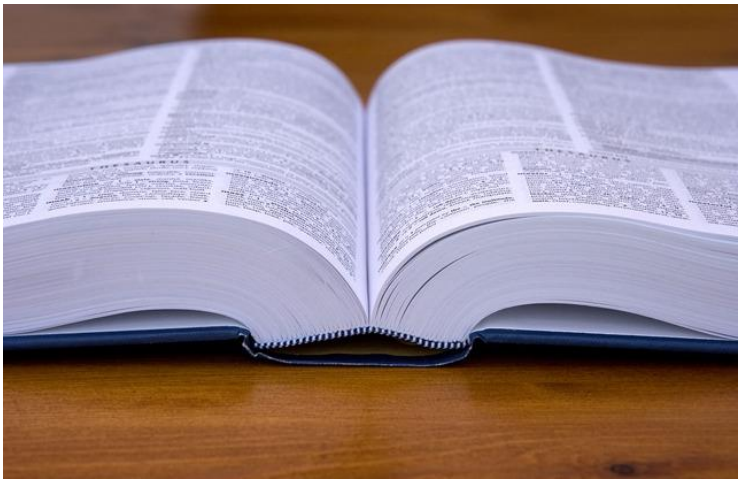
RESILIENCE
SUCCESS CONSORTIUM

SUCCESS IN THE FACE OF UNCERTAINTY

ANNEX E GLOSSARY OF TERMS



29 March 2015

Bowtie, barrier and resilience terminology

Rev 02

Authors: Nijs Jan Duijm, Linda J. Bellamy, Anne van Galen, Olga Aneziris, Arthur Dijkstra

CONTACT

Nijs Jan Duijm
Senior Researcher, Management Engineering, Technical University of Denmark (DTU), Denmark
nidu@dtu.dk

Linda J. Bellamy
Consultant & Managing Director, White Queen BV, PO Box 712, 2130AS Hoofddorp, the Netherlands
linda.bellamy@whitequeen.nl

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

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

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

Consortium

http://www.resiliencesuccessconsortium.com/

Dr Linda J. Bellamy (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**

RESILIENCE
SUCCESS CONSORTIUM

Annex E Glossary of Terms

BOWTIE, BARRIER AND RESILIENCE TERMINOLOGY

Contents

ANNEX E: GLOSSARY OF TERMS

E.1 General terms

Term	Definition	Annotations	Alternative or close terms
Anticipation	Finding out and knowing what to expect in the future; the ability to anticipate future threats and opportunities (Hollnagel)	This is one of the four cornerstones of resilience engineering (Hollnagel et al 2011). Also defined by Wildavsky (1998) - efforts are made to predict and prevent potential dangers before damage is done. [1]; however there may be false alarms so better to remain flexible. See also *Monitoring, Learning, Responding.*	A future oriented form of *sensemaking*
Barrier Elements	The *elements* (as referred to in the definition of the safety barrier by Duijm 2009[2]) that constitute the safety barrier.	An element can also be a system, e.g. an alarm system is an element in a barrier that describes an operator intervention Elements may also be rather abstract, such as "provision of electrical power"	Critical Equipment & Critical Element (Shell 2009)[3]

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

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

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

[3] Shell International Exploration and Production 2009 Safety Critical Element Management Manual, second edition EP2009-9009 Feb 2009

Term	Definition	Annotations	Alternative or close terms
Barrier function	A barrier function is a function planned to prevent, control, or mitigate undesired events or accidents (Sklet, 2006)[4] A barrier function is a function planned to prevent, control, or mitigate the propagation of a condition or event into an undesired condition or event (Duijm, 2009)[2]	The definition by Duijm tries to capture that the barrier function shall intervene in an undesired sequence of events. Such intervention is primarily an unplanned, unexpected activity, as the undesired sequence is unexpected	Safety function
Bowtie	Graphical representation of how different 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.	Deviations are shown on the left hand side, and consequences on the right hand side of the critical event. The left hand side can be considered as a fault tree with the critical event as the top event, while the right hand side can be considered as an event tree.	Similar graphical representations are: Cause-consequence diagrams and safety-barrier diagrams. These representations do not use the notion of a central critical event.
Cognitive bias	Unconscious, automatic influences that change the perception of a condition to be different from what (objectively) can be deduced from accessible information, and thus affects human judgment and decision making about that condition	There are different (psychological) causes for cognitive bias: 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. See also Tversky & Kahneman 1974; Kahneman et al 1982; Kahneman 2011; Pohl 2012[5]	

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

[5] Tversky, A. & Kahneman, D., 1974 Judgment under Uncertainty: Heuristics and Biases. Science Vol. 185, No. 4157. (Sep. 27, 1974), pp. 1124-1131
Kahneman, D., Slovic, P., Tversky, A. (eds.) 1982. Judgment under uncertainty: Heuristics and Biases , Cambridge University Press, New York
Kahneman, D., 2011. Thinking fast and slow. New York: Farrar Straus & Giroux. (Paper back 2012 Penguin Books)
Pohl, R.E. (Ed.) 2012. Cognitive illusions. A handbook on fallacies and biases in thinking, judgement and memory. Psychology Press, Hove, UK.

Term	Definition	Annotations	Alternative or close terms
Confidence bias	An illusion of judgment made by individuals when they assess the correctness of their judgements, inferences or predictions; the subjective probability of a judgement does not match its objective probability. People tend to have too strong a belief in the correctness of their judgements (overconfidence)		
Consequence	The final undesired outcome of an accident. 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.		
Control	All actions that can be considered as being part of normal operation, that aim at ensuring that conditions are within the normal operational variability, and that contribute to mission success.	The BPCS is a typical example of a control	
Critical event	The event at which point a hazard materializes into damaging phenomena. This phenomenon can be described as an unconfined flow of energy (UFOE). So the critical event leads to an UFOE	All paths in a bowtie pass the critical event. This means that a bowtie is linked to the hazard that is released at the critical event.	Central event Top event (Shell HEMP)
Deviation	The event or situation that is outside the normal operating variability and which requires intervention beyond normal process control in order to avoid development towards a critical event	What is "beyond normal process control" may be subject to interpretation, especially in one-off missions, where there is no "normal" reference.	Initial event Initiating event Threat (Shell HEMP)
Element	In the context of decomposition of systems, elements constitute the system and each element can be considered as a separable subsystem or component with a separable function within the system it is a part of.	An element can be a system itself.	

Term	Definition	Annotations	Alternative or close terms
Failure	A failure is an event which causes a loss of ability to perform according to a requirement or goal. In the context of safety the failure will be associated with a safety function like a barrier.		
Hazard	Inherent property of an agent or situation capable of having adverse effects on something. Hence, the substance, agent, source of energy or situation having that property. (UN OECD, 1999) The potential of an agent or situation to cause an Unconfined Flow Of Energy (UFOE)	There are simpler definitions (ISO: potential source of harm), but the UN OECD definition links hazard to both property, potential (capable of) and the agent itself. "Energy" in UFOE should be interpreted in the broadest sense: it includes e.g. toxic "energy": the potential of chemicals or biological agents to damage life. Note that in the Bowtie (Shell HEMP[6]) the hazard is often linked one-to-one to the critical event, so the critical event is the event or point where the hazard is realised (turning from a potential impact into a real impact)	Risk source (sometimes used interchangeably with hazard)
Intervention	Any action, premeditated or not, that prevents, controls, or mitigates the propagation of a condition or event into an undesired condition or event	So all barriers make interventions (if they work)	
Learning	Knowing what has happened. Being able to learn from experience (the right lessons from the right experience). (Hollnagel)	This is one of the four cornerstones of resilience engineering (Hollnagel et al 2011)[7]. See also *Anticipation, Monitoring, Responding*	
Loss of control event	An undesired event or condition that occurs when control is lost	Used in Storybuilder[26]	

[6] Natalie Salter , 2004. Implementation of the Hazards and Effects Management Process (HEMP) At Shell Chemical Facilities. Shell Global Solutions. Unpublished.
http://www.icheme.org/communities/special-interest-groups/safety%20and%20loss%20prevention/resources/~/media/Documents/Subject%20Groups/Safety_Loss_Prevention/WCCE/C29-006.pdf

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

Term	Definition	Annotations	Alternative or close terms
Management deliveries	The organizational processes and structures that control the performance of the safety-barrier tasks	See Section E.2.1 Management delivery systems	Management Issues (ARAMIS[8], SafetyBarrierManager[9])) HSSE-critical Processes (Shell HEMP[6])
Mental models	Internal models of the world that direct attention, integrate information perceived to form an understanding of its meaning and provide a mechanism for generating projection of future system states based on its current state and an understanding of its dynamics. Endsley, M.R. (2000)[10] Theoretical underpinnings of situation awareness	Wilson, J. (2000)[11] Mental models: are internal representations of objects, actions, situations or people, built on experience and observation and are simulations which are run in mind to produce qualitative inferences in order to underpin our understanding of a system and allow us to describe, predict and explain behaviour, and to test 'what ifs' and 'what wills'	Senge, P. (1992) [12]: Mental models are conceptual frameworks consisting of generalizations and assumptions from which we understand the world and take action in it.

[8] ARAMIS Accidental Risk Assessment Methodology for Industries in the context of the Seveso II Directive http://safetybarriermanager.duijm.dk/aramis/ARAMIS_FINAL_USER_GUIDE.pdf

[9] http://www.safetybarriermanager.man.dtu.dk/About-Safety-Barrier-Manager

[10] 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.

[11] Wilson, J., 2000. The place and value of mental models. Proceedings of the. XIVth Triennial Congress of the International Ergonomics Association and 44th Annual Meeting of the Human Factors and Ergonomics Society, San Diego CA

[12] Senge, Peter M., 1990. The Fifth Discipline. UK, Doubleday.

Term	Definition	Annotations	Alternative or close terms
Mindfulness	Within the safety field a concept introduced by Weick (Weick et al 1999)[13], which refers to an enriched awareness of discriminatory detail and specifically referring to the capability of organisations. Highly mindful organizations characteristically exhibit: a) Preoccupation with failure, b) Reluctance to simplify c) Sensitivity to operations, d) Commitment to Resilience, and e) Deference to Expertise. These are characteristics considered to be exhibited by High Reliability Organisations (HROs)	The outcome of mindfulness is the capacity to discover and manage unexpected events	
Monitoring	Knowing what to look for. Being able to monitor that which changes in the short term (Hollnagel)	This is one of the four cornerstones of resilience engineering (Hollnagel et al 2011)14. See also *Anticipation, Learning, Responding.* Monitoring can also be described as the activity of systematically collecting information from a process (or situation) in order to create and maintain a mental model of the state of the process or situation. This is a skill, and a good mental model depends both on knowing where to look as well as understanding (the correctness of the mental model)	

[13] 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.

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

Term	Definition	Annotations	Alternative or close terms
Near miss	A *deviation* (definition in this list) that is disarmed by an *intervention* (definition in this list) before it developed into a critical event (definition in this list)		Incident
Performance specification	Formal description of the requirements of safety barriers and safety-barrier elements, that are linked to the ability to perform the barrier function.	The requirements are linked to the safety-barrier tasks, i.e. it should be possible, by means of a safety-barrier task (such as inspection) to verify whether the barrier fulfils its performance specifications	Performance standard
Resilience	The 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)[15]	The capacity of a system, enterprise, or a person to maintain its core purpose and integrity in the face of dramatically changed circumstances (Zolli)[16]	Resilience is often compared with - but not considered synonymous with - *Robustness*

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

[16] Zolli, A.& Healy, A.M., 2012. Resilience. Headline Publishing Group, London.

Term	Definition	Annotations	Alternative or close terms
Resilience engineering	The ways in which the four capabilities of *Anticipation, Learning, Monitoring and Responding* can be established and managed in an organisation. Resilience engineering strives to identify and correctly value behaviours and resources that contribute to a system's ability to respond to the unexpected.	Hollnagel et al 2011; Nemeth et al 2008.[17] "The focus of Resilience Engineering is on the whole set of outcomes, i.e., things that go right as well as things that go wrong – with the possible exceptions of the areas of serendipity and good luck, where we are mostly in the hands of fate" Eurocontrol (2009)[18]	
Responding	Knowing what to do. Being able to respond to regular and irregular variability, disturbances and opportunities by adjusting or activating ready-made responses. (Hollnagel)	This is one of the four cornerstones of resilience engineering (Hollnagel et al 2011)[16]. See also *Anticipation, Monitoring, Learning* Knowing what to do also depends on the accuracy of the *mental model* of the process o situation.	

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

Nemeth C, Wears R, Woods D, Hollnagel E, Cook R., 2008. Minding the Gaps: Creating Resilience in Health Care. In: Henriksen K, Battles JB, Keyes MA, Grady ML (Eds) Advances in Patient Safety: New Directions and Alternative Approaches (Vol. 3: Performance and Tools). Rockville (MD): Agency for Healthcare Research and Quality (US); 2008 Aug.

[18] 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

Term	Definition	Annotations	Alternative or close terms
Risk	Effect of uncertainties on an organization's objectives. Risk is often expressed in terms of a combination of the consequences of an event and the associated likelihood of occurrence (ISO 31000)[19] The likelihood of a specific effect occurring within a specified period or in specified circumstances ("Seveso III" Directive 2012/18/EU)[20] Risk expresses a combination of: • probability of consequence/effect on the considered object(s); • severity; • extent of the consequence/effect under given specified circumstances. (Christensen et al, J Haz Mat 2003)[21]	The definition in ISO 31000 is broad and "modern"; it covers also economic/financial risk and thus "upside risk" with positive outcomes. Christensen et al, 2003[20] point out that "risk" can be used "unspecified", in that case it includes aspects of probability, uncertainty, and the severity and possible extent of the consequences (note that uncertainty both relates to the probability of occurence and uncertainty in consequence); but that it also often is used to express the probability of a specified adverse event, in which case it is almost synonym with "likelihood": cf. the difference between "risk of collision" (considers both uncertainty in occurrence and uncertainty in consequence) versus "risk of fatality in a collision"="likelihood of fatality in collision"	A situation or event where something of human value (including humans themselves) is at stake and where the outcome is uncertain (Rosa 1998, 2003 as referenced by Aven 2013; for a discussion on different perspectives on risk see Aven 2013[22]
Robust, Robustness	The ability to withstand threat		resilience is often compared with - but not considered synonymous with - robustness

[19] ISO 31000:2009, Risk management – Principles and guidelines. International Organization for Standardization

[20] Directive 2012/18/EU of The European Parliament and of The Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC

[21] Christensen F.M., Andersen O., Duijm N.J., Harremoës, P. (2003) Risk terminology - a platform for common understanding and better communication. J. of Haz. Mat., A103, 181-203

[22] Aven, T., 2013. Practical implications of the new risk perspectives. Reliability Engineering and System Safety 115 (2013) 136–145

Term	Definition	Annotations	Alternative or close terms
Safety	Freedom from unacceptable risk. Freedom from being hurt, injured or receiving loss. Absence of risk. Condition where all hazards are under control .	The definition of safety is subject of a large debate: Many definitions put safety as the antonym of risk. However, "risk" is an assessment of the hypothetical things that can go wrong, therefore considered theoretical and not relevant to shape behaviour. People's perception of "safety" tend to be experience-based instead: no accidents registered=safe. However, no accidents registered may be sheer luck.	
Safety barrier	A safety barrier is a system that implements a barrier function, each element consisting of technical systems or human actions Duijm 2009[23] A barrier system is a system that has been designed and implemented to perform one or more barrier functions. Sklet, 2006[24] A protective measure put in place to prevent threats from releasing a hazard.[25]	A barrier as used in the accident modelling in Storybuilder[26] is a physical entity (object, state, or condition) that acts as an obstacle in an accident path. The barrier is supported by *barrier tasks* which are resourced through *management delivery systems*. See Section E.2 Storybuilder model components	Independent Layer of Protection (LOPA)[27]

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

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

[25] Zuijderduijn, C. 1999. Risk management by Shell refinery/chemicals at Pernis, the Netherlands. Seveso 2000 European Conference, Athens Nov 10-12 (Ed. G Papadakis) Online: www.microkat.gr/microrisk2001/B4-ZUIJDERDUIJN-SHELL-z.doc

[26] **http://www.rivm.nl/en/Topics/S/Storybuilder**

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

RIVM, 2008. The Quantification of Occupational Risk. The Development of a Risk Assessment Model and Software. Report 620801001. National Institute for Public Health and Environment, P.O. Box 1, 3720 BA Bilthoven, the Netherlands. Online: **http://www.rivm.nl/bibliotheek/rapporten/620801001.pdf**

Term	Definition	Annotations	Alternative or close terms
Safety-barrier task	A safety barrier task is a planned activity to ensure that a safety barrier is and remains capable to perform its barrier function and fulfil its performance specifications.	Safety-barrier tasks are specific for a single safety barrier or a group of similar safety barriers. Safety-barrier tasks can be categorized in: - Providing (the barrier); - Using; - Maintaining (inclusive of inspection) and; - Monitoring or supervision See also Section E.2.2 Barrier tasks	Safety-critical activity; Critical activity; Measure (SafetyBarrierManager[9])
Safety-Critical Element (SCE)	"Safety-critical elements" means such parts of an installation and such of its plant (including computer programmes), or any part thereof— (a) the failure of which could cause or contribute substantially to; or (b) a purpose of which is to prevent, or limit the effect of, a major accident (UK Safety case Regulation 2005) [28]	The term "SCE" is primarly used in offshore operations The SCE's of type (b) are safety barriers. The function of SCE's of type (a) are primarily related to fulfilling the mission's purpose. "Containment" (pipes and vessels) and load bearing structures (jacket) are type (a) SCE's	Safety-critical systems (sometimes a difference is made between elements and systems, but the legal definition addresses systems rather than only elements)
Safety-Management	The set of management activities that ensures that hazards are effectively identified, understood and the associated risks minimised to a level that is reasonably achievable		

[27] Gowland, R. (2006). The accidental risk assessment methodology for industries (ARAMIS) / layer of protection analysis (LOPA) methodology: A step forward towards convergent practices in risk assessment? Journal of Hazardous Materials, 130:307–310

[28] The Offshore Installations (Safety Case) Regulations 2005, UK S.I. 2005/3117, 2005

Term	Definition	Annotations	Alternative or close terms
Safety-Management System (SMS)	A documented set of scheduled tasks, procedures, and responsibilities that ensures effective safety management (and its continuous improvement). ISO standards: That part of the overall management system that includes organizational structure, planning activities, responsibilities, practices, procedures, processes and resources for developing, implementing, achieving, reviewing and maintaining the safety policy	Hale et al 1997[29] describe the SMS as a number of linked processes with a number of problem solving cycles with feedback and learning loops..	
Satisficing	In decision-making, instead of seeking the optimum solution, the seeking of a satisfactory solution. Satisficing is a decision-making strategy or cognitive heuristic that entails searching through the available alternatives until an acceptability threshold is met.	Concept developed by Simon[30] http://en.wikipedia.org/wiki/Satisficing	
Sensemaking	Making sense of the world so we can act in it and knowing enough to make contextually appropriate decisions. The process of creating situation awareness and understanding in situations of high complexity or uncertainty.	Dave Snowden: "How do we make sense of the world so we can act in it" which carries with it the concept of sufficiency (knowing enough to make a contextually appropriate decision). Gary Klein: Sensemaking is the ability or attempt to make sense of an ambiguous situation. More exactly, sensemaking is the process of creating situational awareness and understanding in situations of high complexity or uncertainty in order to make decisions. It is "a motivated, continuous effort to understand	

[29] Hale, A.R., Heming, B., Carthey, J. Kirwan, B.1997 Modelling of safety management systems. Safety Science , 26 (1/2) pp. 121-140

[30] Simon, H.A. 1957. Administrative Behavior, 2nd edn., Free Press, New York, 1957,

Term	Definition	Annotations	Alternative or close terms
		connections (which can be among people, places, and events) in order to anticipate their trajectories and act effectively http://cognitive-edge.com/blog/entry/3840/what-is-sense-making/	
Situation awareness	Knowing what is going on around you. The perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future (Endsley, 2000)[31] "what you need to know not to be surprised" (Jeannot, Kelly, & Thompson, 2003)		
Success	The achievement of predetermined goals and expectations with acceptable outcomes	The opposite of failure. Avoiding accidents will normally be a neccessary condition to achieve success, so the "goal" will include explicit or implicit expectations about avoiding accidents. On the other hand Hollnagel et al (2013) [32] consider success to be intended and acceptable outcomes that stem from doing things right (Safety II) as opposed to avoiding failure (Safety I)	
System	An *intentional* system is a structured set of interacting and interconnected elements , where the interaction of the elements delivers a function (*intention*) that cannot be delivered by the	System theory allows (promotes) the analysis of systems in an hierarchical way. So systems can be decomposed into subsystems, etc., until one ends at irreducible "elements" or components. The	

[31] 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.

[32] 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

Term	Definition	Annotations	Alternative or close terms
	elements alone	word "component" fits better to identify macroscopically irreducible items, as we normally are not interested in decomposition to atomic (elemental) level.	
Uncertainty	Uncertainty means that there are various outcomes to any particular decision. 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 (aleatory uncertainties), and those that come from basic lack of knowledge about fundamental phenomena (epistemic uncertainties also known in the literature as ambiguity) .	A situation of inadequate information which can be of three sorts: technical, methodological and epistemological corresponding to inexactness, unreliability and border with ignorance (Funtowicz and Ravetz 1990)[33]. Any departure from the unachievable ideal of complete determinism Walker et al (2003)[34]. a) Deficit view: deficit of available knowledge b) Evidence evaluation view: problematic lack of equivocalness c) post normal view: uncertainty is intrinsic to complex systems and thus a permanent phenomenon stemming from problem framing, choice of system boundaries, indeterminacy, ignorance, assumptions, underdetermination and even institutional dimensions (Petersen et al 2010)[35]	
Unsafe condition	1) A condition that, if not controlled, or in combination with another condition or event, can	In summary one could say that an unsafe condition is a degradation of a *safety-critical*	Precursor "hole in the cheese" (Swiss

[33] Funtowicz S, and Ravetz JR 1990: Uncertainty and Quality in Science for Policy, Kluwer, Dordrecht.

[34] 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

[35] 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

Term	Definition	Annotations	Alternative or close terms
	lead to a *deviation* (definition in this list) but also: 2) A degraded condition of a *safety barrier* (definition in this list) that may cause the safety barrier to fail on demand.	*element* (definition in this list). In Storybuilder the unsafe conditions are PIEs (Probabiity Influencing Entities)[36]	cheese model of system of defences)[37]
Weak signals	Ambiguous information that does not provide a clear indication of a threat The information could be used to anticipate an event but the signals remain difficult to understand and interpret because of their ambiguous, uncertain and fragmentary characteristics. Can also be considered with respect to Signal Detection Theory as difficult to distinguish from background noise. Signals with a very low frequency of occurrence. See Guillaume (2011)[38]	1) Unsafe conditions may leave observable facts in the organization - these signals may or may not be noted and interpreted with respect to safety, ergo in this definition weak signals do not depend on whether or not they are observed (so weak signals may be overlooked, something normally found out in hindsight) 2) some observations may be interpreted to be indicators of unsafe conditions while they are not so; information is acted upon that does not really indicate unsafe conditions (false alarm). When real signals are hard to distinguish from noise false alarms will happen when the strategy is biased towards avoiding misses.	

[36] RIVM, 2008. The Quantification of Occupational Risk. The Development of a Risk Assessment Model and Software. Report 620801001. National Institute for Public Health and Environment, P.O. Box 1, 3720 BA Bilthoven, the Netherlands. Online: http://www.rivm.nl/bibliotheek/rapporten/620801001.pdf

[37] Reason, J. 1990. Human Error. Fig. 7.8. Cambridge University Press

[38] Guillaume, E. 2011. Identifying and Responding to Weak Signals to Improve Learning from Experiences in High-Risk Industry. Proefschrift TU Delft. ISBN: 978-90-8891-264-1 Online: https://www.foncsi.org/fr/recherche/axes/facteurs-reussite-REX/identifying-and-responding-to-weak-signals-to-improve-learning-from-experiences-in-high-risk-industry

E.2 Storybuilder model components

E.2.1 Management delivery systems

Delivery system	Description
Plans & 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, such as: checklist, task list, action steps, plan, instruction manuals, fault-finding heuristic, rules, permits, programs and risk assessments. This delivery system includes planning of activities in time: how frequently tasks should be done, when and by whom.
Availability	Availability delivery system allocates the necessary time and numbers of competent and suitable (including anthropometrics and biomechanics) people to the barrier tasks to be carried out. It emphasises time-criticality, i.e. competent people available in the required time frame.
Competence	Competence delivery system delivers the knowledge, skills and abilities of the people selected for the execution of the barrier tasks. It also covers the selection and training function of a company to deliver sufficient competence for overall manpower planning. This delivery system also refers to 'right person for the job', i.e. with sufficient barrier task knowledge and skills.
Communication/Collaboration	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. Internal communications are those which occur implicitly or explicitly within any primary business activity in order to ensure that the tasks are coordinated and carried out according to relevant criteria. This delivery also refers to task instructions and communication channels and means (such as meetings, logs, phones, radio).
Motivation/Awareness	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. This delivery system includes alertness, care and attention, concern for safety of self and others, concern for risk control and willingness to learn to improve it.
Conflict resolution	Conflict resolution delivery system resolves conflicts between safety and other goals within the performance of tasks. It deals with the mechanisms (such as supervision, monitoring, procedures, learning, group discussion) by which potential and actual conflicts between safety and other criteria in the allocation and use of personnel, hardware and other resources, are recognised, avoided or resolved.

Delivery system	Description
Ergonomics	Ergonomics and man-machine system deals with the fit between the man and the task. The ergonomics delivery system optimises system performance through equipment, tools and software appropriate to the person and task, robust/appropriate/good interface and labelling, good operability and maintainability, good task design. Ergonomics and man-machine system also covers design and layout of control rooms and manually operated equipment, design of inspection and test facilities, maintenance-friendliness of equipment, design of manning and shift systems, ergonomics of tools.
Equipment	Equipment refers to the hardware needed for provision, maintenance and monitoring of barriers (tools, spares, parts). This delivery system covers both the correctness of the equipment for their use (compatibility, suitability, quality), and the availability of equipment where and when needed to carry out the activities. It includes: spares and parts, including those needed for maintenance, and adequate and correct stocks.

E.2.2 Barrier tasks

Barrier task	Description
Provide	The barrier is provided and available when required. The barrier is in place, has been well designed, and is provided and/or sufficiently/easily available when required. For example: the correct tools are provided to carry out the operations safely.
Use/operate	The appropriate use or operation of the provided barrier. E.g. the correct tools are available and used.
Maintain	The barrier is kept available according to its designed function and in an adequate state. It includes inspect & test (when this is part of the maintenance regime), repair, clean etc.. This covers not only the maintenance aspect but also the management of change aspect of a barrier (if a barrier is modified) ensuring that it maintains its barrier function. For example tools are maintained so that they can be properly used according to design.
Monitor	The barrier condition is checked/measured/observed/inspected. This task relates directly to the state of the barrier, or to the supervision of the use of the barrier.

E.2.3 Safety Barriers of the Major Hazard Storybuilder model

There are 36 barriers. Due to some barriers being removed from the original model the numbers 19, 21, 27, 30, 33, 37 are not present

Barrier nr.	Barrier name	Barrier description
1	Equipment selection	E.g. the intended containment is selected
2	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)
3	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.
4	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.
5	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
6	Equipment connection	
7	Installation of equipment	installation/ assembly
8	Control of movement/ position of containment	E.g. securing the containment while it is being transported or stored
9	Process temperature control	Barrier controlling the temperature of the process (heating/ cooling) to stay within the safe operating window
10	Control of reaction	Barriers limiting the power of the agent

Barrier nr.	Barrier name	Barrier description
11	Pressure control	Barrier keeping the pressure of the process to be within the safe operating window
12	Flow control	Barriers preventing no flow/ too much/ too little/ reverse flow
13	Separation of incompatible substances	Prevention of undesired reactions between incompatible substance
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.
15	Common mode control	Barrier to prevent common mode failure through loss of a utility (e.g. steam, power, compressed air)
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
17	Storage/ transportation conditions	
18	Separation with 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
20	Deviation recovery	To restore the process within normal operating conditions
22	Containment bypass	Containment intact but bypassed" (e.g. opened, lose or untight connections, etc.)"
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
24	Explosion/ fire prevention (internal)	Flammable/explosive atmospheres must be protected (keeping separate) from ignition sources.
25	Secondary containment	Additional physical barrier or secondary containment to protect the system against LoC
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

Barrier nr.	Barrier name	Barrier description
		for strength of the containment)
Centre Event	Loss of containment	
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
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'.
31	Dispersion/ evaporation reduction	In order to limit the dispersion of the released material this barrier offers e.g. the 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
32	Emergency containment	e.g. a bund
34	Ignition control	
35	Fire/explosion fighting response	Actions to limit the spreading of a fire/explosion
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
38	Personal Protective Equipment (PPE)	Personal Protective Equipment

Barrier nr.	Barrier name	Barrier description
39	Evacuation	
40	Shelter	This is inside the hazardous area (explosion proof building, etc)
41	Distance to hazardous area	
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.