

# AN EFFICIENT APPROACH FOR THE RELIABILITY ANALYSIS OF PHASED-MISSION SYSTEMS WITH DEPENDENT FAILURES

LIUDONG XING

*Electrical and Computer Engineering Department  
University of Massachusetts-Dartmouth*

LEILA MESHKAT

*Jet Propulsion Laboratory  
California Institute of Technology*

SUSAN K. DONOHUE

*Department of Systems and Information Engineering  
University of Virginia*

## ABSTRACT

We consider the reliability analysis of phased-mission systems with common-cause failures in this paper. Phased-mission systems (PMS) are systems supporting missions characterized by multiple, consecutive, and non-overlapping phases of operation. System components may be subject to different stresses as well as different reliability requirements throughout the course of the mission. As a result, component behavior and relationships may need to be modeled differently from phase to phase when performing a system-level reliability analysis. This consideration poses unique challenges to existing analysis methods. The challenges increase when common-cause failures (CCF) are incorporated in the model. CCF are multiple dependent component failures within a system that are a direct result of a shared root cause, such as sabotage, flood, earthquake, power outage, or human errors. It has been shown by many reliability studies that CCF tend to increase a system's joint failure probabilities and thus contribute significantly to the overall unreliability of systems subject to CCF.

We propose a separable phase-modular approach to the reliability analysis of phased-mission systems with dependent common-cause failures as one way to meet the above challenges in an efficient and elegant manner. Our methodology is twofold: first, we separate the effects of CCF from the PMS analysis using the total probability theorem and the common-cause event space developed based on the elementary common-causes; next, we apply an efficient phase-modular approach to analyze the reliability of the PMS. The phase-modular approach employs both combinatorial binary decision diagram and Markov-chain solution methods as appropriate. We provide an example of a reliability analysis of a PMS with both static and dynamic phases as well as CCF as an illustration of our proposed approach. The example is based on information extracted from a Mars orbiter project. The reliability model for this orbiter considers the various phases of Launch, Cruise, Mars Orbit Insertion, and Orbit. Some of the CCF for the orbiter in this mission include environmental effects, such as micrometeoroids, human operator errors, and software errors.

## INTRODUCTION

A phased-mission system (PMS) is a system that is used in a mission characterized by multiple, consecutive, and non-overlapping operational phases. A classic example of a PMS is an aircraft flight, which involves take-off, ascent, level flight, descent, and landing phases. During each phase of the mission the system has to accomplish a specified (usually different) task, and may be subject to different stresses as well as different reliability requirements. Thus, system configuration, success/failure criteria, and component failure parameters may change from phase to phase. Also, statistical dependencies exist across the phases for a given component. For example, the state of a component in the beginning of a new phase is identical to its state at the end of the previous phase. The consideration of these dynamics and dependencies poses unique challenges to existing analysis methods. The challenges increase when common-cause failures (CCF) are incorporated in the model.

CCF are multiple dependent component failures within a system that are a direct result of a shared root cause, such as sabotage, flood, earthquake, power outage, or human errors [HOYL94]. It has been shown by many reliability studies that CCF tend to increase a system's joint failure probabilities and thus contribute significantly to the overall unreliability of systems subject to CCF [VAUR98]. Considerable research efforts have been expended in the study of CCF for reliability modeling and analysis of computer-based systems; see, for example, [AMAR99, DAI04, FLEM86, PHAM93, TANG05, VAUR98, VAUR03, XING03, XING05]. However, the existing CCF models are mainly applicable to non-PMS systems. They also have various limitations, such as being concerned with a specific system structure [see, for example, PHAM93]; applicable only to systems with exponential time-to-failure distributions [see, for example, FLEM86]; being subject to combinatorial explosion as the redundancy level of the system increases [see, for example, DAI04]; limiting analysis to components belonging to at most a single common-cause group (CCG) [TANG05, VAUR98]; having a single common cause (CC) that affects all components of a system [see, for example, AMAR99, PHAM93]; or defining CC as being statistically-independent or mutually exclusive [see, for example, VAUR03]. We seeked to address some of these limitations in developing a model for the reliability analysis of PMS subject to CCF by allowing for multiple CC that can affect different subsets of system components, and which can occur statistically-dependently in our recent work [XING03]. But [XING03] considered PMS with only static phases, in which the failure criteria depend only on the combination of component failures. In reality, however, most phased-mission systems are composed of both static and dynamic phases. A phase is a dynamic phase if any of the following behaviors occur in that phase: components are functionally independent, meaning that the failure of a component forces several other components to fail; cold/warm/hot spare components are utilized [DUGA01]; the order in which failures occur matters, for example, consider a standby system with one active component and one standby spare connected with a switch controller. If the switch controller fails after the active component fails and thus the standby component is already in use, the system can continue to work. However, if the switch controller fails before the active component fails, the standby component cannot be switched into active operation and thus the entire system fails [DUGA01]. Therefore, existing methods must be modified and/or extended so that the PMS dynamics, dependencies across the phases for a given component, functional dependencies, order of failures, and spare management can be addressed at the same time. We present one such extension to dynamic fault tree analysis in this paper.

The remainder of the paper is organized as follows: Section 2 presents some background on the existing phase-modular fault tree approach to the reliability analysis of PMS with both static and dynamic phases. Section 3 presents a separable phase-modular approach to the reliability analysis of PMS subject to CCF. The approach is illustrated using a hypothetical PMS subject to different CCF depending mission phases. In Section 4 we apply this approach to a space mission example. In the last section, we present our conclusions as well as directions for future work.

## THE PHASE-MODULAR APPROACH

Reliability analysis of PMS has been the subject of considerable research interest. Traditional approaches are either combinatorial or Markov-chain based. The combinatorial approaches, one example of which is the binary decision diagrams (BDD) based approach [XING02, ZANG99], are computationally efficient, but are applicable only to PMS with static phases. Markov based approaches can capture the dynamic behaviors such as functional dependencies among components, required order of failures, or spare management using Markov-chain models. But the major limitation with Markov based approaches is that if the failure criteria in only one phase are dynamic, then a Markov approach must be used for every phase. Due to the well-known state explosion problem of Markov approaches, it is often computationally intensive and even infeasible to solve the model.

Since combinatorial approaches and Markov approaches both have their pros and cons in the system modeling and analyzing, a phase-modular fault tree approach employing both combinatorial binary decision diagram and Markov-chain solution methods as appropriate was proposed [MESH00, MESH03, OU02]. This approach identifies modules of the fault trees that remain independent throughout the phase mission. It then finds the reliability of each independent module in each phase with an appropriate technique and combines the modules in a system level BDD to find the PMS reliability measures. Next we outline the basic elements of the phase-modular approach using a simple example PMS, which has three phases and eight components (Figure 1, adapted from MESH03).

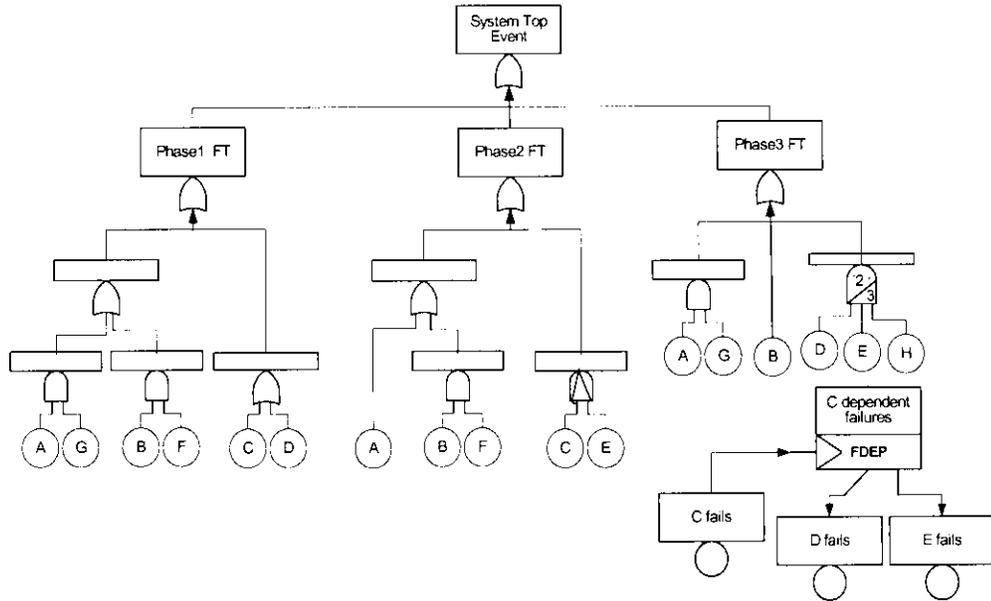


Figure 1. Example PMS Fault Tree

1. Represent each mission phase by a fault tree. Because the reliability of a PMS is the probability that the mission successfully achieves its objectives in all phases, we link the phase fault trees with an OR gate to obtain the entire PMS fault tree. The fault tree for each phase is then divided into independent subtrees. Subtrees are identified as static or dynamic in different phases depending on their characteristics. For example, consider the PMS fault tree in Figure 1, the phase-one fault tree includes two main modules,  $\{A, G, B, F\}$  and  $\{C, D\}$ , which are both static. The phase-two fault tree includes one static module  $\{A, B, F\}$ , and one dynamic module  $\{C, E\}$ . The phase-three fault tree includes two static modules  $\{A, G\}$ ,  $\{B\}$ , and one dynamic module  $\{C, D, E, H\}$ .
2. Find the system-level independent modules. This identification is accomplished by finding the unions of the components in all the phase modules that overlap in at least one component. There are two system-level independent modules,  $\{A, G, B, F\}$  and  $\{C, D, E, H\}$  in our example PMS fault tree.
3. Identify each phase module as static (all AND, OR, and/or K-OF-M gates) or dynamic (has at least one PAND, CSP, WSP, or HSP gate). For example, the module  $\{A, G, B, F\}$  is static and  $\{C, D, E, H\}$  is dynamic.
4. Identify each phase module as bottom-level (has no child modules) or upper-level (has child modules). For example, The module  $\{C, D\}$  in phase one is a bottom level module, and the module  $\{A, G, B, F\}$  is an upper level module since it contains the child modules  $\{A, G\}$  and  $\{B, F\}$  which are each linked to a gate. The identification of child and parent modules is vital information used in solving for these modules' reliability measure.
5. Find the joint phase module probabilities for all system-level modules. We use the BDD method [XING02, ZANG99] on modules that are static across all the phases. We use the combined Markov chain method as presented in [MESH00, OU02] on modules with at least one dynamic property. For the example PMS in Figure 1, we can use the BDD method on phase module  $\{A, G, B, F\}$  since it has

- static behavior in all the three phases. We must use the Markov chain method on phase module {C, D, E, H} since it has dynamic behavior in both phase 2 (a priority AND gate) and phase 3(a FDEP gate).
6. Consider each module a basic event of a static fault tree and solve the corresponding BDD to find the system reliability equation based on the reliability measures of the modules. Since we've already solved for the reliability measures of the modules in step 5, this step concludes the solution.

Figure 2 shows the modularized fault tree for the example PMS. Basically, each module's reliability is solved independent of the other modules, but with consideration of its own behavior in previous phases. For instance, in order to find the reliability of  $M1_2$ , we use a combined BDD approach for  $M1_1$  and  $M1_2$ ; in order to find the reliability of  $M2_3$ , we use the combined Markov chain approach on  $M2_1$ ,  $M2_2$ , and  $M2_3$ . We then consider solving the static PMS fault tree with the basic events  $M1_1$ ,  $M2_1$ ,  $M1_2$ ,  $M2_2$ ,  $M1_3$ , and  $M2_3$  using the combined BDD approach and the reliability measures for each individual phase module computed from previous steps. It is important to note that solving this simple PMS fault tree without using the modularization technique would involve solving a Markov chain with approximately 256 states, while the Markov chain involved in this example has a maximum of only 16 states. The phase-modular approach provides exact reliability measures in an efficient manner. In the next section, we present a separable approach based on the efficient phase-modular approach to the reliability analysis of PMS subject to dependent common-cause failures.

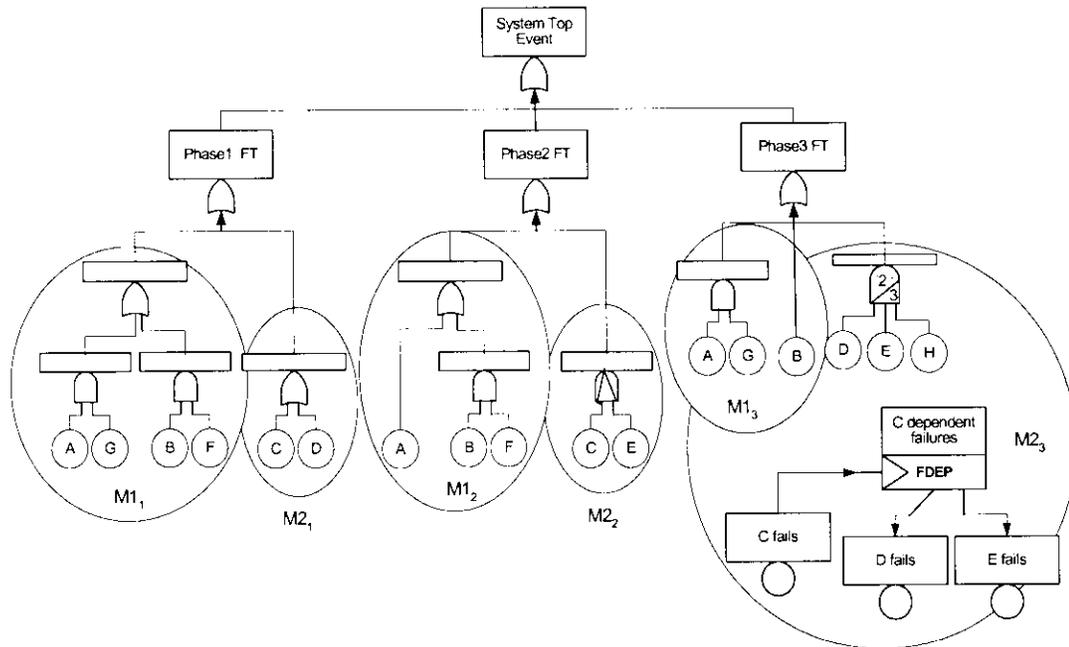


Figure 2. Modularized Example PMS Fault Tree

## SEPARABLE PHASE-MODULAR APPROACH

### General assumptions and our PMS CCF model

We make the following general assumptions for the CCF analysis in the PMS:

1. Component failures are statistically independent within each phase.
2. Phase durations are deterministic.
3. The system is not maintained during the mission: once a component has failed, it remains failed for all later phases.
4. PMS can be subject to CCF due to different elementary common-causes occurring within a phase or in different phases. In general, we express the elementary common-causes (CC) existing in a PMS as:

$$\text{Phase } I: CC_{1I}, \dots, CC_{L_I}$$

Phase 2:  $CC_{21}, \dots, CC_{2L_2}$

Phase  $m$ :  $CC_{m1}, \dots, CC_{mL_m}$

where  $L_i$  denotes the number of elementary CC involved in phase  $i$ ,  $m$  is total number of phases in the PMS, thus  $L = \sum_{i=1}^m L_i$  is the total number of CC existing in the PMS.

5. Different common causes, whether from the same phase or from different phases can be mutually exclusive, or  $s$ -independent, or  $s$ -dependent ( $s$  denotes statistically).
6. A component may be affected by multiple common causes, that is, one single component can belong to more than one common-cause group (CCG). All components that are caused to fail due to the same elementary common-cause  $CC_{ij}$  constitute a common-cause group  $CCG_{ij}$ .

### An illustrating example

To illustrate the basics and advantages of the proposed separable phase-modular approach, we incorporate the following hypothetical scenario about CCF into the example PMS described in Figure 1: the system is subject to CCF from hurricanes (denoted by  $CC_{1i}$ ) during the first phase, from lightning strikes (denoted by  $CC_{2i}$ ) during the second phase, and from floods (denoted by  $CC_{3i}$ ) during the last phase. A hurricane of sufficient intensity in Phase 1 would cause components  $A$  and  $C$  to fail, that is,  $CCG_{11} = \{\overline{A_1}, \overline{C_1}\}$ , where  $A_1$  is the state indicator variable of component  $A$  in Phase 1, and  $\overline{A_1}$  denotes the failure of component  $A$  in Phase 1; serious lightning strikes in Phase 2 would cause  $B$ ,  $E$ , and  $F$  to fail, that is,  $CCG_{21} = \{\overline{B_2}, \overline{E_2}, \overline{F_2}\}$ ; serious flooding in Phase 3 would cause  $C$  and  $G$  to fail, that is,  $CCG_{31} = \{\overline{C_3}, \overline{G_3}\}$ . According to the available weather information, the following data should be able to be extracted: the probability of a hurricane occurring in Phase 1 is  $P_{CC_{1i}} = 0.02$ ; the probability of a lightning strike occurring in Phase 2 is  $P_{CC_{2i}} = 0.03$ ; the floods often occur in conjunction with hurricanes, and the  $s$ -dependency between the two CC can be defined by a set of conditional probabilities, conditioned on the state of hurricanes (occurred or not occurred) in Phase 1: the probability that floods occur in Phase 3 conditioned on the occurrence of hurricanes in Phase 1, is simply denoted by  $\Pr\{\text{flood}_3 / \text{hurricane}\} = P_{CC_{3i}|CC_{1i}} = 0.6$ ; similarly,  $\Pr\{\overline{\text{flood}}_3 / \text{hurricane}\} = P_{\overline{CC_{3i}}|CC_{1i}} = 1 - P_{CC_{3i}|CC_{1i}} = 0.4$ ;  $\Pr\{\text{flood}_3 / \overline{\text{hurricane}}\} = P_{CC_{3i}|\overline{CC_{1i}}} = 0.03$ ; and  $\Pr\{\overline{\text{flood}}_3 / \overline{\text{hurricane}}\} = P_{\overline{CC_{3i}}|\overline{CC_{1i}}} = 1 - P_{CC_{3i}|\overline{CC_{1i}}} = 0.97$ . Other input parameters such as failure parameters and mission time will be provided when needed.

### A separable approach to incorporating CCF

We propose an efficient separable approach for incorporating the effects of CCF into the reliability evaluation of PMS in this section. Our methodology is to decompose an original PMS reliability problem with CCF into a number of reduced reliability problems based on the Total Probability Theorem. The set of reduced problems does not have to consider dependencies introduced by CCF, because the effects of CCF have been factored out. And the problems can be solved using the phase-modular approach [MESH03]. Finally, the results of all reduced reliability problems are aggregated to obtain the entire PMS reliability measure considering the CCF.

Specifically, based on our CCF model for PMS, there exist totally  $L$  elementary CC in a PMS. The  $L$  CC partition the event space into the following  $2^L$  disjoint subsets, each called a common-cause event (CCE):

$$\begin{aligned}
 CCE_1 &= \overline{CC_{11}} \cap \dots \cap \overline{CC_{1L_1}} \cap \dots \cap \overline{CC_{m1}} \cap \dots \cap \overline{CC_{mL_m}}, \\
 CCE_2 &= CC_{11} \cap \dots \cap \overline{CC_{1L_1}} \cap \dots \cap \overline{CC_{m1}} \cap \dots \cap \overline{CC_{mL_m}}, \\
 &\dots, \\
 CCE_{2^L} &= CC_{11} \cap \dots \cap CC_{1L_1} \cap \dots \cap CC_{m1} \cap \dots \cap CC_{mL_m}.
 \end{aligned}$$

We then build a space called “CCE space” over this set of collectively exhaustive and mutually exclusive common-cause events that can occur in a PMS, that is,  $\Omega_{CCE} = \{CCE_1, CCE_2, \dots, CCE_{2^t}\}$ . If  $P(CCE_j)$  denotes the probability of  $CCE_j$  occurring, then we have  $\sum_{j=1}^{2^t} P(CCE_j) = 1$  and  $CCE_i \cap CCE_j = \phi$  for any  $i \neq j$ .

Consider the example PMS presented in the last subsection, the CCE space is composed of  $2^3 = 8$  CCE, that is,  $\Omega_{CCE} = \{CCE_1, CCE_2, \dots, CCE_8\}$ , given that there are 3 elementary common-causes  $CC_{1j}$  (hurricanes),  $CC_{2j}$  (lightning strikes), and  $CC_{3j}$  (floods). Each  $CCE_i$  is a distinct and disjoint combination of elementary CC, as defined in the first column of Table 1. Let  $A_{CCE_i}$  denote a set of components, which are the only ones affected by the common-cause event  $CCE_i$ . In other words, the occurrence of event  $CCE_i$  leads to the failure of all components and only those in  $A_{CCE_i}$ . For non-PMS,  $A_{CCE_i}$  is simply the union of those CCG whose corresponding elementary common-causes occur [XING05]. For example, assume  $CCE_i = \overline{CC_{11}} \cap \overline{CC_{21}} \cap \overline{CC_{31}}$  is a CCE in a non-PMS with three elementary CC, then  $A_{CCE_i}$  is equal to  $CCG_3$  because its corresponding elementary common-cause  $CC_3$  occurs. For non-maintainable PMS, because the system is not maintained during the mission, a component remains failed in all later phases once it fails. The  $CCG_{ij}$  ( $i$  is the phase index in PMS,  $j$  is the CC index within phase  $i$ ) affected by an elementary common-cause  $CC_{ij}$  occurring in some phase  $i$  should be expanded to incorporate the affected components in all subsequent phases  $i+1, \dots, m$ . In addition, for dynamic PMS, if the trigger event of a FDEP gate is affected by an elementary CC in some phase  $i$ , then the related dependent events in the phase  $i$  and all subsequent phases should also be included into the corresponding CCG. We denote the expanded CCG as  $CCG_{ij}^*$  which will be used to find  $A_{CCE_i}$  using similar procedure for non-PMS. For example, the expanded CCG for the example PMS are:  $CCG_{11}^* = \{\overline{A_{(1-3)}}, \overline{C_{(1-3)}}\} = \{\overline{A_1}, \overline{A_2}, \overline{A_3}, \overline{C_1}, \overline{C_2}, \overline{C_3}\}$ ,  $CCG_{21}^* = \{\overline{B_{(2-3)}}, \overline{E_{(2-3)}}, \overline{F_{(2-3)}}\} = \{\overline{B_2}, \overline{B_3}, \overline{E_2}, \overline{E_3}, \overline{F_2}, \overline{F_3}\}$ , and  $CCG_{31}^* = \{\overline{C_3}, \overline{D_3}, \overline{E_3}, \overline{G_3}\}$  (there is a FDEP gate in phase 3 fault tree: the failure of component C cause both D and E to fail); the resulted  $A_{CCE_i}$  ( $i=1, 2, \dots, 8$ ) are shown in the second column of table 1. Based on the statistical relation among the elementary CC: lightning strikes  $CC_{2j}$  occur independently, and the occurrence of floods  $CC_{3j}$  is s-dependent on the occurrence of hurricanes  $CC_{1j}$ , the occurring probability of each  $CCE_i - P(CCE_i)$  can be calculated as shown in the third column of table 1.

Table 1. CCE, Affected Components, CCE's Occurrence Probabilities for Example PMS

$CCE_i$	$A_{CCE_i}$	$P(CCE_i)$
$CCE_1 = \overline{CC_{11}} \cap \overline{CC_{21}} \cap \overline{CC_{31}}$	$\phi$	$P_{CC_{11}} P_{CC_{21}} P_{CC_{31}   CC_{11}}$ = 0.9221
$CCE_2 = \overline{CC_{11}} \cap \overline{CC_{21}} \cap CC_{31}$	$CCG_{31}^* = \{\overline{C_3}, \overline{D_3}, \overline{E_3}, \overline{G_3}\}$	$P_{CC_{21}} P_{CC_{11}} P_{CC_{31}   CC_{11}}$ = 0.0285
$CCE_3 = \overline{CC_{11}} \cap CC_{21} \cap \overline{CC_{31}}$	$CCG_{21}^* = \{\overline{B_{(2-3)}}, \overline{E_{(2-3)}}, \overline{F_{(2-3)}}\}$	$P_{CC_{21}} P_{CC_{11}} P_{CC_{31}   CC_{11}}$ = 0.0285
$CCE_4 = \overline{CC_{11}} \cap CC_{21} \cap CC_{31}$	$CCG_{21}^* \cup CCG_{31}^* = \{\overline{B_{(2-3)}}, \overline{E_{(2-3)}}, \overline{F_{(2-3)}}, \overline{C_3}, \overline{D_3}, \overline{G_3}\}$	$P_{CC_{21}} P_{CC_{11}} P_{CC_{31}   CC_{11}}$ = $8.82e - 4$
$CCE_5 = \overline{CC_{11}} \cap \overline{CC_{21}} \cap \overline{CC_{31}}$	$CCG_{11}^* = \{\overline{A_{(1-3)}}, \overline{C_{(1-3)}}\}$	$P_{CC_{11}} P_{CC_{21}} P_{CC_{31}   CC_{11}}$ = 0.0078
$CCE_6 = \overline{CC_{11}} \cap \overline{CC_{21}} \cap CC_{31}$	$CCG_{11}^* \cup CCG_{31}^* = \{\overline{A_{(1-3)}}, \overline{C_{(1-3)}}, \overline{D_3}, \overline{E_3}, \overline{G_3}\}$	$P_{CC_{11}} P_{CC_{21}} P_{CC_{31}   CC_{11}}$ = 0.0116
$CCE_7 = \overline{CC_{11}} \cap CC_{21} \cap \overline{CC_{31}}$	$CCG_{11}^* \cup CCG_{21}^* = \{\overline{A_{(1-3)}}, \overline{C_{(1-3)}}, \overline{B_{(2-3)}}, \overline{E_{(2-3)}}, \overline{F_{(2-3)}}\}$	$P_{CC_{11}} P_{CC_{21}} P_{CC_{31}   CC_{11}}$ = $2.4e - 4$
$CCE_8 = \overline{CC_{11}} \cap CC_{21} \cap CC_{31}$	$CCG_{11}^* \cup CCG_{21}^* \cup CCG_{31}^* = \{\overline{A_{(1-3)}}, \overline{C_{(1-3)}}, \overline{B_{(2-3)}}, \overline{E_{(2-3)}}, \overline{F_{(2-3)}}, \overline{D_3}, \overline{G_3}\}$	$P_{CC_{11}} P_{CC_{21}} P_{CC_{31}   CC_{11}}$ = $3.6e - 4$

Based on the CCE space we developed in the above, we can calculate the unreliability of a PMS with CCF using Total Probability Theorem as:

$$U_{PMS} = \sum_{j=1}^{2^L} [\Pr\{PMS \text{ fails} | CCE_j\} P(CCE_j)] \quad (1)$$

As described above,  $\Pr(CCE_i)$  in Eq. (1) can be obtained based on the relationship between the elementary common-causes and the occurrence probabilities of elementary CC ( $P_{CC}$ ) which are given as input parameters in this research. The conditional probability  $\Pr(\text{PMS fails}|CCE_i)$  is actually a reduced PMS reliability problems, in which the components affected by  $CCE_i$ , that is the components in the set  $A_{CCE_i}$  do not appear. Specifically, in the system DFT model, each basic event (the failure of a component) that appears in  $A_{CCE_i}$  will be replaced by a constant logic value “1” (*True*). After the replacement, a Boolean reduction can be applied to the PMS DFT to generate a simpler DFT in which all the components of  $A_{CCE_i}$  do not appear. Most importantly, the evaluation of the reduced DFT can proceed using the existing phase-modular approach [MESH03] without further consideration of CCF, thereby reducing the overall complexity of the solution.

Consider the example PMS, the original PMS reliability problem with CCF can now be subdivided into eight reduced problems that need not consider CCF. Based on the system configuration depicted in figure 1, we can derive that:  $\Pr\{\text{PMS fails}|CCE_j\} = 1$  for  $j = 2, 3, 4, 5, 6, 7, 8$ ; because no component is affected by  $A_{CCE_1}$  which is  $\phi$ ,  $\Pr\{\text{PMS fails}|CCE_j\}$  can be obtained by evaluating the original PMS fault tree in figure 1 using the phase modular approach without considering CCF. The value of  $\Pr\{\text{PMS fails}|CCE_j\}$  is 0.000682146 using the failure parameters in table 2. Finally according to Equation (1), the unreliability of the example PMS subject to CCF as 0.0785 for the mission time of 200 hours is obtained by aggregating the results of  $\Pr\{\text{PMS fails}|CCE_j\}$  and  $\Pr(CCE_i)$  (table 1).

Table 2. Component failure rates ( $10^{-6}/\text{hr}$ ) and mission duration for the example PMS

	A	B	C	D	E	F	G	H
Phase 1 (24 hrs)	1	0.5	3	3	1.5	1	2	1
Phase 2 (150 hrs)	2	1	2	2	1	1	1	2
Phase 3 (26 hours)	1.5	1	1	1	2	1	1	2

### AN EXAMPLE PMS SPACE MISSION SYSTEM

The fault tree of our example PMS space mission, given in Figure 3, below, has been drawn from data extracted from expert opinions about the possible risk elements of the Mars Smart Lander project (MSL-09). Note that the failure events considered here are a subset of the existing events that can contribute to a failure. The system characteristics are not fully shown here; rather, we consider a very simplified version for demonstration purposes only.

We consider a three-phased space mission that consists of the following phases: Launch; Cruise; and Entry, Descent, Landing (EDL). In the first two phases, the system can fail because of Radioactive Power Source (RPS) induced failures, such as thermal issues and radiation effects. During the launch phase, the system can also fail due to the launch vehicle failure. During the cruise phase, it can fail as a result of Optimal Navigation (OpNav) issues or Cruise stage related failures. During EDL, propulsion and avionics, thermal, and radiation issues as well as the failure of hazard detection and avoidance issues can lead to a system failure. The hazard detection and avoidance issues occur as a result of the failure of both the LIDAR and the RADAR. Each of the basic events connected directly to the top event are static modules. The RPS induced failure is a dynamic module.

Having established the phase and system fault trees as per step one of the phase-modular method, we then identify the system-level independent modules as per step two. Note that the only components present in all phases are Thermal Issues and Radiation Effects. In the first two phases, the RPS accommodation issues can lead to the occurrence of thermal issues and radiation effects; in the third phase, the only cause for the failure of each of them is their own individual failure rates. This behavior leads us to group these components together in the dynamic phase module {RPS accommodation, Thermal Issues, Radiation Effects}. The basic events “launch vehicle,” “Opnav

system," "Cruise stage," "Avionics" and "Propulsion" are directly linked to the phase fault tree and do not overlap in any component. Therefore, they are phase independent static bottom level modules. "Hazard detection and avoidance" is an upper level parent module that consists of the basic events "LIDAR" and "RADAR."

We then find the reliability of each module as per step 3. The only phase module that needs to be solved using combined Markov chain approach is the module {RPS accommodation, Thermal issues, Radiation Effects}. We solve this module in each phase. The reliability measure of this module at each phase level is obtained and input to the higher level system fault tree. The upper level module, "Hazard detection and avoidance," is also solved for the duration of phase three, and its reliability measure is input to the higher level fault tree.

At this point, each of the phase modules are considered a basic event with a failure rate equal to their reliability measures in the given phase. The reliability of the overall system fault tree is then found using a combined static approach as per step four.

TABLE 3: COMPONENTS FAILURE RATES ( $10^{-6}$ /HR) AND MISSION DURATION FOR EXAMPLE

	Phase 1 (10hrs)	Phase 2 (5050hrs)	Phase 3(24hrs)
Launch Vehicle	1	0.1	1
Thermal Issues	0.1	1	1
Radiation Effects	0.02	0.02	0.02
RPS Accomodation Issues	0.1	0.1	0.2
OPNAV System	0.01	0.1	0.1
Cruise Stage	0.001	0.001	0.1
Avionics	0.001	0.01	0.1
LIDAR	0.001	0.001	0.1
RADAR	0.001	0.001	0.1
Propulsion	0.1	0.01	0.1

Using the approach mentioned above, and the failure rates in table 3, we obtain an unreliability of 0.0121508 for this example.

**CONCLUSIONS AND FUTURE WORK**

We presented a separable approach to incorporate the effects of dependent CCF into the reliability analysis of general PMS consisting of both static and dynamic phases. The approach decomposes the original reliability problem into a number of reduced reliability problems according to Total Probability Theorem. The CCF effects are factored out through reduction. As compared with non-PMS, an expansion on the CCG is needed to include the non-maintainable effects; as compared with static PMS, a special treatment is needed to incorporate the dependent events of a FDEP gate into CCG when the trigger event of the FDEP gate is affected by some CC. Also, the separable approach enables the analysis of multiple CC that can affect multiple components from different phases, and which may be s-dependent. We illustrate the separable phase-modular approach by considering the reliability modeling and analysis of a PMS subject to three CC in three different phases and also show how the approach can be applied to analyze a space mission system.

Out next research tasks include the validation of the separable phase-modular approach, quantifying how effective it is by comparing it in complexity and results with other approaches to analyzing and modeling CCF.

**ACKNOWLEDGMENTS**

The research described in this paper was partially carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration. References herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not constitute or imply its endorsement by the United States Government or the Jet Propulsion Laboratory, California Institute of Technology.

## REFERENCES

- [HOYL94] Hoyland, A and Rausand, M, 1994, *System Reliability Theory: Models and Statistical Methods*, Wiley Series in Probability and Mathematical Statistics, John Wiley & Sons.
- [VAUR98] Vaurio, J. K., 1998, "An Implicit Method for Incorporating Common-Cause Failures in System Analysis," *IEEE Transactions on Reliability*, 47(2), pp. 173-180.
- [AMAR99] Amari, S. V., Dugan, J. B., and Misra, R. B., 1999, "Optimal Reliability of Systems Subject to Imperfect Fault-Coverage," *IEEE Transactions on Reliability*, 48(3) pp. 275-284.
- [DAI04] Dai, Y, Xie, M., Poh, K. L., and Ng, S. H., 2004, "A Model for Correlated Failures in N-Version Programming," *IIE Transactions*, 36 (12), pp. 1183-1192.
- [FLEM86] Fleming, K. N., Mosleh, N., and Deremer, R. K., 1986, "A Systematic Procedure for Incorporation of Common Cause Events into Risk and Reliability Models," *Nuclear Engineering and Design*, 93, pp.245-273.
- [PHAM93] Pham, H, 1993, "Optimal Cost-Effective Design of Triple-Modular-Redundancy-with-Spares Systems," *IEEE Transactions on Reliability*, 42(3), pp. 369-374.
- [TANG05] Tang, Z, Xu, H, and Dugan, J. B., 2005, "An integrated method for incorporating common cause failures in system analysis," *Proceedings of the 51st Annual Reliability and Maintainability Symposium*, Alexandria, VA.
- [VAUR03]Vaurio, J. K, 2003, "Common Cause Failure Probabilities in Standby Safety System Fault Tree Analysis with Testing - Scheme and Timing Dependencies," *Reliability Engineering & System Safety* 79 (1), pp. 43-57.
- [XING03] Xing, L, 2003, "Phased-Mission Reliability and Safety in the Presence of Common-Cause Failures," *Proceedings of The 21st International System Safety Conference*, Ottawa, Ontario, Canada.
- [XING05] Xing, L., Meshkat, L., and Donohue, D., "Reliability analysis of hierarchical computer-based systems subject to common-cause failures," *Reliability engineering and System Safety* (to appear)
- [DUGA01] Dugan, J. B., 2001, "Fault-tree analysis of computer-based systems," Tutorial Notes of the Annual Reliability and Maintainability Symposium, Philadelphia, Pennsylvania.
- [XING02] Xing, L. and Dugan, J. B., 2002, "Analysis of Generalized Phased-Mission System Reliability, Performance, and Sensitivity," *IEEE Transactions on Reliability*, 51(2), pp. 199-211.
- [ZANG99] Zang, X., Sun, H., and Trivedi, K. S., 1999, "A BDD-Based Algorithm for Reliability Analysis of Phased-Mission Systems," *IEEE Transactions on Reliability*, 48(1), pp. 50-60.
- [MESH00] Meshkat, L., 2000, "Dependency Modeling and Phase Analysis for Embedded Computer Based Systems," *Ph.D. thesis*, Department of Systems Engineering, University of Virginia, Charlottesville, VA.
- [MESH03] Meshkat, L., Xing, L., Donohue, D., and Ou, Y., 2003, "An Overview of the Phase-Modular Fault Tree Approach To Phased-Mission System Analysis," *Proceedings of The 1st International Conference on Space Mission Challenges for Information Technology (SMC-IT)*, Pasadena, CA, pp. 393-398; JPL Publication 03-13A, Jet Propulsion Laboratory, California Institute of Technology.
- [OU02] Ou, Y, 2002, "Dependability and Sensitivity Analysis of Multi-Phase Systems Using Markov Chains," *Ph.D. thesis*, Department of Electrical and Computer Engineering, University of Virginia, Charlottesville, VA.