Resilience Assessment Based on Models of Functional Resonance

Rogier Woltjer
Linköpings universitet, IDA/HCS/CSELAB, SE-58183 Linköping, Sweden
rogwo@ida.liu.se

Abstract. Both practitioners and scholars with an interest in Resilience Engineering have expressed the need for model- or process-based methods for the assessment of resilience. This paper explores the potential of the Functional Resonance Analysis Method (FRAM; Hollnagel, 2004) to address five key resilience characteristics (buffering capacity, flexibility, margin, tolerance, and cross-scale interactions, as identified by Woods, 2006). Application of FRAM to the Alaska Airlines flight 261 accident and application and evaluation of these resilience characteristics to the functional model shows that FRAM to some extent allows for resilience assessment through these characteristics. Moreover, FRAM-based assessment of resilience challenges the description and definition of these characteristics and enables to ask some specific questions that further develop their assessment.

1 INTRODUCTION

With definitions of resilience and resilient behaviour of organizations becoming more articulate [e.g., Hollnagel, Woods, & Leveson, 2006], industry representatives as well as scholars within the field of Resilience Engineering have voiced the desire to assess indicators for resilience. Whereas measurements and indicators of resilience based on system outputs can be expected to provide limited insight because they fail to capture the dynamics essential to resilient systems, process measures and model-based assessments may be powerful enough to assess the resilience of dynamic processes and organizations in order to make predictions of resilient performance or the lack thereof [Hollnagel, Woods, & Leveson, 2006; Mendonça, 2008]. The Functional Resonance Accident Model and Functional Resonance Analysis Method [FRAM; Hollnagel, 2004] are being developed to enable Resilience Engineers to model complex socio-technical systems for the purposes of risk assessment [e.g., Lundblad, Speziali, Woltjer, & Lundberg, 2008; Woltjer & Hollnagel, 2008] and accident analysis [e.g., Woltjer & Hollnagel, 2007; Hollnagel, Pruchnicki, Woltjer, & Etcher, 2008]. It is the thesis of this paper that these systems' key resilience characteristics may be assessed using FRAM.

1.1 Resilience and its characteristics

In order to define what Resilience Engineers need to monitor, a description of resilience and essential characteristics of resilience is in place. Woods [2006] describes the essence of resilience as the ability of a system to recognize when variability in its performance is unanticipated and falls beyond the usual competence and adaptations:

> "Resilience ... concerns the ability to recognize and adapt to handle unanticipated perturbations that call into question the model of competence and demand a shift of processes, strategies and coordination ... The focus is on assessing the organization's adaptive capacity relative to challenges to that capacity ... Resilience Engineering must monitor organizational decision-making to assess the risk that the organization is *operating nearer to safety boundaries than it realizes. ...*
>
> Monitoring and managing resilience, or its absence, brittleness, is concerned with understanding how the system adapts and to what kinds of disturbances in the environment, including properties such as:
>
> • **buffering capacity**: the size or kinds of disruptions the system can absorb or adapt to without a fundamental breakdown in performance or in the system's structure;
>
> • **flexibility** versus stiffness: the system's ability to restructure itself in response to external changes or pressures;
>
> • **margin**: how closely or how precarious the system is currently operating relative to one or another kind of performance boundary;
>
> • **tolerance**: how a system behaves near a boundary – whether the system gracefully degrades as stress/pressure increase, or collapses quickly when pressure exceeds adaptive capacity.
>
> In addition, **cross-scale interactions** are critical, as the resilience of a system defined at one scale depends on influences from scales above and below."
>
> [Woods, 2006, pp. 22-23, emphases added].

1.2 Functional modelling and functional resonance

FRAM [Hollnagel, 2004] characterizes socio-technical systems by the functions they perform rather than by how they are structured. Boundaries of systems are thus defined through a description of functions, in accordance with the principles of joint cognitive systems [Hollnagel & Woods, 2005]. It captures the dynamics by modelling non-linear dependencies and performance variability of system functions. FRAM is based on four principles [Hollnagel, Pruchnicki, Woltjer, & Etcher, 2008], compatible with the postulates that form the basis of Resilience Engineering [Hollnagel, Woods, & Leveson, 2006]. First, both successes and failures result from the adaptations that organisations, groups and individuals perform in order to cope with complexity. Success depends on their ability to anticipate, recognise, and manage risk. Failure is due to the absence of that ability (temporarily or permanently), rather than to the inability of a system component (human or technical) to function normally. Second, complex socio-technical systems are by necessity underspecified and only partly predictable. Procedures and tools are adapted to the situation, to meet multiple, possibly conflicting goals, and hence, performance variability is both normal and necessary. The variability of one function is seldom large enough to result in an accident. However, the third principle states that the variability of multiple functions may combine in unexpected ways, leading to disproportionately large consequences. Normal performance and failure are therefore emergent phenomena that cannot be explained by solely looking at the performance of system components. Fourth, the variability of a number of functions may resonate, so that the variability of some functions may exceed normal limits, the consequence of which may be an accident. FRAM as a model emphasises the dynamics and non-linearity of this functional resonance, but also its non-randomness. FRAM as a method therefore aims to support the analysis and prediction of functional resonance in order to understand and avoid accidents.

FRAM as a method consists of four steps. Step 1 identifies essential system functions, and characterizes each function by six basic parameters. Functions are described through six aspects, in terms of their input (I, that which the function uses or transforms), output (O, that which the function produces), preconditions (P, conditions that must be fulfilled to perform a function), resources (R, that which the function needs or consumes), time (T, that which affects time availability), and control (C, that which supervises or adjusts the function).

Step 2 characterizes the (context dependent) potential variability through common performance conditions (CPCs). Eleven common performance conditions (CPCs) are identified in the FRAM method to be used to elicit the potential variability: 1) availability of personnel and equipment, 2) training, preparation, competence, 3) communication quality, 4) human-machine interaction, operational support, 5) availability of procedures, 6) work conditions, 7) goals, number and conflicts, 8) available time, 9) circadian rhythm, stress, 10) team collaboration, and 11) organizational quality. These CPCs address the combined human, technological, and organizational aspects of each function. Variability phenotypes (similar to the earlier term failure modes, Hollnagel, 2004) may then be used to describe in which way this variability expresses itself (for example, in terms of force, direction, speed, etc.).

Step 3 defines the functional resonance based on possible dependencies/couplings among functions and the potential for functional variability. The output of the functional description of step 1 is a list of functions each with their six aspects. These functions may be linked together through their aspects. For example, the output of one function may be an input to another function, or produce a resource, fulfil a pre-condition, or enforce a control or time constraint. The links between functions are found by analyzing functions and identifying common or related aspects. These links may then be combined with the results of step 2, the characterization of variability, to specify how the variability of one function may have an impact on another, hence spread through the system. For example, if the output of a function may vary unpredictably, another function that requires this output as a resource may be affected, depending on that function’s common performance conditions, and as a result perform with increased variability. Many simultaneous occurrences of spreading variability may have the effect of resonance; the added variability becomes a 'signal', a high risk or vulnerability.

Step 4 identifies barriers for variability (damping factors) and specifying required performance monitoring. Barriers are hindrances that may either prevent an unwanted event to take place, or protect against the consequences of an unwanted event [Hollnagel, 2004]. Barriers thus aim to dampen variability. Besides recommendations for barriers, FRAM is aimed at specifying recommendations for the monitoring of performance variability, to be able to distinguish useful or harmless variability from unwanted variability, where it is undesirable to dampen useful variability through barrier use. Performance indicators may thus be developed for (groups of) functions and (groups of) couplings between functions.

1.3 Alaska Airlines flight 261

This paper will develop and illustrate the idea of monitoring resilience and performance variability with reference to the Alaska Airlines flight 261 accident. Therefore, this introduction concludes with a short description of the accident. The executive summary of the National Transportation Safety Board's accident report gives an outline of the accident in the eyes of the NTSB:

"On January 31, 2000 … Alaska Airlines, Inc., flight 261, a McDonnell Douglas MD-83, crashed ... The 2 pilots, 3 cabin crewmembers, and 83 passengers on board were killed, and the airplane was destroyed by impact forces. … The National Transportation Safety Board determines that the probable cause of this accident was a loss of airplane pitch control resulting from the in-flight failure of the horizontal stabilizer trim system jackscrew assembly's acme nut threads. The thread failure was caused by excessive wear resulting from Alaska Airlines' insufficient lubrication of the jackscrew assembly.

Contributing to the accident were Alaska Airlines' extended lubrication interval and the Federal Aviation Administration's (FAA) approval of that extension, which increased the likelihood that a missed or inadequate lubrication would result in excessive wear of the acme nut threads, and Alaska Airlines' extended end play check interval and the FAA's approval of that extension, which allowed the excessive wear of the acme nut threads to progress to failure without the opportunity for detection. Also contributing to the accident was the absence on the McDonnell Douglas MD-80 of a fail-safe mechanism to prevent the catastrophic effects of total acme nut thread loss." [NTSB, 2003, p. xii]

Many more factors that were of interest for describing and explaining the accident are discussed in the accident report, a few of which will be used here to illustrate the assessment of resilience characteristics using functional modelling.

2 RESILIENCE CHARACTERISTICS AND FRAM

This section illustrates how the resilience characteristics of buffering capacity, flexibility, margin, tolerance, and cross-scale interactions may be investigated using a functional model established with the Functional Resonance Analysis Method. For this study a simplified model of how systems' behaviour developed according to the NTSB (2003) accident report was established, describing around 40 functions and around 90 couplings of functions and various instantiations of the model over time. These functions describe system behaviour as designed/prescribed and as actually performed, over a long time period (from the design of the MD-83-predecessor the DC-9 in the 1960s to the crash in 2000) [see Woltjer & Hollnagel, 2007, for an early effort]. (The quantity of functions and couplings is imprecise and the model is called simplified because of modelling detail choices. This is due to the recursive nature of the analysis: The analyst may “split functions up” into sub-functions which in turn generate new couplings if the purpose of the analysis requires the investigation of variability of these functions in more detail.) The characteristics of resilience may, given this model which for a small part is illustrated in Figure 1, be described as follows.

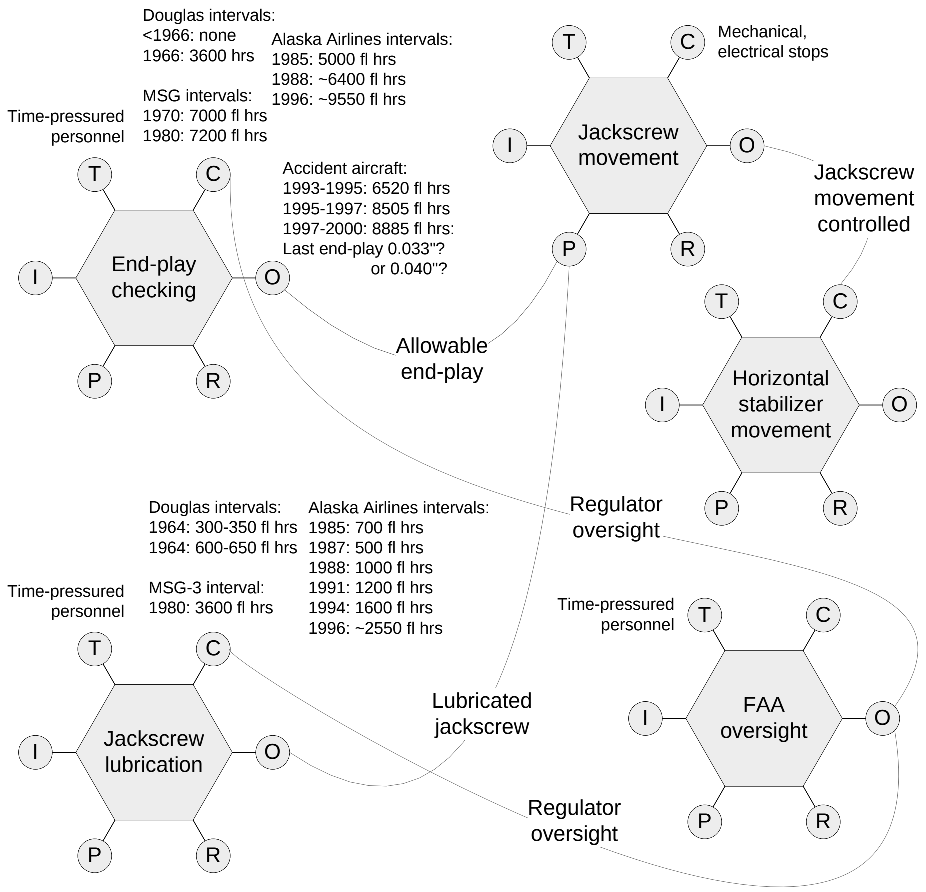

Fig. 1. Examples of functions, couplings, and aspects of various instantiations of the Alaska261 model for resilience characteristics assessment.

2.1 Buffering capacity

Buffering capacity relates to the disruptions the system can absorb or adapt to without a fundamental breakdown in performance [Woods, 2006].

Although examples of buffers that absorbed or adapted to disruptions are hard to find regarding Alaska 261, the case may be used to clarify the concept in that buffering capacity was lacking. Assessment of controls and common performance conditions of the function of *troubleshooting the jammed stabilizer* shows that operational maintenance personnel on the ground, procedures for handling a jammed stabilizer situation, and pilots training and experience with this problem allow for a very low buffering capacity. Also regarding function controls, the redundancy in the (although certified) jackscrew assembly was not found adequate lowering buffering capacity of the *jackscrew movement* function. Buffering capacity also relates to the other aspects, for example a change in the resource of the grease for *jackscrew movement* lessened the ability for the jackscrew assembly to withstand disturbances in the form of water and dirt that may enter the stabilizer. Likewise, the time available for Alaska mechanics and FAA inspectors diminishes the buffering capacity when inspections and assessments of equipment and regulations are most necessary, as in this case.

2.2 Flexibility

Flexibility (the opposite of stiffness) relates to the system's ability to restructure itself in response to events or conditions in the system's environment [Woods, 2006]. (As a reflection on other resilience characteristics that have been suggested: Adaptivity, learning, and creativity may possibly be described as more specific kinds of flexibility or flexibility in certain circumstances.)

Flexibility in models of functional resonance may emerge as new couplings between functions that were not planned and instantiated before, possibly in combination with the introduction and performance of new functions during system functioning. Thus, flexibility and "new" behaviour can be identified through new couplings and functions in the model.

This may be exemplified by the introduction of procedures for end play checking at the beginning of the operational life of the DC-9 model, the predecessor of the MD-83 and later the Boeing 717. In 1966, based on measurements of end play by the Douglas Corporation, engineers decided that an end play check was necessary. The earlier assumption that an acme nut would last for 30 000 flight hours turned out to be hazardous, after some time excessive wear was found which was higher than anticipated in the design phase. Thus a new function was introduced in the operational system, *end play checking*, providing a control on the *jackscrew movement* function.

2.3 Margin

Margin relates to how closely or how precarious the system is currently operating relative to one or another kind of performance boundary [Woods, 2006].

Examples in the Alaska 261 case may be found in the margin that was over time "eaten up" by the extensions of the intervals at which end play checks and lubrication were performed. Figure 1 illustrates this point with FRAM: The controls on the *end play check* and *jackscrew lubrication* functions consist of the intervals that Alaska Airlines employed in its maintenance program. These developed over time, as can be seen in Figure 1. As no-one actually knows where exactly the absolute boundaries of safe intervals lie, recommended intervals serve as indicators of the margins, showing a clear trend in margin decline. These too are controls on the functions. Thus behaviour compared to various margins may be modelled as a combination of function controls, depending on stakeholders that are modelled, and outputs, how actual performance is chosen to strike a balance between various operational goals (e.g., safety vs. efficiency). The outputs, in this case the actual intervals in the case of the accident flight show actual performance, which may be compared to controls. However, a richer picture of margins and their development is obtained when various instantiations of the model, modelling function aspects and couplings over time, are compared. Examples of such instantiations are summarized and illustrated in one figure here due to space limitations, see Figure 1.

We may from this example conclude that the issue of "behaviour relative to a performance boundary" is far from straightforward and may need to be dissected into several issues, such as: Which functions, and thereby actors, trade-offs, and processes lay as a basis for boundary setting? How do these functions (trade-offs, processes) change over time, and how does the boundary change over time as a result of that? Through which functions is assessment of the current situation relative to a boundary performed, how does the performance of these functions vary, and how are they interconnected? Instantiations of a FRAM model may help address these issues in a structured way by following and assessing potential and actual couplings between functions in a system over time.

2.4 Tolerance

Tolerance relates to how a system behaves near a boundary, for example along the lines of graceful degradation or quick collapse, when pressure exceeds adaptive capacity [Woods, 2006].

In the Alaska 261 case this relates to the design, certification, operation, and inspection of the jackscrew assembly, which are all controls on the *jackscrew assembly movement* function. Design of technical systems and subsequent regulator certification in FRAM terms is aimed at foreseeing, dampening and avoiding unwanted variability in system performance. The NTSB concluded that once the acme nut and screw system had failed, the electrical and mechanical stops that were supposed to limit the range of horizontal stabilizer movement were not adequate to hinder the fatal consequences after failure of the acme nut. This lack of barriers makes the probability for a rapid degradation of overall system performance once beyond the boundary of adequate acme nut functioning very high. However this tolerance is in FRAM first understood properly when combined with other controls and conditions. Given the possibility of a quick collapse, this accident shows that training, operational support, HMI issues, and procedures were also inadequate at the same time as the system had passed the boundary of the jackscrew system being jammed (investigated as part of the common performance conditions in

FRAM) and when the pilots were troubleshooting the system. Thus the combination of function controls together with an assessment of common performance conditions may indicate the tolerance that a function may have when performance is near a boundary.

2.5 Cross-scale interactions

Cross-scale interactions relate to how a system defined at one scale depends on influences from systems defined at other scales [Woods, 2006]. The assessment of interactions between various systems is thus highly dependent on the definition of system boundaries. In FRAM, systems are defined in terms of the functions that various joint cognitive systems perform. Influences between systems become explicit in that couplings between functions, for example, between output and resource, output and control, output and input, specify which kind of influence other functions (and thereby, other systems) have. Figure 1 shows various examples of links between functions that denote interactions between systems at different scales. Functions (systems) may also be split or grouped to describe more or less encompassing functions and systems, but still the method forces the analyst to be explicit in how functions may be coupled, how variability in one function may influence aspects of another function, and if variability that spreads actually has an impact on the output of another function depending on that function’s performance conditions.

3 CONCLUSION AND FUTURE WORK

This paper has explored the potential of the Functional Resonance Analysis Method to address five key resilience characteristics, in theory and through application to the Alaska Airlines flight 261 accident. Buffering capacity is assessed for functions by assessing the buffers available for each function aspect, but also how buffers may be present or created through potential couplings to actions that supply a buffer of for example a resource, an input, or time. Flexibility may be identified as the development of couplings between functions in FRAM instantiations over time, new functions being introduced, or changes in function aspects. Margin assessment of a function may be done by examining which other functions set boundaries (controls) and what their controls are in turn, how these controls develop over time, and how actual outputs match boundaries set by control conditions over time. Tracing and assessment of potential couplings in the functional model, together with the assessment of CPCs gives an indication of the tolerance for disturbances. Linear effects may indicate graceful degradation, non-linear effects may indicate radical breakdown. Sets of coupled functions need to be evaluated in this respect because of the functional distribution of the propensity to dampen/amplify variability that determines tolerance. Systems are defined in terms of the functions they perform. Interactions between systems become explicit through couplings between functions over time. Cross-scale interactions are illustrated in dynamic networks without fixed levels or scales, with function aspects providing a richer description than traditional hierarchical models.

Moreover, FRAM-based assessment of resilience challenges the description and definition of these characteristics and enables to ask some specific and more elaborate questions that further develop their assessment. However, many more cases need to be modelled and assessed to enable stronger claims on FRAM-based resilience assessment. Assessment of resilience based on FRAM for risk assessment could provide valuable a test for the usefulness of FRAM for assessing these resilience characteristics. Some work has been done in this respect, combining variability and buffer capacity [Lundblad, Speziali, Woltjer, & Lundberg, 2008], and more encompassing investigation of the characteristics for risk assessment would be an interesting path for future work.

Future research in Resilience Engineering will most likely identify additional characteristics of resilience. Methods and tools will need to develop according to the maturity of the models and theories of resilience.

REFERENCES

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

Hollnagel, E., Pruchnicki, S., Woltjer, R., & Etcher, S. (2008). A functional resonance accident analysis of Comair flight 5191. Paper presented at the *8th International Symposium of the Australian Aviation Psychology Association*. Sydney, Australia.

Hollnagel, E., & Woods, D. D. (2005). *Joint cognitive systems: Foundations of cognitive systems engineering*. Boca Raton, FL: CRC Press/Taylor & Francis.

Hollnagel, E., Woods, D. D., & Leveson, N. (Eds.). (2006). *Resilience engineering: Concepts and precepts*. Aldershot: Ashgate.

Lundblad, K., Speziali, J., Woltjer, R., & Lundberg, J. (2008). FRAM as a risk assessment method for nuclear fuel transportation. In *Proceedings of the 4th International Conference Working on Safety*. Crete, Greece.

Mendonça, D. (2008). Measures of resilient performance. In E. Hollnagel, C. P. Nemeth, & S. Dekker (Eds.), *Resilience engineering perspectives, volume 1: Remaining sensitive to the possibility of failure*. Aldershot, UK: Ashgate.

NTSB. (2003). *Loss of control and impact with Pacific Ocean, Alaska Airlines Flight 261, McDonnell Douglas MD-83, N963AS, about 2.7 miles north of Anacapa Island, California, January 31, 2000* (Aircraft Accident Report No. NTSB/AAR-02/01). Washington, DC: National Transportation Safety Board.

Woltjer, R., & Hollnagel, E. (2007). The Alaska Airlines flight 261 accident: a systemic analysis of functional resonance. In *Proceedings of the 2007 (14th) International Symposium on Aviation Psychology*. Dayton, OH.

Woltjer, R., & Hollnagel, E. (2008). Functional modeling for risk assessment of automation in a changing air traffic management environment. In *Proceedings of the 4th International Conference Working on Safety*. Crete, Greece.

Woods, D. D. (2006). Essential characteristics of resilience. In E. Hollnagel, D. D. Woods, & N. Leveson (Eds.), *Resilience engineering: Concepts and precepts* (pp. 21-34). Aldershot, UK: Ashgate.