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.

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.

A. The WBS architecture and nominal behavior

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 two independent power supply resources. As the result of computation, the BSCU in turn produces the system validity

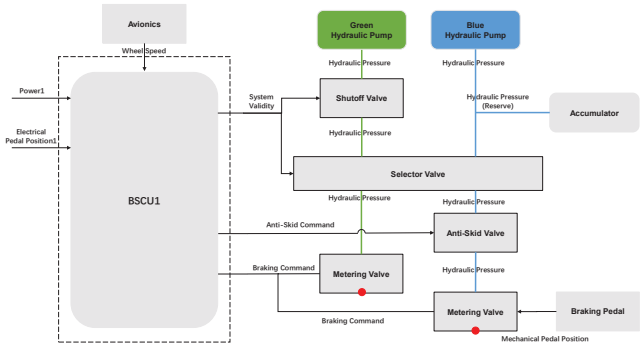

Fig. 1. The WBS BIP model of the nominal behavior

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.

B. The WBS BIP architecture development process

According to the AIR6110 standard, the system architecture evolves throughout the development life cycle and is tightly coupled with the requirements development (especially interface requirements) and is not finished until the requirements associated with the architecture have been validated.

We follow the standard to advance our BIP model. As a result, our WBS BIP model has four versions corresponding to the four architectures in the AIR6110 standard. They are numbered from ARCH1 to ARCH4. Each architecture is obtained after design choices of different types.

ARCH1. The architecture one is regarded as a high level wheel brake system architecture to be analyzed against the system level functions operational and safety requirements, and any design constraints that have been identified early in the standard.

ARCH2. Modified braking system architecture ARCH2 implements the function of ARCH1 and meets various of derived requirements listed in the Wheel Brake System preliminary safety assessment(PSSA). As a feedback of PSSA, things to consider include but are not limited to:

- The modified architecture shall have at least two independent hydraulic pressure sources.
- The modified architecture shall have dual channel BSCU and multimode brake operations to provide the required redundancy.

ARCH3. Following the result of the WBS trade study, The development of architecture three is designed with one BSCU housing two independent systems, each BSCU subsystem has independent command and monitor channels.

ARCH4. Since architecture three has been simulated and the results of the modeling for each system component are that the schematic of the braking system architecture does not work and there are some mistakes in the schematic. Architecture four is established to avoid the risk of hydraulic supply to wheel brake being possible in normal mode by accumulator. An input is added in ARCH4 to the selector valve corresponding to the validity of the control system. Pedal position signal is input in front of the anti-skid valve in blue hydraulic pressure line and the accumulator is moved in front of the selector valve.

IV. Integrating Fault Trees Into WBS BIP model

A. Behavioral fault modeling

In this section, we describe how to integrate a component's fault behavior from system fault tree into the BIP model. First, we decompose the system fault tree. Then we deduce a fault behavior from each leaf node of the system fault tree. Next, we generate a BIP component with fault behavior according to its nominal behavior BIP model. Afterwards, we put the behavioral fault component and the nominal behavior component together with a manager component deciding and monitoring the activition of both fault and nominal behavior components. Finally, we modifies the connection between each component to ensure the input and output ports are the same as the original BIP component. The result of the integration is a fault-based BIP component.

Example 1. We take a commonly used valve component as an example. In general, a valve is used to control the passage of hydraulic pressure. When the valve is open, the output hydraulic pressure is equal to the input hydraulic pressure, indicates that the valve currently allows hydraulic pressure to pass. When the valve is close, the output hydraulic pressure is zero, indicates a rejection of hydraulic passage.

We deduce two fault behaviors for the valve component, the stack-at-open fault and stack-at-close fault. For stack-at-open fault, the output hydraulic pressure is always the same as the input, while for stack-at-close fault, the output hydraulic pressure is always zero.

Figure 2 need to check with W.Q

Figure 2 shows a valve compound containing a valve component with nominal behavior, two valve components with faulty behavior and a manager component.

B. Fault trees for the WBS

Figure 3 shows a fault tree for "Loss of wheel braking" event, which is based on the AIR6110 standard description. Loss of wheel braking is caused either through the Loss of operaton of physical system or due to the loss of BSCU. We focus on the leaf nodes which represent fault behavior for their component respectively. Notice that the expansion of the fault tree nodes "Loss of BSCU channel 1/2" are carried out but not included in figure 3 for the sake of brevity.

C. Modified BIP model for the WBS

In this section, we give a whole view of modified BIP model which is integrated with fault tree introduced in section *B* using the methodology provided in seciton *A*.

Table 1 shows metrics for the different architectures. The later the design version of the architecture, the greater the scale of the BIP model. ARCH1 shows a large delta with other three architectures. From ARCH2 to ARCH3, there is a differ from the design of the BSCU. For ARCH2, the AIR6110 standard only requires a redundency of BSCU which results in a WBS model including two identical BSCU system. For ARCH3, motivated by trade studies on ARCH2, the strcture is modified from two BSCUs to a BSCU with dual channels. Also, as the result of integration, the extended BIP model with fault

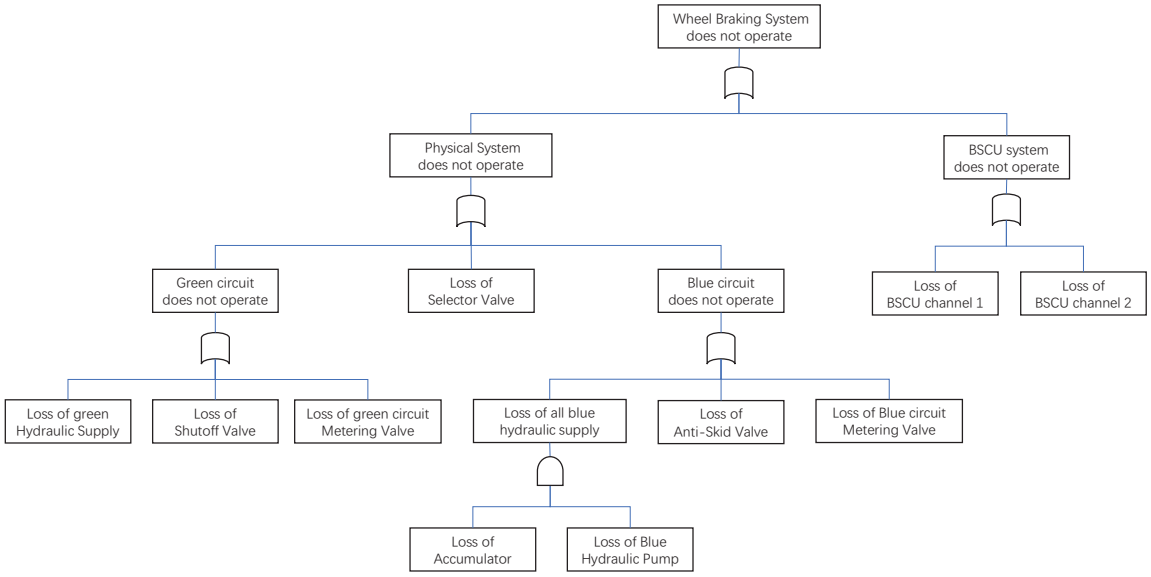

Fig. 2. Fault tree for a loss of WBS occurrence under ARCH4

behavior presents a larger scale than the nominal BIP model. ARCH3 and ARCH4 show the closest metrics for there is only a little change in the physical system.

The full system implementation can be found at https://github.com/Rosaugo/WBSFaultModelingBIP. You can find the nominal WBS model or the BIP model extended with the faults described in the fault tree in section *B*.

TABLE I
BIP NOMINAL/FAULT MODEL STATISTICS

		ARCH1	ARCH2	ARCH3	ARCH4
Component types	Nominal				
	Extended				
Compound types	Nominal				
	Extended				
Max depth	Nominal				
	Extended				
Variables	Nominal				
	Extended				
Internal ports	Nominal				
	Extended				
External ports	Nominal				
	Extended				

V. VERIFICATION METHODOLOGY AND EXPERIMENTS

Giving an overview of verification methodology and experiments here.

A. WBS Requirements formalization and decomposition

The AIR6110 document contains several requirements for the WBS. These can be grouped in two main categories: Requirements corresponding to safety, e.g., *the loss of all wheel braking shall be extremely remote*, and others, e.g., *the WBS shall have at least two hydraulic pressure sources*.

Giving an explaination of how to translate WBS requirements to LTL specifications and taking one requirement to LTL as an example.

B. Experiments and results

Briefly introduction.

1) Probability Estimation:

Will be texted after further experiments finished.

2) Parametric exploration:

Will be texted after further experiments finished.

ACKNOWLEDGMENT

This work was supported by * (check with Prof.Miao). The author wish to thank * (check with everyone)

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.