment themselves. The authors assume no liability whatsoever for any consequences that may arise from using the Guideline.

Content

1 Introduction

The aim of the ProcessNet Working Party "Lessons from Process Safety Incidents" is to support companies of the chemical industry in the investigation of incidents relating to plant and process safety. This was the rationale for developing this guideline. With the aid of the guideline, incidents relating to plant safety can be investigated to identify causes and derive corresponding measures.

In principle, both reportable and non-reportable incidents should be investigated. Reportable incidents are well-anchored in different fields of law, particularly in the German Major Accident Ordinance (Störfall-Verordnung) and the Ordinance on Ordinance on Operational Safety (Betriebssicherheitsverordnung). Within these ordinances it is defined which incidents are to be reported. As a rule, the criteria for reporting are the extent of damage and the damage potential. This is linked with the requirement to present those measures necessary to avoid a recurrence of the incident.

Notwithstanding these legal obligations, there are good reasons for investigating the causes of non-reportable incidents, too. Whilst, such an investigation is not explicitly required, it can be indirectly inferred from the regulations. Reasons for investigating non-reportable incidents[1] include, for example:

- Identification of (root) causes
- Predictive avoidance of (reportable) incidents (lessons learnt)
- Avoidance of business interuption
- Effective monitoring of (preventive) measures
- Improvement of processes
- Operator's or employer's duty of care

Relevant near-miss incidents, in particular, should fall under the category of non-reportable incidents. In this guideline, the term 'incident' is used throughout.

The main target group of the guideline is small and medium-sized companies (SMEs) which, in many cases, do not possess sufficient expertise in the area of incident investigation themselves. The guidance can of course also be used as best practice by experts from other companies in the process of incident investigation. The content of the guideline has been designed so that it is suitable for those with a technical background but little experience in incident investigation. By demonstrating the basic procedure, it gives practical assistance. Through the straight-forward approach and easily comprehensible content it is aimed to increase the motivation of users to carry out a thorough investigation of even minor, non-reportable incidents. This in turn facilitates the continuous improvement of plant and process safety. To meet the individual requirements of a company it is sensible to tailor the guideline to their own situation and methods which are applied.

The comprehensive and precise investigation of incidents is important, as the results of the analysis permit appropriate conclusions and lessons for the future to be derived from them. If such investigations are not conducted promptly and thoroughly, opportunities wil be missed to avoid future incidents by adopting suitable measures. Similarly, the learning from incidents by organisations is an important outcome of such investigations.

This guideline focuses on incidents relating to plant safety. For the investigation of events pertaining to occupational health and safety the reader is referred, for example, to the guideline cited in [1] under Further Literature.

1 Of course, these reasons apply to reportable incidents, too.

2 Objectives and Success Factors of an Incident Investigation

All incidents with a high potential for damage should, in principle, be investigated. The damage potential can be derived from hazards for employees, environment, and neighbourhood and also from damage to property and business interuption. It is irrelevant whether damage has already occurred or not. The very suspicion that relevant damage could occur should entail an investigation.

The rationale for an investigation of incidents is to understand all factors and circumstances and to establish the causes that triggered the incident. This knowledge enables preventive measures to be taken to forestall similar incidents in the future. Additionally, the weak points (MOT: man, organisation, technology)[2] in the operation of a plant can be identified and consequently remedied. This ensures the continuous improvement of process and plant safety.

It is essential that the management responsible assure the performance of comprehensive incident investigations and provide the requisite resources. All investigations must be performed in an atmosphere of openness and trust. The objective of an investigation must always be to identify the causes and to derive appropriate measures. It is counter-productive for a plant operator to look for guilty parties; this must be avoided at all costs.

The necessary resources for an incident investigation cover simple aids (camera, PC, meeting rooms, etc.), guaranteed access to all operating information (work instructions, company documentation, etc.) as well as a budget for the involvement of further (external) experts, where necessary.

To reconstruct procedures, processes and details, those who are directly and indirectly affected by the incident have to be interviewed. Involving the works council at an early stage facilitates the interview procedure with employees.

It should be noted that there may be criminal law restrictions that have to be taken into consideration in the framework of the incident investigation.

2 Also known as the MOT principle: Man, Organization, Technology

3 Process of Incident Investigation

As a basic principle, the incident investigation covers the steps depicted schematically in Figure 1. This guideline focuses chiefly on the first three steps which are addressed in detail in the following chapters.

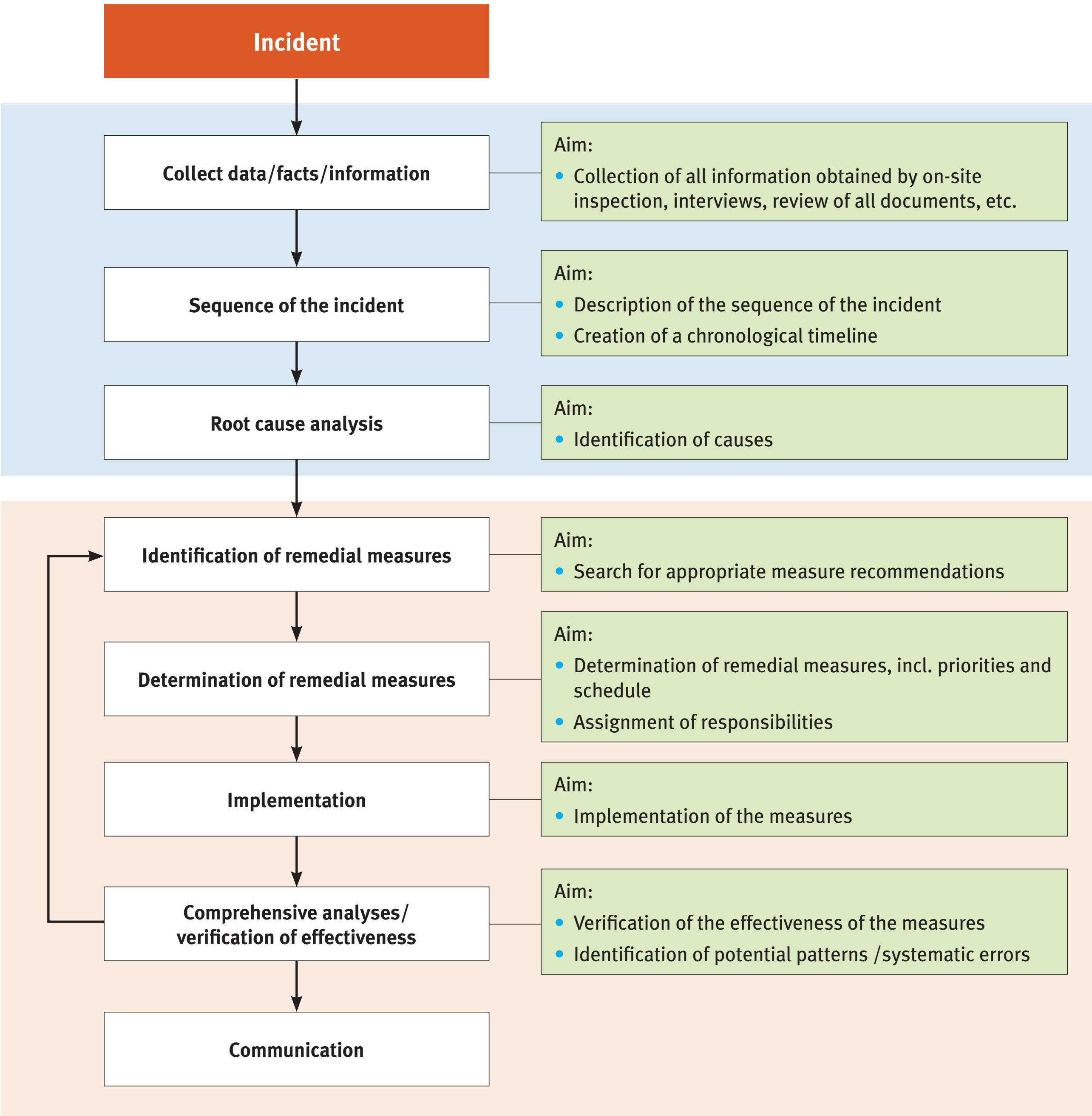


Figure 1: Basic stages of an incident investigation.

3 PROCESS OF INCIDENT INVESTIGATION

3.1 Timing of the Incident Investigation

- » As soon as possible after the incident has occurred
- » Before the incident site has been tidied up or changed
- » Before the persons affected and involved have forgotten what happened

Incidents should be investigated as soon as possible. It goes without saying that measures to limit the damage should not be restricted by the incident investigation. It is vital to keep the scene of the incident undisturbed as far as possible (no tidying-up, cleaning, etc.) in order not to change or even destroy evidence of the cause or course of the event. It can be helpful to cordon off the scene of an incident after damage containment and any necessary safety measures until all evidence and traces have been collected. The cordon should be kept in place until the record of the incident is complete. Longer delays before the incident investigation can start generally hinder the gathering of information (those involved no longer identifiable, sequence of events forgotten or unconsciously changed).

3.2 Team members

An incident investigation should be conducted independently of the organisational structure where the incident has taken place. Ideally the management appoints the leader of the investigation. In addition an investigation team is recommended which accompanies the whole of the investigation. The team should be composed of:

- » persons responsible for HSE[3]
- » appropriate experts from engineering and operations with detailed knowledge of the plant or plant component involved
- » other specialists (e.g. materials scientists, etc.)
- » external experts, if required

The team should have both expertise and experience in MOT areas and contribute their competence to the investigation: Man (human factors, concentration, fatigue, performance, training, etc.), Organisation (organisational processes, responsibilities, documentation, etc.) and Technology (technical processes, instrumentation and control, systems engineering, IT, etc.).

Individuals involved in the incident should not be included in the core team, must, however, be included in the information gathering process.

3.3 Information gathering

The complete, drawing together of information is the key component of an incident investigation.

The aim is to collect all information pertaining to the general circumstances, persons involved and physical/technical systems. This information is then broken down into individual elements and ordered chronologically on a timeline. This enables the course of an incident to be comprehensively reconstructed. It should be borne in mind that there may be a considerable time lag between the cause and the incident itself. Elements that cannot be categorised unambiguously should definitely be taken into account, but entered in a separate list.

It is important to clearly document which information can be classed as verifiable facts, well-founded assumptions, or hypotheses. The general rule is that there is no place in the information collection for subjective opinions or speculations or they are at least to be clearly marked as hypotheses.

The relevant information is acquired by asking 'W' questions:

Who did **what,** with **whom, when, how long, where, what for** and **why.**

3 HSE: Health, Safety, Enviroment

The attached catalogue of questions (Appendix 5.1) contains examples of interrelationships to be clarified.

Information is gathered by:

» Interviews with the individuals involved (i.e. persons affected, supervisors (shift supervisor, plant manager), safety officers, others who were in the facility at the time of the incident (aspects to be taken into account for interview purposes are given in the appendix)

» Evaluation of the data and process control systems

» Documentation available at the establishment (process description, operating instructions, training instructions, etc.)

» Photographs/videos (sketches, where applicable) of the components affected, the environment or other relevant conditions and systems. It must be recorded when, where and by whom they were made

» Technical survey and analysis of the damage (e.g. materials analysis)

» Personal observations

Additional aspects to consider for conducting interviews are described in Appendix 5.2.

3.4 Root cause analysis

The search for the root causes must be conducted systematically to avoid errors or carelessness. Only a systematic analysis and check of the MOT areas: Man – Organisation – Technology can reveal the underlying causes from which lessons can be learned for the future.

It is not fundamentally decisive which of the available and customary incident analysis methods is chosen. It is also not crucial whether a commercial software tool is used or whether the causal relationships are drawn up manually. What counts is that the information, the relationships and the causes derived from them should be described and determined meticulously and systematically.

In the following, one potential method of incident analysis, the causal tree method, is described in detail. The use of this method does not incur additional costs.

3.4.1 Causal Tree Methode

The causal tree method is a simple and systematic procedure to present causal relationships and to work out how similar incidents can be prevented in future. It is neither the aim nor the purpose of this method to identify guilty parties and attribute blame.

As the name indicates, this method consists of generating a causal tree. The causal tree method defines an incident as changes or deviations from normal operation. First of all, this necessitates identifying and listing all deviations in the system and process and determining their interrelationships. Subsequently the causal tree is created. To this end, simple rules define the causal relationships. For this reason the causal tree should only contain “branches” that have actually contributed to the incident.

The following three steps are essential to the implementation of the causal tree method and must always be taken into account.

3.4.1.1 Preparation of a list of relevant information

First, all information must be collated with care. Then it has to be broken down and recorded separately, for example on individual index cards. Then a timeline is created. The following rules should be observed:

» In each case, record only one piece of information at a time. “He fell down and hit his head on the pipeline” contains two pieces of information!

» Only use substantiated information. Avoid judgements or assumptions, such as “The design was bad”.

» No interpretations. “He ran”, not “He ran too quickly”.

Please note: If no substantiated data are available, assumptions about circumstances that may have contributed to the incident should be considered. They are to be clearly designated as assumptions or hypotheses.

3.4.1.2 Creation of the causal tree diagram

Once the information list has been compiled, the information has to be placed in a sequence and the relationships among the items identified. The creation of the diagram is subject to several rules. Here, the timeline generated in the first step can help. By writing the individual pieces of information on index cards, the cards can then be ordered on a magnet board or a free wall.

3 PROCESS OF INCIDENT INVESTIGATION

The causal tree diagram begins with the final result (the incident or near miss) which is placed on the right-hand side of the diagram. From this point, all other information is added in reverse chronological order as causally related factors. The following questions are asked:

» What was the cause?

» Was this factor necessary?

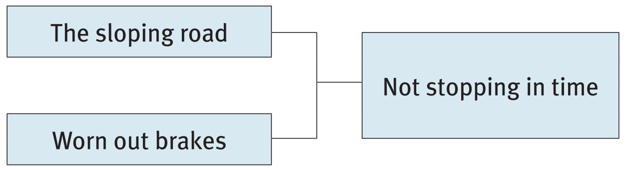
» Was this factor sufficient? If not:

» What was additionally a direct cause of the present result?

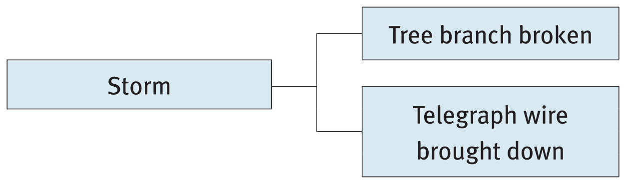
There are two different types of causal relationships:

• Direct progression: one fact has only one cause

• Conjunction: a fact has two or more causes



• Disjunction: two or more facts have only one cause



3.4.1.3 Identification of sufficient causes

Once all available information has been entered in the causal tree diagram and designated as factors or causes, the sufficient causes have to be determined. There is no such thing as a “hard”, unambiguous criterion for a sufficient cause. Rather, all factors have to be evaluated, and subsequently the team has to decide whether the factor in question is sufficient or the occurrence must be prevented in the future. If the team decides that remedial measures are required, it has to consider whether they are feasible and not shy away from more far-reaching measures.

To prevent a root cause analysis from being one-sided, tangible factors should be sought as causes for the MOT categories of Man – Organisation – Technology. Factors that can be excluded require a justification. The exclusion of factors on the basis of an adequate justification helps to determine how many levels need to be investigated and an excluded factor terminates the particular causal factor branch of the tree. Moreover, the justification reveals the potential limits (e.g. professional competence) of those involved, in order to decide when additional expertise should be sought. The following breakdown of cause categories aids the analysis:

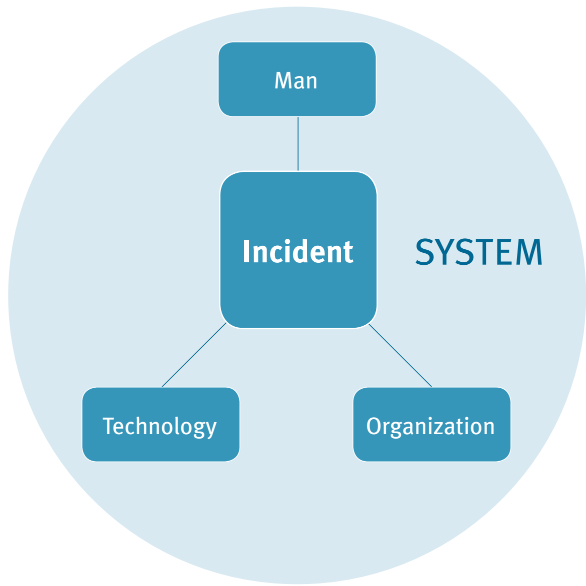


Figure 2: MOT categories of causes.

Detailed explanations of these categories are provided in Appendix 6.3.

3.4.2 Example

The following example aims to clarify the use of the causal tree method. A description of the incident can also be found in the ProcessNet Incident Database under the following Link[4].

Commissioning of a filter despite lack of clearance after maintenance work resulted in discharge of product

Incident

On switching the product flow to two filters operated alternately, a reaction mixture was discharged under the splash guard of the filter which had previously undergone cleaning and maintenance.

3.4.2.1 Comprehensive information gathering (example)

- Discharge of reaction mixture
- filter previously cleaned and maintained
- Switching of product flow
- Two filters operated alternately
- Filter opened after cleaning/maintenance
- Warning signs (equipment open) put in place after maintenance work
- Recommissioning three days after cleaning
- Warning signs not in place at the time of recommissioning
- Filter cover closed at the time of recommissioning
- Filter cover unscrewed at the time of recommissioning
- Operating instructions for recommissioning the filter not available

3.4.2.2 Creation of causal tree diagram and identification of the ultimate causes

The following figure shows a possible variant of the causal tree for the above example. The boxes marked in red represent the factors that were identified as the cause of the incident.
Identified causes:
After cleaning and maintenance the filter should initially have remained open. Warning signs drew attention to the fact that work was still in progress. At the time when the

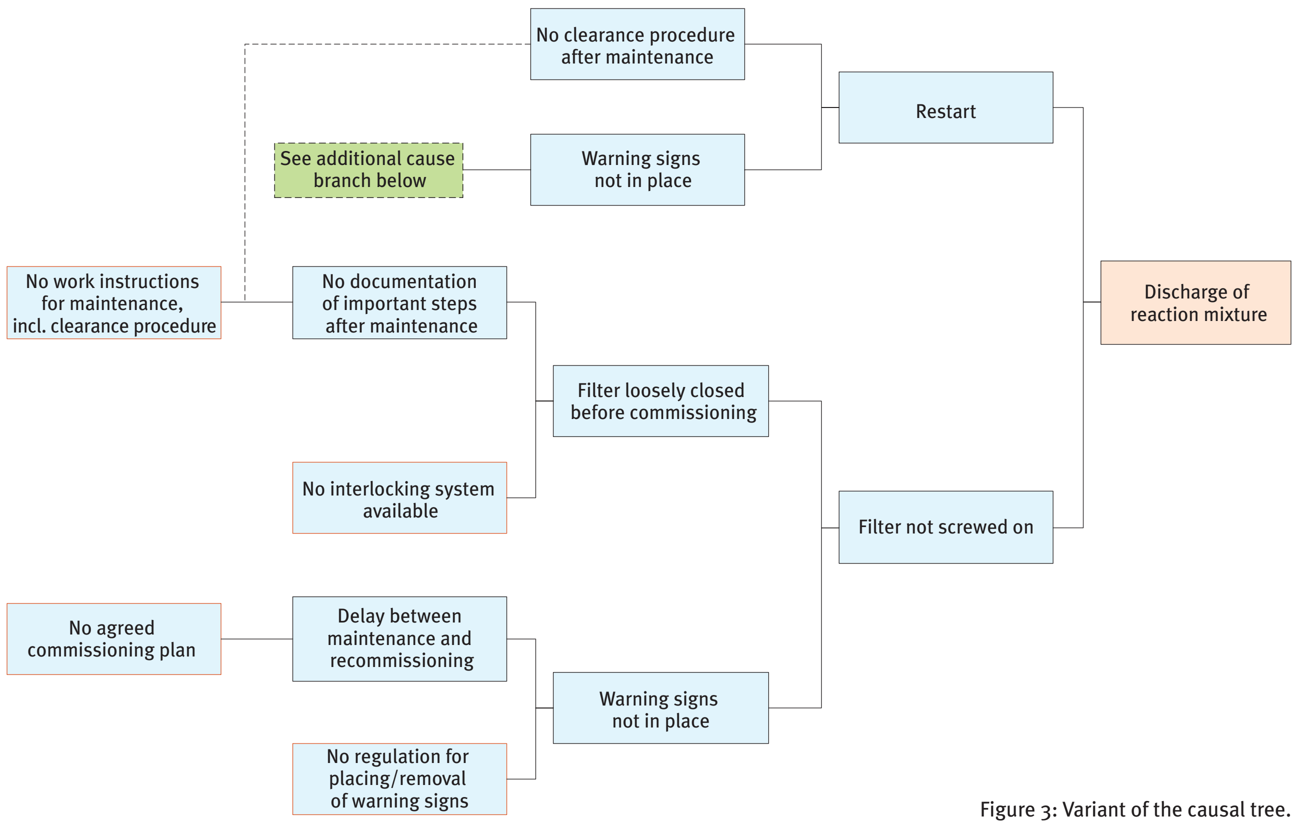


Figure 3: Variant of the causal tree.

4 http://processnet.org/10_2002-p-10590.html

filter was recommissioned – three days after the cleaning and maintenance – the warning signs had been removed, the filter cover closed and the splash guard attached. The splash guard gave the impression that the filter was ready for operation and did not indicate that the filter cover was not screwed on. There were no written instructions available for recommissioning the filter.

The following conclusions and lessons learnt were derived from this real-life example:

- All stages of maintenance work have to be planned: from approval prior to execution, to acceptance and handover for recommissioning of the plant or plant component. Any work instructions derived from these stages, if applicable, are to be recorded in writing. As far as possible and appropriate, procedures should be adopted for maintenance work which ensure against any deviation on site from the planned sequence of events, e.g. in accordance with the “lock out - tag out” principle.

- Any major steps relating to safety during maintenance work are to be documented. Maintenance sign-off notes are to be subjected to a separate check.

- The individual stages of maintenance work should as far as possible be organised and scheduled in close coordination in order to reinforce the exchange and communication of important information on operational procedures.

3.5 Search for and specification of measures

On completion of the root cause analysis, measures derived from the principal causes have to be specified and then implemented. The rationale is to prevent a recurrence of the same or similar incidents and to continuously improve the safety of the system or process. The characteristics of a good set of corrective measures include the following:

- The measures should be practical, realistic and permanently realisable.
- The measures should reduce the risk, and not ransfer the risk to another part of the system or process.
- Clear responsibilities for the implementation of the measures should be described.
- A deadline for the implementation of the measures should be documented

It is imperative that, for all categories of causes identified (MOT), any measures derived should be carefully weighed. The suggestions given in Appendix 6.3 can assist experts in determining appropriate measures for the individual categories of causes.

3.6 Documentation and verification of effectiveness

Each incident investigation should be documented separately. The documentation can be made on paper, but experience has shown that computerised documentation is helpful. It is, however, important to store not only the report, but also all associated documents (plans, graphics, etc.). All data should be stored in a central location. The compilation of the data should clearly indicate whether comparable incidents have occurred in the past and the constellations that have already resulted in a comparable incident.

No incident investigation is complete without verification of the effectiveness of the measures taken. Both during the incident investigation and when determining the measures it is necessary to consider how best their effectiveness can be checked. The verification of effectiveness of the measures must run concurrently with their implementation. This should be an integral component of the investigation report.

In the case of repeated incidents with comparable causes a more intensive scrutiny is necessary so that as far as possible repeat occurences can be excluded.

Many non-reportable incidents in the German chemical industry over the past years have been compiled in the ProcessNet “Incident Database”[5] and can be drawn on for the analysis, derivation of lessons and determination of measures.

3.7 Communication of lessons

Each incident investigation should be followed up by ascertaining whether further activities, not confined to the limits of the incident in question, are required to mitigate potential risks, e.g. in other processes, plants, companies, locations. The results of the incident investigation must, therefore, be critically reviewed so that the causes and necessary measures are presented in a suitable, generally intelligible form. In this context it is important that the plant operator should scrupulously avoid the issue of blame.

Employees should report regularly about their lessons learnt from incidents. Such reports can be based on a standard form for distribution to all groups. In this connection all employees should be requested to check their own areas for potential weak points. All information must be transferred to a knowledge management system. The availability and communication of lessons learnt from an incident helps to maintain and enhance safety.

5 http://processnet.org/en/incident_db.html

4 Additional Literature

1 Fahlbruch B., Meyer I. Ganzheitliche Unfallanalyse. Leitfaden zur Untersuchung von Arbeitsunfällen, BAuA (2013): https://www.baua.de/EN/Service/Publications/Report/F2287.html

2 Kletz T. Learning from Accidents, ELVR(2001):

3 James Reason, Menschliches Versagen: Psychologische Risikofaktoren und moderne Technologien, Spektrum. 1994

4 ESReDA Working Group on Accident Investigation, Guidelines for Safety Investigations of Accidents, 2009, https://esreda.org/wp-content/uploads/2016/07/ESReDA_GLSIA_Final_June_2009_For_Download.pdf

5 P Underwood, P Waterson, Accident analysis models and methods: guidance for safety professionals, 2013 https://dspace.lboro.ac.uk/dspace-jspui/bitstream/2134/13865/4/Underwood%20and%20Waterson%20%282013%29%20-%20Accident%20Analysis%20Models%20and%20Methods%20-%20Guidance%20for%20Safety%20Professionals.pdf

6 Databases

- Umweltbundesamt- Zentrale Melde- und -Auswertestelle für Störfälle und Störungen in verfahrenstechnischen Anlagen https://www.infosis.uba.de/index.php/en/zema
- ProcessNet Incident Database: https://processnet.org/en/incident_db.html

5 Appendix

5.1 Catalogue of questions for information gathering

General

» Where and when did the incident occur? (starting time, duration, exact location)

» How great is the extent of the damage? (names and degree of severity of the injured, incl. exact description of the parts of the body affected, extent of material damage/environmental damage, incl. exact description of the equipment and systems involved)

» Have pictures (photos/sketches) been made of the plant components affected and of the damage incurred?

» Have video recordings been secured?

» What time factors, e.g. time of day, working hour within the shift, type of shift (early, late, night), breaks and mealtimes, overtime hours, etc., were applicable?

» Had there been similar or comparable (near miss) incidents in previous years?

» Were corrective measures immediately or temporarily introduced or implemented?

» Is an up-to-date risk assessment available?

Personal information

» Which persons, including their details (i.e. age, position, qualifications, level of experience, language, training certificates, external employee), were present?

» Has a description been prepared of the duties/activities at the time of the incident (operating instructions (general and specific), exact whereabouts of the persons involved, individual or team work, etc.)?

» Are process descriptions and work permits available?

» Have duty rosters been secured?

» Is information available about supervision, i.e. direct or indirect supervision of the persons involved?

» Where were, if applicable, the persons affected and their supervisor at the time of the incident?

» Was personal protective equipment worn?

» When was the last plant training course of those involved?

» When was the last safety training course of those involved?

» Who trained the persons affected, if applicable?

» Was there anything special, unusual or different about the working conditions?

» Were there risk assessments for the operations performed?

Physical/technical information

» What particular features of the equipment and systems could be connected with the incident, e.g. manufacturer, type, size, operating conditions, special components involved, etc.)?

» Does a description exist of the substances used (incl. possible hazardous effects and properties, and intended and unintended properties) and of potential interactions?

» Have IT and process control and monitoring systems been evaluated, e.g. all camera images, process data from the control system before and during the incident, alarms (non-recorded data, if possible with screenshots)?

» Is a description available of the process conditions before and during the incident (i.e. process parameters, such as pressure/temperature/flow rate, etc., operating status, etc.)?

» What ambient conditions prevailed before and during the incident, i.e. weather conditions, noise pollution, limited visibility due to fog, steam, etc.?

» When was the last service/maintenance of the plant components involved?

» What causal factors, e.g. special procedures and conditions, contributed to the incident?

» How is backup of relevant data performed, e.g. protocols, logs, reaction data of the plant, safety data of the plant?

» Were process conditions changed?

» Are current risk/hazard analyses or other safety reviews available?

» Are inspection protocols of the affected plant components available?

5.2 Aspects to consider when conducting interviews

The aim of an interview is to collect and collate information essential to the investigation and clarification of an incident.

On no account is it concerned with identifying guilty parties, attributing blame or finger-pointing

To obtain the necessary information requires sensitivity and discipline. The question of whether the workers' council should be involved must be assessed.

The following fundamental aspects should be observed when conducting interviews:

Who should be questioned?

» Persons directly affected and involved

» Person who reported the incident

» Supervisor of the area where the incident occurred

» Witnesses

» Colleagues

» HSE / safety officers

» Works manager

» Other persons who were indirectly involved (e.g. maintenance personnel, etc.)

In the case of external persons (as witnesses or as external experts), the formal and legal prerequisites need to be clarified. Matters pertaining to data protection and protection of confidential company information should be borne in mind.

The interviewer should, in principle, be familiar with the plant, should not be (directly) connected with the current incident and should be trained and experienced in conducting interviews.

The interviewer's questions should

» be open-ended (i.e. the interviewee must give a detailed answer, not yes/no answers);
» never contain the interviewer's interpretation or opinion;
» not suggest an answer;
» not aim to attribute blame or responsibility;
» be clear and simple (e.g. no contradictions, no and/or combinations, etc.);
» elicit specific, precise answers;
» not harass or put unnecessary pressure on the interviewee;
» be limited to the interviewee's perception of the happening;
» conclude by enabling the interviewee to make additional and even subjective comments.

If necessary, the interview should be supplemented by other means, e.g. sketches, on-site inspection, explanation of material (e.g. floor plans, photos).

The questions and answers of the interview are to be documented; after the interview they are assigned to the chronological sequence of events of the incident documentation.

5.3 MOT categories of causes

MOT Category	Factors	Examples of Causes
MAN	Concentration / vigilance	Hazard awareness
	Knowledge / experience	Knowledge of processes and work flows
	Motivation / emotion / stress	Physical impairments/ limitations
	Physiological / biomechanical	Mental impairments/ limitations
		Fatigue
		Drugs/alcohol problems
		Behavioural problems
ORGANISATION	Process	Competences / responsibilities not defined
	Integration	Instruction and training courses inadequate
	Life cycle	Operating instructions missing or inadequate
	Commissioning	No audits carried out
	Operation	No adequate plant modification
	Servicing	
	Decommissioning	
TECHNOLOGY	Design	Equipment Design ungeeignet
	Hardware	Mess- und Regeleinrichtungen fehlen oder unzureichend
	Software	Wartungs- und Instandhaltungsarbeiten nicht adäquat
	Components	Spezifikationen unangemessen
	System (technical)	
SYSTEM (OVERALL)	Interactions between MOT	Lack of a higher-level view of the problem
		No silo mentality

Working Party 'Lessons from Process Safety Incidents'

The Working Party 'Lessons from Process Safety Incidents' was founded jointly with the German Chemical Industry Association (VCI) in 1996. The aim of the working party is to support learning from safety-related incidents and thereby maintain and enhance the high level of plant and process safety in the chemical industry. This is accomplished with the help of companies that submit accounts of incidents or near misses on a voluntary basis. The working party members evaluate them and suggest improvements.

Concise, anonymised descriptions (sequence of the event, cause, lessons learnt) are publicised in the Incidents Database where they can be accessed by interested parties.

Incidents Database

The Working Party 'Lessons from Process Safety Incidents' fosters learning from non-reportable, safety-related incidents. It does so pragmatically and unbureaucratically by providing access to lessons learnt that are widely applicable, and this knowledge is continually updated.

Since its founding in 1996, the group of experts constituting the Working Party 'Lessons from Process Safety Incidents' has collated incident accounts voluntarily submitted by VCI members. Provided that a high degree of didactic value is evident, the accounts are anonymised, analysed and made available in a standardised form to the interested public.

Further information on the Incidents Database can be found at **http://processnet.org/en/incident_db.html**

DECHEMA
Gesellschaft für Chemische Technik
und Biotechnologie e.V.
Theodor-Heuss Allee 25
60486 Frankfurt am Main

Phone: +49 69 7564-0
Fax: + 49 69 7564-117
E-mail: info@dechema.de