Enhancing Safety: The Challenge of Foresight

ESReDA Project Group *Foresight in Safety*

Chapter 5

Use of Scenarios as a Support of Foresight in Safety

Miloš Ferjenčík
Miodrag Stručić
Tuuli Tulonen
Eric Marsden
John Stoop

ESReDA
European Safety, Reliability & Data Association

Table of contents

5 Use of Scenarios as a Support of Foresight in Safety

Milos Ferjencik, University of Pardubice, Czech Republic
Miodrag Stručić, EC Joint Research Center, the Netherlands,
Tuuli Tulonen, Tukes, Finland
Eric Marsden, FonCSI, France
John Stoop, Kindunos Safety Consultancy Ltd., the Netherlands

5.1 Executive summary

Incident scenarios are a practical tool for thinking about risk. Scenarios may be results of prospection or retrospection. Both prospective and retrospective scenarios can be used for lessons learning.

Any incident scenario can be reduced to a set of causal events. Lessons learning can reach Early Warning Signs (EWS) through the identification of causal events. EWSs are causes and indicators of causal events.

This chapter shows that results of lessons learning via scenarios can be used:

- to prevent loss of memory,
- to list all possible EWSs,
- to identify whether a failure/error/condition represents an EWS,
- to prioritize EWSs.

All preceding claims are illustrated by examples.

5.2 Key Messages

Foresight requires determining the events/conditions that are to be considered EWSs. The incident scenarios may play useful roles since EWSs can be determined from scenarios obtained by both prospective and retrospective analysis. The path to determine EWSs leads via the determination of causal events.

With the use of incident scenarios, both identifying and prioritizing the EWSs is possible. They help make visible the EWSs, and select EWSs that deserve special attention (e.g. real-time monitoring).

Scenarios as an investigation component of lessons learning help to determine sets of EWSs that should be searched for and tracked during the analyses.

Scenarios as a documentation component of lessons learning help the determination of whether a specific failure/error represents an EWS.

5.3 Introduction

This chapter is based on ideas presented in the paper by Ferjencik (2017). The text uses terminology that is standard in publications issued by the American Institute of Chemical Engineers. Readers interested in a reminder of the meanings and relations of terms such as hazard, control, initiating event, scenario etc. may find instructive illustrations in articles by R. F. Blanco, e.g. in Blanco (2014). A new term, i.e. 'causal event', is introduced in this chapter.

When scenarios are discussed, both accident or incident scenarios are implied throughout this chapter. The word ‘scenario’ has the same meaning as the term ‘accident sequence’ in Benner’s paper (1975), i.e. a possibly multilinear sequence of events representing individual actions of animate or inanimate actors that leads to an injury or damage. If one of the actors fails or is unable to adapt, the perturbation starts the accident sequence. Thus, the scenario begins with a perturbation (initiating event) and ends with the last injurious or damaging event in the sequence.

Scenarios represent a tool for lessons learning. Both prospective and retrospective scenarios can be used for lessons learning. Lessons learning in this chapter focuses on early warning signs (EWS). EWSs are part of lessons learned resulting from the lessons learning process. The main concept introduced in this chapter states that the EWSs can be identified with the use of scenarios via the identification of ‘causal events’.

Additionally, scenarios can be used as an investigation and documentation tool. Use of scenarios as an investigation component of lessons learning helps to identify sets of EWSs that should be searched and tracked during the analyses. As a documentation component of lessons learning, it helps to determine whether a specific failure/error represents an EWS.

This chapter shows that results of lessons learning via scenarios can be used:

- to prevent loss of memory;
- to list all possible EWSs;
- to identify whether a failure/error/condition represents an EWS;
- to prioritize EWSs.

All preceding claims are illustrated by examples.

Moreover, the list of attributes necessary for the tools of lessons learning according to Benner and Carey (2009) is reproduced in this chapter. The question is discussed whether and under what conditions the scenarios and EWSs can carry all these attributes.

5.4 Early warning signs

5.4.1 Definition of EWSs

In this part, only a brief introduction into the concept of EWSs is sketched. CCPS (2012) writes about incident warning signs, which are subtle indicators of a problem that could lead to an incident. Warning signs precede incidents or contribute to them.

In conventional risk terminology, early warning signs can be understood as an indicator of strengthening a hazard or of weakening a safety measure, which can result in an increase of frequency or severity of consequences of scenarios causing damage. Since both an increase of frequency and an increase of consequence severity cause an increase of risk, then, briefly, an early warning sign is an indicator of an increase of risk.

Outside the risk based schemes of thinking, but not in contradiction with them, the occurrence of EWSs could be interpreted as an increase of vulnerability. Thus, foresight in safety could mean the capability to flag an increase of risk with the help of EWSs.

General explanation of foresight can be found in Chapter 2, Røed-Larsen et al., 2020.

5.4.2 EWSs are part of lessons learned and a result of lessons learning

Within the analysis of lessons learning system functions, processes and practices, Benner and Carey (2009) observe that divergent views exist about whether lessons learned are causes, cause factors, conclusions, findings, issues, statements, recommendations or scenarios described in text in narrative reports.

Clearly, they are right. Large accessible literature about incident investigations and lessons learning is not consistent in terminology and approaches. Nevertheless, in this text it is considered that identification of early warning signs is part of lessons learned. EWSs are considered here to be a desirable result of lessons learning. Consequently, lessons learning tools, like scenarios, are expected to detect EWSs.

5.4.3 Examples of EWSs: Kitchen

A simple example shows that in a known environment, some people tend to identify EWSs intuitively.

Kate and William are married; William is taking a parental leave from work. He takes care of the children and also he cooks. He likes cooking. In connection with cooking, he frequently makes small changes – hopefully improvements – in the kitchen.

Kate is glad that William likes cooking; however, she does not agree with all his improvements in the kitchen. For instance, she does not like the bottle with oil in close proximity to the stove, or a heavy bowl in the shelf above the ceramic hob. In addition, she hates William's habit of leaving the frying pan on the stove unattended.

When they had a disagreement over this the last time, William argued that nothing had happened. Kate answers that all these changes are indicators of problems that could lead to an incident. In accordance with CCPS (2012) she calls them warning signs or early warning signs (EWS) and insists that William should avoid making changes in the kitchen that could lead to increasing the risk.

5.5 Scenarios represent a tool for lessons learning

5.5.1 Example: Intuitive use of scenarios

William, in our example, replies that he does not see anything serious in the changes he made in the kitchen. Kate states that this is because he is not intentionally imagining any incident scenarios. Thinking about danger with the help of scenarios comes natural to Kate. The experience gained through the realisation of hazards serves as a stimulus to develop this skill that Kate has. The experience does not need to be personal; knowledge-based experience will be enough. When Kate, for instance, sees a picture where a ceramic hob from a kitchen is damaged by a fall of canned food, she realises that any heavy object above the ceramic hob is a hazard, and starts thinking about scenarios initiated by falls of heavy objects, and about relevant preventive/mitigating controls.

5.5.2 Hypotheses about roles of scenarios

This is quite a common way of thinking. Information about incident serves as an empirical information about a hazard and its behaviour. The term behaviour is used here in accordance with Benner and Carey (2009). When they write about behaviour, they mean actions of animate and inanimate actors (examples, in case of Kate and William's kitchen, could be William's behaviour or behaviour of ceramic hob).

It is possible that the ability to spontaneously develop incident scenarios based on experience gained from observing hazard behaviour is a result of evolutionary selection. For example, we know that for our ancestors living in the cave, the presence of the sabre-tooth tiger in the neighbourhood represented a hazard. It is undeniable that the ability to imagine a scenario initiated in this hazard (ability to predict what can happen if a tiger lurks in front of the cave) and the ability to prepare appropriate preventive/mitigating controls in order to minimise the damage caused by the realisation of this hazard was an advantage during human evolution.

Kate bases her identification of EWSs on the idea of possible incident scenarios. She imagines the scenarios of possible fires in the kitchen and therefore she perceives the above-mentioned EWSs as unacceptable. Kate actually says what is well known from risk analysis:

- Scenarios make it possible to foresee the risk comprehensively.
- Scenarios are a practical tool for thinking about risk.

In addition, since the EWSs are indicators of increased risk described by scenarios, it is expected that Kate may add:

- Early warning signs (EWSs) can be derived from scenarios.
- Scenarios are a practical tool for identifying and prioritising the EWSs.

This set of statements or hypotheses about roles of scenarios will be used as milestones in the following text. First, the usefulness of scenarios for lessons learning will be highlighted. Then it will be shown that (i) lessons learning using scenarios can reach EWSs through the identification of causal events, (ii) results of lessons learning via scenarios can be used for various purposes, and (iii) the use of scenarios as a tool to obtain EWSs has many of the required attributes of lessons learning tools.

5.5.3 Scenarios make it possible to foresee the risk comprehensively

Origins of danger are called hazards. Definition from CCPS (2008) states that hazard is a physical or chemical condition that has the potential for causing harm. Hazards in the industrial environment is usually associated to the presence of a dangerous substance or a possibility of an undesirable reaction or an accumulation of energy.

In case of William's kitchen, the three hazards identified are the following: bottle with oil close to the stove, potential for oil in the frying pan to ignite, and heavy bowl on the shelf above the ceramic hob falling. In case of an industrial plant, the three hazards may be the following: presence of volumes of explosives, potential of decomposition reaction in the explosive, and the energy of compressed air in piping of filling machine.

Hazards can be systematically identified. Several suitable techniques were developed for this purpose. Probably the most universal techniques for hazard identification in industrial installations are FMEA and HAZOP (See CCPS 2008).

Mere identification of hazards however does not say too much about the risk that is connected with a process or with an operated system. Presence of the bottle with oil in the kitchen means only that the risk connected with the use of kitchen cannot be zero. Three reasons exist why mere knowledge about present hazards is not enough:

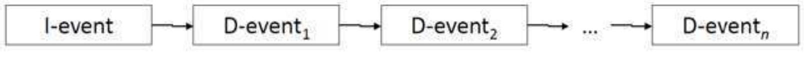
- The article by Kaplan and Garrick (1981) reminds us that risk increases with the increasing presence of hazards, but it also decreases according to measures which are intended to keep control over hazards. Some of such measures may prevent realisations of hazards, and others may mitigate the effects of realisations. Various types of these measures are called barriers, safeguards, regulations, or layers of protection. Here we will mostly use the term controls or preventive/mitigating controls, which seem to be the most general.

- The risk is not only influenced by the interaction of hazards and controls, but also by the interaction of hazards among themselves. This refers to the terms domino effect or knock-on effect. For example, the ignition of the oil in the pan can develop into the ignition of the oil inside the bottle.
- The magnitude of the risk is also influenced by local environmental conditions that change, regardless of hazards and controls. For example, the development of a fire in the kitchen may be different depending on whether the door and/or the window are open. The risk of the industrial plant varies according to the propagation of the shock waves and the gas clouds.

All three reasons mentioned above explain that scenarios describe the complexity of real danger much better than mere hazards. Kaplan and Garrick (1981) consequently argued for this and defined risk as a set of scenarios s_i, each of which has a probability p_i and a consequence c_i. Although this approach has its limits which are discussed in (Aven, 2008), it is preferable when we think about the use of scenarios.

5.5.4 Scenarios are a practical tool for thinking about risk

Crowl and Louvar (2011) state that scenario is a description of the events that result in an incident or accident. According to Marshall and Ruhemann (2001) scenarios describe how the situations can develop when a hazard starts to realise. The above verb "realise" means the process of an event or events by which the *potential* in a hazardous system becomes *actual*. In accordance with this idea, the scenarios are sequences of events in which the first event (initiating event) starts the realisation of a hazard. The sequence can, but does not have to, include other - developing - events in addition to the initiating event. See Figure 1. Developing events may be undesirable events in the hazard, failures or successes of different controls, application of different environmental conditions, or escalation of development to other hazards present.



where *n* is any natural number or zero

Figure 1. Scenario.

In the kitchen, Kate thinks about fire scenarios; in the plant, she would imagine explosions related to the production of emulsion explosive charges. For example, in the kitchen, a scenario may start by the ignition of the oil in the frying pan; followed by extinguishing of fire or by escalation of fire triggering other hazards, including the oil bottle in the vicinity of the stove; and develop until the fire spreads to the entire fire load in the kitchen.

Such scenarios are called incident scenarios since they cause non-negligible damage. Such scenarios have two substantial properties:

1. Each scenario represents one possible interaction of real conditions in the process/system. The scenarios not only take into account the hazards in the process/system but also the ways in which these hazards are realised, how the controls fail or succeed, how the hazards interact and how environmental conditions contribute to the development of the incident.

2. Each scenario represents one contribution to the risk of process/system. Each incident scenario represents one possibility of how damage may arise in the process/system. Or each scenario represents one part of the risk according to the classical definition by Kaplan and Garrick (1981).

Kate obviously has in mind both these two properties when saying that scenarios make it possible to see the risk comprehensively. In accordance with the article by Kaplan and Garrick (1981), the risk of process/system is for her a set of all conceivable incident scenarios in the process/system.

Kate also feels how important the description of scenarios is for thinking about risk. If the scenario describes a specific accident/incident that happened in the past, its description will contain the information relevant to the understanding of its origin, i.e. the origin of this specific part of risk. If a scenario describes a generic incident/accident that may happen in the future, it in fact represents a group of similar specific scenarios. It is accordingly called a representative scenario and explains the origin of a subset of risk.

Having in mind all the preceding properties of scenarios, we start to be aware of another very important feature of scenarios: their clarity and transparency makes them very powerful in explaining the risk to the general public. Scenarios may serve as an extremely useful communication tool with the general public.

5.5.5 Incident scenarios may be results of prospection

Prospective scenarios arise by developing initiating events in hazards. Event trees are commonly used to represent and create them as it is described e.g. by CCPS (2000, 2008). An example event tree is in Figure 2. Figure 3 contains the same list of scenarios as the event tree in Figure 2.

When an analyst constructs an event tree, he starts from a known initiating event in a hazard, knows the behaviour of hazards, and is aware of controls and environmental conditions. He usually begins by considering how and in what order after the initiating event, the controls and environmental conditions should be applied to minimize the damage caused. This sequence of events is called success scenario. Success scenario defines heading of event tree. In Figure 2 it consists of the initiating event and three developing events.

The analyst then considers what the negations of controls and environmental conditions may cause in the development of an incident. He records the findings in the tree graph below the heading. This way he creates a list of prospective incident scenarios, which start with the selected initiating event.

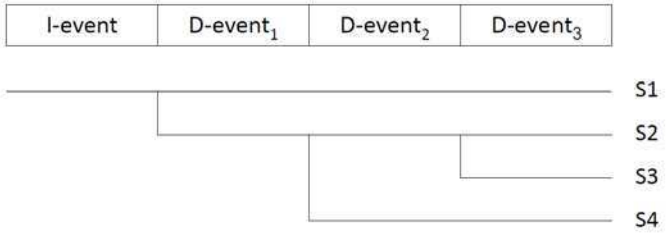


Figure 2. Event tree.

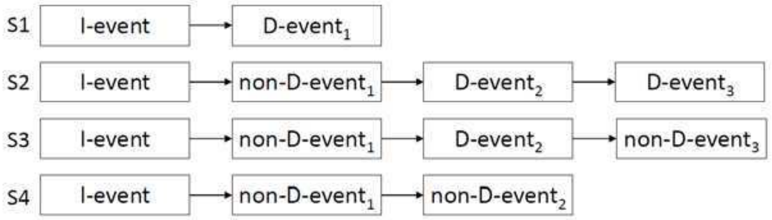


Figure 3. List of incident scenarios from event tree in Figure 2.

Regarding risk analysis, which is essentially a list of scenarios, sometimes it is said that classical approaches to the identification of possible scenarios, which are described by CCPS (2000, 2001, and 2008), do not necessarily reveal all possible scenarios. Scenario-based techniques such as red-teaming (DoD 2003) and anticipatory failure determination (Kaplan et al 1999) can also be used to challenge existing safety cases, attempting to find gaps in the accident scenarios that have been analysed (Masys 2012).

Scenario-based exercises can also be used for simulation-based training exercises which aim is to improve system resilience by strengthening operators' knowledge of system and safety barriers operations.

5.5.6 More about prospective scenarios

Event trees do not represent the only way to identify the prospective scenarios.

Event sequence in an event tree that starts by an initiating event and resulting in an outcome, may be a relatively long and detailed. But it may be simplified and reduced to a mere pair of initiating event and related outcome. This approach represents a starting point for layer of protection analysis (LOPA) described by CCPS (2001).

A bow tie according to CCPS (2008) or according to Hatch et al. (2019) represents another alternative to an event tree. Bow tie is more detailed than the event tree, since the initiating event is expanded into a tree of event causes.

In Part 5.5.4. it can be noticed that a single prospective scenario usually represents a group of similar specific scenarios and is accordingly called a representative scenario. In majority of cases, when individual prospective scenarios are mentioned they could be replaced by sets of scenarios. If bow-ties were used instead of event trees to illustrate scenarios, this would be evident.

Extensiveness, complexity, and level of detail of representative scenarios depend substantially on how the individual events in the sequence are described. Above all, the resolution whether the sequences are characterised in terms of (i) fulfilment of safety functions, (ii) intervention of protection systems or occurrence of physical phenomena, (iii) successes and failures of individual components, may substantially influence the extensiveness and specificity of scenarios. Zio (2007) discusses this problem in more detail.

However, whether event trees, LOPA pairs or bow-ties are used to represent scenarios, it can always be said that scenarios can be used in fully quantitative, semi-quantitative and fully non-quantitative modes. The first one is suitable for quantitative risk estimation, the latter for communicating on risk with non-specialized people, which is mentioned at the end of Part 5.5.4.

5.5.7 Incident scenarios may be results of retrospection

Retrospective accident scenarios are created as a result of the reconstruction of incidents in the process/system. According to Johnson (2003), such reconstruction is always necessary during the investigation regardless of the method used to analyse the causes of the incident.

Retrospective scenario is a sequence of events. But its first event does not necessarily have to be identical with the initiating event that starts the realisation of a hazard. The sequence can, but does not have to, include developing events. Developing events are not limited to undesirable events in hazards, failures or successes of different controls, applications of different environmental conditions, or escalations of development to other present hazards. In addition, the most surprising and unpleasant difference of retrospective scenarios from prospective scenarios is that they do not consist only of one line of events but may variously branch and splice. Example of a retrospective scenario is shown in Figure 4.

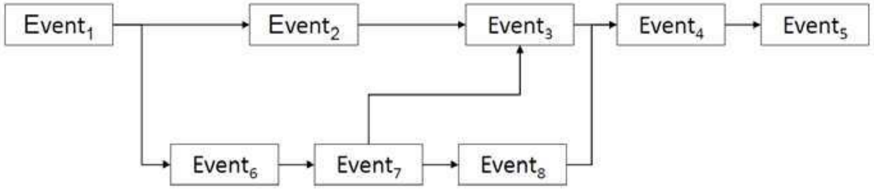


Figure 4. Example retrospective scenario.

Retrospective scenarios generally represent multilinear sequences as described by Benner (1975). Excessive events result from a descriptive effort that does not take into account only undesirable events in hazards, failures or successes of different controls, applications of different environmental conditions, or escalations of development to other present hazards. Branching and splicing (examples can be seen in Figure 4) is result of taking into account different actors, as described by Benner (1975).

In the kitchen, Event_1 can be “Start of frying in the pan”, Event_2 “Chicken breast is fried in oil”, Event_6 “William attempts to take the bowl from the shelf above pan”, Event_7 is “Bowl falls down on the pan and ceramic hob”, Event_8 may be “Ceramic panel above electric heaters is broken”. Event_3 may be “Frying pan overturns” and Event_4 may be “Spilled oil ignites”. In such a case Event_7 will be determined as an initiating event according to Benner’s (1975) definition. Event_8 and Event_3 are failures of controls, and Event_4 is an undesirable event in hazard.

Again, the picture resulting from the retrospection may be more complicated as events in the diagram (for instance Event_7), may be expanded into trees of their causes. The overall picture may then resemble a bow-tie diagram.

5.5.8 Both prospective and retrospective scenarios can be used for lessons learning

Today's designer or an operator of an industrial system, or for instance, a food safety regulator (see Afonso at al., 2017) may think about the realisation of hazards just like Kate thinks about heavy objects over a ceramic hob or like a cave dweller thought about a lurking tiger. For such thinking, it is necessary to know the behaviour of the relevant hazards, to understand them based on natural science or to have experience with them. Scenarios can then be used as a tool that supports the thinking. The effectiveness of such thinking can be enhanced by adopting appropriate techniques.

Benner and Carey (2009) do not limit the use of the term “investigation-oriented lessons learning data sources” only to retrospection related to experienced accidents or incidents, but also to potential or hypothesised accidents or incidents originating from hazard and risk analyses.

Similarly, also here investigation is related both to retrospection and prospection. Incident scenarios can arise in two ways: as a result of retrospection (incident analysis) or prospection (risk analysis). These two options will be discussed in detail in Part 5.

5.5.9 Desirable attributes of scenarios as tools for lessons learning

Based on the preceding considerations, together with Kate we would like to use the scenarios as a tool for lessons learning, namely for the development of EWSs. Benner and Carey (2009) analysed desired attributes of lessons learning tools. They showed that the development of lessons learned can be divided into investigation and documentation. Investigation should support production of lessons-to-be-learned source data. Documentation should facilitate satisfaction of desired user criteria.

If scenarios are to be used in investigation, they need attributes like:

1. A stated investigation purpose of providing lessons learned leading to changed future behaviours.

- For example, Kate could intend to investigate accidents in all the kitchens of all the Williams living throughout the UK, to improve their safety during cooking.

2. An input-output framework for describing what happened, enabling lessons learned data sets, to describe behaviours to change in non-judgmental and logically verifiable terms.

- For example, Kate would require every kitchen accident to be described as a finite set of sequences of simple sentences beginning with an initiating event and ending with a damage description.

3. A focus on behaviour data acquisition and processing, to enhance efficient documentation of lessons learned from accident-generated lessons learning source data.

- For example, the sentences in the sequences would have to describe actions of animate or inanimate actors, or behaviour.

4. Specifications for behavioural building block structure, grammar, syntax, and vocabulary and a structure for input data documentation, to ensure data consistency and economy, and facilitate data coupling and support for documenting lessons learned.

5. Machine support for input data sequencing, parsing, coupling, concatenation, data set display and expansion capabilities, to facilitate lessons learned processing and dissemination, and to reduce latency.

6. Objective quality assurance and validation process for behavioural data sets.

The three above-mentioned examples show that scenarios are able to fulfil the requirements of attributes #1 to #3. Attribute #4 requires the introduction of certain standards on how the events are described, and how the conditions are replaced by the events. Vocabulary can be limited to definite lists of actors and/or actions using checklists. Such a standardization is easier to reach in the industrial environment than in a kitchen since in the industry it may be supported by a marking system. In the kitchen it would need to use, e.g. for the bottle with oil, always the same term.

Attribute #5 is connected with the use of computers for recording the scenarios, which is achievable especially when the attribute #4 is fulfilled. Attribute #6 states only that the use of scenarios for lessons learning cannot be considered satisfactory if it is not subjected to quality assurance.

5.5.10 Attributes of scenarios desirable for documentation part of lessons learning

According to Benner and Carey (2009), desired attributes for documentation would include:

1. Efficient tools to facilitate documentation of behaviour data sets, and reduced latency.

2. Specifications for lessons learned behavioural data outputs meeting users' needs, harmonized with other learning organisation lessons learned sources or knowledge management artefacts, with maximised signal-to-noise ratios, providing context, minimising interpretive and analytical workload for users, and reducing latency.

3. Machine lessons learned processing support and repository uploading capabilities, to accelerate lessons learned documentation and deployment into all repositories.

4. Internet lessons learned output data repository and notification capabilities, to facilitate "push" or "pull" lessons learned data dissemination, enable wide deployment, and minimise latency.

5. Rapid repository access, search and filter capability, to minimise user access time, cost and workloads.

6. Objective lessons learned quality assurance and validation functions, to enable developer to ensure lessons learned quality before entry into repositories.

7. Lessons learned repository modification or updating capability, to ensure lasting lessons learning quality.

The second set of attributes by Benner and Carey (2009) seem to be very demanding, much different from the state existing in many industrial environments. Evidently, they saw the attributes from a very general perspective and created a description of “an ideal state”. Doubtlessly, without the use of computerised database tools they cannot be achieved nor even approached. But hopefully in very simple cases as our kitchen case, the documentation of scenarios may be reasonably used for lessons learning even if it does not achieve the most ambitious standards.

5.6 Lessons learning can reach EWSs through the identification of causal events

5.6.1 Causal events in retrospective incident scenarios

The main purpose of lessons learning is to identify what behaviour of actors was wrong and what behaviour has to be improved in order to prevent or mitigate the recurrence of an incident. Identification of wrong and improvable behaviour is possible, as soon as the incident scenario is reconstructed. The reconstructed scenario usually contains not only individual events, but also a description of context in which the events occurred. Context is described as a set of conditions.

If the analysis of the retrospective scenario is aimed at preventing the repetition of the same or similar scenarios, it must focus on those events in the scenario that worsen the control over a hazard. The events in the sequence have to be identified that influenced unfavourably the behaviour of actors and thus, contributed to the incident.

These events are often called causal factors. CCPS (2003) defines causal factor as a negative event or undesirable condition that, if eliminated, would have either prevented the occurrence (= incident scenario) or reduced its severity or frequency. Since this definition permits causal factor to be a condition, we will modify it slightly. We will require the conditions always to be linked to events which context they describe (we suppose that such a state is always achievable). Then we leave the term causal factor and define causal event as a negative event, including its context that if eliminated would have either prevented the occurrence or reduced its severity or frequency.

Let us suppose that Event$_5$ in Figure 4 is “William uses the fire extinguisher”. This event itself does not seem to be a causal event. But if Event$_5$ happened in the context that William was not able to initially use the extinguisher and hence, the extinguishing started much later than possible, then the Event$_5$, including its context, would visibly be a causal event.

Another approach to retrospective scenarios requires to replace all the conditions within the chart by (sequences of) events. This approach relates to the explanations added as Epilogue to the original article by Benner (1975). The advantage is that constraining the flow chart to events is always possible and solves the problem. (Way to the exclusion of conditions is commented in the end of Part 5.6.6) Causal factors will be then represented only by events and be identical to causal events.

Ideally, the set of causal events represents the set of necessary and sufficient events explaining HOW the incident occurred, while the scenario itself explains WHAT occurred. A reconstructed incident scenario is reduced to a set of causal events during the retrospective incident analysis.

For the incident scenario that might be represented by Figure 4, the set of causal events is Event$_7$ (bowl falls on the pan and ceramic hob), Event$_8$ (ceramic panel above electric heaters is broken), Event$_3$ (Frying pan overturns), Event$_4$ (spilled oil ignites) and Event$_5$ (William uses fire extinguisher later than possible).

5.6.2 Causal events in prospective incident scenarios

Analysis of incident scenarios using event trees uncovers possible interactions of real actors in the system, i.e. interactions of present hazards, controls and environmental conditions. For most of the events in the tree, it is valid that they can change within a certain range without changing the scenario. For example, if in the tree in Figure 2 the initiating event is the ignition of oil in the pan, and the first developing event is a fire intervention with a lid, then the fire intervention can take place at any time within a certain time interval of about tens of seconds without changing the course of the scenario. An event tree analyst considers the ranges within which the events can be changed. Individual scenarios from the tree thus represent whole classes of somewhat different scenarios, which however do not differ in qualitative terms, i.e. by the type of events involved. The event tree thus contains representative incident scenarios. For more details see, for example, article by Kaplan et al. (2001).

Prospective scenario analysis can be used even before the precise form of the individual conditions in the process/system is known. Once an initiating event is defined, all the safety functions that are required to mitigate the incident must be defined and organised according to their time of intervention as Zio (2007) describes it. In the case of ignition in the frying pan, we could consider immediate firefighting, limitation of propagation, delayed firefighting, and extinguishing by an external fire brigade. Defining safety functions can be very useful in the design phase because it can be used to define controls.

Prospective analysis typically seeks to investigate systematically all representative initiating events and related incident scenarios. Scenarios created by prospective analysis take the form of conjunctions of events from which no event can be removed. When thinking about risk, events in scenarios that represent degradation of control over hazards are at the heart of interest. If the convention is kept that the tree heading contains a success scenario, then events that represent degradation are both initiating events and all events that negate successes from the heading, i.e. all the events starting in Figs 2 and 3 with the word "non".

Above we defined causal event as a negative event including its context that if eliminated it would have either prevented the occurrence or reduced its severity or frequency. This is the exact description of both initiating events and negating events in the event tree. Thus, initiating event and negating events in the event tree can be called causal events.

Therefore, prospective analysis using event trees can serve as a tool for the systematic identification of all possible (representative) causal events in the process/system. Visibly, this conclusion does not depend on the form of scenarios mentioned in Part 5.5.6.

In addition, it can be shown that the simplified prospective scenarios used in the layer of protection analysis by CCPS (2001) can serve as a tool for the identification of possible causal events in the process/system. In this case, failures of layers of protection can be identified as causal events.

Similarly, we suppose that all other methods of identification of prospective scenarios can be used to identify causal events.

5.6.3 Comparison of role of causal events in prospection and retrospection

While prospective analysis attempts to predict all possible causal events that might occur, retrospective analysis identifies the combination of causal events that actually occurred. If analyses are flawless, then retrospective analysis should result in one of the scenarios created by prospective analysis.

Nevertheless, if we have a set of possible incident scenarios created by a prospective analysis for the process/system, it is not certain that the scenario generated by the incident retrospection in this process/system can be quickly identified with one of the prospective scenarios. There may be several reasons for unsuccessful identification:

(i) Retrospective analysis may mix several scenarios that took place concurrently;

(ii) Scenario events in retrospective analysis are determined in more detail than those in prospective scenarios;

(iii) Certain conditions that worsen the control over a hazard in real undesirable event in the process/system may be omitted in prospective analysis.

These practical findings represent some of the motivations for achieving the attributes quoted in Parts 5.5.9 and 5.5.10 when using scenarios as a lessons learning tool. Theoretically, such problems should not arise if all the attributions according to 5.5.9 and 5.5.10 are reached. Nevertheless, we know that reality still is quite far from Benner and Carey’s (2009) ideal.

Nevertheless, it is true that the most important common finding is as follows: in both prospective and retrospective scenario analysis, the main outcome in terms of safety is always a set of events that represent a worsening of control over the hazards to which our attention should be focused. In other words, in both cases our interest focuses on events called causal events.

5.6.4 Scenarios make visible the threatening conditions in the process/system

The previous parts have shown that *any incident scenario can be reduced to a set of causal events*. The set of causal events represents a combination of events worsening the control over the hazards. They are at the same time the combination of necessary and sufficient conditions for consequences and frequency of this incident scenario. The causal events can be represented by the following:

- initiating event in the hazard, or
- failures of the measures intended to mitigate the realisation of a hazard, or
- failure of the measures intended to prevent the realisation of additional hazard, or
- events adversely affecting the environmental conditions influencing the realisation of hazards.

This result shows that the scenarios make visible the ways in which hazards realise (come to be) in a particular process/system. They visualise the real role of hazards and related controls and environmental conditions in a particular process/system. This visualisation is the basic purpose of both risk analysis and undesirable event analysis.

5.6.5 Better than prospection or retrospection is the combination of both

Retrospectively, i.e. based on experience with specific undesirable events, only specific accident scenarios can be revealed within the incident cause analysis. From a logical point of view, this is an inductive process. Its advantage is that it identifies the real weaknesses of control over the hazards, usually the most likely ones. It may also reveal weaknesses that within risk analysis remain hidden from our eyes for their delicacy. The disadvantage is that it reveals only some weaknesses and scenarios, not necessarily those that most contribute to the risk. The disadvantage may also be that, in the analysis, causal events are not identified in a sufficient manner. The results may mistakenly adhere only to the partial weakness, which is only a contribution to the general causal event.

Prospectively, i.e. based on a process/system analysis, the risk analysis can reveal theoretically all possible incident scenarios. From a logic point of view, this process is deductive. (This means, of course, that it also contains the inductive component - general rules on behaviour of hazards and controls based on experience). The advantage of this approach is that it systematically searches for all weaknesses in the control across all the hazards. It is able to reveal all the weaknesses and scenarios, including those with low frequencies. It can also reveal weaknesses that, by mere application of experience, remain hidden from our eyes. The disadvantage of the prospective approach, however, is that the analysis cannot avoid various neglects and simplifications because of which some substantial interactions of hazards and controls may be omitted. Hence, the outcome of the prospection may appear to be complete, but in reality, substantial scenarios are missing.

Since it is difficult to avoid the above-mentioned errors when using these approaches, the combination of a prospective and a retrospective approach seems to be a practical and realistic approach to identifying scenarios.

5.6.6 Early warning signs are causes and indicators of causal events

We realised in the previous parts above that *a set of scenarios makes the risk of the process/system visible as a set of sets of causal events*. As we have already mentioned in Part 5.4.1, the essence of foresight is the capability to see EWSs or indicators of problems that could lead to an incident, or the indicators of risk increase. In the context in which risk is decomposed into incident scenarios, and incident scenarios are in turn decomposed into causal events, foresight thus, means the ability to see the signs that some identified causal events could actually occur. In particular, we would like to be able to see signs of possible occurrence of causal events that contribute most importantly to the risk.

It follows from the previous paragraph that the EWSs can be identified as the causes of causal events including causal events themselves, or indicators of causal events, or indicators of causes of causal events. (Among indicators, the leading indicators are preferred.)

This finding means that a correct and complete identification of causal events is of essential importance. An unidentified causal event (CE) represents an invisible set of EWSs, existence and importance of which stay unknown.

In this context it has to be strongly recommended to follow the Epilogue by Benner (1975) and exclude any possibility that a causal event would stay hidden given the presence of conditions within the scenario (retrospective) description. There are various ways how to do this. An approach shown by Accou and Reniers (2018) is a promising way that excludes conditions from a descriptive chart of a scenario and replaces conditions by events. The universal model of safety management activities (safety fractal) promises to help identify a possibility and sort of such a replacement for any condition within the chart.

Also it is recommended to perform a check of identified causal events by rewriting each of them as an adverse influence acting on a vulnerable target due to missing barriers or regulations. This approach originates in MORT by Johnson (1973) and warrants that all CEs identified correspond with the definition of causal events.

5.6.7 Possible approaches to identification of event causes

Unfortunately, the concept of causes does not have clear and unambiguous content. If we talk about the causes, we can talk about many kinds of events and ideas. Nevertheless, it can be repeated here, that the EWSs represent causes of causal events, *whatever the causes mean*.

In technical practice, at least direct causes and underlying causes are usually distinguished. Smaller differences exist with respect to direct causes. They are physically detectable failures, errors, states, conditions, the combination of which leads to an occurrence of causal event.

But there are quite different ideas in various approaches to incident analysis about what are the underlying causes. In the relatively common root cause analysis (RCA) methods, the underlying causes are called root causes and represent deficiencies in the implementation of a safety management system. They could also be referred to as organisational causes.

Verschueren (2018) is focused on the organisational causes and their relation to EWSs. He underlines the importance of organisational dysfunctionalities. According to Verschueren (2018) organisational dysfunctionalities can be detected and can act as EWSs.

General acceptance of contemporary focus on organisational causes is confirmed in Hollnagel (2014):“In the thinking about types of causes, we see a development that goes from technology to the human factor and, most recently, to the organisations and to culture.” In accordance with this, most part of contemporary methods of cause analysis agrees with the idea that organisational causes have to be searched for. They attempt to identify them.

A hierarchy of checklists, called root cause map, is often used to determine underlying causes in RCAs and improved RCAs. Such an approach is described in CCPS (2003). An example of elaborated analysis method that is nowadays used in industry can be found in a paper by Nicolescu (2018) where the method of the Investigation Body of Norway, AIBN, is applied to identify causal events (direct causes) and a tool named SMS wheel is applied in order to identify underlying causes.

Improved RCAs such as described by Ferjencik (2014) would include also the underlying causes in safety culture or attitudes of local management. As shown in the article by Ferjencik, guidelines by CCPS (2007) are useful for this purpose.

There are at least two examples of alternative methods to determine direct and underlying causes. Symptoms would be determined with analysis by ESReDA (2009). Failing processes would be identified instead of root and underlying causes in an analysis by Leveson (2004). Nevertheless, for both approaches, the identification of causal events according to the definition used here would be the necessary starting point. For Leveson’s approach, it is shown in Stoop and Benner (2015). Leveson’s analysis process starts with a step *Identify the systems and hazards involved in the loss*. This requirement can be translated into *Identify the controls and hazards involved in the loss*. Causal events point to such an identification.

This diversity means that EWSs and searching for EWSs can have very variable forms. While these differences in our understanding of causes can discourage us, they all point to the same general fact: EWSs can be determined from incident scenarios as (partial) causes of relevant causal events.

Example: The determination of causal events is very easy in conventional event trees. Four causal events are present in Figure 2 according to Figure 3: I-event, non-D-event$_1$, non-D-event$_2$, and non-D-event$_3$.

Various techniques and approaches can be used for the identification of causes of causal events. Fault tree analysis (FTA) that is recommended in book CCPS (2003), is very productive in prospective analysis. Figure 5 shows possible results of application of FTA to two causal events. It can be observed from Figures 2, 3 and 5 that cause1, cause2, and cause3 represent EWSs for all scenarios S1 to S4. Cause4 and cause5 are EWSs only for scenario S3. Cause2 indicates the possibility of formation of both causal events at the same time. Cause2 may represent a sort of common cause failure. Typically, the EWSs with common-cause nature may be the deficiencies in the local safety management system i.e. underlying causes.

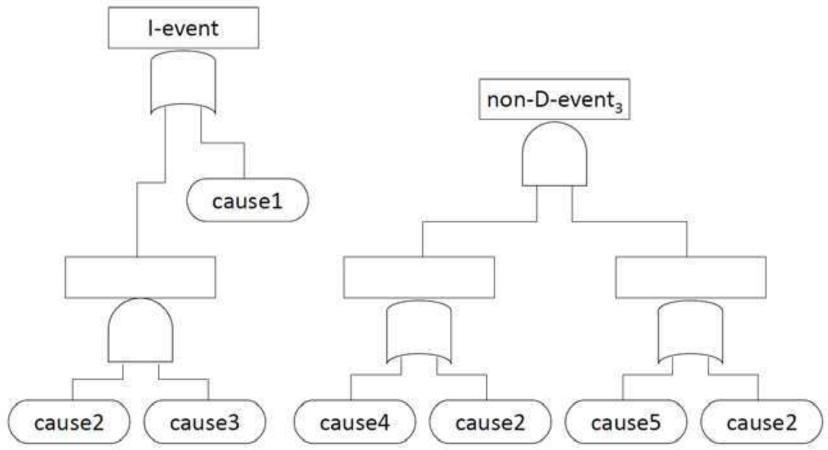


Figure 5. Causes of two causal events from Figure 2 and 3.

5.6.8 Steps to the identification of EWSs

The identification of EWSs begins when the incident scenarios are constructed. They make visible the realisation of hazards, which is the main purpose of the construction of incident scenarios. Scenarios allow the identification of causal events. They make visible the roles of hazards and controls of hazards. Once causal events are known, a way to make EWSs visible is open. Therefore, the visibility of the EWSs emerges through the visualisation of the role of hazards and controls of hazards.

Scenarios can help see the EWSs in two steps. In the first step, we determine the causal events in the incident scenarios; in the second step we determine the causes of the established causal events and indicators of causal events and their causes.

In prospective analysis, causal events are determined as:

- events in hazards that initiate realisation of hazards,
- events in hazards that escalate damages,
- events that represent failure of controls over realised hazards,
- events that allow damage escalation by setting up adverse environmental conditions.

In a retrospective analysis, causal events are selected as events that meet the definition of causal event.

In case of prospective analysis both the elaborated form of scenarios that is used within quantitative risk analysis (and modelled with the help of ETA, FTA, and HRA or with the help of bow ties), and the simplified form of scenarios typical for layer of protection analysis (modelled as an initiating event – consequence pair) can be exploited.

Practical note:

To be used efficiently as a tool for EWS identification, the set of scenarios should not be excessively wide, the scenarios should not be too specific, and the identification of EWS should not be limited to specific direct causes represented by the failures/errors. The set of scenarios should:

- be limited to selected critical scenarios,
- have description of scenarios that prefer functions (not elements),
- have EWSs that are identified in underlying layers, too, i.e. as deficiencies of the safety management system.

5.6.9 Variability in identification of EWSs

As it is visible from preceding parts of the chapter, the detailed understanding on what are early warning signs can be substantially variable. There is no single possible way to identify EWSs. Nevertheless, a few important findings can be stated:

- Based on the definition and procedure for identification of EWSs, it can be understood why we may have known and unknown EWSs and what their existence may signify.
- Based on the understanding of relations of causes, it can be understood why there may be synergic relationships among EWSs.
- Based on the fact that EWSs may be causes it can be understood that Cube (Chapter 8, Stoop et al., 2020) may be applied to identifications and checks of EWSs.

5.7 Application of scenarios as a tool for lessons learning

5.7.1 Example: Kitchen prospection

A frying pan filled with oil is a hazard in the kitchen. Kate worries that the oil in the pan may ignite - she considers the ignition of the oil in the pan to be a possible initiating event. Rapid extinguishing by laying the lid on the pan minimizes damage after the initiating event. If this does not happen, further development depends on whether there is another hazard near the pan - a plastic bottle of oil. If it is not there, the damage is minimized, i.e. it can be expected that the oil in the pan will burn out, the smoke will cause damage, but the fire will not expand further. If the bottle with cooking oil is present and stays nearby, it is a matter of time when a large amount of burning oil is spilled on the stove and on the floor. At this point, the rapid use of a suitable fire extinguisher can minimize damage. If the extinguisher is not used quickly, the fire will spread across the room. Further development depends on whether the door is opened into the adjoining dining room or whether it is closed. Closed door minimizes damage, in the sense that when the fire breaks out, the window and becomes noticeable from the outside of the house, no further rooms are hit so far. If a fire-fighting car arrives in time, it will save most of the house from the fire. The success scenario consists of an initiating event and five developing events.

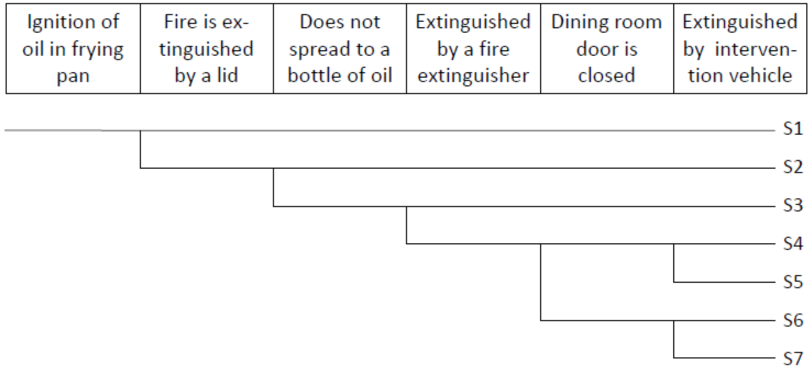

Ignition of oil in frying pan
Fire is extinguished by a lid
Does not spread to a bottle of oil
Extinguished by a fire extinguisher
Dining room door is closed
Extinguished by intervention vehicle
S1
S2
S3
S4
S5
S6
S7

Figure 6. Analysis of possible developments of ignition of oil in frying pan.

Three of the developing events are the use of controls, one event is the realisation of another hazard, and one can be considered to be the application of the environmental condition. The entire event tree (Figure 8) contains seven incident scenarios.

Six causal events are determined: ignition of oil in frying pan; fire is not extinguished by a lid; fire spreads to a bottle of oil; fire is not extinguished by a fire extinguisher; dining room door is open; fire cannot be extinguished by intervention vehicle. EWSs in the kitchen can be determined as analysis results of possible causes of individual causal events. For example, William's habit of leaving the frying pan unattended may contribute to the causes of the initiating event and is the cause of the failure of the first developing event. It is therefore a clear early warning signal. Presence of the bottle of oil in close vicinity of ceramic hob, as well as the absence of fire extinguisher in the kitchen will be identified among EWSs.

5.7.2 Example: Kitchen retrospection

Let's imagine that a fire broke out in the neighbourhood of William and Kate. The fire destroyed the neighbour's kitchen. Investigations have shown that the real incident scenario in the kitchen took place as the scenario in Figure 7 shows.

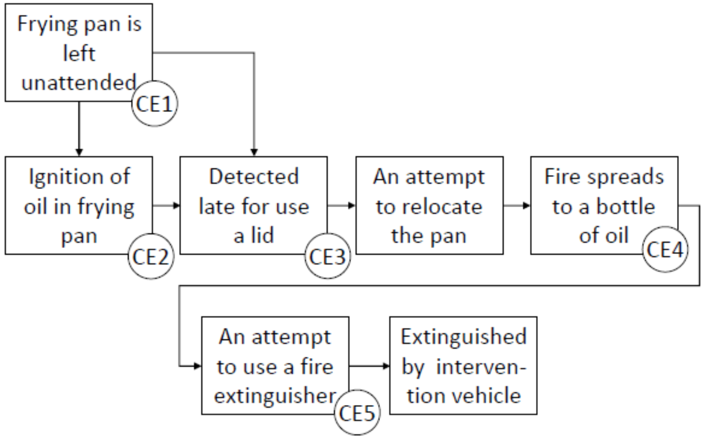

Frying pan is left unattended
CE1
Ignition of oil in frying pan
CE2
Detected late for use a lid
CE3
An attempt to relocate the pan
Fire spreads to a bottle of oil
CE4
An attempt to use a fire extinguisher
CE5
Extinguished by intervention vehicle

Figure 7. Scenario of real incident in William's neighbour's kitchen.

The scenario recalls scenarios S5 and S7 from Figure 6. Because the information about the dining room door status is missing in the scenario, it is not to be expected that this reconstruction of the incident could identify the EWSs causing the door to be opened. On the contrary, the causal event CE1 is identified in the reconstructed scenario, which is missing in the scenarios in Figure 6. The presence of the extra causal event in the scenario can be explained by point (ii) in Part 5.6.3 Causal event CE1 is the cause of causal events that we find in scenarios S5 and S7 from Figure 6. Therefore, this external incident does not bring Kate any new facts she would not know from the prospection. On the other hand, this retrospection makes William change his undesirable habit.

5.7.3 Example: Industrial unit prediction

Let us move from the kitchen into the industrial environment. As an example we will use a unit for production of emulsion explosive charges. (The example is inspired by Ferjencik and Dechy, 2016.) Figure 8 shows a basic arrangement of this plant. Protective walls surround a light building inside of which the automatic filling machine produces explosive charges from the explosive paste. In this environment, William may play a role of personnel and Kate represents his manager.

Initiation of detonation during the start of filling machine represents a possible initiating event in unit for production of emulsion explosive charges. In case that the individual events in the sequence are described as fulfilment of safety functions (see (i) in Part 5.5.6), resulting event tree may look as it is shown in Figure 9.

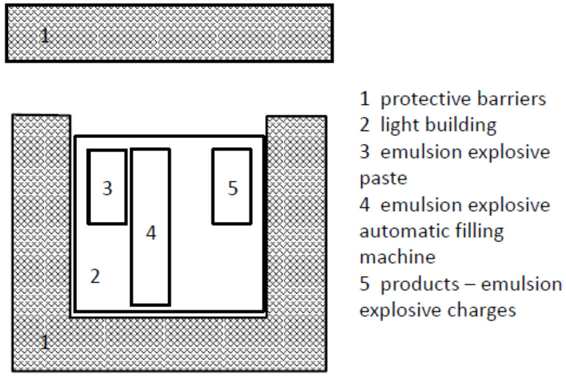

1
1
2
3
4
5
1 protective barriers
2 light building
3 emulsion explosive paste
4 emulsion explosive automatic filling machine
5 products – emulsion explosive charges

Figure 8. Unit for production of emulsion explosive charges (bird's-eye view).

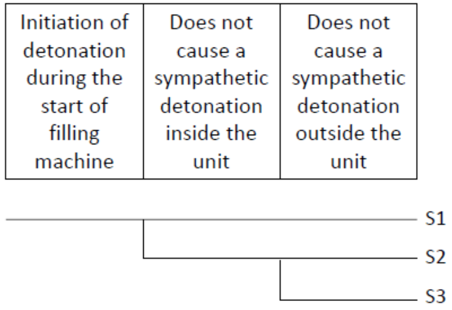

Initiation of detonation during the start of filling machine
Does not cause a sympathetic detonation inside the unit
Does not cause a sympathetic detonation outside the unit
S1
S2
S3

Figure 9. Scenarios of possible incidents in unit for production of emulsion explosive charges.

Causes of sympathetic detonations (inevitable transmission of detonation) have to be analysed in order to identify early warning signs. Typical EWSs that correspond with the second and third identified causal events are excess amount of explosives, inappropriate deployment of explosives, and insufficient resistance of unit.

5.7.4 Example: Industrial object retrospection

Figure 10 shows the scenario that actually occurred in unit for production of emulsion explosive charges.

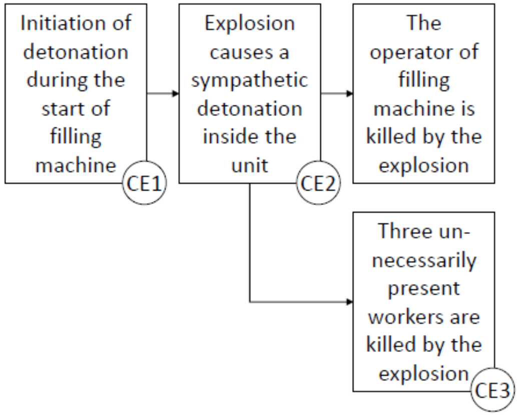

Initiation of detonation during the start of filling machine
CE1
Explosion causes a sympathetic detonation inside the unit
CE2
The operator of filling machine is killed by the explosion
Three un-necessarily present workers are killed by the explosion
CE3

Figure 10. Scenario of real incident in unit for production of emulsion explosive charges.

The scenario contains causal event CE3 that is not identified in the event tree in Figure 9. CE3 represents a fatal impact of a shock wave on three persons present in the he building due to missing protective barriers that could warrant their protection and due to missing regulations that could warrant their absence in the room. This reformulation in accordance with MORT (Johnson, 1973) shows that CE3 really represents a causal event. In this case, the real event revealed a deficiency in the prospective analysis of Figure 9. As stated in Part 5.6.3, point (iii), it was overlooked that controls during the start of filling machine should also include the care of ensuring the absence of surplus persons in the building. In this case, the retrospective analysis reveals EWSs that prospective analysis was not able to detect. An event tree suitable for the identification of relevant EWSs would have to be created by extending the event tree of Figure 9. Its head would include the third developing event “Presence of personnel within the reach of detonation effects is minimised”. This example, which is taken from real experience, illustrates the opinion that the combination of both prospection and retrospection is the better approach, rather than either of them on their own.

5.7.5 Example: NPP retrospection

Figure 11 is reproduced from the paper by Strucic (2017). The figure describes a real incident scenario from a nuclear power plant. The failure of the chiller condenser coil led to the shutdown of all three units at the site. Colour conventions are applied in the scenario. Events are represented by green rectangles, conditions by blue ovals. Red rhombus represents a causal event. In this case, only one causal event is identified (which is identical with an initiating event). The brown circle describes scenario consequences.

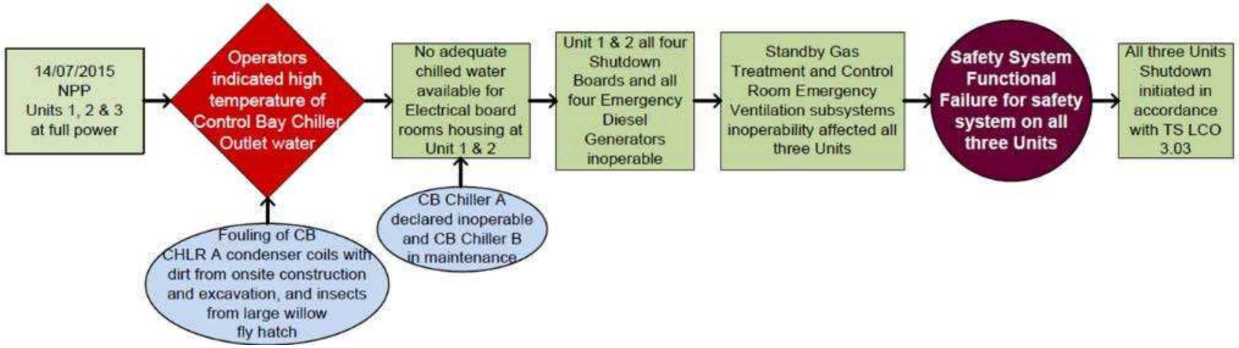

14/07/2015 NPP Units 1, 2 & 3 at full power
Operators indicated high temperature of Control Bay Chiller Outlet water
No adequate chilled water available for Electrical board rooms housing at Unit 1 & 2
Unit 1 & 2 all four Shutdown Boards and all four Emergency Diesel Generators inoperable
Standby Gas Treatment and Control Room Emergency Ventilation subsystems inoperability affected all three Units
Safety System Functional Failure for safety system on all three Units
All three Units Shutdown initiated in accordance with TS LCO 3.03
Fouling of CB CHLR A condenser coils with dirt from onsite construction and excavation, and insects from large willow fly hatch
CB Chiller A declared inoperable and CB Chiller B in maintenance

Figure 11. Incident scenario from NPP according to Strucic (2017).

The identification of early warning signs requires, in this case, the analysis of causes why the fouling of the control bay chiller outlet condenser coils resulting in a high temperature of the outlet water may occur.

Figure 12 reproduces the summary of the analysis of causes of the causal event from Figure 11 according to Strucic (2017).

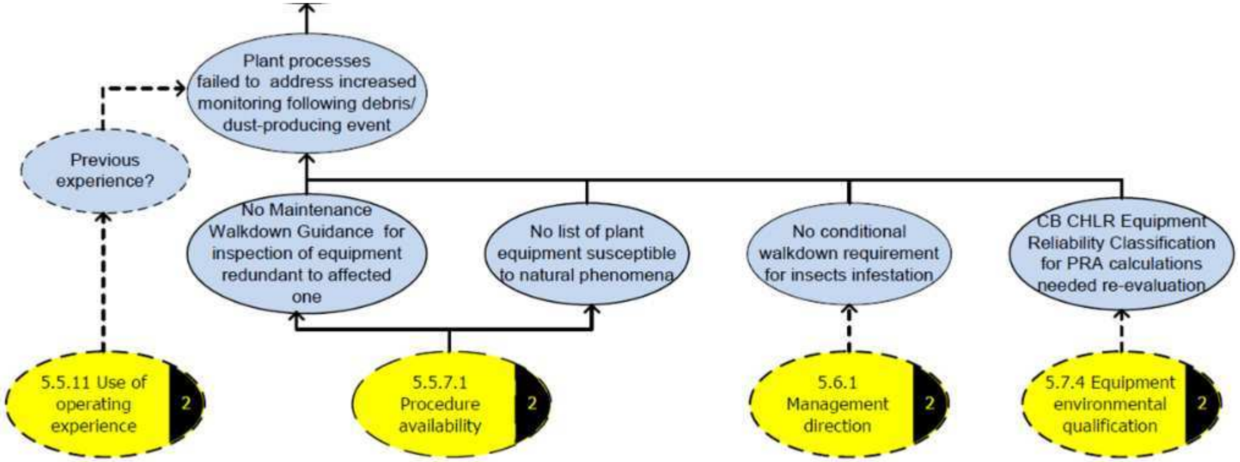

Plant processes failed to address increased monitoring following debris/ dust-producing event
Previous experience?
No Maintenance Walkdown Guidance for inspection of equipment redundant to affected one
No list of plant equipment susceptible to natural phenomena
No conditional walkdown requirement for insects infestation
CB CHLR Equipment Reliability Classification for PRA calculations needed re-evaluation
5.5.11 Use of operating experience
2
5.5.7.1 Procedure availability
2
5.6.1 Management direction
2
5.7.4 Equipment environmental qualification
2

Figure 12. Causes of a causal event from NPP according to Strucic (2017).

Undoubtedly, this graphical summary originates from the analysis that belongs into the family of RCA. This analysis classifies the causes into categories of causes (yellow ovals) in accordance with a manual (i.e. with a list of checklists) and visibly the categories refer to organisational problems. Hence, the analysis uses a prefabricated list of root causes. Terminology of the original analysis is, however, different from the terms used here. Our causal event is called deviation and the term causal factor is reserved for classified root causes.

This cause analysis could be complemented by a fault tree analysing all possible technical causes that can cause fouling of the chiller coil. Some of relevant causes are listed in the description of the condition in Figure 11. Indicators of the causal event or causes of the causal event can be added to the list of EWSs. Increase of temperature on the outlet of chiller or increased presence of willow fly can be examples of such indicators.

5.7.6 Results can be used to list all possible EWSs

Identification of EWSs may result from the identification of causes of specific undesirable events called causal events. Although none of the above examples contains a satisfactory detailed cause analysis, the examples show the way how the identification of early warning signs can be performed and demonstrate that scenarios are suitable for this purpose.

Prospective scenarios are appropriate for the identification of EWSs. They are suitable for a comprehensive analysis of all generic causal events and for the identification of all possible EWSs. This analysis may represent a modification of a systematic risk analysis. Analogous obstacles endanger completeness of the identification of EWSs as completeness of any risk analysis.

Examples also show that retrospective scenarios are appropriate for the identification of EWSs. Nevertheless, the retrospective scenarios cannot be expected to provide a complete list of possible EWSs. They focus our attention only on a certain segment of the complete list. On the other hand, retrospection may easily draw our attention to imperfections and inconsistencies of the specific attempts to identify a complete list of EWSs. This is why in real industrial environment the combination of prospective and retrospective analysis should be considered to be the best possible way to identify early warning signs. Inspiring explanations related to the identification of EWSs in industrial environment can be found in Chapter 7, Strucic, 2020.

5.7.7 Results can be used to prevent loss of memory

Loss of memory means that information, such as:

- the fact that EWSs can arise,
- possible forms of EWSs,
- methods to detect EWSs,
- EWSs that were detected until they are reasonably responded,

(four aspects of memory) is not encoded, stored, or retrieved in minds of humans who can influence form and behaviour of the system.

In accordance with the above description of four aspects of memory, three forms of loss of memory may be distinguished:

- missing knowledge that an EWS can rise in the system,
- missing ability to identify an EWS when it arises,
- missing ability to respond to the EWS that was identified.

These three forms of loss of memory cover all situations, not only those when a specific knowledge or ability has been forgotten (i.e. it was not possible to be retrieved). In addition, situations are covered when this knowledge or ability has never been present (encoded and stored) in memory or has been present (and retrieved) but the will to use it has not existed.

Encoding, storing, and retrieving the above-mentioned information about EWSs represent the documentation of EWSs resulting from lessons learning. Documentation of EWSs can build on the scenario documentation. Documentation of scenarios forms the basis of risk analysis documentation. There is a number of risk analysis documentation technologies ranging from simple procedures to software and database tools.

Kate probably will not require formalised documentation of EWSs resulting from examples in Parts 5.7.1 and 5.7.2. Results of examples in Parts 5.7.3 and 5.7.4 however require proper documentation. The stored results may represent a subset of prioritized process safety information for given socio-technical system according to Wincek (2011). The highest documentation requirements are expected in extremely complicated and sophisticated systems, such as NPP from example in Part 5.7.5. In this case, for instance, a software like Risk Spectrum (refer to www.riskspectrum.com) is conceivable as a documentation tool. More information can be found in Chapter 12, Simic, 2020.

Encoding, storing and making the knowledge about EWSs retrievable are supposed to be actions against the loss of memory. Scenarios as a generally utilised tools make the realisation of EWSs documentation possible.

5.7.8 Results can be used to identify whether a failure/error/condition represents an EWS

Any form of scenarios between an elaborated form of scenarios typical for quantitative risk analysis (modelled with the help of ETA, FTA, and HRA) and a simplified form of scenarios typical for layer of protection analysis (modelled as an initiating event – consequence pair) is expected to be documented.

Regardless of what form of scenarios are being used, the documentation of lessons learning is expected to contain, in addition to scenarios, the causes of causal events. Comparing a specific failure/error/condition with the recorded EWSs makes it possible to determine whether the failure/error/condition represents an EWS.

5.7.9 Results can be used to prioritize EWSs

If the list of identified EWSs is compared with prioritized process safety information for a given socio-technical system, it may serve as a simplified risk analysis of the relevant safety impact or accident near-miss potential of EWSs in other circumstances. As a result, the list of EWSs may be divided into two categories: (a) EWSs, which are important from risk perspective, and thus worth responding; and (b) EWSs not important and not worth responding.

The stored results of risk analysis (critical scenarios) should be characterised in terms of fulfilment of safety functions. Relevant systems, components and/or failure modes or classes of EWS should be readymade within a database serving as a tool for simpler realisation of the task.

Prioritisation of EWSs can be done analogously as determination of quantitative importances of components according to Vesely et al. (1981). Let us assume that prospective analysis of the process/system results in the list of incident scenarios s_i, where i = 1 to N. Let us assume that point estimates of frequency f_i and of damage x_i are determined for each scenario. Point estimates of scenario frequencies are determined with the use of point estimates of frequencies of causes of individual events in scenarios. Point estimate of risk of the process/system R can be determined as a sum of all products $f_i \times x_i$ for i =1, ..., N. Let us determine a modified point estimation of risk R(EWS) as a sum of products $f_i(EWS) \times x_i$ for i =1, ..., N, where frequencies $f_i(EWS)$ are determined with the use of point estimate of frequency of EWS = 0/year. Priority of cause EWS is p(EWS) = R - R(EWS). The higher the priority, the greater the risk reduction can be achieved by suppressing the occurrence of the EWS.

5.7.10 Resulting EWSs may have many of required attributes

Kate may require an ambitious investigation purpose of providing lessons learned. For example, it was suggested in Part 5.5.9 that she may intend to investigate accidents in all the kitchens of all Williams living throughout the UK, to improve their safety during cooking.

In such a case, she needs corresponding software tools, such as Risk Spectrum mentioned in Part 5.7.7, which includes both graphical editors to facilitate investigations and databases to facilitate documentation. With such a powerful tool, it can be expected that resulting EWSs will have many of attributes required in Parts 5.5.9 and 5.5.10.

At this moment, it can be supposed that Investigation attributes 1-3 are easily present and attributes 4-6 can be present. Similarly, Documentation attributes 1-7 can be present.

5.8 Conclusions

This presents scenarios as an extremely useful tool that may support foresight in safety. The concept of scenario is understood here as general as possible.

Both prospective scenarios, mainly derived from risk analyses, and retrospective scenarios, mainly derived from undesirable event investigations, are usable for foresight.

There are no restrictions on how the scenarios are presented. All methods are available, from the simplest pairs of initiating event - consequence to relatively complex bow-tie diagrams.

The chapter introduces the concept of casual events, representing a 'skeleton' of a scenario, no matter the type and form of the scenario. Casual events enable visibility of early warning signs, which is a condition for foresight in safety. The path to the determination of EWSs leads through the determination of causal events.

The examples presented in the chapter show:

(i) Scenarios as an investigation component of lessons learning help the determination of sets of EWSs that should be searched and tracked for during the analyses, and

(ii) Scenarios as a documentation component of lessons learning help the determination, whether a specific failure/error represents an EWS.

5.9 Acknowledgements

To our reviewer, Ana Lisa Vetere Arellano.

5.10 References

Accou, B. and Reniers, G. (2018). Analysing the depth of railway accident investigation reports on overspeeding incidents, using an innovation method called "SAFRAN". In *55th ESReDA Seminar (Session 5),* Bucharest, Romania, October 2018.

Afonso, A., Garnett, K., Noteborn., H., and Maragkondakis, P. A. (2017). Emerging Risks in Food and Feed, the Importance of Foresight. In *53rd ESReDA Seminar*, Ispra, Italy, November 2017.

Aven, T. (2008). *Risk Analysis*. John Wiley & Sons, Chichester, England. ISBN: 978-0-470-51736-9, 194 pages.

Benner, L. (1975). Accident Investigations: Multilinear Events Sequencing Methods (modified by Epilogue added), accessible from ludwigBenner.org, accessed on March 27th, 2018, original article *Journal of Safety Research*, June 1975, Vol. 7, No. 2.

Benner, L. and Carey, W. D. (2009). Lessons Learning System Attributes: An Analysis. In *36th ESReDA Seminar*, Coimbra, Portugal, June 2009.

Blanco, R. F. (2014) Understanding Hazards, Consequences, LOPA, SILs, PFD, and RRFs as Related to Risk and Hazard Assessment. *Process Safety Progress* 33, 208-216.

CCPS (2000). *Guidelines for Chemical Process Quantitative Risk Analysis, 2nd edition.* American Institute of Chemical Engineers, New York, USA. ISBN: 0-8169-0720-X, 754 pages.

CCPS (2001). *Layer of Protection Analysis – Simplified Process Risk Assessment.* American Institute of Chemical Engineers, New York, USA. ISBN: 0-8169-0811-7, 270 pages.

CCPS (2003). *Guidelines for Investigating Chemical Process Incidents, Second Edition.* American Institute of Chemical Engineers, New York, USA. ISBN: 0-8169-0897-4, 452 pages.

CCPS (2007). *Guidelines for Risk Based Process Safety.* John Wiley & Sons, Hoboken, New Jersey, USA. ISBN: 978-0-470-16569-0, 698 pages.

CCPS (2008). AIChE Center for Chemical Process Safety. *Guidelines for Hazard Evaluation Procedures, Third Edition.* John Wiley & Sons, Hoboken, New Jersey, USA. ISBN: 978-0-471-97815-2, 542 pages.

CCPS (2012). AIChE Center for Chemical Process Safety. *Recognizing Catastrophic Incident Warning Signs in the Process Industries.* John Wiley & Sons, Hoboken, New Jersey, USA. ISBN: 978-0-470-76774-0, 227 pages.

Crowl, D.A. and Louvar, J.F. (2011). *Chemical Process Safety, Fundamentals with Applications, 3rd edition.* Pearson Education, Boston, MA, USA. ISBN: 978-0-13-278283-8, 705 pages.

Defence Science Board Task Force (2003), The Role and Status of DoD Red Teaming Activities, Defence Science Board Task Force, Washington, DC.

ESReDA (2009). Guidelines for safety investigation of accidents. Technical report, ESReDA. Available from http://www.esreda.org/Portals/31/ESReDA_GLSIA_Final_June_2009_For_Download.pdf

Ferjencik, M. and Dechy, N. (2016). Three accidents in European dynamite production plants: An attempt to improve the external lessons learning. *Journal of Loss Prevention in the Process Industries* 44, 12-23.

Ferjencik, M. (2014) IPICA_Lite—Improvements to root cause analysis. *Reliability Engineering and System Safety* 131, 1–13.

Ferjencik, M. (2017). Roles of Incident Scenarios in Foresight. In *53rd ESReDA Seminar*, Ispra, Italy, November 2017.

Hatch, D., McCulloch, P. and Travers, I. (2019) Enhancing PHAs: The Power of Bowties. *Chemical Engineering Progress*, February 2019, 20-26.

Hollnagel E. (2014). *Safety-I and Safety-II. The Past and future of Safety Management.* Ashgate Publishing Ltd., Surrey, England. ISBN: 978-1-4724-2305-4, 187 pages.

Johnson, C.W. (2003) *Failure in safety-critical systems: a handbook of incident and accident reporting.* Glasgow University Press, Glasgow, UK. ISBN: 0-85261-784-4.

Johnson, W.G. (1973) *The Management Oversight & Risk Tree – MORT*. SAN 821-2, U.S. Atomic Energy Commission, Division of Operational Safety. Available from www.nri.eu.com.

Kaplan, S. and Garrick, B.J. (1981). On the Quantitative Definition of Risk. *Risk Analysis* 1, 11-27.

Kaplan, S., Haimes, Y. Y. and Garrick, B. J. (2001) Fitting Hierarchical Holographic Modeling into the Theory of Scenario Structuring and a Resulting Refinement to the Quantitative Definition of Risk. *Risk Analysis* 21, 807-819.

Kaplan, S., Visnepolschi, S., Zlotin, B., Zusman, A. (1999). New Tools for Failure and Risk Analysis. Anticipatory Failure Determination (AFD) and the Theory of Scenario Structuring. Detroit: Ideation International Inc.

Leveson, N. (2004) A new accident model for engineering safer systems. *Safety Science* 42, 237–70.

Marshall, V. and Ruhemann, S. (2001) *Fundamentals of Process Safety*. Institution of Chemical Engineers, Rugby, UK. ISBN: 0-85295-431-X, 298 pages.

Masys, A. J. (2012). Black swans to grey swans: revealing the uncertainty. Disaster Prevention and Management: An International Journal, 21(3), 320–335. doi: 10.1108/09653561211234507

Nicolescu, M. (2018) A freight train derailment analyses using Accident Investigation Board Norway method and Safety Management wheel tool. In *55th ESReDA Seminar (Session 6)*, Bucharest, Romania, October 2018.

Stoop, J. and Benner, L. (2015). What do STAMP-based analysts expect from safety investigations? *Procedia Engineering* 128 (2015) 93-102.

Strucic, M. (2017). Use of Event and Causal Factor Short Cart Reports to Assess and Simplify Accident Reports. In *53rd ESReDA Seminar*, Ispra, Italy, November 2017.

Verschueren, F. (2018) Learning from organisational dysfunctionalities. In *55th ESReDA Seminar (Session 2)*, Bucharest, Romania, October 2018.

Vesely, W.E., Goldberg, F.F., Roberts, N.H., and Haasl, D.F. (1981) *Fault Tree Handbook* NUREG-0492. U. S. Nuclear Regulatory Commission, Washington DC, USA.

Wincek, J. C. (2011). Basis of Safety: A Concise Communication Method for Critical Process Safety Information. *Process Safety Progress* 30, 315-318.

Zio, E. (2007). *An Introduction to the Basics of Reliability and Risk Analysis.* World Scientific Publishing, Singapore. ISBN: 978-981-270-639-3, 222 pages.

This chapter is extracted from the final technical report of the ESReDA Project Group *Foresight in Safety*. The full report is freely downloadable from the ESReDA web site and from the EU Joint Research Centre publications repository.

Bibliographic identifiers for the full report are indicated below.

PDF	ISBN 978-92-76-25189-7	ISSN 1831-9424	doi: 10.2760/814452	KJ-NA-30441-EN-N
Print	ISBN 978-92-76-25188-0	ISSN 1018-5593	doi: 10.2760/382517	KJ-NA-30441-EN-C

"Enhancing Safety: The Challenge of Foresight"

Edited by the ESReDA Project Group *Foresight in Safety*.

How to **cite this report**: ESReDA Project Group Foresight in Safety, *Enhancing Safety: The Challenge of Foresight*, EUR 30441 EN, Publications Office of the European Union, Luxembourg, 2020. ISBN 978-92-76-25189-7, doi: 10.2760/814452, JRC122252.

ESReDA
European Safety, Reliability & Data Association