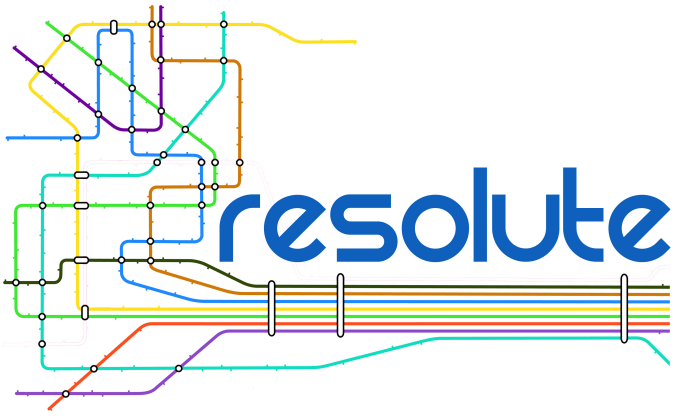

STATE OF THE ART REVIEW AND ASSESSMENT REPORT

Project Title	RESOLUTE
Project number	653460
Deliverable number	D2.1
Version	1-0
State	Final
Confidentially Level	CO
WP contributing to the Deliverable	2
Contractual Date of Delivery	M4 (31/09/2015)
Finally approved by coordinator	M4 (31/06/2015)
Actual Date of Delivery	M4
Authors	Pedro Ferreira, Anabela Simões
Email	pedroferreira@cigest.ensinus.pt
Affiliation	ADI-ISG
Contributors	LEUTERITZ, Jan-Paul (Fraunhofer); GAITANIDOU, Evangelia (CERTH); TSAMI, Maria (CERTH), Anastasios Drosou (CERTH-ITI), Francesco Archetti (CMR)

funded by the Horizon 2020
Framework Programme of the European Union

EXECUTIVE SUMMARY

This document produces the first fundamental basis for the development of RESOLUTE's methodology. It provides a comprehensive overview of concepts, notions and views on resilience, as well as other related aspects of systems theories and risk management.

Resilience is a far reaching idea and has attracted the attention of a wide range of scientific domains. The definition of the concept varies somewhat according to literature domains but bears on a common need to address high complexity, variability and uncertainty that increasingly challenges current risk management practices. Literature often denotes that within many of such domains the term resilience has been used mainly as leverage to re-launch previously existing arguments and views, under a merely renewed terminology. Nevertheless, literature shows that significant advances have been made in risk management approaches, tools and assessment, even if not always grasping the full extent of their implications towards coping with complexity and fast pace changing operations.

The domain of resilience engineering stands out by addressing resilience as an overarching concept, aiming to develop its theoretical foundations beyond its specific application to industrial sectors and risk domains. While empirical evidence clearly supports the foundations proposed by resilience engineering, specific metrics and methodologies remain sparse.

Various proposals for resilience assessment were found, even if originating and focusing on specific domain needs, as opposed to an overall comprehensive assessment. This emphasises the need for research efforts on integrated and comprehensive tools to support the management of system resilience.

A draft conceptual framework is proposed and will be used to support the continued work under work package 2. This work will mainly focus on further analysing the contents of this document, culminating with the development of thorough and applied guidance for RESOLUTE methodology. This will be the subject of Deliverable 2.2 (Synthesis and scoping for RESOLUTE) on month 8 of project development.

PROJECT CONTEXT

Workpackage	WP2: Project Management
Task	T2.1: Review of resilience related literature T2.2: Review of risk analysis and management guidelines at national and EU level T2.3: Review of applied tools and methods
Dependencies	This document will support the development of the ERMG and methodology for pilot testing

Contributors and Reviewers

Contributors	Reviewers
Pedro Ferreira	Paolo Nesi, UNIFI
Anabela Simões	Emanuele Bellini, UNIFI
Jan-Paul Leuteritz	All partners
Evangelia Gaitanidou	
Maria Tsami	
Anastasios Drosou	
Francesco Archetti	

Version History

Version	Date	Authors	Sections Affected
V0.1 to V0.4		Pedro Ferreira, Anabela Simões	All (initial team drafts)
V0.5	03-08-2015	Pedro Ferreira, Anabela Simões, Jan-Paul Leuteritz	All
V0.6	06-08-2015	Pedro Ferreira, Anabela Simões, Jan-Paul Leuteritz, Evangelia Gaitanidou, Maria Tsami	All
V0.7	08-08-2015	Pedro Ferreira, Anabela Simões, Jan-Paul Leuteritz, Evangelia Gaitanidou, Maria Tsami	All
V0.8	17-08-2015	Pedro Ferreira, Anabela Simões, Jan-Paul Leuteritz, Evangelia Gaitanidou, Maria Tsami, Anastasios Drosou, Francesco Archetti	Sections 2, 3 and 4
V0.9	23-08-2015	Pedro Ferreira, Anabela Simões, Jan-Paul Leuteritz, Evangelia Gaitanidou, Maria Tsami, Anastasios Drosou, Francesco Archetti	Section 1, 4.1, 5.2 and Executive Summary
V1.0	31-08-2015	Emanuele Bellini	all

Copyright Statement – Restricted Content

TABLE OF CONTENTS

Executive Summary 2
Project Context 3
Contributors and Reviewers 3
Version History 3
Copyright Statement – Restricted Content 4
1 Introduction 9
2 Complex sociotechnical systems 12
2.1 Systems of systems 12
2.2 Sociotechnical systems 13
2.3 Systems approach 13
2.4 Complex systems 14
2.5 Variability and uncertainty 17
2.5.1 Intractability 18
2.5.2 Understanding uncertainty 19
2.5.3 Managing uncertainty 20
2.5.4 Stability versus flexibility 21
2.5.5 Cascading behaviour 23
2.6 Decision making 24
2.6.1 Distributed decision making 25
2.6.2 Naturalistic Decision Making 26
2.6.3 Risk taking 29
2.7 Risk management in complex systems 31
2.7.1 Background on safety issues 31
2.7.2 The changing nature of accidents 31
2.7.3 Safety culture 32
2.7.4 A system approach to safety 33
2.7.5 Safety I versus Safety II 36
3 Resilience and sustainable adaptability 38
3.1 Definitions 38
3.2 Trade-offs 41
3.3 Functional resonance 43
3.3.1 The Functional Resonance Analysis Method (FRAM) 45
4 Assessing and measuring resilience 47
4.1 Resilience related international programmes and guidelines 49

4.2 Resilience assessment tools 52
4.2.1 The Resilience Analysis Grid (RAG) 53
4.2.2 Matrix for resilience metrics 54
4.2.3 The mean-reverting stochastic model 55
4.2.4 The climate resilience toolkit 56
4.2.5 The Hazus-MH 56
4.2.6 Vulnerability Assessment Scoring Tool (VAST) 56
4.2.7 Hawai's Tsunami Hazard Information Service 57
4.2.8 Integrated Rapid Visual Screening for Tunnels 57
4.2.9 Wave Exposure Model 58
4.2.10 Climate Resilience Evaluation & Awareness Tool (CREAT) 58
4.2.11 Environmental Sensitivity Index 58
4.2.12 Extreme Water Levels 59
4.2.13 Geothermal Prospector 59
4.2.14 HURREVAC 59
4.2.15 Integrated Rapid Visual Screening for Buildings 59
5 Legislation and standards 61
5.1 Concepts and definitions 61
5.1.1 Critical infrastructure and European Critical Infrastructure 61
5.1.2 Sensitive critical infrastructure protection related information 61
5.1.3 Stakeholder 61
5.1.4 Vulnerability 61
5.1.5 Threat 62
5.1.6 Risk 62
5.1.7 Protection 62
5.1.8 Security and security measure 62
5.1.9 Response 62
5.1.10 Interdependency 62
5.2 European Directives 62
5.2.1 The Seveso Directive 63
5.2.2 Directive 2008-114-CE (EPCIP) 63
5.3 International standards 64
5.3.1 ISO 28000: Specification for security management systems for the supply chain 67
5.3.2 ISO 28001: Best practices custody in supply chain security 68
5.3.3 ISO 28002: Development of resilience in the supply chain – Requirements with guidance for use 68

5.3.4 ISO 31000: Risk management - Principles and guidelines 69
5.3.5 BS 65000: Guidance for Organisational Resilience 71
5.3.6 SAFE framework of standards 71
6 Review of training programmes 72
6.1 Training 72
6.2 Training to support resilience 72
6.3 Assessment criteria 72
6.4 Basic principles for training and training objectives 73
6.5 Training methods and tools 73
6.5.1 Classroom training / frontal instruction 73
6.5.2 Simulator training 73
6.5.3 On-the-job training 74
6.5.4 Drills and exercises 74
6.5.5 E-learning and serious gaming 74
6.6 Training at the RESOLUTE pilot sites 74
6.6.1 City of Florence 74
6.6.2 Attiko Metro 75
6.7 Other training programmes 75
6.7.1 EU projects 75
6.7.2 Other sources 75
6.7.3 Serious games 77
7 Going forward for RESOLUTE 78
8 References 79
8.1 Websites 87

List of Tables

Table 1.1: Relation between RESOLUTE planned tasks and the structure of the SotA 10
Table 2.1: Tractable and intractable systems (from Hollnagel, 2009a) 18
Table 2.2: Basic principles of uncertainty management underlying organisation design (from Grote, 2004) 21
Table 2.3: Aspects of stability versus flexibility (from McDonald, 2006) 23
Table 2.4: The four types of decision problems (from Svenson, 1996) 25
Table 2.5: Features of Naturalistic Decision Making (From Klein & Klinger, 1991) 27
Table 2.6: Risk contingencies and outcomes (Fom Vertzberger, 1998) 29
Table 3.1: Definitions of resilience 39
Table 4.1: Characteristics of resilient and non resilient systems (from Wreathall 2006, Hale & Heijer 2006b and Hale *et al* 2006) 47
Table 4.2: 4 scenarios for system behaviour 55
Table 5.1: Standards and ongoing projects under resilience related topics (from www.iso.org on 07-08-2015) 65

List of Figures

Figure 1.1: RESOLUTE draft Conceptual Framework ..... **Error! Bookmark not defined.**
Figure 2.1: The integrative model of Technology, Organisation and People. Adapted from Tschiersch & Schael (2003) 14
Figure 2.2: The interaction between the dynamics, complexity and uncertainty of the environment for the construction of the action (Norros, 2004) 15
Figure 2.3: Framework for uncertainty analysis (from Grote, 2009) 20
Figure 2.4: Sociotechnical system involved in risk management (from Rasmussen, 1997) 35
Figure 3.1: Performance variability and resonance (adapted from Hollnagel, 2008) 44
Figure 3.2: Functional unit of FRAM (adapted from Hollnagel, 2008) 46
Figure 4.1: The London Resilience strategy (London Resilience Forum, 2013) 51
Figure 4.2: Example of a Resilience Analysis Grid - RAG (adapted from Hollnagel, 2011b) 54
Figure 4.3: Components and examples of vulnerability for transportation assets. 57
Figure 5.1: Security management system elements (in ISO 28000) 68
Figure 5.2: Relationships between the risk management principles, framework and process (in ISO 31000) 70

1 INTRODUCTION

The state of the art (SotA) constitutes a key output of work package 2 (WP2) of RESOLUTE. The focus of this WP is the retrieval of evidence, assessment and synthesis of knowledge on resilience, aiming to support RESOLUTE research methodology and produce a suitable conceptual framework. This document constitutes the first deliverable (D2.1) of the WP and integrates the outcome of four different tasks:

- T2.1 addressed the review of resilience related literature and other related domains such as risk management and assessment.
- T2.2 addressed the review of risk analysis and management guidelines, both at EU and member state level.
- T2.3 addressed the review of applied tools and methods on resilience and other related operational and managerial aspects.
- T2.4 addressed the review of training practices and programmes.

As stated in RESOLUTE objectives, while resilience concepts and approaches seem to provide useful solutions to address current needs of urban transport systems, they remain unclear on many aspects. In particular, the broadness of the notion itself challenges many conventional perceptions and practices on risk management. Resilience is conceptually grounded on various overlaps between different engineering and social disciplines, which highlights its multidisciplinary nature. In particular, the growing complexity of relations between humans, humans and technology and increasingly between different types of technology, are at the core of the heightened interest in this domain.

Modern organisations are increasingly shaped by technology (automated processes, computer-based cooperation networks, decision support systems, multimedia applications, etc.) integrating social and organisational elements that are fundamental to understand system behaviours and should be viewed as embedded in the system (Tschiersch and Schael, 2003). In today's society, the more developed and technology-based systems are the more complex and safety-critical they become, thus imposing high performance levels towards safety and efficiency. The more system complexity and safety-criticality increase, the more human operators' skills, competences and abilities become important for system efficiency and safety.

Technology is increasingly interactive and therefore, no system can be regarded as purely technical. Every engineered system, regardless of its technological level and nature, is inherently a human purpose system and foremost relies on human decision making and action. Thus, systems integrate people and their tasks, technology allowing for tasks performance and related communication and cooperation, as well as the organisational structure. They ultimately rely on an adequate cooperation between humans and technology being subject to an intrinsic variability, whose leading factors must be identified and understood. In order to ensure the success of the system, resulting from a good cooperation between humans and technology, the different factors leading to performance variability must be identified and understood. These factors, resulting from the diversity of human characteristics and functioning, as well as their short-term and life span variability, contradict the assumption of the stability of human activity over time that presides to the design and management of numerous sociotechnical systems.

The purpose of this Deliverable is to foremost provide a broad scope insight on resilience theoretical foundations, tools and guidelines. A systems perspective and related notions are initially introduced,

providing the foundations and context on which resilience is considered to become a relevant approach. In particular the implications of high complexity and dynamics over risk management and decision making are explored. An extensive review of resilience definitions, concepts and assessment tools is then provided, followed by an overview of the current European legal framework and existing relevant standards. Finally, relevant training principles and needs are explored.

The structure of the document does not explicitly reflect the four different tasks that are synthesised under this deliverable. While it is important to demonstrate the work developed under each task, the structure used here was considered more coherent towards the need to provide in-depth understanding of resilience and its foundations and towards supporting the objectives to be pursued within RESOLUTE. Table 1.1 provides an overview on how each of the sections in the document relates to each of the four tasks addressed by the deliverable.

Table 1.1: Relation between RESOLUTE planned tasks and the structure of the SotA

RESOLUTE tasks	State of the Art (SotA) structure
Task 2.1: Review of resilience related literature	• Complex sociotechnical systems • Resilience and sustainable adaptability • Assessing and measuring resilience
Task 2.2: Review of risk analysis and management guidelines at national and EU level	• Legislation and standards • Risk management in complex systems • Assessing and measuring resilience
Task 2.3: Review of applied tools and methods	• Risk management in complex systems • Functional resonance • Assessing and measuring resilience
Task 2.4: Training programs review and assessment	• Review of training programmes

A RESOLUTE conceptual framework has been drafted with the aim of steering further work in pursuing project objectives. This conceptual framework is presented in **Error! Reference source not found.** and it is composed of three main parts, representing the system aspects to be addressed by RESOLUTE:

(1) The Resilience theoretical and methodological background that justifies the need for Sustained Adaptability;
(2) The application field within RESOLUTE (the Urban Transport Systems) as complex and safety-critical sociotechnical systems, within which the different modes and related vulnerabilities constitute the targets of RESOLUTE;
(3) The need to address both expected and unexpected (unforeseeable) events, for which four system capacities are considered fundamental (knowing what to do, knowing what to look for, knowing what to expect and knowing what has happened) preparedness and closing the loop from a sustainable adaptability as a basis for a permanent adjustment towards success.

This theoretical framework represents a general guidance for the project development, and will be completed during the project life. It is expected that the next Deliverable 2.2 (Synthesis and scoping for RESOLUTE - M8) will present a significant improvement on the structure and contents of the theoretical framework.

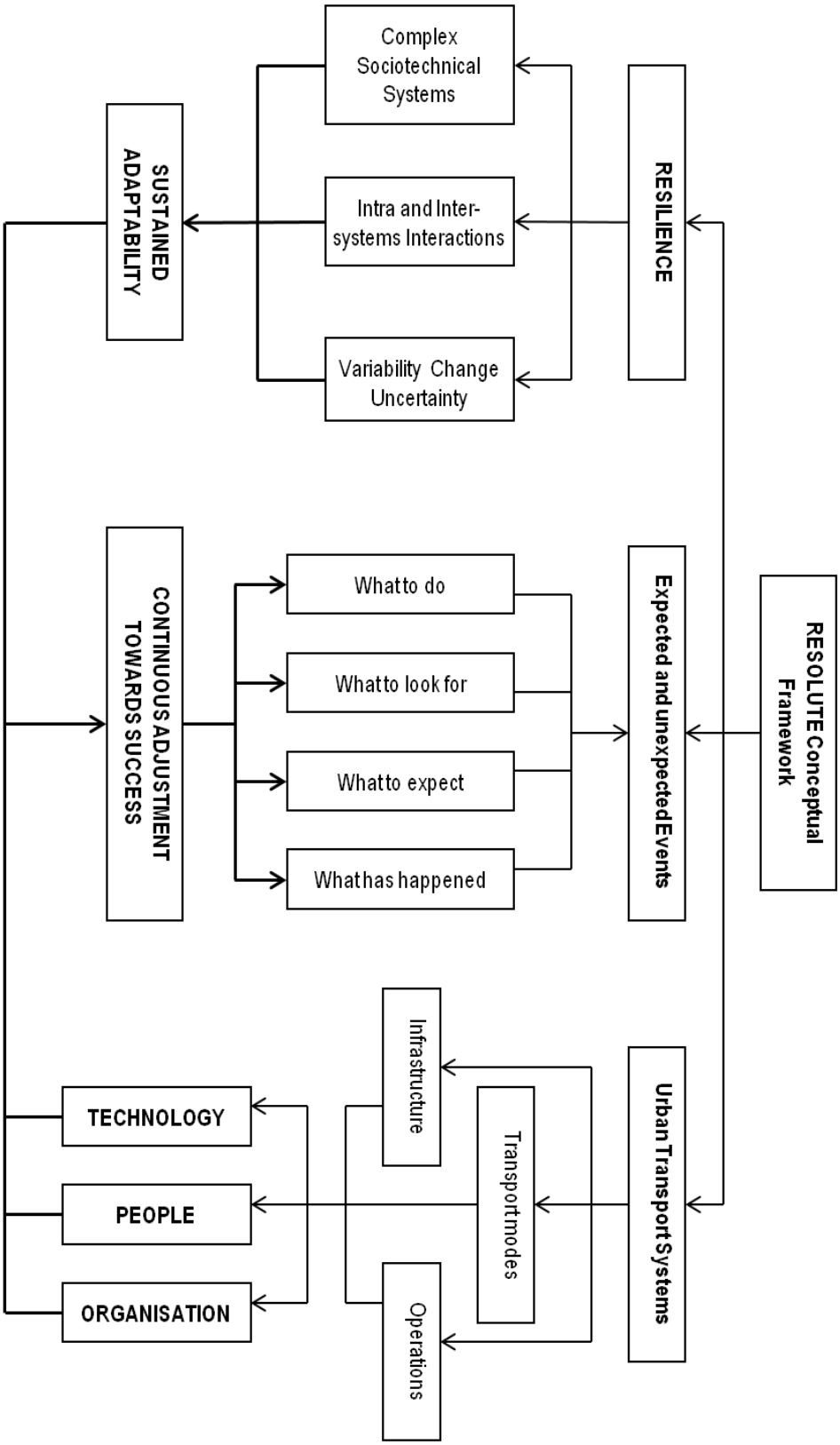

Figure 1.1: RESOLUTE draft Conceptual

2 COMPLEX SOCIOTECHNICAL SYSTEMS

Sociotechnical systems were considered the background for the investigation of growing complexity and its impacts on safety. A complex sociotechnical system is composed of different sub-systems, each one being a system on itself. Several interactions occur within the system environment so that the system is much more than the sum of its parts.

According to Dekker (2011) complex systems present the following characteristics: (1) they are open to influences from the environment where they operate and influence the environment in return; (2) each component of the system is not aware of the system behaviour as a whole neither of the effects of its actions, and its complexity results from the multiple relationships and interactions related to the local actions; (3) as the knowledge of each component is local and limited, the system behaviour cannot be reduced to behaviour of the components; (4) complex systems operate under varied and unstable conditions on the basis of a permanent flow of actions performed by each of their components, which are essential for the system survival within a dynamic environment; (5) interactions within complex systems are non-linear, which means that there is an asymmetry between input and output, that is to say that small events can produce large effects resulting from internal feedback loops generating multiplier effects; finally, (6) the behaviour of a complex system is related to its origin and past, which explains its present behaviour.

In order to allow for a better understanding of sociotechnical complex systems, system theories are discussed below, as well as the characteristics of complexity. This will support the development of a conceptual framework of Resilience Engineering applied to the target field within RESOLUTE: urban public transport systems. This approach highlights human and organisational factors as grounds for understanding and managing safety and security within complex sociotechnical systems. Thus, a review of literature starting from basic concepts is necessary and is described below.

2.1 Systems of systems

Mansfield (2010) defines a system as a “hierarchic or networked group of interdependent components that when regarded as a whole, exhibit a certain behaviour that is not present in any one part, but arises from the interaction of the parts”. In systems, not only the whole is “greater” than the sum of the parts, but also the relations between parts condition the functioning of parts and of the whole system (Jackson, 2010). Jackson (2010) further considers that the nature of the system is defined by the interactions and interdependencies of its parts. Relations between components may be structured by links of physical, social or organisational, or even formal or informal nature, among others. The author also refers that the behaviour exhibited by the system and produced by the existing relations within it, is an emergent property of the system in question. Such properties are the characteristics of the whole and not of its parts (Jackson, 2010). This is also what defines the boundaries of the system. The limits of a given system are the consequence of the relations considered and the behaviours originated. As noted by Hollnagel (2009), this renders the definition of system boundaries dependent on the purpose and scope of its description. Any elements beyond, outside or not involved in the relations and behaviours considered are designated as the environment of the system.

A public transport system operating in an urban environment is an example of a system being composed of different systems as its parts: the different transport modes (road, rail, waterborne, etc.) being each one a system, the related infrastructure (exclusive or shared with other transport modes), the available technology for each one (vehicles, traffic control centres, information and ticketing technologies, etc.), people (operators and users) and the organisational, planning and communication levels of each mode so that the whole system is working as a network of connections allowing for a variety of trip choices. The urban public transport system interacts and/or overlaps with other systems, such as the urban motorised and non-motorised traffic and the logistics of a variety

of urban services. From this perspective, the operational environment of each transport mode is in itself a system, and a given environment may be shared by several “separate” systems.

2.2 Sociotechnical systems

Modern organisations are increasingly shaped by technology (automated processes, computer-based cooperation networks, multimedia applications, etc.) integrating social and organisational elements, which are fundamental to understand the system behaviour and should be viewed as embedded in the system (Tschiersch and Schael, 2003). These systems are not just technical once they integrate people and their tasks, technology allowing for tasks performance and related communication and cooperation, as well as the organisational structure. The notion of sociotechnical system is likely to be one most frequently used in recent studies of organisational contexts. Mansfield (2010) points out that the term was first used in the context of work-related studies and it was aimed at emphasising the interaction between people and technology. This presupposes interactions between people and between people and technology. From this perspective, sociotechnical systems are distinct from purely technical systems, and from natural systems (Vugrin et al, 2010). While technical systems are those created by humans but under normal conditions, operate independently (certain types of software for instance), natural systems includes all those that were not created by humans and where no human intervention exists (natural ecosystems).

Jackson (2010) distinguishes a socioecological system from a human intensive system. Jackson (2010) defines the later as any system where the human element is the dominant one. This would include every organisation, from governmental institutions to companies and communities, as illustrated by the system responsible for the response to the hurricane Katrina (Jackson, 2010). A socioecological system is defined by Jackson (2010) as the result of human intervention in a natural system, such as the building of dams on rivers or any conservation action in forest or other natural habitats. In human-intensive as well as in socioecological systems, there is bound to be some form of interaction between humans and technology, and therefore, both could also be considered sociotechnical systems.

From a human factors perspective, any such systems could be considered “human intensive”, since at any instance, the control of a dam or the management, planning and implementation of conservation measures rely on human decisions and actions. To some extent, different degrees of “intensity” could be considered. As pointed out by Jackson (2010), the key principle of any systems approach is the definition of its boundaries.

2.3 Systems approach

Jackson (2010) considers this a designation for methods dedicated to the design, analysis and management of complex systems. Jackson (2010) synthesises this approach with the following steps:

- The identification of system elements provides grounds for the selection of appropriate methods and disciplines for the study of each element.
- The subdivision of elements into smaller elements enables proper focus on relevant system parts.
- The grouping of elements provides means for better understanding the relations between elements with common goals and of overall system structure.
- The identification of system boundaries supports the definition of the system and its goals, as well as the identification of the elements that most contribute to these overall goals.
- The identification of functions for each system element further develops the understanding of system operations and how system functions are performed.

- The analysis of interactions between system elements complements knowledge of system functions by looking into how elements perform together to achieve system goals.
- Understanding the system environment is crucial for the analysis of constraints on system operations and performance of system elements.

Whenever relevant for system design or analysis, this may include looking at elements independently and their environment within the system, as each system element may have different environments and therefore, also be subjected to different performance constraints.

- The identification of the emergent properties of the system, as previously stated by Mansfield (2010), constitutes a crucial step for understanding system functions and goals, as well as boundaries.
- The development of a synthesis of functions and structures supports interpretation and understanding of system performance.
- Like in any robust scientific approach, verification and validation are fundamental steps to be considered.

Technology-based systems should develop an integrative model of Technology, Organisation and People (Figure 2.1), which means that People are in the centre of the Organisation interacting and/or cooperating with Technology. None of these elements should be targeted separately; instead, they should be linked and interconnected, and viewed as an integrated part of the entire system.

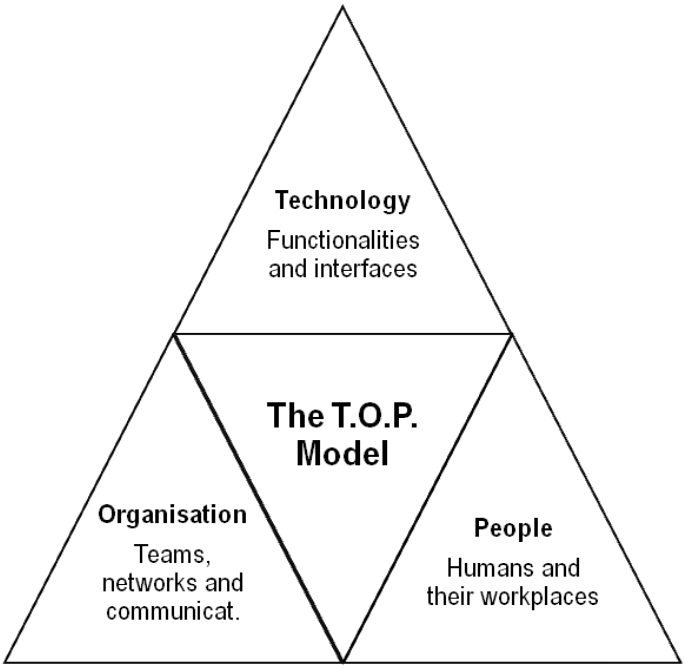

Figure 2.1: The integrative model of Technology, Organisation and People. Adapted from Tschiersch & Schael (2003)

2.4 Complex systems

There is no absolute definition of what complexity means. The only consensus among researchers is that there is no single aspect or feature that can singly justify a state of complexity and that views on factors contributing to complexity vary considerably. However, a characterisation of what is complex is possible. Complexity is generally used to characterize something with many parts where those parts interact with each other in multiple ways. The

study of these complex linkages at various scales is the main goal of complex systems theory. In terms of one person's ability to process information, complexity is seen as a great amount of information to process permanently within a dynamic environment in order to make appropriate decisions in useful time.

In terms of a sociotechnical system, complexity results from interactions and communication among the system parts, both human and technological together with the process dynamics (organisational). In the case of problem-solving, complexity is a function of the interactions between three basic elements (Woods, 1988): (1) the world where the actions are performed, which can be dynamic creating uncertainty and risk; (2) the agent who acts on the world; (3) and the external representation of the world used by the problem-solving agent. In the same document Woods refers that complexity takes its roots in four dimensions of the environment: dynamics, several interacting parts, uncertainty and risk. Norros (2004) defines just three dimensions of the environment: dynamics, complexity and uncertainty, all interacting through action. These dimensions should be seen as attributes of the environment signalling possibilities and constraints with impact on actions towards success. The balance between these three dimensions of the environment is illustrated in the following model (Norros, 2004) highlighting the emergency of skills, knowledge and collaboration needs (Figure 2.2) to enable the construction of the action. This model is mainly directed to the construction of the human action (decision-making) under dynamic and complex environments where the permanent changing conditions introduce uncertainty.

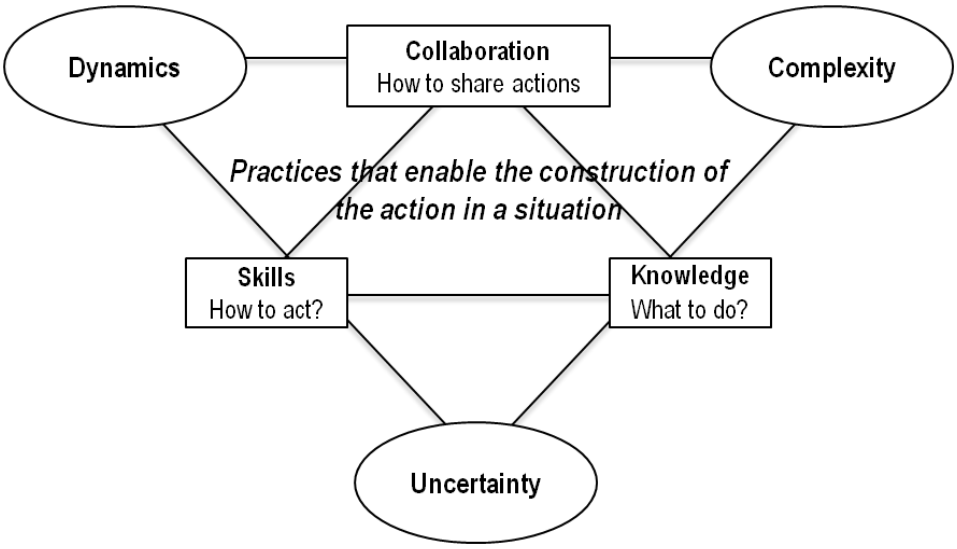

Figure 2.2: The interaction between the dynamics, complexity and uncertainty of the environment for the construction of the action (Norros, 2004)

A fundamental distinction must be made beforehand between complexity and complicatedness: Something is said to be complicated when it possesses large numbers of parts and even perhaps some diversity in the nature and type of such parts but nevertheless, it assumes behaviours that can be fully explained based on linearity principles of cause and effect relations. Within complicated systems, understanding the behaviours of individual parts can lead to the identification of the factors that determine overall system behaviours and therefore, decomposing and describing system elements produces relevant system knowledge. This is the founding principle that still prevails in most risk management approaches, under which probabilistic and deterministic tools have so far been used to respond to risk assessment and control needs.

Complexity on the other hand, emerges from the combination of parts or elements that are, not only relatively numerous but most of all, tend to assume very different natures and they exhibit very distinct patterns of behaviour. This means that the great diversity of system parts and their equally diverse behaviours can potentially produce combinations and interactions that in return, produce emergent system behaviours that cannot be explained or deducted from the knowledge of individual system parts. The variables and the amplitude of

variability of phenomena emerging in complex systems performance cannot be adequately explained through linear reasoning and approaches. A complex system is a system that is more than the sum of its parts and therefore understanding and controlling risk requires looking beyond the behaviour of system parts, into the variability of interactions that are generated amongst them. The challenge then resides partly in the fact that interactions can only be perceived through real system operation (hence being considered as emergent) and cannot be linearly predicted from knowledge of system parts and structure.

Mansfield (2010) defines the distinction between complicated and complex systems, based on the way each of these two types of systems changes and evolves over time. The behaviour of complicated systems follows specific rules and, despite its numerous components, the relations between them remain fairly stable. Mechanical clocks are an example of complicated systems. A change of state in the clock's components will be likely to change the time it displays on the dials, but it will not alter the clock itself and how it works. The behaviour of a complicated system is linear, as it could be described through a representation of the sequence of its relations and how they alter the state of the system in time (Mansfield, 2010). Complex systems on the other hand, are characterised by numerous interactions occurring between many of its parts at each given time. Axelrod & Cohen (1999) define complexity as the outcome of interactions, which lead to current events within the system, critically influencing the probability of future ones. Mansfield (2010) considers that complexity is only perceivable through the behaviour of the system, as opposed to considering its components separately. In this sense, the author considers that complexity is an emergent property. Axelrod & Cohen (1999) add that complexity emerges from the multiple ways in which events in complex systems tend to combine their effects, rather than simply adding, as in a mechanical clock. Consequences of events tend to diffuse unevenly via the multiple interactions occurring in the system. As mentioned by Axelrod & Cohen (1999), Mansfield (2010) and Marais et al (2007), complex systems can change in multiple dimensions. Components in complex systems may alter their state, form or even position within the system's structure, and these changes produce effects across the system through the interactions with other system components. Hence, order in complex systems is emergent, rather than predetermined (Jackson, 2010). Leveson (2004) states that many systems have today reached a level of complexity with a potential for interactions that cannot be fully understood. The author points out the contribution of software for this increasing complexity, as it gave way to "more integrated, multi-loop control in systems with dynamically interacting components" (Leveson, 2004). Bertalanffy (2003) develops a similar distinction when referring to closed and open systems. Closed systems have no communication with their environment and therefore, components tend to settle into a state of equilibrium. Once more, the example of the mechanical clock applies, as no interactions with its environment exist and it operates in more or less accurate constancy. Open systems are subject to information exchanges with their environments. Open systems tend to acquire the traits of complexity, as they develop adapting mechanisms to their environment. Within this context, the main distinction between a complicated and a complex system resides in the fact that while the behaviour of the first remains compatible with principles of linearity and constancy, understanding the latter requires a nonlinear perspective. Nonlinearity is here considered the multiple dimensions that must be perceived concurrently, in order to understand the behaviour of a complex system. In this frame of mind, a complex system is defined as a network of components that interact nonlinearly and give rise to emergent behaviours (and properties), which cannot be perceived from the properties and behaviours of components. Mansfield (2010) proposes the change from caterpillar to butterfly as an example of a complex system. This is clearly a system where a change in one component can initiate interactions difficult to predict, which, as the author states, can either die away or grow to modify the system and its behaviour. Cook (2001) refers to a system of systems to discuss the high scale and complexity that today can be found in a great variety of contexts. When studying complex systems, often its components should themselves be viewed as sub-systems of a larger system, which leads to a more adequate perspective of complexity and its sources of variability and unpredictability (Cook, 2001). Jackson (2010) notes that this perspective should be applied when discussing systems that, despite their ability to operate independently, are often faced with the need to coordinate their efforts towards a common goal, and therefore,

interact as a broader system. Examples of this can be found across all industry domains. Among others, research within transport sectors has widely explored this, even if some lack of suitable tools remains.

2.5 Variability and uncertainty

The safety of complex sociotechnical systems requires the control of numerous factors, both at operational and managerial levels. The tight couplings and strong interdependencies that characterise most complex systems render the behaviour of such factors increasingly dynamic and variable. In relation to the dynamics of operational factors, Fujita (2006a) states that no system can avoid changes. They occur continuously throughout the lifetime of the system and are driven both by internal (e.g. through people's actions) and external (e.g. economic pressures) factors. Mansfield (2010) considers the influences that components exert on each other through their relations as the source of change in the system. The interactions amongst components generate pressures for change in the state of the system and of components themselves. Due to their dynamics, complex systems are rarely in equilibrium, changing over time and leading to unexpected behaviours. Jackson (2010) considers that complexity in systems is also related to the need to constantly adapt to disruptions emanating from system pressures. Hence, complex systems are normally characterised by variability in time. Pressures amongst system components are themselves the result of pressures from the system's environment. Svedung & Rasmussen (1998) refer to pressures generated by changes in public opinion and awareness, political climate, market conditions, and the increasing pace of technological changes, stating that, in order to survive, systems must adapt to such changes in their environment. These changes initiate adaptation processes within systems and, in return, the changes in the system will eventually produce changes in the environment. The shifting pressures between the system and its environment are the source of high dynamics and unpredictability. Axelrod & Cohen (1999) consider that because of the forces (pressures) within the system, which shape future events, cannot be added in a simple and linear manner, prediction in complex systems becomes very difficult. As stated above, complex systems can develop changes across many different dimensions and therefore, they exhibit a non-linear behaviour. Leveson (2004) adds that some systems have developed such degrees of interactive complexity that even experts may have incomplete information about their behaviour. This generates uncertainty in operations of complex systems.

From the human operators' side, variability results from the diversity of human characteristics and functioning, as well as their short-term and life span variability, contradicting the assumption of the stability of human activity over time that presides to the design and management of numerous sociotechnical systems. Indeed, there is no average human being; human variability, resulting from diversity or the instability of human activity, is actually an uncomfortable reality that systems designers and managers have to face and to act accordingly. As people are so different from each other, and are also subject to internal variability, this can lead to an important dispersion of performance even if the circumstances are totally identical. Sociotechnical systems within every context (industry, transport, health or other) are operated by human beings, which results in an increased variability and uncertainty imposing an ability to cope with towards stability. It is assumed that every system involving people is subject to human-related disturbances resulting from several interacting contextual factors. The nature and the dimension of the disturbance depend on the task that is being performed, the individual's skills and their functional abilities and state, as well as the local conditions for the system performance and some related organisational factors (Reason & Hobbs, 2003). However, among highly trained and skilled groups of professionals, it seems that the variability of human performance, instead of being viewed as a constraint, should be viewed as the potential ability to recognize, adapt to and absorb variations, changes, disturbances, disruptions, and surprises, especially disruptions falling outside the set of disturbances the system is designed to handle (Hollnagel et al, 2006). Actually, both the system safety and efficiency rely on people being able to cope with local variability and uncertainty factors whilst maintaining sufficient awareness of the impacts of their actions and decisions across the system. Managing variability and uncertainty within a complex sociotechnical system is a matter of enhancing competencies and skills so that people may become more adaptable to high pace changing performance

conditions. Some pitfalls on this aim of high competencies and team's homogeneity occur as a result of fatigue, sleep deprivation, high workload or temporary health disorder.

According to Jackson (2010), the operation of complex sociotechnical systems tends to be highly unpredictable, as decisions and actions, once initiated, can rapidly produce chain reactions and therefore, become irreversible and difficult to trace back. This aspect, together with human variability, introduces uncertainty into the system, which requires from human operators the ability to cope with. Furthermore, one of the main consequences of the system complexity is the underspecification of operational conditions at all organisational levels. Thus, the system variability together with some lack or ambiguity of information, particularly in dynamic environments, lead to uncertainty. This requires an increased ability of people to cope with variability and uncertainty at a local level, which constitutes a fundamental resource to deal with such operational underspecification. However, this ability is in itself, a source of increased overall system uncertainty and variability. Any decisions made at a local level and the performed actions to manage the high pace changing environment generate an increased system dynamics, which will eventually increase the local uncertainty and variability. This highlights a tendency of complex systems to develop self-reinforced cycles towards unforeseen chain reactions, which rather than singly focusing on minimizing uncertainty and variability, requires the strengthening of people's abilities to anticipate the need to adjust to and manage high pace changing performance conditions.

The shifting pressures between the system and its environment are the source of high dynamics and unpredictability. Jackson (2010) points out that in complex (adaptive) systems, history is irreversible and the future is often unpredictable. Once actions are taken within the system, chain reactions can be produced that cannot be undone. As stated above, complex systems can develop changes across many different dimensions and therefore, they exhibit a non-linear behaviour. Leveson (2004) adds that some systems have developed such degrees of interactive complexity that even experts may have incomplete information about its behaviours. This generates uncertainty in operations of complex systems being one of the aims of resilience engineering often discussed by Hollnagel et al (2006) the ability to cope with variability of system operations and uncertainty about possible outcomes.

2.5.1 Intractability

On the basis of complexity and its resulting patterns of change, Hollnagel (2009) discusses tractable and intractable systems. The low complexity that characterises tractability provides the opportunity for a sufficiently thorough description of the system and its operation. Not only are there fewer components and details to be described, but also the relatively low dynamics of the system allows for the analysis process to be concluded and actions to be taken without compromising the validity of its outcome in view of the system's state and condition. On the contrary, intractable systems incorporate the traits of complexity and therefore, operations tend to be underspecified (Hollnagel, 2009a). The level of complexity that most currently existing sociotechnical systems have attained, places them in the scope of intractability. One of the foremost repercussions of intractability is the underspecified nature of system operations. This means that, to a certain extent, system operations are unknown and therefore, potentially uncontrolled. Therefore, intractability of complex systems presents a major challenge for safety management. Within underspecified conditions, decisions must be made based on incomplete knowledge of operating principles and solutions must be reached within a timeframe compatible with the fast pace change of the system (Hollnagel, 2009a).

Table 2.1 summarises the main characteristics of tractable and intractable systems.

Table 2.1: Tractable and intractable systems (from Hollnagel, 2009a)

	Tractable systems	Intractable systems
Number of details	Descriptions are simple with few	Descriptions are elaborate with many

	details	details
Comprehensibility	Principles of functioning are known	Principles of functioning are partly unknown
Stability	System does not change while being described	System changes before description is completed
Relation to other systems	Independence	Interdependence
Controllability	Easy to control	Difficult to control

The level of complexity which most currently existing sociotechnical systems have attained, places them in the scope of intractability, as described in

Table 2.1. One of the foremost repercussions of intractability is the underspecified nature of system operations. This means that, to a certain extent, system operations are unknown and therefore, potentially uncontrolled.

The lack of control that may result from intractability is mainly associated to the fact that the majority of safety models currently into practice do not account for the increasing dynamics and variability of complex sociotechnical systems. For the last decades, safety management practices have been grounded on a centralised and rigid top-to-bottom control of operations, which presupposes a thorough knowledge of system performance at every operational stage and level. In particular, throughout this period, significant efforts have been devoted to human error. In many cases, automation has been used as a path towards both reduced human intervention and increased dissemination of the top-to-bottom rigid and centralised control. In such many cases, the outcome has been the placement of human decision making at higher and more complex levels of systems control. Within this context, new safety management paradigms become necessary, in such a way that systems may cope with the high dynamics and uncertainty that result from the underspecified nature of their operations. Safety management practices must be capable of integrating certain degrees of flexibility within operational conditions, in order to cope with high dynamics and uncertainty.

2.5.2 Understanding uncertainty

Understanding uncertainty requires identifying its content, sources, causes and potential consequences. According to Grote (2009), uncertainty may concern the probability of an event (state uncertainty), a lack of information on the outcomes of an event and the underlying cause-effect relationships (effect uncertainty), or a lack of information about response options and their consequences (response uncertainty). Uncertainty can arise from incomplete information and inadequate understanding or undifferentiated alternatives of the available information (Lipshitz & Strauss, 1997, cited by Grote, 2009). Incomplete information can be objectively identified and so, the appropriate correction can be performed; however, both inadequate understanding and undifferentiated alternatives are not clear and easily identifiable sources of uncertainty involving several interactions between the characteristics of the decision, the related environment and the decision-maker. Due to these differences, just the incomplete information is usually defined as a source of uncertainty, being the other two aspects considered as a separate category: ambiguity. The undifferentiated alternatives are linked to the decision-makers goals, values, needs and attitudes together with the related expected benefits to the organisation. Concerning the inadequate understanding, it can result from too much or insufficient information, as well as potentially conflicting meanings in the information leading to confusion.

Causes of uncertainty can be searched at an individual level, trying to explain individual differences in dealing with ambiguous information. However, it is essential to go one step back and search the causes of uncertainty at the situational level, which involves both the external environment and internal processes of the organisation.

Taking as example a public transport operator in urban environment, urban traffic represents a previewed and manageable environmental cause of uncertainty in what concerns the delivery of the scheduled service. In the same context, a delay at the maintenance service resulting from dysfunction or lack of spare components could create uncertainty due to the risk of compromising the available spare vehicles and, consequently, the scheduled service delivery. These causes of uncertainty are related to the concept of task interdependence (Grote, 2009), which refers to the way individual tasks are linked through technical and organisational design creating uncertainties and allowing for particular ways of handling them. Grote (2009) distinguishes three types of interdependences, each one involving particular causes of uncertainty:

1. Pooled interdependence – the system performance is an additive function of individual performance, such as a service organisation where each individual performs the whole service for a particular group of customers; uncertainty is mainly created by inappropriate coordination of individual tasks or by a machine breakdown leading to problems in fulfilling the individual tasks.
2. Sequential interdependence – unidirectional workflow organisation where individual performance depends on the fulfilment of prior tasks, such as an assembly line; uncertainties appear along with the process and when not adequately handled they create problems throughout the process.
3. Reciprocal interdependence – more complex systems where information and outputs of work activity must be continuously exchanged between team members; there are multiple parallel causes of uncertainties, such as misunderstandings of task requirements, changes in the task performance, or inadequate interfaces design.

2.5.3 Managing uncertainty

Uncertainties are usually avoided as they may compromise success; however, they can also be viewed as sources of innovation where the ability to flexibly handle uncertainties becomes a competitive advantage. Managing uncertainties within any complex sociotechnical system requires the identification of the different kinds of uncertainties that are currently faced, in terms of their sources, causes, contents and potential consequences, to support the decisions about the best way to handle the identified uncertainties. This process requires an uncertainty analysis for which Grote (2009) proposes a framework adopting a rationalistic and objective perspective on managing uncertainty, taking into consideration the impact of individual and collective enactment and sensemaking, which is particularly important in situations with high levels of uncertainty (Figure 2.3).

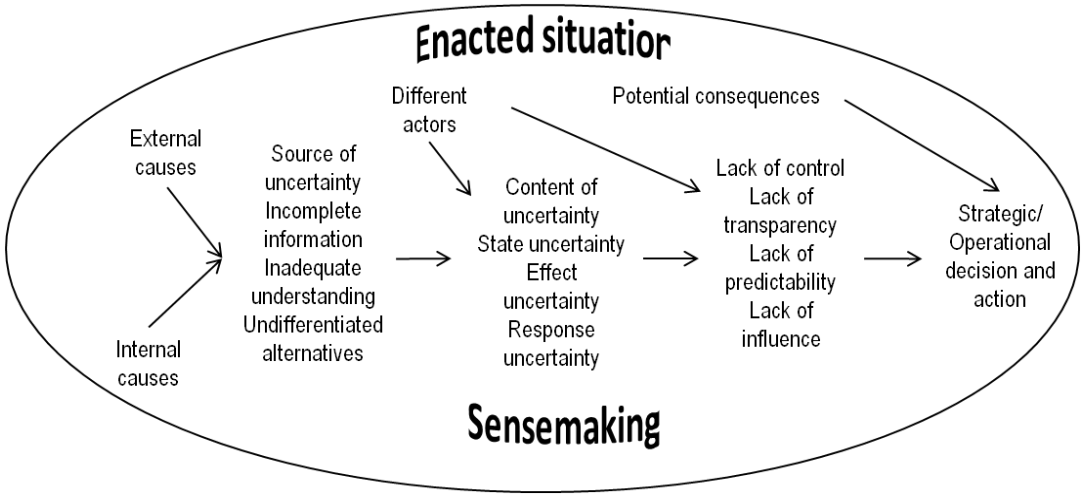

Figure 2.3: Framework for uncertainty analysis (from Grote, 2009)

Being uncertainties identified and analysed, a choice has to be made between the two approaches to managing uncertainty: minimising uncertainty or coping with uncertainty. An approach focused on minimising uncertainty clearly corresponds to most of the existing safety practices. Although such traits remain necessary to achieve

high standards of safety performance, in view of system complexity and its inherent underspecification and variability, the ability to cope with uncertainty must be integrated at all operational levels. Therefore, instead of fighting uncertainties in an attempt to minimise them or their effects in the system, every member of a system should be enabled to cope with uncertainties locally having a feedback control. Local actors should have as many degrees of freedom as possible with lateral and task-induced coordination. Furthermore, disturbances should be regarded as opportunities for the use and expansion of individual competencies and organisational innovation and change (Grote, 2009). Table 2.2 summarises the characteristics of these two distinct approaches to managing uncertainty in organisations.

Table 2.2: Basic principles of uncertainty management underlying organisation design (from Grote, 2004)

Minimising uncertainty	Coping with uncertainty
Complex central planning system	Planning as a resource for situated action
Reducing operative degrees of freedom through procedures and automation	Maximising operative degrees of freedom through local (lateral as opposed to top-to-bottom) coordination and cooperation
Disturbances are symptoms of inefficient system design and are to be avoided at all cost through heighten and cumulative control measures (regulations and procedures)	Disturbances are opportunities for the use and enhancement of competencies and for system change
Local dependence from centralised feed-forward control	Local autonomy coordinated through feedback control

Overall, safety must be based on a dynamic balance of a degree of stability and rigidity on which to ground a robust coordination and management structure against a degree of flexibility that allows for local adjustment to high pace changing performance conditions. Therefore, stability and flexibility will be balanced in accordance with internal and external demands, which requires addressing and managing strategic contradictions, such as short-term performance and long-term adaptability or differentiation and integration (Smith and Tushman, 2005, in Grote, 2009). From a contingency perspective, the issue is to establish a balance between stability and flexibility using rules and routines that allow coping with uncertainty while at the same time providing sufficient standardization to ease coordination demands. The balance between stability and flexibility forms the centre of all further considerations to managing uncertainties.

2.5.4 Stability versus flexibility

Widalvsky (2004) suggests that the search for constancy that characterises the engineering perspective defines more appropriately a condition of stability, rather than resilience. Widalvsky (2004) further argues that, under stable conditions, the future is less uncertain. In such conditions, risks can be known, predicted and therefore, anticipated more easily. Hence, the ability to anticipate threats is closely related to the existence of some form of operational stability in the system. If there is a well known condition of equilibrium in which the organisation aims to remain, then safety management can be built around anticipation capabilities. This is the scope of safety measures such as fire drills, which aim to prepare people for a known threat. Safety management in HROs, such as nuclear power plants, is an example of this evolution: Safety regulations and measures were added cumulatively in the attempt to anticipate new dangers (Widalvsky, 2004). Woods & Hollnagel (2006) consider that safety practices have always been dominated by hindsight in the sense that their focus was set on preventing undesired events from happening again. This path of development was based on the experience of well known and stable system operations, as pointed out by Hale *et al* (1998).

System complexity has led organisations to consider other safety requirements, beyond the anticipation of known events. Organisations face today constant pressure and must be capable of adapting to rapidly changing environments (Marais *et al*, 2007). The rapidly changing environment inherent to high complexity requires systems to be flexible in order to adjust to ever changing environmental conditions (McDonald, 2006). Dealing with variability is clearly in line with the principles of the ecological perspective of resilience, rather than the engineering one (stability), as this perspective focuses on the development of means to manage change and its unpredictability (Widalvsky, 2004). The rationale for accepting variability, as opposed to enforcing stability, lies with life's inherent uncertainty and complexity (Widalvsky, 2004). Management under complex conditions is necessarily based upon incomplete understanding, and in face of uncertainty, we are unlikely to attain a sufficient degree of anticipation (Gunderson *et al*, 2002). Widalvsky (2004) proposes the human body as an example of ecological resilience and its ability to cope with change. Rather than resisting aggressions from the environment, the human body takes on contaminations and builds on them to improve its immunity.

As argued by Gunderson *et al* (2002), aiming for stability requires less effort than considering the potential unknown threats and the need for flexibility. Even from an individual perspective, it is fundamentally human to continuously strive for efficiency (reduction of resources consumed when pursuing a given goal) and from a cognitive point of view, we continuously try to achieve that by developing and perfecting rule-based and skill-based behaviours (Rasmussen, 1996), which in practice means operating based on simplified (mental) models of reality and assumptions. An absolute stable condition could only be achieved through perfect anticipation (Widalvsky, 2004). In order to make decisions, no matter how complex or simple they might be, people are forced to simplify scenarios and make assumptions on a number of factors. Like people, organisations must assume that certain aspects of their operation and their environment remain stable, in order to reduce uncertainty and define possible courses of action and make a decision (Widalvsky, 2004 and Hollnagel, 2009). Within this context, even when faced with high complexity and the uncertainty of constant change, organisations must find some form of stability on which to ground their (safety) management decisions. It is only based on stability that the need for change and adjustment can be perceived (Widalvsky, 2004). McDonald (2006) further explores this by discussing the relation of sociotechnical systems with their environment in terms of a balance between stability and flexibility. Achieving stability with the physical, social and economic elements of the operating environment is characterised as an otherwise positive or successful outcome. However, rather than a static condition, this stability constitutes a dynamic (therefore, flexible) equilibrium with the system's environment. It is only by achieving such equilibrium and maintaining it (therefore, having stability) that undesired variability and its potential for failure can be detected. Maintaining stability requires the capacity to adjust (McDonald, 2006). Hence, both stability and flexibility must be considered for resilience in complex systems.

Walker & salt (2006), suggest that while robustness is often associated with the image of a tree that resists firmly, flexibility is pictured as the plant that bends with the wind. Stability, as the ability to primarily avoid undesired events, provides the means for robustness. Accepting variability means maintaining a degree of flexibility necessary to deal with constant change. Hutter (2010) discusses resilience in the German public sector and refers to the need for strategies for dealing with natural hazards, which are both robust enough to deal with partly known and unknown contexts and simultaneously, flexible enough to manage "radical surprise". Resilience engineering relates to achieving and maintaining a balance between the need for stability, in order to achieve avoidance, and flexibility as a way to develop survival and recovery capacities. McDonald (2006) places resilience in the successful management of a balance between aspects that reinforce stability and others that work towards flexibility. Table 2.3 summarises the main aspects considered by McDonald (2006).

The challenge resides in the fact that although both stability and flexibility are needed to achieve and maintain resilience, at some point these might be contradictory objectives. For instance, organisations must realise when and how procedures should be made robust and what informal practices should be allowed to enrich local autonomy and response to operating variability (McDonald, 2006). The opposing nature of these organisational aspects will require trade-offs to be made. Where decisions are made to formalise, centralise or standardise,

opportunities for informal practices, decentralisation and adjustability will have to be sacrificed. Grote *et al* (2009) discuss a demand for concurrent standardisation and flexibility.

Table 2.3: Aspects of stability versus flexibility (from McDonald, 2006)

Stability	Flexibility
Formal procedures as a way to develop stronger routines and improve coordination	**Informal work** practices are developed on the base of local autonomy and consolidate it
Centralisation can increase reliability by reducing the variance induced by individual skills and experience	**Decentralisation** is at the core of distributed decision making
Standardisation facilitates and contributes to increased product quality	**Adjustability** of product standards in response to market or operational feedback and acquired expertise
Automation of routine or complex functions enforces standardisation (normally through the use of well tested technology)	Technologies that enable **appropriate human control**, rather than constraining it (normally requires innovative technology)

The challenge resides in the fact that although both stability and flexibility are needed to achieve and maintain resilience, at some point these might be contradictory objectives. For instance, organisations must realise when and how procedures should be made robust and what informal practices should be allowed to enrich local autonomy and response to operational variability (McDonald, 2006). The opposing nature of these organisational aspects will require trade-offs to be made. Where decisions are made to formalise, centralise or standardise, opportunities for informal practices, decentralisation and adjustability will have to be sacrificed. Grote et al (2009) discuss a demand for concurrent standardisation and flexibility.

2.5.5 Cascading behaviour

Network of networks or systems-of-systems (Jamshidi, 2008) are prone to cascading behaviours in the sense that events in a given part or element of a sytem (or sub-system) may bring about unforeseeable (often catastrophic) cascading effects across other interdependent parts of the network. For transportation the interdependent networks might be metro, bus and vehicles. Understanding which conditions might lead to cascading effects and fragmentation of the network can be achieved through a mathematically principled framework, as the one provided in D'Agostino & Scala (2014), which offers a general presentation of models and algorithms for resilience assessment. Buldyrev (2010) and Gao et al (2012) have proposed the theory of random graphs and percolation models.

Another method proposed by De Domenico et al (2014) uses random walks in dynamic networks and considers an application to the public transport of London. An increase in connectivity might be detrimental to resilience as shown in Brummitt et al (2012) and D'Souza et al (2014), where the resilience optimal connectivity level is computed using the "sandpile model". This "optimal" connectivity level is shown to minimize for each interdependent network the risk of undergoing a large cascade.

The same problem of resilience of a complex independent network is taken up, at a different time/space scale, in using the Interdependent Multi-layer Model (IMM) to investigate horizontal/vertical interdependence among networks within the international trade system. The IMM has been also tested under potential shocks and shown to be able to model post shock scenarios (Caschili et al, 2015).

2.6 Decision making

Managing is making decisions. In any system, every person makes decisions at all levels. From a manager who makes decisions that regard the whole system, such as finance-driven decisions, to an operator who makes decisions regarding the task under performance, the system functioning is supported by different decisions that are made at its different levels. Decision-making involves a cognitive process that leads to an action with aim of producing satisfying outcomes (Elliot, 2005). Theoretically, decision-making can be described in relation to various dimensions such as rational versus irrational, cognitive versus emotional, goal-driven versus event-driven (Boy, 2013). Decision-making involves three main attributes: goals and objectives, alternatives and selection principles, criteria and processes. In every dimension, decision-making results from trade-offs between efficiency and thoroughness (Hollnagel, 2009). If the efficiency goal prevails some control may be lost due to some incompatibility between the performed actions and the related performance conditions; if the thoroughness goal dominates, actions may be delayed and miss their performance useful time. Thus, decision-making requires a balance between efficiency and thoroughness, which is made of experience in practice so that the right actions will be performed in due time.

From a cognitive perspective, decision-making can be broadly defined as the mental processes resulting in the selection of a course of action among several alternatives (Wicklund & Brehm, 1976). In practice, Svenson (1996) defines decision making as the response to pressures generated by conflicting circumstances or differing goals that have to be negotiated and reconciled. The notion of conflict as the source of the need to decide has lead to the development of two important concepts:

- Festinger (1985) describes this conflict as the source of cognitive dissonance. Festinger (1985) refers to dissonance as the existence of non-fitting knowledge (cognition) or opinion about the environment or about oneself. For instance, within the rail engineering work environment, a dissonance could be described as having to allocate resources to a given work item when such resources are unavailable or simply having more work items to schedule than the available access necessary to deliver it. Dissonance pressures the individual to search for a more suitable circumstance, which implies making choices.
- In opposition to dissonance, Wicklund & Brehm (1976) refer to cognitive consonance when one element psychologically implies another, within one's cultural or behavioural patterns, or experience. The authors mention psychological implication in regards to cognitions, which are logically connected. For instance, allocating resources to one particular work item is consonant with knowing that such item is approved for delivery. In general terms, voting for a candidate is consonant with believing that this person has the necessary qualities to hold the office in question, whilst dissonance would be voting for a candidate knowing that such a person is unfit for the duties.

Svenson (1996) presents two different approaches to the study of decision-making:

- The structural research approach relates choices and their ratings to the input variables. This involves analysing aspects of decisions such as the possible maximum gains across different options and probabilities of decision outcome. The author points out that under this perspective, no attempts are made to infer the psychological processes that occur at different stages between problem presentation and reaching a decision.
- The process research approach focuses on these particular psychological aspects of decision making. The recognition and description of different stages from the conflicting circumstance to reaching a decision are envisaged by means of methods such as information search patterns and think aloud protocols.

In contrast with a structure approach, Crozier & Ranyard (1997) consider three attributes of decisions when viewed as a process:

- Reaching a decision acquires a dimension in time. Decisions are assumed to take a period of time to be reached, which could be minutes, hours or days.
- Decision makers explore a range of possible strategies to reach decisions and adapt their decision rules to changing circumstances.
- The representation of the problem at hand initially built by the decision maker evolves as the decision process develops.

Svenson (1996) argues that a process perspective is essential for the exploration of regularities (invariant elements) in decision making. Svenson (1992) had previously advocated that beyond the analysis of pre-decision information gathering and processing stages, research on decision-making should also focus on post-decision processes, which further emphasises the importance of a process approach. Within this context, Svenson (1996) introduces the four types of decision problems described in Table 2.4, which embed different levels of complexity.

Table 2.4: The four types of decision problems (from Svenson, 1996)

	Description
Level 1	Quick decisions that tend to recur to automatic and unconscious decisions. Decisions made based on previous experience (recognition-primed decisions – Klein, 1989 in Svenson, 1996).
Level 2	The decision involves one or a few attributes but these are not generating any kind of conflict. The solution remains relatively obvious.
Level 3	Decisions involving alternatives with conflicting goals.
Level 4	The alternatives are not known, nor the attributes that define them. Problem solving constitutes an important sub-process at this level.

Svenson (1996) points out that these levels should not be interpreted as being isolated and that decision makers may refer to several levels within a broader decision process. “Lower level processes are also nested within higher level decision processes as sub-processes of the latter”.

2.6.1 Distributed decision making

Institutions are today required to make decisions regarding investments, research and development or the deployment of resources in complex and uncertain environments (Crozier & Ranyard, 1997). This means that beyond individual people, the way organisations reach solutions to their problems should also be considered.

The concept of distributed decision making has been particularly relevant for research in organisational contexts and management. Schneeweiss (2003) describes this as the design and coordination of decisions connected within a broader decision process. Schneeweiss (2003) considers that the growing complexity of society can no longer be understood and governed by the paradigm of centralised decision making and that distributed decision making has become a predominant methodology of handling complex systems. Zeleny (1981) cites Stafford Beer in “Platform for change” (1975), where he considers that “the real decision making process involves a lot of people and the whole structure is redolent with feedback. At every decisive moment, of which there will be great many within the total decision, we range ahead and back and sideways”. Schneeweiss (2003) further considers that complex decision problems are solved by splitting them up into their components, either by a single individual through intellectual segregations and subsequent coordination, or by multiple individuals participating in some problem of mutual interest.

Zeleny (1981) considers that it is only when people are faced with multiple objectives, criteria, functions and attributes that a decision making process emerges. Zeleny (1981) describes decision making as dynamic

processes of information searching in many different directions. The information gathered is then assessed, reconsidered or discarded. This generates numerous sources of feedback, which in return, renews the information search. “Man is a reluctant decision maker, not a swiftly calculating machine” (Zeleny, 1981). Zeleny (1981) proposes four generic stages for decision making processes:

- The **pre-decision stage** regards the initial sense of conflict, tension or dissatisfaction that provides the motivation for a decision process to be initiated. This conflict emerges from the lack of satisfying or feasible alternatives in view of the existing circumstances or perceived scenarios. Zeleny (1981) points out that if a feasible and satisfying alternative is found then the conflict no longer exists and the decision process ceases. The author considers such circumstances quite rare and therefore, the effort towards resolving the conflict shifts to an attempt to minimise the conflicting aspects. This amounts to containing the conflict within an acceptable level.

- As the process develops, **partial decisions** are made, which constitute a directional adjustment of the decision problem. Alternatives are discarded, new ones may be admitted and the remaining ones redefined. Overall, this generates a review of the conflicting elements, and thus, a redefinition of the problem at hand. Zeleny (1981) considers that two elements contribute to the development of partial decision processes: the prevalence of the pre-decision conflict and the post-decision dissonance which emerges as confidence in the choice made is questioned. Svenson (1996) refers to this process as **differentiation**. Svenson (1996) advocates that the purpose of a decision process is not to simply fulfil the decision rules in question but rather to generate an alternative course of action sufficiently distinct from the remaining alternatives. This is achieved by restructuring the decision process according to the context and persons involved.

- Through partial decision processes, the alternatives deemed feasible and the ideal scenario are progressively brought closer together, which eventually leads to an acceptable level of satisfaction and a **final decision** is reached. A partial decision differs from a final decision in the sense that in the latter case, the decision makers were able to reduce the post-decision dissonance to an acceptable level. At this point, Zeleny (1981) argues that there are few alternatives being pondered and these tend to be very similar.

2.6.2 Naturalistic Decision Making

The way “*experienced people, working as individuals or groups in dynamic, uncertain and often fast-paced environments, identify and assess their situation, make decisions and take actions whose consequences are meaningful to them and to the larger organisation in which they operate*” (Zsambok, in Zsambok & Klein, 1997), is today called Naturalistic Decision Making (NDM). The way people use their experience and knowledge to make decisions in naturalistic environments is the centre of research in NDM. The issue is to understand how people make decisions in real-world settings, which include dynamic and continually changing conditions, real-time reactions to these changes, ill-defined tasks, time pressure, significant personal consequences for mistakes, and experienced decision makers (Table 2.5) (Klein & Klinger, 1991). These task conditions exist in operational environments associated with crew systems, so it is essential to determine how people handle these conditions. Furthermore, the set of conditions usually faced in natural environments impose team interactions and actions to be performed under time pressure, changing conditions, unclear goals, as well as ambiguous or missing information. This requires high expertise and experience on emergency response organisation, particularly in the addressed contexts, together with positive risk-taking behaviour. Previous models of decision making were limited in their ability to encompass these operational features.

Table 2.5: Features of Naturalistic Decision Making (From Klein & Klinger, 1991)

Ill-defined goals and ill-structured tasks
Uncertainty, ambiguity, and missing data
Shifting and competing goals
Dynamic and continually changing conditions
Action-feedback loops (real-time reactions to changed conditions)
Time stress
High stakes
Multiple players
Organisational goals and norms
Experienced decision makers

Expertise can be built from experience of real accidents, allowing for the development of a repertoire of response patterns. Fortunately, in most safety-critical and complex environments there is not much experience on which to build this repertoire. Thus, context-related knowledge and problem solving strategies are usually provided through training activities so that they are stored in memory as normal operational role to be implemented in an emergency.

Understanding the way people make decisions in unexpected emergency situations in natural settings require a review of models and theories supporting naturalistic decision making.

- The Recognition/Metacognition Model (Cohen, Freeman & Thompson, in Zsambok & Klein, 1997) describes a set of metacognitive skills that enhance recognitional processes in decision events involving novel situations. These skills include: "(1) identifying key situational assessments and the recognitional support for them; (2) checking stories and plans based on those assessments for completeness; (3) noticing conflicts among the recognitional meanings of cues; (4) elaborating stories to explain a conflicting cue rather than disregarding it; (5) sensitivity to problems of unreliability in explaining away too much conflicting data; (6) attempting to generate alternative coherent stories to account for data; and (7) sensitivity to available time, stakes and novelty that regulates the use of these techniques". The use of these metarecognitional skills requires a solid base of familiarity in a context. This model was developed in two military domains.

- The Recognition-Primed-Decision Model (Klein, in Zsambok & Klein, 1997), including a diagnostic function, explaining how experienced fireground commanders identify and carry out a course of action using their expertise without analysing alternative options for comparison. This model describes what people do under conditions of time pressure, ambiguous information, unclear goals and changing conditions, fitting the criteria of NDM defined by Zsambok (in Zsambok & Klein, 1997): describing rather than prescribing, addressing situation awareness and problem solving as a part of the decision making process, involving experienced agents working in complex and uncertain conditions, facing personal consequences of their actions. However, this model does not address the influence of team and organisational constraints.

- Endsley (in Zsambok & Klein, 1997) reinforce the importance of situation awareness highlighting the importance of making a decision on the basis of wrong perception and evaluation of environment cues. This model provides a general framework to understand processes and factors impacting situation awareness emphasising the role of SA in the decision event. Being similar to other models of human

performance and decision making, this model describes the three levels of SA: perception, comprehension and prediction. This process plays a vital role in dynamic and complex environments so that the explanation of any inappropriate decision making should be searched at each one of the different levels of situation awareness. On one hand, a lack of attention doesn't allow for detection and perception of information cues in the environment; but, on the other hand, inappropriate decisions (errors) result from an incorrect projection of the situation. In complex and dynamic environments, human decision-making is highly dependent on SA. In these cases, the consequences of inattention or of any unsafe act can be severe.

- Serfaty, MacMillan, Entin & Entin (in Zsambok & Klein, 1997) developed a mental model to study expertise in military settings highlighting differences between experts and novices. This model is based on a three-stage process involving Recognition, Exploration and Matching by which mental models are developed and used by the expert. Experiments have been carried out evidencing the following: (1) Recognition – experts organise their knowledge so that they store and retrieve information in a different way from novices; (2) Exploration – experts may have a better set of analysis techniques making a better use of the available information-gathering resources than novices; (3) Matching – experts have a better model of the tactical situation so that they can better anticipate outcomes or problems. This model has important implications for training and the evaluation of decision making expertise.

- Lipshitz & Shaul (in Zsambok & Klein, 1997) provided a contribution to NDM models and theory by means of a critical review of the above-referred models. Based on literature review, the authors conclude that a theory of NDM must include contents referred to memory structures and current representations. Furthermore, results from a simulated sea-combat have shown that (1) experts collect more information on the situation before making a decision; (2) experts engage in more efficient information search; (3) experts read the situation more accurately; (4) experts make fewer bad decisions; (5) experts communicated more frequently and elaborately with friendly units. These findings have implications for theory, research and training being particularly important the set of four hypotheses constituting a diagnostic tool for training in decision making. Thus, instructors should provide trainees with detailed and accurate feedback being guided by the four hypotheses to test if: (H1) an inappropriate decision should be attributed to an inadequate mental model; (H2) the trainee's mental model as a proximal cause of a bad decision making; (H3) the trainee's ignorance of the appropriate option; (H4) inability to identify correctly when this option applies. Identifying expert-novice differences regarding the four hypotheses can help the process by adapting the training design.

Different decision strategies require different levels of cognitive functioning imposing different cognitive demands. Based on Rasmussen's cognitive control model of task performance (Rasmussen, 1996), two different levels of decision-making are described by Orasanu & Fischer (in Cook, Noyes & Masakowski, 2007): (1) rule-based decision-making relying on a prescriptive rule defining a situational-tailored response, either under a condition/action or go/no go strategy; (2) knowledge-based decision-making relying on knowledge and experience involving different strategies: choice problems, selection problems, situational management or creative strategy. In natural settings imposing the right actions performed in due time, decision making in rather supported by knowing what to do in a given situation than choosing the best alternative. Therefore, the three assumptions of rational decision making are no longer acceptable in natural settings (Hollnagel, in Cook, Noyes & Masakowski, 2007) once (1) a dynamic environment cannot provide a *complete information*, which requires sampling the necessary information without changes during this process; (2) for the same reason, *infinite sensitivity* would require time to differentiate among alternatives; and (3) the lack of time to consider all the alternatives people have found would advice against *weak ordering*.

Finally, every NDM model has important implications for training, particularly addressing Resilience. They should be taken into account in the design of further training programs in the frame of RESOLUTE. Prescriptive models

of decision making have shown their inappropriateness to support decision making in risky, complex and uncertainty real-world settings. Instead, the development of appropriate training programs and decision support systems should be targeted in order to fit the objectives of RESOLUTE.

2.6.3 Risk taking

Decision-making in real world settings, particularly in complex and dynamic environments, involves an important relation between time and action, as the right action must be performed in due time; otherwise, the same action is not anymore suitable. Together with time and action, effectiveness, risk and safety complete the set of factors involved in decision-making in naturalistic environments (Pettersson, in Cook, Noyes & Masakowski, 2006). Safety and effectiveness are both aimed as the highest ones but they are consequences of the available time and actions in the contextual situation. However, a balance between all these factors is necessary once too much time spent on actions supporting high safety may result in low effectiveness. The same can happen if too much attention is given to high effectiveness, which can result in reduced safety increasing the risk of errors. Risk is here defined as the probability of the mission failure. Safety can be improved if more time is available to be spent on the control of the mission in progress. This requires understanding of interactions between time and action and their effects on the system performance. Actually, these influences are the most important and must be known and used.

Any decision in real world settings and its outcomes are associated to a degree of uncertainty, being risk an inherent part of everyday life and being present in many decision-making situations. Risk is present in everyday decision-making. As stated by Vertzberger (1998), risk is a "*real-life construct of human behaviour representing a complex interface among a particular set of behaviours and outcome expectations in a particular environmental context*". Risk is associated to uncertainty, particularly in what concerns the outcome value (in terms of being positive or negative, desirable or undesirable) and ambiguity (in terms of being known or unknown). The level of risk is another issue being defined by the answers to the following questions: (1) What are the gains and losses associated with each known outcome? (2) What is the probability of each outcome? (3) How valid are the outcome probabilities and gain-loss estimates? Thus, risk is the "*likelihood that validly predictable direct or indirect consequences with potential adverse values will materialise, arising from particular events, self-behaviour, environmental constraints, or the reaction of an opponent or third party*" (Vertzberger, 1998). In this perspective, risks can be estimated according to: (1) the desired or undesired outcomes values, (2) the probability of outcomes, and (3) the validity attributed to the estimates of outcomes values and probabilities.

In risk theory (Vertzberger, 1998), risk is disaggregated into three categories: real, perceived and accepted risk. A real risk is the actual risk related to a situation or behaviour being decision makers aware or not of it. A perceived risk is the level of risk attributed to a situation or behaviour by decision makers. An acceptable risk is the level of risk representing the net cost that decision makers perceive as sustainable and are willing to tolerate with the aim of attaining their goals. Before deciding whether to take the opportunity and intervene, decision makers have to compare the option for intervening with other options assessing the balance between risks and gains. Then, the decision on how to proceed is shaped by the balance of the real and perceived risks against acceptable risks (Table 2.6).

Table 2.6: Risk contingencies and outcomes (Fom Vertzberger, 1998)

RR – Real Risk; PR – Perceived Risk; AR – Acceptable risk

1	RR>PR & PR≤AR	Risk seeking policy. Damage from misperception is maximised
2	RR=PR & PR≤AR	Potential for taking optimal risk levels
3	RR<PR & PR≤AR	Disposition to take moderate risks
4	RR>PR & PR>AR	Preferences not clear. Damage from misperception is limited

5	RR=PR & PR>AR	Risk-averse policy. Likely error on the side of overcaution
6	RR<PR & PR>AR	Risk-averse policy. Misperceptions could lead to missed opportunities

Decision-making and risk-taking are closely related (Boy, 2013): (1) both involve important and related cognitive processes; (2) decision-making entails risk-taking; (3) risk-taking involves action resulting from a decision-making process with more or less knowledge of its possible outcomes; (4) risk-taking requires preparation, training and knowledge, together with situation awareness, which is an important part of the regulation loop of human activity (Bellet *et al.* 2011). Every action, particularly having uncertain outcomes, requires risk-taking, which is an inevitable behaviour in every complex and dynamic environment. Risk-taking is necessary when there is no prescribed solution for a particular situation. Above all, risk-taking is an essential behaviour in human development. A child takes risks to stand up and start walking without knowing the possible outcomes; every step on the child's development takes its roots on risk-taking behaviour.

Taking a risk means that a decision has to be made and the corresponding action has to be performed sometimes without complete information about the conditions that will be found and/or the related outcomes. Within complex and dynamic systems risk-taking requires professionals with high levels of skills, competence and expertise, being prepared to (1) take risks out of any predefined solution for eventual problems and (2) to deal with the unexpected. Thus, risk-taking requires training, knowledge, skills and experience to mobilize the required attention being the grounds of a focus choice onto success or survival (Buljan & Saphira, 2005). Depending on the self-perception of one's abilities and skills, as well as the individual's maturity of practice, there will be a decision directed by an attitude that can vary from heightened awareness of the situation onto high-variance alternatives, these ones leading to risk-prone behaviour. Therefore, risk-taking behaviour depends on: (1) the available resources and related self-perception; (2) risk-taking perceived as success or failure; and (3) the way attention is allocated between both reference points (targeted performance or survival).

A study carried out by Desrichard & Denarié (2005) compares frequent and occasional risk-taking behaviour amongst adolescents and younger adults, focusing on the related triggers. It seems that sensation seeking, age and negative affectivity modulate the frequent risk-taking behaviour, whilst just sensation seeking contributes to occasional risk-taking behaviour. Furthermore, just the parental control or a lack of opportunity can prevent younger people from engaging in frequent risky behaviours. They seem to be more susceptible to the influence of their peers in risky situations; this means that adolescents and younger adults take risks rather for pleasure and a need for recognition from their peers than to face a real need to overcome a difficulty or to survive. Therefore, they take risks for nothing in a total absence of (1) a self-assessment of the conditions they will find in relation to their available resources, (2) any knowledge to understand the situation and direct the appropriate decision, (3) or the ability to anticipate the evolution of the situation. These are negative risk-taking behaviours. With increasing age and education, this risk-taking behaviour will change towards more responsible attitudes underlying appropriate behaviour in risky situations. Then, risk-taking behaviour in particular situations will be led by a contextual-related knowledge, the identification of the existing risks, the balance of the situation demands and the available resources to make the appropriate decision and perform the related action successfully. This is a positive risk-taking behaviour once it is conscientious, knowledge-directed and supported by the required skills and competence knowing what to do.

Many critical situations require immediate actions without complete information about the conditions people will find. This requires decision-making based on deep knowledge, skills, experience, courage and creativity towards a survival performance level instead of a common targeted performance level. This is the case of safety-critical systems where fault-tolerance absorbing the variability of human performance becomes the way to enhance the system reliability. Furthermore, taking a risk is not an isolated decision once each potential risk taker is a member

of a team and the success or failure of his/her action will affect positively or negatively the team and, probably, the whole system.

2.7 Risk management in complex systems

The recent history of all industrial sectors clearly illustrates the impacts of systems complexity on various domains of management and operations, particularly in terms of risk management. As illustrated by the investigation into the NASA shuttle accidents (Marais *et al*, 2007), the uncertainty and variability associated with complexity renders risk management equally complex. Empirical evidence shows that, on the one hand, systems complexity emerges from systems tight couplings and interdependencies. On the other hand, while such couplings and interdependencies are the means through which systems seek to optimise levels of resources and their allocation, they are also the paths through risks are propagated and producing unforeseeable complex chain reactions.

2.7.1 Background on safety issues

Safety is commonly defined as the absence of unacceptable risks (Hurst, 1998). This implies that a system is able to achieve its goals without loss of life or material damage (Jackson, 2010). Owens & Leveson (2006) consider safety to be a control problem. The purpose of safety oriented activities is to eliminate risk and therefore, to control events or courses of action that could lead to unsafe circumstances and potential accidents. From this perspective, accidents are the consequence of "component failures, external disturbances, and/or dysfunctional interactions among system components" (Owens & Leveson, 2006 pp 8). According to Kirwan (1998), managing safety relates to decisions on all practices, roles and functions involved in preventing such failures and disturbances. It involves all aspects of how safety is achieved or how other activities are performed in a safe way.

Hale *et al* (1998) argue that most of the current safety management practices and tools are rooted in the experience of earlier large scale organisations, in which changes would tend to be less frequent and of little magnitude. Strict regulations and standards applicable across all industrial activities were the core of safety management in organisations characterised by stable and well known operations. Hale *et al* (1998) further argue that "traditional" safety principles may be inadequate in the face of today's complex and fast pace changing organisations. Hale et al (1998) question whether safety can be managed through a careful analysis of past occurrences and prediction methods for what may be the consequences of each possible course of action. By the time such an approach produces a decision, the organisation may have shifted and the solution found may no longer be applicable or even safe.

Because the pathways that convey people and goods also enable risks to travel, as the degree of economical, political and social interchange between states increases, disasters rapidly acquire the potential to cross boundaries (Boin et al, 2010). Leveson (2004) explains fast pace changes with the introduction of new technologies into systems. While in the early twentieth century, new technologies would take about 30 years to reach the market, this can today take three years and products may become obsolete in five years Leveson (2004). Dekker (2004) adds that although computational speed has drastically improved access to information and the ability to generate data, humans are unable to keep up with such evolutions. People cannot process and make sense of the volumes of information that currently flow across complex systems. This is the context in which high complexity can lead to an increased risk exposure, and as initially mentioned, it can create additional challenges for the management of safety. Within complex environments, safety cannot be merely chosen, rather it must be searched (Widalvsky, 2004). This is also the context in which Hollnagel (2011a) places resilience engineering's view on safety: The ability to succeed under varying conditions.

2.7.2 The changing nature of accidents

There is a common understanding of the term accident as being an unforeseen and unplanned event or

circumstance, which leads to an undesired outcome, normally of loss or injury (Hollnagel, 2004). It is today widely recognised that dependence on technology has produced new and important sources of risk, and as a direct consequence, the nature of accidents has also shifted (Leveson, 2004). The scale that systems have attained creates the power to impact future generations through environmental pollution and genetic damage. As an example, Perrow (1999) mentions that activities such as the production of nuclear power, chemical and biological derivates, or the transportation of hazardous materials, are today a common presence, even in the vicinity of populated areas. The catastrophic potential of these industries has become evident in past disasters like the Three Mile Island, Bhopal or Chernobyl.

Leveson (2004) considers that complex systems cannot be managed under the assumption that accidents are produced by an uncontrolled and undesired release or transfer of energy between technical components. Technology is evolving faster than the methods to control and manage it, and consequently, unknown elements are introduced into system operations. Therefore, partially unknown operations must be taken into account as a contribution for the production of accidents in complex systems. Leveson (2004) further discusses the widespread use of computers and observes how this has created a potential for information loss, imprecision or incompleteness, which can lead to severe physical and financial losses.

Within complex scenarios, risk does not emerge solely from the presence of toxic or explosive materials Perrow (1999). Examples of this can be found in railway accidents like Clapham Junction (Hidden, 1989) or Ladbroke Grove (HSE, 2000), among others. Perrow (1999) considers that high risk systems are characterised by an interacting tendency that can lead to unexpected combinations of events. This is described as a system characteristic, as opposed to one of components or operators. In accordance to what was previously defined as a complex system, Perrow (1999) also refers to interactive complexity in high risk systems. Due to the numerous possible combinations of events and even greater number of potential outcomes, the author considers this interactivity the source of “normal accidents”, in the sense that occurrences in complex environments must be considered inevitable. Accidents in complex environments tend to be the result of unpredicted interactions and thus, as supported by Owens & Leveson (2006), the spread of potentially harmful interactions throughout the system have to be controlled.

As Leveson (2004) points out, accidents within complex environments tend to produce unpredicted chain reaction effects, which could rapidly reach intolerable proportions. Prevention of accidents requires a more proactive approach, in order to develop the ability to anticipate threats. Hindsight has become a benefit that complex systems may no longer afford. Weick & Sutcliffe (2007) add that high risk technologies must be controlled by means other than trial and error learning, as in many cases, the first error may also be the last trial. The challenge at hand within complex scenarios, is linking events that are further away in time and space than what would normally be the case when managing risks purely derived from technical or operator failures (Hale et al, 1998). Within this context, there is clearly a need to innovate safety practices in order to contemplate new types of accident aetiology.

2.7.3 Safety culture

The increasing awareness of factors that shape the behaviour of people and their decisions, as well as their resulting impact on the safety of organisations, has lead to a growing interest in organisational culture and in particular, safety culture (Hale & Hovden, 1998). Hurst (1998) generally describes safety culture as a set of ideas and beliefs that all members of the organisation share about risk, accidents and health. These shared values, attitudes and patterns of behaviour give the organisation its particular character (“the way we do things around here”).

Safety culture issues are today widely reported in the outcome of investigations into several major disasters such as the one of the Columbia space shuttle (Woods, 2003). However, a great deal of misunderstanding remains

around the concept of safety culture. Although people often refer to the need to improve safety culture as if this constituted a concrete feature of the organisation, as pointed out by Hurst (1998), most aspects of safety culture are intangible even though they lead to tangible and observable manifestations.

Similarly to high reliability issues, safety culture is also closely related to aspects of resilience. Because of this overlap and the evident need to clarify the domain of this concept, some discussion on the subject was considered relevant.

Both Kirwan (1998) and Hurst (1998) cite the Advisory Committee for the Safety of Nuclear Installations (ACSNI) in its formal definition of safety culture:

> *The safety culture of an organisation is the product of the individual and group values, attitudes, perceptions, competencies and patterns of behaviour that determine commitment to, and the style and proficiency of, an organisation's health and safety management (ACSNI, 1993).*

Hurst (1998) further points out that this definition leads to consideration of two important elements as constituents of safety culture: The underlying beliefs and attitudes towards safety, which are expressed both at an individual and group level, and the tangible safety manifestations through which these beliefs and attitudes are expressed. The relevancy for the management of safety resides in the strong relations between these tangible manifestations and the underlying elements of the culture. In order to shape behaviours and decisions, safety management practices must focus on the underlying elements of safety culture, rather than their manifestations (Hurst, 1998). Turner & Pidgeon (1997) add that safety culture encompasses the gaps between what is formally determined by the safety management system and the non-formalised aspects of operations. These are the informal strategies put in place to manage "grey areas" (the gaps). These strategies constitute the tangible manifestations of safety culture and they are developed based on experience according to the beliefs in terms of what is safe and unsafe of those applying them (Turner & Pidgeon, 1997).

The challenge becomes then the development of strategies and methods to identify and act upon the existing beliefs and attitudes. The purpose of an organisation would be to incorporate into its safety management, features that work towards what Kirwan (1998) considers a positive safety culture. According to Kirwan (1998), organisations with a positive safety culture are characterised by communications founded on mutual trust, by shared perceptions of the importance of safety and by confidence in the efficacy of the existing preventive measures. Hurst (1998) considers that a good (positive) safety culture results from adequate resources, good communications and a cooperation that ensures a balance between safety imperatives and production needs. The focus on communications and cooperation derives from the importance of group attitudes and processes to the management of safety (Kirwan, 1998). As noted above, factors shaping decision making are crucial for safety culture and most decisions will involve at least two people and often more. Communications and group factors become dominant, as the set of values and attitudes (safety culture) greatly influences the quality of the information flows developed within the organisation (Kirwan, 1998).

As observed by Jackson (2010), there are many different approaches to safety culture and the only certainty is that there are no right ones and no wrong ones. At each place in time and for each organisation, some methods to approach safety culture may be more adequate and efficient than others.

2.7.4 A system approach to safety

Hale & Hovden (1998) point out the importance of major accidents (e.g. Three Mile Island, Bhopal or Chernobyl) in the shift of safety management perspectives. Investigations into major occurrences of the 19070's and 1980's concluded that the bureaucratic and strict safety structures in place could not account for causal factors that were found to be beyond human and technical failures (Turner & Pidgeon, 1997). The perception of the widening gap between systems complexity and existing safety practices lead to the adoption of more flexible approaches,

aiming to better respond to the fast pace changes and heterogeneity of modern organisations. To this end, Hale *et al* (1998) discuss the self-regulation and certification approaches initiated in the 1970's. The principle at stake was that responsibility and accountability had to fall on those creating the risks, rather than governments and their agents issuing regulations and standards to control such risks. In line with this shift in safety practices, aviation and nuclear power are among the first industries to develop safety management systems. These systems constitute an organised approach to managing safety (Dijkstra, 2006), and beyond supporting specific safety needs, they facilitate the oversight role of national authorities.

The development of self-regulating management systems incentivised organisations to investment in research directed at their specific safety endeavours. Hale *et al* (1998) mention the growing interest of companies in developmental studies focusing on organisational design learning and management. Through such studies, safety research has gained interest in system theories, as a way to better understand complex synergies and combinations of events. Hale & Hovden (1998) refer to this as the "third age of safety". After a first age, during which safety focused on purely technical issues (initial industrial contexts), a second age with strong emphasis on human factors (human error and information technology), this third age of safety focuses on risks emerging from interactions between system components.

In terms of accident analysis, an approach to safety based on system theories allows more complex relationships between events to be considered and provides a way to look more deeply at why the events occurred (Leveson *et al,* 2003). Traditional models such as event trees, aim at building chains of events, either by placing those at the origin as route causes, or at the "sharp end" as immediate causes of accidents. System based models consider all events at the "sharp end" of the undesired outcome (Hollnagel, 2004). Although a timeline remains essential to understand occurrences, the focus is set on the relations between events, rather than their sequence in time. Events are considered as parts of the whole rather than distinct elements. Instead of looking at accidents as an end result, they are considered "emergent phenomena", as they arise from the combination of the concurrent events (Hollnagel, 2004).

The work of Rasmussen (1997) explains the relevancy of system views to understand safety in complex environments. Rasmussen (1997) refers to safety sociotechnical systems, which span across legislators, managers, work planners and operator levels. This model was earlier mentioned when discussing organisational decision making perspectives (Svedung & Rasmussen, 1998) and is here represented in Figure 2.4.

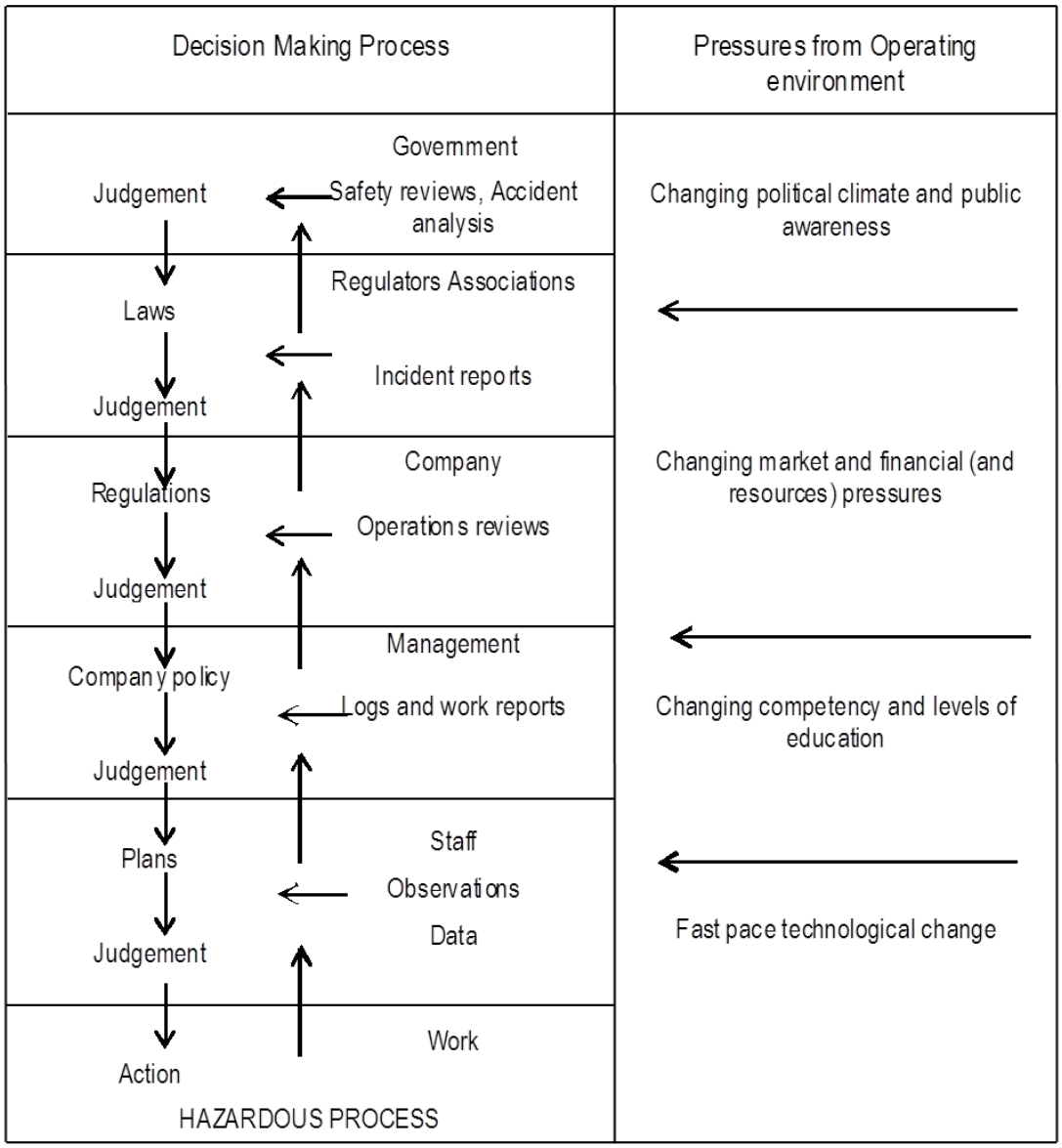

Figure 2.4: Sociotechnical system involved in risk management (from Rasmussen, 1997)

The control of hazardous processes relies on a series of laws, rules, instructions and procedures that are produced and applied throughout this system. Rasmussen (1997) argues that in order to address risks emerging from dynamic social contexts, the decisions made by politicians, safety officers, work planners and operators, as well as the pressures that constrain them, must be considered within a functional approach, as opposed to a structural decomposition into static elements. As earlier discussed, decisions are triggered by conflicting circumstances that pressure people towards making some kind of choice. Therefore, Rasmussen (1997) and later Svedung & Rasmussen (1998) maintain that risk management in complex systems requires understanding how pressures at each level affect decision making, and how decisions at one level affect decisions of the next one. An example of this can be found in the response to the devastation caused by the hurricane Katrina in 2005. As Westrum (2006b) discusses, despite the availability of supplies and resources to relieve the victims, these were not used because of authority disputes or breakdowns in communication. The failure of the hierarchical structure and its communications led to a complete stall in the system. Whatever possible ways there might have been to minimise the damage to the system and enable it to recover its operation more quickly had failed.

Leveson *et al* (2003) address the same hierarchical system perspective. They argue that the downstream decisions such as the ones represented in Figure 2.4, introduce the boundaries deemed necessary to carry out

the hazardous process within acceptable safety limits. On the upstream flow, information on system performance is provided to the higher hierarchical levels, which will then support future decisions, as necessary. Leveson *et al* (2003), define this flow of information as a safety control loop. From this perspective, lack of control over the system may arise whenever the information flow is interrupted, inaccurate or is taking too much time, among other information related issues. The authors point out the relevancy of this concept, as systems become increasing dependent on information technologies.

In light of a systems approach to safety, Leveson (2004) considers that many accidents attributed in a recent past to human error, would be more accurately described as the result of inadequate system and interface design. Models based on system theories consider accidents as arising from the interactions among system components and lead to the investigation of multiple causal factors and concurrent events (Leveson *et al*, 2003). Woods (2003) discusses the findings of the Columbia Accident Investigation Board and points out the identification of "holes in the organisational decision making". The organisational factors identified as causes for such holes were not considered unique to NASA and its programmes, but rather "generic vulnerabilities that have contributed to other failures and tragedies across other complex industrial settings".

The integration of system theories into safety management has led to the recognition of concurrent risk factors and system level interactions which would escape "traditional" safety methods that tend to decompose events into linear chains of events. Because the nature of accidents has shifted, safety measures such as the use of "redundancy", are becoming ineffective and in many cases, adding complexity to the system (Leveson, 2004). In this context, research on new ways of managing safety can be considered a crucial endeavour for the survival of today complex systems. A systemic approach to safety appears to be more adequate to the challenges of high complexity, as it focuses on the dynamic nature of system interactions and the non-linearity of its effects (Hollnagel, 2004)

2.7.5 Safety I versus Safety II

Safety is commonly defined as the "absence of undesired risk". While this has for many decades supported significant achievements in risk assessment and overall management, the growing complexity and heightened variability of operations in sociotechnical systems has made apparent many shortfalls of this approach. The following issues are progressively becoming inescapable for all those involved in risk management:

- Complexity renders operations in sociotechnical systems partly unknown. As earlier discussed, this is at the source of the notion of intractability (Hollnagel, 2009a).
- It is unrealistic to presume that risk management singly based on the implementation of various types of barriers (particularly when many those assume a procedural nature) against known hazards and threats can face up to the challenges of high variability and complexity, and the non-linear behaviour of operations in such contexts.
- Across every industry sector and throughout times, despite often continuous investments in risk managements, safety performance remains steady around what appears to be a limit to currently existing practices. This is assumed to be placed around a probability of 10^{-6} of serious events (death) for what are considered to be high reliability industries.
- Even without a careful analysis, it is easily perceived that sociotechnical systems experience successful performance in a proportion that is largely greater that failure. For instance, even in road transport systems in which accident rates are normally considered very high, it is undeniable that transport activities (people and goods) are normally carried out successfully, particularly when compared against the number of ours that we all tend to be exposed to the risks of road systems (we normally get into our cars and safely arrive to our destination; only very rarely experience an accident).

In view of these issues Hollnagel (2014) proposes a new perspective of safety, to which the author refers to as “Safety II”. Under this notion, safety is defined as the promotion of success, as opposed to the avoidance of failure and the learning from successful performance, as opposed to learning and building on from what are perceived as past failures. Safety II constitutes the shift in paradigm that must be placed at the basis of resilience, particularly when adopting the view of resilience engineering. This will be discussed in detail in the following sections.

3 RESILIENCE AND SUSTAINABLE ADAPTABILITY

Beyond the aspects of system complexity previously discussed, the global scenario of resource scarcity, environmental pollution and climate change is also put forward as a cause for many of the serious threats currently faced by societies. Boin *et al* (2010) distinguish such threats from "routine emergencies" such as fires and traffic accidents, and characterise them as "low-chance", "high-impact" events that can compromise life sustaining systems and require governance level intervention under high uncertainty conditions. These are the circumstances in which resilience is highlighted as a possible solution for the sustainability, reliability and safety of systems (Boin *et al*, 2010 and Jackson, 2010).

The concept of resilience covers many different matters (Westrum, 2006a) and is used across many different scientific domains. Resilience is firmly based in the fields of engineering, biology and psychiatry (Gunderson *et al* 2002, Jackson 2010, Vugrin *et al* 2010, Boin *et al* 2010 and Holling 2010). While engineering applies this concept to materials and technical systems, biology focuses on living organisms and systems, and psychiatry aims at understanding resilience from an individual perspective (Boin *et al*, 2010).

3.1 Definitions

Resilience is generally interpreted as the ability to recover from or to resist being affected by some shock, insult or disturbance (Vugrin *et al*, 2010). Foremost, given that it regards the recovery after events, this concept must encompass a given timeline and therefore, should be regarded as a process rather than a given quality. Sutcliffe & Vogus (2003) refer to resilience as an emerging process in organisations, which develops through continually dealing with risks, stresses and strains. Within the same dynamic perspective, Westrum (2006a) considers three conditions as the fundamentals of resilient situations, which Jackson (2010) later paraphrases as follows:

- **Avoidance** relates to the ability to foresee potential threats and prevent something bad from happening.
- **Survival** implies that the system, while experiencing disturbance, maintains operations, even if partially incapacitated. This means that the system is able to cope with ongoing trouble and therefore, prevent something bad from becoming worse.
- **Recovery** refers to the ability of the system to repair itself and regain desired performance after something bad has happened.

Jackson (2010) regards resilience as the opposite of brittleness. In this sense, while the purpose of resilience in systems is achieving safety, brittleness leads to an unsafe condition of the system. Avoidance is clearly the ideal system condition but a total absence of failure is unrealistic within indeterminate and complex scenarios (Weick & Sutcliffe, 2007 and Leveson, 2004). Hence, an organisation needs to develop additional capabilities as, whenever avoidance mechanisms become insufficient to face conditions, survival abilities should be put into action and recovery the envisaged goal. Jackson (2010) considers that at least two of these three conditions must be met in order for resilience to be considered.

The concept of resilience, as previously described, contemplates a wide range of possible applications. It is clearly a trans-disciplinary aspect in organisations (Jackson, 2010). This becomes evident not only in the range of professionals that participate in resilience related activities, but also in the diversity of definitions found in the literature. In order to explore the actual diversity of applications and build an appropriate understanding of the concept, a literature survey was conducted. Keeping in mind the context of sociotechnical systems as the focus of RESOLUTE, this survey was limited to the frame of systems approaches to resilience. Table 3.1 summarises the most relevant definitions found in the literature. For reasons of practicality, only more explicit definitions found in relevant systems literature were considered. The keywords also shown in this table are used as indication for resilience properties in systems.

Table 3.1: Definitions of resilience

Authors	Definition	Keywords
Adger (2000) in Vugrin et al (2010)	Ability of groups or communities to cope with external stresses and disturbances as a result of social, political and environmental change	External stresses
Allenby (2005) in Vugrin et al (2010)	Capability of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must	Internal and external change Degrade gracefully
Boin et al (2010)	Ability to negotiate the flux (of events) without succumbing to it	Negotiate
Comfort (1999) in Vugrin et al (2010)	Capacity to adapt existing resources and skills to new situations and operating conditions	Adapt Resources and skills
Fiksel (2003) in Vugrin et al (2010)	The essence of sustainability. The ability to resist disorder	Sustainability Disorder
Fujita (2006b)	Utilisation of system's potential abilities (engineered features or acquired adaptive abilities) to the utmost extent and in a controlled manner, both in expected and unexpected situations	Potential abilities Utmost extent Controlled manner
Gunderson et al (2002)	Strength of mutual reinforcement between processes, incorporating both the ability of a system to persist despite disruptions and the ability to regenerate and maintain existing organisation	Mutual reinforcement Persist Regenerate
Hale & Heijer (2006a)	Ability to steer the activities of the organisation so that it may sail close to the area where accidents will happen but always staying out of the dangerous area	Steer activities Dangerous area
Holling (1973) in Vugrin et al (2010)	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	Persistence Absorb change and disturbance Maintain relationships
Hollnagel (2006)	Ability of an organisation to efficiently adjust to harmful influences rather than to shun or resist them Intrinsic ability of a system to react to and recover from disturbances at an early stage, with minimal effect on its dynamic stability	Efficiently adjust Harmful influences React and recover Dynamic stability
Hollnagel (2011a)	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	Adjust functioning Sustain required operations Expected and unexpected conditions
Jackson (2010)	Processes, disciplines and infrastructures that need to be in place to make sure that undesired events do not happen or that systems may survive such events and maintain operation	Processes, disciplines and infrastructures Survive Maintain operation
Leveson et al (2006)	Ability of systems to prevent or adapt to changing conditions in order to maintain (control over) a system property	Prevent or adapt Changing conditions

Starbuck & Farjoun (2005)	Continued willingness to drop one's tools in the interest of greater agility	Continued willingness Greater agility
Sutcliffe & Vogus (2003)	Maintenance of positive adjustment under challenging conditions Ability to absorb strain and preserve or improve functioning despite the presence of adversity Continuing ability to use internal and external resources successfully to resolve issues Capacity to rebound from adversity strengthened and more resourceful	Positive adjustment Internal and external resources Strengthened
Tierney & Bruneau (2007) in Vugrin et al (2010)	Inherent strength and ability to be flexible and adaptable after environmental shocks and disruptive events	Strength Flexible and adaptable
U.S. Department of Homeland Security Risk Steering Committee (2008) in Vugrin *et al* (2010)	Ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions Capacity of an organisation to recognise threats and hazards and make adjustments that will improve future protection efforts and risk reduction measures	Resist, absorb, recover Recognise threats and hazards
Vugrin *et al* (2010)	Ability to efficiently reduce both the magnitude and duration of the deviation from targeted system performance levels	Magnitude and duration Deviation from targeted performance
Walker & Salt (2006)	Ability of a system to absorb disturbance and still retain its basic function and structure	Absorb Function and structure
Weick & Sutcliffe (2007)	Intrinsic ability of an organisation (system) to maintain or regain a dynamically stable state, which allows it to continue operations after a major mishap or in the presence of continuous significant stresses	Maintain or regain Dynamically stable state Continuous significant stresses
Westrum (2006a)	Ability to prevent something bad from happening, from becoming worse, or to recover from it once it has happened	Prevent Becoming worse Recover from
Widalvsky (2004)	Capacity to cope with unanticipated dangers after they have become manifest, learning to bounce back	Unanticipated dangers Bounce back
Woods & Hollnagel (2006)	A paradigm for safety management that focuses on how to help people cope with complexity under pressure to achieve success	Safety management Complexity Pressure
Wreathall (2006)	Ability of an organisation (system) to keep, or recover quickly to, a stable state, allowing it to continue operations during and after a major mishap or in the presence of continuous significant stresses Ability to have appropriate levels of resources (particularly reserves) that can react to sudden increasing challenges or onset of a major hazard	Keep or recover quickly Stable state Continuous significant stresses Appropriate level of resources React

Several of the authors mentioned in Table 3.1 (Vugrin *et al* 2010, Gunderson *et al* 2002, Walker & Salt 2006, among others) distinguish two types of resilience, which reflect different views on how humans interact with and manage the world around them (Walker & Salt, 2006):

- **Engineering resilience** is considered a more "classical" view, emanating from physics models. It assumes a system exists around an equilibrium state and its resilience is defined in terms of the ability to resist departure from, or rapidly return to that equilibrium after significant disturbances (Holling, 2010). From this perspective, efforts aim at maintaining a degree of constancy in the system by containing its variability.
- **Ecological resilience** assumes that systems can reorganise themselves and therefore, contemplates the possibility of systems shifting from one domain of stability to an entirely different one. In this sense, resilience is defined by the magnitude of disturbance that a system can absorb (avoid) before it shifts from one set of mutually reinforcing processes and structures to a new one (Gunderson *et al*, 2002). The focus is set on the persistency of relations among parts of the system. Like many plants that bend with the wind instead of stiffly attempting to resist it, ecological resilience assumes the possibility of the system shifting to new equilibrium states in order to ensure its basic structure and function (Walker & salt, 2006).

Following the conditions of Westrum (2006a), both perspectives contemplate some form of avoidance, survival and recovery and therefore, could be considered within the domain of resilience. On the one hand, engineering resilience aims primarily for avoidance capacities (anticipation of threats) and would resort to recovery (and perhaps survival) capabilities to ensure fast return to its known stability condition. On the other hand, ecological resilience maintains more tolerance in the face of threats and endeavours mostly for survival and recovery capacities as a way to deal with the resulting constant change. This constitutes a fundamental distinction between these perspectives: While the engineering perspective aims to achieve and maintain a condition of stability, the ecological perspective aims at creating capacity to cope with variability.

Widalvsky (2004) considers that both perspectives constitute valid and useful safety approaches, depending on the type of organisation and its activities. In line with this view point and within the framework of resilience engineering, Hollnagel (2011a) defines this concept as follows:

> *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* (pp xxxvi)

It should be noted that aside from purely biological systems or ecological systems that have been kept guarded from any human intervention, everything that surrounds us and supports human activities are systems developed by humans. These are referred to under many different contexts and terminologies, of which the most common ones might be: human systems, sociotechnical system, systems of purpose, intentional systems, among others. The fundamental notion that is common to these terms is that every human designed and built system aims to fulfil a more or less clear purpose and that by definition, resilience is only meaningful in view of such system purposes. Therefore, a system can be said to be resilient if it is capable of continuously adapting to its operational environment in the pursuit of its system intention/purpose. This is in line with what Woods (2014) defines as sustained adaptability.

3.2 Trade-offs

One of the most common realisations is that we cannot have everything in life. The immediate consequence is that people are frequently confronted with the need to make choices that involve giving up on one thing in order to have the other. This is generally described as a trade-off. Hollnagel (2009) gives this concept a different level of

consideration and considers it as a constant presence in every aspect of decision making, both individually and collectively within the scope of sociotechnical systems. From this perspective, every decision reached by a person or an organisation gives shape to a trade-off of some kind. Within this frame of mind, this section clarifies the roots of trade-offs and its relevance for systems resilience.

Organisations are today confronted with complex choices regarding the application of their resources (Crozier & Ranyard, 1997). For instance, if investments are to be made in technology, then other necessities will have to wait for new opportunities. In a simplistic way, Hollnagel (2009) describes a decision according to three fundamental steps that are necessary to go from the external event that triggers the decision process, to its resulting course of action:

- An **evaluation** of the current situation and the problem at hand
- The **selection** of a given course of action from a range of options
- The **execution** of the chosen course of action, which amounts to planning the response to the initial problem

From this view point, trading-off is fundamentally generated during selection, as this step shapes the kind of choices made. It should be kept in mind that, as discussed by Zeleny (1981), a decision process is developed through an iteration of multiple partial decisions before a final decision is reached. As a consequence, even within this simple representation of a decision making process, within each evaluation, selection or execution step, several partial decisions must be considered, which themselves originate trade-offs. For instance, when evaluating, decisions have to be made on what information is needed or when that information is sufficient to build a good enough understanding of the situation. This substantiates the importance of trade-offs. They occur not just as the outcome of a decision making process, but also as a shaping factor throughout this same process by means of partial decisions. Hollnagel (2009) describes this as the process (with trade-offs at their core) through which people adjust their performance, aiming to match the perceived conditions.

The scarcity of resources is at the origin of every trade-off (Woods, 2006). Despite any other resource limitation, as pointed out by Hollnagel (2009), everything takes a certain amount of time to be accomplished and everything takes place in time. Hence, for the large majority of situations, time can be considered the most crucial resource of all. When confronted with a task and the need to decide, capacity limitations most often refer to the inability to be fast enough within the time available (Hollnagel, 2009). According to Hollnagel (2009), this places two opposed concepts at the core of trade-offs:

- The need for **Efficiency**, in the sense that something is achieved with minimum expenditure of resources (in particular time), results from the insurmountable scarcity of resources (Hollnagel, 2009). Because of this scarcity, tasks and decision making experiences pressure to keep resource utilisation to a minimum at all times. As noted by Woods (2003) in regards to the Columbia accident, under production pressure people develop shortcuts in reasoning, which leads to decisions being made based on assumptions. Although higher efficiency may be achieved, such shortcuts increase uncertainty and unpredictability (Hollnagel, 2009).
- Conversely, **Thoroughness** stands for the ability to accomplish a given objective with disregard to any limitation. This implies that before an activity is carried out, there is sufficient confidence that all the resources and conditions necessary to achieve the intended outcome are in place (Hollnagel, 2009). Hypothetically, this represents the possibility of carrying decision making processes through as much iteration (partial decisions) as desired. For instance, when carrying out maintenance work in transport infrastructures or within many industrial facilities, setting up safety barriers to “distance” maintenance from other ongoing operations, constitutes a precondition that aims to guaranty (or improve probability) that work will be delivered safely.

Hollnagel (2009) refers to this as the Efficiency-Thoroughness Trade-Off (ETTO) principle. Other authors, such as Dekker (2004), refer to a trade-off between safety and performance. While thoroughness, in principle, works towards safety by improving on preconditions necessary to avoid undesired results (achieve success), efficiency is devoted to performance improvement. From this, it follows that the ETTO principle is concerned with balancing conflicting goals, belonging to the domain of either thoroughness/safety or of efficiency/performance. The use of checklists constitutes a good example of this balancing act: By going through the checklist before taxiing to the runway, the pilot is reinforcing thoroughness (Hollnagel, 2009). The checklist aims to improve certainty that the desired outcome (safety of take off and flight) will be achieved. Because a certain amount of time is needed to go through the checklists, efficiency is sacrificed.

As pointed out by Hollnagel (2009) it rarely (if ever) is possible to be both thorough and efficient at the same time. Woods (2006) illustrates this fact by the "faster, better, cheaper" policy adopted by NASA and its contribution to the Columbia accident. The Columbia accident can be broadly attributed to NASA's failure in balancing safety against intense production pressure, which resulted in a pattern of drift towards failure. While complexity and a fragmented problem solving process hindered the ability to develop sufficient awareness of local and global conditions, pressures for performance led people to trade-off in favour of efficiency (Woods, 2003). Based on this same observation, Dekker (2004) intrinsically relates trade-offs with the drift into failure of complex systems. As illustrated by the Columbia accident, when trading-off favours efficiency beyond the capacities of the system, a drift into failure may occur.

From a systems resilience perspective, the essence of a trade-off resides in the balance between as much efficiency as possible, so as to maintain operations close to safety boundaries, and the thoroughness necessary to ensure that such boundaries are not crossed (Woods, 2006). In this regard, two capabilities are fundamental for trade-offs to contribute to resilience:

- People require information to support their decisions. Progress on safety ultimately depends on providing workers and managers with information about changing vulnerabilities (Woods & Hollnagel, 2006). Only then people can develop awareness of how much pressure for efficiency the system can sustain and when it is time to ponder with more thoroughness on the information available, or even to search for additional information (sacrifice decisions).
- Organisations need to develop ways of monitoring safety boundaries. As pointed out by Woods (2006), systems need to maintain awareness and responsiveness to evidence of any potential shifting of decision criteria, which might lead the system across safety limits.

Woods (2006) further points out that from a resilience perspective, the difficulty in balancing trade-offs ("ETTOing") is that thoroughness and therefore, attention to safety limits, is most necessary when performance pressures are higher. This means that precisely when they are most needed to respond to such heighten pressures, resources must be "sacrificed" to monitor and control the dynamics between system performance and safety boundaries. This is where systems resilience should be placed.

3.3 Functional resonance

The theoretical foundations of functional resonance were firstly introduced by Hollnagel (2004). This concept was developed within the scope of a non-linear and dynamic approach to the safety of complex sociotechnical systems. Rather than the static analysis of processes or components and their sequences in time, the concept of function used conveys aspects of system performance. For the purpose of this discussion a function is regarded as a set of actions that a system performs towards the achievement of a given aim (Woltjer, 2009).

The phenomenon of resonance in system operations is related to the fact that performance in complex environments is inherently variable in time. Variability can either be the result of short-term fluctuations on

resources, demands or working conditions, among others, or slower and longer-term changes such as those depending on economical and commercial relations. Hollnagel (2004) places the slow drifts of systems towards "new norms and emerging tacit standards" within this context and considers as an example, the NASA processes of drift into failure (Woods, 2003).

Operations in complex systems are normally underspecified. Thus, carrying out tasks requires tools and formal procedures to be adapted to meet unforeseen (or unforeseeable) operating conditions. Approximate adjustments that are made by people at all levels of organisations (aiming to match operating conditions) must also be considered as sources of variability. As observed by Hollnagel (2009), in the large majority of cases, these adjustments lead to successful outcomes and only rarely result in undesired events such as incidents and failures. This is clearly demonstrated by most accident rates in complex sociotechnical systems, which are typically beyond 10^{-6} occurrences per number of events (Amalberti *et al*, 2005). Hence, performance variability must be regarded as a useful resource, as it normally leads to success and only rarely, to failure. The processes that lead to success and failure are essentially the same, only their outcome is different, as "failure is the flip side of success" (Hollnagel, 2006).

Failure emerges when local variability produces insufficient or inappropriate adjustments to the variability of the environment (Hollnagel, 2006). This is represented in Figure 3.1. It should be kept in mind that for each system function, the remaining ones constitute its operating environment.

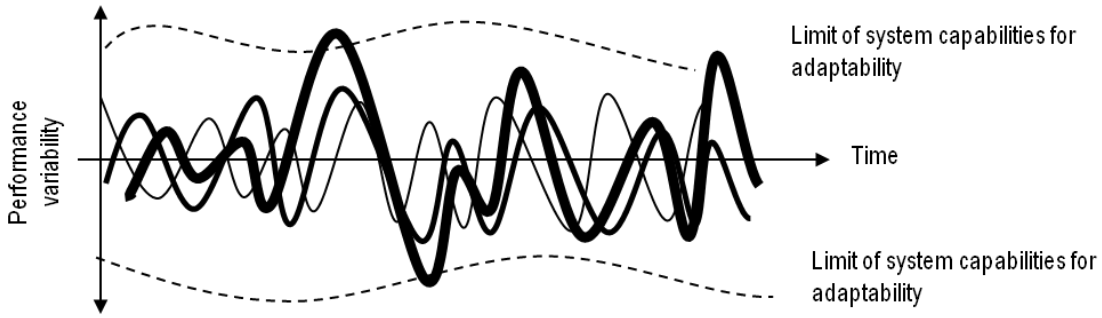

Figure 3.1: Performance variability and resonance (adapted from Hollnagel, 2008)

The variability of a number of functions (represented by thinner lines) may reinforce each other (resonate – represented by the thicker line) and exceed limits of system capacities (represented by dashed), which are also subject to variability. Thus, the thicker line in Figure 3.1 should be seen as the sum of the thinner lines. Functional resonance results from unforeseen interactions between the normal variability of functions. Normal variability of functions are weak signals and the resonance effect they may produce is the detectable signal, which may or may not exceed system capacities (Hollnagel, 2004).

Functional resonance emphasises the dynamic nature and non-linearity of performance in complex systems (Hollnagel, 2008). Based on this concept, accident analysis derives from an understanding of both "normal" and unusual functional relations in the system. Rather than aiming to eliminate variability, safety is built around the control of its sources and preventing it from assuming harmful proportions (Hollnagel, 2004). A system is in control if it is able to minimise to a manageable degree or eliminate undesired variability, or at least, that which is expected to exceed system capabilities (Hollnagel & Woods, 2006). The challenge then resides in providing people and organisations with tools to monitor not only sources of variability from within the system and its environment, but also changes of performance conditions that can lead to variations of system capabilities.

3.3.1 The Functional Resonance Analysis Method (FRAM)

The Functional Resonance Analysis Method is essentially a system modelling tool that focuses on system interdependencies, their dynamics and complexity. While it is not directly related to resilience and its assessment, it provides a fundamental support to such ends by supporting systems understanding.

FRAM is mainly based on the concepts of system function and performance variability (in line with the notion of functional resonance). Within this context, a system function is something of either a human, technological or organisational nature, which transforms the state of the system towards fulfilling the operational purpose of this system. This introduces in the modelling a diversity of factors relating to system dynamics, which frequently are unobserved within models based on organisational structures or process flows.

FRAM takes into account the non-linear nature of performance in complex systems, as opposed to building cause-effect sequences of events in time. It is based on the principle that accidents in complex sociotechnical systems are produced by unexpected combinations (resonance) of “normal performance” variability. Hence FRAM supports risk management by providing an understanding and steering option towards controlling (damping) sources of variability. Understanding ETTOs and the decision making processes that these shape, plays a crucial role in preventing undesired sources of variability. Trade-offs are at the core of every performance adjustment that people develop, aiming to match the perceived operating conditions. Therefore, ETTOs are both a response to, and a source of variability (Hollnagel, 2004).

FRAM is based on four basic principles:

- **Success and failure are equivalent** in the sense that they both emerge from performance variability.
- Variability becomes necessary as a way for people to **adjust** tools and procedures to match operating conditions.
- **Emergence** of either success or failure is not the direct result of variability within a given task or function, but rather to the unexpected combination of variability from multiple functions.
- The unexpected “amplified” effects of interactions between different sources of variability are at the origin of the phenomenon described by **functional resonance**.

The fundamental step in the use of this method is the identification and description of functions. Figure 3.2 illustrates the functional unit of a FRAM. Each function is defined by six descriptors (time, control, output, resource, precondition and input), as shown in Figure 3.2.

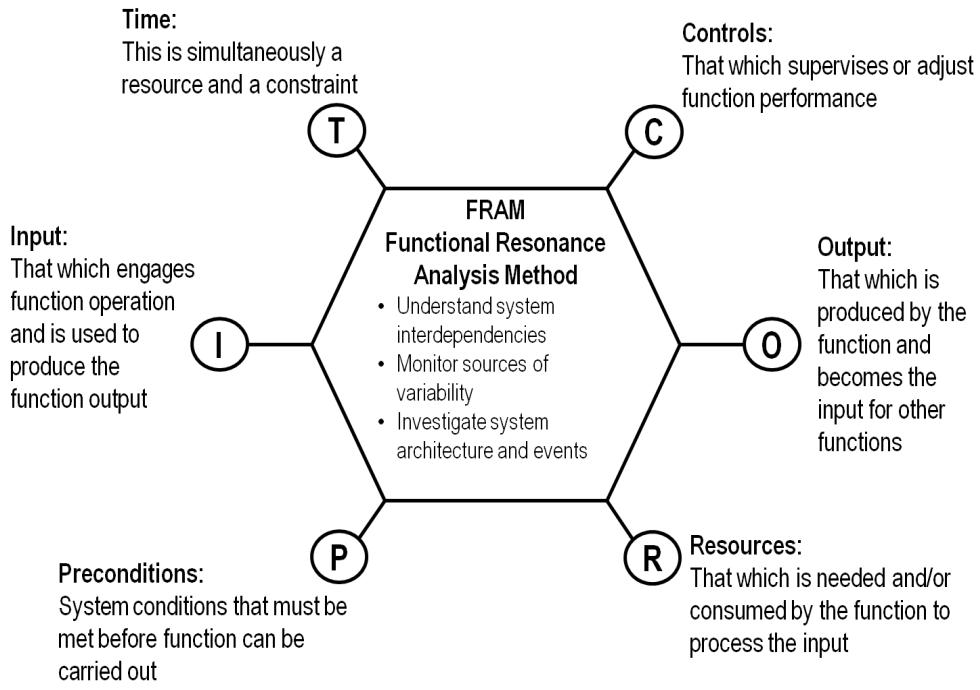

Figure 3.2: Functional unit of FRAM (adapted from Hollnagel, 2008)

Potential sources of variability are then investigated, guided by the identification of context dependent human, technological and organisational aspects. This can then support the assessment of system capacities to cope with variability in view of both expected and unexpected variability emerging from system operation.

The graphical representation of functions as hexagons becomes useful for the remaining steps of FRAM. Using the six aspects of functions (time, control, output, resource, precondition and input), system interactions are studied, aiming to identify potential sources of resonance. For instance, the output of a function may be the input, a precondition or even enforce a control aspect of another function in the system.

This process may also lead to the identification of possible dampening sources for undesired variability. As an example, if resources for a given function are rated as “more than necessary”, it could indicate the existence of a “spare capacity” that could operate as a damping barrier. The process of investigating possible connections between functions, for the identification of both potential undesired variability sources and barriers, is referred to as an instantiation of FRAM.

4 ASSESSING AND MEASURING RESILIENCE

The broadness of the resilience concept is implicit in its various definitions and can be perceived from the keywords mentioned in Table 3.1. Hence, resilience parameters or inferable criteria must be able to capture a great diversity of system features (Hollnagel, 2011a). Hollnagel *et al* (2006) and Jackson (2010) provide ample descriptions for resilience characteristics based on recognisable system aspects of system performance. In particular, Wreathall (2006) summarises characteristics for what could be considered a resilient system, and Hale & Heijer, (2006b) and Hale *et al* (2006) discuss possible topics for measuring and auditing resilience. These are shown in Table 4.1**Error! Reference source not found.** as characteristics for resilient and non resilient systems.

Table 4.1: Characteristics of resilient and non resilient systems (from Wreathall 2006, Hale & Heijer 2006b and Hale *et al* 2006)

Resilient system	Non resilient system
Top level commitment: Management recognises human performance concerns and tries to continuously and extensively address them	Defences erode under production pressures
Just culture: support on reporting of issues upwards through the organisation yet not adopting culpability attribution behaviours	Safety is not **built as inherently as possible into the system** and the way it operates by default
Learning culture: willingness to respond to events not with denial but through repair and reform	There is not a **high enough devotion to safety** above or alongside other system goals
Awareness: Data gathering that provides management with insights about various aspects of performance	There is a failure to revise risk assessments appropriately as **new evidence accumulates**
Preparedness: The organisation actively anticipates problems and prepares for them (constant sense of unease, Hollnagel & Woods 2006)	Past good performance is taken as a reason for future confidence about risk control (**complacency**)
Opacity: The organisation is aware of the boundaries and knows how close it is to the edge in terms of degraded defences and barriers	Fragmented problem solving clouds the big picture
Buffering capacity: Ability to adapt to new or complex problems without disrupting overall functionality. It requires that people are able to make decisions without having to wait on management instructions	The organisation responds **stiffly and slowly** to changing demands and is not able to cope with unexpected situations
Flexibility: Ability of the system to restructure itself in response to external changes or pressures	
Tolerance: how the system behaves near a boundary – slowly degrades or quickly collapses when pressure pushes performance towards depletion of adaptive capacities	**Breakdown at boundaries** impedes communication and coordination, which do not have sufficient richness and redundancy

As previously mentioned, by definition, a system is resilient if it is able to sustain adaptability capacities in view of continuously pursuing its purposes/intents. In terms of measurability, a fundamental distinction between resilience and safety (and most remaining risk domains) must be made, as while risk management "traditionally" resorts to metrics grounded on "external" reference values for a given level of risk exposure deemed acceptable, resilience metrics must be grounded on "internal" references for acceptable response to system purposes. Naturally, risk management is inherently embedded into system purposes and therefore, must be taken into account and integrated into any resilience assessment framework, but many other system aspects are equally meaningful

towards resilience and must also be taken into account and integrated with risk management towards resilience assessment. Empirical evidence (Nemeth & Hollnagel, 2014) shows that many such aspects are often actively managed within many organisations but lack any suitable form of integration and coordination.

As pointed out by Hollnagel & Woods (2006), resilience (like safety) is something that a system "does" rather than something that it "has". This observation highlights the emergence as well as the process nature of resilience. It is a characteristic of how a system performs through time, as opposed to a quality that, once acquired, remains (Hollnagel & Woods, 2006). This means that any means of measuring resilience must also be able to capture this dynamic nature of the concept through some integration over time. The concept of "drift into failure" (Dekker, 2004) clearly contemplates the dynamic nature of systems. However, as pointed out by Hollnagel & Woods (2006), the notion of safety boundaries is only metaphorical and thus, gaining perception of proximity or measuring a "distance" between operations and such limits becomes unrealistic.

Resilience cannot be measured by means of verifications such as the adherence to standards and rules. A measure of resilience must be in direct relation with how a system performs, and how capable it is in monitoring and controlling performance throughout a given period and in view of system purposes. In this sense, Hollnagel & Woods (2006) consider that only the potential for resilience can be measured and not resilience itself. Only the processes the system develops towards resilience can be assessed in time. Keeping in mind the notion of sustained adaptability, these processes relate to adaptability capabilities, which in view of assessing systems resilience, raises the following fundamental questions:

- What capabilities are needed?
- How much of such capabilities?
- Where and when are such capabilities needed?
- Capabilities of sustained adaptability towards what?

Despite the broadness of these questions and the fact that they are inevitably very context dependent, there are a number of principles that be deducted from them, which provide useful support towards the assessment of resilience:

- Adaptability is targeted at both expected and unexpected system variability. Therefore, **guidance as to what capabilities and how much is needed can be offered by foremost understanding and assessing the sources of operational variability in the system**. It should be noted that adaptability capabilities are simultaneously a "response" and a "source" to system variability. Whatever capability is produced to cope with a given type and/or amplitude of potentially critical system variability, will also be generating variability in the system.
- Capabilities for sustained adaptability require the allocation of resources. No system unit, function or organisational area or structure can by itself continuously allocate all types of resources and at the levels needed to produce the potentially needed adaptability capabilities. Resources are by nature finite and no system (or sub-system) is self-sufficient in the pursuit of its purposes, even more in the face of continuous and ever changing operational pressures. Systems develop interdependencies (within and beyond their boundaries) because these are the means through which such high diversity and often high level of resources can be secured. **Hence, capabilities for sustained adaptability are intrinsically related and reliant on system interdependencies and understanding the behaviour of such interdependencies constitutes a fundamental step towards understanding and assessing the sources system resilience, namely by looking at the type and levels of resources that interdependencies provide, and how and when these can be allocated**. It should be noted that while interdependencies are the means through which systems seek to secure resources, they also consume resources and are the means through which exposure to variability increases.

- Assessing the sources of resilience (or the potential for resilience) can be produced from the referencing of the types and levels of resources that a system can secure, how it is able to allocate them to capabilities for sustained adaptability, and **to what extent these capabilities match the actual observed and measured patterns of operational variability in the system**.

From the characteristics in Table 4.1, Hollnagel & Woods (2006) highlight three characteristics as fundamental capabilities of a resilient system. These characteristics are aligned with the three conditions of resilient situations approached by Westrum (2006a):

- Being **prepared** provides the ability to **avoid** something bad from happening.
- Being **flexible** becomes fundamental to ensure **survival** under varying conditions and degraded modes.
- Being **adaptive** supports quick **recovery** from disruptions and regain of desired performance.

Although this constitutes useful guidance towards measuring and monitoring resilience, as discussed by Westrum (2006a), it still raises a number of questions regarding how these capabilities should be embedded in the system in order for it to be considered a resilient one. For instance, the type of events that a system must be capable of avoiding, under what circumstances should it be flexible and how fast should it be capable of recovering, among others.

Within the literature sources consulted on the subject of resilience, several other proposals are put forward as potential sources of measurement. Sutcliffe & Vogus (2003) consider that resilience requires the presence of latent resources that can be activated or recombined as new situations and challenges arise. Therefore, measuring the amount of latent resources, whether this is time, financial, or technical resource, may be one approach to measuring resilience. This still raises questions regarding the amount of latent resources necessary to face each new different challenge. Widalvsky (2004) argues that resilience is the ability to be vitally prepared for adversity and that this requires improving overall capability in a wide range of areas such as investigation, learning and acting, even when not knowing what will be called to act upon. Vugrin *et al* (2010) consider that the measurement of system resilience involves two components. The first is a systemic impact which is defined as the difference between a targeted and an actual system performance, following a disruptive event. The second component is the total recovery effort, which stands for the amount of resources expended during recovery processes, following the given disruption.

4.1 Resilience related international programmes and guidelines

There is a wide range of programmes and approaches regarding resilience, like the National Cooperative Highway Research Program (NCHRP, 2014) for extreme weather conditions, Mega disasters like the Great East Japan Earthquake (Ranghieri & Ishiwatari, 2014), management of port-disaster environments and disaster recovery (Amdal & Swigart, 2010), the role of transit in Emergency Evacuation (Transportation Research Board of the National Academies, 2008) and protection and resiliency of the critical infrastructure and key resources (CIKR) (Chertoff, 2009).

At European level, resilience has gained more prominence in the domain of disaster management and response and the coordination of international efforts towards adaptation to climate change. At domestic level, the EU has developed the following actions on resilience:

- **EU Climate Adaptation Strategy:** Promoting action by member states towards building adaptation capacities, namely through guidance and funding. Promoting informed decision making and the sharing of information namely through the European Climate Change Platform. Promoting adaptation in sectors critically exposed to climate factors, namely the agriculture and fisheries.
- **Green paper on the insurance of natural and man-made disasters:** More appropriate coverage of disaster losses to minimise economic and fiscal impacts on stakeholders and member states.

- **EU Civil Protection Mechanism:** While responsibilities fall on member states, various previous events have shown that much can be improved in terms of disaster response through member state coordination and assistance. This mechanism provides the means to pool resources (i.e. expertise, intervention teams and other in-kind resources) to mitigate impacts of disasters and enhance recovery actions.
- **EU Emergency Response Coordination Centre:** It operates under the Humanitarian Aid and Civil Protection department (ECHO) and among others, supports the operation and deployment of the Civil Protection Mechanism. It bears the capacities to deal with various simultaneous emergency scenarios and across different regions. One of the focuses is the improvement of coordination amongst member states under emergency response scenarios, aiming to optimise the allocation and deployment of resources.

The EU maintains an involvement in international action, namely to support prevention and preparedness for crises across different world regions. In October 2012 the European Commission introduced the EU Approach to Resilience: Learning from Food Security Crises (European Commission 2012). While it mainly relates to food shortage problems in the Horn of Africa region, it addresses many resilience relevant aspects and is at the basis of the policy principles adopted by the EU for action on helping vulnerable communities in "crisis-prone" areas. Such actions are also placed in the scope of the Hyogo Framework for Action 2005-2015: Building the resilience of nations and communities to disasters. This Framework for Action addresses:

- Challenges posed by disasters
- The Yokohama Strategy: lessons learned and gaps identified
- World Conference on Disaster Reduction: Objectives, expected outcome and strategic goals
- Priorities for action 2005-2015
- Implementation and follow-up of actions under this scope

Within the scope of critical infrastructure protection and security, the EU has in recent years produced various efforts. Following guidelines emanating from the Green Paper on European Programme for Critical Infrastructure Protection (EPCIP, 2005) and reflected in the actual EPCIP of 2006, although all hazards should be addressed across all sub-sectors of CI, priority is set on terrorist threats and on the energy and transport sectors. Further details of the implementation of these policies are addressed by Directive 2008/114/EC (section 5.2.2). The targets established under this framework bear significant relevancy for resilience management. According to the guidelines and references provided and to the extent possible, the target should be set on making terrorism, natural disasters, accidents and any disruptions or manipulations of CI:

- brief
- infrequent
- manageable
- geographically isolated
- minimally detrimental to the welfare of the member states, their citizens and the EU

To achieve such goals, the EPCIP of 2006 established four main focus areas:

- A procedure for the identification and designation of ECI and for the assessment of further protection requirements (Directive 2008/114/EC).
- Measures designed to facilitate the implementation of EPCIP, including an Action Plan, the Critical Infrastructure Warning Information Network (CIWIN), the use of CIP expert groups at EU level, a CIP information-sharing process, and the identification and analysis of interdependencies.
- Funding of CIP related measures and projects focussing on "prevention, preparedness and consequence management of terrorism and other security related risks" for the period 2007-2013.

- The development of an EPCIP external dimension.

Based on international experience, most countries develop governmental plans for critical infrastructure protection in a number of human activity sectors. Examples include transportation (UK's Department for Transport, 2014), networks and computer systems (Smith et al, 2011), telecommunications (CPNI, 2006), industrial control (Wei & Ji, 2010), school environments (Rajamaki et al, 2012), sustainability and resilience of electric energy supply in urban environment (Karady & Zhang, 2011) and the demand of energy efficient environments for transport industries (Magniez & Vouters, 2013).

Many cities in different parts of the world have engaged in regional and community programmes targeting the enhancement of resilience in urban contexts. The "100 Resilient Cities" programme (www.100resilientcities.org) initiated by the Rockefeller Foundation provides a far reaching example of such programmes and under particularly broad scope that takes into account a wide range of risk domains (social, economic, environmental, among others). Many cities worldwide have already integrated this programme, namely Athens (Greece), Lisbon (Portugal), London (Great Britain), Melbourne (Australia), Milan (Italy), and Paris (France), among many others. The city of London has developed the London Resilience Partnership (London Resilience Forum, 2013) that aims to implement many of the principles and strategies emanating from this programme. Figure 4.1 shows a comprehensive illustration of the London Resilience strategy.

Figure 4.1: The London Resilience strategy (London Resilience Forum, 2013)

Approaches on critical infrastructures and key resources security start with plans aiming to define more clearly the warning systems (Belluck et al, 2007). The US **National Infrastructure Protection Plan** (NIPP, 2009) for example, identified three specific areas of interest: a. the interdependencies between sectors, b. cybersecurity and c. the international nature of threats to critical infrastructure. The Risk Management Framework (RMF) includes six steps from establishing security objectives to measuring effectiveness. On the other hand, the **European Program for Critical Infrastructure Protection** (EPCIP – described in 5.2.2) has a slightly different objective: to identify and designate European Critical Infrastructures, monitor improvement by the creation of boards, help to member states to protect critical national infrastructure and complementary financing procedures.

4.2 Resilience assessment tools

In most methodologies used for analysis of vulnerabilities in critical infrastructure systems (over 90%), software systems are used and include expert groups that handle system's security incidents like the **Computer Emergency Response Teams** (CERT) (Yusta et al, 2011). To name a few systems:

- Athena is a software tool for analysis of interdependent infrastructure networks, including political, military, economic and social aspects. Athena incorporates several sophisticated reasoning algorithms that allow us to study the dependence between nodes (Drabble et al, 2009).
- In CI^3, the key role of software is to estimate times and costs required to restore a part or the whole set of critical infrastructures in order to return to normality, after an operational interruption (Gillette et al, 2002).
- Following CI^3, a more advanced system called CIP/DSS came to allow the comparison of the effectiveness of strategies to reduce the probability of a risk, based upon the study of scenarios that represent the impacts. This model is taking into account the potentially affected infrastructure, the measures of impact and likelihood of an incident and it is designed in such a way to help analysts and policy makers to evaluate and select the most effective strategies in reducing risk (Bush et al, 2005).

There are other systems applicable to a wide range of sectors like the Fort Future (Usage et al, 2010) and also systems and methods focused on particular aspects of emergency situations like those dedicated to the frequently observed human social behaviours during emergency (Pan et al, 2007). This introduces another group of methods for crowd behaviour modelling in various **macroscopic** approaches that have been applied. Started by relying on crowd motion modelling based on some assumptions, more advanced models have been proposed to study fluid dynamics approaches to include position and velocity of a crowd (Helbing et al, 1992). Also, more up-to-date methods of studying panic effect on the crowd under critical situations have been proposed (Colombo and Rosini, 2005) and most modern approaches rely on simulation systems for crowd behaviour modelling taking into account an extended factor list which includes social and psychological factors (Yeh et al, 2008). Such a crowd behaviour model is used for novel building evacuation methods using mobile robots and other ICT technologies (Boukas et al, 2014). It is worth mentioning that quite often methods can be transferred to other sectors of resilience with slight changes. In Boukas work for example, robots can navigate pedestrians to uncongested gates in a covered rail station or airport sector.

On the other hand, there are individualised approaches (**microscopic** methods) relying on Agents. In those approaches, crowd behaviour is being seen as the result of the overall personal agent's existence. In microscopic methods, the space-time behaviour of individual pedestrians can be described by social force models and cellular automata models (Pelechano et al, 2008). In the work of Chenney et al (2004) **Cellular Automata** (CA) models defined space under study as a grid of cells with local states. Those states depend on a set of rules about behaviour description of the pedestrians. The work of Helbing et al (2000) is a typical example of microscopic method which uses Social Force Models as analogous to real forces (repulsive interaction, friction forces, dissipation and fluctuations). This model was successfully applied to pedestrian movement scenarios of the real world. But most of previous crowd behaviour descriptors may not be as visual convincing as wished. This was

overcome by Sung et al (2004) who have proposed a new approach to control the agent's behaviour in a crowd. With a situation-based control structure and limited agent behaviours, they achieved to let agents to enter new situations by composing additional situation-specific behaviours on the fly. The final result is a more appropriate agent responds as output of a probabilistic mechanism.

There is another '**mesoscopic** layer' approach in which combinations of methods try to save system and computational resources to make simulations by a hybrid combination of macroscopic and microscopic advantages. Such an effort is paid by MATSim (Oliveros & Nagel, 2013) which is a multi-agent transport simulation which uses many modules to cover different research areas and case studies. This approach takes advantage of both kinds of models, in which a microscopic model is applied where needed and a mesoscopic model where plausible.

Recent literature generally agrees to define simulation models for management dimensions, critical infrastructures and representation of operational aspects. Trucco et al (2011), having the severe earthquake and tsunami of March 2011 in Japan as a case study, demonstrated a process-oriented **Discrete-Event Simulation** (DES) model to represent operational aspects of the *Yamagata* airport. The results of the simulation-based analysis of the transport system resilience demonstrated the crucial role of air-side resources (e.g. availability of wide-body aircraft) for high daily passenger's throughput. Also, resilience concepts can be contextualized by adopting methodologies to understand dependencies and interactions between the different components of resilience (Mezzou et al, 2011) or parts of critical urban infrastructures, like the rail system, and identify the contribution of operational rail staff in degraded-mode operation (Hilton et al, 2012).

Other important aspects are the integration of diverse and separate systems or applied methods and the evaluation of resilience on critical infrastructure protection. In a holistic approach, there is the need to integrate infrastructures and processes among institutions, cooperate and undertake common administrative actions. Mugavero et al (2012) proposed to apply high methodological and technological standards in all phases of the emergency. In particular, they emphasise on institutional, geographical, technological and operational connectivity towards a homogeneous and collaborative environment.

As of the assessment issues, we need to develop models able to identify and compare the resilience of emergency institutions. Ni et al (2009) provided such a quantitative assessment model and the proposed model was evaluated on simulated scenarios. The **Climate Resilience Evaluation & Awareness Tool** (CREAT) is another example of a climate risk assessment tool for water utilities (EPA, 2012). The study of Freckleton et al, (2012) is standing from a higher level to study the infrastructure resiliency related to transportation networks in particular, by using well defined metrics and by applying a fuzzy inference approach to calculate the total network resiliency.

Overall, although ambiguities in definitions and central terminology may arise some criticism on continued investigation of risk and protective processes (Luthar et al, 2007), infrastructure protection modelling is a relatively new area of research which can propel actions to provide and maintain an acceptable level of service in a wide range of public services and to face faults caused by territory incidents or large scale natural disasters back to normal operation.

4.2.1 The Resilience Analysis Grid (RAG)

More recently, Hollnagel (2011a) proposes four main capabilities ("four cornerstones of resilience"), which derive from the definition given in Table 3.1:

- **Knowing what to do** corresponds to the ability to address the "**actual**" and respond to regular or irregular disruptions by adjusting function to existing conditions.

- **Knowing what to look for** corresponds to the ability to address the "**critical**" by monitoring both the system and the environment for what could become a threat in the immediate time frame.
- **Knowing what to expect** corresponds to the ability to address the "**potential**" longer term threats, anticipate opportunities for changes in the system and identify sources of disruption and pressure and their consequences for system operations.
- **Knowing what has happened** corresponds to the ability to address the "**factual**" by learning from experiences of both successes and failures.

If by definition these four cornerstones characterise a resilient system then the scope of resilience engineering is to develop and manage the corresponding capabilities in the system. Based on these four capabilities, Hollnagel (2011b) proposes a Resilience Analysis Grid (RAG) as a way to manage resilience in system. An example of a RAG is shown in Figure 4.2.

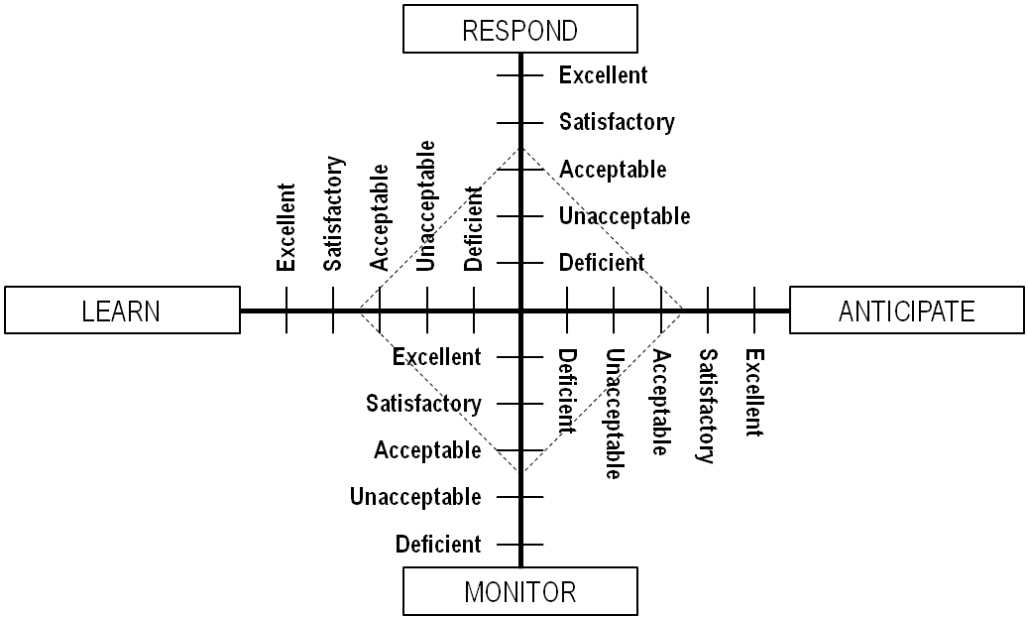

Figure 4.2: Example of a Resilience Analysis Grid - RAG (adapted from Hollnagel, 2011b)

The management of resilience should be based on a balance between the four capabilities, as shown in Figure 4.2. This does not imply that all four capabilities should exist in the same proportion. As mentioned by Hollnagel (2011b), while for systems like a fire brigade, the ability to respond to the actual may be more important than to consider the potential, for others such as sales organisation, the ability to anticipate may be just as important as responding.

4.2.2 Matrix for resilience metrics

While the RAG may provide a more comprehensive perspective on resilience, it remains a qualitative approach to the concept. Linkov et al (2013) proposes an approach to a quantified assessment of resilience based on similar system capabilities:

- **Plan/Prepare**: Lay the foundation to keep services available and assets functioning during a disruptive event (malfunction or attack).
- **Absorb**: Maintain most critical asset function and service availability while repelling or isolating the disruption.
- **Recover**: Restore all asset function and service availability to their pre-event functionality.

- **Adapt**: Using knowledge from the event, alter protocol, configuration of the system, personnel training, or other aspects to become more resilient

Linkov et al (2013) further combines these capabilities with four domains for shared situational awareness and inform decentralised decision-making, in order to produce a matrix for resilience metrics:

- The **Physical** resources and capabilities, and the design of those resources
- The **Information** and its development regarding the physical domain
- The **Cognitive** use of information and the physical domains to make decisions
- The organisational (**Social)** structure and communication channels for making decisions

4.2.3 The mean-reverting stochastic model

Limma and Medda (2015), worked on the resilience with focus on the definition of Pimm (1991), according to which resilience in "how fast a variable that has been displaced from equilibrium returns to it", applying a mean-reverting stochastic model to study the diffusive effects of shocks and applying this model to the London Underground. They focused on quantifying methods of resilience in their approach. In this framework a system is more or less resilient depending on whether it recovers rapidly or slowly from disruptive events or shocks. The temporal dimension of resilience is very important and conspicuously represented in the National Academy of Sciences definition as the ability to *"…to plan and prepare for, absorb, respond to and recover from disasters and adapt to new conditions*". This contribution offers a very promising theoretical framework towards continuous time resilience evaluation. The mean reversion rate captures the rate of recovery of the system after being subjected to random shocks and provides a measure of resilience.

The proposed measure of resilience is defined as the mean-reverting parameter in a specified stochastic mean-reverting model. This parameter captures the rate of recovery of the system after it is subjected to random shocks. The proposed model can capture the behaviour of a wide range of systems, from low to high volatility (the up-and-down variation from the equilibrium value) and from low to high mean reversion (the speed with which a system recovers from a shock). Including jump processes in the model would enable it to capture the response of the system to sharp Poisson shocks, thus capturing the behaviour of the system under acute disruptions. Therefore a mean-reversion model with jumps, once implemented, would provide a powerful predictive tool to assess the resilience of systems.

Authors' examined the case of the London Underground transport system and they found out that the model could be useful to assess the resilience of the Underground lines to shocks. One could obtain a comparative study of all Underground Lines, and ascertain which lines are more or less resilient. Further using the mean-reversion model with jumps, one could also study how resilient a particular Underground line is to small shocks versus large shocks. These studies could assist in making investment decisions on improvements to the Underground Lines or similar application examples.

Shocks in the case of London Underground services can be delays or disruption which affects the passenger counts also in other lines. The model is fitted to the passenger counts time series. The basic behaviour of the system is captured by the 4 scenarios in Table 4.2.

Table 4.2: 4 scenarios for system behaviour

		Volatility	
		High	Low
Recovery Rate	High	Scenario 1	Scenario 2
	Low	Scenario 3	Scenario 4

Scenario 1 is deceptively stable, because in case of major shock will not recover quickly. In scenario 2 the system is highly resilient. In scenario 3 the system displays low resilience and unpredictable behaviour. In scenario 4 the system is predictable and resilient. The basic model is augmented to accommodate large shocks including Poisson Processes and to provide a more realistic representation of the passenger counts processes.

Authors assumed that the state of the system can be measured by some quantifiable quantity that exhibits stochastic behaviour. The shocks that disrupt the functioning of the system are assumed to be random in nature, and the disruption caused by the shock in the next time interval has a Gaussian distribution with variance equal to the square root of the length of the interval.

4.2.4 The climate resilience toolkit

The U.S. climate resilience toolkit (https://toolkit.climate.gov/) has been developed to avail and help managing climate- related risks and opportunities and to help in building resilience to extreme events.

The tools are mainly related to coastal flood risk, ecosystem vulnerability, trival nations, energy and supply and use, human health, water resources, food resilience, transportation and supply chain. These tools apart from the topic that they focus on could be categorized based on their functionality. Therefore, there are tools for planning, risk assessment, mapping/graphics, analysis, scenario development, stakeholder engagement, recovery and rebuilding, climate projections.

4.2.5 The Hazus-MH

Hazus-MH is a standardized methodology developed by the Federal Emergency Management Agency (FEMA). This software package provides users access to FEMA's models for estimating potential losses from earthquakes, floods, and hurricanes. **Hazus-MH** uses the Geographic Information Systems (GIS) to estimate physical, economic, and social impacts of disasters. It illustrates graphically the limits of identified high-risk locations due to earthquake, hurricane, and floods. Users can visualize the spatial relationships between populations and other, more permanently fixed geographic assets or resources for the specific hazard being modelled, a crucial function in the pre-disaster planning process.

4.2.6 Vulnerability Assessment Scoring Tool (VAST)

The U.S. Department of Transportation developed the Vulnerability Assessment Scoring Tool (VAST) to help state departments of transportation, metropolitan planning organisations, and other organisations implement an indicator-based vulnerability assessment of their transportation assets. Vulnerability is a function of exposure, sensitivity, and adaptive capacity. Certain characteristics of transportation assets can serve as indicators of their exposure, sensitivity, or adaptive capacity.

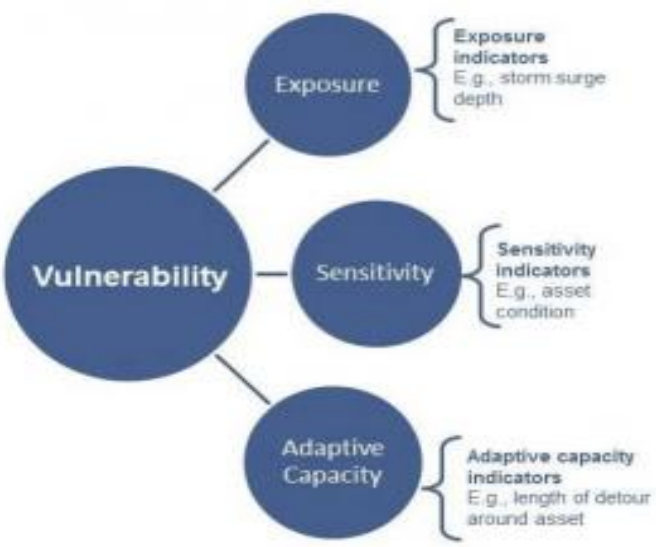

Figure 4.3: Components and examples of vulnerability for transportation assets.

Asset types covered in this tool are (1) rail, (2) ports and waterways, (3) airports and heliports, (4) oil and gas pipelines, (5) bridges, and (6) roads and highways.

Climate stressors covered in this tool are (1) increased temperature and extreme heat, (2) precipitation-driven inland flooding, (3) sea level rise/extreme high tides, (4) storm surge, (5) wind, (6) drought, (7) dust storms, (8) wildfires, (9) winter storms, (10) changes in freeze/thaw, and (11) permafrost thaw.

VAST enables users to document the vulnerability of transportation assets in a study area. The assessment includes (1) determining the scope of the vulnerability assessment, (2) selecting appropriate indicators, (3) collecting data about those indicators, and (4) devising an approach to convert raw data about indicators into scores. The result is a set of vulnerability scores that can be used to rank assets by vulnerability or inform other analyses of the results.

This assessment enables better prioritization in the course of transportation planning and more effective adaptation measures.

4.2.7 Hawai's Tsunami Hazard Information Service

Hawai'i Tsunami Hazard Information Service enables users to access tsunami evacuation maps and other information on how to prepare and what to do if a tsunami occurs. The tool provides online access to tsunami evacuation zone maps, along with information about potential risks, how to prepare, and what to do in the event of a tsunami.

4.2.8 Integrated Rapid Visual Screening for Tunnels

This tool helps users determine the initial or relative risk and resilience of tunnels to a range of hazards, including natural hazards such as fire and floods. Integrated Rapid Visual Screening (IRVS) for Tunnels is a software-facilitated procedure for assessing the risk to tunnels from natural and human-caused hazards that have the potential to cause catastrophic losses. Completing the IRVS procedure for a tunnel results in a quantifiable assessment of the risk of a given tunnel to a terrorist attack or natural disaster leading to catastrophic losses (fatalities, injuries, damage, or business interruption) and a quantifiable assessment of the resiliency of the tunnel (ability to recover from such an event). Risk is determined by evaluating key building characteristics for consequences, threats, and vulnerabilities. A tunnel is defined as a passageway through or under an obstruction,

such as a city, mountain, river, or harbour. Assessment is based on features that can be observed during a visual inspection. The knowledge for calculating both risk and resilience is embedded in the tool.

For natural hazards, the tool uses probability of occurrence to calculate risk. Risk is a product of consequences multiplied by threats multiplied by vulnerabilities. Resilience is computed from a combination of robustness, resourcefulness, and recovery factors based on information such as hardening, training, and redundancies.

4.2.9 Wave Exposure Model

The wave exposure model tool is used to quantify wave energy and its effects on ecosystem functions. Understanding the hydrodynamics of the coast, especially the waves associated with storms, is essential to managing the fragile coastal environment. The Wave Exposure Model (WEMo) features are:

- Forecasts and "hindcasts" wind wave energy and the movement of seafloor sediment in enclosed water bodies such as lakes, coastal bays, and estuaries
- Provides a foundation for studying or modelling restoration efforts, seafloor and shoreline erosion, and the tolerance limits of habitats
- Works well with standard data formats and factors such as shoreline erosion, fauna, and landscape patterns
- Guides the classification of wave data into wave energy patterns useful for choosing sampling regimes
- Adjusts to wind events that are chronic, extreme, or combined with storm surge
- Adapts for use by non-specialists in hydrodynamics
- Requires basic knowledge of geographic information systems

4.2.10 Climate Resilience Evaluation & Awareness Tool (CREAT)

Owners and operators of drinking water and wastewater utilities can use this downloadable tool to assess potential climate change threats and evaluate adaption options at their sites. CREAT provides access to the most recent national assessment of climate change impacts and helps utility operators consider how events such as sea level rise, shifting precipitation patterns, temperature changes, and extreme weather may impact their operations. CREAT gives utilities a way to evaluate potential impacts to their assets using both traditional risk assessment and scenario-based decision making. The tool also provides data and plots for comparing local historical conditions with downscaled climate model projections for the future. CREAT helps users identify threats based on regional differences in climate change projections and designing adaptation plans based on the types of threats being considered. Following assessment, CREAT provides a series of risk reduction and cost reports that enable the user to evaluate various adaptation options as part of long-term planning.

4.2.11 Environmental Sensitivity Index

This tool offers access maps to check the sensitivity of coastal resources to oil spills. Environmental Sensitivity Index (ESI) maps provide a concise summary of coastal resources that are at risk if an oil spill occurs nearby. Examples of at-risk resources include biological resources (such as birds and shellfish beds), sensitive shorelines (such as marshes and tidal flats), and human-use resources (such as public beaches and parks). When an oil spill occurs, ESI maps can help responders meet one of the main response objectives: reducing the environmental consequences of the spill and the cleanup efforts.

4.2.12 Extreme Water Levels

View probability statistics on the likelihood that coastal water levels at select stations will rise above or fall below a given elevation.

Extremely high or low water levels at coastal locations are an important public concern and a factor in coastal hazard assessment, navigational safety, and ecosystem management. Exceedance probability, the likelihood that water levels will exceed a given elevation, is based on a statistical analysis of historic values. This interactive map provides annual and monthly exceedance probability levels for select NOAA Centre for Operational Oceanographic Products and Services (CO-OPS) water level stations with at least 30 years of data. When used in conjunction with real-time station data, exceedance probability levels can be used to evaluate current conditions and determine whether a rare event is occurring. This information may also be instrumental in planning for the possibility of dangerously high or low water events at a local level. Because these levels are station-specific, their use for evaluating surrounding areas may be limited.

4.2.13 Geothermal Prospector

This tool is used to explore map layers—such as geothermal potential, energy infrastructure, and leasing/ownership information—to determine locations that may be favourable for geothermal energy development. The Geothermal Prospector is an interactive map for exploring potential geothermal energy resources by location. The tool gives users a way to visualize relevant environmental, geothermal, infrastructure, and legal/policy data layers to determine locations that may be favourable for geothermal energy development.

4.2.14 HURREVAC

This tool is a storm tracking and decision support tool developed to help with making prudent decisions regarding the timing and extent of evacuations. HURREVAC (***Hurr***icane ***Evac***uation) is a storm tracking and decision support tool which combines live feeds of tropical cyclone forecast information with data from various state Hurricane Evacuation Studies to assist the local emergency manager in determining the most prudent evacuation decision time and the potential for significant storm effects, such as wind and storm surge. HURREVAC tracks hurricanes using the National Hurricane Centre's Forecast Advisories. The software translates forecast track and wind extent information from the National Hurricane Centre's text-based products into interactive maps and reports that are used to chart the progress of an advancing storm. The tool also assembles rainfall, flood, tide, and river forecast information from various sources to assist users in evaluating inland flooding threats.

4.2.15 Integrated Rapid Visual Screening for Buildings

This tool helps users compile a preliminary assessment of the relative risk and resilience of 15 types of buildings to 20 hazardous events, including natural hazards such as floods and wind. Integrated Rapid Visual Screening (IRVS) for Buildings is a software-facilitated procedure for assessing the risk to buildings from natural and human-caused hazards that have the potential to cause catastrophic losses. Completing the IRVS procedure results in a preliminary risk assessment rating for the facility of interest. Risk is determined by evaluating key building characteristics for consequences, threats, and vulnerabilities. The procedure is intended to be used to identify the level of risk for a single building, to identify the relative risk among buildings in a community or region, and to set priorities for further risk management activities. Information from the visual inspection can be used to support higher-level assessments and mitigation options by experts.

The IRVS for Buildings categorizes 15 building types and addresses 20 hazardous events: internal (intrusion, blast, and chemical, biological, and radiological releases or CBR); external blast and external CBR releases from 100, 300, and 1,000 feet; earthquakes (ground shaking and ground failure); floods (still water and velocity surge); wind (hurricane, tornado, and other wind events); landslide (rainfall and earthquakes); and fire (resulting from

earthquakes, blast, or arson). The knowledge for calculating both risk and resilience is embedded in the tool. Major tool interactions are automatically calculated by pre-assigned weights, interaction logic, and context-based algorithms based on knowledge and tool validations. Risk is based primarily in target attractiveness (for man-made hazards).

For natural hazards, the tool uses probability of occurrence to calculate risk. Risk is a product of consequences multiplied by threats multiplied by vulnerabilities. Resilience is computed from a combination of robustness, resourcefulness, and recovery factors based on information such as hardening, training, and redundancies. Information obtained from the IRVS analysis can be used by law enforcement agencies, emergency managers, facility managers, engineers, and architects to support higher-level assessments and mitigation measures.

The IRVS family of tools includes integrated capabilities for assessing mass transit, tunnels, and buildings in one software package.

5 LEGISLATION AND STANDARDS

Risk management is influenced by a great variety of legal and standardisation documents. Even when addressing specific risk domains such as safety or security, empirical evidence and literature show that a growing number of knowledge domains and expertise are into play at various managerial and operational levels. Risk management currently relies on a wide range of national and international institutions and mechanisms. For many decades and within the majority of member states, security issues extending beyond the restrict domain of public safety were mainly handled and managed by national armed forces. Within recent years, not only terrorist threats have become an increasing domestic concern, but also natural and industrial disasters in various regions of the world have highlighted the need for substantial improvements in terms of emergency response and protection of critical infrastructures and the public in general. This appears to have initiated a more or less general tendency for nations to seek delegating and integrating risk management related responsibilities onto civil institutions, namely those falling within the scope of critical infrastructures. The current legal framework in most member states reflects this trend, despite some differences in the way national institutions and resources are allocated. The use of a common approach is evidently intentional and can be partly considered the outcome of the recent legislative efforts undertaken by the European Commission, particularly since the launching of the European Programme for Critical Infrastructure Protection (EPCIP) in 2006.

5.1 Concepts and definitions

This section introduces the key concepts and definitions, in order to adequately set the framework of the ongoing study. The notions provided reflect as much as possible those emanating from legal and official documents, while adding any information deemed relevant.

5.1.1 Critical infrastructure and European Critical Infrastructure

The concept of Critical Infrastructure (CI) defines an asset, system or part that is deemed essential for the provision and maintenance of vital societal functions, such as health care, safety, security and any other economic and social element for the well-being of people. A European CI (ECI) is therefore, considered a CI, the disruption or destruction of which would affect at least two member states.

5.1.2 Sensitive critical infrastructure protection related information

This relates to any facts on CI, which if disclosed, could be used to plan and act with a view to causing disruption or destruction of CI installations.

5.1.3 Stakeholder

This expression designates a person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity. In practical terms, unless demonstrated otherwise through proper assessment, this includes every person, organisation or part of one, that is involved in transport supply chains, or that in some way plays a role in the production or delivery of the transport service in question.

5.1.4 Vulnerability

A characteristic of an element of the critical infrastructure's design, implementation, or operation that renders it susceptible to destruction or incapacitation by a threat.

5.1.5 Threat

Any indication, circumstance, or event with the potential to disrupt or destroy critical infrastructure, or any element thereof. An all-hazards approach to threat includes accidents, natural hazards as well as deliberate attacks. It can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to critical assets.

5.1.6 Risk

The possibility of loss, damage or injury. The level of risk is a condition of two factors: (1) the value placed on the asset by its owner/operator and the impact of loss or change to the asset, and (2) the likelihood that a specific vulnerability will be exploited by a particular threat.

5.1.7 Protection

All activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralise a threat, risk or vulnerability

5.1.8 Security and security measure

Security can be defined as the resistance to intentional, unauthorised acts designed to cause harm or damage. It is basically the opposition to threats. A security measure constitutes therefore, any action, mechanism, device, program or policy that reduces the likelihood of such acts, mainly by minimising the severity of a threat.

5.1.9 Response

Activities that address the short-term direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into nature and source of the threat; ongoing public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at pre-empting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice.

5.1.10 Interdependency

This concept has become widely used on many domains and with various purposes. Some literature distinguishes between dependency and interdependency, where the first would be a unilateral/one-way relation and the later would define a bilateral/two-way relation. Such a distinction was considered of little use for the scope of this study, as relations between systems tend to occur at many different organisational levels and assume equally diverse natures and purposes. Hence, within a given interdependency between two systems, many types of relations (on one given direction or the other) are likely to be developed at any given time and location.

Interdependencies can be characterised according to their nature, as spatial or functional ones. While functional interdependencies relate to the fulfilment of operational and management needs, spatial interdependencies are based on geographical proximity of infrastructures or facilities

5.2 European Directives

A great diversity of EU legislation addresses resilience related issues, even if not explicitly or directly focusing on this domain. The Directive Seveso (named after the major industrial accident that took place in this Italian city in 1976) constitutes an important reference, as it targets industrial safety within a broad scope of risk management,

much beyond purely occupational, technical or procedural aspects of safety. To some extent, social, economic and environmental impacts of major industrial disasters are taken into account by this directive, which renders it a relevant reference when discussing resilience in critical infrastructures. It is not applicable to some high risk activities which fall under specific legislation and international agreements, such as the nuclear industry or the transport of dangerous goods.

Directive 2008-114-CE provided the initial legal framework for the European Programme on Protection of Critical Infrastructures (EPCIP). It focuses on security issues, whilst aiming to introduce an equally broad scope of risk management.

While many other aspects and risk domains must be taken into account when addressing resilience in complex sociotechnical systems, these Directives provide an important framework on two key risk domains (safety and security) and on which RESOLUTE solutions will have to be embedded.

5.2.1 The Seveso Directive

The Seveso Directive aims at the prevention of major accidents involving dangerous substances. However, as accidents may nevertheless occur, it also aims at limiting the consequences of such accidents not only for human health but also for the environment.

The first issue of the Seveso Directive (Directive 82/501/EEC) emanated from the industrial accident in Italy that resulted in large scale and serious chemical exposure of populations. This was then perceived as the consequence of growing scale and complexity of hazardous industrial facilities, under equally growing production pressures. The real repercussions of complexity where yet very poorly perceived. In view of the lessons from later accidents such as Bhopal, Toulouse or Enschede gave way to Seveso-II (Directive 96/82/EC). Seveso-III (Directive 2012/18/EU) issued in 2012 takes on a much deeper understanding of system interdependencies and need for coordinated management and action in risk management. To some extent, Seveso-III starts to bridge the gap between risk management, business continuity and sustainability, acknowledging the criticality of such issues. It currently encompasses a large diversity of industrial facilities (applicable to more than 10 000 industrial establishments in the European Union) and recognises that industrial accidents are not admissible in view of their serious economic, social and environmental impacts and it increases the rights for citizens to access information and justice.

In general terms, under this Directive, operators are obliged to increase the sharing of information regarding concerned industrial establishments and activities, mainly under the form of control of substances and dangerous goods, production of emergencies and response plans taking into account both the industrial facilities and surrounding populations, and the clear attribution of responsibilities and accountability.

5.2.2 Directive 2008-114-CE (EPCIP)

While there is certainly a great diversity of legal references with more or less relevancy for resilience in critical infrastructures, the Council Directive 2008-114-CE clearly constitutes an important legal reference in this domain. It is the first step on a multilevel approach towards improved security of European critical infrastructures, as envisaged in the 2006 European Programme on Critical Infrastructures Protection (EPCIP). The Directive focuses on establishing a common approach for the identification and heightened protection of ECIs, building on already existing resources and mechanisms within each member state. The integration of Directive 2008-114-CE into national legal framework is believed to have led to the adoption of the following common principles:

- Consolidation of responsibilities and increased coordination capabilities, namely around national institutions in charge of civil protection.

- Creation of national committees for the implementation of national CIPs programmes, gathering representatives from industries, and any other public and private stakeholders (the designation of stakeholders will elaborated later in this document).
- Identification of infrastructures fitting the criteria for designation as European critical infrastructure, particularly by distinguishing such infrastructures from those that may be classified as critical at national level.
- Identification and assessment of vulnerabilities and threats, aiming to determine risk levels.
- Identification of additional protection requirements and deployment of appropriate measures in coordination with potentially affected member states.

Directive 2008-114-CE further recognises that such endeavour cannot be accomplished without substantial improvements on the means of communication and coordination, both at member state level and EU level. To this end, the nomination of ECIP contact points is foreseen, through which all matters related to national, bilateral and multilateral coordination should be addressed. The Directive makes an important distinction between national and European critical infrastructures. It defines a European Critical Infrastructure (ECI) as a critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. By doing so, the Directive establishes the boundaries of its action and of the responsibilities of the EU on this domain. Hence, one of the foremost targets of the Directive is the undertaking of an inventory of ECI and its distinction from what could be considered national level critical infrastructures. As noted in a European Commission Staff Working Document on a new approach to the EPCIP (European Commission, 2013), progress in this domain has been relatively feeble and highlights the need for enhanced coordination mechanisms, bridging gaps between sectors, stakeholders and member states.

Evidence suggests that there are many discrepancies amongst member states in terms of the extent to which these principles have been put into practice. While legal and organisational requirements may have been implemented, the coordination between stakeholders at national level remains challenging in many cases, which renders the process of assessment and EU level coordination significantly unaccomplished. As reported by the Commission Staff Working Document of 28.08.2013 (European Commission, 2013), less than 20 ECI have been designated and consequently, very few new Operator Security Plans have been produced. Some clear critical infrastructures of European dimension, such as main energy transmission networks, are not included. Despite having helped foster European cooperation in the CIP process, the Directive has mainly encouraged bilateral engagement of Member States instead of a real European forum for cooperation. Such challenges are clearly within the frame of RESOLUTE and the development and implementation of the European Resilience Management Guidelines (ERMG).

5.3 International standards

Standards have developed an increasing role as a complement to legislation in many different domains. Often they become an extension of the law (sometimes formally recognised as such) that offers organisations a procedure or technical approach towards legal compliance. Within the domain of security, despite their usefulness as organisational guidance and support towards improved risk assessment and protection, it has produced relatively small contribution in meeting EPCIP targets. The causes for this appear to be routed in the fact that actions taken on the basis of certification are mainly internal to organisations, whilst the EPCIP focuses mainly on external relations between organisations. The implementation of some standards like the ISO 28000, because it is based on a supply chain framework, it requires a certain amount of work directed at the organisational operating environment. However, actions taken are mostly reflected within the boundaries of the organisation seeking certification. Nevertheless, as recognised by the Commission Staff Working Document of 28.08.2013 (new approach to the European Programme for Critical Infrastructure Protection), a systems based approach, rather than a sectoral and organisational based one, seem to more appropriate to the goals set for the

EPCIP. Keeping this mind, it becomes readily apparent that a supply chain framework may bring security management closer to the envisaged EPCIP targets. The following sections provide a summarised description of the main standardisation references in the domain of security. Table 5.1 provides an overview of existing standards and ongoing projects under relevant topics.

Table 5.1: Standards and ongoing projects under resilience related topics (from www.iso.org on 07-08-2015)

Standard and/or project	Technical Committee
IWA 9:2011 Framework for managing sustainable development in business districts	ISO/TMBG
ISO/CD Guide 73 Risk management -- Vocabulary	ISO/TC 262
ISO Guide 73:2009 Risk management -- Vocabulary	ISO/TC 262
ISO/CD 11000 Collaborative business relationship management -- Framework	ISO/PC 286
ISO/IEC TS 17021-6:2014 Conformity assessment -- Requirements for bodies providing audit and certification of management systems -- Part 6: Competence requirements for auditing and certification of business continuity management systems	ISO/CASCO
ISO 19600:2014 Compliance management systems -- Guidelines	ISO/TMBG
ISO 20121:2012 Event sustainability management systems -- Requirements with guidance for use	ISO/TMBG
ISO/CD 20700 Management consultancy	ISO/PC 280
ISO/CD 21504 Guidance on programme management	ISO/TC 258
ISO 21504:2015 Project, programme and portfolio management -- Guidance on portfolio management	ISO/TC 258
ISO 22300:2012 Societal security -- Terminology	ISO/TC 292
ISO 22301:2012 Societal security -- Business continuity management systems --- Requirements	ISO/TC 292
ISO 22311:2012 Societal security -- Video-surveillance -- Export interoperability	ISO/TC 292
ISO/TR 22312:2011 Societal security -- Technological capabilities	ISO/TC 292
ISO 22313:2012	ISO/TC 292

Societal security -- Business continuity management systems -- Guidance	
ISO 22315:2014 Societal security -- Mass evacuation -- Guidelines for planning	ISO/TC 292
ISO/CD 22316 Societal security -- Organisational resilience -- Principles and guidelines	ISO/TC 292
ISO/TS 22317 Societal security -- Business continuity management systems -- Guidelines for business impact analysis (BIA)	ISO/TC 292
ISO/PRF TS 22318 Societal security -- Business continuity management systems -- Guidelines for supply chain continuity	ISO/TC 292
ISO/CD 22319 Societal security -- Guidance for involving volunteers in the response to major incidents	ISO/TC 292
ISO 22320:2011 Societal security -- Emergency management -- Requirements for incident response	ISO/TC 292
ISO/AWI 22320 Societal security -- Emergency management -- Requirements for incident response	ISO/TC 292
ISO 22322:2015 Societal security -- Emergency management -- Guidelines for public warning	ISO/TC 292
ISO 22324:2015 Societal security -- Emergency management -- Guidelines for colour-coded alerts	ISO/TC 292
ISO/DIS 22325 Societal security -- Emergency management -- Guidelines for emergency management capability assessment	ISO/TC 292
ISO/TR 22351 Societal security -- Emergency management -- Message structure for exchange of information	ISO/TC 292
ISO 22397:2014 Societal security -- Guidelines for establishing partnering arrangements	ISO/TC 292
ISO 22398:2013 Societal security -- Guidelines for exercises	ISO/TC 292
ISO 25639-1:2008 Exhibitions, shows, fairs and conventions -- Part 1: Vocabulary	ISO/TMBG
ISO 25639-2:2008 Exhibitions, shows, fairs and conventions -- Part 2: Measurement procedures for statistical purposes	ISO/TMBG
ISO 26000:2010 Guidance on social responsibility	ISO/TMBG

ISO/CD 31000 Risk management -- Principles and guidelines	ISO/TC 262
ISO 31000:2009 Risk management -- Principles and guidelines	ISO/TC 262
ISO/TR 31004:2013 Risk management -- Guidance for the implementation of ISO 31000	ISO/TC 262
IEC 31010:2009 Risk management -- Risk assessment techniques	ISO/TC 262
ISO/NP 31020 Risk Management -- Managing Disruption Related Risk	ISO/TC 262
ISO/DIS 34001.3 Security management system -- Fraud countermeasures and controls	ISO/TC 292
ISO/CD 37001 Anti-bribery management systems	ISO/PC 278
ISO 55000:2014 Asset management -- Overview, principles and terminology	ISO/TC 251
ISO 55001:2014 Asset management -- Management systems -- Requirements	ISO/TC 251
ISO 55002:2014 Asset management -- Management systems -- Guidelines for the application of ISO 55001	ISO/TC 251

5.3.1 ISO 28000: Specification for security management systems for the supply chain

This international standard recognises foremost that internal security cannot be achieved within some action aimed at the operational environment of a given organisation. It defines as a boundary for the actions to be taken the supply chain of the organisation, which may lead to useful insight on existing interdependencies, even if limited to a linear perspective of supplier-customer relationships. ISO 28000 proposes a high level management system encompassing supply chain stakeholders under a principle of mutual cooperation towards heightened security of products and services flows. The proposed management system is illustrated in Figure 5.1.

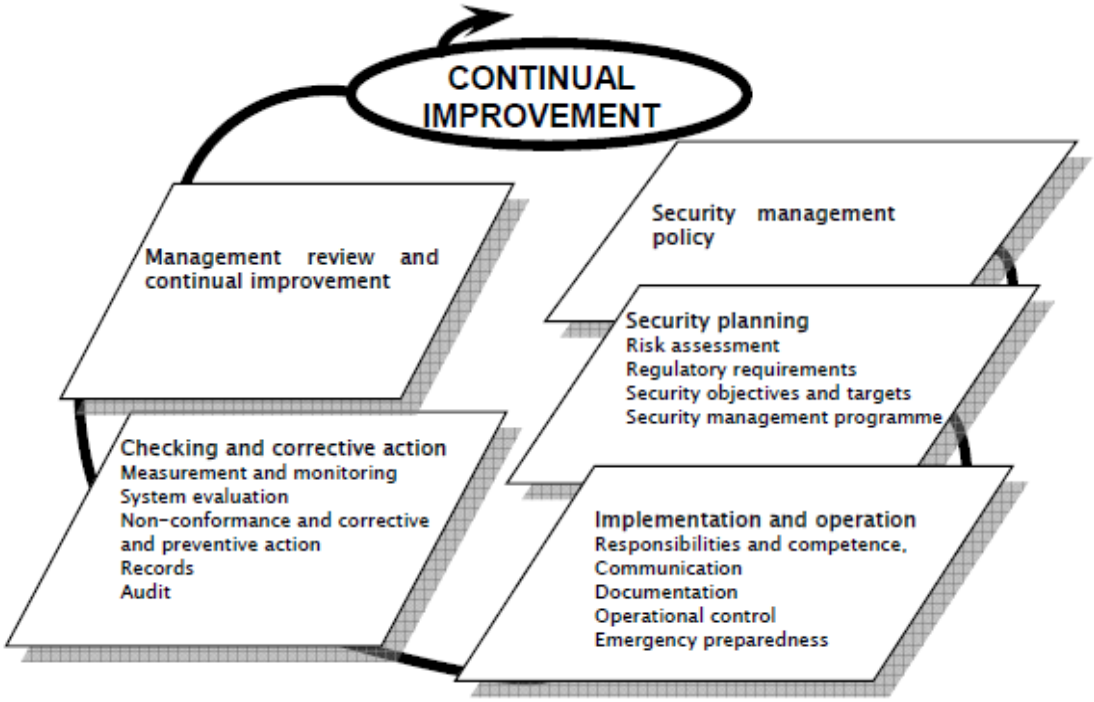

Figure 5.1: Security management system elements (in ISO 28000)

5.3.2 ISO 28001: Best practices custody in supply chain security

This standard is aligned with the framework and process introduced by ISO 28000. It is intended as an additional support in assessing the security measures in place throughout supply chains. The standard proposes the following two stages in carrying out this assessment:

- Identification of vulnerabilities and threat scenarios.
- Determine the likelihood of such scenarios being exploited by persons, and leading to security incidents.

As such, ISO 28001 is proposed as support for various auditing purposes, whilst bearing in mind the need to complement compliance with existing legal and regulatory requirements, rather than duplicating them. As stated in the standard's documentation, the expected outputs are:

- A Statement of Coverage that defines the boundaries of the supply chain that is covered by the security plan.
- A Security Assessment that documents the vulnerabilities of the supply chain to defined security threat scenarios. It also describes the impacts that can be reasonably be expected from each of the potential security threat scenarios.
- A Security Plan that describes security measures in place to manage the security threat scenarios identified by the Security assessment.
- A training programme setting out how security personnel will be trained to meet their assigned security related duties.

5.3.3 ISO 28002: Development of resilience in the supply chain – Requirements with guidance for use

Aiming to promote resilience at every level of the supply chain, ISO proposes ISO 28002:2011. This standard follows the growing recognition that managing risks requires more than singly focusing on internal processes.

While many aspects of resilience are not addressed here, important guidance is given to introduce some resilience factors within risk management systems.

It is interest to notice that this standard is the result of a committee on “ships and marine technology” which denotes some relevant features of the maritime industry such as the international openness and exposure, particularly under international waters.

5.3.4 ISO 31000: Risk management - Principles and guidelines

This international standard focuses on risk assessment and management, based on a broad view of the concept of risk. It takes into account the direct relation between uncertainty and risk exposure, based on which, it proposes a framework for a risk management process. As requirements of any risk management process, it contemplates the following generic stages:

- Establish purpose and scope for implementation of risk management system
- Hazards identification and categorisation
- Assessment of risk exposure
- Determine acceptability of risk levels in view of given criteria and thresholds
- Ascertain the need for risk modification and control measures
- Validate actions taken

While describing the necessary steps, emphasis is placed on the principles and the development of a corresponding framework, which will support the effective integration of the management system across the organisation and the production of the necessary interfaces with relevant stakeholders. The proposed set of principles, framework and risk management system are shown in Figure 5.2.

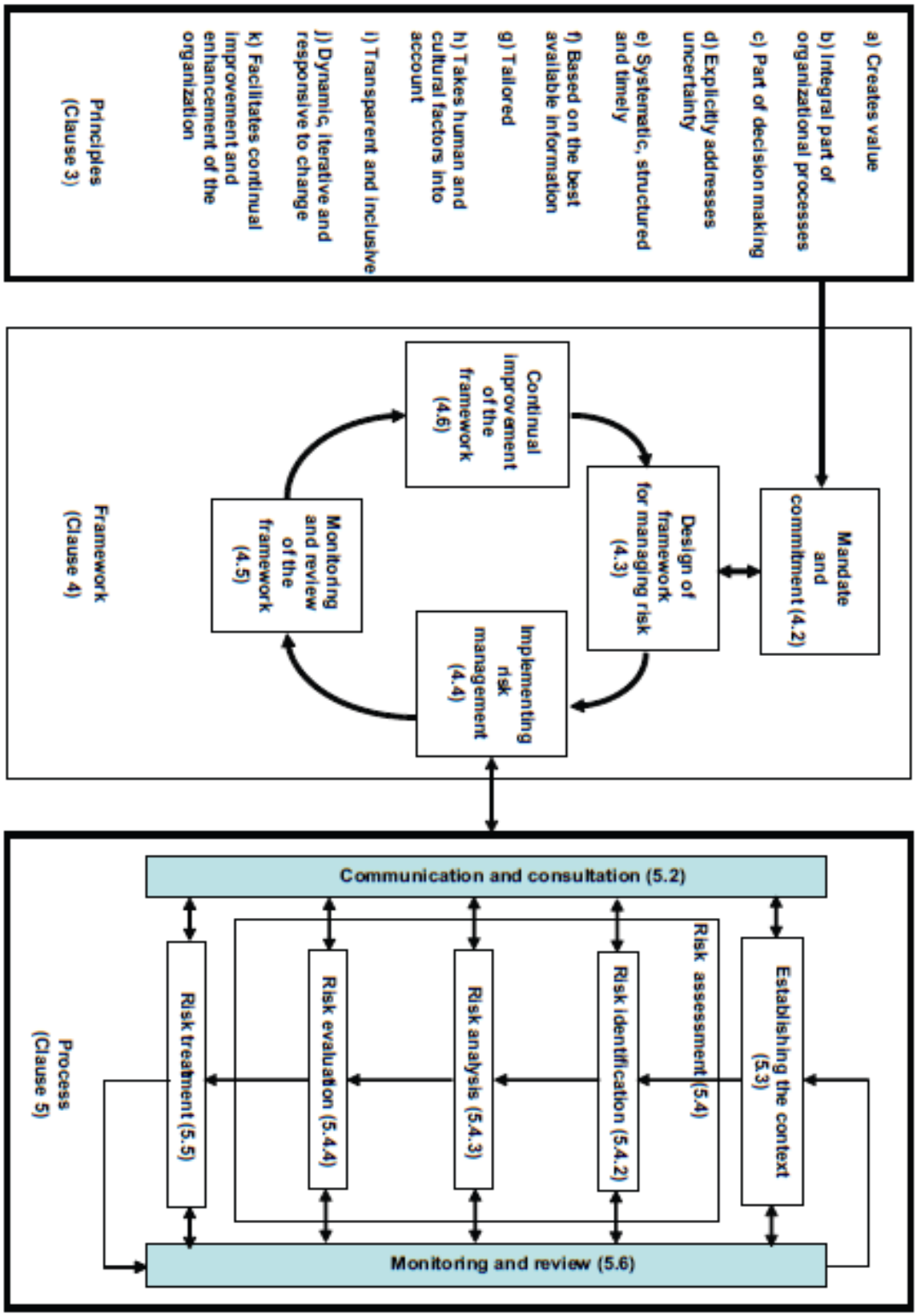

Figure 5.2: Relationships between the risk management principles, framework and process (in ISO 31000)

5.3.5 BS 65000: Guidance for Organisational Resilience

The British Standard BS 65000 provides guidance, describing the nature of resilience and ways to build and enhance resilience in organisations. BS 65000 is based on a definition of organisational resilience that approaches that which advocated for the conceptual framework of RESOLUTE (the ability to anticipate, prepare for, respond and adapt to events – both sudden shocks and gradual change). It recognises the interdependent nature of organisations and the need to further pursue integration and coordination of various critical operational domains, both within organisations and across stakeholders in supply chains and other networks.

5.3.6 SAFE framework of standards

In June 2005 the World Customs Organisation (WCO) adopted the SAFE framework as an integrated approach towards improved security and facilitated world trade conditions. Among other things, this initiative came as a response to increasing costs and disruptions in trade relations, due to the need for heightened security in critical international interfaces. The initial effort focused on creating a unique international instrument for security enforcement, bringing customs and business closer together. This was based on two fundamental types of relationships: Customs-to-customs network arrangements and customs-to-business partnerships. Particularly for the customs-to-business relations, the statute and requirements for recognition as an Authorised Economic Operator (AEO) were a crucial step. According to WCO documentation, the following objectives and principles were established for the SAFE framework:

- Establish standards that provide supply chain security and facilitation at a global level to promote certainty and predictability.
- Enable integrated and harmonized supply chain management for all modes of transport.
- Enhance the role, functions and capabilities of Customs to meet the challenges and opportunities of the 21st Century.
- Strengthen co-operation between Customs administrations to improve their capability to detect high-risk consignments.
- Strengthen Customs/Business co-operation.
- Promote the seamless movement of goods through secure international trade supply chains.

6 REVIEW OF TRAINING PROGRAMMES

The aim of part 4 of this deliverable is to provide a solid basis for the definition of the training materials and the game-based training app to be developed in the RESOLUTE project. The state of the art in training for personnel of Urban Transport Systems (UTS) is depicted and analysed so that project decisions on how to design trainings can be taken based on relevant success criteria.

6.1 Training

Training is defined by ISO 22301:2012 as *activities designed to facilitate the learning and development of knowledge, skills, and abilities, and to improve the performance of specific tasks or roles*.

6.2 Training to support resilience

Implementing resilient systems that involve human actors requires training evaluation to be included into the system's processes. In order to maintain resilience, the results of actions need to be evaluated in order to check if new knowledge, skills, or abilities are required by certain actors, and ways have to be selected or developed how to train these actors properly. Otherwise, new threats or technologies cannot be dealt with properly. In order to do this, existing trainings need to be assessed and evaluated, according to their outcomes. The evaluation should provide a cost-benefit analysis.

6.3 Assessment criteria

Authors of meta-analyses (Alliger, Tannenbaum, Bennet, Traver, & Shotland, 1998; Arthur, Bennet, Edens, & Bell, 2003) have advocated that Kirkpatrick's (1959) can still be very well applied to assess training effectiveness in organisations. These criteria are:

- Reactions (affective and utility judgements)
- Learning (immediate knowledge; knowledge retention; behaviour/skill demonstration)
- Behaviour (Transfer)
- Results

Correlations between these assessment factors indicate theory-conform convergent validity. However, not all criteria are equally recommendable to use for evaluation in all training situations. Particularly, affective reactions do not always serve as good predictors of results or transfer effects. Affective reactions are rather of practical importance when participation in the training is voluntary for the trainees.

These criteria are helpful when evaluating trainings after their realization; however, where data on existing trainings is not available, other criteria must serve to judge which aspects of such trainings are in tune with their main purposes. Other projects, like DRIVER, relied on the technology readiness level (TRL) to assess training procedures.

Training costs can be estimated by the costs for developing the training (not including the analysis of the knowledge or skill gap, as this should be part of previous evaluations) including material and personnel costs, as well as personnel costs, equipment and location costs for implementing the training.

6.4 Basic principles for training and training objectives

Basic principles for training and training objectives

The framework advocated by the DRIVER project (D51.2) may serve the purposes of the RESOLUTE project well as a starting point for clustering important principles of training:

"Knowledge:
1. Professional knowledge in the area of expertise,
2. Knowledge of the legal, administrative and normative framework,
3. Knowledge of the roles, responsibilities, structures and modus operandi of the other organisations.

Analytical and social skills:
1. Problem definition and solution,
2. Analysing information,
3. Prioritization,
4. Communication (to peers, subordinates and hierarchies),
5. Negotiation.

Personal skills:
1. Identifying the personal style of decision making (advantages and disadvantages) and its impact on the processes,
2. Reflecting,
3. Ability to 'use advice',
4. The impact of stress on the specific individual. "

The SECUR-ED project identified the following challenges of crisis management teams which could serve as an alternative concept of what UTS operators need to be prepared for, as far as possible by means of training:

- *"Devising different sequences of tasks*
- *Attending to multiple cues*
- *Sharing tasks (due to time pressure)*
- *Coping with frequent interruptions*
- *Sustaining performance for prolonged hours*
- *Reassigning tasks to team members*
- *Working with incomplete and ambiguous data*
- *Making decisions under time pressure*
- *Taking precautions for possible side effects"*

6.5 Training methods and tools

6.5.1 Classroom training / frontal instruction

The trainer should be an expert with deep knowledge about the subject and about pedagogical/ didactical methods. They present the contents to the trainees and may use methods like small group work, discussions, etc. to support learning. Although this method allows for a great number of trainees to be trained at the same time, the chosen method might not be the best for each individual participant. Low-Fi and High-Fi Media can be used as a support.

6.5.2 Simulator training

In simulator training, the role of the trainer is restricted to defining the training scenario and introducing the trainee to it as far as necessary for its completion. Key element is the use of a simulator technology, for example Virtual Reality (VR)-based. The trainer may have to accompany the trainee during the training and provide supervision and feedback, based on his subjective impression (which although subjective may be based on clear-cut criteria)

or on objective data from the simulator, such as lane-deviation or time-to-break in a driving simulator. Compared to the frontal education approach, simulator training allows for learning by doing, and thus to the development of skills rather than abstract knowledge. This training approach allows for only few, if not even just one trainee to be trained at the same time.

6.5.3 On-the-job training

Here, the role of the trainer is similar as that in the simulator training setting, however, the trainees make their experiences in the field, using real equipment in a real context, in order to solve real problems or completing real tasks. This happens under the supervision and responsibility of the trainer. This approach also limits the number of possible participants.

6.5.4 Drills and exercises

Drills and exercises are fictive scenarios usually to be solved by more than one person, mostly teams. The scenarios resemble real problems for which the exercise is meant to prepare the trainees for. Exercises can reflect only a part of the real-world problem, such as in table-top exercises where trainees sit down at a table together to solve the problem as a group. They can also include physical effects, such as a controlled fire to be put out by fire fighters, in order to not only train the trainees but also to test performance of human actors, equipment, and procedures/plans.

6.5.5 E-learning and serious gaming

Both, e-learning and serious gaming are bound to be performed on the PC or other interactive devices (for example, smartphones). However, both are different from simulator training. In E-learning, trainees use either a locally installed or a web-based training software. E-learning can take the advantages of frontal instruction (such as addressing a large number of trainees simultaneously) across geographical borders, allowing trainees to participate from anywhere. Some forms of E-learning require the trainees to be available at the same time, such as group working over chat functions or similar. Other forms can be paused and resumed whenever the trainee wants to (such as web-based curricula or tests). The disadvantage of E-learning can lie in the possibly greater effort necessary when contents have to be changed in a complex training program.

Serious gaming is different from E-learning in the sense that it uses design features of video games for the purpose of learning instead of the user's entertainment only. Actually, there are training tools that are called serious games and which are not computer-based (Di Loreto & Divitini, 2013). There are various definitions of what a serious game is; we propose adopting the definition by Susi, Johannesson, and Backlund (2007):

Serious games "involve an assigned challenge and employ a compelling form of positive and/or negative reward system". They "use the gaming attributes described above to overcome a designated problem or deficiency, and provide appropriate feedback to the user about their efforts." A disadvantage is, the possibly high cost for producing a good serious game or changing important aspects about it when training goals are redefined. However, it can reach a large number of trainees and may also receive more positive appraisal by the users than frontal instruction or E-learning.

6.6 Training at the RESOLUTE pilot sites

6.6.1 City of Florence

Operator Training in the City of Florence is based on the user manual of the MISTIC tool provided by SWARCO MIZAR. The user manual shows a walkthrough of the main functions, based on detailed edited screenshots. The training includes general procedures (such as login and map), management of events, special functions like messaging and sensor/camera input, as well as scenario management.

6.6.2 Attiko Metro

Generally, training courses for the entire staff at Attiko Metro are designed to cover:

- Rules and procedures
- Safety
- Fire awareness

Attiko Metro trains the "station masters", who are in charge of the technical equipment and supporting other operational staff, are trained in "efficient, responsive and helpful customer service" and passenger information matters, as well as in safety training, communications, signalling, power supply and train driving.

Requirements for managers: Selected and small scale trainings are better, so debriefing can take longer; training should get private feedback; simulations and learning by doing are recommended; trainers need to be experts and "highly appreciated commanders" in the field.

6.7 Other training programmes

6.7.1 EU projects

Several R&D projects co-funded by the European Commission have developed some sort of training or instruction, either as a primary means of the project or in the context of the development of technologies to support the mitigation of a crisis.

Examples are:

- ***DRIVER*** *– Driving Inovation in Crisis Management for European Resilience (2015). http://www. http://www.driver-project.eu/*
  Training: The project has collected information on existing training systems and means to provide new insights on how lessons-learned input can be exploited optimally in crisis intervention.
- ***SECUR-ED*** *- Competence Framework for mass transportation (2013), EU project (TRL 6); source: http://www.secur-ed.eu/*
  Training: The project produced a framework for defining trainings and specific training curricula for the UTS sector (details below).
- ***ACRIMAS*** *- Aftermath Crisis Management System-of-systems Demonstration (2012), EU project (TRL 3); source: http://www.acrimas.eu*
  Training: The project mainly dealt with harmonizing Aftermath Crisis Management, and in this context, trainings and exercises were also taken into account.
- ***SAVE ME*** *–System and Action for Vehicles and transportation hubs to support Disaster Mitigation and Evacuation; source: http://www.save-me.eu/*
  Training: Passengers and Rescue personnel were given an introduction into using the SAVE ME applications designed for these two user groups when the system was pilot tested with real end users in a subway station and a road tunnel.

6.7.2 Other sources

The LÜKEX programme, provided by the German Ministry of Internal Affairs ("BMI") is a strategic crisis management exercise, for the improvement of communication and action across federal and state-based authorities.

The **SECUR-ED** project (D38.1) has produced a framework for defining trainings for the following user groups:

- “Front-line employees and passengers
- Security employees
- Operators in security command and control centres and operational control centres
- Security managers”

The framework comprises three main steps:

1. The preparative work consists in identifying training needs, the relevant environmental conditions for the training and the responsibility for adjusting the training to specific location.

2. The implementation consists in adjusting the training material to the previously identified factors, preparation of the trainers, internal review and assessment of the materials and starting the training.

3. The evaluation framework of the SECUR-ED trainings (D38.1) is based on Kirkpatrick’s (1959) four criteria.

A workshop realized by the SECUR-ED project in Berlin in 2014 (D38.1)resulted in the following list of threats to UTS “that should be covered by training”. This list seems to be also relevant for RESOLUTE trainings, as, with the possible exception of theft/pickpocketing, all threats could lead to a disruption of service:

- “Intrusion
- Behavioural recognition
- Suspicious items
- Bomb threats (by phone for example)
- Graffiti/vandalism/metal theft
- Theft/pick-pocketing
- Aggression
- CRBNe/Pandemics
- Cyber attack
- Demonstrations/large events”

In addition to this, a classification of terroristic acts was taken into account:

- “(Car) bombing
- Hijack/hostage
- Assault, ambush and/or assassination
- Mechanical sabotage
- Bomb threat
- Arson
- Chemical, biological, or radiological attack”

Based on this work, a number of specific training courses were developed in the SECUR-ED project (D38.1):

- AT001: Security awareness course – situational training (SIT) for front line employees
- AT002: Security awareness course for heterogeneous groups of passengers
- AT003: Computer based training (CBT) for recurrent awareness training of front line employees
- ST001: Security course for security agents
- ST002: Refresher training of security agents including a computer based training (CBT) module
- OT001: Security training for OCC operators in security command and control centres
- OT002: Simulator training for operators of CCTV system in the security control room
- SM001: Security training for security managers

- CM001: Emergency and Crisis Preparedness Training Programme: Focused exercises for a single transport system

- *CM002: Emergency and Crisis Preparedness Training Programme: Full scale exercises involving transport operators, first responders, main line rail infra-structure managers, municipal and state level bodies that are responsible for crisis management and other stakeholders*

The trainings developed by the DRIVER project itself (D94.1) are not helpful in our context, as they are directed towards primary mitigation forces. The DRIVER (D52.1) project mentions several training programmes or competence frameworks that could serve as a basis for training. However, the following selection of these may be, at least partly, relevant for the training of UTS employees in the context of RESOLUTE:

- ***Training programs for building competences in early intervention skills*** *(2002), Denmark (TRL 5); source: http://www.who.int/mental_health/emergencies/4.3_key_resource_jensen_and_baron_article.pdf*
- ***DIN PAS 1093 Human Resource Development with special consideration of Learning, Education and Training – Competence Modelling in Human Resource Development*** *(2009), Germany (TRL 1); source: Stracke (2009)*
- ***Master programs on safety and crisis management*** *(2014), France (TRL 9); source: http://www.master-mri.org; http://www.univ-paris1.fr/diplomes/m2ggrc/le-master*
- ***Eight-Dimension Adaptive Performance Model*** *(2000), US; source: Pulakos, Arad, Donovan, & Plamondon (2000).*
- ***Crisis Management Capability analysis and derivation of research needs*** *(2007), EU (TRL 1); source: Prinz, Unger, & Pastuszka (2007).*
- ***IBERO – Instrument for assessment of preparedness with regard to geographic area responsibility*** *(2006), Sweden (TRL 9); source: http://www.lansstyrelsen.se/stockholm/SiteCollectionDocuments/Sv/publikationer/2006/Manual_IBERO.pdf*
- ***Core Competences Framework*** *(2011), UK (TRL 5); source: https://www.the-eps.org/*
- ***Crisis Management Training Programs for local government representatives*** *(2014), France (TRL 9). ; source: http://www.ensosp.fr/SP/sites/default/files/articles/formation-elus-locaux/ENSOSP-2013-PLAQUETTE-ELUS-GESTION-CRISE.pdf*
- ***Training programs at THW "Bundesschule" (****2014), Germany (TRL 9); source: www.thw.de*
- ***Training program for crisis managers*** *(2014), Austria (TRL 9); source: http://www.bmi.gv.at/cms/BMI_Zivilschutz/mehr_zum_thema/skkm/start.aspx*
- ***Competencies for multidisciplinary cooperation in a Network Centric Organization (NCOQ)*** *(2014), Netherlands (TRL 9); source: Theunissen & Stubbé (2014).*

6.7.3 Serious games

We have not identified serious games targeted specifically at the UTS sector, however, there are several games for crisis management (sources DRIVER D52.1; Di Loreto & Divitini, 2013) :

- Incident commander: http://www.incidentcommander.net/product.shtml
- Fukushima disaster: japan.failedrobot.com
- Citizens as rescuers: http://www.dailycamera.com/news/boulder/ci_21204690/satelliteimages-crowdsourcing-emerge-resource-search-missing-trekkers
- The dilemma trainer, by TNO, Thales and University of Arts Utrecht (van de Ven, 2013)
- XVR, by E-semble (see http://www.xvrsim.com)
- Don't panic; Modo; Flooded (by Di Loreto & Divitini, 2013).

7 GOING FORWARD FOR RESOLUTE

The purpose of this deliverable is to provide a state of the art and an overview of knowledge on relevant domains (such as training, legislation and standardisation), aiming to support the development of RESOLUTE. To that end, this document will then be used as grounds for the development of a detailed conceptual framework for RESOLUTE. The knowledge in this document will be further refined and, where relevant, explored in more depth, in order to produce practical consequences and guidance for each of the methodological steps of RESOLUTE and its deliverables.

The notion of resilience has been widely applied and studied under many different domains. However, empirical evidence shows that applied results remain sparse, particularly in view of a comprehensive and innovative understanding of the concept of resilience, such as the one that is proposed in this document. In essence, the full extent of implications of high complexity and variability to system's management and operations must be better understood. Resilience represents a profound shift in paradigm for risk management and any action taken without understanding its far-reaching impacts at every level of organisations defeats its scope and purposes. This perspective is at the core of the innovation proposed by RESOLUTE and at the basis of the integrated and broad range nature of the solutions that it proposes.

8 REFERENCES

Alliger, G. M., Tannenbaum, S. I., Bennet, W. Jr., Traver, H., & Shotland, A. (1998). A meta-analysis oft he relations among training criteria. United States Air Force Research Laboratory. Brooks Airforce Base, TX. http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA368508

Amalberti, R., Auroy, Y., Berwick, D., Barach, P. (2005) Five System Barriers to Achieving ultra safe health care. Annals of Internal Medicine, 142, (9) pp 756-764

Amdal JR., Swigart SL. (2010). Resilient Transportation Systems in a Post-Disaster Environment: A Case Study of Opportunities Realized and Missed in the Greater New Orleans Region, a report of Gulf Coast Research Center for Evacuation and Transportation Resiliency, LA.

Arthur, W.Jr., Bennet, W.Jr., Edens, P.S., & Bell, S.T. (2003). Effectiveness of training in organisations: a meta-analysis of design and evaluation features. Journal of Applied Psychology, 88(2), 234-245.

Axelrod, R., Cohen, M. (1999). Harnessing complexity: Organisational implications of a scientific frontier. New York, USA: The Free Press

Bellet, Th.; Mayenobe, P.; Bornard, J-Ch.; Paris, J-Ch.; Gruyer, D. et al. (2011). Human driver modelling and simulation into a virtual road environment. Human Modelling in Assisted Transportation: Models, Tools and Risk Methods, Milan, Springer, pp.251-262, 2011.

Belluck D., Hull R., Benjamin S., Alcorn J., Linkov I. (2007). Environmental Security, Critical Infrastructure and Risk Assessment: Definitions and Current Trends. In Linkov I. (Ed.), Environmental Security in Harbors and Coastal Areas, NATO security through science series, Springerlink, pp. 3–17.

Bertalanffy, L. (2003) General Systems Theory: Foundations, Development, and Applications. New York, USA: Braziller

Boin, A., Comfort, L., Demchak, C. (2010) The rise of resilience. In Comfort, L., Boin, A., Demchak, C. (eds) Designing Resilience: Preparing for Extreme Events. Pittsburgh, USA: The University of Pittsburgh Press

Boy, G. (2013). Orchestrating Human-Centered Design. Springer, London.

Boukas E., Kostavelis I., Gasteratos A., Sirakoulis G.C. (2014). Robot Guided Crowd Evacuation, IEEE Transactions on Automation Science and Engineering, 12 (2), pp. 739-751.

Brummitt, C.D., D'Souza, R.M, Leicht, E.A. (2012) Suppressing cascades of load in interdependent networks. In Proceedings of the National Academy of Sciences of the United States of America 109 (12) 680-689

Buldyrev, S.V., Parshani, R., Paul, G., Stanley, H.E., Havlin, S. (2010). Catastrophic cascade of failures in interdependent networks. Nature 464, 1025-1028

Buljan, A. & Saphira,Z. (2005). Attention to Production Schedule and Safety as Determinants of Risk-taking in NASA's Decision to Launch the Columbia Shuttle. In Starbuck, W.H. & Farjouin, M. Eds. Organization at the Limit: Lessons from the Columbia Disaster. Blackwell Publishing, Malde, MA, USA

Bush B., Dauelsberg L., LeClaire R., Powell D. (2005). Critical Infrastructure Protection Decision Support System (CIP/DSS) Project Overview. In proceedings of the International System Dynamics Conference, Boston. Available on the Internet at: http://www.systemdynamics.org/conferences/2005/proceed/papers/LECLA332.pdf

Caschili, S., Medda, F.R., Wilson, A. (2015) An Interdependent Multi-Layer Model: Resilience of International Networks. Networks and Spatial Economics. 15 (2) pp 313-335

Centre for the Protection of National Infrastructure-CPNI (2006). Telecommunications Resilience: Good Practice Guide, v4. Available on the Internet at: https://www.cpni.gov.uk/documents/publications/undated_pubs/1001002-guide_to_telecomms_resilience_v4.pdf

Chertoff M. (2009). National Infrastructure Protection Plan: Partnering to enhance protection and resiliency. Available on the Internet at: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

Cohen, Freeman & Thompson (1997). Training the Naturalistic Decision Maker. In Zsambok, C.E. & Klein, G. Eds. Naturalistic Decision Making. Lawrence Erlbaum Associates, Publishers, Mahwah, New Jersey, USA

Cook, S. (2001). On the Acquisition of Systems of Systems. The International Council on Systems Engineering – Proceedings. July 1-5, 2001 Melbourne, Australia

Crozier, R., Ranyard, R. (1997) Cognitive process models and explanations of decision making. In Ranyard, R., Crozier, R., Svenson, O. (eds.) Decision making cognitive models and explanations. (pp 5) London, UK: Routledge

D'Agostino, G., Scala, A. (2014) (eds.) Networks of Networks: The Last Frontier of Complexity. Springer, London

Department for Transport (2014). Transport Resilience Review: A review of the resilience of the transport network to extreme weather events. Available on the Internet at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/335115/transport-resilience-review-web.pdf

Dekker, S. (2004). Ten questions about human error – A new view of human factors and system safety. Aldershot, UK: Ashgate

Dekker, S. (2011) Drift into failure: From hunting broken components to understanding complex systems. Aldershot, UK: Ashgate

Desrichard, O. & Denarié, V. (2005). Sensation Seeking and Negative Affectivity as Predictors of Risky Behaviors: A Distinction between Occasional and Frequent Risk-taking. Adictive Behaviors, 30 (2005) 1449-1453. Elsevier.

De Domenico, M., Solé-Ribalta, A., Gómez, S., Arenas, A. (2014). Navigability of interconnected networks under random failures. In Proceedings of the National Academy of Sciences of the United States of America 111 (23) 8351-8356

Di Loreto, I., & Divitini, M. (2013). Games for learning cooperation at work: the case of crisis preparedness. ECTL meets ECSCW 2013: Workshop on Collaborative Technologies for Working and Learning, Sept. 21, 2013, Cyprus.

Dijkstra, A. (2006) Resilience Engineering and Safety Management Systems in aviation. Proceedings of the second Resilience engineering symposium. Hollnagel, E., Rigaud, E. (eds.) 8-10 November, France: Antibes, Juan-les-Pins D'Lima, M., Medda, F. (2015) A new measure of resilience: An application to the London Underground. Transp. Res. Part A Policy Pract..

D'Lima, M., Medda, F. (2015) A new measure of resilience: An application to the London Underground. Transp. Res. Part A Policy Pract..

Drabble B., Black T., Kinzig C., Whitted G. (2009). Ontology based dependency analysis: Understanding the impacts of decisions in a collaborative environment. IEEE Collaborative Technologies and Systems, New Brunswick (Canada).

DRIVER project (2015). D51.2. Learning in Crisis Management 2025 SoTA and Objectives

DRIVER project (2015). D52.1. Harmonised competence framework.

DRIVER project (2015). D94.1. Training and educational modules.

D'Souza, R.M, Brummitt, C.D., Leicht, E.A. (2014) Modeling interdependent networks as random graphs: Connectivity and systemic risk. In D'Agostino, G., Scala, A. (eds.) Networks of Networks: The Last Frontier of Complexity. Springer, London pp 73-94

Elliot, T. (2005). Expert Decision-Making in Naturalistic Environments: A Summary of Research. DSTO Systems Sciences Laboratory, Edinburgh South Australia, Australia.

Endsley, M.R. (1997). The Role of Situation Awareness in Naturalistic Decision Making. In Zsambok, C.E. & Klein, G. Eds. Naturalistic Decision Making. Lawrence Erlbaum Associates, Publishers, Mahwah, New Jersey, USA

Environmental Protection Agency - EPA (2012).Climate Resilience Evaluation and Awareness Tool Version 2.0: A Climate Risk Assessment Tool for Water Utilities, United States Environmental Protection Agency. Available on the Internet at: http://water.epa.gov/infrastructure/watersecurity/climate/upload/epa817f12011.pdf

European Commission (2005). Green Paper on a European Programme for a critical infrastructure protection. COM 576, Brussels 17.11.2005

European Commission (2012). The EU Approach to Resilience – Learning from Food Security Crises. Communication from the commission to the European parliament and the council. COM 586, Brussels 3.10.2012

European Commission (2013). Commission staff working document on a new approach to the European Programme for Critical Infrastructure Protection - Making European critical infrastructures more secure. SWD 318, Brussels 28.08.2013

Festinger, L. (1985). A theory of cognitive dissonance. Stanford, References 302. Stanford University Press, CA, USA

Freckleton D., Heaslip K., Louisell W., Collura J. (2012). Evaluation of Transportation Network Resiliency with Consideration for Disaster Magnitude, Annual Meeting of the Transportation Research Board (TRB 2012), Washington. Available on the Internet at: http://docs.trb.org/prp/12-0491.pdf

Fujita, Y. (2006a). Systems are ever-changing. In Hollnagel, E., Woods, D.D., Leveson, N. (eds.) Resilience Engineering – Concepts and Precepts. (pp 19) Aldershot, UK: Ashgate

Fujita, Y. (2006b). Resilient systems. In Hollnagel, E., Woods, D.D., Leveson, N. (eds.) Resilience Engineering – Concepts and Precepts. (pp 67) Aldershot, UK: Ashgate

Gao, J., Sergey V. Buldyrev, S.V., Stanley, H.E., Havlin, S. (2012). Networks formed from interdependent networks. Nature Physics 8, 40-48

Gillette J., Fisher R., Peerenboom J., Whitfield R. (2002). Analyzing Water/Wastewater Infastructure Interdependencies. In proceedings of the 6th Probabilistic Safety Assessment and Management Conference, Puerto Rico.

Grote, G. (2004). Uncertainty management at the core of system design. Annual Review of Control, Vo. 28 (pp. 267-274)

Grote, G. (2009). Management of Uncertainty: Theory and Application in the Design of Systems and Organisations. Cranfield, UK: Springer

Gunderson, L., Holling, C., Pritchard, L., Peterson, G. (2002). Resilience of large-scale resource systems. In Gunderson, L., Holling, C. (eds) Resilience and the behaviour of large-scale system. Washington, DC, USA: Island Press Hale et al (1998)

Hale, A., Hovden, J. (1998). Management and culture: The third age of safety. A review of approaches to organisational aspects of safety, health and environment. In Feyer, A., Williamson, A. (eds.) Occupational injury: Risk, prevention and intervention. London, UK: Taylor & Francis Hidden, 1989

Hale, A., Guldenmund, F., Goossens, L. (2006). Auditing resilience in risk control and safety management systems. In Hollnagel, E., Woods, D.D., Leveson, N. (eds.) Resilience Engineering – Concepts and Precepts. (pp 289-314) Aldershot, UK: Ashgate

Hale, A., Heijer, T. (2006a) Defining resilience. In Hollnagel, E., Woods, D.D., Leveson, N. (eds.) Resilience Engineering – Concepts and Precepts. (pp 35-40) Aldershot, UK: Ashgate

Hale, A., Heijer, T. (2006b). Is resilience really necessary? The case of railways. In Hollnagel, E., Woods, D.D., Leveson, N. (eds.) Resilience Engineering - Concepts and Precepts. (pp 125-147) Aldershot, UK: Ashgate

Helbing, D. (1992). A fluid-dynamicmodel for the movement of pedestrians, Complex Syst., 6, pp. 391-415.

Helbing D., Farkas I., Vicsek T. (2000). Simulating dynamical features of escape panic, Nature, 407, pp. 487-490.

Hilton J., Wright C., Kiparoglou V. (2012). Building resilience into systems. In proceedings of IEEE International Systems Conference (SysCon), pp. 1-8.

Holling, C. (2010) Engineering resilience versus ecological resilience. In Gunderson, L., Allen, C., Holling, C., (eds) Foundations of ecological resilience. (pp 51-66) Washington, DC, USA: Island Press

Hollnagel, E. (2004) Barriers and accident prevention: or how to improve safety by understanding the nature of accidents rather than finding their causes. Aldershot, UK: Ashgate

Hollnagel, E. (2006) Resilience – The challenge of the unstable. In Hollnagel, E., Woods, D.D., Leveson, N. (eds.) Resilience Engineering – Concepts and Precepts. (pp 9-17) Aldershot, UK: Ashgate

Hollnagel, E., Woods, D. (2006) Epilogue: Resilience engineering precepts. In Hollnagel, E., Woods, D.D., Leveson, N. (eds.) Resilience Engineering - Concepts and Precepts. (pp 347-358) Aldershot, UK: Ashgate

Hollnagel, E., Woods, D., Leveson, N. (Eds.) (2006). Resilience Engineering: Concepts and Precepts. (pp 1-6) Aldershot, UK: Ashgate

Hollnagel, E. (2008) From FRAM (Functional Resonance Accident Model) to FRAM (Functional Resonance Analysis Method) Presentation at the FRAM workshop, École des Mines de Paris – Centre for Research on Risk and Crises (CRC) 20-22 February, Sophia Antipolis, France

Hollnagel, E. (2009) the ETTO principle: efficiency-thoroughness trade-off: why things that go right sometimes go wrong. Aldershot, UK: Ashgate

Hollnagel, E. (2011a) Prologue: the scope of resilience engineering. In Hollnagel, E., Pariès, J., Woods, D., Wreathall, J. (eds.) Resilience engineering in practice - A guidebook. (pp xxix-xxxix) Aldershot, UK: Ashgate

Hollnagel, E. (2011b) Epilogue: RAG – the Resilience Analysis Grid. In Hollnagel, E., Pariès, J., Woods, D., Wreathall, J. (eds.) Resilience engineering in practice - A guidebook. (pp 275-296) Aldershot, UK: Ashgate

Hollnagel, E. (2014) Safety-I and Safety-II: The Past and Future of Safety Management. Aldershot, UK: Ashgate

Hurst, N. (1998) Risk assessment: the human Dimension. Cambridge, UK: The Royal Society of Chemistry Hutter (2010)

Jackson, S. (2010) Architecting resilient systems: Accident avoidance and survival and recovery from disruptions. Hoboken, New Jersey, USA: John Wiley & Sons

Jamshidi, M. (2008) (eds.) System if systems engineering – Innovations for the 21st Century. New Jersey, USA: Wiley & Sons

Karady GG., Zhang X. (2011). Sustainability and resilience of electric energy supply in urban environment. In proceedings of IEEE Power Systems Conference and Exposition (PSCE), pp. 1-3.

Klein, G.A. & Klinger, D. (1991). Naturalistic decision-making. Human Systems IAC Gateway, Volume XI: Number 3, 2, 1, Winter, pp. 16-19.

Klein, G. (1997). The Recognition-Primed Decision (RPD) Model. In Zsambok, C.E. & Klein, G. Eds. Naturalistic Decision Making. Lawrence Erlbaum Associates, Publishers, Mahwah, New Jersey, USA

Kirkpatrick, D. L. (1959). Techniques for evaluating training programs. Journal of the American Society of Training and Development, 13, 3–9.

Kirwan, B. (1998) Safety Management Assessment and Task Analysis – A missing link? In Hale, A., Baram, M. (eds.) Safety Management management - The challenge of change (pp 67-92) Kidlington, UK: Pergamon

Leveson, N., Daouk, M., Dulac, N., Marais, K. (2003) A Systems theoretic approach to safety engineering. Cambridge, Massachusetts, USA: MIT - Aeronautics and Astronautics Department

Leveson, N. (2004) A new accident model for engineering safer systems. Safety Science, Vol.42 (pp 237-270)

Linkov, I., Eisenberg, D., Bates, M., Chang, D., Convertino, M., Allen, J., Flynn, S., Seager, T. (2013) Measurable resilience for actionable policy. Environ Sci Technol 47:10108–10110

Lipshitz, R. & Shaul, O.B. (1997). Schemata and Mental Models in Recognition-Primed Decision Making. In Zsambok, C.E. & Klein, G. Eds. Naturalistic Decision Making. Lawrence Erlbaum Associates, Publishers, Mahwah, New Jersey, USA

London Resilience Forum (2013). London Resilience Partnership Strategy. The London Resilience Partnership

Luthar SS., Cicchetti D., Becker B. (2007). The Construct of Resilience: A Critical Evaluation and Guidelines for Future Work, Child Dev., 71(3), pp. 543–562.

Magniez C., Vouters M. (2013). Interoperability and resilience of railway transport systems: Development of composites for transports: Challenges and expected development. In proceedings of the 2013 International Conference on Industrial Engineering and Systems Management (IESM).

Mansfield, J. (2010). The nature of change or the law of unintended consequences: An introductory text to designing complex systems and managing change. London, UK: Imperial College Press

Marais, K., Dulac, N., Leveson, N. (2007) Beyond normal accidents and high reliability organisations: The need for an alternative approach to safety in complex systems. Engineering Systems Division Symposium – Cambridge, Massachusetts, USA: MIT, 29-31 March

McDonald, N. (2006). Organisational Resilience and Industrial Risk. In Hollnagel, E., Woods, D.D., Leveson, N. (eds.) Resilience Engineering – Concepts and Precepts. (pp 155-180) Aldershot, UK: Ashgate

Mezzou O., Birregah B., Chatelet E. (2011). A theoretical study of the interactions between the components of resilience in critical urban infrastructures. In proceedings of the IET International Conference on Smart and Sustainable City (ICSSC 2011), pp. 1-6.

Mugavero R., Sabato V., Stallo C. (2012). Territorial Security: Architectures, methodologies and integrated systems for the information management in multi-risk scenarios. In proceedings of the 1st IEEE AESS European Conference on Satellite Telecommunications (ESTEL 2012), pp. 1-5.

National Cooperative Highway Research Program-NCHRP (2014). Response to Extreme Weather Impacts on Transportation Systems, National Academy of Sciences, Available on the Internet at: http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_syn_454.pdf

Nemeth, C., Hollnagel, E. (2014) (eds.) Resilience engineering in practice, Volume 2 – Becoming resilient. Aldershot, UK: Ashgate

Ni H., Chen A., Chen N. (2009). An Assessment Model of Institutional Resilience in Urban Emergency Management. In proceedings of the International Conference on Management and Service Science (MASS 2009), pp. 15-24.

NIPP (2009). National Infrastructure Protection Plan, US Department of Homeland Security. U.S., Department of Home Security, Washington, USA, p. 175. Available on line at: www.dhs.gov/nipp

Norros, (2004). Acting under Uncertainty: the Core-task Analysis in Ecological Study of Work. VTT Publications 546. Espoo, Finland.

Oliveros MM., Nagel K. (2013) Automatic Calibration of Agent-Based Public Transit Assignment Path Choice to Count Data, Conference on Agent-Based Modelling in Transportation Planning and Operations 2013, Virginia.

Orasanu, J. & Fischer, U. (1997). Finfing Decisions in Natural Environments: The View from the Cockpit In Zsambok, C.E. & Klein, G. Eds. Naturalistic Decision Making. Lawrence Erlbaum Associates, Publishers, Mahwah, New Jersey, USA

Owens, B., Leveson, N. (2006) A Comparative Look at MBU Hazard Analysis Techniques. Proceedings of the 9th Annual Military and Aerospace. Programmable Logic Devices International Conference (MAPLD). 26 – 28 September, Scottberg

Pan X., Han C., Dauber K., Law K., (2007). A multi-agent based framework for the simulation of human and social behaviours during emergency evacuations, Ai Soc., 22, pp. 113–132.

Pelechano N., Allbeck J., Badler N. (2004). Virtual Crowds: Methods, Simulation, and Control, Morgan & Claypool Publishers, CA.

Perrow, C. (1999). Normal accidents: Living with high-risk technologies. Princeton, USA: Princeton University Press

Pettersson, G. (2007). Time and Design in Decision Making Environments. In Cook, M.; Noyes, J. & Masakowski, Y. Decision Making in Complex Environments

Prinz, J., Unger, C., & Pastuszka, H.-M. (2007). ESRIF WG4 "CRISIS MANAGEMENT" – Capability analysis and derivation of research needs (pp. 1–22).

Pulakos, E. D., Arad, S., Donovan, M. a., & Plamondon, K. E. (2000). Adaptability in the workplace: Development of a taxonomy of adaptive performance. Journal of Applied Psychology, 85(4), 612–624.

Rajamaki J., Rathod P., Ahlgren A., Aho J., Takari M., Ahlgren S. (2012). Resilience of Cyber-Physical System: A Case Study of Safe School Environment. In proceedings of the Intelligence and Security Informatics Conference (EISIC 2012), p. 285.

Ranghieri F., Ishiwatari M. (2014). Learning from Megadisasters : Lessons from the Great East Japan Earthquake. Washington, DC: World Bank. Available on the Internet at: https://openknowledge.worldbank.org/handle/10986/18864

Rasmussen, J. (1996) Cognitive Control and Human Error. In Rasmussen, Duncan & Leplat, New Technology and Human Error, John Wiley & Sons, New York.

Rasmussen, J. (1997) Risk management in dynamic society: A modelling problem. Safety Science, Vol. 27 (pp 183-213)

Reason, J., Hobbs, A. (2003) Managing maintenance error. Aldershot, UK: Ashgate

Schneeweiss, C. (2003) Distributed decision making. Heidelberg, Germany: Springer-Verlag

SECUR-ED D38.1 (2013). Training organisation and management.

Serfaty, MacMillan, Entin & Entin (in Endsley (in Szambock & Klein, 1997) & Klein, 1997)

Smith P., Hutchison D., Sterbenz J.P.G., Scholler M., Fessi A., Karalipoulos M., Lac C., Plattner B. (2011). Network Resilience: A Systematic Approach, IEEE Communications Magazine, pp. 88-97.

Starbuck, W., Farjoun, M. (2005) Organization at the limit: lessons from the Columbia disaster. Malden, Massachusetts, USA: Blackwell Publishing

Stracke, C. (2009): DIN PAS 1093. Human Resource Development with special consideration of Learning, Education and Training – Competence Modelling in Human Resource Development. Berlin: Beuth Verlag.

Sung M., Gleicher M., Chenney S. (2004). Scalable behaviours for crowd simulation, EUROGRAPHICS 2004. Available on the Internet at: https://graphics.cs.wisc.edu/Papers/2004/SGC04/crowd.pdf

Susi, T., Johannesson, M., & Backlund, P. (2005). Serious games – an overview. Technical Report HS- IKI -TR-07-001. University of Skövde, Sweden. http://www.diva-portal.org/smash/get/diva2:2416/FULLTEXT01.pdf

Sutcliffe, K., Vogus, T. (2003) Organizing for resilience. In Cameron, K., Dutton, J., Quinn, R. (eds.) Positive organisational scholarship. (pp 94-110) San Francisco, USA: Berrett-Koehler

Svedung, I. & Rasmussen, J. (1998) Organisational decision making and risk management under pressure from technological change. In Hale, A., Baram, M. (eds.) Safety Management. (pp 249-264) Oxford, UK: Elsevier Science Ltd

Svenson, O. (1992) Differentiation and Consolidation Theory of human decision making: A frame of reference for the study of pre- and post-decision processes. Acta Psychologica. Vol. 80, (pp 143-168)

Svenson, O. (1996) Decision making and the search for fundamental psychological regularities: What can be learned from a process perspective? Organisational Behaviour and Human Decision Processes. Vol. 65 (pp 252-267)

Theunissen, N. C. M., Stubbé, H. E. (2014). iSELF : The development of an Internet-Tool for Self-Evaluation and Learner Feedback. Electronic Journal of E-Learning (EJEL), 12(4), 313–325.

Transportation Research Board of the National Academies (2008). The Role of Transit in Emergency Evacuation. Available on the Internet at: http://onlinepubs.trb.org/onlinepubs/sr/sr294.pdf

Trucco P., Minato N., Careri N. (2011). Resilience of Transport Systems Under Disaster: Simulation-based Analysis of 2011 Tsunami in Japan. In proceedings of IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), pp. 487-491.

Tschiersch, I., Schael, T. (2003). Concepts of Human-Centred Systems. In Brandt, D. Human-Centred System Design - First: People; Second: Organization; Third: Technology.

Turner, B., Pidgeon, N. (1997) Man-made disasters. Oxford, UK: Butterworth-Heinemann

Van de Ven, J.G.M.; Stubbé, H.; Hrehovcsik, M., (2013). Gaming for Policy Makers: It's Serious!. Second International Conference, GALA 2013, Paris, France, October 23-25, 2013, Revised Selected Papers.

Vertzberger, Y.I. (1998). Risk Taking and Decision Making: Foreign Military Intervention Decisions. Stanford University Press, Chicago, U.S.

Vugrin, E., Warren, D., Ehlen, M., Camphouse, C. (2010). A framework for assessing resilience of infrastructure and economic systems. In gopalakrishnan, k., peeta, s. (eds) Sustainable and resilient critical infrastructure systems: simulation, modelling and intelligent engineering. (pp 77-116) Heidelberg, Germany: Springer-Verlag

Walker, B., Salt, D. (2006) Resilience thinking: sustaining ecosystems and people in a changing world. Washington, DC, USA: Island Press

Wei D., Ji K. (2010). Resilient industrial control system (RICS): Concepts, formulation, metrics, and insights. In proceedings of the 3rd International Symposium on Resilient Control Systems (ISRCS 2010), pp. 15-22.

Weick, K., Sutcliffe, K. (2007) Managing the unexpected: Resilient performance in an age of uncertainty. San Francisco, USA: Jossey-Bass

Westrum, R. (2006) A typology of resilience situations. In Hollnagel, E., Woods, D.D., Leveson, N. (eds.) Resilience Engineering – Concepts and Precepts. (pp 55-65) Aldershot, UK: Ashgate

Wicklund, R. A., Brehm, J. W. (1976) Perspectives on Cognitive Dissonance. Hillsdale, New Jersey: Lawrence Erlbaum Associates

Widalvsky, A. (2004) Searching for safety. New Jersey, USA: Rutgers

Woods, D. (1988). Coping with Complexity: the Psychology of Human Behavior in Complex Systems. In Goldstein, L.P.; Andersen, H.B. & Olsen. S.E., Eds. Tasks, Errors and Mental Models: a Festschrift to celebrate the 60th anniversary of Professor Jens Rasmussen. Taylor & Francis, London.

Woods, D. (2003) Creating foresight: How resilience engineering can transform NASA's approach to risky decision. Testimony on the future of NASA for the Committee on Commerce, Science and Transportation. John McCain, Chair. October 29

Woods, D. (2006) Essential characteristics of resilience. In Hollnagel, E., Woods, D., Leveson, N. (eds.) Resilience Engineering – Concepts and Precepts. (pp 21-34) Aldershot, UK: Ashgate

Woods, D. (2014). The Mystery of Sustained Adaptability. Velocity Conference, September 15-17, New York (retrieved on 08-08-2015 from http://velocityconf.com/velocityny2014/public/schedule/detail/35613)

Woods, D. & Hollnagel, E. (2006) Prologue: Resilience Engineering Concepts. In Hollnagel, E., Woods, D., Leveson, N. (eds.) Resilience Engineering – Concepts and Precepts. (pp 1-6) Aldershot, UK: Ashgate, pp. 128-148.

Wreathall, J. (2006) Properties of resilient organisations: An initial view. In Hollnagel, E., Woods, D.D., Leveson, N. (Eds.) Resilience Engineering – Concepts and Precepts. (pp 275-285) Aldershot, UK: Ashgate

Yeh H., Curtis S., Patil S., (van den) Berg J., Manocha D., Lin M. (2008). Composite agents. In Proccedings of the ACM SIGGRAPH/Eurograph. Symp. Comput. Animation, pp. 39–47.

Yusta J.M., Correa G.J., Lacal-Arantegui R. (2011). Methodologies and applications for critical infrastructure protection: State-of-the-art, Energy Policy, 39(10), pp. 6100-6119.

ZELENY, M. (1981) Multiple criteria decision making. New York, USA: Mcgraw-Hill

Zsambok, C.E. (1997). Naturalistic Decision Making: Where Are We Now? In Zsambok, C.E. & Klein, G. Eds. Naturalistic Decision Making. Lawrence Erlbaum Associates, Publishers, Mahwah, New Jersey, USA

8.1 Websites

100 Resilient Cities: http://www.100resilientcities.org/ - Retrieved on 19 August 2015

http://www.bbk.bund.de/DE/AufgabenundAusstattung/Krisenmanagement/Luekex/TT_Luekex_ueberblick.html

http://www.ima-zlw-ifu.rwth-aachen.de/fileadmin/user_upload/INSTITUTSCLUSTER/Alumni/human-centred_system_design.pdf - Retrieved on October 2012

National Oceanic and Atmospheric Administration: https://toolkit.climate.gov/ - Retrieved on 16 August 2015