A survey of model-based safety analysis

Hong Sun

July 23, 2021

Abstract

Functional safety is an important concept in safety-critical industries like automotive industry, aviation and medical device manufacturing. Safety analysis is mandatory by many regulatory bodies to ensure the final products have no unacceptable risks. Model-based safety analysis has been drawing attention since it allows us to perform the safety analysis, or part of it, automatically. This survey aims at providing a summary of different approaches in model-based safety analysis.

1 Introduction

According to [1], functional safety is defined as the "absence of unreasonable risk due to hazards caused by malfunctioning behavior of electrical/electronic systems". Functional safety analysis is used to evaluate the safety level achieved by the product.

Generally, safety analysis can be classified according to the way they are conducted:

- Inductive analysis methods - bottom-up methods that start from known causes and identify possible effects. For example FMEA - Failure Modes and Effects Analysis
- Deductive analysis methods - top-down methods that start from known effects and seek possible causes. For example FTA - Fault Tree Analysis

Unfortunately, most of the existing safety analysis techniques are highly subjective and dependent on the skill of the practitioner [2]. In the process of model-based development, safety analysis can also be done against the same models created to depict the system. With

the sharing of models between system engineers and safety engineers, we can lower the risk of misinterpretation and miscommunication [2].

The remainder of this survey is organised as follows. Section 2 presents the methodology for finding relative papers. Section 3 summarizes the approaches in model-based safety analysis. Section 4 talks briefly about the future works need to be done.

2 Methodology

Systematic Literature Review (SLR) is used to find the relevant papers in model-based safety analysis. Systematic reviews aim to present a fair evaluation of a research topic by using a trustworthy, rigorous, and auditable methodology [3].

In SLR, we need to figure out how to search the relevant literature. According to [4], an optimum search strategy is expected to provide effective solutions to the following questions.

- **Which** approach to be used in search process (e.g., manual or automated search)?
- **Where** (venues or databases) to search, and which part of article (field) should be searched?
- **What** (subject, evidence type) to be searched, and what are queries (search strings) fed into search engines?
- **When** is the search carried out, and what time span to be searched?

I decided to do an automatic search through search engines like Google Scholar and McMaster library search engine. The key words I used include "model based safety analysis", "model based safety assessment" and "model based safety assurance". To focus on more recent works, I searched only papers published in 2001 or later. The time span is about two decades.

3 Approaches

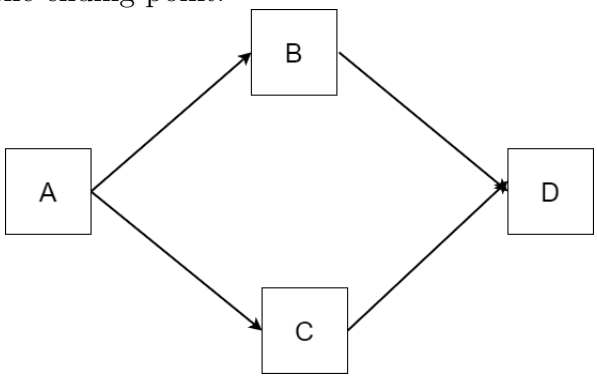
3.1 Modeling systems

3.1.1 Reliability Block Diagram

The idea of Reliability Block Diagram (RBD) is decomposing a system into a group of connected functional blocks. Then we can analyze the reliability of the whole system based on the reliability of every single block.

Typically a RBD looks like a *Directed Acyclic Graph (DAG)*. There is a single starting point and a single ending point.

The following figure shows a simple RBD, with block A representing the starting point and block D representing the ending point.



There are two important concepts associated with RBD - *Minimal Path* and *Minimal Cut*.

- Minimal Path - A path from the starting point to the ending point in RBD. If each of them works, the system works correctly.
- Minimal Cut - A group of blocks in RBD. If the blocks fail together, the system fails.

Generally speaking, we can analyze the RBD in two domains - boolean domain and probability domain [5]. In boolean domain, each block has two states - True or False, representing success or failure respectively. In probability domain, each block is associated with a rate, which means the rate of failure or success. [5] explains the analysis of RBD in boolean domian.

Sometimes the rates of blocks in a RBD change through time. [6] uses Markov Chain to analyse a block diagram.

In my opinion, RBD is a very constrained representation of systems. In reality, we may not be able to model a system as DAG. Also, the rates assigned to the blocks in RBD may not be accurate enough. In the probability domain analysis of RBD, it is always assumed the failure/success rates of blocks are independent. This assumption may not be true in real scenarios.

3.1.2 SysML

According to Object Management Group (OMG), *Systems Modeling Language (SysML)*, is a Domain-Specific Modeling language for systems engineering. It supports the specification, analysis, design, verification and validation of a broad range of systems and systems-of-systems.

There are different diagrams in SysML that can be used in safety analysis. Paper [7] presents an approach that derives RBD from Block Diagrams in SysML. [8] studies how to create a safety model using multiple diagrams in SysML, as well as how to evaluate the hazard propagation.

The lack of formal semantics in SysML presents a hurdle in safety analysis. [9] proposes a framework that extracts model elements from SysML models, then converts the model elements into a formal model using AltaRica [10].

3.2 Modeling safety standards

Modeling the safety standards, such as ISO26262, is a meaningful approach. If we have the metal-model of a standard, we can make an editor in *Eclipse Modeling Framework (EMF)* or some other tools based on the metal-model.

The *Risk Analysis and Assessment Modeling Language (RAAML)* provides a meta-model for some key concepts in ISO26262. RAAML also provides meta-models for *Fault Tree Analysis (FTA)* and *Goal Structuring Notations (GSN)* [11]. All the meta-models in [11] are defined in UML class diagram.

The meta-models mentioned in RAAML focus primarily on concepts instead of processes. There are some papers trying to define the meta-models of processes in safety standards. Paper [12] proposes an approach to extract the meta-model of processes in ISO26262, using *Software and Systems Process Engineering Meta-Model Specification (SPEM)* standard. But

[12] does not provide a complete meta-model for ISO26262.

In my opinion, we still need well defined meta-models for the processes in safety standards. Our WorkflowPlus meta-model may be a good choice for this.

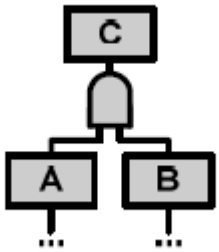
3.3 Incremental Safety

Honestly through my literature search, I did not find sufficient papers to study. The key words that I used in literature search include "incremental safety" and "incremental assurance cases". In this section, I try to conclude what I have found so far.

According to [13], **Incremental Safety** refers to an approach of safety analysis that assesses the safety and risks iteratively through the whole life-cycle of a system. But in each of the iterations, we do not need to re-assess the whole system. Instead, we reuse the results from previous safety analysis.

Ideally, in each iteration of safety assessments, we only add new knowledge. But in reality, we need to introduce *Changes* to the system. Both changes in the design and changes in the understanding of design may trigger a safety assessment. [13] discusses different types of change in safety assessment.

An interesting question that [13] raises is the semantics of safety assessment models, such as the Fault Tree. For example, the following simple Fault Tree can be interpreted as "the combination of conditions A and B leads to C."



But actually, the true meaning of the tree is: "there are no other conditions within the system that can lead to the condition C without both A and B being true". To express the semantics more precisely, I think we can introduce *Tabular Expression* as a complement of the fault tree. Since *Tabular Expression* can put more constraints, such as Completeness and Disjointness, into the Fault Tree model [14]. The downside of using *Tabular Expression* here is we need to maintain the consistence between the safety model and the tabular expression.

[15] provides a formal definition of "lightweight refinement" in safety analysis, using set

theory.

Although Incremental Safety sounds an excellent approach, [16] argues it is not perfect. [16] points out the following pitfalls in the current approach of incremental safety.

- Safety assurance artifacts are not compositional. This is contrary to the incremental design of systems.
- Safety assurance requires a holistic view of the system, but the incremental design of systems only requires local knowledge.

4 Future Works

The papers I have read so far provide some valuable ideas in performing model-based safety analysis. But in my opinion, we still need more examples and statistics to evaluate the efficacy of the approaches. Also different approaches may fit different industries and use cases. More works need to be done to figure out which approach is more useful in a specific area. Last but not least, what I have read is only a small portion in all existing papers. So I still need to read more publications to better understand this topic.

References

[1] *ISO 26262-1:2018(en) Road vehicles — Functional safety — Part 1: Vocabulary.* International Standardization Organization

[2] Joshi, A., Miller, S.P., Whalen, M. and Heimdahl, M.P. (2005) *A proposal for model-based safety analysis.* 24th Digital Avionics Systems Conference (Vol. 2, pp. 13-pp). IEEE.

[3] Kitchenham, B. A. & Charters, S. (2007) *Guidelines for Performing Systematic Literature Reviews in Software Engineering.* Reviews in Software Engineering' (EBSE 2007-001) , Technical report

[4] Zhang, H., Babar, M.A., Tell, P. *Identifying relevant studies in software engineering.* J. Inf. Soft. Technol. 53(6), 625–637 (2011).

[5] R.G. Bennetts (1982) *Analysis of Reliability Block Diagrams by Boolean Techniques.* IEEE TRANSACTIONS ON RELIABILITY, VOL. R-31, NO. 2, JUNE 1982

[6] M. RAMAMOORTY, BALGOPAL (1970) *Block Diagram Approach to Power System Reliability.* IEEE TRANSACTIONS ON POWER APPARATUS AND SYSTEMS, VOL. PAS-89, NO. 5/6

[7] Helle, P. (2012) *Automatic SysML-based safety analysis.* Proceedings of the 5th International Workshop on Model Based Architecting and Construction of Embedded Systems (pp. 19-24).

[8] Zhou, S., Sun, Q. and Jiao, J. (2014) *A safety modeling method based on SysML.* In 2014 10th International Conference on Reliability, Maintainability and Safety (ICRMS) (pp. 1180-1185). IEEE.

[9] Hu, Jun., Tang, Hongying, et. al. *A Model Based Safety Analysis Framework for SysML and A Case Study.* 2019 3rd International Conference on Electronic Information Technology and Computer Engineering (EITCE)

[10] Prosvirnova, Tatiana. (2014). *AltaRica 3.0: a Model-Based approach for Safety Analyses.*

[11] Object Management Group (2021) *Risk Analysis and Assessment Modeling Language (RAAML) Libraries and Profiles, Version 1.0 beta* https://www.omg.org/spec/RAAML

[12] Luo, Yaping, M. Brand, et. al. *Extracting Models from ISO 26262 for Reusable Safety Assurance.* International Conference on Software Reuse 2013

[13] Lisagor, O., Kelly, T (2008) *Incremental safety assessment: Theory and practice.*

[14] A Wassyng, R Janicki (2003) *Tabular expressions in software engineering.* Proceedings of ICSSEA 3, 1-46

[15] Lisagor, O., Bozzano, M., Bretschneider, M., Kelly, T. (2010). *Incremental safety assessment: enabling the comparison of safety analysis results.* 28th International System Safety Conference (ISSC).

[16] Cassano, V., Grigorova, S., et al. (2015) *Is current incremental safety assurance sound* In: Computer Safety, Reliability, and Security - SAFECOMP 2015 Workshops, The Netherlands, September 22, 2015, Proceedings, 22