Behavioral fault modeling and analysis with SBIP: A Wheel Brake System Case Study

1st Xudong Tang
Shanghai Key Lab for Trustworthy Computing
East China Normal University
Shanghai, China
51184501045@stu.ecnu.edu.cn

2nd Qiang Wang
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

3rd Weikai Miao
dept. name of organization (of Aff.)
name of organization (of Aff.)
Shanghai, China
wkmiao@sei.ecnu.edu.cn

***Abstract*—Behavior-Interaction-Priority(BIP) is a component-based framework for modeling complex systems. According to BIP framework, system can be represented by a set of components specifying the behavior which is synchronized and communicated by connectors that corresponds to subset of interactions. Behavioral fault modeling and analysis refers to an integration of model based system design and safety analysis. In this paper, we integrate fault-tree-based safety analysis into BIP model and using statistical model checking engine for the BIP framework(SBIP) to offer a stochastic information to components and the entire system. By using SBIP with statistic model checking, we verify system specification and calculate probability of fault issues. We also trace the simulation result to confirm the extended system model without fault keeps consistence of the norminal system model. We illustrate an airplane wheel brake system meeting the industry standards as case study to show its advantage in analyzing fault behavior of safety-critical systems in aerospace practice.**

***Index Terms*—model checking, safety analysis, fault tree, BIP**

I. Introduction

Giving introduction of BIP framework, BIP toolset, SBIP and, on the other hand, faulttree-based safety analysis. Using structure of the paper as ending.

II. Preliminaries

A. The BIP Framework

We use architecture diagrams [] to model the architecture styles in BIP. An architecture diagram consists of a set of component types, with associated cardinality constraints representing the expected number of instances of each component type and a set of connector motifs. Connector motifs, which define sets of BIP connectors, are non-empty sets of port types, each labelled as either a trigger or a synchron. Each port type has a cardinality constraint representing the expected number of port instances per component instance and two additional constraints: multiplicity and degree, represented as a pair m : d. Multiplicity constrains the number of instances of the port type that must participate in a connector defined by the motif; degree constrains the number of connectors attached to any instance of the port type.

In this section, we present the BIP model with multiparty synchronization and data transfer.A BIP model is a parallel composition of a set of components. A BIP component is formally defined as an automaton extended with linear integer arithmetic as follows.

Definition 1 (BIP component): Given a finite set of variables $\mathbb{V}$, a BIP component is defined as a tuple $B = \langle \mathbb{V}, \mathbb{L}, \mathbb{P}, \mathbb{E}, \ell \rangle$, where 1) $\mathbb{L}$ is a finite set of control locations; 2) $\mathbb{P}$ is a finite set of communication ports; 3) $\mathbb{E} \subseteq \mathbb{L} \times \mathbb{P} \times \mathcal{F}_{\mathbb{V}} \times \mathcal{E}_{\mathbb{V}} \times \mathbb{L}$ is a finite set of transition edges extended with guards in $\mathcal{F}_{\mathbb{V}}$ and operations in $\mathcal{E}_{\mathbb{V}}$; 4) $\ell \in \mathbb{L}$ is an initial control location.

Transition edges in a component are labeled by ports, which form the interface of the component. We assume that, from each control location, every pair of outgoing transitions have different ports, and the ports of different components are disjoint. In other words, transitions with the same ports in the component are not enabled simultaneously. Given a component violating such assumptions, one can easily transform it into the required form by renaming the ports, while retaining the BIP expressiveness power. To ease the presentation, we denote in the sequel the id of the unique component where port p is defined by $id(p)$.

We denote by $\mathcal{B} = \{B_i \mid i \in [1, n]\}$ a set of components. In BIP, coordinations of components are specified by using interactions.

Definition 2 (Interaction): An interaction for $\mathcal{B}$ is a tuple $\gamma = \langle g, \mathcal{P}, f \rangle$, where $g \in \mathcal{F}_{\mathbb{V}}$, $f \in \mathcal{E}_{\mathbb{V}}$ and $\mathcal{P} \subseteq \bigcup_{i=1}^{n} \mathbb{P}_i$, $\mathcal{P} \neq \emptyset$, and for all $i \in [1, n]$, $|\mathcal{P} \cap \mathbb{P}_i| \leq 1$.

Intuitively, an interaction defines a guarded multiparty synchronization with data transfer: when the guard g of an interaction $\mathcal{P}$ is enabled, then the data transfer specified by f can be executed, and after that the transitions labelled by the ports in γ can be taken simultaneously. We denote by Γ a finite set of interactions. A BIP model is constructed by composing a number of components with interactions.

*Definition 3 (*BIP *Model):* A BIP model $\mathcal{M}_{\text{BIP}}$ is a tuple $\langle \mathcal{B}, \Gamma \rangle$, where $\mathcal{B}$ is a finite set of components, and Γ is a finite set of interactions for $\mathcal{B}$.

We do not take priority into account in this paper, as in the previous work [**?**], [**?**], since adding priority will not introduce any errors. If a model without priority is safe, then after adding priority constraints it remains safe. We use a simple mutual exclusion protocol to illustrate BIP.

A state of a BIP model is a tuple $c = \langle \langle l_1, \mathbf{V}_1 \rangle, \ldots, \langle l_n, \mathbf{V}_n \rangle \rangle$, where for all $i \in [1, n]$, $l_i \in \mathbb{L}_i$

and $\mathbf{V}_i$ is a valuation of $\mathbb{V}_i$. A state c_0 is initial if for all $i \in [1, n]$, $l_i = \ell_i$ and $\mathbf{V}_i$ is the initial valuation of $\mathbb{V}_i$. A state c is an error if for some $i \in [1, n]$, l_i is an error location. We say an interaction $\gamma \in \Gamma$ is enabled on a state c if for every component $B_i \in \mathcal{B}$, such that $\gamma \cap \mathbb{P}_i \neq \emptyset$, there is an edge $\langle l_i, \gamma \cap \mathbb{P}_i, g_i, f_i, l_i' \rangle \in \mathbb{E}_i$ and $\mathbf{V}_i \models g_i$. The labeled transition system semantics of a BIP model is defined as follows.

*Definition 4 (*BIP *operational semantics):* Given a BIP model $\mathcal{M}_{\text{BIP}} = \langle \mathcal{B}, \Gamma \rangle$, its operational semantics is defined by a labeled transition system $\mathcal{T}_{\text{BIP}} = \langle \mathcal{C}, \Sigma, \mathcal{R}, \mathcal{C}_0 \rangle$, where

1) $\mathcal{C}$ is the set of states,
2) $\Sigma = \Gamma$,
3) $\mathcal{R}$ is the set of transitions, and we say that there is a transition from a state c to another state c', if there is an interaction γ such that,
   a) γ is enabled in c;
   b) for all $B_i \in \mathbb{B}$ such that $\gamma \cap \mathbb{P}_i \neq \emptyset$, there is an edge $\langle l_i, \gamma \cap \mathbb{P}_i, g_i, f_i, l_i' \rangle \in \mathbb{E}_i$, then $\mathbf{V}_i' = \mathbf{V}_i[\mathbb{V}/f_i(\mathbb{V})]$;
   c) for all $B_i \in \mathbb{B}$ such that $\gamma \cap \mathbb{P}_i = \emptyset$, $l_i' = l_i$ and $\mathbf{V}_i' = \mathbf{V}_i$.
4) $\mathcal{C}_0$ is the set of initial states.

In this paper, we do not use temporal logics to specify safety properties, but recognize a set of locations as error locations. A BIP model is safe if no error states are reachable. Notice that any safety property can be encoded as a reachability problem by necessarily creating additional components.

B. Statistical Model Checking

Giving an introduction of Statistical Model Checking here.

III. The AIR6110 Wheel Brake System

The Wheel Brake System(WBS) description is introducted in Aerospace Information Report 6110(AIR6110)[] as a contiguous aircraft system development process example. According to AIR6110 standard, WBS is a detailed funciton of an aircraft designated model S18. The hypothetical S18 aircraft is a two engine passenger aircraft designed to carry 300 to 350 passengers up to 5000 nautical miles at 0.84 mach, and has an average flight duration of 5 hours. The WBS provides braking on the main gear wheels used to provide safe retardation of the aircraft during taxiing and landing phases, and in the event of a rejected take-off. The wheel brakes also prevent unintended aircraft motion when parked, and may be used to provide differential braking for aircraft directional control. A secondary function of the WBS is to stop main gear wheel rotation upon gear retraction. Braking on the ground is commanded manually, via brake pedals, or automatically (autobrake) without the need for pedal application.

Figure 1 shows the WBS BIP model of the nominal behavior. The WBS is composed of an electronic control system and a physical system. The majority of the electronic control system is Braking System Control Unit(BSCU). The WBS receives several signals including the brake pedal position from upper level avionics system and electically forwards them to the BSCU. The BSCU also receives two power inputs from

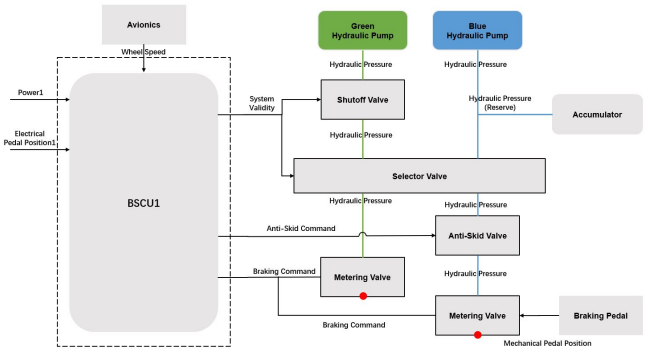

Fig. 1. The WBS BIP model of the nominal behavior

two independent power supply resources. As the result of computation, the BSCU in turn produces the system validity command, anti-skid command and braking command to the physical system. The physical system includes two hydraulic pressure lines which are supplied by the green/blue hydraulic pump respectively.

Operation Mode. There are three operation modes for physical system. In *normal mode*, the wheel brake is supported by the main hydraulic circuit, refers to the green hydraulic circuit. In *alternate mode*, the wheel brake is supported by a second hydraulic circuit. This mode is standby and is selected automatically when the normal system fails. An accumulator supplies the *emergency mode* when blue hydraulic supply is lost and the normal mode is not available.

Braking System Control Unit(BSCU). According to the AIR6110 standard, for redundancy, the BSCU is composed of two independent channels, each channel has its own power supply and avioncs system inputs. Each channel has a command subsystem and a monitor subsystem. The monitor system generates the system validity command and the command system cauculates the anti-skid command and braking command. The BSCU will make an ultimate judgement call between each command output by the two channels respectively.

Hydraulic Pump. In nominal system behavior, both the green and blue hydraulic pumps provide enough hydraulic pressure for their green/blue hydraulic circuit respectively. An accumulator is also a hydraulic pump to provide an emergency reserve of hydraulic pressure for blue hydraulic circuit in emergency mode.

Shutoff Valve. The shutoff valve responds the system validity command from BSCU to decide whether to apply the hydraulic pressure to the selector valve in green hydraulic circuit or not. The system validity command is modeled in BIP as a boolean value.

Selector Valve. The selector valve control the switch between green and blue hydraulic circuits mechanically. It outputs appropriate pressure from green hydraulic pump, and switches to blue hydraulic circuit as soon as it detects a lack of pressure in the green hydraulic circuit. In BIP model, the component selector valve only outputs pressure from either the

green hydraulic circuit input or blue hydraulic circuit input at a time.

Anti-Skid Valve. The anti-skid valve follows anti-skid command to control hydraulic pressure to the metering valve. It is used to restrict the hydraulic pressure to the wheel brake in order to prevent locking of the wheel. Wheel skid happens when the wheel is locked but the vehicle keeps a relative slid speed to the ground. We consider a loss of anti-skid function as a fault and will integrate it into nominal BIP model.

Metering Valve. Metering valve, or metering servo valve controls pressure to the demanded level and provides regulation for the anti-skid function.

IV. Integrating Fault Trees Into WBS BIP model

Before you begin to format your paper, first write and save the content as a separate text file. Complete all content and organizational editing before formatting. Please note sections IV-A–IV-E below for more information on proofreading, spelling and grammar.

Keep your text and graphic files separate until after the text has been formatted and styled. Do not number text heads—LaTeX will do that for you.

A. Abbreviations and Acronyms

Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, ac, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

B. Units

- Use either SI (MKS) or CGS as primary units. (SI units are encouraged.) English units may be used as secondary units (in parentheses). An exception would be the use of English units as identifiers in trade, such as "3.5-inch disk drive".
- Avoid combining SI and CGS units, such as current in amperes and magnetic field in oersteds. This often leads to confusion because equations do not balance dimensionally. If you must use mixed units, clearly state the units for each quantity that you use in an equation.
- Do not mix complete spellings and abbreviations of units: "Wb/m^2" or "webers per square meter", not "webers/m^2". Spell out units when they appear in text: ". . . a few henries", not ". . . a few H".
- Use a zero before decimal points: "0.25", not ".25". Use "cm^3", not "cc".)

C. Equations

Number equations consecutively. To make your equations more compact, you may use the solidus (/), the exp function, or appropriate exponents. Italicize Roman symbols for quantities and variables, but not Greek symbols. Use a long dash rather than a hyphen for a minus sign. Punctuate equations with commas or periods when they are part of a sentence, as in:

$$a + b = \gamma \tag{1}$$

Be sure that the symbols in your equation have been defined before or immediately following the equation. Use "(1)", not "Eq. (1)" or "equation (1)", except at the beginning of a sentence: "Equation (1) is . . ."

D. LaTeX-Specific Advice

Please use "soft" (e.g., `\eqref{Eq}`) cross references instead of "hard" references (e.g., `(1)`). That will make it possible to combine sections, add equations, or change the order of figures or citations without having to go through the file line by line.

Please don't use the `{eqnarray}` equation environment. Use `{align}` or `{IEEEeqnarray}` instead. The `{eqnarray}` environment leaves unsightly spaces around relation symbols.

Please note that the `{subequations}` environment in LaTeX will increment the main equation counter even when there are no equation numbers displayed. If you forget that, you might write an article in which the equation numbers skip from (17) to (20), causing the copy editors to wonder if you've discovered a new method of counting.

BibTeX does not work by magic. It doesn't get the bibliographic data from thin air but from .bib files. If you use BibTeX to produce a bibliography you must send the .bib files.

LaTeX can't read your mind. If you assign the same label to a subsubsection and a table, you might find that Table I has been cross referenced as Table IV-B3.

LaTeX does not have precognitive abilities. If you put a `\label` command before the command that updates the counter it's supposed to be using, the label will pick up the last counter to be cross referenced instead. In particular, a `\label` command should not go before the caption of a figure or a table.

Do not use `\nonumber` inside the `{array}` environment. It will not stop equation numbers inside `{array}` (there won't be any anyway) and it might stop a wanted equation number in the surrounding equation.

E. Some Common Mistakes

- The word "data" is plural, not singular.
- The subscript for the permeability of vacuum μ_0, and other common scientific constants, is zero with subscript formatting, not a lowercase letter "o".
- In American English, commas, semicolons, periods, question and exclamation marks are located within quotation marks only when a complete thought or name is cited, such as a title or full quotation. When quotation marks are used, instead of a bold or italic typeface, to highlight a word or phrase, punctuation should appear outside of the quotation marks. A parenthetical phrase or statement at the end of a sentence is punctuated outside of the closing parenthesis (like this). (A parenthetical sentence is punctuated within the parentheses.)
- A graph within a graph is an "inset", not an "insert". The word alternatively is preferred to the word "alternately" (unless you really mean something that alternates).

- Do not use the word “essentially” to mean “approximately” or “effectively”.
- In your paper title, if the words “that uses” can accurately replace the word “using”, capitalize the “u”; if not, keep using lower-cased.
- Be aware of the different meanings of the homophones “affect” and “effect”, “complement” and “compliment”, “discreet” and “discrete”, “principal” and “principle”.
- Do not confuse “imply” and “infer”.
- The prefix “non” is not a word; it should be joined to the word it modifies, usually without a hyphen.
- There is no period after the “et” in the Latin abbreviation “et al.”.
- The abbreviation “i.e.” means “that is”, and the abbreviation “e.g.” means “for example”.

An excellent style manual for science writers is [7].

F. Authors and Affiliations

The class file is designed for, but not limited to, six authors. A minimum of one author is required for all conference articles. Author names should be listed starting from left to right and then moving down to the next line. This is the author sequence that will be used in future citations and by indexing services. Names should not be listed in columns nor group by affiliation. Please keep your affiliations as succinct as possible (for example, do not differentiate among departments of the same organization).

G. Identify the Headings

Headings, or heads, are organizational devices that guide the reader through your paper. There are two types: component heads and text heads.

Component heads identify the different components of your paper and are not topically subordinate to each other. Examples include Acknowledgments and References and, for these, the correct style to use is “Heading 5”. Use “figure caption” for your Figure captions, and “table head” for your table title. Run-in heads, such as “Abstract”, will require you to apply a style (in this case, italic) in addition to the style provided by the drop down menu to differentiate the head from the text.

Text heads organize the topics on a relational, hierarchical basis. For example, the paper title is the primary text head because all subsequent material relates and elaborates on this one topic. If there are two or more sub-topics, the next level head (uppercase Roman numerals) should be used and, conversely, if there are not at least two sub-topics, then no subheads should be introduced.

H. Figures and Tables

a) Positioning Figures and Tables: Place figures and tables at the top and bottom of columns. Avoid placing them in the middle of columns. Large figures and tables may span across both columns. Figure captions should be below the figures; table heads should appear above the tables. Insert figures and tables after they are cited in the text. Use the abbreviation “Fig. 2”, even at the beginning of a sentence.

TABLE I
TABLE TYPE STYLES

Table Head	**Table Column Head**		
	Table column subhead	***Subhead***	***Subhead***
copy	More table copy[a]		

[a]Sample of a Table footnote.

Fig. 2. Example of a figure caption.

Figure Labels: Use 8 point Times New Roman for Figure labels. Use words rather than symbols or abbreviations when writing Figure axis labels to avoid confusing the reader. As an example, write the quantity “Magnetization”, or “Magnetization, M”, not just “M”. If including units in the label, present them within parentheses. Do not label axes only with units. In the example, write “Magnetization (A/m)” or “Magnetization {A[m(1)]}”, not just “A/m”. Do not label axes with a ratio of quantities and units. For example, write “Temperature (K)”, not “Temperature/K”.

V. Verification Methodology and Experiments

Acknowledgment

The preferred spelling of the word “acknowledgment” in America is without an “e” after the “g”. Avoid the stilted expression “one of us (R. B. G.) thanks . . .”. Instead, try “R. B. G. thanks. . .”. Put sponsor acknowledgments in the unnumbered footnote on the first page.

References

Please number citations consecutively within brackets [1]. The sentence punctuation follows the bracket [2]. Refer simply to the reference number, as in [3]—do not use “Ref. [3]” or “reference [3]” except at the beginning of a sentence: “Reference [3] was the first . . .”

Number footnotes separately in superscripts. Place the actual footnote at the bottom of the column in which it was cited. Do not put footnotes in the abstract or reference list. Use letters for table footnotes.

Unless there are six authors or more give all authors’ names; do not use “et al.”. Papers that have not been published, even if they have been submitted for publication, should be cited as “unpublished” [4]. Papers that have been accepted for publication should be cited as “in press” [5]. Capitalize only the first word in a paper title, except for proper nouns and element symbols.

For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation [6].

REFERENCES

[1] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] K. Elissa, "Title of paper if known," unpublished.

[5] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.