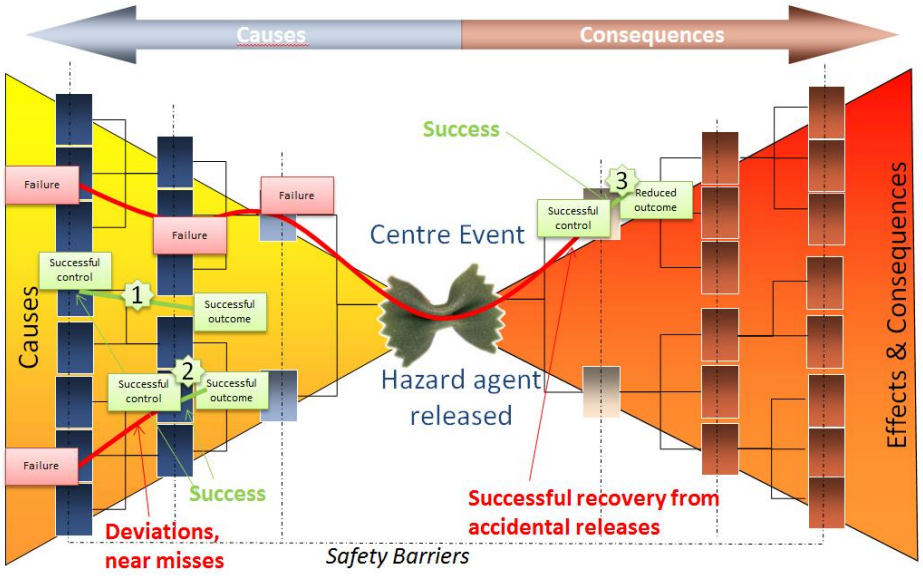
RESILIENCE
SUCCESS CONSORTIUM

SUCCESS IN THE FACE OF UNCERTAINTY



31 March 2015

HUMAN RESILIENCE AND THE ACCIDENT RISK BOW-TIE

Rev 12

Author: Resilience Success Consortium

CONTACT

Consortium

http://www.resiliencesuccessconsortium.com/

Linda J. Bellamy (Coordinator)
Consultant & Managing Director, White Queen Safety Strategies, PO Box 712, 2130 AS Hoofddorp, the Netherlands
T. +31 (0)235 651353, M. +31 (0)6 54648622
www.whitequeen.nl
linda.bellamy@whitequeen.nl

Anne van Galen
Consultant & Managing Director, AvG Consultancy, La Balme 05120 Les Vigneaux, Hautes Alpes, France
http://www.avgconsultancy.com/
anne@avgconsultancy.com

Nijs Jan Duijm
Senior Researcher, Management Engineering, Technical University of Denmark (DTU), Denmark
http://www.man.dtu.dk/english
nidu@dtu.dk

Kirsten Jørgensen
Associate Professor, Management Engineering, Technical University of Denmark (DTU), Denmark
http://www.man.dtu.dk/english
kirj@dtu.dk

Arthur Dijkstra
Pilot, Consultant & Managing Director, ADMC, Nederhorst den Berg, the Netherlands
arthur@admc.pro

Hans Baksteen
Consultant & Managing Director, Rondas Safety Consultancy BV, Nieuwegein, the Netherlands
hans.baksteen@gmail.com

Olga N Aneziris
Senior Researcher, NCSR Demokritos, Aghia Paraskevi, Greece
https://ipta.demokritos.gr/
olga@ipta.demokritos.gr

Ioannis A. Papazoglou
Institute Director, NCSR Demokritos, Aghia Paraskevi, Greece
https://ipta.demokritos.gr/
yannisp@ipta.demokritos.gr

SUCCESS IN THE FACE OF UNCERTAINTY

Contents

1 INTRODUCTION

1.1 Overview

This report describes the approach and findings of a research project carried out for SAF€RA, an ERA-NET project - Coordination of European Research on Industrial Safety towards Smart and Sustainable Growth - funded by the European Commission in the 7th Framework Programme. The work was supported by the Dutch National Institute for Public Health and the Environment (RIVM) and the French Foundation for an Industrial Safety Culture (FonCSI).

A consortium of experts, known as the Resilience Success Consortium[1], carried out the work. The consortium consisted of the following persons and organisations:

- Linda J. Bellamy, White Queen BV, the Netherlands – Coordinator
- Anne van Galen, Anne van Galen Consultancy, France
- Ioannis Papazoglou & Olga Aneziris, NCSR Demokritos, Greece
- Nijs-Jan Duijm & Kirsten Jorgensen, DTU Department of Management Engineering, Denmark
- Hans Baksteen, Rondas Safety Consultancy BV, the Netherlands
- Arthur Dijkstra, Pilot (Captain B777) & ADMC consultancy, the Netherlands- Reviewer

The current research addresses safety success rather than failure, especially the topic of resilience and whether resilience concepts can be integrated into classical bow-tie approaches. The Dutch institute RIVM has an interest in scenario-based methods using their bow-tie structured accident analysis tool Storybuilder™. The tool and databases are publically available[2]. The bow-tie is a linear model with a focus on the negative, the already occurred accidents. Resilience modelling could be considered to be a mirror of this in being proactive rather than reactive in the face of unanticipated scenarios. A common definition of resilience in the safety context is:

> "the intrinsic ability of a system to adjust its functioning prior to, during or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions" (Hollnagel et al 2011)

This research concentrates on the way professional people in operational and management roles deliver success in handling the unexpected and the organisational contexts which foster resilient behaviour. It is particularly concerned with decision making when faced with the uncertainties of managing major accident hazards. In the (petro)chemical industry major accident hazards are the potential for "…a major emission, fire, or explosion resulting from uncontrolled developments in the course of the operation involving dangerous substances… and leading to serious danger to human health and/or the environment…".(EC 1996). Risk is defined as "the likelihood of a specific effect occurring within a specified period or in specified circumstances". However, the risk of having a major accident is not static because the possible consequences and associated likelihoods can change from moment to moment depending, amongst others, on such factors as activities being undertaken, the presence of people, their state of awareness, environmental conditions, the condition of the controls for hazard containment and the organizational context within which the activities take place. How do people manage the uncertainty of such a changing environment?

A resilience questionnaire was developed to address this management of uncertainty. It formed the basis for interviewing people who have to deal with high risk control problems in the following contexts: mountain

[1] http://www.resiliencesuccessconsortium.com/

[2] **http://www.rivm.nl/en/Topics/O/Occupational_Safety/Other_risks_at_work/Dangerous_substances** Information about major hazard model and link to download Storybuilder and databases.
http://www.rivm.nl/en/Topics/S/Storybuilder Information about Storybuilder in context of occupational safety with links to download, user manuals, factsheets and more.

climbing, dangerous maintenance using rope access, management of major hazard (petro)chemical installations and steel-making. The results provided information on the thinking of professional people who manage high risk environments resiliently, how they view uncertainty and the kinds of things they think about and the way they interact with others as part of their management of the uncertainties. It was found in this project that it requires a special kind of multi-dimensional vigilance to monitor the need for intervention and that when something unexpected does suddenly happen it is good to monitor what is going on and have the availability of time and different competences to be able to stop and think with others.

This provided case studies across sectors, to help determine what organisations could do to stimulate resilience within their own human capital. The components of resilience derived from the case studies were incorporated into the publically available Storybuilder™ bow-tie tool. The bow-tie was modelled as one single success bow-tie with the resilience factors connected to the signal detection and response selection components of the intervention. The basis for modelling was a safety barrier approach with the concept of intervention triggered by the occurrence of deviation, a signal.

The model was filled with a set of scenarios from a near miss database of a major hazard company. Lessons learned from major accidents were also considered in the resilience context. It was identified that very little regarding resilience is being collected in incident investigations; resilience lessons learned could be considered using judgement.

The outcomes can benefit current users of bow-tie modelling by providing a better understanding of resilience in the bow-tie context. A checklist of the steps and components in the model was made. This model is downloadable from the consortium website www.resiliencesuccessconsortium.com.

The products produced from the work were as follows:

- Preliminary Product Specifications (Annex A)
- Discussion document: Resilience in terms of bowties and barriers (incorporated after discussion comments as Chapter 4)
- Resilience Questionnaire
- Resilience Case Studies (Annex B)
- IDDR – Indication, detection, diagnosis and response (incorporated in Chapter 6)
- Resilience: At what level of the prevention/ safety stages? (incorporated in Chapter 6)
- Lessons learned, near misses and unsafe conditions: Analysis of a sample of accident reports and a company database of near misses & unsafe conditions (Annex C)
- Uncertainty definition and relationship with resilience (incorporated in Chapters 3 & 7)
- Success bowtie event checklist (Annex D)
- Glossary of terms (Annex E)
- Storybuilder model database (Separate Storybuilder file can be downloaded from http://www.resiliencesuccessconsortium.com/resources)

1.2 Objectives and research questions

The objectives were as follows:

- Identifying through interviews at operational and managerial levels the characteristics of mental models of resilient people who have to manage high consequence risks on a daily basis and turning these into inspiring case studies and components for the bow-tie.
- Incorporating resilience into the bow-tie based on the research on mental models, knowledge within the consortium and developed modelling principles, identifying the key steps.
- Running a set of accidents through the new model to create a showcase of lessons learned to stimulate resilience-thinking in organisations.
-

Research questions from RIVM that were addressed:

- How can the bow-tie model and resilience be integrated to extract additional information from accidents?
- What Human and Organisational Factor (HOF) elements are involved?
- What can be learned from the integration by inputting new scenarios?
- On a more general level the questions addressed are:
- How can safety be improved in practice by adopting the resilience approach?
- Can resilience concepts be integrated into the classical bow-tie approaches to risk assessment, in particular to improve the characterization of the management system's performance and the impact of human and organization factors of safety and loss of control?

1.3 Methodology for achieving objectives

An overview of the processes for achieving the objectives is shown in Figure 1. These were

- Coordination meetings of the researchers in the consortium.
- Functional specifications of the required modelling outcomes.
- Consolidation of consortium knowledge on mental modelling and resilience engineering.
- Development of a resilience questionnaire to support interviewing for the specific modelling requirements of the project.
- 18 face to face or online interviews with:
    - Mountaineers (also called alpinists) who are directly confronting natural hazards (4);
    - Rope Access Workers carrying out dangerous maintenance on man-made structures (3);
    - HS&E Managers and Operations Managers of high hazard chemical (6), petrochemical (3) and steel plants (2).
- Evaluating and consolidating the interview results in order to describe mental models of risk awareness and control and to provide case studies of resilience in handling uncertainty.
- Defining uncertainty and resilience in the bow-tie and development of the success modes of the safety barriers into the human part of the system
- Attaching the mental modelling to success barriers in Storybuilder
- Modelling incidents in the new model to identify lessons learned
- Defining what is needed in the new success bow-tie

The approach made use of the modelling experience of the multi-disciplinary team which brought together psychology, engineering, reliability modelling, crisis management and policy development as well as expertise in practical implementation in the business processes.

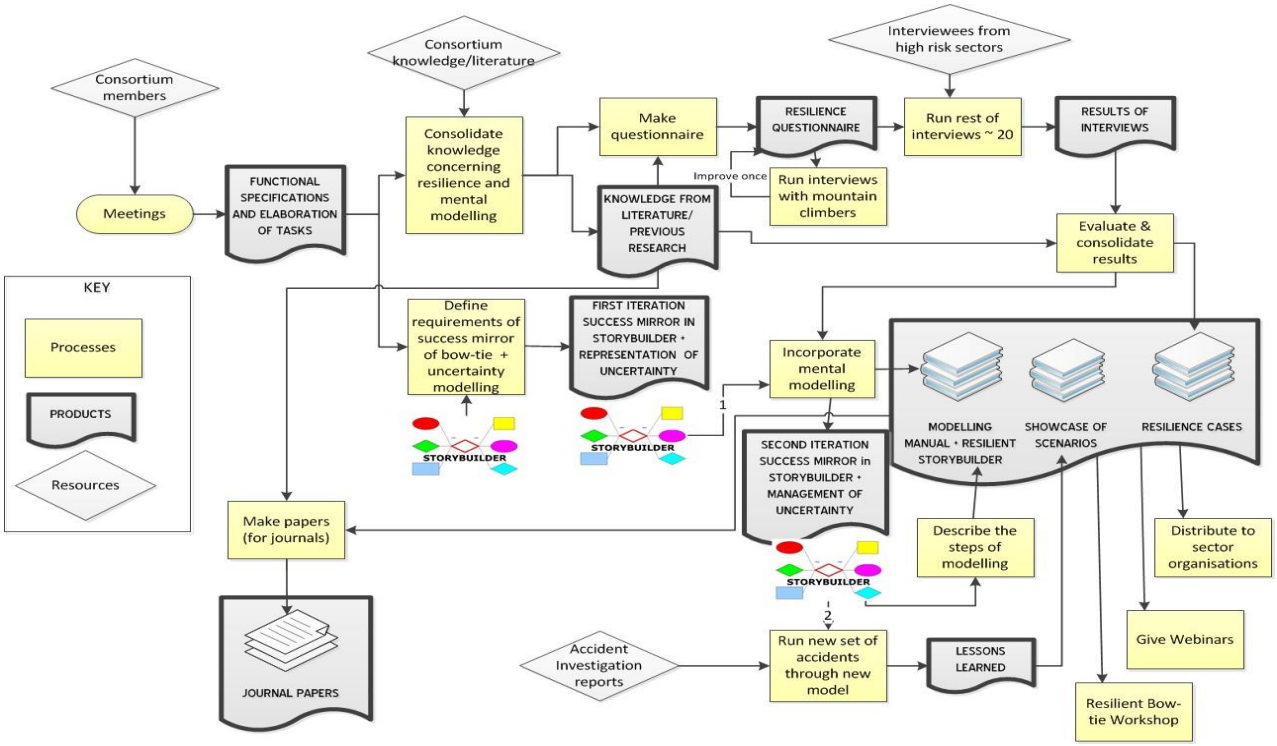


FIGURE 1 OVERALL RELATIONSHIPS IN THE APPROACH PLAN

2 WHAT IS RESILIENCE

2.1 Common concepts

A general definition of resilience is given by Zolli and Healy (2012) as:

> 'the capacity of a system, enterprise, or a person to maintain its core purpose and integrity in the face of dramatically changed circumstances'

The important aspect of resilience which characterises many definitions across many fields is an ability of an entity (forest, person, refinery, city) to adapt to or absorb change and disruption such that the entity continues to be like it was before the change. A key characteristic of a resilient system is that it is dynamic in its adjustment to changes, disturbances, deviations, disruptions, adversity. A resilient individual is able to adapt to adversity or traumatic experiences with outcomes that can be considered to be positive. Recovery is important:

> "First, as a response to stressful events, resilience focuses on recovery, the ability to rebound from stress, a capacity to regain equilibrium quickly and to return to an initial state of health. A second and equally central dimension, sustainability, implies the continuation of the recovery trajectory, and even growth and enhancement of function." Reich et al (2010).

Resilience is also used as a term to describe the ability of cities, regions or countries to deal with major disasters such as hurricanes, flooding's and wars:

> "Local resiliency with regard to disasters means that a locale is able to withstand an extreme natural event without suffering devastating losses, damage, diminished productivity, or quality of life without a large amount of assistance from outside the community." (Mileti 1999).

Resilience exists in engineered systems, as in the construction of Viking ships a millennium ago (Hocker & Ward, 2004); resiliency combined with carefully selected quality materials was a basic pre-condition of

construction. Measures to provide flexibility and to allow controlled movements of the hull in response to wave impacts enabled the Vikings' light ships to withstand the stresses and strains of daily use in a variety of waters.

The nature of this ship construction illustrates a property of resilience which is deemed to be important, and that is to adapt to allow the system to change with the variability rather than to try to cancel it out. A feature of a resilient system is that it has this kind of flexibility – it can survive within a certain bandwidth of change.

Pasman et al (2013) describes resilience in the process industry as follows:

"In process technology terms, it is the capability of a process to return to its steady state after a disturbance or deviation, due to variation of external or internal conditions in one or more of the process variables. This capability is not all autonomously achieved, the operators in the control room and in the field have their steering influence on the course of the process, while the designer has fixed the boundary conditions and has limited the possibilities (to select from)"

Holling, a Canadian ecologist who has been described as the "father of resilience", says that resilience is

> "a measure of the persistence of systems and of their ability to absorb change and disturbance and still maintain the same relationships between populations or state variables" (Holling 1973).

He goes on to say that:

> "..if we are dealing with a system profoundly affected by changes external to it, and continually confronted by the unexpected, the constancy of its behaviour becomes less important than the persistence of the relationships. Attention shifts, therefore, to the qualitative and to questions of existence or not."

Folke (2006), addressing socio-ecological systems, adds capacity for renewal, re-organization and development - disturbance has the potential to create opportunity to do new things:

> "… [M]anaging for resilience enhances the likelihood of sustaining desirable pathways for development in changing environments where the future is unpredictable and surprise is likely."

So, expecting surprise, flexibility in responding to variation, maintaining the relationships of the system as well as the capacity for renewal and reorganisation after disturbance are all important resilience characteristics. These concepts can be applied in the current research context where the concern is industrial safety, managing major hazard risks. Uncertainty, cognitive biases and the limitations in what we are able to think about in terms of what might happen in the future must also be included (Annex B Resilience Case Studies).

2.2 Output measures of resilience

Resilience, besides the properties of responding to variability and change, can also be considered in terms of output measures. Output measures of resilience can include the extent of recovery to the original functional state and the time for recovery after disturbance takes place. For example Tierney & Bruneau (2007) discuss these parameters in recovery of critical infrastructure systems. Scheffer et al (2009), considering environmental and biological complex dynamical systems, provide models to show that rate of recovery is high in high resilience systems and may slow to zero in a system approaching a tipping point of catastrophic transition, what is called "critical slowing down". Relatedly, in the area of major hazards, Stough (2011) has suggested that the most effective leading Key Performance Indicators (KPIs) are associated with reporting and action items for all kinds of unwanted outcomes particularly reporting rate, response rate and timely completion.

2.3 Adaptation and adjustment

From the perspective of safety, resilience has been defined as:

> 'the intrinsic ability of a system to adjust its functioning prior to, during or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions' (Hollnagel et al 2011).

Adaptation in a system is done by people. It has been said that complex adaptive systems are self-organising, with self-regulating feedbacks, and that a way to assist the resilience of a system is by allowing it to probe its boundaries; maintaining resilience requires continual change while keeping things constant reduces resilience (Stockholm Resilience Centre 2015; Walker 2005; Walker et al 2004; Walker & Westley 2011). Routine can be regarded as a such a constant; the Annex B Resilience Case Studies indicated that routine work is resilience reducing:

> "….there are the people who feel very comfortable with the risk; they stop seeing the risk. Routine is a huge danger. I think for that kind of danger it will be important to change tasks now and then." *Lead engineer industrial rope access and maintenance.*

> "There are guides that do the same course over and over again. Each week the Dome des Ecrins or Mont Blanc. And then they do not have the same vigilance anymore. They pass underneath the seracs[3] every day and they get used to the danger, they do not pay special attention anymore and in their decision making they forget about it instead of taking a little distance and think through the consequences." *Mountain Guide & Trainer*

In the field of safety the concept of the *safe boundary* was introduced by Rasmussen (1997) and further considered in the context of resilience (Woods et al 2009). The idea was that people migrate towards the boundary of acceptable performance and that there is a need to make the boundaries explicit and known because crossing the boundary can lead to accidents. The idea of crossing the boundary, especially when that is occurring simultaneously with several actors, is developed to account for accidents especially when defence-in-depth systems erode. Walker (2005), an expert in the field of social-ecological systems, describes a "basin of attraction" which is a set of system states within which a system tends to remain due to its own internal dynamics. Walker (2005) says that:

> "erosion of resilience results in increasing vulnerability to external shocks, such that it takes progressively smaller amounts of disturbance to push the system across a threshold into an alternate regime, with concomitant social, economic and ecological costs."

Walker et al (2004) explain that human optimal body temperature is very close to the threshold for life and death but there are strong negative feedbacks, strong resistance, making it difficult to move across this threshold:

> "..being precariously close to such a threshold has meant the evolution of strong resistance".

This is similar to the idea of antifragility (Taleb 2012) where:

> "..anything that has more upside that downside from random events (or certain shocks) is antifragile".

In the Annex B Resilience Case Studies, experiencing from mistakes and things that go wrong are considered important to maintain success. Just as life and death might be seen as two basins of attraction in the temperature example where the optimal temperature is close to the boundary, so success and failure in safety could be similarly viewed and that resilient performance requires performing close to the boundary of failure, what one interviewee described as *top level sports*:

> "It reminds me of my time as a student and my chess statistics. For example I often replayed the chess-games of a particular grandmaster. I tried to make the right chess moves. Maybe four times it worked well, and the fifth time I made the wrong move and lost the game. What I mean is that you have to keep your error statistics as low as possible. Me and my colleagues we know that we only get better at managing our processes when we reduce our error statistics. And we know we make many mistakes, every day, because a lot of decisions are taken. So what it is

[3] a block or column of glacial ice, which can be the size of a house or larger, that can fall at any time without warning

> all about at the blast furnace is to reduce the error-statistics without the performance going down too much. And this is top level sports." Manager, Blast Furnaces

To operate close to the boundary means that feedback mechanisms are very important. There need to be continuously strong signals to prevent people going over the edge and yet allow behaviour that can elaborate on the nature of the threshold between the states and make appropriate adjustments. You need to know when you are at the threshold. Threshold signals will appear in the form of deviations, unsafe acts and near misses, coming from the "real world". Simulations, emergency response exercises and the like are examples of threshold informing activities (Walker & Westley 2011).

2.4 Resilience Engineering Approach

2.4.1 Success and failure

Resilience Engineering (RE) has been proposed as a new way to think about and manage safety . RE is the capability of systems and organizations to anticipate and adapt to the potential for surprise and failure (e.g. Hollnagel et al 2006). It stimulates negative considerations of what are called traditional approaches to failure and risk. Considerations of human and organisational factors in safety in low probability high consequence technical systems is becoming much more a matter of understanding risk from a cognitive perspective than from a logical analysis of the risks and reliabilities of technical systems coupled with human reliability and errors. Consideration of failure is what has largely dominated models of risk in the (petro)chemical industry – accident analysis, risk assessment, bow-tie models, fault trees, HAZOP, LOPA, FMEA, all failure related models and processes aiming to assist the foreseeing of possible failure routes and to identify the controls and their adequacy for preventing serious losses. However, with newly emerging hazards and risks and with organisations, technology and networks becoming more complex, resilience in the face of uncertainty is coming into demand and being increasingly addressed (Hollnagel 2010, Hollnagel et al 2011; Pasman et al 2013; Shirali et al 2012, 2013; Steen & Aven 2011).

Hollnagel et al (2013) consider that safety is an emergent phenomenon of a complex system that cannot be explained using the principles of decomposition and causality. This also underpins the difference between Hollnagel's Safety II world, addressing success in handling change and variability, and Safety I, addressing failure, which according to Hollnagel is trying to make sure things do not go wrong instead of making sure they are successes. With Safety I, models are employed to trace causes from outcomes and vice versa to identify outcomes from causes - as is typical in accident analysis and risk analysis. Safety I models (called "traditional" or "classical") have been considered too limiting and too linear in handling complex systems.

The resilience engineering approach is stated to differ from the more traditional safety management approaches in the way it looks at disturbances, performance variability, failure and human adaptation to expected and unexpected changes. It is said that within the more traditional safety management approaches the purpose is to rule out all kinds of disturbances and variability in order to make a system 'safe'. Within the resilience engineering way of thinking:

> 'trying to achieve safety by constraining performance variability will inevitably affect the ability to achieve desired outcomes and therefore be counterproductive'. (Hollnagel et al 2013, p.14).

In real systems 'performance variability', change and all kinds of human adaptation should be regarded as 'normal'. From this perspective safety is about managing performance variability and not solely about constraining it. When systems perform reliably, RE would suggest that it is because people are flexible and adaptive, rather than because the systems are perfectly thought out and designed.

The viewpoint of resilience engineering is that failure is the flip side of success: things that go right and wrong are more or less the result of the same underlying processes. This also means that success is an outcome of the management of performance variability. In resilience engineering the focus is shifted away

from the management of risks and 'safety' to performance management in general. Safety is the ability *to succeed* under varying conditions. Because successes and failures both depend on performance variability, failures cannot be prevented by eliminating this variability; in other words, according to RE safety cannot be managed by imposing constraints on normal work.

The argument is that proactive and early responses are just as important as learning from failure: Ensuring that as much as possible goes right, in the sense that everyday work achieves its stated purposes, cannot be done by responding alone, since that will only correct what has happened. Safety management must instead be proactive, so that interventions are made before something happens.

2.4.2 Four cornerstones of resilience

To appropriately intervene, Hollnagel et al (2011) describe the four cornerstones, or four essential capabilities, of resilience. The current project takes these four cornerstones as a starting point for developing the model of the resilient bowtie, and they are extensively elaborated in Annex B Resilience Case Studies. They are:

- Ability to respond to events [RESPONDING] - how to respond to regular and irregular disruptions and disturbances by adjusting normal functioning. This is the ability to address the actual.
- Ability to monitor ongoing developments [MONITORING] - how to monitor that which is or could become a threat in the near term. The monitoring must cover both that which happens in the environment and that which happens in the system itself, i.e., its own performance. This is the ability to address the critical.
- Ability to anticipate future threats & opportunities [ANTICIPATING] - how to anticipate developments and threats further into the future, such as potential disruptions, pressures, and their consequences. This is the ability to address the potential
- Ability to learn from past failures and successes [LEARNING] - how to learn from experience, in particular to learn the right lessons from the right experience. This is the ability to address the factual.

2.4.3 ETTO: Efficiency-Thoroughness Trade-Off

Human performance is affected by the balance between the demands and the resources available. This is what Hollnagel (2009) calls the efficiency thoroughness trade off or the ETTO principle.

It is a fundamental characteristic of human performance, whether individual or collective, that the resources needed to do something often, if not always, are too few. The most frequent shortcoming is a lack of time, but other resources such as information, materials, tools, energy, and manpower may also be in short supply. We nevertheless usually manage to meet the requirements to acceptable performance by adjusting how we do things to meet the demands and the current conditions - or in other words to balance demands and resources.

The essence of this balance or trade-off between efficiency and thoroughness is described by the ETTO principle, which, in its simplest possible form, can be stated as follows: In their daily activities, at work or at leisure, people (and organisations) routinely make a choice between being effective and being thorough, since it rarely is possible to be both at the same time. If demands for productivity or performance are high, thoroughness is reduced until the productivity goals are met. If demands for safety are high, efficiency is reduced until the safety goals are met.

In the current research project, with the case studies (Annex B Resilience Case Studies) there is some evidence for this practice, but the functioning of the ETTO principle must be nuanced. The difficulty lies in the fact that due to uncertainty people are not always capable of estimating the danger and 'demands of safety'. Resilient people therefore rather seem to do 'as much as possible right' in order to be prepared for

unforeseen circumstances. At the same time it is crucial that they are vigilant and aware of changing circumstances.

2.5 Mindfulness, Sensemaking, HROs

Resilience refers to a world in which notions of causality are more or less dismissed and in which ideas about sensemaking and mindfulness (Weick 1995, 2012; Weick et al 1999) are appealing. A principal element of organisations that are highly reliable is mindfulness (Roberts, Stout and Halpern, 1994; Vogus and Welborne, 2003; Vogus et al 2014; Weick and Sutcliffe, 2007; Weick et al, 1999; Wildavsky, 1988). Mindfulness can be described as a rich awareness of discriminatory detail. It requires high quality attention. When people act they are aware of context, of ways in which details differ (in other words they discriminate among details), and of deviations from their expectations.

Sensemaking is a term used to describe the making sense of the world so that we can act in it, knowing enough to make contextually appropriate decisions. For example, Kurtz & Snowden (2003) have developed a sense-making framework called Cynefin which is aimed at helping decision making by separating out the different contexts in which decisions may be made – known, knowable, complex, chaos and disorder. In sense-making the framework emerges from the data and not the other way around as occurs when we use prescriptive models to collect and analyse data.

The characteristics of resilience engineering such as described by Hollnagel and others seem to be strongly related to the characteristics of so called High Reliability Organisations (HRO's). This has already been noted by Hopkins (2014). HRO's or so called mindful organisations (Weick and Sutcliffe 2007) manage the unexpected through five principles:

- Preoccupation with failures rather than successes. Any lapse in the system is treated as a symptom that something may be wrong with the system, something that could have severe consequences if several separate small errors happened to coincide.
- Reluctance to simplify interpretations; in a HRO the recognition of an event as something that has been experienced before and understood is a source of concern rather than comfort. The concern is that superficial similarities between the present and the past mask deeper differences that could proof fatal.
- Sensitivity to operations; HRO's are attentive to the front line where the real work is done. Well developed situational awareness facilitates the continuous adjustments that prevent errors from accumulating and enlarging. This involves looking at the big picture on a constant basis from the viewpoint of real-time information.
- Commitment to resilience; HRO's develop capabilities to detect, contain, and bounce back from those inevitable errors that are part of an indeterminate world.
- Deference to expertise; HRO's cultivate diversity. HRO's push decision making down and around, an under-specification of organisational structures. The deferment of decision making to individuals with the greatest experience and expertise in the organisation occurs regardless of the structured hierarchy, with recognition of more 'fluid' decision making processes.

Of course the perspectives of HRO-principles and resilience engineering differ when it comes to their emphasis on respectively failure and success. The Annex B Resilience Case Studies identifies that resilient people are more preoccupied with failure than with what they learn from successes which is more in line with the HRO principle.

3 WHAT IS UNCERTAINTY

The notion of uncertainty is central to this research. It is the problem people face in the management of risk and one in which resilience could help; in principle, the more resilient the human factor the more the uncertainty can be reduced by the adaptive human function in response to variation and change.

3.1 Types of uncertainty

Uncertainties in decision and risk analyses can be divided into two categories: uncertainties that stem from variability in known (or observable) populations and, therefore, represent randomness in samples (ontic or aleatory uncertainties) and those that come from basic lack of knowledge about fundamental phenomena (epistemic uncertainties) also known in the literature as ambiguity (Pate Cornell 1996). For example, randomness can be illustrated by the occurrence of initiating events and component failures. Epistemic uncertainties arise when making statistical inferences from data and, from incompleteness in the collective state of knowledge about how to represent plant behaviour in the risk model. The epistemic uncertainties of a risk model relate to the degree of belief that the analysts have in the representativeness or validity of the risk model and in its predictions (i.e., how well the risk analysis model reflects the design and operation of the plant and, therefore, how well it predicts the response of the plant to postulated accidents) (USNCR 2009). Most risk analysis problems involve both known statistical samples and unknown or partially known mechanisms. Bayesian probability theory allows the measurement and combination of randomness (aleatory uncertainties) and fundamental (epistemic) uncertainties.

3.2 Sources and treatment of uncertainty

Three generic sources of uncertainty have been presented by the American Institute of Chemical Engineers (2000) which are the following: a) model uncertainty, b) data uncertainty and c) general quality uncertainties. Model uncertainty reflects the weakness, deficiencies and inadequacies intrinsic to the model and is a measure of the degree to which a model fails to represent reality. Uncertainties in the input parameters to the model result from the incomplete data available and the need to fill gaps through estimation, inference or expert opinion. General quality uncertainties involve the issues of completeness and comprehensiveness. It is not possible for an analyst to identify every potential incident. Uncertainty arises from not knowing the risk contributions from omitted incidents.

The identification of the contributors to the overall uncertainty is important to the analyst, as well as to the users of the final results. Isolation of uncertainties due to the quality of the data base of a study from those due to component technique models provides opportunity to reduce the uncertainty and improve estimate quality. This can help determine where increased investment in data collection or model development could significantly reduce uncertainty.

3.3 The analysis of uncertainty in risk assessment

This involves five tasks:

a) Evaluation and representation of uncertainties in input data

Before evaluating uncertainty, the risk analyst needs to determine how to best represent uncertainty from each of the sources discussed. Statistical measures are used to characterize uncertainty in data and weighting techniques are applied to model uncertainty.

b) Propagation of the uncertainties through risk assessment

Various methods are available to propagate uncertainties, such as integration methods and moments methods and various comparisons of these methods have appeared in the literature. Monte Carlo techniques have been widely used. They involve evaluation of the output from a model given a random

sampling of values from distributed assigned to input values. The method of sample generation called LHS (Latin Hypercube Sample) gives very good results as reported in Imam & Helton (1985). It requires as input the distribution of uncertain parameters, the rank correlation matrix among the variables and the size of the sample.

c) Combination of uncertainties in the output from each of the steps is risk assessment methodology

When an uncertainty analysis has been performed for each step, the resulting uncertainties need to be combined to develop an estimate of the overall uncertainty associated with the risk estimate.

d) Display and interpretation of the uncertainties in the final risk estimate

There are various formats available to display uncertainty. These include uncertainty bands e.g. uncertainty 95% confidence intervals, uncertainty bands surrounding F-N curves (Pate Cornell 1996). Other ways to represent uncertainties are difference maps indicating spatial uncertainty. For example risk contour of a specific level could be presented on a map, together with the relevant uncertainty with colours that vary. Uncertainty of risk in chemical installations both in the form of society and individual risk is presented by Lauridsen et al (2002).

e) Treatment of uncertainties in decision making

Walker et al (2003) suggest that uncertainty is a three dimensional concept defined by: location of uncertainty, level of uncertainty and the nature of uncertainty. Location of uncertainty is an identification of where uncertainty manifests itself within the whole model complex. Level of uncertainty has also been described by Walker et al (2010) and presents the spectrum of uncertainty between deterministic knowledge and ignorance in terms of the following levels: determinism, statistical uncertainty, scenario uncertainty, recognised ignorance, total ignorance (unknown, unknowns). Nature of uncertainty refers to whether it is due to imperfection of knowledge or to variability. These three dimension of uncertainty have been incorporated into an uncertainty matrix proposed by Walker et al (2003) and extended by Petersen et al (2013), as a tool to indicate the most important uncertainties and rank them as an initial prioritization based on general knowledge and experience, or even with more advanced studies. Their uncertainty matrix is shown in Figure 2 which could be used to model uncertainties in various cases by considering uncertainties in various elements (e.g. barriers), human errors etc. of risk models.

Location		Level			Nature	
		Statistical uncertainty	Scenario uncertainty	Recognised ignorance	Epistemic uncertainty	Variability uncertainty
Context	Natural, technological economic, social and political, representation					
Model	Model structure					
	Technical model					
Inputs	Driving forces					
	System data					
Parameters						
Model Outcomes						

FIGURE 2 UNCERTAINTY MATRIX (PETERSEN ET AL 2013)

The dimension **'level of uncertainty'** expresses how a specific uncertainty source can be classified on a gradual scale, running from 'known for certain' to 'unknown'. This dimension uses three distinct classes:

> **Statistical uncertainty:** This concerns the uncertainties that adequately may be expressed in statistical terms; for example, as a range with associated probability (e.g. statistical expressions for measurement inaccuracies, uncertainties due to sampling effects, and uncertainties in model-parameter estimates). In the natural sciences, scientists generally refer to this category if they speak of uncertainty, thereby often implicitly assuming that the involved model relations offer adequate descriptions of the real system under study, and that the data or calibration data used are representative of the situation under study. However, when this is not the case, 'deeper' forms of uncertainty are in play, which may surpass the 'statistical uncertainty' in magnitude and seriousness and thus require adequate attention.
>
> **Scenario uncertainty:** This concerns uncertainties that cannot be adequately depicted in terms of chances or probabilities, but can only be specified in terms of (a range of) possible outcomes. For these uncertainties it is impossible to specify a degree of probability or belief, since the mechanisms that have led to the outcomes are not sufficiently known. Scenario uncertainties are often construed in terms of 'what-if' statements.
>
> **Recognised ignorance**: this concerns the uncertainties known to be there – in some way or another – but for which no useful estimate can be established; for example, due to limits to predictability and knowledge ('chaos') or due to unknown processes.
>
> Continuing on the scale beyond recognised ignorance, the area of complete ignorance is entered ('unknown unknowns'), for uncertainties that cannot be addressed and scientists inevitably are in the dark.

The dimension, **'nature of uncertainty'**, expresses whether uncertainty is primarily a consequence of the incompleteness and fallibility of knowledge ('knowledge-related', or 'epistemic' uncertainty) or that it is primarily due to the intrinsic indeterminate and/or variable character of the system under study ('variability-related', or 'ontic' uncertainty).

> **Knowledge-related uncertainty (epistemic)** can, although not necessarily, be reduced by means of more measurements, better models and/or more knowledge.
>
> **Variability-related uncertainty** is typically not reducible through more research (e.g. inherent indeterminacy and/or unpredictability, randomness, chaotic behaviour).

3.4 Uncertainty analysis in Major Hazards plants

Uncertainty analysis of major hazards plants can be distinguished in two major phases: a) quantification of uncertainties in the frequency of the plant damage state (e.g. uncertainty in the frequency of pipe or tank failure etc) and b) quantification of uncertainties in the consequence calculations.

3.4.1 Uncertainty in the frequency of plant-damage states

The frequency of a plant damage state is defined from the frequencies of accident sequences which lead to this damage state, which in turn are determined from the frequencies of the "cut sets" of Fault trees. Uncertainties exist in the following parameters: frequencies of initiating events, failure frequencies of safety related equipment, equipment unavailabilities and probabilities of human errors.

3.4.2 Uncertainty in consequence assessment

An accident sequence resulting in a release of toxic or flammable substance to the environment, if precisely determined, would lead to a unique type of release. Such precise knowledge, is not, however, always available.

The various methodological tasks and associated models in the assessment of the consequences of possible accidents are characterized by uncertainties. These uncertainties can be due to incomplete knowledge of various physical phenomena, to lack of knowledge of the exact value of certain parameters in the models, or to statistical variation of certain parameters of the model. If the parameter serves as an input to a specific model the quantified uncertainty reflects either incomplete knowledge of the value of this parameter or a stochastic variability. If the value of the random variable determines the type of the applicable model the quantified uncertainty characterizes the selection of the model. Various sources of uncertainty are presented in the following Table 1.

TABLE 1 TYPES OF UNCERTAINTIES THAT CAN BE QUANTIFIED IN RISK ASSESSMENT (PAPAZOGLOU ET AL 1996)

TYPE OF UNCERTAINTY	RANDOM PARAMETERS
Released Quantity of Hazardous material	• Total mass of released substance in case of instantaneous releases. • Release rate in case of continuous releases (area of the opening in case of tank or pipe failure). • Duration of evaporation.
Conditions of Release	• Amount of droplets for liquefied gas releases • Initial dilution of gas • Temperature of gas • Pool radius for flammable material
Model uncertainty	• Type of model used for dispersion (e.g. Gaussian or heavier than air)
Conditions, parameters of dispersion	• Soil roughness
Dose received	• Exposure time to toxic substance or high level of thermal radiations.
Vulnerability Model	• Parameters of probit function
Position of Ignition Source	• Time of ignition of flammable cloud
Weather Conditions	• Wind direction • Wind velocity • Atmospheric stability class temperature • Ambient Temperature

3.5 The human experience of uncertainty and cognitive bias

The previous sections described uncertainty from the perspective of risk analysts and their models. As has been made clear from studies by Tversky & Kahneman 1974; Kahneman 2011; Kahneman & Tversky 1982,:

> "psychological analyses of responses to uncertainty reveal a wide variety of processes and experiences, which may follow different rules "(Kahneman & Tversky 1982)

The interpretation of perceived events and expectations about outcomes is a complex process involving both unconscious and conscious elements and what Kahneman (2011) has referred to as thinking fast and thinking slow.

Cognitive biases include:

- Confirmation bias, the tendency to seek out only that information that supports one's preconceptions, and to discount that which does not. For example, hearing only one side of a political debate.
- Anchoring bias: the tendency to rely too heavily, or "anchor", on one trait or piece of information when making decisions (usually the first piece of information acquired). Once an anchor is set, there is a bias toward interpreting other information around the anchor and other judgments are made by adjusting away from that anchor.
- Sunk cost fallacy - a sunk cost is a cost that has already been incurred and cannot be recovered A person or organization is more likely to continue with a project if they have already invested a lot of money, time, or effort in it, even when continuing is not the best thing to do.
- Representativeness heuristic is used when making judgements by judging probabilities on the basis of resemblance. It is the tendency to judge something as belonging to a class based on a few salient characteristics without accounting for the base rates of those characteristics.
- Hindsight bias, the tendency to see past events as being predictable at the time those events happened..
- Availability heuristic, the tendency to estimate that what is easily remembered is more likely than that which is not.
- Recency effect, like the availability bias, placing too much emphasis on information and evidence that is recent
- Overconfidence effect, a well-established bias in which a person's subjective confidence in his or her judgments is reliably greater than the objective accuracy of those judgments, especially when confidence is relatively high.

Errors of intuitive thought, cognitive illusions or biases, while they may be useful short cuts can be perilous when stakes are high. It is argued that cognitive biases of overconfidence, sunk costs effect and overestimating the probabilities of recent successful events contributed to the deaths of experienced climbers in the Everest disaster of 1996 (Roberto 2002). In fact system complexity, shared beliefs at group level and cognitive factors at an individual level were all considered to contribute. The sunk cost effect is the tendency for people to escalate commitment to a course of action in which they have made substantial prior investments (time, money, etc.). An escalation of commitment has been called "summit fever" because of its analogy with the mountaineering experience – wanting to complete the goal at all odds. To overcome such biases is very difficult and certain golden rules may be required like the 2 o' clock rule (if you aren't at the top by 2 its time to turn around). Overconfidence bias is the common tendency to overestimate the likelihood of success. In addition recent successes, recent information, easily imagined events are all sources of bias which can, for example, cause errors in the diagnosis of events and lead to wrong choices. In a complex system bad choices can accumulate. This is illustrated in Pate-Cornell's (1993) post-mortem analysis of the 1988 Piper Alpha disaster highlighting bad judgements with respect to design, safety management procedures and the allocation of responsibilities, resulting in a coincidence of events delivering one of the worst offshore disasters in history.

In the interviews conducted in the resilience case studies (section 5 and Annex B Resilience Case Studies) respondents fully acknowledged the possible variation of the environment, the processes and substances they work with, as well as the organization and themselves.

> "First of all: the environment we work in is so uncertain that you will make mistakes, always, if you want it or not. you will make mistakes and – lets presume the consequences are not too grave - it is up to you to learn from it or not…The danger is not something binary. You start your course, go forward and suddenly you see 'the danger' and – hop - you turn back. The danger is torturous. It is arduous and snaky."

***

"First of all it is not necessarily present, but potentially it is there. Second there is you: you make an evaluation transposing your knowledge and experience into a particular situation. You are making an evaluation of uncertainties. Et voilà: this is our problem!"

***

"There are two main sources [of uncertainty], which are the variability of the parameters and the lack of knowledge or information. There are some things you simply don't know, of course you know it afterwards, that's for sure, but if we take Buncefield for instance – which was in 2005 - , at that time I had 20 years of experience, if you would have asked me to imagine that type of accident, I would never have thought about it. By the way a consultancy did a study; nobody thought about it. The accident Macondo , BP Texas…. Of course afterwards it's very simple to explain. Fukushima, you see this. So you have the uncertainties, simply the reality exceeds the imagination and that is true for natural hazards as well…"

***

"I do not have the illusion that we can secure everything. Our work surroundings are constantly changing, as do our projects. We still have a lot to learn. There is nothing like 100% control."

***

'These processes involve risks. They only become dangerous if you do not manage these risks in a proper way. If I would regard this working environment as dangerous, I would send nobody out there. It is a working environment with risks. And some of these risks we manage really well, and others we manage a little less well. There are always things that you do not control, but often these are the things that you do not know of.'

The acceptance of uncertainty means that they are expecting to face risks, new unknown situations they have to deal with. This makes them vigilant ('watchful especially to avoid danger'). They expect that there will be unforeseen risks. They are open for the unknown to happen. It has been said (Jean Pariès in Hollnagel et al 2011) that a resilient system must be both prepared and be prepared to be unprepared. Being constantly vigilant in an uncertain environment aims to fulfil these requirements:

"Hold each other's hand and be very vigilant not to make mistakes"

***

"Let's say that you are in a room together with a snake that moves around. And therefore you will be in a dynamic state of constant vigilance, asking yourself: from which side does the danger come? …This asks for a lot of concentration and energy."

What consequences does this have for management of personnel?

"You need intelligent people, which is not the same as people that have followed higher education. Intelligent people are people that understand that they have responsibility - for their colleagues, the company, themselves. They are people that are very 'conscious'. Self-selection goes on here in a certain way as well. It is knowledge intense. A lot of what you have to know and do can't be learned at school."

***

"One key - if you ask me – is that it is important to not feel and act like 'superman'. Pay attention to doubt and humility. These things will bring in another way of thinking, other perspectives into the world of enterprises. We often only think in a box like this and you really have to open up this box, be as open as possible. Look in three dimensions. Not only below and above but also right and left. This will make you more competent to deal with risks. But if you are head of a nuclear plant, it would be a pity to wait for an accident before starting to learn. No, you have to be constantly alert, which is extremely difficult. Also in the mountains. In the mountains your vigilance is also killed by routine, habits, repetition of movements.

***

> "…you always have to think three times and do a last minute risk assessment and be sure that you do the right things. But this is a core value of working in the industry. And the same core value goes for driving a car. For sitting behind your desk almost. Alertness and consciousness are always important. Doing things on auto-pilot has risks attached."

Some interviewees described how they were trying to think ahead and anticipate future situations by thinking through scenario's, using their vast experience and constantly cross checking with the current state. They try to manage uncertainties by using what has been called anticipatory thinking. Anticipatory thinking is the process of recognizing and preparing for difficult challenges, many of which may not be clearly understood until they are encountered. It has been defined as a future orientated form of sensemaking (Klein et al 2010). This kind of anticipatory thinking requires a high level of experience: it is mandatory that a lot of situations been 'lived through' before large pattern repertoires are build up. With these pattern repertoires effective pattern matching can be conducted leading to problem detection if something is not right. Or anticipatory thinking will enable people to get 'ahead of the curve': noticing and extrapolating trends.

> "It is all about being able to make a picture in your head how the day will develop and prepare yourself. And the very moment that there is a change, you will have to rethink everything. For example: your client is not as fit as he was the day before; the weather is changing; there is another party ahead of you in the route. These changes do not necessarily mean that you will have to stop and go back. But you have to note it and take it into account for the rest of the day. And if there is another change, you also have to take this into account and review you objectives."

***

> "… this is something I have developed during all my years of training and working experience - we learn to detect on four dimensions: all different directions but also going forwards in time. During the years you get better and better at this. Certainly with high end clients you are investigating every minor detail in the process. For example: when you are going to work on a platform at sea and will be flown in by helicopter you will have to think through every step in the process: I am putting my equipment into a container. what is in my equipment (no dangerous goods?), will it be light enough to take out of the container and hand-carry, is it well secured so that it will not immediately fall out of the container when this is opened? This is something you have to learn, you have to gain experience and you have to be open for it. It is like a film in your head. The more you can really foresee the things that are going to happen, the more you can prevent or prepare for the risks."

Anticipatory thinking and especially pattern matching may however carry important dangers with it: people may wrongly extrapolate the one experienced situation to a new situation, while trusting on their 'experience'.

> "There is the influence of 'the objective' that we have in the mountains. First you are aiming for a certain route or summit and at a certain point the bad weather is coming in. you will say: "Damn! They did not announce this!" But you will turn back and go down - still doubting a little bit. When you are down in the valley, the clouds all disappear. When this happens a number of times, you will be extra focused to proceed – But will it be a good idea to push on? No, not according to me. The probability that something will happen to you is identical to the first time you attempted to go to the summit. Also when you denounced nine times with doubtful weather and nothing happened, and now it is the tenth attempt with the same kind of weather and you decide to go for it the same uncertainty remains. The nine experiences you have had before, will not help you in fact to make a good decision!' (from Annex B Resilience Case Studies).

This is one of the reasons why Langer (2000) and Weick, Sutcliffe and Obstfeld (1999) suggested that mindfulness is important for risk management and decision making under uncertainty. Mindfulness can be described as a state of present-moment awareness. This very much relates to the characteristic of 'real vigilance' as described by various respondents. Anticipate varieties and be prepared for the unexpected has – according to several interviewees – a lot to do with focusing on details and doing as much as possible right. By doing this, people state, you will at least have the best playing cards in case the unexpected happens or mistakes are made. The underlying view is that (major) accidents are often a constellation of things going wrong or in bow-tie terms barriers that did not function or were not put in place. The probability to arrive at an accident diminishes when as much as possible is done right. It is not for nothing that combat soldiers are

trained to be very disciplined in maintaining their equipment (including themselves) in the best possible state. This characteristic or attitude has a lot in common with the things done in preparing for the expected, but the underlying motivation is focused on the inevitable unexpected.

4 BOW-TIE AND BARRIERS

4.1 The resilient success bow-tie

A central question in the overall research project is whether resilience concepts can be integrated into classical bow-tie approaches. The classical bow-tie is a linear model with a focus on the negative, the already occurred or foreseen accidents. The bow-tie provides a structure of the controls in place for preventing the release of a hazard in a particular context, particularly the more dangerous hazards that can result in catastrophic consequences. Its lessons are avoidance of failure through better controls. Resilience modelling is a mirror of this. It is about being proactive rather than reactive in the face of uncertain outcomes, about anticipation of the future and about success as a bouncing back in the face of adversity as opposed to avoidance of failure. In this respect the bow-tie could also be used to model risk control in a way that could be used proactively rather than reactively. For that purpose, new resilient components are needed.

Bow-tie models are usually used as instruments to represent defences and threats and to analyse the causes and effects of incidents, particularly in risk assessment. They are graphical representations of how deviations can develop into a single critical event, and how the critical event can develop into different consequences, and showing the barriers along each line of development that can abort these developments. Normally the bow-tie focuses on failures of these barriers and so to a loss of control rather than the positive ways in which people contribute to the good management of the barriers and containment of the risks. The current research project investigates whether success can be modelled in the bow- tie. The results of case studies (section 5) feed into the process of designing success components which are attached to the safety barriers in the bow-tie.

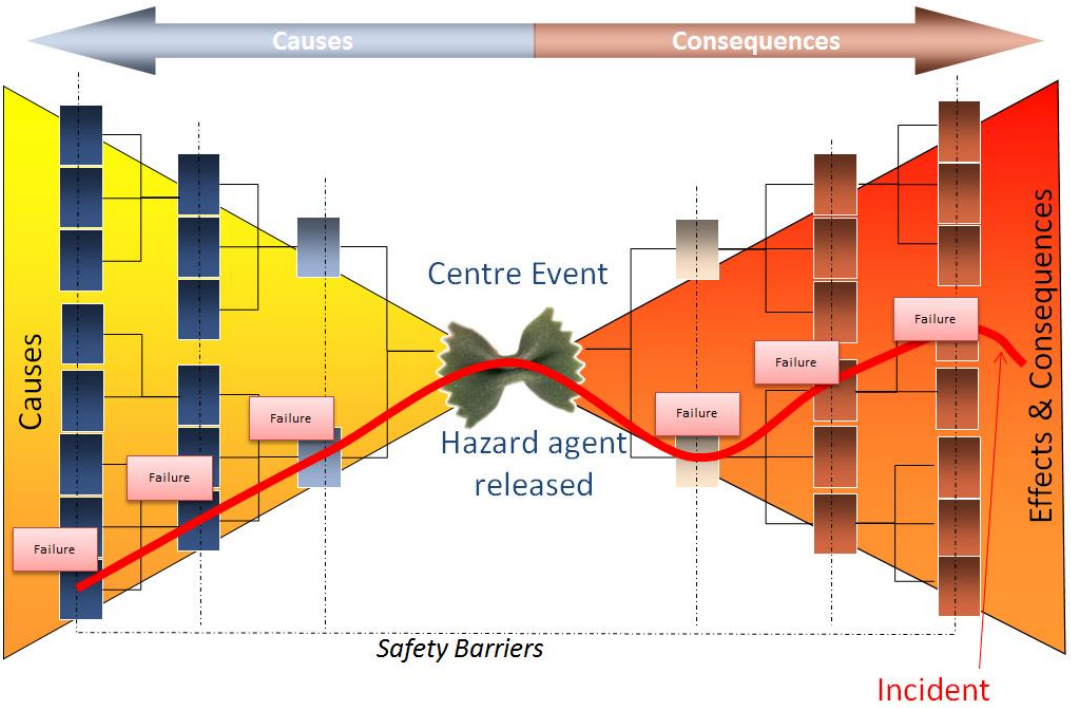


FIGURE 3 BOW-TIE OF SAFETY BARRIERS SHOWING BARRIER FAILURES RESULTING IN AN INCIDENT

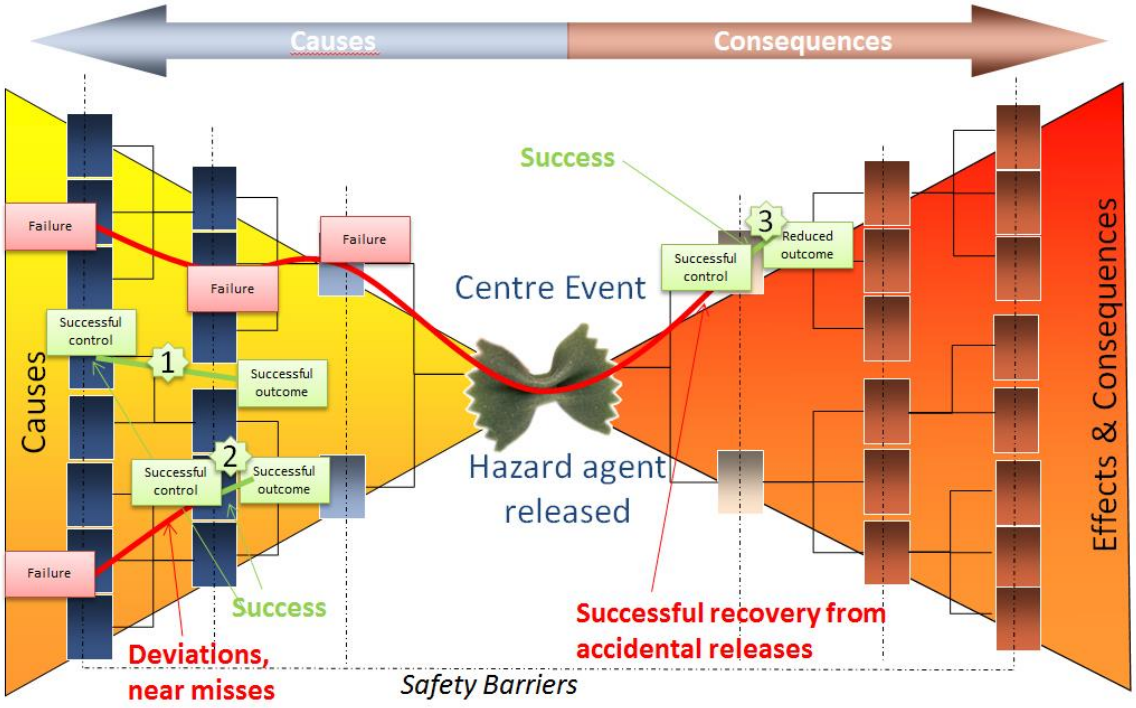


FIGURE 4 BOW-TIE OF SAFETY BARRIERS SHOWING BARRIER SUCCESS WHERE 1 = SUCCESSFUL CONTROL OF CONDITIONS (NO BARRIER FAILURES), 2= EARLY RECOVERY OF BARRIER FAILURES, 3= SUCCESSFUL LIMITATION OF EFFECTS OF A RELEASED HAZARD

Bowties are based on the concept of preventive and protective (safety-) barriers and other key concepts which are described below.

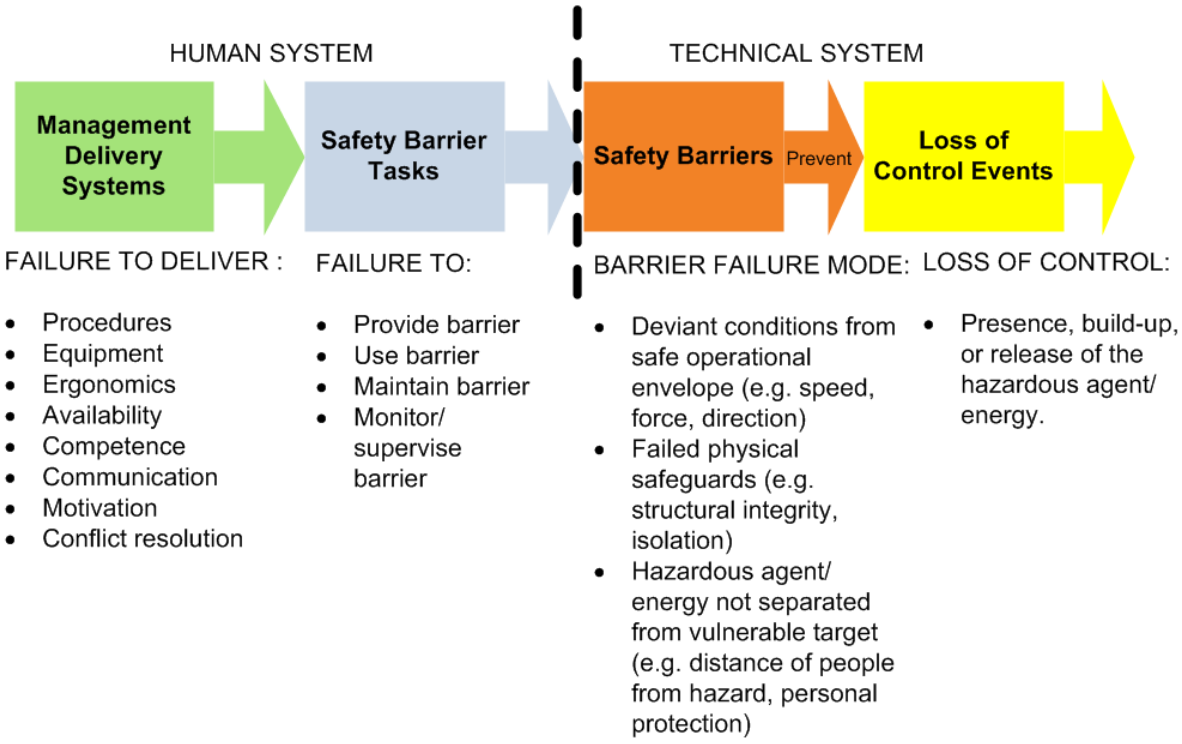


FIGURE 5 STORYBUILDER BARRIER MODEL

Barriers are (at the sharp end) interventions that prevent the realisation of a hazard (or critical event), or mitigate the consequences of the realisation of a hazard. In many representations planned activities like inspection and testing also appear as "barriers". In the Storybuilder™ model the barrier itself is distinguished from the human and organizational factors which are not called barriers but are part of the barrier management system as shown in Figure 5 (Bellamy et al 2013).

Safety Critical Activities are the planned activities that are (or should be) performed in order to ensure that the equipment that may cause deviations or threats are in good condition. These activities are sometimes included as real "barriers" (See Sklet 2006 for general classification). These activities include design, inspection, testing, preventive maintenance, but also activities that shape human performance, such as training and development and maintenance of procedures. These activities are detached from the appearance of deviations (e.g. design will have taken place in the past), but they affect the possibility of successful intervention in the (near) future.: In the Storybuilder model safety critical activities (undertaken by people) are attached to the barrier as barrier tasks. Training, procedures etc. are attached to barriers as delivery systems to the tasks of providing, using, maintaining and monitoring.

Threats, deviations or *initiating events* are the starting point at the left-hand side of the bow tie that, if not prevented and mitigated, will lead to bad consequences. In the Storybuilder model these are prevented by the first line of defence of operational control. If this line of defence fails there is a second line of defence recovery system comprising Indication, Detection, Diagnosis, Decision and Response. This IDDDR concept is further dealt with in Section 6.1.

The *hazard, critical event or centre event* is the pivotal central event in the bowtie (in process industry typically a "loss of containment" event) where the hazard agent is released and can lead to a range of bad consequences if not recovered in time. Another way of looking at this is to say that the system begins losing "requisite variety", the necessary flexibility to deal with the variation in the system. This is a reflection of "Ashby's Law" (Ashby 1957): the larger the variety of actions available to a control system, the larger the variety of perturbations it is able to compensate. Jackson (2010) rephrases this as: "The more ways you have to make a system resilient, the more resilient it will be." The heuristic law is: Provide as many opportunities for accident avoidance, survival and recovery as you can.

Consequences are the descriptions at the right hand side of the bow-tie. Consequences can either be described as physical events of varying severity (fire, explosion) or as a description of the final consequence for human life and health (fatality, injury), and damage to (natural) environment and assets. Elements that normally are not included explicitly in bowties are the organisational processes and qualities that affect the success and quality of the Safety Critical Activities. In the I-Risk (Bellamy et al 1999) and ARAMIS projects (Andersen et al 2004; Salvi 2014) they were called "delivery systems", i.e. the management processes that ensure proper design, inspection, training, communication, man-power allocation, etc.

It is essential to acknowledge that bowties are the outcome (or part) of a prospective risk analysis, i.e. the outcome of a process to anticipate possible hazards, threats and consequences. A good risk analysis is a risk analysis that, using best available knowledge and experience, provides a complete overview (anticipation) of possible hazards, threats and consequences, eventually ordered using some parameter(s) expressing "risk", where risk is some function of the severity, the likelihood and/or the uncertainty of the consequence. However many discussions of resilience emphasize that not all threats and hazards can be anticipated, and that *resilience explicitly should address the capabilities that are in place to deal with unknowns*. In principle, this idea should form the basis of a resilient bow-tie. Due to the nature of complexity, the 'amount' of complexity in the system of analysis, threat and hazard analysis will be incomplete. The design and implementation of adaptive capacity is a way to increase resilience of the system to unanticipated threats. The ability to anticipate when and how calamity might strike has been called 'requisite imagination' (Adamski & Westrum, 2003), the ability to imagine key aspects of the future and anticipating what might go wrong.

A resilient bow-tie, being comprised of barriers, requires resilient barriers. This raises a number of questions:

- What characterises a resilient barrier? Perhaps a resilient barrier is amenable to IDDR Are there adequate **I**ndications in time? Can they be **D**etected and correctly **D**iagnosed and the right **D**ecisions made? Is **R**esponse possible? An IDDR component could be added to every barrier, focused on the human intervention which is the subject of the current study, or included as a generic component that applies in the same way to every barrier. This is further discussed in Section 6.1.

- Is it possible to characterise the resiliency of a whole bow tie, in the sense that barriers are placed at various levels of organization across the bowtie, allowing interventions at different stages? This is discussed in Section 6.5.

- Is it possible to include unanticipated barriers in the model? Although this seems illogical, perhaps is would be possible to anticipate the unanticipated by having "spare intelligence" a capacity to adapt the barrier function to the required threat. In principle, resiliently engineered barriers need effective adaptation which requires the four resilience cornerstones mentioned earlier anticipate, monitor, respond, learn. Can we thus put requirements on the system (e.g. the possibility of human intervention, system feedback, coupling) to allow for the unanticipated? E.g. (from Annex B Resilience Case Studies).

  "This same day one of my other colleagues had the same sort of issue at a different site. He also had to climb out of a tank through a very narrow man hole. He didn't feel good about it at all. That evening we talked on the phone and decided that we would stop immediately and go back and do some training on these kind of problems first. So we built some mock-ups to gain experience. We built 'man holes' and started training." Lead engineer industrial rope access and maintenance.

- Can some anticipated safety critical activities be made more "resilient" than others, and what characterises resilient safety critical activities? These activities could be the ones that support recovery, renewal and regeneration. E.g. good planning improves the chance that deviations are spotted:

  "We will never do something 'quick and dirty'…..sometimes this means a conflict with the client. Procedures force us to take time to think. We never start a project before we have a plan written down - method statement, a JSA/TRA (Job Safety Analyses/ Task Risk Assessment) - a kick off meeting with the client and third parties, every day we will organize a daily organizational meeting: did something change in the environment? What did we learn yesterday? All these aspects will be spoken through. This is something we do very seriously, everyone has to sign up to this." Lead engineer industrial rope access and maintenance.

- How can unanticipated safety critical activities be incorporated? These would typically be interventions at operational level to correct or to improve primary processes and safety barriers in response to new (or newly recognized) threats. How can the organization promote incorporation of those activities when the need appears?

  "These are moments in which things are different. You have to take action, take process-measures, which we call guidelines, no prescription! Guidelines because they define measures which you could take, but nevertheless you have to look at each situation as a whole. It is very difficult to define rules which you cannot foresee. It is better to work from principles, than from rules." Manager blast furnaces.

Suggestions of requirements from interviewees (Annex B Resilience Case Studies) included detailed planning; sticking to the plan, attention to deviations from plan, listening to your people and having a special type of people.

At the level of *delivery systems* (see Figure 5) the following interventions would implement resilience:

- Correcting safety critical activities when detecting flaws or in response to new conditions and requirements. This is part of the continuous improvement cycle of the delivery systems. It requires learning (from own and others' experiences) and monitoring of performance and (changes in) operational conditions.
- Adapting the bowtie (including new threats, adding new and replacing old barriers) in response to new conditions and requirements – this is part of the continuous improvement cycle of risk analysis. It requires learning (from own and others' experiences) and monitoring of performance and (changes in) operational conditions.
- Monitoring the "resilience" of the system and making improvements to it.
- Flexibility (available options) in being able to allocate resources where they are needed. In railway maintenance time is a critical resource because of the enormous pressure to keep going. Having time is a critical property of resilience because of the need for reflection. This property could be made explicit in the success bow-tie whereas excessive workload and fatigue must surely be the enemy of resilience. Thinking in terms of levels in the organization and management system, for simplicity two levels (nested systems) could be considered. The management level should monitor the operational level but multiple perspectives are needed; that means getting rich data out of the operations. That data should be monitored for patterns and critical events on an ongoing basis (but differently different from a preconceived checklist. The monitoring system as an aspect of the safety management system is discussed further in section 6.7.

4.2 Resilient intervention.

"Resilience" is implemented through the possibility of intervention (see also section 2).

> "the intrinsic ability of a system to adjust its functioning prior to, during or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions" (Hollnagel et al 2011).

> "The ability to make adjustments prior to an event means that the system can change from a state of normal functioning to a state of heightened readiness before something happens. A state of readiness means that resources are allocated to match the needs of the expected event, that special functions are activated, and that defences are increased. A trivial example is to batten down the hatches to prepare for stormy weather, either literally or metaphorically." (Dekker et al 2008).

Section 2.4.2 lists four main capabilities of resilience: (to Respond, Monitor, Anticipate, Learn). DTU have converted this into a model of the resilient intervention (see Figure 6) and which is further elaborated in Section 6.1. Central to the model is the notion of situation awareness (Endsley 2000), which combines the perceptions of the present state of a system with how the system arrived at that state (long and short term history, recalling previous states and actions taken) together with the ability to forecast the possible development of the state of the system in future.

If necessary, the agent should act on the situation, being able to forecast how the system will respond to his action and how it will affect the future state. This actual intervention demonstrates the final resilient capability of the agent.

Monitoring supports the situation awareness, providing:

- The possibility to read signals that indicate the present state and trends into the future state of the system;
- Feedback on the actions taken

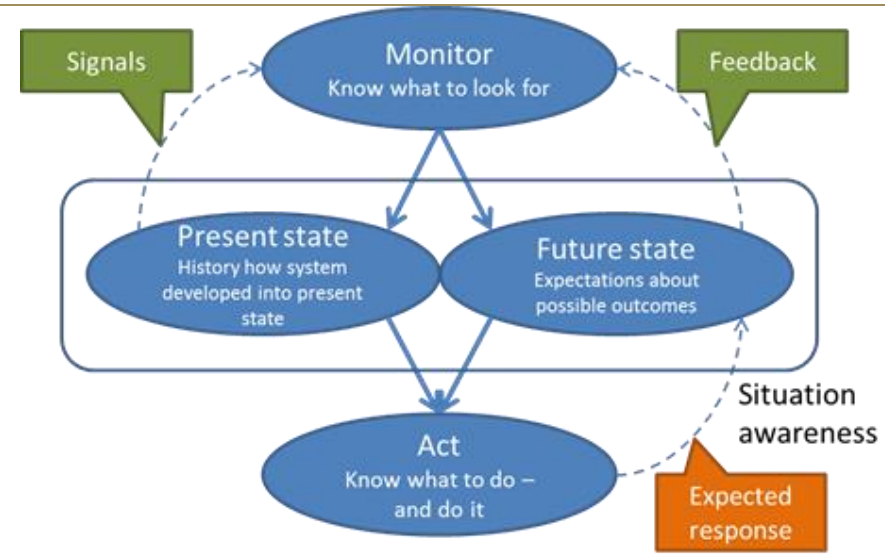


FIGURE 6 GENERAL MODEL FOR AN INTERVENTION THAT PROMOTES RESILIENCE

One can consider what affects the four capabilities – this is illustrated in Figure 7 as "enablers" for each capability in the intervention model. Monitoring requires that the agent (individual, team or organization) is curious to collect information, inquisitive, i.e. searching for information, critical about signals popping up, and attentive (mindful) to signals and situations.

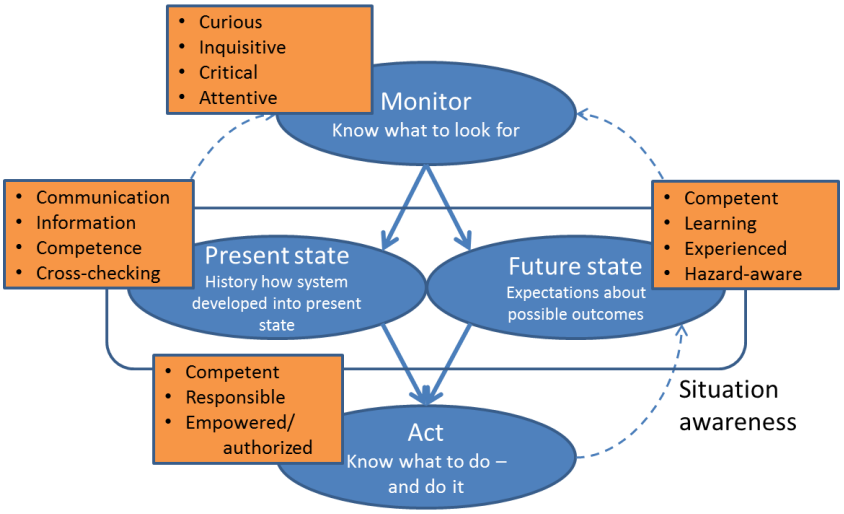


FIGURE 7 ENABLERS FOR RESILIENT INTERVENTIONS

A correct perception about the present state requires free communication about actions and considerations between agents, providing information about the system and its environment. One can think in terms of delivery systems or in terms of barrier systems (Note: systems and not physical units in the world).The agent should be sufficiently competent, i.e. having sufficient knowledge of the system and its environment, to transfer the available information into a sufficiently accurate understanding or perception of the system, and the agent should challenge that understanding by cross-checking with information from and perceptions of other agents.

Competence is also required to forecast the possible future states based on the perception of present state and observed trends in monitored signals. Learning and experience from previous events also contributes to a correct assessment of potential developments. Last but not least, the agent should be hazard-aware, i.e. being able to imagine the safety-related consequences of the potential developments.

Taking proper action also requires competence, knowledge to recognize alternatives for action and being able to forecast the effects on the system, or at least to know, on the basis of feedback from the system, how to find out how the system reacts and conclude whether it was the correct action. The agent should have and take the responsibility to act, but it should also have, or have been given, the authority to act.

Providing the enablers would be part of the "delivery system" of an organization, i.e. the organization should ensure that agents (individuals, teams, the whole organization) are curious, attentive, critical, competent, empowered, mindful, probing.

4.3 The concept of success

DTU's Risk Research group has earlier used "functional modelling" for describing systems, with the aim to perform hazard identification at an early design phase. For this they made use of the well-known "ICOM" blocks (Input-Control-Output.Method) as used by SADT (Marca & McGowan 1988). DTU found it useful to add an extra concept of "Constraints" to this block, which typically indicates that the function is to be performed within restrictions of (typically) safety and environment as shown in Figure 8. This also acknowledges that safety (for most operations) is not a primary goal on its own, but a necessary condition. In other words, if the safety constraint is not met, there is no success.

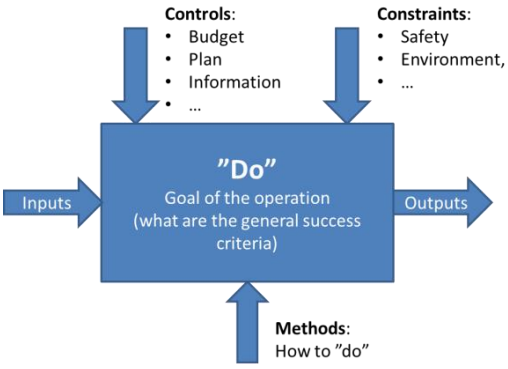


FIGURE 8 ICOM-BLOCK WITH CONSTRAINTS (DTU MODEL)

In the I-RISK project (Bellamy et al 1999) a SADT model was used to determine the management system requirements (Guldenmund et al 1999) where Resources rather than Methods and Activities rather than "Do" were used in the SADT model (Figure 9). In this respect the central block is a process. The FRAM model of Hollnagel (2006, 2012) is also based on SADT and comprised of process blocks (Figure 10).

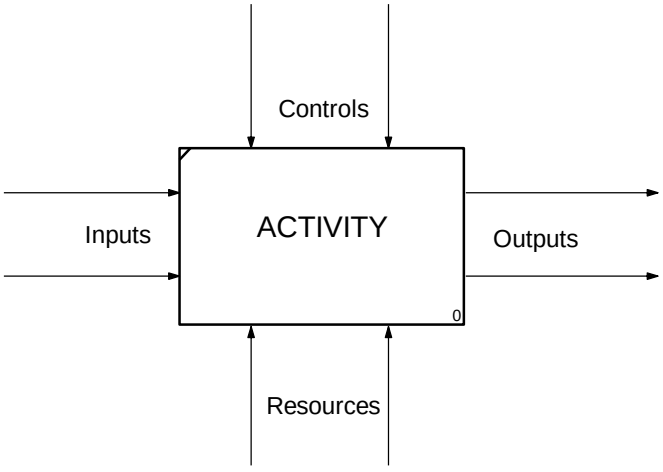


FIGURE 9 SADT MODEL USED IN I-RISK (GULDENMUND ET AL 1999)

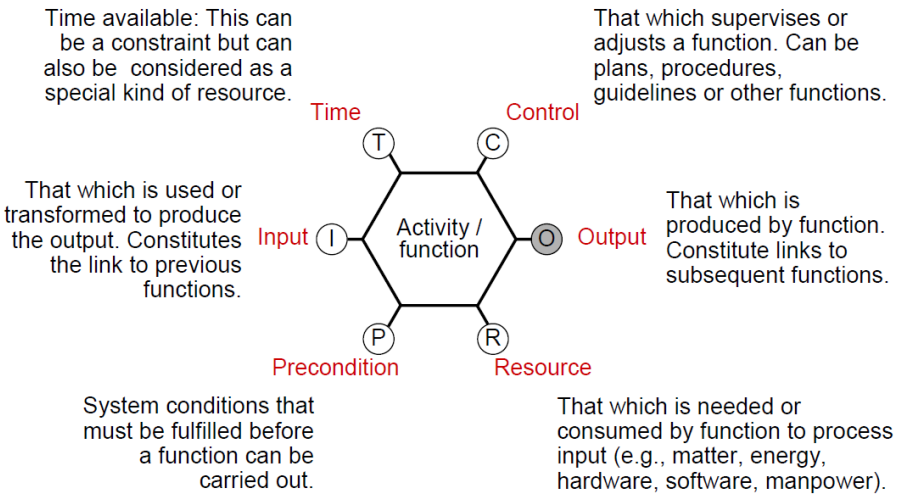


FIGURE 10 FRAM MODEL COMPONENT (FROM HOLLNAGEL 2006 – PRESENTATION: CAPTURING AN UNCERTAIN FUTURE

Resilience addresses success in a broad sense, so it should contain all the activities leading to success. The consortium agreed that the present project is limited to safety, but Figure 8 shows, that there is no success (in the broad sense) without successfully handling safety, like getting to the top of the mountain AND getting back safely.

> "There is this side of exploring which people hardly understand. People earn prizes and get applause. But they get applause for risking their lives. If you look at the stories of the first great explorers, people that tried to fly around the world or got to the poles, a lot of them lost their lives. And they or the survivors have been honoured in all kinds of ways. At the same time society doesn't like risk taking. We want to reduce the risk to zero which is impossible." Solo mountaineer (from Annex B Resilience Case Studies).

Fulfilling the constraint of safety may however require resources or in other ways be in conflict with the aspects that promote success. So safety is not something that is maximized (which would be equivalent to making safety the ultimate goal of the operation), but a balance has to be found where sufficient margins are maintained to avoid damage (damage demonstrating lack of safety), while the main goal (e.g. financial profit) is maximized within, but often on the edge of, the safety envelope (Rasmussen, 1997).

> "Yes, I still climb an easy pitch without belaying myself. But that is something that is inherent to the job of being a guide. You cannot spend all your time on belaying – putting in Friends, pitons etc - when you are in the mountains. Otherwise doing a route will take you three days. You have to be fast as well. So partly this can be regarded as *bêtises* (stupid, foolish things). It is integrated in the job……. And also it can happen that I take care very well of all my clients but I forget myself. For example when I am climbing a ridge with clients. Because I focus on my clients, I forget my own safety…That I understood after my second big fall: I was mentally totally with the person that had to start climbing and I reckoned that I myself was not part of 'the problem'. I was not into it." Mountain Guide (from Annex B Resilience Case Studies).

Viewing safety as a constraint for success, but not being the only criterion for success, means that we cannot invert the fault tree for failure, and by that get the success tree for real success, because the fault tree for failure (a safety incident or accident) does not include all success criteria. The success tree only tells us what is needed to avoid a safety incident or accident, and does not include more information as a fault tree (see Figure 11).

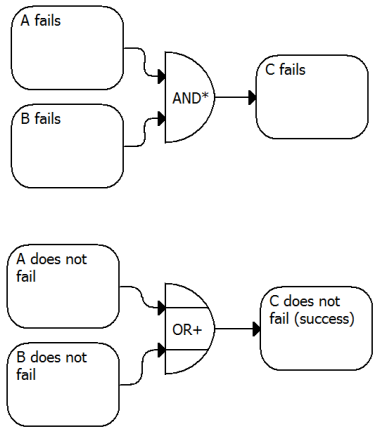


FIGURE 11 INVERSION OF A FAULT TREE INTO A SUCCESS TREE DEFINES ONLY FAILURE AVOIDANCE

The relation between "safety margins" and damage can be treated deterministically or probabilistically. In a deterministic approach, "sufficiently safe" would mean that no damage will occur, i.e. neither foreseen nor unforeseen events will be able to push the operation into causing damage. In a probabilistic approach, no state is considered absolutely safe, and "sufficiently safe" would mean that the probability of damage, due to foreseen or unforeseen events is (perceived to be) so low, that this is acceptable (the risk is accepted). It does not seem relevant at this point to promote either the probabilistic or the deterministic approach. Operators at the "sharp end" are not expected to perform probabilistic assessments, but management may. Note that there may be a mental difference between avoiding the risk and keeping on the safe side.

4.4 Does everyday success provide evidence for resilience?

The discussion on resilience has put success as the prime interest rather than failure (or mere the avoidance of failure). Nonetheless on the whole we do not expect to learn from everyday successes (see Annex B Resilience Case Studies). However, monitoring 'everyday work' could evaluate the gap between 'work as imagined' and 'work as done'. This is useful to reduce surprise in the event of change. Every day successes are mainly (most days) based on *routine*, and as long as there are no events that challenge the routine, the routine needs no adjustment. One may expect explicit resilient behaviour when people or organizations perform operations that they do not *perceive* as being routine. In those cases people will monitor and cross-check their own actions and system responses (which can be as simple as asking a supervisor), and adjust action. Routine is both good and bad. The good thing about routine is knowing (with limited cognitive effort, i.e. fast, based on skill) what to do in situations that are regularly met. The bad thing is that by application of the ETTO (Section 2.4.3) one can become blind for indicators that may tell you when routine no longer applies.

> "I think that we could become 'sloppy' if we would always do the same, for example washing the windows of the same high building every month, year after year. It is in our advantage that we always have new and different projects. This is also part of the law: repetitive work should not be done by rope access workers". (Annex B Resilience Case Studies).

4.5 The reasoning and hypotheses of resilience engineering

The following issues are the basis for Resilience Engineering:

1. Complex systems may produce states (outcomes) that cannot be predicted on the basis of analysis of the individual components or subsystems. Complex systems have emergent properties that cannot be derived from the individual components or subsystems alone, so traditional risk analysis fails to predict all failure modes.

2. The dynamic environment may produce conditions for the systems' functioning that cannot be foreseen, so traditional risk analysis fails to predict all external disruptions.
3. Traditional accident and incident analysis methods fail to reach consensus on causes: considering failures as resulting from linear cause-consequence chains is a fallacy. The notion of "human error" is problematic, this can be considered a special case of this argument.
4. Humans and human organizations show the ability to adapt to internal and external disruptions, also if these disruptions are not foreseen; these adaptions emerge from the system, i.e. they are not designed or planned. These adaptions show a capability of (resilient) systems to cope with problems arising from issues 1) and 2) above.
5. Building on the observation in 4), there is a need to understand the properties of a system that support those beneficial adaptions to internal and external disruptions, in order to enhance the adaptive capabilities.
6. Some high reliability organizations have reached a plateau of reliability (5.10^{-7} disasters per operation?); further improvement requires a new approach.
7. Safety is an emergent property of the system which is not the same as (measuring) the absence of accidents and incidents.
8. The mechanisms for failure of humans and human organizations are the same as the mechanisms for success. Accidents do not represent malfunctioning of normal functions, but failure to adapt the normal functions to changed conditions.

4.6 Safety barriers, interventions and resilience

Resilient interventions, in the sense of "adjusting the system (prior) to an event" can happen throughout the system or system levels. In terms of bow-ties, two levels can be discriminated:

- Interventions at the "sharp end", i.e. "real" (resilient) barriers preventing/mitigating accidents. These are Safety Barriers and factors affecting their condition, the so-called PIEs- Probability Influencing Entities - according to the RIVM (2008) risk model.
- Human interventions and management of resources supporting the operation and supporting the sharp end (real) barriers. These are Barrier tasks and Management Delivery Systems in Storybuilder™ terminology (RIVM 2008).

Normal (foreseen) safety critical systems will include predefined safety barriers, i.e. barriers designed or planned to intervene by hardware and procedural action to anticipated potentially hazardous states of the system. This can be presented in a scenario-like way in a safety-barrier diagram see Figure 12, made using SafetyBarrierManager (2015) - see the legend at the end of this section, Figure 19.

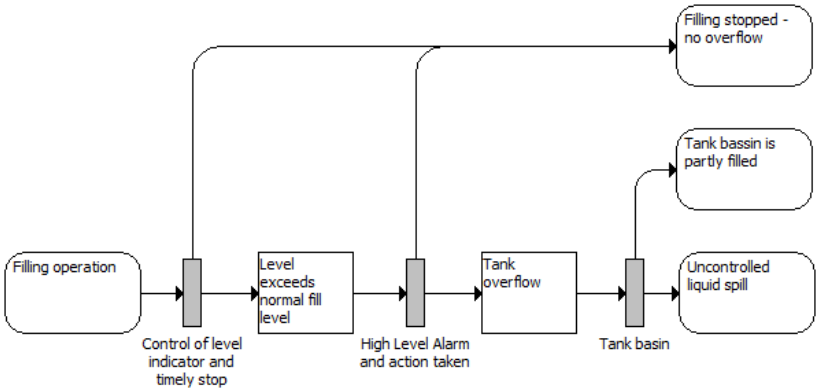


FIGURE 12 EXAMPLE OF A SAFETY-BARRIER DIAGRAM

Within the resilience community, there might be some opposition against this analysis, because it suggests a very linear cause-consequence relationship. One should note however, that each barrier "node" does not address so much cause-consequence analysis, but it demonstrates that when a certain, potentially dangerous, condition arises, there is a need for an intervention, as in the "node" in Figure 13.

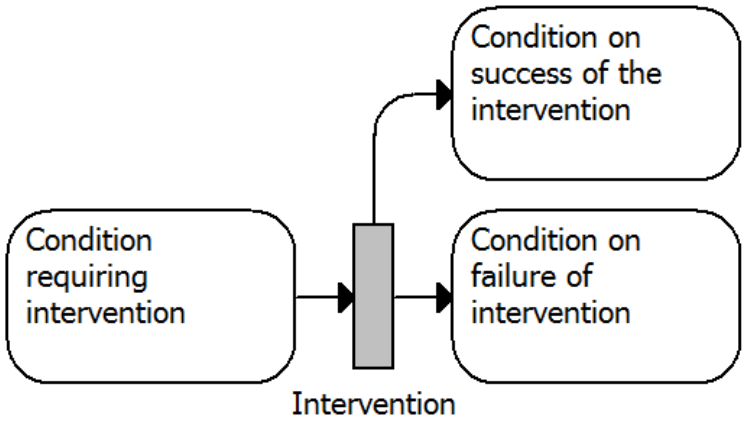


FIGURE 13 BARRIER "NODE": THE INTERVENTION IS A RESPONSE TO A CONDITION, AND DOES NOT CONCERN THE CAUSES OF THE CONDITION

Note that the condition on failure of the intervention may be marginally the same as the condition requiring intervention, apart from the knowledge that the intervention failed.

The scenario in Figure 12 shows the most likely (anticipated) pathway to the potentially dangerous condition, but the barrier node itself is not concerned with how that condition arose, so an intervention will be triggered whatever the cause of, or pathway to, that condition. E.g. the high level alarm will also respond to another reason for high level in the tank, e.g. return flow (although another action than during filling would be required), and the tank basin will capture any spill from the tank. This probably shows a property of a resilient barrier system, i.e. barrier interventions are possible throughout different states (levels of danger), and interventions would be effective for the triggering condition, irrespective of how the triggering condition arises.

The diagram in Figure 12 shows anticipated, scheduled barriers. The risk analyst has identified potentially dangerous conditions, and interventions have been designed, actions to be performed by hardware or by human operators, that are reasonable in order to manage those conditions. Although these barriers are not necessarily considered to be "resilient", most of these barriers (if not all) contribute to the resilience of the system.

Jackson (2010) states that systems with many barriers are more resilient than systems with less barriers. This can be questioned. Resilience would depend on how the barriers are "distributed" as discussed above, and too many barriers may lead to complacency and risk compensation or homeostasis. Is there a maximum number of barriers, above which safety no longer increases because of those effects, or safety even decreases, because people no longer respond to signals, and the attitude of complacency becomes a common cause factor of barrier failure?

Resilience is about the possibility to adapt to deviations, with a focus on adaptations that are not foreseen or purposely built into the system. A resilient safety barrier can be considered to be an intervention in the system to return to a safe condition, Figure 14, or to take the system to a new state that is safe, Figure 15.

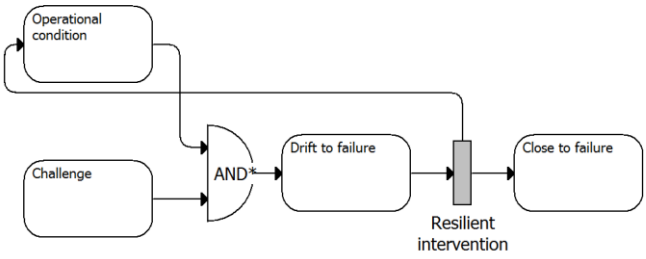


FIGURE 14 INTERVENTION RETURNING TO SAFE OPERATIONAL CONDITION

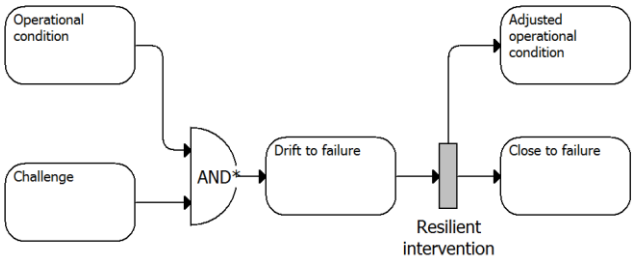


FIGURE 15 INTERVENTION LEADING TO A NEW SAFE OPERATIONAL CONDITION

All anticipated barriers will in principle return to a pre-existing, anticipated condition, and this is useful if the challenge is temporarily. If the challenge persists, a successful intervention will necessarily lead to a new condition that can handle the challenge safely during normal operations.

Figure 16 shows a typology of safety barriers (Duijm 2013), a further development of the typology from the ARAMIS project (Andersen et al 2004). This typology has been developed to support the structuring of anticipated barriers. This typology includes 3 types of interventions requiring human actions. The first two are responses to anticipated situations, where the action that is expected to be successful can be prescribed (using an oral or written instruction or procedure). The last type "Knowledge-based human intervention (ad hoc)" has been added as a "last resort": it is included for completeness, but seldom used in risk analysis (except for "emergency response", a last resort in many risk assessments) as risk analysis deals with anticipated conditions, and thus anticipated successful responses. Unanticipated interventions are by definition of this last type, as no prescription has been designed. If "resilient barriers" mainly have to be understood as unanticipated, human interventions, then they are knowledge-based.

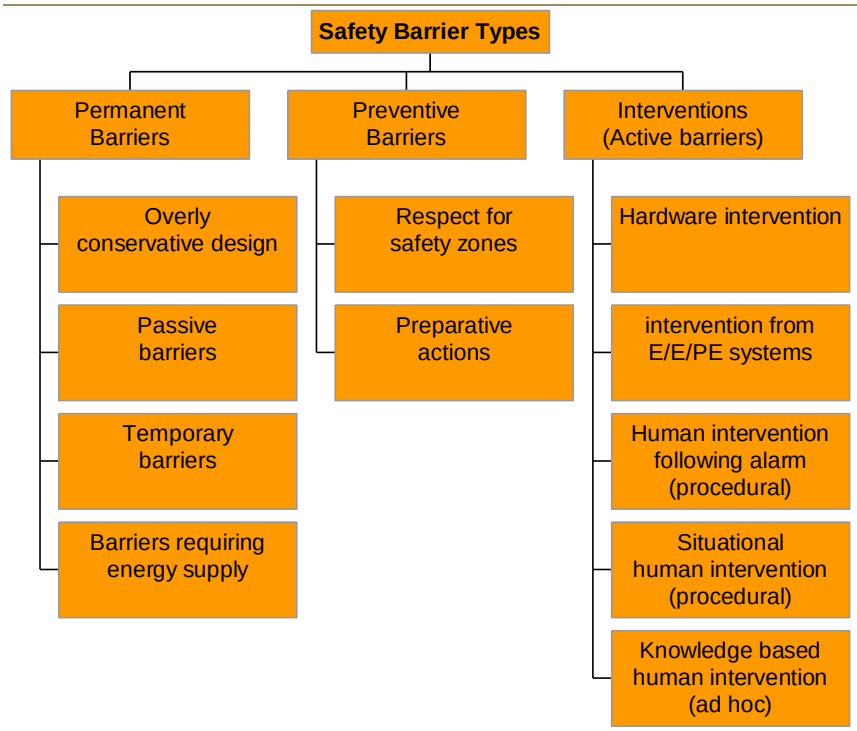


FIGURE 16 BARRIER TYPOLOGY, FROM DUIJM 2013

For the knowledge-based, human intervention on a safety barrier to be possible or successful, the system should fulfill some requisites:

- The system should allow for manual operation, i.e. it should be possible to overrule automatic control at various states of the system;
- The system should provide essential information about its state (or the state of its subsystems) to the human operator in order to enable the operator to make reasonable assessments of the state of the system;
- The development of the system should be sufficiently slow, so that human operators have the possibility to collect and interpret information, to hypothesize and validate assumptions on the system's state, and to develop strategies for intervention. For complex systems (e.g. nuclear power plants) it might require in the order of an hour to arrive at a decision. For comparison, deployment of an emergency or rescue team (typically a "knowledge-based" barrier in risk assessments) typically requires 10 to 30 minutes, depending on the situation.

In principle it is possible to consider an unanticipated intervention for every identified hazardous situation. This corresponds to including the possibility of a "resilient" barrier parallel to the anticipated barrier. This would indicate that, as in the example, Figure 17, the operator has access to other information than only the level- control or high level alarm, to initiate an action. This is an awkward way of displaying, because the resilient interventions would not be triggered at the same time as the anticipated interventions: the "resilient" interventions would depend on more continuous situation awareness, and cover the whole scenario on a more holistic level. This is depicted in Figure 18 suggesting that the operator is open ("mindful") for process deviations becoming clear by indicators other than the level indicator or LAH (which can be faulty), and take appropriate action.

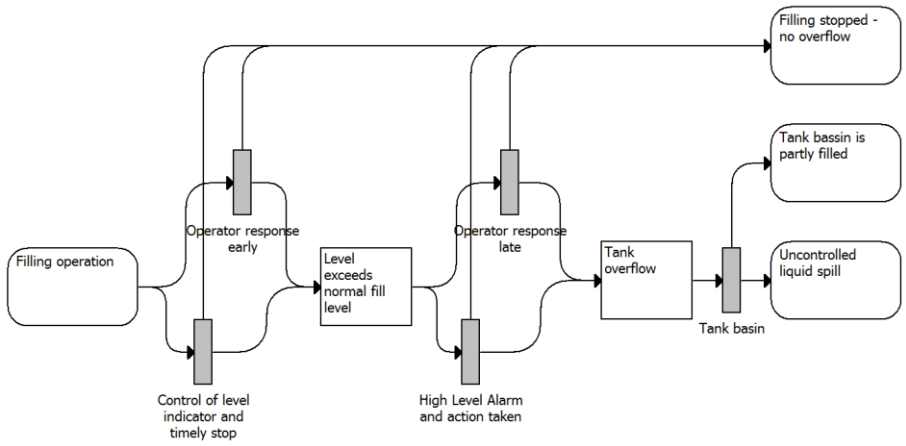


FIGURE 17 PARALLEL "RESILIENT" INTERVENTIONS TO THE POTENTIALLY DANGEROUS CONDITIONS

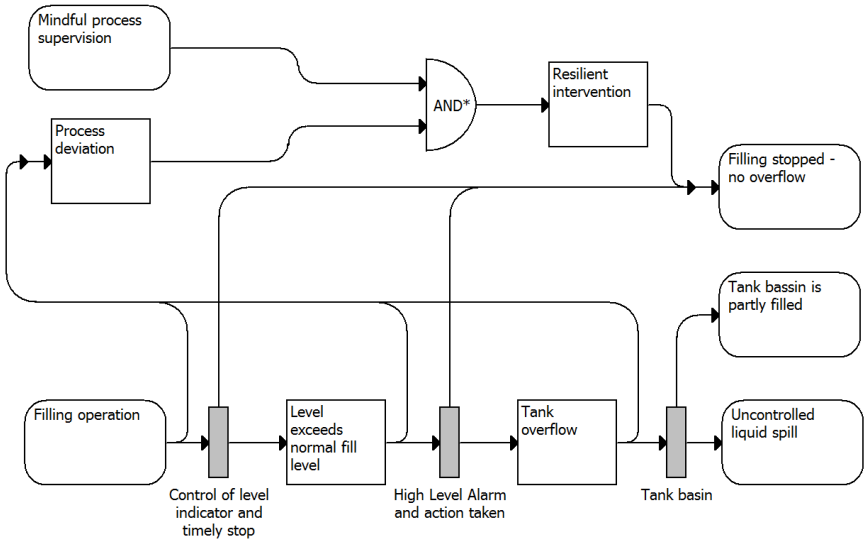


FIGURE 18 RESILIENT INTERVENTIONS INCLUDED AS MINDFUL PROCESS SUPERVISION

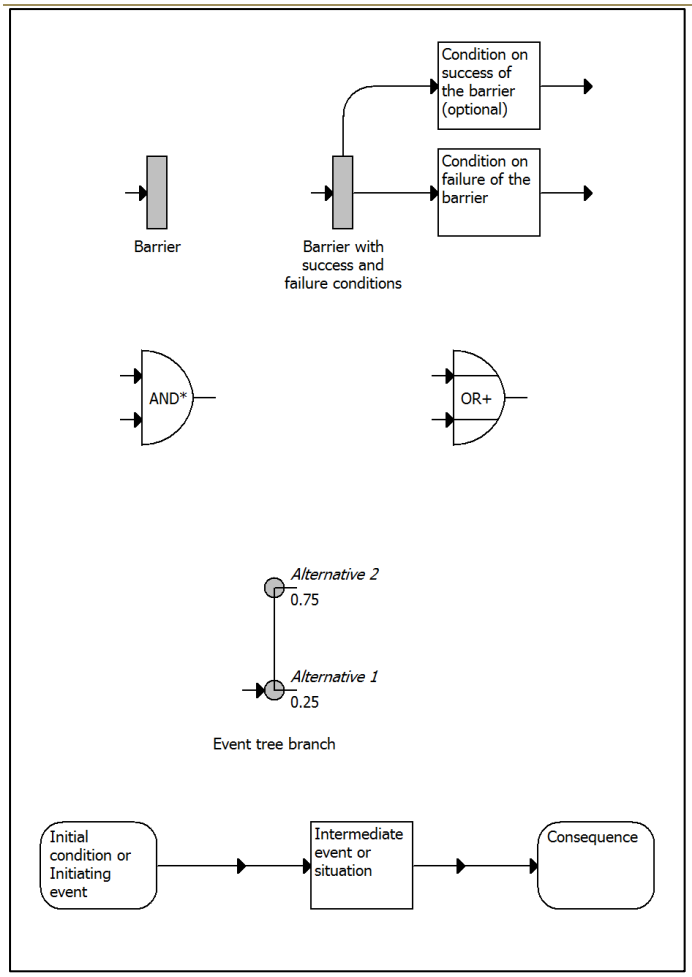
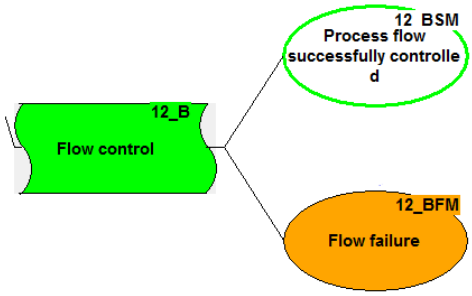


FIGURE 19 SYMBOLS AS USED IN SAFETY-BARRIER DIAGRAMS (SAFETYBARRIERMANAGER 2015)

4.7 Barriers in Storybuilder

In the Storybuilder™ model provided by RIVM[4] there are 36 barriers (See Annex E Glossary, Duijm et al 2015). Each barrier has a failure mode and a success mode as shown in

Figure 20. One of the primary purposes of the current research is to develop the success modes of the Storybuilder model. The idea is to have a generic set of components that attaches to each success node. The success node is the endpoint of an event



.

FIGURE 20 STORBUILDER BARRIER EXAMPLE SHOWING BARRIER (B), BARRIER SUCCESS MODE (BSM) AND BARRIER FAILURE MODE(BFM)

[44] http://www.rivm.nl/en/Topics/O/Occupational_Safety/Other_risks_at_work/Dangerous_substances
Information about major hazard model and link to download Storybuilder and databases.

5 RESILIENCE CASE STUDIES

The full report of the Resilience Success Consortium can be found in:

Annex B: Resilience Case Studies: Dealing With Uncertainty In Practice: Strengths And Traps In Human Intervention, Van Galen & Bellamy 2015.

5.1 Introduction

This part of the project was focused on the following aspects:

- Identifying the resilient qualities of individuals as well as possible traps related to human intervention;
- Mental frameworks with respect to anticipation, learning, monitoring and responding to what is happening;
- Human intervention in the context of teams and organisational processes.

5.2 Questionnaire development

Interviews were designed around a questionnaire that was developed in detail from the Resilience Analysis Grid (RAG) framework (Hollnagel et al 2011). The questionaaire can be found in Annex B Resilience Case Studies). Interviews were carried out in the Netherlands, France, Belgium, Denmark and the UK. There were 18 interviews with three types of people:

- Mountaineers (also called alpinists) who are directly confronting natural hazards (4);
- Rope Access Workers carrying out dangerous maintenance on man-made structures (3);
- HS&E Managers and Operations Managers of high hazard chemical (6), petrochemical (3) and steel plants (2).

After conducting an initial set of semi-structured interviews with the mountaineers, there was a progression to rope access workers doing dangerous maintenance to get a picture of how people operating close to danger think and act. The questionnaire was then refined by making it a more specific set of questions and more focused on major hazard safety, major hazards being fire, explosions or toxic releases from chemical installations. The questionnaire addresses the way people successfully deal with uncertainty and variability. From the interviews, examples and stories about resilience in practice were identified, especially focussing on the commonalities between people in different and similar sectors and roles.

The questionnaire was used as a 'guideline' during the interviews rather than rigid question and answer sessions. It was not aimed at assessing the individual or the organisation but rather to focus on how high risks are identified, understood and managed. The questions were used to evoke an open dialogue and narratives and to cover the fields of interest of this study.

The Resilience Analysis Grid (RAG) framework (Hollnagel et al 2011) upon which the questionnaire was designed, also called 'the four cornerstones of resilience' are:

- Anticipation – Finding out and knowing what to expect
- Responding – Knowing what to do and being able to do it
- Monitoring – Knowing what to look for
- Learning – Knowing what has happened

The questionnaire also has a question on cognitive biases, the concept originating from Tversky & Kahneman (1974), also sometimes referred to as cognitive illusions (Pohl 2012) – see section 3.5. The main feature of cognitive biases is that they are mental short cuts (heuristics) used in judgement & decision making in uncertain conditions which can lead to errors. These biases are unconscious, automatic influences. For

example, confirmation bias is the tendency of people to favour information that confirms their beliefs or hypotheses rather than looking for evidence that falsifies them.

The questionnaire also addresses the (mental) strategies the interviewees use to try to prevent or mitigate these biases.

5.3 Results for the four cornerstones of resilience

The following are excerpts from the resilience case studies report. The four cornerstones of resilience were used as a basic framework to analyse the characteristics of the mind in relation to human resilient intervention and to understand how the organisation should support those characteristics . Figure 21 provides a simple overview and a summary of each of the main points for the 4 cornerstones follows.

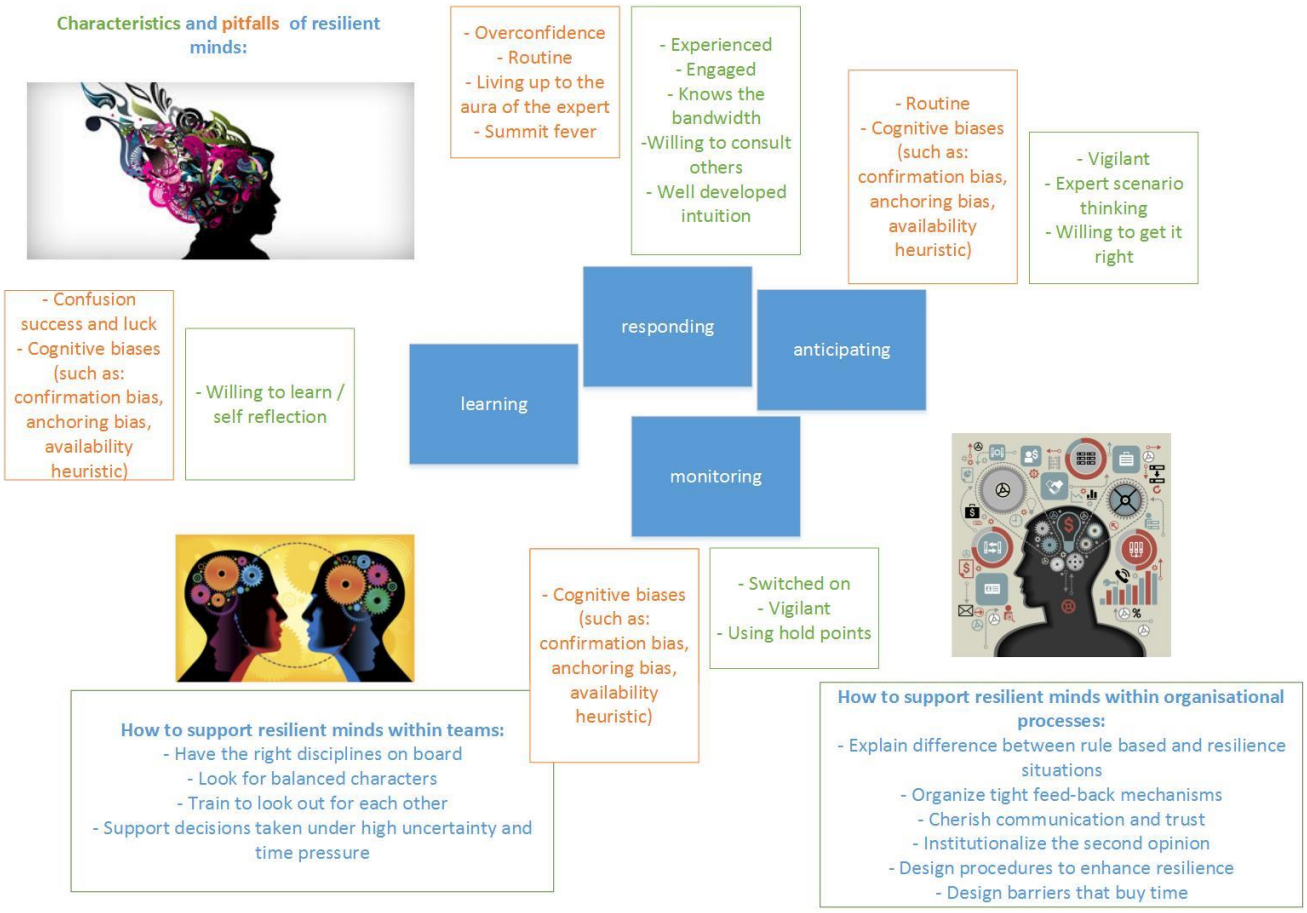


FIGURE 21 CHARACTERISTICS AND PITFALLS OF RESILIENT MINDS

5.3.1 Anticipation

The main points are:

- Interviewees have described how they experience uncertainty in their jobs e.g. "the danger is not binary but like a snake".

- Resilient people say they are risk aware and vigilant, but not afraid;
- That it is important to be good at thinking through the different scenarios;
- That it is even more important to be dedicated to "getting it right".

Most of the interviewees fully acknowledge and in certain ways also appreciate the variety and the danger of their working environment. Being 'switched on' to the now and what it means, what could also be called being aware and vigilant (constant watch for signals) are important for dealing with unforeseen risk-situations. For some that sort of demand draws them to this kind of work or experience.

A resilient mind is also occupied with scenario-thinking. Scenario thinking helps to prepare for the unknown.

The people that have been interviewed stressed the importance of 'getting it right', i.e. to make sure that in the planning and preparation phase as well as 'in the act' as much as possible has to be done right so as to avoid an accumulation of small flaws and errors which could facilitate a big accident.

5.3.2 Learning

The main points deduced from the interviews were:

- Learning from things that go wrong seems to be more effective than learning from 'the positive';
- In order to learn you should not confuse 'luck' and successful operating;
- It is very important to also learn from small things that go wrong or from near-misses;
- Learning from successes might be dangerous (because of certain heuristic traps);
- Resilient minds are self-reflective and 'willing to learn' , also from small accidents and near misses ('the little things').

Despite what some resilience thinkers may say, it remains very important to be preoccupied with failure instead of success. As one of the interviewees stated 'success tastes *moreish'*. Success seduces people into becoming overconfident; it narrows perceptions and evokes dangerous biases such as 'summit fever' which can apply to goal seeking in any task. Failure on the other hand is more engraving in the mind of individuals and of the organisation; it makes people realise the importance of getting it right and their role in risk management. In order to learn from failure it is important not to confuse luck and successful operating. Next to this it is crucial that people are willing to learn and are self-reflective and are also prepared to learn from little things that did not go well and near misses.

Having said this, the case studies are an example of sharing best-practices and focus on how people manage risks successfully on a day to day basis and therefore might be a perfect example of 'looking at things that go right'.

Having learning and experience is good for resilience and so to make use of this in the organisation means having available multidisciplinary knowledge and experience, balancing characters like devils advocates as well as people who want to push forward, applied to both preventive and regenerative tasks.

5.3.3 Monitoring

The main points that came up in the interviews were:

- The importance of being 'switched on', using all your senses, looking in all directions and concentrating on yourself , 'the other' and the environment;
- The importance of hold points and decision nodes;
- Awareness-limiting mental traps like confirmation bias

Being 'switched on' is a key characteristic when it comes to monitoring in a complex high hazard environment. This stands for using all your senses, looking in all directions and concentrate on yourself, the others and the environment. The emphasis is on the detection of change or difference. This is about watching out for every little thing that could signal a change in the risk situation as well as finding out everything that has changed in the situation.

It also has become clear that monitoring can be influenced by mental traps which narrow or distort awareness. To enhance and facilitate monitoring, the importance of hold points and decision nodes has been stressed and to make best use of the competences, individual characteristics and multi-disciplines in thinking together and collecting the right information.

5.3.4 Responding

The main points were:

- Being knowledgeable and experienced are important characteristics for resilient responding;
- Adequate responding requires knowing the extent of the room for manoeuvre;
- Intuition can play a role;
- That there is a negative side to being experienced: overconfidence, routine, living up to the aura of the expert;
- The need for a willingness to consult others;
- Being 'engaged' is important in order to respond but to be aware of 'summit fever'.

To be able to respond it is important to understand (have knowledge of) how an installation/system/process behaves as this supports thinking in unforeseen situations and knowing the margin of safe operation - to understand the principles of safe operation. Good responding requires experienced people where experience can mean very many hours or years of experience. Experience is a guide which can come into play as instinct or intuition. Experience guides to certain decisions that are not per se rational.

A very important finding though is that it seems to be that experience is not an antidote to every risk. Although experience may be beneficial in finding the right solution in risk problems, our and other research (e.g. Weick and Sutcliffe 2007 and McCammon 2002) also show that there are important negative sides to experience, notably overconfidence, routine and living up to the aura of the expert. It seems that every stage of experience has its own pitfalls.

It also became clear that being 'engaged' is important in order to respond adequately, but that one should be aware of 'summit fever'.

To avoid traps and pitfalls interviewees have pointed at the possible advantages of thinking and deciding together. This will be elaborated in the next paragraph.

5.4 Teams

In high hazard industry people often work in teams. Teams have the advantage that the quality of thinking and deciding can be improved by taking the right multidiscipline on board. When there is time available then making decisions under high uncertainty when a lot is at stake should not be taken alone.

Besides this interviewees have mentioned that certain traps like summit fever could be avoided when team members have balancing characters.

The uncertainty and complexity of processes sometimes forces people to make difficult decisions under high time pressure, for example to shut down an installation. The only way to encourage people to keep on making such decisions is to support them, also when the outcome of the decision turned out to be less

favourable (for economical or even safety reasons). Leaders should back-up their team members when it comes to decision making under uncertainty and time pressure.

5.5 Dealing with traps related to resilient intervention

In this study two key problem areas of the resilient mind have also been discussed. The first problem is that resilience-enhancing characteristics of the mind such as awareness, vigilance and 'being switched on' are felt to decrease in automated environments with few accidents. Strategies have been selected from the interviews and literature that might mitigate this problem. For example to embrace modest failure, use simulators and make and keep the risk perceptible through design. High Reliability Organisations (HRO's) are said to be preoccupied with failure: "HRO's encourage reporting of errors, they elaborate experiences of a near miss for what can be learned, and they are wary of the potential liabilities of success, including complacency, the temptation to reduce margins of safety, and the drift into automatic processing. They also make a continuing effort to articulate mistakes they don't want to make and assess the likelihood that strategies increase the risks of triggering these mistakes."(Weick and Sutcliffe 2007, p.9)

The next problem area lies in the fact that cognitive biases weaken decision making under uncertainty and time pressure. Cognitive bias is a concept originating from Tversky & Kahneman (1974), also sometimes referred to as cognitive illusion (Pohl 2012). The main feature of cognitive biases is that they are mental short cuts (heuristics) used in judgement & decision making in uncertain conditions which can lead to errors. These biases are unconscious, automatic influences characteristic of Kahneman's (2011) System 1 thinking and opposed to System 2 rational conscious thought. For example, confirmation bias is the tendency of people to favour information that confirms their beliefs or hypotheses rather than looking for evidence that falsifies them. In the interviews various examples have been given such as summit fever and confirmation bias.

Not many remedies have been proposed by the interviewees for overcoming bias, apart from using prescribed decision making procedures, such as always to seek a second opinion. Some have used training in awareness of mental biases. Next to this 'Train as you fight' (realistic training) and striving to deepen self-knowledge and mindfulness could be useful in mitigating the effects of cognitive biases.

5.6 Organisational processes

In order to make organisations in the high hazard industry more resilient it is not only necessary that employees have the mental abilities to act resiliently when necessary but also the organisation itself should be organised in certain ways so as to facilitate resilient human intervention. This leads to the following points for reflection and recommendations:

5.6.1 Resilient interventions

- The organisation should help people to understand the differences between situations in which one should be resilient and situations in which obeying rules is crucial;
- The organisation should enable tight information & communication feedback mechanisms;
- The organisation should promote a culture in which communication and trust are at a high level;
- Within this culture of trust it is crucial to organise an 'institutionalised' second opinion;
- Also meta procedures for deviating from standard procedures can help human intervention;
- Technical barriers such as automated trips can actually improve human resilient intervention, because these measures can buy time to monitor and reflect before acting.

5.6.2 High vigilance monitoring strategy

- To embrace modest failures because they are essential to resilience;

- To also learn systematically from mistakes that others have already made;
- To keep the organisational memory alive;
- To use simulators;
- To make the risk perceptible through design;
- To organise sensible job- and task-rotation

Kahneman (2011) concludes his book Thinking, Fast and Slow with the following statement:

> "Organisations are better than individuals when it comes to avoiding errors, because they naturally think more slowly and have the power to impose orderly procedures. Organisations can institute and enforce the application of useful checklists (…). At least in part by providing a distinctive vocabulary, organisations can also encourage a culture in which people watch out for one another as they approach [cognitive] minefields."

5.6.3 Time & uncertainty model for interventions

Organisational process requirements for underpinning the human component of resilient adjustment can be better understood in Figure 22.

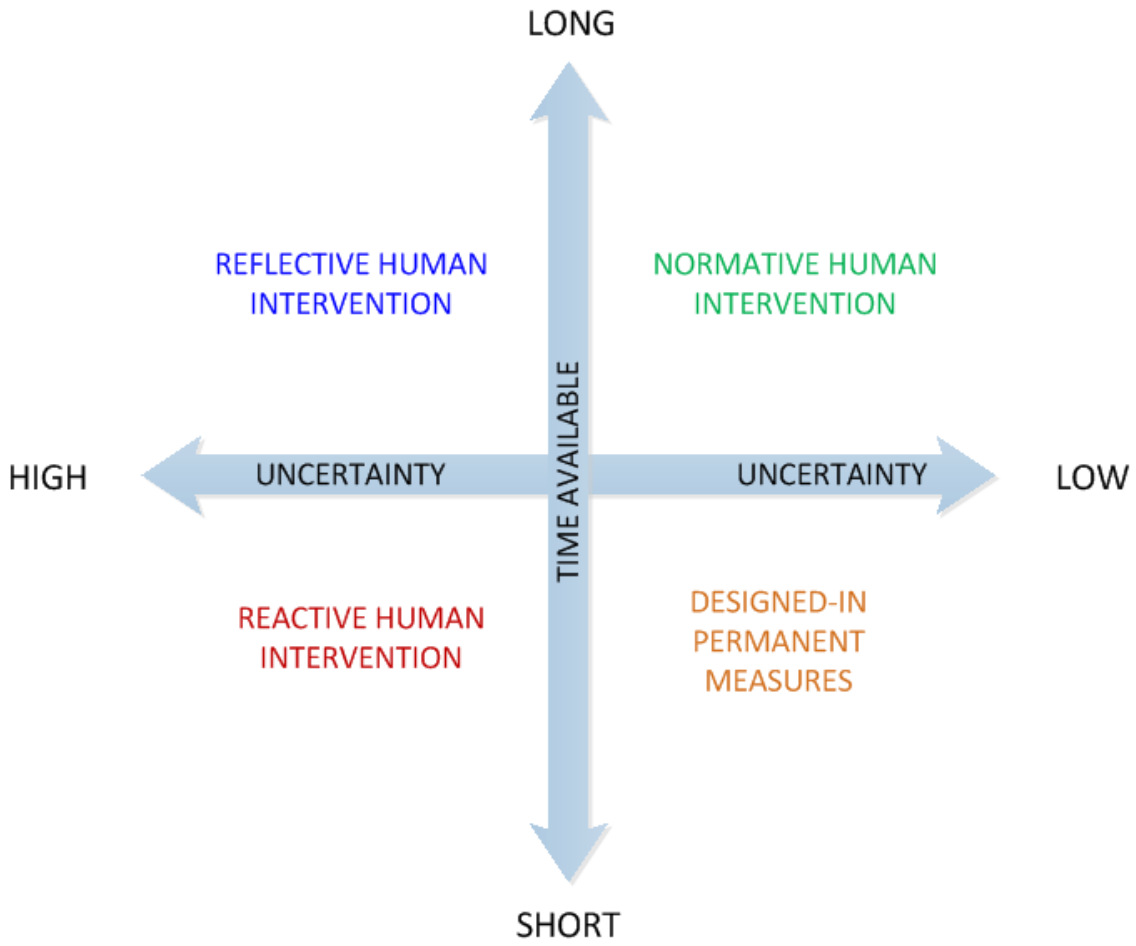


FIGURE 22 ORGANISATIONAL ASPECTS OF HUMAN INTERVENTION DEPENDING ON LEVEL OF UNCERTAINTY AND TIME AVAILABLE

On the right side of this quadrant more traditional rule-based anticipated risk management is represented. For known risks and little time available to respond designed-in permanent (passive) measures might be the

most suitable. In case of known risks and when there is more time left to respond it will be possible to manage risks normatively, i.e. by rules and procedures.

At the left side of the quadrant human resilient intervention is depicted. These kinds of interventions will be triggered by changed conditions with respect to the risk and require management of the uncertainties.

5.6.4 Two types of human intervention

The need for resilient intervention occurs when there is a change in conditions that cannot be responded to by the standard normative approach. Recognising that there is a change together with increased uncertainty is a trigger for intervention. The quadrant in Figure 22 shows that, depending on the amount of time left to react to change, there is something that could be called *'reflective human intervention'* and there is *'reactive human intervention'*. In the case of reflective human intervention it will be possible to reflect, to gather more information, have the right disciplines around the table, develop and follow golden principles or "lines in the sand" (Hayes 2013) and be deliberating and mindful when taking decisions. Such behaviours will be aimed at uncertainty reduction.

In the case of reactive human intervention there is no time or almost no time to reflect. It will then come down to personal skill based on training and experience, and maybe on intuition (Klein, 2003); under time pressure high stakes, and changing parameters, experts used their base of experience to identify similar situations and intuitively choose feasible solutions. The less time there is left to react, the more it will be likely that interventions will not achieve the intended outcome.

Anticipation and making use of a resilience engineering approach are complementary strategies. Companies that want to improve their management of risks should enhance the possibility for resilience which will optimise uncertainty reduction and successful human intervention, without forgetting that evaluating foreseeable risks also requires other means, such as hazard identification and risk assessment, in combination with designed-in measures, procedures, etc.

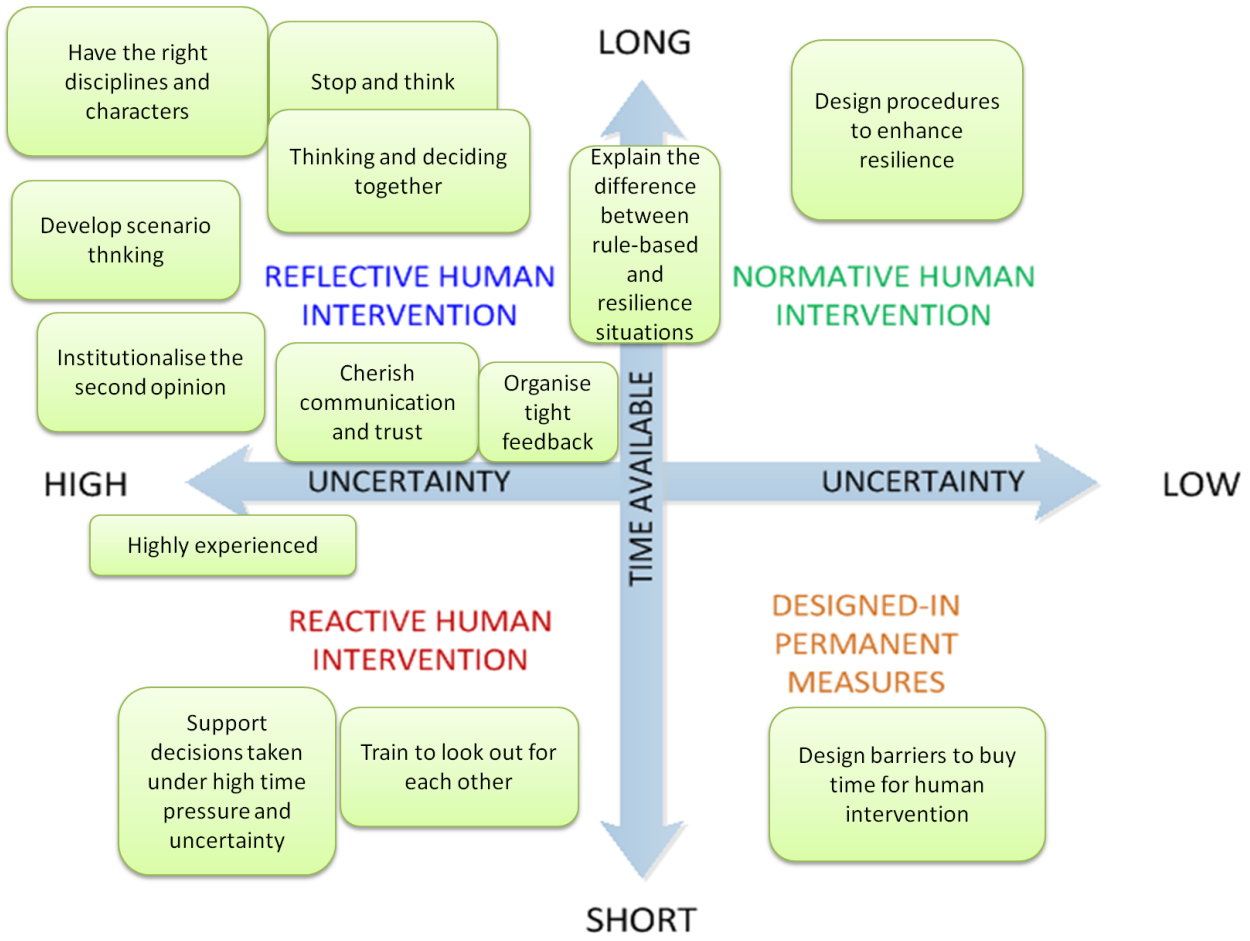


FIGURE 23 KEY COMPONENTS OF UNCERTAINTY MANAGEMENT SUPERIMPOSED ON THE UNCERTAINTY X TIME MATRIX

6 MENTAL MODELLING

This section explains the use of the mental model concept in the interaction between an operator and the process they are trying to control.

> " In order to provide effective control the controller must have an accurate model of the process it is controlling. For human controllers this model is commonly called a mental model . For both automated and human controllers the process model or mental model is used to determine which control actions are necessary to keep the system operating effectively." Leveson (2015)

The developed success bowtie makes use of the recovery components which were identified in the failure bowtie. These were the IDDR components if Indicate, Detect, Diagnose, Respond as shown in Figure 24. The recovery (failure) is only developed once in the failure bowtie, to recover the first line of defence failures. All initial deviations derived from barrier failures in the first line of defence (operational control) fail to be recovered and these then propagate to the third line of defence, containment protection. When this also fails the centre event occurs (loss of containment). For success, an adjustment is required before a serious consequence ensues. Indication/detection failures are almost 65% of failures in the major hazard accidents and was the biggest problem in the Dutch major hazard accidents (Bellamy et al 2013) and the same in the UK accidents analysed in the same framework (Lisbona et al 2012). Sometimes the problem with detection is that the signal is weak or inconclusive.

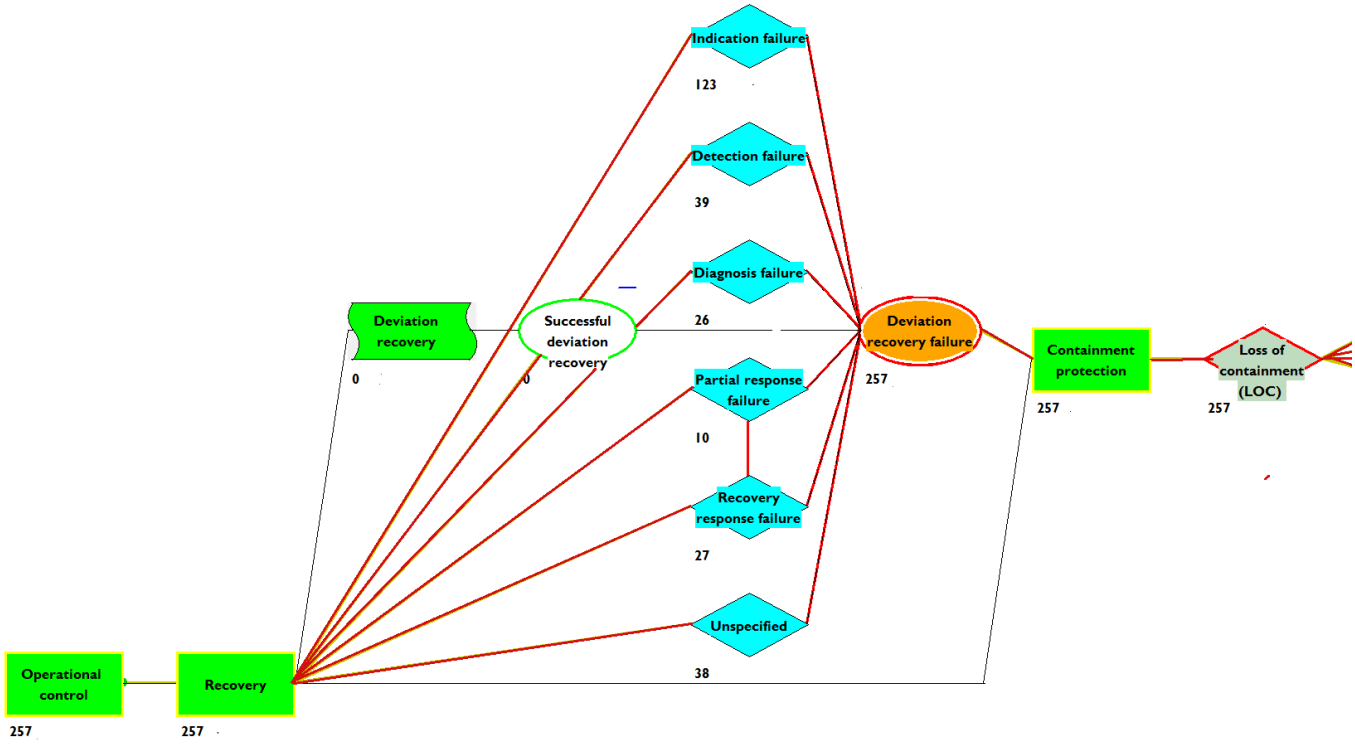


FIGURE 24 RECOVERY FAILURES IN THE MAJOR HAZARD FAILURE BOWTIE. NUMBERS INDICATE NUMBER OF ACCIDENTS. THERE ARE NO SUCCESSFUL RECOVERIES (ADAPTED FROM THE DATABASE OF RIVM (2014))

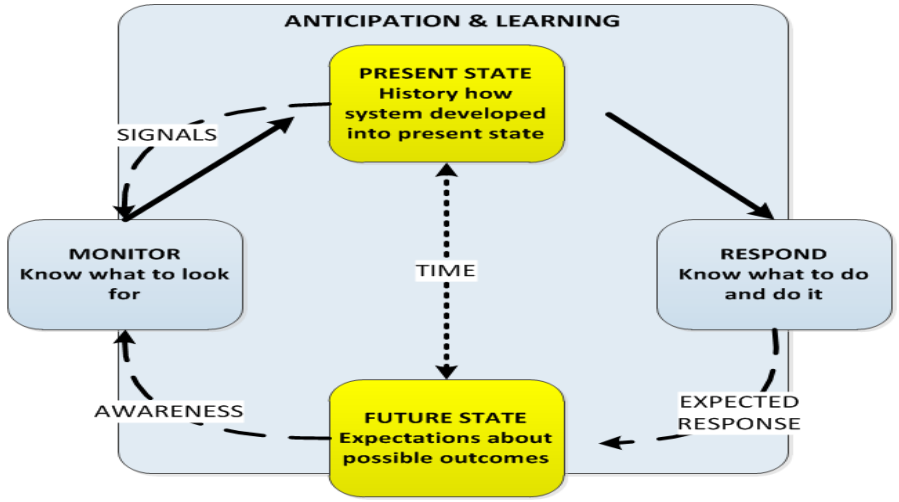
In the success bowtie it is proposed to use this IDDR as a success component. In principle it could be attached to every success mode of all the barriers.

6.1 Indicate-Detect-Diagnose & Decide-Respond (IDDR) for the success model

Endsley (2000) refers to internal models of the world that direct attention, integrate information perceived to form an understanding of its meaning and provide a mechanism for generating projections of future system states based on its current state and an understanding of its dynamics.

In the current project, management of safety is considered in a mental model framework where signals are transformed into response actions (or inaction) (R) through the mental processes of detection (D1) and diagnosis & decision-making (D2,). The signals are indications (I) in the real world that can be detected directly by people such as by sight or smell, or through an instrument with a reading such as a temperature gauge or an alarm such as when the temperature is too high, or through a communication from a person or written down, and so on. There are many forms of signals indicating something about the world whose detection will be driven both bottom-up such as when the nature of the signal itself draws attention because of its saliency, how prominent or noticeable it is, and top down when internal mental models direct attention. A detected signal is interpreted and decisions made on whether and how to respond. Signals about the system and whether it is under control may be present at different stages or levels of control or problem solving, for example a signal about the competence of a person, environmental conditions, the state of a piece of equipment or a trend in a number of readings.

Figure 25 shows IDDR from the perspective of the human operator.



Indicate [**D**etect, **D**iagnose&**D**ecide] **R**espond

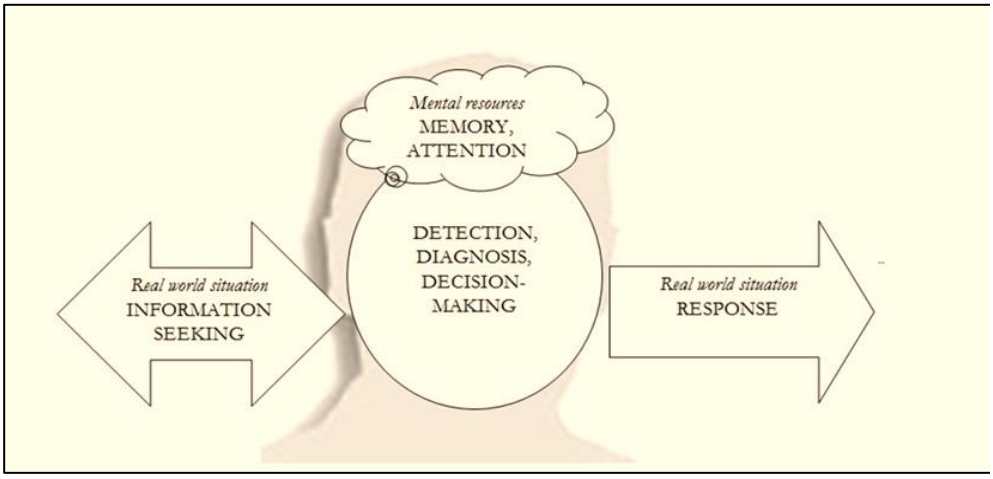


FIGURE 25 THE MENTAL MODEL FORMULATED AS "I-D-D-R": INDICATION, DETECTION, DIAGNOSIS & DECISION-MAKING AND RESPONSE

The following example in Table 2 illustrates IDDR in a successful (in terms of accident avoidance) anticipation of the future. An IDDR sequence for a near miss scenario in a chemical plant is shown in Table 3.

TABLE 2 QUOTES FROM THE NEW YORKER, APRIL 21, 2014 DEATH AND ANGER ON EVEREST BY JON KRAKAUER ILLUSTRATING THE IDDDR (INDICATION, DETECTION, DIAGNOSIS & DECISION, RESPONSE) HTTP://WWW.NEWYORKER.COM/NEWS/NEWS-DESK/DEATH-AND-ANGER-ON-EVEREST

IDDR	Description
(I) HAZARD INDICATION	*A bulge of glacial ice three hundred yards wide that was frozen tenuously to Everest's West Shoulder, hanging like a massive sword of Damocles directly over the main route up the Nepal side of the mountain*
(D1)DETECTION (ICEFALL RISK & EXPOSURE)	*One day, Brice timed how long it took his head guide, Adrian Ballinger ("who is incredibly fast," he wrote in the blog post excerpted below), to climb through the most hazardous terrain: "It took him 22 min from the beginning to the end of the danger zone. For the Sherpas carrying a heavy load it took 30 min and most of our members took between 45 min and one hour to walk underneath this dangerous cliff."*
	…some of his most experienced Sherpas, ordinarily exceedingly stoical men, approached him to say that the conditions on the mountain made them fear for their lives. One of them actually broke down in tears as he confessed this.
(D2)DIAGNOSIS & DECISION	*Brice …became increasingly worried "In my opinion, this is far too long to be exposed to such a danger and when I see around 50 people moving underneath the cliff at one time, it scares me."* *So on May 7th, 2012, Brice made an announcement that shocked most of the thousand people camped at the base of Everest: he was pulling all his guides, members, and Sherpas off the mountain*
(R) RESPONSE	They packed up their tents and equipment, and headed home.
HAZARD REALISED	*On April 18th 2014, shortly before 7 a.m. local time, an overhanging wedge of ice the size of a Beverly Hills mansion broke loose from the same ice bulge that had frightened Brice into leaving Everest in 2012. As it crashed onto the slope below, the ice shattered into truck-size chunks and hurtled toward some fifty climbers laboring slowly upward through the Khumbu Icefall, a jumbled maze of unstable ice towers that looms above the 17,600-foot base camp. The climbers in the line of fire were at approximately nineteen thousand feet when the avalanche struck. Of the twenty-five men hit by the falling ice, sixteen were killed, all of them Nepalis working for guided climbing teams. Three of the bodies were buried beneath the frozen debris and may never be found.*

TABLE 3 ILUSTRATION OF IDDDR WITH A SIMPLE CHEMICAL PLANT EXAMPLE OF A NEAR MISS

IDDDR	Description
(I) HAZARD INDICATION	The flame on a burner goes out which results in fuel being atomised with potential explosion risk
(D1) DETECTION	The absence of the flame is seen visually
(D2) DIAGNOSIS & DECISION	There is a problem with the sensor - fix. Use visual checks and regular checks on the sensor.
(R) RESPONSE	Stop the flow and relight. Regular visual checks.

6.2 Barrier function: the knot at the end of the rope

An example was chosen from an interview.

> "And also I learned a lot more about several techniques to postpone errors.
> *What kind of errors?*
> For example that if you go rappelling, you make a knot at the end of the rope. Before, I did not do that, I just started off and went 'yeeha'." Mountain Guide.

In theory IDDR should apply to any barrier, so it should apply to knots in ropes. The knot is a physical barrier. With a knot it is not possible to "rappel" (descend on a rope) beyond the end of the rope. Without a knot, if you arrive at the end of the rope and do not pay attention you may have a big deadly fall; if you are in a hurry, or if you are looking for the intermediate "belay" (anchor) this may be the case.

IDDR adjusts (or restores) a system to a good state.

I the signal is **I**ndicated in some way; there is a *detectable* signal - an energy pattern detectable by the senses (stimulus) or an automatic sensor

D signal is **D**etected and recognized by a detector like a human (sense) or an automatic detection device

D the detected signal is **D**iagnosed and a **D**ecision is made and the relevant response selected from the response repertoire of the human or logic device

R the selected **R**esponse to adjust the system to an appropriate state is carried out by a human or machine

The example used for ropes is shown in Table 4.

TABLE 4 IDDR FOR THE USE OF THE BARRIER – STOP BEFORE THE END OF THE ROPE - (LOSS OF CONTROL EVENT: FALL FROM HEIGHT)

	Descend with Knot	**Descend with No knot**
Indication (detectable signal)	No knot in rope.	End of rope is visible
Detection (signal is perceived)	Knot is absent.	Look to see where the end of the rope is
Diagnosis & Decision (signal is interpreted and relevant action or no action selected)	Recognise the need to carry out knot procedure	Determine how far from end of rope
Response (action)	Tie knot (person will automatically stop at the end of the rope)	Stop rappelling before end of rope

Diagnosis/Decision to select knot:

- Normal procedure
- Can't see next rappelling belay
- Have a partner who hasn't done it a lot.

Diagnosis/Decision to select no knot:

- Ignorant of need for a knot
- Might forget to untie the knot afterwards = problem because rope gets stuck.
- Might get caught on something like cracks or caught up in the rest of the rope
- Better for a quick descent
- Rope is longer than drop.

6.3 Signals

Signal detection theory (SDT) (Green & Swets 1966, Macmillan 2002) is an explanation for decision making under uncertainty which uses a graphical and notational system. It applies when signal-noise distributions overlap as shown in Figure 26 ; the degree of overlap is an inverse measure of accuracy or *sensitivityor d'* (Figure 27). Perceived events do not conclusively mean a given condition; there is uncertainty e.g. whether bolts are appropriately tight or not. The key assumption of the theory is that the strength of sensory and cognitive events is continuously variable. The only way to improve sensitivity is by reducing the overlap of the distribution along this sensory dimension. On the other hand, the observer has control over where (s)he places the decision criterion, the point at which evidence is placed in the category of signal or noise. This divides the strength axis into two and affects the likelihood of a hit or false alarm.

If there are weak or misleading signals, misses and false alarms are likely. Nonetheless weak signals may precede sudden/strong change.

- Hit – correctly detects the signal (e.g., on checking the equipment the operator identifies that the component is loose when it is indeed loose). Hit probability = Number of hits / number of signal events.
- Miss – the operator missed the signal (e.g., on checking the equipment the operator did not identify that the component was loose). Miss probability = Number of missed signals / number of signal events.
- False alarm – the operator identifies a noise event as a signal (e.g., on checking the equipment although the component is correctly tightened the operator reports that it is loose). False alarm probability = Number of reported signals / Number of noise events.
- Correct reject – it is not a signal; the operator identifies a noise event as noise (e.g., on checking the equipment the operator correctly finds no evidence to suggest the component is loose). Correct accept probability = Number of events reported as noise / number of noise events.

Hits and correct rejects are good. A graph of the probability of hits against the probability of false alarms will indicate the operator's performance where optimum performance is p.Hit=1, p.False Alarm=0. Because of signal-noise overlap not all responses can be good.

Sensitivity or d' (d prime), is the standardized difference between the means of the Signal and Noise distributions.

The formula for d' is as follows:

$$d' = z(\mathrm{FA}) - z(\mathrm{H})$$

where FA and H are the False Alarm and Hit rates, respectively, that correspond to right-tail probabilities on the normal distribution. Thus, z(FA) and z(H) are the z scores that correspond to these right-tail p-values represented by FA and H. Larger absolute values of d' mean that a person is more sensitive to the difference between the Signal and Noise distributions. d' values near zero indicate chance performance. Figure 27 shows a number of sensitivity curves for different separations between the signal and noise distributions. A single curve represents the movement of the criterion line. As the criterion moves from right to left along the decision axis both hits and false alarms increase.

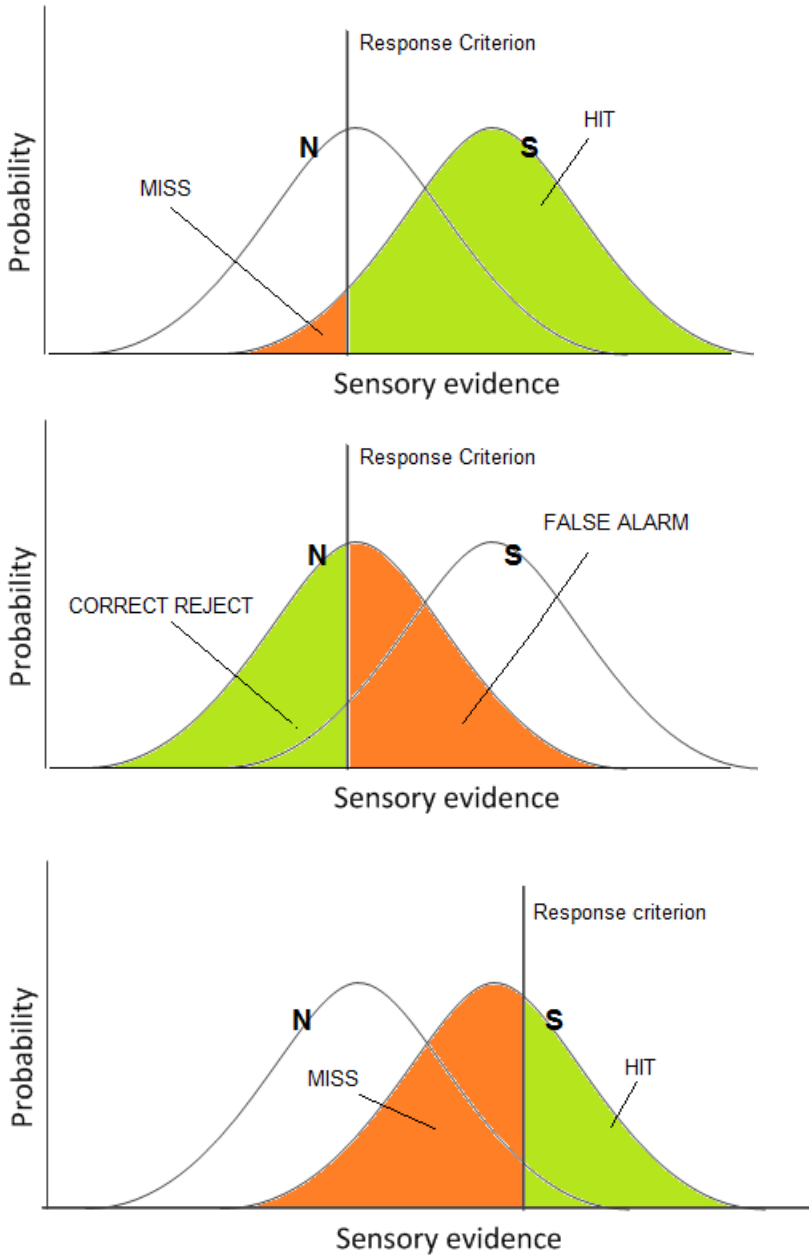


FIGURE 26 THE GRAPHS SHOWS THE SIGNAL DISTRIBUTION (S) ON THE RIGHT, NOISE DISTRIBUTION (N) ON THE LEFT. THE TOP GRAPH IS WHEN THERE IS A SIGNAL AND THE MIDDLE GRAPH FOR THE OCCURRENCE OF NOISE. THE LIKELIHOOD OF HITS AND MISSES (SIGNAL EVENTS) AND CORRECT REJECTS AND FALSE ALARMS (NOISE EVENTS) ARE AFFECTED BY WHERE THE OBSERVER PLACES THEIR RESPONSE CRITERION ON THE BASIS OF EVIDENCE. THE BOTTOM GRAPH SHOWS HOW MOVING THE RESPONSE CRITERION TO THE RIGHT WOULD REDUCE HITS AND INCREASE MISSES WHILE DECREASING FALSE ALARMS IN THE EVENT OF NOISE.

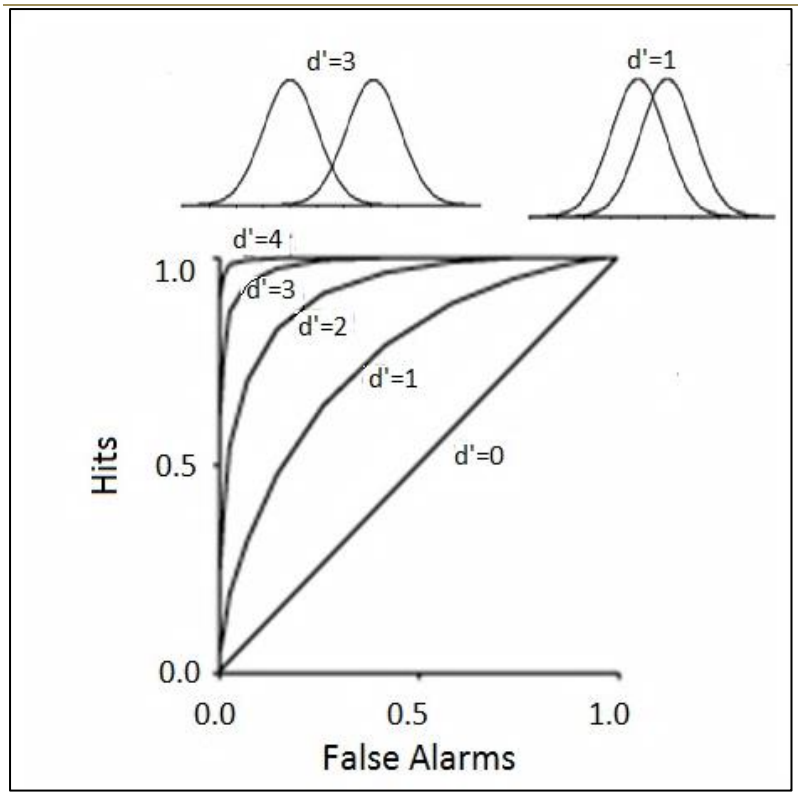


FIGURE 27 RECEIVER OPERATING CURVES (ROC) FOR DIFFERENT SENSITIVITIES (D') - THE SEPARATION BETWEEN THE DISTRIBUTIONS FOR DIFFERENT VALUES OF D' IS SHOWN ABOVE THE ROC CURVES

To put the difficulties of establishing the criterion line into real life contexts the following quotes are taken from managers of major hazard plants.

Example 1:

" *Is there any way you can enhance detection or decision making?*

You try to – again – you try to create a culture of trust where people feel comfortable and say, "this doesn't look right, this doesn't feel right and I can't pinpoint it," and you want people to report that. Because maybe somebody else can say, "hey, I've seen this in this area of the plant, but I've also seen this in this area of the plant," and then you can connect the dots and say, "oh, but that means…"

So it's really about having the confidence.

You want people to be sensitive to: "this is not normal."

I suppose that the criterion line just develops by itself over time in terms of what is something that you should really worry about and what is something that can just be absorbed.

Yes, but there is a lot of experience with that as well.

So it comes from experience …

And a lot of things. If it is just, say, an operator outside in the middle of the night sees something and says, "this doesn't look right," he talks to his colleague and they fix it. It's done, I mean, that's it before it escalates into something material."

Example 2:

"….shutting down this site means that the site can only restart very slowly and each time an operator takes the decision to close down the plant it costs some hundred thousand euros of margin per day. This is a big amount. The economic impact of this plant is relevant at company level, and the same goes for the safety impact.

So the operators have a heavy job to do, because they are probably very much aware of the impact of their decisions. How do you as a manager facilitate their decision making?

Leave the responsibility to act in line with procedures to them, but also back them up when – as it might appear – they have unnecessarily taken the whole plant out of service. Sometimes this is very difficult. Stand by your people; praise them for the fact that they have taken this decision. If you do not do this as a leader they might not want to take the same decision later on – when it is really necessary."

6.4 Signals in context – Analysis of an interview

This section analyses an interview of a mountain guide. It shows the thought processes and actions in relation to signal events and to contexts. Comments are made to identify cognitive de-biasing strategies.

TABLE 5 ANALYSIS OF AN INTERVIEW IN THE SCHEME OF THE MENTAL MODEL WITH INPUTS AND ACTIONS (SEE FIGURE 25)

Input (Signals, environment and contexts)	Thoughts/mental events	Actions	Comments on response criteria and strategies for debiasing
Inspiring lectures from climbers	Dream to be a mountain guide	"I just started off and went 'yeeha'"	Inexperienced
Death of friend	Will die too if continue		
Accidents to self	These are difficult experiences.		
	The mountains are too uncertain and unpredictable. I shouldn't go there. Or maybe rather: I am too uncertain / unpredictable…	Give up	
	If I go back straight away it will be OK (the feeling will go away).	A bit more prudent but still doing risky things	
Married, children, more responsibility	Learning (wisdom) is important	Very very prudent	Debiasing strategy: augmenting personal accountability: A strategy for debiasing and making better decisions is related to augmenting personal accountability[5]. In the case of the guide this meant that as a father he felt more responsible for his actions.

[5] Tetlock PE, Kim JI. Accountability and judgment processes in a personality prediction task. J Pers Soc Psychol 1987;52: 700–9.

Input (Signals, environment and contexts)	Thoughts/mental events	Actions	Comments on response criteria and strategies for debiasing
		Take more time to make decisions	Debiasing strategy: slow down Debiasing and better decision making will also clearly profit from taking time to make good decisions. Instead of using the fast intuitive *system one*, for certain crucial decisions you have to put effort into your thinking and use your *system two*.[6] In healthcare 'slowing down strategies' have proved to lead to less incidents. Accuracy suffers when diagnoses are made too early and improves with slowing down.[7,8]
		Learn new strategies	Debiasing strategy: education Specific educational interventions may lead to greater skill and insight and thus to more resilience.
		Take all possible (foreseen?) consequences into account	
Inherent job pressure	Have to press on. Can't do everything in the time	Cut time consuming safety actions for self	ETTO (see Section 2.4.3)
	Some things are important though		

[6] For example: Kahneman e.a., The big idea, before you make that big decision, *Harvard Business Review*, June 2011. Or: Kahneman, *Thinking, Fast and Slow*, 2011.
[7] Moulton CAE, Regehr G, Mylopoulos M, et al. Slowing down when you should: a new model of expert judgment. Acad Med 2007;82:S109–16.
[8] Moulton CA, Regehr G, Lingard L, et al. Slowing down to stay out of trouble in the operating room: remaining attentive in automaticity. Acad Med 2010;85:1571–7.

Input (Signals, environment and contexts)	Thoughts/mental events	Actions	Comments on response criteria and strategies for debiasing
	Several little things could mean an accident	Put Important things in a checklist.	Debiasing strategy: use checklists Using structured data acquisition or checklists has proved to be an effective way to improve operations and decision making. It has been argued that: "In an age of unremitting technological complexity, where the most basic steps are too easy to overlook and where overlooking even one step can have irremediable consequences, something as primitive as writing down a to-do list to "get the stupid stuff right" can make a profound difference."[9]
	I'm feeling too tired or lazy	Omit checks	The devil is in the detail. Especially in situations with high uncertainty, it will be important to have the details right.
	I am focussing on safety of others	Omissions (forget own safety)	The falling accident he describes was due to – as he himself has analysed – forgetting his own safety, a non-holistic approach.
	I need to do something for myself. I need to prove something	Put self first in action choices	Ego and self-esteem are related to several cognitive biases as people generally try to avoid cognitive dissonance.
	This will be too dangerous.	Inaction - no exposure to the hazard	
	I am not prepared and in shape Positive: I have to be in shape to climb this difficult route	Inaction - no exposure to the hazard Train, get in shape, prepare	Resilience strategy: train physically and mentally for hard risk management problems. Preparation is key.

[9] Gawande, A., *The Checklist Manifesto*, New York: St. Martins Press, 2010.

Input (Signals, environment and contexts)	Thoughts/mental events	Actions	Comments on response criteria and strategies for debiasing
	Pleasing the client is the way I keep my job Positive: I am not here to please my clients, I have to take difficult decisions that bring us back home safely	Forced decisions Take decisions that are not pleasing clients but that do enhance safety	Debiasing strategy: set clear goals Almost all decisions have affective components and biases. Christophe is aware of these biases and has set his goals clear in order to avoid being influenced by that what his clients might think of him while making decisions. This is something that is being taught during the training to become a mountain guide in France: risk management is more important than relation management. Self-awareness training is one of the proposed strategies with regard to these kind of biases.[10] Resilience strategy: build in slack and alternative options
Conditions	The condition of me, the group and the environment are the important integrated factors. . 'are you angry, are you tensed, are you tired? Happy, energetic?'	Check up on the key factors	Debiasing strategy: increasing self-knowledge through mindfulness; check conditions of clients by asking questions and by observations; check the weather, conditions of route etc by asking third parties
Information about conditions	Need to check the conditions myself ALWAYS	Double check the key factors	Debiasing strategy: be sceptical and double check People have the tendency to believe information that is presented by sources that are generally thought of as credible and to look for information that confirms our opinions. Being sceptical is a way to debias.

[10] Croskerry P, Abbass A, Wu A. Emotional issues in patient safety. J Patient Saf 2010;6:1–7.

Input (Signals, environment and contexts)	Thoughts/mental events	Actions	Comments on response criteria and strategies for debiasing
		Collection information progressively (before, during)	Resilience strategy: constant holistic monitoring with all senses.
I am uncertain about the risk of this snow slab	I need a second opinion. What do others think? I need to check by real face to face communication	Consultation to find out what others think	Decision making and debiasing strategy: follow the rules of effective group decision making
	What do others mean?	Consultation to avoid communication errors	Natural languages can be an imperfect means of communication especially when diffierent groups use different concepts. [11] In sensemaking language is central issue[12]
Job Environment (variability/uncertainty in mountain conditions, weather, path finding, other people)	Enormous opportunity for making mistakes		The more uncertainty, the more managed safety (depending on ad hoc judgement from first line participants) is needed. In activities with less uncertainty it will be more possible to develop rules and procedures that ensure safety.
	Good when feel totally at home	Better decisions	Relation to somatic markers?[13] (emotional processes can guide (or bias) behaviour)
Potential difficult situations	Must begin easy and build up to it bit by bit	Progressive adjustment	
Dropped in a difficult situation	Not feeling good about it, not feeling at home. Harder to make the right decisions	Avoid	
Other people & self are happy	This feels like success		

[11] Bellamy, L.J. 1984. Not waving but drowning. Ergonomics Problems in Process Operations. IChemE Symposium series 90. ISBN 0 85295 172 8

[12] Weick, K.E., 2010. Reflections on Enacted Sensemaking in the Bhopal Disaster. Journal of Management Studies 47:3 May 2010

[13] Damasio, A. , 1991. Somatic Markers and the Guidance of Behavior. New York: Oxford University Press. pp. 217–299. Damasio, A.R. (1994). Descartes' Error: emotion, reason, and the human brain. New York: Grosset/Putnam.

Input (Signals, environment and contexts)	Thoughts/mental events	Actions	Comments on response criteria and strategies for debiasing
The client and or the guide overestimates the clients ability	The client can do a difficult climb	Possibly acting outside safe envelope	Christophe mentions judgment errors that can be related to mental biases. For example thinking that a client will be able to do a certain difficult climb which in fact he is not up to, can be related to the optimism bias and be regarded as a type of wishful thinking.
Return safely	This feels like success		
Other people accept your decisions	A sign of success		
	Feel more relaxed	Make less mistakes	

6.5 Signals at different stages of prevention

The resilience concept has been understood in rather different ways, probably because the word is relatively new and has more or less replaced the words safety or prevention and even the argument that resilience covers, for example, more the looking at what goes well instead of what goes wrong. In this section resilience is considered at different stages of potential recovery, with particular emphasis on the IDDR in the recovery process.

Four stages are given and reflect how early an intervention might take place, with stage 4 being the earliest.

6.5.1 Stage 1: An event has happened with some kind of a loss.

Here a barrier function has failed with a loss of control event (LCE). At this stage resilience is about the ability to support recovery so the injury or the harm or losses will be as low as possible and the return to normal situation goes quickly and easily. The first signal (I) will be that the LCE has occurred.

This stage is about emergency situations and action, where the resilience will be to be prepared, to know what to do and support functions are in place (e.g. a fire brigade in case of a fire).

Stage 1 example

> "We always will make rescue plans. What if the lighting goes down? How do we get away in case there are toxic substances released? Do we need gas masks? For us it is important to make sure that we can rescue ourselves. We cannot rely on the fire brigades for example, even if they would rather come and rescue us because formally it is their job. They do not know our business and procedures. In practice it just won't work. Rope access work is maybe something they only train once every two years. And it will take a long time before they will get to us...we have the buddy system in place in case of emergency."

> "Once a colleague of mine had to clean a column, a funnel at a cokes carburettor. There was this thick layer of ashes. My colleague was in this funnel and I was his buddy standing outside. When he had taken away the ashes it appeared that underneath there was this enormous heat covered up that now materialised. The guy immediately got heat stroke. The bad thing was that to get out of this funnel you first had to climb through this small pipe of one and half meter long, 60 centimetres diameter. I just got him out in time. It was a narrow escape."

6.5.2 Stage 2: An event has happened but before the situation has resulted in a loss of control

Here a barrier function has failed but without a loss of control event (LCE). The first signal will be that the barrier is in a failed state. At this stage resilience concerns either human or technical detection and reaction that stops the event in progress from becoming an accident. This concerns some of the technical safety barriers, but also human awareness and knowledge. The IDDR thinking will then be a part of the resilience concept.

Stage 2 Example

> *"Do you still get into situations that you really did not foresee or expect?*
>
> I have to think back. Yes, I recall a situation in which I trusted the client's safety measures. I was working on a tower during a maintenance project and one of the safety measures that had been arranged was that no one would work beneath or above us. The client also provided safety wardens who were given instructions. At a sudden moment I noticed that melted iron was flying all around me. Apparently some decks above me someone was using a cutting torch while I was hanging in my ropes. I first had to get down from my ropes and then had to kick the guy that was working above me. Well it appeared to be some bloke from Eastern Europe that just got this assignment and was not at all conscious of the other things that were happening on other decks. He just had started and was also not able to communicate in a language I could understand. I was able to communicate with my colleague / buddy but not with the client."

6.5.3 Stage 3: A situation is in an unsafe condition

The unsafe condition of this barrier or barrier task is detected before barrier failure occurs perhaps from experience or risk assessment; control of the safety barrier is through the barrier tasks, - also awareness, knowledge, ability and motivation to be able to detect diagnose & decide and respond (IDDR). Resilience is in terms of recovery of unsafe conditions to safe conditions. The discussion about looking at what goes well is at this stage a bit problematic because we know that a situation can be in an unsafe condition without any event or accident happening in a long time because of the human ability to take care and be aware, but the problem occurs at the moment this human ability is not in place. It is necessary to support people to take care or be aware all the time. Resilience means that we understand what needs to be done to create working situations where humans are able to work, understand what is going on and are motivated to carry out the work in such a way that variability can be handled in most cases.

Stage 3 Example 1

> "This same day one of my other colleagues had the same sort of issue at a different site. He also had to climb out of a tank through a very narrow man hole. He didn't feel good about it at all. That evening we talked on the phone and decided that we would stop immediately and go back and do some training on these kind of problems first. So we built some mock-ups[14] to gain experience. We built 'man holes' and started training.
>
> *This colleague that had the heat stroke, how did you detect something was wrong?*
>
> Well, luckily I heard him talking through the radio: "argh, hot" and I reacted immediately. I could pull him out and luckily he also was able to help a little with his legs.
>
> *And your colleague had the same problem on the same day?*
>
> He did not have an incident, but he had a very bad feeling about the whole situation. There was this kettle and several colleagues had to work in there while there was only this narrow manhole. It was not me that put the project on hold. My colleague himself had this nasty feeling and took the consequences of this. These are difficult decisions. Later on that day we decided together on the phone that we had to set up a simulation training."

[14] A mock up is a model or replica built for experimental purposes.

"This (stop with an activity and go back to the drawing table ed.) is not always easy, I must admit. Myself, I was recently offshore for a take in of work (job assessment) and I wanted to loosen a bolt to look at the state of the wire (thread) underneath it. And I caught myself in the act of collecting all kinds of sub-optimal tools to try to get the job done. I was about to start without the appropriate equipment, without proper planning and assessing all the risks. There was no direct danger, but there was a lot that could go wrong. I was there together with an operational manager from another contractor, and I said: "Dude!, we do not want to do this. We really want to finish it, but this is not okay". We were already considering even more drastic measures.. And we had to step back. It was not according to plan, we were not prepared and we did not have the right equipment.

So I had to admit to myself, you think you are the big guy that knows everything, but here you are trying to get the job done, unprepared and with the wrong set of tools creating a potentially dangerous situation. That is not something to be proud of and you rather want to forget about it. But rather than make it disappear, I talked about this incident with my colleagues and I even mentioned it in a formal inspection round on this platform so that we can learn from this."

Stage 3 Example 2

"A client told us for example that we just had to put a piece of plastic around our ropes and get started working at some tank with potential sulphide residue (highly corrosive to ropes). That is not the way we operate. This certainly has to do with the pressure on costs and the current economic situation. It is easier to look for savings at the side of contractors.

And also: sometimes there is a lack of knowledge. This leads to a deficient planning and finally to panic measures (like the access in the tank without 100% assurance for the absence of corrosive chemicals) and this leads to quick fixes with regard to safety.

This does not match with our approach to safety because we only want to work after meticulous preparation. If things go wrong the consequences are enormous."

Stage 3 Example 3

"To be honest, I do not think that our work as rope access workers is dangerous, although there are certainly risks involved. There are very little accidents in our field. The statistics are with us. The feed-back is always very clear. You do your job well, you come back safe on the ground. You make a mistake, you fall down. It is one-zero.

Look, someone who builds a scaffold and who does not have his fall protection, does not necessarily have a problem. In our work it is much clearer: if you don't hang onto something, you fall down.

With rope access work it is easy to manage the risks. You only have to do the right things, all the time.

Can you explain why you say that the risks are easy to manage in your field?

This is related to three things:

First: there always is clear feedback. The risk is very evident. Everyone understands this.

Second: and maybe this is the most important, there is a very strong safety culture. Everyone has safety first, his own safety and also the safety of his buddy (as well as the people around us). When they work people are very conscientious of their safety. It becomes part of yourself.

Third: we have very strict rules. Even if it is only one hour of work., we will always make a plan, a TRA, a description of the scope. We will never do something 'quick and dirty'."

6.5.4 Stage 4: An organisation's resources are not adequately supporting safety

This is about an unsafe condition of resources for supporting safety. The first signal will be that a resource is inadequate or unavailable for the tasks that have to be performed. At this stage we could talk about resilience in terms of recovering or creating an organization that supports, prioritises, takes action, learns and manages good safety activities from the top manager to the supervisors. This is about the management system where you could create a version of the IDDR that identifies signals for things lacking in the management system.

Stage 4 Example 1

> "Yes, maybe you are right. But I think that some companies are more and more hypocritical in their approach. They say that safety is their goal but in the mean time they are just punishing people. Yes, of course, when for the third time someone does not want to wear his safety equipment, the consequences have to be clear. But sometimes they go way too far with their stringent punishment procedures.
>
> These same companies can be rather creative with their safety rules when it is convenient for management or profits. Especially when there are KPI's attached to so called safety targets, strange things are happening. Things are 'swept under the carpet'. In incident analysis they are trying to blame third parties instead of looking at their own share. The safety statistics are becoming a target on their own instead of a way to monitor and to analyse what is going on.""

Stage 4 Example 2

> "*And do you get a lot of signals from your colleagues in the field?*
>
> Yes, glad to say yes. It is not always easy. You can imagine there is also this aspect of a blame culture. And sometimes it is annoying to hear that someone dropped something, or a life jacket was blown up because they were playing around. But it is very important to know as much as possible about near misses and I try always to be positive and thank people for coming to me. Open communication is so extremely important.
>
> You will lose people if you will bash them. And you will also lose them if they give feed-back and you do not take them seriously. If you do not follow up on their remarks.
>
> You must motivate them, stay positive and take everything seriously.
>
> It is the same if you go to the police to report that your bike has been stolen. If you do not hear anything afterwards you will never do it again – and yes, it will look like there is no problem there. But if you hear that they have used your information, if you are reported back to, you will also come for the next time."

6.6 Comparison of human and automatic IDDR

Humans play a key role in adapting to variation and change but in a sociotechnical system humans and automatics work together. Fitts (1951) provided a list of functions which are performed either better by humans or by machines. The original text states that:

Humans appear to surpass present-day machines with respect to the following:

- Ability to detect a small amount of visual or acoustic energy
- Ability to perceive patterns of light or sound
- Ability to improvise and use flexible procedures
- Ability to store very large amounts of information for long periods and to recall relevant facts at the appropriate time
- Ability to reason inductively
- Ability to exercise judgment

Present-day machines appear to surpass humans with respect to the following:

- Ability to respond quickly to control signals and to apply great force smoothly and precisely
- Ability to perform repetitive, routine tasks
- Ability to store information briefly and then to erase it completely
- Ability to reason deductively, including computational ability
- Ability to handle highly complex operations, i.e.to do many different things at once.

Despite the advance of technology people still use Fitts' list today. De Winter & Dodou 2014 provide a detailed review of current research which suggests the list is still applicable although computers can now surpass humans on certain cognitive functions. They explain that currently computers usually take care of

data acquisition and automatic control, whereas the operators are left with the tasks of state identification, diagnosis, planning and decision making. The ironies of this position were pointed out by Bainbridge (1983), irony being "combination of circumstances, the result of which is the direct opposite of what might be expected." The result of automation for the operator is:

- (S)he may be expected to monitor that the automatic system is operating correctly, and
- If the automatic system is not operating correctly (s)he may be expected to call a more experienced operator or to take-over himself.

In the case of the latter, Bainbridge (1983) points out that:

> "the operator has in his head .. not raw data about the process state, but results of making predictions and decisions about the process which will be useful in future situations, including his future actions. This information takes time to build up. Manual operators may come into the control room quarter to half an hour before they are due to take over control, so they can get this feel for what the process is doing. The implication of this for manual take-over from automatically controlled plant is that the operator who has to do something quickly can only do so on the basis of minimum information, he will not be able to make decisions based on wide knowledge of the plant state until he has had time to check and think about it."

With the regards the monitoring process she suggests this is even worse because the human cannot quickly enough check that a computer is following its rules correctly so will make judgements on a meta level as to whether the computer's decisions are acceptable. How does the operator know when to take over? The problem with Fitts list then is that it does not account for the fact that humans and automatics need to be an integrated team and work together.

Humans are good at problem solving when they have enough time. Automatics can be valuable for online control when the human needs time to think and work out what is happening having been freed from that requirement. When there is insufficient time this can mean a switch from knowledge based thinking to reflex reaction. When humans do not interact manually with a system, skills can be lost. Apparently Fitts already identified this problem in 1951 arguing also that activity in any task is conducive to alertness, and helps to ensure that the human will keep abreast of the situation.

6.7 The organisational context

The results of the interviews described in previous sections provided scripts from the interviewees which reflect their mental models in terms of controlling high risk situations. In the Storybuilder model (Figure 5 in Section 4.1) the tasks involved in controlling the hazards of a technical system (represented as safety barriers) are resourced by the management system, represented as a set of 8 management delivery systems of resources, in order to control the performance of front line tasks. At the interface with the technical system, performance is adjusted to meet the requirements of the system by making the necessary adjustments to variation and change, affected by the mental models of the system by the managers and operators.
Safety management can be regarded as the management of potential or actual deviations which occur in the primary process of an organisation or activity (Hale et al 1997). have described the focus of safety management as the potential or actual deviations which occur and which are considered as (potential) problems which must be detected, recognised, studied and resolved. As has been shown in Section 4 the resilient barrier is an adaptive intervention particularly in response to unexpected events.

These management processes are represented in the following model for control of a major hazard installation which is adapted from the I-Risk project (Bellamy et al 1999), shown in Figure 28. This is a process model with 9 processes across 3 levels. The system is also affected by the system climate of external demands and resources to which the management system must adapt across the life cycle of the system. This climate will be a source of variation.

At the highest level is the company management system (1) which affects the quality of the safety management system (2) which implements safety policy through establishing a risk control and monitoring

system (RCMS). In the context of being resilient and striving for success rather than avoidance of failures, management of the uncertainties would become a more explicit part of that system. The SMS (2) receives feedback, which is evaluated to determine how well it or the policy and organisation is working (9). That feedback information is generated by the monitoring system (6, 7, 8) at the next level of the management sub-systems. The data collection is based on feedback about plant behaviour, human behaviour and delivery systems, also with respect to external climate such as the occurrence of incidents at other plants. The delivery systems deliver resources through the eight management delivery systems (competence, communications, procedures, motivation, equipment, ergonomics/man-machine interface, conflict resolution and availability of people) to front line tasks for controlling safety (4). The control and monitoring is made possible by the company system for managing and monitoring the delivery systems (3).

The resilience components of adjustment in Section 5 can apply to any of these levels. They should support the mental modelling of the situation and the understanding of the uncertainties and how these can be reduced in future updates.
Looking overall there are therefore different levels of intervention within the management system:

- Changes to the technical system (task outputs)
- Online adjustment of tasks: At this level changes to the way tasks are performed are not permanent. The criteria for flexibility and the individual freedom of decision making for on-line operators and supervisors in adapting the work to circumstance is given by the relationship between 2 and 5.
- Adjusting the way the delivery systems are used: Such changes may include changing procedures,
- Adjust the delivery systems themselves
- Adjust the safety management system
- Adjust policy and organisation

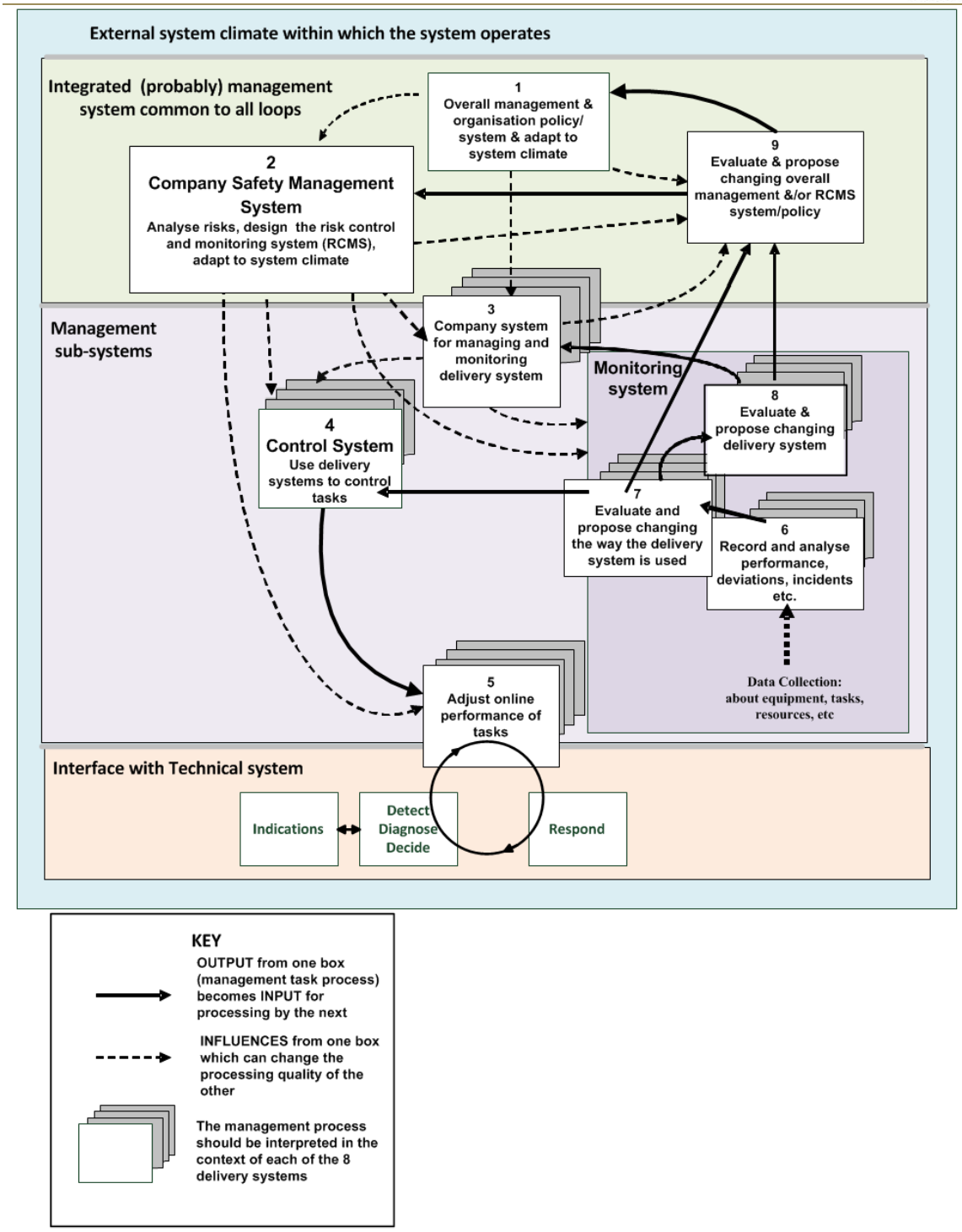


FIGURE 28 THE SAFETY MANAGEMENT SYSTEM AS A CONTROL AND MONTIORING SYSTEM (ADAPTED FROM BELLAMY ET AL 1999)

7 MODELLING THE SUCCESS BOW-TIE

7.1 Introduction

Al the components of the success bowtie have now been introduced in the previous sections. A checklist of the components and guidance on how to use them are provided in Annex D Success Model Event Checklist. An example is given in section 8.2.3.

7.2 STEP 1 Identify the Safety Barriers

The success model event checklist provides a framework for collecting data about the success modes of safety barriers. The success model can be used for analysing deviation events (near misses, unsafe acts, abnormal deviations) with success outcomes. It can also be used for incorporating lessons learned from previous successes and failures.

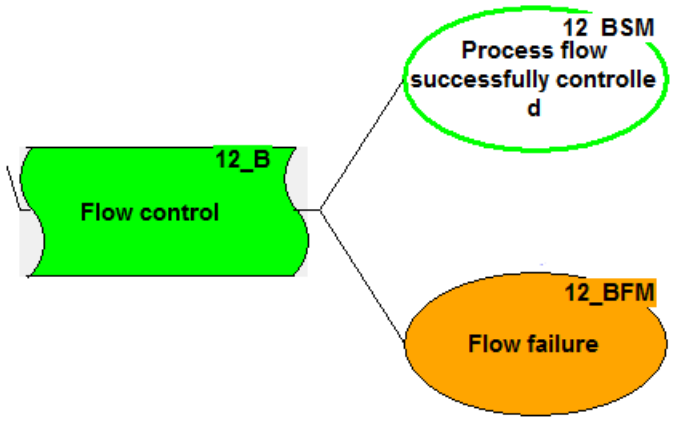


FIGURE 29 STORBUILDER BARRIER EXAMPLE SHOWING BARRIER (B), BARRIER SUCCESS MODE (BSM) AND BARRIER FAILURE NODE(BFM)

Every success mode in a barrier diagram can be developed along the lines of the generic success model

In the model successes are concerned with intervening (or recovering) where a variation or change has been identified that could be a threat to the integrity of the system which controls the hazards. Normal (foreseen) safety critical systems will include predefined safety barriers, i.e. barriers designed or planned to intervene by hardware or procedural action to anticipated potentially hazardous states of the system. This can be presented in a scenario-like way in a safety-barrier diagram. Each barrier "node" demonstrates that when a certain potentially dangerous condition arises there is a need for an intervention (see section 4.6).

7.3 STEP 2 Specify the stage of recovery intervention

The stage of intervention depends on how deep a signal (or precursor) is identified as signalling a condition requiring intervention (see section 6.5). The stages are shown in Figure 30

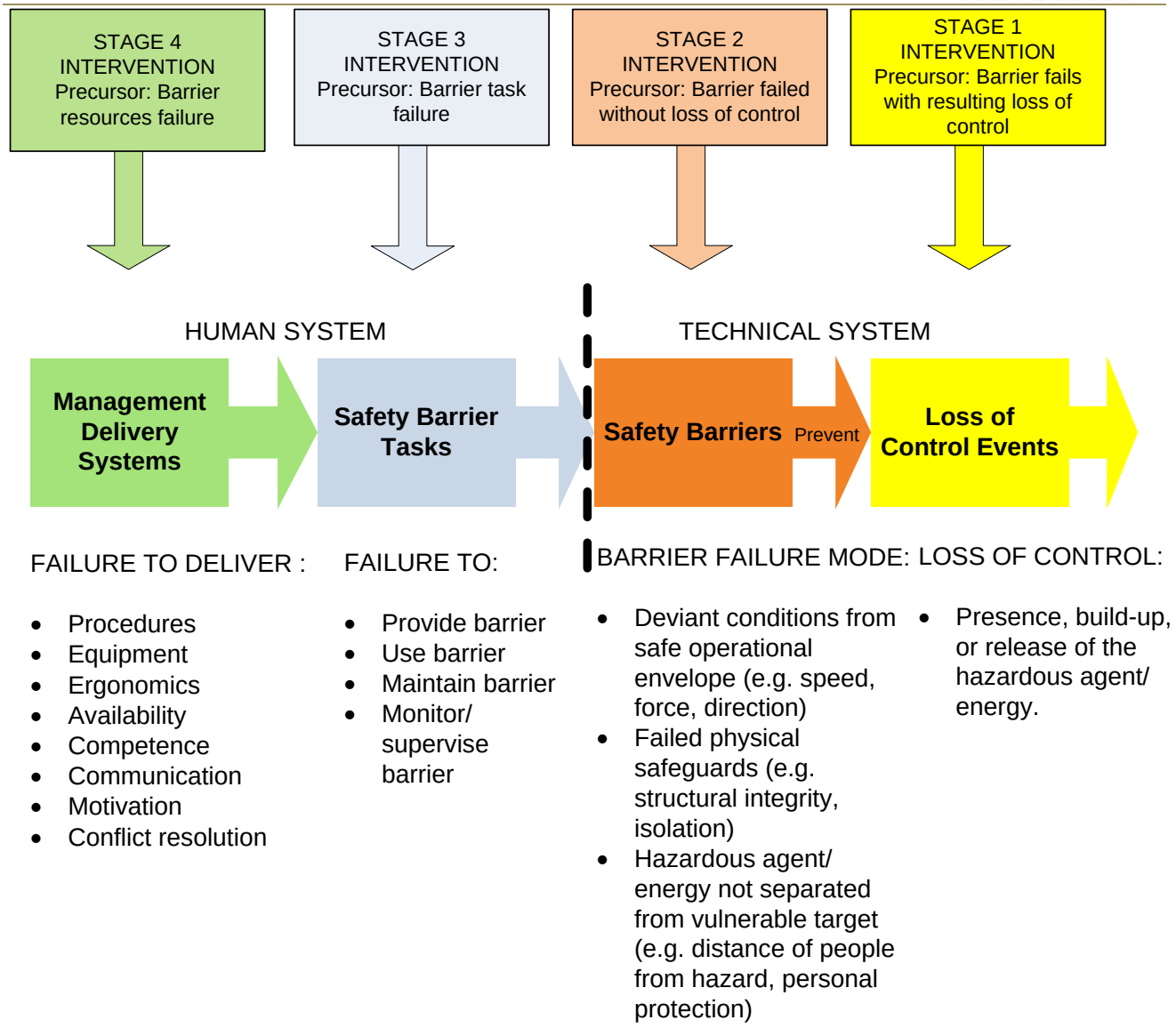


FIGURE 30 STORYBUILDER BARRIER MODEL SHOWING STAGES OF INTERVENTION

The relevant stage depends on the proximity of the precursor to the potential loss of control of the barrier itself. As follows:

- Stage 1 Barrier failure with loss of control
- Stage 2 Barrier failure before loss of control
- Stage 3 Barrier task unsafe
- Stage 4 Barrier management (delivery system) unsafe
- Stage 5 No apparent unsafe condition

e.g. if it is found that a person is carrying out a wrong procedure which could be applied to a major hazard task and result in a major Loss of Containment this would be a Stage 3 or Stage 4 intervention – the person is carrying out the procedure wrongly (stage 3) or the procedure itself is wrong (stage 4).

7.4 STEP 3 Specify the precursors indicating deviation

Identifiable deviations in the different stages can be called potential accident precursors. Precursors can be developed specifically for each intervention stage. These are the events which are signals of deviation or change

7.4.1 Stages 1 & 2

These are failures where there are loss of control events as a result of a barrier failure (Stage 1) or barrier failures but no loss of control yet (Stage 2). For major hazards this is classified into the following types, based on a summation of events from Sonnemans et al (2010).

- Uncontrolled release (Stage 1 only)
- Leakage (Stage 1 only)
- Trip
- Accumulation of materials
- Deviation in process conditions
- Inadequate condition equipment/instrument/storage/tool
- Equipment defects/failures/errors
- Wrong equipment or control settings
- Missing parts/equipment

7.4.2 Stages 3 precursors – barrier tasks

These are failures associated with the human part of the system and may be identified by observation before there is an actual barrier failure. There are potential indications that the tasks which affect the existence and quality of the barriers may be inadequately carried out (See Annex E. Glossary section E.2.2.) e.g. The wrong specification materials have been *provided* for replacing a pipe; an operator goes to *operate* the wrong valve to stop a flow; a maintenance fitter has selected the wrong type of equipment and could fail to *maintain* the barrier function if it is installed; an operator opens a valve and walks away instead of staying to *monitor* that it works as intended

- Provide
- Use/operate
- Maintain
- Monitor

These task failures are identified before they lead to barrier failures.

7.4.3 Stage 4 precursors – management delivery systems

These are failures associated with the management delivery systems which provide the resources to the barrier tasks.:

e.g. nonconformity between drawings (plans and procedures delivery system) and reality as yet without consequence. These delivery systems are defined in the glossary (See Annex E. Glossary section E.2.1.)

- Plans and procedures
- Availability
- Competence
- Communication/ Collaboration
- Conflict resolution
- Motivation/ Awareness
- Ergonomics/ MMI
- Equipment

7.5 STEP 4 Specify process of primary intervention - IDDR

The process between change and outcome is called the IDDR: which is a sequence of Indication, Detection, Diagnosis/Decision, and Response as explained in section 6.1. This process is intended to restore conditions to safety. Following there may also be a longer term intervention (see next step). Of interest in this part of the model are the monitoring of variation or change undertaken by humans and the responses that are made. In this part of the model humans identify change/deviation, decide what to do about it and respond successfully. The IDDR process can be analysed to determine patterns of events and responses that are occurring in response to deviations. Of interest are:

- Indication type and strength of the signal
    - The nature of the signal - salient in an object or the environment (like something missing or smoke) or automated (like an alarm)
    - The strength of the signal (strong, medium of weak)
- Detection
    - Whether it is detected by a person or by automatics
- Diagnosis/decision
    - Whether it is diagnosed/decided by a person or by automatics
- Response
    - Immediate actions. An immediate action might be to operate a valve but further interventions may be carried out (see next section).

Resilient interventions will be primarily human but may have automated components (e.g. alarms and equipment responses to manual initiations).

7.6 STEP 5 Specify process of secondary intervention

The successful outcomes are about adapting to change and variation where the result is that operations can be recovered and sustained. The (improved) barrier conditions that result from the interventions are classified as follows:

- Placement of a new barrier
- Replace barrier with a better one
- Replace barrier: like with like
- Improve or adjust barrier (to its original condition)
- Verify/check barrier
- Analyse barrier problem
- Cease the activity (no new barrier can be identified)

7.7 STEP 6 Specify resilience components present

This concerns components present at the time of decision making. The interventions described in sections 7.5 and 7.6 are the ones to be associated with the resilience components identified in the Resilience Case Studies (Section 5 & Annex B Resilience Case Studies). All the components in place which relate to the successful intervention or lessons learned should be identified and attached to relevant parts of the human system (management delivery systems and/or barrier tasks). A suggested system of attachment is shown in Table 6 based on judgement of how these best relate to one another. E.g. "Getting the little things right" can not only be part of a procedural and competence system but also help resolve conflicts and determine equipment requirements. The resilience components are defined in Annex D. They are;

Learning*: "Knowing what has happened. Capability to learn from past failures and successes - how to learn from experience, in particular to learn the right lessons from the right experience. This is the capability to address the factual."*

- Self-reflection
- Communication/feedback/trust
- Simulation training
- Capture & record
- Cognitive bias mitigation (learning)

Anticipating: *"Knowing what to expect. Capability to anticipate future threats & opportunities - how to anticipate developments and threats further into the future, such as potential disruptions, pressures, and their consequences. This is the capability to address the potential."*

- Scenario-thinking
- Getting (little things) things right (so as not to compromise future states)
- Switched on/vigilant to what can go wrong (risk aware)
- Cognitive bias mitigation (Anticipating)

Monitoring: *"Knowing what to look for. Capability to monitor ongoing developments - how to monitor that which is or could become a threat in the near term. The monitoring must cover both that which happens in the environment and that which happens in the system itself, i.e., its own performance. This is the capability to address the critical, back and forward in time and in three dimensions."*

- Switched on/Vigilant/Alert (for signal detection/change)
- Stop and think (hold points/cross check/pause at critical steps)
- Multidisciplinary/different characters
- Cognitive bias mitigation (monitoring)

Responding: *"Knowing what to do. Capability to respond to events - how to respond to regular and irregular disruptions and disturbances by adjusting normal functioning. This is the capability to address the actual."*

- Experienced people available
- Know the safety margins, one's own limitations
- Consult with others/think together (multidisciplinary/different characters)
- Use of golden rules/principles
- Time and options available
- Cognitive bias mitigation (responding)

TABLE 6 ASSOCIATION OF RESILIENCE COMPONENTS WITH THE MANAGEMENT DELIVERY SYSTEMS

	LEARNING						ANTICIPATING			
DELIVERY SYSTEM	***Self-reflection, willing to learn***	***Communication/ feedback / trust***	***Analyse, discuss & expand events***	***Simulation training***	***Capture & Record***	***Cognitive bias mitigation (learning)***	***Scenario-thinking***	***Getting (little things) things right***	***Switched on/ vigilant/ risk aware***	***Cognitive bias mitigation (anticipating)***
Plans and procedures			•		•			•		
Availability of people									•	
Competence	•			•		•		•		•
Communication/ Collaboration		•	•			•				
Conflict resolution								•	•	
Motivation/ Awareness	•	•					•		•	
Ergonomics				•						
Equipment								•		
	MONITORING				**RESPONDING**					
DELIVERY SYSTEM	***Switched on/dynamic vigilance /alert***	***Stop and think (hold points, pause, check)***	***Multi-disciplinary/ characters***	***Cognitive bias mitigation***	***Experienced people available***	***Know the safety margins***	***Consult/ Think together***	***Use golden rules***	***Time and options available***	***Cognitive bias mitigation (learning)***
Plans and procedures		•						•		
Availability of people	•		•		•				•	
Competence				•	•	•				
Communication/ Collaboration							•			
Conflict resolution		•						•	•	•
Motivation/ Awareness	•		•			•	•			
Ergonomics	•								•	•
Equipment										•

7.8 STEP 7 Uncertainties and outcomes

The "success model" as defined contains all the resilience characteristics that an individual or an organization (the "agent") should exhibit in order to succeed in a specific mission. Regardless of the degree of resilience of an agent there is no certainty that the mission will be always completed successfully. The character of the proposed model is prescriptive, that is it prescribes what an agent should do to be resilient and hence having more chances of successfully completing a specific mission. A basic assumption of the proposed approach is that

- The more resilient the agent, the more likely it is to successfully complete the mission

Given the developed success model, an agent can be characterized by any out of possibly a very large number of combinations of resilient characteristics. Let us assume that it is possible to divide the set of all possible combinations into three classes corresponding to three degrees of resilience:

- High resilience

- Medium resilience
- Low resilience

The number of classes can be as high as necessary but we will consider only three.

An agent of High resilience will face the successful completion of a mission (to be executed either once or repeatedly) with high likelihood. We can then say that the successful completion of the mission is associated with Low Uncertainty. Similarly Medium resilience is associated with Medium uncertainty and Low resilience is associated with High Uncertainty.

This consideration can be included in the success model by adding just before the final success node three (or as many as have been defined) uncertainty nodes:

- Low uncertainty
- Medium uncertainty
- High uncertainty

A success path just before reaching the successful intervention node will have passed through a number of resilience characteristics and hence it will be characterized by a degree of resilience (in this case H, M or L). Depending on the degree of resilience that characterizes the path it will then pass through the corresponding node of uncertainty (Low, Medium or High).

The type of uncertainties that can be reduced in this way are:

- Knowledge (epistemic) uncertainties (see section 3.1).

It is noteworthy that a High-Resilience agent may still fail as a result of a combination of various random variables and parameters that could not be handled by the specific agent. Similarly a Low-Resilience agent may succeed as a result a combination of random variables and parameters that constitute a faced challenge.

Finally we can think of the Centre Event of the success bowtie as a three (or as many levels of resilience we have considered) state event:

- 1 Success coupled with Low Uncertainty;
- 2 Success coupled with Medium Uncertainty; and
- 3 Success coupled with High Uncertainty.

The overall success model with resilience components can be seen as a means to handle uncertainties associated with success of a mission.

It is important to recognize that this type of uncertainty characterizes the degree of belief of an outside observer (but also of the agent himself) that the mission of an agent that has a given degree of the suggested resilience components will be successful. In this sense it can then aid the decision-making (IDDR) process as to whether and to what extent the proposed response will be adopted.

In addition to the overall uncertainties associated with the level of resilience adopted by an agent, there are other types of uncertainties associated with various phenomena and/or parameters that are included in the model. These depend either on the true stochastic nature of the phenomenon (e.g. weather or the strength of a particular component as it comes out of a production process) and other situations faced by the agent during the execution of a mission.

Recognition, evaluation and consideration of these uncertainties are characteristics of resilience. These uncertainties include:

- Statistical uncertainty (aleatory): This concerns the uncertainties that adequately may be expressed in statistical terms; for example, as a range with associated probability. In the natural sciences, scientists generally refer to this category if they speak of uncertainty, thereby often implicitly assuming that the involved model relations offer adequate descriptions of the real system under study, and that the data or calibration data used are representative of the situation under study.
- Scenario uncertainty: This concerns uncertainties specified in terms of possible outcomes. For these uncertainties the mechanisms that could lead to the outcomes are not sufficiently known. Scenario uncertainties are often construed in terms of 'what-if' statements.

These uncertainties can be influenced by the amount of information available to the agent and whether (as a resilient characteristic) the choice of obtaining more information is an option for the agent. E.g. supposing a weather forecast is important for evaluating the risks of undertaking an activity. If the weather after 2 pm is of importance and a weather forecast is available at 8:00 am, the agent might have the option to wait until noon to obtain a new forecast. Additional information might not necessarily decrease the associated uncertainty. For example at 8:00am the forecast might give a 20% chance for stormy weather. A decision could be made on this forecast and let's assume that the decision would be: go ahead. If on the other hand it would be possible to postpone this decision and get a forecast at noon then there would be a more reliable forecast to base the decision. Of course the noon forecast could be 50% chance for a storm and in this case the decision might be not to undertake the excursion. The second forecast represents higher uncertainty about which type of weather will prevail. This however does not hinder the making of a decision. Part of the resilience characteristic is the ability to make decisions in the face of uncertainty and in particular when all the possible future outcomes of uncertain events are not known or prescribed.

Example (as told by a mountain guide):

> "There was this canyoning guide that went canyoning with his clients for some days. Every day the weather forecast was 'sunny with a probability of thunderstorms in the afternoon'. Thus the first day they did something not too long, because of this risk likelihood of thunderstorm. In the evening: blue skies. The second day, same kind of weather and he takes the same decision: not to go into a long more difficult project. The third day: same situation. However his clients started to put a little pressure on him. For four days this went on and for four days there was no thunderstorm in the evening. The fifth day they forecasted the same kind of weather. The guide decides to go into this long and complex canyon because that was the main objective of his clients for this particular week. And paf: the thunderstorm strikes that day which results in 2 deaths".

This behaviour indicates a lack of resilience from the side of the guide; he was biased by the first four days and did not maintain the same decision rule on day 5. The potential outcomes of the uncertain event "weather" are known (i.e. good or bad weather). The relative likelihood of each outcome is assessed by the weather forecast. The degree of risk aversion expressed by the guide in the first four days was not maintained for the fifth with the catastrophic results. If he had done the complex canyoning on day 4 the result would have been a success but this would have been success coupled with high uncertainty. Many of the factors listed in Table 6 could have been used but were not.

7.9 Summary of the success bow-tie scheme

7.9.1 Overall scheme

Figure 31 shows the overall scheme of the success bowtie. The success bow-tie is a single bow-tie. Any type of success event can be taken through the model with the following fields:

- Date
- Type of event
- Stage
- Precursors: Barrier management delivery system deviations (Stage 4)

- Precursors: Barrier task deviations (Stage 3)
- Barriers (per line of defence)
- Precursors: Barrier failures (Stages 1 & 2)
- IDDR block
- Management delivery systems for IDDR
- Resilience components
- Barrier tasks for IDDR
- Indicate, Detect Diagnose, Respond
- Uncertainty
- Management delivery systems for interventions
- Barrier tasks for intervention
- Interventions
- CENTRE EVENT: Successful intervention
- Success outcomes with uncertainties

7.9.2 Calculating the outcomes

The centre event is a 3-state event of success. Interventions may be supported by low, medium or high resilience. The resilience components are uncertainty reducing; occurrences of success are successful interventions with high, medium or low uncertainty depending on whether there was low, medium or high resilience respectively. A simple way to determine the uncertainty reduction of an intervention is to specify the number of resilience components active in a given scenario. There are 20 components. These components have been associated with the 8 management delivery systems of Storybuilder (Annex E.2). A scale of uncertainty reduction can be expressed as follows:

- 0-6 Components identified at least once: Low resilience → High uncertainty
- 7-13 Components identified at least once: Medium resilience → Medium uncertainty
- 14-20 Components identified at least once: High resilience → Low uncertainty

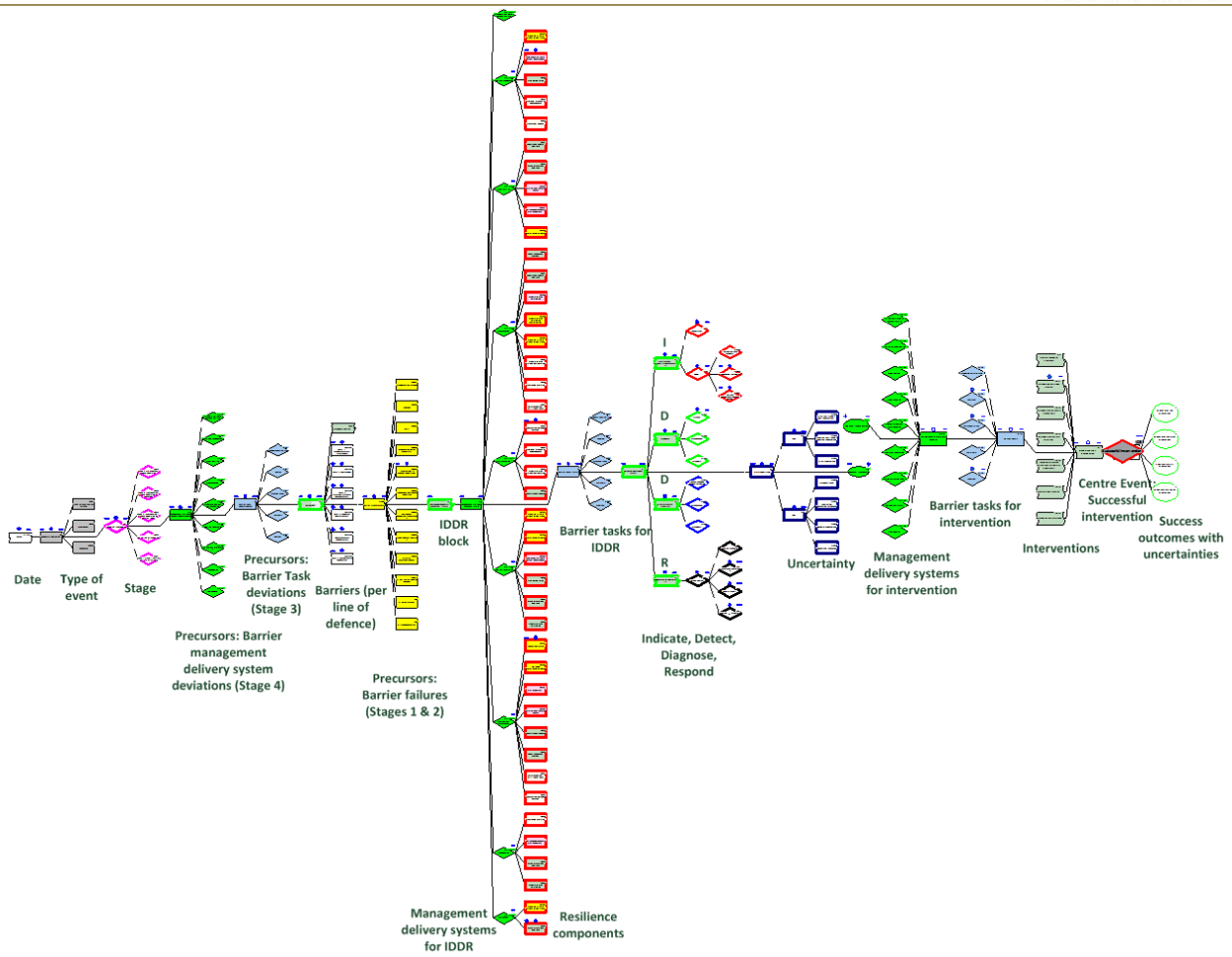


FIGURE 31 SCHEME OF THE SUCCESS BOW-TIE

8 ANALYSIS OF INCIDENTS IN THE SUCCESS MODEL

8.1 Databases

A separate report - Lessons learned, near misses and unsafe conditions (Annex C Lessons learned, near misses and unsafe conditions, Baksteen 2015) provides an analysis of a sample of lessons learned from accident reports and a company database of near misses & unsafe conditions.

The research behind this Annex C examined:

- Accidents from the ARIA database (ARIA 2012) sample of 7 with lessons learned
- A company database of near miss and other incident data, sample of 59 Stage 1 near misses and 27 events with interventions at an earlier stage (see section 6.5).

It should be noted that the analyses were done before the success model was entirely finalised, and in fact the analyses themselves played a feedback role in adjusting the model. So some evaluations in the model have been undertaken in addition to the primary work in Annex C.

The ARIA (analysis, research and information on accidents) database[15] operated by the French Ministry of Ecology, Sustainable Development and Energy lists the accidental events which have, or could have damaged

[15] http://www.aria.developpement-durable.gouv.fr/about-us/the-aria-database/?lang=en

health or public safety, agriculture, nature or the environment. These events are mainly caused by industrial or agricultural facilities that have been or are likely to be classified as hazardous, but also by transportation of hazardous materials and other events with lessons that also apply in this context. The list of accidents and incidents in France and abroad, which cannot be seen as exhaustive, together with analysis of them, has been in place since 1992. With all activities taken together, this database lists over 40,000 accidents and incidents, of which about 37,000 in France. Foreign accidents are listed mainly due to the seriousness of their consequences or their value in terms of experience feedback.

A company database from an 11 year period (1994-2004) contained around 6.000 near misses of which there were nearly 600 "*process*" near misses. Of those process safety near misses 86 near misses were selected based upon the potential risk to result in an undesired release of hazardous substances. This selection was based upon the description of risks in the 'risk description' column of this database. Examples of those 'risk descriptions' are: *environmental load, exposure (to chemicals), fire (risk), explosion (risk), soil contamination, emissions, leakages, overfilling, etc.* Another criterion was the following categorization that was used in the database: *environmental, health, quality, reliability and safety*. These categories combined with the risk descriptions has resulted in the selection of the 86 events with a risk potential for an undesired release of hazardous substances (loss of containment)..

The other process safety events were classified as near misses with other types of potential risks (without any risk for an undesired release of hazardous substances): process failures, damage to equipment, deviating process conditions, productivity loss, decreased plant performance, off spec products, short circuiting, decrease of throughput, contamination of utilities, limitation of process capacities, difficulties with starting up, etc.

The investigated near miss database consisted not only of near misses but also of unsafe conditions and sometimes even accidents. For this project a ***near miss*** was defined as *'a deviation that was disarmed by an intervention before it developed into a critical event'*. When investigating process safety near misses the critical event is the undesired event of the release of a significant amount of hazardous substance(s) (so called Loss of Containment event). Significant amounts of hazardous substances are amounts that could be called a major hazard accident. For the process safety near miss the deviation results in a barrier failure which leads to a loss of control event, such as a process deviation, which is going outside the safe boundary or a loss of containment has already occurred. A process safety ***unsafe condition*** is a condition that, if not controlled, or in combination with another condition or event, can lead to a near miss as defined above or eventually a release of a significant amount of hazardous substance(s), but at this stage there is no loss of control event outside the safe boundary.

Small leakages and small undesired releases of hazardous substances have been classified as near misses because the estimation is that the amount of released hazardous substance(s) is not enough to be a reportable major hazard accident (within company, nationally or at a European level). There were 86 selected near misses/unsafe conditions involving barrier failures; according to the above mentioned definitions 59 were near misses and 27 were unsafe conditions.

The data were entered into Storybuilder™. The actual major hazard *success* database can be downloaded from the resources section of the website of the Resilience Success Consortium[16]. The software for viewing the success bow-tie and the major hazard *failure* database as well as user manuals can be downloaded from the RIVM website[17] [18].

[16] http://www.resiliencesuccessconsortium.com/resources
[17] **http://www.rivm.nl/en/Topics/O/Occupational_Safety/Other_risks_at_work/Dangerous_substances**
Information about major hazard model and link to download Storybuilder and databases.

8.2 Results

8.2.1 Lessons learned

The lessons learned data were disappointing in terms of trying to identify resilience components that were incorporated into lessons. Of the 7 accidents, the lessons learned identified indicated that the following were important issues:

8.2.1.1 PERFORMANCE OF SAFETY STUDIES

Safety studies prior to the design and/or installation of equipment are of major importance for a safe operation of installations. Safety studies should be performed in such a way that all significant hazards are identified and all risks of all identified hazard are properly evaluated. The right standards should be used to determine the requirements of expertise and knowledge of the experts performing the safety studies. Hazards and risks can be easily overlooked because of the fact that the focus is most of the time on the most likely and potentially severe company risks, forgetting other types of risks (e.g. focus on toxic ammonia releases, forgetting the possible adverse effects of high steam pressure, because the hazardous properties of ammonia are much more obvious than the hazardous properties of water).

8.2.1.2 APPLYING A SOUND RISK MITIGATION AND CONTROL SYSTEM

There should also be a good mitigation and control system in place which has to be applied on all evaluated risks. This system should be based on a sound risk mitigation and control philosophy (e.g. the prevention of a runaway reaction cannot be managed by standard operating procedures only but should at least be managed by the use of an inherently safe design of the installation).

8.2.1.3 INSPECTION PROGRAMS

Inspection and/or monitoring programs to control the material condition of equipment are of major importance, not only during the operation of an installation but also prior or at the beginning of the installation of the (process) equipment. It is of major importance to check whether the right equipment materials are used when new equipment is installed. During the operation it is important that inspection programs are followed which cover all kinds of equipment degradation processes and which do not overlook certain significant parts of the installation.

8.2.2 Resilience and lessons learned

The above issues give rise to concerns about the following

8.2.2.1 ANTICIPATION :

In the performance of safety studies scenarios were not identified e.g. Failure to see that a change would give rise to a change in the state of the compounds; failure to include domino effects; failure to consider other hypotheses. The results suggest that cognitive bias mitigation would help to improve the response of individuals and teams when conducting safety studies.

8.2.2.2 MONITORING:

There were failures to detect conditions e.g. failure to systematically record information about certain operational parameters; failure to formalise monitoring procedures; failure to notice environmental conditions; failure to assist operators with rapid detection (such as alarms). The results suggest more formalisation of monitoring is required to maintain alertness and vigilance and to have alarms in place when events can develop rapidly.

[18] **http://www.rivm.nl/en/Topics/S/Storybuilder** Information about Storybuilder in context of occupational safety with links to download, user manuals, factsheets and more.

8.2.2.3 RESPONDING

In responding there were failures to correctly respond under e.g. degraded operational conditions; lack of understanding; knee jerk responses under time pressure. Experienced trained people are needed for changed conditions and emergency response. When an unusual response is called for (like unusual maintenance) this should trigger an evaluation – consult with others, perform a risk analysis (Anticipation), monitor the process in response to actions (Monitoring). Amongst resilient components important here are knowing the safety margins and mitigating cognitive biases of responding like summit fever and overconfidence and switching from Responding to Monitoring (stop and think) before making unusual actions.

8.2.2.4 LEARNING

There were failures to learn from other events. E.g. Not taking account of operator feedback after a recovery; not evaluating whether other events have occurred in order to enhance anticipatory thinking. Even if events turn out successful they should be captured/recorded and quickly responded to. There should be a striving to capture information and to use this as a basis for analysing, discussing and expanding on events. This can help improve safety studies.

8.2.3 Translating lessons learned into the success model

Although the main components of lessons learned are risk focused and concentrate on the normative processes of risk control, it is possible to add resilience components by judgement since in effect the lessons can be translated into lessons for consideration for resilience. For example, not communicating the alarm to the local residents in the event of an incident can damage building up trust with them - so the lesson learned would be that it is important for the resilience component *Communication /feedback/ trust*. Taking the accident for which this is an example, the way in which this can be considered in the model is to implement the lessons learned as IDDR components and to indicate the presence of resilience components which could be enhanced with the specific lesson.

One of the accidents from Annex C was used: Bursting of a high-pressure steam pipe in a French ammonia installation (ARIA nr. 38831). The consequence was that a missile was projected across the plant. The projection of this piece of equipment led to no injuries, yet still caused damages inside the unit: a grated walkway
was torn down, and a safety ladder sustained damage. The missile was ejected above the ammonia receiving

bottle and above an ammonium nitrate conveyor belt to come crashing down between two railway lines. Though these lines happened to be empty on the day of the accident, they were often used to park railcars loaded with ammonia. In other words, the accident could have been much worse. There had been no documentation on the correct specifications of the materials and subsequent investigation found more cases of wrong materials used. The lessons learned scenario was entered into the success model and is shown in Figure 32, Figure 33 and Figure 34. Because the lessons learned do not specifically give an indication about the company's resilience this is a speculative exercise involving judgement about the lessons for resilience.

The results are as follows:

Figure 32:

- Date : 2010
- Type of event: *Lessons learned accident*
- Stage: *Stage 1 signal Barrier failure with loss of control*
- Precursors: Barrier management delivery system deviations (Stage 4): *Plans & procedure, Communications*
- Precursors: Barrier task deviations (Stage 3): *Operate, maintain & monitoring deviations*
- Barriers (per line of defence): *Equipment material failure (barrier 4) and Sheltering failure (barrier 40)*

Figure 33:

- Precursors: Barrier failures (Stages 1 & 2): *Uncontrolled release; Falling, moving obejcts/missiles*
- IDDR block: Showing lessons learned in the following components:-
- Management delivery systems for IDDR: *Plans & procedures, Communication & collaboration, Motivation/awareness, Equipment.*
- Resilience components:
    - Associated with plans and procedures: *Resilient monitoring (RM) - Stop and think (hold points, pause, check)* where thought should be given to what should be checked –. The turquoise diamonds in Figure 33 with the code IF indicate additional information (incident factors) which have been added: These are *List of what to monitor/inspect, Inspection plan, Monitoring procedures and documentation, construction documentation.*
    - Associated with communications is *Resilient Learning (RL) - Communication/ Feedback/ Trust,* which was associated with making the communications in exercising the *emergency plan.*
    - Associated with motivation/awareness is *Resilient anticipation (RA) - Scenario thinking*. This was a near miss with potentially serious *Domino effects* involving *Pressurised steam equipment.* Also *Resilient Responding (RR) - Know the safety margins.* Being aware of the specifications of the materials is one of the considerations of "know the safety margins" and of the motivation/awareness required.
- Associated with equipment: *Resilient Responding (RR) - Time and options available* – associated with the latter is the incident factor *Specialised monitoring equipment*.

Figure 34:

- Barrier tasks for IDDR: *Maintain* and *Monitor*
- Indicate, Detect Diagnose, Respond: There was *salient object/environment change* – signals of *degradation of materials* with *human* detection and response selection followed by *direct action* to *repair/install.* This action was a *change of equipment.*
- Uncertainty: *Scenario uncertainty; Low resilience – High uncertainty*
- Management delivery systems for secondary interventions: *Equipment*
- Barrier tasks for intervention: *Provide*
- Secondary Intervention: *Verify/check barrier; Replace barrier with a better one*
- CENTRE EVENT: Successful intervention
- Success outcomes with uncertainties: *Success with high uncertainty*

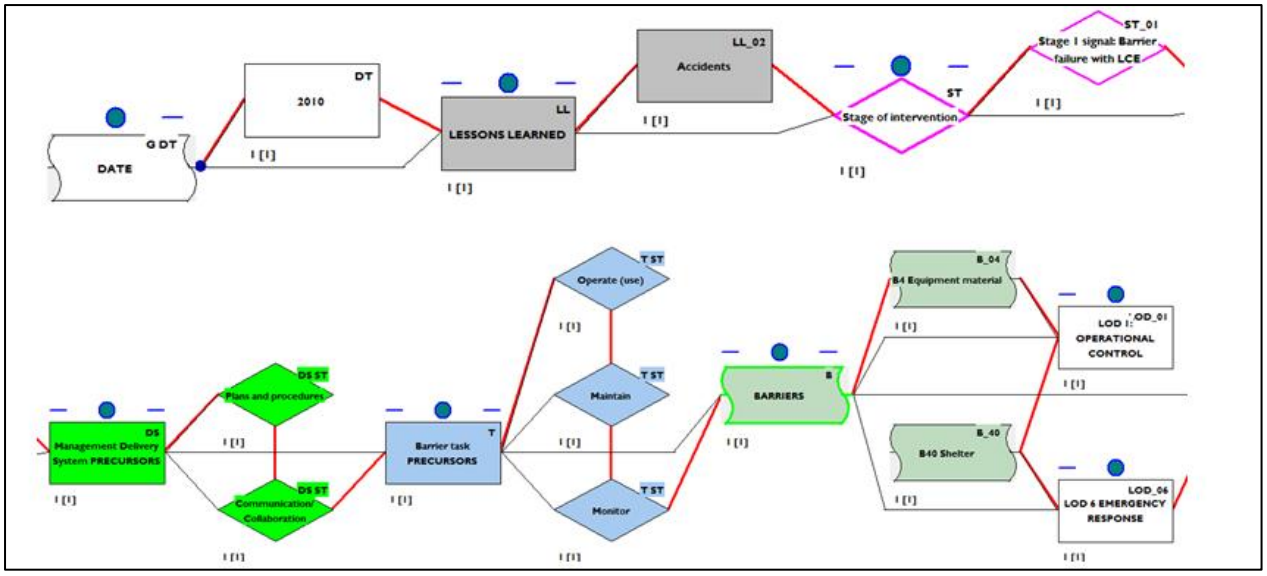


FIGURE 32 ACCIDENT ARIA ACCIDENT 38831: BURSTING OF A HIGH PRESSURE STEAM PIPE, FRANCE 2010[15] (SEE ANNEX C) SEGMENT 1 AS SEEN IN STORYBUILDER. THE NUMBER BELOW THE BOX INDICATE 1 INCIDENT PASSING THROUGH THE BOX, THE RED LINE CONECTING THE EVENTS OF THE ACCIDENT'S LESSONS LEARNED. THE BOTTOM LINE OF EVENTS IS A CONTINUATION OF THE TOP LINE.

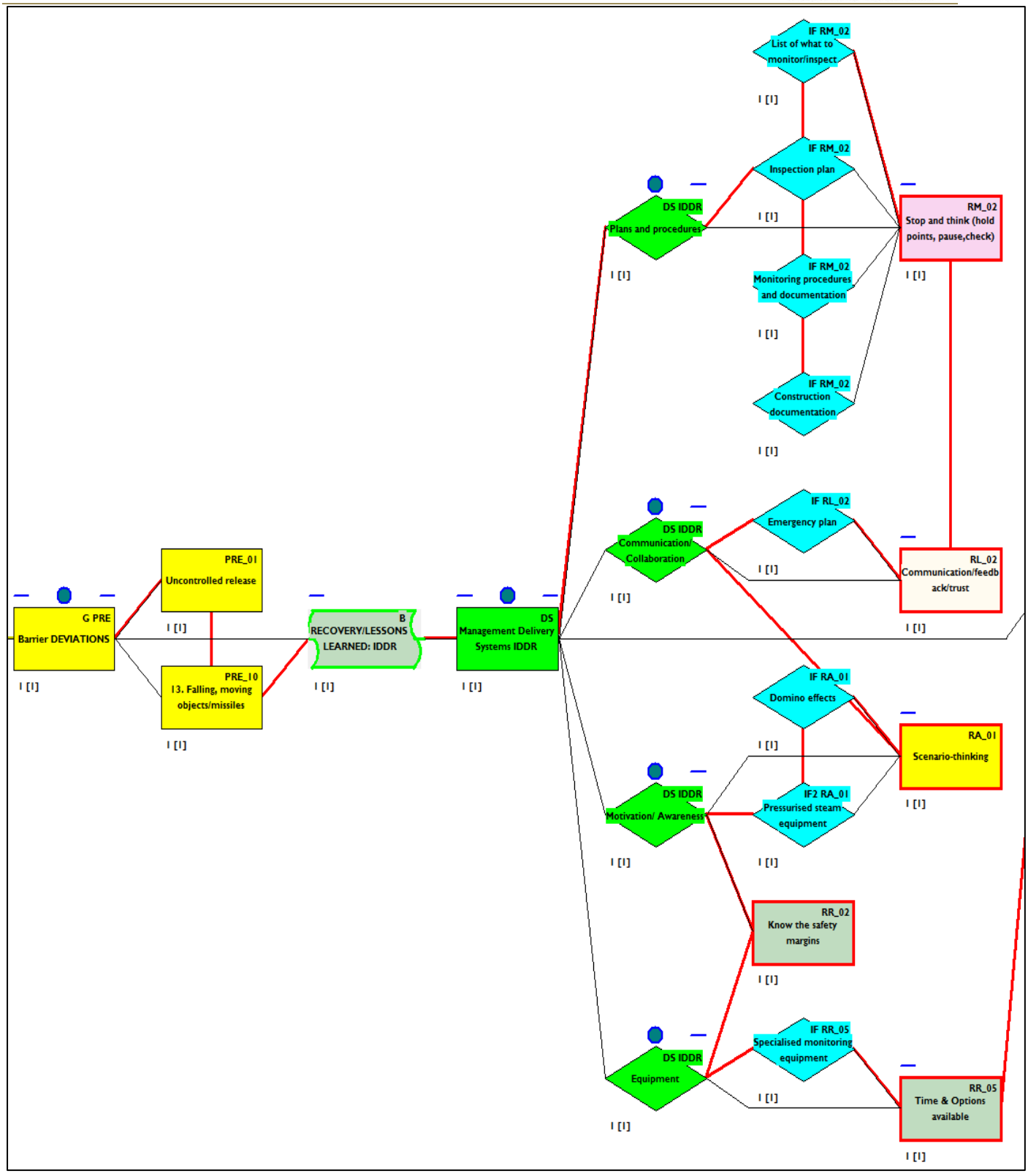


FIGURE 33 ARIA ACCIDENT 38831: BURSTING OF A HIGH PRESSURE STEAM PIPE, FRANCE 2010 (SEE ANNEX C) SEGMENT 2 AS SEEN IN STORYBUILDER. THE NUMBER BELOW THE BOX INDICATE 1 INCIDENT PASSING THROUGH THE BOX, THE RED LINE CONECTING THE EVENTS OF THE ACCIDENT'S LESSONS LEARNED

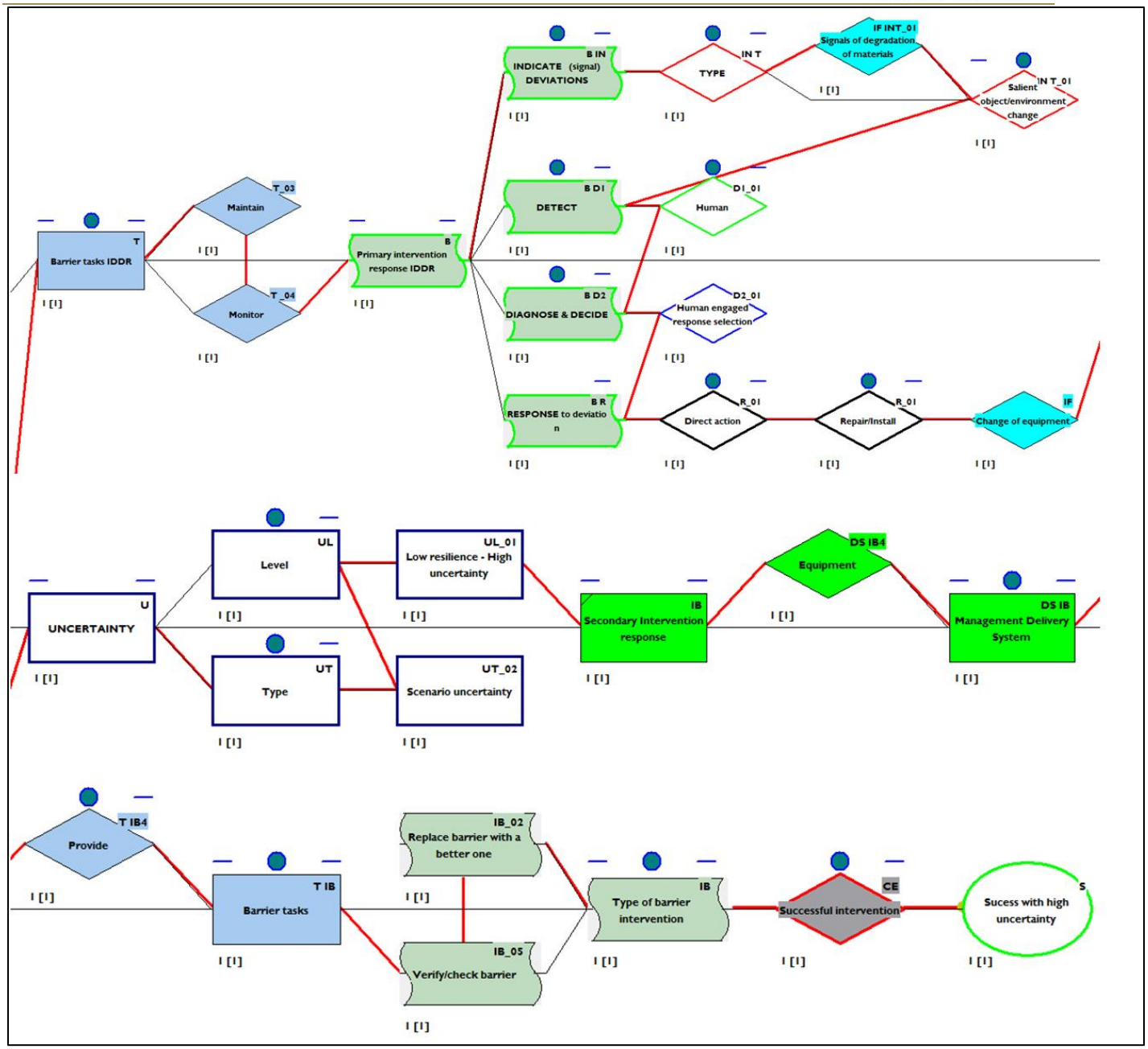


FIGURE 34 ARIA ACCIDENT 38831: BURSTING OF A HIGH PRESSURE STEAM PIPE, FRANCE 201015 (SEE ANNEX C AND) SEGMENT 3 AS SEEN IN STORYBUILDER. THE NUMBER BELOW THE BOX INDICATE 1 INCIDENT PASSING THROUGH THE BOX, THE RED LINE CONECTING THE EVENTS OF THE ACCIDENT'S LESSONS LEARNED. THE 3 ROWS OF EVENTS ARE A CONTINUOUS LINE IN THE DATABASE

8.2.4 Near Misses

The near miss data did not contain any indications of presence or absence of resilience components. Each case was quite short. All cases of the 59 near misses were determined to be Stage 1 failures, meaning that they were not detected until there was a barrier failure with a loss of control event. The aggregated results are shown in the following Figures.

Figure 35 shows the barrier failures which start the near miss incident sequence. These are mostly first line of defence (LOD) failures, these being mostly pressure and flow control failures.

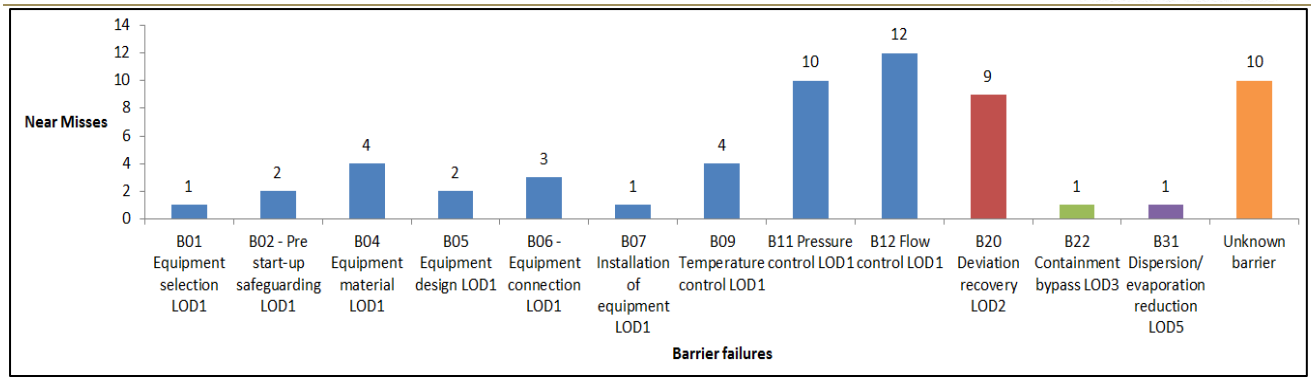


FIGURE 35 STAGE 1 BARRIER FAILURES FOR 59 COMPANY NEAR MISSES, MAJOR HAZARDS RELATED. LOD INDICATES THE LINE OF DEFENCE. N.B. ONE EVENT INVOLVED 2 BARRIERS

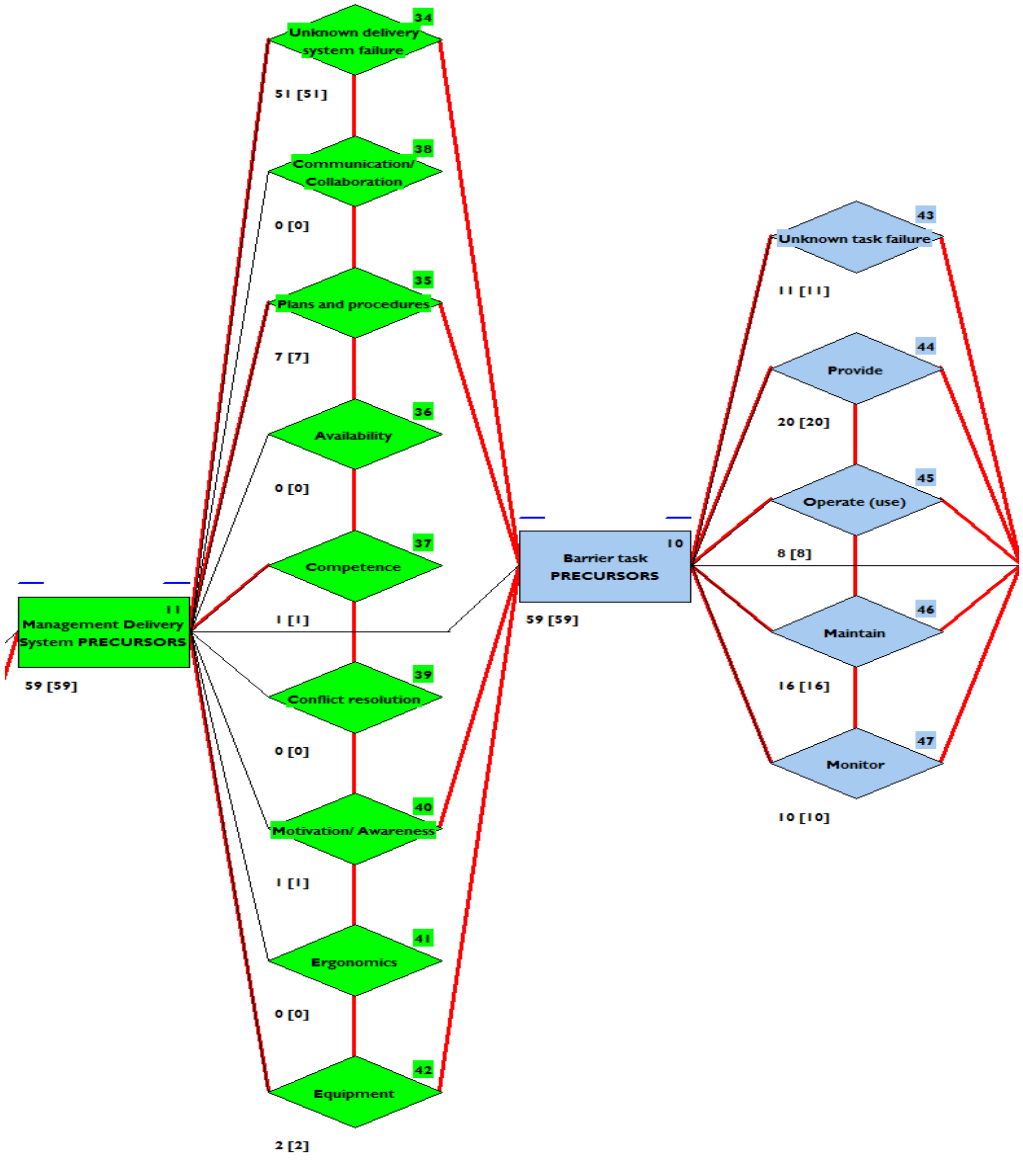


FIGURE 36 MANAGEMENT DELIVERY SYSTEM AND BARRIER TASK FAILURES FOR 59 COMPANY NEAR MISSES, MAJOR HAZARDS RELATED (STORYBUILDER VIEW)

In Figure 36 it can be seen that most management delivery system (DS) failures are unknown (51). Of the known DS failures plans and procedures failures are the most common (7). Barrier task failures have only 11 unknowns. Providing an adequate barrier is the most common task failure (20) followed by failing to

maintain it in the required state (16). Figure 37 shows the number of precursor events which are primarily deviations in process conditions (24 near misses) and 27 loss of containments of which around half were smaller leakages. Figure 38 shows that on the whole the nature of the indication in the IDDR was not specified (66%) but it was identified that 14% were automatic indications and 20% a salient change.

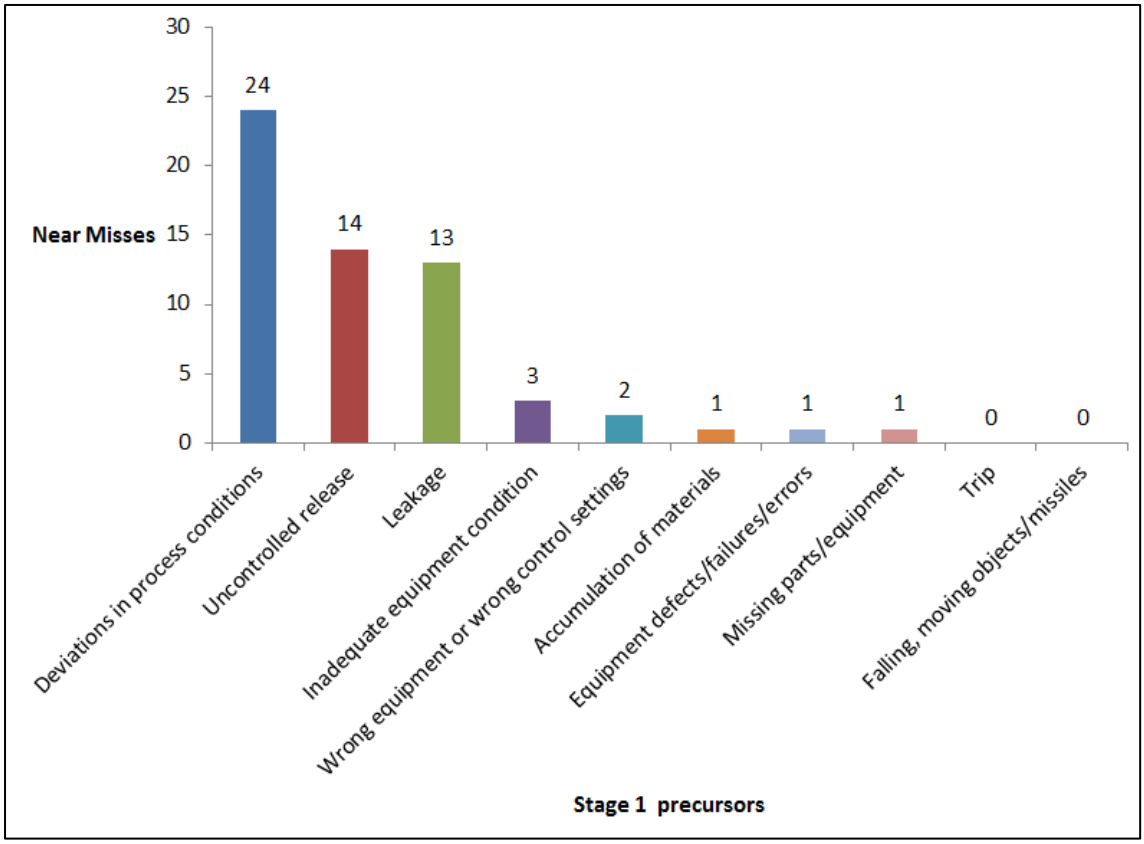


FIGURE 37 NUMBER OF NEAR MISS PRECURSORS AT STAGE 1 INTERVENTION FOR 59 COMPANY NEAR MISSES, MAJOR HAZARDS RELATED

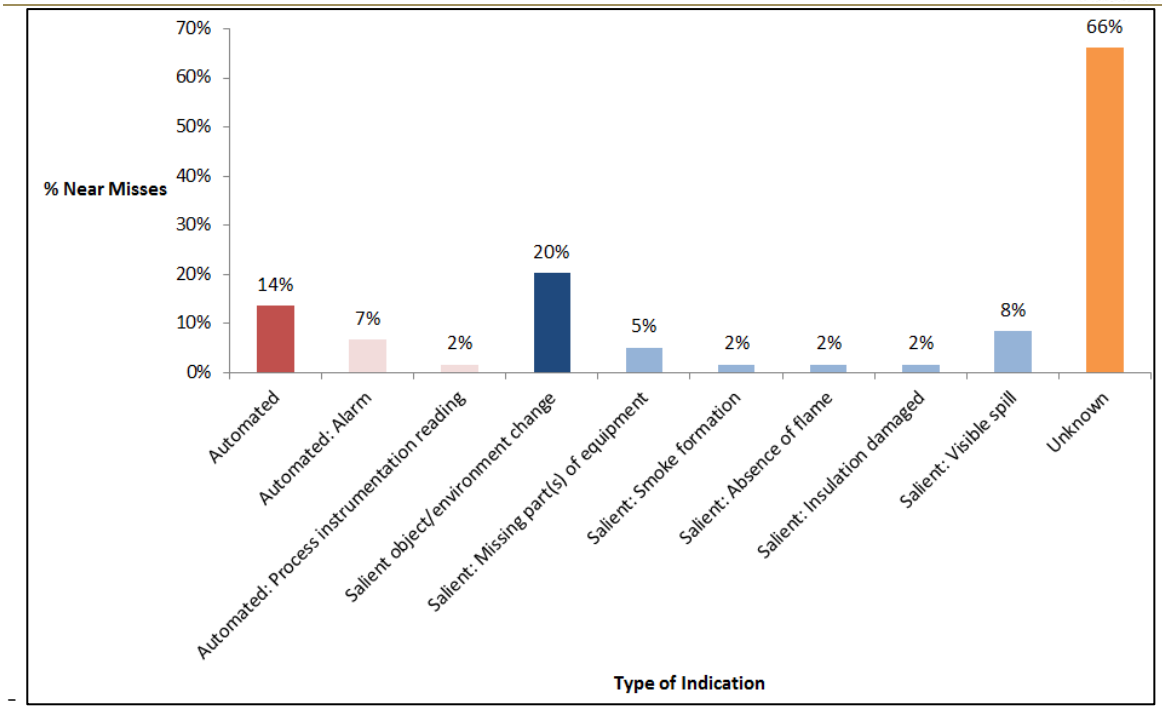


FIGURE 38 TYPE OF SIGNAL INDICATION OF STAGE 1 PRECURSORS: PERCENTAGE OF 59 COMPANY NEAR MISSES, MAJOR HAZARDS RELATED

Detection, where identified, was always human, as shown in Figure 39 and similarly in Figure 40 for diagnosis & decision.

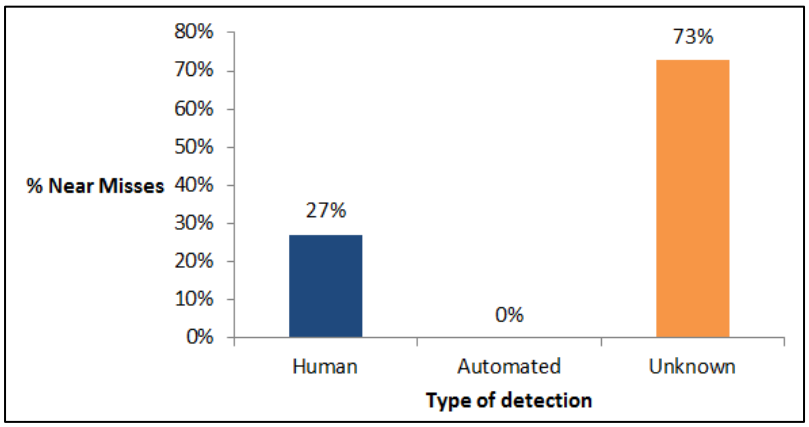


FIGURE 39 TYPE OF SIGNAL DETECTION: PERCENTAGE OF 59 COMPANY NEAR MISSES, MAJOR HAZARDS RELATED

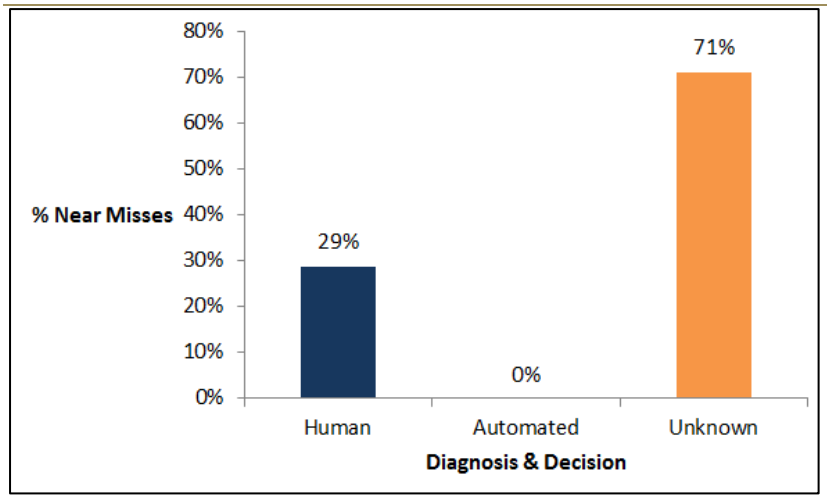


FIGURE 40 TYPE OF DIAGNOSIS & DECISION: PERCENTAGE OF 59 COMPANY NEAR MISSES, MAJOR HAZARDS RELATED

Figure 41 shows the type of direct action (R in the IDDR). This was primarily related to actions on valves/flow (53%, 31 incidents). 13 of these actions involved stopping or reducing flow or stopping equipment and 6 were redirecting gas/liquid (to a safe place). 25% (15 incidents) of direct actions were repairs/corrective actions such restarting pilots/flare or tightening equipment parts or repairing tracing.

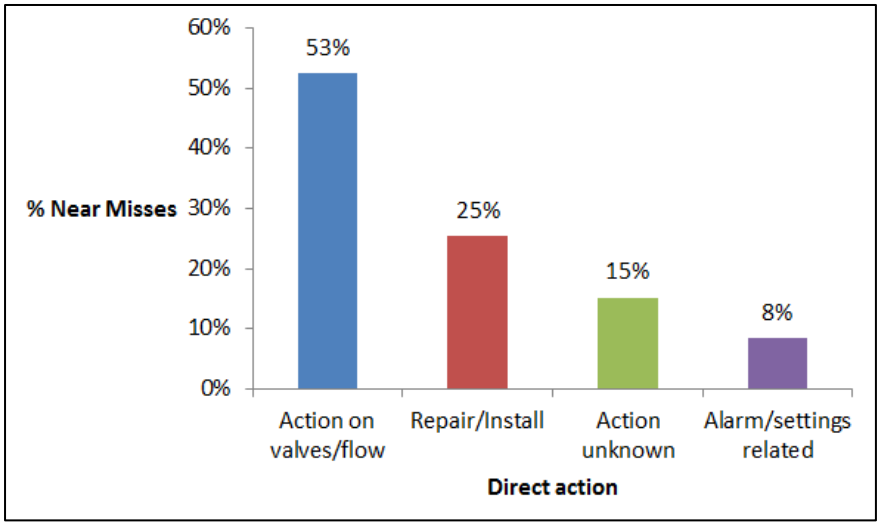


FIGURE 41 TYPE OF DIRECT RESPONSE FOLLOWING DETECTION AND DIAGNOSIS OF STAGE 1 PRECURSORS: PERCENTAGE OF 59 COMPANY NEAR MISSES, MAJOR HAZARDS RELATED

The interventions on the barriers which subsequently occurred, sometimes after investigation or further analysis, are summarised in Figure 42. The results were as follows:

- Improving the barrier or adjusting to its original conditions (34%). In the control of process parameters (pressures, temperatures and flows) it is very important that the settings are right. The analysis shows that in many cases the settings were poor or wrong and that barriers had to be improved by improving barrier settings. Other actions to bring the barrier back to its original function involved cleaning, repair, removing of blockages and tightening of connections and equipment.

- In 20% of cases the action was to verify or keep a check on the barrier. To maintain a barrier function the 'checking' of the (right) barrier function is an important factor to determine whether the quality of the barrier function is still at an acceptable level. The checking concerned the checking of valves, meters, flames, process control rounds, ignition equipment and electronics.
- 12% of cases involved replacement of a barrier with a better one. These are actions where better ways to operate are found (e.g. agitate, dose, etc.), where better materials are introduced or where better equipment (gaskets, valves, seals, etc.) is introduced.
- In 10% of cases a new barrier was provided for the performing of the barrier function. Sometimes barriers are not there at all and should be placed. These are completely new barriers for the specific situation. Examples are: a remotely operated valve in an off gas line, a flow valve, equipment to measure the pressure, a standby steam hose, thermo-couples.
- In 3% of the cases the problem was analysed but the outcome unknown.. In the two cases involved the barrier function was also checked
- In the other cases the barrier response was unknown.

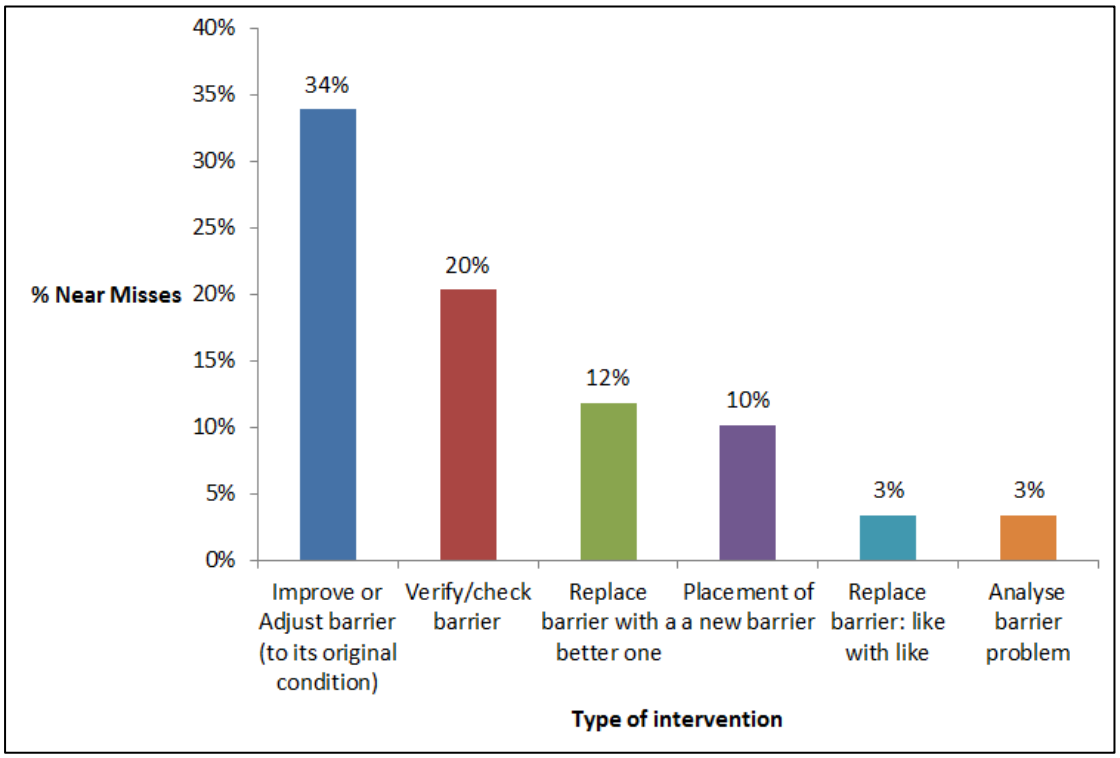


FIGURE 42 TYPE OF SECONDAY INTERVENTIONS ON BARRIERS: PERCENTAGE OF 59 COMPANY NEAR MISSES, MAJOR HAZARDS RELATED

8.3 Limitations of the analyses

Regarding the near misses the data source was extensive but not detailed and is considered fairly typical of databases kept in MS Excel covering a large number of deviation conditions. In such a database the information required for analysing human intervention was very limited, but does give an impression of the kinds of recoveries of barriers being undertaken. Such an analysis could be extended to the whole database but this was beyond the current resources. Therefore the nature of the selection made by the analyst from the complete company "near miss" data set was limited (Annex C). 59 scenarios were selected as readily identifiable as process safety/major hazard related, analysed and entered into Storybuilder for further analysis. These were all found to be Stage 1 failures. The 27 "unsafe conditions" were not entered into

Storybuilder but these appear to be Stage 2 (barrier failures without loss of control). Looking at the database overall there are also events that could be pulled out for earlier stages (Stage 4 delivery systems and Stage 3 barrier tasks). Regarding the latter, some events of the earlier Stages 4 and 3 were events happening with non major-hazard equipment but which could have implications for major hazards.

The 7 ARIA lessons learned data were not all entered into Storybuilder, other than the example given in section 8.2.1. The reader can however examine the examples in Annex C and consider for themselves what lessons learned there might be for resilience as shown in the example. The difference between the potential for resilient evaluation versus the current normative evaluation is illustrated with some examples in Table 7.

TABLE 7 SOME EXAMPLES OF POTENTIAL VERSUS CURRENT FOCUS OF INVESTIGATIONS AND LESSONS LEARNED

POTENTIAL –Resilient	CURRENT –Normative
• Scenario thinking – Multi-disciplines/characters – Think through the Stages x IDDDR – Return on experience • Get the little things right • Second opinion – Cold eyes review – Challenges (not confirmation) – Counteract biases • Hold points, stop and think • Dynamic vigilance – Risk awareness – Challenged – Switched on people – Task engaged/task rotation • Bias mitigation – Self-reflection – Bias awareness	e.g. • Failures in safety studies • Verification failures • Failure in a critical procedure • Failure to consider human detection requirements • Putting off actions • Management blindness • Erosion of layers of protection • Disregard of procedures • Etc

9 CONCLUSIONS

This section provides conclusions on each of the research questions as short summaries.

9.1 How can the bow-tie model and resilience be integrated to extract additional information from accidents?

The resilience components identified from resilience case studies (Section 5 & Annex B Resilience Case Studies) provided the basis for the resilience components of a "success" bow-tie model (Section 7 & Annex D Success model event checklist). The integration was between success modes of barriers derived from a failure bow-tie and human interventions in response to deviations. A generic success bow-tie was developed

that is applicable to any barrier success node. Incidents can be taken through the model as a path through events with successful outcomes. The centre event is "successful intervention".

The integration with the success node starts with precursor signals. An intervention is needed to stop possible propagation an accident. In the first segment of the model this intervention has been classified according to the stage at which it occurs - from inadequacies in organisational resources to the actual accident sequence triggered by a loss of control (see Section 6.5). There were 4 stages from early (stage 4) to late (stage 1) intervention. The potential accident precursors were classified according to the stage of intervention, from deeper underlying causes to loss of control events resulting from barrier failures.

The integration with resilience takes place in the newly modelled success bow-tie in the segment concerning intervention – the IDDR – Indication, Detection, Diagnosis/Decision, Response(see Sections 6.1- 6.4). The IDDR segment concerns intervention with successful outcomes. The resilience components were attached to the management delivery systems this segment (see next section).

The model was built in Storybuilder with 60 specific examples from major hazards and is available on the website **www.resiliencesuccessconsortium.com**. Only the barriers and barrier specific precursors are sector specific. These can be substituted in the bow-tie model which therefore can be applied to any sector and accident hazard.

9.2 What Human and Organisational Factor (HOF) elements are involved?

Resilient interventions are characterised by the fact that they are:

- Uncertainty reducing
- Mindful (enriched awareness of detail)
- Can bring a deviating state to a successful outcome

The identified HOF elements (Section 7 & Annex D Success model event checklist) were built up around the so-called four cornerstones of resilience as follows (see Annex D for definitions):

- Anticipating
  - 1 Scenario-thinking
  - 2 Getting (little) things right (so as not to compromise future states)
  - 3 Switched on/vigilant to what can go wrong (risk aware)
  - 4 Cognitive bias mitigation (Anticipating)
- Monitoring
  - 5 Switched on/Vigilant/Alert (for signal detection/change)
  - 6 Stop and think (hold points/cross check/pause at critical steps)
  - 7 Multidisciplinary/different characters
  - 8 Cognitive bias mitigation (monitoring)
- Responding
  - 9 Experienced people available
  - 10 Know the safety margins, one's own limitations
  - 11 Consult with others/think together (multidisciplinary/different characters)
  - 12 Use of golden rules/principles ("lines in the sand")
  - 13 Time and (multiple) options available
  - 14 Cognitive bias mitigation (responding)
- Learning
  - 15 Self-reflection, willing to learn
  - 16 Communication/feedback/trust
  - 17 Analyse, discuss & expand events

18 Simulation training
19 Capture & record
20 Cognitive bias mitigation (learning)

These components were then attached to the 8 management delivery systems which are found in the Storybuilder model (see Sections 4.1 & 7.7). The delivery systems are as follows (with the above resilience component numbers):

- Procedures: Procedures delivery system delivers performance criteria which specify in detail, usually in written form, a formalised 'normative' behaviour or method for carrying out tasks (2, 6, 12, 17,19)
- Availability: Availability delivery system allocates the necessary time and numbers of competent and suitable (including anthropometrics and biomechanics) people to the barrier tasks (3, 5, 7, 9, 13)
- Competence: Competence delivery system delivers the knowledge, skills and abilities of the people selected for the execution of the barrier tasks (2, 4, 8, 9, 10, 15, 18, 20)
- Communication: Communication delivery system is relevant when the activity is carried out by more than one person (or group), who have to coordinate or plan joint activities e.g. different shifts. It refers to internal communication and coordination (11, 16, 17, 20)
- Motivation: Motivation delivery system delivers goals and incentives for people to carry out their tasks and activities with suitable care, alertness and risk awareness, keeping to criteria and rules specified for the safety of the activities within the organisation (1, 3, 5, 7, 10, 11, 15, 16).
- Conflict resolution: This delivery system resolves conflicts between safety and other goals within the performance of tasks (2, 3, 6, 12, 13, 14).
- Ergonomics: Ergonomics and man-machine system deals with the fit between the man and the task (5, 13, 14, 18).
- Equipment: Equipment refers to the hardware needed for provision, maintenance and monitoring of barriers (2, 14).

These delivery systems supply the resources to the barrier tasks:

- Provide: The barrier is provided and available when required
- Use/operate: The use or operation of the provided barrier
- Maintain: The barrier is kept available according to its designed function and in an adequate state
- Monitor: The barrier condition is checked/measured/observed/inspected including the supervision of the performance of barrier tasks.

9.3 What can be learned from the integration by inputting new scenarios?

86 process safety scenarios from a major hazard company and 7 lessons learned from a major hazard database were analysed (Section 8 and Annex C Lessons learned, near misses and unsafe conditions, Baksteen 2015).

The lessons learned from just 7 ARIA database accidents revealed failures that, using judgement and the list of 20 resilience components, had lessons for resilience (see Section 8.2.1 & 8.2.2). Analyses can be supported by the success model checklist in Annex D.

60 new scenarios were entered in the Storybuilder model (59 stage 1 near misses and 1 accident lessons learned). The results are given in Section 8.2.4 and Annex C. The near misses were primarily deviations in the first line of defence with process deviation precursors dominating. The first action interventions for the 59 near misses were primarily actions on valves and flow. Results showed that, besides 20% unknown interventions, 59% required barriers to be fixed or replaced and the rest to be monitored or checked (see Section 8.2.4).

Resilience components were difficult to identify from the available data. The approach to incident evaluation is to identify normative failures (failures of standard procedures and equipment design and installation). Incident investigation can be improved to look for resilience factors and to provide lessons learned for building resilience.

9.4 How can safety be improved in practice by adopting the resilience approach?

This is a more general level question. The approach to modelling resilience considered resilience as uncertainty reducing (see Sections 3 & 7.8). Responding to change and deviation which cannot be handled by the normative approach requires uncertainty reducing interventions which are best understood in the following diagram (Figure 43). Safety can be improved by reducing high uncertainties through acquisition of knowledge and information. This is addressed primarily in Sections 5 & 6 which deal with enhancing the resilience components and the handling of signals respectively.

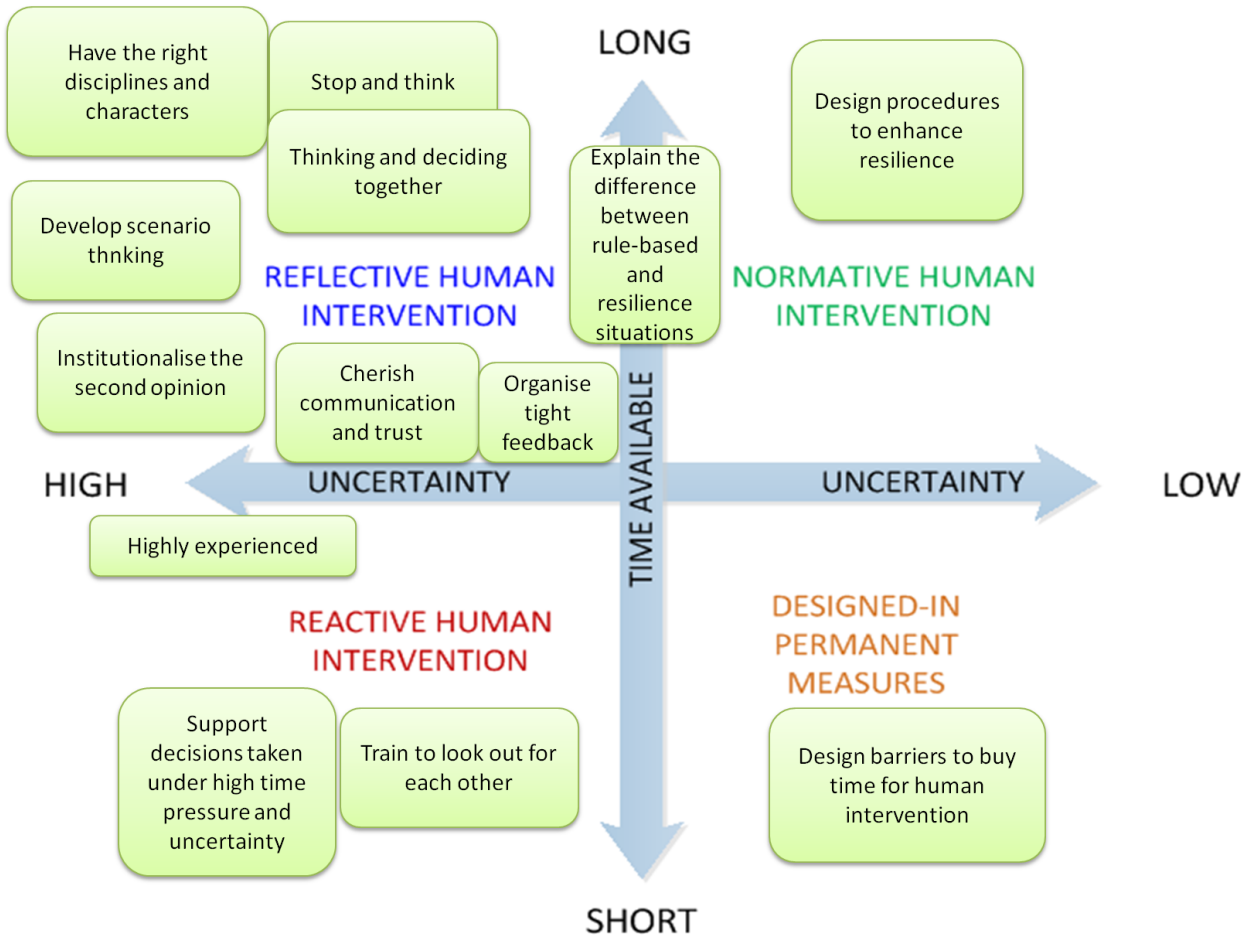


FIGURE 43 KEY COMPONENTS OF UNCERTAINTY MANAGEMENT SUPERIMPOSED ON THE UNCERTAINTY X TIME MATRIX

9.5 Can resilience concepts be integrated into the classical bow-tie approaches to risk assessment?

Another general level question, it was asked in particular whether in the integration of resilience into the classical bow-tie it is possible to improve the characterization of the management system's performance and the impact of human and organization factors on safety and loss control. Figure 44 shows the general

structure of the success bow-tie. It has a management delivery systems block associated with successful IDDR (Indicate, Detect, Diagnose & Decide, Respond) with associated resilience components(red rectangles) attached to each of the delivery systems (green diamonds) which can play a role in successful intervention. Before reaching the central event of successful intervention there is an uncertainty block where it can be evaluated by how much the uncertainty has been reduced by resilience in the intervention, based on the extent to which resilience components were involved. To the right of the centre event the success outcomes can be evaluated in terms of the associated level of uncertainty. Three levels have been suggested as success with low uncertainty, success with medium uncertainty and success with high uncertainty.

The total model can be understood against the background of the report. All the aims of the research project were achieved.

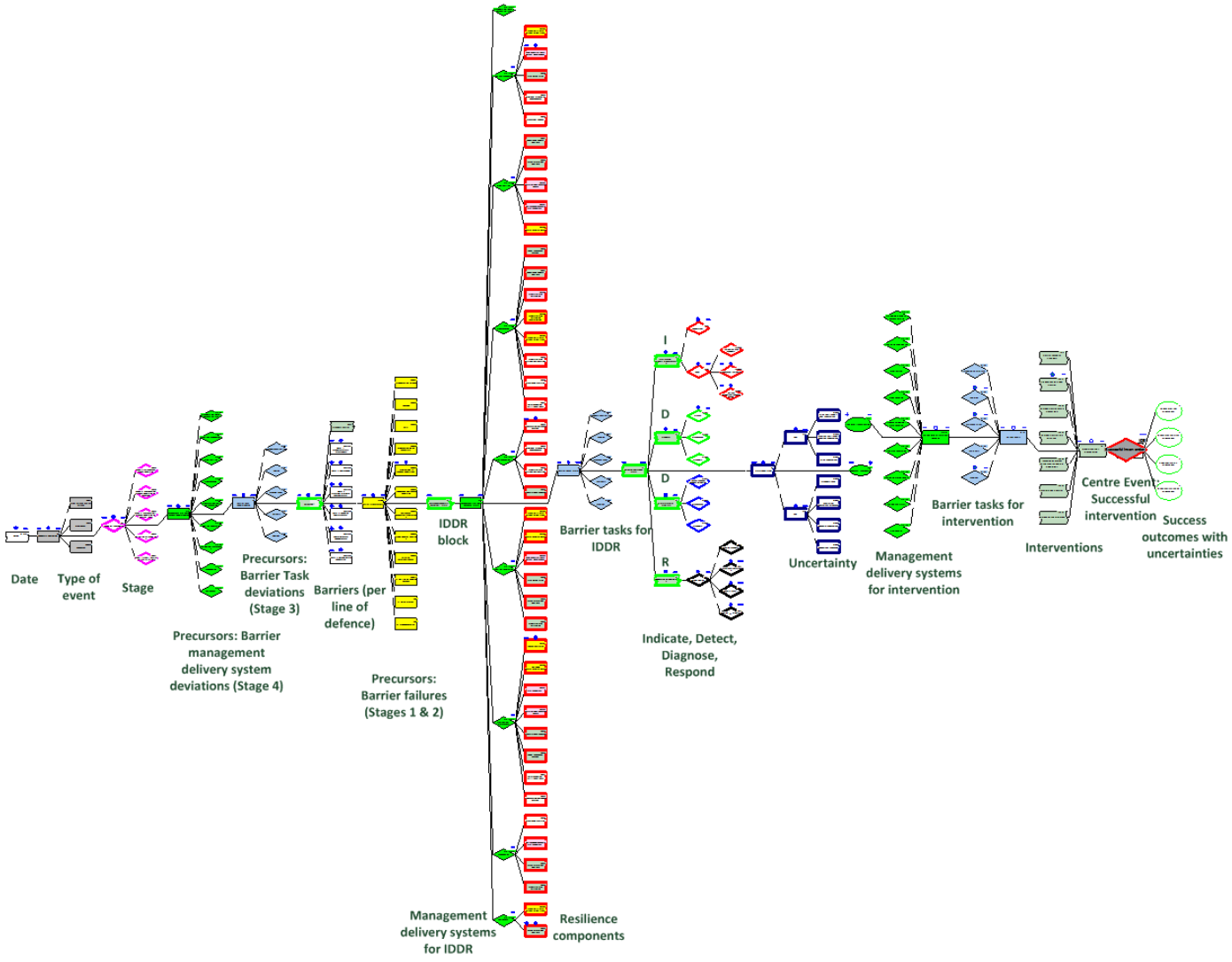


FIGURE 44 SCHEME OF THE SUCCESS BOW-TIE

10 REFERENCES

Adamski, A.J. & Westrum, R. (2003). Requisite imagination: The fine art of anticipating what might go wrong. In Erik Hollnagel (Ed.), Handbook of cognitive task design. Hillsdale, NJ: Lawrence Erlbaum Associates.

American Institute of Chemical Engineers, 2000. Guidelines for Chemical Process Quantitative Risk Analysis. ISBN-0-8169-0720-X.

Andersen, H., Casal, J., Dandrieux, A., Debray, B., De Dianous, V., Duijm, N.J., Delvosalle, C., Fievez, C., Goossens, L., Gowland, R.T., Hale, A.J., Hourtolou, D., Mazzarotta, B., Pipart, A., Planas, E., Prats, F., Salvi, O., Tixier, J., 2004. Accidental Risk Assessment Methodology For Industries In The Context Of The Seveso II Directive. ARAMIS User Guide. EU Contract number : EVG1 – CT – 2001 – 00036.

ARIA, 2012. http://www.aria.developpement-durable.gouv.fr/about-us/the-aria-database/?lang=en

Ashby, W.R., 1957. An introduction to cybernetics. London: Chapman & Hall Ltd

Bainbridge, L., 1983. Ironies of automation. Automatica 19 (6) 775-779
https://www.ise.ncsu.edu/nsf_itr/794B/papers/Bainbridge_1983_Automatica.pdf

Bellamy, L.J. 1984. Not waving but drowning. Ergonomics Problems in Process Operations. IChemE Symposium series 90. ISBN 0 85295 172 8

Bellamy L.J., Papazoglou I.A., Hale A.R., Aneziris O.N., Ale B.J.M., Morris M.I. & Oh J.I.H. 1999. I-Risk: Development of an integrated technical and management risk control and monitoring methodology for managing and quantifying on-site and off-site risks. Contract ENVA-CT96-0243. Report to European Union. Ministry of Social Affairs and Employment. Den Haag.
http://cordis.europa.eu/project/rcn/33974_en.pdf
https://www.researchgate.net/publication/266675230_I-RISK_Main_Report

Bellamy, L.J., Mud, M., Manuel, H.J., Oh, J.I.H., 2013. Analysis of underlying causes of investigated loss of containment incidents in Dutch Seveso plants using the Storybuilder method. J. Loss Prevent. Process Industries 26 (2013) 1039-1059.

Croskerry P, Abbass A, Wu A.2010. Emotional issues in patient safety. J. Patient Safety, 2010, 6 1-7

Croskerry. P., Singhal, G., Mamede, S., 2013. Cognitive debiasing 2: impediments to and strategies for change. BMJ Quality & Safety 2013 ii65-72

Damasio, A. , 1991. Somatic Markers and the Guidance of Behavior. New York: Oxford University Press. pp. 217–299.

Damasio, A.R. 1994. Descartes' Error: emotion, reason, and the human brain. New York: Grosset/Putnam.

De Winter, J.C.F., & Dodou, D. 2014. Why the Fitts list has persisted throughout the history of function allocation. Cogn Tech Work (2014) 16:1–11
http://download.springer.com/static/pdf/19/art%253A10.1007%252Fs10111-011-0188-1.pdf?auth66=1417647800_d4218c7d6af30fbfdd78ec74a2af1631&ext=.pdf

Dekker, S., Hollnagel, E., Woods, D., Cook, R., 2008. Resilience Engineering: New directions for measuring and maintaining safety in complex systems. Final Report November 2008. Lund University School of Aviation. Sweden.

Duijm, N.J. 2009 Safety-barrier diagrams as a safety management tool. Reliability Engineering and System Safety 94 (2009) 332– 341

Duijm, N.J. 2013 Risk analysis by means of safety-barrier diagrams: Types of safety barriers. DTU Management Engineering, Department of Management Engineering.

Endsley, M.R., 2000 Theoretical underpinnings of situation awareness. In Endsley & Garland, D.J. (Eds) Situation awareness analysis and measurement. Mahwah, NJ: Lawrence Erlbaum Associates.

Eurocontrol 2009 A White Paper on Resilience Engineering for ATM. http://www.eurocontrol.int/sites/default/files/article/content/documents/nm/safety/safety-a-white-paper-resilience-engineering-for-atm.pdf

Folke, C., 2006. Resilience: The emergence of a perspective for social–ecological systems analyses. Global Environmental Change 16 (2006) 253–267

Fitts P.M. (ed), 1951. Human engineering for an effective air navigation and traffic control system. National Research Council, Washington, DC

Gawande, A., 2010. The Checklist Manifesto, New York: St. Martins Press.

Green, D.M. & Swets, J.A., 1966. Signal detection theory and psychophysics. Wiley & Sons Inc, N.Y.(Revision 1988)

Guldenmund, F.W., Hale, A.R., Bellamy, L.J., 1999. The development and application of a tailored audit approach to major chemical hazard sites. Proceedings of SEVESO 2000 European Conference Risk Management in the European Union of 2000: The Challenge of Implementing Council Directive 'Seveso II' Athens, Greece. http://publications.jrc.ec.europa.eu/repository/handle/JRC20747)

Hale et al 1997 Modelling of safety management systems. Safety Science 26 121-140

Hayes, J., 2013 Operational Decision-making in High-hazard Organisations Drawing a Line in the Sand. Ashgate Publishing.

Hocker, F.M., & Ward, C.A., 2004. The philosophy of shipbuilding. Texas A&M University Press

Holling, C.S., 1973. Resilience and stability of ecological systems. Annual Review of Ecology and Sustematics, Volume 4 , pp. 1-23

Hollnagel 2006 Capturing an uncertain future. The Functional Resonance Accident Model MS PowerPoint presentation. http://www.eurocontrol.int/eec/gallery/content/public/documents/conferences/2006_Barcelona/Hollnagel%28FRAM_Barcelona_Arial%29.pdf

Hollnagel, E., 2009. The ETTO Principle: Efficiency-Thoroughness Trade-Off. Ashgate Publishing

Hollnagel, E. 2010. How Resilient Is Your Organisation? An Introduction to the Resilience Analysis Grid (RAG). Sustainable Transformation: Building a Resilient Organization, May 2010, Toronto, Canada. **https://hal.archives-ouvertes.fr/hal-00613986/document**

Hollnagel, E. 2012. FRAM The functional resonance analysis method. Ashgate Publishing.

Hollnagel, E., Tveiten, C., Albrechtsen, E., 2010. Resilience Engineering and Integrated Operations in the Petroleum Industry. SINTEF report A16331, ISBN 978-82-14-04901-5, Trondheim, Norway.

Hollnagel, E., Woods, D.D., Leveson, N. (Eds), 2006. Resilience Engineering. Concepts and precepts. Ashgate Publishing Ltd, UK.

Hollnagel, E. Pariès, J., Woods, D.D., Wreathall, J. 2011 Resilience Engineering in Practice. Ashgate Publishing Ltd, UK

Hollnagel, E., Jörg Leonhardt, J., Licu, T., Shorrock, S. 2013. From Safety-I to Safety-II: A White Paper. Eurocontrol 2013. Online: http://www.skybrary.aero/bookshelf/books/2437.pdf

Hopkins, A., 2014. Issues in safety science. Safety Science, vol. 67, pp. 6-14.

Huber, S., van Wijgerden, I., de Witt, A., Dekker, S.W.A. 2009 Learning from organizational incidents: Resilience engineering for high-risk process environments Process Safety Progress 28(1) March 2009

Iman R. L. and Helton J. C., 1985. A Comparison of Uncertainty and Sensitivity Analysis for Computer Models, NUREG/CR-3904.

Jackson, S., 2010. Architecting resilient systems : accident avoidance and survival and recovery from disruptions. NJ: Wiley.

Jørgensen, K.., Duijm, N.J., Troen, H., 2011 Message maps for safety barrier awareness. Safety Science Monitor vol 15 (2)

Kahneman, D., 2011. Thinking fast and slow. New York: Farrar Straus & Giroux. (Paper back 2012 Penguin Books)

Kahneman, D. & Tversky, A, 1982 Variants of uncertainty. Cognition 11 (1982) 143-157

Kahneman, D., Lovallo, D., Sibony, L. 2011. The big idea: Before you make that big decision. Harvard Bus. Rev. June 2011. . https://hbr.org/2011/06/the-big-idea-before-you-make-that-big-decision.

Kahneman, D., Slovic, P., Tversky, A. (eds.) 1982. Judgment under uncertainty: heuristics and Biases , Cambridge University Press, New York

Klein, G., 2003. Intuition At Work. Random House, NY.

Klein, G., Snowden, D. & Pin, C. L., 2010. Anticipatory Thinking. Informed by knowledge: Expert Perfromance in Complex Situations. New York: Psychology Press, Taylor & Francis Group

Kurtz, C. & Snowden, D. 2003. The New Dynamics of Strategy: sense making in a complex and complicated world. in IBM Systems Journal 42(3): 462-483.

Langer, E.J., 2000. Mindful learning. Current directions in psychological science, Volume 9, Number 6, December 2000. http://thehawnfoundation.org/wp-content/uploads/2012/12/Langer_Mindful-Learning.pdf

Larrick, R.P., 2004. Ch. 16 Debiassing in Koehler, D.J. & Harvey, N. (Eds) Blackwell Handbook of Judgement and Decision Making. Blackwell Publishing, Oxford UK.

Lauridsen K., Kozine I., Markert F., Amendolla A., Christou M., Fiori M. 2002, Assessment of Uncertainties in Risk Analysis of Chemical Establishment, The ASSURANCE project, Risø National Laboratory. **http://www.risoe.dk/rispubl/sys/syspdf/ris-r-1344.pdf**

Lekka, C., Sugden, C., 2011. The successes and challenges of implementing high reliability principles: A case study of a UK oil refinery. Process Safety and Environmental Protection 89 (2011) 443–451.

Leveson, N., 2015. A systems approach to risk management through leading safety indicators. Reliability Engineering & System Safety 136 (2015) 17–34

Lisbona, D., Johnson, M., Millner, A., McGillivray, A., Maddison, T., & Wardman, M. , 2012. Analysis of a loss of containment incident dataset for major hazards intelligence using storybuilder. Journal of Loss Prevention in the Process Industries, 25(2), 344-363

Macmillan, N.A., 2002. Ch.2 Signal detection theory. In Stevens' handbook of experimental psychology, third edition, Volume 4: Methodology in Experimental Psychology.

Marca, D.A., & McGowan, C.L. 1988. SADT: structured analysis and design technique. McGraw-Hill Book Co., Inc.: New York, NY.

McCammon, I., Evidence of heuristic traps in recreational avalanche accidents, presented at the International Snow Science Workshop, Penticton, British Columbia, Sept. 30 – Oct 4, 2002.

Mileti, Dennis. Ed. 1999. Disasters by Design: A Reassessment of Natural Hazards in the United States. Washington, D.C.: Joseph Henry Press.

Moulton CAE, Regehr G, Mylopoulos M., MacRae H.M., 2007. Slowing down when you should: a new model of expert judgment. Academic Medicine 2007; 82: S109–16

Moulton CA, Regehr G, Lingard L, Merritt C, MacRae H., 2010 Slowing down to stay out of trouble in the operating room: remaining attentive in automaticity. Acad Med 2010; 85: 1571–15777.

Papazoglou, I.A., Aneziris, O., Bonanos, G., & Christou, M., 1996. SOCRATES: a computerized toolkit for quantification of the risk from accidental releases of toxic and/or flammable substances. In Gheorghe, A.V. (Editor) (1996), Integrated Regional Health and Environmental Risk Assessment and Safety Management, published in Int. J. Environment and Pollution, Vol. 6, Nos 4-6, 500-533.

Pasman, H.J., Knegtering, B., Rogers, W.J., 2013. A holistic approach to control process safety risks: possible ways forward. Reliability Engineering and System Safety 117 (2013) 21–29

Pate Cornell, E., 1993. Learning from the Piper Alpha accident: A postmortem analysis of technical and organizational factors. Risk Analysis 13 (2) 215-232

Pate Cornell, E., 1996. Uncertainties in risk analysis: Six levels of treatment. Reliability Engineering and System Safety 54, 95-111.

Petersen A.C., Janssen P.H.M., van der Sluijs J.P., Risbey J.S., Ravetz J.R., Wardekker J.A., Martinson Hughes H., 2013. Guidance for Uncertainty Assessment and Communication, , 2nd Edition, PBL, 2013. Developed for the Environmental Assessment Agency (PBL), The Netherlands. http://www.pbl.nl/sites/default/files/cms/publicaties/PBL_2013_Guidance-for-uncertainty-assessment-and- communication_712.pdf

Pohl, R.E. (Ed.) 2012. Cognitive illusions. A handbook on fallacies and biases in thinking, judgement and memory. Psychology Press, Hove, UK.

Rasmussen, J., 1997. Risk management in a dynamic society: A modelling problem. Safety Science 27 (2/3) 183-213

Reich, J.W., Zautra, A.J., Hall, J.S., 2010. Handbook of adult resilience. The Guildford Press, US.

RIVM, 2008. The quantification of occupational risk. The development of a risk assessment model and software.RIVM Report 620801001,National Institute for Public Health and Environment, P.O.Box1, 3720 BA Bilthoven, The Netherlands. Online: **http://www.rivm.nl/bibliotheek/rapporten/620801001.pdf**

RIVM 2014 Storybuilder major hazard model - Software download and major hazard database. **http://www.rivm.nl/en/Topics/O/Occupational_Safety/Other_risks_at_work/Dangerous_substances**
http://www.rivm.nl/en/Topics/S/Storybuilder Information about Storybuilder in context of occupational safety with links to download, user manuals, factsheets and more.

Roberto, M.A. 2002 Lessons from Everest: the interaction of cognitive bias, psychological safety, and system complexity. California Management Review 45, 136-158

Roberts K. H., Stout, S. K., and Halpern, J. J. 1994. Decision dynamics in two high reliability military organizations. Management Science, 40: 614-624

SafetyBarrierManager (2015) SafetyBarrierManager, Technical University of Denmark. **http://www.safetybarriermanager.man.dtu.dk/About-Safety-Barrier-Manager**

Salvi, S., 2014. EU-Project ARAMIS Accidental Risk Assessment Methodology for Industries in the framework of the SEVESO II directive. http://hal-ineris.ccsd.cnrs.fr/ineris-00972487/document

Scheffer M, Bascompte J, Brock WA, Brovkin V, Carpenter SR, et al. 2009. Early-warning signals for critical transitions. Nature 461: 53-59.

Shirali G.H.A., Motamedzade, M., Mohammadfam, I., Ebrahimipour V., Moghimbeigi, A., 2012. Challenges in building resilience engineering (RE) and adaptive capacity: A field study in a chemical plant. Process Safety and Environmental Protection 90 (2012) 83–90

Shirali G.H.A., Mohammadfam, I., Ebrahimipour V., 2013. A new method for quantitative assessment of resilience engineering by PCA and NT approach: A case study in a process industry. Reliability Engineering and System Safety 119 (2013) 88–94

Sklet, S., 2006. Safety barriers: Definition, classification, and performance. Journal of Loss Prevention in the Process Industries 19 (2006) 494–506

Sonnemans, P.J.M., Körvers, P.M.W, Pasman, H.J., 2010. Accidents in "normal" operation – Can you see them coming?. Journal of. Loss Prevention in the Process Industries 23 (2010) 351-366

Steen, R. & Aven, T., 2011 A risk perspective suitable for resilience engineering Safety Science 49 (2011) 292–297.

Storybuilder™ 2015 **http://www.rivm.nl/en/Topics/S/Storybuilder** Information about Storybuilder with links to download, user manuals, factsheets and more

Stockholm Resilience Centre, 2015. Applying resilience thinking. Brochure of the Stockholm Resilience Centre.
http://www.stockholmresilience.org/download/18.10119fc11455d3c557d6928/1398150799790/SRC+Applying+Resilience+final.pdf

Stough J., 2011. Strong reporting culture as stepping stone to continuously drive safety performance improvement. Society of Petroleum Engineers – SPE Americas E and P Health, Safety, Security, and Environmental Conference 2011, pp. 74-81.

Taleb, N., 2012. Antifragile: Things that gain from disorder.. Random House..

Tetlock PE, Kim JI. 1987. Accountability and judgment processes in a personality prediction task. J Pers Soc Psychol 1987, 52 700–9

Tierney, K., Bruneau, M., 2007. Conceptualizing and measuring resilience: A key to disaster loss reduction (Review). TR News. Issue 250, May 2007, Pages 14-17

Tversky, A. & Kahneman, D., 1974 Judgment under Uncertainty: Heuristics and Biases. Science Vol. 185, No. 4157. (Sep. 27, 1974), pp. 1124-1131

USNRC 2009.. Guidance on the treatment of uncertainties with PRAs in risk informed decision making (NUREG-1855). Technical report, US Nuclear Regulatory Commission, Washington, DC. **http://pbadupws.nrc.gov/docs/ML0909/ML090970525.pdf**

Vogus, T. J., & Welbourne, T. M. 2003. Structuring for high reliability: HR practices and mindful processes in reliability-seeking organizations. Journal of Organizational Behavior, 24(7), 877–903

Vogus, T.J., Rothman, N.B., Sutcliffe, K.M., Weick, K.E., 2014. The affective foundations of high reliability organizing . Journal of Organizational Behavior, 35, 592–596 (2014)

Walker, B., 2005. A resilience approach to integrated assessment. The Integrated Assessment Journal Vol. 5, Iss. 1 (2005), Pp. 77–97

Walker, B., C. S. Holling, S. R. Carpenter, and A. Kinzig. 2004. Resilience, adaptability and transformability in social–ecological systems. Ecology and Society 9(2): 5. [online] URL: http://www.ecologyandsociety.org/vol9/iss2/art5

Walker, B., and F. Westley. 2011. Perspectives on resilience to disasters across sectors and cultures. Ecology and Society 16(2): 4. [online] URL: http://www.ecologyandsociety.org/vol16/iss2/art4/

Walker W, Harremoes P, Rotmans J, Van der Sluijs J, Van Asselt M, Janssen P, Krayer von Krauss, M., 2003. Defining uncertainty. A conceptual basis for uncertainty management in model-based decision support. Integrated Assessment 4 (1), 5-17

Weick. K.E., 1995a. Sensemaking in organizations. Sage publications

Weick, K.E., 1995b. South Canyon revisited: Lessons from high reliability organizations. Wildfire, 4(4), 54–68.

Weick, K.E., 2010. Reflections on Enacted Sensemaking in the Bhopal Disaster. Journal of Management Studies 47:3 May 2010

Weick, K.E., 2012 Organized sensemaking. A commentary on processes of interpretive work. Human Relations 2012 65: 141-153.
http://www.uk.sagepub.com/zibarras/study/Chapter%2011/Human%20Relations-2012-Weick-141-53.pdf

Weick, K. E., & Sutcliffe, K. M., 2007. Managing the unexpected: Resilient performance in and age of uncertainty, second edition. San Francisco, CA: Jossey-Bass.

Weick, K.E., Sutcliffe, K.M. & Obstfeld, D. 1999.Organizing for High Reliability: Processes of Collective Mindfulness in R.S. Sutton and B.M. Staw (eds), Research in Organizational Behavior, Volume 1 (Stanford:Jai Press, 1999), pp. 81–123.

Wildavsky, A. 1988. Searching for safety. Transaction publishing

Woods, D.D., Schenk, J., & Allen, T.T., 2009. An initial comparison of selected models of system resilience. Ch.4 in C.P. Nemeth, E. Holnagel & S. Dekker (Eds) Resilience Engineering Perspectives Vol. 2 Preparation and Restoration.

Zolli, A. and Healy, A.M., 2012. Resilience. Headline Publishing Group, London.

11 ANNEXES

All Annexes can be found on
http://www.resiliencesuccessconsortium.com/resources

Or accessed on the SAFERA website:
http://projects.safera.eu/project/2

Annex A: Product Specifications: Preliminary considerations (Resilience Success Consortium 2014)

Annex B: Resilience Case Studies. Dealing With Uncertainty in Practice: Strengths and Traps in Human Intervention (Van Galen, A. & Bellamy, L.J. 2015)

Annex C: Lessons learned, near misses and unsafe conditions: Analysis of accident reports (ARIA) and a company near miss database (Baksteen, H. 2015)

Annex D: Success model event checklist: For identifying resilience in handling near misses and other deviations in major hazards with successful safety outcomes (Bellamy, L.J. 2015)

Annex E: Glossary of terms: Bowtie, barrier and resilience terminology. (Duijm, N.J. et al 2015)