WHAT DO YOU DO WHEN YOU BUILD SAFETY?

Practitioners' guide to learning from successful operations

Authors:
Ragnar Rosness, SINTEF
Torgeir Haavik, NTNU Social Research
Ranveig Kviseth Tinmannsvik, SINTEF

The guide is based on research performed by SINTEF, NTNU Social Research and NTNU in the project *"Learning from successful operations"*. The project was sponsored by the Research Council of Norway through the research programme PETROMAKS2. The project comprised theoretical work, interview studies, observations of practices on a semisubmersible drilling rig, and observation from training session in a drilling simulator. The guide also draws on previous research performed by the project partners.

We want to thank our colleagues who have been so kind to comment and provide feedback on earlier drafts of the guide, in particular Lars Bodsberg and Geir-Ove Strand.

Trondheim, December 2016

ISBN: 978-82-14-06185-7

Graphic design: Britt-Inger Håpnes. Trykk: Trykkpartner AS.

SINTEF   NTNU Social Research

CONTENTS

PART I:
Introduction and scope of the guide

Organisations make great efforts to learn from their accidents, but they do not make a similar effort to learn from the operations that are performed without an accident, with adequate safety margins and with appropriate barriers in place. The objective of this guide is to help organisations learn from their successful operations. We discuss how practitioners can initiate reflection and discussion on the actions and practices that contribute to safe operations. We also present a catalogue of actions, interaction patterns and practices that contribute to safe operations. This catalogue provides topics and examples for reflection and discussion.

1 Learning from failure versus learning from success

1.1 We strive to learn from failure, but what about successful operations?

Major accidents, such as Deepwater Horizon, immediately grab our attention. We spontaneously start asking questions: What happened? How could it happen? Can it happen again? Can it happen at my workplace? What can we do to prevent it from happening again?

Not so if an operation runs safely. By 'safety' we refer to a situation where the hazards that could cause an accident are eliminated or kept under control, for instance by means of barriers and adequate safety margins. Have you ever heard anybody ask "why did we not have a blowout today?" We take safe operations for granted. Apparently, nothing happened, there is nothing to be concerned about, nothing to explain, no questions to ask, no actions to be taken. We could have asked: How did it happen? What can we do to make it happen again? But we hardly ever ask these questions when an operation runs safely.

Have you ever heard anybody ask "why did we not have a blowout today?"

We make great efforts to learn from failure. Each major accident in the petroleum industry leads to an investigation. This is followed by efforts to share and learn from the findings in order to prevent similar accidents in the future. Just think of all the reports that have been written about the Deepwater Horizon disaster, all the leaflets that have been distributed, all the presentations that have been given and all the discussions about how to avoid a repetition of the disaster. This is only appropriate. We owe it to the offshore workers and their families, to the natural environment and to the public to do what we can do to avoid serious disasters.

We do not make a similar effort to learn from our successes, from the operations that are performed without an accident, with adequate safety margins and with appropriate barriers in place. When nothing happens, there is no need for action, no sense of urgency. There is always some more pressing issue than finding out why nothing happened. There is also another problem with learning from success: It can be difficult to explain a success in such a way that we can learn from it. Saying that "we did the right things" or "we followed the procedures" may be correct, but it does not necessarily help us improve our practices.

Saying that "we did the right things" or "we followed the procedures" may be correct, but it does not necessarily help us improve our practices.

1.2 Why should organisations learn from successful operations?

There are several reasons why organisations should learn from operations that are successful with regard to safety:

- **If you were to teach a little girl good manners when dining in a restaurant, would you show her the people who are thrown out of the restaurant due to unacceptable behaviour, or would you show her people who enjoy a pleasant meal because they know how to behave?** This is a basic principle of learning: It is more effective to teach people what to do, than to teach them what they should not do. Knowing what not to do does not mean that you know what you should do. Moreover, most of us get uncomfortable and defensive when we receive negative feedback, even if we may try to hide our frustration. Focusing on practices that contribute to success creates a better learning climate.

Focusing on practices that contribute to success creates a better learning climate."

- **We do not have to wait for an accident or a near-accident before we can start improving.** This is particularly important when we face major hazards, such as the possibility of an uncontrolled blowout or a major explosion. We need to learn before an accident occurs, and one way to do this is to learn from successful operations.

- **People deserve attention and feedback when they do the right things.** People who are involved in accidents receive a lot of negative attention, and find their actions scrutinised in detail. Not so when people do the right things and avoid accidents. One gets, at best, a congratulation for a certain number of days without injuries, but it is very rare for anybody to investigate in detail what people did to deliver an excellent safety record.

- **The organisation needs to know what it takes to deliver accident-free performance.** All business organisations and most non-profit organisations are under pressure to deliver "faster, better and cheaper" in order to survive in the market or to ensure political support. The actions they take to do this may or may not compromise safety. By scrutinising successful operations, organisations learn what it takes to deliver accident-free performance. They get in a better position to develop their activities in ways that promote safety, and to avoid removing resources that are essential to safe operations.

- **People and organisations will always learn from the operations that they perceive as successful.** Practices that seem to work tend to be strengthened or maintained without any intervention from management. This is a kind of spontaneous learning that takes place every day in every organisation. Unfortunately, this also applies to practices that happened to be successful due to pure luck, in spite of inadequate safety margins or inadequate barriers. Even an unsafe practice may lead to no harm in 9 out of 10 or even 99 out of 100 cases. This means that organisations may learn to be unsafe from operations they perceive as successful because no harm occurred. Learning from successful operations is not only about identifying and promoting good practice. It is also about detecting the instances where no accident occurred in spite of unsafe practices or unsafe systems.

Learning from successful operations is not only about identifying and promoting good practice. It is also about detecting the instances where no accident occurred in spite of unsafe practices or unsafe systems.

2 Scope and Organisation of the Guide

2.1 Purpose and approach of the learning guide

Many of the actions that contribute to successful operations tend to be invisible for us, even if they take place right in front of us. Either we take them for granted, or we do not intuitively realise how they contribute to safety.

Our objective is to help people "see more", i.e. notice and interpret episodes that might have gone unnoticed without this guide.

The approach of the guide is to help sensitise the user to actions, practices and patterns of interaction that contribute to successful operations. Our objective is to help people "see more", i.e. notice and interpret episodes that might have gone unnoticed without this guide. We focus on how actions or interaction patterns may contribute to successful operations.

The guide is not intended to be used in a "tick off mode" or for quantification purposes. The guide is not exhaustive; i.e. it does not cover every way in which an action or a practice can contribute to safety. The user should therefore be prepared to notice things that are not mentioned in the guide.

2.2 Who is this learning guide for?

The purpose of the guide is to help practitioners and researchers identify actions, collaboration patterns and practices that contribute to successful operations with regard to safety. The term 'practitioner' includes both safety specialists (e.g. HSE personnel), line managers and personnel safety representatives.

Accident investigators may use the guide as a support for identifying positive lessons to be learnt from accidents and near misses. Remember that unwanted events may include exemplary safety efforts such as recovery actions or excellent rescue efforts.

Practitioners may use the guide as a help in arranging discussions and workshops focusing on a specific successful operation, ranging from short debriefs to a one day workshop.

Instructors may use the guide to support observations and debriefing in conjunction with training sessions in real work environments, simulators and tabletop settings.

Researchers may use the guide to support observations in real work environments, as well as simulator environments that allow for observation of patterns of collaboration. Hopefully, such efforts may lead to improvements of the guide.

2.3 The contents and structure of the guide

It is not always obvious whether an operation was successful with regard to safety, because the absence of accident may be due to "pure luck". Therefore, the first chapter in Part II provides guidance on how to scrutinise an operation to sort out in what respects it was successful with regard to safety.

The rest of Part II provides suggestions on how to use the guide for specific purposes, for instance investigating an accident, observation and debrief in conjunction with simulator training, or arranging a workshop in order to extract lessons from a specific incident or successful operation.

Part III can be read as a catalogue of actions, interaction patterns and practices that contribute to successful operations. Each chapter represents a specific perspective on successful operations. For instance, Chapter 10 deals with sharing and interpreting information about conditions that may lead to an accident, whereas Chapter 13 is concerned with how to ensure safety in the face of conflicting objectives. We have included many examples of actions or practices that illustrate the different ways people contribute to safety. We have also included topics for discussion at the end of each chapter.

Part IV addresses questions that researchers may want to raise with regard to the learning guide. You will also find explanations of technical terms such as 'barriers' or 'tight coupling'. In the last chapter, we propose a few selected books, reports and articles for further reading.

2.4 How to use the guide

First of all, you may read this guide out of sheer curiosity. Some people like to read things straight through from cover to cover; others like to pick and choose from the table of contents. The choice is yours! By reading Chapter 3, you may be better prepared to discuss in what respects the performance of a given task was successful with regard to ensuring safety. Having read some of the chapters in Part III may help you to see more clearly the things people do to prevent accidents.

We discuss the practical applications of the guide in Part II. You may, for instance, use the guide to **prepare a short discussion** on a safety meeting. You will find some suggestions about how to do this in Chapter 4.

Alternatively, you may want to go beyond a short discussion and **arrange a workshop** where you can spend a few hours to discuss one successful or partly successful event. This can lead to extensive learning, in particular if you bring together participants with complementary knowledge and experience. You will find more about this in Chapter 5.

You may also use the guide to **support debriefing** in a situation where a team has performed successfully and wants to reflect on why things went well. This is discussed in Chapter 6.

The guide can also be used **to support observations of task performance, either on an ordinary work place or in a training environment such as a simulator.** It can be quite challenging for an observer to pinpoint the actions and practices that contribute to safety from a smooth flow of work. It is often more easy to tell people what they did wrong than to give them precise and informative feedback on what they did right. In Chapter 7 we give you some suggestions on how to do this.

> You should never try to force all the knowledge of the organisation into procedures.

Finally, you may use the guide to **support the investigation of an incident or accident, in order to highlight and learn from things that went well**. See Chapter 8, where we discuss how this can be done.

What you should not do is to turn this guide into a procedure. If you work in the petroleum industry, you probably have a huge amount of procedures to keep track of already. The skills and practices we have described here need to be highly flexible, and people have to see by themselves when and how they need to be applied. They will just not fit into a procedure.

DISCUSSION TOPICS

1. Can you remember an instance when you and your colleagues discussed why you succeeded in completing a demanding task without having any unwanted events? Did you find a way to share your positive experience with people outside the work group?
2. Do you agree with the warning on the next page? Why/why not? How can people in your organisation share knowledge without putting lessons learned into procedures?

Procedures can be helpful in many ways. They can inform people about the safest way to perform the job and about what safety precautions are necessary. Procedures can also help people identify the safe envelope of the job they are going to do, i.e. the limits an operation has to stay within in order to keep the hazards under control. Procedures can also help people remember all steps in a complex task. But you should never try to force all the knowledge of the organisation into procedures. That will leave you with far too many rules and procedures.

PART II:

How to learn from successful operations

In this part, we will give some advice regarding how organisations can learn from their successful operations. The first chapter in this section discusses how to distinguish between safe and unsafe operations.

The guide can be used as a support in these contexts:

- Short discussions
- Workshops
- Debriefings
- Observations
- Incident investigations

3 How do we know a successful operation when we see it?

The absence of an accident is not enough to prove that an operation was safe. OK, we did not have an accident, but was that because we did the right things, or was it due to pure luck? Even an unsafe practice may lead to no harm in 9 out of 10 or even 99 out of 100 cases.

Operations that have proved safe with regard to personal injuries (ordinary workplace accidents) are not necessarily safe with regard to major accidents. The problems that lead to major accidents can be different from the ones that lead to personal injuries. On the day when the Deepwater Horizon disaster happened, managers were visiting the rig to celebrate its excellent record of lost time injuries. The injury record apparently indicated that the rig operations were successful with regard to safety. The explosions and the blowout revealed a different story.

Even a disaster may include aspects of success – for instance an outstanding rescue effort.

Once you have identified an operation that you want to learn from, you need to sort out in what respects the operation was successful. You should be prepared to meet some ambiguities when doing this. Many operations are successful in one respect and less successful in other respects. Even a disaster may include aspects of success – for instance an outstanding rescue effort.

The following criteria may help you sort out in what respects an operation was successful:

1. **Were the safety margins adequate? Was the operation within the safe envelope? Were the boundaries of the safe envelope sufficiently known to everybody involved in the operation?** The 'safe envelope' refers to the limits an operation has to stay within in order to keep the hazards under control. For instance, during drilling operations, the mud weight needs to be kept within certain boundaries (1) to keep formation fluid from entering the well and (2) to avoid fracturing the formation. In process control, pressures and temperatures need to be kept within boundaries. This criterion applies to all operations were it is possible to define one or more boundaries for safe operations.

2. **Were adequate barriers in place throughout the operation? If ordinary barriers had to be made ineffective, were adequate compensating measures taken? Were the involved personnel aware of the barriers and what it takes to ensure that they are effective?** Barriers are means to avoid or halt unwanted event sequences, so that harm is prevented or reduced. Important barriers in drilling operations can be well fluid (mud or brine) with the right properties (weight, viscosity), the casing and the blowout preventer. An important barrier in a process plant is isolation of ignition sources in order to prevent fire or explosion in case of a major hydrocarbon leak. We shall have more to say about barriers in the Chapter 9.

3. **Was the operation carried out in accordance with the applicable rules and procedures?** This issue is more complex than it may appear, because situations may occur when it is safer to divert from the standard procedure. The ideal is not blind compliance, but rather respect for rules combined with sensitivity to situations where the rules do not fit. If the rules do not fit, either for safety reasons or because compliance is physically impossible or impractical, we also need to examine **whether the decision to depart from the rules was taken in an appropriate way.**

The ideal is not blind compliance, but rather respect for rules combined with sensitivity to situations where the rules do not fit.

There are some special situations where other criteria of success are relevant. In some operations, such as drilling a high pressure/high temperature well or performing brain surgery, you just have to operate with close margins. In these situations, a criterion of success could be your capacity to **cope successfully close to the boundaries of harm or system breakdown. Successful recovery from an imminent danger** is also a relevant aspect of success if you have experienced a close call or an accident where actions effectively limited the unwanted consequences.

These criteria may get you started scrutinising how well safety was taken care of during an operation. You should not be surprised or disappointed if it proves difficult to agree on whether an operation was successful or not with regard to safety. A disagreement can be an excellent opportunity to learn from each other – provided that you spend your efforts on listening and scrutinising the arguments of others, rather than striving for a consensus at any price. Summarising the pros and cons on a screen or a flipover could be a good start in the process of learning from (more or less) successful operations.

EXAMPLE:

- A semisubmersible rig on the Norwegian continental shelf was in the early phase of drilling a deepwater well, and was still far from reaching the reservoir. The weather forecast for the day of the incident announced a peak storm, i.e. a storm characterised by a rapid increase and decrease. The rig crew planned and prepared for disconnecting the riser. As the storm developed, the rig crew monitored the heaves of the rig closely. They registered two heaves that exceeded the six meters disconnection criterion before the waves subsided. Due to the expectation that the strong part of the storm would last for a very short time, the rig manager concluded that the equipment would be strong enough to handle the situation, and he decided not to disconnect. No harm occurred. The rig would have lost several days production time if it had disconnected. On the other hand, the disconnection criterion, which had been determined by a careful analysis of the mooring arrangement, had been violated twice.

The operating company discussed this event during a workshop with both operating personnel and HSE staff present. They agreed that the preparations were a success; the rig crew had done all the right things to be ready to disconnect. They did not agree on whether the decision not to disconnect should be counted as a success or not. Some suggested that it was a success, based on the consequences. Others maintained that the operation went outside the safe envelope defined by the disconnection criterion. During the discussion, the participants shared knowledge about the reasons for the disconnection criterion and about how these situations are actually handled by the rig crew. They found that the disconnection criterion was included in a guideline document and not a formal procedure. The decision not to disconnect was therefore not a non-conformity. After the workshop, this document was converted into a formal procedure.

DISCUSSION TOPIC

1. Have you ever discussed with your colleagues how well safety was taken care of during an operation? Did you have disagreements? Can you still remember some of the pros and cons?

4 Using the guide to prepare a short discussion

You do not need to use a half a day or more on a workshop in order to use the guide for discussions. You may pick just one section in Part III as a starting point for half an hour discussion on, e.g., a safety meeting. It is a good idea to find a topic that can be linked to either a recent job that has been successfully performed, or a job that the participants are going to do in the near future. You may, for instance, decide to discuss "Take a timeout" (Section 13.2), after an episode where a work team did take a timeout to discuss safety aspects of their work. This is a good occasion to remind people of the need to take a timeout, and to confirm that the organisation supports taking a timeout, even if it means that the job will take a few minutes more to complete. It is also an opportunity to discuss how you get the most out of the time you spend taking a timeout.

It is a good idea to find a topic that can be linked to either a recent job that has been successfully performed, or a job that the participants are going to do in the near future.

Here is a possible outline for a 30 or 60 minutes discussion on one section from the guide:

1. **Explain what the practice you want to discuss is about.** You may want to link the practice to the topic of the relevant chapter in the guide to put it into context. For instance, if you want to discuss "take a timeout", you may mention that it is one of the things we do to keep safe, even in case of conflicting objectives, such as time pressure versus safety.

2. **Present an example.** You may, for instance, present an occasion from your own workplace when people did take a timeout. It is usually a good idea to explain carefully **why** they chose to take a timeout. It is also often a good idea to invite somebody who was involved to explain the background.

3. **Invite a discussion.** Some examples of discussion topics are given at the end of each chapter in Part III. You may, for instance, start by inviting the participants to **provide additional examples**. You may ask people to spell out in more detail what they do when they build safety, for instance what they will do during a timeout. You could also ask **if there are occasions where people find it difficult** to ask for a timeout. The natural next step is then to ask what can be done to make it easier to ask for a timeout.

4. **Round off the discussion.** You may want to recapture the starting point if the discussion has gone a long way. Then you may want to conclude by looking forward, repeating good ideas for how to support, maintain and strengthen a good practice.

You may also want to discuss one specific practice (corresponding to one section in the guide) in a Safe Job Analysis meeting or a toolbox meeting. You may, for instance, bring in the topic "surprise handling" (Section 14.3) towards the end of a Safe Job Analysis and challenge the participants to think of possible surprises that may occur during the job they are planning.

5 Using the guide to support a workshop

It is also possible to arrange a workshop with duration between a half and a whole day, focusing on one successful or partly successful operation or event. Such a workshop could focus on one chapter in Part III of this guide.

A key to the success of such a workshop is the selection of a suitable event. It is a good idea to avoid events with significant actual injuries, damage or loss, since such events can often lead to defensive reactions and a reluctance of workshop participants to discuss difficult or threatening issues. On the other hand, events with a significant **potential** for unwanted consequences may work well; the opportunity to prevent similar events with adverse consequences in the future can be a strong motivation for the participants.

It is a good idea to select participants with complementary knowledge and experience with regard to the event. You probably need to include people who are closely familiar with the operations, people who know the technology, people who are familiar with HSE systems and regulations, and at least one higher-level manager who can express company policy and commit the company to follow-up actions. It is also a good idea to have two facilitators rather than one. This allows one facilitator to listen and monitor the process, while the other facilitator directs the discussions. (This is actually a way to create organisational redundancy, see Chapter 12.)

It is also a good idea to emphasise the value of disagreement at the outset of the workshop. It is nice to reach consensus on follow-up actions at the end of the workshop, but this does not mean that people have to agree on everything all the way through the workshop. Participants can learn more from each other if they express divergent judgements and opinions, and if they meet disagreement with curiosity. It may be helpful to ask groups to record divergent opinions and present them in plenary sessions.

The opportunity to prevent similar events with adverse consequences in the future can be a strong motivation for the participants.

The first part of the workshop should be devoted to familiarising all participants with the event and the setting where it took place. An effective way to do this, is to let groups of 3-5 participants construct graphical representations of the event sequence, for instance a STEP diagram, see Chapter 8.

The agenda for a lunch-to-lunch workshop on ensuring safety in the face of conflicting objectives is shown below as an example.

Day 1 13:00 – 18:00 + dinner
Introduction to the Workshop
Introduction to case
Introduction to the STEP analysis method
STEP analysis (group work)
Plenary discussion of case, based on STEP analyses

Day 2 09:00 – 12:00 + lunch
Discussion of possible outcomes and consequences
Decision dilemmas – theory & discussion
Looking ahead: Future handling of decision dilemmas
Conclusion

6 Using the guide to support debriefing

"Debriefing" here refers to situations where a team has just performed a job successfully in the real world or in a simulator, and wants to reflect on why things went well. The purpose can be to enhance awareness within the work group about the things people do to ensure successful performance, and/or to promote good practices in other parts of the organisation. In both cases, a good debrief may involve putting into words knowledge and good practices that are usually silent and taken for granted.

A debrief should start with a self-critical discussion: **In what respects was the operation successful?** (See Chapter 3). This discussion leads you to think carefully about the safety margins during each step of the operation, about the safety barriers, and about the use of procedures. This discussion may reveal that safety margins may have been smaller than you thought, that some safety barriers were weakened during a certain stage of the operation, that the procedures were not followed in every detail, or that the procedure did not fit very well to the circumstances when the job was performed. But this discussion may also reveal good practices which maintain adequate safety margins and safety barriers, and perhaps good ways to adapt procedures in a safe manner when they do not fit with the circumstances.

After discussing the success of the operations, you may start asking: **What did we do to make it a success?** It is a good idea to ask in such an open-ended manner initially. You may need to remind yourselves that the things you did to make it a success may seem so obvious that they are easy to overlook.

A common answer to this question is: "We followed the procedures". This may be perfectly true, but you should try to elaborate a little. What parts of the procedures were important to follow, what parts are not always followed? Did you interpret the procedures in a specific way or did you find a specific way to execute the procedures that contributed to the success? Were there different procedures that you had to choose between, and were there trade-offs you had to make in that connection?

Depending on the available time, you may stop at this point, or you may ask more specific questions, based on one or more of the chapters in this guide, for instance "What did we do to ensure adequate sharing and interpretation of information?" (Chapter 10) or "How did we use organisational redundancy to ensure safe operations?" (Chapter 12) or "How did we ensure safety in the face of conflicting objectives (e.g. time pressure)?" (Chapter 13). Perhaps you used one of the specific practices mentioned in the relevant chapter? Perhaps you found a good practice that is not mentioned in the guide?

A good debrief may involve putting into words knowledge and good practices that are usually silent and taken for granted.

You may want to consider carefully who should attend the debriefing. Perhaps there is learning potential for others than those involved in the actual situation. Also, if the learnings from debriefings are considered valuable to others and applicable to future operations, you might want to produce some material (written/video etc.) that might be used to materialise the experiences and make them available for later use.

7 Using the guide for observations

Observations can take place on ordinary work places or in training environments, such as a simulator. The purpose is usually to give people feedback on the way they do their work in order to promote learning. It can also be used to give people recognition for practices that contribute to safe operations, and to identify good practices that can be communicated to other workers or managers.

Giving people feedback on the things they already do to build safety may seem superfluous, since there is no need for them to change their practice. However, the good practices that we take for granted today may disappear tomorrow if the circumstances change. This is a good reason for maintaining consciousness about what people do when they build safety.

It can be quite challenging for an observer to extract the actions and practices that contribute to safety from a smooth flow of work. It helps to have thorough knowledge about the task, the technology and equipment and the relevant administrative systems (e.g. procedures and safety rules). On the other hand, being an outsider to this particular workplace or crew can help the observer "see" actions that are invisible to insiders because they are taken for granted ("factory blindness").

It may also be helpful to have one or two of the perspectives from this guide in mind during the observation. Can you identify actions or collaboration patterns that ensure adequate sharing and interpretation of information (Chapter 10)? What does the crew or work group do to ensure safety in the face of conflicting objectives (Chapter 13)? **However, do not let the chosen perspective keep you from noting other actions and practices that can help you to build safety.**

Another advice is to look for not only isolated individual actions, but also exchanges and patterns of collaboration. Group performance is not just the sum of individual contributions; it is also a result of collaboration patterns and communication styles.

Giving feedback can also be a challenging aspect of observations. In particular, criticisms or negative feedback can be unpleasant and difficult to receive and often leads to defensive reactions. Fortunately, giving feedback about actions and practices that contribute to safety is not likely to trigger such defensive reactions. Another challenge is to be sufficiently specific, but at the same time sufficiently open-ended to encourage the group to reflect on the feedback and possibly challenge the interpretations of the observers. A common way to conclude a feedback session is to identify three positive findings, three improvement points and three "takeaways". "Takeaways" are the learning points you want to profit from in the future. It is a good idea to dig a little into the positive findings. Why did people do the right things? What does it take to ensure that they do the right thing next time, or that other crews do the right thing? "Takeaways" can be derived from positive as well as negative findings.

The good practices that we take for granted today may disappear tomorrow if the circumstances change. This is a good reason for maintaining consciousness about what people do when they build safety.

To ensure that learning is not restricted to those involved in observation sessions, others may be invited into the feedback sessions. Alternatively, one may arrange feedback sessions only for those involved in the observation sessions first, followed up by a more generalised feedback session where others are involved.

8 Using the guide for incident investigations

By 'incident investigations', we mean investigation of accidents, as well as near misses and successful recoveries. By 'successful recoveries' we refer to event sequences where an accident was about to happen, but where humans intervened and managed to prevent or reduce the unwanted consequences (fatalities, injuries, damage, loss). It may seem contradictory to highlight investigation of accidents in a guide to learning from successful operation, but in most accidents and near misses there are something that has gone well, and/or someone has done something that helped or could have helped to reduce the consequences of the accident.

In recent years, it has become more common to highlight safety barriers that have worked as intended in the investigation of accidents in the Norwegian petroleum industry. In the guideline to the Management regulations, section 20[1]: Registration, review and investigation of hazard and accident situations, it is stated that the investigation should clarify:

"... f) which barriers functioned, i.e. which barriers contributed to prevent a hazard situation from developing into an accident, or which barriers reduced the consequences of an accident."

Examples of barriers in this respect are safety systems like emergency shutdown, firewater etc. that have prevented a hydrocarbon leakage or fire to develop into a serious accident, or human interventions that contributed to minimizing the consequences of the event.

Incidents with successful recovery provide a golden opportunity for learning. Accidents can turn an organisation into a defensive mode where people are concerned about avoiding blame and avoiding anything that can subject their colleagues to blame. This can make it difficult to get complete and precise information about what happened. A successful recovery, in contrast, provides an opportunity to celebrate people who did the right things. There is no occasion for blaming people and therefore no incentive for covering up anything.

It is, however, difficult to find accident or incident reports that provide a thorough analysis of successful recovery. The reason for this is probably that there exists no systematic method for doing such an analysis – until now. In this chapter, we will describe how you can use a STEP diagram to **map the event sequence** that led to successful recovery, to identify **preconditions for successful recovery**, and to **identify measures that increase the likelihood of successful recovery** if a similar event should occur in the future. We will also describe a simple method to prioritise among the measures that may result from such an analysis.

A successful recovery, in contrast, provides an opportunity to celebrate people who did the right things. There is no occasion for blaming people and therefore no incentive for covering up anything.

8.1 Constructing a traditional STEP diagram

The STEP analysis (STEP – Sequentially Timed Events Plotting)[2] is a systematic process for accident investigation based on multi-linear events sequences and a process view of accidents/incidents. 'Multi-linear' means that we can identify and display two or more parallel chains of events. This makes the STEP method very effective for analysing and communicating about complex events. The STEP-worksheet provides a systematic way to organise the building blocks into a comprehensive, multi-linear description of the incident process.

[1] Petroleum Safety Authority Norway, Norwegian Environment Agency, Norwegian Directorate of Health (2010).
[2] Hendrick, K. and Benner, L. (1987). Investigating Accidents with STEP. Marcel Dekker Inc.

A simple example of a STEP diagram is shown in Figure 1. The diagram represents an accident where a stone block falls off a truck and ends up in the lane with traffic in the opposite direction. A car driver going in the opposite direction observes the stone block too late to stop the car, collides with the block, and dies. The STEP-worksheet is simply a matrix with a timeline. Each row in the worksheet corresponds to one actor. An actor is a person or an item that directly influences the flow or events constituting the incident process, for instance the truck driver, the truck and the stone block. An event in the STEP diagram is one actor performing one action, for instance "Stone (actor) falls off the truck (action)".

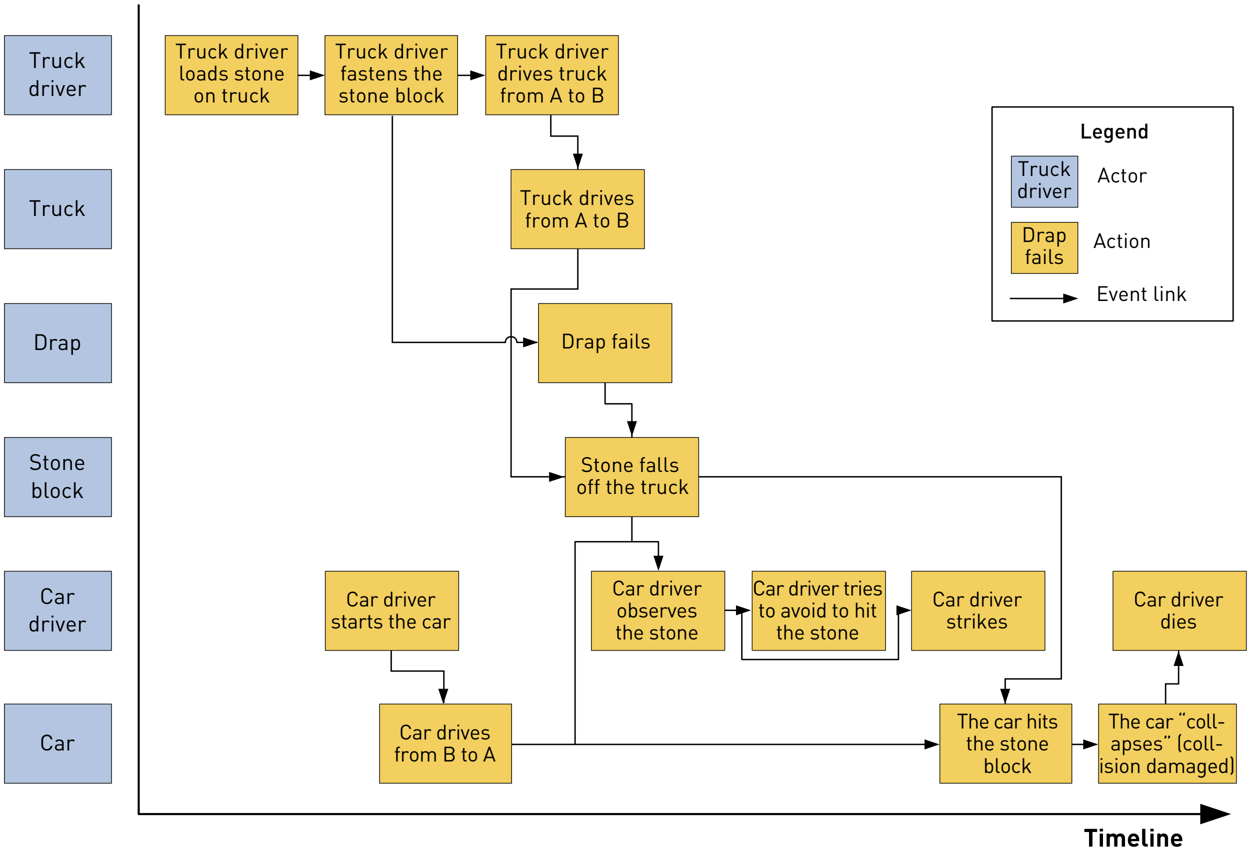


Figure 1. An example of a simple STEP diagram (Sklet, S., 2002. Methods for accident investigation, NTNU report).

Two simple rules can help you create a clear and informative diagram:

1. **Always use the active form** when you label the events in the diagram. For instance, in place of "the stone block is hit by the car", you should write, "the car hits the stone block". The active sentence is shorter and simpler. It identifies the real actor, i.e. the car, and ensures that the car gets a row of its own in the diagram. This rule also prevents you from omitting the actor altogether, for instance by writing, "The stone block was hit".

2. **Things that did not happen should not be included as events** in the worksheet. We have, for instance, not included "the car does not stop before it hits the stone block". This would have been superfluous, since the next event is "the car hits the stone block". The worksheet gets clearer and more concise if you restrict it to the events that actually happened. Some of the things that did not happen may come up as safety problems at a later stage in the analysis.

When creating the diagram, you should repeatedly perform row tests and column tests. A **row test** means that you look at all the actions of one actor, that is one row in the diagram, and see if it is possible to make a "mental movie" of the actions of that actor. If you can, then you probably have the building blocks for that row in place. If you cannot visualise the actions of that actor without gaps, then you probably need to collect and enter some new information. For instance, you may find that one actor suddenly appears in a new location without any event showing how the actor got there.

The **column test** is used to check that the events in each actor's row is correctly placed in relation to the other actors' actions. You should do this check each time you place a new event in the diagram. First, place the event tentatively where you believe it fits in. Then imagine a vertical line through the new event. If the new event is correctly placed, then it should make sense that all events to the left of the vertical line happened **before** the new event. Similarly, it should make sense that all events in all rows that appear on the right side of the line happened **after** the new event. If you find that one of the events on the right side of the vertical line must already have happened for the new event to occur, then you move the new event to the right in the diagram and repeat the column test.

At this point, you have a diagram with actors and events. The sequence of the events, that is their order from the left to the right, has been checked by row tests and column tests. It is now time to apply the **necessary-and-sufficient test**. This test helps you identify possible gaps in the description of the event sequence. It also helps you identify and show the causal links between the events. Identify pairs of events that you think are causally related, so that Event A led to Event B. Ask yourself, "was Event A necessary for Event B to occur?" If the answer is yes, show this by drawing an arrow from Event A to Event B. Ask yourself, "was Event A a **sufficient** condition for Event B to occur"? If the answer is "no", then you should look for additional events that are necessary to explain why Event B occurred. They may be in your diagram already, or you may have to gather more information. It is a good idea to put some effort into this part of the analysis, since it is easy to miss one or more necessary conditions.

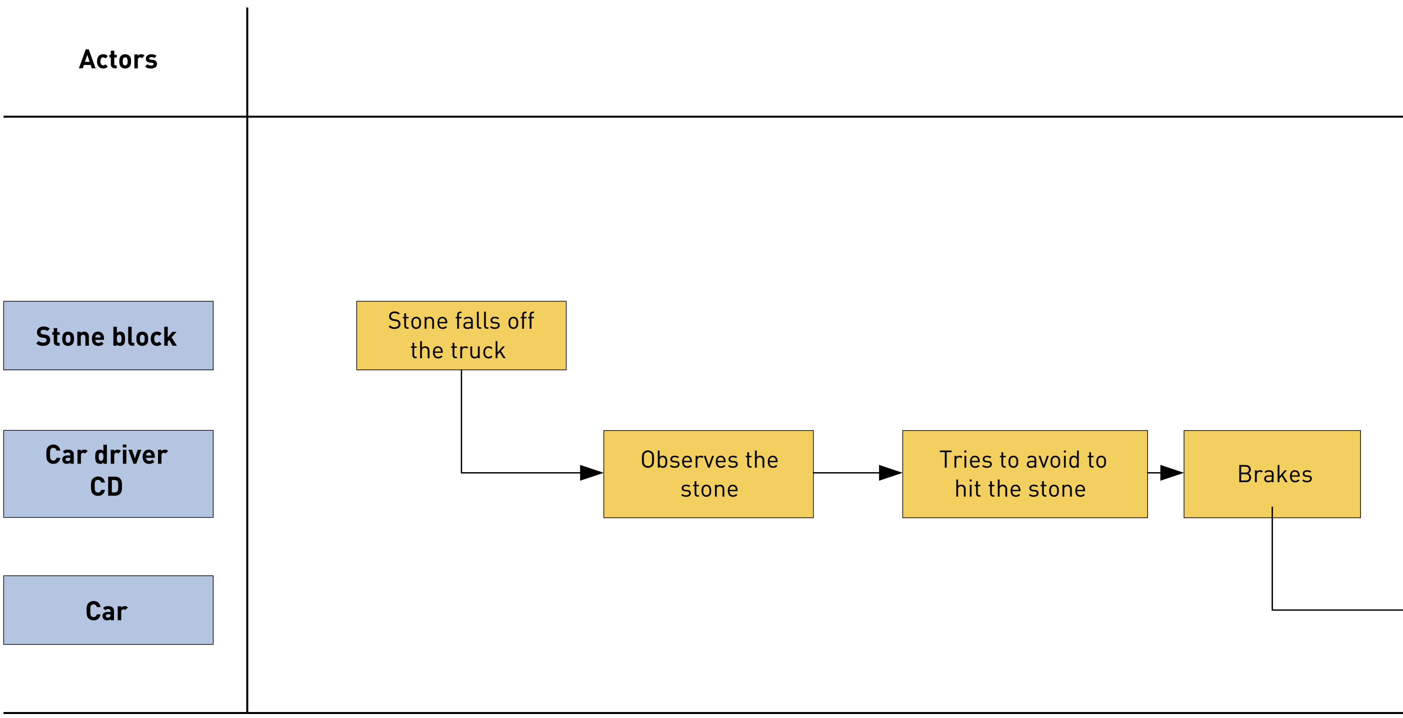


Figure 2. Event sequence for the successful recovery from the truck incident.

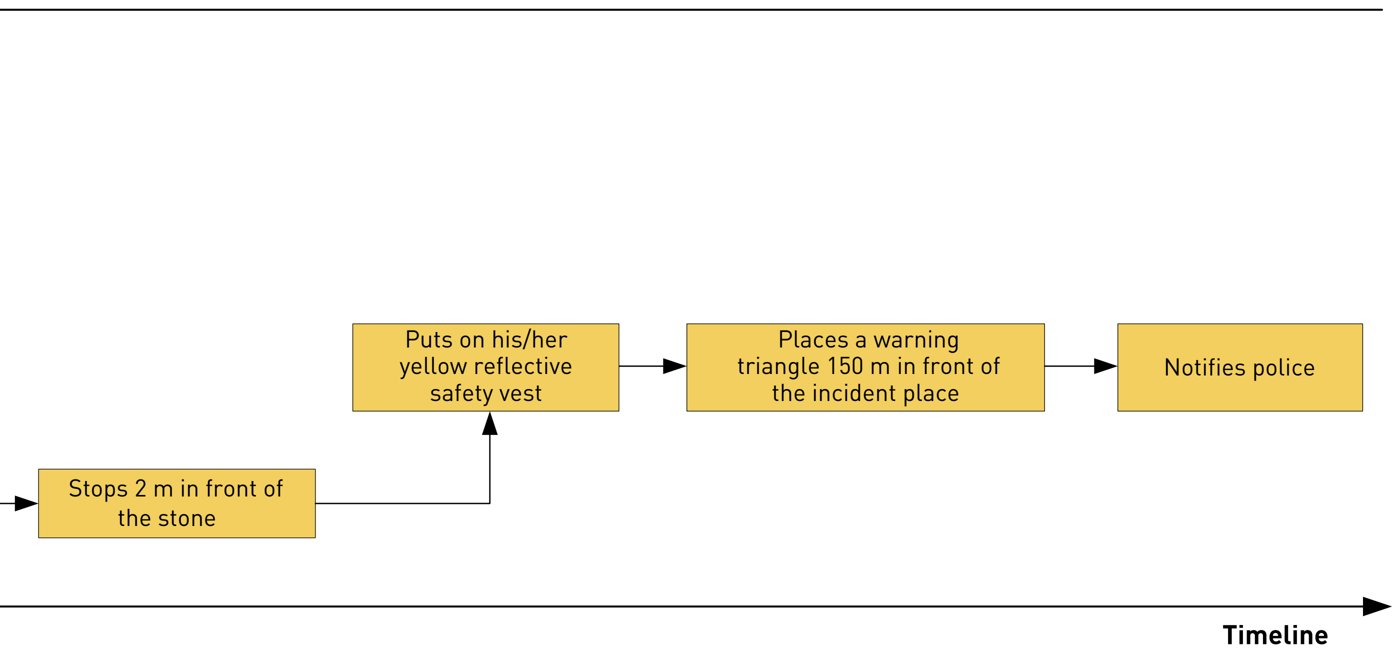
When you have completed a necessary-and-sufficient test, your diagram will look similar to Figure 1. Up to this point, the procedure for constructing a traditional STEP diagram is identical to the procedure for using STEP to identify preconditions for success. The next phase in a traditional STEP analysis is to **look for safety problems in the flow of events**. This is done by considering each of the arrows connecting one event with another event, and asking, "could the unwanted event sequence have been broken at this point?" There is, for instance, an arrow between "Truck driver fastens stone block" and "Truck driver drives from A to B". We might ask whether the event sequence could have been broken at this point, for instance if the driver or somebody else had performed an extra check to make sure that the stone was properly fastened. Finally, the investigators may recommend safety actions based on the safety problems they identified.

8.2 Using the STEP diagram to analyse a successful recovery

The ordinary STEP diagram is an effective way to analyse and communicate what went wrong (events), how (the total pattern of events and links) and why (safety problems). Can we use a similar approach to analyse a success, for instance a successful recovery?

Let us rewrite the story about the truck and the stone block from the point where the stones fall off the truck and turn it into a story about successful recovery: The stone falls off the truck. The car driver observes the stone, she brakes hard, and her car stops two meters from the stone block. The car driver puts on her yellow reflective vest, places a warning triangle 150 meters in front of the incident location, and notifies the police.

The event sequence for the successful recovery can be analysed and represented in the same manner as the event sequence for an accident. This is shown in Figure 2. We have left out the first (left) part of the STEP diagram to save space. You can use the row test, the column test, and the necessary-and-sufficient test in the same way as you do with in ordinary STEP diagram.



In the next part of the analysis, we want to **explain the successful recovery in a way that allows us to learn from the event**. The difficult step is to construct an explanation that is sufficiently specific to support learning. It is not specific enough to say, "we succeeded because everybody followed the procedures" or "we succeeded because the persons involved were the right stuff". The STEP diagram

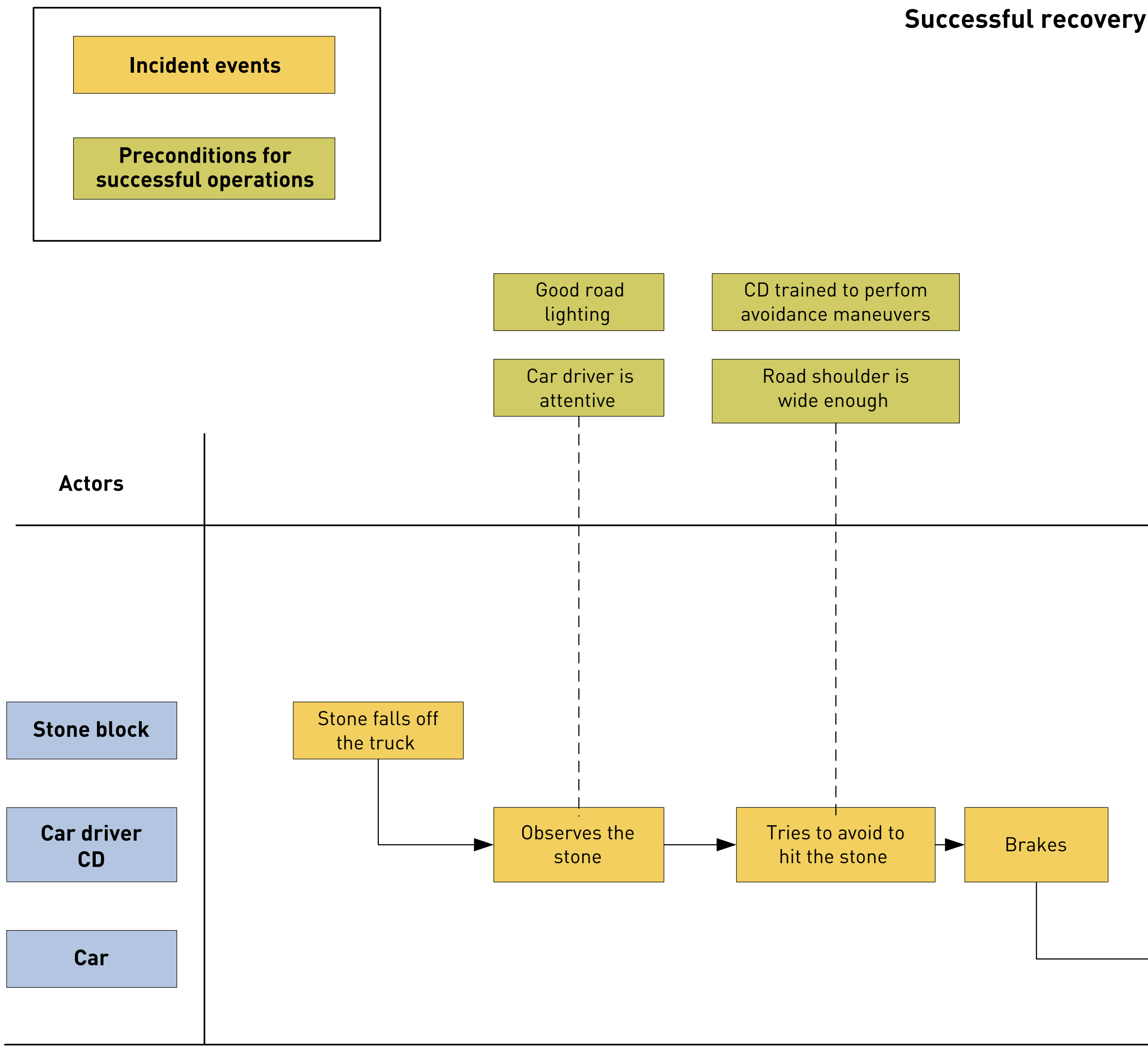
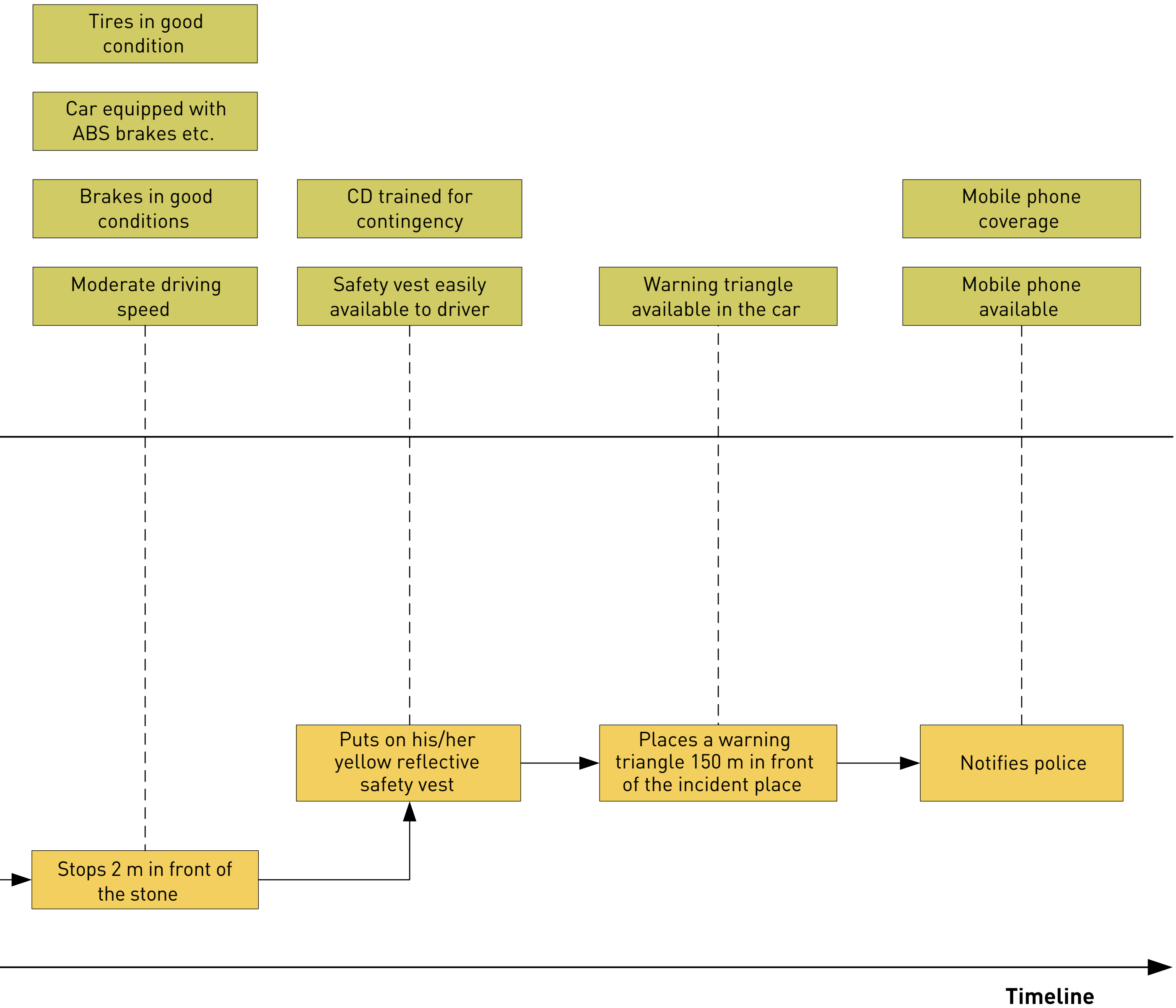


Figure 3. Preconditions for successful recovery from the truck incident.

can help us in being more specific, and in linking our explanation of success explicitly to the event sequence. We can construct a more specific explanation by looking at each event in the diagram that contributed to the success, and ask "what preconditions were necessary for this event to occur?"

from the Truck Incident



In Figure 3, the preconditions for success are shown as green rectangles at the top of the diagram. For instance, the car driver needed to observe the stone sufficiently early in order to stop the car in front of it. Two preconditions have been identified for the driver observing the stone in time to stop; (1) adequate lighting of the road (assuming that it was dark), and (2) the car driver was attentive. When it comes to the event "car stops two meters in front of the stone", relevant preconditions may be that the tyres were in good condition, that the brakes were in good condition, that the friction on the road was sufficient (e.g. that it had been sanded if it was icy) and that the car driver kept a moderate speed.

More generally, preconditions can include, for instance:

- Physical conditions, such as light conditions
- Competence and capacities of the individuals or groups involved
- Availability, quality, reliability and robustness of equipment
- Practices that support successful recovery, e.g. keeping a moderate speed when you drive.

In order to support successful recovery in the future, we want to make sure that these preconditions are present next time a similar incident occurs. Therefore, **each precondition for success may point to a condition that we want to strengthen, maintain or monitor**. For instance, we want to ensure that road lighting is adequate next time an obstacle suddenly occurs in front of a car; we want to ensure that the driver is attentive and that he or she has adequate vision. This is the logic we can use for deriving learning point (actions) from the analysis. **What do we need to do to ensure that the preconditions that enabled success are present next time a similar event occurs?** In this case, the car driver may decide to go on keeping a moderate speed and check her vision regularly. The authorities that are responsible for the road may want consider if there are other places where the lighting needs to be improved.

8.3 What about good luck?

Sometimes good luck plays a critical role in successful recovery. You may come across instances of good luck when you identify the preconditions for successful recovery. For instance, in a man-over-board incident, a second person happened to be present at the right place at the right time to assist a victim and call for help. Without the second person present, the victim would probably have lost consciousness due to low water temperature before anybody detected him.

You do not want safety to depend on good luck. Rather, you want to "ensure good luck" next time a similar incident occurs. You may therefore mark instances of good luck with a warning sign. This indicates a point where things may take an unhappy turn next time something similar happens. You may then identify learning points (actions) as described in the previous section. In the man-over-board case, you may consider if there should be restrictions on working alone in certain areas of the installation.

> You do not want safety to depend on good luck.

8.4 Prioritising preventive actions

As shown in Figure 3, the analysis can produce a long list of preconditions for success. Experience has shown that very long action lists can be counterproductive. They are prone to "overload" the managers and the people that are responsible for implementing the actions. The following criteria can help us narrow down the list of actions:

1. **How likely is it that this precondition will make a difference in the future?** This criterion is related to the likelihood that this precondition will be relevant in future events. It is also related to the severity of the events that can be prevented by improving this precondition. It is more valuable to prevent a fatal accident than it is to prevent a minor injury.

2. **How much can we improve or strengthen the precondition?** This criterion is related to the **effectiveness** of the safety measures that we can think of.

3. **At what price can we improve or strengthen the precondition?** This criterion is related to the **efficiency** of the safety measures we can think of.

Table 1. Possible format for prioritising actions.

Precondition	**How likely is it that this precondition will make a difference in future events?** **0 – impossible** **5 – highly likely to prevent a catastrophic event**	**Proposed action**	**How much can we strengthen the precondition? (Effectiveness)** **0 – we cannot make any difference** **4 – we can make a massive difference**	**At what cost? (Efficiency)** **0 – too high to be feasible** **3 – no cost or negative cost**	**Sum of scores**
Good road lighting	3 – only relevant when it is dark	Install road lighting on 12 kilometres road in the municipality	2 – only a small fraction of the total traffic runs at these 12 kilometres	1,5 – cost is significant but feasible	6,5
	3 – only relevant when it is dark	Reduce the maintenance intervals for road lighting by 50 %	3 – covers a large fraction of the traffic, and many lights are out today	1,5 – cost is significant but feasible	7,5

A possible format for prioritising actions according to these criteria is shown in Table 1.

A few features of this table are worth noting:

1. You may enter more than one proposed action for each precondition. You may also choose not to propose any action for a precondition, either because it makes very little difference, or because your organisation is not able to do anything about it.

2. For all three criteria, a high score indicates a "good" action. Therefore, an inexpensive action scores high on the efficiency rating. This allows us to compute overall scores simply by adding the scores on each criterion.

3. By using different scales on the three criteria (0-5, 0-4 and 0-3 respectively), we give them different weight in the overall score.

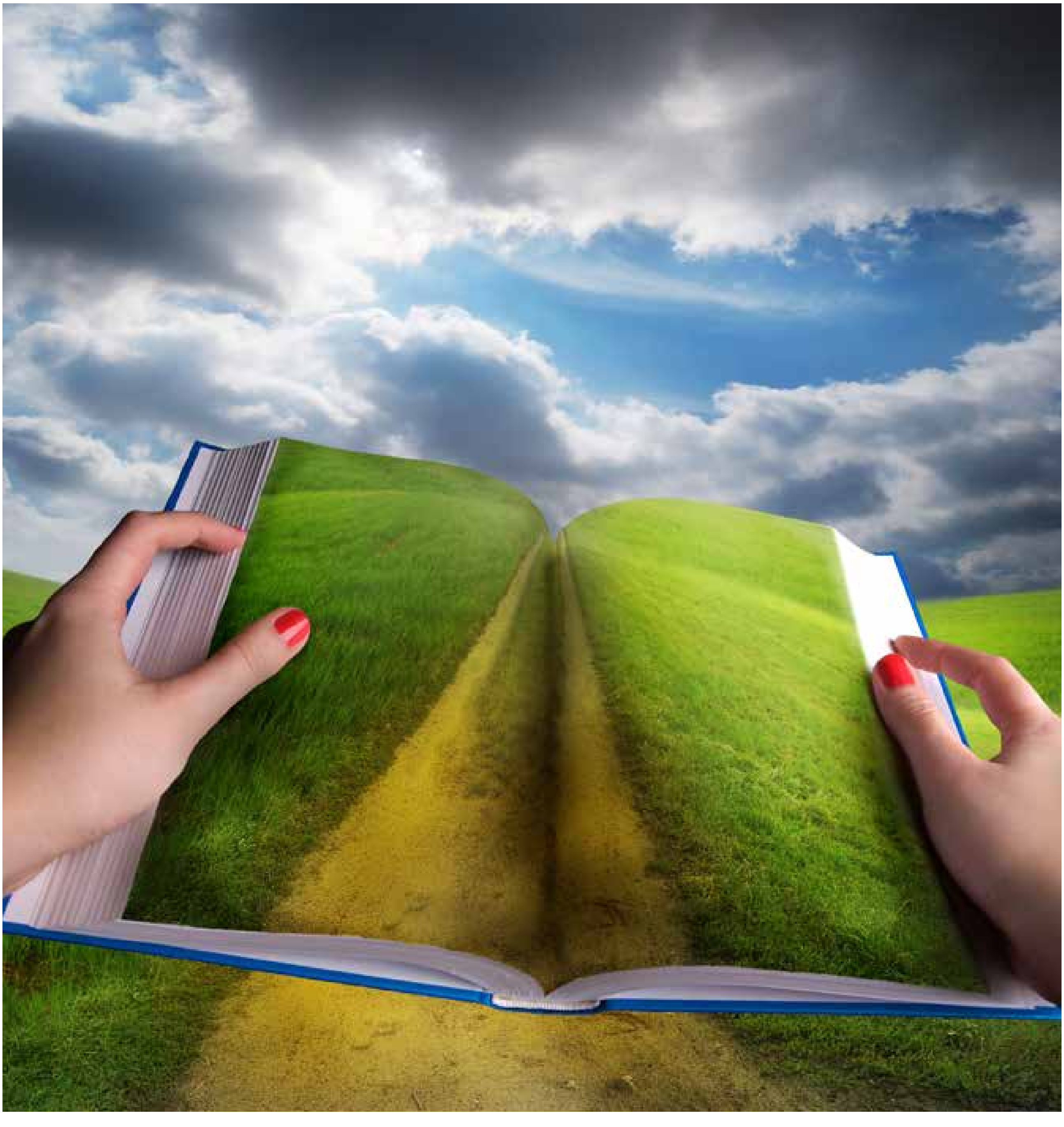
4. If you feel that the appropriate score for a criterion is, e.g. somewhere between 1 and 2, you can score it with a decimal fraction, e.g. 1,5. This adds precision to the rating process.

5. It is a good idea to give a short justification for your scores. First, it forces you to think carefully. Secondly, a justification is a good starting point for discussions and for communicating your priorities to others.

6. Some groups experience that they are very optimistic about the merits of their proposed actions, especially at the start of the rating process. Positive thinking is nice, but you may have a problem if you end up with 30 preventive measures with top score on all criteria. If you are very optimistic at the start, but turn progressively more critical to your own proposals, then you may need to reconsider the ratings of the first proposals. To avoid this, take some time to discuss how the proposed actions may fail to work as expected. For instance, if you propose to introduce a new rule or a new procedure, can you be sure that people will always comply with that rule or procedure? If you propose a technical solution to a problem, can you be sure that it will always be avail-

able when needed, that it will work as intended, and that people will use it in the intended way?

You should feel free to adapt the form and the way you use it to the needs of your organisation. For instance, you may use the form only within an investigation group, as a means to structure the discussion. Alternatively, you may give it a more official status as a means to document the work of the investigation group. You may also think of the form as a tool to support handover of the investigation process from an investigation group to line managers who are responsible for deciding and implementing preventive actions.



PART III:
What do you do when you build safety?

In this part of the guide, we describe how people act and collaborate to get things done without causing harm. To bring some order into the myriad of things people do when they build safety, we have sorted them into the following headings:

- Ensure adequate ***barriers*** against unwanted event sequences (Chapter 9)
- Ensure adequate ***sharing and interpretation of information*** (Chapter 10)
- Handle ***complex and hot-tempered*** technologies and operations (Chapter 11)
- Use ***organisational redundancy*** to ensure safe operations (Chapter 12)
- Ensure safety in the face of ***conflicting objectives*** (Chapter 13)
- Handle ***minor disruptions*** (Chapter 14)
- Prepare for ***a nasty surprise*** (Chapter 15)
- What happens ***when nothing happens***? (Chapter 16)

Each item represents a perspective on safety. When you observe people in a simulator or on the job, you may choose one or two of these perspectives to direct your attention, so that you know what to look for. You may also choose one of the perspectives as the topic of a workshop or a safety meeting. At the end of each chapter, you will find a few discussion topics. You may also use the discussion topics as an inspiration for devising your own topics, adapted to the challenges you are facing right now.

We have included some slightly complex examples to remind the readers that building safety is not always simple. We want to pay respect to the people who perform complex work year after year without causing major accidents.

9 Ensure adequate barriers against unwanted event sequences

There is no such thing as perfect humans or perfect technology. Errors and erroneous actions will occur. Therefore, an important way to ensure successful operations is to make sure that there are adequate barriers or defences in place, which can prevent an accident from happening even if an error occurs.

This idea is illustrated in Figure 4. Simplifying a bit, we may think of barriers as means to prevent or mitigate a specific unwanted event sequence. The figure shows one of the barriers against an event sequence that starts with a gas leak and continues with ignition of the gas leak and an explosion. One of the means that are used to break this event sequence is to isolate ignition sources. This is done in numerous ways, for instance by isolating electrical equipment that is used in the process area (Ex-approved equipment), by strictly regulating hot work in areas where gas leaks may occur, by automatically disconnecting electricity outlets if gas is detected, or by using the public address-system to order people to halt hot work if gas is detected.

We may think of barriers as means to prevent or mitigate a specific unwanted event sequence.

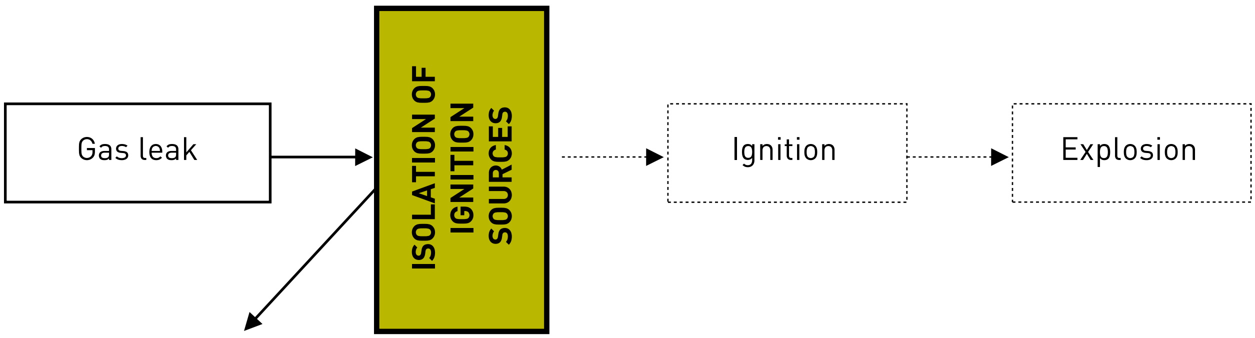


Figure 4. A barrier is means to prevent or mitigate a specific unwanted event sequence.

The consequences of a hydrocarbon fire or explosion on an offshore production facility can be very severe, as illustrated by the Piper Alpha and the Deepwater Horizon disasters. Therefore, several barriers are needed to keep the risk at an acceptable level:

- Process control (manual or automatic) to prevent extreme pressures and temperatures
- High quality containment
- Isolation of ignition sources
- Fire detection and emergency shutdown
- Area separation, fire/blast walls and passive fire protection
- Active fire protection (e.g. deluge system)
- Provisions for escape and evacuation.

In the context of well control, the main task of the barriers is to prevent uncontrolled flows of hydrocarbons from the reservoir, i.e. to avoid kicks or blowouts. The primary barrier in well control is usually the column of well fluid (mud or brine).

The proper function of each barrier depends on several parts or elements. High quality containment, for instance, depends on the integrity of pipes, flange connections, valves, separators and other components. The secondary barrier in well control may include the casing cement, the casing, the wellhead and the blowout preventer. A failure in any of these barrier elements could contribute to an accident. **Any action or practice that helps to ensure the proper**

function of these barrier elements contributes to safe operations.

RELEVANT ACTIONS, INTERACTIONS AND PRACTICES

9.1 Ensure that sufficient barriers are in place

This includes scrutinising plans and procedures to check that the necessary barriers are in place throughout the operation, and rechecking plans and procedures every time they are changed. It also includes carrying out compensating actions if one or more barriers have to be disabled, e.g. for maintenance or testing.

EXAMPLE:

- A safety engineer scrutinises the plan for replacing a valve on a process plant to make sure that sufficient barriers are in place against the pressurised sections of the plant during all steps of the operation. She also makes sure that no components are exposed to higher pressure than they are designed to withstand.

9.2 Testing or checking barriers

Even if barriers are in place, we need to ensure that they will work as anticipated when they are needed.

EXAMPLES:

- A drilling crew performs a pressure test to make sure that the casing and casing cement of the well can withstand the pressures that may occur during a well kick.

- A control room operator and a field operator technician check that the gas detectors function properly.

9.3 Ensure that barriers are independent

We mentioned that several barriers are needed to reduce the risk of some event sequences to an acceptable level. However, having many barriers may not be very helpful if a single event or condition can impair several barriers at the same time. Therefore, we want to ensure that the barriers are as independent as possible. Barriers are not independent if a single event can impair several barriers at the same time.

EXAMPLES:

- During handover between the day shift and the night shift, the supervisors take particular care of ensuring that all work permits have been properly closed, that the work has been completed, and that safety systems have been restored to their normal function. It may be necessary to disable several of the barriers against fires at the same time during testing and maintenance of the fire and gas system. A failure to properly close such work may leave the installation in a vulnerable state.

- An offshore installation manager (OIM) is concerned about increased maintenance backlog (overdue preventive maintenance) for safety critical equipment after a period of strict cost-cutting. Generally, inadequate maintenance could cause more than one barrier to fail at a time, and therefore reduce both the reliability of each single barrier and threaten the independence between barriers. The OIM therefore discusses the matters with his superiors and obtains extra funding for reducing the maintenance backlog.

DISCUSSION TOPICS

1. Has it happened at your installation that a plan for carrying out a job has been changed because somebody detected that not sufficient barriers were in place at some stage of the operation? How was the lack of barriers detected?
2. Does your company make a note of barriers that functioned in its accident investigations? Have you found ways to learn from these findings?

10 Ensure adequate sharing and interpretation of information

Virtually every major accident is perceived as a "fundamental surprise" by the senior managers of the organisations involved. However, precursors or warnings are nearly always identified in hindsight by accident investigators or by the media. More often than not, somebody tried to raise concerns but was not listened to. This means that nearly every major accident is preceded by a breakdown in the sharing or interpretation of information.

Turning this argument around, safety is built by every action and practice that helps the organisation collect, share and interpret information about how accidents may occur and how they can be prevented.

Nearly every major accident is preceded by a breakdown in the sharing or interpretation of information.

RELEVANT ACTIONS, INTERACTIONS AND PRACTICES

10.1 Share information across the boundaries of the organisation

The petroleum industry is criss-crossed by organisational boundaries, e.g. between shifts, companies, disciplines, onshore versus offshore. Many major accidents start at such boundaries – for instance because people fail to share crucial information, due to confusion or misunderstanding, or due to lack of coordination. Bridging across all those interfaces is thus an important contribution to safe performance.

EXAMPLE:

- A supervisor spends considerable time discussing the safety aspects of operations with people working within other disciplines. She has also made an effort to understand the jobs related to other disciplines and how her people can support or interfere with their work.

10.2 Challenge the prevailing understanding of the situation

The following example illustrates how members of a drilling crew discuss and challenge each other with respect to interpretation of data and understanding of the well control situation.

EXAMPLE:

- A drill crew is pulling the drill string out of the well. The mud logger monitors the mud volume. An increase in the mud volume is often the first symptom of a kick, i.e. a situation where oil or gas from the reservoir flows into the well because the pressure inside the well is lower than the reservoir pressure. The mud logger observes that the well takes less mud than required to replace volume of the drill string and he notifies the driller. The driller discusses the observation with the toolpusher and the assistant driller. They conclude that the well takes less mud than expected because of swabbing. Swabbing is a suction effect that may occur because the drill string acts like a piston if it moves too quickly out of the well. They therefore decide to continue tripping out, but at a slower pace, to avoid this suction effect. However, the mud logger checks the calculations of mud weight and finds an error. He calls the driller and argues that too low mud weight may have led to an influx in the well. The driller listens to his argument and makes a flow check, i.e. he stops moving the drill string and monitors the mud volume for a few minutes. The mud volume increases. The driller shuts in the well with the blowout preventer and discusses the situation carefully with the toolpusher and the company man.

10.3 Providing space and time for slow discussion and slow thinking

Many of the issues that confront operative managers are familiar problems with familiar solutions. Experienced managers can resolve such issues quickly, without spending much time on analysis and discussion. However, every now and then more "wicked" problems occur, which require careful deliberation to

find a proper solution. Providing the time to resolve wicked problems is an important contribution to successful operations.

EXAMPLES:

- A drilling rig has daily morning meetings on video between onshore and offshore managers where they discuss the progress of the operations and the problems and issues that have occurred. The time is limited, so the meeting is highly structured and the participants are expected to be brief and to the point. However, the managers have realised that some issues are too complex to be settled within two to five minutes. They have therefore made it a habit to leave the video connection open for another thirty minutes after the formal meeting has finished, thus allowing a few meeting participants to pick up on issues they want to discuss in more depth.

- A drilling crew is experiencing a problem, and the toolpusher feels a pressure to resolve it as quickly as possible to avoid downtime. However, the company man urges him to take the time he needs to make sure that he finds the best solution, and assures him that the operating company will cover the cost of the downtime.

10.4 Anti-scapegoating

Not all information is good news, and some organisations react on bad news by seeking a scapegoat. The effect is that people learn to keep bad news to themselves, in order to protect themselves or their fellow workers. Other organisations find ways to protect or even congratulate and celebrate people who are willing to share information about their erroneous actions. This is what we call "anti-scapegoating".

EXAMPLES:

- A drilling crew had just gone through a session of simulator training on well control. During the debrief they noted that it took a rather long time from the kick was observable until they had shut in the well. One of the crew members said "It was my fault". Another crew member immediately said: **"No, it was not your fault; we all could have spotted it."** Several more crew members confirmed this. This episode demonstrated the willingness of the drilling crew to share responsibility and their commitment to avoiding scapegoating. In this way, the crew members helped to build a culture where people can share bad news with the confidence that it will not be turned against themselves or their fellow workers.

The second example stems from Wernher von Braun, one of the pioneers in rocket development and space exploration[3]:

- "One of our early Redstone missiles developed trouble in mid-flight. The telemeter records indicated that the flight had been flawless up to that instant, and permitted us to localize the probable source of trouble. However, the suspected area had been very carefully checked in numerous laboratory tests so that all explanations sounded highly artificial.

  Several theories were advanced. Finally one theory was accepted as most likely and remedial action based on it was initiated. At this point an engineer who was a member of the firing group called and said he wanted to see me. He came up to my office and told me that during pre-launching preparation he had tightened a certain connection just to make sure that there would be good contact.

  While doing so, he had touched a contact with a screwdriver and drawn a spark. Since the system checked out well after this incident, he hadn't paid any attention to the matter. But now that everybody was talking about a possible failure in that particular apparatus, he just wanted to tell me the story for what it was worth. A quick study indicated that here was the answer. Needless to say, the "remedial action" was called off and no changes were made.

  I sent the engineer a bottle of champagne because I wanted everybody to know that honesty pays off, even if someone runs the risk of incriminating himself. Absolute honesty is something you simply cannot dispense with in a team effort as difficult as that of missile development."

DISCUSSION TOPICS

1. Can you think of an instance when somebody in your organisation drew attention to a safety problem before it had led to an accident? What does it take to make sure that decision makers recognise a safety problem and take appropriate action?
2. Have you experienced a situation when somebody challenged the prevailing understanding of the situation in your work team? How did people react to the challenge? How would you like people to react if you were to challenge the prevailing understanding yourself?
3. Have you experienced any instances of "anti-scapegoating" in you work team or in your organisation? What happened?
4. Are there people in your organisation who pay particular attention to sharing information across organisational boundaries? What do they do to achieve this?

[3] Von Braun, W. (1956). Teamwork: key to success in guided missiles. Missiles and Rockets, October, 36-40, p. 39. Cited from Ron Westrum (1993). Cultures with requisite imagination. In J.E. Wise, V. David Hopkin, P. Stager (Eds.) Verification and Validation of Complex Systems: Human Factors Issues. Berlin: Springer-Verlag.

11 Handle complex and hot-tempered technologies and operations

Some technologies and some operations are particularly difficult to handle. High Pressure, High Temperature (HPHT) wells can be complex and unforgiving, and they can kick furiously. Some production facilities have very complex process units, which can fool even experienced operators.

Complexity is not only about how many parts a system consists of. It is also important how the parts or subsystems interact, i.e. interactive complexity. Complex systems are more likely than other systems to confuse you, to give you nasty surprises, and to react in other ways than you expect. We speak of 'tight coupling' or' tightly coupled systems' when disturbances can develop, propagate and escalate rapidly.

Offshore installations are characterised by a lot of equipment squeezed into a rather small space. This, combined with a high activity level and huge amounts of energy, tends to make offshore installations both complex and tightly coupled.

> Complex systems are more likely than other systems to confuse you, to give you nasty surprises, and to react in other ways than you expect.

Complexity and coupling can also change during an operation. A gas kick with a large influx can turn a well into a more complex and tightly coupled system than it was before the kick occurred. There will be a large amount of gas in the well. When the well is shut in, the pressure at the bottom of the well may increase as the gas migrates towards the surface. This is, however, not visible to the drilling crew. They have to infer the state of the well from parameters such as pressures at the surface level and changes in mud volume.

This chapter is about the things people and organisations do to maintain safety when working with complex and tightly coupled (or hot-tempered) systems.

RELEVANT ACTIONS, INTERACTIONS AND PRACTICES

11.1 Loosen tight couplings

Loosening couplings means to change things so that the effects of an error or a disturbance will propagate less rapidly or will be less likely to escalate into something serious.

EXAMPLE:

- A valve in the process unit needs to be replaced. It is physically possible to do this job on a hot platform. However, due to the design, it is only possible to introduce one barrier (a closed valve) between the valve to be replaced and hydrocarbons under high pressure. The planner decides that this would introduce too tight coupling, since a single failure might cause a major hydrocarbon leak. He therefore decides to defer the job to the next revision shutdown.

11.2 Reduce interactive complexity

Reducing interactive complexity means that you make things simpler and more transparent. You try, in particular, to reduce the likelihood that two activities or two subsystems will interact in an unforeseen manner.

EXAMPLE:

- An offshore installation manager on a complex installation reviews the work permits for the following day. She feels uncomfortable about the activity level, fearing that the platform crew may not be able to coordinate properly if one or more tasks cannot be performed in accordance with the plan. She decides to reduce the number of concurrent tasks by withholding one work permit.

11.3 Strengthen coordination to handle tight coupling

Tightly coupled systems are unforgiving and hot-tempered. Effective coordination can help to avoid that disturbances occur in the first place. Effective coor-

dination is also needed to keep disturbances from propagating and escalating if they should occur.

EXAMPLE:

- The work permit system is an important means of task coordination in the process industry. It helps to prevent conflicts between concurrent activities. It also ensures that compensating actions are taken if some of the ordinary barriers have to be disabled, for instance during testing of gas detectors. The work permit system also helps to keep the control room operator updated on the status of the ongoing activities.

11.4 Prepare to handle complex and tightly coupled system states

We argued that some systems can suddenly turn more complex and tightly coupled. It is often possible to make preparations for such situations.

EXAMPLES:

- A drilling crew is about to drill into a zone where they know that the risk of taking a kick is rather high. The drill crew therefore reviews the steps they have to take in case of a kick. They check the line-up of valves on the BOP panel. A kill sheet has been prepared where a number of calculations needed to handle a kick have been done in advance. They also check that enough kill mud is available. Such preparations increase the crew's autonomy in case of a kick, so that necessary actions may be taken without the need for time-consuming clarifications from higher management levels or outside experts.

- A maintenance team performs a Safe Job Analysis before they start a job on a hot platform. They also discuss what complications or surprises may occur during the job, and how to handle them. This allows them to check out that everybody knows enough to do the job safely, and it makes them mentally prepared to handle contingencies.

11.5 Adapt the informal organisation structure to the situation

In flexible organisations, the decision making structure may be changed dynamically to match the environmental conditions. This is a well-known principle in so-called high reliability organisations, of which aircraft carrier crews may serve as examples.

EXAMPLES:

- LaPorte and Consolini observed that the people at an Air Traffic Control Centre changed collaboration patterns and interaction style according to the nature of the operation. During normal operations with moderate traffic intensity, they worked in a "bureaucratic" way. The line managers made the decisions and the interaction style was rather formal. During high intensity periods, the interaction style became more informal, and the most experienced controllers, irrespective of rank, made many operational decisions. The informal organisation had adapted spontaneously to a different operational context.

- An assistant driller, a toolpusher and a driller (who is in the chair) are talking in an informal way about the next step in the drilling programme. Suddenly, the driller says, "Hey, I think we have a kick". The assistant driller moves rapidly to the shutdown panel, and the toolpusher looks at the screens and confirms that this must be a kick. From this point, the driller and the assistant driller communicate in a highly structured way, repeating orders and crucial information to guard against misunderstandings.

DISCUSSION TOPICS

1. How would you describe the technology and operations you face in your daily work in terms of coupling and complexity? Is it, for instance, hot tempered?
2. How would you describe your organisation in terms of decision-making structure? Do you think the decision-making structure is well adapted to the properties of the technology (complexity and coupling)?
3. Have you experienced critical situations where a coordinated response was essential to gain control? Have you experienced critical situations where it was necessary to improvise to gain control?
4. Would you say that the informal decision-making structure in your organisation is flexible? Can you point to an example where the informal structure changed in accordance with the demands of the situation? Is it desirable to arrange for a more flexible decision-making structure in your organisation? How could it be done in practise?

12 Use organisational redundancy to ensure safe operations

'Redundancy' often means something superfluous. However, redundancy can also be a means to ensure reliability and safety. The hydraulic circuits in the braking system of your car are duplicated in order to increase the overall reliability of the braking system. Redundancy is even used with humans to ensure reliable performance.

Think of the flight deck in an airliner. Two pilots collaborate to deliver exceptionally reliable performance. Most of the time, the non-flying pilot will stay a few minutes mentally ahead of the actions of the flying pilot, and check that the flying pilot does what she is supposed to do. At times of peak workload, the non-flying pilot may relieve the flying pilot. When working through the checklists, the non-flying pilot helps to ensure that no checkpoints are missed. This is an example of organisational redundancy. Organisational redundancy refers to collaboration patterns that allow a group or an organisation as a whole to perform more reliably than each individual operator does. Organisational redundancy is created when individuals ask for advice and second opinions from knowledgeable colleagues, when an operator challenges the judgement of her colleague, or when she intervenes to recover an erroneous action by a colleague.

Organisational redundancy refers to collaboration patterns that allow a group or an organisation as a whole to perform more reliably than each individual operator does.

RELEVANT ACTIONS, INTERACTIONS AND PRACTICES

Some of the actions, interactions and practices related to ensuring adequate sharing and interpretation of information can also be viewed as means to utilise organisational redundancy. This applies to "Raising concerns", "Seeking a second opinion", and "Challenging the prevailing understanding of an organisation". All these actions can help a group as a whole to perform more reliably than a single individual.

12.1 Seek advice or a second opinion

A straightforward way to build organisational redundancy is to seek advice or a second opinion from a colleague, or an expert.

EXAMPLES:

- **A formation integrity test** (FIT) is a method to test the strength of the formation and the cement at the casing shoe prior to drilling a new section of a well. The pressure at the bottom of the well is increased gradually to a predetermined level by pumping mud slowly into the well. Then the pump is stopped and the well pressure is monitored. Ideally, the pressure should increase steadily while the pump is running and remain stable for several minutes after the pump is stopped. However, on one specific occasion, the pressure decreased somewhat after the pump had stopped before it levelled off. The offshore crew did not fully agree on how to interpret the result. They therefore contacted the onshore operations geologist, who again contacted the operating company's onshore second-call night-duty responsible for rock mechanics and well integrity. A little later, they called the drilling superintendent.

- A control room operator notes some unexpected trends in the process plant. He asks the shift supervisor to have a look and help to understand what is happening.

12.2 Offer assistance or advice to co-workers

You can also build organisational redundancy by offering assistance or advice to a colleague.

EXAMPLE:

- Air traffic controllers sometimes compensate for high traffic load by assisting each other. When traffic is particularly intense at one workstation (radar console), a third controller silently joins the two who are coordinating the sector. The third controller provides "an extra pair of eyes" and helps to detect potentially dangerous situations. He or she may provide suggestions, usually in the form of questions rather than directives.

12.3 Intervene when somebody makes a slip or mistake

A slip is an erroneous action that happens in spite of correct intentions. We often attribute slips to "inattention". A mistake implies that the person's intention was not appropriate to the situation. Mistakes may occur when people do not fully understand the state of the system they operate or the consequences of their actions.

EXAMPLE:

- One group of operators were preparing for an inspection of the kill mud system, which is part of the platform's blow-out protection. **They opened a valve toward the flare system**, in order to vent off gas released from a minor leak. The valve was left open for an extended period. At a different place in the same module, another group of workers started preparations for testing a Down

Hole Safety Valve (DHSV, another barrier against blowouts). As part of these preparations, they initiated a pressure release, **thus blowing gas into the flare system**. One of the operators working on the kill mud system, an experienced mechanic, noticed that the pressure release had started. He immediately shouted to the person performing the pressure release that he should close the valve towards the flare system at once. The valve was closed and the pressure release terminated. A moderate amount of gas was released from the flare system at the place where the first group of operators had started work on the kill mud system. A single gas alarm was activated. The intervention of the mechanic prevented a major gas release, which might have caused a shutdown and increased risk of fire or explosions.

12.4 Double check plans and decisions

Organisational redundancy applies not only to the physical execution of work. It can also apply to planning and decision-making.

EXAMPLE:

- The work permit (WP) system implements double checking of plans and decisions concerning safety critical work. According to NOG Guidelines 088, a level 1 WP must be approved by the approver/area/operations supervisor, checked/quality-assured by an HSE function on the installation if such a function exists, and approved by the overall approver / platform manager. All level 1 WPs shall be discussed at the installation's daily meeting for the coordination of WPs and simultaneous activities.

12.5 Utilise information technology to build redundancy

Information technology plays an important role in most parts and processes of the organisation. Still, it may not always be utilised as targeted for safety as it is for administrative means. 'Integrated Operations' is an example of efforts to utilise information technology to connect the offshore organisation with the onshore organisation, i.e., to provide expert support to the operative environment.

EXAMPLE:

- When carrying out challenging drilling operations, the chances are that similar operations have been carried out previously by colleagues under similar conditions, and from which there could be a learning potential. By utilising rich communication channels, offshore personnel may discuss with, and seek advice from colleagues located elsewhere, in real-time, to ensure that optimal methods are chosen for the particular operation.

DISCUSSION TOPICS

1. Has organisational redundancy been established for critical actions and decisions in your organisation? Give one or more examples.
2. Have you experienced a situation where an accident, a near-accident, or a situation with high risk has been avoided because somebody asked for advice, offered advice, or asked a critical question?
3. Have you experienced situations where the interaction style and the informal organisation structure at your workplace changed in response to a demanding situation, for instance, a kick or an alarm?
4. How can onshore and offshore operations rooms be utilised to make the most out of information technology, and to provide redundancy in planning and operations?

13 Ensure safety in the face of conflicting objectives

We live in an open market economy. Organisational survival is a matter of balancing on the edge in order to deliver "cheaper, better and faster" than the competitors, while at the same time delivering the expected return for investments to the shareholders. Safe performance sometimes requires considerable resources such as money, time and competent personnel. Handling tensions between safety and efficiency is an important contribution to safe operations.

One example of this occurs when drilling operations have to stop because of a technical problem. Both operators and drilling contractors consider downtime undesirable. Drilling contractors consider downtime a threat to their reputation even when the operator carries the cost of downtime. The sense of time pressure during downtime can lead to a rush to get back to normal operations, sometimes accompanied by stress and perhaps even violations of safety procedures.

Handling tensions between safety and efficiency is an important contribution to safe operations.

RELEVANT ACTIONS, INTERACTIONS AND PRACTICES

13.1 Keeping tasks in reserve in order to avoid downtime

The idea is to keep tasks on the critical path of the operation in reserve. The crew can then switch to such tasks if the planned operations have to stop. The halt in planned operations will not count as downtime, nobody suffers an economic loss, and there will be less pressure for returning quickly to the planned operations. A drilling supervisor gave the following example.

EXAMPLE:

- *"We have a job which we call 'picking pipes'. When we get deliveries of drill pipes, then they are bundled on the pipe deck, and then we screw them together by threes and stack them in the derrick. When we get a delivery of drill pipes, we never pick up more pipes than we need for the next job, even if we are going to drill further down later in the operation. Then we can save this until we get trouble with something, or have to wait for some equipment, or something that breaks down. Then we can start picking pipes, and perhaps we have enough pipes to keep going for 24 hours without having downtime."*

13.2 Take a timeout

This action also includes legitimising taking a timeout or asking for a timeout.

EXAMPLE:

- A drilling supervisor explains what he usually does if the drilling operations have to stop because of a problem: *"I go with the toolpusher, and we all meet where the job is to be done. Then we talk through the job and what is to be done, have a little chat about it before they get going, and make sure that all the paper work is in order and that they follow the procedures. The point is to make it absolutely clear that there is no stress from our point of view. And then I think it is important to leave them alone while they do the job. There are those who watch them all the time while they do such a job, but then they make people more nervous, and things start to happen ... "*

13.3 Communicating about priorities, making conflicting goals explicit

Most companies are good at stating in general terms that safety is priority number one. The other part of this task is to be clear about priorities in specific situations, in particular when everybody knows that safety comes at a price.

EXAMPLE:

Se Section 13.2.

13.4 Ensuring a good decision process, reaching a conclusion in an orderly manner

This is about adapting the decision process to the criticality of the decision and the complexity of the situation. Rapid decision-making based on intuition can be fine in simple, non-critical situations. Careful decision-making is called for when lives or values are at stake, in particular when the situation is complex or ambiguous. Then you want to make sure you have the necessary information, that you understand the situation properly, that you are aware of the important risks, and that the people involved understand the decision and are able to implement it. You will also want the people involved to support the decision.

EXAMPLE:

- Emergency situations can put the decision-making capability of the organisation to a severe test. Life and values are at stake, the situation may not be fully understood, and there is limited time to reach a decision. In order to prepare for such situations, offshore emergency teams are typically trained to go through a structured decision cycle, which includes information sharing, understanding the big picture, identify the worst case scenario, decide on actions and communicating the decisions. Offshore installation managers are also trained to delegate responsibility when appropriate. This is an effective way to share the workload.

13.5 Provide stop rules

People at the sharp end sometimes have to make critical decisions in stressful situations. Clear stop rules can be an effective safeguard against erroneous judgments. A clear stop rule or decision criterion also means that they can choose the safest alternative in the face of conflicting goals without fear of blame or reprisals.

EXAMPLE:

- The pilots of an aircraft detect an instrument error while they go through their checklist before start-up. They call a technician. The technician examines the problem and checks it against the Minimum Equipment List. The Minimum Equipment List specifies the systems that have to be operative for the aircraft to be considered airworthy. Based on this, the technician decides that plane is not airworthy. The technician can make this decision without weighting pros and cons – for instance the number of unsatisfied customers versus the risk that the error could cause an accident.

13.6 Change the economic trade-offs for a contractor in favour of safety

A client can influence how a contractor handles conflicting objectives by devising appropriate economic incentives. This can, for instance, be done by devising a rate structure that reduces the economic loss of the contractor in case of downtime.

EXAMPLE:

- The rate structure for the drilling contractor on a production platform ensured that the contractor still got paid for the personnel, even when they had downtime. A drilling supervisor explained: *"When [the drilling crew] have downtime, they still get paid for their personnel. They only lose the part that covers maintenance and spare parts. [They get] wages for the personnel, but no profit or extras. … So, of all the places I have been, platform X is the one where people have been least stressed … with regard to downtime."*

13.7 Distinguish between urgent and not so urgent safety issues

Even on an ordinary day, most managers and many others experience an overload of tasks and problems. There is simply not enough time to dig deeply into every single problem. Managers even have to divide their attention between different safety issues, for instance fighting lost time incidents versus preventing major accidents.

EXAMPLE:

- Many companies follow up lost time incident rates closely, and some companies attach bonuses to them. Nobody would disagree that it is a good thing to prevent personal injuries. However, sometimes managers, employees or safety specialists raise a concern that the focus on occupational safety hazards may cause managers to pay too little attention to the hazards that can give rise to major accidents.

DISCUSSION TOPICS

1. Does your organisation keep tasks in reserve in order to avoid downtime? Can you remember an instance when planned operations had to stop, and you switched to such tasks?
2. Can you remember an instance when somebody told you to take a timeout? Have you asked for a timeout yourself? What would you typically do during the timeout?
3. Can you give one or more examples of stop rules that are important to ensure safety in your job? Can you think of situations where you would prefer to have more clear-cut stop rules?

14 Handle minor disruptions

Minor disruptions may lead to serious delays in operations. This may be important and positive consequences of disruptions, since it may reflect adequate barriers or sufficiently loose couplings to prevent errors propagating through the system and developing into situations that are more serious.

Many minor disruptions may find their adequate solutions by organisations and operators properly equipped with knowledge and methods for handling such disruptions.

Sometimes the solution may be to work around the problem rather that tackling it directly.

RELEVANT ACTIONS, INTERACTIONS AND PRACTICES

14.1 Finding ways to get around problems

Certain problems do not follow the usual pattern and are not easily solved by following normal procedures. Sometimes the solution may be to work around the problem rather that tackling it directly.

EXAMPLE:

- Consider the following example: A surgeon has troubled for a long time guiding a stent graft into the right branch of a blood vessel. He has tried different techniques and equipment, and time is about to run out. In such cases, surgeons may experience that instead of continuing trying even harder, an invitation to the assistant surgeon may turn out to be a surprisingly easy solution. It happens not seldom that a new person with a slightly different technique comes past the difficult point, although it may be difficult to articulate exactly what she does differently.

14.2 Recognising patterns based on experience

While technical systems often apply advanced and opaque physical models to evaluate the state of affairs, human perception is particularly good at recognizing patterns. This may be used both for validation and for alternative interpretation.

EXAMPLE:

- One example may be why a formation integrity test[4] (FIT) that shows a drop in the curve where it should be constant may still be considered acceptable from an operational perspective. While one has given up explaining this phenomenon theoretically, substantial evidence from wells in the same area has consistently proven that this FIT pattern is "normal" and to be considered as the local, empirical variant of the general, theoretical pattern.

14.3 Surprise handling

Thinking of possible futures, thinking of the future as an event tree can have a profound impact on how you plan and prepare for a job. Such planning may be the difference that transforms awkward surprises into management by improvisation.

EXAMPLES:

- A surgeon told us about how he prepared for an operation: When the time of the operation drew near, he studied X-rays and planned the surgical procedure. He usually had a "plan B" and perhaps a "plan C" ready at hand. He often had to change his decision based on things he found out while performing the surgery, but this was usually based on plans made up in advance.

- In complex systems, the types of challenges facing the operators are never identical. Drilling is one such example. The underground geological formations are never completely known before they are being drilled through. Hence, the challenges one may face are often unique and un-

[4] See Section 12.1 for a brief explanation of formation integrity tests.

expected. Although the challenges are unique, however, one may apply techniques that reduce novelty and help operators find practical solutions instead of reinventing the wheel every time.

14.4 Deciding to abort a job

Although the primary focus when confronted with challenging situations will be to look for compensating actions or workarounds, abortion should always be a part of the standard repertoire. Although obvious, this option may sometimes be suppressed and forgotten under pressure from colleagues and managers. Some types of work are simply so risky that they should be avoided.

EXAMPLE:

- Formation integrity tests are undertaken to ensure that the geological formations to be drilled into are sufficiently strong to withstand the pressure exerted by the kill fluids in case a kick should occur. When such tests fail (i.e. do not confirm sufficiently strong formations), it is not unusual to advice new tests with adjusted test parameters. Should several consecutive tests fail, it is natural to reflect upon how far the test parameters can be stretched before one changes the diagnosis from mistuned test parameters to deceitful geological conditions. In some rare cases, wells must be abandoned, although this implies high costs.

DISCUSSION TOPICS

1. Can you remember a situation where it was not feasible to follow the standard procedure? How was the decision made to divert from the standard procedure? Who was involved? Did you analyse the safety implications of deviating from the standard procedure?
2. What should be the criteria for accepting experience-based deviations from standard operating procedures?
3. Can you think of a job where you plan for surprises, i.e. where you have a Plan A and a Plan B?

15 Prepare for a nasty surprise

Surprises belong to a strange class of phenomena that are defined by how they are perceived rather than by what they are made up of. This makes surprises particularly difficult to handle. Since surprises are inherently unexpected, they are problematic to prepare for. The research literature suggests several strategies to cope with surprises.

RELEVANT ACTIONS, INTERACTIONS AND PRACTICES

15.1 Managing the unexpected

Managing the unexpected requires development of generic capacities that may respond to a variety of situations, including situations that fall outside the envelope of the known – such as 'black swans'. The term 'resilience' is sometimes used to portray such capacities.

EXAMPLE:

- In order to develop capabilities to handle unexpected situations, one may practice a 'second order of rehearsal', that is, train on improvisation. The point of such training is not to gain expertise on the particular scenarios, but to improve individual and collective skills in improvisation as such. Hence, the training scenarios need not to have anything to do with the type of work one usually is exposed to. Scenarios that are used for teambuilding in organisations, where the aim is collegial unity, may sometimes have qualities that serve the purpose of developing individual and collective improvisation.

15.2 Expansion of expectancies

Another way to prepare for surprises is to fold the unexpected into the envelope of the expected, to try to identify the black swans before they appear. This is sometimes referred to as a central capacity of so-called high reliability organisations.

EXAMPLE:

- One way to expand the expectancies is through the development of scenarios. This is used, for example, to train the emergency services in municipalities. When police, health and fire department must deal interactively with realistic scenarios, novel situations will usually emerge that were not part of the planned scenario. This effect can be exploited to gain genuinely new experiences and thus expand the envelope of the expected.

15.3 Meeting variation with variation

In the fifties, the cybernetic Ashby formulated a 'law' stating that to be able to control an environment that exerts high variety, one must have at disposal an even greater variety of responses. In terms of safety, this has been translated into a requirement of having at disposal a variety of theories, tools and methods in order to control complex and unpredictable high-risk systems.

To be able to control an environment that exerts high variety, one must have at disposal an even greater variety of responses.

EXAMPLE:

- Emergency medical care is organised on the principle of meeting variation with variation; the teams are composed of a great variety of personnel from complementary professions. Emergency care units are usually located with easy and quick access to the different specialised services such as heart, lungs and neurosurgery. In that way, one seeks to meet the natural variety of accidents and injuries with an even greater variety of care.

DISCUSSION TOPICS

1. What do you associate with surprises in your organisation? How can your organisation improve its capability of handling the unexpected?
2. Can you remember an instance when you managed to expand your expectancies during the planning and preparations for a job?

16 What happens when nothing happens?

There are times when apparently nothing of interest happens at a workplace. Things run smoothly, people do "what they always do", everything looks normal to an outsider. There is a tendency to pay more attention to outcomes than to the meticulous work – the adjustments of standard practices, adaptations of procedures and the discretionary judgements – involved in getting there. That is why safety is sometimes regarded as a non-event – as if nothing seemingly happens, or at least it does not receive attention. Learning from safe operations, however, requires a register of attention and methods to describe and analyse this meticulous work.

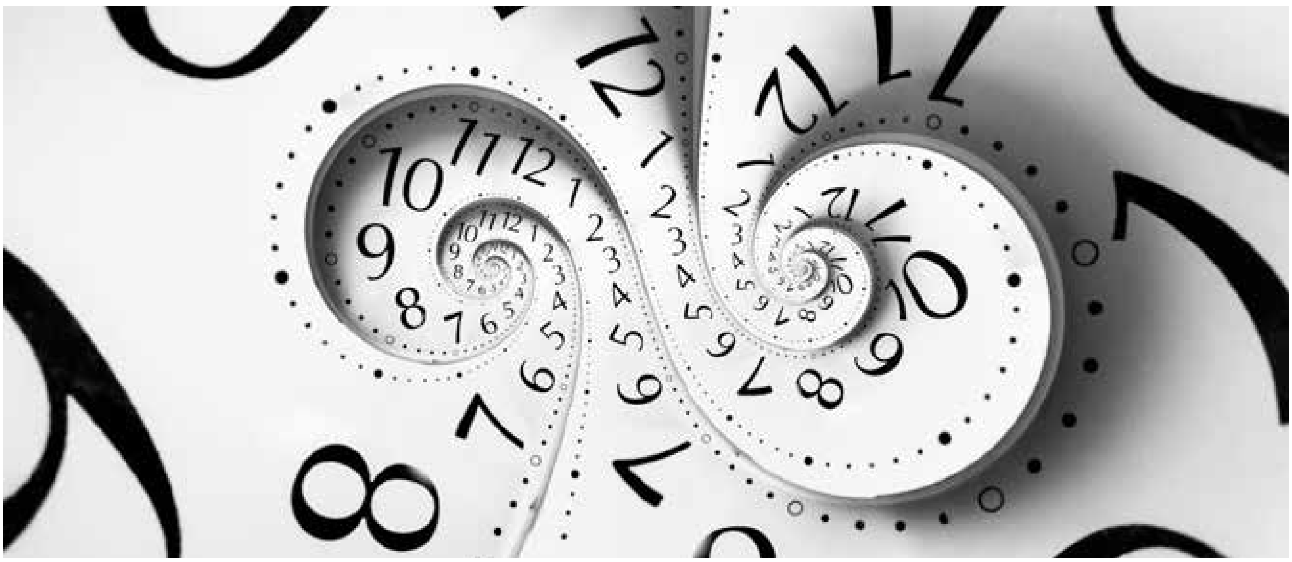
Think for example of the captain and his co-pilot bringing a Boeing aircraft safely down. For an untrained observer – and even for trained pilots – that operation may seem routine, not deserving any particular attention; the work is well described by the standard operating procedures. But if we scrutinise the landing operation and focus on the details, we will see that there is much more going on than what the summarised descriptions indicate. Landing wheels may come down earlier than usual because the speed is a bit high, the descent route may deviate slightly from the standard due to the local wind conditions that particular day, and the fact that the plane lands on time may be due to several experience based time saving practices at different stages of the flight.

There is a tendency to pay more attention to outcomes than to the meticulous work – the adjustments of standard practices, adaptations of procedures and the discretionary judgements – involved in getting there.

RELEVANT ACTIONS, INTERACTIONS AND PRACTICES

16.1 Create and maintain conditions that are necessary to carry out work safely

It is well known that following procedures in a strict and literal manner may turn efficient and safe operations into highly inefficient and not necessarily safe operations. The need to adapt procedures to local and current context is formulated in, or demonstrated by, the ETTO-principle (efficiency-thoroughness trade-off). An alternative to under-communicating or condemning such adaptations is to formulate proce-



dures that are context-sensitive and that are explicit about the type and degree of discretionary judgement that may be necessary and acceptable.

EXAMPLE:

- When working with procedures and designing or re-designing work processes, practitioners may be included in the work to ensure practical relevance and desired level of flexibility of the procedures. Procedures may also be reviewed on a regular basis, since working conditions may change.

16.2 Reflect on everyday practices that keep operations on track under varying conditions

How people work is one of the best kept secrets in America, a sociologist of work once said. While the nitty-gritty details of carrying out procedures under varying conditions are embodied knowledge for each operator, they are often invisible to their colleagues or the rest of the organisation, including those who write the procedures. These nitty-gritty details of making the procedures work – sometimes referred to as articulation work – should be made visible to the organisation in order to take care of the relationship between work as imagined and work as done, and to detect early instances of drift away from preferred practices.

EXAMPLE:

- To make visible discretionary judgements and situated adaptations under varying operational conditions, practitioners should be given sufficient time and suitable tools. The organisation may also consider offering dedicated arenas for regularly discussing these issues. For example, pilots in a helicopter company may have developed the habit of taking off towards angled terrain when they have flights in that direction and are in a hurry. With sufficient time, tools and arenas to articulate and discuss these practices, the organisation may develop a shared understanding on whether or not this is an acceptable trade-off between efficiency and thoroughness. Should it represent an undesired trade-off, such discussions may prevent practices from unconsciously being institutionalised and taken for granted.

16.3 Monitor that which can become a threat in the near term

Variability in both environmental conditions and in performance occurs naturally and is not necessarily a threat to safety. However, rather than merely unsystematically acknowledge such variability one may seek to systematically account for it to be able to reveal 1) trends that may be camouflaged by variability, and 2) potential interaction/resonance between conditions that are not usually thought of as interconnected.

EXAMPLE:

- For system operators experiencing frequent alarms for conditions that are expected or considered safe, it may be normal practice to snooze that alarm for a while. For the period while that specific alarm is silenced, one may miss the trend of the parameter. In addition, one may miss coinciding alarms that would trigger suspicion and investigation. To be able to monitor potential threats indicated by variability, one may consider reviewing the system configuration with this challenge particularly in mind.

DISCUSSION TOPICS

1. How do you distinguish adaptations that are acceptable from a safety perspective from those that are not?
2. Are there details in your job that people outside your team should have known more about?
3. Do you have specific clues that you use to detect things that can become a problem or a threat in the near term?

PART IV:

Terminology, background information and further reading

Part IV starts with explanations of a few terms from safety science that are used in the guide and that may be unfamiliar to some readers. Chapter 18 addresses some questions that students and researchers may want to ask about the learning guide. Chapter 19 contains suggestions for further reading. It is not necessary to read Part IV to use the other parts of the guide.

17 Explanation of key concepts

Barrier	Simplifying a bit, we may think of barriers as means to prevent or mitigate a specific unwanted event sequence. See Chapter 9. The Petroleum Safety Authority Norway proposed a more precise definition in a memo on barrier management: Barrier: Technical, operational and organisational elements which are intended individually or collectively to reduce possibility for a specific error, hazard or accident to occur, or which limit its harm/disadvantages.
Complexity	See 'interactive complexity'
Coupling	See 'tight coupling'
Interactive complexity	Systems with a high degree of interactive complexity are more likely than other systems to confuse you, to give you nasty surprises, and to react in other ways than you expect. Complexity is not only about how many parts a system consists of. Interactive complexity is also a consequence of how different subsystems interact. For instance, a heat exchange unit in a process plant may create a negative feedback loop, and this could cause the process plant to behave in confusing ways. See Chapter 11.
Redundancy	'Redundancy' often means something superfluous. Redundancy can also be a means to ensure reliability and safety. The hydraulic circuits in the braking system of your car are duplicated in order to increase the overall reliability of the braking system. 'Organisational redundancy' refers to co-operation patterns that allow a group or an organisation as a whole to perform more reliably than each individual operator does. Organisational redundancy is created when individuals ask for advice and second opinions from knowledgeable colleagues, when an operator challenges the judgement of her colleague, or when she intervenes to recover an erroneous action by a colleague. See Chapter 12.
Safe envelope	The limits an operation has to stay within, in order to keep the hazards under control.
Safety	By 'safety' we refer to a situation where the hazards that could cause an accident are eliminated or kept under control, for instance by means of barriers and adequate safety margins.
STEP	The STEP analysis (STEP – Sequentially Timed Events Plotting) is an accident analysis technique based on multi-linear events sequences and a process view of accidents/incidents. 'Multi-linear' means that we can identify and display two or more parallel chains of events. The STEP-worksheet is simply a matrix with a timeline. Each row in the worksheet corresponds to one actor. An actor is a person or an item that directly influences the flow or events. An event in the STEP diagram is one actor performing one action. See Chapter 8.
Tight coupling	We speak of 'tight coupling' or 'tightly coupled systems' when disturbances can develop, propagate and escalate rapidly. See Chapter 11.

18 Background information for researchers and students

Readers with an academic interest in safety science may want to know more about the origin of the material presented in this guide. This chapter attempts to answer some of the questions you may want to ask.

What is the research basis for the guide?

The guide is based on research performed by SINTEF, NTNU Social Research and NTNU in the project "Learning from successful operations". The project comprised theoretical work, interview studies, observations of practices on a semisubmersible drilling rig, and observation from training session in a drilling simulator. The guide also draws on previous research performed by the project partners.

How was the structure of Part III developed?

Our point of departure was six perspectives on organisational accidents and resilient organisations summarised by Rosness et al. (2010). We also used these perspectives as a means to sensitise ourselves during observations, as the perspectives gave some direction on what to look for. The chapters on handling minor disruptions, preparing for a nasty surprise, and what happens when noting happens cover different aspects of the resilience engineering perspective.

Where do the "actions, interactions and practices" in Part III come from?

These are the results of iterations between the theoretical perspectives mentioned above and empirical results from observations and interviews. Some of the examples were taken from earlier work performed by the members of the project team. Many of the examples have been slightly adapted to make them fit better into the context, or to make them easier to understand.

Are there any special challenges related to learning from success with regard to safety?

Yes! These are some of the challenges:

1. Characterising an operation as successful may be problematic, since the absence of adverse outcomes does not necessarily imply that the risk was well controlled. There is thus a need for additional criteria or approaches to distinguishing between successful and less successful operations.

2. Safety and successful operations is about the absence of adverse consequences, and may remain more or less invisible (a non-event). When nothing happens, there is no need for action, no sense of urgency. There is a challenge to foster an understanding that when "nothing" happens, a lot of things are actually happening to prevent things from going wrong.

3. Accidents and near accidents offer an obvious starting point for analysis. One may construct a causal chain or tree, starting with the physical processes that caused harm. No such starting point is given if there has not been an accident or near accident.

4. It is easy to get captured by "the official version" or "work as imagined" when describing a successful operation and explaining the success. Those aspects of successful performance that are not included in "the official version" may remain tacit, either because people are not aware of them, or because they lack the language for expressing them, or because they may fear sanctions for deviating from "the official version" as prescribed in rules and procedures. Consequently, learning processes may maintain current dogma and practices, rather than trigger new insight and improvements.

5. Successful operations rarely lend themselves to rigorous approaches for establishing causal connections between how operations are performed and the degree of success, such as true experimental designs.

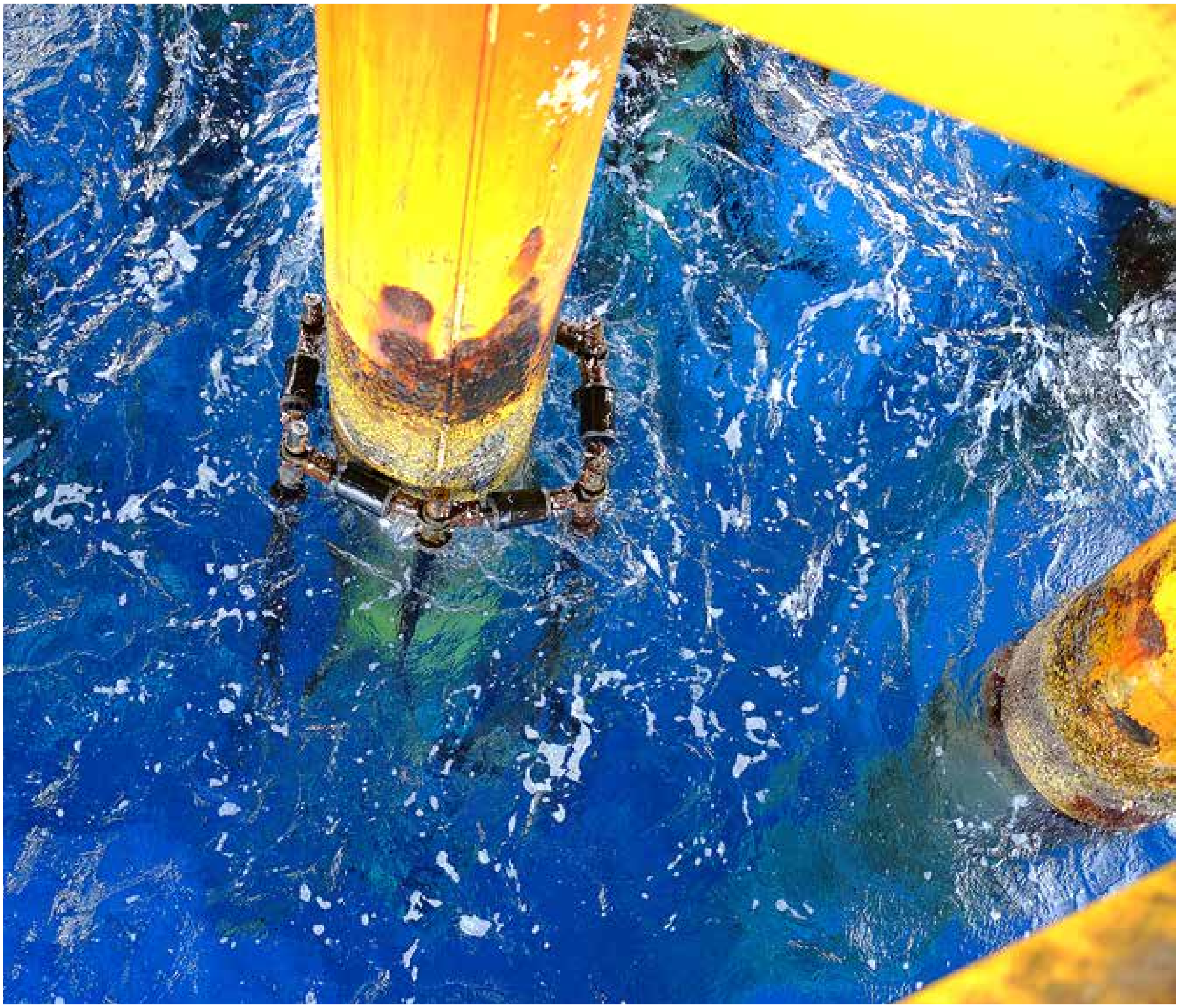
6. Strategies that contribute to successful operations in one class of sociotechnical systems may prove detrimental in sociotechnical systems with other properties. For instance, success in some systems depends on rapid and decisive interventions (e.g. Air Traffic Control), whereas other

systems call for careful deliberation before actions are taken (e.g. Nuclear power plants).

There seems to be a fundamental asymmetry between learning from accidents and learning from success. This asymmetry is to some extent analogous to the asymmetry between falsification and verification in Karl Popper's philosophy of science. A major accident goes a long way towards proving that a system is unsafe, since it falsifies the hypothesis that the system is safe. However, the absence of a major accident within a short or moderate time span does not prove that the system is safe. Even prolonged accident-free performance may not prove that a system is currently safe, since recent changes in the system could have compromised safety without yet causing an accident.

Is the guide exhaustive? Does it cover all the ways in which people build safety?

No! We would like to challenge practitioner-users, students and other researchers to find additional ways in which people build safety. One way to do this is to find a perspective that is different from the perspectives covered in Part III, and to use this perspective to sensitise yourselves to safety-building practices that are not covered in Part III.



19 Further reading

Rosness, R., Grøtan, T.O., Guttormsen, G., Herrera, I.A., Steiro, T., Størseth, F., Tinmannsvik, R.K., Wærø, I. (2010). *Organisational Accidents and Resilient Organisations: Six Perspectives*. Revision 2. Report no. A17034. Trondheim: SINTEF Technology and Society. ISBN 978-82-14-05056-1. http://www.sintef.no/publikasjoner/publikasjon/Download/?pubid=SINTEF+A17034

This report presents a broad selection of research on organisational aspects of safety and resilience and groups this literature into six perspectives. The six perspectives, with the associated literature, was our main inspiration when we worked out the structure of Part III of this guide.

LaPorte, T.R., Consolini, P.M. (1991). Working in practice but not in theory: Theoretical challenges in high reliability organizations. *Journal of Public Administration Research and Theory*, 1, 19-47.

This is a classical paper on High Reliability Organisations, and thus represents the first major research programme directed at explaining why some organisations have very few accidents.

Weick, K.E., Sutcliffe, K.M. (2001). *Managing the Unexpected: Resilient Performance in an Age of Uncertainty.* San Francisco, CA: Jossey-Bass.

This work is strongly inspired by earlier research on High Reliability Organisations. The authors develop a notion of "collective mindfulness" and they describe concrete practices that can be used to build collective mindfulness. The book addresses practitioners as well as academics.

Reason, J. (2008). *The Human Contribution. Unsafe Acts, Accidents and Heroic Recoveries.* Farnham: Ashgate.

This book provides an interesting collection of stories about successful recovery. It also discusses the preconditions for successful recovery in each case. These discussions emphasise individual factors. Reason concludes that "if there is one single most important contributing factor it is having the right people in the right place at the right time" (p. 236). We suspect that this conclusion partly reflects a limitation of his source material. The people who write about heroic recoveries are probably more interested in the heroes than they are in the organisational mechanisms that enable heroic recoveries.

Rosness, R., Haavik, T.K., Steiro, T., Tinmannsvik, R.K. (2016). Learning from successful operations – opportunities, challenges and a paradox. *Policy and Practice in Health and Safety.* DOI: 10.1080/14773996.2016.1255443.
http://dx.doi.org/10.1080/14773996.2016.1255443

The paper reports intermediate results from the project "Learning from successful operations", which provided the research basis for this guide. We discuss (1) criteria to identify an operation as successful with regard to safety, (2) implications concerning successful operations that can be derived from current organisational theories of safety, (3) how learning from successful operations can take place in practice and (4) challenges related to learning from successful operations.

Allspaw, J., Evans, M., Schauenberg, D. (2016): Etsy 2016 *Debriefing Facilitation Guide*. Brooklyn, New York: Etsy.
https://extfiles.etsy.com/DebriefingFacilitationGuide.pdf

This guide contains a lot of useful advice on how to facilitate discussions about incidents. This advice is relevant to short discussions, workshops, debriefing and incident investigations.

Organisations make great efforts to learn from their accidents, but they do not make a similar effort to learn from the operations that are performed without an accident, with adequate safety margins and with appropriate barriers in place. The objective of this guide is to help organisations learn from their successful operations.

We discuss how practitioners can initiate reflection and discussion on the actions and practices that contribute to safe operations. We also present a catalogue of actions and practices that contribute to safe operations. This catalogue provides topics and examples for reflection and discussion.

Accident investigators may use the guide as a support for identifying positive lessons to be learnt from accidents and near misses.

Practitioners, including line managers, safety staff and consultants may use the guide as a help in arranging discussions and workshops focusing on a specific successful operation.

Instructors may use the guide to support observation and debriefing in conjunction with training sessions in real work environments, simulators and tabletop settings.

Researchers may use the guide to support observations in real work environments as well as simulator environments that allow for observation of patterns of collaboration.

SINTEF

NTNU
Social Research