

Simulation-based Design and Validation of Automated Contingency Management for Propulsion Systems

Liang Tang[†], Abhinav Saxena[‡], Marcos E. Orchard^{*†}, Gregory J. Kacprzynski[†],
George Vachtsevanos[‡], and Ann Patterson-Hine^{*}

[†]Impact Technologies, LLC, 200 Canal View Blvd., Rochester, NY 14623.
Email: Greg.Kacprzynski@impact-tek.com^{1,2}

[‡]School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA. 30332

^{*}Department of Electrical Engineering, University of Chile, Santiago, Chile.

^{*}NASA Ames Research Center, MS 269-4, Moffett Field, CA. 94035-1000

Abstract— Automated Contingency Management (ACM), or the ability to confidently and autonomously adapt to fault and/or contingency conditions with the goal of still achieving mission objectives, can be considered the ultimate technological goal of a health management system. To establish confidence on the ACM system, objective performance evaluations should be executed. The need for verification and validation (V&V) techniques for ACM has also been specifically identified by DOD agencies and within the NASA community recently. This paper presents a general process and related techniques for developing and validating ACM systems for advanced propulsion systems. A novel ACM modeling paradigm, optimization-based ACM strategies, V&V approaches and performance metrics are developed. While some well-established formal methods such as model checking techniques are applicable to some sub-problems, this research has been more focused on innovative informal methods that attempt to address ACM performance requirements, optimality, robustness, etc. A pressure fed, monopropellant propulsion system for a small space flight vehicle is utilized as initial proof-of-concept implementation for the proposed techniques and preliminary simulation results are presented.

TABLE OF CONTENTS

NOMENCLATURE.....	1
1. INTRODUCTION.....	1
2. ACM V&V OVERVIEW.....	2
3. OPTIMIZATION-BASED ACM DESIGN & ACM MODELING	4
4. SIMULATION-BASED V&V OF ACM SYSTEM.....	5
5. A CASE STUDY: MONOPROPELLANT PROPULSION SYSTEM.....	6
6. CONCLUSION AND FUTURE WORK	9
ACKNOWLEDGEMENT	9
REFERENCES	10
BIOGRAPHY	10

NOMENCLATURE

ACM:	Automated Contingency Management
COTS:	Commercial Off-the-Shelf
FMECA:	Failure Modes Effect and Criticality Analysis
FSM:	Finite State Machine
HITL:	Hardware-in-the-loop
PACM:	Propulsion ACM
PHM:	Prognostics and Health Management
V&V:	Verification & Validation

1. INTRODUCTION

Stimulated by the growing demand for improving the reliability and survivability of safety-critical aerospace systems, a variety of health management (HM) and fault-tolerant control techniques have been developed. These techniques are capable of detecting the occurrence of faults while still retaining acceptable performance in the presence of faults. In recent years, numerous propulsion health monitoring technologies have been developed by NASA and DoD to aid in the detection and classification of developing propulsion faults for various military and space propulsion applications [1]-[3]. These technologies have focused on the detection and diagnosis of insipient propulsion and instrumentation faults. Emerging technologies such as intelligent life extending control, combustion instability control, emission minimizing control, pattern factor control, and active control of both rotating stall and surge in a high speed compressor stage, have resulted in performance improvements for aero propulsion [4]. The concept of using health monitoring in conjunction with reconfigurable control has been introduced through different techniques and at varying levels of sophistication [5].

An Automated Contingency Management (ACM) system provides a framework, and flexible architecture, to

¹ 1-4244-0525-4/07/\$20.00 ©2007 IEEE.

² IEEEAC paper #1398, Version 1, Updated Oct, 11, 2006

accommodate aforementioned technologies, and leads to the design of high confidence propulsion systems with robust fault accommodation procedures and adaptive engine operation reconfiguration. In order for ACM systems to be used in safety-critical aerospace applications, they must be proven to be highly safe and reliable. Rigorous methods for ACM system verification and validation must be developed to ensure that ACM system software failures will not occur, to ensure the system functions as required, to eliminate unintended functionality, and to demonstrate that certification requirements can be satisfied.

According to results from the recent Validation & Verification of Intelligent and Adaptive Control Systems (VVIACS) Program, design-time testing already consumes over 1/4 (27%) of the total system development costs. According to the VVIACS study, without new technologies, V&V costs may increase to 67% of total development costs for emerging flight control systems.[6] Because of the high cost of V&V, lack of effective V&V strategies, and the difficulty of achieving high levels of confidence in the safety of many advanced ACM approaches (especially with nondeterministic intelligent and/or adaptive controllers), there is a significant gap between state-of-the-art ACM concepts and fielded systems.

The compelling need for verification and validation techniques for complex systems like the ACM system, PHM system or specifically for intelligent and adaptive controllers has in the recent years boosted research in this area. The Automated Software Engineering Group at NASA Ames has developed a comprehensive integrated portfolio of V&V techniques and tools for ISHM systems including Model Checking [7], Compositional Verification, Static Analysis [8], Runtime Monitoring [9], and Program Synthesis. The development of Advanced V&V procedures and tools for the certification of learning systems in aerospace applications were addressed in [10]. These technologies include the application of automated program analysis methods, analytical methods to verify stability, and tools to provide on-line software assurance. Run-time V&V approaches, neural networks performance evaluation, and statistical V&V methods have been developed for guidance and control of advanced autonomous system [11], adaptive aircraft controllers [12], and non-linear real-time UAV controllers [13]. Approaches that highlight comprehensive system development, operational perspective, and sound system engineering principles were presented in [14]. In a closely related area, PHM system V&V was addressed in [15] where methodologies and performance metrics for verifying and validating the capability of PHM system were developed. All these research work has suggested promising approaches to address the V&V of ACM system or subsystems. However, due to the size and complexity of ACM system, the V&V of ACM system still remains a challenging task.

The challenge associated with V&V of ACM system has led us to tackle the problem from two angles: on one side, propose an ACM design methodology that builds the ACM systems on techniques that can be verified and validated by existing and emerging V&V approaches; on the other side, research innovative V&V techniques to address the issues that existing methods fail to address.

The technical scope of this study is the V&V-aware design and validation of ACM systems with an emphasis on propulsion systems. The effort focused on simulation based V&V due to its significance to overall cost reduction. Our objective is to study, develop, and demonstrate V&V-aware ACM design methodology, effective V&V approaches and performance metrics for ACM system in the design phase to help make the design as robust and accurate as possible. Specific technical objectives include:

- Propose a V&V-aware ACM design methodology intended to help overcome the V&V barriers;
- Develop and demonstrate preliminary simulation-based V&V approaches;
- Identify critical V&V process, tool, and techniques for further development.

These technical objectives address relevant technical challenges that, if solved, will potentially result in significantly reduced V&V and certification costs.

The organization of this paper is as follows, Section 2 provides an overview of ACM system and the proposed V&V process. Section 3 presents an optimization-based ACM design methodology and a finite state machine based ACM modeling paradigm. In Section 4, simulation-based V&V approaches are described in details. A pressure-fed monopropellant propulsion system for a small space flight vehicle is utilized as initial proof-of-concept implementation for the proposed techniques and simulation results are presented in Section 5. The paper concludes with remarks on the technical challenges and future developments.

2. ACM V&V OVERVIEW

Conceptually, ACM refers to a system that is designed to provide the ability to confidently and autonomously adapt to fault and/or contingency conditions with the goal of still achieving mission objectives. A typical ACM implementation usually utilizes a hierarchical architecture that covers low level redundancy management, mid level fault accommodation strategies, and higher level adaptive mission re-planning modules. Figure 1 shows the high level conceptual schematics of the interaction of PHM system and ACM system.

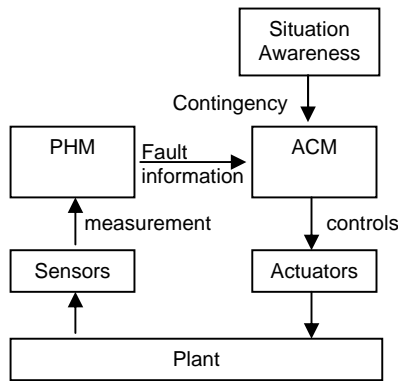


Figure 1 : PHM & ACM Systems

The PHM and situation awareness modules provide fault diagnostics and contingency information to the ACM system, which in turn, figures out and execute the optimal contingency mitigation strategies. Worth pointing out is that the potential for any of the contingency strategies to be successful is dependant on the system status as illustrated in Figure 2. The ACM system is only applicable in the yellow region.

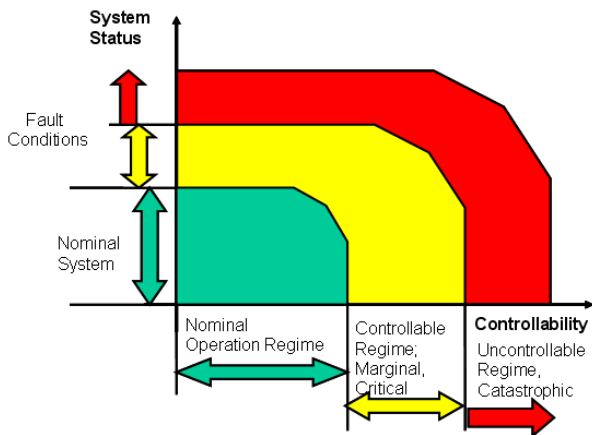


Figure 2 : Regime of interest for ACM

Real world implementations of ACM systems for aircraft, spacecraft or, on a smaller scale, for their propulsion systems have been based on a variety of problem specific solutions. However, the ACM concept and a lot of basic techniques applied in various ACM systems are in common. Conceptually, adaptable control (ACM) strategies can be implemented within a generic hierarchical accommodation strategy shown in Figure 3 [16],[17]. In the presence of a fault condition, the high-level redistribution controller reroutes the available control authority taking advantage of any inherent redundancy in the system. A mid-level set point controller then determines set point trajectories, which maintain stability of the restructured system, possibly at some degraded performance. Finally, the low-level algorithms adjust local controller gains in response to the new set points generated by the mid-level controller.

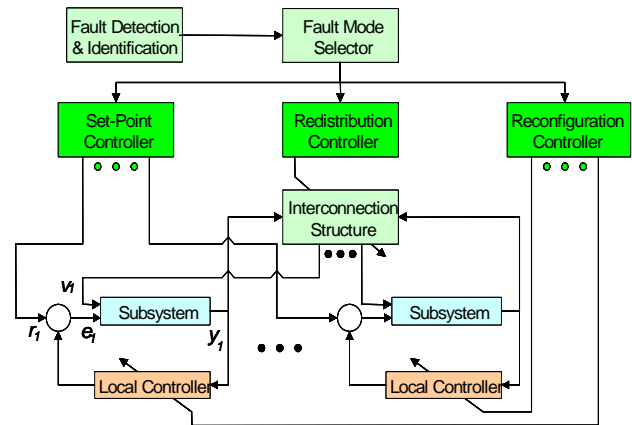


Figure 3 : A Hierarchical Fault Tolerant Reconfigurable Control Structure

The development of an ACM system usually requires advanced health management and fault tolerant systems consisting of unconventional requirements, system architectures, and hardware implementations, which significantly challenges current V&V procedures, methods and tools. It is unlikely that any single approach will address all the V&V challenges. The best hope of bridging this gap is probably to integrate approaches combining automated testing, new analysis tools, run-time assurance methods, and more important, to follow a well-defined V&V procedure from the early stage of the ACM system development.

ACM development begins with system-level requirements and ends with a validated implementation in hardware and software. The whole process can be well represented by the Classic “V” of system development process as illustrated in Figure 4. Particularly, for a ACM system which is focused on fault accommodation and contingency management, a typical ACM development path can be defined as shown in Figure 5. Although V&V seems to be the last step on the development path, it is important that ACM and V&V technologies are defined and selected in concert to ensure that V&V is driven by the needs of ACM applications, and that V&V considerations are infused early on into the ACM development process. The V&V process should take place earlier in the overall system design effort, reducing costly iterations across many design steps.

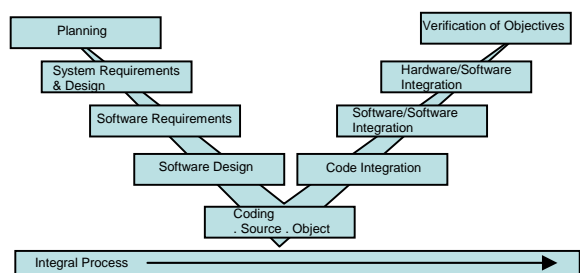


Figure 4 : Classic “V” of System Development

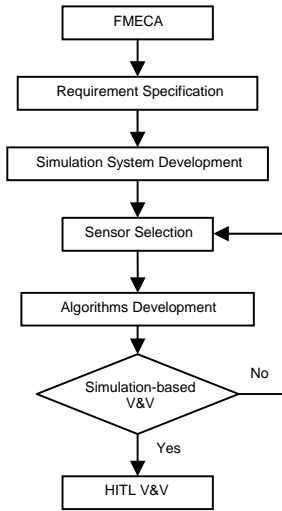


Figure 5 : ACM Development Path

Moreover, in order for the ACM software to be certified by the FAA under the standards presented in RTCA DO-178B, the V&V procedure must be carefully documented and the behavior of the fielded software must be the same as that evidenced during V&V testing.

3. OPTIMIZATION-BASED ACM DESIGN & ACM MODELING

Analytically, the objective of the ACM system is to optimize the utility of the plant with impaired capability to accomplish assigned mission. The ACM system can be formulated as an optimization problem in two levels [18], Mission (upper) Level:

$$J(M) = \max_M U(P_e, M, M_{com}) \quad (1)$$

Controls (lower) level:

$$J(R) = \max_R P_e(F_m, R, M) \quad (2)$$

where U is a cost function that quantifies the usefulness of the plant to accomplish its mission. U is a function of $P_e(F_m, R)$, the closed loop performance, which is a function of fault mode F_m as well as any re-structuring/reconfiguration R applied to the system. F_m is a vector of indicators (0 or 1) that characterizes the fault modes detected on the aircraft; R is a vector of indicators that characterizes all restructuring applied to the system. M_{com} describes the mission assigned to the aircraft. On the other hand, M allows the fault-tolerant control architecture, specifically the mission adaptation component, to modify the parameters of the assigned waypoints based on vehicle performance, P_e .

At the mission level, mission adaptation (M) allows the control architecture to pursue relaxed mission objectives M (instead of M_{com}) in order to achieve greater vehicle usefulness U . At the controls level, the objective is to optimize vehicle performance P_e with consideration of mission requirements, through restructuring and

reconfiguration, R . Practically, the above optimization problems have to be solved with consideration of various constraints including system dynamics and resource limitations.

The benefit of an optimization-based ACM is obvious. If formulated properly, the optimality of the ACM strategy can be proved mathematically. Since the ACM strategy is based on explicit optimization formulation it is amenable to rigorous V&V. Meanwhile, numerous COTS linear programming, mixed integer linear programming, quadratic programming, and convex optimization routines are available to be deployed on the target platform and a lot of these tools have already gone through systematic V&V process.

To facilitate the formulation of the optimization problem, an ACM guarded system can be represented by a Finite State Machine (FSM) as shown in Figure 6. There can be multiple states in each of the three state-spaces, but the general nature of transitions between different states can be described by five types of transitions as depicted.

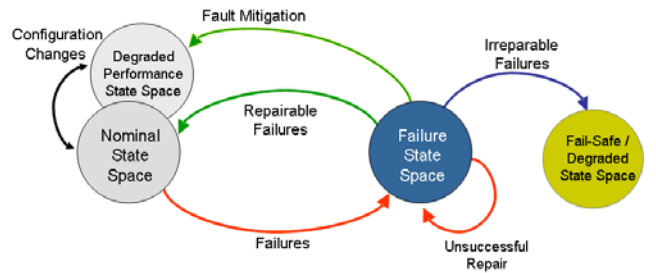


Figure 6 : ACM Modeling

Contingencies move the system to failure state. Repairable failures allow the system to eventually come back to the normal state, whereas irreparable failures will force the system to a failsafe state to avoid further catastrophes and buy some extra time before external help can be sent, if possible. However, in case of faults that may not be completely repairable, ACM tries to find alternatives that will still let the system perform within acceptable limits but with degraded performance.

With the modeling paradigm described above, the ACM algorithm can be formulated as a constrained optimization problem as stated: Given the current states of the system, and subject to predefined system constrains, find the optimal action series that will bring the system to the desired states with a minimal cost and the highest probability of success.

An optimization-based ACM architecture and a test bench with V&V capabilities are shown in Figure 7.

ACM strategies specific to the target system are modeled in the finite state machine model implemented in Stateflow™. The ACM model interacts with the plant dynamic model (a part of the ACM Test Bench) through sensor measurements

to observe the state of the system, and guides the system via control inputs. ACM simulator emulates (formulates) different possible strategies to mitigate a failure mode. The Reasoner or Decision Maker chooses the optimum strategy from among the various options suggested by the ACM simulator. Whenever it receives a fault indication from the Stateflow model, it requests a list of possible transition sequences, from the ACM simulator, that can be taken from the fault state to the normal state.

As a future improvement, the ACM system will be enhanced by a Run-time Monitor to provide online ACM assurance. The Run-time Monitor observes the behavior of the ACM system and disables it in the event of a malfunction.

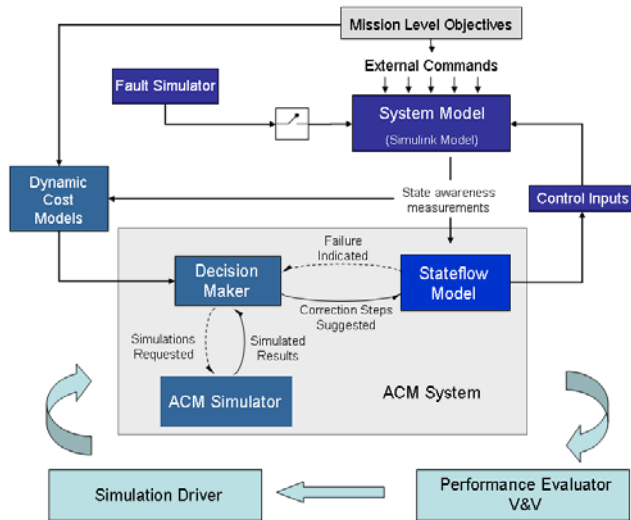


Figure 7 : Optimization-based ACM & Test Bench with V&V Capabilities

4. SIMULATION-BASED V&V OF ACM SYSTEM

As ACM systems become more complex, V&V and system certification costs will increase dramatically due to a projected increase in required testing resources, such as hardware in the loop (HIL) testing labor and hardware costs. The later a flaw is found in ACM design, the more pricy it is to correct it. The design of an ACM Test Bench Software with V&V capabilities will significantly reduce the V&V cost, by running high fidelity system dynamic model with simulated fault scenarios.

Technically, simulation-based V&V plays a very important role in the early ACM design phase due to the following reasons: (1) Limited or improper fault data; available data usually may not cover the entire targeted fault list, and some legacy data may exist for a failure mode that has been eliminated by a new design, and thus, is no longer relevant or has minimal impact. (2) Impracticality of seeding faults; for complex systems like the propulsion system, it is usually impractical or very difficult to seed a fault in the actual system due to cost and technical reasons. A typical hotfire

test of a rocket engine can cost on the order of several hundred thousand dollars. A minimal test series for a PHM targeting 20 or so fault modes could easily end up costing millions of dollars for testing alone not even considering the cost of “repairing” the engine after each test [19].

The concept of simulation based ACM design and V&V is instantiated in the development of an ACM Test Bench with V&V Capabilities [20] as shown in Figure 7.

An important feature of the ACM Test Bench is the ability to manage fault insertion and simulations and evaluate results from a generic Graphical User Interface (GUI) referred to as the Simulation Driver, which can also be used in conjunction with the Performance Evaluator/V&V module to automate the V&V process. The infrastructure for this test bench allows linking requirements (as specified in the system design specification) to parts of the system model (e.g. as implemented in Simulink™) as well as automatically generating references to the original requirements in the code (e.g. Matlab™ code, or code generated from Real-time Workshop™).

Generally speaking, as a software intensive system, many common V&V techniques are applicable to ACM V&V. In line with the “Recommended Practices Guide” (RPG) of the Defense Modeling and Simulation Office (DMSO) [21], we have divided these techniques in five categories. Following is a brief description of these categories as well as how and where they fit in the ACM development and V&V lifecycle:

- **Informal Techniques:** As the name implies, these techniques are defined and implemented in a casual manner. They are usually low-cost and simple to understand. However, to be effective, their implementation should be very structured and specific guidelines should be defined and implemented. These techniques can be for example a *run-time monitoring agent*. Other methods such as *desk checking* can involve detailed check-lists. In case of the ACM V&V, most of these informal techniques such as *review*, *document checking*, *run-time monitoring*, and *inspection*, as part of the regular research and development processes can be utilized.
- **Static Techniques:** These procedures are composed of all the activities that can be performed without executing the code. Therefore, by definition, these techniques do not attempt to check the simulation results rather they only look at the model. For example, the *Fault/Failure Analysis* and *Cause-effect graphing* are useful to ACM design.
- **Formal Techniques:** This class covers those techniques that perform formal mathematical reasoning, inferencing, and proofs of correctness. Although these techniques are extremely effective, they are usually costly and difficult to implement on large-scale systems. NASA has been the pioneer in this area [22].
- **Hybrid Techniques:** As the name implies these techniques combine some of the methodologies

presented above. The works reported under this category draw on the power of formal methods and try to overcome limitations of these methods by utilizing alternate strategies to facilitate large-scale development.

- **Dynamic Techniques:** These techniques look at the results of the execution of a program or simulation. The model/system is usually examined as it is being executed. This almost always requires *instrumentation*, i.e. insertion of additional code (on ACM Test Bench), or sensors (if it is a system) to collect and monitor behavior during execution.

Uniquely to our optimization-based ACM system, the key V&V tasks can be further summarized as:

- (1). **Verify ACM model correctness:** i.e. the model (usually a Finite State Machine) is a valid abstraction of your contingency management plan; Formal model checking techniques can be utilized in this process.
- (2). **Verify ACM algorithms correctness:** the ACM algorithms (e.g. optimization algorithms) and implementation are correct; i.e. all the faults are accommodated optimally as required by specification.
- (3). **Validate ACM coverage:** i.e. validate all the faults that need to be accommodated (specified in ACM Design Specification) can be accommodated by the ACM system.
- (4). **Validate ACM performance:** i.e. pre-specified performance criteria are met;

A number of COTS tools are available for Simulation-based V&V. The Simulink Verification and Validation blockset can be used to expose design flaws, inadequate requirements, incomplete tests, and unnecessary design constructs early in the development process. The user can trace requirement documents to the design models, component tests, and generated code. The user can also verify his designs and tests through model coverage and modeling standards checking. Particularly, the Model Advisor checks a model or subsystem for conditions and configuration settings that can result in inaccurate or inefficient simulation of the system represented by the model or generation of inefficient code from the model. It produces a report that lists all the suboptimal conditions or settings that it finds, suggesting better model configuration settings where appropriate. This is a particularly useful tool when automatically generated code is used on the target system.

In principle, accomplishment of above tasks will provide a certain level of confidence in the ACM system, and it would be ready to move on to the next level of V&V involving HIL testing, flight testing and flight certification, which is

not the focus of this study due to our limited access to flight testing facilities.

5. A CASE STUDY: MONOPROPELLANT PROPULSION SYSTEM

A pressure-fed monopropellant propulsion system for a small space flight vehicle, shown in Figure 8, has been chosen to be used as initial proof-of-concept implementation. The purpose of the system is to provide thrust for the vehicle while in orbit [23]. The system uses hydrogen peroxide (H_2O_2) that passes over a catalyst and decomposes into byproducts of oxygen, water, and heat to create an expanding gas producing a thrust that changes the spacecraft velocity. The system consists of a reservoir TK1 of inert gas that is fed through an isolation valve IV1 to a pressure regulator RG1. The pressure regulator RG1 senses pressure downstream and opens or closes to control the pressure at a constant level. A check valve, CV1 allows passage of the inert gas to the Propellant Tank PT1. Separating the inert gas from the propellant is a bladder that collapses as propellant is depleted. Propellant is forced through a feed line to the Thruster Isolation Valve IV2 and then to the Thrust Chamber Inlet Valve IV3. For the Thruster to fire, the system must first be armed, by opening IV1 and IV2. After the system is armed, a command is sent to IV3, to open, allowing H_2O_2 into the thrust chamber. As the propellant passes over the catalyst, it decomposes producing the byproducts, heat, and the expanding gas that creates the thrust. The relief valves RV1-4 are available to dump propellant overboard should an overpressure condition occur in any part of the system. The electrical command system controls the arming and thrusting of the propellant system. In addition there are pressure and temperature sensors PTK1, PPT1, TTK1 and TPT1 to monitor and regulate the gas pressure in the gas tanks.

To assess the ACM and V&V methodologies, a Simulink model for the monopropellant propulsion system has been developed, as shown in Figure 9. This model mainly consists of three modules that contribute to the overall purpose of simulation and V&V during experimentation:

- System model for the propulsion system
- Fault simulator
- Indicator module or the observation panel

Fault simulator can be used to inject several faults into the system at any point of the simulation. For example, 1) The failure of the system to provide thrust when commanded due to any of the valves IV1-3 are stuck closed, Regulator failure, or low propellant level; 2) Continued system firing after the system has been commanded off due to valve IV3 is stuck open, Timer Relay K6 fails to disengage or manual switch S3 failure; 3) Sensor failures: pressure sensor P_{TK1} or P_{PT1} failures, temperature sensor T_{TK1} or T_{PT1} failures; 4) Inadequate pressure in the gas path due to abnormal (high or low) inert gas path pressure, abnormal (high or low) propellant gas path pressure, pressure regulator failure, or low propellant or inert gas levels (due to leakage).

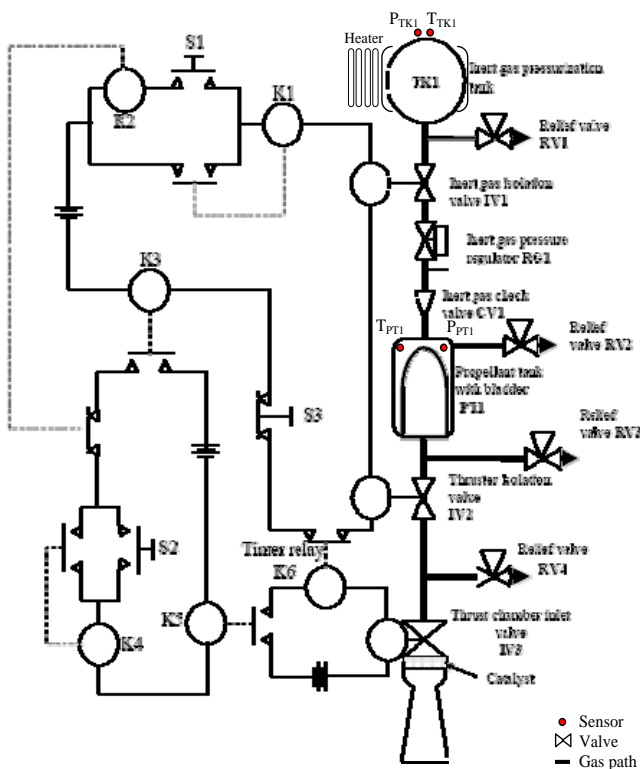


Figure 8: A monopropellant propulsion system schematic (modified from [23])

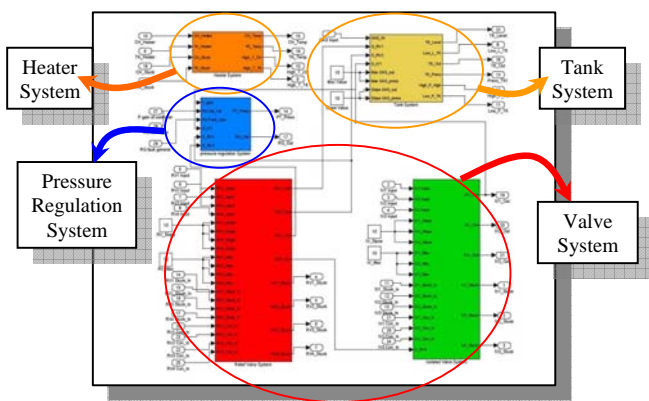


Figure 9: Monopropellant Propulsion System Model

System Requirements

In general, there are a variety of requirements for ACM system development. They typically are formulated in natural language and may contain inconsistencies. In this paper, a small set of high level requirements, listed below, is used to explain the concept. The actual requirements are far more extensive than those presented and in most cases, include requirements on sensors, computer hardware, footprint, weight, etc., and since these are hardware related, the corresponding V&V are not discussed in this paper.

- (1). Fault Coverage: The ACM system should provide optimal contingency strategy for leaking gas tank (TK1), heater malfunction (TK1 heater), defective measurement sensors (P_{TK1} , P_{PT1} , T_{TK1} or T_{PT1}), defective valve (CV1, IV1, IV2, IV3), defective relief valve (RV1, RV2), defective regulator (RG1);
- (2). ACM strategy optimality: the optimality should be defined by safety of the crew (stability of the vehicle), time to accomplish the mission, fuel consumption, in this order.
- (3). Performance assurance: the incorporation of the ACM system should not cause performance degradation to the system in the absence of faults.
- (4). Robustness: the ACM system should be robust to PHM false alarm. The monopropellant system with ACM should not perform worse than a system without ACM in case of PHM false alarm.

The high-level requirements are gradually refined into a set of detailed requirements from which the subsystem specifications can be derived. The lower-level detailed requirements can be linked to the model or code developed in the simulation environment using tools like the Simulink Verification and Validation.

The simulation results presented in this paper were obtained by simulating a regulator (RG1) failure in which the regulator fails to maintain a desired regulated pressure.

ACM Modeling

The ACM model has been developed using Matlab Stateflow™ toolbox. Figure 10 shows a part of the Stateflow diagram for the fault scenarios described above. Whenever the system makes a transition from the normal mode to a fault mode the costs are computed and the action is taken at the moment the total costs are the minimum.

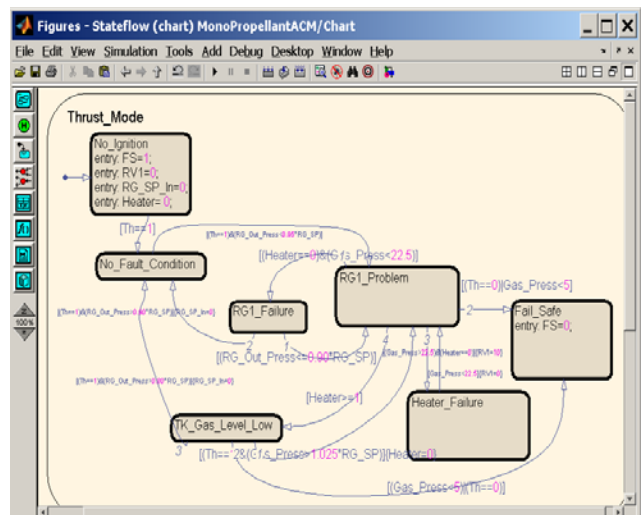


Figure 10 : ACM Model in Stateflow

The stateflow model directly interacts with the simulink model to assess the state of the system. Variables like pressures, temperatures, percentage of mission completion, and fuel level are continuously monitored and (as soon as

something goes beyond normal levels) an action is applied until the abnormal behavior is sufficiently corrected.

Cost Model

As a proof-of-concept, a simple cost model was developed. This model takes two factors into account in calculating the total costs, i.e. fuel consumption and time to accomplish the mission.

$$\text{Total Cost} = w_1 * \text{time}(\text{heater_on})^2 + w_2 * \text{cost}(\text{extra time to complete mission}) \quad (3)$$

Figure 11 shows two scenarios each with fault occurring at an early and a later stage of the mission. As can be seen, if the fault occurs in the early stage of the mission, heater need not be turned on immediately whereas if the fault occurs towards the end heater should be immediately turned on. This example also illustrated the advantage of optimization-based ACM design compared to an ACM system based only on predetermined rules. Once other cost factors need to be considered, a composite cost function can be formulated and incorporated in the decision making process.

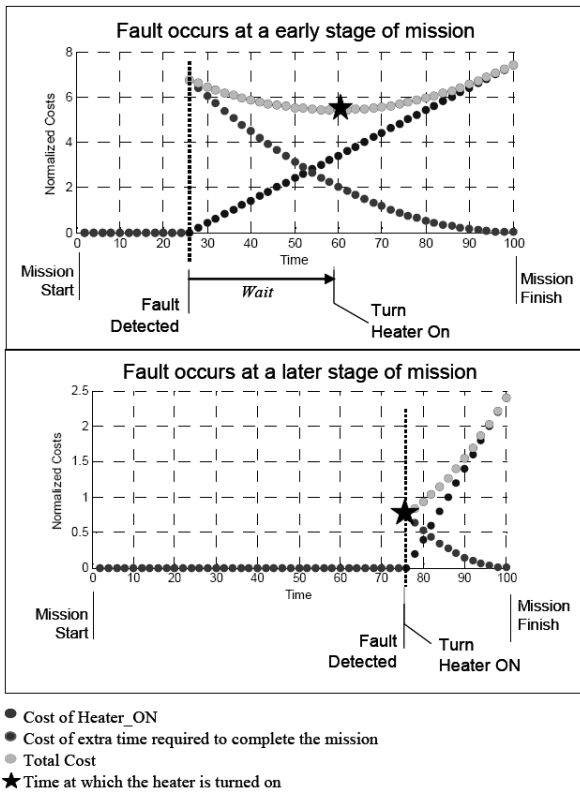


Figure 11 : Cost Model

V&V and Performance Evaluation

The V&V of the performance of the monopropellant propulsion ACM system was conducted following the process depicted in Figure 12. Relevant V&V approaches and tools presented in Section 4 were applied in the whole ACM development process. Particularly, model checker and Simulink Verification & Validation were utilized to check ACM model correctness and model coverage, link

model/code to requirements, build test cases, and generate reports. The optimality of the ACM strategy is obvious in this case. The performance of the ACM system (in terms of optimality) was evaluated by comparing the performance with a system with a fixed-logic ACM (no optimization). Figure 13 shows the comparison between an optimization-based ACM and an ACM based on pre-determined rules (for the select fault scenario) by means of a Monte Carlo Simulation with randomly generated fault occurrence time. It is validated that the performance of optimization-based ACM is always superior when the fault occurs before time 50. Note that the oscillation is caused by the random delay in fault detection time, given a fixed sample rate (2 sec.) for the ACM system.

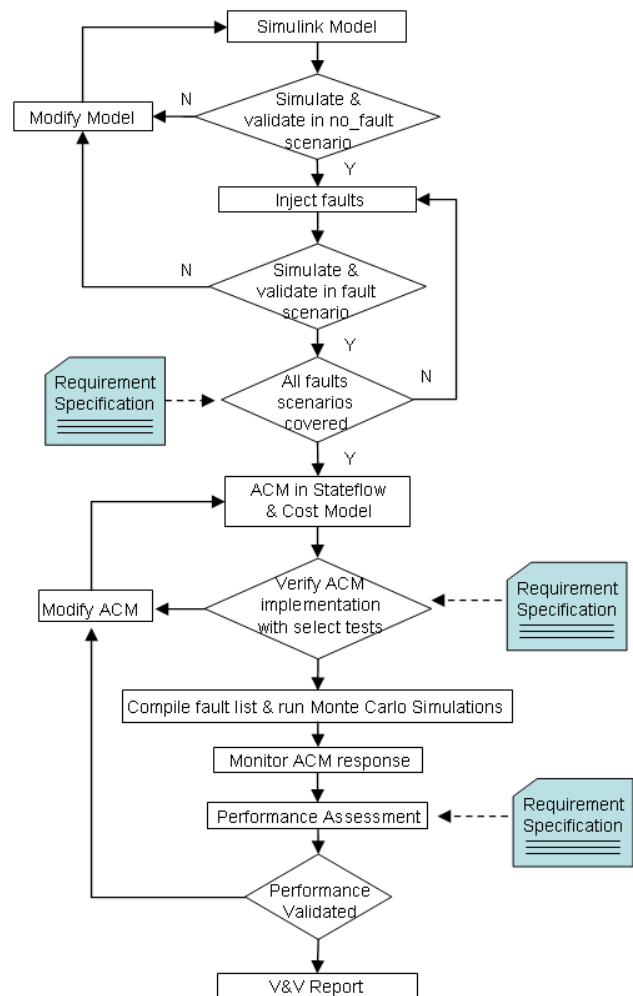


Figure 12 : Performance V&V for Monopropellant ACM

Figure 14 shows the Monte Carlo Simulation results of the performance of the system with ACM in case of PHM false alarm (the TK1 heater was turned on by the ACM system triggered by a false alarm on RG1 failure). In this case, the system with ACM consumed more fuel than the system without ACM (where the cost is 0). This test result showed

a violation of the robustness requirement. Obviously, to secure this requirement, a run-time monitor has to be implemented in the ACM system to check and validate PHM alarms and terminate ACM function when a false alarm was cleared.

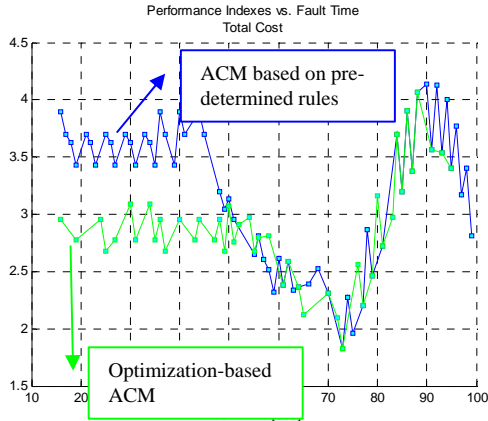


Figure 13 : ACM System Performance Comparison

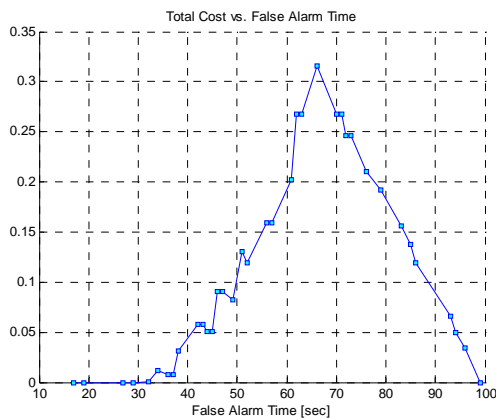


Figure 14 : ACM System Robustness Evaluation

6. CONCLUSION AND FUTURE WORK

V&V is a key enabling technology to the sustainable deployment of advanced ACM for propulsion systems. Ultimately, transition of advanced ACM systems that enable transformational military operations and space exploration will strongly depend on affordable V&V strategies that reduce costs and compress schedules for flight certification.

This paper presented the development of simulation-based design and validation of propulsion ACM system. Main contributions of the work are:

- Developed a systematic process for simulation-based V&V of PACM systems;
- Proposed and developed a V&V-aware, optimization-based ACM design methodology;
- Explored and developed new V&V techniques and

tools.

Future work will be carried out in the following areas,

- Run-time V&V; investigate the development of run-time monitor to provide online ACM assurance. A monitoring process that observes the behavior of the ACM system and disables it in the event of a malfunction in ACM itself is important to the success of ACM system.
- V&V approaches for nondeterministic optimization algorithm, e.g. Genetic Algorithms, Particle Swarm Optimization, etc.
- Integration of V&V tools with the PACM Test Bench;
- Reliability analysis of propulsion system with ACM; i.e. quantify the reliability improvement attributed to the introduction of the ACM system;
- V&V of HITL PACM system.

ACKNOWLEDGEMENT

This work was supported by the NASA Ames Research Center in Moffett Field, CA, under STTR contract No. NNA05AC53C. We would also like to recognize the contributions of Dr. Irtaza Barlas, Dr. Michael Roemer from Impact Technologies, LLC, and Dr. Biqing Wu, Mr. Bhaskar Saha, Mr. Johan Reimann, Dr. Bin Zhang and Dr. Young Jin Lee from Georgia Institute of Technology.

REFERENCES

- [1] Vachtsevanos G., Lewis F. L., Roemer M., Hess A., Wu B., 2006, "Intelligent Fault Diagnosis and Prognosis for Engineering Systems", WILEY.
- [2] Byington C.S., Watson M., Edwards D., Stoelting P., 2004, "A Model-Based Approach to Prognostics and Health Management for Flight Control Actuators", Proc. IEEE Aerospace Conference, Big Sky MN, paper 1047.
- [3] Volponi A., Wood B., 2005, "Engine Health Management for Aircraft Propulsion Systems", First International Forum on Integrated System Health Engineering and Management in Aerospace, November 7-10, Napa, CA.
- [4] Litt J.S., Simon D.L., Garg S. and et al. 2004, "A Survey of Intelligent Control and Health Management Technologies for Aircraft Propulsion Systems", Journal of Aerospace Computing, Information, and Communication, vol.1, no.12, Pp. 543-563.
- [5] Kallappa P., Hailu H., 2005, "Automated Contingency And Life Management For Integrated Power And Propulsion Systems", Proceedings of ASME Turbo Expo, Power for Land, Sea and Air, June 6-9, Reno-Tahoe, Nevada, USA.
- [6] Buffington, J., Crum, V., Krogh, B., Plaisted, C., Prasanth, R., and Bose, P., "Validation & Verification of Intelligent and Adaptive Control Systems," Proceedings of the 2nd AIAA "Unmanned Unlimited" Conf. and Workshop & Exhibit, 2003, AIAA Paper 2003-6603.
- [7] Pecheur, C. and Simmons, R., "From Livingstone to SMV: Formal verification for autonomous systems," Goddard Workshop on Formal Methods, April 2000.
- [8] Silvia Brey, Extending C Global Surveyor. Technical report. NASA Ames Research Center, Moffett Field, USA, September 2004.
- [9] Patrick Regan, Scott Hamilton, "NASA's Mission Reliable," Computer, vol. 37, no. 1, pp. 59-68, Jan., 2004.
- [10] Stephen A. Jacklin, Johann M. Schumann, Pramod P. Gupta, Michael Richard, Kurt Guenther, and Fola Soares, Development of Advanced Verification and Validation Procedures and Tools for the Certification of Learning Systems in Aerospace Applications, Infotech@Aerospace, Arlington, Virginia, 26 - 29 September 2005.
- [11] Alec J. Bateman, Carl R. Elks, David G. Ward, and John D. Schierman, New Verification and Validation Methods for Guidance/Control of Advanced Autonomous Systems, Infotech@Aerospace, Arlington, Virginia. 26-29, September 2005.
- [12] Johann Schumann, Pramod Gupta and Stephen Jacklin, Toward Verification and Validation of Adaptive Aircraft Controllers, IEEE Aerospace Conference, Big Sky, Montana, 5-12 March, 2005.
- [13] P. Binns, M. Elgersma, S. Ganguli, V. Ha, T. Samad, Statistical Verification of Two Non-linear Real-time UAV Controllers, Proceedings of the 10th IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS'04).
- [14] Tallant, G.S.; Bose, P.; Buffington, J.M.; Crum, V.W.; Hull, R.A.; Johnson, T.; Krogh, B.; Prasanth, R., Validation & Verification of Intelligent and Adaptive Control Systems, IEEE Aerospace Conference, Big Sky, Montana, 5-12 March 2005.
- [15] James E. Dzakowic, G. Scott Valentine, Advanced Techniques for the Verification and Validation of Prognostics & Health Management Capabilities, Proceedings of the 60th Meeting of the Society for Machinery Failure Prevention Technology, Virginia Beach, Virginia. April 3-6, 2006.
- [16] George Vachtsevanos, Liang Tang, Graham Drozeski, and Luis Gutierrez, From Mission Planning To Flight Control Of Unmanned Aerial Vehicles: Strategies And Implementation Tools, Annual Reviews in Control, Vol. 29, pp. 101-115, 2005
- [17] Liang Tang, Gregory J. Kacprzynski, Michael J. Roemer, George Vachtsevanos and Ann Patterson-Hine, Automated Contingency Management Design for Advanced Propulsion Systems, Infotech@Aerospace, Arlington, Virginia. 26 - 29 September 2005.
- [18] Drozeski, G. R., A Fault-tolerant Control Architecturs for Unmanned Aerial Vehicles, Ph.D Dissertation, Georgia Institute of technology, 2005.
- [19] Robert Aguilar, Chuong Luu, and Louis M. Santi, Real-Time Simulation for Verification and Validation of Diagnostic and Prognostic Algorithms, 41st AIAA/ASME/SAE/ASEE Joint Propulsion Conference & Exhibit, Tucson, Arizona, 10-13 July 2005.
- [20] Michael Roemer, Liang Tang, Gregory J. Kacprzynski, Jianhua Ge, and George Vachtsevanos, Simulation-Based Health and Contingency Management, IEEE Aerospace Conference, Big Sky, Montana. Mar. 4-11, 2006.
- [21] Defense Modeling and Simulation Office. "Online M&S Glossary." DoD 5000.59M. Washington: Department of Defense. <http://www.dms.o.mil/public/resources/glossary>
- [22] Charles Pecheur, Stacy Nelson, V&V of Advanced Systems at NASA. NASA ARC. Technical Report NASA/CR-2002-211402. Jan 25, 2002.
- [23] Vesely, W., Stamatelatos, M., Dugan, J., Fragola, J., Minarick III, J., Railsback J., "Fault tree handbook with Aerospace Applications" version 1.1, August 2002.

BIOGRAPHY

Dr. Liang Tang is a project manager at Impact Technologies LLC, Rochester, NY. His research interests include fault tolerant control, intelligent control, signal processing, diagnostics, prognostics and health management systems. He obtained a Ph.D. degree in Control Theory and Engineering from Shanghai Jiao Tong University, China in 1999. Before he joined Impact Technologies, he worked as a post doctoral research fellow at Intelligent Control Systems Laboratory, Georgia Institute of Technology.



Abhinav Saxena is a PhD student in the School of Electrical and Computer Engineering at Georgia Institute of Technology. His research is focused on the architecture for Intelligent Diagnosis and Prognosis of Manufacturing Systems using Artificial Intelligence technique Case-Based Reasoning. Abhinav joined Georgia Tech in 2001



at the school of Textile and Fiber Engineering, and earned Master of Science Degree in May 2003. He received bachelor's degree from the Indian Institute of Technology, Delhi in Textile and Fiber Engineering in 2001. Abhinav is a GM manufacturing scholar and also a member of Eta Kappa Nu engineering honor society.

of unmanned aerial vehicles, fault diagnosis and prognosis of complex dynamical systems, vision-based inspection and control of industrial processes and the application of novel signal and imaging methods to neurotechnology related research. Dr. Vachtsevanos has published over 250 technical papers in his area of expertise and serves as a consultant to government agencies and industry.

Marcos Orchard is a Ph.D. Student in the School of Electrical and Computer Engineering at The Georgia Institute of Technology, and Instructor Teacher of the Department of Electrical Engineering at the University of Chile. His current research interest is the design, implementation and testing of a Particle Filtering framework for real-time FDI and failure prognosis. Marcos joined Georgia Tech in 2003, and earned a Master of Science degree in December 2005. He received B. Sc. degree (1999) and a Civil Industrial Engineering degree with Electrical Major (2001) from Catholic University of Chile.



Gregory J. Kacprzyński is Manager of Advanced Programs and co-founder of Impact Technologies with over 10 yrs. of experience in the development and implementation of diagnostic/prognostic systems for compressors, pumps, motors, transmissions, gas and steam turbines and other complex machinery systems. He is responsible for technology development on multiple SBIRs dealing with next generation condition-based maintenance systems, aircraft prognostics, and health management design for DARPA, the Army, Navy and USAF as well as commercial programs for customers like Boeing, Honeywell, General Dynamics and EPRI. Greg received his M.S. and B.S. in Mechanical Engineering from Rochester Institute of Technology.



Dr. George Vachtsevanos is a professor in the School of Electrical and Computer Engineering at The Georgia Institute of Technology, and the director of the Intelligent Control Systems Laboratory where faculty and students are conducting interdisciplinary research in intelligent control, hierarchical/intelligent control

