A quick and dirty evaluation of resilience enhancing properties in safety critical systems

Björn JE Johansson[1] and Mattias Lindgren[2]
[1] Saab Security, BOX 15042, 580 15 Linköping Sweden, Country
bjorn.j.e.johansson@saabgroup.com
[2] Combitech AB, BOX 15042, 580 15 Linköping Sweden, Country
mattias.lindgren@combitech.se

Abstract. During the last years, there has been a great interest in the concept of resilience within the scientific field. The awakening of industrial interest in the concept is however a recent phenomenon. As most practitioners in safety-oriented businesses tend to prefer well-established methods and concepts, resilience engineering may still have a long way to go before it has practical impact on implementation of safety measures. This paper consists of a first step in this direction, presenting an outline for a quick & dirty evaluation method, aiming to evaluate system properties that affect the resilience of an organisation or a system.

1 INTRODUCTION

Resilience engineering is, to our interpretation, a part of the overarching field of engineering safer systems. While several traditional methods within safety engineering aims at improving safety by identifying and minimizing risks, resilience engineering aim at improving a systems capacity to cope with unexpected disturbances (Sheridan, 2008). During the last years, there has been a great interest in the concept of resilience within the scientific field (Hollnagel et al, 2006; Hollnagel & Rigaud, 2006; Woltjer, et al, 2007). The awakening of industrial interest in the concept is however a very recent phenomenon. As most practitioners in safety-oriented businesses tend to prefer well-established methods and concepts, resilience engineering may still have a long way to go before it has practical impact on implementation of safety measures. This paper consists of a first step in this direction, presenting a quick & dirty evaluation method, aiming to evaluate system properties that affect the resilience of an organisation or a system. The intention to create a 'quick & dirty' arises from pragmatic needs of practitioners in the field. Concurrent investigation methods related to resilience, such as FRAM (Hollnagel, 2004) or STAMP (Leveson, 2004), have great potential in for example accident investigation or high-level risk analysis. However, they also share two practical drawbacks, namely 1.) they demand extensive theoretical- and domain knowledge, and, 2.) they are comparatively time demanding in relation to methods used in industry. Our aim is to create a far more simple method that can give a rough indication of an organisation or a system's resilience. The aim is thus not to create detailed descriptions of systems or events, but rather to evaluate whether the organisation/system can present basic properties that indicate resilience to disturbances or not. This assessment is then to be used as a basis for resilience-improving actions. The theoretical basis for the evaluation is founded on system properties that have been pointed out in earlier research, such as flexibility, redundancy, monitoring capacities etc. Practically, the tool will be a form or a query that the investigator use as a basis for his/her evaluation.

2 ENGINEERING RESILIENCE

In contrast to the theoretical perspectives on resilience (see for example Hollnagel et al 2006 or Woltjer et al. 2007) stands the pragmatic need of a practitioner faced with the task of improving resilience in an organization or a system. Although a practitioner preferably should be accustomed to basic perspectives on safety and resilience, there is no guarantee that it is the case. Safety work is indeed often carried out using traditional methods that have a well developed set of tools to support the process. Such methods are often based on comparatively 'old' perspectives on safety such as PSA, Fault trees or other models based on linear causation in some form (Hollnagel et al., 2006; Sheridan, 2008). Such models can be very powerful, but they are generally not designed to cope with events beyond the foreseeable, focusing on introducing barriers against known threats (Hollnagel, 2004). Resilience Engineering is in many respects a response to the limitations of such perspectives, focusing on flexibility and adaptive capacities of an organisation or a system. However, the field of resilience engineering has not yet reached the maturity of its predecessors in the respect of available methods to be applied 'in the field'. Sheridan (2008) compares resilience engineering with earlier methods and concludes that:

> "It is now too early to expect resilience engineering to offer much in terms of quantitative models, but eventually human factors engineers will demand it."
>
> (Sheridan, 2008, p. 425)

Although Sheridan's statement about human factors engineers in general demanding quantitative methods may be a little exaggerated, there is definitely a demand for some kind of method, be it quantitative or not. To our experience, safety assessments are in practice only based on quantitative measures to some extent; a large part is based on subjective, or 'anecdotal' data. Methods that help the investigator to identify areas and structure data gathering can thus be of great help even if they are not purely aimed at providing a quantitative assessment. Suppose that someone representing a safety-critical organization asks you to help them with assessing their 'resilience'? This is not an unrealistic question for the practitioner – he or she often face the situation of having to make an assessment of 'how safe' something is, the question on how resilient something is, is bound to emerge.

3 A QUICK AND DIRTY METHOD FOR ASSESSING RESILIENCE

As indicated above, pragmatic needs exist for a resilience assessment method that is easy to use. We suggest a simple method that can give a rough indication of an organisation or a system's resilience. The tool is in the form of queries that the investigator use as a basis for his/her evaluation. In addition to this, descriptive information about the overall purpose of the system under investigation and the context in which it operates has to be described. The tool does not make any claims to be a complete assessment tool for resilience. Even in the unlikely event that such a tool should be possible, this tool is mainly designed to make a swift assessment which could be a basis for deeper analysis. We have identified three main analytical steps that has to be undertaken, namely a definition/description of the system, a description of the environment in which the system exists and an evaluation of the resilience enhancing properties. These categories are decomposed into specific questions, where each question is scored. The final outcome is not intended to be a singular score, but rather a set of scores that describes the strength and weaknesses in terms of resilience. The outcome of an investigation is thus a 'resilience pattern' rather than a score. Since most systems/organisations also only share some basic characteristics, some adaption of the query is probably necessary depending on the type of system under scrutiny.

3.1 Definition/description of the system

The purpose of this is to state the purpose/function of the system. It is an essential starting point for the assessment of resilient properties to follow since the evaluation has to be based on a basic understanding of the system/organisation under investigation. The questions asked on this level are objective in the sense that there official descriptions and documentation that answers them in almost every case should exist. A fixed query is not appropriate on this level since the concerned questions will vary depending of the type of system/organisation. There are three main clusters that have to be answered:

System purpose: What is the main task of the system/organisation?: production, administration, safety etc. This cluster gives an indication to the kind of goals the system will pursue – the driving variables - for example a system focusing on production is likely to aim on maximising profit, while a system focusing on safety will make different prioritizations. Naturally, all systems will exhibit most of these driving variables, but this will at least give some indication.

Maturity of the system/organization: Is this the first version of the system/organisation? How long has the system/organisation existed? Number of experienced employees? Recent organizational changes (how many)? This cluster gives an indication on how experienced and competent the system is, but also how stable it is. A well established system with many senior employees is likely to have a broader repertoire of actions that can be produced in the event of an undesired development. A system that often is re-organised is likely to respond slower to events since confusion could emerge regarding responsibilities and resources available.

Development process/validation of system/organization: How was the design of the system/organization conducted? Was it evolutionary? Is validation/testing part of the process? Are standards used? For systems with a short operating history, these are highly relevant questions when assessing resilience. By knowing how the design of the system/ organisation was conducted, the investigator will get some indication on whether the designer (if there is one) has taken flexibility and adaptation into account, or if the system is intended to work in only one state of stability (Lundberg & Johansson, 2007).

3.2 Description of the system/organisation environment

When the basic properties of the system/organisation are described, the environment in which it exists should be described. As in for example CREAM (Hollnagel, 1998), performance conditions beyond the control of the system/organisation must be known in order to understand the operating conditions. These are also hard to formalise into strict query-questions, and the investigator should take guidance from the suggested ones and adapt according to circumstances. Again, there are three sets of questions.

Climate: What are the weather conditions (if relevant)? Is work mainly conducted in-doors or out-doors? Is the work/equipment sensitive to heat/coldness, humidity, dust, water, icing (as for example airline operations)? These questions provide answers to some basic issues about the operating conditions. A system/organisation operating in varying conditions also have to be able to monitor and make prognoses about them, otherwise it has to be able to cope with changes rapidly.

Temporal conditions: Are there operations around the clock? Does workload indicate a risk for fatigue? Is it common with sudden changes in workload? Is there external time-pressure (for example production demands, deadlines etc)? Are there 'time windows' in which control actions have to be performed? The temporal conditions indicate if the system/organisation has to cope with factors that may impair safety and resilience. It is common knowledge that human performance is affected by having to work odd hours, lack of sleep or stress. Systems/organisations that operate under such temporal conditions are less likely to be able to maintain safety and preparedness for unforeseen events.

3.3 Evaluation of resilience enhancing properties

In the evaluation of resilience enhancing properties, the investigator works with a query. In the example below, only extremes on the end of a scale is shown. The exact scale could vary from a very rough one (for example 1-3) to a wider range depending on the system/organisation investigated. The query is divided into two sets, detection and adaptation. This is based on the basic idea that resilience comes from the capacity of detecting unwanted developments and the ability to respond to such developments. After the investigator has made his/her assessment, the outcome of the scoring will form a pattern in the two sets, presenting a distribution of scores. This distribution can then be used to firstly assess in which area(s) the system/organisation lacks resilience, and then also gives a more specific indication of where there are problems that need looking into. We expect that more properties will be added to those presented below in tables 1. and 2.

as the method is used in practice. It is important to notice that the scoring of the properties listed below depend on the individual judgement of the investigator.

Table 1. Resilience enhancing properties - detection

Property	**Negative**	**Positive**
1. Capacity to predict changes in the process/environment	Low predictability of changes	High predictability of changes
2. Possibilities of detecting differences between normal (desired) and non-normal (undesired) states.	Low probability to detect differences between desired and undesired events.	High probability to detect differences between desired and undesired events.
3. How are detected problems disseminated within the system/organisation?	Very limited potential for dissemination of problems within system	Very efficient dissemination of detected problems within system
4. Time available to be able to identify unwanted events	Very limited time	No limitation of time for impact on potential for identification

Motivation: 1.) A system which cannot predict changes is likely to be taken by surprise, giving less time for counter-measures. 2.) The greater the difference between desired and undesired states, the easier it is to detect anomalies 3.) If a detected deviation cannot be disseminated to concerned parts of the system/organization, response may be delayed or lack completely 4.) If too little resources are given to monitoring, there is little chance of detection of undesired developments.

Table 2. Resilience enhancing properties - adaptation

Property	**Negative**	**Positive**
1. Possible states available (shutdown possible, “graceful” degradation possible, emergency states available, reversibility etc)	No possible states except for operational	Several states available
2. Potential for controlling external variables.	Limited potential for controlling external variables	Great potential for controlling external variables

3. Willingness in organisation to temporarily relax the efficiency goal for the safety goal when circumstances suggest doing so.	No willingness in organisation	Great willingness in organisation
4. Willingness in organisation to temporarily deviate from regulations when circumstances suggest doing so.	No willingness in organisation	Great willingness in organisation
5. Resource preparedness, availability of resources	Low availability of resources	High availability of resources
6. To what degree does employees understand the organisation and overall system functioning	Degree of understanding in organisation of overall system functioning is low	Degree of understanding in organisation of overall system functioning is high
7. Potential for learning from past experiences.	Low potential for learning from past experiences	High potential for learning from past experiences
8. Functional redundancy	No functional redundancy	Total redundancy of functions
9. Site specific	System/organisation is totally site specific	System/organisation is not at all site specific

Motivation: 1.) A system that can perform at different operating states is more resilient than a system with only one or few operating states 2.) A system/organisation that can control or limit external influence is less sensitive to changes in the surrounding world 3.) If the system/organisation is unwilling to relax efficiency goals, resources needed to cope with disturbances may be unavailable in straining situations 4.) A highly autocratic system/organisation may be inflexible and overly rule-bound even when flexibility and adaption is needed to cope with unwanted developments 5.) Systems/organisations with little slack in terms of resources have less chance to maintain an acceptable degree of performance when resources are needed to cope with disturbances 6.) In highly specialised systems/organisations, understanding of overall system functioning may lack, providing little flexibility in terms of switching roles etc 7.) By learning from earlier disturbances, the performance repertoire for coping with such events can be increased 8.) A highly redundant system/organisation can cope with disturbances by using back-up functions or transferring a task in the event of a break-down of a original function 9.) A system/organisation that easily can be moved from one physical location to another will be less affected by location-specific disturbances. (for example fires, earthquakes, storms etc).

4 DISCUSSION/CONCLUSION

An assessment of this type can easily be criticised from a scientific point of view for being overly simplistic, mixing theoretical concepts or lacking in accuracy. Neither are the properties suggested for investigation new, most of them have already been suggested, but in different publications. For example, step 2. is similar to a CPC in CREAM (Hollnagel, 1998) and step 3. above has many similarities with the properties suggested by Wreathall (2006) and Foster (1993). But, by combining these different sources, we believe that this poster contributes by presenting the outcome of resilience *engineering*, i.e. the construction of a new tool aimed at improving resilience. The aim is to give the practitioner that has not followed the development of the resilience engineering movement a tool that can be used as a complement to 'traditional' methods. This is line with an earlier paper by Lundberg & Johansson which suggests that stability enhancing measures must be combined with resilience enhancing measures (2006). As stated in the introduction, the main advantage of the assessment is that it can be performed within a reasonable (from an industrial point of view) period of time and without much theoretical background knowledge. As the Quick & Dirty method still has not been tested in practice, our next aim is to try it in practice and examine how useful it actually is. By this we do not necessarily mean a scientific evaluation, but rather to examine how it is received by safety engineers – do they experience the method as helpful, and does it meet any of the demands put on them by their 'customers'?

REFERENCES

Foster, H. D. (1993) Resilience Theory and System Evaluation. In (Eds.) J. A. Wise, V. D. Hopkin & P. Stager, *Verification and Validation of Complex Systems: Human Factors Issues.(pp. 35-60)* Springer Verlag: Berlin.

Hollnagel, E. (1998) *Cognitive Reliability and Error Analysis Method*. Oxford: Elsevier Science Ltd.

Hollnagel, E. (2004) *Barrier analysis and accident prevention.* Aldershot, UK: Ashgate

Hollnagel, E. Woods, D.D. and Leveson, N. (2006) *Resilience Engineering: Concepts and Precepts*. Aldershot, UK: Ashgate.

Hollnagel, E. & Rigaud, E. (2006) Proceedings of the Second Resilience Engineering Symposium, 8-10 November, Antibes, Juan-les-Pins, Paris: Mines Paris, Les Presses.

Leveson, N. (2004) A new accident model for engineering safer systems. Safety Science,42(4) 237-70.

Lundberg, J. & Johansson, B. (2006) Resilience, Stability and Requisite Interpretation in Accident Investigations. In (Eds.) Hollnagel, E. & Rigaud, E. *Proceedings of the Second Resilience Engineering Symposium*, *(pp. 191-198)* 8-10 Nov 2006, Ecole des Mines de Paris: Paris.

Lundberg, J. & Johansson, B. (2007) Pragmatic Resilience. In (Eds.) Woltjer, R., Johansson, B. & Lundgren, J. *Proceedings of the Resilience Engineering Workshop (pp. 37-41)* 25-27 June, Vadstena, Linköping: Unitryck. (www.ep.liu.se/ecp/023/)

McDonald, N. (2006) Organizational Resilience and Industrial Risk. In (Eds.) Hollnagel, E., Woods, D. D. & Leveson, N., *Resilience Engineering: Concepts and Precepts*. *(pp. 155-179)* Aldershot, UK: Ashgate.

Sheridan, T. B. (2008) Risk, Human Error, and System Resilience: Fundamental Ideas. *Human Factors*, 50(3) 418-426.

Westrum, R. (2006). A typology of Resilience Situations. In (Eds.) Hollnagel, E., Woods, D. D. & Leveson, N., *Resilience Engineering: Concepts and Precepts*. *(pp. 55-65)* Aldershot, UK: Ashgate.

Wreathall, J. (2006).Properties of Resilient OrganizationsIn (Eds.) Hollnagel, E., Woods, D. D. & Leveson, N., *Resilience Engineering: Concepts and Precepts*. *(pp. 258-268)* Aldershot, UK: Ashgate.

Woltjer, R., Johansson, B. & Lundberg, J. (2007) *Proceedings of the Resilience Engineering Workshop*, 25-27 June,Vadstena, Linköping: Unitryck. (www.ep.liu.se/ecp/023/)