Automation of the FRAM method for the purpose of hazard analysis

M. Pielick
Slovenia Control Ltd., Zgornji Brnik, Slovenia

prof. M. Mraz, PhD
Faculty of Computer and Information Science University of Ljubljana, Slovenia

Current way of work

The only acceptable means of compliance to ESARR4 (EC1035/2011) as of today is SAM.

SAM is a toolbox mainly known for its FHA-PSSA-SSA phases:

- Functional Hazard Assessment
- Preliminary System Safety Assessment
- System Safety Assessment

SAM most suitable for hardware changes for which we can have an influence on the design.

Usage much more difficult for many other changes, procedures, airspace etc…

Goal

Slovenia Control is looking into automating FRAM to be used as a complimentary tool in safety assessment process.

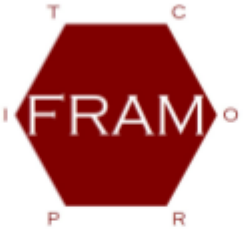
A way to automation is to describe FRAM as a finite state machine. Our goal is to come up with an algorithm.

Technical specifications of application

Feasibility study

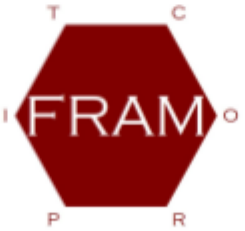
The way ahead: FRAM extensions and add-ons

FRAM combined with other methods



Quantification of FRAM models

Visualisation / animation of FRAM models



Interpretation / simulation of FRAM models

References

Van Kleef. Discrete event simulation of a FRAM model in Simpy. functionalresonance.com.

Martinie et Al. From modelling to performance prediction. SESAR Innovation Days 2013.

Pasquini et Al. Modelling of automation degradation: a case study. Third SESAR Innovation Days.

Patriarca et Al. A Monte Carlo evolution of the functional resonance analysis method (FRAM) to assess performance variability in complex systems. Safety Science 91, 49–60.

Tian et Al. FRAMA: A safety assessment approach based on functional resonance analysis method. Safety Science 85, 41– 52.

Yang et Al. Model-based safety assessment using FRAM for complex systems. ESREL 2015, 3967–3974.

Yang et Al. Safety is an emergent property: Illustrating functional resonance in air traffic management with formal verification. Safety Science 93, 162–177.

Zheng et Al. Refining operation guidelines with model-checking-aided FRAM to improve manufacturing processes: a case study for aeroengine blade forging. Cogn Tech Work 18, 777–791.

Different approaches to automation

1. Discrete event simulation
2. System modeling using a combination of techniques
3. Semi-quantitative approach using Monte Carlo simulation
4. Formal verification with Model checking

Simulation vs quantification

Simulation clarifies the consequences of the relations that are described in the FRAM model, which can then be tested against observations in the real world.

The simulation does not aim at quantification of the model, but merely at identifying the possible scenarios.

Quantification in FRAM can be done on level of variability description

Performance variability of a function

Simple description (only timing and precision) - able to capture most consequences

Elaborate description (speed, distance, sequence, object, force, duration, direction, timing) – allows for a more refined description of consequences

Potential variability

Linked to a function type (e.g. all Technological functions are assigned the same variability)

Assigned to each function separately

Description of performance variability

Current FRAM = qualitative description of performance variability (e.g. Output occurs too late)

Quantification approach = to assign a numerical value to a performance variability state.

Improvement: instead of a static numerical value, variability is more accurately defined by discrete probability distribution functions.

Idea: Could fuzzy sets be used instead of discrete probability distribution?

Description of couplings

Tabular form - one-to-one match

Express the degree of variability with quality

Assign each upstream f. with a weight which represents a relative significance of the function

Assign a specific index to represent damping or amplifying effect of each coupling

Calculated instantiations

In a calculated instantiation FRAM is interpreted as a network or a graph, where the functions are the nodes and the potential couplings are the edges.

Calculated instantiations provide a solution to the practical demands for quantitative results.

Interpreting a FRAM model as a graph or network makes it difficult to consider alternative instantiations using the same model.

Thank you!

miha.pielick@sloveniacontrol.si