A Model-Based Approach for Reliability Assessment in Component-Based Systems

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

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

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

[2,3,5]*Department of EECS/ISIS, Vanderbilt University, Nashville, TN, 37235, USA*

dabhishe@isis.vanderbilt.edu
sherif@isis.vanderbilt.edu
sandeep@isis.vanderbilt.edu

ABSTRACT

This paper describes a formal framework for reliability assessment of component-based systems with respect to specific missions. A mission comprises of different timed mission stages, with each stage requiring a number of high-level functions. The work presented here describes a modeling language to capture the functional decomposition and missions of a system. The components and their alternatives are mapped to basic functions which are used to implement the system-level functions. Our contribution is the extraction of mission-specific reliability block diagram from these high-level models of component assemblies. This is then used to compute the mission reliability using reliability information of components. This framework can be used for real-time monitoring of system performance where reliability of the mission is computed over time as the mission is in progress. Other quantities of interest such as mission feasibility, function availability can also be computed using this framework. Mission feasibility answers the question whether the mission can be accomplished given the current state of components in the system and function availability provides information if the function is available in the future given the current state of the system. The software used in this framework includes Generic Modeling Environment (GME) and Python. GME is used for modeling the system and Python for reliability computations. The proposed methodology is demonstrated using a radio-controlled (RC) car in carrying out a simple surveillance mission.

1. INTRODUCTION

In recent years, model-based design (Schattkowsky & Muller 2004; Mosterman, 2007), which is a simulation-based approach, has become a powerful framework for the design of complex systems using component behavior models. It is also used to analyze and manage the complexities and failures due to component-to-component interactions during the design phase of the system. Several design alternatives are possible for the same system and a single design is to be chosen based on several factors such as cost, performance, reliability. Each design choice is associated with a different cost, performance, reliability. The selection of a particular design is made through a tradeoff between the cost, performance and safety of the system. (eg., In an inertial measurement unit (IMU) (Dubey, Mahadevan & Karsai 2012) used in Boeing aircraft, 6 accelerometers are provided even though only 4 are necessary to improve the reliability under additional costs). For commercial airplanes where people are involved, safety takes preference over performance and cost. For unmanned vehicles where people are not involved, performance might take preference over safety. Each design alternative is tested under several scenarios before the final design alternative is selected. A scenario is termed as mission in this paper. A mission can be understood as a collection of activities or functions to be performed. A more formal definition of a mission is provided in Section 4.

Usually, mission requirements are independent of the systems used to undertake the mission. The components used to accomplish the mission functions are indigenous to the system that is carrying the mission. As an example, a simple

Saideep Nannapaneni et al. This is an open-access article distributed under the terms of the Creative Commons Attribution 3.0 United States License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

mission description 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 completely 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 the mission. In such cases, all the components corresponding to those functions will be unused and do not appear in the reliability assessment. Assume that B can be reached from A without taking any diversion. In such a case, the steering wheel component will be unused and does not appear in reliability assessment.

Reliability assessment in component-based systems provides a mechanism to predict the failure probabilities for the overall system from the failure probabilities of individual components (Kececioglu, 1972; Krishnamurthy & Mathur, 1997). It is used to evaluate design feasibilities, compare design alternatives, identify potential failure areas in design, trade-off between design factors, provide an insight on the need for redundant systems, and replace existing systems with better reliable systems (Elsayed, 2012). There are two types of mechanical components – repairable and irreparable components. Repairable components are the components that if failed can be brought to working condition. Similarly, irreparable components cannot be brought back to the working state 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 to be irreparable. Reliability assessment is essential before the beginning of mission and also during the mission. Reliability assessment during the mission is necessary to calculate the reliability of the mission in real-time during the mission in the presence of failure of any of the components. This provides an idea on the redundancy available in the system and assists in real-time decision making process.

Some of the traditional techniques used for system reliability assessment include Failure Modes, Effects and Criticality Analysis (FMECA; Bauti & Kadi, 1994; Teng & Ho, 1996), Fault Tree Analysis (FTA; Lee, Grosh, Tillman & Lie, 1985), Event Tree Analysis (ETA; Ericson, 2005), Reliability Block Diagrams (RBD; Elsayed, 2012), Probabilistic Risk Assessment (PRA; Modarres, 2008; Greenfield; 2001). FMECA is an extension to Failure Modes and Effects Analysis (FMEA) developed by NASA to improve the reliability of space hardware program. In this method, all the potential failures in the design are identified and their severity on the system output is included. In FTA, the system is represented in a hierarchical form using Boolean logic such that the system output occurs at the top. For each system failure, the causes are inferred using a top-down approach. Event trees are used to follow a sequence of events from an initiating event of a component until the end state of the system. The probability of the outcome of end state is determined from the probabilities of individual events. In the RBD approach, the system is represented using a network diagram of blocks representing components connected in series and/or in parallel. The PRA approach uses fault tree and event tree diagrams in a probabilistic framework to compute the probability of a failure outcome. In this paper, reliability assessment is performed using reliability block diagrams because they can be constructed easily using the Boolean expressions employed in the proposed methodology. A detailed introduction to reliability block diagrams is provided in Section 2.

The main contribution of this paper is the extraction of the components involved in carrying out the mission and then constructing the mission-specific reliability block diagram to compute the reliability of the mission using the reliability information of the components in the system. Also, a procedure to extend the proposed methodology to real-time reliability assessment is provided.

The paper is organized as follows. Section 2 discusses the reliability modeling of mechanical components and the procedure for construction of the reliability block diagram. Section 3 provides the details of systems for which the proposed methodology can be applied. In Section 4, the proposed methodology for reliability assessment in component-based systems is presented. In Section 5, 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 6. A list of necessary definitions are provided in the appendix.

2. BACKGROUND

2.1 Reliability Modeling of a Component

A typical component is subjected to three kinds of failures during its service life – (1) early life failures, (2) random failures, and (3) wearout failures. The failure rate corresponding to the early-life failures decreases as a function of service time of component. Random failures are characterized by constant failure rates because failures can occur at any time during the service time of the component. Wearout failures are characterized by an increasing failure rate, where the failure rate of a component increases with the service time of the component. The total failure rate at any time instant is equal to the sum of all the three failure rates. The total failure rate can be modeled using a bathtub curve.

Figure 1 shows a typical failure rate curve for a typical component (Filliben, 2002). The bathtub curve consists of three phases. In the first phase, the early-life failures are predominant; this is known as infant mortality period. In the second phase, random failures are predominant and this phase is known as stable failure period or intrinsic failure period. In the third phase, wearout failures are predominant and this phase is known as wearout failure period. The failure probability during the third phase is generally modeled using a Weibull distribution (Eq. 1) and that during the second phase is modeled using an exponential distribution (Eq. 2). The first phase does not have a failure probability evaluation but early failures are used for design and development.

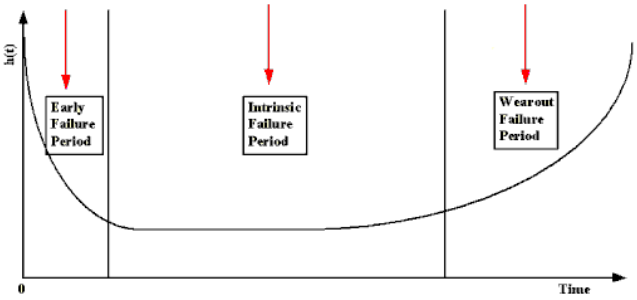


Figure 1. Bathtub curve showing failure rate of a component

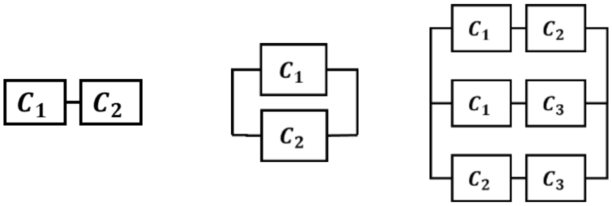
$$P_f(t) = 1 - e^{\left(-\frac{t}{\eta}\right)^{\beta}} \qquad (1)$$

$$P_f(t) = 1 - e^{-\lambda t} \qquad (2)$$

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

2.2 Reliability Block Diagrams

A reliability block diagram is a graphical representation showing the logical connections between the components in the system. These diagrams are used to compute the overall reliability of the system/functions 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. The terms series and parallel carry the same meaning as in the electrical circuits. Figures 2(a) and 2(b) shows series and parallel connections for two components $C_1$and C_2. When components are connected in series, the overall reliability is the product of individual reliabilities of components assuming independence between components (Eq. 3). When components are connected in parallel, the overall reliability is obtained using the union rules from set theory. Also assuming independence between components the expression for overall reliability is obtained using Eq. (4).



(a) Series (b) Parallel (c) r from n

Figure 2. Series and Parallel connections of components

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

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

In Eq. (3) and Eq. (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 "r from n" operator, then all possible combinations are obtained and connected in parallel. The reliability of this component-system is calculated using series and parallel connection rules as stated above. The number of combinations is equal to ${}^{n}_{r}C$, 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 combinatory can be represented in the reliability block diagram as shown in Figure 2(c).

3. SYSTEM MODEL

The systems under consideration are mechanical systems or cyber-physical systems (CPS). Though, CPS have both mechanical and software components, we currently consider the reliability and failure possibility of mechanical systems only. Software components are assumed to be functional. Consideration of software component reliability metrics require additional future work as these components do not typically age as mechanical components and do not follow the typical bathtub curve. All the mechanical components are assumed to be in the second phase of the bathtub curves, where the failures are random ie the failure rates are constant and the failure probabilities are modeled using exponential distributions. Also, it is assumed that the failures in the components are independent, thus the failure of one component does not influence the functioning of other components in the system. Once a component fails in the system, it remains in the failed state till the end of mission.

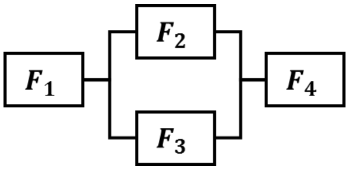
Also, it is assumed that the Mean Time to Failure (MTTF) information is available for all the components in the system.

4. PROPOSED METHODOLOGY

In this section, a step-by-step procedure is developed demonstrating the proposed methodology for reliability assessment.

Step 1. System Modeling: The system undergoing 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. The proposed methodology is independent of the language used for modeling. During modeling, each component in the model is associated to the list of functions that require this component. Each component is associated with a corresponding MTTF (mean time to failure) value. The MTTF values for all the components are assumed to be available for analysis.

Step 2. 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 4. 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 take a left at A, move forward from A to C, take a right turn at C, move forward from C to D. Let 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 6 becomes a function-time diagram). For each of the high-level functions, functional decomposition is carried out to obtain the leaf-level functions. 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 7. From the tree-structure, a Boolean expression for the high-level function can be obtained in terms of the leaf-level functions. This Boolean expression can be converted to a reliability block diagram. The symbol $\wedge$ represents series connection (i.e., both components are needed) and $\vee$ represents parallel connection (i.e., one of the components is needed). For example, consider a high-level function F which is expressed in terms of leaf-level functions as $F_1 \wedge (F_2 \vee F_3) \wedge F_4$. This Boolean expression when expressed as a reliability block diagram becomes



Step 3. 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. 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. (Eg., 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 derived from GME because in the modeling stage, the association of each component to the list of functions has been made. Again the function-component associations can be expressed using Boolean expressions, which can be extended to obtain the corresponding reliability block diagrams as stated in Step 2.

Step 4. 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. Apart from the function-component associations, there are additional constraints called implication constraints (Mahadevan, Dubey, Balasubramanian & Karsai, 2013) that arise from the system model. For example, consider a simple function of power generation in an automobile, which requires an internal combustion engine. When the function-component association is made, the power generation will be associated with the internal combustion engine. But for the working of internal combustion engine, 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. Therefore, these implications should also be included in constructing the reliability block diagram. 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 also the time each function is required for. Using this function-time information, we can calculate the time each of the components is required for. 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).

Step 5. Real-Time monitoring for 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. Mission feasibility, as defined in the previous section, can also be analyzed using the health of the components. At any time instant, real-time reliability assessment of the system can be carried out using Step 4. Using the results of real-time reliability assessment, decisions on continuing the mission, aborting the mission or carrying out a simpler mission (a mission with lower outcomes than originally intended) can be made. Also, decisions in choosing alternate paths to maximize the reliability of the mission can be made. When a component becomes unavailable, it can be specified in PyEDA, and it produces a resultant Boolean expression by removing the unavailable component(s). The resultant Boolean expression can be used for reliability assessment of the mission. Figure 3 shows the proposed methodology for reliability assessment.

In Figure 3, the mission is described using high level functions F_1, F_2, F_3, F_4. Then, using functional decomposition, the high level functions are decomposed to leaf-level functions. Then each of the leaf-level functions F_k (k = 5 to 14) is associated to 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.

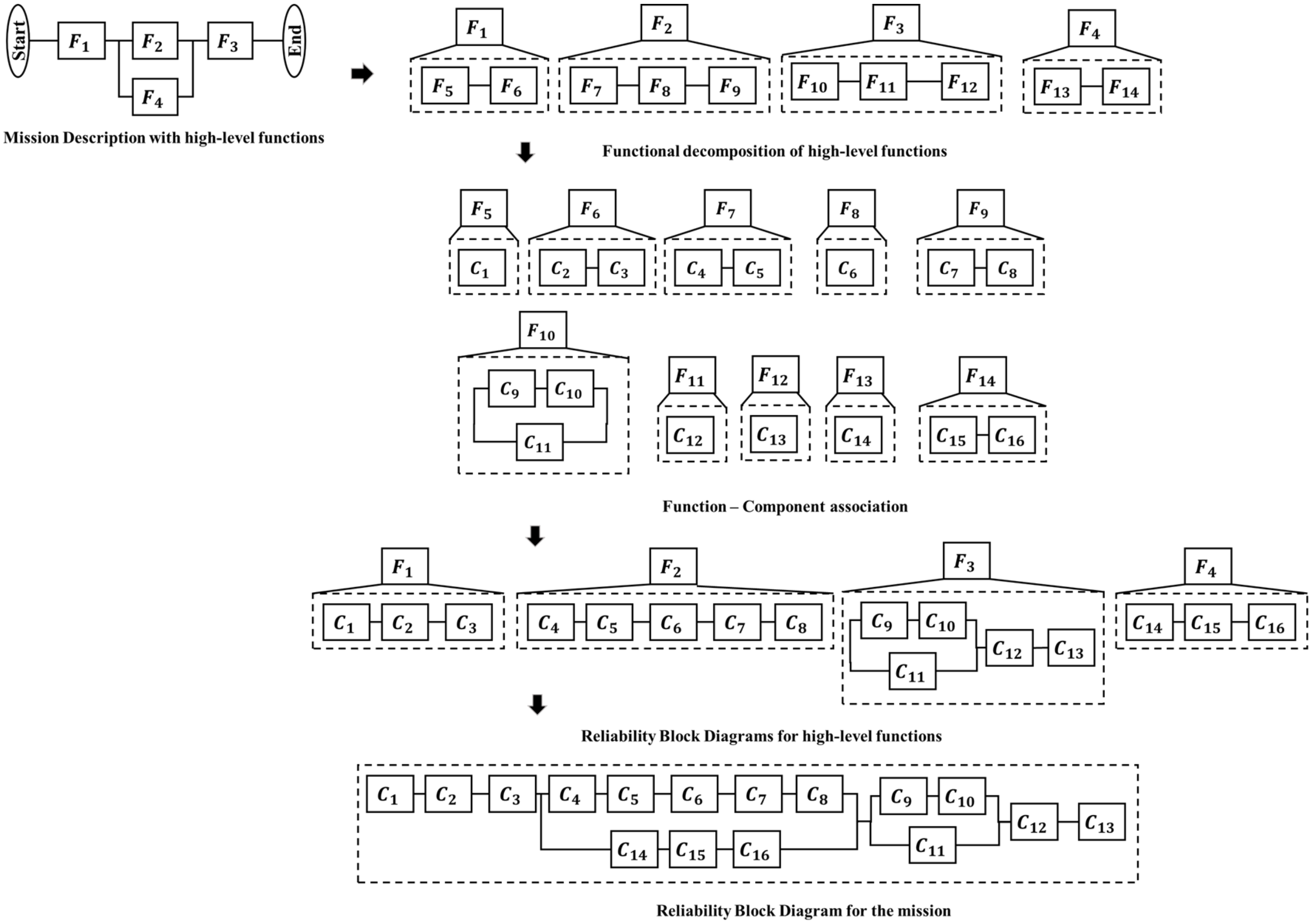

Start
F1
F2
F3
F4
End
Mission Description with high-level functions
F1 F5 F6
F2 F7 F8 F9
F3 F10 F11 F12
F4 F13 F14
Functional decomposition of high-level functions
F5 C1
F6 C2 C3
F7 C4 C5
F8 C6
F9 C7 C8
F10 C9 C10 C11
F11 C12
F12 C13
F13 C14
F14 C15 C16
Function – Component association
F1 C1 C2 C3
F2 C4 C5 C6 C7 C8
F3 C9 C10 C11 C12 C13
F4 C14 C15 C16
Reliability Block Diagrams for high-level functions
C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 C12 C13 C14 C15 C16
Reliability Block Diagram for the mission

Figure 3. Methodology for Reliability Assessment

5. 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 4. 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 mile. The total distance to be covered when moving on land from A to B is 2.5 mile. The speeds when moving on land and in water are assumed to be 7.5 mph and 3 mph respectively. The RC Car as modeled in GME (Ledeczi, Maroti, Bakay, Karsai, Garrett, Thomason & Volgyesi, 2001) is shown in Figure 5. A simple model of the RC Car is used for illustration and 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 along with this, a secondary emergency braking system is also assumed to be available. From the mission description, the function-time plot can be constructed as shown in Figure 6. 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, D are shown in Figure 4. 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 1 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. Figure 7 provides the decomposition of the high- level function in moving from A to B (F_{AB}) along with duration of each of the leaf-level functions required.

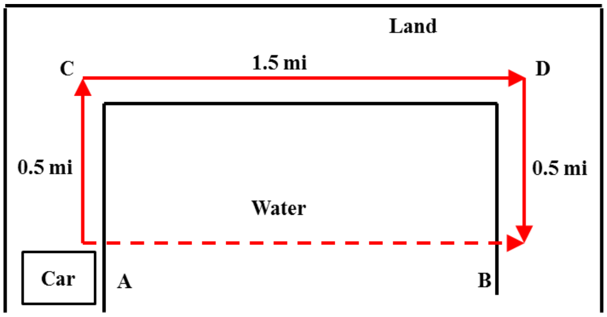


Figure 4. Mission Description

Table 1.Sub-functions of $\boldsymbol{F_{AB_L}}$ and their leaf-level functions

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

Using the hierarchical decomposition, the function F_{AB} can be expressed in terms of the leaf-level functions as

$$F_{AB} = \big((F_1 \wedge F_2 \wedge F_3 \wedge F_4 \wedge F_5 \wedge F_6 \wedge F_7 \wedge F_8) \vee (F_9 \wedge F_8)\big) \qquad (5)$$

The next step after obtaining the hierarchical decomposition is to associate component assemblies to carry out each of the atomic-level functions. Table 2 shows the list of component assemblies available in the RC Car system along with their MTTF values and Table 3 shows the association between atomic-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 atomic functions in Equation 1 are substituted with their associated component assemblies from Table 3, (2) all the components connected with $'\wedge'$ are written in series, whereas components connected with $'\vee'$ are written in parallel. The reliability block diagram for the mission is assembled using the PyEDA package in python.

All the components are assumed to be in the second phase of the bathtub curve where the failure rates are constant and failure probability is modeled using exponential distribution as stated in Section 3.

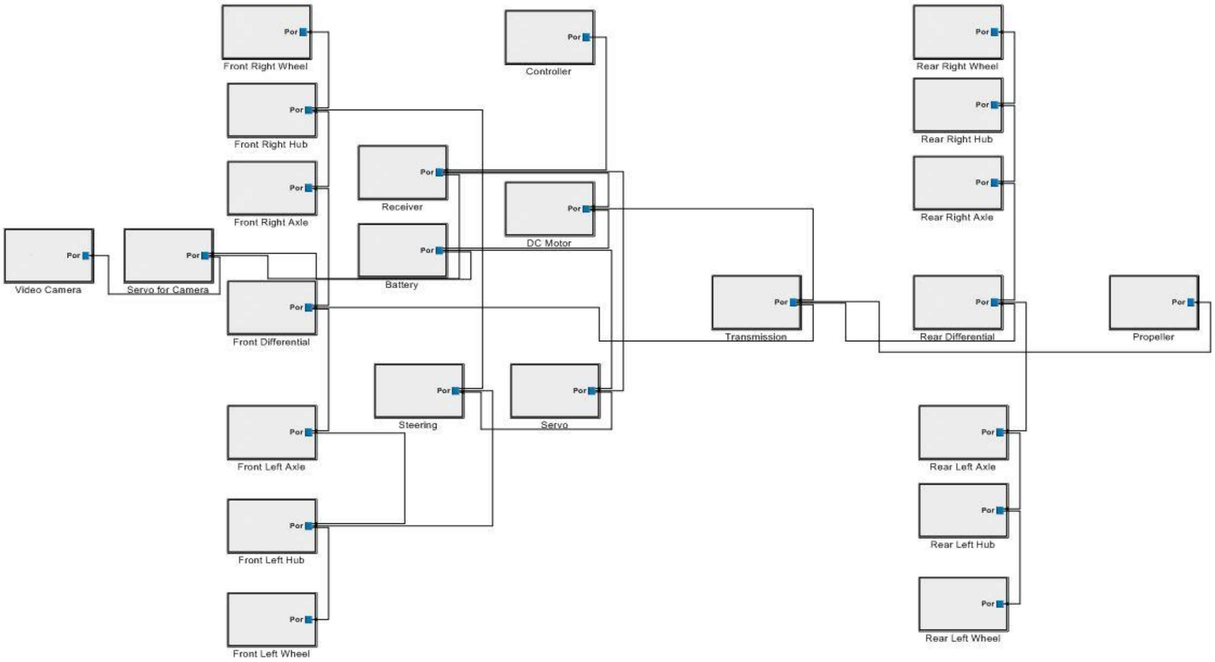


Figure 5. Modeling of the RC Car

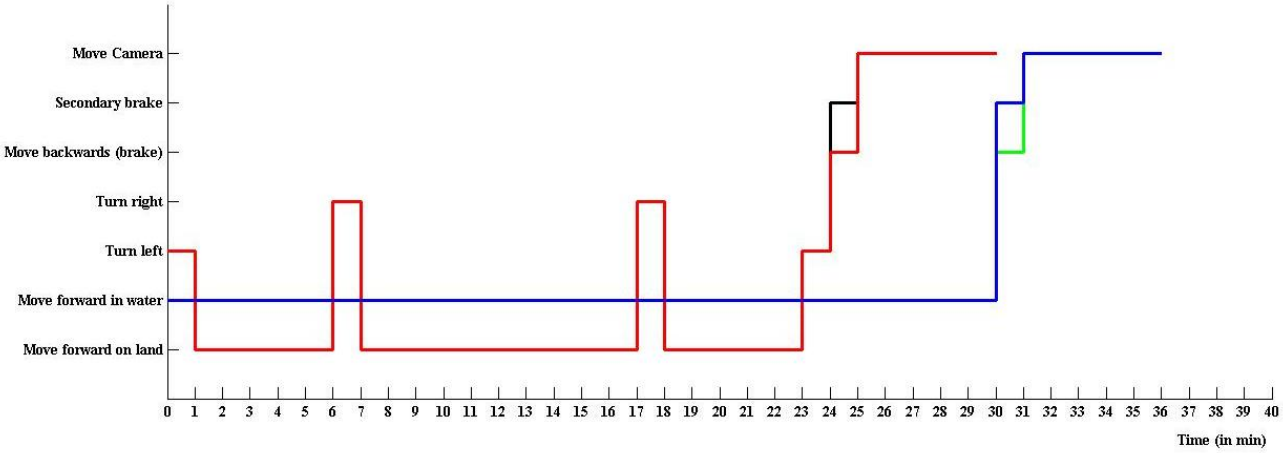


Figure 6. Function-Time Diagram for the mission

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 as 0.909.

Case 1: Real-time reliability assessment

Assume that the mission was being undertaken by moving in water to reach from A to B. Let T denote the time into the mission, therefore T=0 and T=36 refer to the start and the end of the mission (Figure 6). Tables 4 show the functions required to complete the mission at time T=0 and time T=20.

The third column in Table 4 can be interpreted as follows - At T=20, for successful completion of the mission, F_{AB_W} is required for 10 more minutes (T=20 to T=30), Braking is required for 1 minute and surveillance for 5 minutes. And all these three functions are required in succession, as shown in the function-time diagram (Figure 6). The reliability block diagram for the mission at time T=20, is assembled using the PyEDA package. Using the reliability block diagram and the MTTF values of the components, the reliability (probability of success) of the remaining portion of mission can be computed.

Case 2: Component unavailability

Assume that at time T = 20, 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. The reliability of the remaining mission, given that there is no failure up to T = 20, decreases from 0.963 to 0.959.

Case 3: Mission Feasibility

Assume that the camera fails during the travel from A to B in water. Since camera component becomes unavailable, the surveillance cannot be carried out at point B because there is no redundancy available for the surveillance function. Therefore, the mission cannot be carried out successfully. A real-time decision can be made to abort the mission and bring back the RC Car to point A.

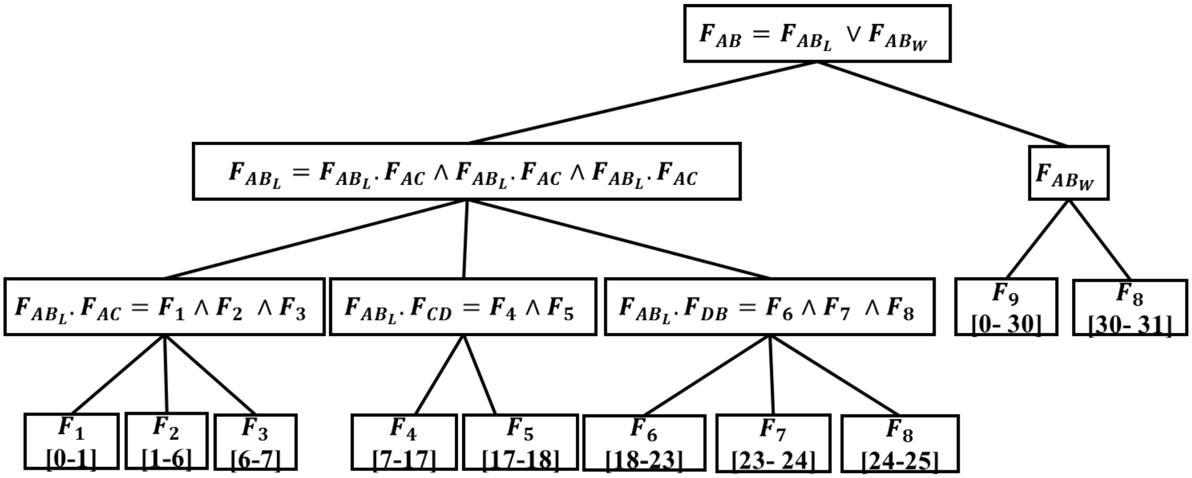

$F_{AB} = F_{AB_L} \vee F_{AB_W}$
$F_{AB_L} = F_{AB_L}.F_{AC} \wedge F_{AB_L}.F_{AC} \wedge F_{AB_L}.F_{AC}$
F_{AB_W}
$F_{AB_L}.F_{AC} = F_1 \wedge F_2 \wedge F_3$
$F_{AB_L}.F_{CD} = F_4 \wedge F_5$
$F_{AB_L}.F_{DB} = F_6 \wedge F_7 \wedge F_8$
F_9 [0- 30]
F_8 [30- 31]
F_1 [0-1]
F_2 [1-6]
F_3 [6-7]
F_4 [7-17]
F_5 [17-18]
F_6 [18-23]
F_7 [23- 24]
F_8 [24-25]

Figure 7. Hierarchical decomposition of the function of moving from A to B (F_{AB})

Table 2. Components in the RC Car and their MTTF values

Component Assembly	Notation	MTTF
Front Wheel System	W_F	5000
Front Hub System	H_F	3000
Front Axle System	A_F	4000
Front Differential	D_F	3000
Transmission	T	2000
DC Motor	DCM	2000
Battery	B	5000
Receiver	R	5000
Servo	S	2000
Steering	St	2000
Servo for Camera	S_C	2000
Camera	C	3000
Rear Differential	D_R	3000
Rear Axle System	A_R	4000
Rear Hub System	H_R	3000
Rear Wheel System	W_R	5000
Propeller	P	700
Chassis	Ch	5000
Secondary Brake System	E_B	1000

Table 3.Leaf-level functions and their components

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. Functions required at T=0 and T=20

Function	Duration required	
	T=0	T=20
Moving in water (F_9)	30	10
Brake at point B (F_8)	1	1
Surveillance (F_S)	5	5

6. CONCLUSION

In this paper, a formal framework has been proposed for reliability assessment of component-based systems, in carrying out specific missions. The key concepts are (1) Functional decomposition, (2) Function-Component association, and (3) Extraction of mission-level reliability diagram. The system undergoing the mission is modeled in Generic Modeling Environment (GME) and each component is associated to the list of functions that it is required for. Functional decomposition is performed for each of the high-level functions in the mission and represented using a hierarchical tree-structure. For each of the leaf-level function, the corresponding components are extracted from the GME and exported to the PyEDA package in Python, where a reliability block diagram is obtained using Boolean expressions. Using the reliability information of the components, the reliability assessment of the mission can be carried out. This procedure can be used for real-time reliability assessment and monitoring of the mission. Using the reliability estimates of the mission as a function of time, 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. Future work should address reliability assessment in the presence of dependencies between failures in the components, operational dependencies, and mission dependencies. Also, failure rates that depend on the degradation of the components will need to be considered.

ACKNOWLEDGEMENT

The research presented in this paper was supported by funds from DARPA as part of the Adaptive Vehicle Make (AVM) Project. The support is gratefully acknowledged. The authors also thank Dr. Gautam Biswas and Dr. Xenofon Koutsoukos of Vanderbilt University for valuable discussions during this research.

REFERENCES

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

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.

Dubey, A., Mahadevan, N., & Karsai, G. (2012). The inertial measurement unit example: A software health management case study. ISIS, 12, 101.

Elsayed, E. A. (2012). *Reliability engineering*. Wiley Publishing.

Ericson, C. A. (2005). Event Tree Analysis. *Hazard Analysis Techniques for System Safety*, 223-234.

Filliben, J. J. (2002). NIST/SEMTECH Engineering Statistics Handbook. Gaithersburg: www. itl. nist. gov/div898/handbook, NIST.

Greenfield, M. A. (2001). NASA's use of quantitative risk assessment for safety upgrades. *Space safety, rescue and quality*, 153-159.

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

Krishnamurthy, S., & Mathur, A. P. (1997). On the estimation of reliability of a software system using reliabilities of its components. *Proceedings of 8th International Symposium in Software Reliability Engineering* (pp. 146-155). IEEE.

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. & Volgyesi, P. (2001). The generic modeling environment. *Workshop on Intelligent Signal Processing,* Budapest, Hungary (Vol. 17).

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.

Modarres, M. (2008). Probabilistic Risk Assessment. *Handbook of Performability Engineering* (pp. 699-718). Springer London.

Mosterman, P. (2007). Model-based design of embedded systems. *IEEE International Conference on Microelectronic Systems Education,* IEEE.

Phillips, A. M. (2002). Functional decomposition in a vehicle control system. *Proceedings of American Control Conference* (Vol. 5, pp. 3713-3718). IEEE.

Python library for Electronic Design Automation (PyEDA) Documentation [Online]. https://media.readthedocs.org/pdf/pyeda/latest/pyeda.pdf. Last accessed – May 30, 2014

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). IEEE.

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.

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

APPENDIX

Definitions

Mission: A mission can be regarded as a time-interval sequence of high-level functions. A mission provides information of all the high-level functions to be carried out at each instant of time. At each time instant, one or more high-level functions can be carried out. The mission is usually represented using a function-time plot.

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 dependency relationships can be written using the following 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 dependency trees are active. A leaf-level function might be required for several high-level functions and therefore appears in several trees

Function-Component association: The next step after functional decomposition is association of each leaf-level function to corresponding component or component assemblies (Kurtoglu, Tumer & Jensen, 2010). Again, Boolean relationships are used to represent the association of components to its functions. The Boolean relationships – and, or, r-out-of-n, are used to associate each leaf-level function to its component assembly. A component can provide more than one 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 operation. 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 at later times 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 at a later time, then the corresponding function cannot be carried out. If there are no alternate possibilities available to carry out this function, then this 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.