Disaster Management, Control, and Resilience

Erik Hollnagel

Abstract This chapter looks at disaster management as a form of safety management, using the perspective of resilience engineering. In safety management, control can be lost by not being ready to respond, by having too little time, by lacking knowledge of what is going on, or by lacking the necessary resources. To maintain control unsurprisingly requires the converse of these conditions. Resilience engineering looks at how systems can sustain required operations under both expected and unexpected conditions by adjusting its functioning prior to, during, or following changes, disturbances, and opportunities. To do so requires the abilities to respond to what happens, to monitor the situation, to learn from what has happened, and to anticipate what may happen. The same type of analysis can be applied to disaster management, to better understand how it succeeds.

Keywords Resilience · Control · Responding · Monitoring · Learning · Anticipating · Positive capacity

1 Introduction

Disaster management is an exercise in dealing with rare and therefore unexpected events. Safety management also deals with the unexpected, although the events on the whole are less surprising. In both cases the unexpectedness usually refers to the timing of what happens, in terms of the onset as well as the duration, rather than to the type of event as such. We know that a fuse may blow, that an engine may fail, or that torrential rains may flood an area, but we do not know *when* it will happen, *how serious* the consequences will be, or *how long* it will take before a stable condition has been re-established. The unexpectedness may, of course,

E. Hollnagel (✉)
Institute of Regional Health Research, Region of Southern Denmark, Center for Quality, University of Southern Denmark, Odense, Denmark
e-mail: erik.hollnagel@rsyd.dk

A. Masys (ed.), *Disaster Management: Enabling Resilience*,
Lecture Notes in Social Networks, DOI 10.1007/978-3-319-08819-8_2

also refer to *what* happens as such, in the sense that the event or occurrence may be unusual or novel. This is obviously more unpleasant, since it is practically impossible to be prepared for events that have not happened before.

Westrum [17] proposed a distinction between three types of threats based on how expected—or unexpected—they were: regular threats, irregular threats, and unexampled events. We can apply this distinction not only to threats but to events in general. The **regular events** are those that happen so often that an organisation is likely to have experienced them, which means that it is possible to recognise them and to learn how to respond. Regular events more importantly happen so often that it is cost-effective to prepare a standard response and to maintain a state of readiness even though it is uncertain *when* they will happen. Examples are the typical occurrences that make everyday work difficult such as interruptions and disturbances, delays, equipment malfunctions and failures, and the mistakes that generally lead to insufficient time, insufficient resources, insufficient information, etc. Any organisation must obviously be able to cope with the regular events in order to 'stay in business'. Coping with regular events is therefore not a defining feature of a resilient organisation, although it clearly necessary that it can do so.

The **irregular events** are those that happen rarely but where each event by itself is imaginable. Irregular events occur outside the everyday experience of an organisation and are therefore commonly portrayed as unique, unprecedented, or even beyond categorisation. Their number is so large that it is practically impossible to think of, let alone prepare, a response to more than a few of them. Irregular events are so infrequent that an organisation may never have encountered them, hence has no experience to refer to, although it may know about them from the general lore or shared war stories. Irregular events are of course always unexpected and may often be difficult to recognise because they go beyond the experience of everyday work. Since they furthermore happen rarely, it will not be cost-effective to prepare a response to them or to maintain a general response capability. Responding to them therefore requires the ability to make rapid adjustments on all levels of an organisation – in other words, resilience.

Finally, the **unexampled events** are those that have not happened before, and that exceed not only the experience of an individual organisation but the collective experience of all organisations of the same type, or even of the society. (The financial crisis in 2008–2009 was an example of that.) Since unexampled events are virtually impossible to imagine, it is clearly also impossible to prepare any kind of general response to them or even to consider a general readiness. Unexampled events are the catastrophes or apocalyptic events that take everyone by surprise and thereby severely challenge the resilience of an organisation.

The characteristic features of the three classes of events are summarised in Table 1.

1.1 Be Prepared

A main concern in safety management is the need to be prepared. This is accomplished by trying to identify every serious event that could happen and then

Table 1 Management demands of three types of events

	Regular events, everyday nuisances, incidents, accidents	Irregular events (critical accidents, disasters)	Unexampled events (catastrophes)
Frequency of occurrence	High, everyday	Low, but events are imaginable	Rare and mostly unimaginable (until they occur)
Magnitude of consequences	Low, and in most cases well-known	High, with reason for concern	Extremely high, may exceed the organisation's ability to cope
Relevant data or information	Statistics, event reports (regular)	Simplified models, shared experience	Hunches, intuition, 'expertise'
Readiness, preparedness to respond	High, and costs are justifiable	Low, and costs are disputed	No readiness, cost are prohibitive
Presence of resources to respond	Available and appropriate	In principle available, but never exclusively	Rudimentary or non-existent
Predictability (of occurrence or of development)	Very high on both accounts	Low on both accounts	Very low, guesswork. May challenge readiness and resources

prepare a response to those that cannot be eliminated. Since it is assumed that technological or industrial systems are well-known and well-structured it is possible, at least in principle, to identify all possible 'negative' events. This assumption is behind approaches such as 'safety through design' or 'prevention through design' [13]. Yet 'prevention through design' will always be limited, if for no other reason then because the cost of prevention for some of the irregular events may exceed what an organisation—or a society—is willing to bear. This has been recognised by the As Low As Reasonably Practicable (ALARP) principle [19], where 'as low as reasonably practicable' refers to a level of risk that cannot be reduced further without an increase in cost that is disproportionate to the gain in safety. The risks that in this way fall by the wayside will nevertheless happen every now and then, and it is necessary to be prepared for those. Safety management therefore often spends considerable efforts to calculate the probability that specific events—or rather, specific outcomes—may occur. In this way we try to convince ourselves that only the low probability events remain, hence that we can feel safe [2].

The situation is different for disaster management, regardless of whether the disasters are natural or human-made. Just like safety management, effective disaster management depends on the organisation's preparedness, its ability to respond and the presence of recovery plans that can lessen the impact of a disaster. Disasters differ from accidents mainly in terms of the magnitude of their

consequences, which by definition are both substantial and long lasting—and furthermore rarely limited to the place where the initial event occurred. The type of events that are associated with disasters are usually known, such as earthquakes, floods, tsunamis, volcano eruptions, pandemics, uncontrolled large-scale releases of hazardous materials, catastrophic accidents, fires, or explosions. But unlike safety management it is practically impossible to prevent them even though they are known.

When unexpected events happen it is necessary to be able to control them and/or to absorb their impact. While this applies to both safety management and disaster management, it is more important for the latter because fewer of the events (earthquakes, floods, pandemics, etc.) can be prevented. The purpose of control—and, indeed, almost a definition of the term—is to change the developments of the event from being unforeseeable or uncontrolled to become foreseeable or controlled. The acute loss of control that follows an unexpected event will change the organisation from a normal and stable condition to an unstable condition. If it is possible to respond fast enough, it may be possible to regain control and return the organisation to the normal condition. If that is not possible, the organisation will sooner or later enter a state of disturbed condition from which it is impossible to recover directly to a normal state. When control eventually is regained, the organisation will enter a recovered, stable condition and may from there transition to the previous normal condition by a full restoration of control. The restored stable condition need, however, not be identical to the previous one, but will often represent a new equilibrium.

1.2 Surprises

Unexpected events are always to some degree surprising. Lanir [11] has proposed that surprises can come in two forms, called situational and fundamental surprises respectively. An event is called a **situational surprise** if it happens when it was not expected. It is not a surprise because of *what* it is—its nature—but because of *when* it occurs. Once it has happened, the further evolution is generally predictable and will therefore presumably be matched by the prepared responses. An event is a **fundamental surprise** if it either is a kind of event that had not been imagined, or if it develops—spreads or propagates—in ways that have not been envisaged. A fundamental surprise may challenge the existing assumptions about the world either in terms of the type of event that can happen or in terms of how events may develop. The former is characteristic of classical safety management while the latter is characteristic of disaster management.

Disaster management and safety management both start by the occurrence of an unexpected event and look for ways by which it can be contained or controlled. Disaster management must nevertheless more often face fundamental surprises, for which it is impossible to think of, let alone prepare a set of responses. This is why resilience engineering becomes of interest.

2 Resilience Engineering

The difference between 'classical' safety management and resilience engineering is made clear by the definitions of safety that the two approaches use. Safety is commonly defined as a condition where as little as possible, and preferably nothing, goes wrong. A typical definition is thus that safety is the "freedom from unacceptable risk" [13]. As a consequence of that, the main concern of safety has been with situations where things go wrong, particularly if there have been significant adverse consequences, such as major industrial accidents. But these are also the situations where safety by definition is absent, rather than present. Safety science and safety management has thus strangely enough been occupied with the logical opposite of safety [6]. The accepted way to accomplish this is by preventing failures and malfunctions from happening, for instance as in 'prevention through design'. Resilience engineering avoids this problem by defining safety as the ability to succeed rather than as the 'freedom from unacceptable risks', hence as associated with situations where things go well and where safety therefore is present. Resilience is more precisely defined as "the intrinsic ability of a system to adjust its functioning prior to, during, or following changes, disturbances, and opportunities so that it can sustain required operations under both expected and unexpected conditions" [5]. (This definition logically includes the classical definition of safety, since 'the ability to sustain required operations' is tantamount to the 'freedom from unacceptable risks.')

The definition of resilience engineering also points to qualities that are central to disaster management, namely the ability to restore or sustain required operations by responding in the situation (adjusting performance during the disaster), by being prepared when the disaster happens (adjusting performance prior to the disaster), and finally by using the lessons learned to rearrange or restructure how it works (adjusting performance after the disaster).

According to the definition of resilience proposed above, the goal of resilience engineering is to establish and maintain resilience in an organisation, which more precisely means that an organisation can function in a resilient manner. This can be achieved by focusing on four fundamental abilities: the ability to respond, the ability to monitor, the ability to learn, and the ability to anticipate. The four abilities are, of course, not independent of each other, and the dependencies must be carefully considered in planning any changes. Neither is it possible to define an ideal 'mixture' or proportion in general. Although it may be argued that an organisation cannot be resilient if any of the four is missing, the proper balance among them can only be established from a thorough understanding of the organisation and its typical operational environment.

2.1 The Ability to Respond

No organisation or system—indeed, no living organism—can survive unless it is able to respond to what happens. If this ability is missing, the survival will be

endangered in either the short or the long term, depending on how unstable the environment is. The ability to respond entails knowing what to do when confronted with regular and irregular disruptions and disturbances as well as with opportunities. The response can either be the implementation of a prepared procedure or activity, or the temporary adjustment of the ongoing functioning to match the new conditions. Since the ability to respond is a question of maintaining control of the situation, the inability to take advantage of an unexpected possibility may be as serious as the inability to respond to a threat.

The ability to respond can be elucidated by considering what is necessary for a response to be made. The organisation must first of all detect that something has happened; it must then recognise what has happened and determine whether it, given the circumstances, is so serious that a response is needed; and it must finally be able to deliver an appropriate response in the sense that it can bring about the desired outcome or change before it is too late.

In order to take action it is necessary either to have the requisite resources ready or to be flexible enough to make the necessary resources available when needed. If the event is a serious one, it may be necessary for the organisation to change from a state of normal operation to a state of increased readiness before it is able to respond. This points to other issues, such as the availability of resources, the urgency of the response, the ability to sustain a response for a prolonged period of time, the monitoring of the effects, etc.

A focus on the ability to respond can be the starting point for more specific questions about how the organisation works. One question concerns the events for which the organisation is able to respond. No organisation can be ready to respond to every situation or event—quite apart from the impossibility of thinking of everything. But it is important to know how the set of events (for which a response is possible) has been selected or defined, and whether the set—and the responses—are ever revised. Another question concerns the threshold for responding, i.e., how strong or clear a 'signal' or condition must be before something is done. It may be damaging to miss a critical situation, but it may also be damaging to respond to too many false alarms. Yet another concern is how the readiness to respond is maintained, for instance how plans are kept up-to-date, and equally important how the readiness to respond is verified.

2.2 The Ability to Monitor

Next in importance to the ability to respond, and in some sense inseparable from it, is the ability to monitor. Monitoring refers to the ways the organisation looks for that which may happen at the next moment or in the short term, both in the sense of opportunities and threats. The monitoring must include both that which happens in the environment, outside the organisation's boundaries, and that which happens in the organisation itself, i.e., its own performance. A prerequisite for monitoring is, of course, knowing what to look for. The essence of monitoring is actively to look for signs of what may happen rather than passively noticing what happens.

One obvious benefit from monitoring developments is that it becomes possible to respond faster, or perhaps even to respond pre-emptively. (Prevention is better than cure, as the saying goes.) Indeed, without some kind of monitoring all responses will be reactive because they will follow events; without monitoring, responding regresses to unsystematic and ineffective fire-fighting. The disadvantages of that are well known, such as losing time or spending more resources than necessary because (negative) consequences have had more time to spread. Effective monitoring enables the organisation to address possible changes before they become reality, both changes in the situation or environment—progress as well as deterioration—and changes inside the organisation, for instance depletion of resources or growing brittleness.

An analysis of monitoring cannot be separated from an analysis of the indicators or signals that the organisation looks for. Two important categories are lagging or leading indicators, respectively (e.g., [8]). Lagging indicators show what has happened—often with a considerable delay, such as the number of injured or dead, while leading indicators are *bona fide* precursors for changes and events that are about to happen. The main difficulty with 'leading' indicators is that their interpretation requires an articulated description or model of the process they represent. In the absence of that, 'leading' indicators are just defined by association or spurious correlations. Another important distinction is between clear and weak signals, and the trade-offs that the organisation must make in that respect. To play it safe, most organisations rely on clearly defined lagging indicators, such as on-line process measurements and accident statistics. The dilemma of lagging indicators is that while the likelihood of a successful response increases the smaller the lag is (because early interventions are more effective than late ones), the validity or certainty of the indicator increases the longer the lag (or sampling period) is.

A focus on the ability to monitor can also be the starting point for asking more specific questions about how well the organisation works. Just as for the ability to respond, one central question is how the indicators or signals have been chosen or defined, whether they are traditional or based on an articulated understanding of how the organisation and its environment functions. Another important question, already alluded to above, is whether the indicators are leading or lagging. A further question is how and when the indicators are 'read'. Is it done continuously, regularly, or when the situation seems to make it necessary? This can also be seen as a trade-off between efficiency and thoroughness of data collection, which is a question of costs and benefits. Yet another question is about the validity of the indicators and the validity of the signals or measurements that are being monitored. Is the validity based on a general agreement ('common sense') or does it have an empirical basis?

2.3 The Ability to Learn

The ability to respond depends on the ability to monitor, in the sense that the timing and precisions of responses can be improved by effective monitoring. But the

ability to respond and the ability to monitor also both depend on the ability to learn. Neither responding nor monitoring can improve unless some kind of learning takes place. Learning is the ability to make use of experience and is generally defined as 'a change in behaviour as a result of experience.' Yet while it is indisputable that future performance only can be improved if something is learned from past performance, it is essential to learn the right lessons from the right experience—to learn from what went well as well as from what went badly.

In areas where safety is important—safety management and disaster management—the accepted wisdom has been that one should learn from failures in order to avoid making them again. Learning has therefore typically been in the form of a post mortem or an autopsy of what went wrong. Consistent with that philosophy, it has been assumed that more can be learned from events with serious outcomes—unusual accidents and catastrophes—than from events with minor outcomes—everyday accidents and incidents. Nothing could be farther from the truth.

The effectiveness of learning depends on the basis for learning, on which events or experiences the organisation takes into account, as well as on how the events are analysed and understood. General learning theory tells us that effective learning requires three conditions. First, that there is sufficient opportunity to learn. Second, that there is some similarity between the situations or events. And third, that it must be possible to confirm that something has been learned. Learning is not just a random change in behaviour but a focused change that makes some outcomes more likely and other outcomes less likely. It must therefore be possible to determine whether the learning (the change in behaviour) has occurred and has had the desired effect. If learning has had no effect then it has not been effective, and if it has had the opposite effect then it has certainly been wrong.

In learning from experience it is important to separate what is easy to learn from what is meaningful to learn. The three conditions mentioned above favour events that happen frequently rather than events that happen rarely, which means events with minor or moderate outcomes rather than events with serious outcomes. Furthermore, since the number of things that go right, including near misses, is many orders of magnitudes larger than the number of things that go wrong, it makes good sense to try to learn from everyday events rather than from failures alone. Learning should also be qualitative rather than quantitative. Although it often is convenient to express experience in terms of the number or frequency of occurrence of specific types of events or outcomes, compiling extensive accident/outcome statistics does not mean that anyone will actually learn anything.

A focus on the ability to learn can in the same manner as before be the starting point for asking more specific questions about how the system works. The primary concern here is whether learning is based on what failed or went wrong (avoidance learning) or on what worked or went right (approach or audience learning). Another issue is when learning takes place. Here the big difference is whether learning takes place—and is supported—continuously, or whether learning takes place—and is supported—only in the aftermath of a significant (attention attracting) event. A further issue is how learning is implemented, i.e., the target of

learning. One example is that learning takes the form of (re)education of personnel, another that it takes place as revision of procedures or design of equipment. A fourth and for now final issue is how the effects of learning are verified—and importantly how the effects of learning are maintained—forgetting (individual and organisational) being what it is.

2.4 Ability to Anticipate

While monitoring makes immediate sense, it may be less obvious that it also is useful to look at the more distant future. Monitoring refers to what happens at the moment, and to the consequences of the actions that are taken. But the choice of which actions to take must include some kind of anticipation or consideration of the future, lest they be reduced to routine and reflective responses. The difference between monitoring and anticipation is whether the time horizon is limited to the current situation and the current activities (responses), or whether it is expanded to include parts of the future. Monitoring is associated with what is being done here and now, whereas anticipation is associated with tactics and strategy [14].

Risk assessment can be seen as a formalised form of anticipation that looks at future threats. Risk assessment is suitable for systems where the principles of functioning are known, where descriptions do not contain too many details, where descriptions can be made relatively quickly, and where the systems—and their environments—are sufficiently stable for their descriptions to remain valid for reasonable time after they have been made. For many present day systems these conditions are unfortunately not likely to be fulfilled.

Anticipation is similar to monitoring because it must consider both opportunities and threats. But anticipation differs by looking to the potential changes in the environment, rather than the potential changes in the organisation itself. One reason is that future changes in an organisation are more likely to be a function of changes in the environment than the other way around.

The purpose of looking for what may potentially happen is to identify possible future events, conditions, or state changes that may affect the organisation's ability to function in either a positive or negative way. The inevitable problem of anticipation is that the longer one looks into the future, the more uncertain the predictions will be. This is, however, not an acceptable reason for refraining from trying to anticipate, although that sometimes is the case. Neither should anticipation be skipped because it is 'unscientific', in the sense that it a qualitative rather than a quantitative endeavour.

The anticipation of threats or hazards has already been mentioned above. This type of activity has considerable support in formalised risk assessment methods such as FMEA, HAZOP, PRA, Fault Trees, and the like. The anticipation of future opportunities has little support in current methods, although it rightly ought to be considered just as important as the search for threats. This shortcoming is at least acknowledged by resilience engineering.

The ability to anticipate can be expressed in more operational terms by looking into some central issues, just as for the other abilities. One issue is what the organisation's view or 'model' of the future is, i.e., which assumptions are made about the future. Here we can distinguish between three characteristic views. In a *mechanistic* view, the future is conceived of as a mirror image of the past, and anticipation is therefore mainly extrapolations from the past. Typically, things that have gone wrong in the past are seen as (more) likely to go wrong in the future. In a *probabilistic* view, the future is described as a (re)combination of past events and conditions. This is the view that dominates traditional risk assessment methods, which put great weight on quantification and precise formulae and on calculating the probability that a specific hazard is realised. Finally, the future can be recognised for what it is, namely something that has not been seen before. What is going to happen is, however, not completely random but involves a combination of known performance variability that usually is seen as irrelevant for safety. This third view, which may also be called the *realistic* view, corresponds to the ideas of requisite imagination [1, 16].

Another important issue is what the time horizon of the organisation is. Here we are not talking about the time horizon for managing the event or disaster, but the time horizon for looking into the future. Many different priorities may determine that, and strong economic concerns tend to shrink the time horizon. But it is clearly important for an industry or a rescue organisation to consider what the types of events (requiring responses) may be five or ten years from now, what the resources or possibilities will be, and what the constrains (legal, environmental, political) may be.

A third issue is which risks are acceptable. Looking into the future is always associated with uncertainty, and the further one tries to look into the future, the larger the uncertainty will be. Despite that it will be necessary to make some decisions—either to prevent something from happening or to be ready in case an opportunity should arise (for instance by having sufficient reserves to put in action)—and the organisations willingness to trust its own predictions is therefore of considerable interest. Finally, one may also look at how often the future is considered, whether it is a regular or irregular (most likely reactive) event, and by whom. For instance whether there are specific organisation functions to do that, or whether it is outsourced to consultants or a think tank.

The detailed issues that can be derived from each of the four abilities demonstrate how it is possible to think about resilience engineering in a practical manner, for instance by using the Resilience Analysis Grid. The abilities and the issues can be considered on all levels of the organisation, from the level of management and planning to the level of operations and maintenance. The four abilities should, however, not be considered in the abstract but always by referring to a specific domain or field of activity, or even to a specific organisation at a certain point in time. For any given domain or organisation it will also be necessary to determine the relative weight or importance of the four main abilities, i.e., how much of each is needed. The right proportion cannot be decided analytically, but must be based on expert knowledge of the system under considerations and with due consideration of the characteristics of the core business. Yet the minimum requirement is that none of the four can be left out if a system wants to be able to perform in a resilient manner.

3 Management as Control

A system that is resilient is by definition able to remain in control of both expected and unexpected conditions. In order to understand how the four basic abilities contribute to that, it is necessary first to consider the typical reasons for loss of control. The industry-wide experience, ranging from single individuals interacting with independent and relatively simple machines such as a truck-driver, to groups of people engaged in complex collaborative undertakings such as a team of doctors and nurses in the operating room, points to a number of common conditions that may lead to the loss of control. These conditions are [1] not being ready or prepared when the unexpected happens, [2] not knowing enough about the situation, [3] not having sufficient time to think and to do, and [4] not having sufficient resources. Conversely, the ability to remain in control is enhanced if the organisation is ready or prepared for what happens, if it has or can get the information it needs, if there is sufficient time to assess the situation and decide what to do, and if the resources needed to effectuate the responses are available. Thinking in terms of resilience engineering makes this more concrete.

3.1 Lack of Readiness/Preparedness

Not knowing how to respond when something unexpected happens is practically a recipe for disaster. It effectively means that the situation is not only unexpected but also unrecognised and perhaps even unimagined—possibly even a fundamental surprise. There are two main reasons why an organisation may not be ready to respond. One is that it has not learned anything from previous situations, from the past; the other that it has not been able to anticipate or imagine what could happen.

The failure to learn is the most serious because it indicates that the organisation has ossified or become stale in established routines. Since, in the words of Norbert Wiener [18] “the present is unlike the past, and the future is unlike the present”, an organisation cannot rely on already established responses, but must constantly revise and update them. The most effective basis for that is learning from how well a response has worked in the past, both when it succeeded and when it failed. In relation to safety it has generally been taken for granted that it was best to learn from failures [9], and indeed that more could be learned the larger the failure or accident was. But as argued above, learning should consider the frequency of an event rather than the seriousness of the outcome.

Readiness can also be incomplete or deficient because the organisation has not been able or willing to think ahead or to anticipate. In some cases it may be due to a narrow focus on the current problems, hence a trade-off between thoroughness and efficiency. In other cases it may be due to oversimplified or overoptimistic assumptions about what the future might bring, either as a reluctance to look at potential problems and risks, or a confirmation bias. It may also be due to the general difficulties in acknowledging the importance of imagination, as in requite imagination described above.

The importance of being ready to respond was pointed out by Lagadec [10], who noted that:

> "… the ability to deal with a crisis situation is largely dependent on the structures that have been developed before chaos arrives. The event can in some ways be considered as an abrupt and brutal audit: at a moment's notice, everything that was left unprepared becomes a complex problem, and every weakness comes rushing to the forefront."

Considerable efforts in both safety management and disaster management should therefore be used to prepare for how to respond when something happens.

3.2 Lack of Knowledge

In addition to being ready or prepared to respond, which means knowing what to do once the situation has been recognised, the management of unexpected events and disasters may also suffer from a shortage of information about what is going on. This refers to the details of the situation, both the actual status and the way in which it is likely to develop. Even if responses are available, they should not be deployed without knowledge of the situation. Such knowledge can be critical in relation to the timing of responses (when to start and when to end) or the magnitude or focus of responses (how much effort to deploy and where).

Having sufficient knowledge about the situation clearly depends on the ability to monitor what is going on, both in the outside world—the objective situation—and in the organisation. Monitoring is itself an activity that may require resources, and will therefore to some extent compete with the need of resources for other purposes. Monitoring can also be time critical, for instance to ensure the synchronisation of responses with how the events develop.

Without sufficient knowledge about what is going on, all the time in the world will not make much difference. To take an extreme example, if you put an untrained person into a control room of a refinery, he or she will have no real chance of controlling the process. To take a less extreme example, if you put people in charge of a job without giving them proper training and instructions, then they are likely to lose control of the situation and to respond in ways that may have serious adverse outcomes [3].

3.3 Lack of Time

The loss of control of a situation very often happens because of a lack of time. Every dynamic process has certain demand characteristics because the process continues to develop and possibly changes state, even if the organisation does nothing. The concrete consequence is that there is limited time to understand what is going on and to plan, prepare, and execute actions. It is necessary to be ready to respond and to know what the situation is, but that is not in itself

sufficient. Knowing what to do is no good if there is no time to do it. The control over unexpected events is closely related to the amount of time that is available to the organisation in two different, but complementary ways. Firstly, the realism of the expectations about what is likely to happen depends, among other things, on the available time. If the expectations or predictions are inaccurate, then additional unexpected events or developments are more likely to follow. Secondly, unexpected events inevitably require additional time, since they fall outside or interrupt the planned, ongoing activities. The organisation needs time to take in the new information, to decide what to do about it, and to update the current understanding.

The only practical ways in which to increase available time are to improve the efficiency of responding and monitoring. But in neither case should the temporal improvements (speeding up) be achieved by sacrificing thoroughness over efficiency. While doing so may provide a temporary respite, it will in the long run exacerbate the problems, because a lack of thoroughness in the present will be detrimental to efficiency in the future [4]. Thus being less precise in monitoring—a condition that may result from input information overload [7, 12]—or being less thorough in actions or responses will make the outcomes less predictable, hence only contribute to the unexpectedness of future events.

3.4 Lack of Resources

Finally, control may be lost if the necessary resources—other than time—are lacking. A lack of resources, whether it be equipment or supplies, can be the consequence of an acute condition, such as a loss of power or pressure, or of a systemic failure, for instance the result of latent conditions or a mistake made at the blunt end. One example was the spread of the influenza in Sweden in the winter of 2001. In early January it was realised the influenza epidemic was coming but that all the vaccine had already been used, hence that a number of people would be left exposed. An unfortunately more frequent example is wildfires. Here a fire can be regarded as a dynamic process, which is reasonably predictable (although random events such as changing winds may play an important role). In the case of a wildfire there are organisations ready to intervene and there are few problems in knowing what is going on or what should be done. There may sometimes be a lack of time, but the limiting factor is often that resources needed to extinguish the fire become depleted. The result may be that a wildfire goes out of control, such as the bushfire near Sydney in December, 2002.

Just as for the lack of readiness, a lack of resources can be the result of inadequate learning and inadequate anticipation. The experience from similar situations in the past, both those that failed and those that succeeded, is essential to plan ahead and to ensure that the proper resources are available. There is, however, a conflict that most organisations have experienced at one time or another. On the one hand the concern for safety, or even a concern for being able to operate,

is an argument for having adequate resources. On the other hand, resources that are unused quickly come to be seen as a cost, hence as something that should be avoided. This is easily illustrated by Hansung Airlines, a low cost carrier in South Korea. When it began operations in August 2005, it only had stocked spare parts locally for highly likely situations, assuming that they could be flown in from Singapore should the need arise. When one of their three aircraft in October 2005 suffered a blowout of both left rear tires, it turned out to be impossible to transport the spares due to safety reasons. Because of that flights were cancelled for three days, with disastrous economical consequences for the company.

Even if such economic concerns are set aside, unrealistic (optimistic) anticipation may lead to serious problems. This happens, for instance, when the anticipation relies on assumptions that are widely shared but rarely questioned. In relation to nuclear power plants, for instance, a Level 1 Probabilistic Risk Assessment (PRA) assumes that the disturbance (e.g., loss of external power) will last for no more than 24 h. Resources are therefore designed to be sufficient for 24 h only. The contentious issue here is that imagination has become standardised and embedded in a methodology that is applied on the tacit assumption that it is adequate. But if anticipation is mindless rather than mindful [15] it erodes the organisation's ability to remain in control.

4 All in All

This chapter has looked at safety management and disaster management as the ability to deal with events that are unexpected, either in terms of *when* they happen or in terms of *what* they are. The greatest challenges are presented by what Westrum [17] called irregular events. Since these events occur outside the organisation's everyday experience, it may not always know how to respond nor have the proper resources available. In such cases the organisation's resilience plays a crucial role.

Resilience engineering has developed a consistent approach to analyse and understand resilient performance. The practical experiences so far have shown that it makes sense to describe resilient performance as based on four abilities: the ability to respond, the ability to monitor, the ability to learn, and the ability to anticipate. The four abilities should, however, not be thought of or described as independent factors. Each depends on one or more of the others and they must therefore be analysed and managed together in order to understand how they contribute to the organisation's overall ability to remain in control of a situation. This is summarised in Table 2, where the 'X' in a cell marks how an ability can counteract a loss of control.

The conclusion is that resilience engineering concepts can be used to understand how the unexpected can be managed (or controlled). One part of that is that the organisation is able to respond to and monitor the ongoing in an effective and flexible manner. Another is that the organisation is able to learn and

Table 2 RMLA and maintaining or sustaining control

	Lack of readiness/ competence	Lack of knowledge	Lack of time	Lack of resources
Respond			**X**	
Monitor		**X**	**X**	
Learn	**X**			**X**
Anticipate	**X**			**X**

anticipate—and also to monitor itself in both the short and the long term (proprioceptive mindfulness). Finally, to manage the unexpected we must accept that it can happen—not by proving it through probability calculations, but by acknowledging that our ability to produce socio-technical systems for some time has exceeded our ability to understand them.

References

1. Adamski AJ, Westrum R (2003) Requisite imagination: the fine art of anticipating what might go wrong. In: Hollnagel E (ed) Handbook of cognitive task design. Lawrence Erlbaum Associates, Mahwah, pp 193–220
2. Amalberti R (2006) Optimum system safety and optimum system resilience: Agonist or antagonists concepts? In: Hollnagel E, Woods D, Leveson N (eds) Resilience engineering: concepts and precepts. Ashgate, Aldershot
3. Furuta K et al (2000) Human factor analysis of JCO criticality accident. Cogn Technol Work 2(4):182–203
4. Hollnagel E (2009) The Etto principle: efficiency-thoroughness trade-off (why things that go right sometimes go wrong). Ashgate, Farnham
5. Hollnagel E (2011). Prologue: the scope of resilience engineering. In E Hollnagel, J Pariès, DD Woods, J Wreathall (Eds) Resilience engineering in practice: a guidebook (pp xxix–xxxiv). Ashgate, Farnham
6. Hollnagel E (2014) Safety-I and Safety-II: the past and future of safety management. Ashgate, Farnham
7. Hollnagel E, Bye A, Hoffmann, M (2000) Coping with complexity: strategies for information input overload. 2nd conference on cognitive systems engineering in process control (CSEPC 2000). Taejon, South Korea, Nov 22–24
8. Hopkins A (2009) Thinking about process safety indicators. Saf Sci 47:460–465
9. Kletz TA (2001) Learning from accidents. Routledge
10. Lagadec P (1993) Preventing chaos in a crisis strategies for prevention, control, and damage limitation. McGraw Hill Europe, Berkshire
11. Lanir Z (1983) Fundamental surprises. Center for Strategic Studies, University of Tel Aviv, Ramat Aviv
12. Miller JG (1960) Information input overload and psychopathology. Am J Psychiatry 116:695–704
13. National institute for occupational safety and health (2010) Prevention through design: plan for the national initiative (DHHS Publication No. 2011–121). Washington, DC
14. Schützenberger MP (1972) A tentative classification of goal-seeking behaviours. In: Emery FE (ed) Systems thinking. Penguin Books, Harmondsworth
15. Weick KE, Sutcliffe KM, Obstfeld D (1999) Organising for reliability: processes of collective mindfulness. Res Organ Behav 21:81–123

16. Westrum R (1993) Cultures with requisite imagination. In: Wise JA, Hopkin VD, Stager P (eds) Verification ad validation of complex systems: human factors issues. Springer, Berlin, pp 401–416
17. Westrum R (2006) A typology of resilience situations. In: E Hollnagel, DD Woods and N Leveson (eds) Resilience engineering: concepts and precepts. Ashgate, Aldershot, pp 55–65)
18. Wiener N (1954) The human use of human beings. Houghton Mifflin Co, Boston
19. Woodruff JM (2005) Consequence and likelihood in risk estimation: a matter of balance in UK health and safety risk assessment practice. Saf Sci 43:343–353

http://www.springer.com/978-3-319-08818-1

Disaster Management: Enabling Resilience
Masys, A.J. (Ed.)
2015, XVI, 338 p. 45 illus., 33 illus. in color., Hardcover
ISBN: 978-3-319-08818-1