Modelling ATM

Paula Santos
paula.santos@nav.pt

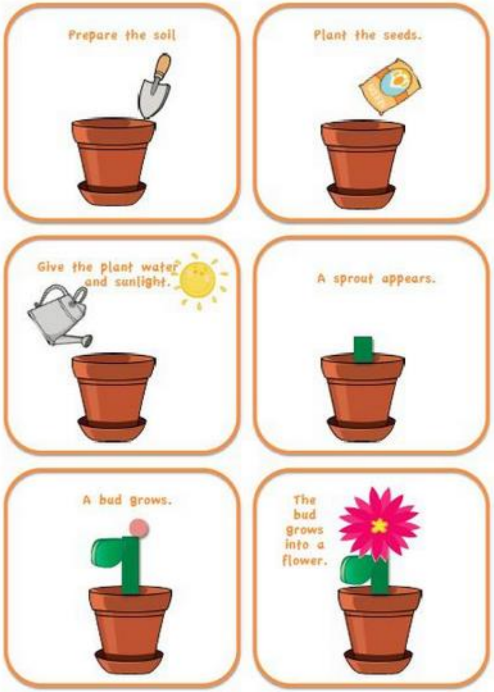
Summary

Modelling day to day ATM System

The modelling of functional system architecture is essential not only from the business and management point of view but also for the safety activities – NAV Portugal experience in modelling ATM system looking at Day to Day Operations

Agenda

1. Why model?
2. What to model?
3. How?
4. The result – the model
    - Overview
    - Main characteristics
5. Usage
6. Future


Prepare the soil
Plant the seeds.
Give the plant water and sunlight.
A sprout appears.
A bud grows.
The bud grows into a flower.

Why

To comply with regulation EU1035/2011, annex II paragraph 3.2 – *Safety requirements for risk assessment and mitigation with regard to changes*

To assess a change we need to know the system before the change – have a reference.

Why

To have a global view of the functional system, to know it.

What is the functional system?

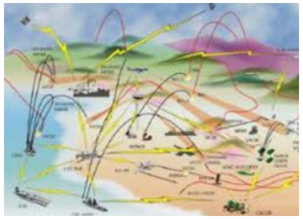
“the equipment, procedures and human resources of the ATM functional system, the interactions between these elements and the interactions between the constituent part under consideration and the remainder of the ATM functional system”

+

+

= $f(x)$

+



Why

To show the dependencies between processes

- Be the starting point to understand the connection between high level processes and their global impact on safety

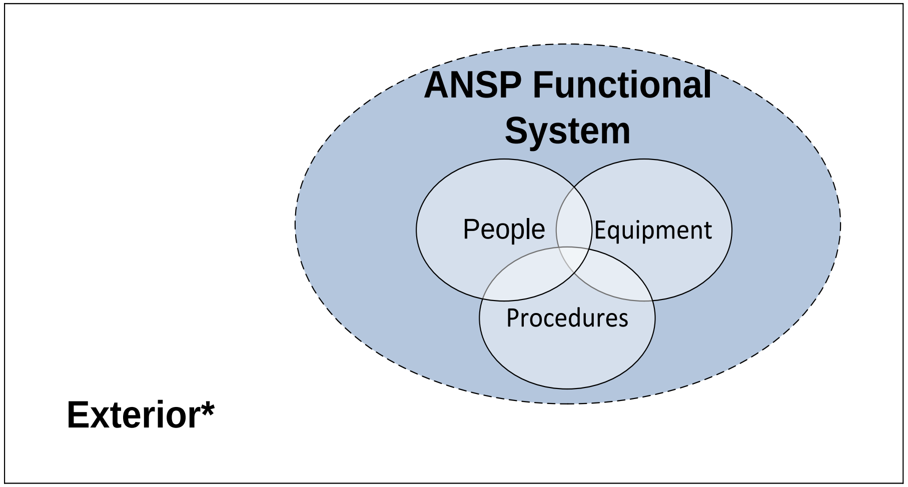
To allow description of architecture

What

The aim of ATM is to prevent accidents.

- Five ICAO defined accidents, namely: mid-air collision, wake turbulence, runway collision, taxing collision and CFIT.

Scope:

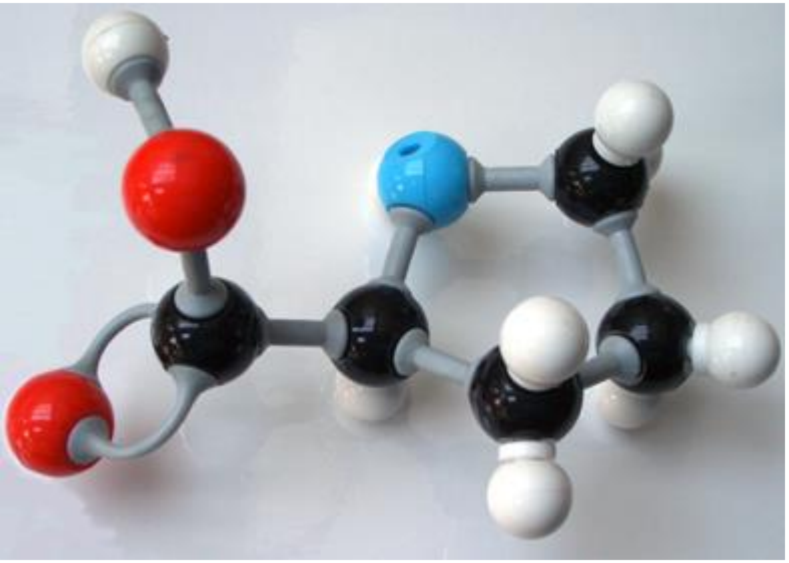


What

What do we do everyday to prevent accidents?

That is what we have modelled.
What is modelling? Simplifying reality.

What do we have?
A knowledge database.



How

Usually in ATM safety analysis we look backwards after an incident. Something went wrong, why?

Reactive approach: Incident, backwards

(Safety I)

How

In business modelling we describe what is done to have success.

Proactive approach: Success, what is done to…

(Safety II)

How

Build the model (knowledge database) using the proactive approach.

It will never be finished…

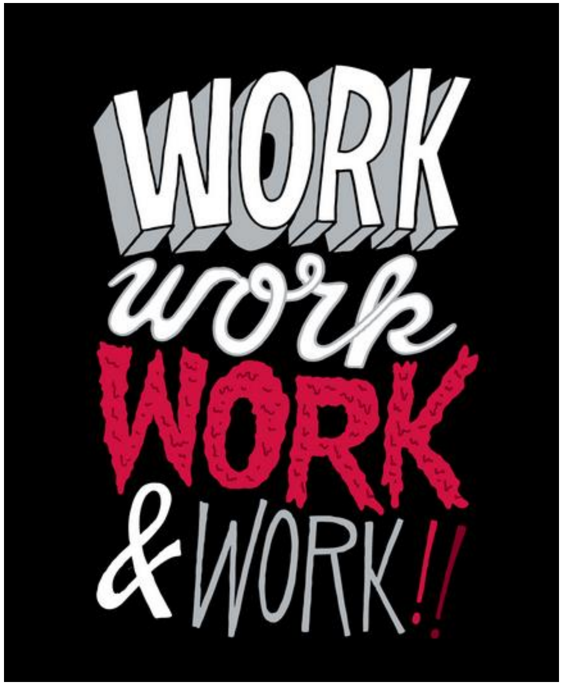
Improve it, refine it also with the feedback from the analysis of incidents – reactive approach.

Both approaches complement each other.

How

What do we do?

- Airspace management
- Flow and capacity management
- Provide meteorological information
- Provide aeronautical information
- Manage traffic
- Respond to anomalies
- Alert
- Manage operational room
- Technical support
- Maintain infrastructure



How

Interviews with operational staff from every area.

Structure of the interview:

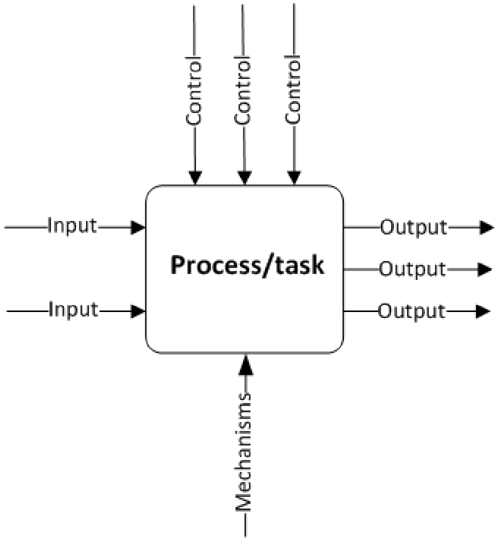
- Presentation of the aim of the modelling activity
- Tell us what you do (Normally with a lot of details)
- Tell us what you need to do the work
- Tell us what you produce and to whom
- We report what we understood (very, very high level)

The results were later reviewed by others.

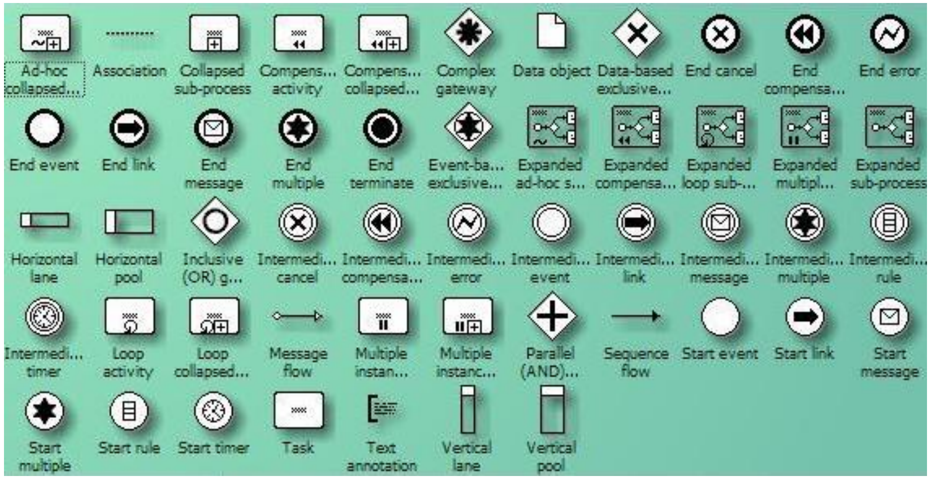
How

Choice of representation

- SADT - Static
  (Structured Analysis and Design Technique)



- BPMN - Dynamic
  (Business Process Modelling Notation)



How

The complexity of the model required the development of a framework to build it and validate it.

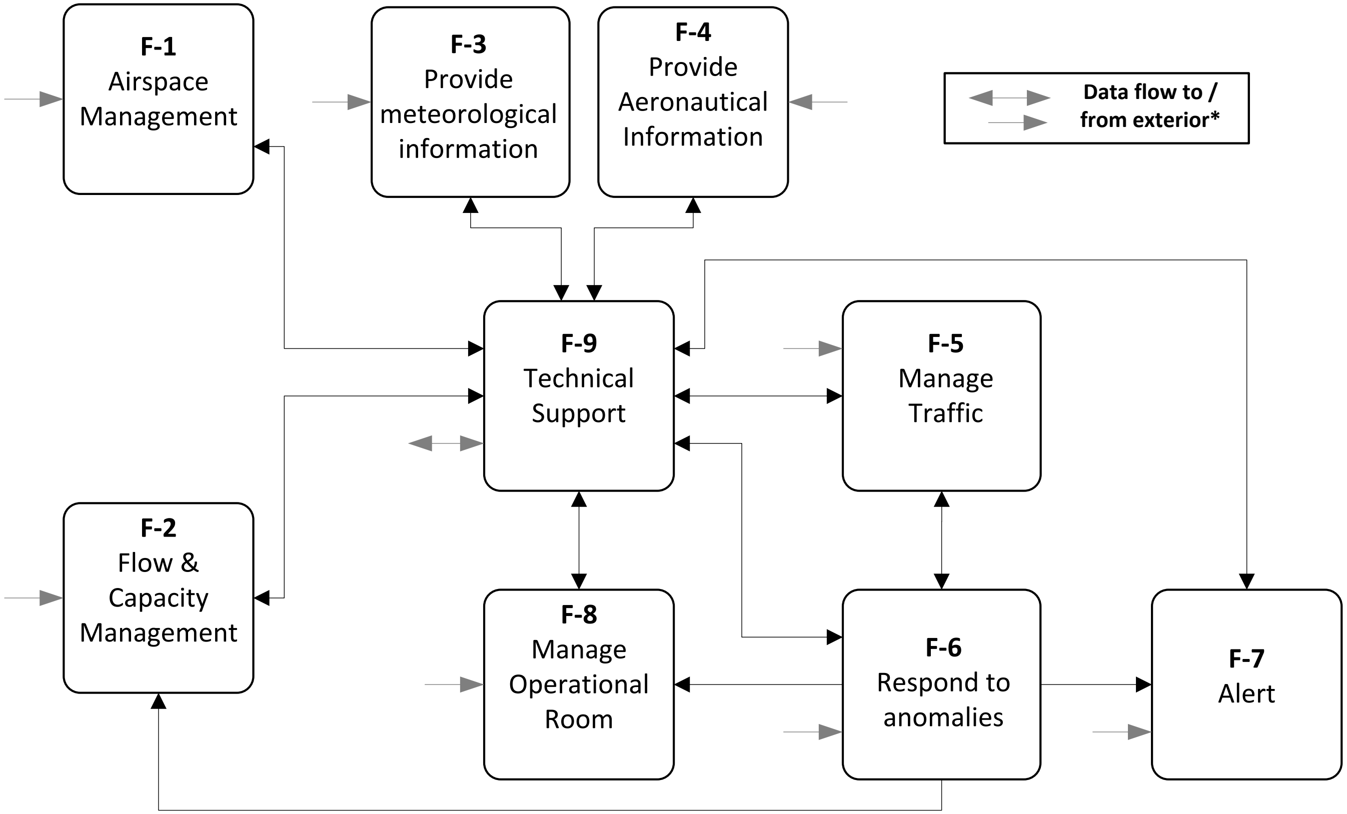
Yes, it is a simplification but it is anyway very complex…

It is a knowledge repository.

Knowledge needs to be captured and coded.

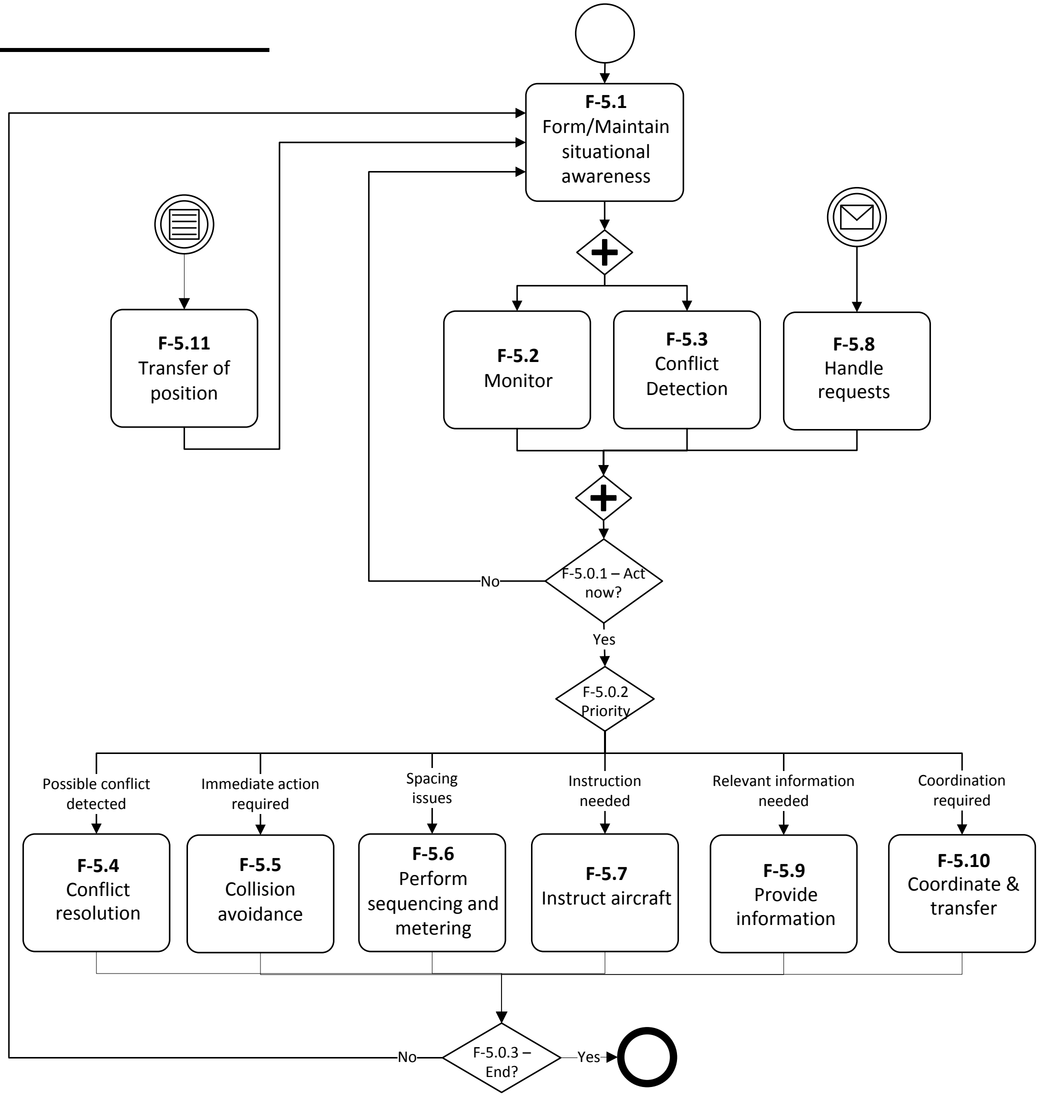
Result

Top level



Result

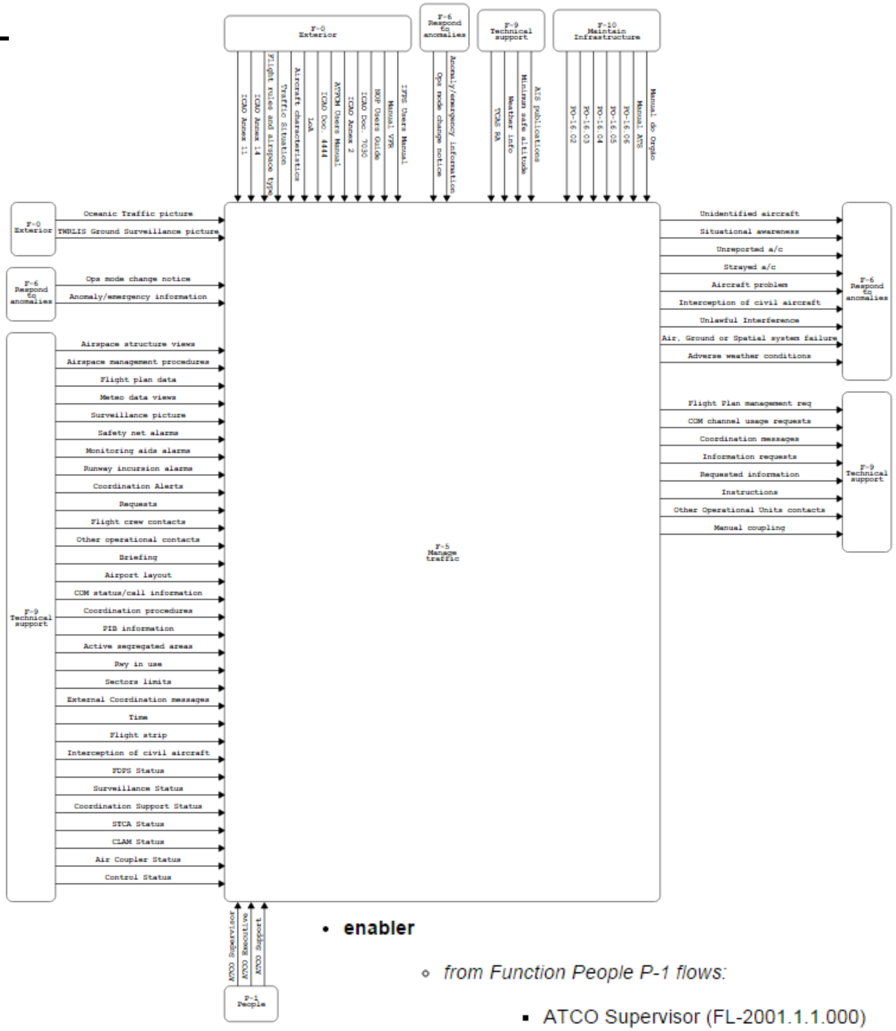
Manage traffic (BPMN)


F-5.1 Form/Maintain situational awareness
F-5.11 Transfer of position
F-5.2 Monitor
F-5.3 Conflict Detection
F-5.8 Handle requests
F-5.0.1 – Act now?
No
Yes
F-5.0.2 Priority
Possible conflict detected
Immediate action required
Spacing issues
Instruction needed
Relevant information needed
Coordination required
F-5.4 Conflict resolution
F-5.5 Collision avoidance
F-5.6 Perform sequencing and metering
F-5.7 Instruct aircraft
F-5.9 Provide information
F-5.10 Coordinate & transfer
No
F-5.0.3 – End?
Yes

Result

Manage traffic (SADT)

- **output**
  - *to Function Respond to anomalies F-6 flows:*
    - Unidentified aircraft (FL-5.000)
    - Situational awareness (FL-5.001)
    - Unreported a/c (FL-5.002)
    - Strayed a/c (FL-5.003)
    - Aircraft problem (FL-5.004)
    - Interception of civil aircraft (FL-5.005)
    - Unlawful Interference (FL-5.006)
    - Air, Ground or Spatial system failure (FL-5.007)
    - Adverse weather conditions (FL-5.016)
  - *to Function Technical support F-9 flows:*
    - Flight Plan management req (FL-5.008)
    - COM channel usage requests (FL-5.009)
    - Coordination messages (FL-5.010)
    - Information requests (FL-5.011)
    - Requested information (FL-5.012)
    - Instructions (FL-5.013)
    - Other Operational Units contacts (FL-5.014)
    - Manual coupling (FL-5.015)



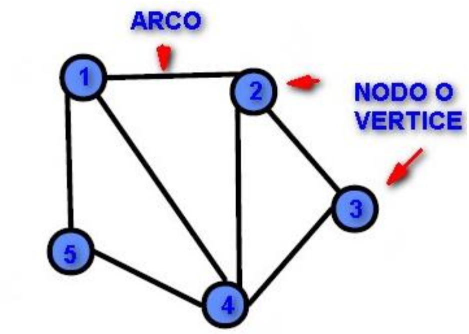
- **enabler**
  - *from Function People P-1 flows:*
    - ATCO Supervisor (FL-2001.1.1.000)
    - ATCO Executive (FL-2001.1.2.000)
    - ATCO Support (FL-2001.1.3.000)

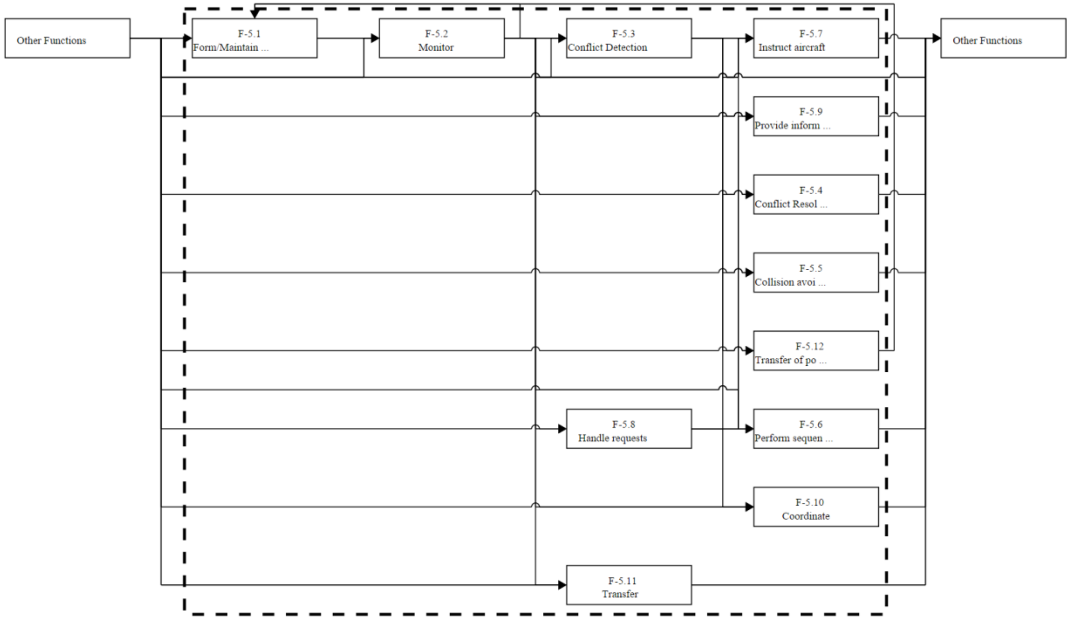
Result

Finally the model is SADT.

Mathematically it is a graph:

- Functions are nodes
- Data flows are arcs





Result

Functions are constituted by sub-functions

Decomposition of function is up to the level where enablers are clearly identified

One can dig deeper and deeper in the model and view details of each function

Result

- To allow readability, only shows links to top level functions or to the function’s own top level

- No “printable drawing” of the complete model
  (but the model is coded / accessible)

- All flows start and end at an existing node

- The framework verifies the model – no loose ends

Result

Started March 2012

Involved already more than 50 people

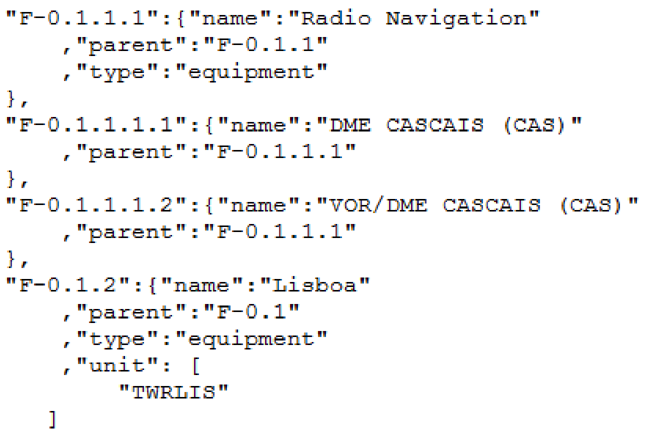
Effort (approximate values – excluding external support):

- 500 m/h (Functional system description)
- 1400 m/h (Architecture + framework)
- 500 m/h (Validation)

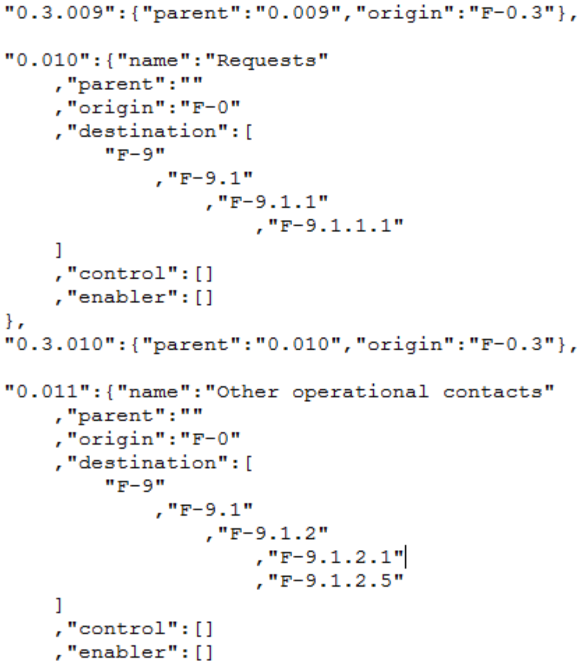
Result

What is the model in reality?

- A bunch of files with data: flows, nodes
- A set of scripts (programs) to read the data



```
"F-0.1.1.1":{"name":"Radio Navigation"
    ,"parent":"F-0.1.1"
    ,"type":"equipment"
},
"F-0.1.1.1.1":{"name":"DME CASCAIS (CAS)"
    ,"parent":"F-0.1.1.1"
},
"F-0.1.1.1.2":{"name":"VOR/DME CASCAIS (CAS)"
    ,"parent":"F-0.1.1.1"
},
"F-0.1.2":{"name":"Lisboa"
    ,"parent":"F-0.1"
    ,"type":"equipment"
    ,"unit": [
        "TWRLIS"
   ]
```



```
"0.3.009":{"parent":"0.009","origin":"F-0.3"},

"0.010":{"name":"Requests"
    ,"parent":""
    ,"origin":"F-0"
    ,"destination":[
        "F-9"
            ,"F-9.1"
                ,"F-9.1.1"
                    ,"F-9.1.1.1"
    ]
    ,"control":[]
    ,"enabler":[]
},
"0.3.010":{"parent":"0.010","origin":"F-0.3"},

"0.011":{"name":"Other operational contacts"
    ,"parent":""
    ,"origin":"F-0"
    ,"destination":[
        "F-9"
            ,"F-9.1"
                ,"F-9.1.2"
                    ,"F-9.1.2.1"
                    ,"F-9.1.2.5"
    ]
    ,"control":[]
    ,"enabler":[]
```

Usage

Defines functional system(s)

Defines system architecture

- For safety analysis
- For interoperability (reg. EC 552/2004)
- To harmonize naming / concepts (e.g. training new staff)
- To specify architecture at each unit

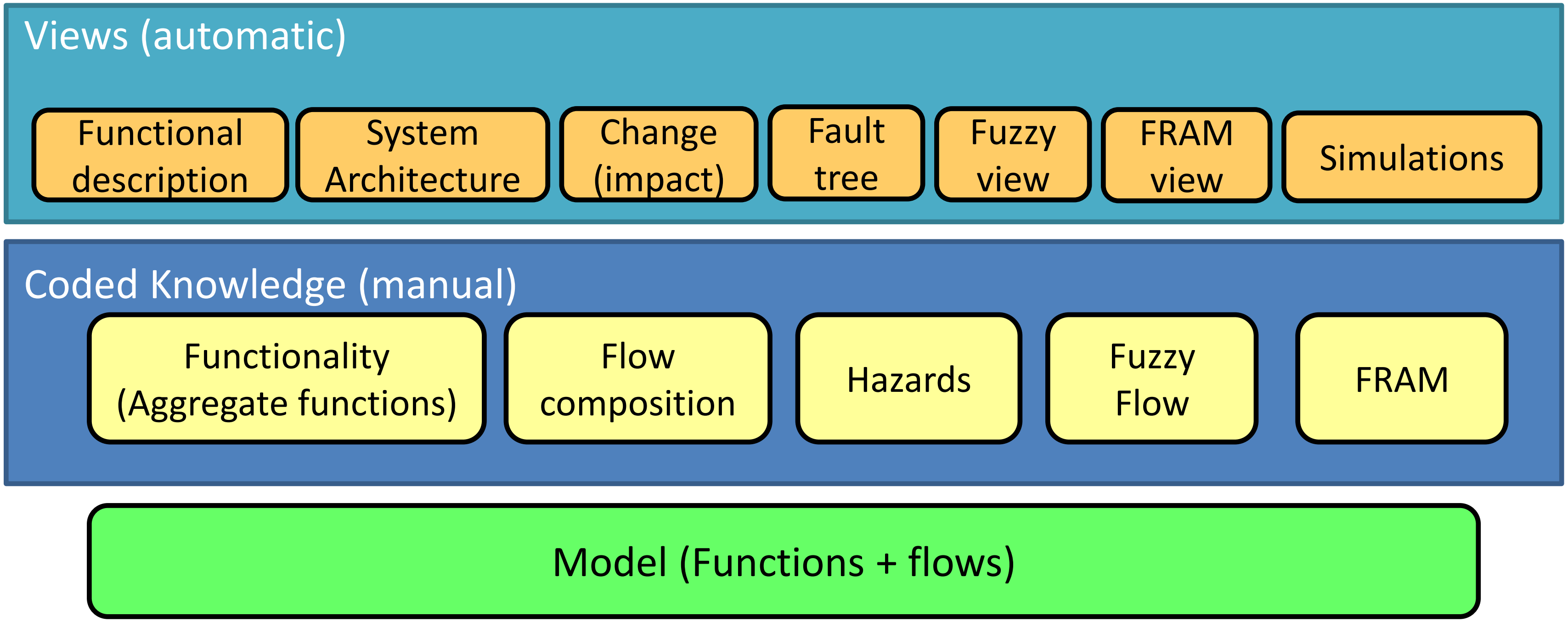
Used for hazard identification (high level - service)

- Used in the Lisboa ACC FHA

Usage

The model (knowledge database) allows:

- Step by step building – integrating new knowledge
- Several views



Views (automatic)

Functional description

System Architecture

Change (impact)

Fault tree

Fuzzy view

FRAM view

Simulations

Coded Knowledge (manual)

Functionality (Aggregate functions)

Flow composition

Hazards

Fuzzy Flow

FRAM

Model (Functions + flows)

Usage

What if others want to use this model?

How to adapt it to another reality?

1. Understand model
2. Check the functions – add / remove as necessary
3. Verify / adapt flows
    - Verify inputs / outputs
    - Verify control
4. Change enablers (architecture)
5. Build in more knowledge

Future

Aggregate flows - simplify model (Status $\subset$ xxxx status)

Apply graph theory to obtain more from the model

- Fuzzy logic layer (allow for more than OK / Unavailable)
- Do simulations (stimulate the model an see what happens)

Integrate dynamics

- FRAM (extra layers with pre-requisites and timing)

Derive hazard causes

- Construct fault trees

Future

To go further we need help!

Questions