Application of the Dynamic Flowgraph Methodology to the Space Propulsion System Benchmark Problem

Michael Yau[a*], Scott Dixon[a], and Sergio Guarro[a]
[a] ASCA, Inc., Redondo Beach, USA

Abstract: This paper discusses ASCA's experience in applying the Dynamic Flowgraph Methodology (DFM) to a space propulsion system problem specified by the Idaho National Laboratory (INL). This problem serves as a benchmark for comparing and evaluating the capabilities of advanced Probabilistic Risk Assessment (PRA) tools that are suitable for the risk analysis of future space systems.

Future space systems will likely be highly automated, with self-diagnosis and recovery capability. They will be also likely to have multiple configurations to respond to mission events and contingencies. As a result of these complex features, traditional integrated Event/Fault Tree analysis may not be best suited for accurately performing PRA in future space missions.

DFM is a general-purpose dynamic Multi-Valued Logic (MVL) modeling and analytical methodology supported by the Dymonda software tool. This tool and methodology can represent complex, time-dependent systems and processes, with inductive and deductive analysis capabilities that permit the systematic identification and quantification of success and failure events of interest. This benchmark study expands on the experiences of applying DFM in past projects, to include modeling and analysis of the system demand/time-based characteristics and redundancies, as well as the phased mission features of the benchmark problem.

Keywords: PRA, Dynamic Modeling and Analysis, Phased Mission Analysis, Dynamic Flowgraph Methodology

1. INTRODUCTION

Future space systems will likely be highly automated, with self-diagnosis and recovery capability. They will be also likely to have multiple configurations to respond to mission events and contingencies. As a result, the success criteria will change from mission phase to mission phase, depending on the orderly execution of sequential events.

Although Event/Fault Trees are well-established tools in the field of Probabilistic Risk Assessment (PRA), integrated Event/Fault Tree analysis is not best suited for accurately performing PRA in future space missions. Event/Fault Trees essentially constitute a binary logic tool that has limited capability for analyzing non-coherent structures or dynamic systems. For example, the inclusion of "NOT" or negated logic in order to define multiple degrading outcomes for a system will produce a model with a non-coherent structure. For such a structure, classical quantification by Boolean reduction, which is the staples of all Event/Fault Tree analysis software tools, produces inaccurate and inconsistent results.

To address the need for more advanced PRA tools that are suitable for the risk analysis of future space systems, Idaho National Laboratory has defined a benchmark case study to explore and evaluate their capabilities. This benchmark case study simulates a spacecraft ion-propulsion system to be used for a science mission to the outer Solar system. The propulsion system is composed of redundant hardware in a phased mission for which demand and time-based failure criteria are defined in the problem statement.

[*] Email: mike.yau@ascainc.com

This paper discusses ASCA's application of the Dynamic Flowgraph Methodology (DFM) to the benchmark case study. A general introduction to DFM is provided in Section 2, a brief overview of the features of the benchmark problem is presented in Section 3, and the application of DFM to the benchmark problem is discussed in Section 4.

2. DYNAMIC FLOWGRAPH METHODOLOGY

DFM is a general-purpose dynamic Multi-Valued Logic (MVL) modeling and analytical methodology supported by the Dymonda software tool. The DFM system modeling and analysis approach was initially developed in the 1990's [1, 2]. The approach is based on representing the system of interest in a "directed graph" model. This directed graph model also contains the explicit identification, in multi-valued-logic and discrete time-step approximation form, of the cause-and-effect and timing correspondences among the significant states of the parameters that are best suited to describe the system behavior. Once a DFM system model has been constructed with the model editor included in the Dymonda tool, automated deductive or inductive algorithms implemented into the tool analytical engine can be applied to analyze it. The deductive procedures can be used to identify how system states -- which may represent specific success or failure conditions of interest -- can be produced by combinations and time-sequences of basic component states. Conversely, inductive procedures can be applied to the same model to determine how a particular combination of basic component states which is assumed as an initial system condition can produce various possible timed-event sequences and subsequent system-level states. Thus, DFM can provide, in the deductive and inductive analysis modes respectively, a multi-state and time-dependent extension of both fault tree analysis (FTA) and failure modes and effects analysis (FMEA).

Besides its capability to track time-dependent causality in discrete states and time-steps, DFM also differs from FTA and FMEA in that a single DFM system model typically contains all the information necessary for a wide range of automated deductive or inductive analyses of interest to a user. In other words, once a DFM model has been constructed for a given system, multiple automated deductive analyses can be conducted to obtain the "cut-sets" for any user-defined system "top event" of interest. Each top event of interest can be expressed as a conjunction ("ANDED" combination) of system variable states and conditions, concerning both hardware and/or software variables and even involving variable states at different time frames ("time steps" in the DFM discrete time representation). Typical FTA terminology (e.g., "top-event" and "cut-sets") has been used here to take advantage of the conceptual analogy between a DFM automated deductive analysis and the process by which binary fault trees are manually constructed. However it is also appropriate to make clear that several substantial differences between the two processes exist. One difference is that in a typical FTA process a "top-event" is normally defined as a single event with or without a specific time frame of occurrence, not as a combination of events, each defined with its own possible separate time of occurrence. Perhaps more practically relevant is the fact that in normal FTA each system top event of concern requires the manual construction of a distinct fault-tree model before an analysis for the associated cut-sets can be executed by automated means, whereas an almost unlimited number of FTA-like deductive analyses can be automatically executed from a single DFM model, each for a separate and distinct "top-event". Corresponding differences exist between FMEA and the DFM inductive analysis process, since in performing a failure modes and effects analysis, one single initiating failure event is hypothesized and the specific threads of causality relationships producing resulting effects in the system have to be manually identified and tracked. In the DFM framework, on the other hand, once a system model has been developed, the analysis engine can produce without further reasoning inputs from the analyst a full array of separate automated inductive analyses, to show how some combination of initial component failures, hypothesized to occur even at separate times, may progress through the system. This inductive algorithm can also automatically handle cases in which the failure modes may branch into different areas of the system, with separate effects that recombine later in interactions further downstream in the flow of system cause and effect.

DFM deductive and inductive analysis techniques, implemented in the Dymonda software tool, have been applied to nuclear and process plant digital control systems assurance [1, 3], space systems flight

software safety analysis [4, 5], electronic device design verification and testing [6], human team reliability modeling [7], and several types of time-dependent system safety analyses [8, 9].

2.1. Implementation of DFM

DFM can be applied within a larger PRA framework, such as the Context-based Software Risk Model (CSRM) [10] for software risk-related scenarios of complex systems, or independently on its own for less complex systems. Typically, the application of DFM is a three-step process:

Step 1: Build a model of the system for which a safety analysis is required. The model encompasses both the controlling software and the system being controlled, and may also contain human and environmental factors.

Step 2: Using the model constructed in Step 1:

- Perform a deductive analysis to search for system and process failure states. These states may be the results of propagation through the system, of perturbations produced by basic "root cause" events. These root cause events can be system component faults or manifestations of process-control logic errors; and/or

- Perform an inductive analysis to generate the sequence of events that will result from a specific set of initial and boundary conditions.

Step 3: Integrate the results of the analysis in Step 2 into a larger PRA framework such as the CSRM as appropriate.

The reader should note while the construction of a DFM system model requires a certain level of system knowledge and effort, the DFM system model, once constructed, can be used for a wide range of analyses, e.g., to analyze many different top events and many different combinations of sub-system failures. Thus, because the same model can be used repeatedly to check many different system conditions/states of interest, the time and resource investment associated with the construction of a DFM model has a corresponding high return in terms of the system-analytical results, such as fault trees or event sequence diagrams, that the automated analysis engine can generate as needed and requested by the user. For critical systems that carry a high "cost of failure" and, accordingly, require extensive reliability and safety assurance analyses, the convenience and time gained in the execution of such wide range of analyses via DFM more than compensates for the initial effort that may be spent in building the model.

2.2. Applications Benefiting from DFM Analysis

The DFM methodology is compatible for use with all PRA and reliability methodology logic constructs. The binary-logic formalisms and structure functions of event tree (ET) models, fault tree (FT) models, event sequence diagrams (ESDs) and reliability block diagram (RBD) models are in logic modeling terms all subsets of the broader DFM multi-valued logic modeling constructs. Thus they have fully equivalent DFM representations if such a "translation" is desired, or, as may be the case when separate portions of reliability or PRA analysis are to be integrated, input and output interfaces to pass information back and forth between these models and DFM models can be easily defined and implemented. The results of a DFM analysis can thus be integrated easily into the result of a conventional PRA that primarily utilizes ET, ESD and FT models. This flexibility makes DFM appropriate for use in system models that combine a variety of PRA methods to meet modeling needs, such as the Context Based Software Risk Model recommended in the "Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners" [11]. Applying composite methods like the CSRM involves identifying which PRA tool is best suited to each part of a risk-scenario, using these tools, and integrating the results. Simple static and binary risk scenarios are usually modeled using classical ET/ESD/FT methods, while scenarios that involve complex system interactions and dynamic

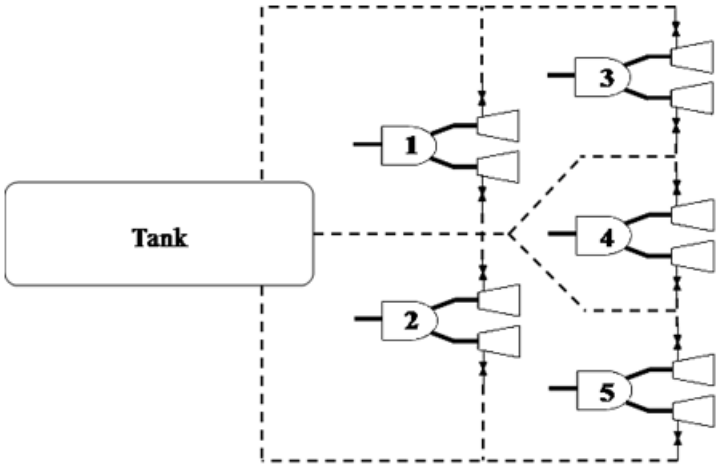
or time-dependant behavior may be modeled using a more advanced technique like DFM. Examples of scenarios that can be advantageously modeled with DFM are time-dependent failure and recovery scenarios, phased mission scenarios, and software risk-related scenarios [9].

This benchmark study expands on the experiences of applying DFM in past projects, to include modeling and analysis of the system demand/time-based characteristics and redundancies, as well as the phased mission risks of the case study. In the first step, a DFM model of the space propulsion system is constructed, capturing the key redundancy and common cause failure possibilities, as well as the time dependent system dynamic and failure characteristics specified in the benchmark system definition. New DFM features are being developed to address special features of this benchmark system, such as the stochastic cumulative damage of components. Once the model of the benchmark system is developed and verified, deductive and the inductive analyses will be carried out to identify and quantify the prime implicants that contribute to the failure of this system. The approaches to modeling and analyzing this system, as well as the results and the insights will be discussed in the conference paper.

3. DEFINITION OF THE BENCHMARK PROBLEM

The benchmark problem is based on an ion propulsion system that is needed for a science mission in order to reach the orbit of a distant planet. The system is depicted in Figure 1 and consists of a propellant tank, a set of propellant distribution lines (dashed lines in Figure 1), and 5 ion propulsion thrusters. Each ion propulsion thruster is in turn composed of a Propulsion Power Unit (PPU), 2 ion engines (in a primary and backup configuration), and 2 associated propellant valves.

Figure 1: Schematic of the Ion Propulsion System



The mission is divided into alternating propulsion and coast phases. Different number of thrusters is needed to provide thrust for the various propulsion phases. Whereas, the thrusters are turned off in the coast phases. A summary of the phased-mission configuration is shown in Figure 2.

Failure modes (independent and common cause) as well as their associated probabilities, are specified for the components of the ion propulsion system. The objective is to estimate qualitatively and quantitatively the mission failure event, where an insufficient number of thrusters is available to propel the spacecraft.

Figure 2: Summary of the Phased-Mission Configuration

4. DFM APPLICATION TO THE BENCHMARK PROBLEM

The first step in constructing a dynamic DFM model is to select the duration for a time step. From the phased-mission definition in Figure 2, the duration of each mission phase was calculated, and the greatest common divisor among these phase durations was determined to be 200 hours. With 200 hours as the length of each time step, phase 1 lasts 14 time steps, phase 2 lasts 12 time steps, and so on. This results in a total of 390 time steps for the entire mission. Performing a dynamic analysis for 390 time steps would be beyond the scope of this benchmark study. Instead, approximations were made regarding the end time of the first mission phase and the end time of the second mission phase. The first mission phase was assumed to end at 3000 hours instead of 2800 hours, and the second mission phase was assumed to end at 5000 hours instead of 5200 hours. With these assumptions, a time step duration of 1000 hours can be used. This results in the revised mission phase durations shown in Table 1. Using this revised phase durations, the estimate for the mission failure probability would be slightly conservative, as the propulsion phases 1 and 3 are slightly longer, and the coast phase 2 is slightly shorter than the original specification.

Table 1: Revised Phased-Mission Durations Summary

Phase	Start	End	Duration	# Thrusters	# Steps
1	0	3000	3000	2	3
2	3000	5000	2000	0	2
3	5000	12000	7000	3	7
4	12000	21000	9000	0	9
5	21000	28000	7000	3	7
6	28000	38000	10000	0	10
7	38000	50000	12000	3	12
8	50000	69000	19000	0	19
9	69000	78000	9000	2	9
					78

4.1. DFM Modeling of the Space Propulsion System

After the selection of the duration for a time step, the development of the DFM commenced. Given the system redundancy and the mission phase characteristics, it was natural to adopt a modularization procedure to develop the DFM model. At the top level is a model (Figure 3) that characterizes the progression of the mission phases and the success/failure criteria of the 5 ion thrusters in the various mission phases. In Figure 3, the progression of the mission phases is modeled with the DFM elements highlighted in blue. The success of each mission phase depends on the status of the propellant distribution lines as well as the availability of sufficient thrusters.

The health of the propellant distribution lines was modeled with the dynamic construct shown in red on the right hand side of Figure 3. The node "P-Line", representing the status of the propellant distribution lines, was discretized into 2 states to represent the normal state and the leakage state. The node "PLine-T" was used to model the possible transitions between the normal and leakage state of the node "P-Line". As repair of the propellant distribution lines was not allowed in the problem

specification, "PLine-T" was discretized into 3 states; OK:OK, OK:Leak, and Leak:Leak. The "OK:OK" state represents the propellant distribution lines being normal before and remain normal, whereas the "OK:Leak" state signifies the propellant distribution lines were normal before but begin leaking in the current time step. The transition box that connects the nodes "P-Line" and "PLine-T" has "P-Line" as both input and output, and "PLine-T" as input. This shows that the current status of the propellant distribution lines depends on the previous status of the distribution lines and whether any leakage starts to occur. The dynamic behavior of the leakage of the propellant lines is embedded in the decision table for this transition box. This decision table has 3 rows and is shown in Table 2.

Figure 3: Top Level DFM Model of the Ion Propulsion System

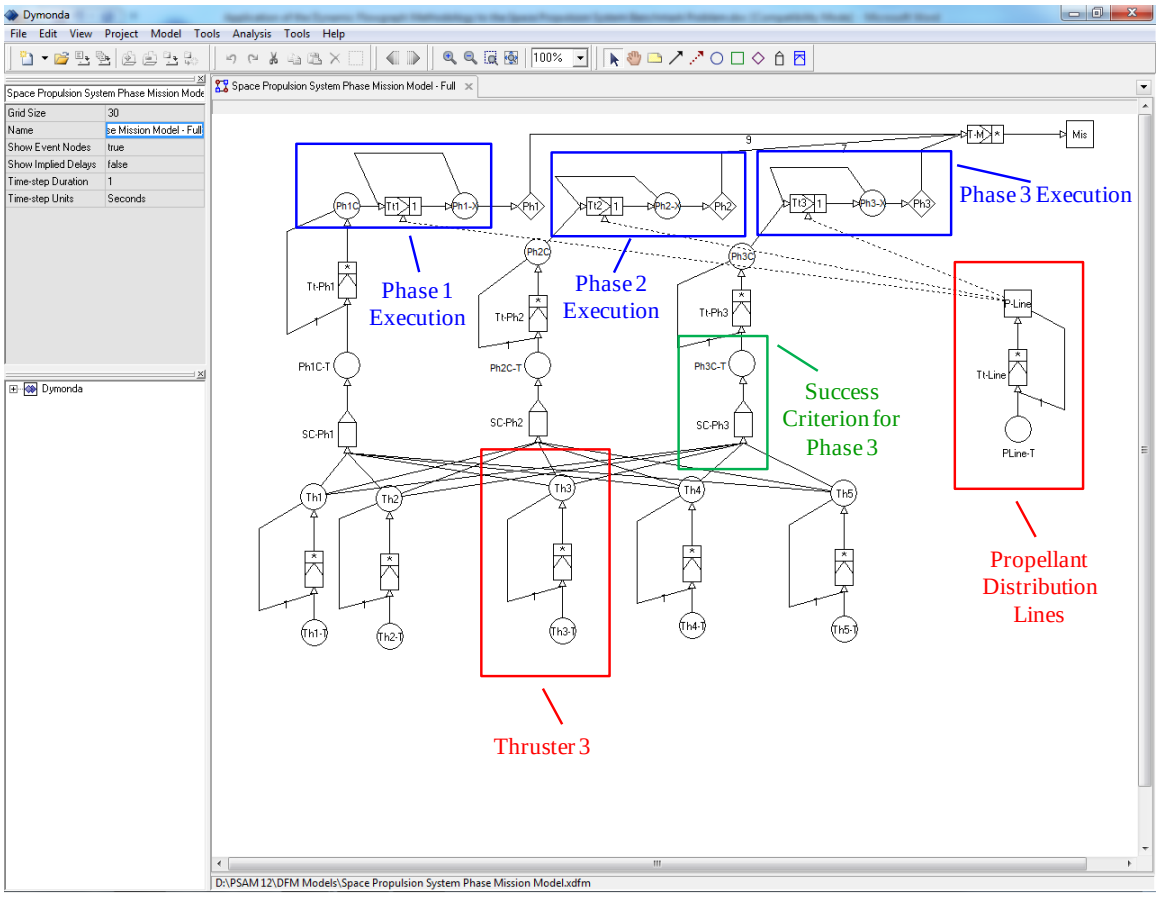


Table 2: Decision Table that Captures the Dynamic Behavior of the Propellant Lines

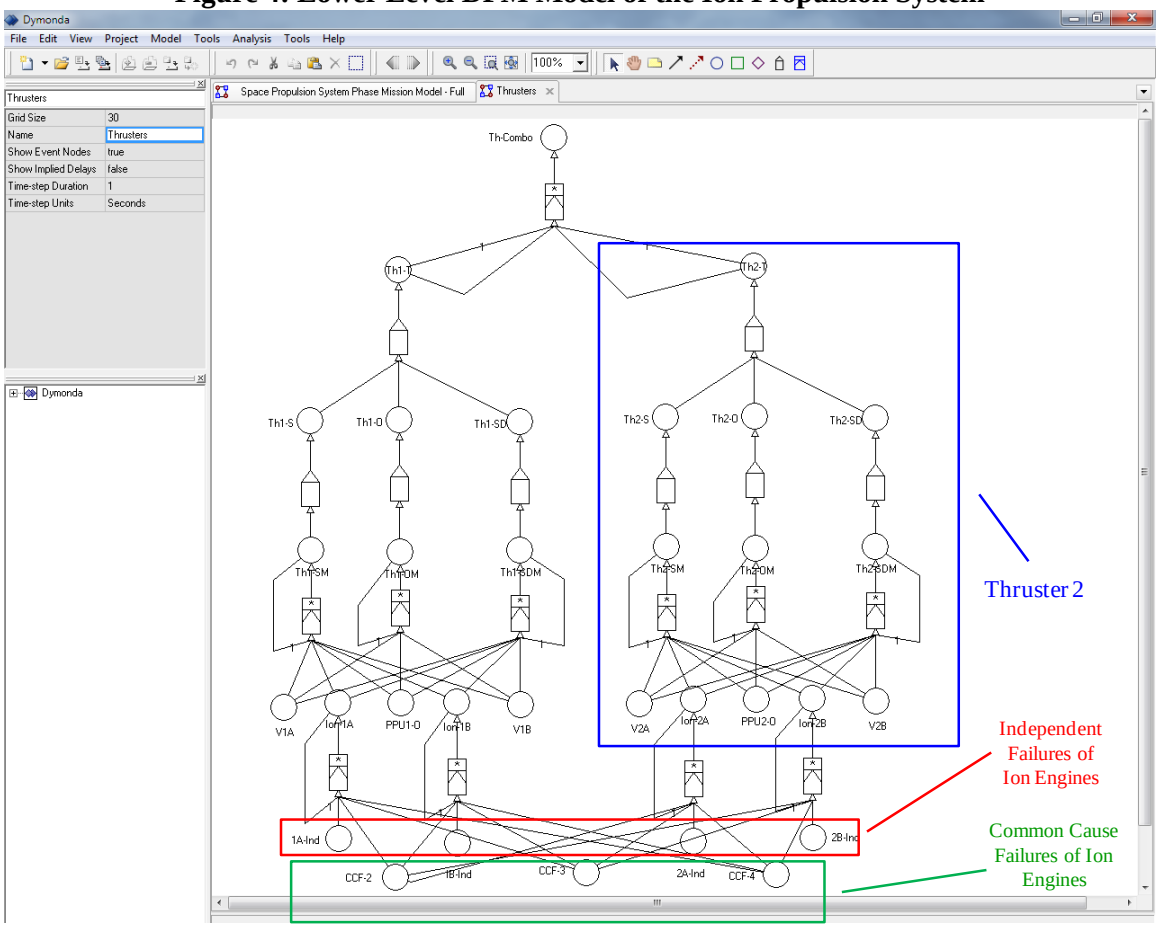
P-Line (@ t = -1)	PLine-T (@ t = -1)	**P-Line (@ t = 0)**
Normal	OK:OK	**Normal**
Normal	OK:Leak	**Leak**
Leak	Leak:Leak	**Leak**

Besides the status of the propellant distribution lines, the success of each mission phase depends on the availability of the thrusters as well. In particular, Phase 3 requires 3 thrusters. This thruster criterion for phase 3 is captured in the DFM model with the parts shown in green in Figure 3. The decision table for the box with the label "SC-Ph3" details the logic for satisfying the success criterion for Phase 3. This logic is slightly different from a standard 3-out-of-5 logic, as the thrusters are assumed to activate in series in the problem specification. In particular, thruster #4 will not be activated unless one of the first three thrusters suffers a failure, either in Phase 3 or previously in Phase 1. Each of the 5 thrusters was modeled with a time transition similar to the propellant distribution lines discussed above. However, due to the multiple failure modes of each thruster (failure to start on demand, failure to operate, and failure to shutdown on demand), more states were

used for the corresponding variables, resulting in decision tables with higher number of rows. The reader should note that by capturing the dynamic behaviors of the thrusters, the failure history of these thrusters is retained within the model. This representation allows the analysis to identify correctly that the success/failure of a mission phase not only depends on the thruster events in the current phase, but thruster events in earlier mission phases as well. This will be revisited in the discussion of the preliminary analyses in Section 4.2.

The detailed components that make up the thrusters, as well as the redundancy management between these components were expanded in a lower level DFM model. A portion of this model, showing thrust #1 and thruster #2 is presented in Figure 4. The portion corresponding to thruster #2 is highlighted in blue in Figure 4. The three different vertical branches correspond to the three failure modes of a thruster; failure to start, failure to operate and failure to shutdown. These three failure modes are caused by the failure modes of the thruster components, which are the Propulsion Power Unit, the two ion engines, and the two propellant valves. For instance, the failure of the ion engines can be caused by independent failure modes of the engines (highlighted in red in Figure 4) or by common cause failure modes of the engines (groups of 2 up to group of 4, highlighted in green in Figure 4). In summary, the detailed model in Figure 4 shows how the redundancy between ion engine 2A and ion engine 2B, as well as the switching function of the PPU affect the operation of thruster #2 during a propulsion phase.

Figure 4: Lower Level DFM Model of the Ion Propulsion System



4.2. Preliminary DFM Analysis of the Space Propulsion System

After the construction of the top level and lower level DFM models for the space propulsion system, a few preliminary analyses were carried out to validate the accuracy of these models. In these preliminary analyses, portions of the DFM models were turned off to help the debugging process. In one particular analysis, thruster #1 was assumed to work all the time and thrusters #4 and #5 were

deactivated. As a result of this simplifying assumption, the success criterion for Phase 1 becomes 1-out-of-2 and the success criterion for Phase 3 becomes 2-out-of-2. For the validation of the top level DFM model, this preliminary deductive analysis was carried out to investigate the failure of the mission before the thrusters are turned off for the coast in Phase 4. The "Top Event" was defined as a conjunction of DFM variables as follows:

Mis = F @ 0	(Mission Failure at time 0)	AND
Ph3-X = Start @ -7	(Phase 3 starts at time -7)	AND
Ph3C = InAct @ -8	(Phase 3 inactive before time -7)	AND
Ph2-X = Start @ -9	(Phase 2 starts at time -9)	AND
Ph2C = InAct @ -10	(Phase 2 inactive before time -9)	AND
Ph1-X = Start @ -12	(Phase 1 starts at time -12)	AND
Ph1C = InAct @ -13	(Phase inactive before time -12)	AND
P-Line = Normal @ -13	(Propellant lines were normal at the start of the mission)	AND
Th2 = OK @ -13	(Thruster #2 was normal at the start of the mission)	AND
Th3 = OK @ -13	(Thruster #3 was normal at the start of the mission)	

This DFM top event consists of the undesirable outcome (the first term), the boundary conditions for the mission commands (the next six terms), and the boundary conditions for the initial component states (the last three terms). The preliminary deductive analysis was carried out for 12 time steps, backtracking from the end of Phase 3 to the beginning of Phase 1. 398 implicants were identified. Implicants are the multi-valued logic equivalent of binary cut-sets. These implicants characterized the combinations of leak in the propellant distribution lines and failures of thrusters #2 and #3 at different time steps. A subset of these implicants (#270 to #299) is shown in Table 3.

In these 30 implicants, the propellant distribution lines were normal. The mission failure was caused by combinations of thruster #2 and thruster #3 at different time steps. For example, implicant #272 shows thruster #2 failed to operate @-12 (right after Phase 1 start) and thruster #3 failed to start @-7 (beginning of Phase 3). After the failure of thruster #2, thrust #3 was activated in Phase 1 and shut down in Phase 2. When thruster #3 failed to start again for Phase 3, the mission failed due to an insufficient number of thrusters.

Table 3: Subset of Implicants for Validation Analysis of Top Level DFM Model

#	PLine-T (-1)	Th2-T (-12)	Th2-T (-11)	Th3-T (-9)	Th3-T (-8)	Th3-T (-7)	Th3-T (-6)	Th3-T (-5)	Th3-T (-4)	Th3-T (-3)	Th3-T (-2)	Th3-T (-1)
270	OK:OK	OK:FtO	FtO:FtO	OK:FtSD	FtSD:FtSD	FtSD:FtSD	FtSD:FtSD	FtSD:FtSD	FtSD:FtSD	FtSD:FtSD	FtSD:FtSD	FtSD:FtSD
271	OK:OK	OK:FtO	FtO:FtO	OK:OK	OK:OK	OK:FtO	FtO:FtO	FtO:FtO	FtO:FtO	FtO:FtO	FtO:FtO	FtO:FtO
272	OK:OK	OK:FtO	FtO:FtO	OK:OK	OK:OK	OK:FtS	FtS:FtS	FtS:FtS	FtS:FtS	FtS:FtS	FtS:FtS	FtS:FtS
273	OK:OK	OK:FtO	FtO:FtO	OK:OK	OK:OK	OK:OK	OK:FtO	FtO:FtO	FtO:FtO	FtO:FtO	FtO:FtO	FtO:FtO
274	OK:OK	OK:FtO	FtO:FtO	OK:OK	OK:OK	OK:OK	OK:OK	OK:FtO	FtO:FtO	FtO:FtO	FtO:FtO	FtO:FtO
275	OK:OK	OK:FtO	FtO:FtO	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:FtO	FtO:FtO	FtO:FtO	FtO:FtO
276	OK:OK	OK:FtO	FtO:FtO	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:FtO	FtO:FtO	FtO:FtO
277	OK:OK	OK:FtO	FtO:FtO	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:FtO	FtO:FtO
278	OK:OK	OK:FtO	FtO:FtO	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:FtO
279	OK:OK	OK:FtO	FtO:FtO	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK
280	OK:OK	OK:FtS	FtS:FtS	OK:FtSD	FtSD:FtSD	FtSD:FtSD	FtSD:FtSD	FtSD:FtSD	FtSD:FtSD	FtSD:FtSD	FtSD:FtSD	FtSD:FtSD
281	OK:OK	OK:FtS	FtS:FtS	OK:OK	OK:OK	OK:FtO	FtO:FtO	FtO:FtO	FtO:FtO	FtO:FtO	FtO:FtO	FtO:FtO
282	OK:OK	OK:FtS	FtS:FtS	OK:OK	OK:OK	OK:FtS	FtS:FtS	FtS:FtS	FtS:FtS	FtS:FtS	FtS:FtS	FtS:FtS
283	OK:OK	OK:FtS	FtS:FtS	OK:OK	OK:OK	OK:OK	OK:FtO	FtO:FtO	FtO:FtO	FtO:FtO	FtO:FtO	FtO:FtO
284	OK:OK	OK:FtS	FtS:FtS	OK:OK	OK:OK	OK:OK	OK:OK	OK:FtO	FtO:FtO	FtO:FtO	FtO:FtO	FtO:FtO
285	OK:OK	OK:FtS	FtS:FtS	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:FtO	FtO:FtO	FtO:FtO	FtO:FtO
286	OK:OK	OK:FtS	FtS:FtS	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:FtO	FtO:FtO	FtO:FtO
287	OK:OK	OK:FtS	FtS:FtS	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:FtO	FtO:FtO
288	OK:OK	OK:FtS	FtS:FtS	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:FtO
289	OK:OK	OK:FtS	FtS:FtS	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK
290	OK:OK	OK:OK	OK:FtO	OK:FtSD	FtSD:FtSD	FtSD:FtSD	FtSD:FtSD	FtSD:FtSD	FtSD:FtSD	FtSD:FtSD	FtSD:FtSD	FtSD:FtSD
291	OK:OK	OK:OK	OK:FtO	OK:OK	OK:OK	OK:FtO	FtO:FtO	FtO:FtO	FtO:FtO	FtO:FtO	FtO:FtO	FtO:FtO
292	OK:OK	OK:OK	OK:FtO	OK:OK	OK:OK	OK:FtS	FtS:FtS	FtS:FtS	FtS:FtS	FtS:FtS	FtS:FtS	FtS:FtS
293	OK:OK	OK:OK	OK:FtO	OK:OK	OK:OK	OK:OK	OK:FtO	FtO:FtO	FtO:FtO	FtO:FtO	FtO:FtO	FtO:FtO
294	OK:OK	OK:OK	OK:FtO	OK:OK	OK:OK	OK:OK	OK:OK	OK:FtO	FtO:FtO	FtO:FtO	FtO:FtO	FtO:FtO
295	OK:OK	OK:OK	OK:FtO	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:FtO	FtO:FtO	FtO:FtO	FtO:FtO
296	OK:OK	OK:OK	OK:FtO	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:FtO	FtO:FtO	FtO:FtO
297	OK:OK	OK:OK	OK:FtO	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:FtO	FtO:FtO
298	OK:OK	OK:OK	OK:FtO	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:FtO
299	OK:OK	OK:OK	OK:FtO	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK	OK:OK

As discussed earlier in Section 4.1, capturing the dynamic failure history of the thrusters allows the analysis to identify correctly that the success/failure of a mission phase depends on the thruster events in the current phase as well as thruster events in earlier phases. This is shown in implicants #279, #289, and #299 in Table 3. For instance, implicant #299 corresponds to the failure of thruster #2 to operate @-11 (1 time step into Phase 1) and no failure for thruster #3. Although the mission does not fail during Phase 1, as the success criterion is 1-out-of-2, the mission will fail later at the beginning of Phase 3, as both thrusters are required. If this dependence is not properly captured, the final mission risk will be underestimated.

For the validation of the lower level DFM model, preliminary deductive analyses were carried out to validate the proper qualitative and quantitative modeling of failure of components across thrusters. For example, one particular deductive analysis investigated the failure of common primary ion engines across thruster #1 and thruster #2. The "Top Event" for this lower level DFM model analysis was defined as a conjunction of DFM variables as follows:

Ion-1A = F @ 0	(Primary ion engine for thruster #1 failed at the end of Phase 1)	AND
Ion-2A = F @ 0	(Primary ion engine for thruster #2 failed at the end of Phase 1)	AND
Ion-1A = OK @ -3	(Primary ion engine for thruster #1 was normal at mission start)	AND
Ion-2A = OK @ -3	(Primary ion engine for thruster #2 was normal at mission start)	

Similar to the top event for the top level model, this DFM top event consists of the undesirable outcome (the first two term), and the boundary conditions for the initial component states (the last two terms). The preliminary deductive analysis was carried out for 3 time steps, backtracking from the end of Phase 1 to the beginning of Phase 1. 12 implicants were identified. The implicants #1 through #9 express the independent failure of the 2 ion engines in different combination of time steps in Phase 1, and implicants #10 through #12 show common cause failure of the 2 ion engines in each of the three time steps in Phase 1.

Table 4: Implicants for Validation Analysis of Lower Level DFM Model

#	1A-Ind (-2)	1A-Ind (-1)	1A-Ind (0)	2A-Ind (-2)	2A-Ind (-1)	2A-Ind (0)	CCF-2 (-2)	CCF-2 (-1)	CCF-2 (0)	Prob.
1	W:F	F:F	F:F	W:F	F:F	F:F	W:W	W:W	W:W	**3.90E-04**
2	W:F	F:F	F:F	W:W	W:F	F:F	W:W	W:W	W:W	**3.82E-04**
3	W:F	F:F	F:F	W:W	W:W	W:F	W:W	W:W	W:W	**3.75E-04**
4	W:W	W:F	F:F	W:F	F:F	F:F	W:W	W:W	W:W	**3.82E-04**
5	W:W	W:F	F:F	W:W	W:F	F:F	W:W	W:W	W:W	**3.75E-04**
6	W:W	W:F	F:F	W:W	W:W	W:F	W:W	W:W	W:W	**3.67E-04**
7	W:W	W:W	W:F	W:F	F:F	F:F	W:W	W:W	W:W	**3.75E-04**
8	W:W	W:W	W:F	W:W	W:F	F:F	W:W	W:W	W:W	**3.67E-04**
9	W:W	W:W	W:F	W:W	W:W	W:F	W:W	W:W	W:W	**3.60E-04**
10	W:W	W:W	W:W	W:W	W:W	W:W	W:F	F:F	F:F	**1.42E-03**
11	W:W	W:W	W:W	W:W	W:W	W:W	W:W	W:F	F:F	**1.42E-03**
12	W:W	W:W	W:W	W:W	W:W	W:W	W:W	W:W	W:F	**1.41E-03**
										7.62E-03

As the independent and common cause failure rates for the ion engine failure to operate failure mode was specified (2×10^{-5} per hour and 1.6×10^{-6} per hour respectively), the implicants themselves can be quantified. For example, implicant #3 consists of ion engine 1A failing in the first 1000 hours and ion engine 2A failing in the third 1000 hours. The exact probability for this implicant is:

$$P_3 = P(\text{1A failing, t = 0 to 1000}) \times P(\text{2A working, t = 0 to 2000}) \times P(\text{2A failing, t = 2000 to 3000})$$

$$P_3 = [1 - \exp(2 \times 10^{-5} \times 1000)] \times \exp(2.16 \times 10^{-5} \times 2000) \times [1 - \exp(2 \times 10^{-5} \times 1000)]$$

$$P_3 = 3.76 \times 10^{-4}$$

The estimated probability for implicant #3 was 3.75×10^{-4} (Table 4), which is close to the exact value. The difference is likely due to the discretization of continuous time into discrete time steps.

5. ONGOING WORK

More validation analyses of the DFM models are being carried out, with all model features activated, to check the accuracy of the key characteristics of these models. Once the validation analyses demonstrate that the models are reasonably accurate, the top level and the lower level DFM models will be solved in sequence to obtain the final results. The top level results will provide the implicants in terms of the thrusters and the propellant distribution lines. These thruster combinations will then be partitioned into subsets and solved with the lower level model qualitatively and quantitatively. The reason for partitioning is to preempt the onset of combinatorial explosion.

6. CONCLUSION

Future space systems will likely be highly automated, with self-diagnosis and recovery capability. They will be also likely to have multiple configurations to respond to mission events and contingencies. As a result, the success criteria will change from mission phase to mission phase, depending on the orderly execution of sequential events. It is well understood that traditional PRA tools are not best suited for accurately modeling and analyzing these complex features.

To address the need for more advanced PRA tools that are suitable for the risk analysis of future space systems, Idaho National Laboratory has defined a benchmark case study to explore and evaluate their capabilities. This benchmark case study simulates a spacecraft ion-propulsion system to be used for a science mission to the outer Solar system. The propulsion system is composed of redundant hardware in a phased mission for which demand and time-based failure criteria are defined in the problem statement.

This paper discusses ASCA's application of the Dynamic Flowgraph Methodology (DFM) to the benchmark case study. First, the duration for a time step in the DFM model was selected. In order to select a time step duration that keeps the modeling and analysis activities within practical scope, the duration of some of the mission phases were approximated close to their original values. After the selection of the duration for a time step, the model of the space propulsion system was constructed. This model was developed as a hierarchy of models at two levels. The top level model characterized the progression of the mission phases and the success/failure criteria of the 5 ion thrusters in the various mission phases. The lower level model captured the detailed interaction of the components that make up the thrusters. In this DFM model hierarchy, the dynamic behaviors and the failure history of the components are captured within the model. This representation properly characterized the fact that the success/failure of a mission phase not only depends on the events that happen in the current phase, but events that happened in earlier mission phases as well.

After the construction of the top level and lower level DFM models for the space propulsion system, a few preliminary analyses were carried out to validate the accuracy of these models. In these preliminary analyses, portions of the DFM models were turned off to help the debugging process. Preliminary analyses of the top level DFM model demonstrated that dependence on prior failures was properly modelled and identified. Preliminary analyses of the lower level DFM model showed that the independent and common cause failure modes of components were correctly represented and quantified.

Work is ongoing to complete the validation analyses. Once this activity is completed, the top level and the lower level DFM models will be solved in sequence to obtain the final qualitative and quantitative results.

References

[1] S. Guarro, M. Yau and M. Motamed, "Development of Tools for Safety Analysis of Control Software in Advanced Reactors," NUREG/CR-6465, U.S. Nuclear Regulatory Commission, April 1996, Washington, DC.

[2] M. Yau and S. Guarro, "Dynamic Flowgraph Methodology (DFM) for Safety Analysis of Critical Control Software," in 3rd International Conference on Probabilistic Safety Assessment and Management (PSAM-3), June 24-28, 1996, Crete, Greece.

[3] T. Aldemir, S. Guarro, J. Kirschenbaum, D. Mandelli, L. Mangan, P. Bucci, M. Yau, B. Johnson, C. Elks, E. Ekici, M. Stovsky, D. Miller, X. Sun, S. Arndt, Q. Nguyen and J. Dion, "A Benchmark Implementation of Two Dynamic Methodologies for the Reliability Modeling of Digital Instrumentation and Control Systems," NUREG/CR-6985, U.S. Nuclear Regulatory Commission, February 2009, Washington, DC.

[4] M. Yau, S. Guarro and G. Apostolakis, "Demonstration of the Dynamic Flowgraph Methodology using the Titan II Space Launch Vehicle Digital Flight Control System," Reliability Engineering and System Safety, vol. 49, pp. 335-353, (1995).

[5] M. Yau and S. Guarro, "Application of Context-based Software Risk Model (CSRM) to Assess Software Risk Contribution in Constellation Project PRAs," in 10th International Conference on Probabilistic Safety Assessment and Management (PSAM 10), June 7-11, 2010, Seattle, Washington.

[6] M. Houtermans, G. Apostolakis, A. Brombacher and D. Karydas, "Programmable Electronic System Design & Verification Utilizing DFM," in Computer Safety, Reliability and Security, October 24-27, 2000, Rotterdam, The Netherlands.

[7] A. Milici, R. Mulvihill and S. Guarro, "Extending the Dynamic Flowgraph Methodology (DFM) to Model Human Performance and Team Effects," NUREG/CR-6710, U.S. Nuclear Regulatory Commission, March 2001, Washington, DC.

[8] S. Dixon, M. Yau and S. Guarro, "Extension of CAFTA with Dymonda Module to Analyze Dynamic Accident Scenarios," in International Topical Meeting on Probabilistic Safety Assessment and Analysis (PSA 2011), March 13-17, 2011, Wilmington, North Carolina.

[9] S. Guarro, M. Yau and S. Dixon, "Application of the Dynamic Flowgraph Methodology (DFM) to Dynamic Modeling and Analysis," in 11th International Conference on Probabilistic Safety Assessment and Management (PSAM-11), June 25-29, 2012, Helsinki, Finland.

[10] National Aeronautics and Space Administration, "Context-Based Software Risk Model (CSRM) Application Guide," NASA/CR-2013-218111, NASA Headquarters, October 2013, Washington, DC.

[11] National Aeronautics and Space Administration, "Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, Second Edition," NASA/SP-2011-3421, NASA Headquarters, December 2011, Washington, DC.