

# On the Formalization of Importance Measures using HOL Theorem Proving

Waqar Ahmad<sup>1</sup>, Shahid Ali Murtza<sup>2</sup>, Osman Hasan<sup>2</sup>, and Sofiène Tahar<sup>1</sup>

<sup>1</sup>Electrical and Computer Engineering,  
Concordia University, Montreal, QC, Canada  
Email: {waqar,tahar}@ece.concordia.ca

<sup>2</sup>School of Electrical Engineering and Computer Science,  
National University of Sciences and Technology, Islamabad, Pakistan  
Email: {smurtza,msee15seecs,osman.hasan}@seecs.nust.edu.pk

**Abstract**—Importance measures provide a systematic approach to scrutinize critical system components, which are extremely beneficial in making important decisions, such as prioritizing reliability improvement activities, identifying weak-links and effective usage of given resources. The importance measures are then in turn used to obtain a criticality value for each system component and to rank the components in descending manner. Simulations tools are generally used to perform importance measure based analysis, but they require expensive computations and thus they are not suitable for large systems. A more scalable approach is to utilize the importance measures to obtain all the necessary conditions by proving a generic relationship describing the relative importance between any pair of components in a system. In this paper, we propose to use higher-order-logic (HOL) theorem proving to verify such relationships and thus making sure that all the essential conditions are accompanied by the proven property. In particular, we formalize the commonly used importance measures, such as Birnbaum and Fussell-Vesely, and conduct a formal importance measure analysis of a railway signaling system at a Moroccan level crossing as an application for illustration purpose.

**Keywords**—Importance Measures, Higher-order Logic, Fault Tree, Theorem Proving.

## I. INTRODUCTION

Importance measures [1] provide an effective way to evaluate the relative criticality of components in a system. Particularly, they are employed to identify a subset of components that are more important to a system so that given resources can be effectively utilized. The underline concept is to focus on the most problematic areas in a system aiming to achieve the most significant gains. A study at Microsoft Corp. has revealed that about 20% of the entire pool of detected bugs lead to about 80% of the errors and crashes in Microsoft Windows and Office software [2]. In reliability engineering, determining the importance of components significantly helps to solve several reliability problems, such as component assignment, redundancy allocation, system upgrading, and fault diagnosis and maintenance.

In 1968, Birnbaum was the first to propose the concept of *importance measure* for binary systems of two states, either functioning or failed [3]. This led to the development of more sophisticated importance measures, such as Fussell-Vesely [1], to analyze more complicated systems, like nuclear

power plants. These importance measures are primarily defined for coherent systems [1], which are systems satisfying the following conditions: (1) their structure function or system failure model exhibits non-decreasing behavior, i.e., the probability of the given failure model increases with the increase in the number of failures; and (2) each of their components is relevant, i.e., every component is actively contributing to the system failure.

A typical method in importance measure analysis involves calculating a criticality value for each component in a system and then tabulating the obtained data in descending manner [4]. In other words, a component with higher value is regarded as highly critical and placed above in the ranking than a component with a lower value. Simulation based reliability analysis tools, such as ReliaSoft [5], determine the component's importance by computing the percentage of times that a system failure event is caused by a failure of a particular component over the simulation time 0 to  $t$ . However, for analyzing the relative importance between all pairs of components, these methods have very high computational requirements especially when dealing with systems with many components.

The scalability limitations of simulation based importance measure analysis can be resolved by using mathematically verified reduction methods in this context. For instance, Boland et al. [6] developed a relationship stating that the component  $i$  is structurally more critical than the component  $j$  if its structure function is larger when  $i$  is down and  $j$  is up as compared to the opposite case. This work is further extended by Meng [7] to obtain the necessary conditions, based on Birnbaum and Fussell-Vesely importance measures, that are essential for proving the analytical relationships describing the relative importance of any pair of system components. These analytical relationships can be extremely helpful in practical scenarios since calculating the exact values of a component importance measures can be tedious for large and complex systems. However, these analytical relationships have been manually verified using paper-and-pencil based proof methods and thus there is no guaranty that all necessary conditions are explicitly identified. This is a grave concern considering the safety-critical nature of some importance measure analysis. Thus, there is a dire need of developing more rigorous analysis of these foundational relationships to guarantee their correctness and their appropriate usage.

In this paper, we propose to utilize higher-order-logic

(HOL) theorem proving to assure the formal guarantees about the relationships, obtained by Boland and Meng, governing the relative importance of any pair of system components. The HOL theorem prover is a system of deduction with precise semantics and provides a sound reasoning support for verifying the given properties, stated as a theorem, rigorously [8]. We first formalize the properties of coherent systems by describing their structure function as a fault tree (FT) [9] model, which is a graphical model for analyzing the conditions and factors causing the system failure. Secondly, we formalize commonly used importance measures, such as Birnbaum, Fussell-Vesely, Reduction Worth and Achievement Worth [1]. We then use the formalization of Birnbaum importance measure to formally verify the relative importance properties of any pair of system components as described by Boland and Meng using HOL theorem proving. For illustration purposes, we conduct the formal importance measure analysis of a railway signaling system at a Moroccan level crossing (LC) [10] consisting of several critical components, such as lights, programmable logic controllers, alarms and also human factor, using the HOL theorem prover [11].

The rest of the paper is organized as follows: An overview of the related work is presented in Section II. In Section III, we provide a brief summary of the HOL theorem prover and the fundamentals of the HOL probability theory. A brief introduction to the recent formalization of FT analysis is also described to facilitate the understanding of the paper. Section IV presents the HOL formalization of the concept of importance measure and its related properties. Section V applies our proposed approach by describing the formal importance measure analysis of the signaling system at a Moroccan level crossing. Finally, Section VI concludes the paper.

## II. RELATED WORK

Importance measure is a useful concept in reliability engineering and has been analyzed analytically [1] as well as using simulation tools [5]. The latter approach is practically adopted by industrial engineers due to their powerful features. These tools follow the typical approach of ranking the system components according to their criticality value. However, this approach requires high computations to obtain the criticality value for all system components and then perform the successive analysis, which may not be possible for large and complex systems. An alternate approach is to verify a relative measure relationship for any pair of components and obtain the necessary conditions, as described by Meng [7].

Recently, a formal dependability analysis framework [12], based on Reliability Block Diagram [13], [14] and FT modeling techniques, has been developed using HOL theorem proving. This framework has been successfully utilized to carry out the reliability analysis of a railway traction drive system [15], failure analysis of satellite solar arrays [16] and an air traffic management system [17]. In the current work, we formalize the notion of coherent system and the importance measure by representing the system structure function based on existing FT models. To the best of our knowledge, this is the first formal work describing the formalization of the importance measures using HOL theorem proving.

## III. PRELIMINARIES

In this section, we first give a brief introduction to the HOL theorem prover, formalization of probability theory and an approach for the formal FT analysis to facilitate the understanding of the rest of the paper.

### A. HOL Theorem Prover

HOL [18] is an interactive theorem prover, developed at the University of Cambridge, UK, for conducting proofs in higher-order logic. It utilizes the simple type theory of Church [19] along with Hindley-Milner polymorphism [20] to implement higher-order logic. HOL has been successfully used as a verification framework for both software and hardware as well as a platform for the formalization of pure mathematics.

The HOL core consists of only 4 basic axioms and 8 primitive inference rules, which are implemented as ML functions. The ML's type system ensures that only valid theorems can be constructed. Soundness is assured as every new theorem must be verified by applying these basic axioms and primitive inference rules or any other previously verified theorems/inference rules.

In this paper, we utilize the HOL theories (libraries) of Booleans, lists, sets, positive integers, *real* numbers, measure and probability [21]. In fact, one of the primary motivations of selecting the HOL theorem prover for our work was to benefit from these built-in mathematical theories. Table I provides the mathematical interpretations of some frequently used HOL symbols and functions, which are inherited from existing HOL theories.

TABLE I. HOL SYMBOLS AND FUNCTIONS

HOL Symbol	Standard Symbol	Meaning
$\wedge$	<i>and</i>	Logical <i>and</i>
$\vee$	<i>or</i>	Logical <i>or</i>
$\neg$	<i>not</i>	Logical <i>negation</i>
$::$	<i>cons</i>	Adds a new element to a list
$++$	<i>append</i>	Joins two lists together
HD $L$	<i>head</i>	Head element of list $L$
TL $L$	<i>tail</i>	Tail of list $L$
EL $n$ $L$	<i>element</i>	$n^{th}$ element of list $L$
MEM $a$ $L$	<i>member</i>	True if $a$ is a member of list $L$
$\lambda x.t$	$\lambda x.t$	Function that maps $x$ to $t(x)$
SUC $n$	$n + 1$	Successor of a <i>num</i>

### B. Probability Theory

Mathematically, a measure space is defined as a triple  $(\Omega, \Sigma, \mu)$ , where  $\Omega$  is a set, called the sample space,  $\Sigma$  represents a  $\sigma$ -algebra of subsets of  $\Omega$ , where the subsets are usually referred to as measurable sets, and  $\mu$  is a measure with domain  $\Sigma$ . A probability space is a measure space  $(\Omega, \Sigma, Pr)$ , such that the measure, referred to as the probability and denoted by  $Pr$ , of the sample space is 1. In the HOL formalization of probability theory [21], given a probability space  $p$ , the functions `space`, `subsets` and `prob` return the corresponding  $\Omega$ ,  $\Sigma$  and  $Pr$ , respectively. This formalization also includes the formal verification of the commonly used probability laws, which play a pivotal role in formal reasoning about dependability properties.

A random variable is a measurable function between a probability space and a measurable space. The measurable

functions belong to a special class of functions, which preserve the property that the inverse image of each measurable set is also measurable. A measurable space refers to a pair  $(S, \mathcal{A})$ , where  $S$  denotes a set and  $\mathcal{A}$  represents a nonempty collection of sub-sets of  $S$ . Now, if  $S$  is a set with finite elements, then the corresponding random variable is termed as a discrete otherwise it is called continuous.

The cumulative distribution function (CDF) is defined as the probability of an event where a random variable  $X$  has a value less than or equal to some value  $t$ , i.e.,  $Pr(X \leq t)$ . This definition characterizes the distribution of both discrete and continuous random variables and has been formalized [22]:

$$\vdash \forall p \ X \ t. \text{CDF } p \ X \ t = \text{distribution } p \ X \ \{y \mid y \leq \text{Normal } t\}$$

The function `Normal` takes a *real* number as its input and converts it to its corresponding value in the *extended-real* data-type, i.e, it is the *real* data-type with the inclusion of positive and negative infinity. The function `distribution` takes three parameters: a probability space  $p$ , a random variable  $X : (\alpha \rightarrow \text{extreal})$  and a set of *extended-real* numbers and returns the probability of the given random variable  $X$  acquiring all the values of the given set in probability space.

The unreliability or the probability of failure  $F(t)$  is defined as the probability that a system or component will fail by the time  $t$ . It can be described in terms of CDF, known as the failure distribution function, if a random variable  $X$  represents the time-to-failure of the component. This time-to-failure random variable  $X$  usually exhibits the exponential or Weibull distribution.

The notion of mutual independence of  $n$  random variables is a major requirement for reasoning about the failure analysis of the given systems. According to this notion, a list of  $n$  events are mutual independent if and only if for each set of  $k$  events, such that  $(1 \leq k \leq n)$ , we have:

$$Pr\left(\bigcap_{i=1}^k A_i\right) = \prod_{i=1}^k Pr(A_i) \quad (1)$$

The mutual independence concept has been formalized in the HOL theorem prover and more details can be found in [22].

### C. Fault Trees

Fault Tree (FT) analysis is a widely used technique to determine the dependability of real-world systems, like railways signaling, automotive or avionics. It mainly provides a graphical model for analyzing the conditions and factors causing an undesired top event, i.e., a critical event, which can cause the complete system failure upon its occurrence. The preceding nodes of the FT are represented by gates, like OR, AND and XOR, which are used to link two or more cause events of a fault in a prescribed manner.

The FT gates are formally modeled by using a new recursive datatype *gate* in HOL as follows [17]:

```
Hol_datatype `gate = AND of gate list |
              OR of gate list |
              NOT of gate |
              atomic of `a event`
```

The type constructors AND and OR recursively function on *gate*-typed lists and the type constructor NOT operates on *gate*-type variable. The type constructor `atomic` is basically a typcasting operator between *event* and *gate*-typed variables.

A semantic function is then defined over *gate* datatype that can yield the corresponding event from the given FT gate as follows:

$$\begin{aligned} \vdash & (\forall p. \text{FTree } p \ (\text{AND } []) = p\_space \ p) \wedge \\ & (\forall xs \ x \ p. \\ & \quad \text{FTree } p \ (\text{AND } (x::xs)) = \\ & \quad \text{FTree } p \ x \ \cap \ \text{FTree } p \ (\text{AND } xs)) \wedge \\ & (\forall p. \text{FTree } p \ (\text{OR } []) = \{\}) \wedge \\ & (\forall xs \ x \ p. \\ & \quad \text{FTree } p \ (\text{OR } (x::xs)) = \\ & \quad \text{FTree } p \ x \ \cup \ \text{FTree } p \ (\text{OR } xs)) \wedge \\ & (\forall p \ a. \\ & \quad \text{FTree } p \ (\text{NOT } a) = \\ & \quad p\_space \ p \ \text{DIFF } \text{FTree } p \ a) \wedge \\ & (\forall p \ a. \text{FTree } p \ (\text{atomic } a) = a) \end{aligned}$$

The function `FTree` takes a list of type *gate*, identified by the type constructor AND, and returns a complete probability space  $p\_space \ p$  if a given list is empty and otherwise returns the intersection of events in a given list. Similarly, to model the behavior of the OR FT gate, the function `FTree` returns the union of all the events after applying the function `FTree` on each element of a given list or an empty set if a given list is empty. The function `FTree` takes the type constructor NOT and returns the complement of a failure event obtained from the function `FTree`. The function `FTree` returns the failure event using the type constructor `atomic`.

If the occurrence of a failure event at the output is caused by the occurrence of all the input failure events, then this kind of behavior can be modeled by using the AND FT gate. Similarly, in the OR FT gate, the occurrence of an output failure event depends upon the occurrence of any one of its input failure event. The NOT FT gate can be used in conjunction with the AND and OR FT gates to formalize other FT gates. The formalization of these gates is based on [17], given in Table II. The NAND FT gate, represented by the function `NAND_FT_gate` in Table II, models the behavior of the occurrence of an output failure event when at least one of the failure events at its input does not occur. This type of gate is used in FTs when the non-occurrence of a failure event in conjunction with other failure events cause the top failure event to occur. This behavior can be expressed as the intersection of complementary and normal events, where the complementary events model the non-occurring failure events and the normal events model the occurring failure events. The output failure event occurs in the 2-input XOR FT gate if only one, and not both, of its input failure events occur.

The verification of the corresponding failure probability expressions, of the above-mentioned FT gates, is presented in Table III. These expressions are verified under the following assumptions: (i) `prob_space p` ensures that  $p$  is

TABLE II. HOL FORMALIZATION OF FAULT TREE GATES

FT Gates	Formalization
	$\vdash \forall p \text{ L1 L2.}$ AND_FT_gate p L1 L2 = FTree p (AND (gate_list L))
	$\vdash \forall p \text{ L.}$ OR_FT_gate p L = FTree p (OR (gate_list L))
	$\vdash \forall p \text{ L1 L2.}$ NAND_FT_gate p L1 L2 = FTree p (AND (gate_list (compl_list p L1 ++ L2)))
	$\vdash \forall p \text{ L.}$ NOR_FT_gate p L = FTree p (NOT (OR (gate_list L)))
	$\vdash \forall p \text{ A B.}$ XOR_FT_gate p A B = FTree p (OR [AND [NOT A; B]; AND [A; NOT B]])

a valid probability space; (ii)  $2 \leq \text{LENGTH } L$  makes sure that the given list  $L$  must have at least two elements; (iii)  $\text{in\_events } p \text{ L}$  ensures that all the corresponding events in the given list  $L$  are drawn from the events space  $p$ ; and (iv)  $\text{mutual\_indep } p \text{ L}$  guarantees that events in the given list  $L$  are mutually independent [22].

TABLE III. PROBABILITY OF FAILURES OF FAULT TREE GATES

Mathematical Expressions	Theorem's Conclusion
$F_{AND}(t) = Pr(\bigcap_{i=2}^N A_i(t))$ $= \prod_{i=2}^N F_i(t)$	$\vdash \forall p \text{ L1 L2.}$ (prob p (AND_FT_gate L) = list_prod (list_prob p L))
$F_{OR}(t) = Pr(\bigcup_{i=2}^N A_i(t))$ $= 1 - \prod_{i=2}^N (1 - F_i(t))$	$\vdash \forall p \text{ L1 L2.}$ (prob p (OR_FT_gate p L) = 1 - list_prod (one_minus_list (list_prob p L)))
$F_{NAND}(t) = Pr(\bigcap_{i=2}^k \bar{A}_i(t) \cap \bigcap_{j=k}^N A_j(t))$ $= \prod_{i=2}^k (1 - F_i(t)) * \prod_{j=k}^N F_j(t)$	$\vdash \forall p \text{ L1 L2.}$ (prob p (NAND_FT_gate p L1 L2) = list_prod (list_prob p (compl_list p L1)) * list_prod (list_prob p L2))
$F_{NOR}(t) = 1 - F_{OR}(t) = \prod_{i=2}^N (1 - F_i(t))$	$\vdash \forall p \text{ L.}$ (prob p (NOR_FT_gate p L) = list_prod (one_minus_list (list_prob p L)))
$F_{XOR}(t) = Pr(\bar{A}(t)B(t) \cup A(t)\bar{B}(t))$ $= (1 - F_A(t))F_B(t) +$ $F_A(t)(1 - F_B(t))$	$\vdash \forall p \text{ A B.}$ prob_space p $\wedge$ A $\in$ events p $\wedge$ B $\in$ events p $\Rightarrow$ (prob p (XOR_FT_gate p A B) = (1 - prob p A) * prob p B + prob p A * (1 - prob p B))

### D. PIE Principle

In FT analysis, the first step is to identify all the basic failure events that can cause the occurrence of the system top failure event. These failure events are then combined to model the overall fault behavior of a given system by using the fault gates. These combinations of basic failure events, called cut sets, are then reduced to minimal cut sets (MCS) by using set-theory rules, such as idempotent, associative and commutative. Then, the Probabilistic Inclusion Exclusion (PIE) principle is used to evaluate the overall failure probability of a given system based on the MCS events. According to the PIE principle, if  $A_i$  represents the  $i^{th}$  basic failure event or a combination of failure events, then the overall failure probability of a given system can be expressed as follows:

$$\mathbb{P}\left(\bigcup_{i=1}^n A_i\right) = \sum_{t \neq \{\}, t \subseteq \{1, 2, \dots, n\}} (-1)^{|t|+1} \mathbb{P}\left(\bigcap_{j \in t} A_j\right) \quad (2)$$

The above equation has been formally verified in HOL and details can be found in [17].

## IV. IMPORTANCE MEASURES

The concept of importance measure is proposed by Birnbaum mainly for components of coherent systems. This section describes the essential properties of a coherent system that is then followed by the commonly used importance measures and their respective formalizations in HOL.

### A. Coherent System

Let,  $\phi(\bar{x})$  be the structure function of a system functioning on the  $n$ -components state vector  $\bar{x} = (x_1, x_2, \dots, x_i, \dots, x_n)$ , where  $x_i$  is the state of the  $i^{th}$  component. According to Birnbaum [3], a system of binary state, where both the system and its components can either be in state of failure or success, is said to be coherent if its structure function,  $\phi(\bar{x})$ , satisfies the following conditions:

- (1)  $\phi(\bar{0}) = 0$  with  $\bar{0} = (0, 0, \dots, 0)$
- (2)  $\phi(\bar{1}) = 1$  with  $\bar{1} = (1, 1, \dots, 1)$
- (3)  $\phi(\bar{x}) \leq \phi(\bar{y})$  if  $\bar{x} \leq \bar{y}$  with relationship  $\bar{x} \leq \bar{y}$  means  $x_i \leq y_i, \forall i = 1, 2, \dots, n$ .

The first two conditions state that a system must go in state 0 (full working) or 1 (complete failure) if all of its components are in state 0 or 1, respectively. The third condition defines the monotonicity property of a system structure function ensuring that a component in working state must not contribute in causing a system failure and vice versa. The use of the NOT gate in a FT model (structure function) results in a non-coherent structure, which also means that components not failing, i.e., working, can contribute to a system failure event and thus violating the condition (3). Therefore, the use of the NOT logic is often discouraged [23].

In order to formally verify that a given failure structure function (FT model) satisfies the Birnbaum coherent system conditions, we first formally define a structure function in HOL as follows:

**Definition 1:**  $\vdash \forall f \text{ L. } \phi \text{ f L} = f \text{ L}$

where  $\phi$  is a HOL Unicode character that is used as a pretty-printing of the function `coherent_struct` mapping an arbitrary real-valued function  $f : (\alpha \rightarrow bool) \rightarrow real$  to a list of sets  $L : (\alpha \rightarrow bool)list$ . Using the above definition, Conditions (1-2) can be verified in HOL on a given fault tree (structure function) consisting of AND and OR FT gates as:

**Theorem 1:**  $\vdash \forall p \text{ L.}$   
prob\_space p  $\wedge$   $\neg$ NULL L  $\wedge$   
coherent\_state\_vec ( $\lambda a. a = \{\}$ ) (FLAT L)  $\Rightarrow$

```

(prob p
  (φ (λb.
    FTree p ((OR of
      (λa. AND (gate_list a))) b)) L) = 0)

```

**Theorem 2:**  $\vdash \forall p L.$   
 $\text{prob\_space } p \wedge \neg \text{NULL } L \wedge$   
 $\text{coherent\_state\_vec}$   
 $(\lambda a. a = \text{p\_space } p) (\text{FLAT } L) \Rightarrow$   
 $(\text{prob } p$   
 $(\phi (\lambda b.$   
 $\text{FTree } p ((\text{OR of}$   
 $(\lambda a. \text{AND } (\text{gate\_list } a))) b)) L) = 1)$

where, the HOL function FLAT is used to flatten the two-dimensional list, i.e., to transform a list of lists, into a single list. The assumptions in the above theorems are almost similar. The first two assumptions ensure that the variable  $p$  is a valid probability space and the given list of state vectors is not empty. In the last assumption, the function coherent\_state\_vec asserts that all the system components are either in fully working or in completely failure state, which are modeled using empty event ( $\{\}$ ) and the complete probability space ( $\text{p\_space } p$ ), respectively. The conclusions of the above theorems model the probabilistic sense of the conditions (1-2).

Now, we formally verify the Condition 3 for the given structure function in HOL as follows:

**Theorem 3:**  $\vdash \forall p L.$   
 $\text{prob\_space } p \wedge$   
 $\text{in\_events } p (\text{FLAT } (\text{XL\_vec } L)) \wedge$   
 $\text{in\_events } p (\text{FLAT } (\text{YL\_vec } L)) \wedge$   
 $\text{mem\_subset\_vec } L \Rightarrow$   
 $\text{prob } p$   
 $(\phi (\lambda b.$   
 $\text{FTree } p ((\text{OR of}$   
 $(\lambda a. \text{AND } (\text{gate\_list } a))) b)) (\text{XL\_vec } L)) \leq$   
 $\text{prob } p$   
 $(\phi (\lambda b.$   
 $\text{FTree } p ((\text{OR of}$   
 $(\lambda a. \text{AND } (\text{gate\_list } a))) b)) (\text{YL\_vec } L))$

where the function in\_events ensures that each element of a given list belongs to a valid event space  $p$ . The functions XL\_vec and YL\_vec returns the first and second member of the two-dimensional pair list, respectively. The relationship between these two lists, XL\_vec and YL\_vec, is described by the function mem\_subset\_vec, which ensures that each member of XL\_vec list is a subset of the corresponding member of YL\_vec list. The conclusion of the above theorem models Condition 3. The proof of Theorem 3 follows from the fact that if  $A \subseteq B$ , then their corresponding probabilities satisfy the monotonicity property, i.e.,  $\Pr(A) \leq \Pr(B)$ .

### B. Birnbaum Importance

For a coherent system of  $n$ -components with independent failures, the Birnbaum importance ( $I_B^{(i)}$ ) of component  $i$  is defined as a probability that the  $i^{\text{th}}$  component is critical to the system failure or functioning. Mathematically, it can be expressed as follows [3]:

$$\frac{\partial h(\bar{x})}{\partial p_i} = I_B^{(i)}(\phi(\bar{x})) = \Pr\{\phi((1_i, \bar{x}))\} - \Pr\{\phi((0_i, \bar{x}))\} \quad (3)$$

where  $\phi(\bar{x})$  represents the structure function of a given coherent system, which is applied on components state vector  $\bar{x}$  and returns the corresponding state of a system. The notations  $\phi((1_i, \bar{x}))$  and  $\phi((0_i, \bar{x}))$  represent the state of a system if the  $i^{\text{th}}$  component is updated with the state values 1 (failure) and 0 (working), respectively.

To formalize Equation 3 in HOL, we first formally define the notion of component state update in a given structure function as follows:

**Definition 2:**  $\vdash \forall i f L.$   
 $\phi' e i f L = \phi f (\text{LUPDATE } e i L)$

where the HOL function LUPDATE updates the given list  $L$  with element  $e$  at index  $i$ . The above function updates the state of the component  $i$  in a state vector  $L$  before passing it to the system structure function. Similarly, we can formally define a function to update the states of any two system components in HOL as follows:

**Definition 3:**  $\vdash \forall e e' i j f L.$   
 $\phi'' e e' i j f L =$   
 $\phi f (\text{LUPDATE } e' j (\text{LUPDATE } e i L))$

Now, using Definition 2, we can formally model Equation 3 in HOL as follows:

**Definition 4:**  $\vdash \forall p i f L.$   
 $I_\beta p i f L =$   
 $\text{prob } p (\phi' (\text{p\_space } p) i f L) -$   
 $\text{prob } p (\phi' \{\} i f L)$

As described earlier in Section I, Meng [7] developed the analytical relationship describing the relative importance of any pair of system components and obtained the necessary conditions based on Boland and Birnbaum importance measures. We formally verify this relationship in HOL as follows:

**Theorem 4:** Meng [7]: Suppose that  $i \stackrel{c}{=} j$  and  $\frac{\partial^2 h(\mathbf{x})}{\partial p_i \partial p_j} \geq 0$  for all  $\mathbf{x}$ . Then,  $I_\beta(j, \mathbf{x}) \leq I_\beta(i, \mathbf{x})$  for all  $\mathbf{x}$  satisfying  $p_i \leq p_j$ .

```

⊢ ∀ p L i j.
[A1]: prob_space p ∧ in_events p L ∧
[A2]: ¬NULL L ∧ i < j ∧
[A3]: mutual_indep p
      ({} :: {} :: p_space p :: p_space p :: L) ∧
[A4]: SUC (SUC j) < LENGTH L ∧
[A5]: I''_β p i j
      (λa. FTree p (AND (gate_list a))) L ≥ 0 ∧
[A6]: prob p (EL i L) ≤ prob p (EL j L) ⇒
(I_β p j (λa. FTree p (AND (gate_list a))) L ≤
I_β p i (λa. FTree p (AND (gate_list a))) L)

```

In the above statement, the symbol  $i \stackrel{c}{=} j$  is described by Boland et al. [6] as components  $i$  and  $j$  are permutation equivalent if  $\phi(1_i, 0_j, \mathbf{x}) = \phi(0_i, 1_j, \mathbf{x})$  for all  $\mathbf{x}$ . Using Definition 3, we formally verify this property in HOL as follows:

**Lemma 1:**  $\vdash \forall p \ i \ j \ L. \text{prob\_space } p \wedge i < j \wedge$   
 $\text{in\_events } p \ L \wedge \text{SUC } (\text{SUC } j) < \text{LENGTH } L \wedge$   
 $\text{mutual\_indep } p \ (\{\} :: p\_space \ p :: L) \Rightarrow$   
 $(\text{prob } p \ (\phi'' \ (p\_space \ p) \ \{\} \ i \ j$   
 $\ (\lambda a. \text{FTree } p \ (\text{AND } (\text{gate\_list } a))) \ L) =$   
 $\text{prob } p \ (\phi'' \ \{\} \ (p\_space \ p) \ i \ j$   
 $\ (\lambda a. \text{FTree } p \ (\text{AND } (\text{gate\_list } a))) \ L))$

Similarly, the notation  $\frac{\partial^2 h(x)}{\partial p_i \partial p_j}$  is a partial differentiation w.r.t probability of components  $i$  and  $j$  that can be represented mathematically as:

$$\frac{\partial^2 h(x)}{\partial p_i \partial p_j} = \text{Pr}(\phi''(1_i, 1_j, \mathbf{x})) - \text{Pr}(\phi'(1_i, 0_j, \mathbf{x})) - \text{Pr}(\phi''(0_i, 1_j, \mathbf{x})) + \text{Pr}(\phi''(0_i, 0_j, \mathbf{x})) \quad (4)$$

The above equation is formalized using Definition 3 and it is represented by the function  $I''_{\beta}$  in the assumption (A5) of Theorem 4.

The assumptions of Theorem 4 are similar to the ones used in Theorems 1-3. The inclusion of  $\{\}$  and  $p\_space \ p$  in assumption (A3) reflects the change caused by flipping the state of the  $i$  and  $j$  components and also makes sure that they are mutually independence. The assumption (A4) ensures that the index  $j$  starts after two increments since we require at least two components in a list. Although a brief proof sketch of Theorem 4 is described by Meng [7], the sound environment of the HOL theorem prover provides additional formal guarantees in the verification of Theorem 4 accompanying all the necessary conditions. The formal proof of Theorem 4 utilizes several essential lemmas, which can be found in [24].

### C. Other Common Types of Importance Measures

Another well-known importance measure is Fussell-Vesely [1], which describes the importance of component  $i$  as a probability that the failure of component  $i$  contributes to a system failure given that system fails. It can be expressed mathematically as follows:

$$I_{FV} = \frac{\text{Pr}(\phi(\mathbf{x})) - \text{Pr}(\phi'(1_i, \mathbf{x}))}{\text{Pr}(\phi(\mathbf{x}))} \quad (5)$$

We can formally define the above function by using Definitions 1-2 in HOL as follows:

**Definition 5:**  $\vdash \forall f \ i \ L.$

$$I_{FV} \ p \ i \ f \ L = \frac{\text{prob } p \ (\phi \ f \ L) - \text{prob } p \ (\phi' \ (p\_space \ p) \ i \ f \ L)}{\text{prob } p \ (\phi \ f \ L)}$$

Similarly, the criticality importance measures Reduction Worth ( $I_{RW}$ ) and Achievement Worth ( $I_{AW}$ ) describe a probability when component  $i$  is always functioning and failed, respectively. They can be expressed as follows:

$$I_{RW} = \frac{\text{Pr}(\phi(\mathbf{x}))}{\text{Pr}(\phi'(1_i, \mathbf{x}))} \quad (6)$$

$$I_{AW} = \frac{\text{Pr}(\phi'(0_i, \mathbf{x}))}{\text{Pr}(\phi(\mathbf{x}))}$$

Using Definitions 1-2, we formally define the above functions in HOL as follows:

**Definition 6:**  $\vdash \forall f \ i \ L.$

$$I_{RW} \ p \ i \ f \ L = \frac{\text{prob } p \ (\phi \ f \ L)}{\text{prob } p \ (\phi' \ (p\_space \ p) \ i \ f \ L)}$$

**Definition 7:**  $\vdash \forall f \ i \ L.$

$$I_{AW} \ p \ i \ f \ L = \frac{\text{prob } p \ (\phi' \ (\{\}) \ i \ f \ L)}{\text{prob } p \ (\phi \ f \ L)}$$

The HOL formalization of the above-mentioned importance measures is also available at [24]. The proof script of the above formalizations and proofs consists of about 1400 lines of HOL code that roughly took 70 man-hours of development time. To illustrate the effectiveness of our proposed approach, we conduct the formal importance measure analysis of a railway signaling system at Moroccan level crossing in the next section.

## V. SIGNALING SYSTEM AT MOROCCAN LEVEL CROSSING

There are three main parts in the Moroccan level crossing railway signaling (LC) system [10]: (1) Rail part consisting of a material component (train and rail-road), and human component (the train operator); (2) Road part containing a material component (vehicle and road), and a human component (vehicle driver); and (3) Level crossing, which is further composed of three main components: (i) Power and communication network between the components of the railway signaling system; (ii) Control component consisting of Programmable Logic Controller and its program; (iii) Operative component representing sensors, such as road lights, the alarms and the barriers. Table IV describes the basic failure events along with the corresponding failure rates ( $\lambda$ ) associated with the components of Moroccan signaling system [10]. The FT diagram of the signaling system at Moroccan LC is depicted in Figure 1 [10].

TABLE IV. EVENTS FOR SIGNALING SYSTEM AT MOROCCAN LC

Symbol	Basic Events	$\lambda \ (h^{-1})$
x1	Vehicle Failure	$18 * 10^{-3}$
x2 & x4	Human Factor	$1.347 * 10^{-4}$
x3	Rail Failure	$2.85 * 10^{-6}$
x5	Program Error	$5 * 10^{-8}$
x6	Programmable Logic Controller Failure	$4 * 10^{-6}$
x7	Network Communication Failure	$5 * 10^{-6}$
x8	Power Network Failure	$5 * 10^{-6}$
x9 & x10	Alarm Failure	$4 * 10^{-4}$
x11 & x12	Light Failure	$4 * 10^{-4}$
x13 & x14	Motor Failure	$3 * 10^{-6}$
x15 & x16	Transmission System Failure	$5 * 10^{-5}$

### A. Formal Model and Failure Analysis

Using the FT gates, described in Section III-C, we can formally model the FT diagram of the Moroccan signaling system in HOL as follows:

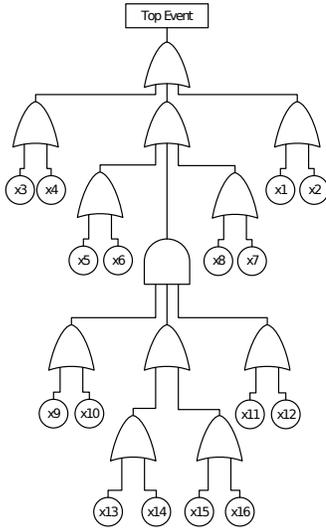


Fig. 1. FT of the Signaling System at Moroccan LC

**Definition 8:**  $\vdash \text{Signal\_FT } p \ x1 \ x2 \ \dots \ x16 \ t =$   
 $\text{FTree } p \ (\text{OR } [\text{OR } ([\omega \ p \ x3 \ t; \omega \ p \ x4 \ t])$   
 $\text{OR } ([\omega \ p \ x5 \ t; \omega \ p \ x6 \ t])]);$   
 $\text{AND } [\text{OR } ([\omega \ p \ x9 \ t; \omega \ p \ x10 \ t]);$   
 $\text{OR } ([\omega \ p \ x13 \ t; \omega \ p \ x14 \ t]);$   
 $\text{OR } ([\omega \ p \ x15 \ t; \omega \ p \ x16 \ t]);$   
 $\text{OR } ([\omega \ p \ x11 \ t; \omega \ p \ x12 \ t])]);$   
 $\text{OR } ([\omega \ p \ x7 \ t; \omega \ p \ x8 \ t]);$   
 $\text{OR } ([\omega \ p \ x1 \ t; \omega \ p \ x2 \ t])]);$

where  $\omega \ p \ x \ t$  represent various failure events, such as an alarm, associated with the various component of the Moroccan signaling system. It is defined in HOL as  $\text{PREIMAGE } x \ \{y \mid y \leq t\} \cap \text{p\_space } p$  [17].

Now, we obtain the minimal cut sets (MCS) of the above FT model by utilizing some set properties, like distribution of intersection over union and idempotent law of intersection [9].

$$C_1 = \{x3, x4, x5, x6\}, C_2 = \{x9, x13, x15, x11\}, \dots, \quad (7)$$

$$C_{17} = \{x10, x14, x16, x12\}, C_{18} = \{x7, x8, x1, x2\}$$

We can also formally verify the equivalence of the obtained signaling system MCS with the original FT model as follows:

**Lemma 2:**  $\vdash \text{Signal\_FT } p \ x1 \ x2 \ \dots \ x16 \ t =$   
 $(\lambda b.$

$$\text{FTree } p \ ((\text{OR of}$$
  
 $(\lambda a. \text{AND } (\text{gate\_list } a))) \ b))$   
 $[\omega \ L \ p \ [x3; x4; x5; x6] \ t;$   
 $\omega \ L \ p \ [x9; x13; x15; x11] \ t; \dots;$   
 $\omega \ L \ p \ [x10; x14; x16; x12] \ t;$   
 $\omega \ L \ p \ [x7; x8; x1; x2] \ t]$ 

where the function  $\omega \ L \ p \ L \ t$  returns the list of events by mapping the function  $\omega \ p \ x \ t$ , described in Definition 8, on each element of the given list of random variables.

By using the above lemma and Definition 8, the failure probability of the Moroccan signaling system can be formally verified in HOL as follows:

**Theorem 6:**  $\vdash \forall p \ x1 \ x2 \ \dots \ x16 \ c1 \ c2 \ \dots \ c16 \ t.$

$$[A1]: 0 \leq t \wedge$$

$$[A2]: \text{FT\_conds } p \ [x1; x2; \dots; x16] \ t$$

$$[A3]: \text{exp\_dist\_list } p \ [x1; x2; \dots; x16]$$

$$[c1; c2; \dots; c16] \Rightarrow$$

$$(\text{prob } p \ (\text{Signal\_FT } p \ x1 \ x2 \ \dots \ x16 \ t) =$$

$$1 - e^{-(\lambda_{c3}t)} * e^{-(\lambda_{c4}t)} * e^{-(\lambda_{c5}t)} * e^{-(\lambda_{c6}t)} *$$

$$e^{-(\lambda_{c7}t)} * e^{-(\lambda_{c8}t)} * e^{-(\lambda_{c1}t)} * e^{-(\lambda_{c2}t)} *$$

$$(1 - (1 - e^{-(\lambda_{c9}t)} * e^{-(\lambda_{c10}t)} *$$

$$(1 - e^{-(\lambda_{c13}t)} * e^{-(\lambda_{c14}t)} *$$

$$(1 - e^{-(\lambda_{c15}t)} * e^{-(\lambda_{c16}t)} *$$

$$(1 - e^{-(\lambda_{c11}t)} * e^{-(\lambda_{c12}t))))))$$

where the function  $\text{exp\_dist\_list}$  takes a list of random variables and a list of failure rates and makes sure that each random variable is exponentially distributed and assigned with its corresponding failure rates [17], i.e.,  $\text{exp\_dist\_list } [x1; x2] \ [c1; c2] = (!t. 0 \leq t \implies ((\text{Pr}(\omega \ p \ x1 \ t) = 1 - e^{-\lambda_{c1}t}) \wedge (\text{Pr}(\omega \ p \ x2 \ t) = 1 - e^{-\lambda_{c2}t})))$ . The function  $\text{FT\_conds}$  contains two predicates  $\text{mutual\_indep}$  and  $\text{in\_events}$ , which ensure that all events associated to  $\text{rail\_signal\_FT}$  are mutually independent and belong to events space  $p$ , respectively. The proof of Theorem 6 is based on formally verified expressions of the AND and OR FT gates, presented in Table III, and the PIE principle described in Section III-D.

To evaluate Theorem 6, we wrote an ML function  $\text{auto\_signal\_morco\_FT}$  [24] that takes failure rates and time index, given in Table IV, and returns the following in HOL environment:

**Under the following assumptions**

$$\vdash [A1]: 0 \leq 5 \wedge$$

$$[A2]: \text{FT\_conds } p \ [x1; x2; \dots; x16] \ 5$$

$$[A3]: \text{exp\_dist\_list } p \ [x1; x2; \dots; x16]$$

$$[0.00000285; 0.00000005; \dots; 0.0004] \Rightarrow$$

**Failure probability of Moroccan Railway Signaling System**

$$(\text{prob } p \ (\text{Signal\_FT } p \ x1 \ x2 \ \dots \ x16 \ 5) =$$

$$0.0003494028541)$$

We can also plot these values to get a better understanding of the dependability of the Moroccan signaling system as given in Figure 2. It can be observed from the plot that initially the probability of failure is very low but as the time passes, in hours, the failure probability gradually increases and at 2,000 hours the failure becomes absolutely certain, i.e., with a probability 1.

## B. Formal Importance Measure Analysis

As described in Section IV, the importance measure analysis requires the given system structure function to be coherent in nature. Therefore, we start by formally verifying the conditions of a coherent system for the railway signaling system MCS, described in Lemma 2, in HOL as:

**Theorem 7:**  $\vdash$

$$\text{prob\_space } p \wedge$$

$$\text{coherent\_state\_vec } (\hat{\text{I}}z a. a = \{\}) \ (\text{FLAT}$$

$$[\omega \ L \ p \ [x3; x4; x5; x6] \ t;$$

$$\omega \ L \ p \ [x9; x13; x15; x11] \ t; \dots;$$

$$\omega \ L \ p \ [x10; x14; x16; x12] \ t];$$

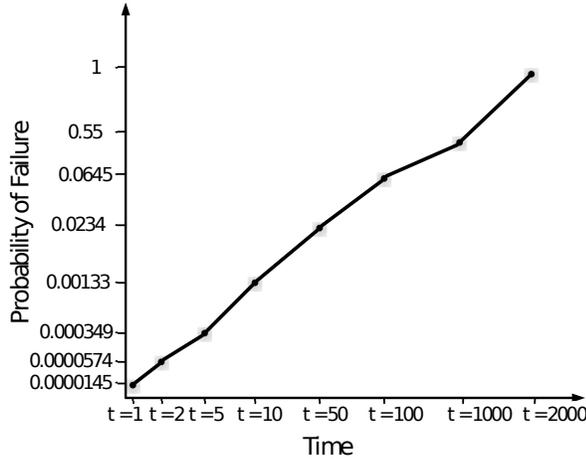


Fig. 2. Plot for Probability of Failure of Signaling System at Moroccan Level Crossing

```

ωL p [x7;x8;x1;x2] t)) ⇒
(prob p
  (φ (λb.
    FTree p((OR of
      (λa. AND (gate_list a))) b))
    [ωL p [x3;x4;x5;x6] t;
      ωL p [x9;x13;x15;x11] t;...;
      ωL p [x10;x14;x16;x12] t;
      ωL p [x7;x8;x1;x2] t]) = 0)

```

**Theorem 8:** ⊢

```

prob_space p ∧
coherent_state_vec (Îza. a = p_space p) (FLAT
  [ωL p [x3;x4;x5;x6] t;
    ωL p [x9;x13;x15;x11] t;...;
    ωL p [x10;x14;x16;x12] t;
    ωL p [x7;x8;x1;x2] t]) ⇒

```

```

(prob p
  (φ (λb.
    FTree p((OR of
      (λa. AND (gate_list a))) b))
    [ωL p [x3;x4;x5;x6] t;
      ωL p [x9;x13;x15;x11] t;...;
      ωL p [x10;x14;x16;x12] t;
      ωL p [x7;x8;x1;x2] t]) = 1)

```

**Theorem 9:** ⊢

```

prob_space p ∧
(!t. in_events p (FLAT
  [ωL p [x3;x4;x5;x6] t;
    ωL p [x9;x13;x15;x11] t;...;
    ωL p [x10;x14;x16;x12] t;
    ωL p [x7;x8;x1;x2] t])) ∧

```

$t_1 < t_2 \Rightarrow$

```

prob p
  (φ (λb.
    FTree p((OR of
      (λa. AND (gate_list a))) b))
    [ωL p [x3;x4;x5;x6] t1;
      ωL p [x9;x13;x15;x11] t1;...;
      ωL p [x10;x14;x16;x12] t1;
      ωL p [x7;x8;x1;x2] t1]) ≤

```

```

prob p
  (φ (λb.
    FTree p ((OR of

```

```

(λa. AND (gate_list a))) b))
[ωL p [x3;x4;x5;x6] t2;
ωL p [x9;x13;x15;x11] t2;...;
ωL p [x10;x14;x16;x12] t2;
ωL p [x7;x8;x1;x2] t2])

```

It can be seen that Theorems 7-8 are formally verified based on a very straight-forward utilization of Theorems 1-2, described in Section IV-A, on a given list of railway signaling MCS. Similarly, Theorem 9 is formally verified by utilizing Theorem 3 by discharging the assumption `mem_subset_vec` based on the fact that by increasing the time-of-failures, i.e.,  $t_1 \leq t_2$ , the corresponding failure probabilities also monotonically increase.

**C. Formal Birnbaum Importance Measure Analysis**

After formally satisfying the conditions for coherent system on the railway signaling system failure model, we can now determine the Birnbaum importance measure of any component of the railway signaling system. For illustration purposes, we describe the formal importance measure analysis of an alarm failure ( $x_9$ ) in the railway signaling system by utilizing Definition 4 and the FT model, described in Definition 8, in HOL as:

**Definition 9:**  $\vdash I_{\beta}^9 p \ x_1 \ x_2 \ x_3 \ \dots \ x_{16} \ t =$

```

I_{\beta} p 0
  (λb. FTree p (OR [OR ([ω p x3 t; ω p x4 t])
    OR ([ω p x5 t; ω p x6 t]);
    AND [OR b ;
      OR ([ω p x13 t; ω p x14 t]);
      OR ([ω p x15 t; ω p x16 t]);
      OR ([ω p x11 t; ω p x12 t]);
      OR ([ω p x7 t; ω p x8 t]);
      OR ([ω p x1 t; ω p x2 t])]])
    ([ω p x9 t; ω p x10 t]))

```

The above model can also be used to quantitatively analyze the Birnbaum importance of alarm failure by associating the exponential distribution to each component of the railway signaling system as:

**Theorem 10:**  $\vdash \forall p \ x_1 \ x_2 \ \dots \ x_{16} \ c_1 \ c_2 \ \dots \ c_{16} \ t.$

```

[A1]: 0 ≤ t ∧
[A2]: prob_space p ∧
[A3]: mutual_indep p (ωL p
  [x1; x2; ...; x16] t) ∧
[A4]: in_events p (ωL p
  [x1; x2; ...; x16] t) ∧
[A5]: exp_dist_list p [x1;x2; ... ;x16]
  [c1;c2;...;c16] ⇒
(I_{\beta}^9 p x1 x2 x3 ... x16 t =
  e^{-λ_{c3}*t} * e^{-λ_{c4}*t} * e^{-λ_{c5}*t} * e^{-λ_{c6}*t} *
  e^{-λ_{c7}*t} * e^{-λ_{c8}*t} * e^{-λ_{c2}*t} * e^{-λ_{c1}*t} * e^{-λ_{c10}*t} *
  (1 - e^{-λ_{c13}*t} * e^{-λ_{c14}*t}) *
  (1 - e^{-λ_{c15}*t} * e^{-λ_{c16}*t}) *
  (1 - e^{-λ_{c11}*t} * e^{-λ_{c12}*t}))

```

The assumptions of the above theorem is quite similar to the ones used in Theorem 6. It can be observed from the conclusion of Theorem 9 that the importance of alarm failure component ( $x_9$ ) is calculated from the failure probabilities of other components in the FT model.

Similarly, we can also determine the Fussell-Vesely importance measure for the alarm component by using Definition 5 in HOL as follows:

**Theorem 11:**  $\vdash \forall p \ x1 \ x2 \ \dots \ x16 \ c1 \ c2 \ \dots \ c16 \ t.$

```
[A1]: 0 ≤ t ∧
[A2]: prob_space p ∧
[A3]: mutual_indep p (ωL p
[x1; x2; ...; x16] t) ∧
[A4]: in_events p (ωL p
[x1; x2; ...; x16] t) ∧
[A5]: exp_dist_list p [x1;x2; ... ;x16]
[c1;c2;...;c16] ⇒
(I_FV_9 p x1 x2 x3 ... x16 t =
(1 - e-(λc3*t)) * e-(λc4*t)) * e-(λc5*t)) *
...
(1 - e-(λc9*t)) * e-(λc10*t)) *
(1 - e-(λc13*t)) * e-(λc14*t)) *
(1 - e-(λc15*t)) * e-(λc16*t)) *
(1 - e-(λc11*t)) * e-(λc12*t)) -
(1 - e-(λc3*t)) * e-(λc4*t)) * e-(λc5*t)) *
...
(1 - e-(λc13*t)) * e-(λc14*t)) *
(1 - e-(λc15*t)) * e-(λc16*t)) *
(1 - e-(λc11*t)) * e-(λc12*t)) /
(1 - e-(λc3*t)) * e-(λc4*t)) * e-(λc5*t)) *
...
(1 - e-(λc9*t)) * e-(λc10*t)) *
(1 - e-(λc13*t)) * e-(λc14*t)) *
(1 - e-(λc15*t)) * e-(λc16*t)) *
(1 - e-(λc11*t)) * e-(λc12*t)))
```

By using the above-mentioned approach, we can formally determine the Reduction Worth (RW) and Achievement Worth (AW) importance measures, given in Equation 6. Next, we conduct the formal relative importance measure analyses of relative importance among alarm and vehicle failure, using Theorem 4, as follows:

**Theorem 12:**  $\vdash \forall p \ x1 \ x2 \ \dots \ x16 \ c1 \ c2 \ \dots \ c16 \ t.$

```
[A1]: 0 ≤ t ∧
[A2]: prob_space p ∧
[A3]: mutual_indep p (ωL p
[x1; x2; ...; x16] t) ∧
[A4]: in_events p (ωL p
[x1; x2; ...; x16] t) ∧
[A5]: exp_dist_list p [x1;x2; ... ;x16]
[c1;c2;...;c16] ∧
[A6]: fail_rate_pos [c1;c2;...;c16] ∧
[A7]: c9 ≤ c1 ⇒
Iβ9 p x1 x2 x3 ... x16 t ≤
Iβ1 p x1 x2 x3 ... x16 t
```

where the function `fail_rate_pos`, in assumption (A6), ensures that the given list of failure rates must be positive. It can be implied from assumption (A7) that the Birnbaum relative importance of any two components in a system is related by their failure rates relationship. In other words, a component with higher failure rate is highly critical in a FT model (structure function) compared to a component with lower failure rate. The proof of Theorem 12 is based on Theorem 4 and some fundamental facts of probability

theory. The HOL proof script of Theorems 6-12, which can be downloaded from [24], took about 1200 lines of HOL code and about 24 man-hours.

It is quite evident that our proposed HOL-based formalization approach provides the required rigor to the importance measure properties about system components compared to [10]. Also, all the necessary conditions are accompanying the formally verified properties. Most importantly, the formal relative importance measure analysis reveals that the relative importance of any pair of components is related according to their failure rates (Theorem 12). In other words, we can accurately analyze the components' importance, due to the sound theorem proving approach, without using the traditional methods of ranking the system components for large systems. By conducting the formal importance analysis of the railway signaling system at a Moroccan LC, we believe that our proposed approach provides a sound framework to reliability design engineers to meet the quality standards of their safety-critical systems.

## VI. CONCLUSION

In this paper, we formalized the commonly used importance measures, such as Birnbaum, Fussell-vesely, Reduction worth and Achievement worth, in HOL theorem proving. We also formalized Meng's approach of obtaining the relative importance measure among any pair of system components. For illustration purposes, we conducted the formal importance measure analysis of a signaling system at a Moroccan level crossing consisting of traffic lights, programmable logic controllers and alarms, within the HOL theorem proving environment. We plan to extend the formalization of Fussell-vesely importance measure to obtain the relative importance of system components. Just like the Birnbaum importance measure, it has great potential to highlight the critical components without running the computationally expensive simulations.

## REFERENCES

- [1] W. Kuo and X. Zhu, *Importance Measures in Reliability, Risk, and Optimization: Principles and Applications*. John Wiley & Sons, 2012.
- [2] P. Rooney, "Microsoft's CEO: 80-20 Rule Applies to Bugs, Not Just Features," 2019. [Online]. Available: <https://www.crn.com/news/security/18821726/microsofts-ceo-80-20-rule-applies-to-bugs-not-just-features.htm>
- [3] Z. W. Birnbaum, "On the importance of Different Components in a Multicomponent System," University of Washington, Seattle, Washington, USA, Tech. Rep., 1968. [Online]. Available: <http://www.dtic.mil/dtic/tr/fulltext/u2/670563.pdf>
- [4] J. F. Espiritu, D. W. Coit, and U. Prakash, "Component Criticality Importance Measures for the Power Industry," *Electric Power Systems Research*, vol. 77, no. 5-6, pp. 407-420, 2007.
- [5] ReliaSoft, 2019. [Online]. Available: <https://www.weibull.com/hotwire/issue66/reliasics66.htm>
- [6] P. J. Boland, F. Proschan, and Y. L. Tong, "Optimal Arrangement of Components via Pairwise Rearrangements," *Naval Research Logistics*, vol. 36, no. 6, pp. 807-815, 1989.
- [7] F. C. Meng, "Comparing Birnbaum Importance Measure of System Components," *Probability in the Engineering and Informational Sciences*, vol. 18, no. 2, pp. 237-245, 2004.
- [8] J. Harrison, *Handbook of Practical Logic and Automated Reasoning*. Cambridge University Press, 2009.
- [9] IEC, "International Electrotechnical Commission, 61025 Fault Tree Analysis," 2006. [Online]. Available: <https://webstore.iec.ch/publication/4311>

- [10] J. Boudnnaya, A. Mkhida, and M. Sallak, "A Dependability Analysis of a Moroccan Level Crossing Based on Fault Tree Analysis and Importance Measures," in *MOdeling, Optimization and SIMlation*, 2014, pp. 1–5, [https://recif.hds.utc.fr/wp-content/uploads/2014/11/MOSIM\\_2014\\_1.pdf](https://recif.hds.utc.fr/wp-content/uploads/2014/11/MOSIM_2014_1.pdf).
- [11] HOL Interactive Theorem Prover, 2019. [Online]. Available: <https://hol-theorem-prover.org/>
- [12] W. Ahmad, "Formal Dependability Analysis using Higher-order-logic Theorem Proving," PhD Thesis, National University of Sciences and Technology, Islamabad, Pakistan, 2017.
- [13] K. S. Trivedi, *Probability and Statistics with Reliability, Queuing and Computer Science Applications*. John Wiley and Sons Ltd., 2002.
- [14] W. Ahmed, O. Hasan, and S. Tahar, "Formalization of Reliability Block Diagrams in Higher-order Logic," *Journal of Applied Logic*, vol. 18, pp. 19–41, 2016.
- [15] W. Ahmad, O. Hasan, and S. Tahar, *Handbook of RAMS in Railways: Theory and Practice*. Taylor and Francis, 2018, ch. Formal Reliability Analysis of Railway Systems using Theorem Proving Technique, pp. 651–668.
- [16] W. Ahmad and O. Hasan, "Towards Formal Fault Tree Analysis Using Theorem Proving," in *Intelligent Computer Mathematics*, ser. LNCS. Springer, 2015, vol. 9150, pp. 39–54.
- [17] W. Ahmad and O. Hasan, "Formalization of Fault Trees in Higher-order Logic: A Deep Embedding Approach," in *Dependable Software Engineering: Theories, Tools, and Applications*, ser. LNCS. Springer, 2016, vol. 9984, pp. 264–279.
- [18] M. J. Gordon and T. F. Melham, *Introduction to HOL A Theorem Proving Environment for Higher-order Logic*. Cambridge University Press, 1993.
- [19] A. Church, "A Formulation of the Simple Theory of Types," *Journal of Symbolic Logic*, vol. 5, pp. 56–68, 1940.
- [20] R. Milner, "A Theory of Type Polymorphism in Programming," *Journal of Computer and System Sciences*, vol. 17, pp. 348–375, 1977.
- [21] T. Mhamdi, O. Hasan, and S. Tahar, "On the Formalization of the Lebesgue Integration Theory in HOL," in *Interactive Theorem Proving*, ser. LNCS. Springer, 2011, vol. 6172, pp. 387–402.
- [22] W. Ahmad, O. Hasan, S. Tahar, and M. S. Hamdi, "Towards the Formal Reliability Analysis of Oil and Gas Pipelines," in *Intelligent Computer Mathematics*, ser. LNCS. Springer, 2014, vol. 8543, pp. 30–44.
- [23] J. D. Andrews and S. C. Beeson, "Birnbaum's Measure of Component Importance for Noncoherent Systems," *IEEE Transcation on Reliability*, vol. 52, no. 2, pp. 213–219, 2003.
- [24] W. Ahmad, "On the Formalization of Importance Measures using HOL Theorem Proving," 2019. [Online]. Available: [https://github.com/ahmedwaqar/Formal-Dependability/tree/importance\\_measures/Importance\\_Measures](https://github.com/ahmedwaqar/Formal-Dependability/tree/importance_measures/Importance_Measures)