Pragmatic Resilience

Jonas Lundberg and Björn Johansson

Department of Computer and Information Science, Linköpings universitet, Sweden
{jonlu, bjojo}@ida.liu.se

Abstract. There are different approaches to achieving persistence in system safety functions in the face of disturbances. Whereas some systems strive towards only maintaining stability of one stable state of maximum performance, other systems also rely on resilience, on the ability to make transitions to other stable states, of lower performance, when facing changes to driving variables or state variables. We discuss three kinds of systems, stable, bi-stable, and multi-stable systems, and their persistence when facing regular, irregular, and unexampled events.

1 INTRODUCTION

The aim of resilience engineering is to achieve persistence in systems functions in the face of disturbances. In particular, we are interested in persistence of the safety functions of the system. The focus thus lay on persistence of functions, rather than persistence of physical components that realize the functions. When engineering the resilience of a system, it is vital to balance the ability to achieve stability in the face of regular disturbances and threats, with the ability to achieve adaptive behavior when facing more irregular or unexampled events (Lundberg & Johansson, 2006). That can be summarized as

- The ability to respond, quickly and efficiently, to regular disturbances and threats.
- The ability continuously to monitor for irregular disturbances and threats, and to revise the basis for the monitoring when needed.
- The ability to anticipate future changes in the environment that may affect the system's ability to function, and the willingness to prepare against these changes even if the outcome is uncertain.

To engineer resilience, we need to know something about the variables we wish to control, and something about the variables that might be in flux. If these are well-known, the principal strategy may be increased stability. Physical barriers and safeguards are primary examples. If they are less well-known as in irregular events, the primary strategy may be to control the transitions between states of stability, to avoid both long periods of instability, and states of functional extinction. Examples of that may be to go from a stable up-time state of a nuclear facility, to a stable down-time state. Furthermore, the exact state to reach or how to manage the transition, may be partly unknown at the time of the event, and may have to be invented as the event unfolds, such as in the flooding of New Orleans. When ecologists use the term resilience, the variables that describe the system are called state variables, and those state variables that affect other variables, are called driving variables. For instance, economy and the acceptance of

risks are often seen as important driving variables for safety, affecting the states of many other variables, such as the existence of backup resources, or physical safeguards.

What we will discuss in this paper is different kinds of systems, and how they are characterized in terms of their ability to perform transitions between different functional states. We will also discuss some of the driving variables that affect the viability of safe transitions.

2 WHEN AND WHY IS A SYSTEM RESILIENT?

A system can be described in terms of functional states and state variables, together with state transitions (Ashby, 1960). State transitions can be described in terms of the variables that drive the system from one state to another between different stable states, or towards extinction (non-function in terms of functional states). Systems can also be described in relation to different event types in their environment that affect state variables or driving variables. This will be elaborated below.

2.1 Transitions between Functional States

A 'functional state' is a level of performance that a system can achieve under specific performance conditions. For example, an air traffic control center can, under normal operating conditions (equipment fully operational, normal weather, fully manned) handle a certain number of flights. In the case of a breakdown in for example a technical system needed for handling flights, performance will be hampered and this number will be reduced. The system will move from one functional state to another. However, as the observant reader notices, it is not self-evident that such a transition is possible. First of all, there has to be state to make a transition to. Secondly, some type of safe way to perform the transition must exist. A common approach to this is to keep an old technical system, with a certain performance level, operational when introducing a new one with a higher performance level. As long as the old system is operational and the personnel know how to use it, it will be possible to step back to it.

2.2 Driving Variables

The ability to make transitions between different functional states is essential for anyone that aim at creating a viable system. But the system characteristics promoting this ability must also be created and maintained. The driving force behind this, or the 'driving variable', is, in theory, safety. By creating barriers, redundancy and capacity for coping with different kinds of events, we improve stability and resilience. However, we must not forget that the driving variables in most real-world systems are not safety nor resilience, but rather other things such as profit, simplicity and complacency. When suggesting to a company CEO that safety should be improved, the first question is not likely to be "how?" but rather "how much will it cost?". When instructing a worker on the factory floor that he/she should check his/her equipment every day, he/she may firstly be enthusiastic, but when some time has passed, the checks are likely to become

more rare, or even stop completely. Although there are examples of highly reliable organizations, even those sometimes have accidents, and such accidents often have high consequences.

2.3 Stable, Bi-Stable, and Multi-Stable Systems

To exemplify the difference between stability and adaptivity through the transition between states, we can consider three kinds of systems, *stable, bi-stable* and *multi-stable systems*. These systems can in turn have control systems, which may be in need of protection, an issue that is termed the Matryoshka problem. That problem is discussed in detail in Lundberg and Johansson (2006). The state variables of a system, for instance the number of fire trucks in a fire brigade, are driving variables for the function of controlling fire, in a forest fire-fighting situation. The state variables of the system in turn have driving variables, such as economy. In the following three examples we describe the stable, bi-stable and multi-stable system types. We consider stable states to be states where the system has some level of functioning, whereas the alternative is states of functional extinction. The levels of performance may differ between stable states, and we assume that most systems strive towards states of as high performance as possible, while still being safe.

Firstly, we have the *stable system*. Here, stability is increased by defenses such as barriers that deflect damage, and by having spare resources, giving slack to the system. For instance, there might be resources for buying new kinds of equipment, or many spare parts for equipment. The idea here is to re-establish the previous control organization as soon as possible. This system does not adapt to unknown circumstances, only to the previously foreseen. The resources are driving variables, whereas items and people in the system are state variables. The key characteristic of a stable system is that is *stable in relation to one state*, to which it constantly tries to come back.

Second, we have the *bi-stable system*. This system may for instance be prepared for a loss of hierarchical control, where top level nodes are lost. The preparation could for instance consist of exercises in independent actions of remaining nodes, and establishment of cooperation between nodes. The state of instability is the transition stage, during which the functionality is not working as in the stable states. In this example, the state of instability might persist, if also one or more of the lower level nodes are damaged. The system can thus *strive towards a limited set of different states*, depending on damage to the state variables. Driving variables of the transitions are for instance resources and redundancy of skills to take up the roles needed for the alternative states.

Third, we have *multi-stable systems*. For instance, rescue services might need many different kinds of configurations, depending on the situation they face. Preparation is also in this case exercises in establishing different organizational setups, but it is done more thoroughly than in the preceding case. A multi-stable system can thus *adapt to a number of different states*. In this case, the driving variables are things like the economical resources for achieving more external resources, and the state variables are associated with the size of the event. If the size of the event surpasses the ability of the organiza-

tion, it might loose functionality, to the extent of complete loss of functionality (extinction). Another typical characteristic of multi-stable systems is the ability to reconfigure, or join up with other systems, forming an ad-hoc configuration with different capacities than the individual parts. The system might also be able to invent new ways of coping, increasing its performance.

2.4 Events

Systems may be subjected to events that affect the state variables or the driving variables. Ron Westrum describes three different types of events that can be related to resilience, *regular, irregular* and *unexampled* events (Westrum, 2006). The regular event is well-known, for example machine failure or bad weather. Irregular events are possible to imagine, but are normally so rare (or expensive to handle) that little specific preparation is taken. Earthquakes, large fires or chemical outlets are typically mentioned as examples of irregular events. Unexampled events are so rare that normally no organized mechanisms for coping with them exist. The 9/11 terrorist bombing or the flooding of New Orleans are often mentioned as examples of unexampled events. If a system is to be considered as 'safe', it needs to present stable characteristics in the face of regular events, a mixture of resilience and stability in the face of irregular events and finally high resilience when facing the unexampled.

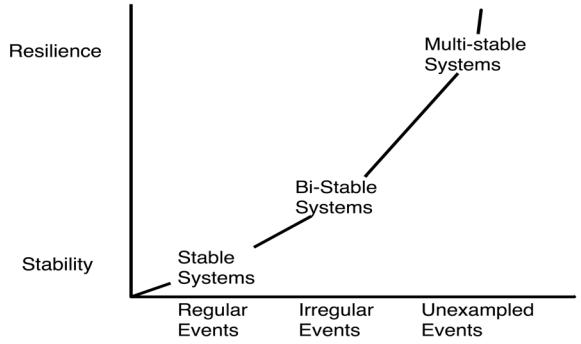

Figure 1. The relation between Westrum's event types and the different system types in relation to the stability-resilience continuum.

There is thus a connection between the stable, bi-stable and multi-stable systems and the event types (see figure 1.). In other terms, a 'safe' system must match the variety of its environment, as in the case of the law of requisite variety described by Ashby (1956). Different types of systems have different abilities to do this by practically coping with changes in the environment (McDonald, 2006).

3 DISCUSSION - PRAGMATIC RESILIENCE

To engineer resilient systems in the face of regular, irregular, and unexampled events, we need strategies for engineering state transitions, and for monitoring the driving variables that make safe state transitions possible. Due to the Matryoshka problem and the

occurrence of unexampled events, we can never be completely safe. However, we can strive towards maximizing the safety of each system that we in practice can affect. Epstein pointed out the logical problem that resilience is something that cannot be measured until the fact of impact (Epstein, 2006). This is true in one sense, but not very helpful from a resilience engineering perspective. Instead, we suggest another approach: on the one hand, we may be unable to foresee some kind of events, like unexampled ones. On the other hand, we can always ask our selves what will happen if a system is exposed to a disturbance or loose its intended functional state, regardless of the cause. Since we are aware that things that cannot be predicted are bound to happen it is far easier to simply try to describe what happens if one or more stable states are lost than to try to predict all possible disturbances and prepare for them. As long as some possible state to move to exists, the system at least has a theoretical possibility to survive.

A last important point is the fact that systems are vulnerable and low performing when they are in a state of transition between stable states. Transitions may also be characterized by uncertainty, especially in multi-stable systems if the system adaptively is searching for a stable state. The duration of the transition is another factor: if the time needed to make a transition is very long, the system may be of little or no use during that time. To promote the ability to make rapid transitions is thus essential if the system operates in a context where time is limited, as most safety-critical systems do.

REFERENCES

Ashby, W. R. (1956). *An introduction to cybernetics*. London: Chapman & Hall.

Ashby, W. R. (1960). *Design for a brain: The origin of adaptive behavior* (2nd ed.). London: Chapman & Hall.

Epstein, S. (2006). Unexampled events, resilience and PRA. In E. Hollnagel & E. Rigaud (Eds.). In E. Hollnagel & E. Rigaud (Eds.), *Proceedings of the Second Resilience Engineering Symposium* (pp. 105-116), Antibes, Juan-les-Pins, France, 8-10 Nov.

Lundberg, J. & Johansson, B. (2006). Resilience, stability and requisite interpretation in accident investigations. In E. Hollnagel & E. Rigaud (Eds.), *Proceedings of the Second Resilience Engineering Symposium* (pp. 191-198), Antibes, Juan-les-Pins, France, 8-10 Nov.

McDonald, N. (2006). Organizational resilience and industrial risk. In E. Hollnagel, D. D. Woods & N. Leveson (Eds.), *Resilience engineering: Concepts and precepts* (pp. 155-179). Aldershot, UK: Ashgate.

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