Mission-based reliability prediction in component-based systems

Saideep Nannapaneni[1], Abhishek Dubey[2], Sherif Abdelwahed[3], Sankaran Mahadevan[4], Sandeep Neema[5], Ted Bapty[6]

[1,4]*Department of Civil & Environmental Engineering, Vanderbilt University, Nashville, TN, 37235, USA*

saideep.nannapaneni@vanderbilt.edu
sankaran.mahadevan@vanderbilt.edu

[2,5,6]*Department of EECS/ISIS, Vanderbilt University, Nashville, TN, 37235, USA*

dabhishe@isis.vanderbilt.edu
sandeep@isis.vanderbilt.edu
bapty@isis.vanderbilt.edu

[3]*Department of ECE, Mississippi State University, Starkville, MS, 39762, USA*

sherif@ece.msstate.edu

ABSTRACT

This paper develops a framework for the extraction of a reliability block diagram in component-based systems for reliability prediction with respect to specific missions. A mission is defined as a composition of several high-level functions occurring at different stages and for a specific time during the mission. The high-level functions are decomposed into lower-level functions, which are then mapped to their corresponding components or component assemblies. The reliability block diagram is obtained using functional decomposition and function-component association. Using the reliability block diagram and the reliability information on the components such as failure rates, the reliability of the system carrying out a mission can be estimated. The reliability block diagram is evaluated by converting it into a logic (Boolean) expression. A modeling language created using the Generic Modeling Environment (GME) platform is used, which enables modeling of a system and captures the functional decomposition and function-component association in the system. This framework also allows for real-time monitoring of the system performance where the reliability of the mission can be computed over time as the mission progresses. The uncertainties in the failure rates and operational time of each high-level function are also considered which are quantified through probability distributions using the Bayesian framework. The dependence between failures of components are also considered and are quantified through a Bayesian network (BN). Other quantities of interest such as mission feasibility and function availability can also be assessed using this framework. Mission feasibility analysis determines if the mission can be accomplished given the current state of components in the system, and function availability provides information whether the function will be available in the future given the current state of the system. The proposed methodology is demonstrated using a radio-controlled (RC) car to carry out a simple surveillance mission.

1. INTRODUCTION

Model-based design (Schmidt, 2006; Schattkowsky & Muller 2004; Mosterman, 2007) provides a powerful framework for the design of complex systems using system architecture and component behavior models. It provides a common platform for modeling, data analysis and system verification. It is also used to analyze and manage the complexities and failures due to component-to-component interactions during the design of the system. The errors in the system design can be located early and corrected even before the system goes into the manufacturing phase. In addition, the component models can be re-used, which helps in upgrading existing systems and development of new systems.

The first step in the creation of domain-specific models is the creation of a domain-specific custom modeling language that encodes all the syntactic and semantic information such as various objects, properties and relationships in the models that will be created using the modeling language. The GME (Ledeczi et al, 2001) provides a flexible platform for the creation of such modeling languages. During the design phase, several models can be created and evaluated

against several criteria such as performance, reliability and cost. Each design is associated with a different cost, performance and reliability. The selection of a particular design is made through a tradeoff between the cost, performance and reliability of the system. For example, in an aircraft inertial measurement unit (IMU) (Dubey, Mahadevan & Karsai 2012), six accelerometers were provided even though only four were necessary. This improved the reliability but incurred additional costs. For commercial airplanes where people are involved, reliability takes priority over performance and cost. For unmanned vehicles where people are not involved, performance might take preference over reliability. Each design alternative is tested under several scenarios before the final design alternative is selected. A scenario is termed as a mission in this paper. A mission can be understood as a collection of activities or functions to be performed. In this paper, reliability is considered as the evaluation criterion and a framework for reliability prediction is proposed. As mentioned above, model-based design framework provides a common platform for modeling and data analysis. Here, the model-based design framework is utilized for modeling a system and for mission-based reliability prediction.

Given a mission description, the components used to accomplish the mission functions are indigenous to the system that is undertaking the mission. As an example, a simple mission can be to move from point A to point B. There can be many choices to move from A to B such as using a gas-powered car or an electric car. The components used in the gas-powered car (fuel tank, engine) are different from the components used in the electric car (batteries) to carry out the same function. In general, not all the components in the system are used to carry out the mission. A system may provide many more functions that are not necessary for a particular mission. In such cases, all the components corresponding to those functions will be unused and do not appear in the reliability assessment. Therefore, it is necessary to extract the components that will be associated with a particular mission based on the mission functions. This is accomplished through the concepts of functional decomposition and function-component association that is later explained in Section 4. For example, assume that B can be reached from A in a straight path without taking any turns. In such a case, the steering wheel component will be unused and does not appear in reliability prediction.

Reliability prediction in component-based systems provides a mechanism to estimate the failure probability for the overall system from the failure probabilities of individual components (Kececioglu, 1972; Krishnamurthy & Mathur, 1997). Here, component-based systems refer to the systems that can be assembled from individual components. Reliability prediction may also be used to evaluate design feasibilities, compare design alternatives, identify potential failure areas in design, trade-off between design factors, provide insight on the need for redundant components, or replace an existing system with a more reliable system (O'Connor, Newton & Bromley, 2002). There are two types of mechanical components – repairable and irreparable components. Repairable components are the components that if failed can be restored to working condition. On the other hand, irreparable components cannot be restored to the working condition when failed. In the case of repairable components, mean time between failures (MTBF) is a measure of reliability whereas mean time to failure (MTTF) is a measure of reliability for irreparable components (Wood, 2001). In this paper, all the components are assumed irreparable. Reliability prediction is essential before the beginning of the mission and during the mission. Reliability prediction is necessary to calculate the reliability in real-time during the mission in the presence of failure of any of the components.

Well-known techniques for reliability assessment include Failure Modes, Effects and Criticality Analysis (FMECA; Bouti & Kadi, 1994; Teng & Ho, 1996), Fault Tree Analysis (FTA; Lee, Grosh, Tillman & Lie, 1985), Event Tree Analysis (ETA; Kenarangui, 1991) and Reliability Block Diagrams (RBD; O'Connor, Newton & Bromley, 2012). In this paper, reliability prediction is performed using a reliability block diagram because it can be constructed easily using the Boolean expressions employed in the proposed methodology. An introduction to a reliability block diagram is provided in Section 2.

In some cases, the reliability information (failure rates) of some components may not be known precisely but some estimates might be available from historical records or from similar components. In addition, the operational time taken by the system in carrying out some functions cannot be identified deterministically since it is influenced by several factors such as the environment, condition of the system etc. Therefore, factors such as variability (randomness) and uncertainty (due to lack of knowledge) in variables should be considered in computing the reliability of the system in carrying out a mission. Here, it is assumed that the uncertainty in the operational times is due to the uncertainty in the environmental conditions (weather, pathways and other surroundings) and future loadings. Thus, other aleatory uncertainty sources can also be included by translating them into the uncertainty in operational times. Numerous approaches are available to represent the various aspects of uncertainty such as Bayesian probability theory (Sankararaman & Mahadevan, 2011; Nannapaneni & Mahadevan, 2015), possibility theory (Alola, Tunay & Alola, 2013), interval analysis (Rao & Cao, 2002), evidence theory (Bae, Grandhi & Canfield, 2004). Bayesian probability theory is employed in this paper where probability distributions are used to represent variability as well as uncertainty in variables.

In systems where several components are connected to each other, the failure of a component during the mission may increase the failure rates of other working components. Such dependencies should also be considered while assessing the reliability which influences the real-time decision making process. Bayesian networks (Koller & Friedman, 2009) have been used in several applications such as bioinformatics (Friedman, Linial, Nachman & Pe'er, 2004), epidemiology (Jiang & Cooper, 2010), software systems (De Campos, Fernández-Luna & Huete, 2004), civil infrastructure (Bensi & Der Kiureghian, 2010), mechanical systems (Urbina, Mahadevan & Paez, 2012), manufacturing systems (Nannapaneni & Mahadevan, 2014) for modeling the dependence between several variables. This technique is used in this paper for modeling the dependence between failures of components.

In this paper, we pursue a combination of unit-level monitoring and MTTF-based methods for real-time reliability prediction. Before the beginning of the mission, the reliability prediction for the mission is made using available data, i.e., data on similar systems, historical data, model simulation data, data from previous missions of the same system. When the mission in progress, the reliability prediction is carried out by updating the system parameters (health of components) through health monitoring, which now becomes unit-specific reliability prediction for the mission.

The overall contributions of this paper are as follows – (1) Extraction of mission-specific reliability block diagram for reliability assessment; (2) Quantification of uncertainties in reliability analysis parameters (failure rates and operational times) and their incorporation in reliability estimate; (3) Modeling the failure rate dependence of a component on the health of other components using a Bayesian network; and (4) Decision-making under uncertainty based on real-time reliability estimates during the mission.

A key benefit of the proposed methodology is that the reliability prediction can be carried out in an automated manner. The automation procedure is briefly discussed at the end of Section 3.1.

The rest of the paper is organized as follows. Section 2 provides background concepts on the reliability modeling of mechanical components, reliability block diagrams, expressions for reliability analysis, uncertainty characterization in reliability analysis parameters, and Bayesian networks to model failure dependence between components. Section 3 discusses the system assumptions and presents the proposed methodology for reliability assessment in component-based systems. In Section 4, the proposed methodology is demonstrated using an example in which a radio-controlled (RC) car is used to carry out a simple surveillance mission. Concluding remarks are provided in Section 5.

2. BACKGROUND

2.1. Reliability modeling of a mechanical component

Three kinds of failures are considered at different stages during the service life of mechanical components – (1) early life failures, (2) random failures, and (3) wear out failures. The failure rate corresponding to the early-life failures decreases with the service time of the component. Random failures are characterized by constant failure rates since failures can occur at any time during the service of the component. Wear-out failures are characterized by an increasing failure rate, where the failure rate of a component increases with the service time of the component. The first phase does not have a failure probability evaluation but early failures are used for design and development. The failure probability during the second phase is generally modeled using an exponential distribution (Eq. 1) and during the third phase is modeled using a Weibull distribution (Eq. 2)

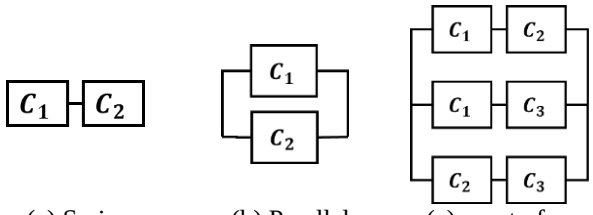
$$P_f(t) = 1 - e^{-\lambda t} \tag{1}$$

$$P_f(t) = 1 - e^{\left(-\frac{t}{\eta}\right)^{\beta}} \tag{2}$$

In Eq. (1), λ represents the inverse of mean time between failures (MTTF), also called the failure rate. In Eq. (2), η represents the scale parameter (time at which the failure rate is 0.632) and β represents the shape parameter. The values of these parameters can be obtained from the manufacturer, historical data, experimental data or simulations. In this paper, all the components are assumed to be in the second phase of random failures.

2.2. Reliability Block Diagram

A reliability block diagram is a graphical representation showing the logical connections between several components in a system. They are used to compute the reliability of a system in carrying out a function using the reliability information of individual components and Boolean rules of combinations (Bennetts, 1982). When two components are connected in series, then the function requires both the components and if the components are connected in parallel, either of the components is sufficient to carry out the function. Figures 1(a) and 1(b) shows series and parallel connections for two components C_1 and C_2.



(a) Series (b) Parallel (c) r out of n

Figure 1. Different connections of components in an RBD

If components are connected in series, the overall reliability is the product of individual reliabilities of components if the component failures are independent.

$$R(S) = R(C_1) \times R(C_2) \quad (3)$$

If the components are connected in parallel, the overall reliability assuming independence between components is obtained as

$$R(S) = R(C_1) + R(C_2) - R(C_1)R(C_2) \quad (4)$$

In Eqs. (3, 4), $R(S)$, $R(C_1)$, $R(C_2)$ refer to the reliabilities of the overall system, components C_1 and C_2 respectively. When the component requirement for a function is specified using the "r out of n" operator, then all possible series combinations are obtained and connected in parallel. The reliability of this component-system is calculated using series and parallel connection rules as given above. The number of combinations is equal to $\binom{n}{r}$, which is equal to $\frac{n!}{(n-r)!r!}$. Consider an example where a function F requires two out of available three components. Let the three components be C_1, C_2, C_3. In this case, F can be carried out using C_1, C_2 or C_2, C_3 or C_1, C_3. The combinations can be represented in the reliability block diagram as shown in Figure 1(c).

2.3. Quantification of uncertainty in failure rate and operational time

The failure rate of a component is estimated using the available failure data of that component. In this regard, consider the following three cases – (1) time-to-failure data from a single source, (2) time-to-failure data from multiple sources (multiple batches), and (3) Multiple MTTF values are available for the same component but from different sources (batches).

In the first case, an entire probability distribution can be obtained for MTTF (λ) by using the available data in the Bayesian framework. Let D_t represent the available time-to-failure data, then the posterior distribution of MTTF (λ) can be computed in the Bayesian framework using Eq. (5).

$$f(\lambda|D_t) \propto L(D_t)f(\lambda) \quad (5)$$

In Eq. (5), $L(.)$ and $f(.)$ refer to the likelihood function and PDF respectively. If the available data is a combination of point and interval data, then the technique developed in (Sankararaman & Mahadevan, 2013) for likelihood construction can be used.

In the second case, when time-to-failure data is available from multiple sources, then MTTF can be estimated after aggregating all the data (one-step estimation) or perform sequential estimation (multi-step estimation) where a posterior distribution is obtained by using first set of time-to-failure data, then this posterior is used as a prior for updating the MTTF estimate using the second dataset. This process is carried out until all the time-to-failure data are used.

The third case represents the case when different sources provide MTTF values corresponding to their batches. In a parameter estimation problem, this represents the case when data is directly available on the parameter. In such a case, non-parametric distribution is directly fit to the data. The non-parametric PDF construction technique is briefly discussed below. Let T represent the MTTF of a component and T_i $(i = 1\ to\ n)$, $[T_j^l, T_j^u]$ $(j = 1\ to\ m)$ represent the available point data and interval data respectively. The domain of T is then discretized into Q points and let the PDF values at these points be equal to q_i $(i = 1,2\ldots, Q)$. Since $\boldsymbol{q} = q_i (i = 1,2 \ldots Q)$ is unknown, they can be estimated by solving the following optimization problem:

$$Max\ L(\boldsymbol{q}) = \prod_{i=1}^{n} f_T(T = T_i|\boldsymbol{q}) \prod_{j=1}^{m} [F_T(T = T_j^u|\boldsymbol{q}) - F_T(T = T_j^l|\boldsymbol{q})] \quad (6)$$

such that

$$\boldsymbol{q} \geq 0; f_T(T) \geq 0; \int f_T(T)dT = 1$$

In Eq. (6), $L(.)$ refers to the likelihood function and $f(.)$, $F(.)$ refer to the PDF and CDF respectively. More details about the PDF construction are available in (Sankararaman & Mahadevan, 2013).

2.4. Modeling failure dependencies between components

Bayesian networks, as stated in Section 1, are used in this paper for dependence modeling of failures between several components. A BN is a probabilistic graphical model that represents a joint probability distribution of several random variables as a directed acyclic graph where nodes represent random variables and arcs represent their conditional dependencies. The random variables in a BN can be both discrete and continuous. For discrete variables, conditional or marginal probability tables are defined whereas for continuous variables, conditional or marginal probability distributions are defined.

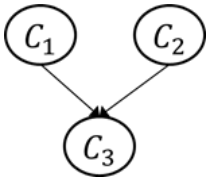


Figure 2. Bayesian network for modeling failure dependence relations

Consider the BN shown in Figure 2. Let the failure rate for component C_3 be dependent on two components - C_1 and C_2. Let the health of a component be modeled as a discrete variable with two values 0 and 1, representing working and

failed conditions respectively. The MTTF values of C_3 conditioned on the states of components C_1 and C_2 can be represented as shown in Table 1.

	C_1, C_2 = (0,0)	C_1, C_2 = (0,1)	C_1, C_2 = (1,0)	C_1, C_2 = (1,1)
MTTF of C_3	2000	[1925, 1975]	[1940, 1960]	1900, 1906, 1913, 1920, [1920, 1925]

Table 1. MTTF values of C_3 dependent on C_1 and C_2

Table 1 indicates that the MTTF values decreases with failure of C_1 and C_2. When both C_1 and C_2 are in working state, the MTTF value for C_3 is 2000 and when C_2 fails, the MTTF is a uniform distribution between 1925 and 1975. Similar observations can be made when only C_1 fails, and when both C_1 and C_2 fail, some point and interval data might be available on the MTTF value of C_3. Note that the MTTF values in Table 1 are arbitrarily chosen with no units, for the sake of illustration.

3. PROPOSED METHODOLOGY

Assumptions: This paper considers only mechanical systems where all the components are assumed to be in the second phase of their bathtub curves, i.e., the failures are random and represented using exponential distributions. When a component fails, it is assumed to remain in the failed state until the end of the mission. In addition, the mean time to failure (MTTF) information are assumed to be available for all the components.

3.1. Extraction of reliability block diagram

System Modeling: The system performing the mission is modeled using a domain-specific modeling language (DSML). The procedure for modeling is not discussed and out of the scope of this paper as the aim is to extract the mission-specific reliability block diagram from the system model for reliability prediction. The proposed methodology is independent of the language used for modeling. During modeling, each component in the model is associated with a list of functions that require this component and with its corresponding MTTF value. As stated above, the MTTF values for all the components are assumed to be available.

Functional Decomposition: From the mission description, the function-time diagram can be obtained which provides information about the list of high-level functions required and the time when they are required during the mission. Consider Figure 5. Assume a hypothetical mission description that requires the car to move from A to D. To accomplish the mission, the car which initially is along the line AB should turn at A, move forward from A to C, take a right turn at C, move forward from C to D. Suppose the car takes 't_{left}' min to turn and 't_{AC}' min to move from A to C. Therefore, from time t = 0 to t = t_{left}, the high-level function required is to turn left. From t = t_{left} to t = t_{left} + t_{AC}, the high-level function of moving forward is required. Thus, function-time information can be obtained from mission description. This information when represented by a diagram as shown in Figure 7 becomes a function-time diagram.

For each of the high-level functions, functional decomposition is carried out to obtain the leaf-level functions. A definition for functional decomposition is provided in the appendix. The high-level function can be hierarchically represented in terms of lower level functions and leaf functions using a tree-structure, as shown in Figure 8. A leaf level function is a function that cannot be further decomposed. From the tree-structure, a Boolean expression for the high-level function can be obtained in terms of the leaf-level functions that can then be converted to a reliability block diagram. The symbol '∧' represents a series connection (i.e., both components are needed) and '∨' represents a parallel connection (i.e., one of the components is needed). For example, consider a high-level function F that is expressed in terms of leaf-level functions as $F_1 \wedge (F_2 \vee F_3) \wedge F_4$. The reliability block diagram corresponding to the Boolean expression is shown in Figure 3.

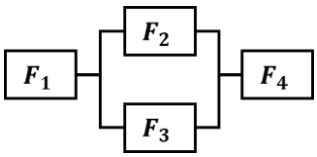


Figure 3. Reliability block diagram from functional decomposition

Function-Component association: Each of the leaf-level functions is associated with a component or a component assembly in the system that is undertaking the mission. A definition for function-component association is provided in the appendix. The components associated with each function depend on the system that is undertaking the mission. The components providing the same function may be different in different systems. (For example, the power generation function can be accomplished through a battery or an internal combustion engine). A component may be associated with more than one leaf-level function. For each leaf-level function, the corresponding set of components can be obtained from the system model because in the modeling stage, the association of each component to the list of functions has been made. The function-component associations can be expressed using Boolean expressions similar to the functional decomposition of high-level functions.

In some cases, there are additional constraints called implication constraints (Mahadevan, Dubey, Balasubramanian & Karsai, 2013) that arise from the system model. For example, consider the function of power

generation in an automobile, which requires an internal combustion engine. However, additional components like chassis are required to hold the combustion engine for it to be working. If the chassis breaks down, even though the engine is in working state, the function becomes unavailable. This is an additional implication constraint coming from the system model.

Reliability Assessment: Each leaf-level function has a set of components associated with it and a reliability block diagram can be obtained from the connections of the associated components. The reliability block diagrams of all the leaf-level functions are used to obtain a reliability block diagram of the high-level function. Similarly, reliability block diagrams can be obtained for all the high-level functions. The reliability block diagrams of all the high-level functions can be combined to obtain the reliability block diagram of the entire mission. Sometimes a component may be required for several function in the mission, therefore the component appears several times in the Boolean expression. The PyEDA package available in Python environment is used here to simplify the Boolean expression and from the simplified Boolean expression, a simplified reliability block diagram can be obtained.

From the mission description, we can obtain the required functions and the time each function is required for. Using this function-time information, we can calculate the time for which each of the components is required. Using the time information, MTTF values and the reliability block diagram, the reliability of the mission can be calculated using series and parallel connection rules given in Eqs (3) and (4). Figure 4 shows the proposed methodology for reliability assessment.

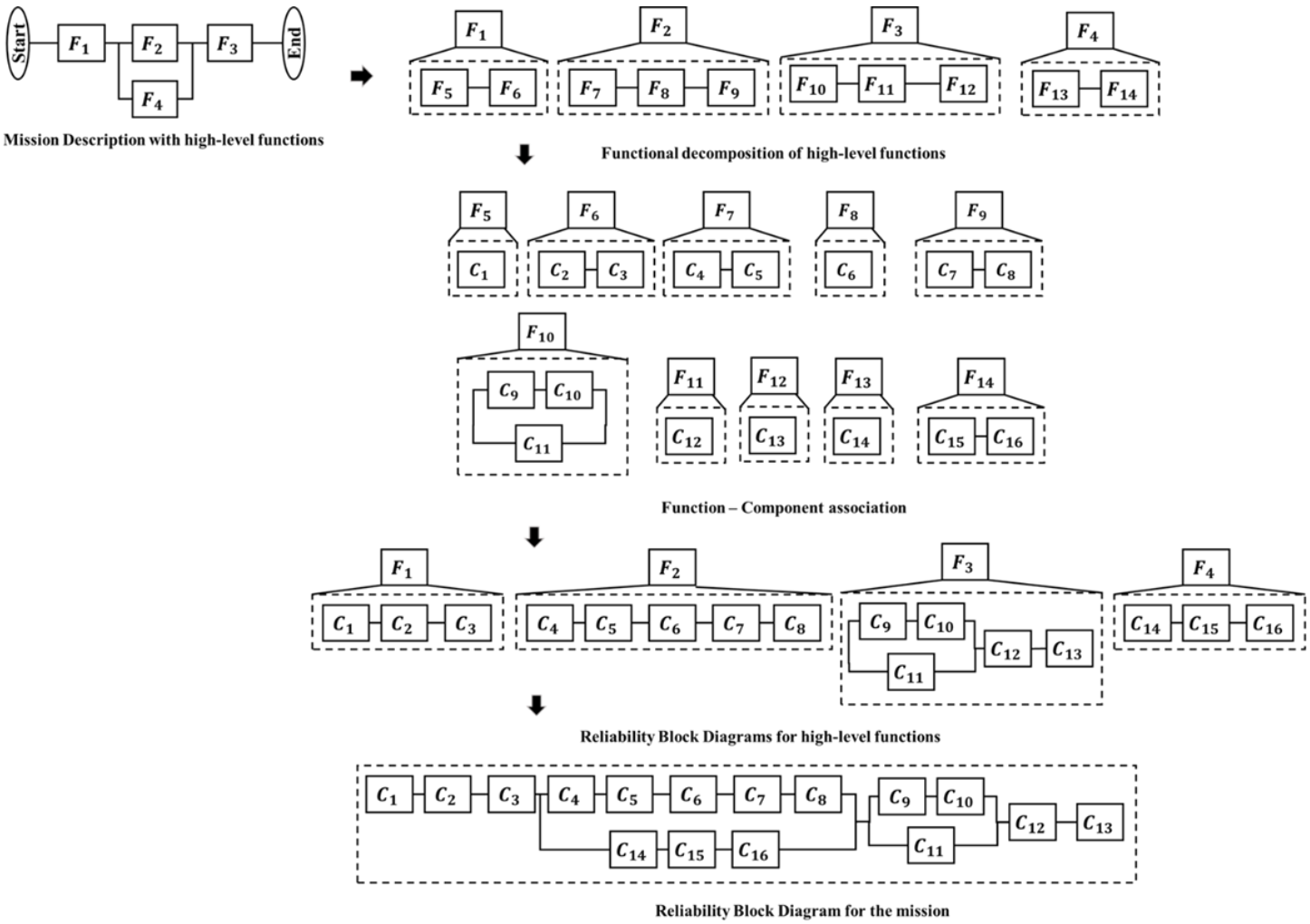


Figure 4. Methodology for reliability assessment

In Figure 4, the mission is described using high level function F_1, F_2, F_3, F_4.Then, using functional decomposition, the high level functions are decomposed to leaf-level functions, F_k (k = 5 to 14), and each leaf-level function is associated with its component assembly. The function-component association also represents the reliability block diagram of the leaf-level function. The reliability block diagrams of the leaf-level functions are combined to obtain the reliability block diagram of the high-level functions. The reliability block diagrams of all the high-level functions are combined to obtain the reliability block diagram of the mission.

Capability for automation: A key advantage of the above framework for reliability prediction is that it can be automated. The mission description is provided by the client and an analyst obtains the function-time diagram from the mission description. As mentioned earlier, information about the functional decomposition of high-level functions and the association of component(s) to each leaf-level function can be represented in the system model. Therefore, the Boolean expression (which can be converted to a reliability block diagram) can be obtained from the function-time diagram using functional decomposition and function-component association. Note that the reliability information (MTTF values) can be provided for all components in the system model. Therefore, the mission reliability can be programmatically computed using the reliability block diagram and reliability information of the components. In this work, the reliability of all the individual components are assumed to be modeled through exponential distributions (constant failure rates) but it should be noted that the same procedure can be adopted when Weibull distributions (increasing failure rates) are used or a combination of Weibull and exponential distributions for reliability modeling.

3.2. Uncertainty in failure rates and operational times

As stated in Section 2.3, probability distributions using the Bayesian framework are used to represent the uncertainty in failure rates and operational times. When all the parameters are known deterministically, the reliability estimate is a deterministic value. However, when some parameters are uncertain, the uncertainty in them results in uncertainty in the reliability estimate. Sampling techniques such as Monte Carlo simulation can be used to quantify the uncertainty in the reliability estimate. Each realization of the uncertain parameters provides a sample of the reliability estimate. Several realizations of the uncertain parameters provide several samples of the reliability estimate. These samples can then be used to obtain the PDF of the reliability estimate.

3.3. Dependence between failures of components

During the course of the mission, the failure of one component may affect the failure rate of other connected components and this dependence is modeled using a Bayesian network (BN) as discussed in Section 2.4. The failure rate dependence modeling can be divided into two tasks – (1) determine the list of components that affect the failure rate of a component, and (2) estimate the conditional failure rates, i.e., failure rates of the component when conditioned on the health of the components that influence it. The above two tasks can be accomplished through aggregation of information from historical records, tests, model-based simulation and expert opinion. Details regarding the construction of the BN are outside the scope of this paper and a BN is assumed available for reliability analysis. Note that the failure rate that initially is a fixed value can become uncertain after the failure of certain components as shown in the illustration example in Section 2.4. Depending upon the health of the parent nodes in the BN, the corresponding failure rate of the child node can be used for reliability prediction.

3.4. Real-time reliability prediction and decision making

During the course of the mission, the health of all the components can be monitored (failed or working). If a component is in failed state, all the functions that the component is associated with will not be available. From the health of the components, availability or unavailability of the functions can be inferred. At any time, real-time reliability prediction of the system can be carried out using the approach in Section 3.1. Using the results of real-time reliability prediction, decisions on continuing the mission, aborting the mission or carrying out a simpler mission (a mission with reduced outcomes than originally intended) can be made. In addition, decisions regarding alternate paths to maximize the reliability of the mission can be made. When a component becomes unavailable, the initial Boolean expression for the reliability block diagram can be updated to include the component unavailability. The updated Boolean expression can then be used for further reliability assessment of the mission. If the failure rates of all the components are fixed values, then the reliability estimate is also a fixed value and decision-making can be made using the fixed value. However, when the failure rates of some parameters are uncertain, the reliability estimate is not a fixed value but a PDF as mentioned in Section 3.2. Given the PDF of the reliability estimate, decision-making can be based on the maximum a posteriori (MAP) of the reliability estimate, mean value, 95^{th} percentile or the 5^{th} percentile depending on the analyst preferences and mission requirements.

The current framework can be extended to handle partial failures and component degradations. For any component M, we can define the MTTF as a function of

component degradation factor d_M ($0 < d_M < 1$), where '$d_M = 0$' represents working state and '$d_M = 1$' represents failed state. In the presence of dependence between failures of components, the MTTF value of the child component (C_3 in Figure 2) should also be defined as a function of its degradation and component degradations of parent components (C_1, C_2 in Figure 2). The amount of degradation (d_M) in each component can be quantified through real-time component health monitoring. Thus, the real-time health monitoring data can also be included in predicting the mission reliability.

4. EXAMPLE: RADIO-CONTROLLED CAR

Mission Description: The RC Car, which initially is at point A has to move to point B and perform surveillance at point B using a camera mounted on it. The car is amphibious and can move from A to B either on land or in water as shown in Figure 5. Along with the land powertrain, a propeller system is also built-in to the RC Car to move in water. The width of the water body is assumed to be 1.5 miles. The total distance to be covered when moving on land from A to B is 2.5 miles. The speeds when moving on land and in water are assumed to be 7.5 mph and 3 mph respectively.

Figure 6 shows the RC Car modeled using a DSML in GME. As mentioned in Section 3.1, the creation of the DSML is out of the scope of this paper. Following the DSML, the RC Car (components and their connections) is modeled. The blocks represent the components and connections represent the physical connections between the components. Each component is also associated with a list of functions that it is needed for. A simple model of the RC Car is used for illustration; therefore has limited capabilities in terms of functions that can be carried out. The RC Car can move forward, backward, turn left and turn right. To stop the car, thrust is to be exerted in the opposite direction of motion i.e., if the car is moving forward then thrust is to be exerted in the reverse direction to stop the car. This forms the primary braking system and a secondary emergency braking system is also assumed available.

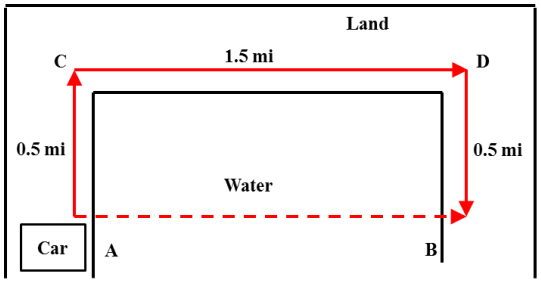


Figure 5. Mission description

From the mission description, the function-time plot can be constructed as shown in Figure 7. The function-time plot has time and functions to be carried out on the X and Y-axes. The plot shows two possible paths to complete the mission – one on land (shown in red and black) and other on water (blue and green). It can be seen from the plot that the times taken to complete the mission through land and water are 30 and 36 min respectively. If the mission is undertaken on water, then the function "Move forward in water" is required for 30 min, then either the primary or the secondary brake is required for 1 min, and "Move Camera" is required for the next 5 min. Similar interpretation can be made if the mission is carried out on land. A variation of 5% and 2% are assumed around the remaining travel time in water and on land respectively; these variations are modeled through uniform distributions. For example, the function 'Move forward in water' in Figure 7 is required for 30 min; a uniform distribution is assumed with lower and upper bounds as 28.5 min and 31.5 min respectively (5% of 30). Note that Figure 7 provides the mean value of required time for each function.

The mission can be divided into two high-level functions – 1) A function F_{AB} that represents the movement of the RC Car from A to B, and 2) a function F_S that represents the surveillance activity at point B. To complete function F_{AB}, the RC Car can choose between two alternate paths – to move on land, represented by F_{AB_L} or in water, represented by F_{AB_W}. The function F_{AB_L} is decomposed into three sub-functions - 1) Moving from A to C, represented by $F_{AB_L}.F_{AC}$ 2) Moving from C to D, represented by $F_{AB_L}.F_{CD}$, 3) Moving from D to B, represented by $F_{AB_L}.F_{DB}$. The locations of points C and D are shown in Figure 5. The successful completion of all these three sub-functions results in the successful completion of function F_{AB_L}. Each of the sub-functions is further decomposed into a number of smaller leaf-level functions and successful completion of all the leaf-level function results in the completion of a sub-function. Table 2 shows the sub-functions of F_{AB_L} and their associated leaf-level functions.

In the case of function F_{AB_W}, the function itself is a leaf-level function and therefore cannot be decomposed further. Using hierarchical decomposition, the function F_{AB} can be expressed in terms of leaf-level functions (Figure 8) as

$$F_{AB} = ((F_1 \wedge F_2 \wedge F_3 \wedge F_4 \wedge F_5 \wedge F_6 \wedge F_7 \wedge F_8) \vee (F_8 \wedge F_9)) \quad (7)$$

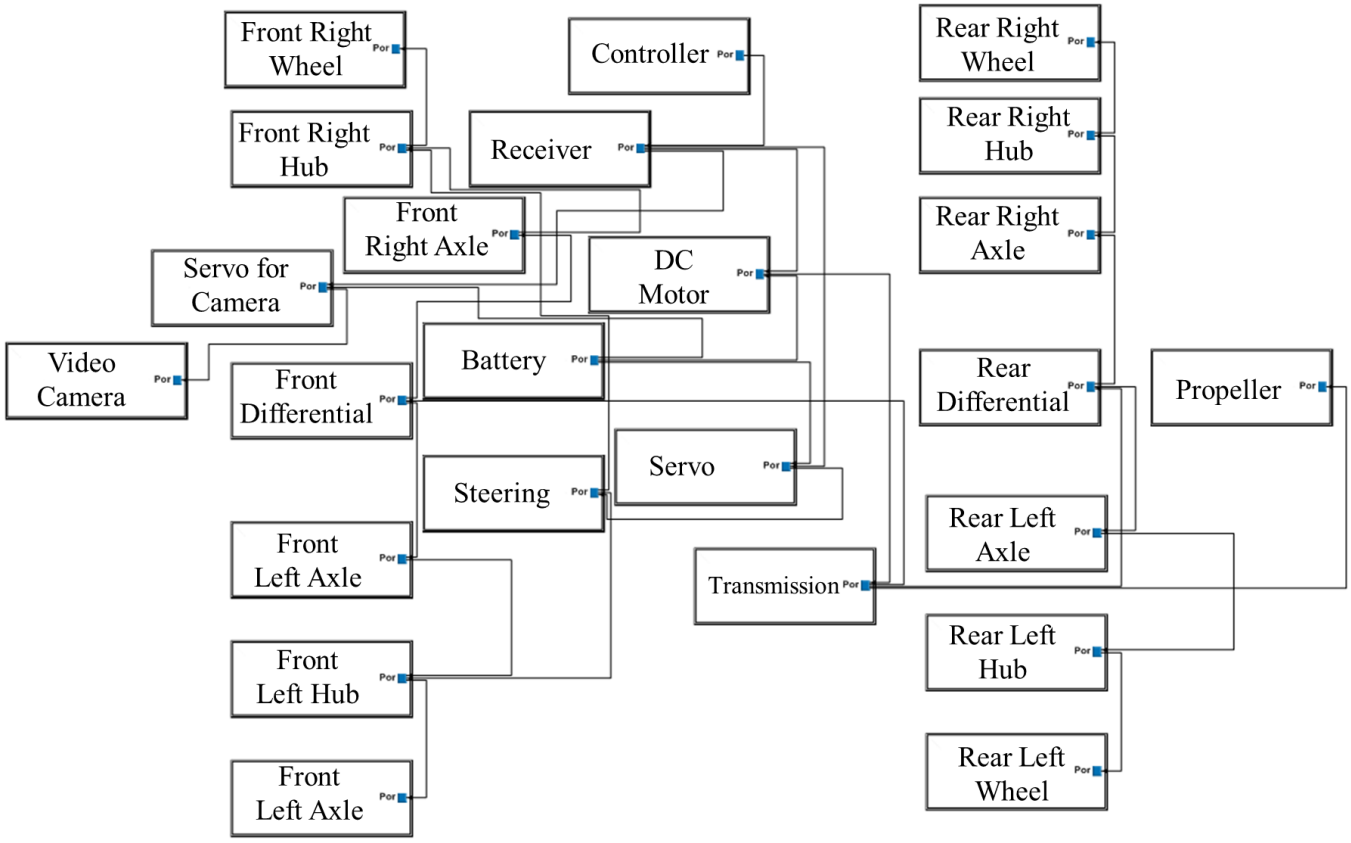


Figure 6. Modeling of the RC Car

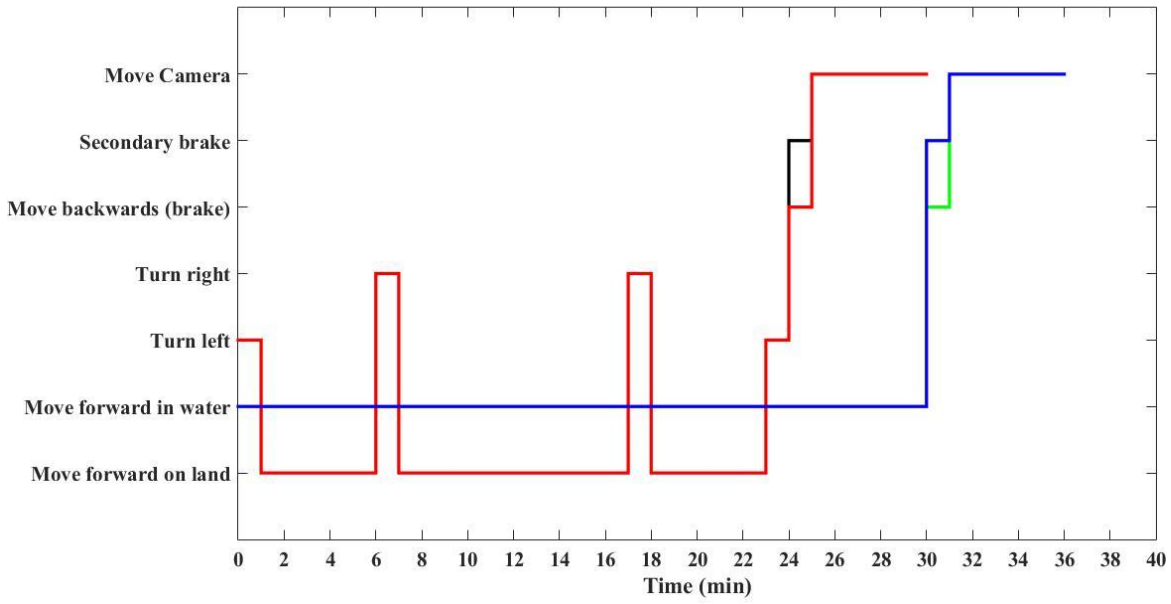


Figure 7. Function-time diagram for the mission

Sub-Function	Leaf-Level Function	Notation
$F_{AB_L}.F_{AC}$	Turn Left at A	F_1
	Move Forward from A to C	F_2
	Turn right at C	F_3
$F_{AB_L}.F_{CD}$	Move forward from C to D	F_4
	Turn right at D	F_5
$F_{AB_L}.F_{DB}$	Move forward from D to B	F_6
	Turn left at B	F_7
	Brake and stop at B	F_8

Table 2. Sub-functions of F_{AB_L} and their leaf-level functions

The next step after obtaining the hierarchical decomposition is to associate component assemblies to carry out each of the atomic-level functions. Table 3 shows the list of component assemblies available in the RC Car system along with their assumed MTTF values. The MTTF values for Camera and Propeller are assumed unknown but some point and interval data are assumed available, given in Table 3. Table 4 shows the association between leaf-level functions and component assemblies. To demonstrate the methodology, MTTF values for the components are assumed. After obtaining the functional decomposition (hierarchical decomposition) and associations between functions and components, the reliability of the overall mission is computed from reliability information of component assemblies through a reliability block diagram. The construction of a reliability block diagram can be carried out in two steps – (1) the leaf-level functions are substituted with their associated component assemblies from Table 4, (2) all the components connected with $'\wedge'$ are written in series, whereas components connected with $'\vee'$ are written in parallel.

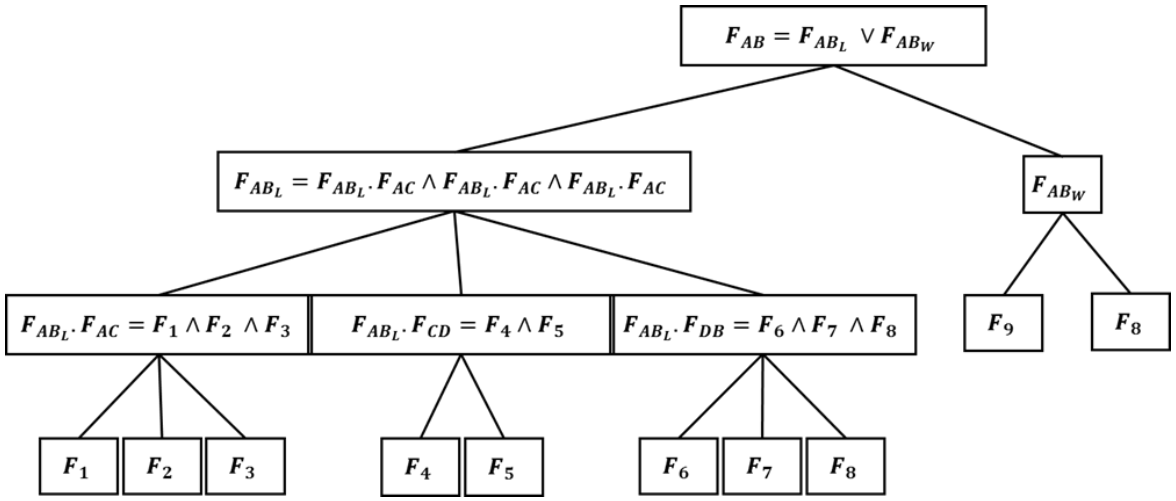


Figure 8. Hierarchical decomposition of the function of moving from A to B (F_{AB})

Component Assembly	Notation	MTTF* (min)
Front Wheel System	W_F	2000
Front Hub System	H_F	2000
Front Axle System	A_F	2000
Front Differential	D_F	1000
Transmission	T	2500
DC Motor	DCM	1000
Battery	B	2500
Receiver	R	2500
Servo	S	1000
Steering	St	2000
Servo for Camera	S_C	1000
Camera	C	998,1000, 1002 1005,1008, [995, 1010]
Rear Differential	D_R	1000
Rear Axle System	A_R	2000
Rear Hub System	H_R	2000
Rear Wheel System	W_R	2000
Propeller	P	500, 503, 497, 505, [495, 500]
Chassis	Ch	2500
Secondary Brake System	E_B	500

Table 3. Components in the RC Car and their MTTF values

Function	Component Assembly
F_1, F_3, F_5, F_7	$R \wedge B \wedge S \wedge St \wedge H_F \wedge W_F \wedge Ch$
F_2, F_4, F_6	$R \wedge B \wedge DCM \wedge T \wedge D_F \wedge D_R \wedge A_F \wedge A_R \wedge H_F \wedge H_R \wedge W_F \wedge W_R \wedge Ch$
F_8	$(R \wedge B \wedge DCM \wedge T \wedge D_F \wedge D_R \wedge A_F \wedge A_R \wedge H_F \wedge H_R \wedge W_F \wedge W_R \wedge Ch) \vee (E_B \wedge Ch)$
F_9	$R \wedge B \wedge DCM \wedge T \wedge P \wedge Ch$
F_S	$R \wedge B \wedge S_C \wedge C \wedge Ch$

Table 4. Leaf-level functions and their components

* MTTF values used here are assumed values, for illustration purposes only.

Using the available point and interval data on MTTF values for 'Propeller' and 'Camera' components, non-parametric distributions are constructed using spline-based interpolation as discussed in Section 2.3. The reliability block is constructed using the functional decomposition and function-component association. Using the available MTTF values, the reliability of the mission can be computed. Since the MTTF values of some variables and operational times of each function are uncertain, the reliability estimate is reported as a PDF given in Figure 9.

Case 1: Real-time reliability assessment

Assume that the mission was being undertaken by moving in water to reach from A to B. Table 5 show the functions required to complete the mission at the beginning of mission (point A) and midway between A and B.

Function	Mean duration required (min)	
	Beginning, at point A	Midway, between A and B
Moving in water (F_9)	30	15
Brake at point B (F_8)	1	1
Surveillance (F_S)	5	5

Table 5. Functions required at the beginning and at midway between A and B

The third column in Table 5 can be interpreted as follows – When the RC Car is at the midpoint between points A and B, for successful completion of the mission, F_9 is required for a mean duration of 15 more minutes, Braking and surveillance are required for mean durations of 1 and 5 minutes respectively.

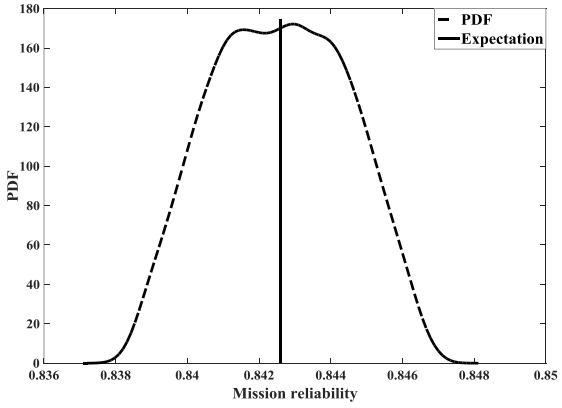


Figure 9. Reliability estimate at the beginning of mission

Moreover, all these three functions are required in succession, as shown in the function-time diagram (Figure 7). The reliability block diagram for the mission is constructed and using the MTTF values, the reliability of the remaining portion of mission can be computed as shown in Figure 10.

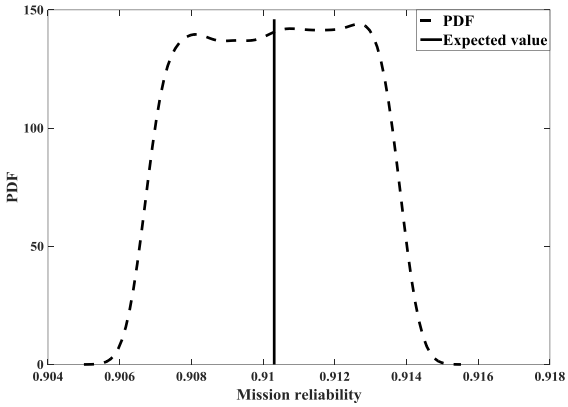


Figure 10. Reliability estimate at midway for the remaining mission

Case 2: Component failure

Assume that at the midway between A and B, the secondary brake fails and becomes unavailable (due to some unknown reason). Since the braking function has redundancy (primary and secondary), the reliability of the braking function decreases. In a hypothetical case, assume that the failure of the secondary brake component causes the failure rate of the transmission component to increase i.e., MTTF value decreases. The dependence of the MTTF value of the transmission on the health of secondary brake component can be represented using a BN as shown in Figure 11. In Figure 11, E_B and T represent the secondary brake component and the transmission component respectively. The MTTF values of T conditioned on the health state of E_B are provided in Table 6.

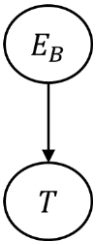


Figure 11. Bayesian network showing the dependence between secondary brake and transmission components

	E_B = 0 (working)	E_B = 1 (failed)
MTTF of T	1000	[600, 650]

Table 6. MTTF values of transmission component conditioned on the health of secondary brake component

The reliability of the remaining mission given that the secondary brake failed is computed and shown in Figure 12. Note that the mean value for the reliability estimate decreased from 0.912 to 0.895 after the failure of secondary brake component.

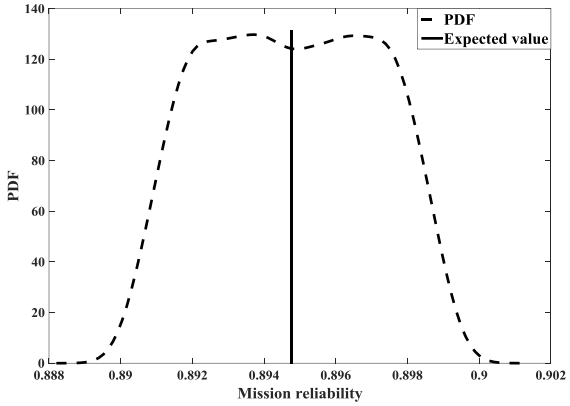


Figure 12. Reliability estimate after the failure of secondary brake component

Case 3: Decision-making under uncertainty

The expected value of the mission reliability estimate at midway in the mission is 0.895 (Case 2). Let us assume that the mission reliability requirement is 0.9. Therefore, we have at least a couple of options here – (1) Abort the mission, and (2) Perform a mission with a reduced outcome than initially desired. Note that the primary objective of the mission is to have surveillance for 5 min. The reliability estimate is less than the threshold (0.9); therefore, the time for surveillance need to reduced. The surveillance time for which the reliability estimate is greater than the threshold can be estimated through Monte Carlo sampling to be equal to 3.2 min. Note that in this case, we consider the expected value of the PDF of reliability estimate to be greater than the threshold value. As mentioned in Section 3.4, we can also consider 5^{th} percentile or 95^{th} percentile or any other criterion depending on the analysis requirements.

Discussion: In this work, we developed a basic conceptual framework for mission-level reliability prediction in component-based systems and demonstrated using an RC Car for surveillance mission. The same framework can also be used for complex missions such as spacecraft and military missions. Consider a spacecraft mission such as the OSIRIS-Rex† to asteroid Bennu. Reliability and sustenance are key elements in such critical missions. The ideal scenario would be that no component(s) fail during the mission. However, any amounts of testing and analysis cannot guarantee 100% reliability of every component, failure of component(s) do occur. Redundancy is often provided in such complex systems and in the event of a component(s) failure, it is desired to re-configure the system in such a way that the reliability of completing the mission is maximum. Multiple plausible re-configurations could be available, the proposed framework can be used to assess the reliability of completing the mission in every plausible re-configuration, and consequently the best re-configuration can be deployed. Note that in this discussion, we consider only component-based failures and not consider random unexpected failures from external sources such as space radiation. We also assume that the MTTF values of the components are comparable to the mission time and therefore choosing the right re-configuration is necessary to increase the probability of mission success.

† http://nssdc.gsfc.nasa.gov/nmc/spacecraftDisplay.do?id=OSIRISREX

5. CONCLUSION

This paper proposed a framework to extract a mission-specific reliability block diagram for reliability assessment in component-based systems. The system undergoing the mission is modeled using a domain-specific modeling language in Generic Modeling Environment (GME). In the system model, each component is associated with the list of functions for which it is required. From the mission description, functional decomposition is performed for each high-level function and is represented using a hierarchical tree-structure. Each of the leaf-level functions is then associated with the set of components or component assemblies from the GME model (also called function component association) and a reliability block diagram is obtained using the Boolean expressions. Using the reliability information of the components and operational times of system components from the mission description, the reliability prediction can be carried out.

When the reliability analysis variables such as failure rates and operational times are uncertain, the uncertainty is quantified by constructing probability distributions using the Bayesian framework. The presence of uncertainty in the failure rates and operational times results in an uncertainty in the reliability estimate that is quantified using Monte Carlo simulations. In systems where the failure rate of a component is dependent on the health of other connected components, a Bayesian network is constructed to model such dependencies. The failure rate of the component is updated depending on the current state of health of the other connected components and used in reliability prediction.

This procedure can also be used for real-time decision-making during the mission. The reliability of the system in carrying the mission can be calculated as a function of time during the mission. Using the reliability estimates, real time decisions can be taken such as to continue the mission, abort the mission, perform a simpler mission, or choose a particular path that maximizes the reliability of the mission when there is redundancy available in carrying out functions in a mission. The proposed methodology is demonstrated using a radio-controlled car in carrying out a simple surveillance mission.

This work proposed a framework for the extraction of mission-specific reliability block diagram for reliability prediction in systems that consist of only hardware

components. Future work should address reliability prediction in cyber-physical systems that consist of interconnected software and hardware components. In this work, the automation capability of the proposed methodology is briefly discussed. Future work should develop a more formal automated approach in which algorithms should be developed to extract necessary information from the DSML model for real-time reliability prediction and decision-making.

ACKNOWLEDGEMENT

The research presented in this paper was supported by funds from the Defense Advanced Research Projects Agency (DARPA) under Contract No. HR0011-13-C-0041. The support is gratefully acknowledged. The authors also thank Professors Gautam Biswas and Xenofon Koutsoukos at Vanderbilt University for initial discussions during this study.

REFERENCES

Alola, A. A., Tunay, M., & Alola, V. (2013). Analysis of Possibility Theory for Reasoning under Uncertainty. *International Journal of Statistics and Probability*, 2(2), 12–23.

Bae, H.-R., Grandhi, R. V., & Canfield, R. A. (2004). Epistemic uncertainty quantification techniques including evidence theory for large-scale structures. *Computers & Structures* 82(13), 1101-1112.

Bennetts, R. G. (1982). Analysis of reliability block diagrams by Boolean techniques. *IEEE Transactions on Reliability*, 31(2), 159-166.

Bensi, M., & Der Kiureghian, A. (2010). Seismic hazard modeling by Bayesian network and application to a high-speed rail system, *Proceedings of International Symposium on Reliability Engineering and Risk Management*, (Ed: J. Li), Tongji University Press, Shanghai, China.

Bouti, A., & Kadi, D. A. (1994). A state-of-the-art review of FMEA/FMECA. *International Journal of Reliability, Quality and Safety engineering*, 1(04), 515-543.

De Campos, L.M., Fernández-Luna, J.M., & Huete, J.F. (2004). Bayesian networks and information retrieval: an introduction to the special issue, *Information Processing & Management, Elsevier*, 40 (5): 727–733.

Dubey, A., Mahadevan, N., & Karsai, G. (2012). The inertial measurement unit example: A software health management case study. *Technical Report. ISIS-12-101, Institute for Software Integrated Systems, Vanderbilt University*, http://isis.vanderbilt.edu/node/4496.

Friedman, N., Linial, M., Nachman, I., & Pe'er, D. (2004) Using Bayesian Networks to Analyze Expression Data, *Journal of Computational Biology*, (3/4): 601–620.

Jiang, X., & Cooper, G.F. (2010). A Bayesian Spatio-Temporal Method for Disease Outbreak Detection, *Journal of American Medical Informatics Association* 17 (4): 462–71.

Kececioglu, D. (1972). Reliability analysis of mechanical components and systems. *Nuclear Engineering and Design*, 19(2), 259-290.

Kenarangui, R. (1991). Event-tree analysis by fuzzy probability. *IEEE Transactions on Reliability*, 40(1), 120-124.

Koller, D., & Friedman, N. (2009). *Probabilistic graphical models: principles and techniques*. MIT press.

Krishnamurthy, S., & Mathur, A. P. (1997). On the estimation of reliability of a software system using reliabilities of its components. *Proceedings of Eighth IEEE International Symposium in Software Reliability Engineering* (pp. 146-155). 2-5 November, Albuquerque, New Mexico, USA.

Kurtoglu, T., & Tumer, I. Y. (2008). A graph-based fault identification and propagation framework for functional design of complex systems. *Journal of Mechanical Design*, 130, 051401.

Kurtoglu, T., Tumer, I. Y., & Jensen, D. C. (2010). A functional failure reasoning methodology for evaluation of conceptual system architectures. *Research in Engineering Design*, 21(4), 209-234.

Ledeczi, A., Maroti, M., Bakay, A., Karsai, G., Garrett, J., Thomason, C., Nordstrom, G., Sprinkle, J. & Volgyesi, P. (2001). The generic modeling environment. *Workshop on Intelligent Signal Processing, Budapest, Hungary (Vol. 17, p. 1).*

Lee, W. S., Grosh, D. L., Tillman, F. A., & Lie, C. H. (1985). Fault Tree Analysis, Methods, and Applications. A Review. *IEEE Transactions on Reliability*, 34(3), 194-203.

Mahadevan, N., Dubey, A., Balasubramanian, D., & Karsai, G. (2013). Deliberative, search-based mitigation strategies for model-based software health management. *Innovations in Systems and Software Engineering*, 9(4), 293-318.

Mosterman, P. (2007). Model-based design of embedded systems. *Proceedings of IEEE International Conference on Microelectronic Systems Education*, June 3-4, San Diego, California, USA.

Nannapaneni, S., & Mahadevan, S. (2014). Uncertainty quantification in performance evaluation of manufacturing processes. *Proceedings of the IEEE International Conference on Big Data* (pp. 996-1005), October 27-30, Washington DC, USA.

Nannapaneni, S., & Mahadevan, S. (2015). Model and Data Uncertainty Effects on Reliability Estimation. *Proceedings of the 17th Non-Deterministic Approaches Conference, AIAA SciTech*, Kissimmee, Florida, USA.

O'Connor, P. D. T., Newton, D., & Bromley, R. (2002). *Practical Reliability Engineering*, John Wiley and Sons. Chichester, England.

Python library for Electronic Design Automation (PyEDA) Documentation [Online].

https://media.readthedocs.org/pdf/pyeda/latest/pyeda.pdf. Last accessed – January 31, 2016

Rao, S. S., & Cao, L. (2002). Optimum Design of Mechanical Systems Involving Interval Parameters. *Journal of Mechanical Design*, ASME, 124(3), 465-472.

Sankararaman, S., & Mahadevan, S. (2011). Likelihood-based representation of epistemic uncertainty due to sparse point data and interval data, *Reliability Engineering and System Safety*, Vol. 96, No. 7, pp. 814-824.

Sankararaman, S., & Mahadevan, S. (2013). Distribution type uncertainty due to sparse and imprecise data. *Mechanical Systems and Signal Processing*, 37(1), 182-198.

Schattkowsky, T., & Muller, W. (2004). Model-based design of embedded systems. *Proceedings of Seventh IEEE International Symposium on Object-Oriented Real-Time Distributed Computing* (pp. 113-128), Vienna, Austria.

Schmidt, D. C. (2006). Guest editor's introduction: Model-driven engineering. *Computer*, *39*(2), 0025-31.

Teng, S. H. G., & Ho, S. Y. M., (1996). Failure mode and effects analysis: an integrated approach for product design and process control. *International Journal of Quality & Reliability Management*, 13(5), 8-26.

Urbina, A., Mahadevan, S., & Paez, T.L. (2012). A Bayes Network Approach to Uncertainty Quantification in Hierarchically Developed Computational Models, *International Journal for Uncertainty Quantification*. Vol. 2, No. 2, pp. 173-193.

Wood, A. P. (2001). Reliability-metric varieties and their relationships. *Proceedings of IEEE Annual Reliability and Maintainability Symposium* (pp. 110-115), January 22-25, Philadelphia, Pennsylvania

APPENDIX

Functional Decomposition: Functional decomposition is the process of decomposing a high-level function into a set of leaf-level functions (Kurtoglu & Tumer, 2008). A leaf-level function is a function that cannot be decomposed any further. All the leaf-level functions are required for the successful completion of the high-level function. Functional decomposition of a high-level function can be represented using a hierarchical tree-structure. The dependence relationships can be written using the Boolean relationships: and, or, r-out-of-n. The number of branches in the tree depends on the fidelity of the analysis required. At any instant of time, one or more high-level functions can be happening; therefore, one or more dependence trees are active. A leaf-level function might be required for several high-level functions and therefore might appear in several trees.

Function-Component association: Boolean relationships (and, or, r-out-of-n) are used to associate each leaf-level function to its component or a component assembly (Kurtoglu, Tumer & Jensen, 2010). A component can provide multiple leaf-level functions but a leaf-level function cannot be associated with more than one component unless the components are the same.

Component availability: Component availability refers to the availability of a component for usage at any time instant during the mission.

Function availability: Function availability refers to the availability of a function for a future use during a mission. For a function to be available, all the components required for the implementation of this function should be available.

Mission Feasibility: Mission feasibility refers to the possibility of completion of the mission given the current state of the components. At any instant of time, if all the components are available to carry out all the functions required later in the mission, then it can be concluded that the mission is feasible given the current state of the components. If any of the components becomes unavailable and the component is required later, then the corresponding function cannot be carried out. If there are no alternate possibilities available to carry out this function, then these results in the mission being infeasible.

Redundancy: If a function can be carried out even when a component becomes unavailable, then it can be concluded that there is redundancy in the function with respect to that component.