Model Based Mission Assurance: Emerging Opportunities for Robotic Systems

Tony DiVenti, Branch Head – Reliability and Risk Analysis (371), NASA Goddard Space Flight Center

John W. Evans, Office of Safety and Mission Assurance, NASA HQ

The emergence of Model Based Systems Engineering (MBSE) in a Model Based Engineering framework has created new opportunities to improve effectiveness and efficiencies across the assurance functions. The MBSE environment supports not only system architecture development, but provides for support of Systems Safety, Reliability and Risk Analysis concurrently in the same framework. Linking to detailed design will further improve assurance capabilities to support failures avoidance and mitigation in flight systems. This also is leading new assurance functions including model assurance and management of uncertainty in the modeling environment. Further, the assurance cases, a structured hierarchal argument or model, are emerging as a basis for supporting a comprehensive viewpoint in which to support Model Based Mission Assurance (MBMA).

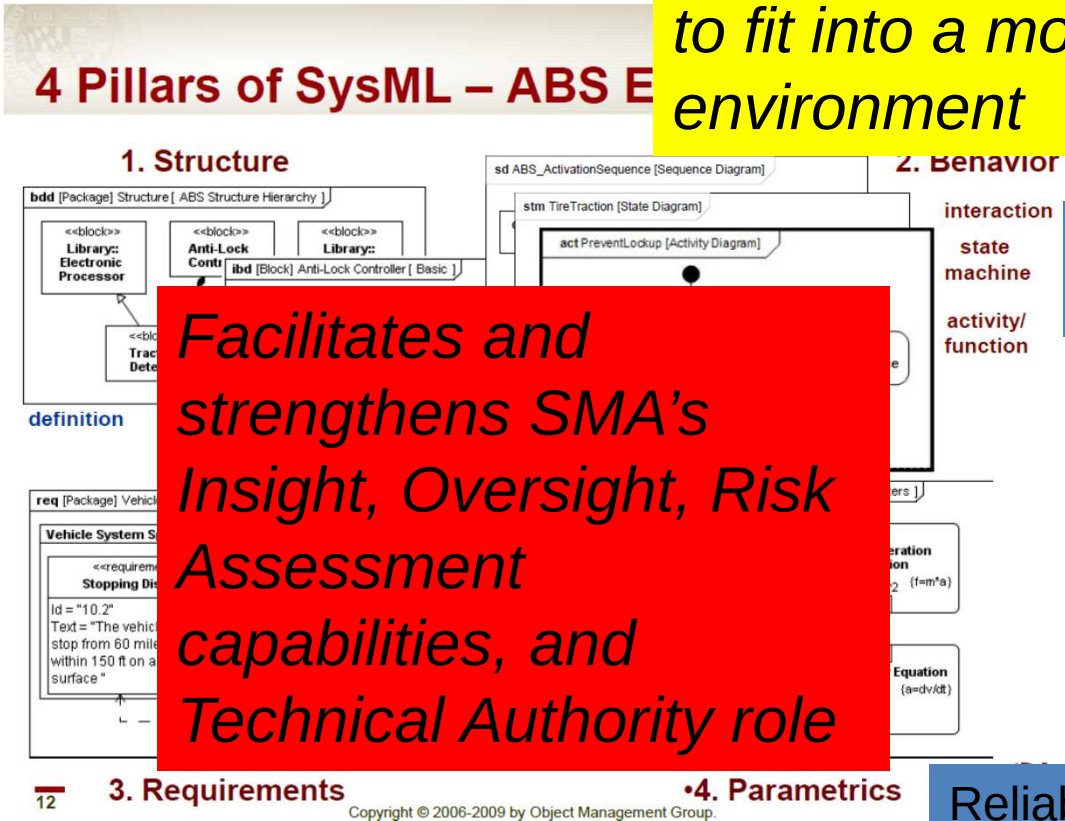
Model Based Mission Assurance

Tony DiVenti, Branch Head – Reliability and Risk Analysis (Code 371), Goddard Space Flight Center

John W. Evans, Office of Safety and Mission Assurance, NASA HQ

MBSE – How does SMA fit in

Assurance products modified to fit into a model based environment



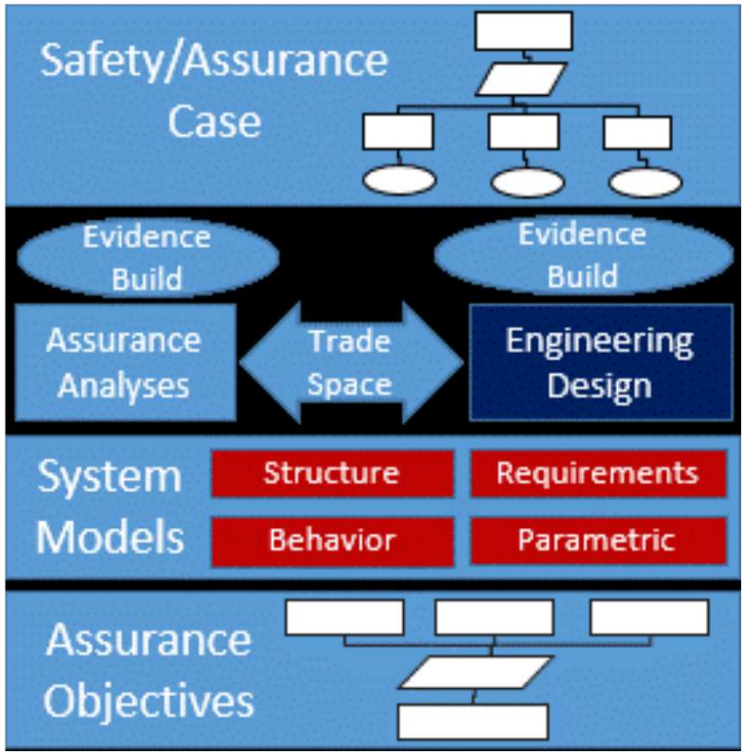
Facilitates and strengthens SMA's Insight, Oversight, Risk Assessment capabilities, and Technical Authority role

FMEA & Hazard Analysis

Reliability Models

Safety Requirements and Quality Demands

MBMA – Model Based Mission Assurance

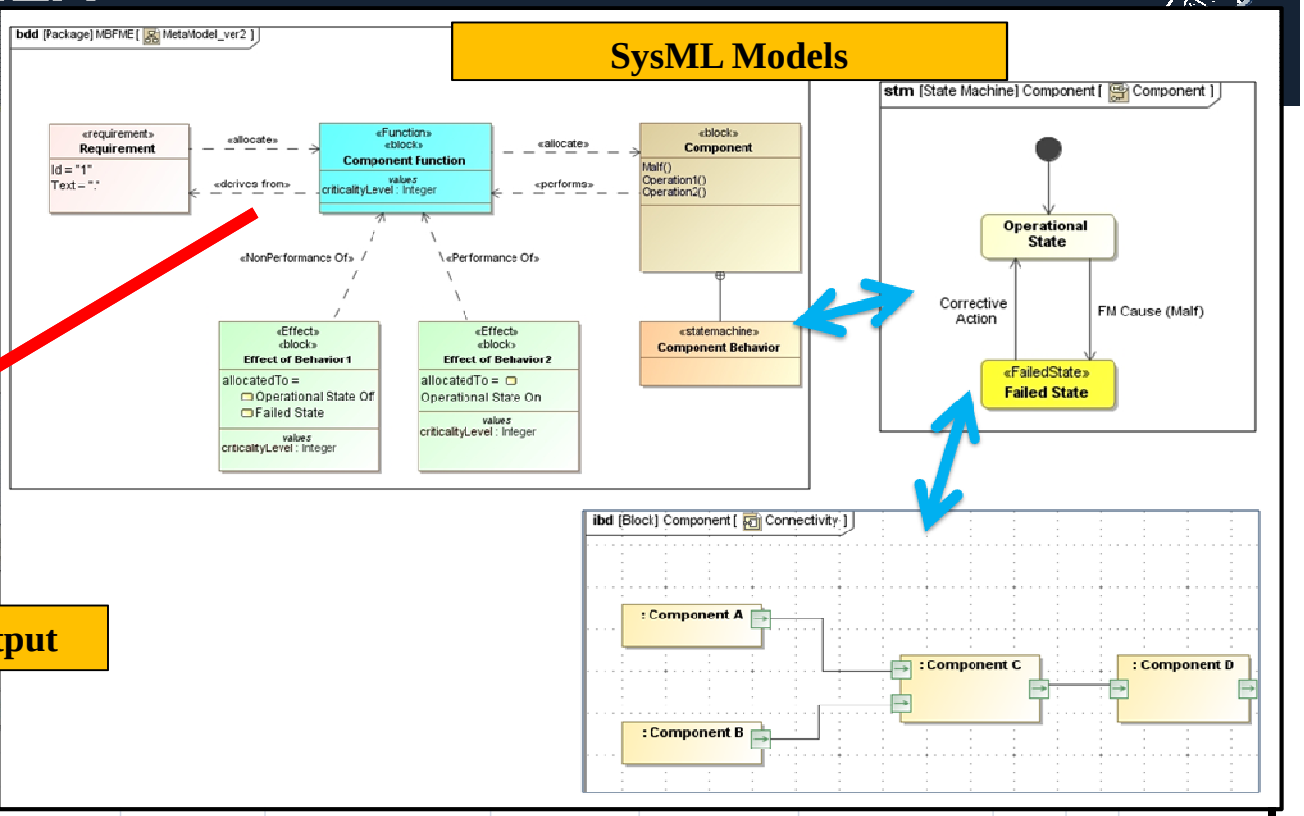


Example - MBSE FMEA

Courtesy Lui Wang
Johnson Space Center

Magic Draw Plug-Ins

SysML Models



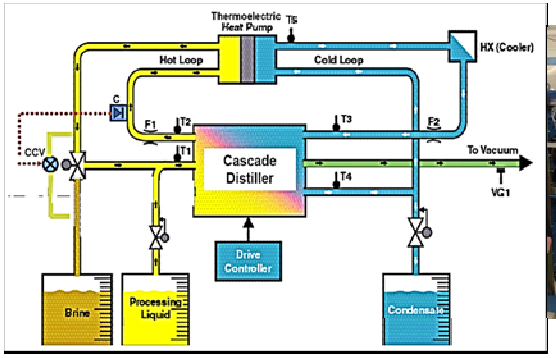
FMECA Output

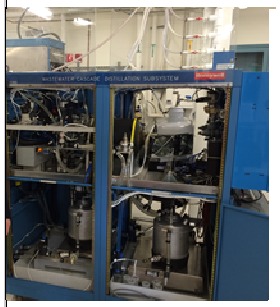
Failure Modes and Effects Criticality Ana

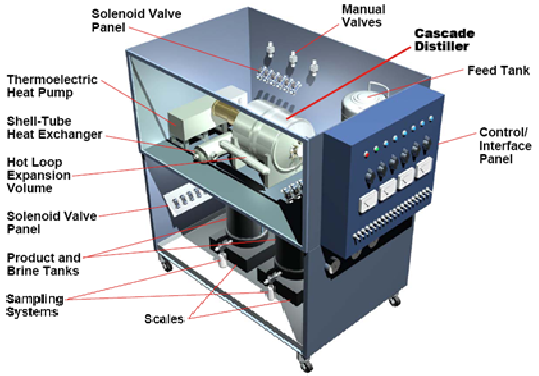
Project Name:	Fan in the Can SysML Model

System	Subsystem	LRU/ Assembly Type	LRU/ Assembly Name	Item Function	Potential Failure Mode	Effect				CRIT LEVEL	SEV	Potential Causes
						Immediate Failure Effect	End Effect	Number of Independent	Other Independent Failures			
FaninCan	ECLSS	CCAA	CCAA1	CCAA1 Ciruculates Air	Failed Off	Loss of CCAA1 air Circultation	Loss of CCAA1 air Circultation	1		1		Internal Malf
FaninCan	Power Subsystem	MBSU	MBSU1	MBSU_Distribute_Power	Failed Off	Loss_of_Mbsu1_output_power	Loss of CCAA1 air Circultation	2	MBSU2 Failed Off	1		insertInternalMalf
FaninCan	Power Subsystem	MBSU	MBSU1	MBSU_Distribute_Power	Failed On	MBSU1_Ouput_Power_On						insertInternal2Malf
FaninCan	Power Subsystem	MBSU	MBSU1	MBSU_Distribute_Power	Failed On	Loss_of_ability_to_manage_MBSU1_loads						insertInternal2Malf
FaninCan	Power Subsystem	MBSU	MBSU2	MBSU_Distribute_Power	Failed Off	Loss_of_Mbsu2_output_power	Loss of CCAA1 air Circultation	2	MBSU1 Failed Off	1		insertInternalMalf
FaninCan	Power Subsystem	MBSU	MBSU2	MBSU_Distribute_Power	Failed On	MBSU2_Ouput_Power_On						insertInternal2Malf
FaninCan	Power Subsystem	MBSU	MBSU2	MBSU_Distribute_Power	Failed On	Loss_of_ability_to_manage_MBSU2_loads						insertInternal2Malf
FaninCan	Power Subsystem	PDU	PDU1	PDU_Distribute_Power	Failed Off	Loss_of_PDU_output_power	Loss of CCAA1 air Circultation	1		1		insertInternalMalf
FaninCan	Power Subsystem	PDU	PDU1	PDU_Distribute_Power	Failed On	PDU_Output_Power_On						insertInternal2Malf

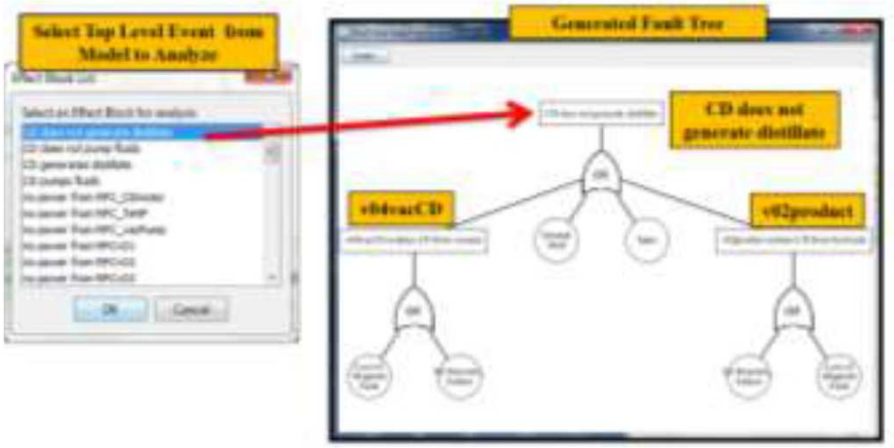
Example - CDS System Fault Tree





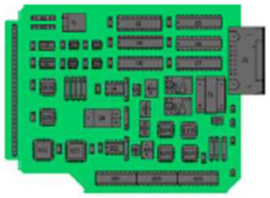


Courtesy Lui Wang
Johnson Space Center



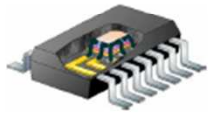
FY16 Planned Collaboration – UMD Center for Advanced Life Cycle Engineering (CALCE)

Simulation Assisted Reliability Assessment (SARA®) Software

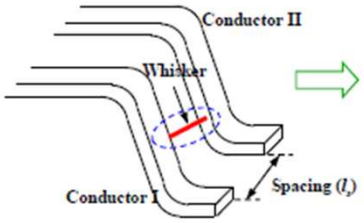


calcePWA
Circuit Card Assemblies

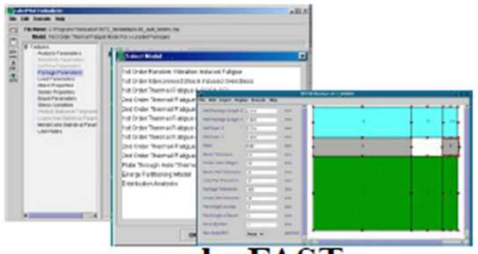
Thermal Analysis
Vibrational Analysis
Shock Analysis
Failure Analysis



calceEP
Device andPackage
Failure Analysis



calceTinWhisker FailureRiskCalculator

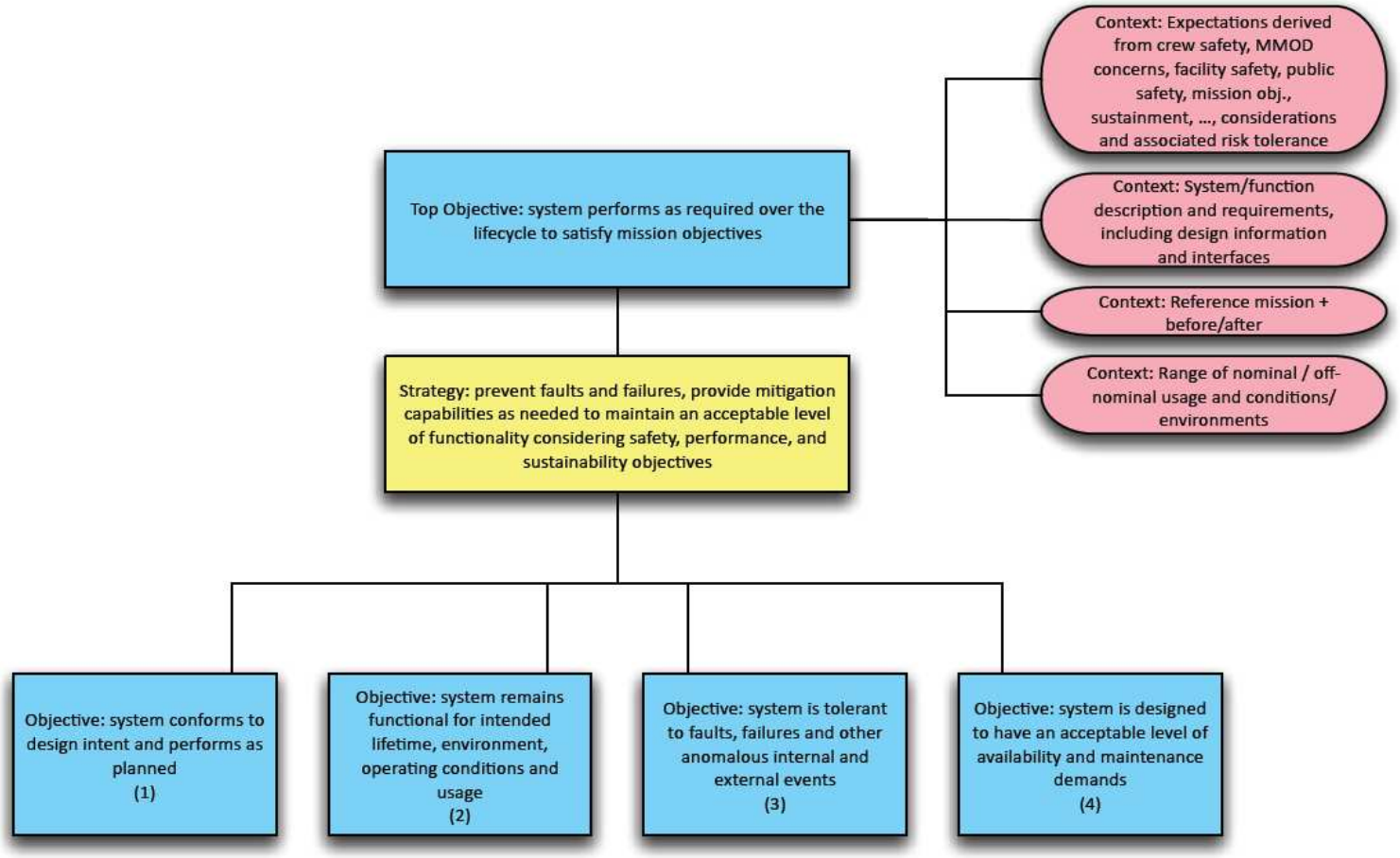


calceFAST
Failure Assessment
Software Toolkit

- GSFC has access to CALCE SARA® software to perform in depth parts reliability analysis
- A system model that links to SARA® could produce more accurate reliability analyses
- MBSE provides a framework to support this activity

Objectives Based Assurance

R&M Objectives Structure – Top-Level

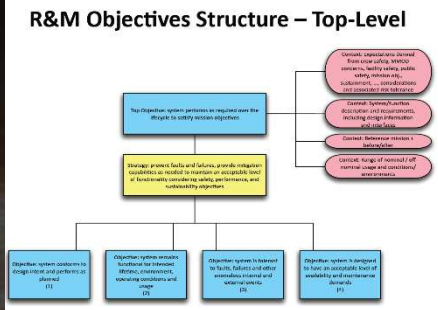


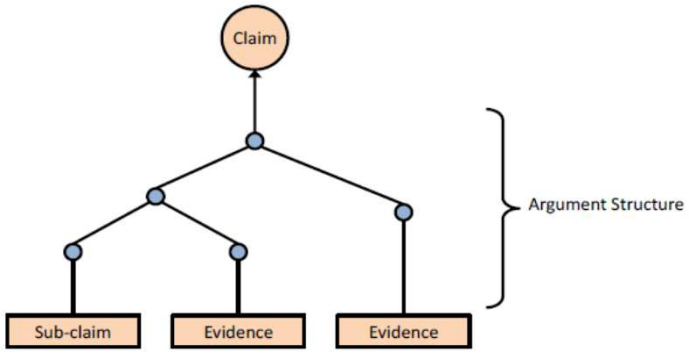
Laying the Foundation

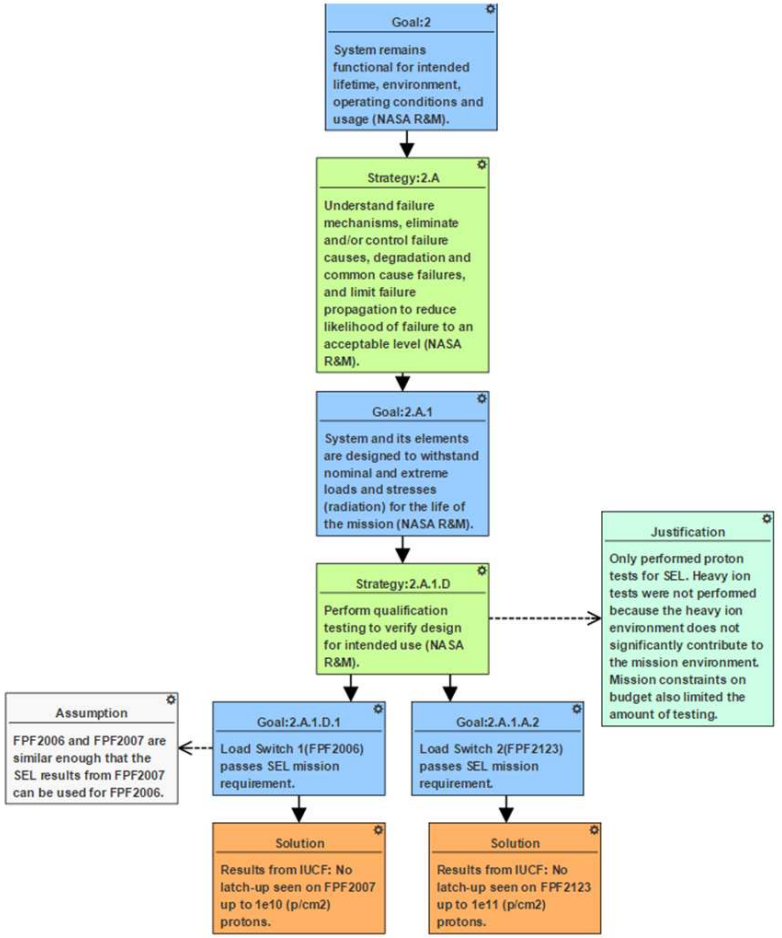
- Logically decompose top-level R&M objective
  - Use elements of the Goal Structuring Notation
  - Structure shows why strategies are to be applied

- Structure forms basis for a proposed R&M standard
  - Specifies the technical considerations to be addressed by projects
  - Forms basis for evaluation of plans, design, and assurance products

Assurance Case







Summary

- MBSE provides an unprecedented opportunity to integrate SMA and Engineering Analysis concurrently as part of a common modeling framework.
- MBMA, part of the MBSE environment, facilitates and enhances SMA's analytical and risk assessment capabilities.
- MBSE and MBMA fully supports GSFC's Risk Based SMA Approach and the Agency's R&M Objectives Structure and as part of a larger Safety/Assurance Case.