Introduction

The IV&V program identified a need to address software-centric safety analysis and assess the quality of software safety engineering early in the development of a system of systems to ensure the software manages safety requirements while not introducing system hazards. IV&V has created a process which documents how a mission specific dependability and safety case is transformed to a generic dependability and safety case which can be reused for any type of space mission with an emphasis on software fault conditions and can also be applied to any industry.

Phase I - the specific model (completed)

A safety case study was conducted for a science satellite mission. Requirements validation and a system reference model was developed. Figure 1 portrays the IV&V analysis process created and followed. Figure 2 is a high-level depiction of the safety case which maps high-level safety requirements and lower-level safety requirements.

Figure 1 - IV&V Analysis Process

Safety case analysis

Safety case analysis

Figure 2 - High-Level Safety Case

Figure 3 is an example of an activity diagram which depicts a high-level overview of fault management for a safe-hold event for a specific science mission. Each subsystem is comprised of specific devices in which specific failures would result in a safe-hold event.

Mission specific fault management

Fault conditions for the Phase I science mission were device dependent. When comparing space missions to each other, it was immediately obvious that all missions share many of the same characteristics regardless of the mission’s purpose.

Instead of focusing on the specific subsystem device with a specific fault, the focus will be on the functionality of a specific subsystem (Figure 4) with the fault conditions captured at a high and generic level to more easily be reused across other future missions.

Focus on functionality - not devices

Figure 4 - Change the focus

Look for common functionality

Figure 5 - Identifying common functionality

Reusable fault identification process for any mission

Figure 6 - Identifying common functionality

Figure 7 - Activity diagram for generic fault management

Future direction - fault management tool

Develop a fault management database containing system/subsystem faults maintained by IV&V with support from satellite developers.

Dependability and safety through tools

Fault Management Database

Benefits to IV&V and developer

1. Enhanced validation against a list of known faults
2. Improved quality of analysis
3. Improved quality of IDMs
4. Improved quality of safety data
5. Enhanced communication with the developer
6. Quickier identification of missing requirements and faults
7. Enhanced mission dependability and safety
8. Improved overall mission success

Applying the process to any industry

Your organization can apply similar fault management techniques even if your projects do not have the system of systems complexity (Figure 8). Replace the space mission examples with your system information. Decompose the system into subsystems (Figure 4) with a focus on subsystem functionality. Don’t think spaceflight - think your business (Figure 9).

Industry applications

Figure 9 - Thinking about the same thing in a different way

Figure 8 - Applying Phase II to your project

Feature image: A high-level overview of fault management for a safe-hold event.

Judy Murphy, Judy.L.Murphy@ivv.nasa.gov, MPL
Steve Driskell, Stephen.B.Driskell@ivv.nasa.gov, TASC
Marcus Fisher, Marcus.S.Fisher@nasa.gov

NASA Independent Verification and Validation Facility

Fairmont, West Virginia