On The Art of Creating and Managing Policies: Facilitating the Emergence of Resilience

Gunilla A. Sundström, Erik Hollnagel

On The Art of Creating and Managing Policies: Facilitating the Emergence of Resilience

Gunilla A Sundström[1] and Erik Hollnagel[2]

[1] Wachovia Corporation, 301 S. Tryon Street, Charlotte, NC 28288, USA
Gunilla.Sundstrom@wachovia.com

[2] École des Mines de Paris, Pôle Cindyniques, Rue Claude Daunesse, F-06904 Sophia Antipolis France
Erik.Hollnagel@cindy.ensmp.fr

Abstract. Resilience denotes an organization's ability to adjust effectively to the multi-faceted impact of internal and external events over a significant time period. To be resilient, an organisation must be able to deal with unexpected and disruptive events as well as to understand the longer term impact of such events. In the Financial Services domain this translates into the ability to identify and successfully manage risk at all levels in the organization while sustaining a profitable business. Key tools for risk management include effective policy design and policy management processes. Based on a system state view of businesses, the paper outlines some principles for organising policy design and processes related to policy management, using an example from the Financial Services as an illustration.

1 INTRODUCTION

Resilience has been defined as the ability of an organisation to "adjust effectively to the multifaceted impact of internal and external events over a significant time period" (Sundström & Hollnagel, 2006, page 235). As noted already by Holling (1973, page 2), such a view shifts attention away from the mechanisms that stabilise a system to the conditions that enable a system to persist over time. In this paper we propose that for an organisation one such condition is that it can deal with unexpected and disruptive events and another that it can effectively understand the consequences of these events. In the Financial Services industry this means the ability to identify and successfully and simultaneously manage various types of risks at operational, tactical, and strategic business levels. To do so requires, among other things, effective policy design and effective policy management processes.

This paper provides a basis for understanding the nature of organisational variety ('laws') at all business system levels by exploring the role of policies and their associated processes. It outlines a framework for structuring elements of policies and policy management processes referring to the three key business system states described in Sundström & Hollnagel (2006). These are: (1) the healthy state, where business goals are met and where risks are understood and accepted; (2) the unhealthy state, where business goals are not met and/or the risk of incurring losses is unacceptably high; and finally (3) the catastrophic state, where either one or more elements of the system, or the overall system, ceases to function.

We further propose that effective policy analysis, design and policy management can prevent the transition from a healthy to a catastrophic state. The three states differ with

respect to the predictability of events and the organization's ability to trade-off gains and losses in an efficient and reliable manner. This apparently corresponds to Westrum's (2006) description of three types of risk, called regular, irregular, and unexampled, although the similarity needs to be explored further. Finally, throughout the paper, policy analysis is defined as the "laying out of alternative choices" by predicting impact of system variables than can be influenced by policies in scope (cf. Weimar & Vining, 2005, pp. 24-26) .

2 THE BASIC FRAMEWORK

We define a business system as a combination of people, social structures and information technology (information systems) organised to satisfy a particular set of business objectives, specifically to provide shareholder value, profitability and customer equity (Sundström & Hollnagel, 2006). Fig. 1 shows the three basic states of a business system and the behavioral characteristics associated with each, in particular the types of associated control behaviors (Hollnagel, 1998). In a healthy state, focus is on detecting risky and non-compliant behavior to prevent unwanted developments and their consequences. System behavior is proactive and the level of control is strategic emphasising understanding of medium and long-term consequences. In an unhealthy state, focus is on how to manage impact of disruptions to improve short term control. As a result, systemic detection of risky and non-compliant behavior becomes less likely. The system primarily reacts to events and the level of control is opportunistic and not strategic. Finally, in a catastrophic state the primary concern is how to recover from loss of control to make the transition back to a healthy state. System behavior is entirely reactive and as a result the level of control is scrambled, i.e., choice of course of action is random. In the catastrophic state, the same actions might be fruitlessly repeated in the vain hope that something will happen.

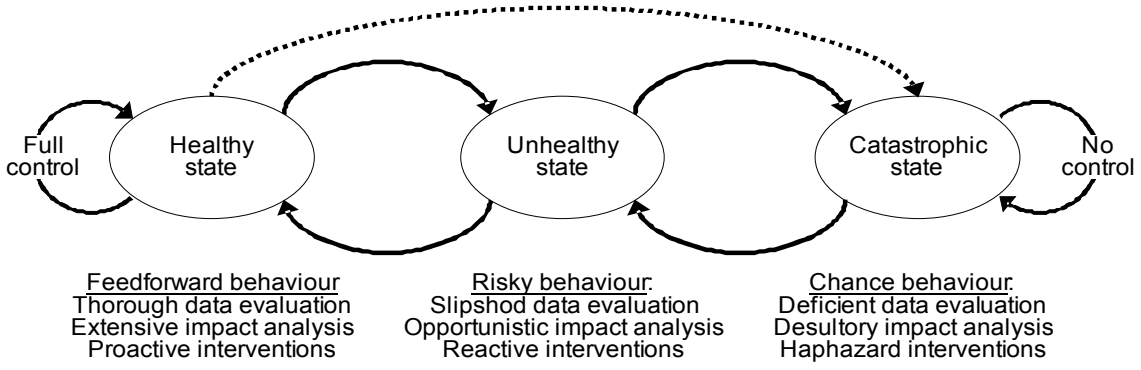

Fig. 1*:* Three key states of a business system (from Sundström & Hollnagel, 2006)

Recovery from a catastrophic state is mostly due to chance. Recovery from an unhealthy state, as well as remaining in a healthy state, primarily depends on the ability to improve and prevent loss of control by the competent application of various types of resources and timely and correct analyses of impacts. A key ingredient of this is proactively to detect and address risky behavior at a system level.

2.1 What are Policies and Policy Management?

Richards (2004, p. 8) defined a policy as "a statement reflecting a guiding principle intended to influence and determine decision and actions". An important distinction is between a policy statement and the standard operating procedures, where the former focuses on strategies and programmes while the latter focuses on performance (cf. Table 1). Richards (2004) argues that a policy without an active policy management process is unlikely to have any impact on performance. As illustrated by the three system states described above, it is not enough that policies effectively guide decisions and actions in response to events. In order to prevent that control is lost, it is also necessary to have proactive policy analysis management. This in turn requires that valid indicators of the state of key policy analysis and of policy management processes can be defined.

Table 1: Key definitions used in policy management

Category	Definition	Example
Policy statement	Guiding principle intended to influence and determine decision and actions across business system.	The Bank for International Settlements (BIS) Basel II have created regulations that will require Financial Services providers to establish policies to determine how to manage Operational Risk
Standard	Distinct requirement for what actions are required to be compliant with a corporate policy.	A Basel II related standard would define what needs to be measured to capture operational risk
Recommended practice	A "How to" for what to do to meet a standard.	A recommended practice would define the practice to be used within a specific Organization to measure risk
Standard operating procedure (SOP)	A procedure that defines the "How – To" in a specific operational setting.	An operating procedure would define what procedure should be used to produce the data required to measure a particular risk in a specific entity of a Business system.

The key metric for business systems (and a key condition for system persistence) is *profitability*. Adopting the control theoretical view of business systems (see Sundström & Hollnagel, 2006) one important symptom is the uncontrolled variability in key metrics or critical functions such as sudden or unexpected operational losses and / or revenue. Organizational policies and policy management serve to help an organization detect and track risky and non-compliant practices in time. Building on Richards' (2004) and Bardach's (2005) view of the key elements in a policy life cycle, we propose to view policy analysis and management as a form of process control (cf. Fig. 2). Policy definition should provide overall guidance for what decisions are in scope of the policies; policy implementation should include procedures for implementation of policies and standards; policy management should have defined procedures enabling collection and evaluation of data leading to an overall assessment of "policy performance" aligned with key business objectives and systems states. The policy life cycle as portrayed in Fig. 2, needs to be monitored and policy definitions needs to be adjusted as needed.

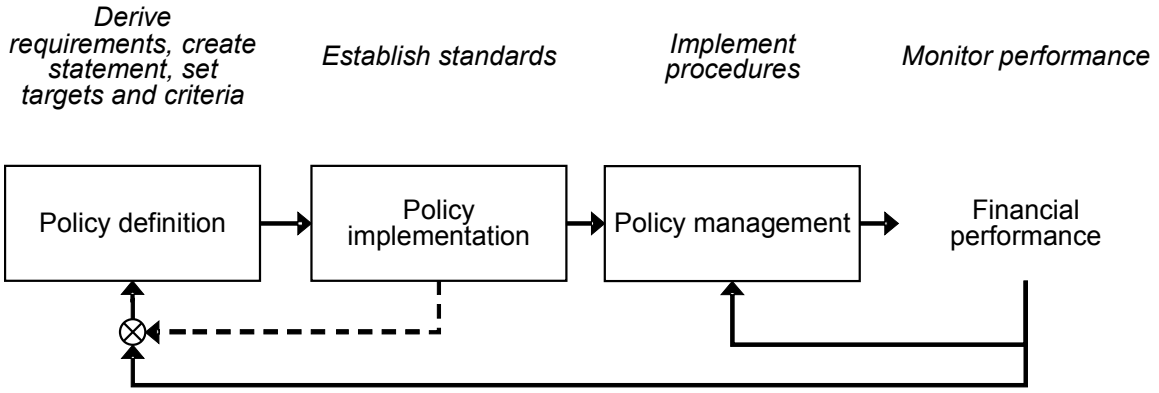

Fig. 2: A Simple policy life cycle view

In control theoretic terms, the policy life cycle is described by two nested feedback loops. The initial inputs to the process are the types of decisions that must be governed by policy, and the overriding performance criterion is to prevent a loss of control, defined as uncontrolled transitions between the states described in Fig. 2.

2.2 Policy Requirements Derived from the State View of Business Systems

As shown by Fig. 2, goal states (defined by policies and ultimately by business strategies) should drive decisions and behaviors in a business system. Going back to the three system states described by Fig. 1, policies should be designed either to prevent loss of control or to improve the degree of control over a system. Note that framing policies in the context of improved control and/or to prevention of loss of control integrates all policy types within a single framework that can be shared across all entities of a business system. Policies that provide guidance for improving and/or preventing loss of control therefore exemplify behavioral "laws" that apply at all system levels. As a result, pursuing the following operational goals becomes a key characteristic of a system persistent over time (i.e., a resilient system) .

(1) *Improve (efficiency of) control*. This can be accomplished by improving the system's ability to detect and respond to risky and non-compliant behavior, for instance by keeping monitoring track of day-to-day performance, by improving impact analysis, by preparing more detailed (contingency) procedures, by ensuring that there is enough spare resource capacity to match all likely contingencies. In technical terms this corresponds to an increase in the system's requisite variety (Conant & Ashby, 1970). A complementary approach is somehow to reduce the variety of the environment, e.g., by constraining other actors. For a business system, an example of such a complementary approach is to acquire competitors and thereby change the market environment.

(2) *Prevent loss of control*. Prevention requires anticipation, the ability to foresee what is likely to happen. In Financial Services systems this means proactive impact analysis, proactive opportunity analysis and proactive risk management at a business portfolio level. As illustrated in Fig. 1 all these behaviors are associated with the healthy business system state. In order to prevent the loss of control it is

necessary to invest in something that is likely, but not certain. This in itself creates a risk, although one that is moderate and controllable.

(3) *Assess scope of catastrophic impact*. A key concern in a catastrophic state is whether the impact can be isolated to a subset of the system or whether it will spread across the system as a whole. In the former case it may be possible to contain the losses, although normal operations may have to be suspended in part or in whole. In the latter case it may be necessary to abandon attempts of regaining stability, and instead look for alternate ways of operating, for instance by completely restructuring the operation.

Whereas the first goal in principle can be found in practically all systems, the second and the third goals are particular for resilient systems. To facilitate emergence of resilient behavior, policies should therefore be designed and implemented to prevent loss of control and to provide guidance when a loss of control has occurred.

3 HOW THE DEMISE OF BARINGS PLC COULD HAVE BEEN PREVENTED BY RESILIENCE

In the following, we use the Barings' PLC collapse as our example. The Barings case has been described in several places, e.g., Kurpianov (1995); Reason (1997); and Sundström & Hollnagel (2006). Barings PLC was a 233 year old highly reputable British financial institution that unexpectedly went into a state of bankruptcy in February 1995. The reason was a loss of US $ 1.3 billion primarily caused by the trading practices of a single trader, Nick Leeson. Fig. 3, adapted from Sundström & Hollnagel, (2004), provides an overview of the key components of the dynamic system of which Nick Leeson was part.

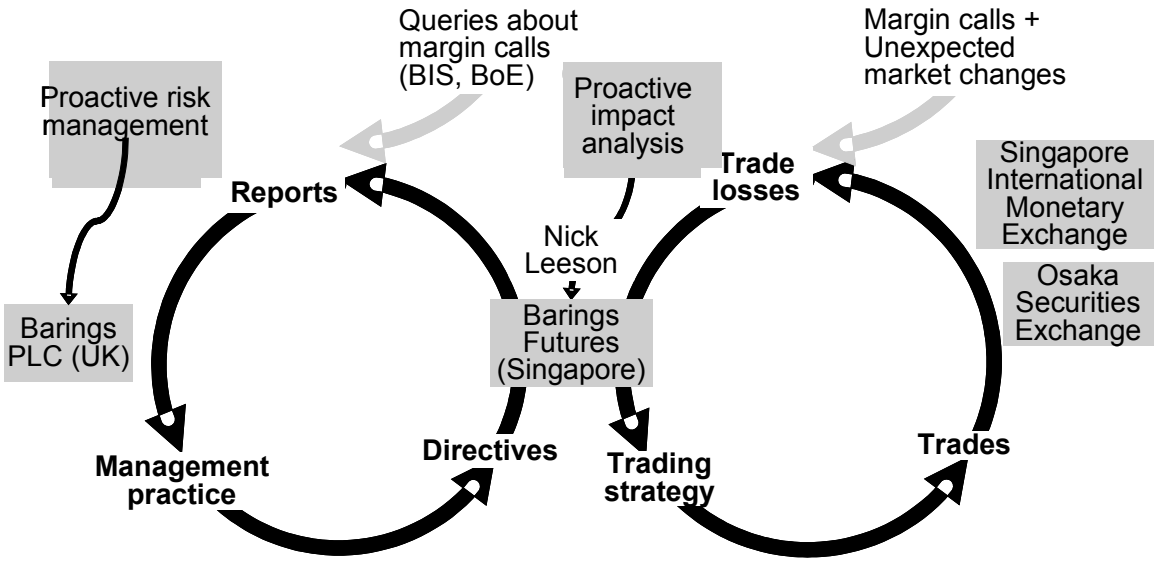

Fig. 3: Dynamic system view of the Nick Leeson scenario at Barings Securities

Using the representation of the policy life-cycle shown in Fig. 2, Barings PLC (UK) was responsible for system-wide policy definition and for system wide policy management monitoring as described in Fig. 2. Barings Futures in Singapore were responsible for the standards and recommended practices that comprised policy implementation and monitoring as well as for any specific policy requirements related to securities trading in Barings Futures. The trader (i.e., Nick Leeson), was responsible for executing operating procedures aligned with policy requirements and standards. Barings PLC should have developed controls to monitor securities business processes, strategic business risks and to proactively monitor operational risks. These controls should have included the ability to ensure that duties for sales and reconciliation functions were appropriately separated. They should also have set the principles for a strategic opportunity analysis and policy life cycle management.

However, the reality at Barings was very different. Senior management did not understand the securities trading business well and as a result did not leverage policy analysis to establish appropriate system wide management feedforward strategies and controls (i.e., they implemented a policy life cycle management process without appropriate monitoring). In addition, Barings Futures (Singapore) should have developed standards and recommended practices to manage securities business processes, to separate duties for sales and reconciliation functions, to manage strategic business risk, and to manage operational risk. As pointed out by Barings Internal Audit in 1994, the fact that Nick Leeson was in charge of both front and back office created "…an excessive concentration of powers" (cf. Chew, 2006). This dual responsibility was coupled with the fact that Nick Leeson, was new in the trading position and lacked experience. The compounded result was that Barings PLC did not have a mechanism in place to help to translate both excessive revenues (given the trading strategy used by Nick Leeson) and the excessive margin calls[1] into an understanding that the system at a minimum had transitioned in to an unhealthy state. Barings management completely failed to recognize the overall impact of the excessive margin calls since they did not detect that Barings available capital was much less than the losses incurred by Lesson's trading practices. Thus, Barings PLC failed to increase control by trying to minimize losses and maximizing available capital. They also failed to prevent loss of control by not hedging potential trading losses by setting aside reserve capital. As a result, the system transitioned into a catastrophic state.

3.1 How the System Failed

We can use the Barings case to identify some of the policy requirements at an enterprise level (i.e., system level and hence need to be applied to all part of a business system) for any Financial Services system. The method we use is a mixture of what Bardach referred to as the diagnostic and latent opportunity approach. While Fig. 3 only points to operating procedure at an individual level, operating procedures need to be defined at each level of the system and tailored to the specific environment of a particular system entity. For

[1] A margin call is a call for additional funds. This demand for more funds in either cash and/or securities is to restore an account to its initial margin requirement level. Generally, this occurs when the price action is adverse to the account holder's positions. It can also reflect an increase in margin requirements. From Barkley's Comprehensive Financial Glossary

example, in a Financial Services system, operating procedures need to be sensitive to the competitive drivers and regulations of a specific financial market.

A key question is how to maximize alignment among operating procedures and system states. For example, an operating procedure tied to a set of policies to prevent loss of control in the securities business could prescribe that management reviews trading reconciliation reports on a periodic basis, which in a healthy state could be every four weeks. However, whenever the system goes into an unhealthy state, the time period could be weekly instead of monthly and the nature of data included in the reports might change (e.g., to include a contrast between potential losses and capital reserves). Moreover, an unhealthy system state could make operating procedures obsolete, thereby further increasing the risk. It is essential that policies are in place to mandate what actions need to be taken to identify overall system state as well as the state of particular system entities that are believed to be unhealthy. Such polices could indeed facilitate emergence of resilience. Sundström & Hollnagel (2006) identified some key behaviors including the ability to explicitly articulate system goals and acceptable risk levels and to focus on monitoring key state variables. As described in the previous section, Barings PLC management team did not exhibit any of these behaviors, which may be one reason why the organization transitioned into a catastrophic state.

3.2 Two Policy Problems: Preventing Loss and Improving Level of Control

In Bardach's (2005) method for policy analysis, the first step is to define the right problem. Among the several suggestions for how to do this, one is the principle "Think in terms of deficit and excess". The excessive margin calls made by Leeson is an example of this and noting that should, as previously mentioned, have been a trigger to Barings' management to either enforce business controls defined by a policy designed to guide control of securities related business processes, or, to (re-)design policies focused on enforcing proactive monitoring of margin calls.

Assuming that Barings' management team had noticed the excessive margin calls, they could have taken the following actions.

(1) Review the policy and standards inventory to make sure that appropriate controls were in place and enforced across the Barings business system to:

i. monitor key securities trading business processes;
ii. adequately separate Front (i.e., sales) and Back office (i.e., account reconciliation) functions;
iii. analyze impact of securities business on Barings overall business.

If actions had been taken to address any of these issues, it would have resulted in improved the control over the business system and therefore reduced the probability of the system transitioning to a catastrophic state.

(2) Establish and implement new policies and standards based on a policy problem gap analysis. For example, applying the "diagnose conditions that could cause problems" rule (Bardach, 2005), could have lead Barings' management team quickly to request the separation of Front and Back office functions and perhaps even removed Leeson from his position, given his lack of experience in the securities trading area.

However, as described in numerous case studies (e.g., Chew, 2006), and mentioned in a previous section, Barings' management neglected reports from their Internal Audit organization and apparently did not understand the nature of the securities business. In general, not understanding the nature of the business you operate in almost automatically leads to an unhealthy business state since it will be very difficult to establish an appropriate policy life cycle management process and as a result an effective management control system. A more recent example are the problems of the European Aeronautic Defence and Space Company following the production delays of the A380 aircraft.

Fig. 4 illustrates how policies can be used to define feedforward control loops to complement the conventional feedback loops – and perhaps even compensate for them, should they fail. What this means is that management actively looks for expected behaviours, rather than wait for failures. This will enable the early detection of risky and non-compliant practices, hence help guide management decisions to prevent loss of control. While Fig. 4 portrays this at an overall system level, similar loops can be constructed for various layers of a business system. As a result, policies can be used to define the "laws" or desired organizational regularities and to set requirements for the business control system.

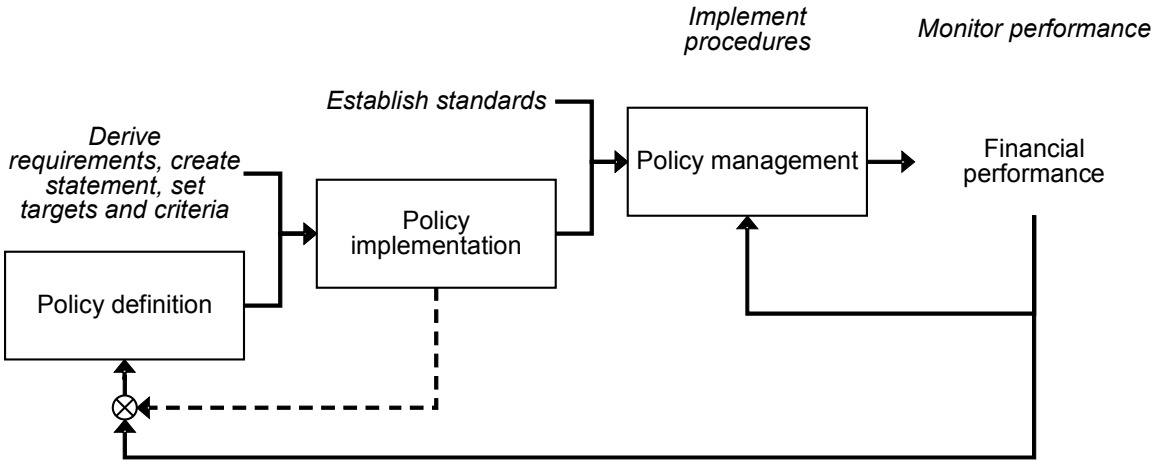

Fig. 4: Linking policy design and management to business control monitoring

4 CONCLUSIONS

A business system's ability to persist over time depends on its ability to proactively identify and manage the impact of unexpected and/or disruptive events. A key premise of the present work is that an organization's ability to manage risk will create conditions that facilitate the emergence of resilience and thereby contribute to the system's longevity. We proposed that an organization's ability to design and manage policies will enable it to reduce the risk of loss of control and improve its degree of control. In particular, the goal was to use the previously proposed state view of business systems to

drive the way policies are design and as well as the way they are managed. The proposed framework has been illustrated using the Barings case and has shown how concrete guidelines, for instance Bardach's policy analysis steps, can be used to target areas in which policies ought to be established and/or developed.

REFERENCES

Bardach, E. (2005). *A Practical Guide for Policy Analysis. The Eightfold Path to More Effective Problem Solving*. Washington D.C.: CQ Press, USA.

Barkley's Comprehensive Financial Glossary: www.oasismanagement.com , accessed on 01-09-06.

Chew, L. (2006). Not Just One Man. Institute of the Chief Risk Officers, www.riskinstitute.ch, accessed on 01-09-06.

Conant, R. C. & Ashby,W. R. (1970). Every good regulator of a system must be a model of that system. *International Journal of Systems Science*, *1*, 89-97.

Holling, C. S. (1973). *Resilience and Stability of Ecological Systems*. Annual Review of Ecology & Systematics, XX , 1-23.

Hollnagel, E. (1998). *Cognitive reliability and error analysis method (CREAM)*. New York, NY: Elsevier Science Inc.

Kurpianov, A. (1995). Derivatives debacles. *Economic Quarterly (Federal Reserve Bank of Richmond)*, 81, 1-24.

Reason, J. (1997). *Managing the risks of organizational accidents*. Ashgate, Aldershot.

Richards, N. (2004). The Problem with Policies. *Credit Union Magazine*, August, 68-70.

Sundström, G. A. and Hollnagel, E. (2006). Learning How to Create Resilience in Business Systems. In E. Hollnagel, D.D. Woods & N. Leveson (Eds.) *Resilience Engineering. Concepts and Precepts.* Ashgate: Aldershot, UK

Sundström, G. A. & Hollnagel, E. (2004). Operational Risk Management in Financial Services: A Complex Systems Perspective. *Proceedings of 9th IFAC/IFORS/IEA Symposium Analysis, Design, and Evaluation of Human-Machine Systems.* Atlanta, GA, USA, September 7-9.

Weimar, D.L. & Vining, A.R. (2005). *Policy Analysis. Concepts and Practice*. Upper Saddle River: Prentice Hall, 3rd Edition.

Westrum, R. (2006). A typology of Resilience Situations. In E. Hollnagel, D.D. Woods & N. Leveson (Eds.) *Resilience Engineering. Concepts and Precepts*. Ashgate: Aldershot, UK