A Dependability Analysis of a Moroccan Level Crossing based on Fault Tree Analysis and Importance Measures.

Jaouad Boudnnaya, Abdelhak Mkhida, Mohamed Sallak

▶ **To cite this version:**

Jaouad Boudnnaya, Abdelhak Mkhida, Mohamed Sallak. A Dependability Analysis of a Moroccan Level Crossing based on Fault Tree Analysis and Importance Measures. . 10ème Conférence Francophone de Modélisation, Optimisation et Simulation (MOSIM 2014), Nov 2014, Nancy, France. hal-01166695

HAL Id: hal-01166695
https://hal.science/hal-01166695v1

Submitted on 23 Jun 2015

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

10^{th} *International Conference on MOdeling, Optimization and SIMlation - MOSIM14 - November 5-7-2014- Nancy - France "Toward circular Economy"*

A Dependability analysis of a Moroccan level crossing based on Fault tree analysis and importance measures

Jaouad BOUDNAYA, Abdelhak MKHIDA
Laboratory of Mechanics,
Mechatronics and Control (L2MC)
ENSAM Meknes , Moulay Ismail University
Marjane 2, PO Box 15290, Al-Mansour
Road Agouray, 50500 Meknes, MOROCCO
j.boudnaya@gmail.com, abdelhak.mkhida@gmail.com

Mohamed SALLAK
Heudiasyc UMR CNRS 7253
Compiègne University of Technology
60200 Compiègne, France
sallakmo@utc.fr

ABSTRACT : *In this paper, we propose a methodology to evaluate the unavailability of level crossings systems and to identify their critical components. First, a fault tree analysis to evaluate the occurrence probability of the Feared Event (Collision between train and vehicle) over the time is proposed. The human factors and devices failures are also taken into account. Then, an importance measures study is proposed to identify critical components in level crossing systems.*

KEYWORDS : *Railway Signalling System, Level Crossing, Minimal Cut, Fault tree, Importance measures.*

1 INTRODUCTION

The railway safety is one of the most complex problems which is necessary to approach in order to estimate better and improve the performances of the railway systems. Particularly, the level crossings constitute the major source of the risks of accidents in the railway domain. Several works related to this problem were presented in the literature. In (Collart Dutilleul, Defossez & Bon 2006), level crossings are modelled by p-time Petri nets in order to satisfy time specifications defined in safety requirements. In (Ghazel 2009), the authors propose a global model of the level crossing implying at the same time the rail and road traffic by using stochastic Petri nets. This model is obtained by a progressive integration of the developed elementary models ; each of them describes the behaviour of a section. It allows the follow-up and the qualitative and quantitative evaluation of the effect of various factors on the level of the risk. The study reported in (Lalouette, Caron, Scherb, Brinzei, Aubry & Malassé 2010) presents a new approach of the operating safety aiming at the evaluation of a set of hazards likely to be met during the operational life cycle of a system. This new approach is applied to the study of a new European railway signalling system (ERTMS), superimposed on the French lateral signalling by using coloured Petri nets. In (Qiu, Sallak, Schön & Cherfi 2014), the modelling of the ERTMS level 2 is made by Statecharts. This work proposes the evaluation of performances of this system in terms of availability and of mean time spent in every state (nominal way of functioning, degraded mode and failure mode) by integrating human factors as well as network failures. In this paper, we model the Feared Event (Collision between train and vehicle) of the Moroccan level crossing using Fault Trees. We also taken into account human factors. The failure data used in this approach are based on Moroccan statistics of railway accidents (Bouchiba 2013). Then, we compute the unvailability of the level crossing system as a function of the time. Furthermore, we identify the components within the level crossing system that more significantly influence the level crossing's behavior with respect to its unavailability. As we cannot improve all components at one time to improve the level crossing's availability, priority should be given to components that are more important.

2 THE LEVELS CROSSING IN MOROCCO

2.1 Generalities

Level crossings are crossings at the level of a railway with a highway or pedestrian path. They constitute one of the most important sources of accidents in the railway domain in Morocco. Within the framework of the global program of the security of the crossing of the Morocco railway, it was decided in July, 2012 to strengthen the safety of all the level crossings not guarded and situated on lines with high traffic. New equipments will be installed on the unguarded level crossing and will allow announcing to

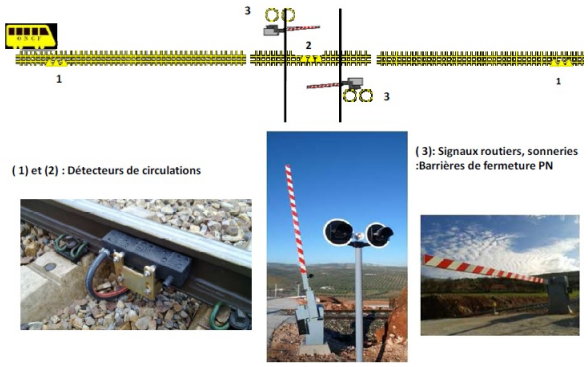

FIGURE 1 – Prototype of the Level crossing

FIGURE 2 – Principle of functioning of the automated level crossing

the road users the approach of the train. For instance, Figure 1 represents a prototype which is put in service (department) in the level crossing N° 3080 situated at km 168+088 between Tangier and Sidi Kacem (Morocco 2013).

2.2 Principle of functioning

The principle of security of the level crossing not guarded is as follows (cf. Figure 2) :

- Rest situation (Level crossing open) : the road fires and the bell switched off, and barriers rose.
- Activation of the system : a device of detection (pedal of announcement) is placed at a distance of the level crossing, when the train attacks this device, the road fires ignite in red and the bell rings (announcement of the train).
- Closure of barriers : after approximately 7 seconds of the release of the announcement, the barriers begin to fall. The low position of the barriers is reached after 10 seconds.
- Reopening of the level crossing : when the train arrives at the level crossing (35 seconds after the announcement), attacks the device of rearmament (pedal of surrender). After the complete release of the train, the barriers go up, the road fires and the bell stop ringing.

3 FAULT TREE ANALYSIS

3.1 Introduction

The fault tree (FT) method is very widely used in the field of the dependability of systems. It offers a privileged setting to the deductive analysis which consists in looking for the diverse possible combinations of events leading to the realization of a Feared Event, and allows representing simply these combinations under graphic shape by means of a tree structure of logical gates (cf. Figure 3). The FT displays information in a structured, graphic way that makes it easy to interpret and communicate. However, FTs require detailed knowledge of the design, construction and operation of the system. Furthermore, they are not suitable for assessing dependability of systems with multi-states components.

FTs may fail if the technique is not implemented in a disciplined fashion or if the system problem is so complex that multiple levels of potential causes exist for each problem type.

3.2 Probability calculation

In this work, the following key assumptions are taken into account.

- System and components are allowed to take only two possible states : either working, or failed.
- Component failures are stochastically-independent. Failure of one component does not impact the failures of the other components.
- The system is coherent. That is, improvement of component states cannot damage the system.
- The components are not repairable.

The main treatments made on the fault trees are the research for the minimal cuts (the smallest combinations of events which the simultaneous realization of which leads to the Feared Event) which are used for quantitative evaluation of the probability of occurrence of the Feared event from the probability of occurrence of basic events using the following theorem :

Given a probability space (Ω, Θ, P) and a collection $\mathcal{A} = \{A_1, A_2, \ldots, A_N\}$ of measurable subsets of Θ, Sylvester-Poincaré equality says that

$$P\left(\bigcup_{j=1}^{N} A_j\right) = \sum_{\mathcal{I}\subseteq\mathcal{A}} (-1)^{|\mathcal{I}|+1} P\left(\bigcap_{A_j\in\mathcal{I}} A_j\right) \quad (1)$$

This equality is particularly useful in Fault Tree analysis in which its use in conjunction with the notion of minimal cuts facilitates the computation of the probability of occurrence of the Faired event.

For example, let us consider the Fault Tree presented in Figure 3. The minimal cuts of the Fault Tree are : $\{A\}$,$\{BC\}$, and $\{BD\}$. Then, applying the Sylvester-Poincaré equality, the probability of occurrence of the Feared Event T is given by (all the basic events are

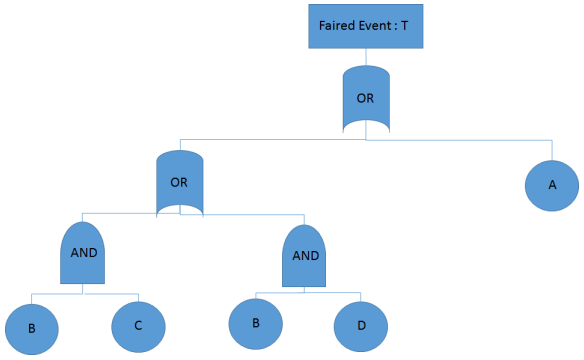

FIGURE 3 – Fault tree example

considered to be independent) :

$$\begin{aligned} P(T) &= P(A \bigcup BC \bigcup BD) \\ &= P(A) + P(BC) + P(BD) - P(ABC) - P(ABD) \\ &\quad -P(BCD) + P(ABCD) \end{aligned}$$

We say that a model of Fault Tree is solved exactly when the full Sylvester-Poincaré development is applied. Unfortunately, applying this development fully is exponential in the number of products. Due to algorithmic limitations, most quantification engines approximate it by computing only the first term of this development (rare event approximation).

4 STUDY OF THE HUMAN FACTOR

The human error can be defined as a fault of the operator which leads to an accident or a railway incident. In the literature, several works taking into account human factors were proposed. In (Labadi 2005), the human reliability is defined as the probability that a task or a work is successfully achieved by a person at a required time if a temporal requirement is necessary. In the latter, several models were proposed to estimate and study the human factor, among these models :

- Models stemming from the psychology and from the ergonomics of the work : Among these models, the model SRK of Rasmusen, supposes that the cognitive control and the human cognition are made at several levels of abstraction. The highest layers correspond to a more and more complex data processing.
- Models stemming from engineering sciences : The method THERP (Techniques for Human Error Rate Prediction), which is a method centred on the operator (individual level), is said first generation because of the sequential model of accident on which it is based.
- Models stemming from human and social sciences : By taking for example the method MERMOS which is developed to update the approach of evaluation of the missions of the operators in accidental conduct, the failure of the mission can arise by several independent scenarios of failures (that will be necessary to quantify).

In our study, we suppose that the rate of error of the operator is constant. The distribution appropriate for the model of rate constant is the exponential distribution. Thus, the rate of transition of the state of functioning to the state of failure is $\lambda_{HF}\Delta t$. To obtain a significant value of the rate of error, we considered the statistics presented in (Morocco 2013) in Morocco from 2000 till 2008. The numbers of accidents on 10 busiest lines are given in the Table 1.

Years	Numbers of accidents
2000	11
2001	6
2002	18
2003	13
2004	15
2005	21
2006	12
2007	7
2008	15
Total	118

TABLE 1 – Statistics of the railway accidents in Morocco

The safety experts at the National Office of the Moroccan Railroad confirmed that about 90% of railway accidents are caused by human error. Thus the error rate of the operator on every line is

$$\begin{aligned} \lambda_{HF} &= \frac{118 * 0.9}{9\ years * 10} \\ &= 1.347 * 10^{-4} h^{-1} \end{aligned}$$

5 IMPORTANCE MEASURES OF BASIC EVENTS OF FAULT TREE

In 1969, Birnbaum first introduced the concept of components' reliability importance (Birnbaum 1969). This measure was defined as the probability that a component i is critical to system failure, *i.e.* when component i fails it causes the system to move from a working to a failed state. The Birnbaum's importance measure of a component i can be interpreted as the rate at which the system's reliability improves as the reliability of component i is improved. Analytically, Birnbaum's importance interval measure of a component i is defined by (Birnbaum 1969)

$$I^B(i) = R_S|\{R_i = 1\} - R_S|\{R_i = 0\}$$

Where $R_S|\{R_i = 1\}$ and $R_S|\{R_i = 0\}$ denote respectively the reliability of the system when it is known that component i is in a working state and

when component i is in a failed state.

In this study, we propose to define the importance measure of an event i which represents the failure occurrence of a component c as follows

$$I(i) = P_S|\{P_i = 1\} - P_S|\{P_i = 0\} \quad (2)$$

Where $P_S|\{P_i = 1\}$ and $P_S|\{P_i = 0\}$ denote respectively the probability of top event occurrence when it is known that event i is occurring (i.e., $P_i = 1$) and when it is known that event i is not occurring (i.e., $P_i = 0$).

6 CASE STUDY

6.1 Description of the system

The Moroccan railway signalling system consists of three parts :

- Rail part : it consists of a material part (train and rail-road) and of a human part (the operator of the train).
- Road part : it contains a material part (vehicle and road) and a human part (the driver of the vehicle).
- Level crossing : it consists of three main parts :
  - Power network and communication network between the components of the railway signalling system.
  - Control part : it consists of Programmable Logic Controller and its program.
  - Operative Part : it consists of sensors (Sensor Ad and Sensor Surrender) and actuators (the road lights, the alarms and the barriers).

Note that in this case study, since the components are not repairable, the system availability is equal to its reliability.

Symbol	Basic Events	Failure Rates (h^{-1})
HF	Human Failure	$1.347*10^{-4}$
VF	Vehicle Failure	$18*10^{-3}$
RF	Rail Failure	$2.85*10^{-6}$
PLCF	Programmable Logic Controller Failure	$4*10^{-6}$
PE	Program Error	$5*10^{-8}$
NCF	Network Communication Failure	$5*10^{-6}$
PNF	Power Network Failure	$5*10^{-6}$
SAF	Sensor Ad Failure	$2*10^{-4}$
SSF	Sensor Surrender	$2*10^{-4}$
AF	Alarm Failure	$4*10^{-4}$
LF	Light Failure	$4*10^{-4}$
MF	Motor Failure	$3*10^{-6}$
TSF	Transmission System Failure	$5*10^{-5}$

TABLE 2 – Failure rates of components

6.2 Fault Tree analysis

From the description of the railway signalling system, we were able to model the Feared Event (Collision between train and vehicle) by a Fault Tree. The basic events which produce the Feared event are given in the Table 2. We suppose that these events follow exponential laws with an approached failure rates (cf. Table 2). Thus, the probability of occurrence of each basic event i at time t is given by $P_i(t) = 1 - exp(-\lambda_i t)$. The symbols of intermediate events of the fault tree are given in Table 3.

Symbol	Intermediate Event
FE	Feared Event
ROP	Road Part
RAP	Rail Part
LC	Level Crossing
N	Network
CP	Control Part
OP	Operative Part
SE	Sensors
AC	Actuators
BA	Barriers
AL	Alarms
LI	Lights
M	Motors
TS	Transmission Systems

TABLE 3 – Symbols of intermediate events

The Fault Tree which describes the Feared event (Collision between train and vehicle) is given in Figure 6.

6.3 Results and discussion

To evaluate the availability of the railway signalling system, we use Henry-Poincaré Formula applied to minimal cuts of the Fault Tree presents in Figure 6. We launched the calculation in the interval [0,300h] with a step $\Delta t = 1h$. Then we plot the unavailability of the railway signalling systems as a function of time (cf. Figure 4). As we can see, the level crossing system become unavailable at time t=300h. This is due to the fact that no maintenance policies are done on the system in this study. In Figure 5, we plot important measures of components as a function of time. As we can show, the most critical components are : VF, HF1, PLCF, PNF and NCF. Even though we can not obviously reduce the vehicle failures (which is the most critical component but it is out of scope of the paper because we are only concerned by the level crossing system), we can focus our efforts on Human Failure (HF), Programmable Logic Controller Failure (PLCF), and Failures Networks (PNF and NCF) in order to reduce efficiently the Faired Event occurrence.

7 CONCLUSION

In this paper, the unavailability of the level crossing system was computed using a Fault Tree analysis by taking into account human errors and components failures data. The critical components were also identified. In our future works, we will complete our study, by considering epistemic uncertainties as well as dependency between components.

ACKNOWLEDGMENTS

First, we thank the ONCF as well as the Center of Doctoral Studies of ENSAM MEKNES. Many thanks go to our colleagues and experts for the source of information and advice they gave us. we also thank obviously the steering committee of the International Conference of Modelling and Simulation (MOSIM'14), to allow us to participate in this conference and so to communicate our research and to share our conclusions with colleagues. This work

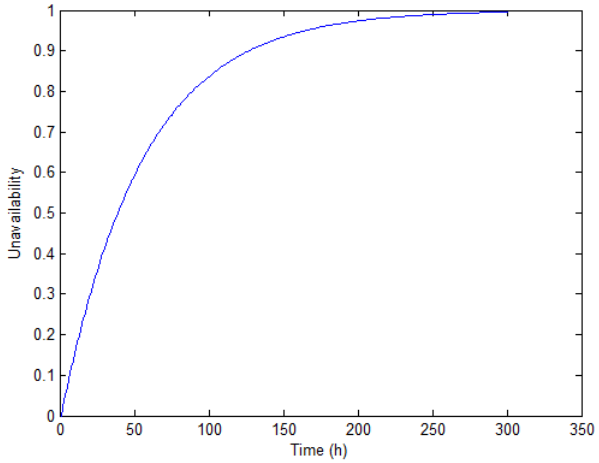

FIGURE 4 – Unavailability of the level crossing system over the time

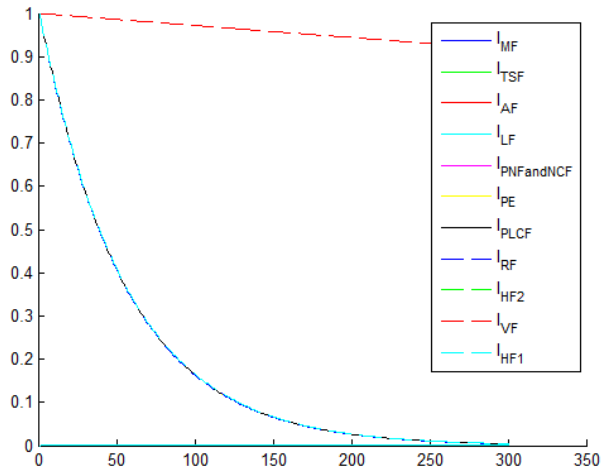

FIGURE 5 – Importance measures of components

was also supported and part-funded by the French National Research Agency, ANR-13-JS03-0007 RECIF.

Références

Birnbaum, Z. W. (1969). *On the Importance of Different Components in a Multi-Component System*, Academic Press, New York.

Bouchiba, A. (2013). *Evaluation de Dysfonctionnement d'un Système par Approche Bayésienne : Cas du Système Ferroviaire*, PhD thesis, Ecole doctorale dAngers, France.

Collart Dutilleul, S., Defossez, F. & Bon, P. (2006). Safety requirements and p-time petri nets : A level crossing case study, *IMACS Multiconference on "Computational Engineering in Systems Applications"(CESA), Beijing, China.*

Ghazel, M. (2009). Using stochastic petri nets for level-crossing collision risk assessment, *IEEE Transactions on Intelligent Transportation Systems* **10** : 668 – 677.

Labadi, K. (2005). *Contribution à la modélisation et à l'analyse de performances des systèmes logistiques à laide dun nouveau modèle de réseaux de Petri stochastiques*, PhD thesis, Université de Technologie de Troyes (UTT), France.

Lalouette, J., Caron, R., Scherb, F., Brinzei, N., Aubry, J.-F. & Malassé, O. (2010). Performance assessment of european railway signalling system superposed of the french system in the presence of failures, *17e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement, Lambda-Mu'2010, La Rochelle, France.*

Morocco (2013). Sécurisation de la traversée des voies ferrées au droit des passages à niveau : Equipement des passages a niveau non gardés par système automatique dannonce et de protection, *ILCAD.*

Qiu, S., Sallak, M., Schön, W. & Cherfi, Z. (2014). Modeling of ertms level 2 as an sos and evaluation of its dependability parameters using statecharts, *IEEE Systems Journal* **DOI : 10.1109/JSYST.2013.2297751**.

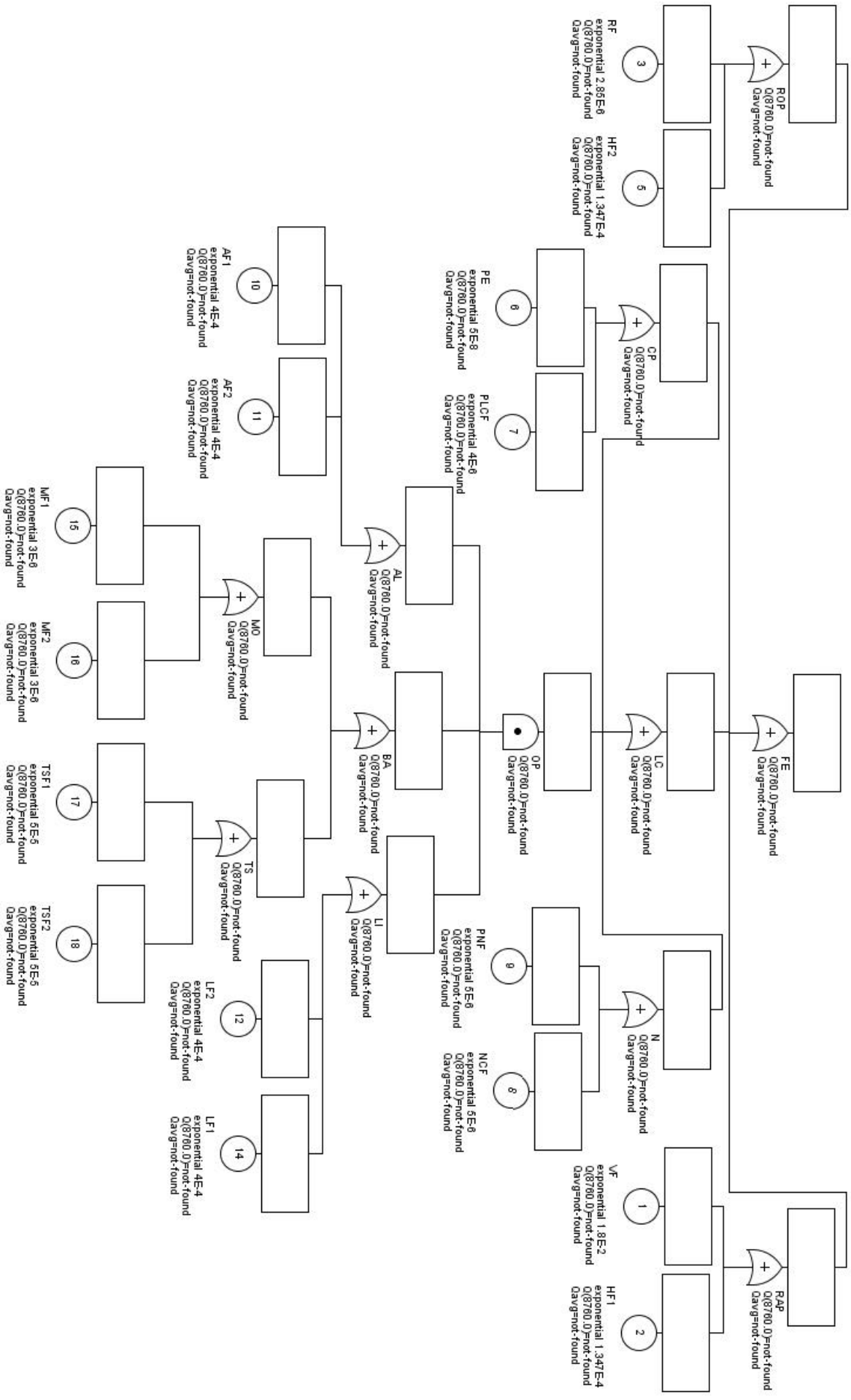

FIGURE 6 – Fault Tree of Level crossing