The Functional Resonance Accident Model

Erik Hollnagel
Cognitive Systems Engineering Laboratory
Department of Computer and Information Science
University of Linköping, SE-58183 Linköping, Sweden
E-mail: eriho@ida.liu.se

Örjan Goteman
Captain/Industry Graduate
Scandinavian Airlines and Linköping Institute of Technology
SE-58183 Linköping
orjan.goteman@sas.se

Abstract

Accident models have over the last 70 years slowly developed from linear cause-effect sequences to systemic descriptions of emergent phenomena. An example of the latter is the Functional Resonance Accident Model (FRAM), which uses the principle of stochastic resonance in a system context. The model can be used both to account for complex accidents and to identify risks in dynamic systems. The latter is demonstrated by means of the area navigation (RNAV) approach operation.

1. Introduction

The understanding of accidents has over the last 20 years or so changed dramatically. The thinking was initially based on relatively simple cause-effect propagations, as in Heinrich's (1931) well-known Domino Model. This view was widely adopted and in many ways remains the industry standard, despite its several shortcomings. It was nevertheless seriously challenged towards the end of the 1970s by a number of major industrial accidents that could not be adequately explained in terms of simple cause-effects links. This created a need both to improve the explanation of human performance failures beyond the concept of "human error", and to account for the complexity that unfortunately had become the trademark of large-scale industrial systems, thereby making accidents look like normal rather than exceptional events (Perrow, 1984).

More formally, accident models can be described as having gone through three major stages, called sequential, epidemiological and systemic models. These stages partly match the developments in the engineering, social, and behavioural sciences. Sequential accident models represent the accident as the outcome of a series of individual steps that occur in a given, and in principle also predictable, order. Sequential models are not limited to a single sequence of events but may be represented in the form of hierarchies such as the traditional event tree or networks such as Critical Path models or Petri networks. They may also represent either the scenario as a whole, or only the events that went wrong. Sequential models are attractive both because they allow thinking in causal series rather than causal nets (cf. Dörner, 1980) and because they are easy to represent graphically. While sequential models were adequate for industrial systems in the first half of the 20th Century, they are insufficient to explain accidents in the more complex systems that now are common.

Epidemiological models describe accidents in analogy with the spreading of a disease, i.e., as the outcome of a combination of manifest and latent factors that happen to exist together in space and time. The term was defined as "the unexpected, unavoidable unintentional act resulting from the interaction of host, agent, and environmental factors within situations which involve risk taking and perception of danger" (Suchman, 1961; quoted in Heinrich, Petersen & Roos, 1980, p. 50). According to this view an accident results from a combination of "agents" and environmental factors that together create an unhappy setting. These models overcome the limitations of sequential models in describing the complexity of accidents. Since latent factors simply cannot be reconciled with the simple idea of a causal series, the analysis cannot be a search for simple causes but must involve an account of more complex interactions among different factors (Reason, 1987). Yet epidemiological models are only as strong as the analogy behind and cannot easily account for an accident with such details as are needed to develop specific countermeasures.

The systemic accident model endeavours to describe the characteristic performance on the level of the system as a whole rather than on the level of specific cause-effect "mechanisms" or even epidemiological factors. Instead of using a structural decomposition of the system, the systemic view considers accidents as emergent phenomena, which therefore are "normal" or "natural" in the sense of being something that must be expected. Systemic models have their roots in control theory (Sheridan, 1992) and emphasise the need to base accidents analysis on an understanding of the functional characteristics of the system, rather than on assumptions or hypotheses about internal mechanisms or cause-effect chains. Systemic models deliberately try to avoid a description of an accident as a sequential or ordered relation among individual events or even as a concatenation of latent conditions, and are therefore difficult to represent graphically.

The three main types of accident models are summarised in Table 1. Each type carries with it a set of assumptions about how an accident analysis should take place and what the response should be.

2. Resonance as a Cause

The conceptual and philosophical problem in searching for causes to accidents is that "nothing comes from nothing". This means that even an initiating event or "root cause" requires an explanation. If this is sought following the principle of backwards cause-effect chaining, the outcome is an infinite regress, which is unacceptable from both an intellectual and practical point of view. While it in most cases is plausible to assume that the cause lies within the system itself, a search or an explanation based on linear reasoning is bound to be inconclusive. (Even if the cause resides outside the system, the same principle holds, since for the purpose of analysis the system boundaries can be enlarged to include the cause.)

The solution to this problem is to dispense with linear reasoning and instead consider non-linear system models. There are many arguments in favour of non-linear models, which have been used in a number of other fields, for instance biology and meteorology. The best-known example of a non-linear model is probably chaos theory (Lorenz, 1993), which has been very useful in dealing with complexity and fractality. For the purpose of understanding the nature of accidents, it is, however, possible to use a simpler concept, namely that of stochastic resonance (Benzi et al., 1981).

Resonance is defined in physics as a relatively large selective response of an object or a system that vibrates in step or phase with an externally applied oscillatory or pushing force, as anyone who uses a swing quickly discovers. Resonance is the increase in amplitude of oscillation of an electric or mechanical system exposed to a periodic force whose frequency is equal or very close to the natural undamped frequency of the system. The difference between normal and stochastic resonance is in the nature of the forcing function. Stochastic resonance is a phenomenon in which a non-linear input is superimposed on a periodic modulated signal. This signal is so weak as to be normally undetectable, but becomes detectable due to resonance with the stochastic noise, cf. Figure 1.

Complex systems, such as socio-technical systems, are by definition composed of a number of subsystems, which in turn may comprise multiple functions. Although the technological and human (individual, organisational) system components are designed to function in a reliable and predictable manner, performance is always variable to a smaller or larger extent. If a subsystem or a component is considered by itself, this performance variability can be seen as a weak modulated signal, which normally is undetectable, i.e., it is within the limits of tolerance of the system. In relation to any subsystem or component, the rest of the system is the environment. This environment consists of a number of subsystems, for each of which the performance also is variable. Relative to the subsystem under consideration, the aggregated performance variability of this "environment" can be understood as random noise, and it is this random noise that can give rise to resonance, i.e., to a performance variability that is too high.

Table 1: The main types of accident models.

Model type	Search principle	Analysis goals	Example
Sequential models	Specific causes and well-defined links	Eliminate or contain causes	Linear chain of events (domino) Trees / networks
Epidemiological models	Carriers, barriers, and latent conditions	Make defences and barriers stronger	Latent conditions Carrier-barriers Pathological systems
Systemic models	Tight couplings and complex interactions	Monitor and control performance variability	Control theory models Chaos models, stochastic resonance.

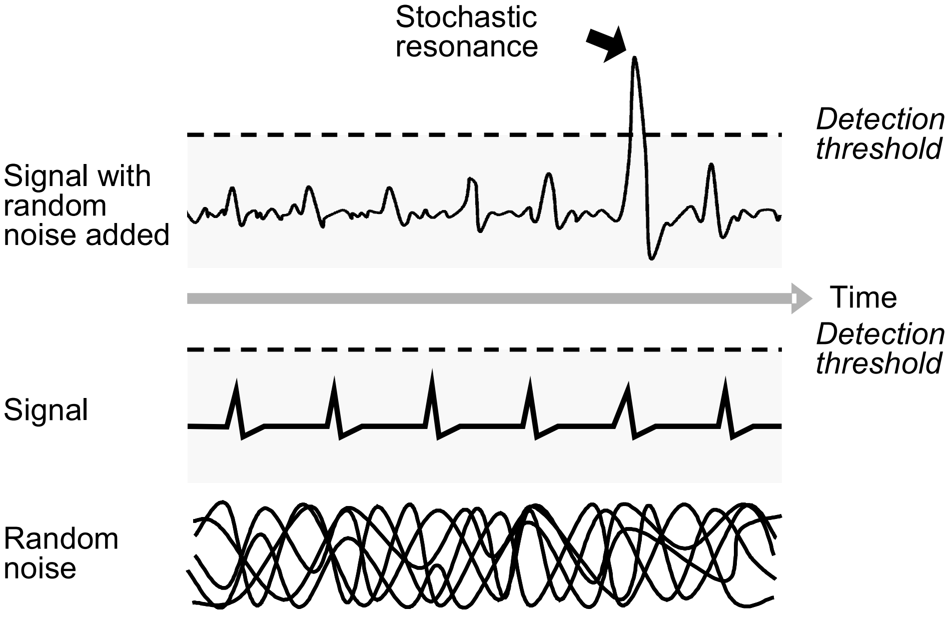

Figure 1: Stochastic resonance

2.1. Functional Resonance

In stochastic resonance the noise is a truly random input that is superimposed on the signal. In that sense the signal is a property of the system while the noise is a property of the environment. In the systemic accident model the delineation between system (weak signal) and environment (noise) is relative, and any part of the system variability can in principle be the signal with the rest being the noise. The noise is furthermore not truly stochastic but is to a large extent determined by the variability of the functions of the system. Since the resulting resonance does not depend on an unknown source but is a consequence of functional couplings in the system, it is more correct to call it functional resonance than stochastic resonance. Even though functional resonance does not provide the final explanation of why accidents happen, it can serve as a useful analogy to think about accidents and understand how large effects can accrue, and therefore also ultimately how to prevent them.

The basis for either accident analysis or risk assessment using the Functional Resonance Accident Model (FRAM), is to first delineate the functional entities that are of importance for the given scenarios or tasks. This is not a trivial exercise, since it must be based on an understanding of system functions rather than system structures. The entities are therefore more likely to be characteristic or recurrent functions than to be system structures or physical units. In some cases a characteristic function may, of course, be closely associated with a structural unit. A function may, for instance, be to check the identity of an object; if this is done automatically, it will typically refer to a specific unit, although a one-to-one correspondence between units and functions is rare. The functional entities are described in terms of the following relations:

As in this heading, they should be Times 11-point boldface, initially capitalized, flush left, with one blank line before, and one after.

- Inputs (I), which are needed to perform the function. Inputs constitute the links to previous functions and can be either transformed or used by the function in order to produce the outputs.
- Outputs (O), that are produced by the function. Outputs constitute the links to subsequent functions.
- Resources (R), representing what is needed by the function to process the input (in terms of, e.g., hardware, procedures, software, energy, manpower).
- Controls (C), or constraints, that serve to supervise or restrict the function (to monitor it and adjusts it when it goes astray). Controls can be active functions or just plans, procedures and guidelines.
- Preconditions (P), which are system conditions that must be fulfilled before a function can be carried out. A common precondition is that another step or process has been completed or that a specific system condition has been established.
- Time (T), which can also be considered a special kind of resource. All processes take place in time and are governed by time. Time can also be a constraint in the sense that there is a time window for an activity (a duration).

A graphical representation of a generic functional entity is shown in Figure 2.

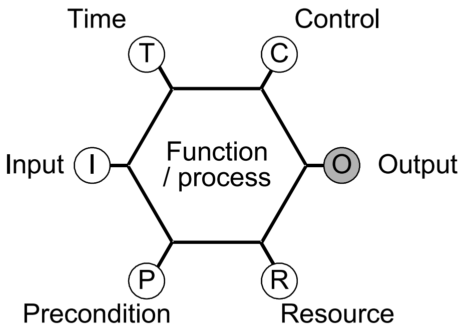

Figure 2: The hexagonal function representation.

The systemic view emphasises how functions depend on each other and how unexpected couplings may suddenly appear. Since the representation is at the level of individual functions, there is no explicit description of the overall structure of the system. Instead it can be derived from how connections between functions are specified. This structure, however, represents the normative organisation of functions, when everything goes according to plan. Since it is unrealistic to assume that this will always be the case, it is preferable to use a representation that makes it possible to account for how events may develop in reality.

2.2. FRAM Analysis Principles

Whereas risk analysis normally looks for how individual functions or actions may fail, FRAM focuses on how conditions leading to accidents may emerge. In practical terms accident prediction therefore requires the following steps:

- Identify and characterise essential system functions; the characterisation can be based on the six connectors of the hexagonal representation.
- Characterise the (context dependent) potential for variability using a checklist.
- Define functional resonance based on identified dependencies among functions.
- Identify barriers for variability (damping factors) and specify required performance monitoring.

The following section will present the four steps in further detail, to give a concrete idea of what they entail in practice. The example is area navigation (RNAV) operations.

3. A FRAM Description of Area Navigation

Contemporary flight guidance avionics is capable of area navigation (RNAV) operations. RNAV is a method of navigation, which permits aircraft operation on any desired flight path within the coverage of station-referenced navigation aids or within the limits of the capability of self-contained aids, or a combination of these (JAA, 2004).

The RNAV operational method allows the construction of both a lateral and a vertical path in the sky. RNAV can therefore be used as an instrument approach procedure to line up the aircraft for final approach to a runway. For smaller aerodromes that cannot financially bear the investment and maintenance costs for a full an Instrument Landing System to provide the pilot with lateral and vertical guidance to the landing runway, RNAV offers a computer-generated lateral and vertical path that the pilot can use.

3.1. Essential system functions

The purpose of RNAV approach operations is to fly the aircraft on a pre-defined lateral and vertical track down to the decision height, where the pilot decides whether to land or to follow the missed approach procedure. This track is defined without the use of land-based navigational aids.

The system under analysis is RNAV approach operations as a whole. Both aircraft artefacts and operators are included and will be considered as subsystems of the analysis. The boundaries will be functionally defined to include not only the hardware artefacts of the cockpit, but also procedures and humans.

3.1.1. Operational boundaries. The RNAV approach starts geographically at the RNAV transition point and ends at the missed approach holding point. The RNAV approach does not include phases of flight prior to the RNAV transition. Neither does it include the landing phase from altitudes below decision height. It is important to understand that at decision height the pilot must decide whether he has sufficient visual cues to land the aircraft safely from the position he is.

3.1.2. Hardware boundaries. The RNAV artefacts considered are the Flight Management System (FMS), consisting of the Flight Management Computer (FMC) and the Autopilot Flight Director System (AFDS) and the Auto Throttle (AT). The RNAV approach does not include flight control surfaces or the wheel autobrake systems. Although they are used during RNAV approach, they are used in a way that does not separate them from other operations.

3.1.3. Operators. The humans in the RNAV approach system are the two pilots (the minimum flight crew). Their number and tasks are described in the aircraft's Aircraft Flight Manual. The ATC controller, responsible for aircraft separation and sometimes also radar vectoring for lining up the aircraft for final approach, is also considered as a part of the RNAV approach system. The cabin crew is not considered in the analysis; neither are central flight operations department staffs, such as chief fleet pilots etc.

3.1.4. System functions. The RNAV approaches shall be able to take the aircraft from the start of the RNAV Transition to the decision height with a required navigational performance of 0,3 Nautical miles (Nm) and a within 125 feet vertical distance from the centreline of the defined lateral and vertical flight path (JAA, 2003). The functions needed for the RNAV approach are presented in Table 2.

Table 2: Functions in the RNAV approach

1. Code procedure from paper into a digital navigation database
2. Load navigation database in A/C
3. Insert RNAV procedure in FMC flight plan
4. Check correct procedure inserted
5. Engage Autopilot (AP) and/or Flight Director (FD) in LNAV and VNAV modes
6. Monitor navigation performance
7. Control Flight Technical Error (FTE)
8. Manage speed to be appropriate for landing latest at Decision Height
9. Land the aircraft with the use of visual cues from DH

Each function must now be described using the six relations defined above. For example, function 4 "check correct procedure inserted", may look as follows (Table 3):

Table 3:

Relation	Function 4: Check correct procedure inserted
Input	RNAV waypoint data
Preconditions	O3. RNAV procedure in FMC flight plan
Resources	RNAV approach chart
Time	60 seconds
Control	PF and PNF verification procedure
Output	Correct procedure is verified in active FMS flight plan

When all nine functions have been described, the normal couplings among them can be identified by going through the descriptions of the six relations for each. This results in the configuration shown in Figure 3. While the main links are between outputs and inputs, there are also links between outputs and resources, meaning that the output from one function is a resource for another. Figure 3 also shows that the dependencies do not represent a simple sequence of the functions, but that there are both one-to-many and many-to-one couplings. Although the functions generally follow a left-right temporal relation, it is not possible to apply that consistently. The relative positions of the functions therefore do not carry any meaning.

3.2. Potential for Variability

Each of the functions described above may potentially vary due to the influence of the context of the RNAV system. The potential for variability can be rated using a number of common performance conditions proposed elsewhere (Hollnagel, 1998). The rating for each function was performed by the second author, and reflected extensive domain knowledge from aircraft operation, airworthiness issues and navigation support issues. Each performance condition was rated as (1) stable or variable but adequate; (2) stable or variable but inadequate and (3) unpredictable. The outcome for function 4 is shown in Table 4 below.

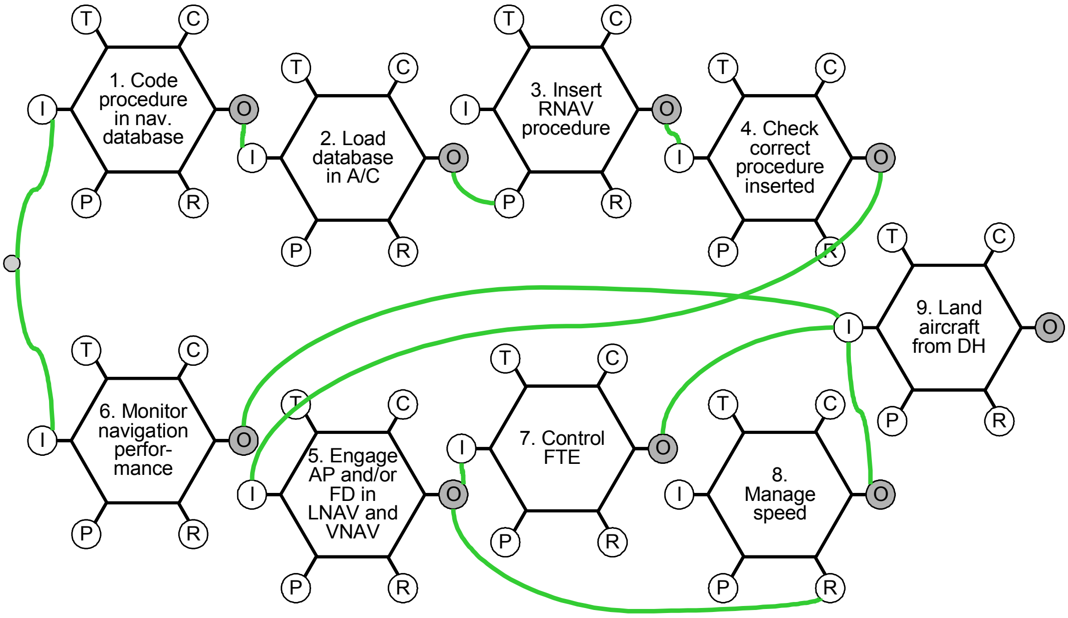
1. Code procedure in nav. database
2. Load database in A/C
3. Insert RNAV procedure
4. Check correct procedure inserted
5. Engage AP and/or FD in LNAV and VNAV
6. Monitor navigation perfor-mance
7. Control FTE
8. Manage speed
9. Land aircraft from DH
T
C
I
O
P
R

Figure 3: FRAM representation for normal conditions.

Table 4: Potential variability of Function 4

Common performance condition	Rating category
Availability of resources	adequate
Training and Experience	adequate
Quality of communication	unpredictable
HMI and operational support	adequate
Access to procedures and methods	adequate
Conditions of work	adequate
Number of goals and conflict resolution	unpredictable
Needed time/available time relation	unpredictable
Circadian rhythm	inadequate
Crew collaboration quality	adequate
Quality and support of organisation	adequate

The rating of the potential for variability shows that there are a number of performance conditions that are rated inadequate or unpredictable. For function 4 these are quality of communication, number of goals and conflict resolution, needed time/available time relation, and circadian rhythm. Considering all functions together this shows that the system RNAV approach is susceptible to performance variability that may affect the outcome.

3.3. Possibilities for Functional Resonance

The next step is to identify the possibilities for functional resonance, i.e., cases where the variability of the functions may interact or combine so that a specific function is incorrectly performed or even missed. Here it is important to note if some of the inadequate conditions are common to several functions, since that may indicate a general susceptibility. High performance variability may mean that inputs, or preconditions, are skipped or insufficiently checked, hence that improper couplings among functions can occur. In the case of the RNAV approach, the analysis found several cases where normal connections might fail shown as red lines, as well as a number of potential unexpected connections shown as dashed red lines (Figure 4).

3.4. Potential Barrier Functions and Barrier Systems

The risk analysis is based upon the assumption that RNAV approach operations are performed by an operator that is supervised by authorities to at least the supervision level required by the Joint Aviation Requirements. This means that the steady-sate performance of the underlying air navigation infrastructure and operational structure is assumed to be acceptable as it is.

The analysis points to four possible failures, namely: Function #2 [incorrect RNAV procedure in the navigation database], Function #4 [bypass of cockpit check that correct procedure is inserted in active FMS flight plan], Function #6 [failure to monitor navigation performance], and Function #7 [bypass of Flight Technical Error and speed control]. For each of these it is necessary to consider possible barriers that can either prevent the failure from occurring or minimise the unwanted consequences.

For the purpose of illustration we shall consider the failure of Function #4 [bypass of cockpit check that correct procedure is inserted in active FMS flight plan]. If this failure happens, then a failure of Function #1 [code procedure from paper into a digital navigation database] will not be detected, which means that the flight crew will fly according to the wrong RNAV procedure. This may introduce a risk for collision with other aircraft, particularly if the operation is performed in a non-radar environment. One precaution could be a symbolic barrier such a flight deck procedure prescribing a check of chart and FMC active flight plan from the map display, which has low susceptibility to failure modes of action targeted against wrong object. The correct procedure check could be both pilots comparing the RNAV procedure on the chart with the pictorial representation of the FMC flight plan on the map display. A more detailed discussion of barriers can be found in Hollnagel (2004).

4. References

Benzi, R., Sutera, A. & Vulpiani, A. (1981). The mechanism of stochastic resonance. J. Phys. A: Math. Gen. 14L 453.

Dörner, D. (1980). On the difficulties people have when dealing with complexity, Simulation and Games, 11, 87-106.

Heinrich, H. W. (1931). Industrial accident prevention. McGraw-Hill: New York.

Heinrich, H. W., Petersen, D. & Roos, N. (1980) Industrial accident prevention (5th Ed). McGraw-Hill: New York.

Hollnagel, E. (1998). Cognitive reliability and error analysis method. Oxford, UK: Elsevier Science.

Hollnagel, E. (2004). Barriers and accident prevention. Aldershot: Ashgate Publishing Limited.

Joint Aviation Authorities, (2003), Certification of aircraft, commercial aircraft, JAR-25, Hoofddorp

Joint Aviation Authorities, (2004), Airworthiness And Operational.

Lorenz, E. (1993). The essence of chaos. London: Routledge.

Perrow, C. (1984). Normal accidents: Living with high risk technologies. New York: Basic Books, Inc.

Reason, J. T. (1987b). The Chernobyl errors. Bulletin of the British Psychological Society, 40 (April), 201-206.

Sheridan, T. B. (1992). Telerobotics, automation, and human supervisory control. Cambridge, MA: MIT Press.

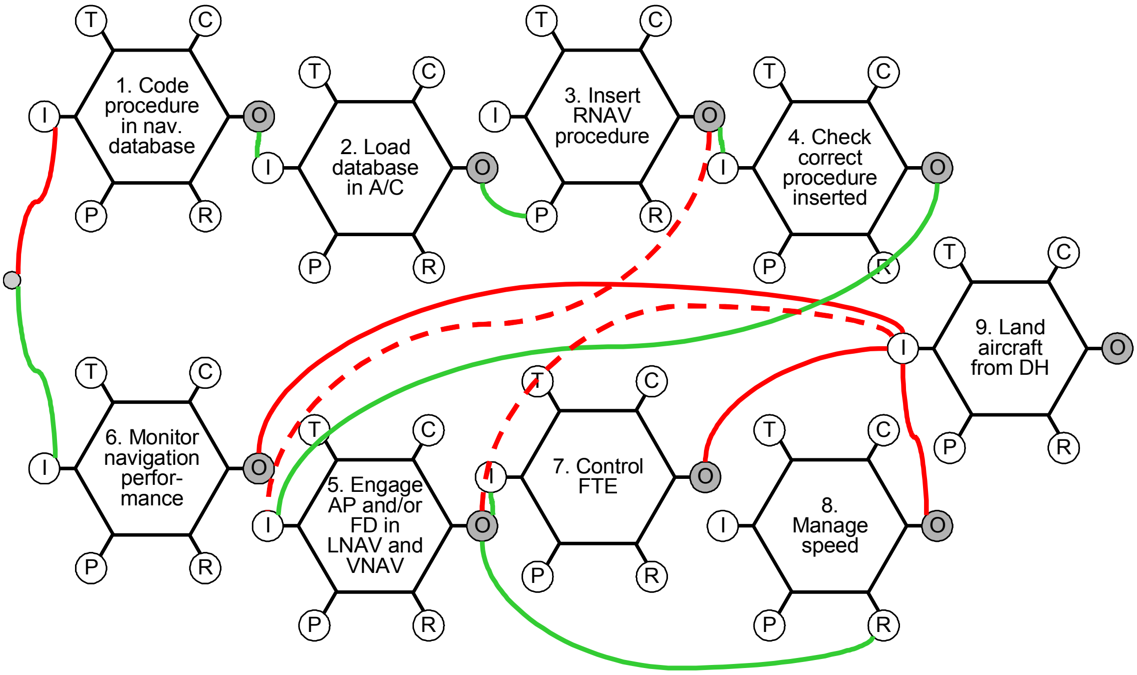
1. Code procedure in nav. database
2. Load database in A/C
3. Insert RNAV procedure
4. Check correct procedure inserted
5. Engage AP and/or FD in LNAV and VNAV
6. Monitor navigation perfor-mance
7. Control FTE
8. Manage speed
9. Land aircraft from DH
T
C
I
O
P
R

Figure 4: Functional resonance for the RNAV approach