Assurance Case Patterns for Flight Software

Alex Ellis
Elisabeth Nguyen
Software Systems Engineering Department
The Aerospace Corporation

Workshop on Spacecraft Flight Software
8-10 December 2010
alex.ellis@aero.org

© The Aerospace Corporation 2010
Outline

• Mission Assurance at Present
• Assurance Cases Overview
• Goal Structuring Notation
• Assurance Lifecycle
• Assurance Case Pattern Excerpt – Safe Mode
• Summary
Mission Assurance (MA) at Present

• Many types of MA activities
  – Analyses
    • Failure Mode and Effects Analysis (FMEA), Functional Failure Analysis (FFA)
  – Tests
    • Unit, Formal Qualification Test (FQT)
  – Processes /standards
    • Software Development Plan (SDP), Quality Assurance (QA), SEI CMMI

• All are important contributors to ensuring mission success
  – Mix of the above driven by the individual evaluator’s engineering judgment and competence
  – Little assistance from rigorous methodology

• What is sufficient?
  – Necessary analyses may not be identified
  – Interplays between subsystems may not be considered
  – Sparse record of what was actually looked at
  – Little visibility into evaluator’s thought process

Mission Assurance is the full life-cycle engineering process to identify and mitigate design, production, test, and field support deficiencies of mission success. (Wikipedia)
Assurance Cases

• Based on Safety Cases commonly used in the United Kingdom
  – Adopted as a UK military aircraft platform requirement in 2002
  – MoD Defence Standard (Def-Stan) 00-56
• University of York and Adelard (UK) major research contributors
• Basic Approach:
  1. Agreement on what needs to be assured
  2. Construction of the assurance argument
  3. Selection of evidence to satisfy argument
• We use graphical language called Goal Structuring Notation
  • With our own enhancements

An Assurance Case is a structured argument, supported by a body of evidence, that provides a compelling, comprehensible and valid case that a system operates correctly for a given application in a given environment. [Based on Def-Stan 00-56 9.1]
Goal Structuring Notation (GSN)
Assurance Lifecycle

• Assurance cases are developed at multiple stages of the lifecycle
  – *In the requirements and design phase* assurance cases identify missing analyses, requirements, or architectural/design elements
  – *In the integration and verification phase* assurance cases provide verification that actual product will function as expected
Assurance Case Pattern Excerpt – Safe Mode

• Critical function that must work right
• Focus in this presentation is on the structure of the Assurance Case pattern, with emphasis on the computing platform’s role
  • First 4 excerpt slides will show the overall case structure and how the computing platform fits into the larger assurance picture
  • Last 2 excerpt slides show a pattern for assuring the platform
• Extract from a much larger Assurance Case
• Applied on USAF missions
• On-going IR&D activities to develop patterns and processes for using them
Safe Mode (Top Level)

CAssuranceReqs
(System) mission assurance requirements

CMissionPhase
(System) defined mission phases

CMissionPhaseExamples
Phases may include launch, early orbit, vehicle checkout, normal operations, disposal

GT topLevel
(System) safe mode will protect the vehicle with sufficient confidence

ArgMissionPhase
Argument over each mission phase

JAllMissionPhases
Safe Mode should cover all mission phases

GMissionPhase
(System) safe mode will protect the vehicle with sufficient confidence during (Phase P)

Number of mission phases

GSimilarToOtherPhase
(System) safe mode is substantially the same in (Phase P) as it is in (Phase Q)

GSafingReqs
(System) safe mode will satisfy major safing requirements with sufficient confidence during (Phase P)

At least 1 of 2

CMajorSafingReqs
High level goals of safing: safing can be entered; safing will carry out its function to protect the vehicle; safing will enable the vehicle to be commanded to resolve the problem and resume the mission. These requirements are common across vehicles but may not be documented for a particular vehicle at such a high level.

(System) will enter safe mode if a critical subsystem is endangered, with sufficient confidence

SM—Entry

Ground commanding can cause safe mode exit, with sufficient confidence

SM—Exit
Safe Mode – Entry

(System) will enter safe mode if a critical subsystem is endangered, with sufficient confidence

Fault responses to noncritical threats will not prevent safe mode entry when necessary

(System) will detect when a critical subsystem is endangered, with sufficient confidence

Credible failures that could prompt entry into safe mode have been identified

Safering hardware and software will effect safe mode entry if a critical subsystem is endangered, with sufficient confidence

All critical subsystems will be able to carry out their safe mode entry capability, even in the presence of unforeseen failures

Entry mechanisms possess no single point failure

Critical subsystems are: power; thermal; altitude; communications; structure. Communications is treated elsewhere as a separate branch. Payload was added because payload protection may also be necessary for successful fault management.

Argument over each critical subsystem:

The power subsystem will carry out its safe mode entry capability, even in the presence of unforeseen failures

Entry—EPS →

The thermal subsystem will carry out its safe mode entry capability, even in the presence of unforeseen failures

Entry—Thermal →

The attitude subsystem will carry out its safe mode entry capability, even in the presence of unforeseen failures

Entry—Attitude →

The payload will carry out its safe mode entry capability, even in the presence of unforeseen failures

Entry—Payload →
Safe Mode – Entry – Attitude

The attitude subsystem will carry out its safe mode entry capability, even in the presence of unforeseen failures

The vehicle will be able to determine its attitude w.r.t. the sun, even in the presence of unforeseen failures

The vehicle will be able to determine the rate at which its attitude is changing, even in the presence of unforeseen failures

The vehicle will be able to control its attitude, even in the presence of unforeseen failures

The vehicle will prevent excessive thruster firing, even in the presence of unforeseen failures

The vehicle will prevent structural damage due to excessive attitude change rates, even in the presence of unforeseen failures

Computing platform will carry out Attitude functions, even in the presence of unforeseen failures

Entry—Computer →
Safe Mode – Entry – Attitude – Platform (1)

Computing platform will carry out Attitude functions, even in the presence of unforeseen failures

- Hung board is recoverable
  - SBC design, e.g., watchdogs

- Failure or switchover to redundant SBC is acceptably mitigated
  - FSW determines failed components
  - FSW comes up in correct mission state (operational, transfer orbit, mid-maneuver, safe mode, etc.)
  - No ping-ponging
  - Does not switch over to failed or unusable backup
  - FSW determines whether spacecraft was in the middle of critical activity at time of switchover, and takes appropriate action
  - Bus connectivity is restored to SBC and all remote devices

- Hung or unresponsive tasks are detected and recovered from
  - task design
Safe Mode – Entry – Attitude – Platform (2)

Computing platform will carry out Attitude functions, even in the presence of foreseen failures

Data bus failure is acceptably mitigated

Bus failure will be detected

Independent hardware is available

Hazards to bus switchover are acceptably mitigated

Ground connectivity is restored following recovery from bus failure

Bus switch can be accomplished, even in the presence of anticipated failures

FSW can recover from bus failure

Remote devices react appropriately to bus failure

Independent bus is available

Independent bus connection is available
Summary

• Assurance Cases synthesize mission assurance evidence and add rigor to mission assurance throughout a program lifecycle
• Excellent for the rigorous validation of critical functions
  – Safe Mode
  – Fault Management
  – Safety-related properties
  – Security-related properties
• We developed patterns for fragments of spacecraft Safe Mode assurance
  – Can be used across different vehicles to support MA activities

Thank you for your attention!