System Hazard Analysis of a Complex Socio-Technical System: The Functional Resonance Analysis Method in Hazard Identification

Brendon Frost[1] and John P.T. Mo
School of Aerospace, Mechanical and Manufacturing Engineering
Royal Melbourne Institute of Technology
GPO Box 2476, Melbourne 3001, Victoria

[1]brendon.frost@gmail.com

Abstract

The value of characterising systems in high-risk industries as complex and socio-technical systems is increasing. Using complex and socio-technical system view-points, high profile industrial and transport accidents can be investigated by focusing attention to interactions between skilled operators, technology, and automation in geographically dispersed operations, as well as unintended design risk factors to arise from complex and non-linear interactions can be highlighted.

Currently there are methods for identifying and assuring the safety of interactions between and within systems but the modeling is incomplete. However, one potentially valid method is the Functional Resonance Analysis Method (FRAM). FRAM is a qualitative approach generating a functional (rather than structural) model of the relationships between sub/systems, and has the potential to produce inputs suitable for safety assurance and risk analysis methods.

This paper presents a methodology for incorporating a modified FRAM technique within a System Hazard Analysis (SHA). The application of the FRAM/SHA methodology in this case study is to explore the validity of this approach for assessing hazards arising from structural and process changes to the operational control center of an international airline, as a result of the introduction of a new software system into an existing suite of COTS software tools. This paper will explore the methodology in terms of requirements that include the creation of a new work team, the functional division of an existing operator role, and changes to system performance and safety critical processes.

Keywords: Socio-Technical system, Functional Resonance Analysis Method, FRAM, System Hazard Analysis, operational control center, risk analysis, COTS requirements.

1 Introduction

A significant challenge in designing and operating complex systems is the potential for unpredictable system behavior to 'emerge' from the complex (and often transient) interconnections that can arise under dynamic operating conditions. Limited understanding of these factors can manifest as an undefined gap between the system as intended and the system as implemented/operated (Leveson, 2011a).

This arises partly as a result of the limited guidance available to support the design of effective interactions between system elements (such as human operators and technology), particularly where they are separated by time and geography, and where system function is constrained by time, conditions of information uncertainty, and decentralised control mechanisms (Vicente, 1999). In addition, the development of tools for analysing and modeling complex and non-linear system behavior (particularly for degraded performance modes), and the assessment of organisational, social, and human factor impacts, are in their relative infancy when compared to the traditional reliability driven approaches used across the system engineering life-cycle (Allenby & Kelly, 2001).

This paper describes a novel systems modeling technique, the Functional Resonance Analysis Method (FRAM), modified for use within the context of a System Hazard Analysis (SHA). FRAM has been used within the Cognitive Systems Engineering domain to model and assess the complex functional interactions between elements within socio-technical systems, but primarily for accident investigation purposes (Hollnagel, 2012). However, the technique potentially has greater utility than traditional hazard identification techniques (e.g. HAZOPs variants, FMEA/FMECA approaches, etc.) in supporting risk analysis through identifying system level hazards and defining the specific (and often transient) scenarios/conditions under which they arise.

The system case study highlighted in this paper is the Operations Control Centre (OCC) of a large international airline, where the modified FRAM/SHA method was applied in order to define system functional and safety requirements prior to the introduction of new industry mandated software interfacing airline operations and the Australian air traffic management system. The utility of the FRAM technique will be outlined for identifying scenario/condition-specific hazards, specifically to inform design requirements at the different levels of system performance and function, safety critical processes, and operator function and role accountabilities.

2 Complex System SHA

The identification of potential hazards in complex systems is fundamental to establishing safety and reliability across the design, production, and operational stages of the System Engineering (SE) lifecycle (Bahr, 1997). A complete and comprehensive picture of the hazards present or likely to exist in a system, and determination of the escalation of hazards to become mishap or accident scenarios, supports the early establishment of performance and safety requirements for design and operational objectives. This supports a more complete and comprehensive analysis to reduce the uncertainty of any subsequent risk quantification,

while providing higher levels of safety assurance (Seligmann et al, 2012).

The SHA is a SE hazard analysis process applied during the design phases to assess the integration of designs. The SHA aims to identify hazards arising from the functional interfaces between subsystems, as well as the presence of latent design hazards with the potential to escalate into interrelated fault events (Ericson, 2005). Roland and Moriarty (1990) list the primary objectives of the SHA process as including consideration of:

- Compliance with specified safety criteria;
- Hazardous events, including failure or degradation of safety devices, controls, and safety constraints and functions;
- Degradation of the system's safety levels under normal or abnormal conditions;
- The impact of design or engineering changes, and;
- Human System Interfaces (HSI) including human performance errors and control functions.

The SHA process may draw from a broad range of established hazard identification techniques, but will typically commence with qualitative techniques to establish the causality of credible mishap/accident scenarios before proceeding to quantification techniques (NASA, 2011).

The foundation of hazard identification and analysis (HAZID), therefore, is identifying credible mishap and accident event scenarios. However, HAZID within safety critical systems is often challenging due to the stochastic effects of interactive and dynamic system complexity, and the presence of system intractability (or under-specification) as commonly found in complex and socio-technical systems (Hollnagel, 2012). Established risk analysis practice adopts the scenario driven approach to the systematic review of safety-critical systems, in order to identify potential mishap and accident scenarios (CCPS, 2008; Mannan, 2005).

The development of credible scenarios enables system complexity to be reduced to discrete 'snapshots' of the system under a range of conditions and in different system states, where they can be modeled as deterministic functional relationships between system elements (Bossel, 2007). A scenario consists of an expected situation/characteristic sequence or combination of events, and describes a generic situation that encompasses and relates a set of reasonably probable events/situations. Khan (2001) cautions against focusing on identification of the 'worst-case' scenarios through risk assessment activities, as this may unnecessarily restrict the scope and coverage of the scenario set identified: he suggests that it is preferable to focus efforts on identifying *"…credible accident[s] … within the realm of possibility and likely to be severe enough to cause significant damage"*.

An effective risk analysis process for a complex system must therefore combine appropriate hazard identification and analysis techniques in order to generate as complete and comprehensive a set of mishap and accident scenarios as possible for subsequent quantification (Cameron & Raman, 2005). Siu (1994) particularly identifies dynamic system dependencies (e.g. common-cause initiators, functional coupling, and shared equipment/components) as requiring 'complexity decomposition' before the modeling approaches commonly used in risk analysis can provide valid scenario quantification. In addition, Leveson (2011a) suggests that the selection of HAZID techniques should consider the system's complexity and socio-technical characteristics, so that the HAZID process is able to describe system scenarios resulting from dependent incredible events, and/or transient system states.

2.1 Complexity System Properties

Complex systems are typically dynamic, with changes in system complexity leading to changes in the system's needs and objectives, which in turn 'orients' system behavior towards these new objectives. As a result, complex systems can exhibit changes in characteristic behaviors and states that are not easily observed or predicted, except through changes in state variables (Bossel, 2007). Perrow (1984) describes complexity simply as *"…those of unfamiliar sequences. Or unplanned and unexpected sequences, and either not visible or not immediately comprehensible."* Expanding upon this definition through use of Systems Theory, complexity can take a number of forms (Leveson, 2011a):

- **Interactive complexity** between components/elements within the system, or between sub/systems.
- **Dynamic complexity**, or system changes in relation to time.
- **Decompositional complexity**, where the system's structure and function are not obviously consistent/linked.
- **Non-linear complexity**, where cause and effect are intractable or not easily described or specified.

Hollnagel (2012) employs a Cognitive Systems Engineering perspective to relate dynamic complexity and non-linear complexity as a reflection of the extent to which system function is discernable or tractable: "Dynamic complexity refers to situations where cause and effect are subtle, and where the effects over time of interventions are not obvious". This perspective is complemented by Perrow's (1984) original concept of coupling within systems, where unintended or increased functional interactions and dependencies within a system can cause a sub-system/element event to cascade and resonate through the system, leading to 'incredible' event scenarios.

Emergence is a system characteristic that describes the effects of decompositional and non-linear complexity within a complex system, and refers to cases where system behavior or state changes cannot be explained in terms of a direct cause and effect relationship to discrete underlying processes or events (Hollnagel, 2012). For example, dependence between two or more low-probability or 'incredible' events may occur as a result of the influence of common systemic factors, rather than via a temporal or direct cause-and-effect relationship (Leveson, 2011b; Hollnagel, 2004). Concepts of direct causality may therefore be inadequate for predicting and describing mishap or

accident event scenarios within a HAZID process, particularly where complexity interactions may occur that are not easily understood or identified.

Finally, Dekker, Cilliers and Hofmeyr (2011) summarise complexity as a property of distributed systems:

"Complex systems are held together by local relationships only. Each component is ignorant of the behavior of the system as a whole, and cannot know the full influences of its actions. Components respond locally to information presented to them, and complexity arises from the huge, multiplied webs of relationships and interactions that result from these local actions. The boundaries of what constitutes the system become fuzzy; interdependencies and interactions multiply and mushroom."

2.2 Socio-technical System Properties

System performance variability is a common feature of large-scale socio-technical systems, where demands arising from interaction with the external environment, social, organisational, and individual operator system factors within the system, must be met through trade-offs against the purpose and objectives of the system and within finite time and resource constraints. This leads to a situation where a complete description of the system of work (i.e. how work is to be accomplished) is intractable, or cannot be fully specified due to the effect of elaboration (the presence of significant detail), the rate of change (dynamic complexity), incompleteness of functional knowledge, and/or process heterogeneity and irregularity (Hollnagel, 2012). Performance variability therefore can be seen as a response to the presence of dynamic complexity in the system over time.

Socio-technical systems can be defined as having a human-intensive and organisation focused architecture, and can be defined as increasingly common classes of large-scale system that feature a combination of technological systems (where hardware and software technology feature as significant elements within the system), human interfaces, and human-intensive organisational systems (Jackson, 2010). Common to these complex and large-scale socio-technical systems are characteristic behaviors that include (Bossel, 2007):

- Self-organisation: the system can change structure, parameters, rules, etc., to adapt to environmental demands independently of centralized control.
- Co-existence: the system modifies its behavior in order to respond to interactions with others systems that it cannot operate in isolation from.
- Self-replication: the self-organising system can be capable of generating similar systems, particularly in the case of industrial organisations.

Groth, Wang and Mosley (2010) note the difficulty of quantitatively determining the causal role of non-deterministic/uncertain factors arising from human or organisational system elements in system failure or dysfunction, particularly the probabilistic modeling of "soft" relationships. They further note the challenges of modeling uncertain relationships between system elements, particularly where sequence, direct causality, and event independence cannot be assumed.

The FRAM technique was selected for application in this case study because it was specifically designed to assess systems with these features, and due to its demonstrated capability for identifying the impact of both complexity and socio-technical system properties in retrospective accident analyses.

2.3 Implications for the Risk Analysis of Complex Systems

Consideration of system socio-technical and complexity factors informs the decomposition of system structure and function as a basis for identifying how perturbations of, and interactions within, the system under study can propagate in undesirable ways and lead to 'system mishaps/accidents' (Dekker, Cilliers & Hofmeyer, 2011; Bahr, 1997).

These properties have significant implications for HAZID activities, as hazards may emerge infrequently under rare combinations of circumstances or unique system states, be difficult to predict, and mean that the use of HAZID techniques that assume linear causality and independence between low-probability events will likely lead to significant underestimates of system risk (Jackson, 2010; Leveson, 1995). Hollnagel (2012) points to the limitations of existing HAZID techniques that presume as a starting point a complete and unambiguous description or specification of the structure and function/s of the system, and that are based on assumptions that are invalid for complex systems:

- That a system can be meaningfully decomposed into constituent elements – i.e. that the whole is the sum of the parts.
- That these elements operate according to binary modes – i.e. elements either function or fail.
- That the system functions as intended, and that system events follow pre-determined sequences in a consistent, orderly, and linear manner.

The presence of complexity in a large-scale system therefore means that a complete understanding (and particularly a precise structural or process description) of a complex system may well be unobtainable, and that there is always likely to be a degree of uncertainty as to the way the system will function under all possible conditions, respond to unforeseeable demands or changes in system objectives/needs over time, or how it may change to suit the external environment (Hollnagel, 2012; Modarres & Cheon, 1999). Similarly, socio-technical system features (such as intractability and performance variability characteristics) mean that a structural decomposition of a system is unlikely to provide adequate insight into a system and may lead to the identification of an incomplete set of event scenarios descriptors for HAZID and subsequent risk analysis (Rasmussen & Petersen, 1999).

A number of approaches have been suggested for conducting HAZID processes while taking complexity and socio-technical factors into account, however, to date none have achieved widespread adoption outside of specific communities of practice. Most address these

challenges through modification of existing techniques/approaches, but two techniques have been specifically developed to address this need:

- *System Theoretic Process Analysis* (STPA: Leveson, 2011a, 2004); and,
- *Functional Resonance Analysis Method* (FRAM: Hollnagel 2012, 2004).

FRAM was chosen as the basis for this research partly because of the body of literature available, but primarily because of it's potential for modeling graduated/degraded functional variability (Herrera & Woltjer, 2010). FRAM is most likely to be of value from the detailed design phase of the Systems Engineering life cycle, and following the availability of a detailed Concept of Operations (CONOPS). In this context FRAM could replace or complement established techniques such as HAZOPs, Functional Failure/Hazard Analysis, etc., and could identify system hazards missed during the Preliminary Hazard Identification (PHI) process.

3 FRAM in Context

The Functional Resonance Analysis Method (FRAM) is a qualitative analysis technique that supports modeling of complexity and socio-technical factors, including the interfaces between adaptable human agents and technology, coupling and dependence effects, non-linear dependencies between sub-systems, and functional performance variability (Woltjer & Hollnagel, 2008b).

FRAM has previously been used to conduct qualitative system analyses: initially as a system accident investigation technique (see: De Carvalho, 2011; Hollnagel et al, 2008; Nouvel et al, 2007; Sawargi et al, 2006), and more recently as a self-contained qualitative risk assessment method to inform design activities for large distributed systems (see: Belmonte et al, 2011; Herrera & Woltjer, 2010; Macchi et al, 2008; Woltjer & Hollnagel, 2008a; Woltjer & Hollnagel, 2008b). To date, FRAM analyses have been undertaken for air traffic management, rail transport, financial market, and nuclear waste transport systems.

FRAM theory contains different definitions of terms to those commonly used in HAZID activities:

- Functions are defined as representing the set of activities (the actual or likely work done, rather than an idealized work-as-imagined) required to produce an outcome or achieve sub/system objectives. More formally, the concept of a function is associated with activity intended to produce something of relevance to the system's objectives or change system state; the function's output describes a system condition or state (Hollnagel, 2012).
- Mishap/accident scenarios are seen as a product of uncontrolled hazards that emerge from performance variability and led to unintended or increased functional interactions and dependencies within a system, causing a sub-system/element event to cascade and resonate through the system (Hollnagel, 2004).
- Performance variability is considered to arise from the intractability of work management within complex systems, as agents independently trade-off efficiency against thoroughness (known as the Efficiency-Thoroughness-Trade-Off: ETTO) in achieving the purpose and objectives of the system (Hollnagel, 2009).
- Failure is defined differently to existing HAZID techniques as "*the temporary or permanent loss of a system's ability to anticipate risks and make proactive approximate adjustments to understand and adjust to the current conditions (resources, demands, conflicts, interruptions, underspecified work requirements)*" (Hollnagel, 2013b).

FRAM supports a systemic decomposition methodology, with analysis of a unique FRAM model (of a specific system) describing the functionality needed to meet the system's objectives and the range of functional variation that supports the achievement of these objectives (Hollnagel, 2013a). Through characterizing the variability of these functions, specific *instantiations* (or snapshots) of the system under defined situations and conditions can be determined to identify how interactions and relationships within the system (and with other systems) reconfigure, leading to undesirable functional variability and resonance within the system (Hollnagel, 2012).

This is where FRAM differs in concept from established HAZID techniques, in that it focuses on determining the likelihood of functional variability rather than the probability of malfunction or failure (in the traditional use of the term as the loss of function/binary failure modes). However, in applications the FRAM approach remains compatible with established HAZID techniques used in many industries, in that the technique guides the decomposition and/or analysis of the system under study in order to identify plausible scenarios that form the basis for subsequent risk assessment activities.

3.1 The FRAM Methodology

In order to allow activities that build and validate a functional model of the system under study, FRAM has been adapted into a HAZID technique in this case study. The functional characteristics of the adopted FRAM model are "perturbed" to identify the hazards arising from coupling and system interactions within defined scenarios. The FRAM process, as outlined by Hollnagel (2012) and as applied in this research, includes three key process steps:

- **Step 1: Functional Identification and Description**: The first step in building a FRAM model is the identification and description of the actual (or likely) functions (rather the idealized functions), or activities that represent the likely "work-as-done". This includes characterizing the functions and identifying the possible linkages (couplings) between functions via each of the defined characteristics.
- **Step 2: Performance Variability Description**: Once a model has been defined, the variability of functions are determined, effectively creating the 'instantiations' or scenario precursors that can be

used in HAZID workshops. Of direct interest is the variability of a function's output, as this is the aspect that can affect coupling and interactive complexity and is therefore the representation of performance variability.

- **Step 3: Aggregation of Performance Variability**: The remaining step used in the FRAM analysis process is to determine how performance variability can combine and drive non-linear system effects and outcomes through "upstream-downstream coupling" of functions. (Note: The FRAM approach established in the literature has an additional step that generates the productive output for a stand-alone process, but which has been omitted in this research as redundant due to the integration of FRAM into the SHA process.)

The process for using FRAM in a prospective hazard analysis therefore involves building a system model from the constituent functions, with six characteristics used to define each function: The input/trigger that starts the function, relevant time constraints, limiting control/s, resources required, preconditions needing to be met, and the output's quality determinants. The functions can then be linked to build a functional baseline model of the system that identifies coupling and interactions under defined (ideal) conditions. This is followed by the development and analysis of a number of scenarios or instantiations of the model that identify how functions can be coupled under a range of favorable or unfavorable conditions. Details of the standard approach to applying FRAM can be found in Hollnagel (2012).

While the majority of the FRAM process involves the development of the model in a table format, FRAM models and instantiations can also be represented in a graphical form using a modular 'hexagon' representation of each function and its six defining characteristics. An example of a FRAM module graphic is shown in figure 1.

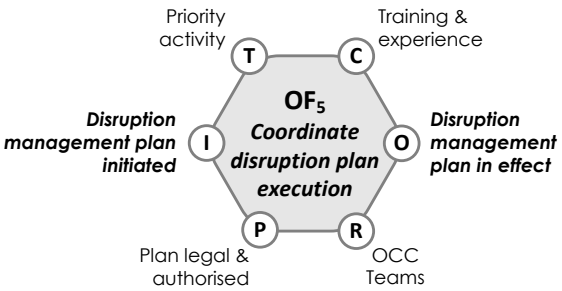

Figure 1: A graphic representation of a FRAM module

The FRAM/SHA method used in this research differs from that published (Hollnagel, 2012; Hollnagel, 2004) as follows:

- Once the model is constructed, a small, representative group of system experts are consulted to both refine/confirm/agree that the model was representative of the intended functional system, and to provide advice on the nature of credible functional 'perturbations' likely in the system.
- The baseline FRAM model is then reviewed by an expert group of system experts in a facilitated HAZID workshop following a guideword process, in order to identify hazards, their escalation paths to incidents/accidents (represented by sets of discrete scenarios that formed the primary products/outputs from the HAZID process), and the barriers in place to prevent this.
- The validated model and credible system perturbations are then used to develop 'instantiations' of the model, representing the revised couplings between functions and any impacts on function performance/efficacy under defined conditions.
- In this case study, the HAZID workshop outputs and three FRAM instantiations were then used as the basis for developing risk models.

The adoption of the guideword concept from (amongst others) the popular HAZOPs technique was used to improve the efficiency of the HAZID workshop process through consistent prompting and guidance of system experts. The function aspects defined in the FRAM (i.e. input, time, preconditions, resources, controls, output) can be considered equivalent to the 'keywords' concept from HAZOPs, which act to focus attention on the parameters of interest. Specific guidewords were developed to facilitate the FRAM process and ensure consideration of two different aspects of function variability:

- Factors affecting the variability of the function itself due to the operation of the function (i.e. internal influences on variability), through determining different aspects of the output variability,
  and;
- Factors affecting inputs to the function that affect the Input, Time, Control, Resource, or Precondition characteristics of the function (i.e. external influences on variability).

Consequently, the modified FRAM method uses two separate sets of guidewords, used separately in two sequential 'passes' across the baseline FRAM model by the system experts to identify hazards arising from interactivity, defined conditions, and the effect of potential variability on function coupling and performance:

Pass 1: Determination of function variation where the input, time, control, precondition, resource is *Early*, *Delayed*, *Absent*, *Wrong Rate*, *Under specified* (insufficiently constrained), *Over-specified* (too constrained).

Pass 2: Determination of variation where the function is impacted by the specific conditions or socio-technical and individual factors of:

- *Time pressures/constraints/duration*
- *Information certainty/sufficiency*
- *Quality of human-technology interfaces*

- *Quality of communications*
- *Procedures and authorisations*
- *Competence and preparation (e.g. training)*
- *Goal objectives/conflicts*
- *Circadian and stress factors*
- *Organisational influences and support*

Despite the complexity of the system problem studied in this research, the available access to system experts (both in terms of total contact time and the number of individuals) was limited. As a result, the development of the FRAM process used in this paper was influenced by this need to minimize the total system expert resource required, and the time that they were required. In practice this led to a number of process efficiencies:

- The model validation step (and identification of system perturbations) could be conducted quickly (around 1 hour) with a small number of system experts (2 individuals were sufficient for this analysis);
- The HAZID workshop could be constrained to a session of just a few hours (2 hours were all that was available for this research), as a concise number of representative instantiations (3 were sufficient to explain the outputs of the process for this research) of the FRAM model were developed following the workshop and used to precisely focus and contain the HAZID process.
- The validation of hazard scenarios used graphic FRAM model representations, as a convenient way to represent process differences due to functional interaction and coupling under different scenarios, in a way that allowed domain and specialist experts a common terminology or representation upon which to agree likely HAZID outcomes (Nemeth & Bartha, 2009).

It can be seen that the involvement of system experts is required in order to ensure model validity, improve the quality of the analysis and utility of the process products, and to make explicit the objectives of each process step for all involved.

4 The Airline Operations Control System

Operations in a modern airline environment are complex, requiring the coordination of a number of different business units to ensure the availability and operation of aircraft to meet strategic objectives and market commitments and opportunities. These services are coordinated and directed to manage operational disruptions due to weather, technical failures, air traffic and airspace/aerodrome management, with oversight by the Operations Control Centre (OCC). The OCC typically monitors all aspects of the airline's daily operations, with key accountabilities including:

- Maintaining the integrity of the planned operational service schedule.
- Responding to any known and controllable risks that could cause variation to the planned operational service schedule.
- Managing variation to the planned service schedule, including developing, implementing, monitoring, and managing plans to minimise or recover from unplanned operational disruptions.

From a systems theory perspective the OCC represents a socio-technical system (i.e. composed of elements of technical, psychological, and social cooperation) that is also part of a larger, distributed complex socio-technical system (i.e. the Australian air transport/aviation system of systems): together they demonstrate identifiable features of such systems including (Vicente, 1999):

- The problem space is large: there are an enormous number of potentially interactive factors/elements with variable degrees of in/dependence.
- Social cooperation is required from a large workforce across distributed/geographically-spread operations, often representing different organisational and professional perspectives.
- The potential exists for significant hazards with significant consequences.
- Many sub-systems are coupled together, without being subject to unified organisational or social control.
- There is a significant reliance on automation within sub-systems, and system interactions mediated through computers.
- There is incomplete and uncertain data on system state/s and dynamics, which becomes more significant when the operators must regularly respond to system disturbances and disruptions.

An OCC is comprised of a number of specific sub-systems with specific functions, each of which must interact effectively in order to achieve the system objectives and fulfill the system purpose:

- **Operations Control**, tasked with monitoring aircraft movements to minimise disruption to the planned schedule of services, but also to manage disruptions to the planned schedule as a result of weather, traffic, aircraft serviceability, and crew availability impacts. Operations Control is the hierarchical center of the OCC and has final decision-making authority for disruption response management.
- **Dispatch**, who provide flight planning services to pilots, lodge detailed airspace access requests with the ANSP, and monitor operational conditions to determine planning variations (including following on from Operations Control activities).
- **Crewing Control**, who ensure that adequate regulatory flight crew (pilots and cabin attendants) are available to crew planned services (including following-on from Operations Control activities).
- **Maintenance Control**, who monitor aircraft serviceability in operations, and advise of unplanned maintenance requirements and disruptions to planned maintenance that impact on the service schedule.
- **Slot Control**, who monitor and procure the availability of operational 'slots' in the airspace access control system.

An OCC typically includes other functional areas

(e.g. passenger recovery, etc.), but these 'down-stream' functions have no influence on the primary operational functions of an OCC, and therefore have been excluded from this analysis.

The context for the analysis was restricted to OCC activities, functions, and interfaces specific to the 'day of operations' tactical management efforts (i.e. 'Disruption Management'). Similarly, the analysis did not consider any OCC activities, functions, and interfaces not occurring on the current or next immediate day ("day + 1"). Time constraints also meant that FRAM- was the only HAZID technique used – the established HAZID practice of using multiple/independent techniques to increase the likelihood of capturing all hazards was not followed.

4.1 The OCC Problem Space Defined

The organization sponsoring this analysis was a large international airline operating within Australian airspace, with the scope of operations managed by its OCC reaching approximately 10,000 separate aircraft movements per month. To support these functions, a number of COTs and adapted COTs systems were in use, largely independent of each other, and designed as interfaces with external systems that included:

- Air navigation service provider systems (e.g. Australian and international air traffic management systems).
- Airline 'front-line' systems, primarily through the pilot Captain operating each aircraft and local airport tactical control centers.
- International/national weather forecasting systems.
- Australian regulatory systems.

The need for the analysis outlined in this paper was two-fold: The immediate need related to assessing the impact and system change requirements following the introduction of a new slot management (SMGR) software (adapted COTS) supplied/mandated by the Australian Air Navigation Services Provider (ANSP); The strategic driver was to develop a formal representation of the OCC system that would support decision-making on how best to support complexity and capacity demands emerging from future airline growth. Specific questions arising from the immediate need included better understanding the impact of introducing SMGR, particularly integration with existing OCC software systems, and the addition of new operational functions into an established and defined set of functions.

Initial work undertaken to describe and decompose the system identified a number of potential issues likely to arise in the proposed OCC system, including:

- The expansion of OCC subsystems to include Slot Control (created through absorbing some existing functions from Operations Control and integrating them with new functions imposed by the implementation of the SMGR system) was likely to increase the number of interactions between the OCC subsystems (i.e. increased complexity) and independent interactions with systems external to the OCC system.
- Operations Control is accountable for leading the activities of the OCC system, but under the proposed system would need to be led by, and react to, Slot Control activities to a greater extent than currently. In reacting to externally imposed disruptions, Slot Control is likely to increase the number of disruption inputs that Operations Control must respond to and integrate into the revised service schedule, increasing operator workload and task complexity.
- The nature of the disruption inputs to Operations Control are likely to be of a more complex and dynamic nature than those currently received (i.e. more bi-modal and certain in nature): consequently Operations Control will need to respond at a higher tempo, as well as needing to continue to monitor the status and effects of these disruptions.
- Both the OCC system and the service schedule become more directly linked to other systems through SMGR, and system dynamics are likely to change as a result of all (airline operators, airports, ANSP) systems becoming more tightly coupled and therefore less predictable to the operators within the systems. This potentially increases the risk that slot coordination activities within the OCC may have unintended consequences due to both the Slot Control and Operations Control subsystems having inadequate awareness of all information relevant to disruption management decision-making and planning actions.
- The development of feedback loops, including introducing time constraint and response delay, between the Slot Control and Operations Control functions.
- Tighter coupling to other systems operating within the Australian airspace system.

A graphic representation of the proposed OCC system, interfaces, functional flows, and COTS software is provided in figure 2.

5 A FRAM Model of the Proposed OCC

A baseline FRAM model of the proposed OCC was developed and validated as described in section 3.1, and is presented in figure 3. The model shows the twenty-one key OCC functions required for disruption management activities, in addition to one external input and two external output functions.

5.1 Baseline FRAM Model Analysis

Key/notable features in the baseline FRAM model that are highlighted include:

- The OCC can only react to, and not anticipate, disruption given the functional arrangement of the system and design of sub-system activities and support software.
- The role of Operations Control as the central control 'hub' for disruption management activities, previously suggested through the system description and decomposition processes, was confirmed. In addition, the baseline FRAM

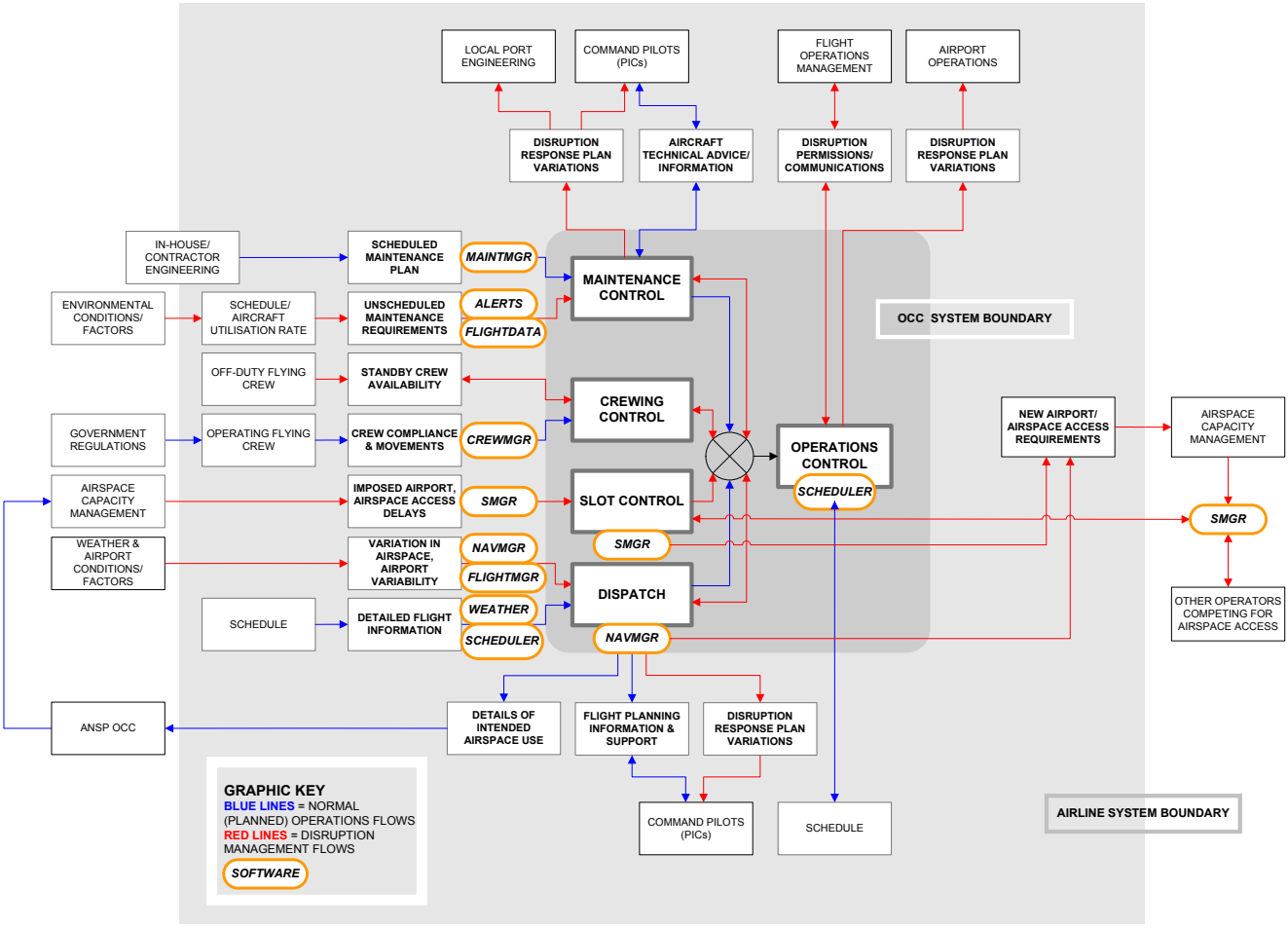

Figure 2: A systems representation of the proposed OCC System

model provided additional insights into the type and nature of functional interactions within the OCC and with external systems/the environment, particularly:

- The external disruption input originating with the release of the SMGR delay schedule.
- The downstream flow of system outputs (information, instructions) to local operational elements tasked with carrying out disruption management tasks. The model disputes the assumption that early consultation and interaction with local operational elements, intended to occur at OC functions, are sufficient and accurate – therefore no feedback loops are required other than software systems representations that the disruption management plan has been executed in the local environment.

The assumed nature and type of interactions between OCC sub-systems was explored and some previously unappreciated interactions uncovered, including:

- All OCC areas have goal conflicts with each other, apply different trade-off parameters, and have overlapping objectives to be satisfied when responding to disruption events.
- The concentration of accountability was noted with respect to making sense of operational information and reducing information uncertainty, managing risk, and leading disruption management planning and responses. The limited accountability of OCC sub-systems for processing and integrating disruption indicators was highlighted.
- The reliance of Operations Control on OCC sub-systems to monitor and advise of disruption conditions and events as promptly as possible.
- The nature of connections between existing OCC sub-systems (i.e. excluding the proposed Slot Control function) are predominantly 'green', reflecting normal and direct connections/coupling between OCC sub-systems (including Operations Control).

Analysis of the model suggested a number of new couplings and interactions between the OCC sub-systems due to the introduction of the proposed Slot Control function:

- Tighter coupling appeared likely between Operations Control and the proposed Slot Control sub-system than seen with other OCC sub-systems. This suggested a different dynamic and raised the potential risk of uncoordinated OCC activities as a result of a lack of clarity as to which of Operations Control or Slot Control would 'lead or follow' under different conditions – this was in contrast to the clear lead accountability that Operations Control had in relation to existing OCC sub-systems.
- Increased complexity and coupling of OC

functions, particularly as a result of dependence on Slot Control functions. This had two main effects to increase complexity: a) an increase in the number of connections, particularly around the primary disruption management response functions, and; b) the nature of the new connections that reflected an increase in the indirect influence of Slot Control functions, on Operations Control functions, through the introduction of constraints and dependence on Slot Control.

- Disruption in the Operations Control disruption sequence, particularly with respect to new connections/coupling from Slot Control functions that bypass the OC functional sequence and that have the potential to create uncoordinated activities between the two sub-systems.
- Finally, functions for SC (Monitor and identify slot non-compliance) and OC (Identify aircraft movement variations) are, from an OCC system perspective, essentially the same activities. Slot Control and Operations Control undertake this activity independently with different objectives, using the same data source (i.e. indicators of push-back at origin, takeoff, touch-down, and parking at destination), but interfacing with different interface representations on different support software. This has the potential to drive different views of a disruption event and uncoordinated/incorrect response activities.

5.2 Derivation of Hazard Scenarios

Once the FRAM baseline model had been validated through System Expert workshop/s, a further series of two workshops employed the keyword/guideword approach to explore perturbations to the model in response to variations in operational conditions, excessive demand on the system, or performance failures within the different OCC sub-systems. The products of this process were:

- Defined sets of system conditions under which the OCC would functionally change, leading to changes in the functional arrangement, different interactions and coupling between OCC sub-systems, and in some cases the redundancy or obsolescence of OCC functions present in ideal conditions.
- Specific FRAM instantiation models of the different functional systems emerging from changes in the defined system conditions, with each instantiation model providing the basis for the development of specific HAZID scenarios.
- Specific HAZID scenarios suitable for formal risk modeling (e.g. full quantification through Probabilistic/Quantitative Risk Assessment, or semi-quantitative techniques such as Bow-tie Analysis, Safety Barrier Diagrams, etc.).

As a result of this process three instantiation models were identified through the FRAM process, linking together through a single Top Event:

An underspecified disruption event occurs in local operations leading to a time loss of >15 minutes, where: The disruption event information is incomplete, uncertain, or subject to time constraints.

The three representative instantiation models developed were SCF-1 (Slot Control Failure), HSI-1 (Human-System Interface), and DRM-1 (Disruption Management). Two of the instantiation models (SCF-1 and HSI-1) describe scenarios that lead to the defined Top Event – i.e. they identify possible causative pathways leading to the Top Event), whereas the third instantiation model (DRM-1) describes the scenarios and outcome events following the Top Event. In these FRAM models the common location for this Top Event is coincident with the primary Operations Control function defined in the model.

5.2.1 Analysis of FRAM Scenario SCF-1

The Slot Control Failure instantiation model (SCF-1) describes the consequences of a situation where the proposed Slot Control function fails to perform to the required standard, and the OCC undergoes a sudden reconfiguration with Slot Control activities being commandeered by Operations Control. The degraded Slot Control sub-system performance is most likely after the initial implementation of the new OCC configuration, under conditions of high workload (such as during peak airspace usage times, in the lead-up to curfews at specific airports, etc.), and likely to be exacerbated by the relative inexperience of the Slot Control operators during early operations with the new system. Analysis of the SCF-1 instantiation model suggests that:

- The transfer of functional activity to Operations Control is likely to increase the volume of Operations Control work tasks, and a larger information set will need to be tracked and integrated to produce an adequate description of the disruption event – this will introduce time delays into the disruption response process.
- Operations Control is unlikely to have the training and competency with SMGR to enable the same ease of data identification and integration as Slot Control operators, taking more time and with a greater risk of missing or misinterpreting critical information.
- While sufficient controls exist with the airline and airspace management systems to capture the effect of any errors and mitigate safety hazards/risks, the introduced time delays impact commercial performance by reducing the availability of suitable recovery options following a disruption event, some functions will be performed in a ‘degraded mode’, and the optimisation function in the model will be deactivated during disruption recovery.
- Slot Control shifts to a ‘response on demand’ mode solely triggered by Operations control requests; monitoring of aircraft movement is constrained, and subsequently becomes less capable of anticipating and projecting the likely future consequences/impacts on available slot options.

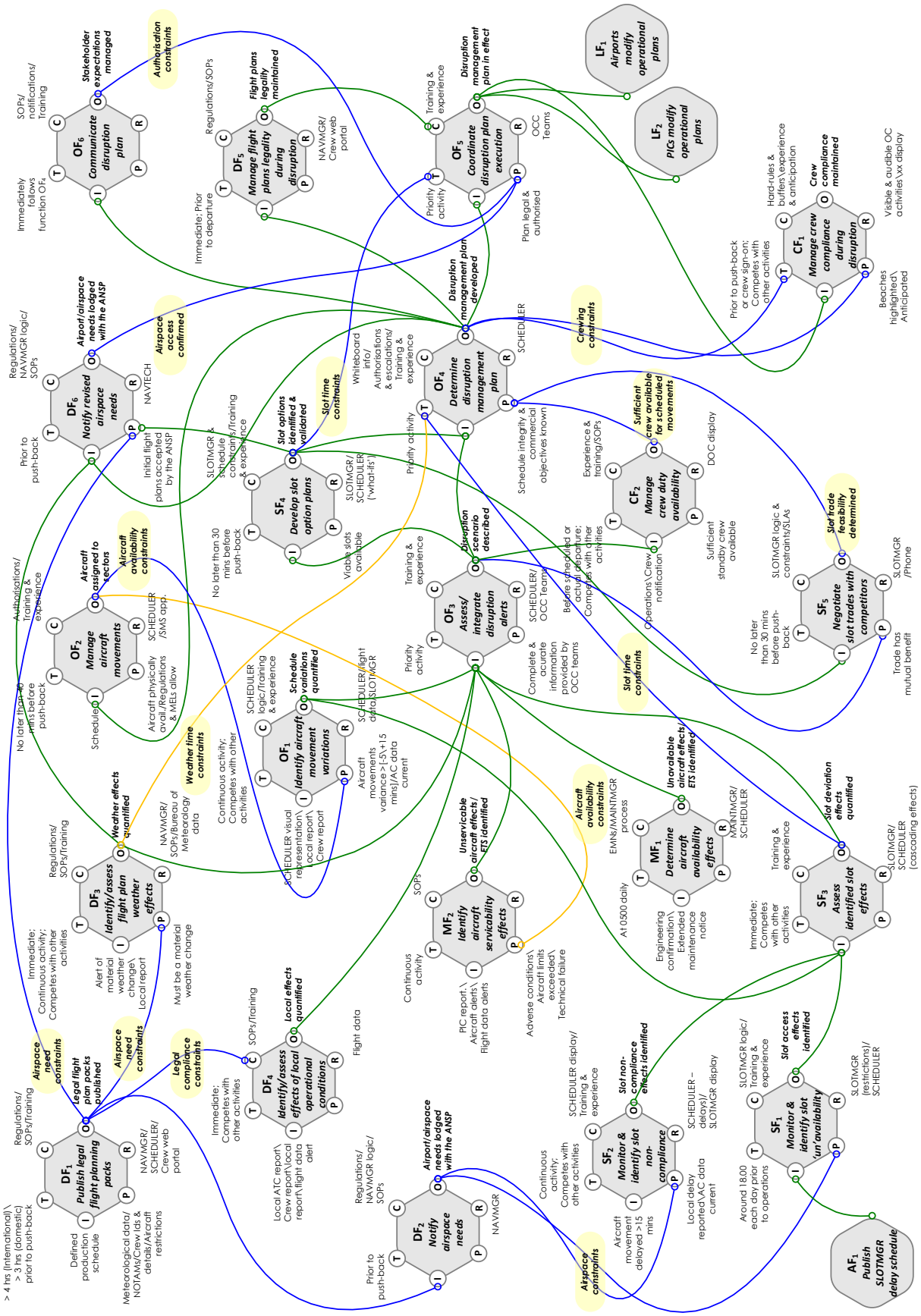

Figure 3: FRAM baseline model of the proposed OCC System

In summary, the SCF-1 model proposes a situation where changes in system configuration and an increase in coupling between Slot Control and Operations Control functions leads to commercial impacts and reduced system performance.

5.2.2 Analysis of FRAM Scenario HSI-1

The Human-System Interface instantiation model (HSI-1) describes numerous Human-System and Human-Computer Interface issues, including a number of factors directly impacting on the accurate description of disruption events and the timely monitoring of disruption management plan implementation/execution. These factors included underspecified software data, obsolete information representations, information supply delays, support software limitations with information presentation, and limited support for 'what-if' modeling of possible scenarios.

These effects are present to varying degrees under all conditions, but are exacerbated and the Top Event identified previously more likely under conditions where local reporting is delayed or not available to reduce information uncertainty, or where time pressures increase the likelihood that OCC operators will fail to identify or misinterpret critical information, or where they incorrectly integrate information.

Analysis of the HSI-1 instantiation model suggests that there are a number of functional connection/coupling changes possible, all independent and that therefore could occur simultaneously under credible scenarios:

- The SMGR input function provides processed information that is conservative and restricts OCC activities. However, airspace access is subject to sudden capacity changes due to shifts in environmental conditions, resulting in a sudden state transition within (geographical sections of) the Australian airspace system; The type and timing of data delivery through SMGR is delayed and changes without warning, such that the OCC is unlikely to be able to take advantage of sudden increases in airspace system capacity.
- The impact of information incompleteness, uncertainty, and access delay, leads to a situation where Operations Control becomes more reliant on the Dispatch and Slot Control functions, resulting in tighter coupling between key OCC functions.

In addition, there are a number of possible effects likely to eventuate under enabling conditions:

- SMGR does not use absolute 'real-time' data, and the obsolescence of the data presented needs to be judged by the operator. This slows decision-making and forces a conservative approach that requires information uncertainty to be resolved to reduce disruption response risk, but incurs time and opportunity cost.
- The main data set used by other scheduling and planning systems within the OCC is underspecified, as it does not provide continuous data to track progress towards milestone events, nor for critical unanticipated failure events (such as an aborted taxi maneuver and return to the terminal).
- Finally, there are only limited links between some of the support software, leaving the sub-system operators to largely act as the link to process the different representations, cross-check the processed data, and integrate the information to support planning and decision making activities.

This analysis has shown that there are HSI features present in the OCC system and the different support software used by each OCC sub-system that lead to inefficiencies and delays in the identification of, and access to, critical information: the consistency of information delivery varies, and the completeness and certainty of information received is also variable. This serves to force the OCC in general, and the Operations Control sub-system in particular, to rely more on local reports to adequately describe a disruption event, in addition to increasing communication and event validation workload.

Finally, these aspects of the HSI-1 instantiation model highlight the conditions that arise under a specific (and likely) set of operating conditions whereby the previously identified Top Event can occur. However, they can also contribute to the set of conditions associated with the situation identified in the previous SCF-1 instantiation model, which highlights a contradiction: Operations Control increasing coupling with, and dependence on, Slot Control immediately prior to a sudden system state transition where dependence is reduced and the actual coupling interaction altered.

5.2.3 Analysis of FRAM Scenario DRM-1

The Disruption Management instantiation model (DRM-1) describes a situation where the Operations Control sub-system responds to a disruption event without an accurate description of the event, and directs local activities that are inconsistent with the actual operational requirements. This is most likely to occur in the situation described by the SCF-1 instantiation model and is strongly influenced by the presence of the conditions described in HSI-1 – particularly when coupled with conditions of high workload (such as during peak airspace usage times, in the lead-up to curfews at specific airports, etc.), and time pressures. Analysis of the DRM-1 instantiation model suggests that:

- There are significant increases in downstream coupling between functions, and a corresponding increase in system complexity: Existing connections to the supporting sub-system functions are significantly impacted or degraded, as a result of enacting incorrect instructions and undertaking activities that will be inadequate or ineffective in responding to the actual disruption event at the local operational level;
- The 'downstream' functions acting in local operations now play a significant role in quality checking the adequacy of the disruption response

instructions for addressing the disruption event. As a result a feedback loop is created between local (airport/aircraft) functions and key OCC functions: however, this feedback may be subject to a significant time delay, and reduce the opportunity for Operations Control to recover an unplanned event without incurring increased commercial costs.

- Also of note is the fact that some of the local operational functions now become temporary functional controls for managing flight plan legality and crew duty limit compliance instead of the designated OCC functions.

The effect of unresolved information uncertainty, incompleteness, or delay on the OCC system is dramatic: decision-making and response to disruption events are significantly delayed or incorrect. The effect of implementing an erroneous disruption management plan is to shift the responsibility for identifying and preventing the error is transferred outside of the OCC system, with local airport and pilot operations and the local Air Traffic Controller acting as the barriers that prevent inappropriate operational activities. This creates a new and significant feedback loop, but one that carries a significant time penalty and associated commercial cost.

6 The Utility and Limitations of the FRAM Technique for SHA

While only applied to a single and quite specific system problem in this research, assessment of the utility of a modified FRAM technique within a SHA process suggests the technique's relative strengths and value for identifying hazards and mishap scenarios, and for assessing barrier effectiveness:

- FRAM has increasing utility when assessing degraded performance of safety devices and controls, increasing further to strong utility in relation to the assessment of safety constraint/function efficacy. However, the utility is context dependent on the level of system decomposition applied in response to the defined system problem: in general FRAM utility decreases as the system analysis tends towards decomposition at the component level. FRAM has strong utility for establishing hazards emerging from system complexity and interaction/coupling, but reduced value for establishing technical design issues; it would appear that as the HAZID process/application becomes more detailed and component focused, FRAM becomes less valuable to the point where the use of established inductive/deductive HAZID techniques would be preferable.
- It would appear that as the nature of the system problem requires a more detailed understanding of specific operator tasks and activities the utility of the FRAM technique reduces, requiring supplementary analysis using established Human Factors and Cognitive Systems Engineering techniques/methods. Despite this, application of the FRAM technique does lead to specific human factors issues being highlighted, and therefore provides useful guidance to the analyst in selecting particular techniques/methods suitable for providing insight into specific and detailed system questions.

The utility of the FRAM technique in SHA is therefore largely dependent on the nature of the system under study, and the features of the particular system problem to which HAZID techniques are being applied. FRAM has utility for HAZID activities where the system under study has features that are suitable for the application of the technique:

- System decomposition occurs at the system/sub-system level, where interactions, connections, and coupling behavior at this level would provide system behavior insights useful in addressing the defined system problem.
- The effects of interaction and complexity are likely to be relevant to answering the defined system problem, particularly where the system under study can be considered a socio-technical system.
- Human-System interface issues are likely, particularly when the system under study includes geographically isolated operators needing to coordinate activities, decentralized/delegated control functions, or high functional variability (including volatile system dynamics) that rely on local response activities to address disruption events.
- Where system decomposition is required that indicates where further specific analysis techniques are required, and that can help define specific questions for further targeted analysis.
- Conversely, FRAM is likely to have reduced utility when applied to the analysis of systems that are predominantly technical, geographically distinct, or where performance can be defined in binary mode terms (i.e. failed/not failed).

The completeness (or more correctly, the incompleteness) of any technique remains a limitation of all HAZID methods: No single hazard evaluation technique or methodology can be guaranteed to identify all hazards; similarly, the hazard evaluation process cannot provide certainty that all incident situations and scenarios of importance have been described (CCPS, 2008). Future research could explore this issue by incorporating FRAM and traditional hazard identification techniques (e.g. HAZOPs variants, FMEA/FMECA approaches, etc.) into a SHA to compare the relevant contributions of each singly and in combination.

Nonetheless, the singular use of a modified FRAM technique, as presented within this case study, has identified specific system performance factors and hazards arising under defined scenarios and conditions that would not have been identified using traditional risk analysis techniques alone. However, further work would be required to specifically evaluate and confirm the efficacy of the technique for this purpose.

7 Conclusion

This paper has presented a novel methodology for conducting a SHA in a complex and safety-critical system, for the case of an airline OCC. FRAM analysis of changes to the OCC of a international large airline confirmed the presence of complexity and socio-technical system features, including the integration of technological systems (where hardware and software technology feature as significant elements within the system), human interfaces, and human-intensive organisational systems.

Notable requirements identified emerged from the analysis of interactive, dynamic, and decompositional complexity, and highlighted potential system performance improvement options through consideration of:

- The degree to which the existing software systems supported operator activities and OCC functions, and the impact of introducing new COTS software into an existing software suite.
- Information/data flows and currency, with particular attention to the efficacy of feedback loops.
- Coordination between OCC sub-systems.

The use of FRAM within a SHA context has utility for hazard identification purposes, with a useful set of potential hazards identified at the functional interfaces between sub-systems and systems outside of the boundary of the system under study, and in relation to latent functional design hazards. The FRAM technique has potential utility for modeling and analysing complex and non-linear system behavior, including degraded (i.e. non-binary) functional modes and performance variability, and particularly in relation to describing the influence of organisational, social, and human factors on system function. The technique was useful in the context of the scenario driven approach to SHA, as it enabled system-level mishap scenarios to be identified, while highlighting the relationship between structural elements and the functional capability required to meet the system purpose and objectives.

With the increasing emergence of large scale and complex systems, including those that evolve independently of a central organizing architecture, the importance of techniques (such as FRAM) that allow the exploration of system complexity and behavioral effects will become increasingly critical to architecting systems that are safe by design.

8 References

Allenby, K., Kelly, T., (2001): Deriving safety requirements using scenarios. *Proc. Fifth IEEE International Symposium on Requirements Engineering*, Toronto, Canada, 27 Aug 2001 - 31 Aug 2001, pp.228-235

Bahr, N.J. (1997): *System Safety Engineering and Risk Assessment: A Practical Approach*. New York, Taylor & Francis.

Belmonte, F., Schön, W., Heurley, L., and Capel, R. (2011): Interdisciplinary safety analysis of complex socio-technological systems based on the Functional Resonance Accident Model: an application to railway traffic supervision. *Reliability Engineering and System Safety* **96**: 237-249.

Bossel, H. (2007): *Systems and Models: Complexity, Dynamics, Evolution, Sustainability*. Norderstedt, Books on Demand GmbH.

Cameron, I., Raman, R., (2005): *Process Systems Risk Management*. Process Engineering Series, San Diego, Elsevier Inc.

CCPS, (2008): *Guidelines for Hazard Evaluation Procedures*. 3rd edition, Hoboken, American Institute of Chemical Engineers.

Dekker, S., Cilliers, P., Hofmeyr, J.-H. (2011): The complexity of failure: Implications of complexity theory for safety investigations. *Safety Science* (**49**): 939-945.

Ericson, C.A., (2005): *Hazard Analysis Techniques for System Safety*. Hoboken, John Wiley & Sons, Inc.

Groth, K., Wang, C., Mosleh, A. (2010): Hybrid causal methodology and software platform for probabilistic risk assessment and safety monitoring of socio-technical systems. *Reliability Engineering and System Safety* (**95**): 1276-1285.

Herrera, I.A., Woltjer, R. (2010): Comparing a multi-linear (STEP) and systemic (FRAM) method for accident analysis. *Reliability Engineering and System Safety* (**95**): 1269-1275.

Hollnagel, E., (2004): *Barriers and Accident Prevention*. Surrey, Ashgate Publishing Limited.

Hollnagel, E., (2009): *The ETTO Principle: Efficiency-Thoroughness Trade-Off, Why Things That Go Right Sometimes Go Wrong*. Surrey, Ashgate Publishing Limited.

Hollnagel, E., (2012): *FRAM: the Functional Resonance Analysis Method: Modeling Complex Socio-Technical Systems*. Surrey, Ashgate Publishing Limited.

Hollnagel, E., (2013a): *Publications*. http://www.functionalresonance.com/FRAM_Publications.html. Accessed 12 Jun 2013.

Hollnagel, E., (2013b): *Introduction to FRAM: The Functional Resonance Analysis Method*. http://www.functionalresonance.com/FRAM-2_introduction_to_FRAM.pdf. Accessed 15 Jul 2013.

Jackson, S., (2010): *Architecting Resilient Systems: Accident Avoidance and Survival and Recovery from Disruptions*. Hoboken, John Wiley and Sons, Inc.

Khan, F.I. (2001): Use Maximum-Credible Accident Scenarios for Realistic and Reliable Risk Assessment. *Chemical Engineering Progress* **97**(11): 56-64.

Leveson, N.G., (1995): *Safeware: System Safety and Computers*. New York, Addison-Wesley publishing Company.

Leveson, N.G., (2011a): *Engineering a Safer World: Systems Thinking Applied to Safety*. Cambridge, The MIT Press.

Leveson, N.G. (2011b): Applying systems thinking to analyze and learn from events. *Safety Science* (**49**): 53-64.

Macchi, L., Hollnagel, E., and Leonhardt, J. (2008): A systemic approach to HRA: A FRAM modeling of Control Overflight activity. *4th Eurocontrol Annual Safety R&D Seminar*, Southampton, UK.

Mannan, S., (2005): *Lee's Loss Prevention in the Process Industries: Hazard Identification, Assessment and Control.* 3rd edition, Burlington, Elsevier Butterworth-Heinemann.

Modarres, S.W., Cheon, S.W. (1999): Function-centered modeling of engineering systems using the goal tree-success tree technique and functional primitives. *Reliability Engineering and System Safety* (**64**): 181-200.

NASA, (2011): *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*. NASA/SP-2011-3421, 2nd edition, Washington, NASA.

Nemeth, E., Bartha, T. (2009): Formal Verification of Safety Functions by Reinterpretation of Functional Block Based Specifications. In *FMICS 2008, LNCS 5596*. 199-214. Cofer, D., Fantechi, A. (eds.).

Nouvel, D., Travadel, S., and Hollnagel, E. (2007): Introduction of the Concept of Functional Resonance in the Analysis of a Near-Accident in Aviation. *33rd ESReDA Seminar: Future challenges of accident investigation*, Ispra, Italy.

Perrow, C., (1984): *Normal Accidents: Living with High-Risk Technologies*. New York, Basic Books, Inc.

Rasmussen B., Petersen, K.E. (1999): Plant functional modeling as a basis for assessing the impact of management on plant safety. *Reliability Engineering and System Safety* (**61**): 201-207.

Roland, H.E., Moriarty, B., (1990): *System Safety Engineering and Management*. 2nd edition, New York, John Wiley & Sons, Inc.

Seligmann, B.J., Nemeth, E., Hangos, K.M., Cameron, I.T. (2012): A blended hazard identification methodology to support process diagnosis. *Journal of Loss Prevention in the Process Industries* (**25**): 746-759.

Sui, N. (1994): Risk assessment for dynamic systems: An overview. *Reliability Engineering and System Safety* (**43**): 43-73.

Vicente, K.J., (1999): *Cognitive Work Analysis: Towards Safe, Productive, and Healthy Computer-Based Work*. Mahwah, Lawrence Erlbaum Associates.

Woltjer, R., Hollnagel, E. (2008a): Modeling and evaluation of air traffic management automation using the functional resonance accident model (FRAM). *8th International Symposium of the Australian Aviation Psychology Association*, Sydney, Australia.

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