University of Ljubljana
Faculty of Computer and Information Science

Graz University of Technology
Faculty of Computer Science and Biomedical Engineering

Karmen Gostiša

The unification of inter-functional couplings in FRAM

MASTER'S THESIS

THE 2ND CYCLE MASTER'S STUDY PROGRAMME

COMPUTER AND INFORMATION SCIENCE

Ljubljana, 2020

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Tehniška univerza v Gradcu
Fakulteta za računalništvo in biomedicinsko inženirstvo

Karmen Gostiša

Poenotenje medaspektnih povezav v metodi FRAM

MAGISTRSKO DELO

ŠTUDIJSKI PROGRAM DRUGE STOPNJE

RAČUNALNIŠTVO IN INFORMATIKA

Ljubljana, 2020

ACKNOWLEDGEMENTS

This thesis is a small piece of a puzzle in the vast scientific world. I would not have been able to complete it without the help of people to whom I am deeply grateful.

I would first like to thank my thesis supervisor Miha Mraz for giving me an idea for the thesis topic, providing guidance and critical feedback on a regular basis, and for inspiring my interest in computer systems reliability and safety.

Many thanks also to my thesis co-supervisor Wolfgang Vorraber for the valuable feedback and insightful comments that improved this work.

I thank my committee, Miha Moškon, Uroš Lotrič, and Nikolaj Zimic for their comments and suggestions that allowed me to improve my thesis.

I am also very grateful to my family for their invaluable support in my life.

— Karmen Gostiša, Ljubljana, June 2020.

CONTENTS

University of Ljubljana
Faculty of Computer and Information Science

Graz University of Technology
Faculty of Computer Science and Biomedical Engineering

Karmen Gostiša

The unification of inter-functional couplings in FRAM

ABSTRACT

With a growing complexity of socio-technical systems and event outcomes that cannot be understood in terms of causality, traditional accident modelling approaches are no longer adequate to analyse accidents in such systems. Thus, in recent years novel systemic approaches have been developed. Functional Resonance Analysis Method (FRAM) is a means to understand how seemingly small performance variations of functions in a complex socio-technical system coincide and mutually affect each other in unexpected ways resulting in the functional resonance. A FRAM model consists of essential system functions, each characterised by six aspects. The functional resonance is defined based on couplings among aspects.

Currently, the method provides only a general classification of couplings: *Matter*, *Energy* or *Information* (MEI). Such classification prevents an analytical view on the complex structure of relations in observed socio-technical systems and permits the construction of non-uniform models. This thesis, thus, seeks to unify FRAM models by developing a classification scheme of inter-functional couplings. The proposed MEDI classification helps to maximise compatibility, safety and quality of FRAM models in general. It represents one of the necessary steps towards the method automatisation.

Key words: safety, socio-technical systems, Functional Resonance Analysis Method (FRAM), inter-functional protocol

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Tehniška univerza v Gradcu
Fakulteta za računalništvo in biomedicinsko inženirstvo

Karmen Gostiša

Poenotenje medaspektnih povezav v metodi FRAM

POVZETEK

Ob vse večji zapletenosti socio-tehničnih sistemov in izidov dogodkov, ki jih ni mogoče razumeti z vidika vzročnosti, tradicionalne metode za modeliranje nesreč v takšnih sistemih ne ustrezajo več. V zadnjih letih so bili zato razviti novi analitični pristopi. Metoda FRAM ali metoda analize funkcijske resonance je metodologija, ki omogoča razumevanje, kako na videz majhne variacije delovanja funkcij v zapletenem socio-tehničnem sistemu sovpadajo in medsebojno vplivajo na nepričakovane načine, ki povzročijo funkcijsko resonanco. Model FRAM sestavljajo ključne sistemske funkcije, opisane s šestimi aspekti. Funkcijska resonanca je opredeljena na podlagi povezav med funkcijami.

Trenutno metoda ponuja le splošno klasifikacijo povezav: *Materija*, *Energija* ali *Informacija* (MEI). Takšna klasifikacija onemogoča analitični pogled na zapleteno strukturo relacij v opazovanem sistemu in dopušča gradnjo nepoenotenih modelov. Cilj pričujočega dela je poenotiti modele FRAM z razvojem klasifikacijske sheme medaspektnih povezav. Predlagana nova klasifikacija medaspektnih povezav MEDI pripomore k večji združljivosti, varnosti in kakovosti modelov FRAM na splošno, ter predstavlja enega od potrebnih korakov k avtomatizaciji metode.

Ključne besede: varnost, socio-tehnični sistemi, metoda analize funkcijske resonance (FRAM), protokol medaspektnih povezav

Universität Ljubljana
Fakultät für Computerwissenschaft und Informatik

Technische Universität Graz
Fakultät für Informatik und Biomedizinische Technik

Karmen Gostiša

Die Vereinheitlichung der interfunktionalen Kopplungen im FRAM

KURZFASSUNG

Mit der zunehmenden Komplexität sozio-technischer Systeme und Ereignissen, die nicht im Sinne der Kausalität verstanden werden können, sind die traditionellen Unfallmodellierungen nicht mehr geeignet, um Unfälle in solchen Systemen zu analysieren. Daher wurden in den letzten Jahren neue systematische Ansätze entwickelt. Die Methode der funktionellen Resonanzanalyse (Functional Resonance Analysis Method, FRAM) ist ein Mittel, um zu verstehen, wie scheinbar kleine Leistungsschwankungen von Funktionen in einem komplexen sozio-technischen System zusammenkommen und sich gegenseitig in unerwarteter Weise beeinflussen, so dass eine funktionelle Resonanz entsteht. Ein FRAM-Modell besteht aus wesentlichen Systemfunktionen, die jeweils durch sechs Aspekte charakterisiert sind. Die funktionelle Resonanz wird auf der Grundlage von Kopplungen zwischen den Aspekten definiert.

Gegenwärtig liefert die Methode nur eine allgemeine Klassifizierung der Kopplungen: *Materie*, *Energie* oder *Information* (MEI). Eine solche Klassifikation verhindert eine analytische Sicht auf die komplexe Struktur der Beziehungen in überwachten sozio-technischen Systemen und erlaubt die Konstruktion nicht einheitlicher Modelle. Die vorliegende Arbeit versucht daher, FRAM-Modelle zu vereinheitlichen, indem sie ein Klassifikationsschema interfunktionaler Kopplungen entwickelt. Die vorgeschlagene MEDI-Klassifikation trägt dazu bei, die Kompatibilität, Sicherheit und Qualität von FRAM-Modellen im Allgemeinen zu maximieren. Sie stellt einen der notwendigen Schritte zur Automatisierung der Methode dar.

Schlüsselwörter: Sicherheit, sozio-technische Systeme, die Methode der funktionellen Resonanzanalyse (FRAM), interfunktionales Protokoll

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Tehniška univerza v Gradcu
Fakulteta za računalništvo in biomedicinsko inženirstvo

Karmen Gostiša

Poenotenje medaspektnih povezav v metodi FRAM

RAZŠIRJENI POVZETEK

Motivacija Današnji socio-tehnični sistemi s področij kot so letalstvo, zdravstvo, gradbeništvo in elektroenergetika prinašajo udobje in učinkovitost v različne vidike človeškega življenja. Ob vse večji zapletenosti tovrstnih sistemov in nesrečah, za katere ne najdemo razloga v odpovedi računalniške komponente ali človeški napaki, tradicionalne metode za ocenjevanje varnosti sistema ne zadostujejo več. V zadnjih letih so bili zato razviti novi analitični pristopi, med katere spada tudi metoda FRAM.

Metoda FRAM ali metoda analize funkcijske resonance [1] je metodologija, ki na podlagi opisov sistemskih funkcij in interakcij med njimi določi možnost pojava funkcijske resonance. Vzroki za ta pojav so težko določljivi in ne temeljijo na preprostem linearnem razmišljanju, ki zaporedna dogodka obrazloži s principom "vzrok-posledica". Resonanco povzročijo na videz majhne variacije delovanja funkcij, ki v zapletenem sistemu sovpadajo in medsebojno vplivajo na nepričakovane načine, kar ima lahko pozitiven ali negativen vpliv na delovanje sistema. Do variabilnosti posameznih funkcij prihaja zaradi prilagajanja sistema spremembam in motnjam, s čimer ohranja željeno funkcionalnost. Metoda se danes uporablja na številnih področjih, tako za analizo preteklih neželjenih dogodkov kot tudi ocenjevanje porajanja bodočih neželjenih dogodkov, do katerih lahko pride v opazovanem sistemu.

Model FRAM sestavljajo ključne sistemske funkcije, opisane s šestimi aspekti. Funkcijska resonanca je opredeljena na podlagi povezav med funkcijami. Trenutno metoda opredeljuje le naslednje tipe povezav: *Materija*, *Energija* ali *Informacija* (MEI). Takšna klasifikacija onemogoča analitični pogled na zapleteno strukturo relacij v opazovanem sistemu in dopušča gradnjo nepoenotenih modelov. V tem delu se posvetimo razvoju medaspektnega protokola, ki bo poenotil modele FRAM, s tem pa pripomogel k večji združljivosti, varnosti in kakovosti modelov, obenem pa postavil temelj avtomatizaciji metode.

Medaspektni protokol V pričujočem delu predstavljamo klasifikacijsko shemo medaspektnih povezav MEDI (Materija, Energija, Data, Informacija) kot razširitev obstoječe klasifikacije MEI. Razvoj protokola je potekal v več korakih. Najprej je bilo izbranih pet modelov FRAM z različnih področij. Vsak model smo temeljito preučili in ugotovili, da niso izraženi tako, da bi jih lahko predstavili računalniškem sistemu, ki terja določeno organizacijo in ustreznost podatkovnih struktur. Pred razširjanjem obstoječe klasifikacije smo zato rekonstruirali modele s pomočjo konceptov iz računalništva kot sta abstrahiranje in logična organizacija podatkov, v našem primeru funkcij in povezav. V takšnih modelih smo po večkratnih iteracijah pričeli prepoznavati vzorce tipov povezav. Pridobljene rezultate smo ovrednotili na dveh modelih, ki nista bila vključena v procesu postavljanja protokola.

Protokol je sestavljen iz štirih glavnih kategorij: Materija, Energija, Data in Informacija. Materijo in Energijo smo ohranili iz obstoječe klasifikacije, medtem ko smo vpeljali novo kategorijo Data in Informacijo podrobneje opisali ter razdelili. Pri preučevanju modelov je bilo ugotovljeno, da se povezave, ki smo jih po stari klasifikaciji uvrščali pod Informacijo, med seboj razlikujejo po tem, ali gre za gole podatke, ali pa vsebujejo podatke že umeščene v kontekst. Lep primer modela, ki prikazuje to razliko, je prikazan na sliki 4.1, kjer ena izmed povezav predstavlja rezultate laboratorijske preiskave in druga spremenjen načrt zdravljenja. Prva vsebuje številske in opisne podatke, pri drugi pa gre za bolj zapleteno podatkovno strukturo, ki zajema navodila in zapise povezane z zdravljenjem. Razlika je torej v tem, da druga povezava vključuje kontekst in s tem predstavlja neposredno uporaben podatek. Takšno povezavo zato poimenujemo Informacija.

Kategorijo Data nadalje razvrstimo na tri podkategorije, in sicer številsko, opisno ter mešano. Na povezavah med funkcijami v modelu FRAM se namreč prenašajo različne vrste podatkov, ki so lahko številski ali opisni.

Omenili smo že, da Informacija poleg osnovnih podatkov (Data) zajema še kontekst. V modelih, ki smo jih uporabili za razvoj klasifikacije, smo razpoznali nekatere ponavljajoče vzorce, ki so nam omogočali nadaljnjo delitev Informacije na podkategorije. Prvi dve sta povezani s časovnim aspektom funkcij, in sicer sta to Prekinitev in Časovno okno. Prekinitev je akcija, ki prekine opazovano funkcijo in lahko vpliva na njen časovni potek ter kakovost izvedbe. Časovno okno je interval, v katerem mora biti funkcija izvedena. Naslednji dve podkategoriji, Opazka in Opozorilo, se nanašata na zaznavo nečesa, ponavadi akcije ali posledice neke akcije. Razlika med njima je, da je Opazka vedno izhod človeške funkcije, medtem ko Opozorilo izda tehnična naprava in je zato izhod tehnološke funkcije. Naslednja podkategorija, imenovana Sprememba, predstavlja povezavo med funkcijama, ko sprememba v prvi funkciji vodi do spremembe v drugi. Primer te povezave je prikazan na sliki 4.8, in sicer gre za primer, ko sta dve strukturi (parkirna garaža in nasip) fizično povezani in stanje prve vpliva na drugo. Predzadnjo podkategorijo Informacije smo poimenovali Pogoj in pomeni dogovor, ki mora biti izpolnjen, preden se lahko nekaj izvede. Pogosto gre za množico pogojev, ki skupaj omogočajo izvedbo funkcije, do katere teče omenjena povezava. Zadnji tip povezave je Navodilo, vsebujoč pravila in smernice, ki usmerjajo opazovano funkcijo, da proizvede pravilni izhod.

Zaključek Klasifikacija medaspektnih povezav MEDI prinaša boljšo opredelitev relacij med funkcijami v modelih FRAM in postavlja temelje za prevedbo modela v računalniški jezik. Dobro definiran nabor povezav omogoča standardizacijo modelov, kar pripomore k večji združljivosti, varnosti in kakovosti modelov FRAM na splošno.

Izhodišče za razumevanje pojava funkcijske resonance leži v opisu variabilnosti posameznih funkcij. Kot je navedeno v [1] so tehnološke funkcije sorazmerno stabilne, medtem ko pri človeških in organizacijskih funkcijah prihaja do variacij delovanja. Klasifikacija MEDI ponuja nekaj razlikovanja glede na vrsto funkcije, na primer: Opazka je vedno izhod človeške funkcije in Opozorilo vedno tehnološke. V izbranih modelih za razvoj tega protokola se je variabilnost izhodov večinoma prenašala po informacijskih povezavah kot so Časovno okno, Opazka, Sprememba, Pogoj in Navodilo. Klasifikacija MEDI v trenutni obliki pomaga hitreje zaznati možne vire variabilnosti, če predpostavimo, da so prej omenjeni tipi povezav bolj dovzetni za prenašanje variabilnosti.

Proces izgradnje modela FRAM za izbrano aktivnost vključuje prepoznavo funkcij, potrebnih za uspešno dokončanje aktivnosti, in opis možnih povezav med funkcijami. Modeliranje aktivnosti na podlagi metode FRAM z uporabo protokola MEDI ni samo hitrejše in bolj enostavno, temveč tudi zagotavlja, da je model postavljen v skladu z nekaterimi pravili, ki omogočajo avtomatizacijo analize v prihodnosti.

Materija je lahko v računalniku predstavljena s spremenljivko, ki hrani besedilo. Za odkrivanje variabilnosti je pogosto pomembno tudi stanje Materije, zato je smiselno priključiti tudi spremenljivko, ki opisuje njeno stanje. Energija je že po definiciji kvantitativna in tako kot Data ne predstavlja problema pri shranjevanju v obstoječe računalniške podatkovne tipe. Večji izziv predstavlja shranjevanje Informacije. Če jo želimo predstaviti današnjim računalniškim sistemom, moramo poiskati način, kako jo razgraditi na računalniku poznane podatkovne tipe. Nekatere izmed podkategorij lahko hitro definiramo, na primer: Časovno okno je sestavljeno iz dveh spremenljivk, ki hranijo datum in čas (angl. *datetime*), in Pogoj je množica pogojnih stavkov. Navodilo je največkrat sestavljeno iz množice številskih in opisnih podatkov. Opazka in Opozorilo predstavljata dogodek ali rezultat dogodka, opažena s strani človeka ali tehnične naprave. V računalniškem jeziku bi to pomenilo spremenljivko, ki hrani besedilo (podobno kot pri Materiji) in dodatno množico vrednosti, ki natančneje opisujejo dogodek ali rezultat dogodka. Princip Prekinitve izhaja iz digitalnega računalništva, a ker predstavlja poljubni dogodek, ki je prekinil delovanje opazovane funkcije, je z vidika predstavitve računalniku podoben Opazki ali Opozorilu.

Prenos metodologije FRAM v računalniško obliko in s tem algoritmična izvedba analize bi predstavljala veliko izboljšavo v učinkovitosti in nenazadnje tudi natančnosti odkrivanja funkcijske resonance v socio-tehničnih sistemih.

1 Introduction

Trying to find an explanation is a natural reaction after something unexpected happens. It can serve various purposes, such as diminishing uncertainty, assigning responsibility (or blame) or taking action to prevent something from going wrong in the future. It is reasonable to think of events that are part of the same situation as if they progress step-by-step, where one event follows another. For example, when we press the computer power button, the computer will turn on. The same way goes backwards, meaning that when something happens (an effect), we believe something has happened shortly before (a cause). Such thinking can be found at the very roots of Western culture. Leucippus of Miletus is supposed to have said that “nothing happens in vain, but everything from reason and necessity” in 5th century BCE. This is called linear thinking and it implies there is a cause-effect relationship between two consecutive events. [1]

From the late 1700s to mid-1900s accident analyses looked for causes in the world of technology such as failures of technical components. It was not before the mid-1900s it was realised that technology involves human too. The acceptance of a human posing a risk in a human-machine system or a socio-technical system intensified in 1979 after the accident at the Three Mile Island nuclear power plant. [2]

During the 1990s the simple explanation in terms of "human error" was not enough anymore. Several human reliability assessment methods were developed. It was realised that different situation factors and work conditions affect human activities both in a positive or negative way. Humans always adjust their work approximately to match the working conditions. Those adjustments or performance variability may lead to a functional resonance, a phenomenon having positive or negative consequences. A method that builds on that concept is FRAM[1]. [1, 2]

1.1 Motivation

Nowadays, FRAM is a widely used methodology to describe the interactions and couplings among functions of a complex socio-technical system. It has been used to model risks or investigate accidents in many fields such as:

- *Healthcare*: an early detection of sepsis [3], a neuro-surgery [4], blood sampling [5];
- *Air traffic management*: ATM[2] system [6], MSAW[3] [7];
- *Sea traffic management*: VTS[4] system [8], maritime mooring at quay [9];
- *Construction*: multifunctional flood defences [10], recycling construction waste [11], a sinter plant [12].

The basic idea of FRAM is to identify performance variability that may cause functional resonance in order to amplify positive outcomes and damp negative ones. This is accomplished by describing essential system functions and characterising each function using six basic aspects. The functional resonance is then defined based on couplings among aspects. [1]

According to the current literature on FRAM [1, 2], interaction among functions is based on the transfer of *Matter*, *Energy* or *Information* (MEI). This classification is too imprecise to allow an analytical view on the complex structure of relations in observed socio-technical systems which in turn hinders the development of a method automatisation.

[1] Functional Resonance Analysis Method.

[2] Air Traffic Management.

[3] Minimum Safe Altitude Warning.

[4] Vessel Traffic Service.

1.2 Scientific contributions

In this work we take a first step to a more accurate classification of inter-functional couplings that will contribute to FRAM in the following ways:

- The construction of a FRAM model will be faster and easier if given options of possible inter-functional couplings in advance.
- The classification scheme will provide standardisation among models, and thus maximise compatibility, interoperability, safety and quality of FRAM models in general.
- Proposed classification will represent one of the necessary steps to the method automatisation. Currently, the characterisation of variability and identification of functional resonance in a FRAM model is found manually by a team of analysts. Computerised FRAM analysis would not only save time but also be resistant to human error since the number of functions in observed socio-technical systems quickly becomes extremely large and difficult to analyse.

1.3 Methodology

Our approach to the identification of inter-functional protocol comprised the following steps:

- *Selection of FRAM models*: To analyse inter-functional relations several publications of FRAM models from different fields were selected.
- *Reconstruction of FRAM models*: After initial review of selected FRAM models it was evident they were not expressed in ways a computer could understand. Hence, we reconstructed them using the principles of computational thinking such as abstraction and logical organisation of data (functions and couplings).
- *Identification of a protocol*: Reconstructed models served as a basis for development of a classification scheme. In this step couplings and their roles in a model were examined and generalised.
- *Evaluation of a protocol*: To assess the protocol, couplings of other (yet unseen) FRAM models were classified using a proposed scheme.

1.4 Thesis overview

This work is divided into five chapters: Chapter 2 provides the background of the research and overview of existing related work. Chapter 3 describes the general characteristics of FRAM and presents an example of a FRAM analysis. In Chapter 4 we focus on the identification of inter-functional protocol, describing our work and results. In Chapter 5 conclusions are drawn.

2 Background

In this Chapter we provide the background of the study presented in this thesis. In Sections 2.1 and 2.2 we start with a review of the development of risk analysis, safety assessment methods and socio-technical systems examined in [13]. Afterwards, Section 2.3 describes resilience engineering and in Section 2.4 related safety assessment methods are reviewed.

2.1 The development of risk analysis and safety assessment

The management of safety, health and environment has been considered since the beginnings of civilisation. The Code of Hammurabi ordered a punishment of the mason if the house he built fell down and killed the owner. The punishment is extreme but the principle of a company being liable to produce safe products and services is modern. The management of safety was regulated by the government, however, it was practical rather than scientific. [14]

As Hale and Hovden discussed in [14] there are three ages in the scientific study of safety: the age of technology, the age of human factors and the age of safety management.

In the first age many technical measures were developed to guard machinery, prevent structures from collapsing and stop explosions. It began with the Industrial Revolution from about 1760 and ended after the Second World War. Accident investigators were only interested in accidents with technical causes, because others could not be reasonably prevented and therefore out of the scope of then specified safety management [15]. Despite some important examples of safety concerns such as the Railroad Safety Appliance Act from 1893 and Heinrich's book on Industrial accident prevention from 1931 [16], the need for reliable equipment and thus the need for reliability analysis emerged only towards the end of Second World War. This was due to two reasons. First, the military equipment faced many problems of maintenance and failures. Second, the emergence of new technological components such as digital computers, transistors and integrated circuits required more caution since they were part of larger and more complex technical systems, for example, military missile defence system and space programme. The complexity also grew in the fields of communication and transportation. Methods such as FTA[1] [17], FMEA[2] [18], HAZOP[3] [19] were developed to analyse possible causes of accidents and to identify risks. By the early 1950s a new engineering field, reliability engineering, was formed. Reliability theory was merged with probability theory and this combination became known as probabilistic risk assessment, later also named probabilistic safety assessment. The pioneering work of Rasmussen and the WASH-1400 report represented a successful application of such assessment to the field of nuclear power generation in 1975. It has since then become the standard approach in the safety assessment of modern nuclear power plants. [13]

The second age came suddenly after the accident at the Three Mile Island nuclear power plant in 1979. An electrical or a mechanical failure caused a series of events resulting in a partial meltdown of the one of two reactors. Established methods such as FTA, FMEA and HAZOP proved to be insufficient to ensure safety of nuclear stations. They did not consider the human factor that played a key role in the accident. Although research of human factors had already been done in the mid 1940s, it had only focused on the efficiency of systems design and not on the safety issues at all. Thus, new methods had to be developed. Probabilistic risk assessment felt as a natural starting point and so it led to the development of human reliability assessment, that at first considered human

[1] Fault Trees Analysis.

[2] Failure Mode and Effects Analysis.

[3] Hazard and Operability Study.

errors in the same way as failures of technical components. Later more specialised approaches followed but there has never been any fully standardised method or a reasonable agreement among the results produced by different methods. [13]

The third age was introduced by accidents such as Challenger and Chernobyl, both from year 1986 and in hindsight also Tenerife in 1977. Established approaches had their limits and it was clear that organisation had to be considered along the human factor [20]. Introduction of organisational factors was however less straightforward than human factors. Initial researchers hoped the organisational factors would bring significant dependence among probabilistic safety assessment parameters [21]. However, another approach was required. The school of high reliability organisations emphasised the importance to understand organisational processes necessary to safely operate technologically complex organisations [22]. On the other hand, Pidgeon [23] discussed that organisational safety and learning are under influence of organisational culture. In addition to that, safety is limited by political processes as much as from technology and human factors. [13]

A similar view on the development of safety to Hale and Hovden was shared by Hudson, who suggested that safety has evolved through three waves - technical, systems and culture wave [24]. Both of these views imply the process of development has been sequential. In contrast, Glendon et al. [25] proposed a different view, that each phase of development builds on findings of previous phases. If the fourth age of safety was to be predicted, he would refer to it as the integration age, where previous knowledge is helpful as new and more complex perspectives evolve. [26]

Borys et al. [26] proposed that we are moving into the fifth age of safety, the adaptive age. It is an age that deals with adaptive cultures and resilience engineering. Resilience is the ability of a system to recognise the dangerous variability as a potential threat to system malfunctioning and to generate appropriate responses before the accident occurs [27]. The human variability is not anymore seen as a threat, but rather an asset to proper functioning of modern technological systems [1]. Learning from successful performance variability is as important as learning from failure [1]. These concepts are all adopted in FRAM. Additional information about resilience engineering is provided in Section 2.3.

2.2 Socio-technical systems

The socio-technical concept was created in the British coal mining industry by the Tavistock Institute in 1949 on the grounds that mine productivity failed to increase in step with increases in mechanisation while high labor turnover and absenteeism averaged 20%. The Institute had two action research projects in relation to postwar reconstruction of industry. One was about innovative work practices and organisational arrangements that looked promising for raising productivity without major capital investment. The other focused on group relations in a single organisation - an engineering company in the private sector. The latter project was the first project to bring the application of socio-clinical ideas regarding groups in an industrial setting into focus. However, the project approached the organisation exclusively as a social system. [28]

Some of the fundamental concepts of socio-technical theory were discussed in a seminal paper by Trist and Bamforth in 1951 [29]. The case study was based on the observation that in the coal industry productivity was falling despite improved technology and the absenteeism was increasing despite higher pay and better amenities. The underlying cause was hypothesised to be the appearance of innovations in production technology. Consequently the bureaucratic form of organisation was created in which the technology represented a retrograde step in organisational design terms. [29]

Instead of creating separate approaches to social and technical systems, Trist imagined work organisations as socio-technical systems rather than simply as social systems. Some of the principles involved were [28]:

- The work system became the basic unit rather than single jobs that it consisted of.
- Accordingly, the work group became essential rather than individual job holder.
- The internal organisation of the system by the group was thus enabled and there was no more need for external regulation of individuals by supervisors.
- The individual was now seen as a complement to the machine rather than as an extension of it [30].

The conditions for successful organisational performance - as well as unsuccessful one - are therefore created by the interaction between social and technical factors including both linear (cause and effect) and non-linear relationships. Two important consequences of such interactions arise. First, the optimisation of system performance can be achieved only by the optimisation of both social and technical aspect. The optimisation of only one aspect would result in unpredictable relationships that may worsen system performance. Second, the safety of socio-technical system cannot be achieved only by considering the system components and their failure probabilities since the “social” factor also has to be taken into account. [13]

2.3 Towards the Resilience Engineering

First safety analysis methods were developed in the late 1950s for large-scale technological systems. Even though the underlying assumptions that were used for their development are not stated explicitly, one can easily recognise them by studying established methods such as FMEA, HAZOP and FTA. [1]

Those assumptions are [1]:

1. the system can be decomposed into meaningful parts or components that either work or fail so the probability of failure can be analysed;
2. events that are part of the same situation are developed in a linear progression, where one event follows another;
3. the order of events is fixed as the chosen representation describes it, that is, if a different order of events needs to be analysed, a new representation is necessary, for example, a new fault tree.

The first assumption was reasonable when technological systems were relatively easy to understand, fully described and their functioning principles were completely known. Today we are dealing with the opposite. There are large socio-technical systems in our daily lives (health care system, transport, communication) that are difficult to fully understand. They are incompletely described and their functioning principles are only partially known. These two types of systems are called tractable and intractable, respectively, and the main differences between them are summarised in Table 2.1. Traditional risk and safety assessment methods are no longer suitable since they require a clear description or specification of a system and therefore indirectly require that systems are tractable. [1, 2]

	Tractable system	**Intractable system**
Description	Simple description with minimal details.	Thorough description with many details.
Functioning principles	Completely known. Processes are homogeneous and regular.	Only partially known. Processes are heterogeneous and possibly irregular.
Stability	High. The system does not change while being described. Possible to predict most situations.	Low. The system changes before a description is completed. Impossible to predict all situations.
Relation to other systems	The system can operate independently.	The system is interdependent and cannot operate independently.

Table 2.1: Tractable and intractable systems [1, 2].

The second and third assumptions are part of the linear thinking in a way that events can be represented as sequences of causes and effects. This is typical of traditional methods developed in 1970s or earlier. Nowadays with the increasing intractability of socio-technical systems, accidents and unwanted outcomes can occur also due to performance variability or other transient phenomena. The relationship between events is non-linear so the outcome of the event cannot be predicted from the preceding event but is rather a result of coincidences. Generally such events are called emergent. As pointed before, socio-technical systems are intractable and the traditional methods are therefore not suitable. It is also not possible to reduce complexity and simplify system description to such a degree that it become tractable. Thus, a new approach is needed. Resilience engineering represents a possible way to manage the safety of such systems. [1, 13]

The definition of resilience has changed over the years to extend the scope of resilience performance. The most recent definition documented in a book from the year 2013 [31] is:

> *The intrinsic ability of a system to adjust its functioning prior to, during, or*

> *following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions.*

The emphasis is on the ability to perform under a variety of conditions and to respond appropriately to both disturbances and opportunities. Performance conditions of socio-technical systems are always insufficiently specified thus individuals and organisations dealing with such systems must always adjust their work to the current conditions. Due to finite resources and time, those adjustments are approximate, consequently introducing performance variability that can have negative as well as positive impacts. [32]

The more specific definition of resilience can be put together by considering characteristics of resilient performance independent of any specific domain. Resilience engineering has introduced the following four qualities [33]:

- the ability to *respond* to regular and irregular disturbances, opportunities and changes by adjusting current state of processing;
- the ability to *monitor* or regularly check anything that could affect system performance;
- the ability to *learn* from experience by collecting and analysing data from negative as well as positive outcomes;
- the ability to *anticipate* possible disruptions, opportunities or constraints in the longer term.

The four qualities are clearly dependent on each other (see Figure 2.1), for example, the ability to respond requires the ability to monitor. All four qualities depend on the model the organisation is using. The model accurately represents the nature of all the processes that are happening in and around the organisation, specifically the cause-effect relations, and is of great importance for risk analysis and safety assessment. [33]

2.4 Related safety assessment methods

During the buildup of many complex system accidents, there were no critical failures of technical components, human performance error or root cause as required by traditional accident models. Instead, accidents were result of performance variability introducing functional resonance and unexpected links among system processes. [6]

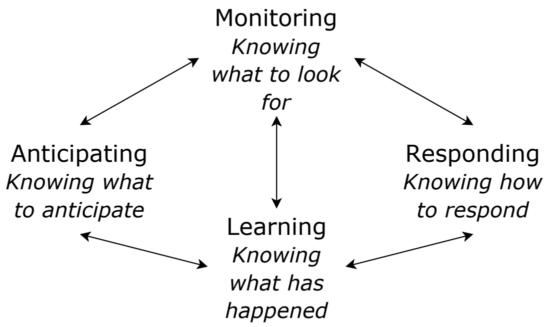
Monitoring
Knowing what to look for
Anticipating
Knowing what to anticipate
Responding
Knowing how to respond
Learning
Knowing what has happened

Figure 2.1: The four qualities of resilience. Adapted from [34].

For this reason new models have been developed over the last years such as STAMP[4] [35] and AcciMap [36].

STAMP is an accident causation model that explains accidents as a result of inadequate control or enforcement of safety-related constraints rather than as a result of component failures. Systems are viewed as dynamic processes that are continually adapting to achieve their purposes and to react to changes in themselves and the environment. The constraints define relationships between system variables or components and in turn establish safe system state. From that view STAMP reformulates the safety as an emergent property of the system that is achieved when constraints are met. [35]

STAMP treats systems as hierarchical levels of controls, where each level enforces constraints on the level below. On the contrary, the information about the adequacy and condition of controls and constraints at the lower levels travels up to the upper levels of the hierarchy. In accident analysis it provides a description of the system's control structure and then determines failures in this structure that led to the accident. The control failures can be divided into categories: inadequate enforcement of constraints (control actions), inadequate execution of control actions and inadequate or missing feedback. [37]

AcciMap is a method used to represent results of one particular accident analysis aimed to design an improved system. For its development is therefore important to identify all factors that have contributed to the accident and at the same time can be improved to prevent future accidents. Then, AcciMap typically maps them onto six organisational levels: government policy and budgeting; regulatory bodies and associations; local area government planning and budgeting (including company management); techni-

[4] Systems-Theoretic Accident Model and Processes.

cal and operational management; physical processes and actor activities; and equipment and surroundings. The method usually tries to identify factors starting from the physical sequence of events and working its way up to the causes of governmental, regulatory and societal levels. [36]

3 Functional Resonance Analysis Method (FRAM)

This Chapter first presents the basic principles of FRAM in Section 3.1. Following that, Section 3.2 focuses on the description of functions and aspects used in FRAM modelling. Steps of a FRAM analysis are described in Section 3.3. The Chapter concludes with an example of a FRAM analysis in Section 3.4.

3.1 The basic principles

FRAM is built on the following four basic principles [1, 2]:

1. *The equivalence of successes and failures*: Both positive and negative consequences happen due to same reasons.

2. *The approximate adjustments*: Humans that are part of socio-technical systems always adjust their work to match the conditions.

3. *The emergence*: Many outcomes cannot be explained with a specific cause for they are different from any anticipated or targeted outcomes (emergent outcomes).

4. *The functional resonance*: Any non-linear interactions and outcomes of events that cannot be explained using the simple cause-effect principle (causality) can be explained using the functional resonance.

The equivalence of successes and failures

Failure is typically explained as a malfunctioning of a system or its components. The explanation for the unwanted outcome is based on finding one or more components that have failed, or a step that was not performed correctly. From that point of view, success and failure have completely different nature. This is based on the *hypothesis of different causes*, meaning that the positive and negative outcomes have completely different causes. Nevertheless, the resilience engineering has introduced the new way of thinking that is reflected in the principle of the approximate adjustments that in turn has also became a basis for FRAM. [1, 2]

The approximate adjustments

As described in Section 2.3, the work situation in large-scale socio-technical systems is partly intractable. In order to carry out work, individuals and organisations always adjust their work to the current conditions such as time, information, tools, requirements, opportunities, interruptions and conflicts [1, 2]. Because the resources are mostly limited, these adjustments are approximate. Such performance variability leads to one of the following results [1, 2]:

- *success*, if the approximate adjustment is correct in the sense that individual or organisation managed to correctly anticipate the failure and therefore prevented it;
- *failure*, otherwise.

From that point of view, success and failure have the same origin in contrast with the aforementioned hypothesis of different causes. [1, 2]

The emergence

After every unwanted or unexpected outcome, an explanation needs to be found. In large number of cases the explanation is the malfunction of a system component or an incorrectly performed step. In such cases the outcome is the result of inner functioning of the system and therefore technically called *resultant*. On the other hand, there are cases where the outcome cannot be explained by referring only to malfunctions in specific components. Such cases have the *emergent* outcome, meaning the explanation in terms of causality and decomposition is inappropriate and perhaps even impossible. The causes for emergent outcomes are unstable short-term combinations of states and events. In FRAM, such phenomenon is called the functional resonance. [1, 2]

The functional resonance

It is a known fact that human and organisational work is always adjusted approximately to match the conditions of work, in other words there is always a performance variability. However, there is a regularity in how people respond to unexpected situations. People react to what others do and what they expect others will do, so their approximate adjustments are based both on response and anticipation. The performance variability of each individual is thus not random but dependent on other individuals resulting in *mutual approximate adjustments*. In other way of saying, the functions in a system become linked, meaning the variability of multiple functions coincide and mutually affect each other in unexpected ways. The phenomenon called functional resonance occurs. This way of explaining consequences is technically called *non-linear* and is typically suitable for the systems that are in part or in whole intractable. [1, 2]

3.2 Functions and aspects

The purpose of FRAM is to provide a systematic description of everyday activity. It is important to provide a description of work that is actually carried out (*work-as-done*) since FRAM is about what actually happens rather than what is assumed to happen (*work-as-imagined*). This description is called a FRAM model. The selected activity is represented with the functions that are necessary to carry out the activity, the potential couplings between the functions and the typical variability of the functions. [2]

A FRAM function represents the activity or a set of activities that are needed to achieve a goal. It can refer to: what people - individual or a group - have to do in order to produce a certain result; what an organisation does, or what a technological system does either by itself or in a cooperation with one or more humans. [2]

Each FRAM function can be characterised by the following six aspects [1, 2]:

- *Input*: The Input can represent matter, energy or information; an example of the latter would be a clearance or an instruction to begin doing something. In other words, it denotes a state change that is recognised by a function as a signal to start. The role of the Input as a signal proposes a way how variability of functions can occur: The signal may not be detected due to too high or too low detection threshold; The Input may be misinterpreted or mistaken for something else.

- *Output*: The Output describes the result of processing the Input. The Output can thus be a matter, an energy or an information - the latter being a permission or clearance or the outcome of a decision. The important thing to consider is the variability of the function. If the function varies, then it is possible that the Output will also vary and will in turn lead to variability in the other functions as it is the Input of other functions. However, it is also possible that the function will be able to damp the variability of the Input so the Output will remain unaffected.
- *Precondition*: A Precondition is a system state that must be true or conditions that must be verified before a function is carried out.
- *Resource (or Execution Condition)*: A Resource is something that is consumed or needed while a function is being carried out. A Resource is consumed by an active function, for example, matter and energy. An Execution Condition is not consumed but it must be present while a function is active, for example, information, tools, technology, competence and manpower.
- *Control*: This aspect represents something that controls a function so it produces the correct Output, for example, instructions, guidelines, an algorithm or a plan.
- *Time*: Time, or rather temporal relations, affect how a function is carried out. Time can be viewed as: Control, when it represents the sequencing conditions; Resource, when something must be done before certain deadline or within a certain duration; or Precondition, when a function must not begin before a certain time of the day or another function.

Generally, it is not necessary to describe all six aspects of every function, but only those that are seen appropriate by the analysis team. Describing every aspect of every function may be impossible or can easily result in reduced model clarity. [1]

A FRAM function can be represented graphically by a hexagon with one aspect in each corner as in Figure 3.1. This is useful for communication or to gain quick insight into the activity being analysed. However, the functions and all the couplings can easily become unwieldy, so a FRAM analysis should be based on textual descriptions, like the one in Table 3.1. [1]

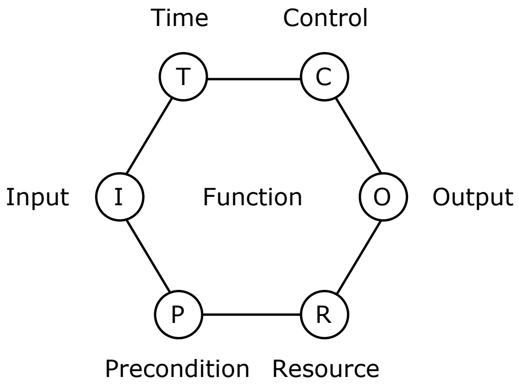

Figure 3.1: A FRAM function with six aspects adapted from [1].

Function name	
Aspect	**Aspect description**
Input	Something that is used or transformed by the function to produce the Output.
Output	The result of processing the Input.
Precondition	Conditions that must be verified before a function can start.
Resource	Something that is needed or consumed while a function is being carried out.
Control	Something that regulates a function so it produces the desired Output.
Time	Temporal relations that affect how a function is carried out.

Table 3.1: A FRAM function form. Aspect descriptions are based on [1, 2].

3.3 Method steps

A FRAM analysis is currently carried out in the following steps [1]:

1. *Determining the purpose of the analysis:* In the first step it should be evident whether the analysis refers to the investigation of a past event or a risk assessment of something that may happen in future as the method is slightly different for each of the two.

2. *Identifying functions:* The goal of the second step is to describe functions that are necessary to carry out chosen everyday activity based on six functional aspects. Furthermore, internal and external factors for potential variability of the function must be added to the description.

3. *Characterising the variability of functions:* In this step variability of each function is determined.

4. *Characterising potential functional resonance:* The purpose of this step is to identify the functional resonance that may appear as a result of couplings among functions.

5. *Proposing ways to manage the variability:* Possible performance variability that has been found in the previous steps is managed by monitoring or dampening its effects.

3.3.1 Determining analysis purpose

In FRAM based event investigation analysis the event data may help to identify functions and their variability, but on the other side it may also represent a cognitive barrier of thinking all possibilities. The last step of analysis should also focus on managing variability and not only preventing this specific event from happening again. [1]

If FRAM is used for risk assessment, descriptions of identified functions determine the analysis scope. The variability of functions and functional resonance are identified by looking at possible scenarios. The last step is the same as in an event based investigation analysis. [1]

3.3.2 Identifying functions

The selected everyday activity is described in terms of the functions and aspects as presented in Section 3.2. In addition to describing aspects, each function must also include a list of potential internal and external factors of variability in order to determine the reason of the Output variability as presented in the following Subsection.

3.3.3 Identifying function variability

The starting point for understanding unexpected outcomes is to identify the variability in a FRAM model, namely variabilities of Outputs and in case the Output varies, also the variability of the function [1].

Generally the Output varies due to one of the following reasons [1, 2]:

- The function itself varies because of its nature. This can be considered as internal or endogenous variability.
- The work conditions or environment varies. This can be considered as external or exogenous variability.
- The Output from the upstream[1] function varies. This kind of variability is a result of a functional upstream-downstream coupling and forms the basis of functional resonance.

FRAM distinguishes among three common types of functions: technological, human and organisational [1].

Technological functions are carried out by various types of machinery. Although a FRAM analysis assumes they do not vary significantly as they are designed to be reliable, this is not always the case. In terms of internal variability we can talk about intractability and component malfunction due to working conditions or wear and tear. There are also several external variability factors such as improper maintenance or operating conditions, misuse and overloading. [1, 2]

Human functions are performed by humans, either individuals or small groups. The default assumption of FRAM is that human functions vary with high frequency and large amplitude. High frequency indicates that the performance can change very quickly and large amplitude signifies large differences in performance. Variations appear due to

[1] Upstream function is a function that happens before the observed function.

internal factors, such as stress, well-being, personality traits, problem-solving style, cognitive style, judgement and decision heuristics, or external factors, such as peer pressure, expectations, requirements and political considerations. [1, 2]

Organisational functions are carried out by large groups of people and even though they consist of people, they differ from human functions and are therefore described on an organisational level. A FRAM analysis assumes they have low frequency and large amplitude. Performance can vary due to several internal reasons such as bad communication, distrust and inflexible culture, or external factors such as customer requirements or expectations, the legal regulations, the availability of resources and commercial pressures. [1, 2]

In short, technological functions are relatively stable, while human and organisational functions may vary. A FRAM analysis therefore focuses on the variability of human and organisational functions.

3.3.4 Identifying performance variability

After the variability of the Output has been characterised it is time to look at how it may affect downstream[2] functions. Currently there are two possible solutions to describe the consequences of performance variability, complemented by ETTO[3] rule [38]:

- an efficient solution lacking thoroughness,
- a thorough solution lacking efficiency.

The efficient solution

The efficient solution suggests that the Output of a function can vary in terms of timing and precision. In terms of timing, the Output may appear too early, on time, too late or not at all. In terms of precision, the Output may be precise, acceptable or imprecise. [1]

The degree of variability is different for each function type (human, technological or organisational) and is described in detail in [1].

The thorough solution

The thorough solution is based on failure modes that are included in many safety models. Failure modes, also called phenotypes, are categories in which the wrong action can

[2] Downstream function is a function that happens after the observed function.

[3] Efficiency-Thoroughness Trade-Off.

appear: speed, distance, sequence, object, force, duration, direction and timing. [1]

In FRAM, it is practical to divide the variability into the following subgroups: object, sequence, timing/duration, and force/distance/direction, all presented in detail in [1].

When the variability of a function in a system affects its downstream functions in unexpected ways, a phenomenon called functional resonance occurs. The identification of potential sources of functional resonance is currently performed by a group of analysts relying on the efficient or thorough solution. [1]

3.3.5 Managing performance variability

If the accident is a result of the performance variability, the safety experts and managers cannot simply eliminate it since variability is also a source of safety and productivity. The right solution is to manage it by monitoring or dampening the resonance effects in line with the four principles of FRAM presented in Section 3.1. [1]

The goal of monitoring is to keep the processes on track. A FRAM model can be used to propose which performance indicators to track by identifying couplings that may lead to an increase in performance variability. [1]

Dampening the resonance effects takes more work as there are no root causes to be addressed. Internal and external variability may be reduced by changing the work conditions, however, this may take time and resources. The variability that appears due to functional upstream-downstream couplings can be dampened by reducing the variability in the Output from upstream functions. [1]

3.4 Example of a FRAM analysis

In this Section we describe a FRAM analysis presented in [39].

The purpose of the analysis

The analysis is a risk assessment of an activity from the aviation domain, namely a set of actions that must be performed by a pilot of a small aircraft in order to take off. The starting point of this activity is a moment when the pilot reaches an entry point in front of the runway. Although the analysis is not an event investigation, it includes descriptions of several aviation accidents that happened due to the functional resonance in this particular model.

Functions and the model

Tkalec [39] identified functions as follows:

- “`Ground check checklist`”: Pilot performs some tests of vital aircraft system components such as the magneto and carburetor heat check.
- “`Before takeoff checklist`”: Still at the same position as during ground check, pilot sets an aircraft into takeoff configuration and then asks ATC[4] for a takeoff clearance.
- “`Receive ATC instructions`”: Pilot receives ATC instructions.
- “`Interpret ATC instructions`”: Pilot interprets ATC instructions.
- “`Readback ATC instructions`”: Pilot repeats the instructions after controller.
- “`ATC check`”: Controller either confirms or corrects pilot’s readback of instructions.
- “`Adapt to ATC instructions`”: If there is any adjustment from the ATC check, the pilot adapts. After this function is carried out, the aircraft is expected to be on the runway facing the direction corresponding to ATC instructions.
- “`Get takeoff clearance`”: Pilot receives a takeoff clearance.
- “`Takeoff`”: Pilot begins a takeoff procedure.

A graphical adaption of the model is shown in Figure 3.2. Since a FRAM model is the description of functions rather than the diagram, couplings are not associated with a specific direction [1]. Even so, to understand the flow of the activity the model describes, reader can imagine that every coupling starts at the Output and points to the destination aspect.

Sources of variability

The original work identified sources of variability summarised in Table 3.2. The variability is described in terms of an efficient solution presented in Subsection 3.3.4.

[4] Air Traffic Control.

Function	**Output**	**Output variability**
Interpret ATC instructions	Interpreted ATC instructions	Imprecise. The pilot may misinterpret the instructions due to various psychological and cognitive factors.
Readback ATC instructions	Repeated ATC instructions	Imprecise. The pilot may misinterpret the instructions and not repeat them but use a phrase "Wilco", which is short for "will comply" or "Roger" which stands for "received". The pilot may also repeat the instructions correctly but later fail to follow them.
ATC check	Adjustment or confirmation	Imprecise. The controller may confirm pilot's incorrectly repeated instructions.
Adapt to ATC instructions	Aircraft in position for takeoff at the runway	Imprecise and too early. The pilot may make a wrong adaptation. The output may be generated before ATC check is done.
Takeoff	Aircraft in the air	Imprecise and too early. The aircraft may face a wrong takeoff direction. The pilot may takeoff before getting a takeoff clearance.

Table 3.2: The variability of the Output for various functions from the example FRAM model in [39].

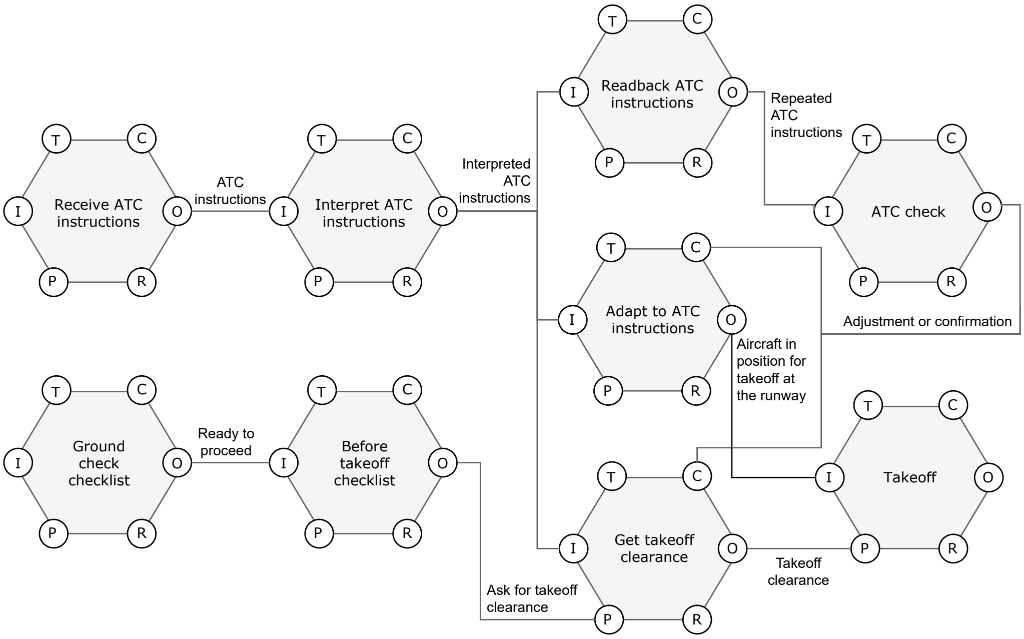
Receive ATC instructions
ATC instructions
Interpret ATC instructions
Interpreted ATC instructions
Readback ATC instructions
Repeated ATC instructions
ATC check
Adjustment or confirmation
Adapt to ATC instructions
Aircraft in position for takeoff at the runway
Ground check checklist
Ready to proceed
Before takeoff checklist
Ask for takeoff clearance
Get takeoff clearance
Takeoff clearance
Takeoff
T
C
I
O
P
R

Figure 3.2: The FRAM model adapted from [39].

The functional resonance

The author found out that a combination of several functions from the model may lead to an unexpected outcome and linked those with several known aviation accidents. The combination includes the following functions: "`Interpret ATC instructions`", "`Readback ATC instructions`", "`ATC check`", "`Adapt to ATC instructions`" and "`Takeoff`".

The functional resonance emerges when the pilot misinterprets the instructions and the mistake remains undetected. The variability of "`Interpret ATC instructions`" propagates via "`Readback ATC instructions`" and "`ATC check`" to "`Adapt to ATC instructions`", resulting in an unexpected outcome such as an attempt to takeoff in a wrong takeoff direction. Following are scenarios leading to a functional resonance that occurs if the pilot misinterprets the instructions [39]:

- The pilot uses a phrase like "Wilco" or "Roger" instead of reading back the instructions. The controller is not able to correct the pilot.
- The pilot incorrectly repeats the instructions and the controller overlooks the mistake.
- A poor communication between the pilot and ATC leads the pilot into thinking

that the readback and ATC check were performed while in reality they were not.

Another potential source of a functional resonance appears when the pilot correctly repeats the instructions but fails to follow them later. The pilot may forget a part of the instructions or think that he is following the correct instructions. [39]

4 Inter-Functional Protocol

In this Chapter we describe development of the inter-functional protocol in Section 4.1. The protocol is presented in Section 4.2 and evaluated in Section 4.3. The protocol contributions are summarised in Section 4.4. We discuss how the new protocol can help in further efforts to automate the method in Section 4.5.

4.1 Protocol development

The protocol was developed by examining five selected FRAM models. Each of the following Subsections presents a selected model, its reconstruction, identified types of couplings and findings.

4.1.1 Model 1: Ward rounds

The first model we take into consideration is described in [40] and represents how ward rounds are normally started and conducted in the Geriatric ward of a specific hospital. The activity is carried out by the physician in charge in a cooperation with nurses at the ward.

Hounsgaard [40] identified functions as follows (see Figure 4.1):

- "`To start ward round`": Ward round starts sometime between 9 a.m. and 12 noon when the physician and nurses are prepared.
- "`To call the physician in charge of the ward round`": Physician in charge is interrupted by a phone call.
- "`To decide date of discharge`": Date of patient's discharge is determined by the physician in charge and nurses.
- "`To ordinate examination/medication`": Patient is referred to further examination or medication.
- "`To treat and care patient`": Patient may receive revised treatment plan.
- "`To discharge patient`": Patient is discharged on decided date.
- "`To schedule staffing`": Physicians and nurses are scheduled for the ward round.
- "`To receive test results from laboratory`": Test results are received.
- "`To prepare - the nurses`": Nurses are prepared to do ward round.
- "`To prepare - the physician`": Physician in charge is prepared to do ward round.
- "`To measure early warning scores`": Patient's vital signs are measured to determine the degree of illness.

The reconstruction

The function "`To do ward round`" starts between 9 a.m. and 12 noon so in this case the Input is specified by time relation. The function can also start because of a change in a system state [1]. From the computer point of view the second case is more acceptable because in reality it is not time that starts the function but (prepared) physician and nurses. Exact time interval in which the function has to be carried out may still be specified using Time aspect. This is considered in our reconstruction (see Figure 4.2), where "`To prepare - the physician and nurses`" represents the Input and specified time interval controls the Time aspect. "`To schedule staffing`" as a Resource is removed since this is a function that has to take place even before the physician and nurses get prepared so it could be moved to "`To prepare - the physician and nurses`"'s upstream functions.

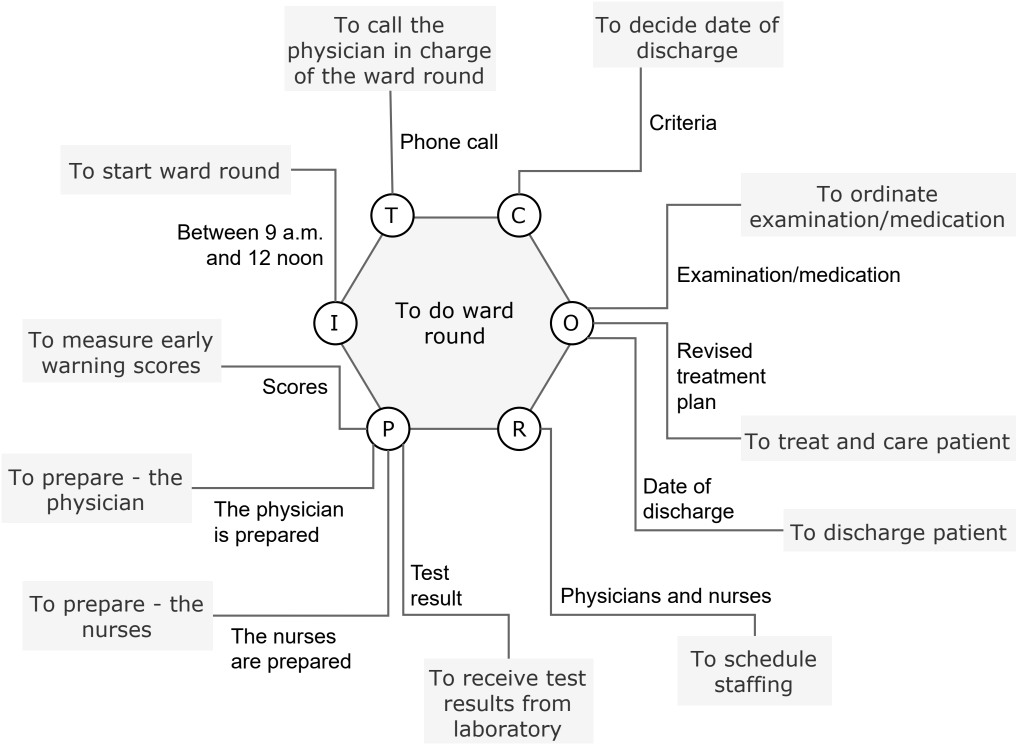
To call the physician in charge of the ward round
To decide date of discharge
Phone call
Criteria
To start ward round
To ordinate examination/medication
Between 9 a.m. and 12 noon
T
C
Examination/medication
To do ward round
I
O
To measure early warning scores
Revised treatment plan
Scores
P
R
To treat and care patient
To prepare - the physician
Date of discharge
The physician is prepared
To discharge patient
Test result
Physicians and nurses
To prepare - the nurses
The nurses are prepared
To schedule staffing
To receive test results from laboratory

Figure 4.1: FRAM model 1 adapted from [40].

The identification of couplings

First, it is worth mentioning that several iterations of examining all five selected FRAM models were needed to obtain the final classification of couplings in this model.

Starting from MEI classification, the model provides an example of Matter in a form of humans, namely physicians and nurses who start the function "`To do ward round`". Energy cannot be found in the model, so according to MEI, all remaining couplings represent Information. Looking closer at couplings "Early warning scores" and "Revised treatment plan" it is clear those are very different in nature. Early warning scores include raw data, for example a body temperature and AVPU[1] score, whereas revised treatment plan is much more complex. At the most basic level it represents a set of instructions

[1] AVPU (an acronym for "Alert, Verbal, Pain, Unresponsive") is a system by which healthcare professionals measure patient's level of consciousness.

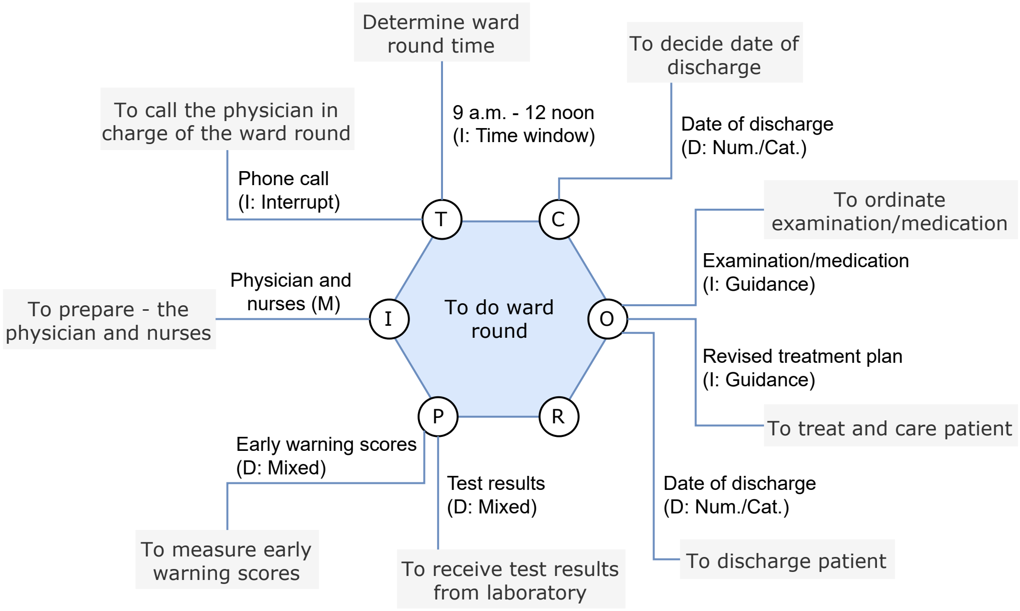
Determine ward round time
To decide date of discharge
To call the physician in charge of the ward round
9 a.m. - 12 noon (I: Time window)
Date of discharge (D: Num./Cat.)
Phone call (I: Interrupt)
T
C
To ordinate examination/medication
Examination/medication (I: Guidance)
Physician and nurses (M)
To prepare - the physician and nurses
I
To do ward round
O
Revised treatment plan (I: Guidance)
P
R
To treat and care patient
Early warning scores (D: Mixed)
Test results (D: Mixed)
Date of discharge (D: Num./Cat.)
To measure early warning scores
To receive test results from laboratory
To discharge patient

Figure 4.2: Reconstructed FRAM model 1 from [40] with identified types of couplings (M: Matter, D: Data, I: Information).

and records relating to the treatment of an illness. The main difference between the two is that revised treatment plan already contains a context, while early warning scores only become useful when the physician and nurses put them into a context. That was the main reasoning behind introducing a new category to MEI, named *Data*.

Data represents a set of values that flow from one function to another and only become useful when put into context. Based on the ability to express the value numerically, the value can either be numerical (quantitative) or categorical (qualitative). Data can thus be further divided into *Numerical* (containing only numerical values), *Categorical* (containing only categorical values) and *Mixed* (containing both types of values). In case the coupling contains only one value it is called *Datum* instead of Data. In our reconstruction, early warning scores and test results are examples of Mixed type. Date of discharge is an example of either Numerical or Categorical data: if we are interested in total days of patient's stay at the ward, then it is Numerical; if we are interested in what day of the week the patient is discharged, then it is Categorical.

We define Information as a complex data structure already put in context. In addition to raw data, Information includes a context that makes data useful. Since FRAM is all about relations between functions, we further divide Information based on the nature of a relation between functions it connects. For example, in the model we are currently describing, the revised treatment plan is a set of instructions or guidelines relating to the treatment of patient's illness. We therefore introduce a new subcategory of Information, named *Guidance*. The same classification can be applied to the "Examination/medication" coupling.

By examining this model we defined two more subcategories of Information, both having a temporal relation. First, a phone call for the physician while he is doing ward round can be seen as *Interrupt*, an event having a temporal impact on doing ward round. And second, time interval in which a ward round must be carried out (9 a.m. to 12 noon), is *Time window*.

Findings

Although this model includes quite a few different types of couplings, the idea for such classification did not arise while examining this model solely, but somewhere between the iterations of the study of all five selected models.

The model contains one Matter coupling and several Data and Information couplings that we were able to further divide into subcategories as shown in Figure 4.3. Data category represents a novelty to existing MEI classification (now called MEDI[2]) and based on properties of the values the coupling contains, it is further divided into Numerical, Categorical or Mixed category. The meaning of Information is reformed to comply with the meaning of Data: if Data contains only raw data with no meaning attached, Information consists of Data and a context. Based on the context or relation between two functions, Information is further divided into Interrupt, Time Window and Guidance.

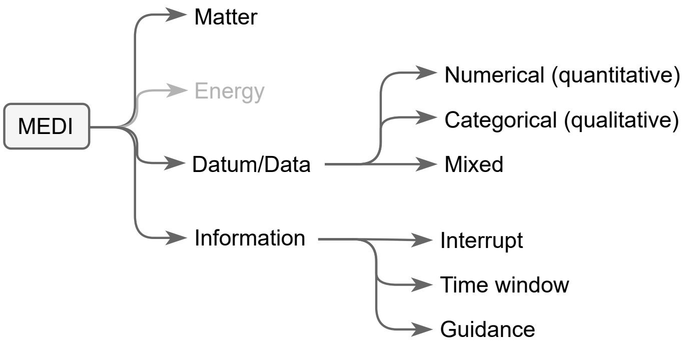

Figure 4.3: Identified types of couplings in FRAM model 1. Energy was not identified in this model but it still written as it is a part of MEI classification we are extending.

[2] Matter, Energy, Data, Information.

4.1.2 Model 2: Fire fighting

The second model is taken from [41] and it describes automatic and manual fire fighting on an offshore platform. Åhman [41] identified the following functions:

- "`Automatically detect fire`": Smoke, heat or flames are detected by fire detectors.
- "`Manually observe fire`": Smoke, heat or flames are detected by a human.
- "`Interpret fire detection`": After fire is automatically detected, start automatic fire fighting system, run firewater pump and activate an alarm.
- "`Fight fire automatically`": Automatic fire fighting systems such as sprinkler and foam system are applied.
- "`Fight fire manually`": Extinguishing agents against the fire using manual fire fighting equipment are applied.
- "`Activate alarm`": Set off audio/visual alarm and send a signal to the control room. It is possible to activate alarm manually.
- "`Start firewater pump`": Automatically start the pump under assumption that it is not running continuously. Possible to start it manually.
- "`Provide extinguishing agent`": Firewater is provided.
- "`Provide emergency power`": Power by emergency generators or other installation is provided.
- "`Communicate`": Communication between personnel and control room provides an overview of the situation.
- "`Supervise from control room`": Operators monitoring the platform from the control room give an overview of the situation.

A graphical adaption of the original model can be seen in Figure 4.4.

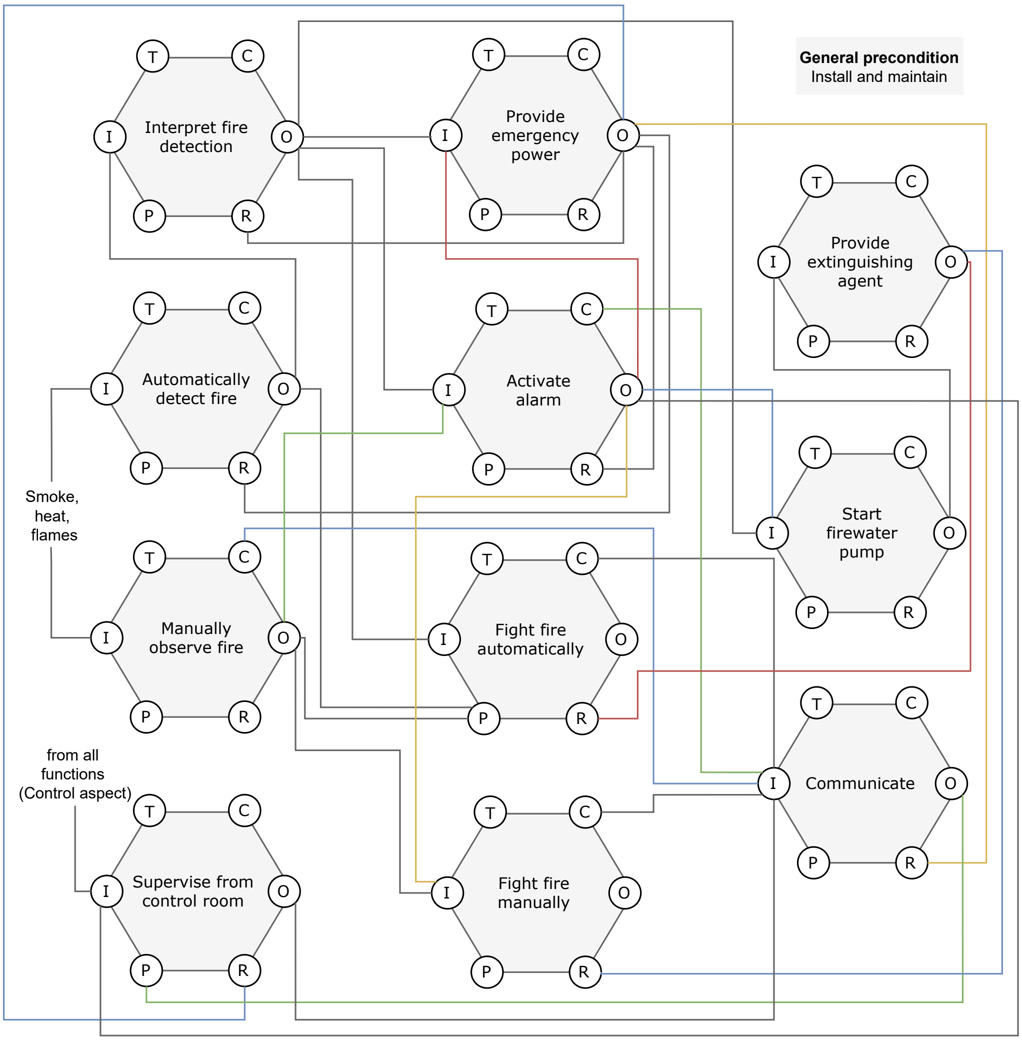

Figure 4.4: FRAM model 2 adapted from [41]. Potential couplings between functions are drawn according to the Table 4.3 from the original work.

The reconstruction

Upon careful examination of the model along with potential couplings, it turned out the model can be simplified preserving its purpose and increasing clarity. For example, "`Interpret fire detection`" is an intermediate step between "`Automatically detect fire`" and its other downstream functions so it can be left out. The same goes for "`Provide extinguishing agent`", whose only task is to provide firewater that already comes as an Output of "`Start firewater pump`".

Since the Control as an input to a function must be the Output from one, or more, other functions [1], this is also corrected in the reconstruction. The Outputs of "`Communicate`" and "`Supervise from control room`" are now linked with the Control aspect of corresponding functions. It may be also reasonable to treat these two functions as background functions since they are same for many situations and connected to all other functions which makes the model quite unwieldy to analyse. Of course this does not mean to cross them out completely of the model, background functions still must be considered during a FRAM analysis. If they represent an important role in, for example, accident analysis, they must be added to the set of foreground functions.

The final reconstruction can be seen in Figure 4.5.

The identification of couplings

In the model we discover two Energy couplings known from existing MEI classification, namely "Smoke, heat, flames" (which is the Output of "`To burn`") and "Electrical power" from "`Provide emergency power`. Matter is also found, namely firewater in the Output of "`Start firewater pump`".

Human observation and alarm detection of fire (Outputs of "`Manually observe fire`" and "`Automatically detect fire`") are put into new subcategories of Information: *Observation* and *Alert*, respectively.

Findings

First, this model contains several Energy couplings and it therefore confirms the need to keep the Energy category also in the new classification (see Figure 4.6). Second, the model brought two new perspectives of Information into focus, namely Observation and Alert. Both represent something that can be seen or detected, the only difference being whether it was perceived by a human or a device.

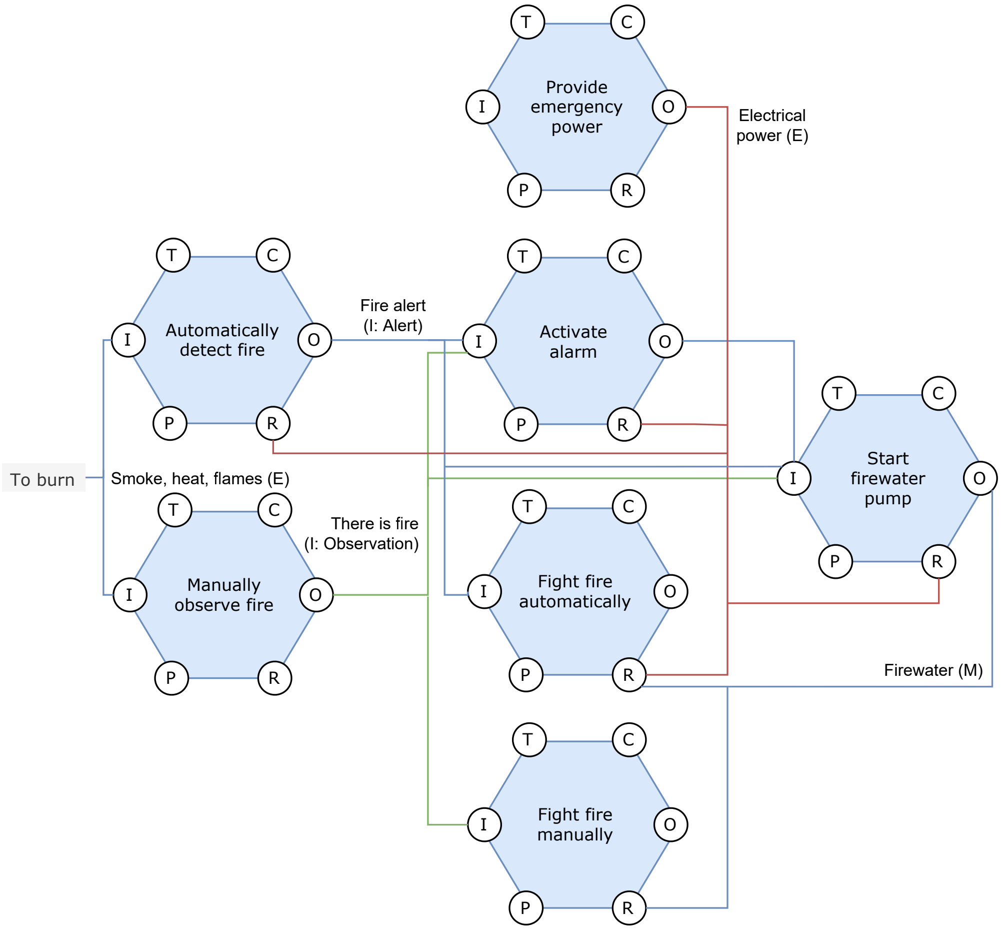

Figure 4.5: Reconstructed FRAM model 2 from [41] with identified types of couplings (M: Matter, E: Energy, I: Information).

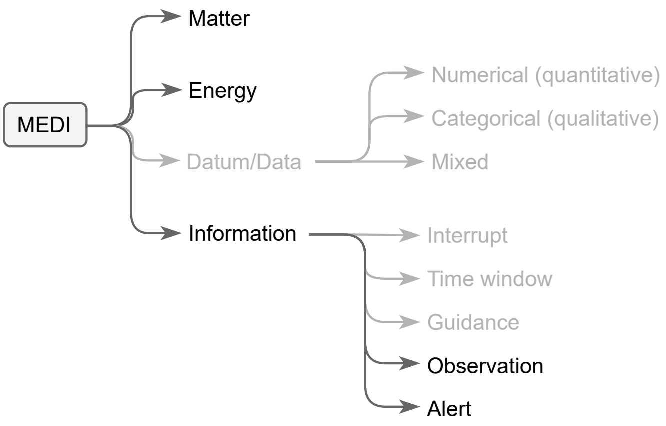

Figure 4.6: Identified types of couplings in FRAM model 2 (written in black) and the remaining classification scheme (written in grey).

4.1.3 Model 3: Multifunctional flood defences

The model presented in [10] describes the use of flood defences in combination with other secondary functions such as transportation, housing, shopping centres. This is achieved by co-locating and connecting two structures: the parking garage and the dike, a man-made earthen structure for flood protection, both covered with sand [10]. Anvarifar et al. [10] investigated two design alternatives with different levels of intended geographical dependency. We selected a model presented as Alternative A2 in the original work. In this case the garage is built right next to the dike so there is a geographical dependency between them. In the scenario specified, there is an extreme event during which the sand cover is washed away and a car crash causes a serious crack of the parking garage.

Figure 4.7 depicts the model comprised of the following functions [10]:

- "`Flood protection`": One of the two core functions of the model is to ensure a protection against flood by a structure that resists high water levels and wave attack during extreme events (also called the dike).
- "`Providing car parks`": The second core function is to provide car parks in a parking garage structure.
- "`Inspection`": Inspection includes regular observations and monitoring of the core functions.
- "`Maintenance`": Maintenance provides the structural integrity of the dike and the parking garage.
- "`Operations`": Human operations are required for the parking service during normal working hours.
- "`Parking the car`": Parking the car in the garage. Its Output, according to the scenario authors specified, is a car crash.

"`Inspection`" and "`Maintenance`" are duplicated in the model, one for each of the two core functions. Identified potential dependencies are [10]:

- The structural integrity of the garage impacts the structural integrity of the dike, e.g. a well-maintained garage has a positive impact on the structural integrity of the dike.

- Car crash represents a threat to the structural integrity of the garage, therefore has a negative impact on the dike as well.

- The inspection of the garage during the extreme event may increase the chance of detecting a dike failure as well, and thus has a positive impact on the flood protection function.

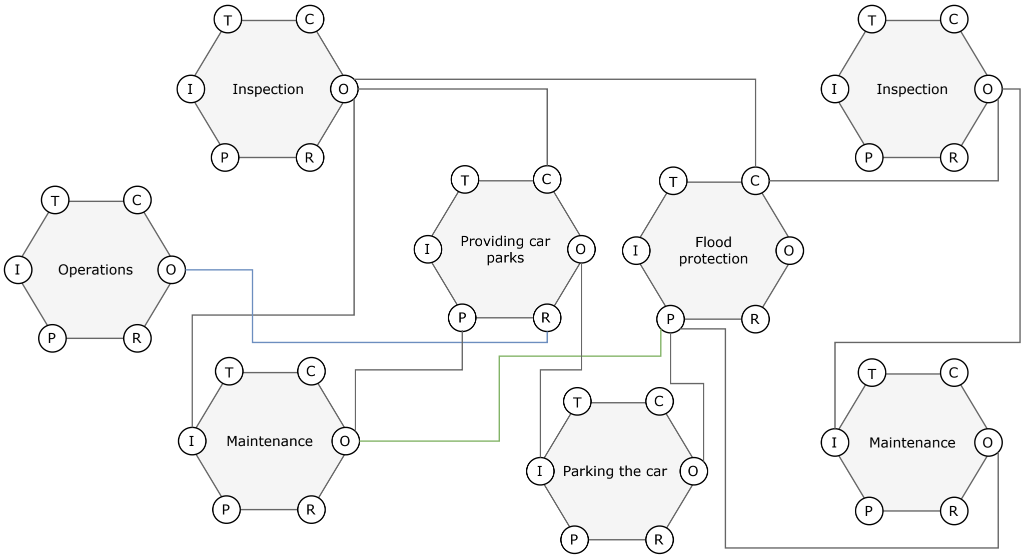

Figure 4.7: FRAM model 3 adapted from [10].

The reconstruction

In this model we are dealing with two core functions: "`Providing car parks`" and "`Flood protection`" enabled by parking garage and dike. In the original model, structural integrities are ensured via "`Maintenance`" whose Output is a Precondition for core functions, i.e. a Precondition for "`Providing car parks`" is the structural integrity of parking garage assured by the "`Maintenance`" function. Strictly speaking, a Precondition is a system state that must be established before a function is carried out [1]. Verifying structural integrities only at the beginning of core functions may bring a serious flaw in the analysis of such model. If, for example, an earthquake knocks down one of the garage walls, the parking garage will still provide car parks until it is closed by personnel (which can be assured via "`Operations`" function). The structural integrity (the result of "Maintenance" function) is actually a property of the parking garage so it is more accurate to link it directly to Resource as can be seen in Figure 4.8. The *condition* of the Resource then in turn affects the performance of "`Providing car parks`" function. This, however, indicates a huge deviation from current FRAM modelling that is based on linking functions, not Resources. Even so, a Resource having defined state may be viewed as a function. The first and foremost task of the parking garage is to ensure a structural integrity by keeping it well-maintained. Only the second task is then providing car parks.

Exposing parking garage and the dike as Resources (or functions) in a reconstructed model works well with all identified potential dependencies. It is more obvious that the state of the garage impacts the state of the dike than in the original model. Although the "`Extreme event`" function is not included in the original model (as it is actually a part of the scenario), it was added to the reconstruction to illustrate and justify the exposure of Resources. Extreme event washes away sand cover from both the parking garage and the dike. It also has a temporal constraint on "`Flood protection`" as the function must be able to provide flood protection for at least as long as the extreme event lasts.

The identification of couplings

Although the "`Inspection`" function is not described in detail in the original source, we will assume it contains general observations and monitoring of the performance of core functions. Some of its possible Outputs would be "There is not any vacant parking lot.", "Someone is trying to break into a car." or "There is a crack in the dike.". What all these cases have in common is that they are all (human) observations. Thus, we introduce a new category to our classification, named *Observation*.

Functions "`Operations`" and "`Maintenance`" are also poorly described and give only a very general idea of their tasks. In both cases, the Output is the result of an action, for example "The parking barrier is raised." in the former case and "A crack in the wall is repaired." in the latter. It would be tedious to analyse the model with such general functions and for this reason we do not provide a classification of such couplings.

Similarly, scenario based functions "`Parking the car`" and "`Extreme weather`" also output a result of some action. They only differ in who or what performed it. The first one is caused by human, and the other one by nature.

The last Information coupling that is different from all others presented so far, is a coupling connecting the parking garage and the dike. It starts at the parking garage and

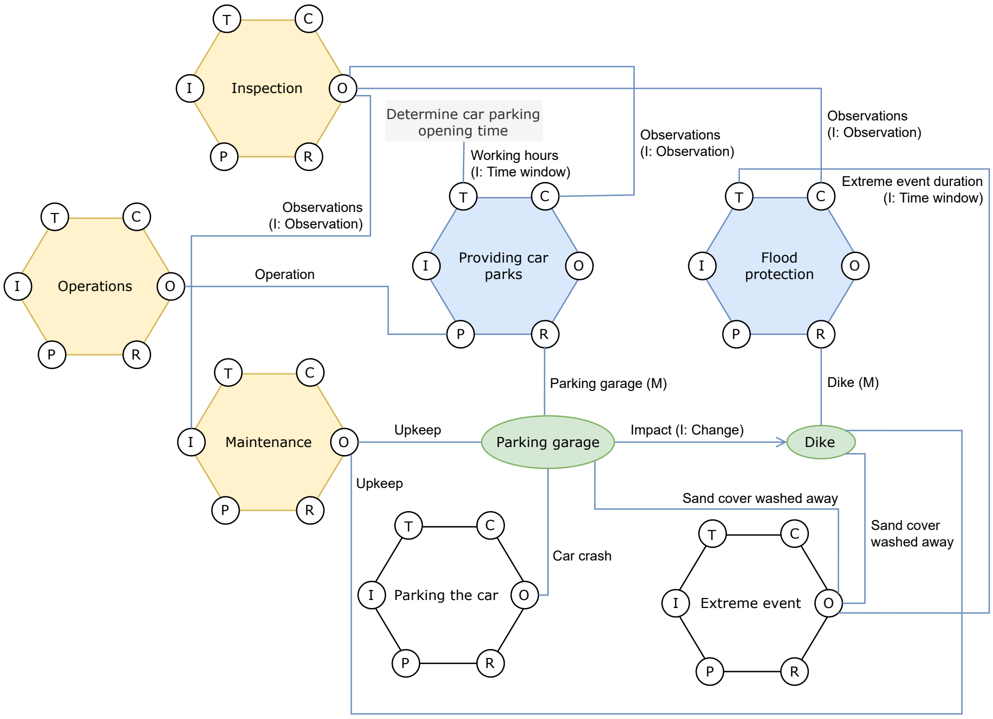

Figure 4.8: Reconstructed FRAM model 3 from [10] with identified types of couplings (M: Matter, I: Information). Hexagons representing the core functions are coloured blue, sub-functions orange and scenario specific functions are black. A green ellipse is not part of the standard FRAM modelling. It represents the Resource of the linked function (via Resource aspect) and it is exposed because it makes more sense to associate some couplings with the state of a resource than the function to which the resource is linked.

points to the dike indicating a dependence. The condition of the parking garage affects the condition of the dike, either in a positive or negative way. We named such relation *Change* since the change in the first structure leads to a change in the second.

Findings

This model provides several more examples of the following couplings: Matter, Time window and Observation. Moreover, a new subcategory of an Information coupling was discovered, namely Change. This relation was discovered after defining the Resources as standalone functions (parking garage and dike) and it means that two functions can be in a dependent relationship.

Identified types of couplings in this model along with previous classifications can be seen in Figure 4.9.

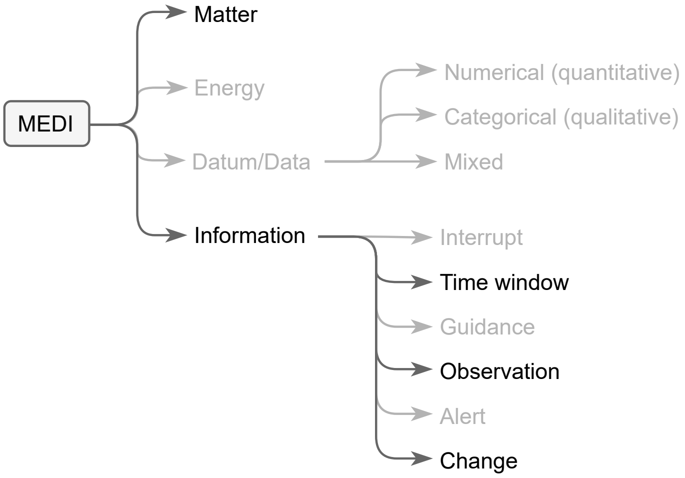

Figure 4.9: Identified types of couplings in FRAM model 3 (written in black) and the remaining classification scheme (written in grey).

4.1.4 Model 4: Recycling construction waste

The model taken from [11] presents a typical sustainable activity that handles the construction waste. It takes the demolished concrete and transforms it into a base construction material using the crusher machine. The activity is divided into the following steps: selection of the waste that will be sent for recycling at the construction site, delivery of sorted waste to the crusher using loaders, crushing the waste in the crusher machine and delivery of the crushed waste (base material) to the endpoint [11].

Rosa et al. [11] identified the following functions (see Figure 4.10):

- "`Material selection`": Material that will be sent for recycling is selected.
- "`Receive material`": Selected material is delivered to the place where it will be crushed.
- "`Initial checklist`": Vital items of equipment are checked before crushing.
- "`Operation under load`": This function is not explicitly described in the original source. We assume it refers to the crushing process in the machine.
- "`Operation without load`": This function is also not explicitly described. Given the couplings we assume it concerns the process between delivery and crushing such as making sure the delivery is correct and everything is ready to begin the crushing.

- "Levelling control": Visual levelling control ensures the consistent feeding of the crusher.
- "Control of the finished product": Control check of the crushed waste is performed at the end.
- "Material delivery": Crushed waste is delivered.

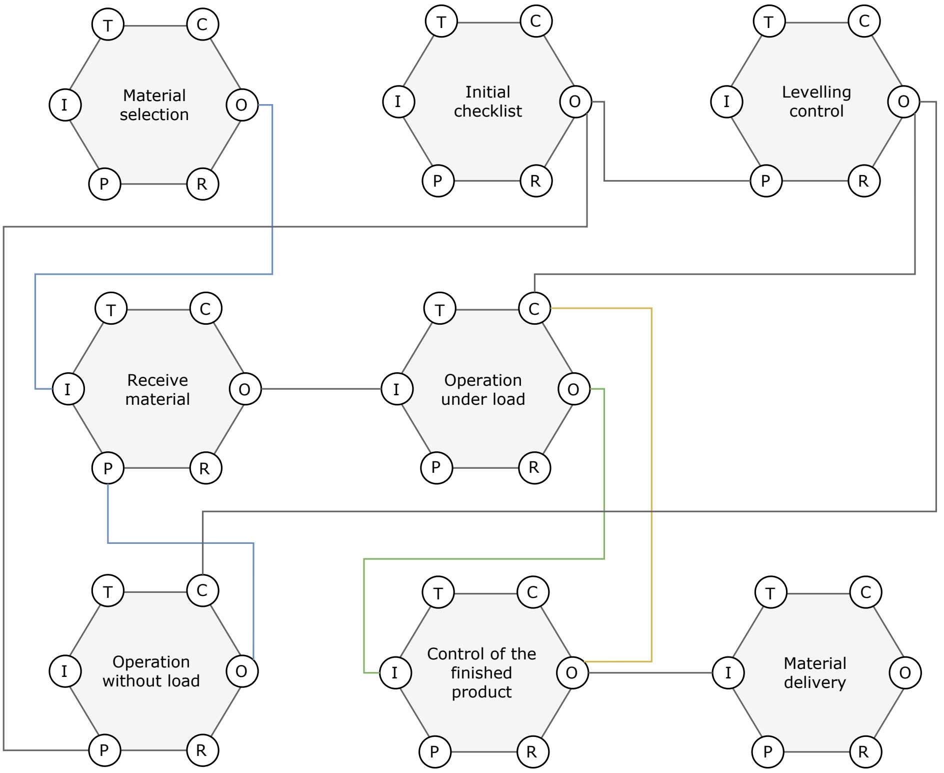

Figure 4.10: FRAM model 4 adapted from [11].

The reconstruction

To clarify the main parts of the activity, functions "Operation without load" and "Operation under load" were replaced by specific function names: "Delivery of sorted waste" and "Crushing the waste", respectively. The function "Receive material" was then left out as it falls under "Delivery of sorted waste".

In the original model, the function "Control of the finished product" is controlling the "Operation under load" at the same time as taking the input from it. Either the function name is misleading or there should not be the Control coupling. As the function name implies, it is an independent task to be performed only after the crushing, so the Control coupling is omitted in the reconstruction (see Figure 4.11). Should we want to include the function that controls the crushing, the function had to be renamed or another one added. To demonstrate a latter case, a new control function "`Crusher settings control`" was added to the reconstruction.

In the last step of the activity, the material is delivered to another place, that is, if all conditions from control of the finished product are satisfied. As this may not always be the case, another coupling has been added, to return to crushing if the finished product does not meet the standards specified.

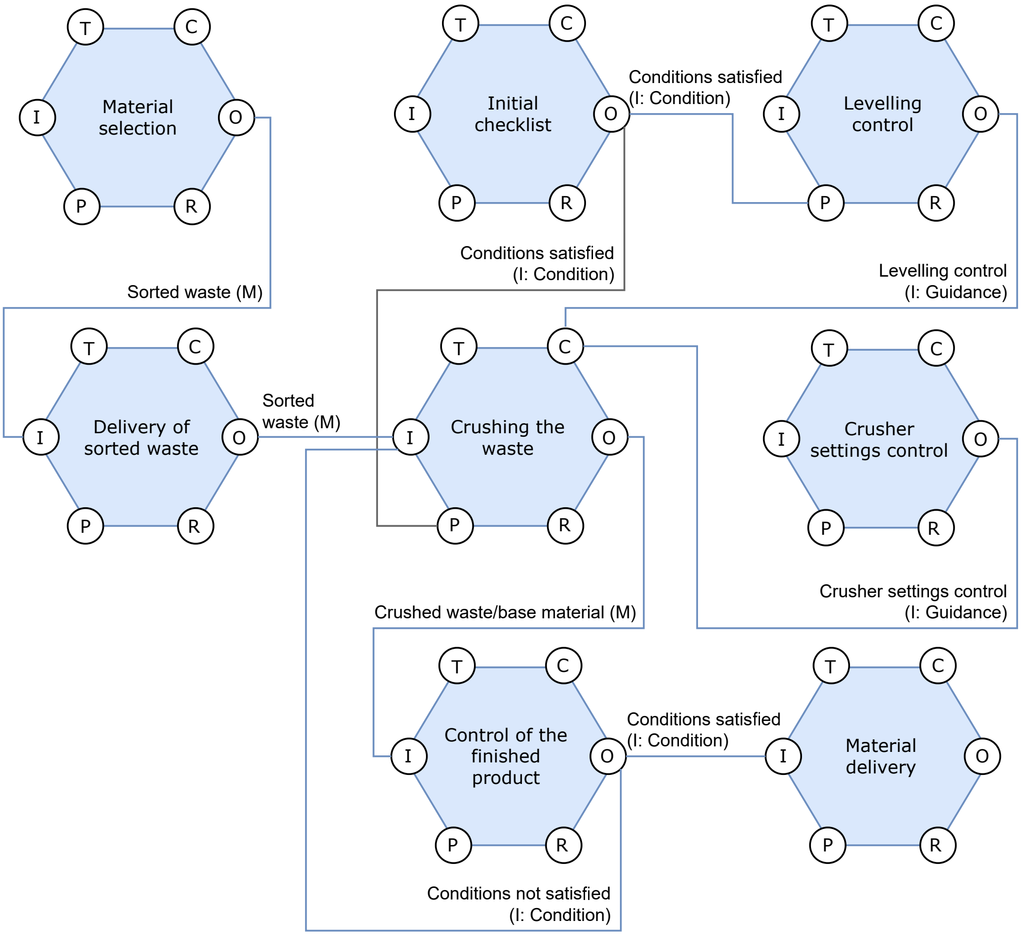
Material selection
Initial checklist
Conditions satisfied (I: Condition)
Levelling control
Conditions satisfied (I: Condition)
Sorted waste (M)
Levelling control (I: Guidance)
Delivery of sorted waste
Sorted waste (M)
Crushing the waste
Crusher settings control
Crushed waste/base material (M)
Crusher settings control (I: Guidance)
Control of the finished product
Conditions satisfied (I: Condition)
Material delivery
Conditions not satisfied (I: Condition)
T
C
I
O
P
R

Figure 4.11: Reconstructed FRAM model 4 from [11] with identified types of couplings (M: Matter, I: Information).

The identification of couplings

Regarding the couplings, the model includes Matter and Information couplings. Matter appears in different states; first sorted waste arrives, then it is crushed and base material (crushed waste) comes out. Other couplings are classified as Information. "`Initial checklist`" and "`Control of the finished product`" both output a set of conditions that need to be checked. We define this new type of coupling as Condition. There are also two typical control functions ("`Levelling control`" and "`Crusher settings control`"), each outputting Guidance.

Findings

This model introduces a new subcategory of an Information coupling, namely Condition. It represents an arrangement that must exist before the next function can happen. This subcategory is added to the existing classification scheme in Figure 4.12.

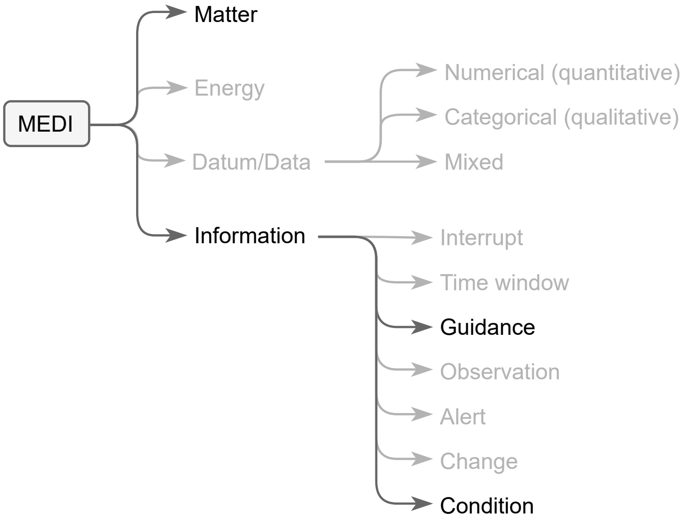

Figure 4.12: Identified types of couplings in FRAM model 4 (written in black) and the remaining classification scheme (written in grey).

4.1.5 Model 5: Air traffic management

The model presented in [7] describes the behaviour of MSAW[3], a component that works jointly with other parts of the ATM system. It periodically processes surveillance and flight data for estimation of flight safety. It warns the controller about increased risk of flight into obstacle or terrain by generating an alert of aircraft proximity. The controller then warns the pilot. Furthermore, data is recorded for an offline analysis that can help to optimise MSAW parameters.

The model in Figure 4.13 consists of the following functions [7]:

- "`MSAW management`": Manage the performance of MSAW.
- "`Providing surveillance data`": Provide system tracks of aircrafts, including tracked pressure altitude.
- "`Providing flight data`": Provide various flight data.
- "`Exclusion areas definition`": Define areas where no MSAW conflict detection is done.
- "`Modelling terrain and obstacles`": Model the terrain and obstacles outside exclusion areas.
- "`Providing meteorological data`": Provide meteorological data, such as barometric pressure, temperature, etc.
- "`Providing SSR code`": Provide Secondary Surveillance Radar (SSR) code to MSAW, used to determine if the track should be processed.
- "`System track eligibility test`": Test whether a system track is eligible to generate an alert.
- "`Terrain conflict filter`": If the predicted altitude is lower than the altitude value, generate a conflict hit.
- "`Obstacle conflict filter`": If the predicted altitude is lower than the altitude value, generate a conflict hit.

[3] Minimum Safe Altitude Warning.

- “`Terrain conflict alert confirmation`”: Confirm if a terrain conflict alert should be processed on the current cycle.
- “`Obstacle conflict alert confirmation`”: Confirm if an obstacle conflict alert should be processed on the current cycle.
- “`Recording`”: Record MSAW system data.
- “`Offline analysis`”: Analyse recorded data for optimisation.
- “`ATC procedures and local instructions`”: Guide the performance of controllers.
- “`Displaying data on working positions`”: Display meteorological, radar and flight data along with MSAW alerts to controllers.
- “`Pilot-controllers communication`”: Communication between the pilot and controllers who release warnings.
- “`Supervision`”: Supervise controllers’ performance.
- “`Changing climb rate`”: Pilot changes the climb rate of the aircraft after the warning.
- “`Changing altitude`”: Pilot changes the flight altitude of the aircraft.

The reconstruction and identification of couplings

On the grounds that the MSAW is a part of the larger technical system, most identified functions transfer Data, for example meteorological data, flight data, modelled terrain, etc. They represent raw technical data that is yet to become useful in a function to which it is flowing. In general most functions are well specified and we know exactly what their outputs are. However, the role of “`MSAW management`” is unclear. It is not described in what way it controls the behaviours of “`Modelling terrain and obstacles`” and “`Providing surveillance data`”. Does it periodically check whether they properly output data, or does it schedule them or maybe even correct their outputs? The function also outputs the parameter “terrain warning time” that has a temporal relation on “`Terrain conflict alert confirmation`”. Since this parameter is important for

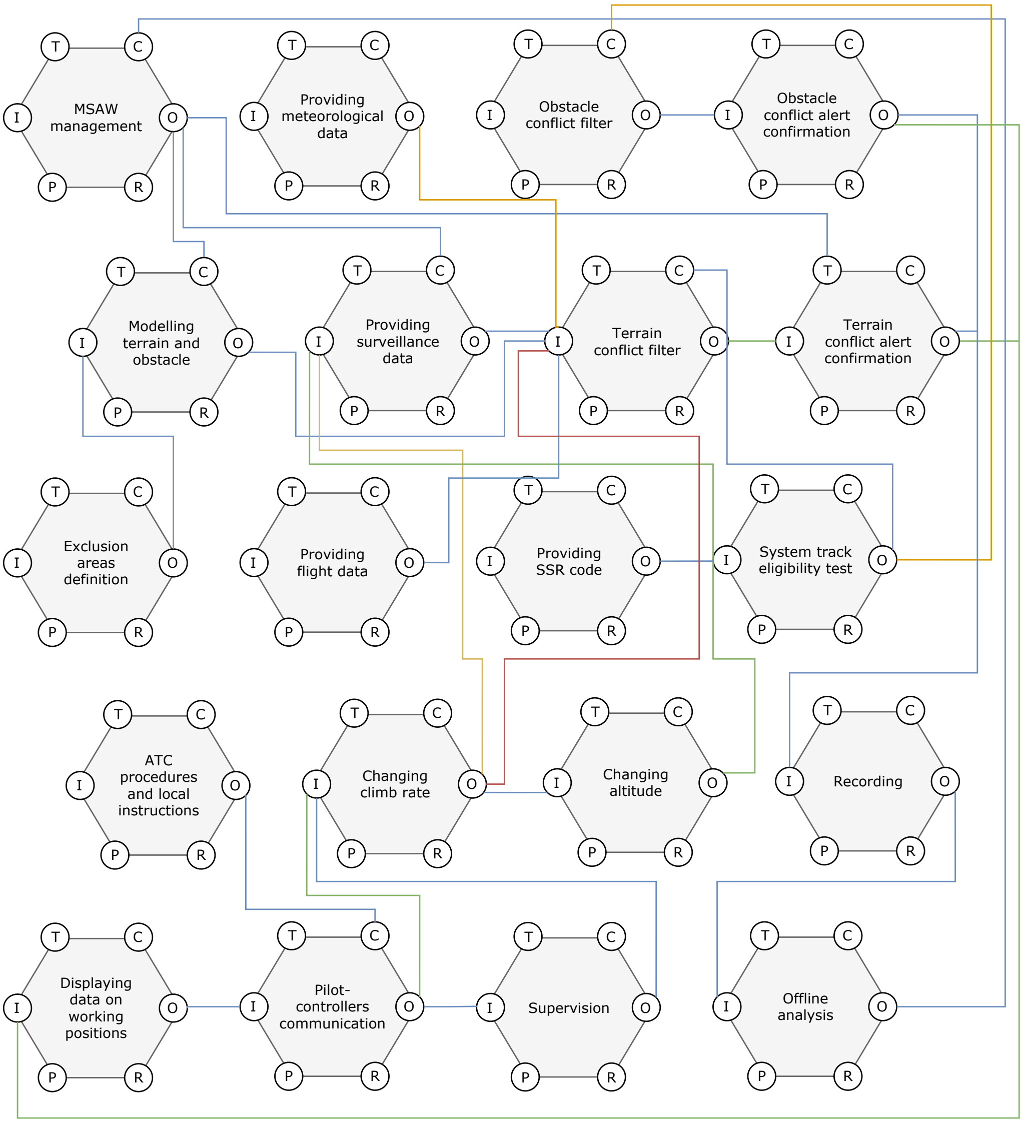
MSAW management
Providing meteorological data
Obstacle conflict filter
Obstacle conflict alert confirmation
Modelling terrain and obstacle
Providing surveillance data
Terrain conflict filter
Terrain conflict alert confirmation
Exclusion areas definition
Providing flight data
Providing SSR code
System track eligibility test
ATC procedures and local instructions
Changing climb rate
Changing altitude
Recording
Displaying data on working positions
Pilot-controllers communication
Supervision
Offline analysis
T
C
I
O
P
R

Figure 4.13: FRAM model 5 adapted from [7].

explaining a potential source of variability, it seems the function was put into model for this purpose.

"`MSAW management`" along with "`ATC procedures and local instructions`" and "`Offline analysis`" represent typical Control functions that in most cases are underspecified as they represent general supervision. The output of such function comprises rules, guidelines or instructions and is therefore classified as Guidance.

Figure 4.15 depicts the reconstruction and classification of couplings.

Findings

This model nicely displays the difference between Data and Information since it contains many examples of both. As Figure 4.14 displays, identified are all subcategories of Data (Numerical, Categorical, Mixed) and several subcategories of Information (Observation, Alert, Condition, Guidance).

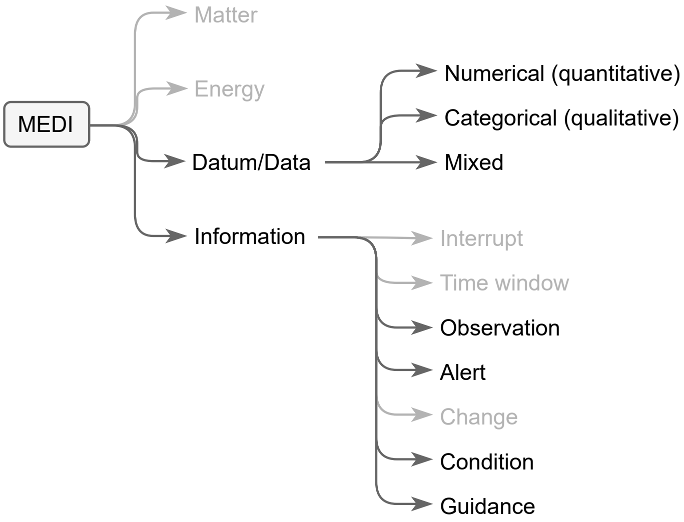

Figure 4.14: Identified types of couplings in FRAM model 5 (written in black) and the remaining classification scheme (written in grey).

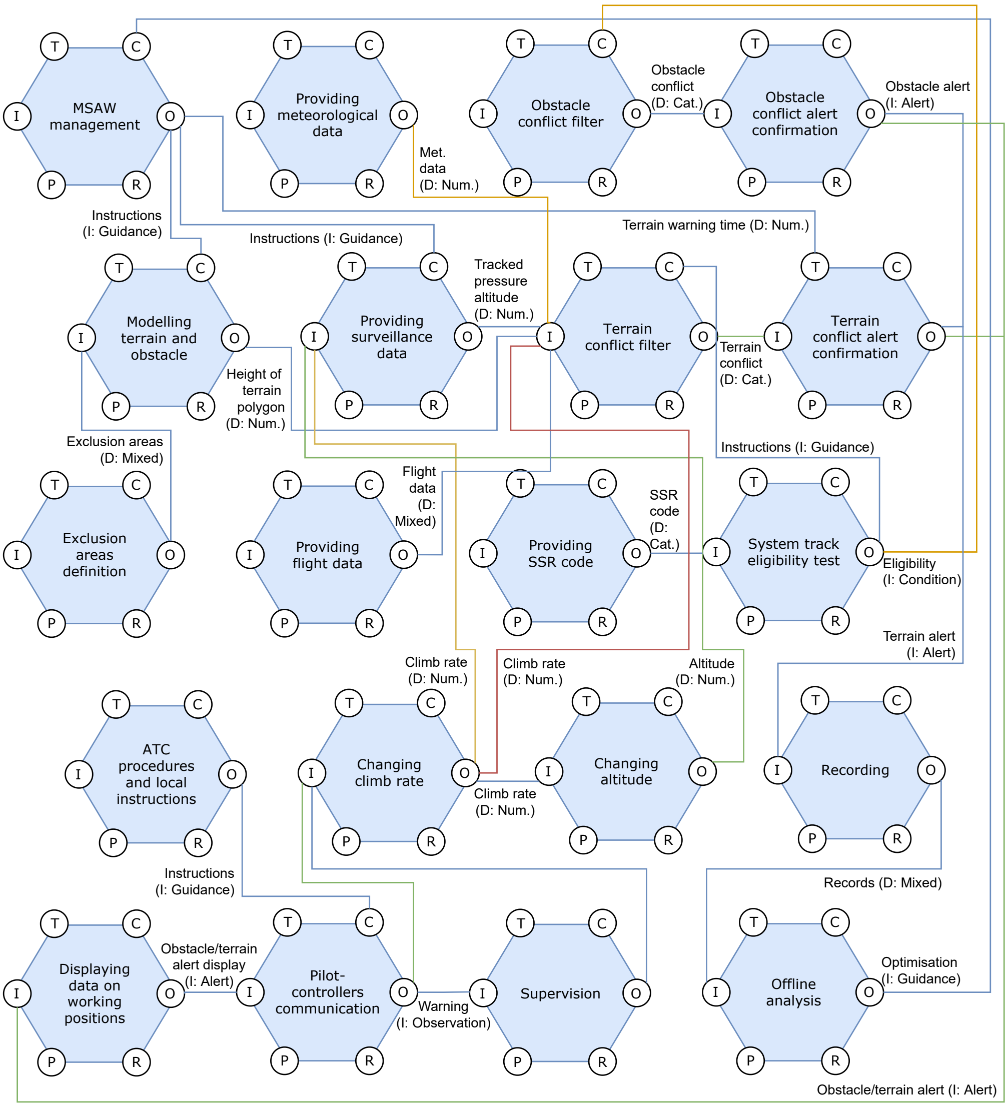
MSAW management
Providing meteorological data
Obstacle conflict filter
Obstacle conflict (D: Cat.)
Obstacle conflict alert confirmation
Obstacle alert (I: Alert)
Met. data (D: Num.)
Instructions (I: Guidance)
Instructions (I: Guidance)
Terrain warning time (D: Num.)
Modelling terrain and obstacle
Providing surveillance data
Tracked pressure altitude (D: Num.)
Terrain conflict filter
Terrain conflict (D: Cat.)
Terrain conflict alert confirmation
Height of terrain polygon (D: Num.)
Exclusion areas (D: Mixed)
Instructions (I: Guidance)
Exclusion areas definition
Providing flight data
Flight data (D: Mixed)
Providing SSR code
SSR code (D: Cat.)
System track eligibility test
Eligibility (I: Condition)
Terrain alert (I: Alert)
Climb rate (D: Num.)
Climb rate (D: Num.)
Altitude (D: Num.)
ATC procedures and local instructions
Changing climb rate
Changing altitude
Recording
Climb rate (D: Num.)
Instructions (I: Guidance)
Records (D: Mixed)
Displaying data on working positions
Obstacle/terrain alert display (I: Alert)
Pilot-controllers communication
Warning (I: Observation)
Supervision
Offline analysis
Optimisation (I: Guidance)
Obstacle/terrain alert (I: Alert)
T
C
I
O
P
R

Figure 4.15: Reconstructed FRAM model 5 from [7] with identified types of couplings (D: Data, I: Information).

4.2 Protocol description

Based on FRAM couplings that were identified during reconstruction of selected models in the previous Section, we extend existing MEI classification with *Data* and divide *Information* into subcategories. The new MEDI[4] classification is displayed in Figure 4.16 and presented in the following subsections.

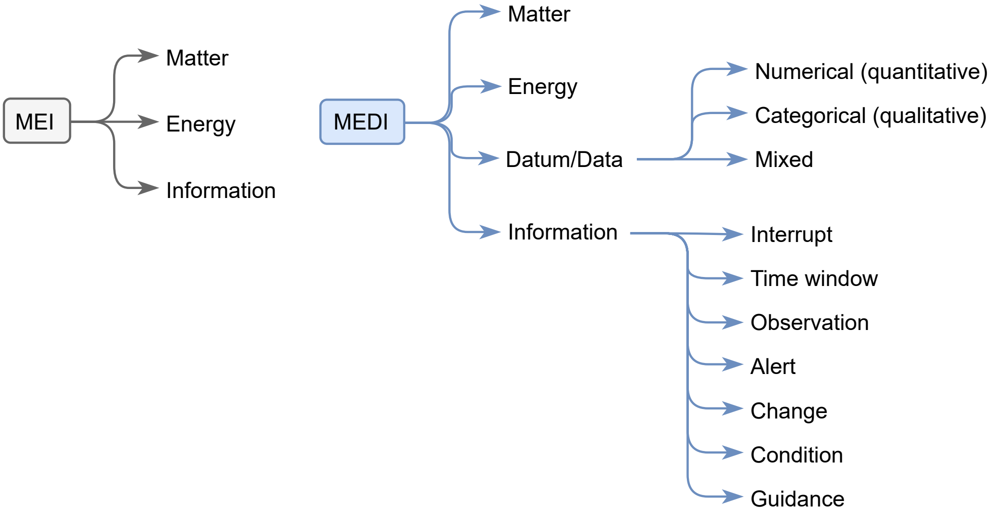

Figure 4.16: Existing MEI classification on the left and the new MEDI classification on the right.

Matter

Saunders and Harvey [42] defined matter as any substance that has mass and takes up space by having volume. In reconstructed FRAM models we discovered Matter in a form of humans (physician and nurses), firewater, physical structures (a parking garage and a dike) and waste.

Energy

Energy is the quantitative property that must be transferred to an object in order to perform work on or to heat it [43]. In reconstructed FRAM model 2 (see Subsection 4.1.2) we discovered smoke, heat, flames and electric power.

[4] Matter, Energy, Data, Information.

Data

Data represents a set of values flowing from one function to another that have no meaning and only become useful when a function puts them into a context. The coupling can contain either a single value (in which case the coupling is called *Datum*) or more values. Each value has either a quantitative or a qualitative property and based on that, we further divide Data into the following subcategories:

- Numerical: The coupling contains only values that have a quantitative property (can be expressed numerically).
- Categorical: The coupling contains only values with a qualitative property (can only be observed and generally cannot be expressed numerically).
- Mixed: The coupling contains both types of values.

Examples of Data from our selected FRAM samples are laboratory test results (Mixed Data), date of patient's discharge (Categorical Data) and the altitude (Numerical Datum).

Information

Sometimes a data structure flowing from one function to another cannot be classified as Matter, Energy or Data. For example, a function "`To inspect`" outputs (human) observations that are in general *actions* or *results of actions*. There may also exist a coupling between functions representing an arrangement that must be true in order to begin the second function (a precondition). All of these are complex representations of data that have something in common: they all are put into *context*. This is also the main reason they cannot be equated with Data. We define such data structure as Information and divide it into the following subcategories:

- Interrupt: An action that "interrupted" the observed function. It may affect the overall execution time of the observed function as well as its performance (degree of precision).
- Time window: Time interval in which a function must be carried out.
- Observation: Something one has seen, heard, or noticed.

- Alert: Something a technical device detected.

- Change: A change in the first function (with regard to the state of its Resource) leads to a change in the second function.

- Condition: An arrangement that must exist before something else can happen. Composed of several pieces of information together determining whether the condition is satisfied.

- Guidance: Rules, guidelines or instructions. A complex composition of multiple sub-functions that regulate the observed function so that it produces the correct output.

4.3 Protocol evaluation

In an effort to validate the findings, the couplings of yet unseen FRAM models were classified using a proposed MEDI classification in Subsections 4.3.1 and 4.3.2. We discuss the results in Subsection 4.3.3.

4.3.1 Validation model 1: Small aircraft takeoff procedure

Our first validation model is the FRAM model described in Section 3.4. As Figure 4.17 depicts, all couplings are classified as Information, either Guidance or Condition.

ATC instructions along with the interpreted and repeated version represent Guidance couplings. The author of the original model found out that the functional resonance emerges due to a misinterpretation of instructions. This indicates that in every Guidance coupling human cognitive perception and psychological factors represent a possible source of performance variability, for example, “Turn left heading 250.” may become “Turn right heading 250.”. From this it is evident that the Guidance link is highly prone to transfer the variability. This is something that needs to be taken into consideration in future steps towards method automatisation.

“`Ground check checklist`” and “`Adapt to ATC instructions`” both output a set of conditions that must be satisfied to start the corresponding downstream function. As they are the only Input to the corresponding downstream function, they also serve as start signals. “`Before takeoff checklist`” and “`Get takeoff clearance`” also output Conditions but with a difference that they are not start signals but preconditions.

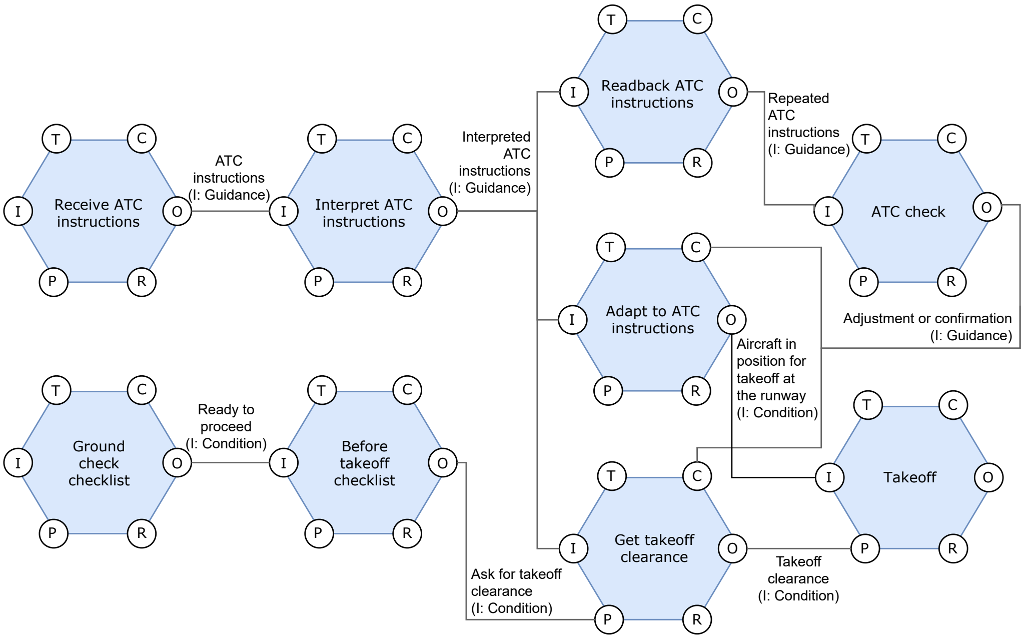
Readback ATC instructions
Repeated ATC instructions (I: Guidance)
Interpreted ATC instructions (I: Guidance)
ATC check
Receive ATC instructions
ATC instructions (I: Guidance)
Interpret ATC instructions
Adapt to ATC instructions
Adjustment or confirmation (I: Guidance)
Aircraft in position for takeoff at the runway (I: Condition)
Ground check checklist
Ready to proceed (I: Condition)
Before takeoff checklist
Takeoff
Get takeoff clearance
Ask for takeoff clearance (I: Condition)
Takeoff clearance (I: Condition)
T
C
I
O
P
R

Figure 4.17: Validation model 1 with identified types of couplings (I: Information).

4.3.2 Validation model 2: VTS system

The second validation model is presented in [8] and describes Vessel Traffic Service (VTS), a service to promote safe and fluent traffic in port entrances. VTS Operators (VTSOs) monitor the traffic and provide information relevant for the safe passage to all vessels in a designated area. For example, information can include reports on position, identity and intentions of other vessels, or information regarding the geographical and meteorological state of the area. The original work considers VTS as a socio-technical system and applies FRAM to describe its everyday operations. [8]

VTS under review belongs to the local port infrastructure of one of northern European largest ports. It consists of a single VTSO on duty, located in a joint port operation centre next to the harbour master and pilot dispatch. VTSO offers information service and is responsible for issuing berth clearances, as well as clearances to leave anchorage. [8]

The model (see Figure 4.18) consists of the following functions [8]:

- "`Enter VTS area`": A vessel enters a port area monitored by VTS.
- "`Pass reporting point`": A vessel passes the reporting point upon which VTS starts to work with it. Prior to that, VTS does not get any notice of incoming

vessel.

- “`Receive vessel report`”: VTSO receives a vessel report such as vessel’s name and destination.
- “`Establish VHF contact`”: VTSO establishes a contact with the vessel through the use of VHF[5] radio.
- “`Establish harbour infrastructure`”: Maritime administration provides a harbour infrastructure.
- “`Install VTS`”: Maritime administration sets up a VTS system.
- “`Provide forecast to VTS`”: Weather service sends an email containing meteorological forecast information to VTSO.
- “`Read hydrometeorological data`”: VTSO takes measurements on sight, for example, a water current.
- “`Collect hydrometeorological information`”: VTSO combines hydrometeorological information received from the weather service with measurements on sight.
- “`Collect traffic information`”: VTSO collects traffic information provided by a harbour master.
- “`Monitor traffic`”: VTSO estimates current traffic situation by means of received traffic and hydrometeorological information and monitoring traffic.
- “`Provide traffic information`”: VTSO provides traffic information to a vessel.
- “`Request to leave berth`”: Vessel requests permission to leave berth.
- “`Give/deny berth clearance`”: VTSO issues or denies a berth clearance.
- “`Request to leave anchorage`”: Vessel requests permission to leave anchorage.
- “`Give/deny clearance to leave anchorage`”: VTSO issues or denies a clearance to leave anchorage.

[5] Very High Frequency.

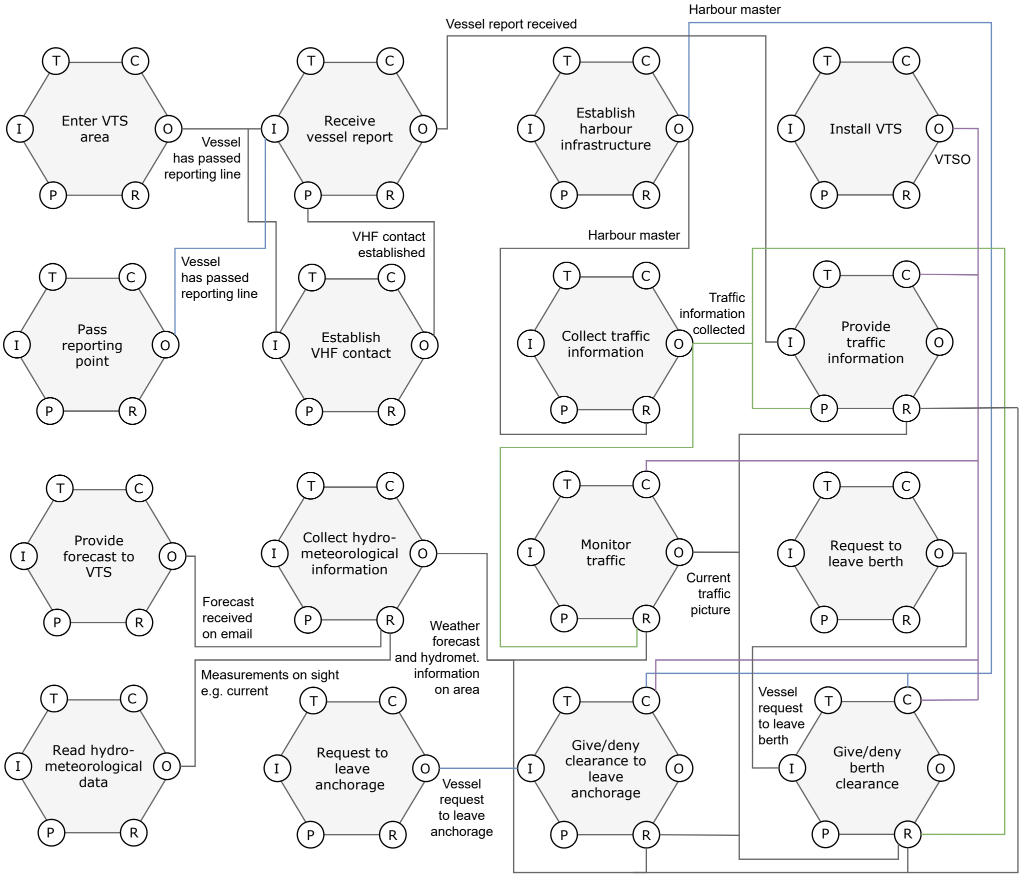
T
C
I
O
P
R
Enter VTS area
Receive vessel report
Establish harbour infrastructure
Install VTS
Pass reporting point
Establish VHF contact
Collect traffic information
Provide traffic information
Provide forecast to VTS
Collect hydro-meteorological information
Monitor traffic
Request to leave berth
Read hydro-meteorological data
Request to leave anchorage
Give/deny clearance to leave anchorage
Give/deny berth clearance
Vessel report received
Harbour master
Vessel has passed reporting line
VTSO
VHF contact established
Harbour master
Vessel has passed reporting line
Traffic information collected
Forecast received on email
Weather forecast and hydromet. information on area
Current traffic picture
Measurements on sight e.g. current
Vessel request to leave berth
Vessel request to leave anchorage

Figure 4.18: Validation model 2 adapted from [8].

The classification of couplings

Figure 4.19 depicts model and couplings classified using MEDI classification.

Matter appears in a form of humans as an Output of "`Install VTS`" and "`Establish harbour infrastructure`", representing Resources of some of the main tasks of VTS system.

Data couplings contain traffic and weather information: traffic information provided by the harbour master (numerical and categorical), a forecast VTSO received on email (numerical and categorical) and VTSO's measurements on sight (categorical).

There are three types of Information coupling in the model: Observation, Alert and Condition. Assuming that both a technical device and VTSO are able to detect the vessel entering VTS area, we classify Outputs of "`Enter VTS area`" and "`Pass reporting point`" as Alert and Observation, consecutively. Other example of Observation is "Current traffic picture", a result of VTSO's perception of current traffic situation.

The Output of "`Collect traffic information`" is interesting as it appears both as Data or Condition, depending on the function aspect it leads to: in case of a Resource, the coupling is classified as Data, and in case of a Precondition, the coupling is classified as Condition.

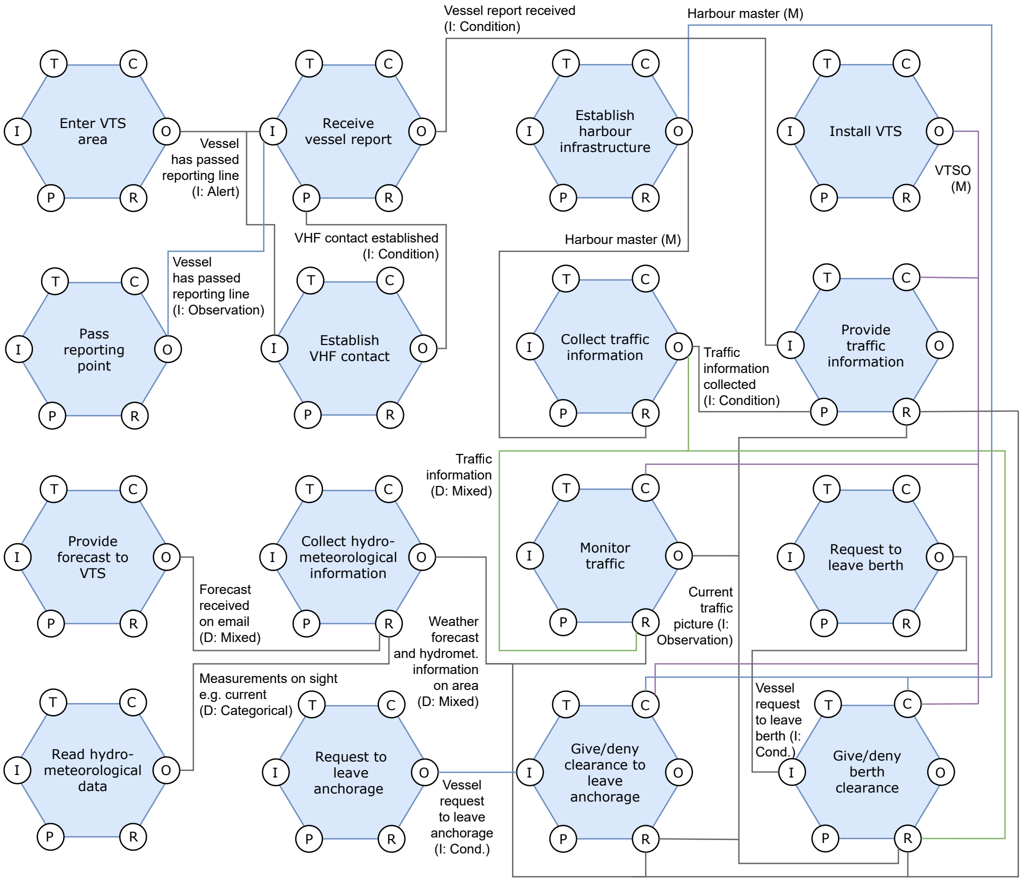
Enter VTS area
Vessel has passed reporting line (I: Alert)
Receive vessel report
Vessel report received (I: Condition)
Establish harbour infrastructure
Harbour master (M)
Install VTS
VTSO (M)
Pass reporting point
Vessel has passed reporting line (I: Observation)
VHF contact established (I: Condition)
Establish VHF contact
Harbour master (M)
Collect traffic information
Traffic information collected (I: Condition)
Provide traffic information
Provide forecast to VTS
Collect hydro-meteorological information
Forecast received on email (D: Mixed)
Traffic information (D: Mixed)
Monitor traffic
Current traffic picture (I: Observation)
Request to leave berth
Weather forecast and hydromet. information on area (D: Mixed)
Measurements on sight e.g. current (D: Categorical)
Read hydro-meteorological data
Request to leave anchorage
Vessel request to leave anchorage (I: Cond.)
Give/deny clearance to leave anchorage
Vessel request to leave berth (I: Cond.)
Give/deny berth clearance
T
C
I
O
P
R

Figure 4.19: Validation model 2 with identified types of couplings (M: Matter, D: Data, I: Information).

4.3.3 Discussion

The classification results of validation models demonstrate the adequacy of the MEDI classification. Figure 4.20 illustrates identified types of couplings in validation models as well as the remaining classification scheme.

Validation model 1 (see Subsection 4.3.1) consists of Information couplings, namely Guidance and Condition couplings. Validation model 2 (see Subsection 4.3.2) contains

Matter, Data (Categorical and Mixed) and several subcategories of Information, namely Observation, Alert and Condition.

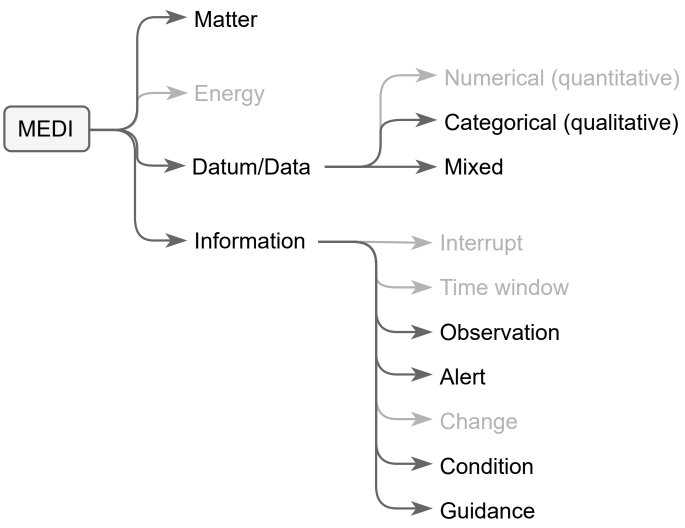

Figure 4.20: Identified types of couplings in validation models (written in black) and the remaining classification scheme (written in grey).

4.4 Protocol contributions

The main contribution of this thesis is the MEDI classification described in Section 4.2 and depicted in Figure 4.16. It provides a better definition of relations among functions in a FRAM model and lays the foundations for translating the model into a computer language. A well-defined set of couplings can provide standardisation and thus maximising compatibility, interoperability, safety and quality of FRAM models in general.

The starting point for understanding how functional resonance occurs in a FRAM model is to characterise the variability of functions. As stated in [1] technological functions are relatively stable, while human and organisational functions may vary. MEDI contains some constraints based on function type, for example, Observation (Information) is always an output of a human function and Alert (Information) is always an output of a technological function. In our selected models variability is mostly transferred over Information couplings such as Time window, Observation, Change, Condition and Guidance. The MEDI classification in its current form can help to detect potential variability sources faster if we assume that the aforementioned types of couplings are more prone to spreading variability than other types.

The process of constructing a FRAM model of the selected activity includes identifying functions necessary to complete the activity and describing potential couplings between functions. Specifying couplings using MEDI is not only faster and easier but it also ensures that the model is set up according to some rules allowing the automatisation of the analysis in the future. How MEDI contributes to the development of FRAM automatisation is described in the following Section.

4.5 Towards method automatisation

The first challenge of FRAM automatisation is presenting the model along with its couplings to the computer. In this work we focused on FRAM couplings, extending existing MEI classification to develop new MEDI classification. In this discussion we look at ways how to represent FRAM couplings to the computer using the new classification.

Matter is any substance that has mass. The name of the matter could be stored in a text variable. However, many times additional information about the state of the matter is crucial for identifying the variability. For example, in FRAM model 4 "`Delivery of sorted waste`" is a potential source of variability if delivered waste is unsorted due to an error. So it makes sense to describe a Matter coupling with both name and state of the matter.

Energy is by definition a quantitative property and just like Data it should not be a problem to store it in a computer variable. However, an Information coupling is more complex.

In computer terms we can say Information is a composite data type that must be decomposable into primitive data types if we want the computer (based on current technology) to operate with it. Some of identified Information subcategories are obvious transformations such as: Time window is composed of two time variables that many programming languages implements in their modules (e.g. datetime); Condition is a set of conditional statements evaluating to true or false, a long known concept in the computer world. Transformations of other subcategories are not so obvious.

Guidance represents a set of rules, guidelines or instructions. Examples of instructions from chosen FRAM models are: "Take medication X every Y days.", "Taxi to runway two-seven right via alpha two, bravo and delta. Cross runway three-five.", "Turn left heading 250, descend flight level 120.". Looking closely, each instruction contains

Data, for example "Take medication X every Y days." contains two values, a type of medicine X (categorical) and number of days Y (numerical). The same applies to rules or guidelines, for example in FRAM model 4 "`Levelling control`" controls crushing the waste and prevents the crusher from overflowing the jaw cavity. Levelling control coupling may contain maximum allowed level value for normal functioning of the crusher. Each Guidance coupling thus consists of Data. What makes it different and more complex than Data is that it contains a context, for example number of days Y from the first example is associated with taking medicine.

Observation and Alert indicate the ongoing event or the event outcome that was observed by a human or a technical device. In computer languages these two categories would be represented with a set of values including event type and additional information about the event. For example, "There is fire." is an output of "`Manually observe fire`" and it may be stored as a text variable (similar to Matter) or a Boolean variable set to true since the function is very specific and it only outputs information denoting the presence of fire. Additional values such as fire intensity and time may be stored as well. However, this is only possible for well-defined functions whose outputs are predictable to some extent.

Our definition of Interrupt resembles the one used in digital computing. In our case it is an input signal to the function indicating an event happened, affecting temporal and performance aspect of the function. For example, a phone call for the physician while he is doing the ward round can extend or reduce time needed to complete the ward round and distract the physician affecting his performance. Like Observation or Alert, Interrupt is an event and represents the similar challenge to storing it in a computer variable.

5 Conclusion

Socio-technical systems from fields such as aviation, healthcare, construction and power engineering bring comfort and efficiency in various aspects of human lives. At the same time, accidents such as aircraft crashes, medical radiation overexposures and nuclear power plant incidents have never stopped taking place. Safety has thus become one of the most important concerns in any socio-technical system.

A FRAM model shows how the functions of a socio-technical system are linked. It can be used to find the conditions in which system functions get out of control by identifying couplings leading to an increase in performance variability. A computerised FRAM analysis would allow us to analyse such systems more efficiently. In order to computerise a method, the relations between functions should be clear and precise. Hence, this thesis focused on the development of a more accurate classification of FRAM inter-functional couplings.

After an initial review of literature on safety and the method, we selected several FRAM models from different fields to gain an overall impression of relations among functions. Step by step we analysed functions and couplings of each model, soon to discover there was no common “rule” among different types of couplings. It became clear this was due to the fact the method does not provide more accurate classification of couplings than “Matter, Energy, Information (MEI)”, consequently introducing many ways to construct a model. Therefore, in the next step we reconstructed the models preserving their purposes and increasing clarity by removing redundant functions and correcting coupling aspects if necessary. On such models we were then able to start recognising patterns in couplings.

In the course of this work we provided a more accurate classification of FRAM interfunctional couplings. We extended existing MEI classification with Data and divided Information into subcategories. The new MEDI classification scheme includes Matter, Energy, Data and Information. Matter and Energy retain their meaning from previous classification while Data and Information introduce a new concept. Data represents “raw” quantitative or qualitative data that only becomes useful when the function puts it into a context. Meanwhile, Information is seen as a higher presentation of Data, already involving its own context.

Based on different contexts contained in a FRAM coupling, we divided Information into the following subcategories: Interrupt, Time window, Observation, Alert, Change, Condition and Guidance. Interrupt represents an action affecting the overall execution time and performance of the observed function. Time window is defined as a time interval in which the observed function must be carried out. Observation is a remark about something one has noticed. Alert is similar to Observation except it was detected by a technical device. Change represents the relation in which the change in the first function leads to a change in the other one. Condition is an arrangement that must exist before something else can happen. Guidance is a set of rules, guidelines or instructions that regulate the observed function so that it produces the correct output.

Identified MEDI classification provides a better understanding of what is being transferred among functions of a socio-technical system. It is a result of striving for a more “computational” presentation of FRAM models. Although our evaluation results showed it is adequate, it is by no means complete. The classification could further be expanded by examining more models, possibly to discover additional types of couplings. Once the classification proved to be sufficient for most models, it could be implemented into various FRAM modelling tools; the user who is building a FRAM model would be able to choose among MEDI classified couplings. This would not only reduce the effort needed to construct the model but also bring a standardisation among models.

The most important future direction is the automatisation of the method. Performing FRAM analysis algorithmically as opposed to the current method would represent a large improvement in efficiency of discovering the emergent phenomenon in socio-technical systems, the functional resonance.

Bibliography

[1] E. Hollnagel, FRAM: The Functional Resonance Analysis Method: Modelling Complex Socio-Technical Systems, Ashgate Publishing Limited, England, 2012.

[2] E. Hollnagel, J. Hounsgaard, L. Colligan, FRAM – the Functional Resonance Analysis Method – a handbook for the practical use of the method, Centre for Quality, Southern Region of Denmark, 2014.

[3] D. C. Raben, B. Viskum, K. L. Mikkelsen, J. Hounsgaard, S. B. Bogh, E. Hollnagel, Application of a non-linear model to understand healthcare processes: using the functional resonance analysis method on a case study of the early detection of sepsis, Reliability Engineering & System Safety 177 (2018) 1–11.

[4] R. Patriarca, A. Falegnami, F. Costantino, F. Bilotta, Resilience engineering for socio-technical risk analysis: Application in neuro-surgery, Reliability Engineering & System Safety 180 (2018) 321–335.

[5] D. C. Raben, S. B. Bogh, B. Viskum, K. L. Mikkelsen, E. Hollnagel, Proposing leading indicators for blood sampling: application of a method based on the principles of resilient healthcare, Cognition, Technology & Work 19 (4) (2017) 809–817.

[6] P. Carvalho, The use of Functional Resonance Analysis Method (FRAM) in a midair collision to understand some characteristics of the air traffic management system resilience, Reliability Engineering & System Safety 96 (2011) 1482–1498.

[7] Q. Yang, J. Tian, T. Zhao, Safety is an emergent property: Illustrating functional resonance in air traffic management with formal verification, Safety science 93 (2017) 162–177.

[8] G. Praetorius, E. Hollnagel, J. Dahlman, Modelling Vessel Traffic Service to understand resilience in everyday operations, Reliability Engineering & System Safety 141 (2015) 10–21.

[9] R. Patriarca, J. Bergström, G. Di Gravo, Modelling complexity in everyday operations: Functional resonance in maritime mooring at quay, Cognition, Technology & Work 19 (2017) 711–729.

[10] F. Anvarifar, M. Z. Voorendt, C. Zevenbergen, W. Thissen, An application of the Functional Resonance Analysis Method (FRAM) to risk analysis of multifunctional flood defences in the Netherlands, Reliability Engineering & System Safety 158 (2017) 130–141.

[11] L. V. Rosa, A. N. Haddad, P. V. R. de Carvalho, Assessing risk in sustainable construction using the Functional Resonance Analysis Method (FRAM), Cognition, Technology & Work 17 (4) (2015) 559–573.

[12] R. Patriarca, G. Di Gravio, F. Costantino, M. Tronci, The Functional Resonance Analysis Method for a systemic risk based environmental auditing in a sinter plant: A semi-quantitative approach, Environmental Impact Assessment Review 63 (2017) 72–86.

[13] E. Hollnagel, An Application of the Functional Resonance Analysis Method (FRAM) to Risk Assessment of Organisational Change, The Swedish Radiation Safety Authority (SSM) 2013:09, Sweden, 2012.

[14] A. Hale, J. Hovden, Management and culture: the third age of safety. A review of approaches to organizational aspects of safety, health and environment, in: A.-M. Feyer, A. Williamson (Eds.), Occupational Injury: Risk, Prevention and Intervention, Taylor & Francis, England, 1998, pp. 129–166.

[15] A. Hale, The role of H.M. Inspectors of Factories with particular reference to their training, PhD dissertation, University of Aston in Birmingham (1978).

[16] H. Heinrich, Industrial accident prevention, McGraw-Hill, US, 1931.

[17] H. Watson, et al., Launch control safety study, Bell labs, US, 1961.

[18] MIL-STD-1629A, Military Standard: Procedures for Performing a Failure Mode Effects and Criticality Analysis, Department of Defense: Washington, DC, US, US, 1980.

[19] H. G. Lawley, Operability studies and hazard analysis, Chemical Engineering Progress 70 (4) (1974) 45–56.

[20] J. T. Reason, Managing the risks of organizational accidents, Ashgate Publishing Limited, England, 1997.

[21] K. Savoudian, J.-S. Wu, G. Apostolakis, Incorporating organizational factors into risk assessment through the analysis of work processes, Reliability Engineering & System Safety 45 (1-2) (1994) 85–105.

[22] K. H. Roberts, Some Characteristics of One Type of High Reliability Organization, Organization Science 1 (2) (1990) 160–176.

[23] N. Pidgeon, The Limits to Safety? Culture, Politics, Learning and Man-Made Disasters, Journal of Contingencies and Crisis Management 5 (1) (1997) 1–14.

[24] P. Hudson, Implementing a safety culture in a major multi-national, Safety science 45 (6) (2007) 697–722.

[25] A. I. Glendon, S. G. Clarke, E. F. McKenna, Human safety and risk management (2nd ed.), Boca Raton, US, 2006.

[26] D. Borys, D. Else, S. Leggett, The fifth age of safety: The adaptive age, Journal of Health Services Research and Policy 1 (2009) 19–27.

[27] E. Hollnagel, D. Woods, N. Leveson, Resilience Engineering: Concepts and Precepts, Ashgate Publishing Limited, England, 2006.

[28] E. Trist, The evolution of socio-technical systems, Ontario Quality of Working Life Centre, Occasional paper 2 (1981) 6–11.

[29] E. Trist, K. Bamforth, Some social and psychological consequences of the long wall method of coal-getting, Human Relations 4 (1951) 3–38.

[30] N. Jordan, Allocation of functions between man and machines in automated systems, Journal of Applied Psychology 47 (3) (1963) 161–165.

[31] J. Pariès, J. Wreathall, E. Hollnagel, Resilience Engineering in Practice: A Guidebook, Taylor & Francis, England, 2013.

[32] E. Hollnagel, Resilience Engineering, http://erikhollnagel.com/ideas/resilience-engineering.html, [Online; accessed July 10, 2020].

[33] E. Hollnagel, Resilience Assessment Grid (RAG), http://erikhollnagel.com/ideas/resilience%20assessment%20grid.html, [Online; accessed July 10, 2020].

[34] S. Gulbransen, F. A. Drews, Elements of an Agile Safety Culture in Health Care, https://slideplayer.com/slide/4614229/, [Online; accessed July 10, 2020].

[35] N. Leveson, Engineering a Safer World: Systems Thinking Applied to Safety, MIT Press, US, 2011.

[36] J. Rasmussen, S. I., Proactive risk management in a dynamic society, Swedish Rescue Services Agency, Sweden, 2000.

[37] N. Leveson, A new accident model for engineering safer systems, Safety Science 42 (2004) 237–270.

[38] E. Hollnagel, The ETTO Principle - Efficiency-Thoroughness Trade-Off, http://erikhollnagel.com/ideas/etto-principle/, [Online; accessed July 10, 2020].

[39] M. Tkalec, Reliability analysis of a socio-technical system example based on the FRAM method, BSc thesis, University of Ljubljana (2017).

[40] J. Hounsgaard, Patient Safety in Everyday Work: Learning from things that go right, MSc thesis, University of Southern Denmark (2016).

[41] J. Åhman, Analysis of interdependencies within the fire fighting function on an offshore platform, MSc thesis, Lund University (2013).

[42] S. Saunders, H. R. Brown, The Philosophy of Vacuum, Oxford University Press, 1991.

[43] R. L. Lehrman, Energy is not the ability to do work, The Physics Teacher 11 (1) (1973) 15–18.