Chapter 15

RESILIENCE IN RISK ANALYSIS AND RISK ASSESSMENT

Stig Johnsen

Abstract Resilience is the ability of a system to react to and recover from disturbances with minimal effects on dynamic stability. Resilience is needed as systems and organizations become more complex and interrelated and the consequences of accidents and incidents increase. This paper analyzes the notion of resilience based on a literature survey and an exploration of incidents. In particular, resilience involves the ability of systems to undergo graceful and controlled degradation, the ability to rebound from degradation, the presence of redundancy, the ability to manage margins close to the performance boundaries, the establishment and exploration of common mental models, the presence of flexibility in systems and organizations, and the reduction of complexity and coupling. The paper describes how resilience can be included in system development and operations by considering organizations, technology and human factors. Also, it shows how past strengths and weaknesses can be considered in risk analysis to enhance safety, security and resilience.

Keywords: Safety, security, resilience, risk analysis

1. Introduction

Resilience engineering is an important aspect of safety and security due to the increased complexity and connectivity of systems and organizations. Safety is the "freedom from accidents or losses" while security is "the degree of protection against danger, loss and criminals" [10]. Resilience is "the ability of a system or organization to react to and recover from disturbances at an early stage, with minimal effect on the dynamic stability" [5]. Accidents and incidents are often due to a combination of vulnerabilities. The ability to foresee or rebound from accidents and incidents enhances both safety and security. Resilience involves the avoidance and reduction of the consequences of disturbances from a safety and security perspective.

T. Moore and S. Shenoi (Eds.): Critical Infrastructure Protection IV, IFIP AICT 342, pp. 215–227, 2010.

There are resilient systems that are not safe and safe systems that are not resilient; however, our goal is to ensure that systems are both safe and resilient. We focus on oil and gas installations in the North Sea, especially those that use integrated operations. Integrated operations leverage information and communication technology (ICT) to change work processes, improve decision making, enable remote operation of equipment and processes, and move functions and people onshore [11]. Integrated operations are complex and employ technologies so rapidly that learning from prior incidents is difficult because there is little, if any, experience regarding their use. Resilience in integrated operations is critical because the consequences of an accident or incident in an offshore facility can be catastrophic.

This paper attempts to define resilience in terms of a few key principles based on a review of the literature and of incidents in the oil and gas industry. The main questions are: (i) how can resilience be specified in more detail? and (ii) how can resilience be specified in order to enhance safety and security? To increase safety and security, we believe that resilience should be incorporated in a development lifecycle model [10] and in risk and hazard analysis.

2. Approach

Our approach involves the analysis of notions of resilience in the literature [4, 5, 10] along with accidents and incidents in the oil and gas industry related to integrated operations [7] in order to use resilience as a strategy to improve safety and security in complex systems. This is accomplished by specifying a few resilience (functional) principles (e.g., ability to manage margins) and using these principles to describe resilient operational techniques based on organizational, technological and human factors. A resilient organizational technique involving the management of margins could clarify organizational responsibility at the boundaries related to the overlaps between organizations and the interfaces between organizations.

In particular, our approach: (i) performs a literature review focusing on resilience as a strategy; (ii) identifies "tactical" resilience principles as goals, constraints and root causes to support resilience; and (iii) explores these principles in an operational setting in risk analysis. Our literature review attempts to explore previous incidents involving brittle practices and prior successes involving resilient practices. Based on the chain of events, we identify the conditions and the underlying constraints or root causes (e.g., management systems, culture and policies [10]), which we call "resilience principles."

2.1 Accident Models and Accident Avoidance

Accident models help identify resilient events, conditions and constraints [5]. Sequential models assume that accidents have simple linear dependencies and model accidents as malfunctions or failures using constructs such as fault trees. Epidemiological models assume that accidents have complex linear dependencies and model accidents as unsafe acts in combination with weak defenses.

Barrier models assume that accidents are caused by missing barriers or holes in barriers; in this context, resilience can be viewed as the improvement of barriers or better management of barriers using proactive indicators to signal the status of the barriers. Systemic models assume that accidents have non-linear dependencies and model accidents in terms of complex interactions, tight couplings and performance variability [12]. When interactions are complex and couplings are tight, the outcome is a normal accident. Resilience can be explored in this context as a mechanism to avoid normal accidents, i.e., to reduce complexity and/or reduce tight couplings.

Analysis of the positive aspects of safety and security can help avoid incidents and facilitate "bounce back." Consequently, we explore models and theories that have been used to describe positive characteristics of organizations and complex systems such as resilience, safety culture and high reliability organizations (HROs). We attempt to identify principles that would enable accidents to be foreseen and avoided, as well as to increase resilience in general, such as the ability to recover from an adverse situation or reduce the consequences. The notion of a safety culture can help explain accidents and avoid accidents. Indeed, the notion of a safety culture clarifies the differences between carriers in the airline industry [14] – the probability of occurrence of an airline accident varies by a factor of 42 across air carriers, regardless of the standardization of technology, organization and human competence in the airline industry [14]. Many alternative definitions of safety culture exist and there is disagreement about how the culture can be changed or improved; however, in this paper, we focus on the ability to improve safety using safety culture as an element of a change process. Finally, HRO has important positive properties [9, 15], which we explore in order to identify key resilience principles.

2.2 Improving Risk Analysis

A standard development lifecycle model [10] is a useful framework for positioning risk analysis. The steps in the lifecycle model are: conceptual development, design, implementation and operations. We attempt to integrate resilience in the lifecycle model in order to create a framework for improving safety [3]. There are several examples of how resilience can be used to increase safety throughout the lifecycle model. During the concept phase, the objectives and use of resilience can be identified. During the design phase, resilience and proactive indicators can be explored to remove or reduce hazards and incidents; scenario analysis and safety cases can help ensure that safety, security and resilience are integrated. During operations, hazards can be controlled using proactive indicators; the consequences of variability and incidents are reduced or contained by the focus on resilience.

3. Resilience Principles

Based on our exploration of the chains of events in accidents and accident recovery, and an analysis of the literature, we have identified several factors

that contribute to resilience and are applicable to integrated operations in the oil and gas sector.

Woods and Cook [19] describe an improvisation scenario involving manual system and organizational crosschecking to avoid medical administration errors. This is an example of graceful degradation that can be used as a resilience principle. Graceful degradation is a major challenge in information operations where the integration of ICT and process control systems can lead to unanticipated stoppages [7].

An HRO is alert and can foresee unwanted performance by efficiently handling local cues and local interactions. Such an organization has the ability to detect drifts towards boundaries or danger zones. On the other hand, brittle organizations do not read signals well and cannot foresee the occurrence of adverse incidents [18]. The management of margins is a good resilience principle that focuses on the boundaries of acceptable safety performance [13]. This is important in integrated operations, where the failure to manage critical operations is a major cause of incidents [7].

An HRO also has a strong focus on shared beliefs and values that facilitate collaboration, support organizational crosschecking and system insight. Also, common information and information flow across the organization enhances resilience [18]. Problems often arise in integrated operations due to the presence of multiple organizational silos with poor collaboration between ICT and process control personnel [7]. Consequently, engaging common mental models is a good resilience principle.

An HRO has the ability to handle deviations and unexpected chains of events using redundant solutions (organizations, personnel and technology) [15]. Jackson and Madni [6] stress the importance of handling incidents using alternate functions. Thus, redundancy is a key resilience principle. A major hazard in integrated operations is the loss of network communication, which can be mitigated by redundancy [7].

An HRO responds in a flexible manner to unexpected events [2]. Many accidents and incidents in the oil and gas industry can be prevented or mitigated by flexible responses [7]. Flexibility is, therefore, a key resilience principle.

Normal accidents often occur as a result of complexity and the tight coupling of systems [12]. Reducing complexity and tight couplings are key resilience principles. ICT and process control systems used in integrated operations are unduly complex and should be simplified [7].

Based on our discussion, we describe seven resilience principles:

- **Graceful and Controlled Degradation:** Proactive impact analysis must be performed and risky behavior should be identified and mitigated when system functions or barriers are failing. There should be an ability to perform a partial shutdown of functions; this should be designed in the system to ensure safety and security in the intermediate states during the shutdown process. The complementary principle is the ability of a degraded system to rebound or recover and return to normal conditions. The ability to recover is based on knowledge of the state of the system

and human intervention may be needed to aid in the recovery. Effective recovery is based on timely impact analysis and competent mobilization. Organizational competence and the appropriate technical systems can contribute to resilience. This abilities to achieve controlled degradation and rebound from adverse situations are key elements of resilience [16].

- **Management of Margins:** The ability to manage margins is a key aspect of resilience. The effective management of margins ensures that performance boundaries are not crossed; this is accomplished using proactive indicators. Another important aspect is to design for controllability. Extensive testing should be conducted to analyze the ability of a system to manage margins. In addition, testing should be based on worst case scenarios and scenarios involving human decision making in stressful environments. Sacrificial decisions, i.e., decisions that balance productivity versus safety or security, must also be a part of the scenarios. The management of margins should consider the slow erosion of margins and more dynamic sacrificial decisions that lead to the crossing of boundaries. When an optimum stress level is reached, it is necessary to identify the changes of states from positive to negative values using signals and indicators. Margins can be managed by examining trends (e.g., network traffic and network congestion) and reporting maintenance using proactive indicators. Decreases in error rates and increases in reliability can cause the risk of accidents to increase; it is important to measure and manage such drift. Awareness of risks can provide a better measure of accident potential than the actual evaluation of risk; this should also be explored when establishing proactive indicators.

- **Common Mental Models:** The use of common mental models ensures communication and collaboration across systems and organizations. Mental models play an important role in handling deviations and recovery; they also facilitate the understanding of the causes of accidents and learning from accidents [10]. Developing the appropriate mental models is important to improve resilience, but it needs careful analysis and reflection. Key stakeholders and management personnel should participate in the process; the involvement of personnel across organizational silos is key to creating a common understanding.

- **Redundancy:** Redundancy involves having alternate ways to perform a function. The function can be performed by different organizations, by different technical systems or by different procedures. Redundancy supports the ability of a system to degrade gracefully. Redundancy can be achieved via standby spares or through the concurrent use of multiple devices. However, redundancy can introduce complexity and increase the vulnerability to common cause failures. An alternative to redundancy is diversity, which is an aspect of flexibility. The use of redundancy should be assessed and improvements in safety and security should be evaluated

against the costs and unwanted side effects such as increased complexity and the risk of common failures.

- **Flexibility:** Flexibility involves diversity and having different ways of performing a function. Flexibility should incorporate error tolerance; errors should be immediately observable and reversible. Flexibility also involves improvisation (and "thinking outside the box") during stressful situations. Systems should be designed for improvisation and error tolerance.

- **Reduction in Complexity:** Complexity can be reduced by going from proximity to segregation, from common mode connections to dedicated connections, from interconnected systems to segregated systems, from limited substitution to easy substitution, from several feedback loops to few (or no) feedback loops, from multiple and interacting controls to single purpose and segregated controls, from indirect information to direct information, and from limited understanding to extensive understanding [12]. A reduction in the complexity of organizations can decrease the likelihood of accidents, especially those occurring as a result of inefficient organizational structures such as multilayered hierarchies with diffuse responsibilities and poor communication.

- **Reduction of Coupling:** Coupling can be reduced by enabling processing delays, flexibility in sequencing, flexibility in methods used, flexibility in resources, redundancies and availability of substitutes [12].

4. Resilience in Risk Analysis

The resilience principles should be incorporated in a standard development lifecycle model, which has four steps: (i) conceptual development; (ii) design; (iii) implementation; and (iv) operations. An accompanying hazard and resilience analysis must identify future risks as well as positive resilience attributes that can be engineered. Thus resilience, hazards and risks must be analyzed in terms of positive and negative factors.

Hazards, resilience and past successes (accident avoidance) should be identified using techniques such as preliminary hazard analysis (PHA), FMECA and HAZOP [10]. Accident avoidance should be explored in order to understand and support resilience. Resilience should be prioritized based on the impact on safety and cost as with other mitigating actions in regular hazard analysis. Hazards are deemed to be acceptable or not acceptable based on an assessment of hazard criticality. Unwanted side effects of resilience must be assessed and mitigated. The use of proactive indicators to signal safety levels should be discussed in all phases; also, there should be a focus on establishing common mental models. Stakeholders should participate in the entire process; they should reflect on the safety objectives, relevant hazards and resilience. Westrum [17] discusses such a process and emphasizes that organizations that focus on alignment, awareness and empowerment in the workforce are better at address-

ing underlying problems, which ultimately increases resilience. Key results from the phases must be discussed to ensure common understanding and that major hazards and resilience principles have been identified and applied properly. Operations usually involve collaboration across multiple organizations and organizational silos. The process should be performed during the conceptual development phase and should use a complete risk picture that involves perspectives from multiple organizations to ensure that safety and resilience are designed into the system.

4.1 Conceptual Development

Safety, control and resilience should be considered during the conceptual development phase. A list of key functions to be implemented in the system should be listed, and the hazards and relevant resilience principles corresponding to the functions should be identified. PHA may be used to identify hazards. The elimination of hazards and adjustments to achieve resilience should be evaluated by going through the seven resilience principles. Hazards related to boundary conditions should be described and high-level information needs related to boundary conditions should be identified together with proactive indicators.

The main results of the activities related to resilience during the conceptual development phase are:

- Specification of the safety, control and resilience objectives.
- Specification of the accountability (responsibility) of safety and resilience.
- List of functions with the appropriate hazards and resilience principles.
- List of the main boundary conditions to be controlled using proactive indicators.

4.2 Design

During the design phase, the functions to be performed are elaborated and hazard analysis is performed. Experiences from past accidents should be used to identify the hazards and risks; also, experiences from prior successes should be considered to ensure that resilience is propagated in future designs.

HAZOP analysis should be used to build in resilience during the design phase. HAZOP analysis, which is based on systems theory, assumes that accidents are caused by deviations. It has five main steps: (i) documenting and elaborating the design intentions; (ii) identifying the potential deviations from the design intentions; (iii) analyzing the reasons for the deviations from the design intentions; (iv) exploring the consequences of the deviations; and (v) exploring how the deviations and their consequences can be prevented, avoided or reduced.

The results of the HAZOP analysis include the deviations, the possible causes and consequences, and the mitigating actions that are devised with resilience in

mind. The management of margins is a key focus area in resilience engineering. Thus, the testing of boundary conditions and other resilience principles should be elaborated.

The main results of the activities related to resilience during the design phase are:

- List of major hazards in the system.
- Documentation of the critical margins, proactive indicators, and the information and reporting needs related to proactive indicators.
- Test plan focusing on the critical margins and the possibility of degraded operations and recovery.

4.3 Implementation

During the implementation phase, resilience should be integrated in the technical solution, in the organizational routines and in the knowledge and ability of the users of the system. The identified hazards and critical margins should be updated based on decisions made during the implementation phase.

Testing is a key issue related to safety and resilience; it ensures that deviations and degraded performance are handled properly. There should be at least one safe shutdown state and the transition to and from a fully operational state to each safe shutdown state should be defined and tested.

When the system has moved to a safe state, the ability to use the organization and manual procedures on the degraded system should be examined. Also, critical scenarios should be explored; these scenarios should be used in training to enhance the perception and understanding of risk.

The main results of the activities related to resilience during the implementation phase are:

- List of major hazards in the system.
- Documentation of critical margins and proactive indicators.
- Critical scenarios whose exploration increases safety and resilience, and creates the appropriate risk perceptions.

4.4 Operations

Safety and resilience should be managed during the operations phase. Hazards should be controlled and the consequences of variability or incidents should be reduced or contained. Key issues related to increasing resilience are the continuous monitoring of the system, and the tracking of indicators that identify boundary conditions and slow drift towards the boundaries.

An updated list of major hazards and indicators should be available to enhance risk perception and understanding. Dynamic indicators show the performance related to network load, stress levels of individuals in key positions,

levels of alarms and levels of gas emissions or small fires. Drift indicators, on the other hand, show long-range slow drift.

Technical and organizational drift can both impact safety. In many systems, minor daily modifications or small changes in operation can accumulate and create a risky environment. Organizational drift occurs as a result of complacency with regard to risk perceptions in the workplace, which can lead to serious incidents due to the erosion or ignorance of barriers. A safety climate questionnaire [1], which provides data about worker perceptions of safety, is a useful tool for evaluating drift.

It is important to measure and track the development of resilience in the organization as well as the system. Management plays a key role in prioritizing safety versus production. Scenario analyses [1] can be used to examine management prioritization in upward appraisals or managerial scripts. Safety cases should be used to explore emergency preparedness in the organization. Periodic audits and assessments of risk and resilience should be conducted based on unwanted incidents and successful recovery from incidents.

The main results of the activities related to resilience during the operations phase are:

- List of major hazards.
- Documentation of the critical margins and the relevant proactive indicators.
- Subjective assessment of risk.
- Audit of risks and resilience.

5. Discussion

This paper has attempted to answer two questions: (i) how can resilience be specified in more detail? and (ii) how can resilience be specified in order to enhance safety and security? With regard to the first question, based on a literature review, we have suggested a more detailed specification of resilience that describes root causes. The identification of resilience principles is based on accidents (brittle practices) and successful recovery (resilient practices). The three steps in identifying the resilience principles are:

- Identify a chain of events.
- Identify the conditions and lack of conditions.
- Identify the underlying constraints and root causes.

Different root causes are identified based on different perceptions. Thus, different approaches may engage different interpretations of resilience and identify different resilience principles. Clearly, there is no consensus on the list of resilience principles. It is, therefore, important that the principles be considered

as a set, not as individual standalone concepts. Two of the principles mentioned in this paper are also described by Rasmussen [13]: the ability to manage margins close to the performance boundaries, and the ability to achieve graceful and controlled degradation and rebound from adverse situations. These principles embody key issues related to resilience and their presence in the literature provides a degree of validation for our approach.

With regard to the second question of how resilience can be specified to enhance safety and security, we believe that the key is to consider the resilience principles during systems development and as a part of safety management. The resilience perspective improves the quality of a risk analysis. This is based on three arguments. First, the scope of past incidents explored in the risk analysis is increased; the understanding of how to avoid accidents and enhance recovery improves resilience and reduces the risk of future accidents. Second, considering current challenges in the analysis of future risk helps make the unexpected expected, leading to increased focus on graceful degradation and recovery. Note, however, that the ability to rebound and other resilience properties may increase system complexity, which can lead to accidents. Consequently, to avoid increased risk, resilience should be considered during risk analysis just like other mitigating actions. Third, there is increased focus on the management of margins and boundary conditions through the use of proactive indicators; this enhances the understanding of the key processes that influence safety.

Performing risk analyses with and without the consideration of resilience provides an opportunity to compare perspectives and mitigating actions and to identify differences. As suggested by Hale and Heijer [2], the results obtained should be measured in terms of the safety performance of the organization as well as productivity and quality gains.

6. Oil and Gas Production Systems

Safety and automation systems (SAS) are commonly used in integrated operations in the oil and gas sector. These systems comprise production control systems, process shutdown systems and safety instrumented systems. Undesirable ICT/SAS incidents typically involve general virus attacks or unanticipated network traffic. However, it is expected that directed attacks on the oil and gas infrastructure will be encountered in the future.

Key hazards impacting ICT/SAS used in integrated operations are the result of organizational, technical and human factors [8]. The hazards along with their mitigating resilience principles and associated resilience techniques are:

- **Common Failures:** Common failures impacting ICT/SAS are mitigated by graceful degradation. A technical assessment should be conducted to analyze the possibility of common failures due to the loss of power, communications and other common items. Graceful degradation should be achieved using redundant solutions. An organizational assessment should be conducted to identify structures that support graceful degradation.

- **High Network Traffic:** Large amounts of ICT network traffic that potentially impact SAS can be mitigated by graceful degradation. A technical assessment should be conducted to ensure that SAS can handle unanticipated ICT traffic.

- **Poor Collaboration:** Poor collaboration between ICT and SAS professionals can be mitigated by using a common mental model. An organizational assessment should be conducted with the goal of establishing design teams with cross-functional ICT and SAS competence. It is necessary to improve risk perceptions and awareness of the challenges when developing critical software that spans ICT and SAS. Also, it is necessary to conduct hazard analysis involving ICT and SAS personnel.

- **Virus Attacks:** Directed virus attacks that halt production can be mitigated by reducing complexity. A technical assessment should focus on hardening computers and reducing services that are connected to critical infrastructure components such as SAS. Virus attacks can also be mitigated by managing margins. A technical assessment should focus on establishing proactive indicators that identify hazard levels.

- **Communication Infrastructure Breakdown:** A communication infrastructure breakdown that causes the loss of connectivity to onshore facilities can be mitigated by graceful degradation. A technical assessment should be conducted to analyze the availability of an independent communication infrastructure. An organizational assessment should establish clear responsibility and routines; scenarios involving the loss of communications should also be tested. A communication infrastructure breakdown can also be mitigated by managing margins. In this case, a technical assessment should be conducted with a focus on indicators and reporting network traffic and loads.

An assessment of frequency and severity must be performed to prioritize the mitigating actions. Using the identified resilience principles tends to make the list of mitigating actions more complete and helps cover more of the relevant issues. This approach can also be used to improve hazard analysis when resilience is required.

7. Conclusions

Resilience is a highly desirable property for critical infrastructure assets. Resilient systems can react to and recover from disturbances with minimal effects on dynamic stability. Our strategy for incorporating resilience in system development and operations is accomplished by considering organizational, technological and human factors issues. The stragegy is also promising because it engages known strengths and weaknesses in risk analysis to enhance safety, security and resilience.

References

[1] R. Flin, Erosion of managerial resilience: From Vasa to NASA, in *Resilience Engineering: Concepts and Precepts*, E. Hollnagel, D. Woods and N. Leveson (Eds.), Ashgate, Aldershot, United Kingdom, pp. 223–233, 2006.

[2] A. Hale and T. Heijer, Defining resilience, in *Resilience Engineering: Concepts and Precepts*, E. Hollnagel, D. Woods and N. Leveson (Eds.), Ashgate, Aldershot, United Kingdom, pp. 35–40, 2006.

[3] Health and Safety Executive, Organizational Change and Major Accident Hazards, Chemical Information Sheet No. CHIS7, Caerphilly, United Kingdom (www.hse.gov.uk/pubns/chis7.pdf), 2003.

[4] E. Hollnagel, C. Nemeth and S. Dekker, *Resilience Engineering Perspectives – Remaining Sensitive to the Possibility of Failure*, Ashgate, Aldershot, United Kingdom, 2008.

[5] E. Hollnagel, D. Woods and N. Leveson (Eds.), *Resilience Engineering: Concepts and Precepts*, Ashgate, Aldershot, United Kingdom, 2006.

[6] S. Jackson and A. Madni, A practical framework for the architecting of resilient enterprises, *Proceedings of the Third Resilience Engineering Symposium*, pp. 125–132, 2008.

[7] S. Johnsen, Suggested proactive indicators to be used in the oil and gas industry based on a survey of accidents in the industry, presented at the *European Safety and Reliability Conference*, 2009.

[8] S. Johnsen, T. Skramstad and J. Hagen, Enhancing the safety, security and resilience of ICT and SCADA systems using action research, in *Critical Infrastructure Protection III*, C. Palmer and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 113–123, 2009.

[9] T. LaPorte and P. Consolini, Working in practice but not in theory: Theoretical challenges of "high-reliability organizations," *Journal of Public Administration Research and Theory*, vol. 1(1), pp. 19–48, 1991.

[10] N. Leveson, *Safeware: System Safety and Computers*, Reading, Massachusetts, 1995.

[11] Norwegian Ministry of Petroleum and Energy, Om Petroleumsvirksomheten, Stortingsmelding No. 38 (2003-2004), Oslo, Norway, 2004.

[12] C. Perrow, *Normal Accidents: Living with High Risk Technologies*, Princeton University Press, Princeton, New Jersey, 1999.

[13] J. Rasmussen, Risk management in a dynamic society: A modeling problem, *Safety Science*, vol. 27(2-3), pp. 183–213, 1997.

[14] J. Reason, *Managing the Risks of Organizational Accidents*, Ashgate, Aldershot, United Kingdom, 1997.

[15] K. Roberts, Some characteristics of one type of high reliability in organizations, *Organization Science*, vol. 1(2), pp. 160–176, 1990.

[16] G. Sundstrom and E. Hollnagel, Learning how to create resilience in business systems, in *Resilience Engineering: Concepts and Precepts*, E. Hollnagel, D. Woods and N. Leveson (Eds.), Ashgate, Aldershot, United Kingdom, pp. 235–252, 2006.

[17] R. Westrum, Removing latent pathogens, presented at the *Sixth International Australian Aviation Psychology Conference*, 2003.

[18] R. Westrum, A typology of resilience situations, in *Resilience Engineering: Concepts and Precepts*, E. Hollnagel, D. Woods and N. Leveson (Eds.), Ashgate, Aldershot, United Kingdom, pp. 55–65, 2006.

[19] D. Woods and R. Cook, Incidents – Markers of resilience or brittleness? in *Resilience Engineering: Concepts and Precepts*, E. Hollnagel, D. Woods and N. Leveson (Eds.), Ashgate, Aldershot, United Kingdom, pp. 69–76, 2006.