Reliable, Resilient: Towards a Dialectic Synthesis?

Eric A. van Kleef, M.Sc.
Van Kleef Consultancy
Geulwijk 16
3831 LM Leusden, The Netherlands

John A. Stoop, Ph.D.
Kindunos Veiligheidskundig Adviesbureau
Spijksedijk 8a
Gorinchem, The Netherlands

Abstract

Infrastructural and transportation systems have become more and more complex and non-linear. They both have the characteristics of adaptive socio-technical systems. Understanding the actual functional relations and coupling in such systems has become challenging.

This complexity made those systems less tractable, requiring new notions for reliability and safety assessment. Controversies between those notions started to occur, although being counterproductive.

This paper argues to refrain from controversies between safety notions and put those notions into one dialectic synthesis to tackle reliability and safety issues in different kind of systems. System states and safety envelopes are used to illustrate the way several notions cohere. This concept offers a way to regain awareness of the system's dynamic behavior during missions and life cycle among designers and operators.

keywords: resilience; safety; complexity; operating envelope; adaptive systems.

1. Introduction

Infrastructural and transportation systems have become more and more complex and interrelated. They have the characteristics of adaptive socio-technical systems. Understanding the actual functional relations and couplings in such systems has become challenging. The situation awareness of designers and operators is compromised.

Safety studies tend to focus on one organizational level or unit. This results in the danger of system breakdown at the edges between these levels or units (Rasmussen, 1997; Woods, 2003). Different actors use different views on safety and reliability. Safety discussions between organizational levels, stakeholders and disciplines are severely hampered. This calls for a system's approach in which all safety arguments can be viewed together in order to achieve consensus on control and governance.

2. Controversy Between Safety Views

2.1 Quantitative Risk Analysis and Scenario Analysis

The safety debate in the Netherlands has been dominated in the last 20 years by the contrast between probabilistic and deterministic views. After the 1953 flooding in the Netherlands, the Deltacommissie introduced a probabilistic view on the safety of dykes (Maris et al., 1961). The report takes a probabilistic view on the maximum water level that can attack the Dutch coast. The costs that have to be made for the reinforcement of the dykes are then balanced against the economic losses in the case of a flooding.

Traditional safety and reliability studies approach the system failure in a probabilistic way. The use of quantitative risk assessment with industrial installations dates back to 1975, when the U.S. Nuclear Regularity Commission published the (later withdrawn) Reactor Safety Study. The accidents in DSM (1975), Seveso (1976), Los Alfaques (1978) and Flixborough (1994) inspired new European legislation on safety in installations with hazardous materials. This legislation came with the COMAH directive in 1982. In the Netherlands this directive was implemented by introducing the societal risk and individual risk. In spatial planning legislation probabilistic safety calculations were introduced in 1989 (*Omgaan met risico's*, 1989). As a failure criterion a lethal victim was chosen. Societal risk played a role in the design decisions that the government had to make. This way of thinking objectified the safety limits to be taken into account around hazardous installations. Risk is a social construct, which makes it difficult to find an objective risk criterion that is independent of the kind of risk (RIVM, 2003).

Emergency services have difficulties to cope with the probabilistic approach. Van Ravenzwaaij (1994) showed that the capacity that emergency services need, is more related to the number of injuries than the number of lethal victims. Probabilistic methods make it possible to assess safety and reliability quantitatively, but they provide no understanding of dynamic failure modes. Emergency services often talk about the 'maximum credible accident'. The Deltacommissie already concluded in 1961 that it was not possible to assess the sea level during the largest storm surge that could threaten the Dutch shore (Maris et al., 1961). Every scenario has a probability, so no objective way exists to determine the maximum credible accident. Another problem with the maximum credible accident is, that it implies that if we can cope with the maximum credible accident, we can deal with everything. This is a

dangerous misconception. Many scenarios can threaten a system and it is not possible to create a set of scenarios that guarantee that every scenario is catered for. Application of only scenario analyses can lead to inconsistent decisions (Jonkman et al., 2003).

The debate between probabilistic risk information and scenario analyses did not prove constructive. In many projects this discussion was the cause of much delay in the project execution without adding any value to the safety. Both probabilistic risk information and scenario analyses influence people's perception of risk, expressed by the phrase of 'How versus how often' (Hendrickx, 1991). Over the past two decades, notions of affect and emotion, dealing with impact of the subconscious on decision making, risk awareness and acceptance were set against the notion of rational decision making, the (Slovic, 1999; Slovic et al., 2004; Kahneman, 2012). A synthesis between those two approaches seems necessary.

2.2 Safety and Resilience

In order to cope with the system's dynamics, the notion of resilience has been developed. Resilience (from Latin *resilio*: to rebound) means the ability to recover from a disturbance. The resilience notion is used in many fields of research, resulting in many definitions of the same word (Longstaff et al., 2013).

A resilient system can have a large latitude, so it always returns to its old equilibrium point. It is also possible that the system settles at a new equilibrium that is also fit for its function. Holling (1973) made this distinction for ecological systems, observing that some ecosystems vary a large amount but still retain their integrity. He called those systems resilient systems.

An analogy can be found in vessel stability. A vessel that rolls heavily when one enters the vessel seems unstable and has a small initial stability. This is a different kind of beast than the ultimate stability that gives us the maximum load the vessel can bear before capsizing. Some vessels have little sail carrying power and heel easily, but can upright themselves no matter how great the heel angle. They have little initial stability but a large ultimate stability. Other vessels can fly a lot more sail, but are prone to tipping over. After tipping over, the vessel enters a new equilibrium, floating upside down. Their initial stability is large, but their ultimate stability small.

These two kinds of stability are comparable to what Woods et al. (2009) called resilience. Woods et al. distinguished between engineering resilience or resistance on one hand and ecological resilience or latitude on the other. If we look at the example of the heeling vessel, we can compare the initial stability to Woods' resistance and the ultimate stability to Woods' latitude.

In resilience theory the notion of 'emergent properties' is used. Properties are called emergent if they are existent in a system without being explicitly designed. By design, complex systems also contain inherent properties from their subsystems or through interrelations between subsystems. Some additional properties are only

present on the system level and cannot be attributed to one or more subsystems. In such cases the phrasing of ‘system of systems’ is frequently used. This makes it difficult to assign them to one subsystem or another, explaining the use of the word ‘emergent’ for them (Pariès, 2006).

Such a classification of systemic properties can be expressed in the following scheme (Table I).

Table I: Classification of systemic properties

	tractable	**intractable**
stable	robust	redundant
instable	reliable	resilient

In contrast with ‘built in by design’ properties such as robustness, redundancy or reliability, safety and resilience are typically emergent properties of systems. This makes it important to find ways to control emergent properties in the design phase. Emergent properties should not be treated as accidental properties. They need, however, a specialized approach. Because emergent properties are integral properties of the system, it is necessary to control and guarantee them on system level.

Resilience engineering should not be just another way to look at the safety and reliability of a system. There should not be discussion whether one way of looking to safety is better than another. This paper proposes a synthesis between those views.

3. Complexity and Envelopes

3.1 Complexity

Perrow (1999) showed that lack of situation awareness may give rise to system accidents. Perrow first noted that in complex systems accidents could happen that nobody understood. He called these accidents ‘normal accidents’ or ‘system accidents’. Many of these accidents seemed to relate to the complexity and coupling in the system. Perrow pointed at the observability and controllability of the system from the point of view of the operator. In Perrow’s view designing complex and tightly coupled systems make accidents unavoidable.

Of course, Perrow’s view evoked opposition. Many authors argued that it was

possible to create an organization that could cope with complex systems. They called such an organization a high reliability organization. Marais et al. (2004) observed that both the normal accident theory and the high reliability organization theory define the safety problem too narrowly, thereby limiting the progress toward safer systems, and that a systems approach deemed to be necessary to achieve safer systems.

The simplest system is a static system, which stays in one system state during its mission. Typical examples are constructions like bridges or dams. Constructional safety has a longstanding practice of dealing with safety. In the Eurocodes, the European constructional safety directives, several limit states are used. The serviceability limit state is related to the criteria governing functionality, durability, user comfort and appearance. Ultimate limit states are related to situations that jeopardize people's safety or safety of the structure. Margins between loads and strength of the construction are expressed as safety coefficients (Sanpaolesi, 2004).

The design principles of graceful degradation and the prevention of progressive collapse aim at the prevention of sudden collapse in case of overload. Brittle constructions are to be avoided. A construction should begin to bend, than crack. In this way time is gained for the load to be diminished and the people using the construction to evacuate.

Simple linear systems have one equilibrium point. They can either move towards this equilibrium point (stable systems) or move away from the equilibrium point (unstable systems). Periodic movement in linear systems is a limit situation between a stable and an unstable equilibrium. If a linear system is disturbed it will return to its equilibrium.

Non-linear systems can have a more complex behavior. The system can have more equilibrium points. For every system state the system will move towards an equilibrium point. The set of system states belonging to one equilibrium point is called a basin. In case of large disturbances of the system, the system leaves its operational basin and enters another basin. This is the point where non-resilient systems differ from resilient ones. Resilient systems can function equally well in the new basin as they were doing in the old one, whereas non-resilient ones cannot.

Czerwinski (2008: 36-39) views complexity as an intermediate situation between a linear system and a chaotic system. Characteristically, those complex systems can be in several equilibriums. Hollnagel (2008) substituted 'complexity' by 'manageability'. In his view, a system is more manageable if the tractability is high, and the system can be described without many details.

3.2 Safety Envelopes

Reliability, safety and resilience can be considered concentric notions (figure 1). They are not conflicting but should be taken into account simultaneously. In dynamical systems a set of limit states or envelopes exists, defining and allocating responsibilities between infrastructure, process control and human operator performance. Such allocation aims to facilitate recovery and return to safe and stable

system states.

A different approach to safety is to assess the boundaries of safe operation. In aviation the idea of the operational envelope has been developed. The operational envelope is defined as the set of conditions under which the airplane should be able to fly. In construction engineering the serviceable limit state is the equivalent. Van der Top (2010) has made an extension to the operating envelope by defining the viable envelope. The viable envelope marks the boundary where the system is collapsing. In construction engineering the ultimate limit state is used for this condition.

The possible system states can be described with a system state diagram. In such a diagram, the operating envelope bounds the set of system states, where the system is within its design limits. Within the operating envelope, the operator can focus on performance. Outside the operating envelope, focus should be on safety and damage mitigation. The conditions where damage occurs form the viable envelope. After the occurrence of damage, the focus changes to survival and recovery, a focus that is known as resilience. If the limits of resilience are reached, the old system can no longer be re-established and innovation is necessary.

One can state, that while the system is within the operating envelope, it will behave in the way it is designed. The aircraft can be flown within usual safety margins, the construction does not deform too much. Within the operating envelope, the use of the system is aimed at efficiency. Within the operating envelope, the operator should have enough information and enough possibilities to control the system.

The moment the operating envelope is exceeded, the system cannot be used anymore in the usual way. Exceeding the operating envelope, however, does not mean that the system will immediately collapse or become damaged in any other way. The use of the system is now aimed at preventing or mitigating damage. The operator now should have enough information and possibilities to prevent damage.

As soon as the viable envelope is passed, damage occurs. The construction will degrade. The damage is not yet beyond repair. The operation will now be aimed at survival. This is the area where resilience engineering aims at. Now the operator should have the information and possibilities to survive.

In the end, the system breaks down and can no longer be restored. The airplane will crash, the construction collapses. Resilience is aiming at the system’s ability to recover from a disturbance. Improvising or organizational adaptation may be necessary. Outside the resilience envelope the system’s resilience is no longer adequate. The set of conditions where collapse takes occurs, can be called the resilience envelope.

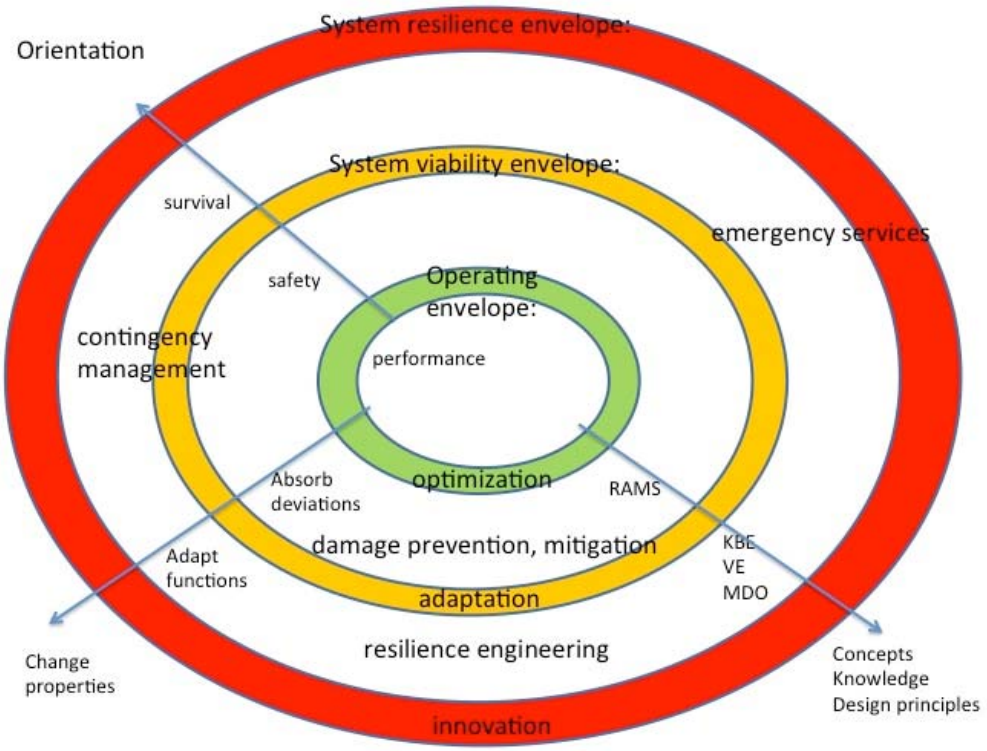

Figure 1: Safety envelopes

The safety margin between the operating envelope and the viable envelope shall be large enough to enable correcting actions to prevent or mitigate damage. In construction engineering it is a usual requirement that the construction should deform a lot before collapsing to prevent brittleness and sudden collapse. The idea is that the large deformation will warn the users to reduce the load in order to prevent collapse. In the same way the safety margin between viable envelope and resilience envelope should also be large enough to enable resilience measures. In this way a system is created that can survive large disturbances, albeit with damage.

Time is a very important factor when looking at safety envelopes. It makes no sense to have a large safety margin between two safety envelopes, if there is not enough time to take mitigating actions. Safety is created because the time that passes between the exceeding of two safety envelopes is enough to take actions. This response time includes the time that is needed to comprehend the situation.

There is of course a relation between the safety envelopes. The viable envelope should include the operating envelope, or damage would occur under normal conditions of use. The resilience envelope should include the viable envelope, or the system would already be beyond repair when damage occurs. These envelopes are a formal description of the idea of graceful degradation. The damage to the system should gradually increase with the disturbance. The system should at first lose its function, then become damaged and only after that, collapse.

Within the viable envelope, an area might exist, where the system will remain within the viable envelope, without the operator taking any actions. Within this area, the system is intrinsically safe. In this case, the operator dropping out will cause the failure of the system to perform its primary function. If a train driver gets a heart attack, the train should come to a standstill. The primary function is not fulfilled, but the train remains safe. The train gets outside its operating envelope, but remains within the viable envelope. Within intrinsic safe situations, the operator can control the system by doing nothing. The most important condition is, that the operator knows he has to do nothing.

4. Evolution in Time

4.1 Life Cycle and Mission

It is useful to distinguish between the time scale of the system's life cycle and the time scale of the system's mission cycle. A mission has a mission profile, being a time-phased description of the events and environments a system experiences from initiation to completion of a specified mission, to include the criteria of mission success or critical failures (Department of Defense, 1981). The life cycle of a system contains one or more mission cycles, associated with a specific operational usage of a system (Department of Defense, 1998).

In a complex system, the operating envelope is normally well inside one basin. The system might encounter a disturbance that brings it into another equilibrium. This might be an accident, forcing the system to alter into a more safety oriented but less performing state (Amalberti, 2006). A resilient system does not break down when exceeding its limits, but enters a new equilibrium. Performance may be less than in the operating state, but the system continues to work.

4.2 Adaptive Systems

During a mission, a dynamic system goes through transient states, sometimes reaching a steady state that can be maintained during a longer time. Between missions the system is typically in a steady or dormant state.

Adaptive dynamic systems adapt their characteristics between missions. Neither the construction nor the procedures of a aircraft change in midair, but between the missions, while the aircraft is on the ground, the characteristics of the system may change. Examples of a change in system characteristics between missions are the installation of new software versions or changes in procedures. Resilience literature tends to focus on these systems.

Organizations tend to economize on the system's attributes that contribute to a large

latitude. These are situations that are not encountered in daily operation and it is difficult to maintain enough sense of urgency on these attributes of the system. This causes systems to become more brittle over time (Woods et al., 2009). Making the resilience margin more explicit may help to stress the importance of resilience to a system's behavior.

During the life cycle of the system, many changes in the system take place. The operational envelope is enlarged, the controllable envelope and the resilience envelope are restrained. The operational envelope is enlarged because this means that the usual business remains undisturbed under more circumstances, bringing more profits to the operating company. A trade-off exists between safety, economy and workload. During operation, the system has a working point that is a result of counteracting forces, like productivity, workload and safety (Rasmussen, 1997; Cook and Rasmussen, 2005). These changes have a repercussion on the safety envelopes. On the next mission the operator may be confronted with a system that has a different behavior than he expects. System behavior that was within safety limits during the latest mission, is now outside the safety limit. This represents drift into failure (Dekker, 2011).

5. Conclusions

Technological systems have become more complex and less tractable, posing new challenges. Those new challenges have induced new safety notions. Systems becoming less tractable and adaptive encouraged the development of resilience engineering, because traditional reliability analysis methods could no longer cope with the problems introduced by those systems.

However, resilience engineering cannot replace reliability engineering. On the contrary, emergence of new safety notions should be seen as a dialectic process. Synthesis should be looked for between resilience engineering and reliability engineering, to handle complex, adaptive systems.

This paper shows a possible way to achieve such synthesis. The relation between operational envelope, viable envelope, and resilience envelope is shown. Analyzing a system by determining those envelopes offers a way to regain awareness of the system's dynamic behavior among designers and operators.

References

Amalberti, R. (2006) Optimum system safety and optimum system resilience: Agonistic or antagonistic concepts. In: Hollnagel, E., Woods, D.D. and Leveson, N. (Eds), *Resilience engineering: Concepts and precepts.* Ashgate, Aldershot, England, pp. 253-271.

Cook, R.I. and Rasmussen, J. (2005) 'Going solid': A model of system dynamics and

consequences for patient safety. *Quality & Safety in Health Care*, vol. 14, nr. 2, pp. 130-134.
Czerwinski, T.J. (2008) *Coping with the bounds: A neo-clausewitzian primer*. CCRP, Washington, DC.
Dekker, S. (2011) *Drift into failure: From hunting broken components to understanding complex systems*. Ashgate, Farnham, England.
Department of Defense (1981) *Definition of terms for reliability and maintainability*. Military standard 721C, Washington, DC.
Department of Defense (1998) *Electronic reliability design handbook*. Military handbook 338B, Washington, DC.
Hendrickx, L.C.W.P. (1991) *How versus how often: The role of scenario information and frequency information in risk judgement and risky decision making*. Ph.D. Groningen, The Netherlands.
Holling, C.S. (1973) Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics*, vol. 4, pp. 1-23.
Hollnagel, E. (2008) The changing nature of risks. *Ergonomics Australia Journal*, vol. 22, nr. 1-2, pp. 33-46.
Jonkman, S.N. et al. (2003) Evaluation of tunnel safety and cost effectiveness of measures. In: Bedford, T. and van Gelder, P.H.A.J.M. (Eds), *Safety and reliability*. Balkema, Lisse, The Netherlands, pp. 863-871.
Kahneman, D. (2012) *Thinking fast and slow*. Penguin, London, England.
Longstaff, P.H., Koslowski, T.G. and Geoghehan, W. (2013) Translating resilience. A framework to enhance communication and implementation. *REA 2013*, Soesterberg, The Netherlands, 25-27 June 2013.
Marais, K., Durac, N. and Leveson, N. (2004) Beyond normal accidents and high reliability organisations: The need for an alternative approach to safety in complex systems. *MIT Engineering systems symposium*, Cambridge, MA, 24 March 2004.
Maris, A.G. et al. (1961) *Rapport van de Deltacommissie. Deel 1. Eindverslag en interimadviezen*. [Report of the Delta commission. Part 1. Final report and interim recommendations]. Staatsdrukkerij, Den Haag, The Netherlands.
Omgaan met risico's (1989) [Dealing with risks]. Appendix to Nationaal Milieubeleidsplan, SDU, Den Haag, The Netherlands.
Pariès, J. (2006) Complexity, emergence, resilience. In: Hollnagel, E., Woods, D.D. and Leveson, N. (Eds), *Resilience engineering: Concepts and precepts*. Ashgate, Aldershot, England, pp. 43-53.
Perrow, C.B. (1999) *Normal accidents: Living with high-risk technologies*. Princeton University Press, Princeton, NJ.
Rasmussen, J. (1997) Risk management in a dynamic society: A modelling problem. *Safety Science*, vol. 27, nr. 2/3, pp. 183-213.
Ravenzwaaij, A. van (1994) *Risico-informatie in het veiligheidsbeleid: Een analyse van de bruikbaarheid van kwantitatieve risico-informatie in het Nederlandse externe veiligheidsbeleid*. [Risk information in the safety policy]. Ph.D. Utrecht, The Netherlands.
RIVM [National Institute for Public Health and the Environment] (2003) *Nuchter omgaan met risico's*. [Dealing with risks down-to-earth]. Rijksinstituut voor Volksgezondheid en Milieuhygiëne, Bilthoven, The Netherlands.
Sanpaolesi, L. (2004) Limit states and method of partial factors. In: Leonardo da Vinci Pilot Project CZ/02/B/F/PP-134007 (Ed), *Basis of structural design.*

Garston (Hedfordshire), England.
Slovic, P. (1999) Trust, emotion, sex, politics and science: Surveying the risk-assessment battlefield. *Risk Analysis*, vol. 19, nr. 4, pp. 689-701.
Slovic, P. et al. (2004) Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk and retionality. *Risk Analysis*, vol. 24, nr. 2,
Top, J. van der (2010) *Modelling risk control measures in railways: Analysing how designers and operators organise safe rail traffic*. Ph.D. Delft, The Netherlands.
U.S. Nuclear Regulatory Commission (1975) *Reactor safety study: An assessment of accident risks in US nuclear power plants*. WASH-1400.
Woods, D.D. (2003) *Creating foresight: How resilience engineering can transform nasa's approach to risky decision making*. Testimony on *The Future of NASA* for Commitee on Commerce Science and Transportation, John McCain, Chair.
Woods, D.D., Schenk, J. and Allen, T.T. (2009) An initial comparison of selected models of system resilience. In: Nemeth, C.P., Hollnagel, E. and Dekker, S. (Eds), *Preparation and restoration.* Ashgate, Farnham, England, pp. 73-94.