Some myths about industrial safety

Denis Besnard, Erik Hollnagel

▶ **To cite this version:**

Denis Besnard, Erik Hollnagel. Some myths about industrial safety. 2012. hal-00724098v1

HAL Id: hal-00724098

https://minesparis-psl.hal.science/hal-00724098v1

Submitted on 17 Aug 2012 (v1), last revised 10 Dec 2012 (v2)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Besnard, D. & Hollnagel, E. (2012). Some myths about industrial safety. CRC technical Report.

Some myths about industrial safety

Denis Besnard & Erik Hollnagel

Centre for research on Risks and Crises
Mines ParisTech
Rue Claude Daunesse, BP 207
06904 Sophia Antipoli, France

Abstract. There are many definitions of safety, but most of them are variations on the theme that safety can be measured by the number of adverse outcomes. This vision has consequences for how industry thinks safety can be achieved. This paper looks at six safety-related assumptions, or safety myths, which impact industry practices. We argue that these practices are littered with fragile beliefs, which in many cases make the safety management flawed and ineffectual. The open acknowledgement of these myths is a necessary first step to genuinely improve industrial safety.

Keywords. Human error and procedures, risk perception, root cause, accident investigation, safety first

1 On myths and safety

In the best of all possible worlds, safety is managed by highly trained and rational specialists using carefully chosen indicators and methods. In reality, safety management is usually a collection of best practices based on a number of assumptions that are taken for granted. Examples include the traditional dictum of '*safety first',* the belief that increasing protection will increase safety, or the notion that most accidents are caused by human error. These assumptions are common to many (if not all) industrial sectors and determine both individual attitudes and corporate policies. Since these assumptions express common beliefs rather than facts, they are not verifiable in a logical sense and can therefore be considered as myths. This paper will consider some of the major safety myths and for each try to determine how much is fact and how much is fiction.

1.1 Myths do matter

For the scope of this paper, an assumption is something that is taken for granted rather than verified. Assumptions, whether as 'hunches,' 'guesses,' or 'hypotheses,' are an important and essential part of human activity since we rarely have sufficient time to make sure that what we assume is actually true (Hollnagel, 2009a). While assumptions are usually considered in relation to what individuals think and do, assumptions may also be shared among social or professional groups. This is demonstrated by the classical definition of safety culture as "that assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance," (INSAG, 1986). Schein's (1992) definition of organisational culture is

also relevant here : it is “a pattern of shared basic assumptions that the group learned as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems.”

The step from an assumption to a myth is not very large. Whereas an assumption is ‘*a statement that is assumed to be true and from which a conclusion can be drawn*,’ a myth is *‘an idea or story that many people believe, but which is not true.’* This definition emphasises both the fictional or non-verifiable aspect of myths and their social nature. Myths are rooted in our culture, they influence our beliefs and often determine what we decide and do. Being social objects, they are widely shared and easily attract a community around them.

In the industrial world everyone, from the sharp end to the blunt end, seems to share a number of safety myths. Also, as argued by Bohnenblust & Slovic (1998), risks are a social object that is submitted to many biases. The consequences are that safety managers may be unaware of the potential misalignment between beliefs and practices, and that some safety targets may be out of reach. Since safety myths have a direct impact on safety management and safety performance, it is worth considering them more closely. Our objectives in doing so are to encourage reflection among the stakeholders of industrial safety, and to propose some alternatives from which new safety practices may be derived.

1.2 Safety

Safety comes from the French *sauf*, which interestingly means both ‘without’ and ‘unharmed’. The origin of the word is the Latin *salvus,* meaning uninjured, healthy, and safe. The definition of safety usually refers to the absence of unwanted outcomes, either seriously as ‘the freedom from unacceptable risk’, or tongue-in-cheek as ‘a dynamic non-event’ (Weick, 2001, p. 335). For the discussion in this paper, we will adopt the following definition: *Safety is the system property that is necessary and sufficient to ensure that the number of events that could be harmful to workers, the public or the environment is acceptably low*. This definition does not cover all the relevant dimensions such as management systems, indicators, norms, etc. Nor do we intend to discuss the relations among concepts such as hazards, risks, accidents, and so on. Instead, our definition of safety emphasises the relative nature of the concept: safe systems produce *acceptably* low numbers of unwanted events. This definition is a starting point for looking at safety assumptions as well as some aspect of the industrial safety culture. In doing so, we will rely on a human factors perspective, even though that is not yet fully integrated in industrial safety practices.

This paper will review a number of myths that are part of the practice of safety. For several of these myths, entire books could be (and in some case already have been) written. It is therefore impossible to provide an extensive discussion in a short paper. We will instead look at a number of representative myths to see how much is fiction and how much is fact. For each myth we will provide a short description and attempt to analyse the underlying assumptions. We do so by providing examples and by referring to evidence that motivates reconsidering the assumption. We end with a short alternative view. The order in which the myths are considered is (almost) arbitrary.

2 Human error

2.1 The myth

Human error is the largest single cause of accidents and incidents.

2.2 Description and criticism

The web announcement for the Intersec Trade Fair and Conference (held in Dubai, January 2010), included the following topic under the heading *Latest News*: 'Human error is involved in over 90% of all accidents and injuries in a workplace' (Intersec, 2009). The details of the announcement contain the following statements[1]:

Human error and unsafe behaviour accounts for almost 90% of all accidents, including those caused by inexperienced and unskilled workers. […] The most common cause of accidents or industrial accidents is often attributed to human error such as operational error, judgemental error, or job-related error, all of which are caused by human characteristics. Most of these errors are said to be associated with psychological factors affecting human behaviour. […] The disasters caused by human errors are serious, because the automation in the construction is difficult and a lot of workers support the construction work. The larger the number of workers who work on the site is, the higher the possibility that human errors cause accidents.

Numerous books and papers have been written about human error. An increasing number of them openly question the simple-minded use of the term (e.g. Dekker, 2005; Hollnagel & Amalberti, 2001; Woods et al., 1994). Yet as the above announcement shows, the myth of human error as the cause of most accidents prevails. Human error is also a fundamental part of many accident investigation methods and, of course, the very foundation of human reliability assessment. The tradition is old; one of the early candidates for a theory to explain industrial accidents was a single-factor model of accident proneness (Greenwood & Woods, 1919). In methods such as root cause analysis, for instance, the 'human error' level often marks the maximum depth of analysis, in the sense that a human error is accepted as the coveted root cause. In human reliability assessment the focus is still the Human Error Probability (HEP), despite numerous criticisms (e.g. Dougherty, 1990; Hollnagel, 2000). The concept of a human error became part of the safety lore when Heinrich (1931, p. 43) noted that as improved equipment and methods were introduced, "accidents from purely mechanical or physical causes decreased, and man failure became the predominating cause of injury". This assumption became the second of the five dominoes in the famous domino model, described as 'Fault of person – proximate reason for committing unsafe act, or for existence of mechanical or physical hazard' (Heinrich, 1934, p. 1). Observers of the human mind, philosophers and psychologists alike, have studied human error at least since the days of David Hume (Cf. Hollnagel, 2000), and have generally treated human error as an individual characteristic or a personality trait. A good example of that is the zero-risk hypothesis of driving (Summala, 1985; 1988), which proposes that drivers aim to keep their subjectively perceived risk at zero-level.

Our daily lives are littered with instances of the expression 'human error'. They can be found in the news, in accident reports, in public statements, etc. Recent examples include a piece of news relayed by the BBC (2009) about a software problem with Google's search services where a 'human error' by a Google's member of staff caused all search results to be unduly

1 Note that the last claim alludes to another myth, namely that safety can be enhanced by replacing humans by automation.

flagged to users as malevolent. Also, the French radio France Info (Colombain, 2009) announced that a (programming) 'human error' in a piece of software, handling operations on bank accounts from the BNP bank, caused almost 600,000 debits or credits to be performed two or three times.

The futility of using human error as a cause of accidents can be demonstrated through the following argument. If we consider a safe – or even an ultra-safe – system, then there will be at least 9.999 cases of normal performance for every failure. This makes accidents very rare. If the so-called human error is the cause the event that goes wrong, then what is then the cause of all the other events that go right? In our opinion, the only possible answer is humans. Humans try to have their actions produce some intended effect. However, they behave in the same manner regardless of whether the outcomes of their actions will actually reveal positive or negative. It follows that 'human error' should not be used to explain adverse outcomes. Instead we should try to understand why the same behaviour usually makes things go right and occasionally makes things go wrong.

2.3 A possible revision of the myth

'Human error' is an artefact of a traditional engineering view, which treats humans as if they were (fallible) machines and overlooks the role played by working conditions in shaping performance.

The expression 'human error' contains assumptions that are counter-productive for the effective understanding of things that have gone wrong. To start with, it is a judgement, a loaded term that implies some form of wrongdoing and asks for a culprit to be found. It is a judgement made after an action has been performed, and is therefore heavily influenced by the hindsight bias (Woods et al., 1994). It is also in practice limited to people at the sharp end, i.e., the operators who are direct involved with the process. People, however, work under constraints that are imposed by managers and higher strata of organisations and this must be considered in trying to understand failures. Finally, 'human error' pays no attention to the context of work, thereby limiting the cause of mishaps to people's actions without including the working conditions.

3 Procedure Compliance

3.1 The myth

Systems will be safe if people comply with the procedures they have been given.

3.2 Description and criticism

Generally speaking, procedures are essential references for how to carry out a given task, for instance as a memory aid, or as guides for decisions in situations where people have little or no experience. Procedures vary in nature, size and complexity and may range from a 6-line cooking recipe to entire bookshelves of ring binders in control rooms of nuclear power plants. The safety myth is that safety can be ensured by following the procedures and conversely that safety is jeopardised if they are not followed.

This conservative position implies that humans are a source of uncontrollable variability that contributes to the occurrence of unsafe events. The assumption is that following the procedure will not only get the job done, but will also get it done well, i.e., safely. Similarly, it is assumed that departing from the procedures constitutes a risk. In relation to safety, the idea that safe and effective performance requires procedure compliance reflects the principles of Scientific Management (Taylor, 1911) and also the assumption that people can be considered as 'machines' – possibly complex, but machines nonetheless.

Looking at procedures from a human factors standpoint tells a somewhat different story. Procedure compliance will not always guarantee safety. One reason is that procedures are inherently underspecified both in scope and in depth: a procedure cannot cover *all* possible configurations a worker might face when performing a task, nor can it completely describe *what* a worker has to do, *how*, and *when*. Numerous studies tell us that humans overcome these limitations by interpreting the procedure vis-a-vis the situation and by adjusting it if necessary. Humans also rely on their experience to 'tune' procedures when actions are described in vague terms such as 'enough,' 'quickly,' 'slowly,' etc.

An example of operators reacting to an exception by adapting the procedure is the near-loss and recovery of the Snorre A platform (Wackers, 2006; Cf. Figure 1).

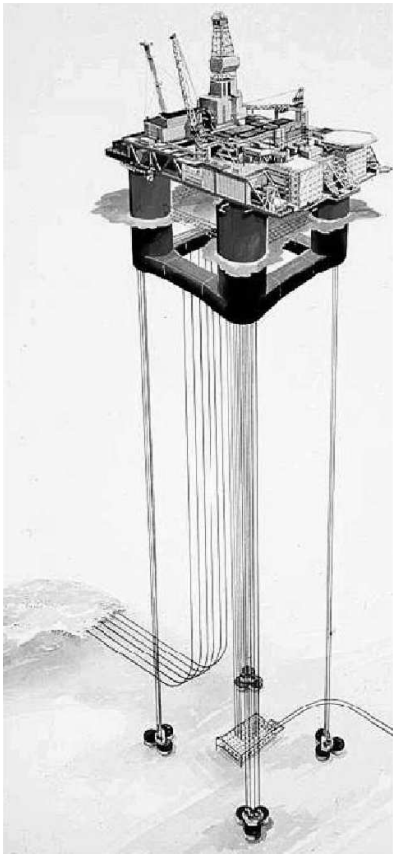

Figure 1: Graphical representation of the Snorre A platform showing the wells on the seabed between the four tension legs (from Wackers, 2006)

On November 28, 2004, one of the gas wells attached to the platform started to leak from the seabed. The leak was serious enough for a large gas cloud to build up around the platform, putting the entire installation under a high risk of explosion. Under such circumstances, safety procedures required that the platform be evacuated. However, applying this procedure meant that the leak would be left unplugged, and that the unattended platform would be exposed to potential destruction. Should this happen, the platform would sink and crash onto

the seabed, obliterating the wells themselves and for a long time make the plugging of the leak virtually impossible. With such a catastrophic scenario in mind, and taking into account the long-term consequences, the platform manager decided to remain aboard the platform with a small team in order to plug the well with concrete. They succeeded, stopped the leak, and were able to put the platform back into service; it still is today. This case is a clear demonstration of a *'safe violation'* (Besnard & Greathead, 2003) whereby mandatory compliance to a safety procedure is deliberately disregarded in order to respond proactively to the potential evolution of a catastrophic situation (Reason, 2009).

3.3 A possible revision of the myth

Actual working situations usually differ from what the procedures assume and strict compliance may be detrimental to both safety and efficiency. Procedures should be used intelligently.

Safe operations cannot be ensured by rigid and blind compliance but require that operators can interpret and adapt the procedures (Besnard, 2006). Humans constantly compensate for the discrepancies between procedures and reality, and fill in the gaps between the procedures and actual operational conditions. This is the only way industrial operations can be conducted, given that it is impossible to anticipate all the possible configurations of a work situation and prescribe each and every step of an activity. It is human flexibility that compensates for brittleness of procedures, turning the latter into a useful tool for the control of systems, and contributing to safety by doing so. Strict procedure compliance may even have detrimental consequences since it will limit the beneficial effects of human adaptation in response to underspecification of the work situation. Just think of situations where people 'work to rule.'

4 Increasing protection increases safety

4.1 The myth

Safety can be improved by barriers and protection; more layers of protection results in higher safety.

4.2 Description and criticism

At first glance it seems reasonable to expect that safety improves the more protection there is and the better designed it is. This is the philosophy behind the concept of defence-in-depth (INSAG, 1996). It is also the philosophy behind safety in many systems such as motor vehicles, where multiple active and passive safety systems (ABS, ESP, crumble zones, safety belts, airbags, etc.) protect drivers from physical injury.

However, the relation between protection and risk exposure is not simple. In the case of individual protective equipment (hard hats, goggles, etc.), one factor is the expected utility of being protected versus being unprotected. When the consequences of being unprotected are immediate and tangible, protection will be used. For instance, welders seldom have to be reminded to use their welding shield. This is simply because not using a shield leads to accute pain in the eyeballs within a matter of hours due to the intense UV light emission during welding. Conversely, when the consequences of being unprotected are remote or diffuse, or when the risks are seen as insignificant, then the protection is likely to be disregarded. An example is the safety belt in cars. It is obviously possible, although risky, to drive for an entire lifetime without using the safety belt and without having an accident. As a matter of fact, this was the norm until a few decades ago.

The message here is that the perceived consequence of risk exposure are strong determinants of human safety-related behaviour. The longer the delay between risk exposure and consequences, the less likely it is that protection will be used. The psychological explanation is that the potential negative outcomes are less salient (or available; Tversky & Kahneman, 1974). One might think that potential losses due to a lack of protection would be sufficient motivation. In other words, if life is at stake, then protection will be used even if the feedback is delayed. Unfortunately, this argument does not hold. In the case of the safety belt, life is indeed at stakes. However, only enforcement led drivers to wear it.

There are two main reasons why more protection is not necessarily better. One is psychological and has to do with perceived risk exposure. According to the hypothesis of risk homeostasis (Wilde, 1994), people seem to be comfortable with a certain level of risk, depending on experience, life-style, personality, etc. If technology is introduced to reduce risks, people may it to achieve different aims, for instance to increase performance efficiency while keeping the perceived level of risk constant. The classical example is the introduction of ABS braking system in the automotive industry. A large-scale study conducted by Aschenbrenner and Biehl (1994; quoted by Wilde, 1994) showed that taxi drivers whose cars were equipped with ABS tended to drive more aggressively in curves. The other interesting result was that the drivers of ABS-equipped vehicles had an accident rate that was slightly *higher* than that of the other taxi drivers. This clearly demonstrates the counter-intuitive nature of the human response to increased protection. Another example is what happened when bendy Finnish country roads were equipped with reflector posts: people drove faster and closer to the edge of the road, thereby vastly increasing the number of accidents at night (Hamer, 1991).

The second reason why more protection is not necessarily better is of a technical nature. Adding protection invariably increases the complexity of the system, regardless of how that is measured (more components, more couplings, etc.) The added components or functions can not only fail, but may also significantly increasing the number of combinations that can lead to unwanted and undesired outcomes; the latter typically being exponential.

4.3 A possible revision of the myth

Technology is not value neutral. Additional protection may change people's behaviour so that the intended improvements fail to obtain.

Expected increases in safety from additional barriers and protection can be defeated by psychological reactions. The introduction of new and better (safer) technology should not be treated as the simple replacement of one function by another. Any change will affect the established equilibrium, and people will usually respond by changing their behaviour. The risk homeostasis hypothesis described above is one illustration of that. A more general expression of this principle is found in the *Law of stretched systems,* originally proposed by Lawrence Hirschhorn. The law states that:

"Under resource pressure, the benefits of change are taken in increased productivity, pushing the system back to the edge of the performance envelope" (Woods & Cook, 2002, p. 141).

This means that every system is stretched to operate at its full capacity and that any (technological) improvement will be exploited to achieve a new intensity and tempo of activity. Thus, rather than just enabling humans to manage existing risks better, additional barriers and protection may lead people to take greater risks. This does of course not mean that less protection is the way to improve safety. It only means that one should carefully

consider both the intended and the unintended effects of implementing protection in socio-technical systems.

5 Accidents have root causes, and root causes can be found

5.1 The myth

Accident analysis can identify the root cause (the 'truth') of why the accident happened.

5.2 Description and criticism

Root cause analysis is a common method in many industries. It is used to find the various factors that led to a specific (adverse) outcome such as an accident. The basic steps of root cause analysis are: determine *what* happened, determine *why* it happened (by going stepwise backwards from an effect to the causes) and finally, find ways to *reduce* the possibility that it will happen again. Root cause analysis assumes that the parts of a system are causally related so that effects propagate in an orderly fashion. This assumption makes it justified to follow the cause-effect links in reverse order to discover where the problem started. In this way, one maps out the various steps in a tree-like diagram of causes (Cf. Figure 2).

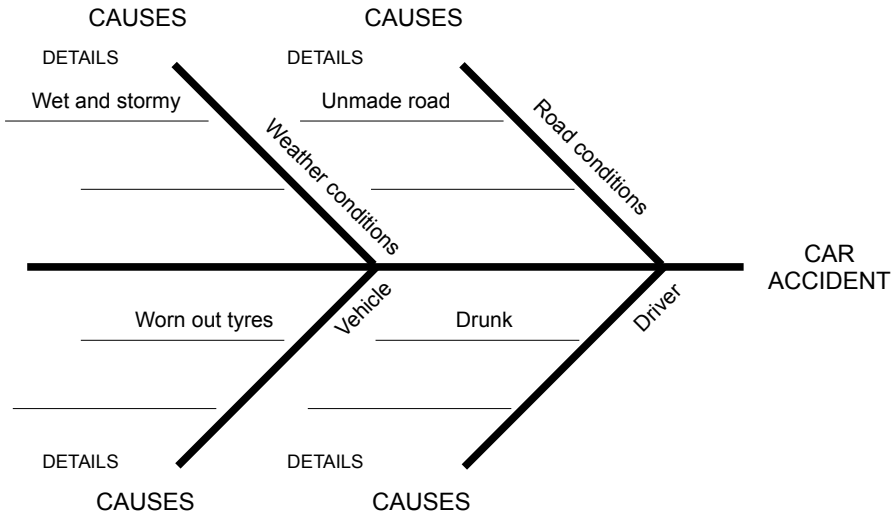

Figure 2: A 'fish-bone' model of a car accident and causes

Root cause analysis is attractive because it is simple, but the validity of the method depends on three critical assumptions. First, it is assumed that events that happen in the future will be a repetition of events that happened in the past (Cf. the procedure myth in Section 3). Second, it is assumed that outcomes of specific events are bimodal; i.e., outcomes are either correct or incorrect. Third, it is assumed that the cause-effect relations can be exhaustively described.

Using a bimodal causal model may be reasonable for purely technical systems where components are designed to provide a constant performance within well-defined limits until they fail for some reason. However, the bimodal view is not appropriate for the performance of complex socio-technical systems. Neither individual nor collective human performance is bimodal: it normally varies considerably but rarely fails completely. And even when performance for some reason fails, the change is usually temporary. Unlike technical

components, humans can individually or collectively recover from failures and resume normal operation (a fundamental characteristic of resilience). Indeed, the very flexibility and adaptability of human performance is a unique contribution to safety (Reason, 2009). Yet this flexibility is disregarded when a root cause analysis points to a human as the origin of an unwanted event. The analysis only sees the failure (Cf. human error in Section 2) and fails to recognise that things go right and wrong for the same reasons. The possible elimination of the human activity that was deemed the cause of the outcome will unfortunately also prevent the far more frequent and far more likely positive contribution.

The preference for clear and simple methods has both psychological and pragmatic explanations. The psychological explanation is what the philosopher Friedrich Wilhelm Nietzsche (2007; org. 1895, p. 33) called the "error of imaginary causes," namely the psychological fact that:

"To trace something unfamiliar back to something familiar is at once a relief, a comfort and a satisfaction, while it also produces a feeling of power. The unfamiliar involves danger, anxiety and care – the fundamental instinct is to get rid of these painful circumstances. First principle – any explanation is better than none at all."

The pragmatic explanation is that a simple methods will output results faster than a complicated method, and that the results will often be familiar ones. The increase in efficiency is, however, offset by a reduction in thoroughness (Hollnagel, 2009a).

5.3 A possible revision of the myth

Unwanted outcomes in socio-technical systems do not necessarily have clear and identifiable causes.

This means that there are many cases where root cause analysis cannot – and should not – be used. Fortunately, there are several alternatives that are more appropriate. One is the well-established MTO approach that considers huMan, Technical and Organisational factors either alone or in combination. This approach has been used by both nuclear and off-shore industries for more almost twenty years. Another is the Swiss cheese model (Reason, 1990), which offers a high-level view of how latent conditions can combine with active failures and thereby lead to unexpected and unwanted outcomes. More recently, the Functional Resonance Analysis Method (FRAM) replaced the cause-effect relation by the concept of functional resonance (Hollnagel, 2004; Woltjer & Hollnagel, 2007). This approach provides a way to describe unexpected events as emerging from the low-amplitude variability of normal performance.

6 Accident investigation is a rational process

6.1 The myth

Accident investigation is the logical and rational identification of causes based on facts.

6.2 Description and criticism

The purpose of accident investigation is to discover the causes of unexpected and adverse outcomes. Accident investigations within large industries are taken extremely seriously and are often in the hands of special boards or commissions. Accident investigation requires extensive knowledge of the domain as well as competence in the use of specialised methods. Commercial aviation has been setting a good example for decades, and this has undoubtedly

contributed to the excellent safety record of this industry in western countries (Boeing, 2009).

It is a regrettable fact of modern life that the number of serious unwanted outcomes is so large that it is impossible to investigate them all. Even the use of simple methods, such as root cause analysis, is insufficient to cope with this challenge. Furthermore, when unwanted events are investigated it is often necessary that the outcome is ready by a certain date, for judicial reasons, for communication purposes, or because of a lack of resources. Because of that, the depth or extent of analysis, the methods deployed, or the choice of data that get scrutinised are not determined only by the characteristics of the case at hand (its complexity, severity, potential for learning, etc.). Instead, resources and demands dictate what will be done and how. The management of the investigation then becomes a trade-off between what can be done and what should be done: a trade-off between efficiency and thoroughness (Hollnagel, 2009a).

Another obstacle for the rationality myth is that accident investigations in practice always imply some assumptions about how accidents happen and what one should do to prevent them. Benner (1985), for instance, evaluated the merits of 17 investigation methodologies from the United States, and found considerable differences in their effectiveness. Accident investigation guidelines can be seen as embodying a set of assumptions about how accidents happen and what the important factors are. The guidelines reflect the safety aspects that the organisation finds important; they imply how accidents are assumed to occur and how they can best be prevented in the future. They also define an implicit (and sometimes explicit) norm for what a satisfactory investigation is.

Yet another factor may challenge rationality even more: the need to establish responsibilities. This can be an extremely strong bias in investigations, to the extent that the causes of the unwanted event become a secondary issue. This approach is paramount within judicial enquiries. A recent example is the crash of a Rafale air fighter in December 2007 in France, causing the death of the pilot. Shortly after the accident, a representative of the French Air Force declared on a national radio channel that all responsibilities would be established by the investigation. This mindset was clearly not oriented towards causes but aimed at finding someone to blame. This can be a major obstacle to safety because it confuses responsibility and cause. At best, it makes it easier to find who to blame next time a similar event occurs. But it also means that the investigation is quite remote from any common form of rationality. As Woods et al. (1994, p. xvii) puts it, "*attributing error to the actions of some person, team, or organisation is fundamentally a social and psychological process and not an objective, technical one.*"

6.3 A possible revision of the myth

Accident investigation is a social process, where causes are constructed rather than found.

An accident investigation must always be systematic, hence follow a method or a procedure. There are many different methods available (Benner, 1985; Sklet, 2002), both between and within domains, and these may differ with respect to how well formulated and how well founded they are. The method will direct the investigation to look at certain things and not at others. Indeed, it is simply not possible to begin an investigation with a completely open mind, just as it is not possible passively to 'see' what is there. Accident investigations can therefore be characterised as conforming to the What-You-Look-For-Is-What-You-Find (WYLFIWYF) principle (Lundberg et al., 2009).

One important consequence of this view on the investigation process is the need to pursue 'second stories' (Woods & Cook, 2002). 'First stories' are "are overly simplified accounts of the apparent 'cause' of the undesired outcome" (Ibid, p. 137). In order to avoid the bias of

'first stories' it is necessary to develop the deeper 'second stories,' by looking out for the many simplifying assumptions that are part of the common, but not so rational, accident investigations.

7 Safety first

7.1 The myth

Safety always has the highest priority and will never be compromised.

7.2 Description and criticism

This is by far the most commonly heard myth in the realm of safety management. Here, the assumption is that safety is an absolute priority in the sense that it cannot be compromised. An instance of this myth appeared in a statement by the Chief Executive Officer of Air France, in the aftermath of the AF 447 accident (Amedeo & Ducros, 2009):

"The company is safe. It was safe yesterday, it is safe now but it will be even safer tomorrow. Because everything will be scrutinized: the mechanical parts, human factors, the weather. Every possible accident scenario will be analysed. Everything will be looked at and we will improve the elements that may be related to the accident as well as others that are not. There is no contradiction between safety and economy. When safety improves, it improves the image of the company and therefore also improves its economic performance. There has never been any trade-off between these two areas. For example, it is clearly written that pilots should fly around thunderstorms. There is no question of saving on fuel. Pilots are free to choose their route."

Statements like these are often used because they are concise and suited for communication purposes. They basically express a value that is both clear and noble. They also provide a basis for daily practice, although other considerations play a role as well. If one looks at the safety management of an industry such as commercial aviation in western countries, there are clear examples of 'safety first'. One is scheduled maintenance for aircraft bodies. At regular intervals, every wide-body commercial aircraft goes through total dismantling, down to the very last piece of wire, and is then rebuilt with the necessary upgrades or replacement parts. It is hard to be more dedicated to safety than that and, to our knowledge, aviation is the only industry to have adopted such a radical practice.

There may, however, sometimes be a discrepancy between policy statements and reality. One example is provided by an assessment of 'safety behaviour and culture' at the BP Texas City refinery that was carried out between 8 and 30 November 2004. In 2004, BP Texas City had the lowest injury rate in its history, nearly one-third the average of the oil refinery sector. In the following year, on March 23, a major explosion occurred in an isomerisation unit at the site, killing 15 workers and injuring more than 170 others. This was the worst US industrial accident in over a decade. The 2004 study interviewed 112 individuals to solicit their views on a number of issues (Telos, 2005). In the context of this discussion, the most interesting finding was when employees were asked to rank their perception of the priorities at the Texas City site, using a set of given options. The first three choices were *Making money*, *Cost/budget* and *Production*, respectively. *Major Incident* and *Security* only came in fifth and seventh position.

Safety has financial implications that cannot be ignored and it is understandable that costs do have an influence on the choice and feasibility of safety measures. It is all the more

understandable because safety costs are immediate and tangible whereas the benefits of safety investments usually are potential and distant in time. A further complication is that safety performance is often measured by the relative reduction in the number of cases where things go wrong rather than as an increase in the number of cases where things go right. This means that there is less and less to 'measure' as safety improves. But when the absence of negative events is taken as a criterion for success, a consequence is often that the same criterion is used to reduce investment in safety management. The lack of information is (mis)interpreted to mean that the process is under control, when in actual fact the opposite is the case, at least from a control engineering perspective. Ironically, the costs incurred by a major catastrophe are often higher than the cost of the actions that could have prevented it.

7.3 A possible revision of the myth

Safety will be as high as affordable – from a financial and ethical perspective.

An illustration that 'safety first' is a relative rather than an absolute statement is provided by Negroni (2009):

"In October, the agency, the Federal Aviation Administration, issued an operations bulletin for 'ultra-long-range flights' that doubled the amount of time that pilots and flight attendants must remain at their overseas destination. The change to 48 hours from 24 was intended to ensure that flight crews got two full periods of sleep before making the return flight. But seven airlines have asked the U.S. Court of Appeals for the Federal Circuit in Washington to set aside the new requirements, arguing that they would impose 'substantial burdens and costs.'"

In other words, safety comes first if the organisation can afford it. If not, safety is traded off against economy. Safety budgets, like any other, are limited and constrain decisions. It is not realistic to expect that all possible safety measure, however good they may be, can be implemented without prioritisation, or without considering feasibility and consequences.

8 Discussion

In this paper, we have looked at six common safety assumptions and compared them to actual practices, policies, and scientific knowledge. The assumptions were seen as myths for the following reasons:

- They are shared by large groups of people inside and outside of companies, including managers, politicians, and sometimes the public, and can be found in various industrial sectors and social contexts.
- They express a set of attitudes and values that determine decisions and actions related to safety.
- They are not usually noticed or questioned.
- They resist change.

Safety involves all layers of organisations, from operators to CEOs, as well as society, in the form of investigation boards, regulators, and the courts. Since the myths permeate all these layers, the practice of safety is potentially flawed everywhere. Taken together these myths, and possible others as well, are part of the common safety culture, i.e., the pattern of shared assumptions that affect how we perceive, think, and respond to adverse outcomes. Because they are myths and therefore rarely questioned, it will take more than just facts and reason to undo them and alleviate their effects. A better approach may be to consider the object of

safety myths, namely safety itself. By changing how safety is defined it may perhaps be possible to change both the myths and the role they play.

First, we would like to revise the working definition of safety that we proposed at the start of this paper. Instead of defining safety as a system property, we argue that safety should be seen as a process. Safety is something that a company *does*, rather than something that it *has*. Safety is dynamic, it is under constant negotiation, and the safety process varies continuously in response to and anticipation of changes in operating conditions.

Second, we would like to emphasise that the goal of safety should be what goes right rather than what goes wrong. Safety has traditionally focused on what goes wrong and rarely noticed what goes right. We are preoccupied with failures because it is assumed that we know how a system should work in minute detail. In reality, however, we may know how we would *like* the system to work, but we do not always know how it *actually* works. Today we have many methods that focus on unsafe functioning but few, if any, that focus on safe functioning. We spend considerable efforts on how to prevent unsafe functioning, but almost none on how to bring about and sustain safe functioning. We naively assume that the absence of unsafe functioning, or rather the absence of the conspicuous outcomes of unsafe functioning, means that we are safe. Yet the aim of safety should not only be to reduce the number of adverse events (the 'visible'). It should also improve the ability to succeed under varying conditions; that is to deal with the 'invisible.' This is consistent with the principles of resilience engineering (e.g. Hollnagel, Woods & Leveson, 2006), which defines safety as the ability of an organisation to succeed under varying conditions. It is a consequence of the changed definition that the level of safety cannot be expressed in terms of (a low number of) negative outcomes. The preoccupation with what goes wrong fails to recognise that the purpose of safety is to ensure that things go right and that normal performance can be sustained.

In light of this it seems odd, indeed, that safety is measured by simple, context-free performance indicators such as fatality rates or accident tallies. Safety should rather be tied to indicators of the dynamic stability of an organisation. An alternative measurement of safety would be one that accounts for the various parameters it actually relates to: technical control of the process at hand, available resources, social acceptance, and so on. Or as proposed by resilience engineering, the ability to respond, to monitor, to anticipate, and to learn (Hollnagel, 2009b). This view is consistent with Slovic's (2001) plea that traditional safety measurements (fatality rates or accident frequencies) should be combined with others, in order to measure the efficiency of the (safety) process rather than the number of outcomes. As disturbing as it might seem, this would recognise the way that safety is actually managed: as a complicated trade-off.

9 Conclusion

We live in a complex world, composed of multiple interacting technical, financial, cultural and political constraints. Doing things perfectly under such conditions is hardly a feasible option. But a view of safety management as involving complicated trade-offs does not blend well with that ideal of a well thought through endeavour, driven by scientific knowledge and practices, and conducted by rational people. The safety myths described in this paper support this ideal. Yet the myths can easily be proven to be wrong, i.e., to be myths rather than reasonable assumptions or facts. They are also counter-productive in the sense that they lead to unrealistic safety management attitudes, policies and targets. In order to have any chance of successfully operating increasingly complex socio-technical systems, we need to abandon the myths and the ideal approach to safety that they imply. We should begin adopting a more

sensible definition of safety and by replacing the myths with more reasonable and sustainable assumptions.

10 Acknowledgements

This article was written thanks to the sponsorship of the industrial partners of the Industrial Safety Chair at Mines-ParisTech.

11 References

Amedeo, F. & Ducros, C. (2009). AF 447: Tous les scénarios du drame vont être analysés. *Le Figaro*, July 9th. On-line at http://www.lefigaro.fr/actualite-france/2009/07/08/01016-20090708ARTFIG00504-af-447-tous-les-scenarios-du-drame-vont-etre-analyses-.php (last accessed on 08 Dec 2009).

Aschenbrenner, M. & Biehl, B. (1994). Improved safety through improved technical measures? Empirical studies regarding risk compensation processes in relation to anti-lock braking systems. In R. M. Trimpop & G. J. S. Wilde, *Challenges to accident prevention: The issue of risk compensation behaviour*. Groningen, The Netherlands: Styx Publications.

BBC (2009). '*Human error' hits Google search*. On-line at http://news.bbc.co.uk/2/hi/technology/7862840.stm (last accessed on 08 Dec 2009).

Benner, L. (1985). Rating accident models and investigation methodologies. *Journal of Safety Research*, 16, 116-126.

Besnard, D. (2006). Procedures, programs and their impact on dependability. In Besnard, D., Gacek, C. & Jones, C.B. (Eds) S*tructure for Dependability: Computer-Based Systems from an Interdisciplinary Perspective.* London, Springer.

Besnard, D. & Greathead, D. (2003). A cognitive approach to safe violations. *Cognition, Technology & Work*, 5, 272-282.

Boeing (2009). *Statistical summary of commercial jet airplanes accidents. Worldwide operations 1959-2008*. On-line at http://www.boeing.com/news/techissues/pdf/statsum.pdf (last accessed on 08 Dec 2009).

Bohnenblust, H. & Slovic, P. (1998). Integrating technical analysis and public values in risk-based decision-making. *Reliability Engineering and System Safety*, 59, 151-159.

Colombain, J. (2009). Quand le cybermonde s'emballe. *France Info*, 02 march, 2009. On-line at http://www.france-info.com/spip.php?article259661&theme=34&sous_theme=35 (last accessed on 08 Dec 2009).

Dekker, S. (2005). *Ten questions about human error*. Mahwah, NJ: Lawrence Erlbaum.

Dougherty, E. M. Jr. (1990). Human reliability analysis - Where shouldst thou turn? *Reliability Engineering and System Safety*, 29(3), 283-299.

Greenwood, M. & Woods, H. M. (1919). A report on the incidence of industrial accidents upon individuals with special reference to multiple accidents. *Reports of the Industrial Fatigue Research Board*, 4, 3-28.

Hamer, M. (1991). Safety posts make roads more dangerous. *New Scientist*, 1786.

Heinrich, H. W. (1931). *Industrial accident prevention*. McGraw-Hill.

Heinrich, H. W. (1934). *The accident sequence*. Presentation given to the Detroit Industrial Safety Council, November 30, 1934.

Hollnagel, E. (2000). Looking for errors of omission and commission or the hunting of the Snark revisited. *Reliability Engineering and System Safety*, 68, 135-145.

Hollnagel, E. (2004). *Barriers and accident prevention*. Aldershot, Ashgate.

Hollnagel, E. (2009a). *The ETTO principle: Efficiency-Thoroughness Trade-Off: Why things that go right sometimes go wrong*. Aldershot: Ashgate.

Hollnagel, E. (2009b). Extending the scope of the human factor. In E. Hollnagel (Ed.), *Safer complex industrial environments*. Boca Raton, FL: Taylor & Francis.

Hollnagel, E. & Amalberti, R. (2001). *The Emperor's New Clothes, or whatever happened to "human error"*? 4th International Workshop on Human Error, Safety and System Development. Linköping, Sweden.

Hollnagel, E., Woods, D. D. & Leveson, N. G. (2006). *Resilience engineering: Concepts and precepts*. Aldershot, UK: Ashgate.

INSAG (1986). International Nuclear Safety Advisory Group. Summary Report on the Post-Accident Review Meeting on the Chernobyl Accident. INSAG-l. Vienna: IAEA.

INSAG (1996). International Nuclear Safety Advisory Group. Defence in depth in nuclear safety. INSAG-10. Vienna, IAEA.

Intersec (2009). On-line at http://www.intersecmiddleeast.com/index.asp?url_id=1&pgName=Home

Lundberg, J., Rollenhagen, C. & Hollnagel, E. (2009). What-You-Look-For-Is-What-You-Find - The consequences of underlying accident models in eight accident investigation manuals. *Safety Science*, 47, 1297-1311.

Negroni, C. (2009). Air safety debate focuses on rest. *International Herald Tribune*, March 4.

Nietzsche, F. (2007; org. 1895). *Twilight of the Idols*. Ware, Hertfordshire: Wordsworth Editions Limited.

Reason, J. (1990). *Human error*. Cambridge, Cambridge University Press.

Reason, J. (2009). *The human contribution*. Aldershot: Ashgate.

Schein, E. H. (1992). *Organizational culture and leadership*. Jossey-Bass, San Francisco

Sklet, S. (2002). *Methods for accident investigations*. Report N° ROSS (NTNU) 200208, Norwegian University of Science and Technology, Norway.

Slovic, P. (2001). The risk game. *Journal of Hazardous Materials*, 86, 17-24.

Summala, H. (1985). Modeling driver behavior: A pessimistic prediction? In Evans, L. & Schwing, R. C. (Eds), *Human behavior and trafic safety* (pp. 43-65). New York: Plenum.

Summala, H. (1988). Risk control is not risk adjustment: The zero-risk theory of driver behaviour and its implications. *Ergonomics, 31*(4), 491-506.

Taylor, F. W. (1911). *The principles of scientific management*. On-line at http://www.gutenberg.org/dirs/etext04/pscmg10.txt (last accessed on 08 Dec 2009).

Telos (2005). *BP Texas City site report of findings. Texas City's protection performance, behaviors, culture, management, and leadership* (BPISOM00122320). The Telos Group.

Tversky, A. & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science*, 185, 1124-1131.

Wackers, G. (2006). *Vulnerability and robustness in a complex technological system: Loss of control and recovery in the 2004 Snorre A gas blow-out*. University of Maastricht, Research report 42/2006.

Weick, K. E. (2001). Making sense of the organization. Oxford, UK: Blackwell Publishing.

Wilde, G. J. S. (1994). *Target risk. Dealing with the danger of death, disease and damage in everyday decisions*. On-line at http://psyc.queensu.ca/target/index.html#contents (last accessed on 08 Dec 2009).

Woltjer, R. & Hollnagel, E. (2007). The Alaska Airlines flight 261 accident: a systemic analysis of functional resonance. Proceedings of the *14th International Symposium on Aviation Psychology*, Dayton, OH.

Woods, D. D. & Cook, R. I. (2002). Nine steps to move forward from error. *Cognition, Technology & Work*, 4, 137–144.

Woods, D. D., Johannesen, L. J., Cook, R. I. & Sarter, N. B. (1994). *Behind human error: Cognitive systems, computers and hindsight*. Columbus, OH: CSERIAC.