Advances in Reliability, Safety and Security, Part 1 – Kołowrocki, Dąbrowska (eds.)
 ISBN 978-83-68136-13-5 (printed), ISBN 978-83-68136-00-5 (electronic)

Advances in Reliability, Safety and Security

ESREL 2024
Monograph Book Series

ETFPGs Model Based Safety Assessment Method For Interval-Probabilistic Hybrid Uncertainty System

Wensheng Peng, Zhaoyang Zeng

China Aero-Polytechnology Establishment, Beijing, China

Abstract

In this paper, a system safety assessment method based on evidence theory framework and time failure propagation graphs (ETFPGs) model is proposed for complex systems containing hybrid uncertainty of probability and interval. Firstly, a six-tuple system failure propagation model based on Belief and Plausibility metrics is constructed by using the uncertainty representation and quantification ability of DS Evidence theory, the event trigger conditions and transmit rules of this new failure propagation process are defined. Then, in view of the mixed interval-probability uncertainty information contained in the system, a unified uncertainty representation framework is established based on the basic probability assignment (BPA) function and the interval discretization technique. By using the evidence theory, the belief interval as well as time interval values of the occurrence of failure events in the system could be obtained. Finally, the fault propagation logic in the ETFPGs model is used to solve the final safety assessment of the system. The unified ETFPGs model based safety assessment method can deal with the interval uncertainty information and probabilistic uncertainty information existing in the system at the same time, and it could avoid existed information waste, as well as make use of subjective and empirical information in the process of system design and operation, which could greatly expand the engineering application of failure propagation model. A case study of power supply system of an aircraft flight control processor is carried out to prove the feasibility and engineering adaptability of the method.

Keywords: probability interval, hybrid uncertainty, failure propagation, system safety, evidence theory

1. Introduction

Safety and security have always been the focus of attention in most industry aeries such as transportation, aerospace, nuclear power, etc. System safety modeling and assessment are the main works of safety science and engineering. At present, different system safety assessment methods are conducted in this field, mainly including event based safety assessment methods (such as FHA, FMEA, RBD, FTA, etc.), state based safety assessment methods (such as stochastic Petri net, Monte Carlo simulation), safety assessment methods based on failure propagation (or fault propagation) model (such as FPTN, TFPGs method, HIP-HOP method, etc.). With the increasing integration and complexity of the systems, the event based methods are difficult to completely describe the hazards in the environment and the failure of the systems, and the state based analysis methods extremely rely on the behavior model of the system. More and more attention has been paid to the analysis methods based on failure propagation model, especially time failure propagation graphs(TFPGs) method, which can represent the propagation of failures in the complex system, including the information about the time delay of propagation path and mode constraints. Traditional failure propagation based methods are using probability theory to quantify and evaluate safety information. However, it always being that mix uncertainty information of probability and interval in the same systems in real engineering. This will result in some difficulties to handle this problem with the traditional TFPGs, such as some of the subjective information existing in engineering is difficult to be used, so its application value in the safety assessment can not be exhibited. This paper proposes a system safety modeling and assessment method based on evidence theory and failure propagation for complex systems containing the hybrid uncertainties. This new method uses the quantitative ability of evidence theory for hybrid uncertainty under the unified representing framework, as well as the ability of TFPGs for time failure

propagation. The Evidential TFPGs(ETFPGs) could quantify the uncertainty of evidence considering time failure propagation, and has higher decision value for the evaluation of events affecting safety.

This paper is organized as follows: the first section is introduction, the second section contains briefly introduction of evidence theory and the definition of ETFPGs model, the unified uncertainty representation and quantification of hybrid probability-interval are given in section three as well as the specific steps of the safety assessment method based on ETFPGs, the fourth section is the case study, and the last section is conclusion.

2. Evidence theory and ETFPGs model

2.1. Brief framework of Evidence theory

Basic mass assignment

The frame of discernment is the basic definition in the D-S evidence theory, it is defined by a set of q elements, and these elements are mutually exclusive and exhaustive:

$$\Omega = \{H_1, H_2, \ldots, H_q\} \tag{1}$$

Ω is the finite set of all possible issues where each proposition or hypothesis Hi can support any information from different sources. In the frame of discernment, every subset Ai can be distributed masses on by the sources information:

$$A_i \in 2^{\Omega} : \{\phi, A_1 = \{H_1\}, \ldots, A_q = \{H_q\}, A_{q+1} = \{H_1, H_2\}, \ldots, A_{2^q+1} = \{H_1, \ldots, H_q\}\} \tag{2}$$

A source of information assigns a belief mass between 0 and 1 only on hypotheses A_i on which it has a direct knowledge.

$$0 \le m(A_i) \le 1 \tag{3}$$

This process called basic mass assignment, also as basic probability assignment (BPA) is represented by a function m defined by

$$m : 2^{\Omega} \to [0,1] \tag{4}$$

$$m(\phi) = 0 \tag{5}$$

$$\sum_{A_i \in 2^{\Omega}} m(A_i) = 1 \tag{6}$$

Each A_i supporting $m(A_i)$ 0 is a focal set. The constraint defined on ϕ by (5) is not mandatory. It means that all hypotheses H_i are known, i.e. we are in the context of closed world assumption. The goal of ϕ is to formalize that all hypotheses are not known. In this case, $m(\phi) = 0$ supports this consideration.

Belief and Plausibility measures

In evidence theory, the uncertainty measures of a set of hypotheses or focal sets are a probability interval defined by the belief mass distribution. The lower bound is the measure called belief (*Bel*) and the upper bound is the measure called plausibility *Pl*. The *Bel*(A_i) is the lower bound of a focal set A_i. It is defined as the sum of the belief masses of all subsets B that contribute to A_i such as $B \subseteq A_i$. The *Pl*(A_i) is the sum of all belief masses assigned to subsets B such as $B \cap A_i \neq \varnothing$ and *Bel*(A_i) are defined by the following equations:

$$Pls(A_i) = \sum_{B | A_i \cap B \neq \varnothing} m(B) \tag{7}$$

$$Bel(A_i) = \sum_{B | B \subseteq A_i} m(B) \tag{8}$$

The Plausibility and Belief measures are shown in Figure 1. And the bounding property defined by the following equation:

$$Bel(A_i) \le \Pr(A_i) \le Pls(A_i) \tag{9}$$

where Pr(A_i) defines the occurrence probability of A_i but remains unknown. It can take any value in:

$$\text{Belief Interval} = \left[Bel(A_i), Pls(A_i) \right] \tag{10}$$

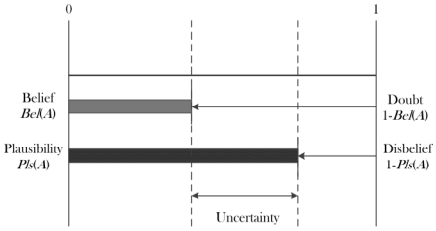

Fig. 1. Plausibility and belief measure.

2.2. Definition of ETFPGs

Formal definition of ETFPGs

According to the objective situation that system components may fail, this paper proposes a new failure propagation model modeling method based on evidential time failure propagation graphs (ETFPGs), which extends the TFPGs model and adds the attribute description of failure occurrence uncertainty to calculate the final hazard occurrence Belief interval as in equation (10).

Directed graph is used to represent the propagation of failure in the system in the ETFPGs, where nodes represent failure modes (root events of failure propagations) and discrepancies (deviations from nominal behavior caused by failure modes). Edges model the temporal dependency between the nodes. They are labeled with propagation delay bounds, and system modes indicating the system configurations in which the propagation is possible. TFPGs are formally defined as follows. The formal definition of ETFPGs model will be given below.

Definition 1: ETFPG

EG represent ETFGs, where the failure propagation model can be defined as a 6-tuple model：

$$EG = \left\langle F, D, E, ET, BI_{fm}, DC \right\rangle \tag{11}$$

where:

- F represents a non-empty finite set of failure modes;
- D is a non-empty finite set of deviations;
- $E \subseteq V \times V$, represents a non-empty finite set of edges, where $V = F \cup D$;
- ET: $E \to T$, represents the mapping between the edge and the propagation time interval, where $[t_{min}, t_{max}] \in \mathrm{I}$, represents the minimum or maximum propagation time on the arc, $\mathrm{I} \in R_{\geq 0} \times \left(R_{\geq 0} \cup \{+\infty\} \right)$, and $t_{\min} \leq t_{\max}$;
- BI_{fm}, $F \to BI$, represents the mapping between failure mode and its occurrence Belief interval;
- DC: $D \to$ {AND, OR} is the mapping that defines the deviation type.

In the directed graph of ETFPGs model, it should be noted that:

(1) In the directed graph ETFPGs, the entry degree of the failure mode node is strictly 0, that is, the failure mode is root event in the process of failure propagation;

(2) The entry degree of any deviation node is at least 1, and the deviation node can be reached from one failure mode node.

(3) There is a loop in the ETFPGs model, but there is no self-cycle or 0 delay cycle.

(4) Only the failure mode node has the Belief interval of occurrence. Since the deviation node expresses that the component or system deviates from the normal behavior due to the failure mode, the deviation node itself does not have the Belief interval of occurrence. When the failure propagates in the system over time, the propagation process can be represented by the states of the failure mode variables and the deviation variables in the ETFPGs model. To indicate which failure mode variable or deviation variable has been activated, *active* state of the node is used. When the failure propagates further through the system, the subsequent deviation will also be set to the *active* state.

Activation conditions of ETFPGs

The activation conditions of nodes and edges in the ETFPGs model can be divided into four cases, and they will be illustrated in following section. It should be noted that in the following figures, the default solid line rectangular view frame represents the failure mode node, the solid line circular view frame represents the or type deviation node, the solid line square view frame represents the and type deviation node, and the dotted line circular view frame represents any node in the ETFPGs model.

(1) Node activation conditions

For any node in the ETFPGs model, when the failure propagates to a certain node *d* with a BI, the node *d* is activated. If and only if the conditions are satisfied:

a: The source node v is activated

b: Edge e is activated in time units of $[t_{\min}(e), t_{\max}(e)]$

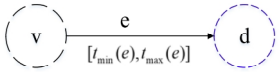

Fig. 2. Activation of the node.

As shown in Figure 2 above, when both node v and edge e are activated, node d is activated

(2) Edge activation conditions

For any edge in the ETFPGs model, if a failure propagates through the edge $e = (v, d)$, if and only if the condition is satisfied:

a. The edge e is active in the whole propagation process;

b. Node d is activated.

(3) Activation condition of OR type deviation node

For the deviation node d of the or type in the ETFPGs model, if any input edge $e = (v, d)$ of the node d is activated at time *t*, and if the failure propagation causes the node *d* to be activated at time t ', the following conditions shall be met:

$$t_{\min}(e) \le t' - t \le t_{\max}(e) \tag{12}$$

where $t_{\min}(e)$ and $t_{\max}(e)$ represents the function $t_{\min}$ and $t_{\max}$ of the edges *e*

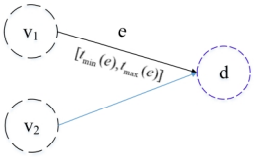

Fig. 3. Activation of OR type deviation node.

As shown in Figure 3, any leading node (such as node v_1) of the OR type deviation node *d* and the edge *e* that propagates to the node d are activated, then the OR type deviation node d will also be activated.

(4) Activation condition of AND deviation node

For the node d of AND type in the ETFPGs model, if the failure propagation causes the node *d* to be activated at time t', then the following conditions should be met:

a. $t_{\min}(e) \le t' - t$, *t* represents a certain time, each input edge $e = (v, d)$ has been activated;

b. For at least one input edge e, there must be $t' - t \le t_{\max}(e)$, it means that any other edges (except one edge) can exceed the upper limit.

As shown in Fig. 4, the AND type deviation node d can be activated only when all the leading nodes (such as nodes v_1 and v_2) of the AND type deviation node d and its edge *e* are activated.

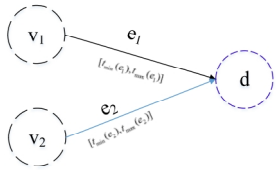

Fig. 4. Activation of AND type deviation node.

3. System safety assessment method for hybrid uncertainty system

3.1. Unified representation of hybrid uncertainties

Although evidence theory was originally used to quantify cognitive uncertainty information, in many cases in engineering, in addition to cognitive uncertainty variables, there are also random variables in a model. In the case of both cognitive and random uncertain variables, one approach (Eldred) is to process the mixed uncertain variables into a two-layer optimization model. Another method (Shah) is to discretize random variables into a set of finite intervals according to the characteristics of probability distribution.

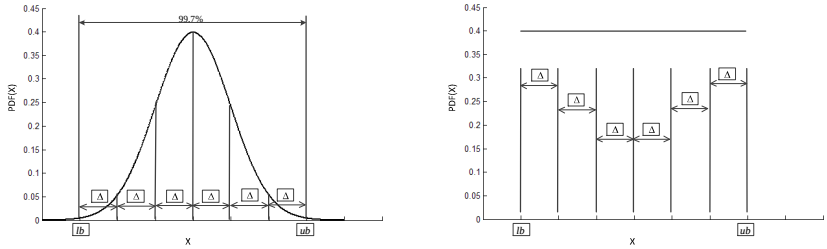

Fig. 5. Discretization of normal and uniform distributions.

In this paper, random variables are discretized into a set of finite intervals, and then BPA is assigned to each interval according to its distribution characteristics. The process of discretization of random variables depends on the amount required to accurately cover the uncertain region in the evidence structure. For example, for a random variable that follows a uniform distribution, you can discretize the random variable evenly between n cells, and then assign 1/*n* BPA to each subinterval. In order to discretize a normally distributed random variable, we need to define the upper and lower boundaries of the forward variables. Figure 2 shows the discretization process of a standard normally distributed random variable and a uniformly distributed random variable. For normal random variables, the mean is 0 and the standard deviation is 1. According to the 3σ principle of the standard normal distribution, that is, within a range, the probability values of 99.7% can be included. Thus, one can act as the upper and lower boundary points of a discrete set, and then uniformly discretize the variables within this range. However, for the assignment of BPA between each cell, the following formula can be solved and assigned according to the characteristics of Gaussian distribution.

$$P(a, X < b) = \int_a^b f(X)dx$$

$$where \quad f(X) = \frac{1}{\sigma\sqrt{2\pi}} \exp \frac{1(X-\mu)^2}{2\sigma^2} \tag{13}$$

where a and b represent the upper and lower bounds of the subinterval, and $P(a<X<b)$ represents the probability value of X within the range of a and b.

In order to make the sum of BPA equal to 1, the BPA is normalized.

$$m_i' = \frac{m_i}{\sum_{i=1}^{n} m_i} \tag{14}$$

3.2. The process of the system safety method based on the ETFPGs for the hybrid uncertainty system

Section 2.2 introduces the model of ETFPGs. This section will give the general process of system safety modeling and assessment method based on ETFPGs model.

ETFPGs represent the propagation of failure in the system in the form of a directed graph. When a component fails, the failure propagation will also affect the components that depend on it. How to realize the construction of ETFPGs model in the context of system structure and safety related requirements has become a key point. The general steps of safety assessment method based on ETFPGs model are as shown in Figure 6, and given below.

Step 1: Get the structure information of the system according to the design documents of the system, including the component composition of the system, the dependency relationship between components, etc;

Step 2: Obtain relevant information such as failure mode, deviation and failure propagation delay according to the requirements related to system safety

Step3: Identify and classify the uncertainty information in the system, including aleatory uncertainty class variable A and epistemic uncertainty class variable B, and normalize the mixed uncertainty information to obtain the interval form and BPA of all variables.

Step 4: Determine the quantitative information related to the system safety, quantify the information based on the evidence theory, and form the quantitative Belief interval value of the uncertainty degree of the failure occurrence of the failure mode;

Step 5: Analyze the failure propagation process according to the structure of the system, such as the dependency relationship between components. Building the logical relationship of the failure propagation. By default, the logical relationship of the deviation is OR. If there is a current deviation that requires the front nodes (not less than two front nodes) to be activated, the logical relationship of the current deviation is AND.

Step 6: Based on the logical architecture of the system, the safety assessment and calculation of the hazardous events are carried out to obtain the Belief Interval value and propagation time value of the top event.

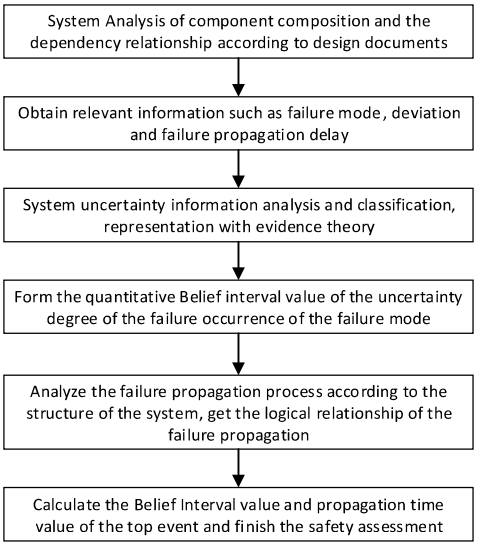

Fig. 6. The process of safety assessment method.

There are two points should be noted during ETPGs modeling:

1) It is necessary to determine whether the current node is a failure node or a deviation node

2) If the current node is a deviation node, it should need to determine whether the node is OR node or AND node.

4. Case study

Taking the power supply system of an aircraft flight control processor as an example, the safety modeling and analysis of the power supply system of the processor are carried out by using the ETFPGs method. The power supply system of the processor includes 3 special generators, 3 batteries and 5 sensors, wherein the special generators charge the batteries, the batteries supply power to the sensors, and the sensors output the collected data to the processor. Where Reference1(R1) and Reference2(R2)are signal processing systems. For R1, if the difference between the data output from Sensor2(S2) and Sensor3(S3) is not large, R1 comprehensively collates the data output from S2 and S3 and provides a parameter processor. Similarly, for R2, if the difference between the data output from Sensor4(S4) and Sensor5(S5) is not large, R2 comprehensively processes the data output from S4 and S5 and then provides a parameter to the processor. According to the existed experience information , the G2,S3 and S5 has the aleatory uncertainty information, and other components only have epistemic uncertainty information.

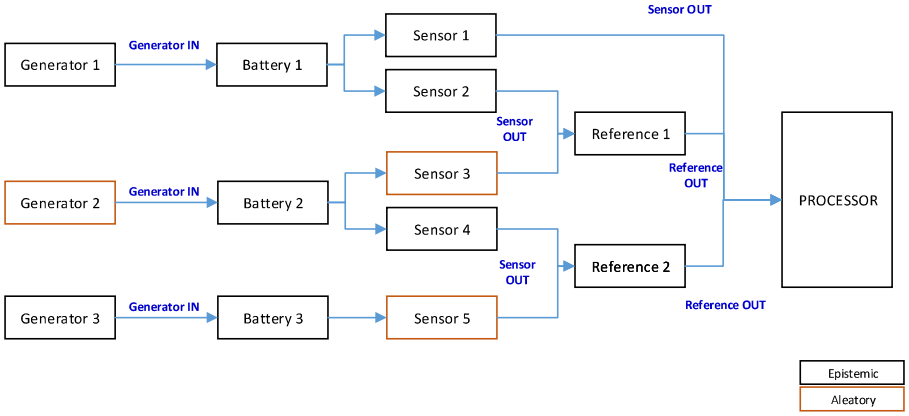

Fig. 7. Structure of the flight control power supply system.

Main failure modes of the system

Through the use experience in the project, it is found that during the operation of the power supply system, the generator and sensor are prone to fault. Therefore, this case takes the generator and sensor as the fault source to conduct the safety modeling analysis of the power supply system. The fault modes of generator and sensor are defined in the following table. Failure of the generator will cause permanent loss of power supply to the system, and failure of the sensor will cause permanent loss of its reading and no output value.

Table 1. the node type in the ETFPGs.

Component	Type of nodes	Failure modes	Failure effect	Symbol in the model
Generator	Failure node	Permanent damage of generator	Stop the power supply	G_{off}
Sensor	Failure node	The sensor is damaged	Stop the data supply	S_{NO}
Battery	Deflection mode			B_{LOW}
Reference	Deflection mode			R_{NO}

Failure propagation process and safety analysis

After the generator fails, the battery starts to discharge. When the power is exhausted, the corresponding sensor will stop working. If both S2 and S3 fail, R1 fails. Similarly, if both S4 and S5 fail, R2 also fails. When S1 has no output and R1 and R2 fail, the processor system fails, resulting in system damage.

Therefore, the deviation nodes of the system include: nodes of all batteries, R1 and R2, and processor nodes.

According to above uncertainty classification types, it could be seen that the nodes of G1, G3, S1, S2, S4 are given epistemic uncertainty information directly. Through the quantitative analysis of the basic element and basic belief assignment function of the generator damage event, the basic element and basic belief assignment function of the sensor fault, the Belief interval of these failure event is obtained as follows:

BI_{G1}=[0.28,0.32]; BI_{G3}=[0.24,0.26]; BI_{S1}=[0.15,0.17]; BI_{S2}=[0.11,0.15]; BI_{S4}=[0.12,0.14].

For the nodes of G2, S3, S4, they obey normal distribution N(0.37,0.02^2), N(0.13,0.013^2), N(0.72,0.01^2) respectively, and after the discretization process, the Belief intervals are as follows:

BI_{G2}=[0.36,0.38];BI_{S3}=[0.11,0.15]; BI_{S5}=[0.05,0.10]

Then ,the quantification failure propagation model of the whole system is as shown in Figure 8.

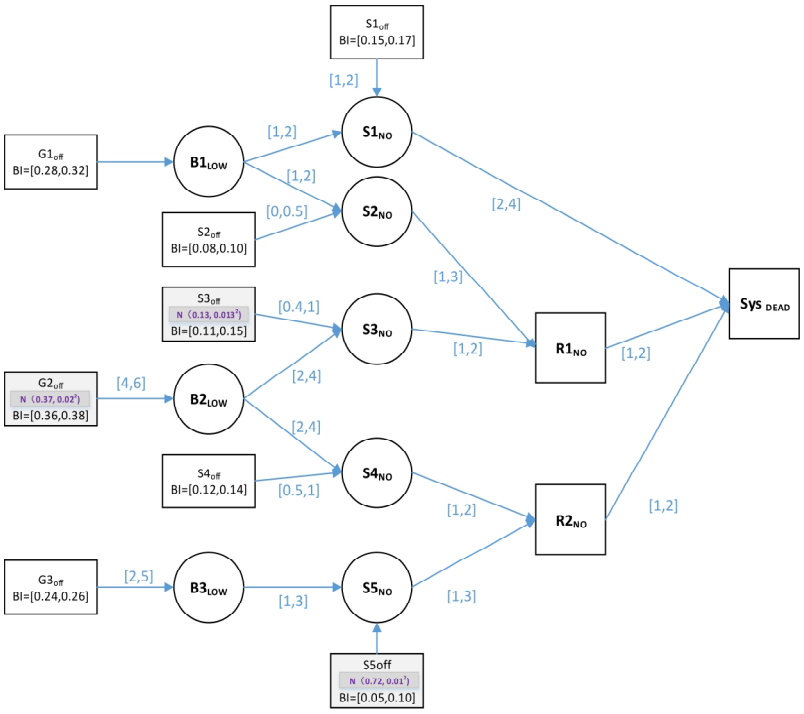

Fig. 8. EFTPGs of the FC power supply system.

Through the analysis of all failure propagation paths, it is found that {$G1_{off}$, $G2_{off}$, $G3_{off}$} has the highest occurrence belief, which is BI= [0.65,0.68], but its propagation time is long, which is [10,14], while {$S1_{off,}$ $S2_{off}$, $S3_{off}$, $S4_{off}$, $S5_{off}$} has the shortest propagation time [3.6], and the occurrence belief is also low BI=[0.12,0.16].

5. Conclusion

Based on the time failure propagation graph model and evidence theory, this paper proposes a system safety assessment method of evidential time failure propagation graph for complex system with hybrid uncertainty of probabilistic and interval. This method uses the evidence theory to quantify the uncertainty of the occurrence of failure events in the cases of limited samples as well as sufficient samples. and the belief interval measurement is used to get the uniform uncertainty quantification of for the occurrence of different failures in the propagation process. By describing the failure propagation time, this method can obtain the propagation time of different failures in complex systems and the belief interval of failure occurrence. ETFPGs model can not only reduce the limitation of assumptions caused by the lack of statistical information in some components, but also make use of some subjective information in engineering, and meanwhile avoid to waste the existed statistical information. This safety assessment method could provide an effective quantification way for the mixed uncertainty system in real engineering.

Acknowledgements

The work in this paper was supported by National Natural Science Foundation of China(72131002).

References

Abdelwahed S, Karsai G, Mahadevan N, et al. 2009. Practical implementation of diagnosis systems using timed failure propagation graph models. IEEE Transactions on instrumentation and measurement, 58(2), 240-247.

Bittner B, Bozzano M, Cimatti A. 2017. Timed Failure Propagation Analysis for Spacecraft Engineering: The ESA Solar Orbiter Case Study. International Symposium on Model-Based Safety and Assessment, 255-271

Bittner, B., Bozzano, M., Cimatti, A., Zampedri, G. 2016. Automated Verification and Tightening of Failure Propagation Models. In: Proceedings of the 30th AAAI Conference on Artificial Intelligence (AAAI 2016)

Eldred M S, Swiler L P, Tang G. 2011. Mixed aleatory-epistemic uncertainty quantification with stochastic expansions and optimization-based interval estimation. Reliab Eng Syst Saf 96,1092–113.

Flaus, Jeancmarie. 2013. Preliminary Hazard Analysis. John Wiley & Sons, Inc. NY

Library, 2015 World Public. Reliability block diagram.

Ruijters E, Stoelinga M. 2015. Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools. Computer science review, 15-16(03), 29-62.

Shah H R, Hosder S, Winter T. A mixed uncertainty quantification approach with evidence theory and stochastic expansions. In: AIAA Sci Tech 2014, National Harbor, MD AIAA Paper 2014-0298.

Technometrics H J. 2003. Failure Mode and Effect Analysis: FMEA From Theory to Execution 38(1), 80-80.

Zhang Z D. 2009. Monte Carlo simulation of an antiproton annihilation detector system. Chinese Science Bulletin 54(19, 3494.