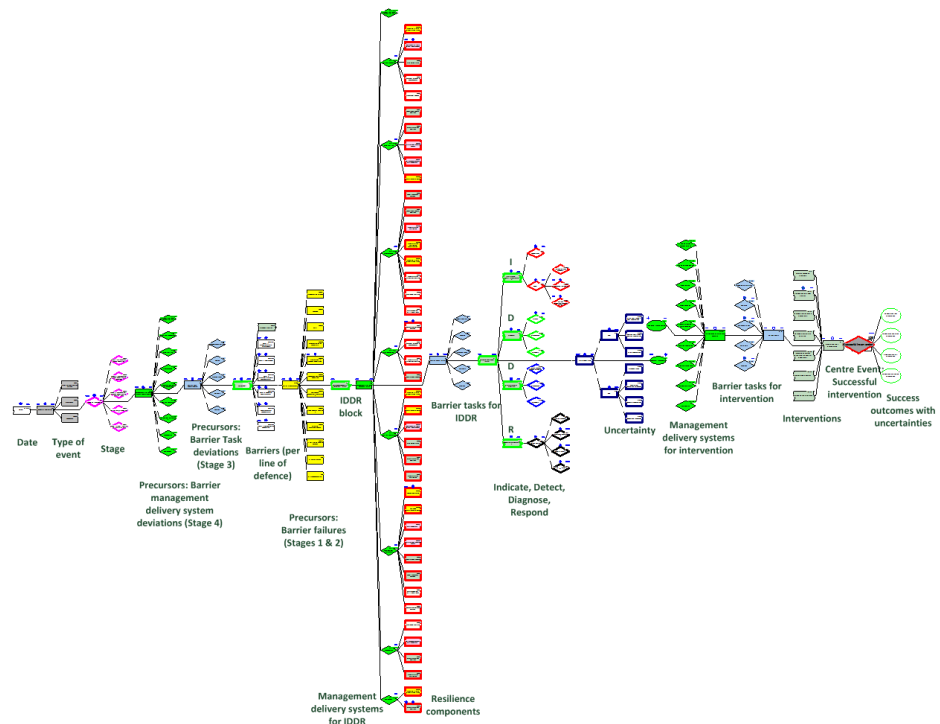


ANNEX D: SUCCESS MODEL EVENT CHECKLIST



29 March 2015

For identifying resilience in handling near misses and other deviations in major hazards with successful safety outcomes

Rev 01

Author: Linda Bellamy

CONTACT

Consortium

<http://www.resiliencesuccessconsortium.com/>

Dr Linda J. Bellamy (Author & Coordinator)

White Queen Safety Strategies

PO Box 712

2130 AS Hoofddorp

The Netherlands

T. +31 (0)235 651353

M. +31 (0)6 54648622

E. linda.bellamy@whitequeen.nl

W. www.whitequeen.nl

Annex D: Success Model Event Checklist

FOR IDENTIFYING RESILIENCE IN HANDLING NEAR MISSES AND OTHER DEVIATIONS IN MAJOR HAZARDS WITH SUCCESSFUL SAFETY OUTCOMES

Contents

| | | |
|-----------|--|-----------|
| 1 | TYPES OF EVENT | 4 |
| 2 | KEY ANALYSIS STEPS | 4 |
| 3 | STEP 1 SAFETY BARRIERS | 5 |
| 4 | STEP 2: THE STAGE OF INTERVENTION | 11 |
| 5 | STEP 3: PRECURSORS | 12 |
| 5.1 | Stages 1 & 2..... | 12 |
| 5.2 | Stages 3 & 4..... | 12 |
| 6 | STEP 4 PROCESS OF PRIMARY INTERVENTION - IDDR | 14 |
| 7 | STEP 5 PROCESS OF SECONDARY INTERVENTION | 16 |
| 8 | STEP 6 RESILIENCE COMPONENTS | 16 |
| 9 | STEP 7 UNCERTAINTY | 24 |
| 10 | OVERVIEW OF FIELDS | 26 |

1 TYPES OF EVENT

The purpose of the checklist is to provide components for building a bow-tie success model for any type of hazard. The checklist helps to incorporate resilience components and provides a framework of analysing deviations such as near misses and for incorporating information concerning lessons learned. Further information can be found in the main report of the Resilience Success Consortium (2015) and the Annexes (Annex B, Annex C, Annex E). The type of events that can be included in the model are:

Table 1 Types of event for inclusion in the success model

| Type of event | Description |
|---------------------------------------|---|
| Near and “far” misses | Near miss is defined in the Glossary E as <i>A deviation that is disarmed by an intervention before it developed into a critical event.</i> The use of the term “far” miss is additional to this definition, simply to emphasise that some deviations may be well in advance of a potential incident. |
| Accidents with lessons learned | These are investigated accidents where lessons have been drawn. The failure events essentially belong in a failure bow-tie but the main loss of control event can be regarded as a precursor in the success model and the lessons learned associated with the process of diagnosis, decision and intervention where lessons result in success outcomes. |
| Success | The opposite of failure, successes that could be included in the model are successful responses to change or deviation. Success is the achievement of predetermined goals and expectations with acceptable outcomes |

2 KEY ANALYSIS STEPS

The key steps are as follows:

STEP 1 Identify the safety barriers. These will be the barriers where success modes can be attached.

STEP 2 Specify the stage of intervention – how early was a deviation detected? What were the precursors (at the different stages)?

STEP 3 Specify the precursors indicating deviation

STEP 4 Specify the process of primary intervention

STEP 5 Specify the process of secondary intervention:

STEP 5 Recount the outcomes for barrier conditions, including introducing previously unanticipated barriers.

STEP 6 Specify resilience components present

STEP 7 Specify uncertainties and outcomes.

For an analysis example see the main report, section 8.2.1. Lessons learned.

3 STEP 1 SAFETY BARRIERS

The success model event checklist provides a framework for collecting data about the success modes of safety barriers.

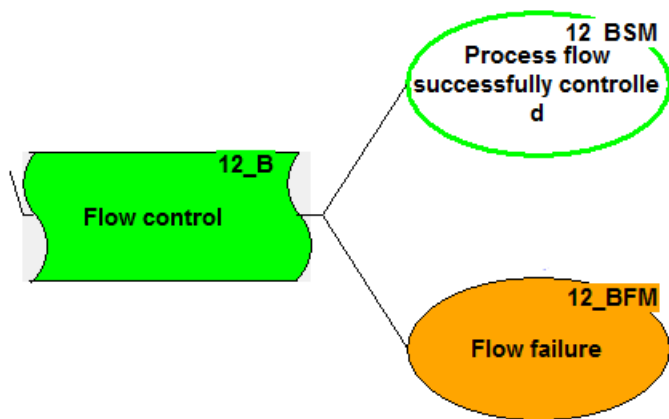


FIGURE 1 STORYBUILDER BARRIER¹ EXAMPLE SHOWING BARRIER (B), BARRIER SUCCESS MODE (BSM) AND BARRIER FAILURE MODE (BFM)

Every success mode in a barrier diagram can be developed along the lines of this generic checklist.

The success model can be used for analysing deviation events (near misses, unsafe acts, abnormal deviations) with success outcomes.

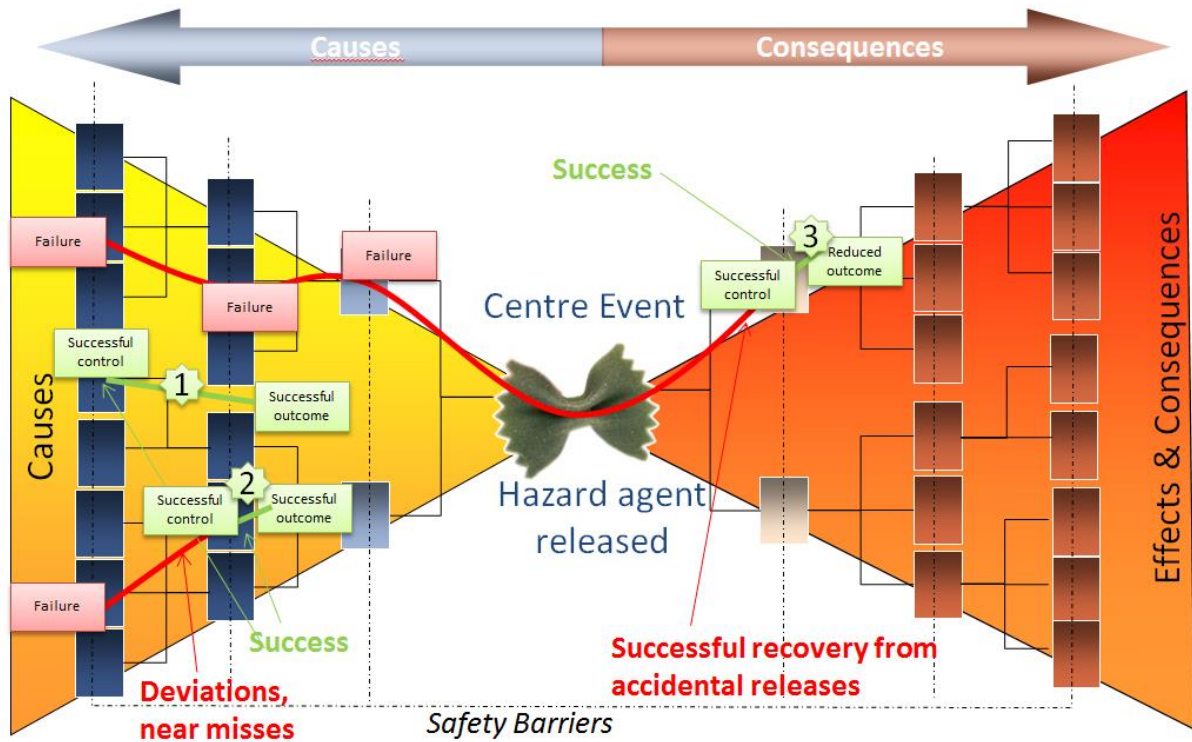
It can also be used for incorporating lessons learned from previous successes and failures.

The focus is on barrier systems represented in risk models, as in the bow-tie shown in Figure 2. In the model successes are concerned with intervening 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 (see Figure 3). Each barrier “node” demonstrates that when a certain potentially dangerous condition arises there is a need for an intervention. This is represented in Figure 4.

¹ 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.

FIGURE 2 ROUTE 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

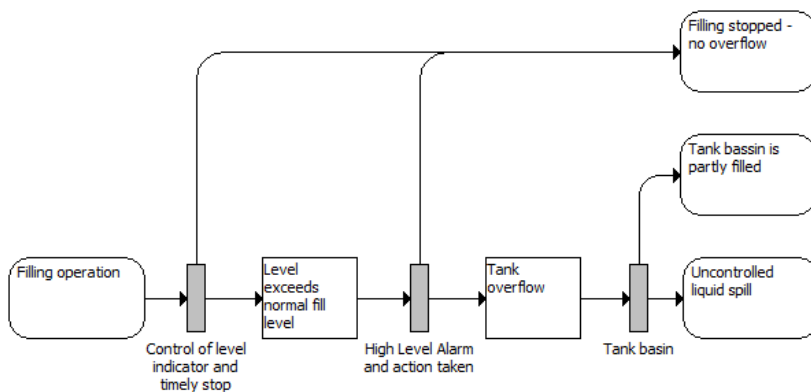


FIGURE 3 EXAMPLE OF A SAFETY-BARRIER DIAGRAM (FROM SAFETYBARRIERMANAGER² 2015 DTU³). SAFETY BARRIERS ARE REPRESENTED BY THE GREY BARS

² SafetyBarrierManager (2015) SafetyBarrierManager, Technical University of Denmark. <http://www.safetybarriermanager.man.dtu.dk/About-Safety-Barrier-Manager>

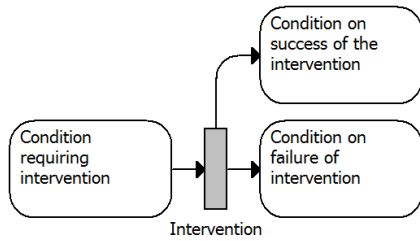


FIGURE 4 BARRIER "NODE": THE INTERVENTION IS A RESPONSE TO A CONDITION, AND DOES NOT CONCERN THE CAUSES OF THE CONDITION

When there are challenges to maintaining a safe condition there may be a drifting towards failure. The resilient intervention comes before the system fails as shown in Figure 5.

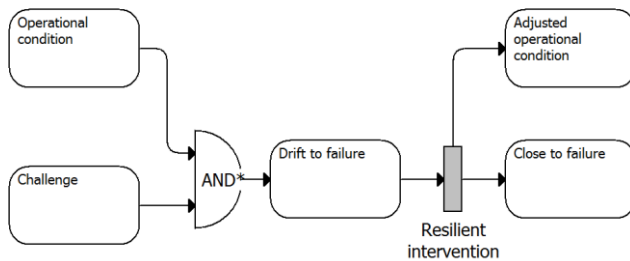


FIGURE 5 INTERVENTION LEADING TO A NEW SAFE OPERATIONAL CONDITION

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

There are 36 barriers in the Dutch major hazard model (from analysis of loss of containment data of the Dutch Labour Inspectorate, Bellamy et al). Due to some barriers being removed from the original model the numbers 19, 21, 27, 30, 33, 37 no longer exist.

TABLE 2 BARRIERS IN THE DUTCH MAJOR HAZARD DATABASE³

| Code | Barrier name | Barrier description |
|------|--|---|
| B_X | Not a MH barrier | Not a major hazard barrier but failures in the barrier system may have implications for MH barriers (see Precursors) |
| B_nn | New barrier | A new barrier, unanticipated, not previously encountered (requires a new number) |
| B_00 | Unknown | Not enough information to identify the barrier |
| B_01 | Equipment selection | E.g. the intended containment is selected |
| B_02 | Pre-start-up safeguarding | Safeguarding of a containment means: bringing the containment in such a state that it can be opened safely. Safeguarding can be done in a number of ways: 1. by emptying 2. by emptying and cleaning 3. by isolation 4. by depressurisation 5. by cooling 6. by bringing the content into a certain phase (e.g. from liquid to solid) |
| B_03 | Operating conditions | This refers to the (control of) normal operating conditions in which the installation is operated (flow, temperature, pressure, etc.), as well as to specific operating conditions, such as erosive or corrosive, vibrating, fatiguing or other process related conditions that might lead to a deviation outside the normal operating window. |
| B_04 | Equipment Material | Containment or support materials (type of materials, thickness of materials, design etc) which can withstand the specified conditions. The 'containment (support) material barrier' has to prevent that the materials of the containment or the containment support deteriorate because wrong containment materials for the process are selected, or because wrong containment support materials are selected or the thickness of the materials is too low. This failure mode leads to one or more deviations or Loss of Control Events, such as corrosion, erosion or other material weakening/fracturing. |
| B_05 | Equipment design | e.g., the configuration of a containment can sometimes lead to undesired conditions such as 90 degrees bends in pipelines which can lead to higher rates of erosion |
| B_06 | Equipment connection | |
| B_07 | Installation of equipment | installation/ assembly |
| B_08 | Control of movement/ position of containment | E.g. securing the containment while it is being transported or stored |
| B_09 | Process temperature control | Barrier controlling the temperature of the process (heating/ cooling) to stay within the safe operating window |
| B_10 | Control of reaction | Barriers limiting the power of the agent |
| B_11 | Pressure control | Barrier keeping the pressure of the process to be within the safe operating window |
| B_12 | Flow control | Barriers preventing no flow/ too much/ too little/ reverse flow |
| B_13 | Separation of incompatible substances | Prevention of undesired reactions between incompatible substance |

³ 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.

| Code | Barrier name | Barrier description |
|---------------------|---|---|
| B_14 | Control site environment | This refers to the protection of the ((critical) process equipment, containment with the hazardous substances against external influences from extreme weather, water, traffic, etc. |
| B_15 | Common mode control | Barrier to prevent common mode failure through loss of a utility (e.g. steam, power, compressed air) |
| B_16 | Collision prevention | Separation from moving objects - containments by distance or control of flow. A moving object can also be a (part of a) human body |
| B_17 | Storage/ transportation conditions | |
| B_18 | Separation from heat sources | Barriers of separation. Separation of containments and: - high temperature equipment or piping in the vicinity (e.g. outlets of furnaces, steam piping). - hot work activities - external fires |
| B_20 | Deviation recovery | To restore the process within normal operating conditions |
| B_22 | Containment bypass | Containment intact but bypassed" (e.g. opened, lose or untight connections, etc.)" |
| B_23 | Impact protection | A physical separation barrier or additional strength / constructions to protect against: 1. an object hitting the containment 2. the containment hitting an object (in case of mobile containments like drums, etc). 3. the falling/ capsizing of the containment |
| B_24 | Explosion/ fire prevention (internal) | Flammable/explosive atmospheres must be protected (keeping separate) from ignition sources. |
| B_25 | Secondary containment | Additional physical barrier or secondary containment to protect the system against LoC |
| B_26 | Emergency protection | This is the barrier to protect the containment from losing its integrity, once the safe operating limits have been reached. The barrier refers to the safety function related to countermeasures that eliminate the deviation outside safe operating limits and/or mitigates the effects in such a way that the containment integrity is kept. This could be a in lot of different forms, either active (automatically initiated or manual, like a pressure relieve valve to a safe location) or passive (like an additional safety factor for strength of the containment) |
| Centre Event | Loss of containment | |
| B_28 | Release shut-off response | In order to limit the released material this barrier offers four options: 1. Closure of the containment (this is only an option in case of a by-pass LOC) 2. Stopping the feed flow to the open containment (= isolating the involved containment) by closing valves. 3. Reconnection of the loose connection 4. Covering/sealing the damaged containment opening Ad1. Example of containment closure: If a valve of a containment is accidentally open(ed) and substance is released an action can be taken to close that valve Ad 2. Examples of stopping the feed flow: If the pressure in a tank drops too quickly because of a release the valve controlling the feed flow might be closed automatically |
| B_29 | Reduction of driving sources behind the release | This barrier has to prevent or reduce prevent driving sources behind the release, other then by shut-off. Examples: - prevent contact with other substances to prevent formation of hazardous reaction products - prevent contact with heat sources - cooling This failure mode leads to the Loss of Control Event 'Uncontrolled Release of Hazardous substance'. |
| B_31 | Dispersion/ evaporation | In order to limit the dispersion of the released material this barrier offers e.g. the |

| Code | Barrier name | Barrier description |
|-------------|--------------------------------------|---|
| | reduction | following two options: 1. For automatic and semi-automatic static systems: a piece of hardware (mostly a valve or a pump) is activated and releases the medium or objects which prevent or limit the dispersion (foam, water, etc) 2. For (manual) mobile systems: a piece of hardware is transported to the right location and is activated manually (fire brigades bringing a water pump to the location of interest) 3. Passive: installation inside a building |
| B_32 | Emergency containment | e.g. a bund |
| B_34 | Ignition control | |
| B_35 | Fire/explosion fighting response | Actions to limit the spreading of a fire/explosion |
| B_36 | Hazardous substance separation | The separation of one containment to the other could have prevented the spreading of the fire or the domino-effects of the explosion. There are two types of separation: - physical barriers (like fire walls): compartment - distance |
| B_38 | Personal Protective Equipment (PPE) | Personal Protective Equipment |
| B_39 | Evacuation | |
| B_40 | Shelter | This is inside the hazardous area (explosion proof building, etc) |
| B_41 | Distance to hazardous area | |
| B_42 | Emergency response - remedial action | The remedial action barrier has to prevent that consequences of an exposure to hazardous substances or to the effects of a fire or an explosion will increase because of no or delayed medical attention. Any aid directly given after the exposure might be of significant importance with regard to minimizing the final effects of the exposure. The failure of this barrier is represented by the Barrier Failure Mode Storybuilder box: 'no, late or inadequate first aid'. The failure mode of this barrier leads to prolonged negative effect of exposure to a hazardous substance, fire or explosion. |

4 STEP 2: THE STAGE OF INTERVENTION

The stage of intervention depends on how deep a signal (or precursor) is identified as signalling a condition requiring intervention. The stages are shown in Figure 6.

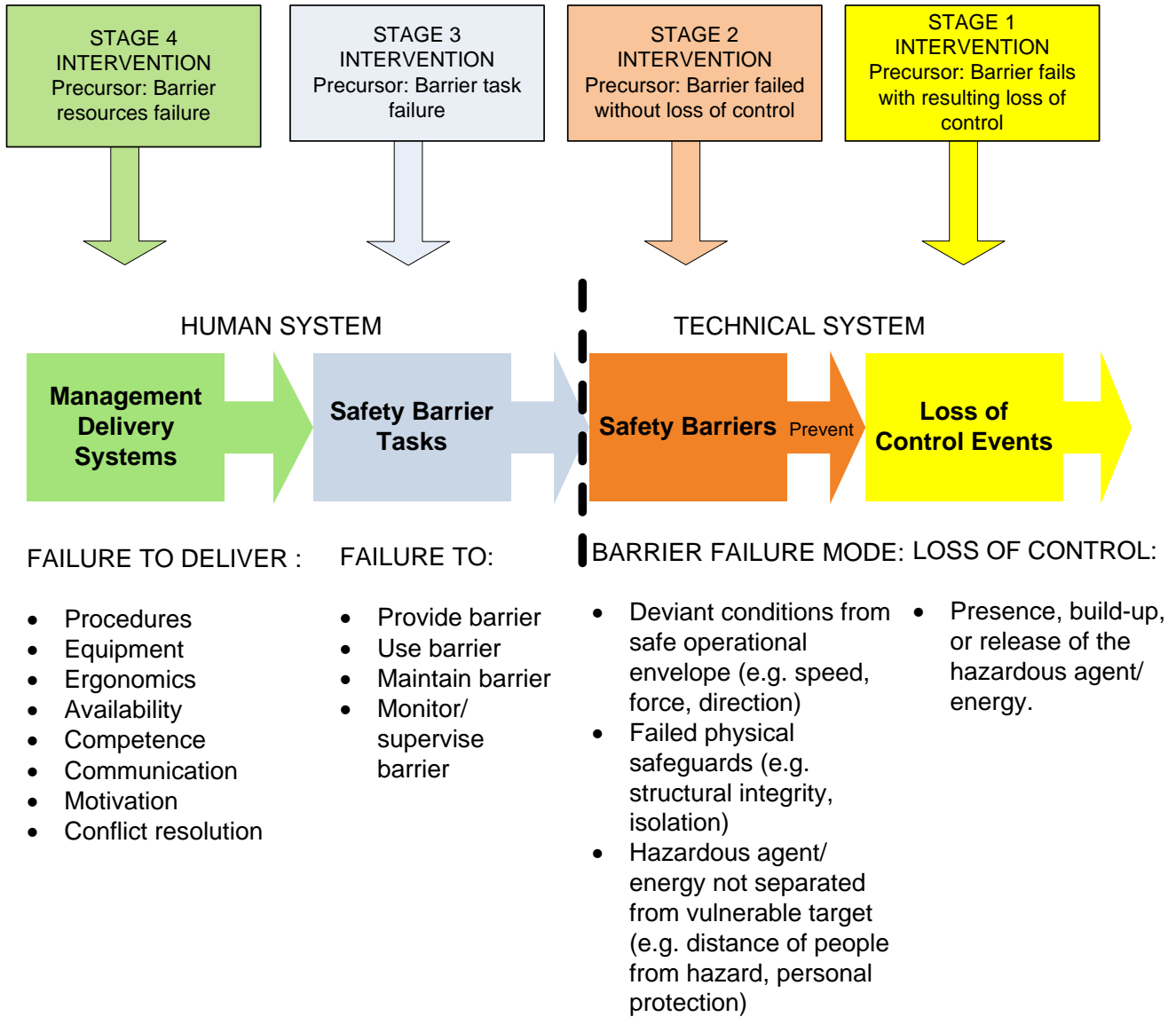


FIGURE 6 STORYBUILDER BARRIER MODEL SHOWING STAGES OF INTERVENTION

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

The definitions of the management delivery systems and the barriers tasks are given in Annex E. Glossary section E.2.

TABLE 3 STAGE AT WHICH AN INDICATION OF AN UNSAFE CONDITION IS DETECTED AND RESPONDED TO.

| Intervention stage |
|---|
| 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).

5 STEP 3: PRECURSORS

Precursors can be developed specifically for each intervention stage. These are the events which are signals of deviation or change. Recount the process of intervention, through the Indication, Detection and Diagnosis of signal, the Decision and carrying out of the Response (IDDDR).

5.1 Stages 1 & 2

For major hazards this is classified into the following types.

TABLE 4 A SET OF STAGE 1 AND STAGE 2 PRECURSORS (MAJOR HAZARD RELATED)

| Stage 1 & 2 precursor |
|--|
| 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 |
| Falling or moving objects/missiles |
| ..Other |

5.2 Stages 3 & 4

These are failures in the human part of the system. These may be failures associated with MH barriers or non-MH barriers but which could otherwise happen with a MH barrier.

A barrier has not been *provided* (designed) which can handle all the operating conditions.

An operator has used the wrong specification material when replacing a pipe and in so doing has failed to *maintain* the barrier function

An operator opens a valve and walks away instead of staying to *monitor* that it works as intended

TABLE 5 BARRIER TASKS (STAGE 3) E.G. PROVIDE (DESIGN, INSTALL) INADEQUATE OR WRONG BARRIER
USE THE WRONG WAY OF WORKING

| Barrier task |
|----------------------|
| Provide |
| Use/Operate |
| Maintain |
| Monitor |
| Unknown barrier task |

TABLE 6 MANAGEMENT DELIVERY SYSTEMS (STAGE 4) E.G. NONCONFORMITY BETWEEN PROCEDURES/DRAWINGS AND
REALITY AS YET WITHOUT CONSEQUENCE

| Management Delivery System |
|-----------------------------------|
| Equipment |
| Ergonomics/ MMI |
| Conflict resolution |
| Motivation/ Awareness |
| Communication/ Collaboration |
| Plans and procedures |
| Availability |
| Competence |
| Unknown delivery system failure |

The definitions of the management delivery systems and the barriers tasks are given in Annex E. Glossary section E.2.

6 STEP 4 PROCESS OF PRIMARY INTERVENTION - IDDR

Of interest in this model are the monitoring of variation or change undertaken by humans and the responses that are made. Figure 5 represents the issues involved in humans making adjustment to real world situations.

In this part of the model humans identify change/deviation, decide what to do about it and respond successfully. This is called the IDDR: which is a sequence of Indication, Detection, Diagnosis, Decision, and Response as shown in Figure 7.

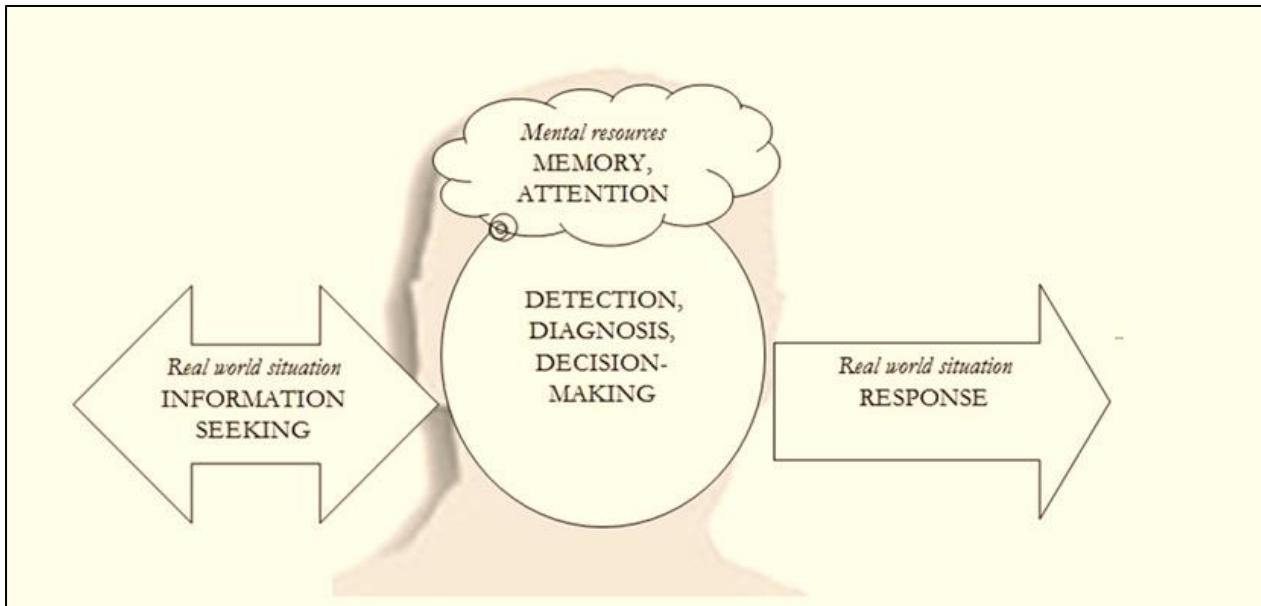


FIGURE 7 THE MENTAL MODEL FORMULATED AS “I-D-D-R”: INDICATION, DETECTION, DIAGNOSIS, DECISION-MAKING AND RESPONSE

The IDDR process can be analysed to determine patterns of events and responses that are occurring in response to deviations.

The successful outcomes are about adapting to change and variation where the result is that operations can be sustained. The process between change and outcome is IDDR. The components are given in Table 7

TABLE 7 BASIC IDDR COMPONENTS

| IDDDR component | Details (describe the nature of the signal) |
|--|---|
| INDICATION TYPE & STRENGTH | <i>The indication is a <u>signal</u> of deviation or change</i> |
| TYPE (I) | <i>The signal type is either generated by automation or is itself a salient property of the change</i> |
| Indication type unknown | |
| Salient object/environmental/human change | e.g. smoke, corrosion, human fatigue |
| Automated indication | e.g. alarm, instrument reading |
| SIGNAL STRENGTH (I) | <i>This is in relation to a human – how strong is the signal, how likely to be perceived? The sensitivity to the signal depends on the separation of the signal distribution from the noise event distribution. Low sensitivity</i> |
| Signal strength unknown | Nothing is said about the signal |
| Strong | e.g. attention gaining; hard to miss |
| Medium | not particularly strong or weak |
| Weak | e.g. near detection threshold; hidden in noise, easy to miss, ambiguous |
| DETECTION MODE (D1) | <i>This is picking up the signal</i> |
| Detection mode unknown | |
| Human | How does detection come about? e.g. inspection, measurement, being present |
| Automated | e.g. automatic gas detection |
| DIAGNOSIS/DECISION/RESPONSE SELECTION MODE (D2) | <i>This is diagnosing the problem and deciding on the appropriate response...aiming for success</i> |
| Decision mode unknown | |
| Human | How does the diagnosis and decision come about? E.g. monitored for an hour and brought in the experts |
| Automated | Fixed response; response thresholds e.g. a trip system operates. |
| RESPONSE (R) | |
| Action | Was there an immediate action? |
| Specify direct response action | e.g. operate second valve |
| | |

7 STEP 5 PROCESS OF SECONDARY INTERVENTION

In the model the (improved) barrier conditions that result from the intervention are classified as in Table 8.

TABLE 8 RESULTING BARRIER CONDITIONS AFTER INTERVENTION

| New condition | Description |
|---|---|
| Barrier response unknown | Unknown what barrier intervention was performed |
| Placement of a new barrier | Sometimes barriers are not there at all when they need to be. These are completely new barriers for achieving the specific function. |
| Replace barrier with a better one | These are actions where operators find better ways to operate, or where better materials or better equipment is introduced. |
| Replace barrier: like with like | The failed barrier is replaced with the same one |
| Improve or adjust barrier (to its original condition) | Barriers are restored to their original function (e.g. by improving settings, repair, cleaning, removing blockages, tightening equipment) |
| Verify/check barrier | To maintain a barrier function the ‘checking’ of the (right) barrier function done to determine whether the quality of the barrier function is still at an acceptable level |
| Analyse barrier problem | The barrier problem is required to be analysed but the result is unknown. |
| Cease the activity (no new barrier can be identified) | If no barrier can be found for controlling the hazard the activity which creates the hazard is stopped |

8 STEP 6 RESILIENCE COMPONENTS

Resilience components are uncertainty reducing.

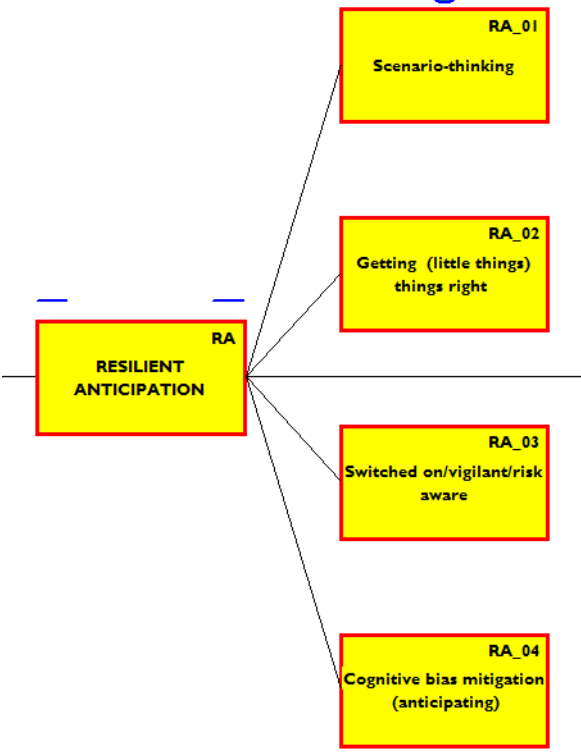
There are 4 capabilities required for a system to be resilient according to the Resilience Engineering approach. These capabilities are developed on the basis of resilience case studies (Van Galen & Bellamy 2014).

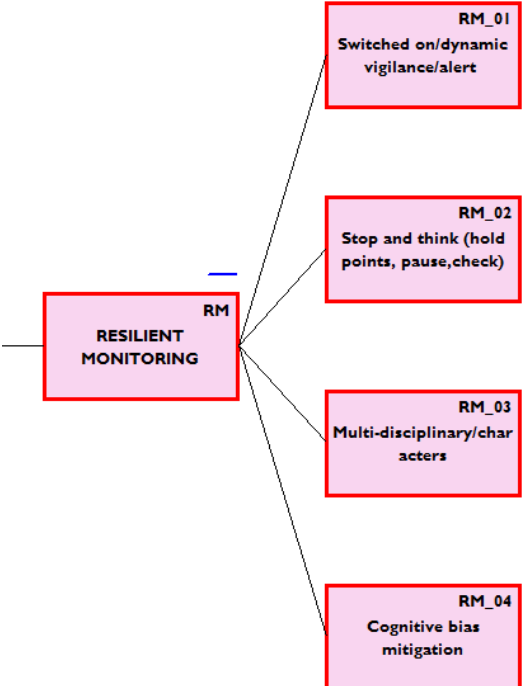
Resilience components can be added to relevant points in the recovery process on the management delivery systems which are shown in Stage 4 or the Barrier task in Stage 3. A suggested use of the components with the delivery systems is shown in Table 9.

TABLE 9 ASSOCIATION OF RESILIENCE COMPONENTS WITH THE MANAGEMENT DELIVERY SYSTEMS

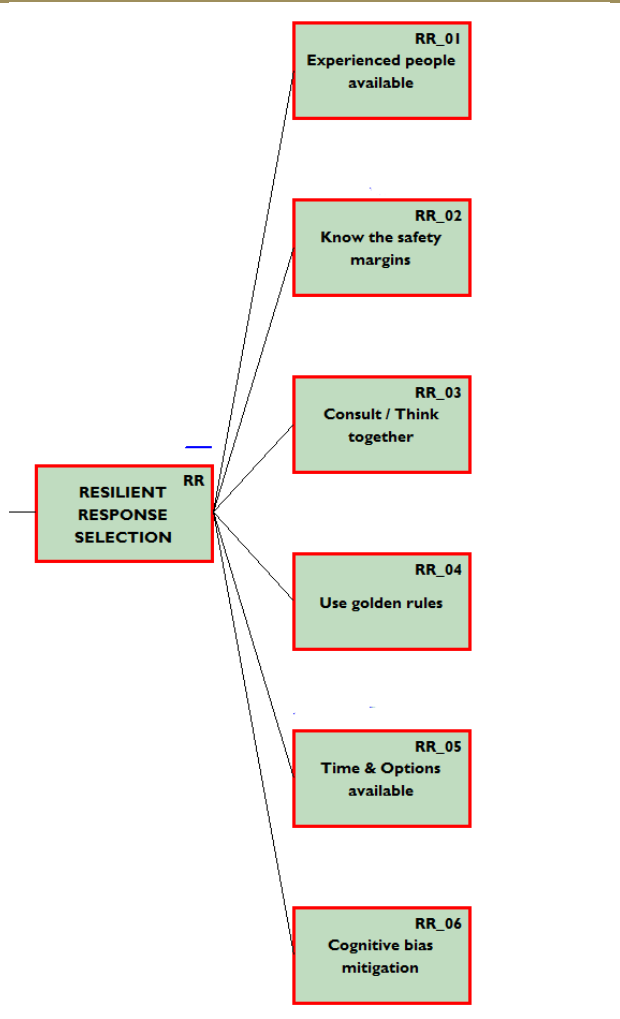
| DELIVERY SYSTEM | LEARNING | | | | | | ANTICIPATING | | | |
|-----------------------------|-------------------------------------|--|------------------------------------|---------------------------|------------------------------|--------------------------------------|------------------------|--------------------------------------|---------------------------------|--|
| | RL_01 | RL_02 | RL_03 | RL_04 | RL_05 | RL_06 | RA_01 | RA_02 | RA_03 | RA_04 |
| | 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 | | | | | | | | • | | |
| DELIVERY SYSTEM | MONITORING | | | | RESPONDING | | | | | |
| | RM_01 | RM_02 | RM_03 | RM_04 | RR_01 | RR_02 | RR_03 | RR_04 | RR_05 | RR_06 |
| | Switched on/dynamic vigilance/alert | Stop and think (hold points, pause, check) | Multi-disciplinary/characteristics | 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 | | | | | | | | | | • |

TABLE 10 FOUR CORNERSTONES (ABILITIES) OF RESILIENCE

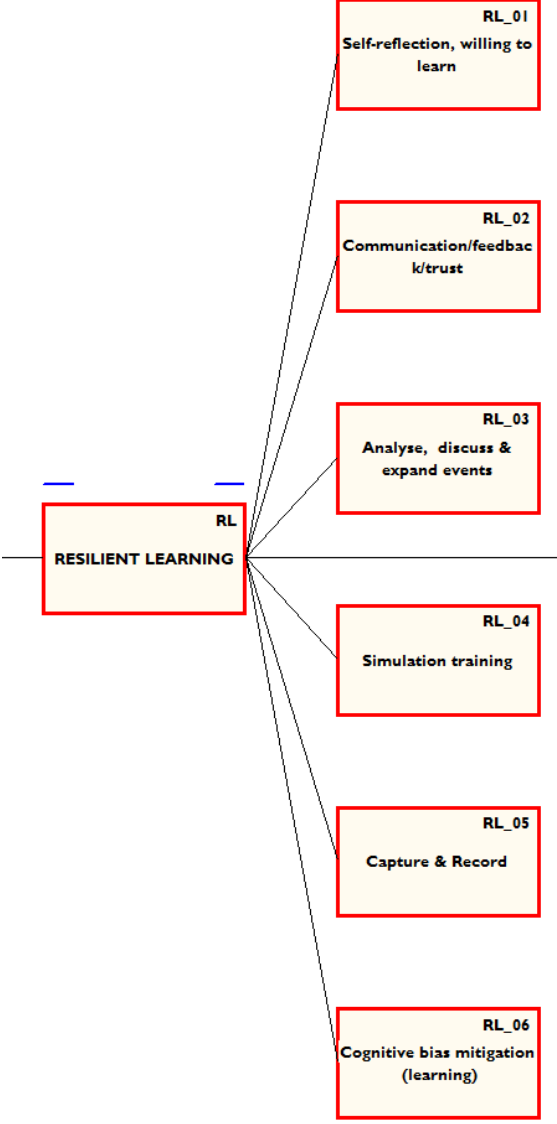
| Cornerstones | Capabilities | Description (using case studies) |
|---|---|--|
| ANTICIPATING (Storybuilder code: RA) | <i>Knowing what to expect. Capability to anticipate future threats & opportunities - how to anticipate developments and threats further into the future, such as potential disruptions, pressures, and their consequences. This is the capability to address the potential.</i> |  |
| ANTICIPATING | Scenario-thinking | Trying to think ahead and anticipate future situations, a future-oriented form of sense-making. Thinking through scenarios, using experience and cross checking with the current state. Being able to make a picture in your head about how things will develop and preparing for that. The more you can foresee things happening, the more you can prevent or prepare for the threats |
| ANTICIPATING | Getting (little things) things right (so as not to compromise future states) | Dedicated to getting the little things right on a daily basis means that you will have the best cards when the time comes e.g. making sure you have all the right tools and equipment, things are being done properly; sticking to the plan. Focussing on the details. |
| ANTICIPATING | Switched on/vigilant to what can go wrong (risk aware) | Aware means aware of risks and uncertainties, sensitivity to deviations. It is about being able to recognise and understand what is happening around you. Looking at the past and future in relation to now (looking in 4- dimensions) |

| Cornerstones | Capabilities | Description (using case studies) |
|---------------------------------------|---|--|
| ANTICIPATING | Cognitive bias mitigation (Anticipating) | <p>Getting round the problems of biases/shortcuts which threaten anticipation. Routine is a threat (to being switched on), also confirmation bias (looking for confirming information), anchoring bias (tendency to rely too heavily on the first piece of information offered - the "anchor"), availability heuristic (if something can be recalled, it must be important).</p> <p>Mistakes, near misses and incidents play a role in becoming and staying vigilant, learning, improving and adjusting.</p> <p>The difference between situations requiring a normative approach and the transition to a resilient approach should be clear.</p> |
| MONITORING (Storybuilder code: RM) | <p><i>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. It includes looking out for each other.</i></p> |  <pre> graph LR RM[RESILIENT MONITORING RM] --- RM01[RM_01 Switched on/dynamic vigilance/alert] RM --- RM02[RM_02 Stop and think (hold points, pause, check)] RM --- RM03[RM_03 Multi-disciplinary/characters] RM --- RM04[RM_04 Cognitive bias mitigation] </pre> |

| Cornerstones | Capabilities | Description (using case studies) |
|--------------|--|--|
| MONITORING | Switched on/Vigilant/Alert (for signal detection/change) | <p>The person is actively engaged in their task. 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 (looking out for each other) 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. This has been called detecting on four dimensions. Could be threatened by fatigue especially under time pressure.</p> <p>This is all about continuously maintaining a high level of alertness and awareness, not shutting your eyes to things. Vigilance is a state in which a high level of attention must be maintained over long periods of time, watching out for signals that could be precursors of larger change.</p> |
| MONITORING | Stop and think (hold points/cross check/pause at critical steps) | <p>Organisational process which needs time and resources for reflection when dealing with uncertainties. Hold points and decision nodes provide the opportunity for coming together, thinking together, getting second opinions. In dynamic situations with developing scenarios it is important to have time-spaced hold points to allow for data gathering, assessment and balanced decision making. These hold points can be discerned beforehand, while planning an activity, or they can be defined when there is a novum: a new - not thought of – situation or change.</p> |
| MONITORING | Multidisciplinary/different characters | <p>Having available multidisciplinary knowledge and experience, balancing characters like devils advocates as well as people who want to push forward, to be able to reduce uncertainties. Seeing the world from different perspectives.</p> |
| MONITORING | Cognitive bias mitigation (monitoring) | <p>Mitigating awareness-limiting mental traps like confirmation bias (looking for confirming information) and the dangers of routine and narrowed attention..</p> <p>The difference between situations requiring a normative approach and the transition to a resilient approach should be clear.</p> |

| Cornerstones | Capabilities | Description (using case studies) |
|--|---|---|
| <p>RESPONDING (Storybuilder code RR)</p> | <p><i>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.</i></p> |  <pre> graph LR A[RESILIENT RESPONSE SELECTION] --- B[RR_01 Experienced people available] A --- C[RR_02 Know the safety margins] A --- D[RR_03 Consult / Think together] A --- E[RR_04 Use golden rules] A --- F[RR_05 Time & Options available] A --- G[RR_06 Cognitive bias mitigation] </pre> |
| <p>RESPONDING</p> | <p>Experienced people available</p> | <p>Experienced people simply have already encountered many different situations and know on the basis of past experiences how to (re)act on the actual.</p> <p>Knowing the rules and procedures in combination with training are important aspects of experience. A certain number of hours in practice can be a measure of expertise.</p> <p>Assertive and confident.</p> |
| <p>RESPONDING</p> | <p>Know the safety margins and one's own limitations</p> | <p>Knowing and keeping within the safety margins. This requires good feedback about one's position in relation to margins.</p> <p>Working things out in advance.</p> |

| Cornerstones | Capabilities | Description (using case studies) |
|--------------|--|---|
| RESPONDING | Consult with others/think together (multidisciplinary/different characters) | Open up communications. This is an organisational process which brings together people who can help to reduce the uncertainty. Having different disciplines, experience and characters (risk averse, devil's advocates, pushers) enhances getting data on the different perspectives of the situation. For every resilience cornerstone, thinking together can enhance the information gathering, decision-making and help the avoidance of the effects of cognitive biases |
| RESPONDING | Use of golden rules/principles | Setting golden rules and keeping to them e.g. if you can't get to the summit by 2 o'clock turn around. |
| RESPONDING | Time and options available | Having time and options for responding, including redundancies. This can include support from automatics for buying time. |
| RESPONDING | Cognitive bias mitigation (responding) | Avoiding biases such as summit fever – where the danger is ignored and there is an urge to reach the goal ...summit fever could be avoided when team members have balancing characters and by applying the golden rules. Other biases include overconfidence, routine, living up to the aura of the expert. The difference between situations requiring a normative approach and the transition to a resilient approach should be clear. Under time pressure in an emergency there is an urge to react immediately. |

| Cornerstones | Capabilities | Description (using case studies) |
|--|--|---|
| <p>LEARNING (Storybuilder code RL)</p> | <p><i>“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.”</i></p> |  |
| <p>LEARNING</p> | <p>Self-reflection</p> | <p>Being willing to look back and learn from the past – also when things turned out right. Also the deepening of self-knowledge, “mindfulness” – the quality of attention to concrete detail. Comprehensively analysing behavior and evaluating the contribution of its components to performance outcomes.</p> |
| <p>LEARNING</p> | <p>Communication/feedback/trust</p> | <p>Communication and trust are essential to encourage human resilient intervention. Tight feedback mechanisms, extensive and fast networks. Communication and trust contribute to the data sharing and the feedback and to the sensitivity of people to signals. Decisions made under high time pressure and uncertainty should be supported.</p> |

| Cornerstones | Capabilities | Description (using case studies) |
|--------------|---------------------------|--|
| LEARNING | Simulation | An activity that models through imitation and enactment how something happens in reality to enable training and practice e.g. emergency response exercise, process control computer simulation. |
| LEARNING | Capture & record | The activity of identifying relevant data and recording it such that it remains in organisational memory and is available for scrutiny e.g. a showcase of lessons learned |
| LEARNING | Cognitive bias mitigation | There is a danger of being attracted to success. Sometimes success is just luck and not the result of being resilient. The difference between situations requiring a normative approach and the transition zone to a resilient approach should be clear. |

9 STEP 7 UNCERTAINTY

| Uncertainty Component | Description |
|------------------------------------|--|
| TYPE | |
| TYPE UNKNOWN | Insufficient information available to specify type of uncertainty |
| KNOWLEDGE (EPISTEMIC) UNCERTAINTY | <i>Uncertainty is primarily a consequence of the incompleteness and fallibility of knowledge ('knowledge-related', or 'epistemic' uncertainty).</i> Epistemic uncertainty (also called reducible uncertainty or incertitude) is a potential deficiency that is solely due to a lack of knowledge. It can arise from assumptions introduced in the derivation of the mathematical model used or simplifications related to the correlation or dependence between physical processes. It is obviously possible to reduce the epistemic uncertainty by using, for example, a combination of calibration, inference from experimental observations and improvement of the physical models. Epistemic uncertainty is not well characterized by probabilistic approaches because it might be difficult to infer any statistical information due to the nominal lack of knowledge. Typical examples of sources of epistemic uncertainties are turbulence modeling assumptions and surrogate chemical kinetics models. |
| Scenario Uncertainty | 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 | Uncertainties known to be there in some way or another (known unknowns) but for which no useful estimate can be established; for example, due to limits to predictability and knowledge ('chaos') or due to unknown processes. |
| ALEATORY (VARIABILITY) UNCERTAINTY | Uncertainty due to the intrinsic indeterminate and/or variable character of the system under study ('variability-related', or 'ontic' uncertainty). Aleatory uncertainty (also referred to as variability, stochastic uncertainty or irreducible uncertainty) is the physical variability present in the system being analysed or its environment. It is not strictly due to a lack of knowledge and cannot be reduced.. Aleatory uncertainty is normally characterized using probabilistic approaches. |
| Statistical uncertainty | The uncertainties that adequately may be expressed in statistical terms; for example, as a range with associated probabilities (e.g. statistical expressions for measurement inaccuracies, uncertainties due to sampling effects, and uncertainties in model-parameter estimates). However this may not be an adequate description of the real world and other (deeper) forms of uncertainty may be at play |

| Uncertainty Component | Description |
|-----------------------|--|
| LEVEL | <i>Determined from the point of view of the decision-maker, the level of uncertainty is coupled to the resilience involved in decision-making</i> |
| LEVEL UNKNOWN | Insufficient data to come to any conclusion |
| HIGH | <p>A brittle decision which incorporates no learning, anticipation, monitoring or any real evidence of knowing what to do. <i>“For example 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’.”</i></p> <p>Number of Resilience components 6 or less.</p> |
| MEDIUM | <p>A decision which incorporates some of the components of resilience but which misses a comprehensive approach to information seeking, awareness of what is and could happen and knowing what to do. <i>“One thing we hadn’t anticipated was that the hoods fogged. That was something daft and simple. Again we reacted really quickly because we didn’t want anyone else getting sprayed. If you go too quickly then you miss things so that’s where you need that balance between going quickly for all the right reasons, but not necessarily doing the right thing, and checking before you implement things.”</i></p> <p>Number of Resilience components 7-13</p> |
| LOW | <p>A decision which incorporates all the key components of resilience: taking learning into account, anticipating future states, switched on monitoring and knowing what to do – also involving: consultation with others with appropriate experience/intelligence/discipline knowledge.</p> <p><i>“There’s always, of course, knowledge limitations. I am the first person to say that I do not have all of the knowledge. That’s part of my role. In risk management is, of course, a very large chunk of that. Enabling people to do good risk management, and sometimes a call-by role that I have it’s more in making sure that, “were the right people involved? Were the right questions asked?” And I’m not stupid, I will poke and fool around a little bit as well with my questions to challenge them, if they looked at the different aspects and what are the probabilities. Where are the knowledge gaps? Because there are always certain things you don’t know, you can’t always look into the pipe. What’s happening on the inside? How a certain degradation mechanism, corrosion mechanism, how is that going to progress? There are uncertainties there.</i></p> <p><i>The global corporation that we are, there is a solid base on engineering, on data. So based on that history, based on the knowledge that we have within the corporation, we try to assess as well as we can the probabilities of what is happening or what could happen, and what could then be the consequence. Based on that we try to assess, “what kind of preparations do we need to do? What kind of mitigations do we need to do? Continue operation or not?” Those kind of assessments. You use the combined knowledge that we have within the corporation. But there are always uncertainties.”</i></p> <p>Number of Resilience components 14+</p> |

10 OVERVIEW OF FIELDS

Any type of success event can be taken through the model using 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

For an analysis example see the main report, section 8.2.3 Translating lessons learned into the success model.