Formal Lifetime Reliability Analysis Using Continuous Random Variables

Naeem Abbasi, Osman Hasan, and Sofiène Tahar

Dept. of Electrical & Computer Engineering, Concordia University
1455 de Maisonneuve W., Montreal, Quebec, H3G 1M8, Canada
{n_ab,o_hasan,tahar}@ece.concordia.ca

Abstract. Reliability has always been an important concern in the design of engineering systems. Recently proposed formal reliability analysis techniques have been able to overcome the accuracy limitations of traditional simulation based techniques but can only handle problems involving discrete random variables. In this paper, we extend the capabilities of existing theorem proving based reliability analysis by formalizing several important statistical properties of continuous random variables, for example, the second moment and the variance. We also formalize commonly used reliability theory concepts of survival function and hazard rate. With these extensions, it is now possible to formally reason about important reliability measures associated with the life of a system, for example, the probability of failure and the mean-time-to-failure of the system operating in an uncertain and harsh environment, which is usually continuous in nature. We illustrate the modeling and verification process with the help of an example involving the reliability analysis of electronic system components.

1 Introduction

Tragedies such as the industrial accident in the union carbide pesticide plant in Bhopal India [2], space shuttles Columbia and Challenger accidents [18], and the high-speed train accident near the village of Eschede in Lower Saxony in Germany [13] all highlight the importance of design reliability in various disciplines of engineering. The reliability of a system is defined as the probability that it will adequately perform its specified purpose for a specified period of time under the specified environmental conditions [14]. The two most popular representations of the distribution of the lifetime of a system are the survival function and the hazard function [14]. The survival function describes the probability that a system is functioning at any time t, and the hazard function describes the failure risk at a time t.

Traditionally, reliability analysis has been done using paper and pencil and simulation based approaches. In engineering applications, the paper and pencil approach very quickly becomes impractical because of the amount of detail involved. Simulation based reliability analysis is popular because of the availability of a number of automated tools. Unfortunately, the simulation based analysis

A. Dawar and R. de Queiroz (Eds.): WoLLIC 2010, LNAI 6188, pp. 84–97, 2010.

is neither accurate not can it truly model random behavior. Computer simulations rely on floating-point numbers representation of system parameters which can lead to errors in reliability analysis and thus can have costly consequences. Moreover, simulation based techniques use pseudo random number generators for simulating the random behavior and require a large amount of computing resources. Formal methods based techniques are 100% accurate and allow the modeling and analysis of true random behavior and thus provide an alternative approach for reliability analysis of the critical parts of a system.

In this paper, we build on the work of [10] and [11] and formalize important definitions of the statistical properties of continuous random variables that play an important role in reliability engineering. The work in [11] deals with discrete random variables whereas the work in [10] only presents the formal verification of expectation properties for continuous random variables. In this paper, we verify a general expression for the second moment of positive continuous random variables, that range over a positive unbounded interval $[0, \infty)$, hence suitable for modeling lifetime behavior of engineering system components.

$$E[X^2] = \lim_{n \to \infty} \left[\sum_{i=0}^{n2^n - 1} (\frac{i}{2^n})^2 P \left\{ \frac{i}{2^n} \leq X < \frac{i+1}{2^n} \right\} + nP(X \geq n) \right] \quad (1)$$

where X is the random variable and P represents the probability measure. We utilize this general expression to verify several important reliability analysis related statistical properties such as the second moment and variance of the exponential random variable.

The rest of the paper is organized as follows: Section 2 reviews related work. Section 3 presents the formalization and verification of statistical properties of continuous random variables. Section 4 describes the formalization of reliability theory concepts of survival and hazard functions. For illustration purposes, Section 5 presents the reliability analysis of a capacitor. Finally, Section 6 concludes the paper.

2 Related Work

One of the earliest example of detailed reliability studies in engineering systems dates back to 1938 [4]. In this study, factors for the improvement of service reliability for electrical power systems were considered. In the field of electronics the concepts of reliability were initially introduced after second world war to improve the performance of communication and navigational systems [16].

In order to predict the reliability one must model the system and its constituent components in such a way that captures the failure mechanisms. For example in case of electronic systems a method called the part failure method has been shown to be very accurate [5]. This method has been extensively used by military engineers to predict useful life times of systems and to develop highly reliable systems and equipments. This method is based on calculation of failure rates of individual components that make up the system and then by using appropriate formulas transform it into the reliability of the whole system. Standards

such as [6,7,17] are some of the examples which specify adequate performance requirements and environmental conditions for reliability modeling, analysis, and risk assessment.

In order to analyze systems formally in a theorem proving environment it is important to have an infrastructure for reasoning about the underlying mathematical concepts of probability and statistics. Until recently it was only possible to reason about reliability problems that involved discrete random variable in a theorem proving environment. Hurd [12] formalized a probability theory and discrete random variables in the HOL theorem prover [8]. Building upon [12], Hasan [9] formalized statistical properties of single and multiple discrete random variables. Hasan [9] also formalized a class of continuous random variables for which the inverse CDF functions can be expressed in a closed form. Hasan *et. al* [11] presented higher-order-logic formalizations of some core reliability theory concepts and successfully formalized and verified the conditions for almost always repairability for reconfigurable memory arrays in the presence of stuck-at and coupling faults. In this paper, we build upon the higher-order-logic formalization of [11], and formalize new representations of the lifetime distributions, namely the survival and hazard functions, and statistical properties such as the moments and variance of continuous random variables which was not possible in the framework presented in [11]. In [10], Hasan *et. al* formalized expectation for both bounded and unbounded continuous random variables in the HOL theorem prover. Their work utilized the Lebesgue integration theory developed in [3] and [15]. In this paper, we utilize the formalization of Borel sigma algebra of [15] and several key Lebesgue integral properties of [3].

Other formal methods based techniques, such as probabilistic model checking, can be used to analyze reliability, however, they do not have support for the verification of statistical properties (moments and variance) of the commonly used lifetime distributions [1,19]. The proposed reliability analysis approach on the other hand is capable of handling both probabilistic and statistical reliability properties.

3 Statistical Properties of Lifetime Distributions

In this section, we present the formalization of the definitions of several important statistical properties of random variables in HOL. These statistical properties summarize some of the most important aspects of the probability distribution of a random variable. For example, the coefficients of skewness is a measure of symmetry of the probability distribution of a random variable. Other formalized definitions include the expectation of a function of a random variable, first, second and n-th moments, variance, standard deviation, mean absolute deviation, and coefficients of variation and kurtosis of a random variable, as summarized in Table 1. In these formalized definitions, rv is a random variable. m represents a probability space defined as: $m = (\mathcal{U}, \mathcal{E}, \mathbb{P})$, where $\mathcal{U}$ is a sample space, $\mathcal{E}$ is a set of events, and $\mathcal{P}$ is the probability measure. The function *expec* represents the expectation or the first moment of the random variable.

Table 1. Statistical Properties and their HOL Formalizations

Property	Definition	HOL Formalization
expec. h(X)	E[h(X)]	⊢ ∀m rv h. fun_rv m rv h = expec m (λx. h (rv x))
first moment	E[X]=μ	⊢ ∀m rv. first_moment m rv = expec m (λx. rv x)
second moment	E[X^2]=μ_2	⊢ ∀m rv. second_moment m rv = expec m (λx. (rv x) pow 2)
Nth moment	E[X^N]=μ_N	⊢ ∀m rv N. nth_moment m rv N = expec m (λx. (rv x) pow N)
variance	σ^2	⊢ ∀m rv. variance m rv = expec m (λx. ((rv x) - expec m rv) pow 2)
standard deviation	σ	⊢ ∀m rv. std_dev m rv = sqrt(variance m rv)
coef. of variation	$\frac{\sigma}{\mu}$	⊢ ∀m rv. coef_of_var m rv = (std_dev m rv)/(expec m rv)
mean abs. deviation	E[$\lvert X-\mu\rvert$]	⊢ ∀m rv. m_abs_dev m rv = expec m (λx. abs((rv x) - expec m rv))
coef. of skewness	E[$(\frac{X-\mu}{\sigma})^3$] =α_3	⊢ ∀m rv. skew m rv = expec m (λx. ((rv x) - expec m rv) pow 3) /((std_dev m rv) pow 3)
coef. of kurtosis	E[$(\frac{X-\mu}{\sigma})^4$] =α_4	⊢ ∀m rv. kurt m rv = expec m (λx. ((rv x) - expec m rv) pow 4) /((std_dev m rv) pow 4)

3.1 Verification of Statistical Properties

The verification of the second moment relation for an unbounded continuous random variable, given in Equation (1), is described in this section.

Definition 1: *Second Moment of a Random Variable*

$$\vdash \forall\ \texttt{rv.}\ \texttt{second\_moment}\ (\mathcal{U},\mathcal{E},\mathbb{P})\ \texttt{rv} = \int_{\mathcal{U}} \texttt{rv}^2\ \texttt{d}\mathbb{P}$$

The function `second_moment` accepts a probability space, $(\mathcal{U},\mathcal{E},\mathbb{P})$, and a random variable rv that maps infinite Boolean sequences to real numbers [9]. In Hurd's [12] formalization of the probability space $(\mathcal{U},\mathcal{E},\mathbb{P})$, $\mathcal{U}$ represents the universal set of all Boolean sequences.

Theorem 1 formally states the second moment relation for a positive valued unbounded continuous random variable.

Theorem 1: *Second Moment of an Unbounded Random Variable*

$$\begin{aligned}\vdash\ &\forall\ \texttt{rv.}\ (\forall\ \texttt{s.}\ 0 \le \texttt{rv s}) \wedge (\forall\ \texttt{x.}\ \{\texttt{s} \mid \texttt{rv s} \ge \texttt{x}\} \in \mathcal{E})\\ &\quad (\forall\ \texttt{x y.}\ \texttt{x} < \texttt{y} \Rightarrow \{\texttt{s} \mid \texttt{x} \le \texttt{rv s} < \texttt{y}\} \in \mathcal{E}) \Rightarrow\\ &\quad \Bigg(\texttt{second\_moment}\ (\mathcal{U},\mathcal{E},\mathbb{P})\ \texttt{rv} =\\ &\lim_{\texttt{n}\to\infty}\left[\sum_{\texttt{i}=0}^{\texttt{n}2^{\texttt{n}}-1}\left(\frac{\texttt{i}}{2^{\texttt{n}}}\right)^2 \mathbb{P}\left\{\texttt{s} \;\middle|\; \frac{\texttt{i}}{2^{\texttt{n}}} \le \texttt{rv s} < \frac{\texttt{i}+1}{2^{\texttt{n}}}\right\} + \texttt{n}\mathbb{P}\left\{\texttt{s} \;\middle|\; \texttt{rv s} \ge \texttt{n}\right\}\right]\Bigg)\end{aligned}$$

The first assumption in Theorem 1 states that the random variable rv is positive. The second and third assumptions guarantee that the sets that arise in this

verification are measurable events. The entire range of the unbounded random variable is divided into two main intervals, namely $[0, n)$ and $[n, \infty)$. The first interval corresponds to $[0, n2^n - 1]$ summation term, while the second term covers the rest of the positive unbounded interval. It is assumed that the sequence (rv_n) is defined as:

$$\mathtt{rv_n(x)} = \sum_{\mathtt{i}=0}^{\mathtt{n}2^{\mathtt{n}}-1} (\tfrac{\mathtt{i}}{2^{\mathtt{n}}}) \mathbb{I}_{\left\{ \mathtt{s} \;\middle|\; \frac{\mathtt{i}}{2^{\mathtt{n}}} \le \mathtt{rv\ s} < \frac{\mathtt{i}+1}{2^{\mathtt{n}}} \right\}} (\mathtt{x}) + \mathtt{n} \mathbb{I} \left\{ \mathtt{s} \;\middle|\; \mathtt{rv\ s} \ge \mathtt{n} \right\} (\mathtt{x})$$

where $\mathbb{I}_A(x)$ is a real-valued function of a set A, such that: $\mathbb{I}_A(x) = 1$ if $x \in A$, and $\mathbb{I}_A(x) = 0$ if $x \notin A$.

In order to utilize any definition or property of Lebesgue integration theory with the above theorem, we first needed to show that the triplet $(\mathcal{U}, \mathcal{E}, \mathbb{P})$ is a measure space with a positive measure. We verified these conditions based on the corresponding theorems available in Hurd's [12] formalization of the probability space $(\mathcal{E}, \mathbb{P})$ along with the definition of measure in [3] under the given assumptions.

The convergence of a positive measurable function to the Lebesgue integral property [3] and the Modus Ponens (MP) rule are then used to split the proof goal of Theorem 1 into the following five subgoals. They correspond to the monotonicity (equation 2) and positive simple-function requirement on rv_n (equations 3, 4, and 5) and the three other assumptions (equation 6) described below [3]:

$$\mathtt{mono\_increasing} \left[\sum_{\mathtt{i}=0}^{\mathtt{n}2^{\mathtt{n}}-1} (\frac{\mathtt{i}}{2^{\mathtt{n}}})^2 \mathbb{I}_{\left\{ \mathtt{s} \;\middle|\; \frac{\mathtt{i}}{2^{\mathtt{n}}} \le \mathtt{rv\ s} < \frac{\mathtt{i}+1}{2^{\mathtt{n}}} \right\}} (\mathtt{x}) + \mathtt{n} \mathbb{I} \left\{ \mathtt{s} \;\middle|\; \mathtt{rv\ s} \ge \mathtt{n} \right\} \right] \tag{2}$$

$$\left[\sum_{\mathtt{i}=0}^{\mathtt{n}2^{\mathtt{n}}-1} (\frac{\mathtt{i}}{2^{\mathtt{n}}})^2 \mathbb{I}_{\left\{ \mathtt{s} \;\middle|\; \frac{\mathtt{i}}{2^{\mathtt{n}}} \le \mathtt{rv\ s} < \frac{\mathtt{i}+1}{2^{\mathtt{n}}} \right\}} (\mathtt{x}) + \mathtt{n} \mathbb{I} \left\{ \mathtt{s} \;\middle|\; \mathtt{rv\ s} \ge \mathtt{n} \right\} \right] \le \mathtt{rv(x)}^2 \tag{3}$$

$$\lim_{\mathtt{n} \to \infty} \left[\sum_{\mathtt{i}=0}^{\mathtt{n}2^{\mathtt{n}}-1} (\frac{\mathtt{i}}{2^{\mathtt{n}}})^2 \mathbb{I}_{\left\{ \mathtt{s} \;\middle|\; \frac{\mathtt{i}}{2^{\mathtt{n}}} \le \mathtt{rv\ s} < \frac{\mathtt{i}+1}{2^{\mathtt{n}}} \right\}} (\mathtt{x}) + \mathtt{n} \mathbb{I} \left\{ \mathtt{s} \;\middle|\; \mathtt{rv\ s} \ge \mathtt{n} \right\} \right] = \mathtt{rv(x)}^2 \tag{4}$$

$$\exists \mathtt{y}. \lim_{\mathtt{n} \to \infty} \left[\sum_{\mathtt{i}=0}^{\mathtt{n}2^{\mathtt{n}}-1} (\frac{\mathtt{i}}{2^{\mathtt{n}}})^2 \mathbb{P} \left\{ \mathtt{s} \;\middle|\; \frac{\mathtt{i}}{2^{\mathtt{n}}} \le \mathtt{rv\ s} < \frac{\mathtt{i}+1}{2^{\mathtt{n}}} \right\} + \mathtt{n} \mathbb{P} \left\{ \mathtt{s} \;\middle|\; \mathtt{rv\ s} \ge \mathtt{n} \right\} \right] = \mathtt{y} \tag{5}$$

$$\left(\forall \mathtt{i}. (\mathtt{i} < 2^{\mathtt{n}}) \Rightarrow \left\{ \mathtt{s} \;\middle|\; \tfrac{\mathtt{i}}{2^{\mathtt{n}}} \le \mathtt{rv\ s} < \tfrac{\mathtt{i}+1}{2^{\mathtt{n}}} \right\} \in \mathcal{E}\right) \wedge \left(\forall \mathtt{i}. 0 \le \tfrac{\mathtt{i}}{2^{\mathtt{n}}}\right) \wedge \left(\mathtt{FINITE}\{\mathtt{i} | \mathtt{i} < 2^{\mathtt{n}}\}\right) \tag{6}$$

We verified the monotonically increasing property in the first subgoal based on the following two facts. First, the indicator function in the subgoal only becomes 1 for only one interval or one particular value of i. Second, as the argument of the sequence, i.e., n, increases the intervals become finer and the resulting value of the sequence becomes larger and from the way rv_n is defined, it is then possible to show that $rv_n^2(x) \leq rv_{n+1}^2(x)$.

The second subgoal, which corresponds to the pre-conditions for the function rv_n to be a positive simple-function, consists of three subgoals. These three subgoals can be discharged based on the third assumption of Theorem 1, arithmetic reasoning and set theory principles, respectively.

We consider two cases for the third subgoal. For the case when $i < n2^n$, the third subgoal is true as there is only one i, say i', for which the real value of $(rv\ x)$ would fall in the interval $[\frac{i}{2^n}, \frac{i+1}{2^n})$ out of all $n2^n$ possible values for i. Thus the indicator function would be 1 for this particular i only and 0 otherwise, which means that the summation would be equal to $(\frac{i'}{2^n})^2$. Now, substituting this value for the summation in the third subgoal along with the fact that $rv\ x$ lies in the interval $[\frac{i'}{2^n}, \frac{i'+1}{2^n})$ leads to its verification. Similar reasoning and properties of rv_n are used to discharge the case when $i \geq n2^n$.

The fourth subgoal is proved using the definition of limit of a real sequence, the monotonicity of the given sequence and reasoning regarding the indicator function similar to the previous subgoal. Finally, the real sequence in the fifth subgoal can be verified to be pointwise convergent by verifying that it is monotonic, just like the sequence in the first subgoal since the probability term will only be non-zero for one particular value of i, either between 0 and $n2^n$ interval or when i is greater than or equal to $n2^n$. In both cases, it is shown that $rv_n(x) \leq rv(x)$ thus concluding the verification of Theorem 1.

3.2 Moments and Variance of Lifetime Distributions

In this section, we utilize Theorem 1 for the verification of the second moment and variance properties of the exponential random variable. The second moment for the continuous exponential random variable, is formalized as follows:

Theorem 2: *Second Moment of the Exponential(m) Random Variable*
$\vdash \forall$ `m. (0 < m)` $\Rightarrow$ `(second_moment` $(\mathcal{U}, \mathcal{E}, \mathbb{P})$ `(exp_rv m) =` $\frac{2}{\mathtt{m}^2}$`)`

We start the proof process by rewriting the left hand side using the general second moment theorem for the unbounded random variables (Theorem 1).

$$\lim_{\mathtt{n}\to\infty} \sum_{\mathtt{i}=0}^{\mathtt{n}2^{\mathtt{n}}-1} (\tfrac{\mathtt{i}}{2^{\mathtt{n}}})^2 \mathbb{P}\left\{ \mathtt{s} \;\middle|\; \tfrac{\mathtt{i}}{2^{\mathtt{n}}} \leq (\mathtt{exp\_rv\ m})\ \mathtt{s} < \tfrac{\mathtt{i}+1}{2^{\mathtt{n}}} \right\}$$
$$+\mathbb{P}\left\{ \mathtt{s} \;\middle|\; \mathtt{n} \leq (\mathtt{exp\_rv\ m})\ \mathtt{s} \right\} = \tfrac{2}{\mathtt{m}^2}$$

Then using set theory properties and the definition of *CDF* of the exponential random variable, we show that

$$\mathbb{P}\left\{\mathtt{s} \;\middle|\; \tfrac{\mathtt{i}}{2^{\mathtt{n}}} \leq (\mathtt{exp\_rv\ m})\ \mathtt{s} < \tfrac{\mathtt{i+1}}{2^{\mathtt{n}}}\right\} + \mathtt{n}\mathbb{P}\left\{\mathtt{s} \;\middle|\; \mathtt{n} \leq (\mathtt{exp\_rv\ m})\ \mathtt{s}\right\}$$
$$= \left[(\mathtt{e}^{-\mathtt{m}\frac{\mathtt{i}}{2^{\mathtt{n}}}})(1 - \mathtt{e}^{-\frac{\mathtt{m}}{2^{\mathtt{n}}}}) + \mathtt{n}\mathtt{e}^{-\mathtt{mn}}\right]$$

We then rewrite the left hand side of the subgoal with the above result and arrive at the following subgoal.

$$\lim_{\mathtt{n}\to\infty}\left[\sum_{\mathtt{i}=0}^{\mathtt{n}2^{\mathtt{n}}-1}(\tfrac{\mathtt{i}}{2^{\mathtt{n}}})^2(\mathtt{e}^{-\mathtt{m}\frac{\mathtt{i}}{2^{\mathtt{n}}}})(1 - \mathtt{e}^{-\frac{\mathtt{m}}{2^{\mathtt{n}}}}) + \mathtt{n}\mathtt{e}^{-\mathtt{mn}}\right] = \tfrac{2}{\mathtt{m}^2}$$

In order to evaluate the limit terms, we first prove the following sum of a sequence containing terms of type $(\mathtt{i}^2\mathtt{P}^{\mathtt{i}})$.

$$\sum_{\mathtt{i}=0}^{\mathtt{M}-1}(\mathtt{i}^2\mathtt{P}^{\mathtt{i}}) = \tfrac{\mathtt{P}^{\mathtt{M}}(\mathtt{M}^2\mathtt{P}^2-2\mathtt{M}^2\mathtt{P}+\mathtt{M}^2-2\mathtt{M}\mathtt{P}^2+2\mathtt{M}\mathtt{P}+\mathtt{P}^2+\mathtt{P})}{(\mathtt{P}-1)^3} - \tfrac{\mathtt{P}(\mathtt{P}+1)}{(\mathtt{P}-1)^3}$$

We then specialize this result for the case when $M = n2^n$ and $P = e^{\frac{-m}{2^n}}$ as follows:

$$\sum_{\mathtt{i}=0}^{\mathtt{n}2^{\mathtt{n}}-1}\mathtt{i}^2(\mathtt{e}^{-\frac{\mathtt{m}}{2^{\mathtt{n}}}})^{\mathtt{i}} = \tfrac{\mathtt{n}^2\mathtt{2}^{2\mathtt{n}}\mathtt{e}^{\frac{-\mathtt{m}}{2^{\mathtt{n}}}(\mathtt{n}2^{\mathtt{n}})}}{(\mathtt{e}^{-\frac{\mathtt{m}}{2^{\mathtt{n}}}}-1)} - \tfrac{2(\mathtt{n}2^{\mathtt{n}})(\mathtt{e}^{\frac{-\mathtt{m}}{2^{\mathtt{n}}}(\mathtt{n}2^{\mathtt{n}}+1)})}{(\mathtt{e}^{-\frac{\mathtt{m}}{2^{\mathtt{n}}}}-1)^2} + \tfrac{(\mathtt{e}^{\frac{-\mathtt{m}}{2^{\mathtt{n}}}(\mathtt{n}2^{\mathtt{n}})}-1)(\mathtt{e}^{\frac{-\mathtt{m}}{2^{\mathtt{n}}}})(\mathtt{e}^{\frac{-\mathtt{m}}{2^{\mathtt{n}}}}+1)}{(\mathtt{e}^{-\frac{\mathtt{m}}{2^{\mathtt{n}}}}-1)^3}$$

Using the above results and with a fair amount of rewriting effort together with product and sum limit theorems, we arrive at the following subgoal.

$$\lim_{\mathtt{n}\to\infty}[-\mathtt{n}^2\mathtt{e}^{-\mathtt{mn}}] + \lim_{\mathtt{n}\to\infty}\left[-\tfrac{2\mathtt{n}\mathtt{e}^{-\mathtt{mn}}\mathtt{e}^{\frac{-\mathtt{m}}{2^{\mathtt{n}}}}}{2^{\mathtt{n}}(1-\mathtt{e}^{\frac{-\mathtt{m}}{2^{\mathtt{n}}}})}\right] + \lim_{\mathtt{n}\to\infty}\left[-\tfrac{(\mathtt{e}^{-\mathtt{mn}}-1)(\mathtt{e}^{\frac{-\mathtt{m}}{2^{\mathtt{n}}}})(\mathtt{e}^{\frac{-\mathtt{m}}{2^{\mathtt{n}}}}+1)}{2^{2\mathtt{n}}(1-\mathtt{e}^{\frac{-\mathtt{m}}{2^{\mathtt{n}}}})^2}\right]$$
$$+ \lim_{\mathtt{n}\to\infty}[\mathtt{n}\mathtt{e}^{-\mathtt{mn}}] = \tfrac{2}{\mathtt{m}^2}$$

We then show that the first and fourth terms on the left hand side of the above subgoal approach zero as n tends to ∞, that is, $\lim_{n\to\infty}\left[-n^2e^{-mn}\right] = 0$ and $\lim_{n\to\infty}[ne^{-mn}] = 0$.

The evaluation of the second and third limit terms required a lot of rewriting effort in HOL, and the proof steps are explained in the following. First we prove the following two limit expressions in HOL using L'hopital's rule.

$$\lim_{\mathtt{x}\to 0}\left[\tfrac{\mathtt{x}\mathtt{e}^{\mathtt{mx}}}{1-\mathtt{e}^{-\mathtt{mx}}}\right] = \lim_{\mathtt{x}\to 0}\left[\tfrac{\mathtt{x}(-\mathtt{m}\mathtt{e}^{\mathtt{mx}})+\mathtt{e}^{\mathtt{mx}}}{0-(-\mathtt{m}\mathtt{e}^{-\mathtt{mx}})}\right] = \tfrac{1}{\mathtt{m}}, \text{ and}$$

$$\lim_{\mathtt{x}\to 0}\left[\tfrac{\mathtt{x}}{1-\mathtt{e}^{-\mathtt{mx}}}\right] = \lim_{\mathtt{x}\to 0}\left[\tfrac{1}{0-(-\mathtt{m}\mathtt{e}^{-\mathtt{mx}})}\right] = \tfrac{1}{\mathtt{m}}$$

Then we specialize the above two results for the case when $x = \frac{1}{2^n}$ and show that $\lim_{\mathtt{n}\to\infty}\left[\frac{\mathtt{e}^{\frac{-\mathtt{m}}{2^{\mathtt{n}}}}}{2^{\mathtt{n}}(1-\mathtt{e}^{\frac{-\mathtt{m}}{2^{\mathtt{n}}}})}\right] = \frac{1}{\mathtt{m}}$ and $\lim_{\mathtt{n}\to\infty}\left[\frac{1}{2^{\mathtt{n}}(1-\mathtt{e}^{\frac{-\mathtt{m}}{2^{\mathtt{n}}}})}\right] = \frac{1}{\mathtt{m}}$

Then using the sum and product limit theorem we rewrite the second and third limit terms as follows:

$$\lim_{n\to\infty}\left[2ne^{-mn}\frac{e^{\frac{-m}{2^n}}}{2^n(1-e^{\frac{-m}{2^n}})}\right] = (2)\left(\lim_{n\to\infty}[ne^{-mn}]\right)\left(\lim_{n\to\infty}\left[\frac{e^{\frac{-m}{2^n}}}{2^n(1-e^{\frac{-m}{2^n}})}\right]\right)$$
$$= (2)(0)(\tfrac{1}{m}) = 0$$

$$\lim_{n\to\infty}\left[-\frac{(e^{-mn}-1)(e^{\frac{-m}{2^n}})(e^{\frac{-m}{2^n}}+1)}{2^{2n}(1-e^{\frac{-m}{2^n}})^2}\right] =$$
$$\lim_{n\to\infty}[-(e^{-mn}-1)]\lim_{n\to\infty}\left[\frac{e^{-mn}}{2^n(1-e^{\frac{-m}{2^n}})}\right]\left(\lim_{n\to\infty}\left[\frac{e^{-mn}}{2^n(1-e^{\frac{-m}{2^n}})}\right]+\lim_{n\to\infty}\left[\frac{1}{2^n(1-e^{\frac{-m}{2^n}})}\right]\right) =$$
$$(1)(\tfrac{1}{m})(\tfrac{1}{m}+\tfrac{1}{m}) = \tfrac{2}{m^2}$$

Finally, we substitute these limits in the above subgoal and show that the left hand side is equal to the right hand side thus completing the proof of the second moment of the exponential random variable.

Theorem 3: *Variance of the Exponential(m) Random Variable*
$\vdash \forall$ `m. (0 < m)` $\Rightarrow$ `(variance` $(\mathcal{U},\mathcal{E},\mathbb{P})$ `(exp_rv m) =` $\frac{1}{m^2}$`)`

The verification steps for the variance of the exponential random variable involve some rewriting using the definition of the variance and the expectation and the second moment theorems. The resulting subgoal $(\frac{2}{m^2}) - (\frac{1}{m})^2 = \frac{1}{m^2}$ is easily shown to be true, based on arithmetic reasoning, thus completing the proof of the variance of the exponential random variable.

4 Reliability Theory Formalization

In this section, we present the formalization of the concepts of survival and hazard functions.

4.1 Survival Function

The survival function represents the probability that a component is functioning at one particular time t and is formalized in HOL as follows:

Definition 2: *Survival Function*
$\vdash \forall$`rv. survival_function = (`λ`t. 1 - CDF rv t)`

where `CDF` is the cumulative distribution function of random variable *rv*. Both survival function and `CDF` in HOL are of type (((num $\rightarrow$ bool) $\rightarrow$ real) $\rightarrow$ real $\rightarrow$ real).

Theorem 4: *Survival Function, Exponential(m) Random Variable*
$\vdash \forall$ `m t. (0 < m)` $\wedge$ `(0 ≤ t)` $\Rightarrow$
`(survival_function (`λ`s. exp_rv m s) t = (`λ`s.` e^{-ms}`) t)`

Theorem 4 was verified using the definitions of survival function and CDF of exponential random variable together with set theory properties. If T represents the Time-to-Failure of an electronic system component, for example, then using

Theorem 4, we can now formally reason about probabilities of failure events at any time t i.e., $\mathtt{P}\{T \leq t\}$, or between any two times t_1 and t_2, i.e., $\mathtt{P}\{t_1 \leq T \leq t_2\}$.

Besides Theorem 4, we also formally verified three important existence properties of the survival function in HOL:

Property 1: *Survival function at time 0 is equal to 1*

```
⊢ ∀rv. (∀x. CDF_in_events_bern rv x) ⇒
                  (survival_function rv 0 = 1)
```

where the assumption of Property 1 ensures that events of the type $\{s|fs \leq x\}$, which define the CDF, are in the sample space.

Property 2: *Survival function approaches 0 for very large values of times*

```
⊢ ∀rv. (∀x. CDF_in_events_bern rv x) ⇒
               (λn. survival_function rv ((λn. &n) n)) → 0
```

and

Property 3: *Survival function is a non increasing function*

```
⊢ ∀rv a b. (a<b) ∧ (∀x. CDF_in_events_bern rv x) ⇒
                  (survival_function rv b ≤ survival_function rv a)
```

4.2 Hazard Function

The hazard function or instantaneous failure rate is used to model the amount of risk associated with a component at a given time t and is formalized in HOL as follows:

Definition 3: *Hazard Function*

```
⊢ ∀rv t. hazard_function rv t = @l.
   ((λa. (survival_function rv t - survival_function rv (t + a))
                          / ((a) (survival_function rv t))) → l) 0
```

The HOL function `hazard_function` takes as input a random variable rv and a real value t and returns a real value l such that the incremental parameter a in the above definition approaches zero.

Using the definitions of hazard function, survival function, and CDF of exponential random variable we formally verify that the hazard function of an exponential random variable is a constant and is given by its parameter m.

Theorem 5: *Hazard Function, Exponential(m) Random Variable*

```
⊢ ∀ m t. (0 < m) ∧ (0 ≤ t) ⇒
             (hazard_function (λs. exp_rv m s) t = m)
```

The hazard function gives an indication of how a component ages. Its units are usually given as the number of failures per unit time. A larger hazard function suggests that the component is under greater risk of failure. Using Theorem 5, we can now formally reason about the amount of failure risks associated with a component when operating under certain stress conditions. The results presented in this section are 100% accurate, completely general and exhaustive as opposed to simulation based techniques where approximate numerical results are available for a very restricted set of parameters.

5 Reliability Analysis of a Capacitor

Capacitors are an essential component of many electrical systems ranging from basic electronics used in medical devices to avionics used in aircrafts, artificial satellites and space shuttles. Uninterruptable power supplies and inverters commonly used in renewable energy power systems contain capacitors for filtering and smoothing of rectified power line voltages. Moreover, they are used in electrical power transmission and distributions networks for power factor correction. Their reliability is absolutely essential for correct behavior of electronics used in safety critical systems and in efficient operation of electrical power systems.

Exponential distribution is the most appropriate distribution for modeling the reliability behavior of a capacitor. The exponential probability distribution parameter in reliability theory is sometimes also called the failure rate. Definition 4 gives the base failure rate for a capacitor [5].

Definition 4: *Base Failure Rate, Capacitor*

```
⊢ ∀ A B VRop Ns Top NT G H.
     res_failure_rate_base A B VRop Ns Top NT G H =
     (A) (real_pow (real_pow (VRop / Ns) H + 1) B)
     (exp (real_pow ((Top + 273) / NT) G))
```

where `A` is the adjustment and `B` is the shaping factor (specified in [5]), `VRop` is the electrical stress ratio and is defined as the ratio of the operating to rated power. `Ns` is a stress constant, `Top` is the operating temperature, `NT` is the temperature constant, and `G` and `H` are called the acceleration constants (specified in [5]). The HOL function `real_pow` takes two real numbers as input and returns a real number. The returned number is equal to the first argument raised to the power of second argument of the function (i.e., `real_pow A b` $= \mathtt{A}^{\mathtt{b}}$). `exp` represents the exponential function. In the part failure method, the quality and environment stress factors are used to adjust the base failure rate of a component according to the operating environment and expected stress levels. The definitions of these two factors are given in [5] and are formalized in HOL as follows.

Definition 5: *Quality Stress Factor*

```
⊢ ∀ quality.
     cap_stress_factor_quality quality =
     (if quality = 0 then 15 / 10 else
     (if quality = 1 then 1 else
     (if quality = 2 then 3 / 10 else
     (if quality = 3 then 1 / 10 else 3 / 100))))
```

Definition 6: *Environment Stress Factor*

```
⊢ ∀ environment.
     cap_stress_factor_environment environment =
     (if environment = 0 then 1 else
     (if environment = 1 then 1 else
     (if environment = 2 then 2 else
```

```
(if environment = 3 then 4 else
(if environment = 4 then 5 else
(if environment = 5 then 7 else
(if environment = 6 then 15 / 2 else
(if environment = 7 then 8 else 15)))))))
```

The HOL formalization of these stress factors accepts a natural number as input and returns the corresponding stress value. The formalization of the capacitor part failure rate, operating in a certain environment under certain electrical stress levels, is given in Definition 7.

Definition 7: *Part Failure Rate, Capacitor*

```
⊢ ∀ A B VRop Ns Top NT G H n m.
   cap_failure_rate_part A B VRop Ns Top NT G H n m =
   (cap_failure_rate_base A B VRop Ns Top NT G H )
   (cap_stress_factor_environment n) (cap_stress_factor_quality m)
```

5.1 Capacitor Lifetime Model

The capacitor life time in HOL is modeled using a function that takes as input the capacitor failure rate and returns a function of exponential random variable of type ((num→bool)→real).

Definition 8: *Capacitor Lifetime Model*

```
⊢ ∀ A B VRop Ns Top NT G H n m. cap_lifetime_model
cap_failure_rate_part A B VRop Ns Top NT G H n m = (λs. exp_rv
(cap_failure_rate_part A B VRop Ns Top NT G H n m) s)
```

5.2 Verification of Reliability Properties

The survival and hazard functions and three important statistical properties of capacitor life time are presented in this section.

Survival and Hazard Functions. Theorems 6 and 7 formally prove the survival and hazard function properties of the capacitor.

Theorem 6: *Survival Function, Exponential Random Variable*

```
⊢ ∀ A B VRop Ns Top NT G H n m t.
    (0 < t) ∧ (0 < A) ∧ (0 ≤ B) ∧ (0 ≤ G) ∧ (0 ≤ H) ∧
    (0 < Ns) ∧ (0 < NT) ∧ (0 ≤ VRop) ∧ (VRop ≤ 1) ∧
    (0 ≤ n) ∧ (0 ≤ m) ⇒ (survival_function (λs.
    exp_rv (cap_failure_rate_part A B VRop Ns Top NT G H n m) s) t
    = exp(-(cap_failure_rate_part A B VRop Ns Top NT G H n m) t))
```

All assumptions except for (`0 < t`) ensure that the capacitor part failure rate (`cap_failure_rate_part A B VRop Ns Top NT G H n m`) is a positive real number.

Theorem 7: *Hazard Rate, Exponential Random Variable*

$$\vdash \forall \texttt{A B VRop Ns Top NT G H n m t.}$$
$$\texttt{(0 < t)} \wedge \texttt{(0 < A)} \wedge \texttt{(0} \leq \texttt{B)} \wedge \texttt{(0} \leq \texttt{G)} \wedge \texttt{(0} \leq \texttt{H)} \wedge$$
$$\texttt{(0 < Ns)} \wedge \texttt{(0 < NT)} \wedge \texttt{(0} \leq \texttt{VRop)} \wedge \texttt{(VRop} \leq \texttt{1)} \wedge$$
$$\texttt{(0} \leq \texttt{n)} \wedge \texttt{(0} \leq \texttt{m)} \Rightarrow \texttt{(hazard\_function (}\lambda\texttt{s.}$$
$$\texttt{exp\_rv (cap\_failure\_rate\_part A B VRop Ns Top NT G H n m) s) t}$$
$$\texttt{= cap\_failure\_rate\_part A B VRop Ns Top NT G H n m)}$$

The proof of Theorem 7 involved rewriting with the definitions of survival and hazard functions, part failure rate and the CDF of the exponential random variable. The limit term is simplified using L'hopital's rule.

Statistical Properties. We formally verified several statistical properties of the capacitor lifetime using the proposed reliability analysis method in the HOL theorem prover. Three of which are presented below, namely, the mean, the second moment, and the variance of Time-to-Failure of the capacitor.

Theorem 8: *Mean Time-to-Failure (MTTF), Exponential(m)*

$$\vdash \forall \texttt{A B VRop Ns Top NT G H n m t.}$$
$$\texttt{(0 < t)} \wedge \texttt{(0 < A)} \wedge \texttt{(0} \leq \texttt{B)} \wedge \texttt{(0} \leq \texttt{G)} \wedge \texttt{(0} \leq \texttt{H)} \wedge$$
$$\texttt{(0 < Ns)} \wedge \texttt{(0 < NT)} \wedge \texttt{(0} \leq \texttt{VRop)} \wedge \texttt{(VRop} \leq \texttt{1)} \wedge$$
$$\texttt{(0} \leq \texttt{n)} \wedge \texttt{(0} \leq \texttt{m)} \Rightarrow \texttt{mttf } (\mathcal{U}, \mathcal{E}, \mathbb{P}) \texttt{ (}\lambda\texttt{s.}$$
$$\texttt{exp\_rv (cap\_failure\_rate\_part A B VRop Ns Top NT G H n m) s) =}$$
$$\frac{1}{(cap\_failure\_rate\_partABVRopNsTopNTGHnm)}$$

Theorem 9: *Second Moment of Time-to-Failure, Exponential(m)*

$$\vdash \forall \texttt{A B VRop Ns Top NT G H n m t.}$$
$$\texttt{(0 < t)} \wedge \texttt{(0 < A)} \wedge \texttt{(0} \leq \texttt{B)} \wedge \texttt{(0} \leq \texttt{G)} \wedge \texttt{(0} \leq \texttt{H)} \wedge$$
$$\texttt{(0 < Ns)} \wedge \texttt{(0 < NT)} \wedge \texttt{(0} \leq \texttt{VRop)} \wedge \texttt{(VRop} \leq \texttt{1)} \wedge$$
$$\texttt{(0} \leq \texttt{n)} \wedge \texttt{(0} \leq \texttt{m)} \Rightarrow \texttt{second\_moment } (\mathcal{U}, \mathcal{E}, \mathbb{P}) \texttt{ (}\lambda\texttt{s.}$$
$$\texttt{exp\_rv (cap\_failure\_rate\_part A B VRop Ns Top NT G H n m) s) =}$$
$$\frac{2}{(cap\_failure\_rate\_partABVRopNsTopNTGHnm)^2}$$

Theorem 10: *Variance of Time-to-Failure, Exponential(m)*

$$\vdash \forall \texttt{A B VRop Ns Top NT G H n m t.}$$
$$\texttt{(0 < t)} \wedge \texttt{(0 < A)} \wedge \texttt{(0} \leq \texttt{B)} \wedge \texttt{(0} \leq \texttt{G)} \wedge \texttt{(0} \leq \texttt{H)} \wedge$$
$$\texttt{(0 < Ns)} \wedge \texttt{(0 < NT)} \wedge \texttt{(0} \leq \texttt{VRop)} \wedge \texttt{(VRop} \leq \texttt{1)} \wedge$$
$$\texttt{(0} \leq \texttt{n)} \wedge \texttt{(0} \leq \texttt{m)} \Rightarrow \texttt{variance } (\mathcal{U}, \mathcal{E}, \mathbb{P}) \texttt{ (}\lambda\texttt{s.}$$
$$\texttt{exp\_rv (cap\_failure\_rate\_part A B VRop Ns Top NT G H n m) s) =}$$
$$\frac{1}{(cap\_failure\_rate\_partABVRopNsTopNTGHnm)^2}$$

The proofs of the above statistical properties were greatly facilitated by corresponding exponential random variable statistical properties, described in Section 3. It is important to note that the reliability analysis results proved in this section are completely generic expressions rather than numerical values as is the case in simulation based techniques. Moreover these results are 100% accurate as we are dealing with real numbers rather than floating point numbers as is the

case in simulation based techniques. Such analysis was not previously possible in a theorem proving environment and we believe it to be a major step forward in the direction of the formal reliability analysis of engineering systems.

6 Conclusions

In this paper, we presented an approach for the reliability analysis of engineering systems in the sound environment of the HOL theorem prover. The approach builds upon existing formalizations of continuous random variables. We presented the formalization of two commonly used lifetime distribution representations, namely the survival and hazard functions. We also presented the formalizations of several important statistical properties of random variables and the formal proof of a general expression for the second moment of a continuous random variable using probability, measure and Lebesgue integration theories. We then used this expression to prove the second moment and variance relations for the exponential random variable. The usefulness of the proposed reliability analysis method was demonstrated with the help of reliability analysis of a capacitor, an essential building block in electrical and electronic systems. The HOL formalization and proof effort described in this paper took approximately 110 man-hours and consists of around 4000 lines of HOL code.

We are currently working on the formalization of other lifetime probability distributions such as Weibull and Gamma distributions to further enhance the proposed reliability analysis approach. The proposed method at this time allows one to define arbitrary lifetime distributions as long as a closed form expression for its CDF inverse exists, which makes it suitable for a large set of reliability analysis problems in engineering. We also plan to conduct the reliability analysis of multi component systems with and without redundancy.

References

1. Baier, C., Haverkort, B., Hermanns, H., Katoen, J.P.: Model Checking Algorithms for Continuous time Markov Chains. IEEE Transactions on Software Engineering 29(4), 524–541 (2003)
2. Broughton, E.: The Bhopal Disaster and its Aftermath: A Review. Environmental Health 4(6), 1–6 (2005)
3. Coble, A.: Anonymity, Information and Machine-assisted Proof. PhD Thesis, University of Cambridge, Cambridge, UK (2009)
4. Dean, S.M.: Considerations involved in making system investments for improved service reliability. EEI Bulletin (6), 491–496 (1938)
5. U. S. Department of Defence. Reliability Prediction of Electronic Equipment, Military handbook, MIL-HDBK-217B (1974)
6. U. S. Department of Defense. Reliability-Centered Maintenance (RCM) Requirements for Naval Aircraft, Weapon Systems, and Support Equipment, MIL-HDBK-2173 (1998)
7. FIDES. Reliability Methodology for Electronic Systems (2009)

8. Gordon, M.J.C., Melham, T.F.: Introduction to HOL: A Theorem Proving Environment for Higher-Order Logic. Cambridge University Press, Cambridge (1993)
9. Hasan, O.: Formal Probabilistic Analysis using Theorem Proving. PhD Thesis, Concordia University, Montreal, QC, Canada (2008)
10. Hasan, O., Abbasi, N., Akbarpour, B., Tahar, S., Akbarpour, R.: Formal Reasoning about Expectation Properties for Continuous Random Variables. In: Cavalcanti, A., Dams, D.R. (eds.) FM 2009. LNCS, vol. 5850, pp. 435–450. Springer, Heidelberg (2009)
11. Hasan, O., Tahar, S., Abbasi, N.: Formal Reliability Analysis using Theorem Proving. IEEE Transactions on Computers 59(5), 579–592 (2010)
12. Hurd, J.: Formal Verification of Probabilistic Algorithms. PhD Thesis, University of Cambridge, Cambridge, UK (2002)
13. Investigative Documentary on National Geographic Channel. Derailment at Eschede (High Speed Train Wreck), Seconds From Disaster (2007)
14. Leemis, L.M.: Reliability, Probabilistic Models and Statistical Methods (2009)
15. Mhamdi, T., Hasan, O., Tahar, S.: On the Formalization of the Lebesgue Integration Theory in HOL. In: Interactive Theorem Proving. LNCS, vol. 6172, pp. 387–402. Springer, Heidelberg (2010)
16. Myers, R.H., Ball, L.W.: Reliability Engineering for Electronic Systems. Wiley, Chichester (1964)
17. Institute of Electrical and Electronics Engineers. IEEE Standard Reliability Program for the Development and Production of Electronic Systems and Equipment, IEEE 1332 (1998)
18. Rogers Commission report, Report of the Presidential Commission on the Space Shuttle Challenger Accident, vol. 1, ch.4. p. 72 (1986), `http://history.nasa.gov/rogersrep/v1ch4.htm`
19. Rutten, J., Kwaiatkowska, M., Normal, G., Parker, D.: Mathematical Techniques for Analyzing Concurrent and Probabilisitc Systems. CRM Monograph Series, vol. 23. American Mathematical Society, Providence (2004)