DEPENDABILITY STUDY OF AN ANTILOCK BRAKING SYSTEM: APPLICATION OF BAYESIAN BELIEF NETWORKS

Andrew J. Kornecki [1], Janusz Zalewski [2]

[1] Embry Riddle Aeronautical University
Electrical, Computer, Software and System Engineering Department
Daytona Beach, FL 32114, USA
kornecka@erau.edu

[2] Florida Gulf Coast University
Dept. of Software Engineering
Fort Myers, FL 33965, USA
zalewski@fgcu.edu

Abstract: *This paper discusses application of Bayesian Belief Networks (BBN) to assess dependability of a safety critical system. Taking as a case study popular antilock braking system (ABS), the authors present system hazard analysis with fault trees and subsequent analysis of the system properties using BBN. The presented approach allows for a probabilistic assessment of specific system properties, both deductive and inductive, and thus ultimately provides a method of quantitative assessment of system dependability.*

Keywords: *Software Dependability, Software Safety, Fault Trees, Bayesian Belief Networks, Anti-Lock Braking System.*

1 Introduction

The objective of the paper is to discuss dependability assessment of a safety critical system. An example case study, antilock braking system (ABS), is widely used in automotive applications. Vehicle's wheels may slip and lockup during severe braking or when braking occurs on an icy road surface, causing exceedingly long stopping distance and potential loss of vehicle steering stability. The ABS, which is designed to keep a vehicle steerable and stable during heavy braking moments by preventing wheel lock, is an important contribution to the road safety. The ABS system detects the wheel slip and reduces braking so that the friction is restored and the steering stability is maintained. Such design reduces braking distance while maintaining the directional control.

For any safety critical system, such as an ABS, it is necessary to conduct a rigorous dependability analysis from the perspectives of safety and reliability. A general approach to analyzing dependability of a standard conventional ABS includes two phases: (1) preliminary assessment of the hazards to identify what hazard conditions may exist, and (2) general analysis of what would cause abnormal conditions in the system. Subsequently, well established more formal methods can be utilized to model the system for fault analysis and reliability of components. The methods may include [1]: fault tree analysis (FTA), event tree analysis (ETA), failure modes and effects analysis (FMEA), Markov chains, Petri nets, Bayesian belief networks (BBN) and others.

The purpose of this study is to analyze dependability and impact of an antilock device on braking system using BBN's. The rest of the paper is structured as follows. Section 2 describes briefly the ABS system analyzed, Section 3 discusses potential hazards, and Section 4 presents the application of the BBN method to model and analyze system dependability from the perspective of its safety. Section 5 derives some observations and conclusions.

2 ABS System Description and Operation

ABS was developed to reduce skidding and maintain steering control when brakes are used in an emergency situation. Typical ABS components include: vehicle's physical brakes, wheel speed sensors, an electronic control unit (ECU), brake master cylinder, a hydraulic modulator unit with pump and valves. Some of the advanced ABS systems include also accelerometer to determine the deceleration of the vehicle.

The example of ABS discussed in this paper is a relatively simple one-channel/one-sensor ABS. This type of system controls only the rear wheels and is typically found in pickup trucks. The system has one valve which controls both rear wheels and one speed sensor located in the rear axle. The rear wheels are monitored together and both wheels need to begin to lock before the ABS activates. In this system it is also possible that one of the rear wheels will lock reducing brake effectiveness. Since the purpose of an ABS is to prevent loss of control, one wheel locking does not mean that the ABS system is not effective. What this ABS prevents is both rear wheels locking which could create a loss of control situation [2].

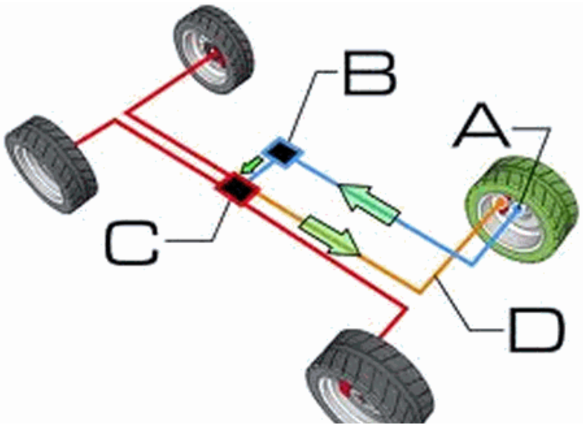

Figure 1: ABS Components [*www.drivingfast.net*]

The following components are included in the analyzed system (Fig. 1):

- A: Wheel Speed Sensor
- B: ABS control module: Real Wheel Anti Lock Controller (RWAL) [3].
- C/D: Hydraulic pump and valves subsystem containing two solenoid valves: Isolation Valve (normally open, used to block the pressure during anti-lock action) and Dump Valve (normally closed, used for relieving the pressure)

When the ABS control module detects a difference in the average speed of the rear wheels compared to the vehicle's overall speed, it initiates antilock braking. The difference between the wheel and vehicle velocity provides an input to a control algorithm in the RWAL, which generates an output signal to the brake actuator. The control logic is based on the objective to keep the wheels from getting locked up and to maintain the traction between the tire and road surface at an optimal maximum. The task of keeping the wheels operating at maximum traction is complicated given that the friction-slip curve changes with vehicle, tire and road changes.

3 Preliminary Hazard Analysis

Overall, multiple problems may arise with ABS and its components that may have impact on safety, so respective measures need to be taken. One of such measures, the self-diagnostic capability of the system is limited to storing only one fault code at a time. When a fault is detected, the ABS warning light comes on and the ABS function is disabled. However, the warning light may be shared with other components of the braking systems (e.g., the light also comes on if a hydraulic failure occurs in the brake system, or the parking brake has been set).

Self-diagnosis, however, does not cover all potential fault paths and a more comprehensive analysis is needed. A good starting point to any dependability assessment is the Preliminary Hazard Analysis (PHA) [4]. PHA identifies scenarios in which hazardous conditions could occur. These scenarios examine those events controlled by the internal design of the system as well as external environmental factors that could inhibit or degrade the system operation. As an example, Table 1 presents an excerpt of the PHA identifying hazardous events and the resulting hazardous effects that may lead to the top level mishap which is the loss of vehicle control. The relations between these base events and subsequent hazards can be analyzed using a Fault Tree (FT) diagram [5] as presented in Fig. 2.

Table 1. Preliminary Hazard List: PHA excerpt for the ABS

Hazardous Event	**Primary Hazardous Effect**	**Resulting Hazardous Effect**	**Top Level Mishap**
Brake Fluid Leak	Brake Problem	Brake Pressure Loss	Loss of Control
Air/Water in Brake Fluid	Brake Problem	Brake Pressure Loss	Loss of Control
Master Cylinder Failure	Brake Pressure Loss	Brake Pressure Loss	Loss of Control
Isolation Valve Fails	Solenoid Failure	ABS Malfunction	Loss of Control
Dump Valve Fails	Solenoid Failure	ABS Malfunction	Loss of Control
Missing/Flawed Recalibration	RWAL Malfunction	ABS Malfunction	Loss of Control
Speed Sensor Malfunction	RWAL Malfunction	ABS Malfunction	Loss of Control

An example of fault tree analysis can be performed using Reliability Workbench [6] (Fig. 2). A simplified case assumes fixed frequency of events causing brake problems (once per month), sensor and recalibration problems (once per six months), and valves failures (once per year). In such "nominal" case a potential loss of control mishap may occur with likelihood of 0.36% (i.e., approx. every 277 years). However, in case of speed sensor malfunction (Fig. 3), the resulting mishap has been calculated to increase tenfold to a likelihood of ~4.3% per year (i.e., every 23 years).

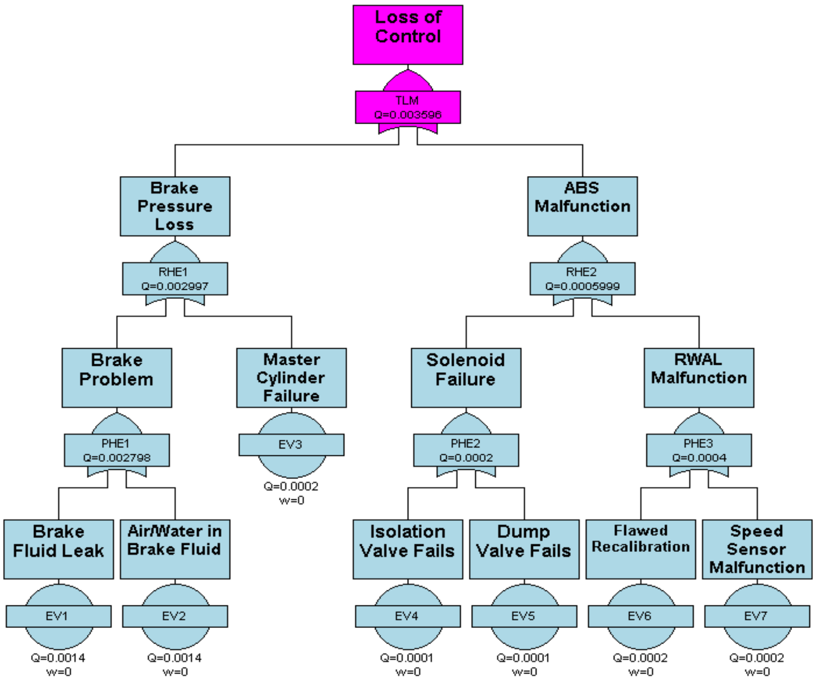

Figure 2: ABS Fault Tree Analysis – Nominal Case

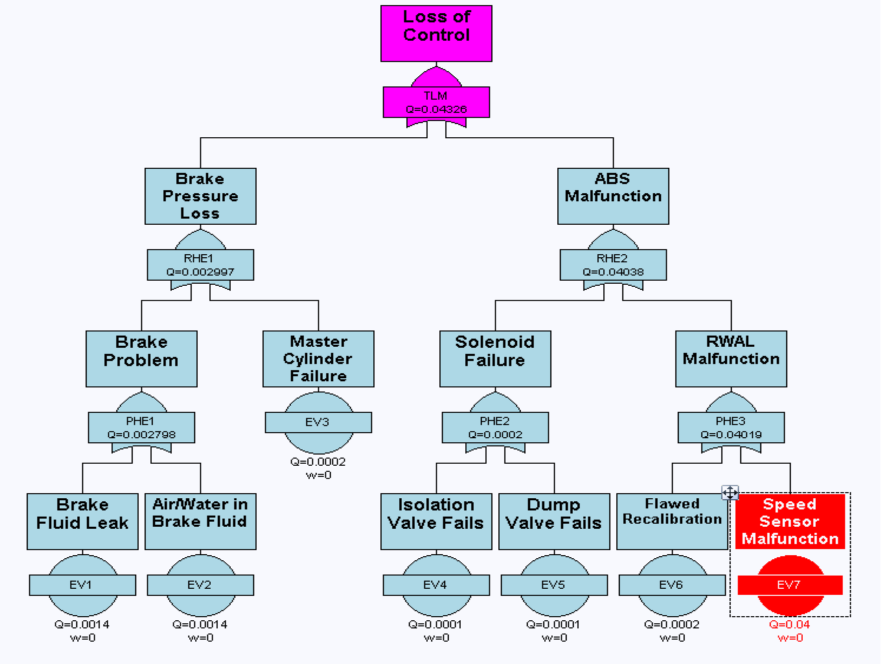

Figure 3: ABS Fault Tree Analysis – Faulty Sensor Case

4 Application of Bayesian Belief Networks

The hazard analysis allows identifying the cause-effect relationships in the ABS system and thus becomes the base for building the Bayesian Belief Network (BBN) model to conduct a more comprehensive safety analysis. The basics of BBN's are covered extensively in the literature, for example, [7], and are not discussed here due to the lack of space.

In this model, the ABS is represented as a set of nodes tied to variables dependent on each other in unidirectional way, with each node corresponding to either a system component or a situation. Each node (variable) is characterized by a set of states assumed with certain likelihood. The relation between the nodes is conditional since the state of specific node may depend on the state of its parent nodes. Thus, to fully specify the BBN it is necessary to derive for each node the probability distribution conditional upon the potential causes (states of parent nodes). Subsequently, the BBN can be used to perform inference after variables at some nodes are determined to be equal to observed values, which corresponds to finding evidence of certain events. Using the BBN approach allows analyzing the likelihood of the system to be in certain state assuming evidence is gained on the state of its components or the situation.

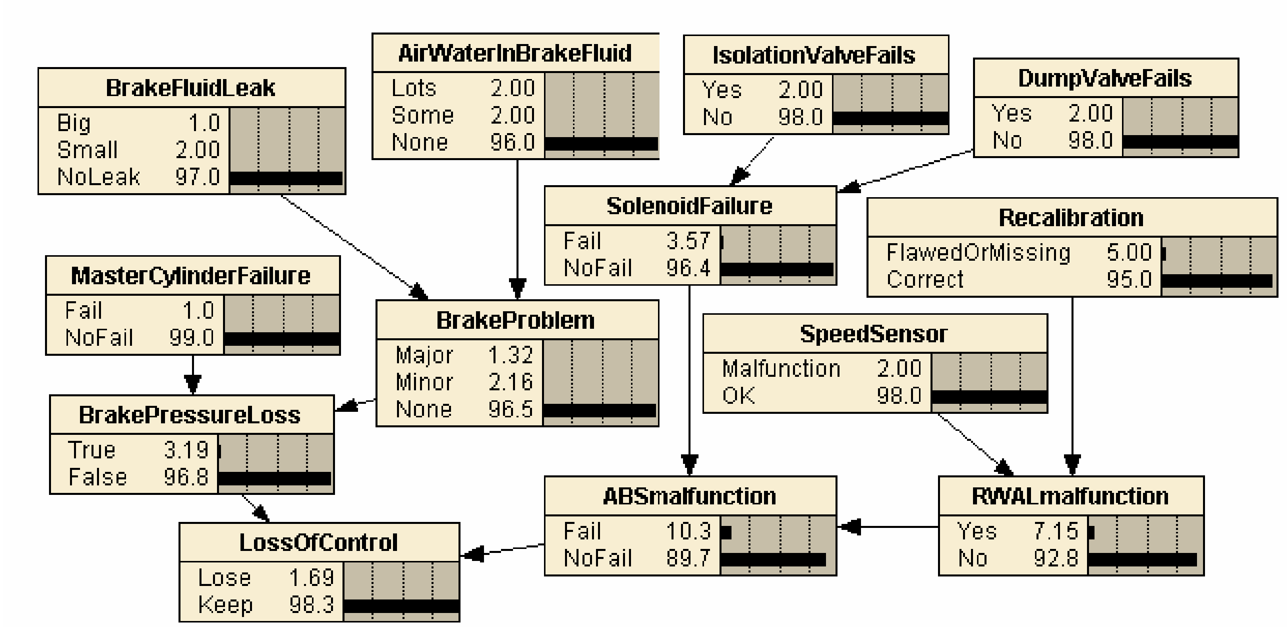

Figure 4: BBN Model of ABS: a “nominal” case

Figure 4 shows a BBN for a simple ABS described in Section 2, derived from a Fault Tree discussed in Section 3. This particular model’s focus is to determine likelihood of the vehicle losing control depending on the braking system scenario and availability of the ABS. The system was modeled using the Netica software [8].

As determined by PHA, it is evident that the loss of vehicle control may be caused by the brake pressure loss with the ABS malfunction contributing to this mishap. In turn, there are several potential causes of the loss of brake pressure, as well as multiple causes of potential malfunctioning of the ABS. Each of the causes and effects may lead to specific states in the model’s nodes. Nominal likelihood values are assumed for both independent and dependent nodes.

As shown in Fig. 4, when ABS and brakes hardware are working in a nominal state (i.e., no failures are indicated), the likelihood of losing vehicle control is relatively low. However, from this nominal case, we analyzed various scenarios reflecting the failure of specific factors contributing to ABS malfunction. Assuming that the brakes are in a nominal state, the example cases shown in Table 2 identify the potential impact of different levels of the ABS malfunction on the loss of vehicle control. Particularly interesting is the extent of impact which various malfunctions of the ABS components may have on the overall dependability in a view of the loss of control. On average, the ABS malfunction doubles likelihood of loss of vehicle control.

Table 2. Impact of the ABS contributing factors on loss of control in relation to the nominal case

Case – brake nominal	**Loss of Control %**	**ABS malfunction %**	**Impact**
All ABS causes OK	1.49	1.89	-12%
ABS nominal	1.69	10.3	0%
ABS bad recalibration	3.41	81.9	102%
ABS sensor malfunction	3.42	82.1	102%
ABS valve fails	3.43	82.5	103%
All ABS causes FAIL	3.85	99.9	128%

The BBN allows analyzing situations when brakes system experiences some malfunctions and the impact of ABS on potential loss of vehicle control. As an example of potential failure in the brake path, Fig. 5 presents the situation when the evidence that a brake leak occurred has been found while ABS works in a nominal state.

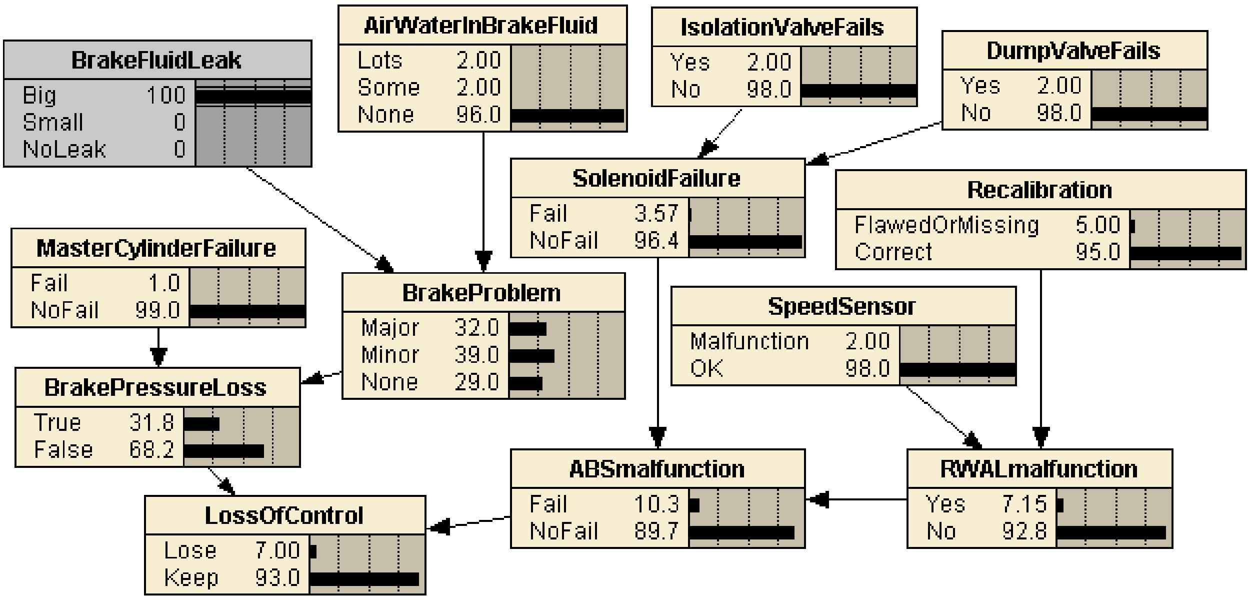

Figure 5: BBN ABS Model Predictive Reasoning: impact of brake fluid leak

A related but more dangerous situation is reflected in Fig. 6. In this case, modeling the brake leak and ABS malfunction shows nearly threefold increase in the likelihood of the loss of control.

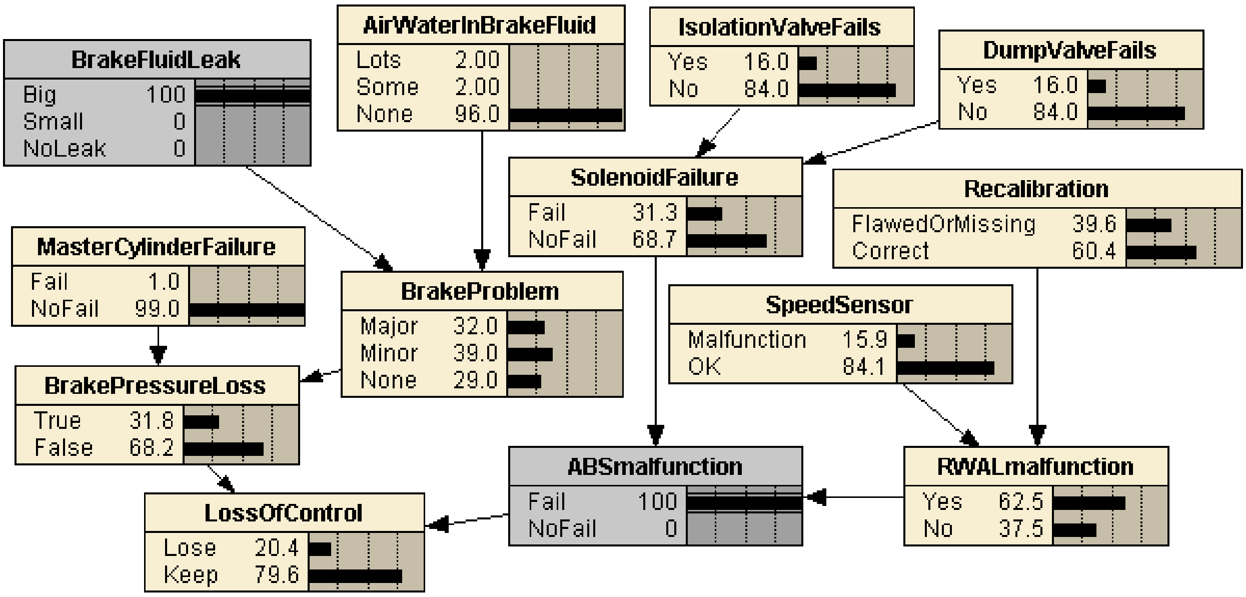

Figure 6: BBN ABS Model Predictive Reasoning: brake fluid leak and the ABS malfunction

The analysis of multiple other scenarios in potential brake problems, combined with the evidence on various states of the ABS, leads to interesting observations about potential impact on the loss of vehicle control. These considerations are reflected in Table 3. The two rightmost columns reflect the impact of ABS failures. On average, failure of the ABS combined with some brake malfunctions causes that loss of vehicle control is three to four times more likely.

Table 3. Impact of the ABS status on loss of control

BRAKE STATUS	**Loss of Control (%)**			**ABS impact (times more likely)**	
	ABS all OK	**ABS nominal**	**ABS all Fail**	**Fail/OK**	**Fail/nominal**
Brake fluid leak	5.3	7.0	20.4	3.6	2.9
Master cylinder failure	13.0	16.0	48.6	3.7	3.0
All brake causes FAIL	15.7	19.5	59.4	3.8	3.0
All brake causes OK	1.17	1.29	2.58	2.2	2.0

As shown above, BBN's allow exploring a variety of scenarios and determining the final outcome (e.g., loss of control) using a predictive reasoning. However, it is important to stress that diagnostic reasoning can be also pursued, for example, to determine a likelihood of brake components failure assuming the evidence of loss of control with working ABS. Knowing that loss of control occurred, one can determine numerically what its potential cause was, e.g., that likelihood of brake pressure loss was 37.0% and the likelihood of ABS malfunction was 23.5% (Fig. 7).

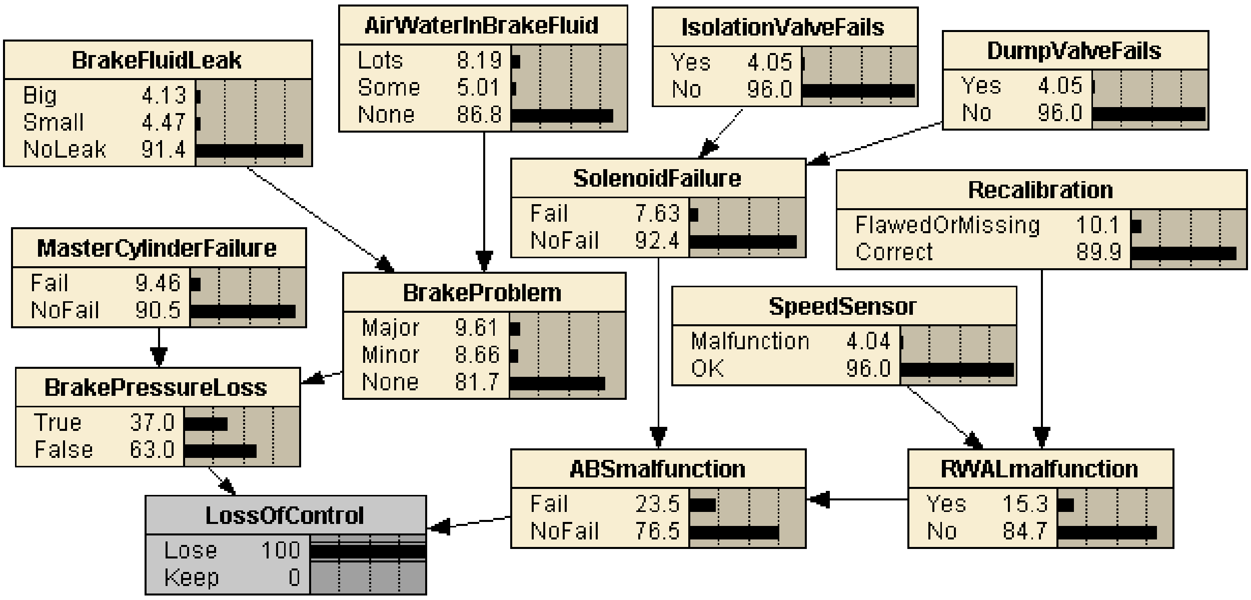

Figure 7: BBN ABS Model Diagnostic Reasoning: a loss of control evidence

5 Conclusion

This paper demonstrates the use of BBN to analyze the ABS system from the perspective of numerical assessment of its dependability. To develop a BBN a Preliminary Hazard Analysis has been applied, first, with the use of Fault Trees to identify potential paths of failures.

An interesting observation resulting from the predictive reasoning experiment with the BBN is that the working ABS improves significantly vehicle control and the improvement can be assessed numerically. It is also possible to estimate likelihood of the loss of control having evidence of the system state. For potential accident investigation, it is possible to use diagnostic reasoning leading to determining the likelihood of faults in particular elements. Thus, the application of BBN's leads to a quantitative assessment of the system safety and dependability properties.

The shortcoming of this type of analysis is the scarcity of publicly available industrial data on probabilities of failures of specific components under some particular assumptions. But once such data are available for a specific project, the BBN's present a solid approach to form the basis for analytical calculations. This could be a potential extension of the current work. Other possible extensions may involve building ABS systems with more wheels and subsystem interactions. That way, design alternatives could be considered to further enhance the reliability of the ABS.

References

[1] Leveson, N., *Safeware: System Safety and Computers*, Addison-Wesley, 1995.

[2] Aly, A., Zeidan, E., Hamed, A., Salem, F. An antilock-braking systems (ABS) control: A technical review. *Intelligent Control and Automation*, Vol. 2, No. 3, pp. 186-195, 2011.

[3] *Automotive Diagnostic & Repair Help. Kelsey-Hayes RWAL Antilock Brakes*. Available from URL: http://www.aa1car.com/library/abs_kelseyhayes_rwal.htm

[4] Roland, H.E., Moriarty, B., *System Safety Engineering and Management*, John Wiley and Sons, 1990 (Chapter 23)

[5] Vesely W. et al., *Fault Tree Handbook with Aerospace Applications*, NASA Office of Safety and Mission Assurance, August 2002.

[6] *Reliability Workbench*, Isograph Software, Irvine, Calif., URL: http://www.isograph-software.com/

[7] Jensen, F.V., Nielsen, T.D. *Bayesian Networks and Decision Graphs. 2nd Edition*, Springer-Verlag, 2007.

[8] *Netica Software Package*. Norsys Software Corp., Vancouver, BC. URL: http://www.norsys.com/netica.html