

RISK-SIGNIFICANT ADVERSE CONDITION AWARENESS STRENGTHENS ASSURANCE OF FAULT MANAGEMENT SYSTEMS

Rhonda Fitz

MPL Corporation, rhonda.s.fitz@ivv.nasa.gov

ABSTRACT

As spaceflight systems increase in complexity, Fault Management (FM) systems are ranked high in risk-based assessment of software criticality, emphasizing the importance of establishing highly competent domain expertise to provide assurance. Adverse conditions (ACs) and specific vulnerabilities encountered by safety- and mission-critical software systems have been identified through efforts to reduce the risk posture of software-intensive NASA missions. Acknowledgement of potential off-nominal conditions and analysis to determine software system resiliency are important aspects of hazard analysis and FM. A key component of assuring FM is an assessment of how well software addresses susceptibility to failure through consideration of ACs. Focus on significant risk predicted through experienced analysis conducted at NASA's Independent Verification & Validation (IV&V) Program enables the scoping of effective assurance strategies with regard to overall asset protection of complex spaceflight as well as ground systems. Research efforts sponsored by NASA Office of Safety and Mission Assurance (OSMA) defined terminology, categorized data fields, and designed a baseline repository that centralizes and compiles a comprehensive listing of ACs and correlated data relevant across many NASA missions. This prototype tool helps projects improve analysis by tracking ACs and allowing queries based on project, mission type, domain/component, causal fault, and other key characteristics. Vulnerability in off-nominal situations, architectural design weaknesses, and unexpected or undesirable system behaviors in reaction to faults are curtailed with the awareness of ACs and risk-significant scenarios modeled for analysts through this database. Integration within the Enterprise Architecture at NASA IV&V enables interfacing with other tools and datasets, technical support, and accessibility across the Agency. This paper discusses the development of an improved workflow process utilizing this database for adaptive, risk-informed FM assurance that critical software systems will safely and securely protect against faults and respond to ACs in order to achieve successful missions.

INTRODUCTION

NASA OSMA sponsors the Software Assurance Research Program (SARP) and has funded Fault Management Architectures (FMA) initiatives centered at the IV&V Program out of the Safety and Mission Assurance (SMA) Support Office (SSO) since 2014. Transitioning research products to application for IV&V and Software Assurance (SA) across the Agency supports the goal to advance risk-informed decision making with respect to safety- and mission-critical FM systems. A FMA Technical Reference (TR) Suite¹ and AC Database were deliverables from the FMA research and are to be integrated within the Enterprise Architecture framework established at NASA IV&V. This research has provided the following benefits:

- Improved capability-based assurance from the provision of more comprehensive data
- More rigorous IV&V analysis from identification of off-nominal scenarios
- Increased efficiency of analyst workflow and broader test coverage
- Greater focus on FM and project areas of vulnerability or significant risk
- Support for reliability and resiliency for critical system safety

The approach and preliminary findings from early research were imparted in a Tech Track paper and presentation at the 31st Space Symposium entitled "Fault Management Architectures and the Challenges of Providing Software Assurance"². Additional findings and the description of the continuation of that effort were presented at the 32nd Space Symposium in a Tech Track paper and presentation entitled "Technical Reference Suite Addressing Challenges of Providing Assurance for Fault Management Architectural Design"³. Keeping the redundancy to a minimum, the reader is advised to refer to those publications for more in-depth details on the

FMA TR Suite. Beginning with a brief introduction to NASA's IV&V Program, context is given for assurance of FM systems. IV&V technical standards and a thread approach to performing analysis across the lifecycle are then described. How one project applies assurance based on mission capabilities is explored at a high level, followed by a query into the current view of hazard analysis from IV&V project managers' perspective. A case is made for the need to better define methodologies for incorporating ACs into assurance processes focused on reducing the risk inherent in complex, safety-critical software systems. A description of the scope of the new SARP initiative and then the AC Database design and implementation details are illustrated with an architectural model and database screenshots. Conclusions are drawn, with a look at progress that is ongoing. The data and product depictions provided in this paper have been condensed in order to avoid including any developer-specific or regulation-controlled information. The FM lexicon used is in agreement with that established in the NASA Fault Management Handbook, which is considered the central authority on FM terminology for the Agency.⁴

NASA'S INDEPENDENT VERIFICATION AND VALIDATION PROGRAM

NASA's IV&V Program was founded in 1993 under NASA Office of Safety and Mission Assurance (OSMA) as a direct result of recommendations made by the National Research Council (NRC) and the Report of the Presidential Commission on the Space Shuttle Challenger Accident.⁵ NASA's IV&V Program was established as part of an Agency-wide strategy to provide assurance that NASA safety- and mission-critical software will operate reliably, safely, and securely, and to advance systems and software engineering disciplines.

NASA's IV&V Program has a primary business focus to support NASA missions. The Program takes a systems engineering approach to enable the highest achievable levels of safety and cost-effective IV&V services through the use of broad-based expertise using adaptive engineering best practices and tools. NASA IV&V performs independent testing and analysis throughout the software development lifecycle resulting in objective evidence that provides a level of assurance that system software has been developed in accordance with quality standards, will operate reliably, safely, and securely and that sufficient risk mitigation has been applied to the software that controls and monitors critical NASA systems.

NASA IV&V Technical Framework

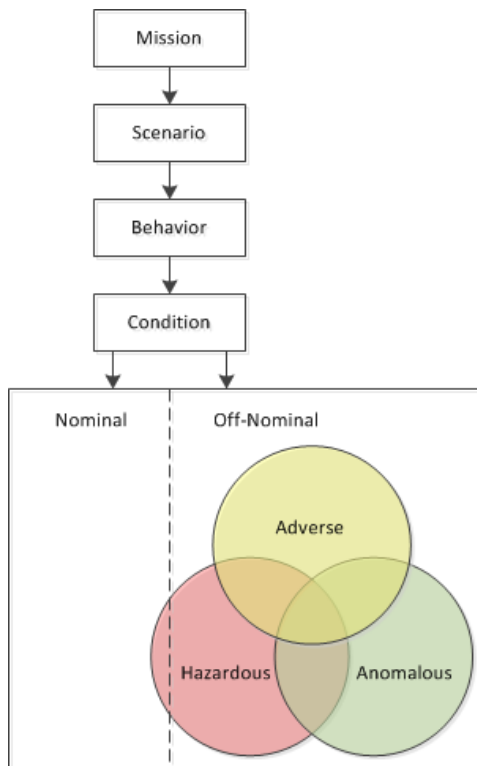
The IV&V Technical Framework (TF), IVV 09-1⁶, is a NASA system level procedure that establishes a foundation for a consistent set of methods for providing IV&V technical services to customers, sufficient to ensure safety and risk mitigation for the successful deployment of software-intensive systems. The TF is structured with a set of main objectives that correlate loosely to lifecycle phases, including the verification and validation of:

- 1.0 Management and Planning
- 2.0 Concept Documentation
- 3.0 Requirements
- 4.0 Test Documentation
- 5.0 Design
- 6.0 Implementation
- 7.0 Operations and Maintenance

One of the key concepts for software assurance is that there are certain perspectives that should be considered during all IV&V analysis, expressed in terms of The Three Questions (3Qs):

- Q1 Will the system's software do what it is supposed to do?
- Q2 Will the system's software not do what it is not supposed to do?
- Q3 Will the system's software respond as expected under adverse conditions?

Additionally, the awareness must be maintained that requirements or any of the objects being assessed cannot be evaluated in isolation and that content under evaluation should always be related back to the acquirer needs and system goals.



Examining Q2 and Q3 are major challenges of FM software. To clarify, an *adverse condition* is considered a subset of an off-nominal state that prevents a return to nominal operations and compromises mission success unless an effective response to the causal fault is employed. How a system is architected to handle faults and adverse conditions is crucial for the satisfaction of functional and performance requirements for mission success.

Exhibit 1: Adverse conditions illustrated by the decomposition of an off-nominal state associated with a specific behavior within a scenario of a particular mission

NASA IV&V ANALYSIS THREADS

With a Capability Development initiative focused on the IV&V of Agile developed projects⁷, these TF goals were extracted and decoupled from traditional waterfall phase dependencies in order to define IV&V analysis activities for incremental software integration and to examine necessary information needed to achieve assurance. In particular, addressing the off-nominal cases described by Q2 and Q3 above, five threads were defined: Hazards, Dependability, Emergent Behavior, Security, and Testing. These threads guide SA analysis activities to ensure that risk-significant ACs get the attention that is warranted to add confidence that mission- and safety-critical capabilities will be achieved as intended and will meet the needs of the system.

Following the Hazard Thread, for example, the analyst is tasked to ensure that known software-based hazard causes, contributors, and controls are identified and documented; and to ensure that the software requirements, the design, and the source code provide the capability of controlling identified hazards and do not create hazardous conditions. Note that software architecture, including the FM system architecture, is included in the design analysis.

The Dependability Thread partially overlaps these same TF elements as the analyst is tasked to ensure that the software requirements, the design, and the source code meet the dependability and fault tolerance required by the system. The rigor of the FM analysis will help assure the reliability and resiliency of the system.

The Emergent Behavior Thread addresses Q2, and is meant to protect from unintended features being introduced as the analyst is tasked to ensure that requirements (parent or child) and design do not introduce capability that is not required; that software architectural and software detailed design choices do not result in unacceptable operational risk; and that the implementation of source code has no emergent behaviors.

The Security Thread introduces more deliberate focus in providing information assurance as an important element of FM that has been neglected on spaceflight systems in the past. Objectives include tasks to:

- Ensure that security threats and risks are known, up to date, appropriately documented, and are correct for this mission and that relevant regulatory requirements are identified;
- Ensure that appropriate plans are in place to update the security threats and risks over the course of the development lifecycle to allow for introduction of new or changing threats;
- Ensure the security risks introduced by the system itself, as well as those associated with the environment with which the system interfaces, are appropriately accounted for in the known threats;
- Ensure the system concept from a security perspective and assure that potential security risks with respect to confidentiality (disclosure of sensitive information/data), integrity (modification of information/data), availability (withholding of information or services), and accountability (attributing actions to an individual/ process) have been identified;
- Ensure that the requirements address the security threats and risks identified within the system concept specifications and/or the system security concept of operations;
- Ensure that requirements define appropriate security controls to the system, subsystem, according to NASA Procedural Requirement 2810 and driven by the project's security needs and requirements;
- Ensure that the architecture and detailed design adequately address the identified security requirements both for the system and security risks, including the integration with external components and information and data utilized, stored, and transmitted through the system;
- Ensure that identified security threats and vulnerabilities are prevented, controlled, or mitigated via proposed design components or are documented and addressed as part of the system operations;
- Ensure that the implementation adheres to the system and software design in that it addresses the identified security risks and that the implementation does not introduce new security risks through specific code constructs, features, or coding flaws;
- Ensure that the system and software-required threat controls and safeguards are correctly implemented per proposed design components and validate that they provide the desired levels of protection against threats to the system, or are documented and addressed as part of the system and software operations;
- Ensure the appropriate level of data protection is defined and maintained across all instances and transactions throughout the system and that the security controls are defined to provide comprehensive (end-to-end) protection for the life of the data;
- Ensure that test cases under analysis verify specific security controls (physical, procedural and automated) that cannot be breached leading to compromise of information confidentiality, integrity, or availability;
- Ensure that the integrated system testing covers any areas that may potentially increase the security risk.

The Test Thread is even more complex and better described with a diagram as shown in Exhibit 2.

Following these SA analysis threads along with other lessons learned from the NASA Agile Benchmarking report⁸ is particularly helpful when providing SA on nontraditional software development projects. The important concept is that the evaluation of ACs is inherent throughout the lifecycle of analysis, not just at the origin with the planning and scoping of the IV&V project⁹, or even worse, left to the end with system level integration testing. An adaptive, iterative process to "follow the risk", shown in Exhibit 3, is established from the beginning with a TR of system understanding, which should evolve as the project matures. The performance of a risk assessment, the design of an assurance strategy balancing rigor with allotted resources and safety considerations, the execution of analysis to capture evidence along with critical assumptions, and finally the articulation of resulting assurance conclusions occurs iteratively at multiple stages in the software lifecycle. Periodic reassessment based on IV&V findings, development project schedule changes, or discovery of additional information should occur as frequently as is practical.

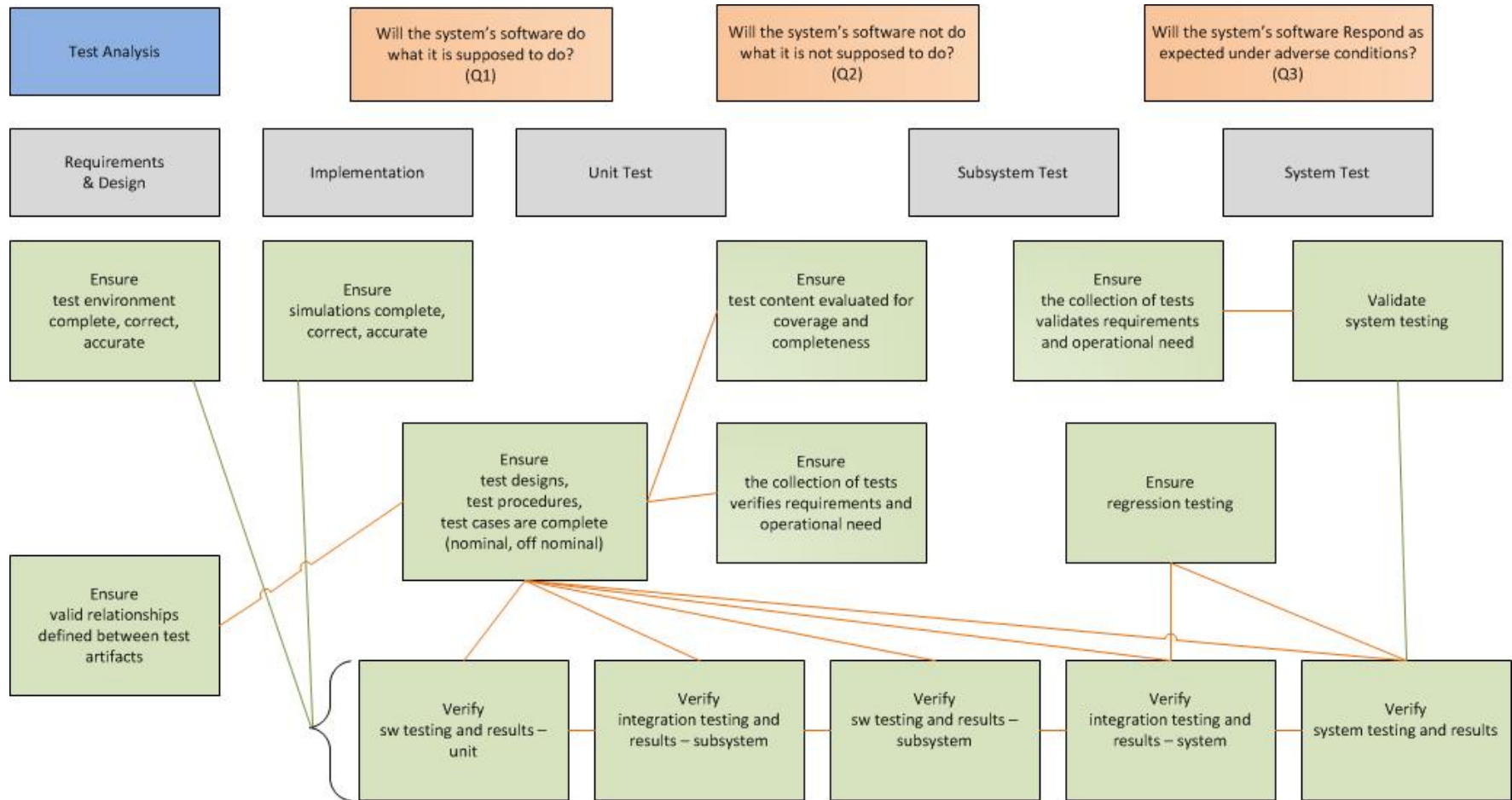


Exhibit 2: How the IV&V Analysis Test Thread crosses all phases of the software development lifecycle, covering nominal and off-nominal behaviors

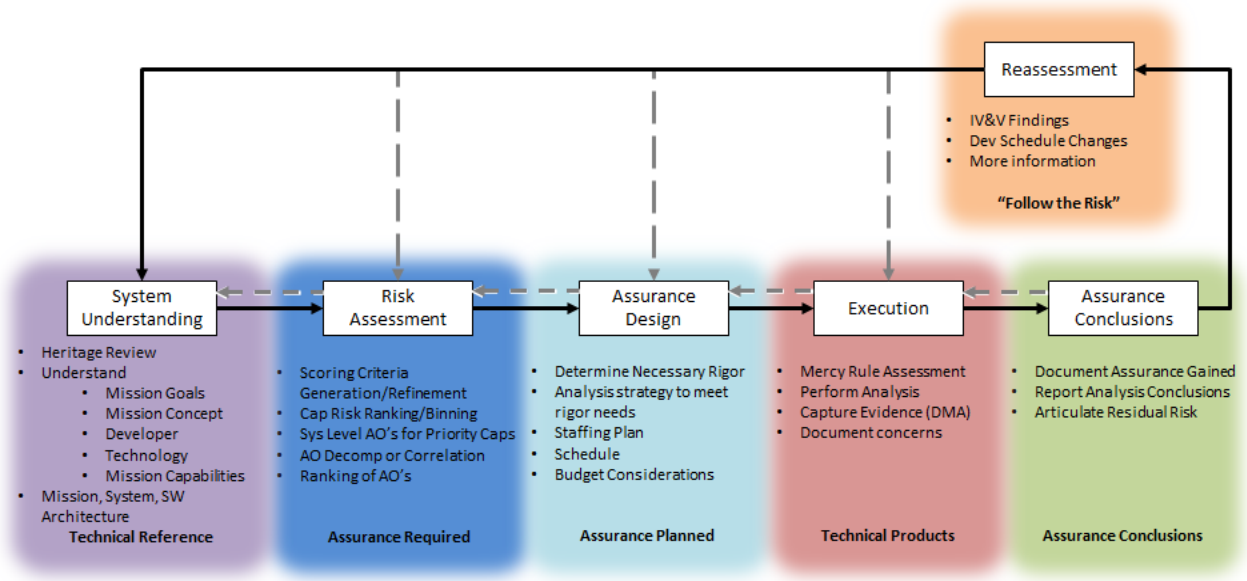


Exhibit 3: Adaptive, iterative NASA IV&V assurance process to “follow the risk”

The coordination of this workflow process is enabled by several tools incorporated within the Enterprise Architecture at the IV&V Program. The AC Database that is under development will improve the adaptive, risk-informed FM assurance so that critical software systems will safely and securely protect against hazards and faults and will respond to ACs in order to achieve successful missions. Synergies have been established with the NASA IV&V FM Community of Interest, SA working group, SA tools group, SSO, and IV&V analysts. With the support of NASA OSMA SARP and IV&V management, SA analysts will be increasingly able to provide risk-significant AC awareness to enhance capability-based assurance for software systems with increased confidence.

CAPABILITY-BASED ASSURANCE

Capability-based assurance (CBA)¹⁰ focuses the perspective of IV&V analysis from being based on artifacts or on Computer Software Configuration Items (CSCIs) to a tactic that allows a “follow the risk” approach, leveraging the understanding of technical risk to drive IV&V focus and rigor. Assurance objectives are written in the context of the capabilities to be analyzed, with the goal of providing assurance for mission success. CBA is a framework that enables SA workflow in an adaptive manner, infusing agility in order to accommodate change, with a clear trace to mission objectives and success criteria. It crosses all lifecycle phases, helping to identify IV&V scope and rigor, prioritize and frame analysis, influence static and dynamic test coverage, and more comprehensively communicate findings and assurance conclusions.

When FM systems for NASA projects are being assessed, an integrated system perspective is necessary in order to encompass the many interactions between components, systems, and subsystems within a complex architecture of data and control flow, usually organized within several layers or tiers. There is a deliberate flow-down of mission capabilities through system capabilities and to software capabilities. CBA enables SA professionals to gather broad system knowledge for the purpose of meaningful, risk-based decision making to provide the rigorous assurance necessary for safety and mission-critical NASA FM systems, effectively synchronizing Q1 with Q2 and Q3 considerations. One aspect of CBA may entail modeling systems for a TR that supplies analysts with confidence in the defined approach to understand and decompose risk-significant aspects of the software. These representations should reflect nominal as well as off-nominal scenarios, bringing AC awareness to the forefront in a manner that strengthens SA.

As one example, the Multi-Purpose Crew Vehicle IV&V project team has been instrumental in refining guidance for isolating the driving risks for capabilities, evaluating the role the software entities play, and translating the key factors into an approach that successfully implements CBA within a complex, to-be-human-rated project. The following (nonlinear, iterative) steps were outlined for planning and executing a CBA approach¹¹:

- Step 1: Develop and model a system understanding linked to capabilities
 - Nominal and off-nominal behaviors are included
- Step 2: Perform a criticality analysis to determine the in-scope capabilities
 - This is highly dependent on AC awareness and all aspects of FM and hazard analysis
- Step 3: Strategize assurance objectives to avoid or mitigate the most significant risks
 - Prioritizing effort requires balancing available resources
- Step 4: Determine the evidence necessary to achieve assurance
 - IV&V TF threads (described above) prescribe objectives to be met and desired outcomes
- Step 5: Perform analysis tasks with identified TF methods and acquire evidence
 - COMPASS, a catalog of methods, exists with options to tailor to individual projects
- Step 6: Perform analysis along IV&V capability threads and acquire evidence
 - This will be influenced by artifact availability or maturity and should be highly adaptive
- Step 7: Consolidate and document evidence
 - Enterprise Architecture tools are recommended for ease of compatibility
- Step 8: Present assurance conclusions
 - Keep in mind forward work or potential for AC behaviors that may be dynamically tested

The ability to map critical capabilities to ACs or hazard causes that are prevented or mitigated by software controls and verifications is one benefit the AC Database will provide. Also, dependencies or vulnerabilities in capabilities that may indicate missing requirements, weak design, incomplete implementation, or a need for expanded test coverage, either static or dynamic, will become apparent from the AC data accumulated by IV&V projects. The strategy of reducing risk improves the reliability, safety, security and overall quality of NASA missions.

NASA IV&V HAZARD ANALYSIS

A questionnaire was formulated and conducted across 15 IV&V projects to ascertain the status of hazard analysis and AC consideration within the IV&V Program¹². The results are an indicator of the variety of approaches to handling ACs and indicate where some projects might benefit from others' successes. Further investigation is necessary, but as of now, there is little commonality across projects in the consideration of ACs, and devising a strategy for optimizing assurance of FM by leveraging risk-significant AC awareness is proposed. Six questions were posed to IV&V project managers, and the responses are summarized below:

1. Are hazards/faults/adverse conditions being considered when performing IV&V analyses?
Unanimously, all projects were scoped to include FM as an integral part of assurance. Software IV&V necessarily includes a system approach to addressing faults and assessing hazards with the 3Qs mentioned above. Safety-critical aspects of hardware systems often have a software component in monitoring, in communicating status, and in responses or mitigations. This understanding impacts every level of analysis, and the identification of ACs occurs at the outset of every project. In fact, the majority of SSO support has been directly reviewing hazard reports and software safety analyses and actively participating in Safety Technical Review Boards where risks are addressed.
2. What specific documentation does the IV&V Project have access to that identifies the hazards/faults/adverse conditions?
Documentation varies from project to project, but generally the artifacts listed as source material for AC awareness include: Concept of Operations, Preliminary (and Final) Hazard Report, System (and Software) Safety Analysis, Portfolio Based Risk Assessment, Risk Based Assessment, Software Hazard List, Failure

Modes and Effects (and Criticality) Analysis, Fault Tree Analysis, System Assurance Analysis, Reliability and Safety Analysis Report, Criticality Assessment, Critical Item List, FM Design Specification, Fault Protection Plan, Fault Monitor Database, Branch Termination Analysis, Autonomous Safing Specification, AC List, Anomaly Report, Key Decision Point Review Material, Technical Reference.

3. Do the IV&V analysts ever generate/brainstorm other hazards/faults/adverse conditions to which the system should be capable of responding?

The responses to this question varied from 'occasionally' to a resounding 'yes', with in-depth analysis being done in modeling scenarios, critically assessing capabilities or behaviors, and running independent dynamic tests. This is one key area where the IV&V Program brings forth great value to its customers, by identifying additional ACs that may impede mission success or inhibit safety. By employing critical thinking and by always questioning, 'Is there something else here that could go wrong?', looking at timing, looking at state transitions, or looking at multiple, concurrent faults, ACs and potential failure scenarios are more fully anticipated and investigated from a risk perspective. This is where the AC Database comes into play, enabling expertise from other projects to be shared in a manner similar to brainstorming, as queries may be made of projects that have similar characteristics. With their process of assurance often taking into account other project examples, the SSO team alone has submitted over a thousand comments that captured missing information (hazards, causes, controls, and verifications) to the great appreciation of the commercial developers.

4. How are these hazards/faults/adverse conditions being utilized during the actual analyses?

The multitude of ways that AC awareness is incorporated into analysis is evidence of the importance of Q2 and Q3 for IV&V. For most projects, an independent list of ACs allows IV&V to provide mission assurance at all phases or for all objectives of analysis: concept, requirements, design, implementation, test, operations and maintenance. Off-nominal conditions are addressed throughout the development lifecycle, ensuring that coverage is complete with respect to safety, security, and dependability. As was described in the IV&V Technical Framework Threads section above, the software requirements/design/implementation must meet the reliability and fault tolerance required by the system, must provide the capability of controlling identified hazards, and must not create hazardous conditions. FM branches across all project domains, and is nearly always in scope for IV&V analysis. SSO support includes insight and oversight activities that focus on crew safety, utilizing hazard analysis activities as the main mechanism for communication of software-related risk. There is, however, wide variance in the usage of ACs for assurance and the need for information and process sharing is evident.

5. Is there a way in which you capture all of the hazard references you come across and store them for use across future projects?

At this point, the majority of the hazard considerations and AC lists for IV&V projects is embedded within IV&V work documents (including reports, spreadsheets, flow diagrams, models, databases) and tools meant for tracking issues or risks. The Enterprise Content Management server maintains configuration management and is organized on a project basis, with visibility limited to analysts working on that particular project. The AC Database provides a common, cross-project repository for ACs and corresponding relationships with capabilities, hazard types, risks, etc. and can be used as a valuable resource for current and future projects. Opening up this information promotes increased understanding, classification, and alignment among projects, as all are working toward a common goal of decreasing risk on critical NASA missions.

6. How do you summarize your assessment of the systems coverage and consideration of hazards/faults/adverse conditions?

IV&V projects' assessments range from 'adequate' to 'very good', based largely on how much experience the Program has with a particular developer. This supports the theory that a void currently exists in the AC knowledge-sharing domain; if best practices are collected along with a searchable database of expected ACs, time savings and increased value will be realized with the assurance provided. Q2 and Q3 analysis will result in a higher level of rigor when capitalizing on the benefits of CBA. Assurance objectives drawn from risk-significant AC awareness will be evident through experience gleaned from the success of other projects. The AC Database facilitates continuous improvement of the SA process.

SARP FM INITIATIVE FOR INTEGRATED ASSURANCE OF FAULT MANAGEMENT

The overriding goal in the SARP FM initiatives is to leverage research results to positively impact the application of SA at NASA IV&V and across the Agency. The transition of products to improved process is occurring with deliberate steps in the provision of the FM Architecture TR Suite¹³ and the AC Database. Coordination of efforts to further develop the AC Database tool that was conceptualized and prototyped with earlier initiatives will provide access to analysts within the IV&V Program and in incremental deployment, across the Agency.

Risk-significant AC awareness for FM assurance entails the assessment of how software systems address susceptibility to failure, identifying and mitigating potential risks to software resiliency, and defining an assurance strategy relevant to Q2 and Q3 with preventative, responsive, and adaptive behavior. The success of this transition from SARP research to the realization of an effective analysis method that integrates a tool designed for comprehensive AC awareness within the current framework of analysis tools will effectively add value to the assurance process, particularly with regard to Q3 consideration. Successful technology transfer will be ensured by partnering to create a tool that supports an adaptive, risk-focused process. User stories have been acquired from stakeholders to determine functionality to be provided by the AC Database, and initial datasets from 15 IV&V projects have been compiled. The prototype is an instantiation of working software that should, with minimal effort, be formalized into an enterprise tool available to accommodate analysts' workflow. As integration occurs, this initiative will be able to provide feedback during deployment for modifications or additional requirements.

In order to proliferate the application and benefits from the research in a logical, prioritized manner, the continuation of this effort is described in four main thrusts:

- **Integration:** Leverage knowledge of the AC Database to inform the developer of use case requirements in order to integrate within the IV&V Program framework
- **Data Population:** Assist projects in further populating the database for more comprehensive query capabilities. Accommodate further categorization of data fields in collaboration with subject matter experts
- **Process Definition:** Draft or adapt current methods for FM analysis using the AC Database for assurance expedience and improved Q3 analysis
- **Dissemination:** Publish products to share knowledge for the advancement of FM assurance across the Agency

PLAN TO FURTHER THE ADVERSE CONDITION DATABASE DEVELOPMENT

Integration

Capitalizing on prior FM SARP initiatives, the integration of the AC Database and FMA TR suite within the Enterprise Architecture framework will be the successful culmination of the past research efforts. With deployment of this tool and the development of associated guidance, a process to "follow the risk" and accordingly scope assurance efforts is availed. NASA OSMA has promoted the need for identification and test coverage of off-nominal conditions for software systems. Understanding what ACs missions may face, and ensuring they are prevented or addressed is the responsibility of the assurance team, which necessarily should have insight into ACs beyond those defined by the project itself. Earlier research efforts defined terminology, categorized data fields, and designed a baseline repository that centralized and compiled a rudimentary listing of ACs and correlated data relevant to NASA missions. Further development advanced the prototype tool into a working database, designed to improve analysis by informing the creation of a comprehensive AC list, tracking ACs, and allowing queries based on project, mission type, domain/component, causal fault, and other key characteristics. The repository has been architected, populated with project data, and an interface established for core functionality, including informational search queries, enter, edit, copy, and batch import of ACs. The user interface was designed to improve efficiency for a typical analyst workflow scenario and the underlying architecture provisions for connectivity with other databases and the TR suite in order to correlate information associated with risks, faults,

failures, hazards, and anomalies. This integration effort will encompass informing the developer in the expanded development and deployment for efficient access by the IV&V and SA community, based on user feedback, ensuring the expected investment return of value.

Data Population

Previous research efforts collected FM and AC data from 15 NASA IV&V projects, each at a different level of fidelity. The project datasets are representative of Deep Space Robotic, Human Spaceflight, Earth Orbiter, Launch Vehicle, and Ground mission software, most often of Classification A. Categorization of AC data and related fields is an ongoing effort, predicated on use cases and adaptive FM analysis processes. Further refinements are proposed with the addition of data and entity relationships from IV&V and SSO projects looking at ACs from a hazard analysis and security perspective for improved query capability. Investigating how a system responds to ACs is an important aspect of hazard analysis and fault management. As the user population increases and AC Database fields grow, the benefits increase primarily as a tool for the SMA community to provide assurance, and secondarily as a mechanism to connect into the knowledge base of related efforts including anomalies, hazards, information assurance, independent testing, and reliability.

Process Definition

The AC Database enables more effective analysis (Q3 in particular) and provides greater test coverage for critical missions, helping projects via a risk-informed dynamic look into FM. Formally codifying expectations and methods for the database will help kick-start its socialization and use among projects. Buy-in from analysts will lead to additional use case development and new features, including consideration of information assurance, potentially advancing overall asset protection of flight software systems. Capitalizing on the integrated framework of the TR and learned expertise in FM analysis and AC use among projects will enable the development of methods that will be applicable to the assurance of a wide variety of FM architectures and varied development approaches.

Dissemination

Innovative strategies for improving SA methods and tools have been gleaned from earlier initiatives. Broadening outreach to socialize research outcomes with what is the state of the practice at several NASA centers is proposed. The publication of research findings and results was tremendously successful with paper presentations at the 31st and 32nd Space Symposia, published on the NASA Engineering Network and NASA Technical Report Server, with benefit to the wider FM community as well as the SMA and IV&V teams. Continuing this approach to disseminate results is proposed, both at technical conferences, as well as on a smaller scale at several NASA centers. The provision of an integrated AC Database and assurance approaches with SMA personnel and FM subject matter experts will provide an environment of technical knowledge exchange and form connections that will improve the state of FM assurance practice.

AC DATABASE ARCHITECTURAL REQUIREMENTS AND DESIGN

A 'User Story Workshop' was held to better understand how the IV&V Program could most effectively utilize meaningful AC data to enhance SA capability. Q3 analysis brings high value to projects from an independent perspective, focusing on areas of significant risk, and assessing the projects' attention to off-nominal scenarios. With this innovation, the objective was to gather requirements to create a database that centralizes a compilation of adverse conditions and related data from IV&V and SSO projects, and to architect the fields such that there may be sharing of data between SA projects for more rigorous analysis. The workshop was a forum to acquire theories of how the Program could use more rigorous AC data and formulate these into 'user stories' to inform the development process. Input was requested from all stakeholders and user groups that recognize that the IV&V

Program as well as the SA community across the Agency will benefit from increased attention to Q3 and the rigorous identification of potential ACs, related mitigations, and verifications for overall CBA.

The format of the 'user story' was:

As a <user type>, I want to <meet this goal>, so that <some value is created>

The resulting concepts became the backlog of features that were developed in an agile-like fashion, with weekly demonstrations of working software for peer review and discussion. A sampling of the brainstormed use cases that drove functionality is illustrated in Exhibit 4.

Designing the relational database was done in an incremental fashion as various tables for the SQL database as well as the fields associated with them were defined and refined. The resulting architecture is shown in Exhibit 5. Complete descriptions of all types of data to be found in the fields along with some examples may be referenced in the AC Database user manual¹⁴. In the next two sections, the primary table 'adversecondition' is described to illustrate the capacity to include multiple fields for data relevant to ACs, and the functionality that is provided in the prototyped AC Database is outlined.

AC Database Primary Table: 'adversecondition'

The 'adversecondition' table is used for the primary information about a particular AC. Each AC is linked to at least one mission from the 'mission' table. The following fields are included:

1. AC_IDNum
 - Unique identifier for the adverse condition
 - Auto-populated by the database. Primary Key of the table
2. AC_Identifier
 - Unique identifier for the adverse condition
 - Made up of the Mission Name (MPCV, SLS, GPM, etc.) followed by a '-' and the AC_IDNum value
 - Example: MPCV-2
 - This value should be auto-populated when an adverse condition is created
 - When an adverse condition is copied to a particular Mission, this value should be auto-populated
3. ACName
 - Adverse Condition Name
 - Text field with a descriptive name for the adverse condition
4. Open_ACName
 - Adverse Condition Name that has been scrubbed of any SBU/ITAR information
 - Text field with a descriptive name for the adverse condition
5. Desired_Reaction_System
 - Text field for the system response for when the event of the adverse condition occurs
6. Desired_Reaction_Software
 - Text field for the software response for when the event of the adverse condition occurs
7. AC_Likelihood
 - Short text field for the risk likelihood of the AC happening, or the severity of the AC, or the risk to focus on
8. AC_Result_Timing
 - Text field for specific timing for the adverse condition as to when it could occur (or not occur)
9. ComponentName
 - Text field for identification of the related component affected by the adverse condition
10. Component_Description
 - Text field for a detailed description of the related component. The ComponentName offers merely identification for the related component

11. SW_Cause_Indicator

- Indicator field to show if an AC is caused by software
 - Ex Y, N

User Type	AC Database Goal	Value Description
Technical Quality & Excellence (TQ&E) Analyst	To be able to become familiar with the contents of the entire database at a high level.	To provide references to my projects.
User	To know how many times an adverse condition has been found across the projects.	To understand how likely the condition is.
Analyst	To have some ideas for what to have the requirement author to consider adding as a requirement or comment something to do if the requirement fails.	Some system requirements state what the system and its components shall successfully do. Sometimes a requirement is written with what shall be done if the requisite action fails (Q2).
IVV Project Manager	To see a list of all adverse conditions that were or are going to be analyzed on my IVV project or on any specified IVV project.	To provide a comprehensive assurance statement.
Project Lead	To be able to find adverse conditions from similar domains and missions.	To plan the analysis activities that will most likely prevent problems from occurring on the mission I'm reviewing.
Analyst	To search the adverse conditions list by Domain for power management conditions.	To assure that batteries can be charged under identified conditions.
TQ&E Analyst	To filter an adverse conditions list on a project or Domain basis.	To determine if an IVV project is adequately covering Q3 conditions within their analysis focus.
Project Analyst	To be able to search for and rely on consistent terminology in AC descriptions, scoring, and classification.	To have confidence that I will see relevant items from other projects and not have to wade through numerous irrelevant ones.
User	To find correlating ACs.	To have a quick reference to similar ACs.
Project Analyst	To be able to search adverse conditions/hazards for software categories.	To find software "caused" AC's. To find software "detected" AC's. To find software "mitigated" AC's.
Analyst	To have adverse conditions created as a hierarchy of related pairs.	To find root cause or expected behavior.
Information Assurance	To understand the context and origin from which an adverse condition was derived.	To help identify similar origins/contexts of interest which may be a "trouble" area.
Quality Assurance / Metrics Team	To figure out what metrics might be useful to capture.	To better capture what might be useful to assist in either helping to capture adverse conditions, etc.
Project Analyst	To search adverse conditions from a centralized location.	To see if my adverse condition is already stored in the database.
Project Analyst	To read/search adverse conditions from a centralized location.	To see if any of the adverse conditions stored in the database are applicable to my project.
TQ&E Analyst	To search for relevant adverse conditions based on Mission type (launch vehicle, earth orbiter, etc.) or Domain (C&DH, GN&C, EPS, etc.).	To support the Assurance Strategy planning of IVV activities or the preparation of heritage reports.
Project Analyst	To search adverse conditions from a centralized location.	To see the proposed methods of resolving this adverse condition.
Project Analyst	To search adverse conditions from a centralized location.	To see if any of the adverse conditions do not have any proposed methods of resolving this adverse condition.
Project Analyst	To see queries related to Mission type (i.e., science, weather, human exploratory, etc.) and to adverse condition type (i.e., hardware, space related, software, security violation, etc.)	To link Mission and adverse condition.
Project Analyst	To search through Ascent (Mission Phase), Dynamic Separation events (Category Groupings).	To gather a set of common causes along with their associated adverse conditions and components.

Exhibit 4: Use cases for desired AC Database functionality

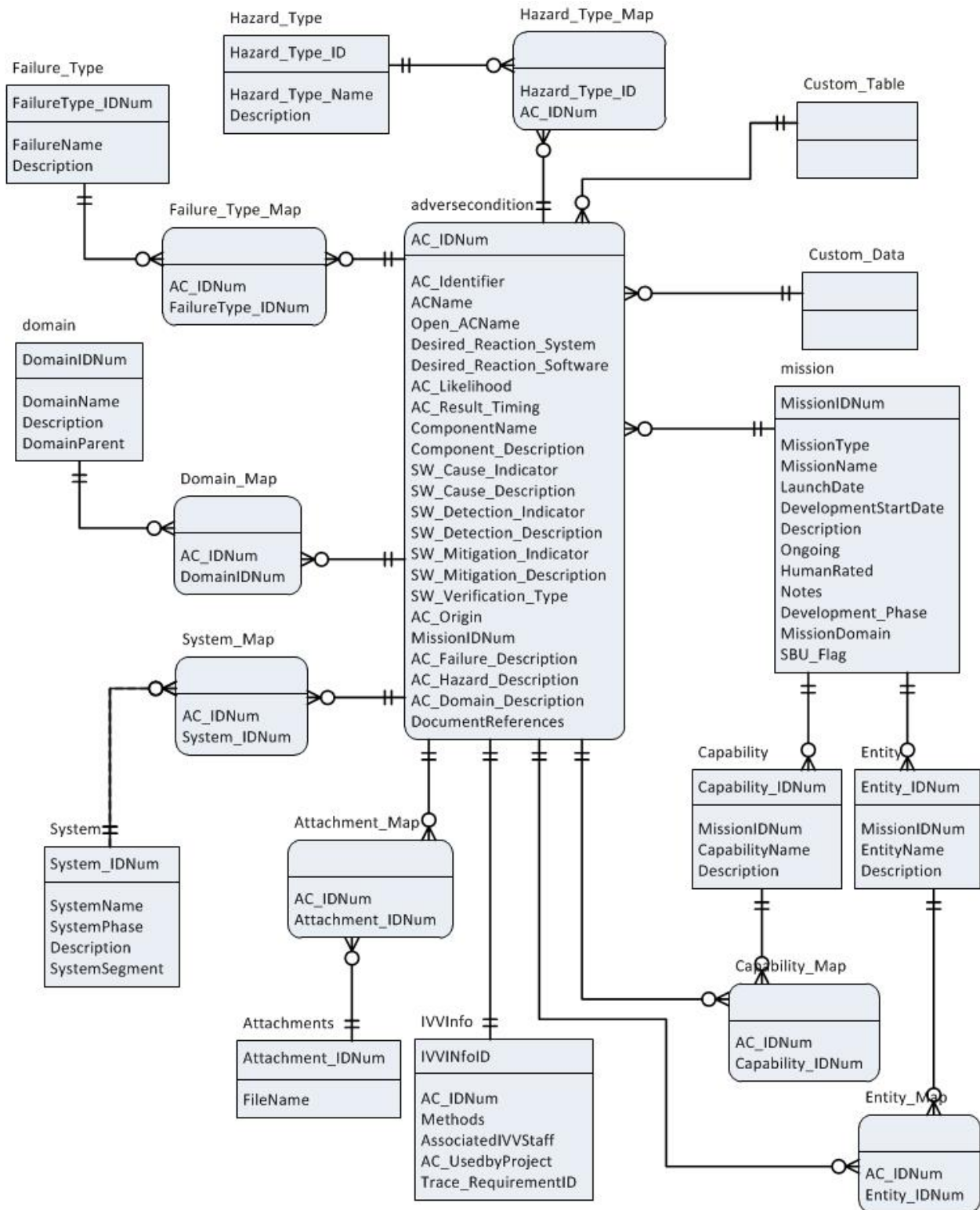


Exhibit 5: AC Database architecture expressed as an Entity-Relationship diagram

12. SW_Cause_Description
 - Text field for a detailed description of the related software cause for the AC. The SW_Cause_Indicator offers merely an indication of whether the AC was caused by software
13. SW_Detection_Indicator
 - Indicator field to show if the AC is detected by software
 - Ex Y, N
14. SW_Detection_Description
 - Text field for a detailed description of the related software detection. The SW_Detection_Indicator offers merely an indication of whether the AC can be detected by software
15. SW_Mitigation_Indicator
 - Indicator field to show if the AC can be mitigated by software
 - Ex Y, N
16. SW_Mitigation_Description
 - Text field for a detailed description of the related software mitigation for the AC. The SW_Mitigation_Indicator offers merely an indication of whether the AC can be detected by software
17. SW_Verification_Type
 - Text field for the related software verification type
18. AC_Origin
 - Text fields for the source or origin for an adverse condition
 - Ex: Document detailing test results
19. MissionIDNum
 - Unique identifier for the Mission
 - Auto-populated by the database
 - Foreign key to link the Adversecondition table and the Mission table
20. AC_Failure_Description
 - Text field for a detailed description of the Failure Type that is particular to an AC. The Failure_Type table offers merely a general category
21. AC_Hazard_Description
 - Text field for a detailed description of the Hazard_Type that is particular to an AC. The Hazard_Type table offers merely a general category
22. AC_Domain_Description
 - Text field for a detailed description of the Domain that is particular to an AC. The Domain table offers merely a general category
23. DocumentReferences
 - Text field for documentation references that are related to an adverse condition

AC Database Import Data Functionality

The AC DB Import Template file format must be used. This file is in Microsoft Excel format.

- Only data on the first tab of the Microsoft Excel spreadsheet will be imported
- The first row of the spreadsheet must have the names as they are given. Do not change, alter, re-order them
 - Column Names: Adverse Condition Name, Open AC Name, Related Capabilities, Related Entities, Mission, Spaceflight Domains, Domain Description, Causal Failures for the AC, Failure Types, Hazard Description, Hazard Types, Spacecraft/Mission Systems Relevant to the AC, Desired System Reaction, Desired Software Reaction, Likelihood, Timing, Software Cause Description, Software Cause Description Indicator, Software Detection Description, Software

Detection Description Indicator, Software Mitigation Description, Software Mitigation Description Indicator, SW Verification Type, AC Origin, Hardware/Software Components Relevant to the AC, Component Description, Document References

The following fields in the template must have values that match data that already exists in the Adverse Condition Database. If the data to be imported does not match existing data in the database, attempted row in the import spreadsheet will error and not be imported into the database. In Developer Mode, new data may be entered to this table to enable the row to be imported.

- Mission
 - If the Mission has not been added, go to the Add/Edit Mission form to enter the information
- Domain
- Failure Type
- Hazard Type
- Spacecraft/Mission System Relevant to the AC
- Related Capabilities
- Related Entities

The following fields must have a Y, N or blank.

- Example: the data may be upper or lower case or blank
- Software Cause Description Indicator
- Software Detection Description Indicator
- Software Mitigation Description Indicator

The following fields must have the delimiter ';' (a semicolon) between multiple entries for the same AC.

- Example: the Domain field on the spreadsheet may have more than one and should have each Domain separated by a single semicolon [Guidance Navigation and Control; Propulsion].
- Related Capabilities
- Related Entities
- Domain
- Hazard Type
- Failure Type
- Spacecraft/Mission System Relevant to the AC


To import data:

- Click 'Import Data' button on the Search Form screen
- Select the Microsoft Excel import data file that follows the import template
- Import routine will then ensue
- At the end of the import, a dialogue box will appear giving the statistics of the import (# of records parsed, # of records imported, # of records failed)
- If errors are encountered, see the ErrorLog.txt file for the types of error and the ImportErrors.xlsx file for the error data
 - The Error files will be located in the same folder as the Microsoft Access database file
 - The date in the ImportErrors.xlsx file may be corrected and then used as the import file. Prior to import, delete the first column of the spreadsheet (IDCOUNT). The file will then be in the proper format for importing

Additional AC Database Functionality

Exhibits 6 through 10 illustrate several screen shots of the Microsoft Access user interface for the AC Database. Usability studies were performed with various user groups during the development.

Search Form


 Select Mission: MPCV [Clear] Select Domain: Electrical Power [Clear] Show as Datasheet [Add/Edit Mission] Add a New AC [Close Database]

Record Count: 12 Select Failure Type: [Clear] Import Data


Select Hazard Type: [Clear] Select System: MPCV Crew Module [Clear]

AC Identifier	AC Name	Open AC Name	Domain Name	Failure Type	Hazard Type	System Name	ComponentName
MPCV-1012	CAUS6: A software-based control error could result in a loss of command and control capability to		Electrical Power		Loss of Command / Control Capability	MPCV Crew Module; MPCV Service Module	CM: Electrical Power System, SM: Electrical Power Subsystem
MPCV-1013	CAUS4: Software Based Control Errors - Software errors could result in premature or inadvertent		Spacecraft Structures and Mechanisms; Electrical Power		Vehicle Structural Damage	MPCV Crew Module; MPCV Service Module	CM: Electrical Power System, SM: Structures; CM: Mechanisms
MPCV-1015	CAUS6: Software Based Control Error 1) Failure of Timeline Management software to properly		Spacecraft Structures and Mechanisms; Pyrotechnics; Wiring; Avionics /		Degraded Vehicle Performance; Premature / Inadvertent Pyrotechnic	MPCV Crew Module; MPCV Service Module	CM: Avionics, CM: Electrical Power System, SM: Structures; CM: Guidance, Navigation
MPCV-1017	CAUS17: Software Based Control Errors - A failure occurring within EDC controller monitoring		Electrical Power		Loss of Crew; Loss of Power to Safety Critical Functions	MPCV Crew Module; MPCV Service Module	CM: Electrical Power System, SM: Electrical Power Subsystem
MPCV-1018	CAUS11: Software-based Control Errors - Software-related causes include: (1) The Electrical Power		Electrical Power		Fire / Explosion; Habitat / Suit Depressurization; Hazardous Gas /	MPCV Crew Module	CM: Electrical Power System
MPCV-1019	CAUS7: Software-Based Control Error - Software commanding errors may cause incorrect control		Avionics / Command and Data Handling; Electrical Power; Environmental		Hazardous Thermal Conditions	MPCV Crew Module; MPCV Service Module	CM: Avionics, CM: Electrical Power System, SM: Environmental
MPCV-1020	CAUS5: Software-Based Control Error - Improper software commanding of EDCSS components		Avionics / Command and Data Handling; Electrical Power; Environmental		Habitat / Suit Depressurization; Loss of Command / Control	MPCV Crew Module	CM: Avionics, CM: Electrical Power System, SM: Environmental
MPCV-1022	CAUS9: Software-Based Control Error - Software errors may cause generation of incorrect commands		Spacecraft Separation; Pyrotechnics; Wiring; Avionics / Command and		Loss of Command / Control Capability; Loss of Vehicle	MPCV Crew Module; MPCV Launch Abort System	CM: Avionics, CM: Electrical Power System, SM: Guidance, Navigation
MPCV-1043	the vehicle loses all power		Electrical Power		Loss of Command / Control Capability; Loss of Crew	MPCV Crew Module	CM
MPCV-3869	CAUS4: Software-Based Control Error - Software commanding errors may cause incorrect control		Avionics / Command and Data Handling; Electrical Power; Environmental		Crew Incapacitation, Illness, or Injury; Loss of Command / Control	MPCV Crew Module	CM: Avionics, CM: Electrical Power System, SM: Environmental
MPCV-3870	CAUS9: Software-Based Control Error - Software commanding errors may cause incorrect control		Avionics / Command and Data Handling; Electrical Power; Environmental		Crew Incapacitation, Illness, or Injury; Hazardous Gas /	MPCV Crew Module	CM: Avionics, CM: Electrical Power System, SM: Environmental
MPCV-3871	CAUS6: Software-Based Control Error - Software commanding errors may cause incorrect control		Avionics / Command and Data Handling; Electrical Power; Environmental		Crew Incapacitation, Illness, or Injury; Loss of Crew	MPCV Crew Module	CM: Avionics, CM: Electrical Power System, SM: Environmental

Exhibit 6: AC Database Search Form with full query functionality in terms of mission, domain, failure, hazard, etc.

Exhibit 7: AC Database Detail Form for consolidating AC-specific data and relationships to other tables

Exhibit 8: Cloning an AC from one mission to another is accomplished with functionality to duplicate AC records



Mission Form

Add/Edit Mission Data

Mission Name:

Mission Description:
The Orion Multi-Purpose Crew Vehicle (MPCV) is a spacecraft intended to carry a crew of four astronauts to destinations at or beyond low Earth Orbit (LEO). Current under development by NASA for launch on the Space Launch System (SLS).

Mission Notes:

Launch Date: Development Start Date:

Ongoing: Mission Domain:

Human Rated: Data Marked as SBU (Y or N):

Mission Type:

Capabilities:

Capability Name	Description
Abort	Provides abort capabilities while systems are on the pad, during launch and ascent and on-orbit operations
Ascent Environment	Capability to withstand natural and induced environments experienced during ascent mission phases.
Attitude Control	Provide attitude control.
Auxiliary Comm	Auxiliary Voice Communication link capabilities.
Early Mission Termination	Provides early mission return capabilities while systems are performing in-orbit operations.
ECLSS and ECS Services	Maintain habitable atmosphere, partial pressure, humidity, temp control, trace contaminant, hazard detect
EDL and Recovery Environment	Capability to withstand natural and induced environments experienced during applicable recovery phases.
Entry Descent and Landing	Entry, Descent, and Landing Capabilities associated with MPCV and Mission Systems.
Fueling and Conditioning	Includes propellant loading storage and pressurizations capabilities.
Ground Processing	Provide ground operations capabilities for off-line processing, integrated operations, pad and launch opera
Guidance and Navigation	Determine state vector, targeting, and control functions.


Record: 1 of 30 No Filter Search

Entities:

Entity Name	Description
BEL	Backup Engage Logic
BFS	Backup Flight Software
CDH	Command & Data Handling
CFSW	Common Flight Software
CMT	Communicate & Track
CORE	Core Flight Software
DACF	Display and Control Formats
DACM	Display and Control Management
ECLS	Environmental Control & Life Support
EPS	Electrical Power Systems
GNCP	Guidance, Navigation, Control, and Propulsion

Exhibit 9: AC Database Mission Form for describing missions along with their capabilities and software entities

Add New AC Form



Save Record
Cancel Changes

Mission AC Identifier ACName

AC Data AC Likelihood

AC Origin Document References

Open AC Name AC Domain Description

Component Name Component Description

AC Failure Description

AC Hazard Description

Exhibit 10: Adding new ACs is accomplished with this form for an individual AC or with an import template and script for multiple ACs and their associated fields

CONCLUSION

The strengthening of SA strategies by renewed emphasis on risk-significant AC awareness brings potential for far-reaching impact across the Agency. The complexity of FM and the importance of effectively providing assurance that NASA safety- and mission-critical software will operate reliably, safely, and securely demands rigorous attention to methodologies applied. NASA's IV&V Program is in a position to leverage technical expertise and broad project experience to improve software assurance strategies. In this arena, IV&V technical standards and a thread approach to performing analysis throughout the software development lifecycle has been documented as a solid approach to CBA. The integrated role of hazard analysis as it supports the "follow the risk" approach enables assurance strategies aimed at critical FM systems necessary for mission success. The current SARP initiative furthering the development of the AC Database is illustrated with design details and rationale for functionality that has been stakeholder-defined and implemented in an incremental fashion. This initiative brings forth value by assessing how software systems address susceptibility to failure, identifying and mitigating potential risks to software resiliency, and defining assurance strategies particularly focused on preventative, responsive, and adaptive behavior in the complex environments in which NASA systems are deployed. As research progresses, the AC Database and supporting assurance methodologies seek to:

- Improve capability-based assurance from the provision of more comprehensive data
- Provide more rigorous IV&V analysis from identification of off-nominal scenarios
- Increase efficiency of analyst workflow and enable broader test coverage
- Allow greater focus on FM and project areas of vulnerability or significant risk
- Deliver support for reliability and resiliency for critical system safety

Continual improvement on SMA is the goal, affording analysts deeper understanding of FM SA strategies, methods, and tools in order to be efficient in providing FM assurance, particularly with regard to addressing risk-significant ACs. Collaboration and infusion of results will continue as the AC Database is deployed to a wider audience and methods are enhanced to take advantage of the tool as a dynamic, living resource tailored to improve workflow in the ultimate goal of reducing risk and increasing confidence in NASA mission success.

¹ Fitz, R., Whitman, G. (2016, Sept. 30). *FM Architectures Technical Reference Suite*. Retrieved from https://nen.nasa.gov/web/sarp/documents?p_p_auth=eGV2k8I2&p_p_id=20&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&_20_struts_action=%2Fdocument_library%2Fview&_20_folderId=1445885&_20_entryStart=0&_20_entryEnd=20&_20_folderStart=0&_20_folderEnd=20&_20_displayStyle=list&_20_viewEntries=1&_20_viewFolders=1&_20_action=browseFolder&_20_expandFolder=0.

² Savarino, S., Fitz, R., Fesq, L., & Whitman, G. (2015, Apr. 17). *Fault Management Architectures and the Challenges of Providing Software Assurance*. Proceedings of 31st Space Symposium. Retrieved from <https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20150005781.pdf>.

³ Fitz, R., Whitman, G. (2016, Apr. 11). *Technical Reference Suite Addressing Challenges of Providing Assurance for Fault Management Architectural Design*. Proceedings of 32nd Space Symposium. Retrieved from <https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20160005440.pdf>.

⁴ *Fault Management Handbook*. (2012, Apr. 2). Draft 2. National Aeronautics and Space Administration. Retrieved from https://www.nasa.gov/pdf/636372main_NASA-HDBK-1002_Draft.pdf.

⁵ Asbury, Michael. (2017, Mar. 14). *NASA IV&V Facility*. National Aeronautics and Space Administration. Retrieved from <https://www.nasa.gov/centers/ivv/home/index.html>.

⁶ *Independent Verification and Validation Technical Framework*. (2016, Feb. 26). IVV 09-1 Version P. National Aeronautics and Space Administration. Retrieved from https://www.nasa.gov/sites/default/files/atoms/files/ivv_09-1_-_ver_p.pdf.

⁷ Shaffer, T. (2016, Oct. 5). *Capability Development: Agile*. Retrieved from NASA IV&V website with limited access.

⁸ Wetherholt, M. (2016, Jul. 29). *Final Report of the NASA Office of Safety and Mission Assurance Agile Benchmarking Team*. Retrieved from <https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20160011219.pdf>.

⁹ Turner, D. (2017, Jan. 1). *Capability Development: Planning and Scoping*. Retrieved from NASA IV&V website with limited access.

¹⁰ Theeke, P. (2016, Nov. 30). *The Impact of CBA on Planning, Execution, and Reporting of IV&V*. Retrieved from NASA IV&V Enterprise Content Management with limited access.

¹¹ Whitman, G. (2017, Mar. 7). *CBA Planning and Execution Approach*. Retrieved from NASA IV&V website with limited access.

¹² Gilbert, H. (2016, Jul. 19). *Hazard Analysis Among IV&V Projects*. Retrieved from NASA IV&V website with limited access.

¹³ Fitz, R., Whitman, G. (2016, Sept. 30). *FM Architectures Technical Reference Suite*. Retrieved from https://nen.nasa.gov/web/sarp/documents?p_p_auth=eGV2k8I2&p_p_id=20&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&_20_struts_action=%2Fdocument_library%2Fview&_20_folderId=1445885&_20_entryStart=0&_20_entryEnd=20&_20_folderStart=0&_20_folderEnd=20&_20_displayStyle=list&_20_viewEntries=1&_20_viewFolders=1&_20_action=browseFolder&_20_expandFolder=0.

¹⁴ Fitz, R., Stichweh, R., Whitman, G. (2016, Sept. 30). *SARP Initiative FY16 Adverse Conditions Database User Manual*. Retrieved from NASA IV&V Enterprise Content Management with limited access.