Identifying where Mission Assurance can benefit from Model Based Systems Engineering

Martin S. Feather, Steven L. Cornford
John Evans (NASA)

Jet Propulsion Laboratory
California Institute of Technology

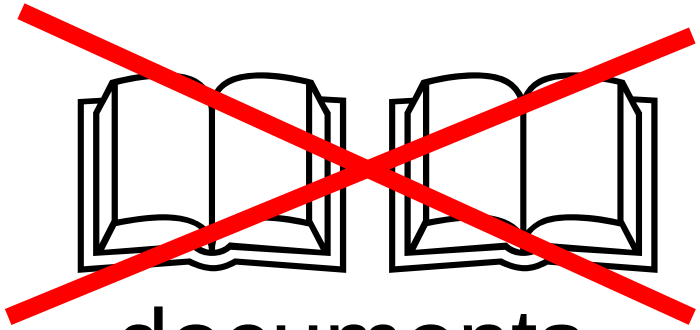
© 2016 California Institute of Technology. Government sponsorship acknowledged.

Model Based Systems Engineering benefits

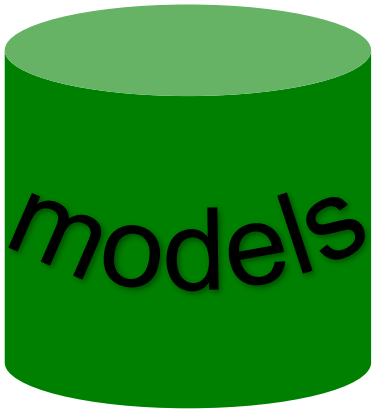
- **MBSE benefits often cited include:**
  - **Single authoritative source of truth**
  - **Unambiguous definition of terms and relationships**
  - **Ability to explore the engineering data**
  - **…**

- **How can MBSE help Mission Assurance?**

More timely and accurate assurance products



documents



Assurance Products
e.g., Fault Trees

Identifying where MBSE helps Assurance

Assurance Objectives

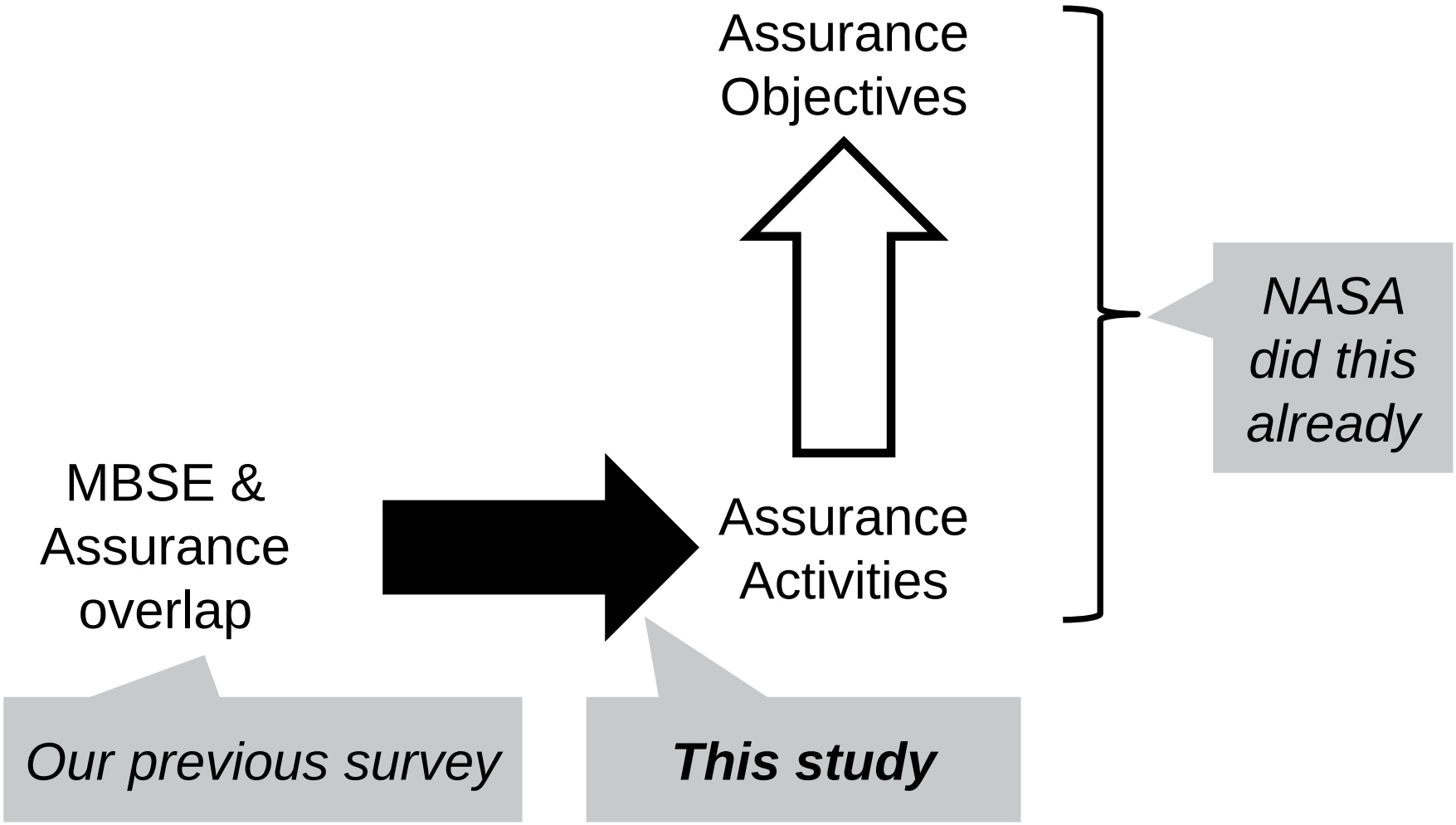
Assurance Activities

NASA did this already

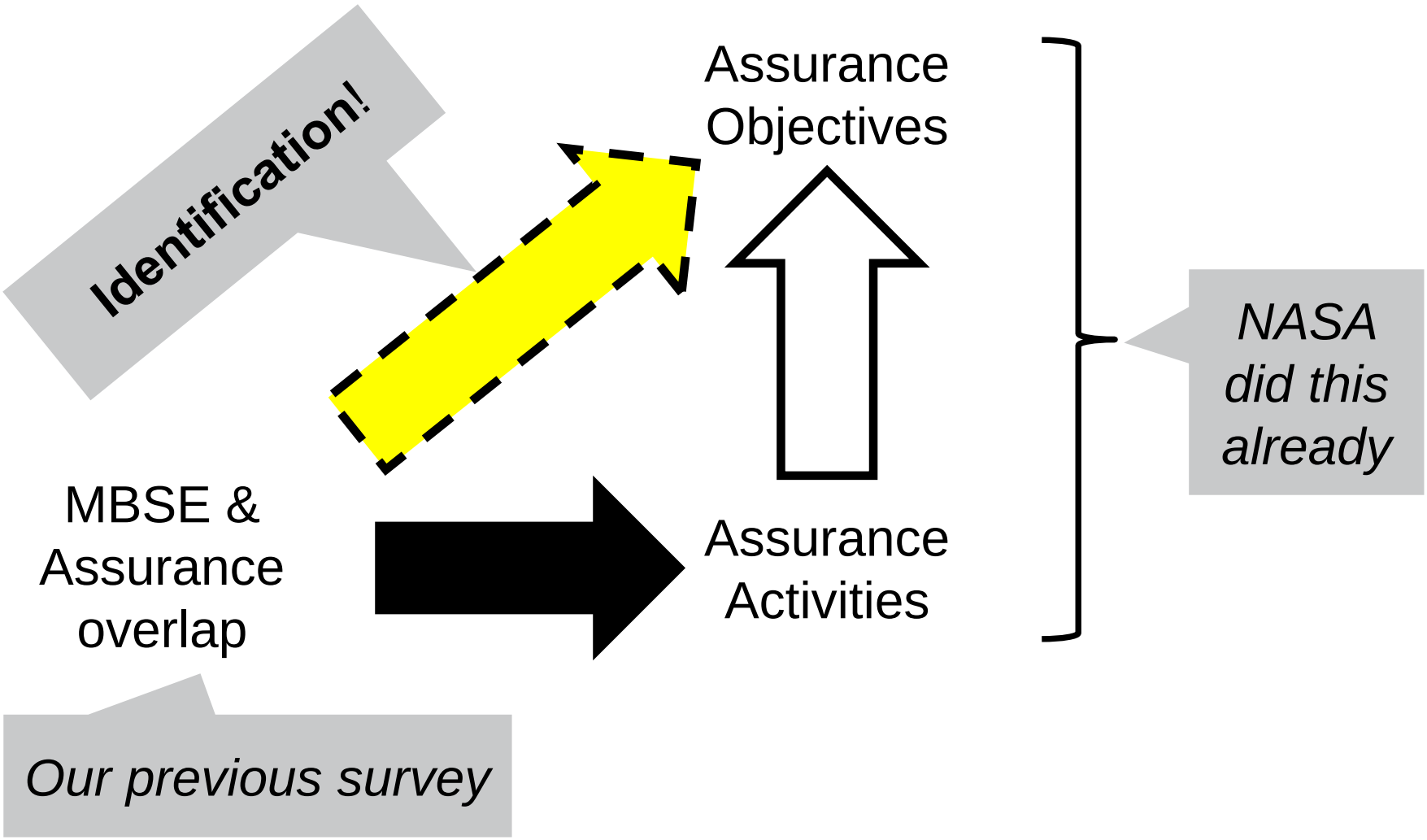
MBSE & Assurance overlap

Our previous survey

Identifying where MBSE helps Assurance

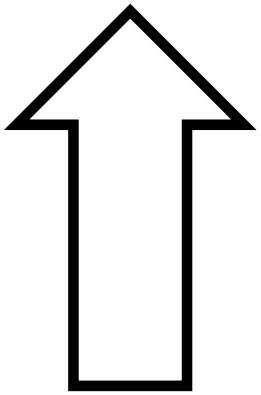


Identifying where MBSE helps Assurance



Identifying where MBSE helps Assurance

Assurance Objectives



Assurance Activities

MBSE & Assurance overlap

MBSE & Assurance Overlap

(from a previous survey we did)

- Systems engineering information …
- Contractual interface…
- Review documentation…
- Correctness of the MBSE models...
- Generating reliability artifacts…
- Off-nominal states and behaviors…
- Post-design activities…

Identifying where MBSE helps Assurance

Assurance Objectives

Assurance Activities

MBSE & Assurance overlap

Reliability & Maintainability Objective Hierarchy

Objective

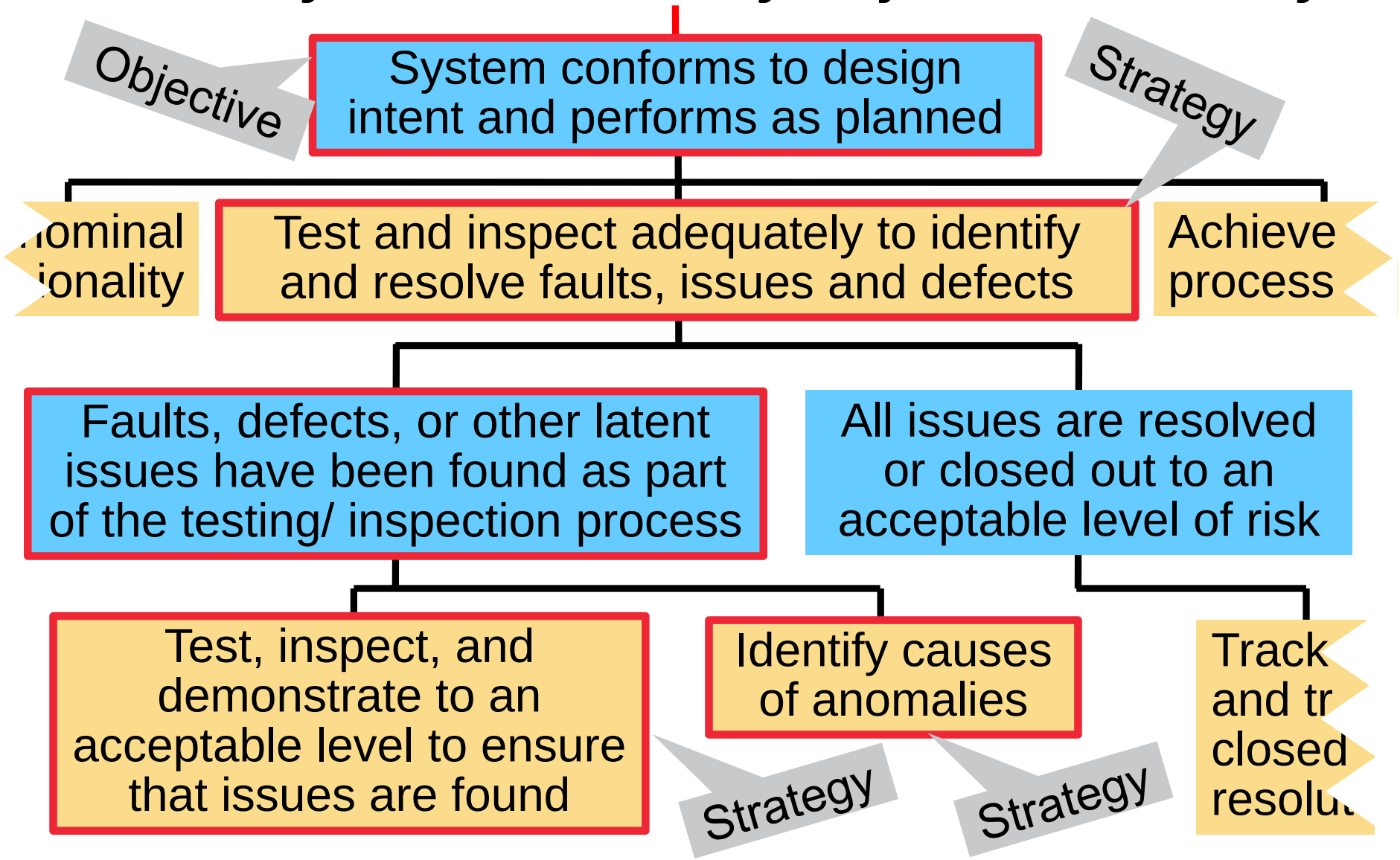
System performs as required over the lifecycle to satisfy mission objectives

Strategy

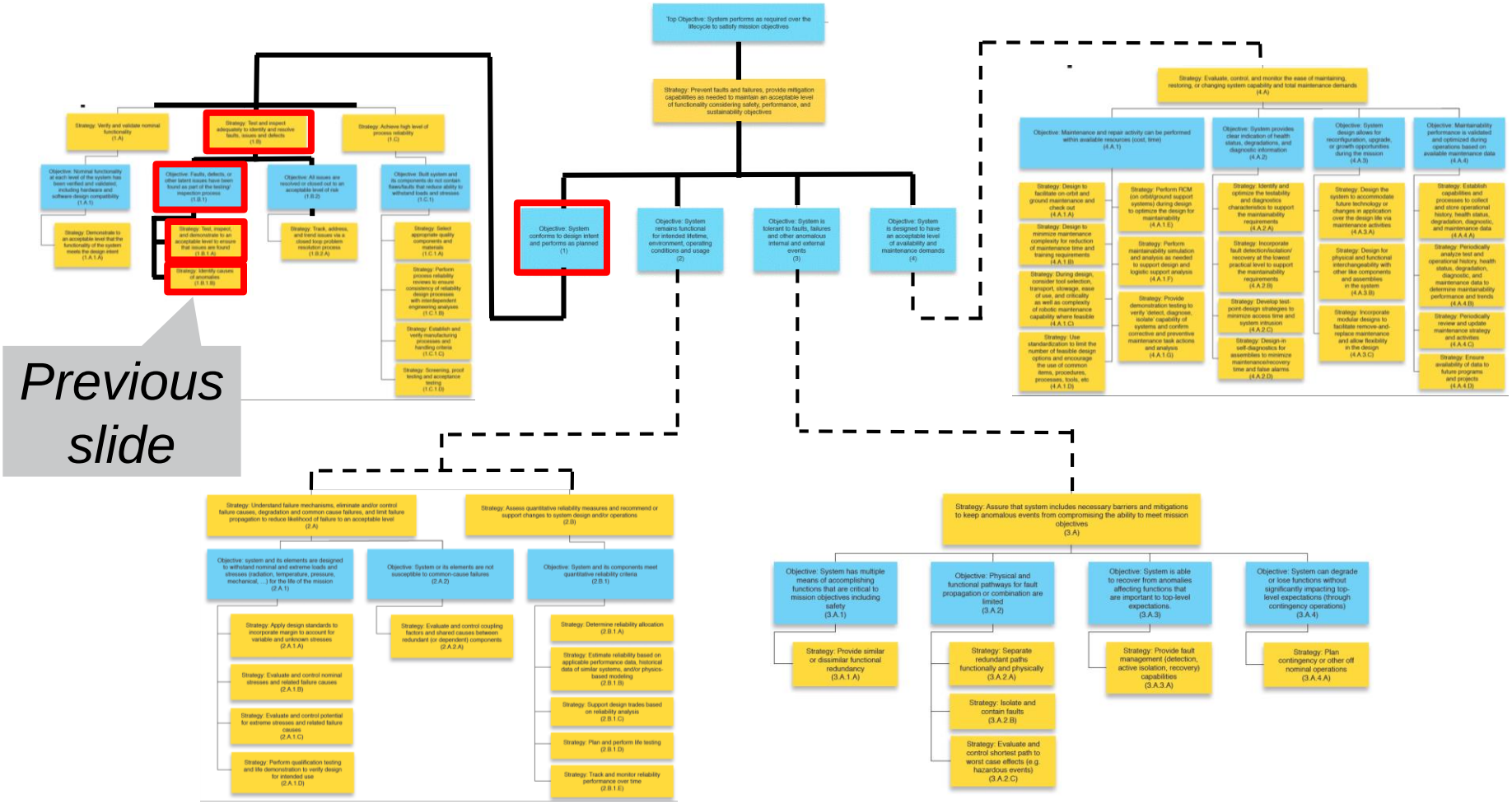
Prevent faults and failures, provide mitigation capabilities as needed to maintain an acceptable level of functionality considering safety, performance, and sustainability objectives

- System conforms to design intent and performs as planned
- System remains functional for intended lifetime, environment, operating conditions and usage
- System is tolerant to faults, failures and other anomalous internal and external events
- System is designed to have an acceptable level of availability and maintenance demands

Reliability & Maintainability Objective Hierarchy



The entire R&M Objectives Hierarchy



Identifying where MBSE helps Assurance

Assurance Objectives ✓

Assurance Activities

MBSE & Assurance overlap ✓

Assurance Activities

Some of the 55 activities

- **Acceptance Test Plan**
- **Accessibility Analysis**
- **Acoustic test**
- **Aging margins**
- **Allocation Analysis**
- **Ambiguity Analysis**

- **Thermal test**
- **Trade Study Analysis**
- **Training Plan and Material**
- **Verification and Validation Testing**
- **Voltage/temperature margin test**
- **Worst Case Analysis**

Identifying where MBSE helps Assurance

Assurance Objectives

Assurance Activities

NASA did this already

MBSE & Assurance overlap

Assurance Activities fulfil Strategies

Strategy

Test, inspect, and demonstrate to an acceptable level to ensure that issues are found

A mix of these **activities** fulfils the strategy

- EMC emissions test
- EMC isolation test

…

- Highly Accelerated Life Test (HALT)

…

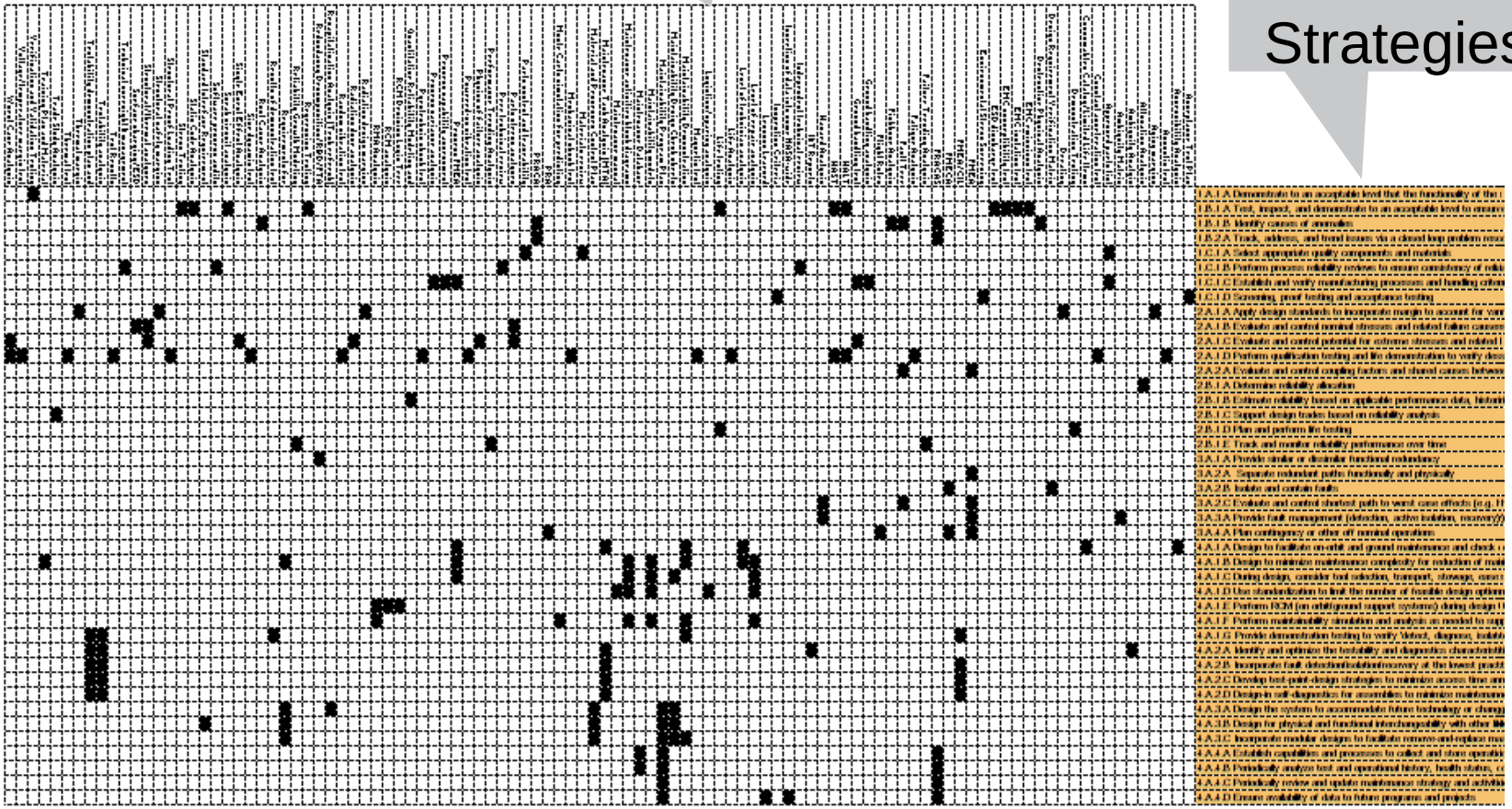
- Static Code Analysis

…

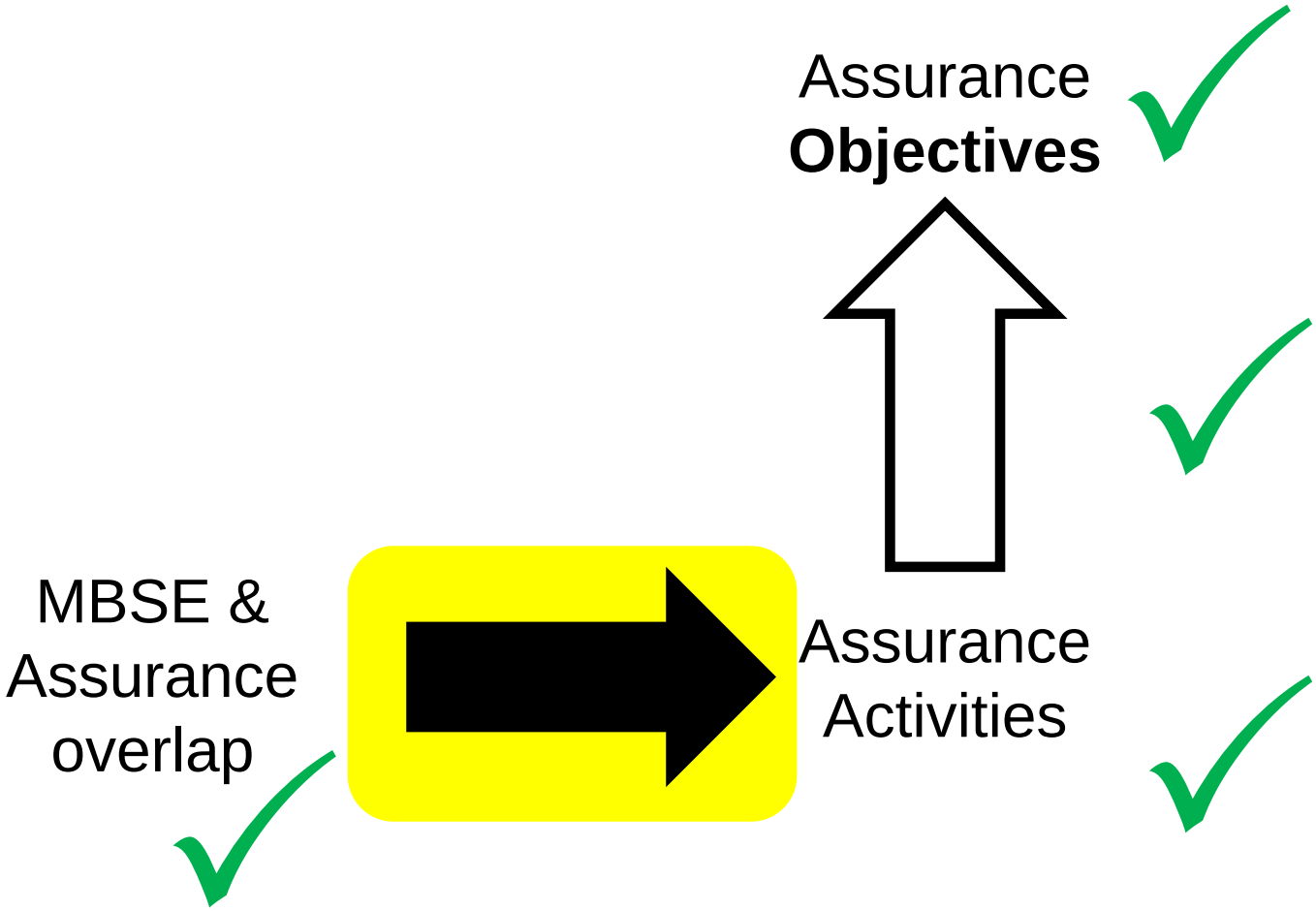
Bird's Eye View of Assurance Activities x Strategies

55 Assurance Activities

42 Strategies



Identifying where MBSE helps Assurance



MBSE → Assurance Activities

MBSE & Assurance overlap

…

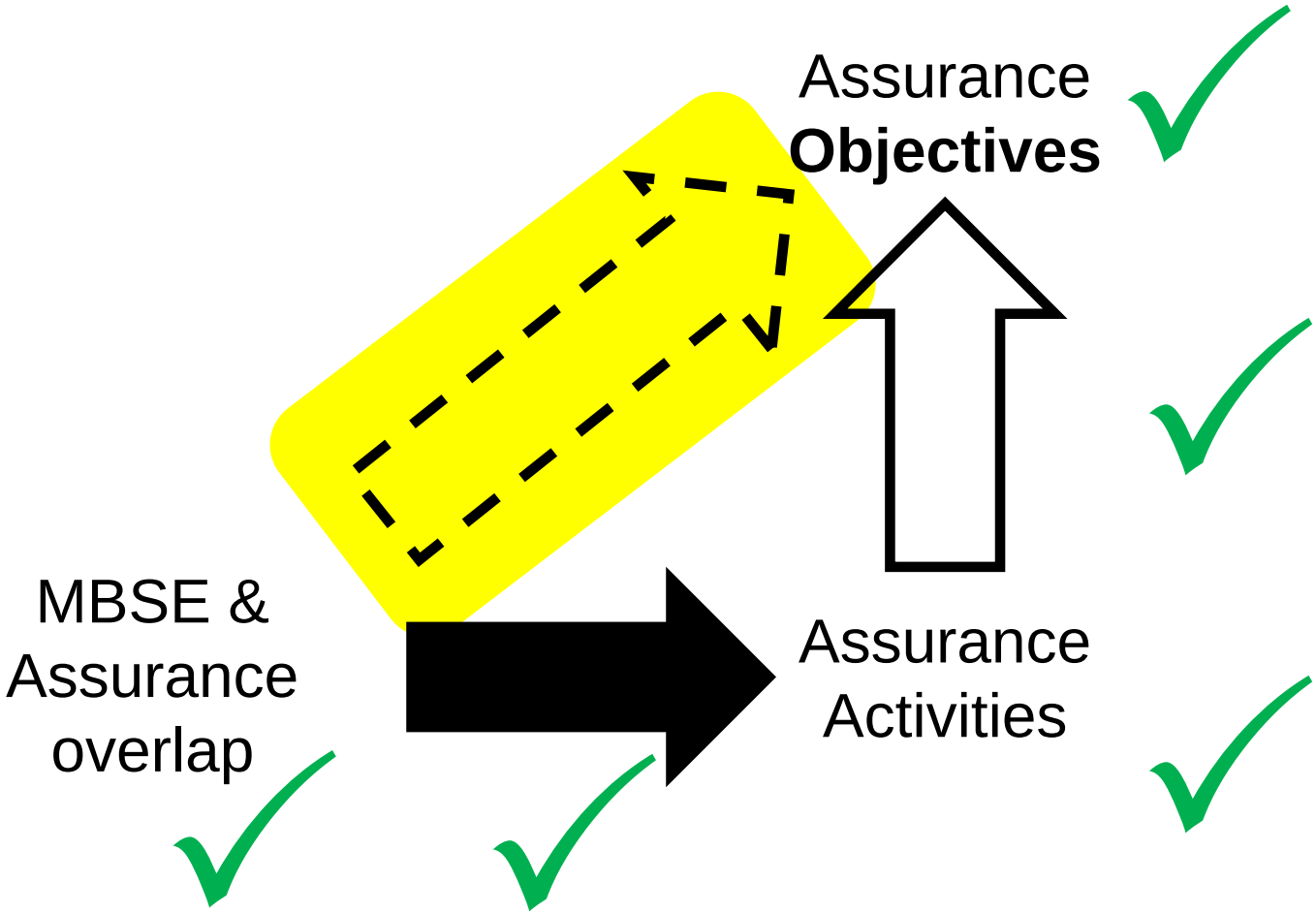
- Generating reliability artifacts…

…

Assurance Activities

FMEA
FMEA/CIL
FMECA
Fault Tree
Fishbone Analysis
Hazard Analysis
PRA
Process FMEA
Quantitative Reliability Modeling and Analysis
Redundancy Decomposition/RBD/FTA
Reliability Growth Modeling
Root Cause Analysis
Worst Case Analysis

Identifying where MBSE helps Assurance



MBSE → Activities → Assurance

"Leaf" strategy nodes of the R&M Objectives Hierarchy

MBSE supports these reliability activities

	1.A.1.A Demonstrate to an	1.B.1.A Test, inspect, and	1.B.1.B Identify causes of	1.B.2.A Track, address, and trend	1.C.1.A Select appropriate quality	1.C.1.B Perform process	1.C.1.C Establish and verify	1.C.1.D Screening, proof testing	2.A.1.A Apply design standards to	2.A.1.B Evaluate and control	2.A.1.C Evaluate and control	2.A.1.D Perform qualification	2.A.2.A Evaluate and control	2.B.1.A Determine reliability	2.B.1.B Estimate reliability based	2.B.1.C Support design trades	2.B.1.D Plan and perform life	2.B.1.E Track and monitor	3.A.1.A Provide similar or	3.A.2.A Separate redundant	3.A.2.B Isolate and contain faults	3.A.2.C Evaluate and control	3.A.3.A Provide fault	3.A.4.A Plan contingency or other	4.A.1.A Design to facilitate on-	4.A.1.B Design to minimize	4.A.1.C During design, consider	4.A.1.D Use standardization to	4.A.1.E Perform RCM (on	4.A.1.F Perform maintainability	4.A.1.G Provide demonstration	4.A.2.A Identify and optimize the	4.A.2.B Incorporate fault	4.A.2.C Develop test-point-	4.A.2.D Design-in self-diagnostics	4.A.3.A Design the system to	4.A.3.B Design for physical and	4.A.3.C Incorporate modular	4.A.4.A Establish capabilities and	4.A.4.B Periodically analyze test	4.A.4.C Periodically review and	4.A.4.D Ensure availability of data
FMEA													■							■		■	■	■																			
FMEA/CIL																														■		■	■	■									
FMECA																					■			■																			
Fault Tree			■										■									■																					
Fishbone Analysis			■																																								
Hazard Analysis																						■	■																				
PRA																								■																			
Process FMEA							■																		■	■	■																
Quantitative Reliability Modeling and															■																												
Redundancy Decomposition/RBD/FTA																			■																								
Reliability Growth Modeling																		■																									
Root Cause Analysis			■																																								
Worst Case Analysis											■	■																															

■ = contributes to the strategy

MBSE offers many contributions to Assurance

Reliability Activities

	1.A.1.A Demonstrate to an	1.B.1.A Test, inspect, and	1.B.1.B Identify causes of	1.B.2.A Track, address, and t	1.C.1.A Select appropriate	1.C.1.B Perform process	1.C.1.C Establish and verif	1.C.1.D Screening, proof t	2.A.1.A Apply design stan	2.A.1.B Evaluate and cont	2.A.1.C Evaluate and control	2.A.1.D Perform qualification	2.A.2.A Evaluate and control	2.B.1.A Determine reliability	2.B.1.B Estimate reliability based	2.B.1.C Support design trades	2.B.1.D Plan and perform life	2.B.1.E Track and monitor	4.A.1.A Design to facilitate on-	4.A.1.B Design to minimize	4.A.1.C During design, consider	4.A.1.D Use standardization to	4.A.1.E Perform RCM ion	4.A.1.F Perform maintainability	4.A.1.G Provide demonstration	4.A.2.A Identify and optimize the	4.A.2.B Incorporate fault	4.A.2.C Develop test-point-	4.A.3.D Design-in self-diagnostics	4.A.3.A Design the system to	4.A.3.B Design for physical and	4.A.3.C Incorporate modular	4.A.4.A Establish capabilities and	4.A.4.B Periodically analyze test	4.A.4.C Periodically review and	4.A.4.D Ensure availability of data
FMEA													■							■		■	■	■													
FMEA/CIL																											■			■	■	■					
FMECA																					■			■													
Fault Tree			■										■									■															
Fishbone Analysis			■																			■															
Hazard Analysis																						■	■														
PRA																								■													
Process FMEA							■																		■	■	■										
Quantitative Reliability Modeling and															■																						
Redundancy Decomposition/RBD/FTA																			■																		
Reliability Growth Modeling																		■																			
Root Cause Analysis			■																																		
Worst Case Analysis											■	■																									

Analysis Activities

	1.A.1.A Demonstrate to an	1.B.1.A Test, inspect, and	1.B.1.B Identify causes of	1.B.2.A Track, address, and t	1.C.1.B Perform process	1.C.1.C Establish and verif	1.C.1.D Screening, proof t	2.A.1.A Apply design stan	2.A.1.B Evaluate and cont	2.A.1.C Evaluate and control	2.A.1.D Perform qualification	2.A.2.A Evaluate and control	2.B.1.A Determine reliability	2.B.1.B Estimate reliability based	2.B.1.C Support design trades	2.B.1.D Plan and perform life	2.B.1.E Track and monitor	3.A.1.A Provide similar or	3.A.2.A Separate redundant paths	3.A.2.B Isolate and contain faults	3.A.2.C Evaluate and control	3.A.4.A Provide fault management	3.A.4.B Plan contingency or other	4.A.1.A Design to facilitate on-	4.A.1.B Design to minimize	4.A.1.C During design, consider	4.A.1.D Use standardization to	4.A.1.F Perform maintainability	4.A.1.G Provide demonstration	4.A.2.A Identify and optimize the	4.A.2.B Incorporate fault	4.A.2.C Develop test-point-	4.A.3.D Design-in self-diagnostics	4.A.3.A Design the system to	4.A.3.B Design for physical and	4.A.3.C Incorporate modular	4.A.4.A Establish capabilities and	4.A.4.B Periodically analyze test	4.A.4.C Periodically review and	4.A.4.D Ensure availability of data
Allocation Analysis													■																								
Ground handling analysis							■																														
Monte Carlo simulation for predicting MMH																									■												
RCM analysis																									■												
Radiation dose analysis											■																										
Single Event Effect Analysis											■																										
Sneak circuit analysis	■																																				
Static Code Analysis	■																																				
Testability analysis																										■	■	■	■	■							
Trade Study Analysis																■																					
Acoustic test											■																										
Constant acceleration test											■																										
EMC emissions test	■																																				
EMC isolation test	■																																				
EMC susceptibility test	■																																				
ESD discharge test	■																																				
Ground handling test							■																														
HALT	■										■																										
HAST	■										■																										
Life testing	■															■																					
Magnetic test											■																										
Mechanical shock test											■																										
Powered-on vibration test											■																										
Pyrotechnic shock test											■																										
Random vibration test											■																										
Sine dynamic test											■																										
Stress Testing	■																																				
Structural Proof Loading Test											■																										
Thermal test											■																										
Voltage/temperature margin test											■																										

Test Management Activities

	1.A.1.A Demonstrate to an	1.B.1.A Test, inspect, and	1.B.1.B Identify causes of	1.B.2.A Track, address, and t	1.C.1.A Select appropriate qu	1.C.1.B Perform process rella	1.C.1.C Establish and verify	1.C.1.D Screening, proof test	2.A.1.A Apply design standar	2.A.1.B Evaluate and control	2.A.1.C Evaluate and control	2.A.1.D Perform qualification	2.A.2.A Evaluate and control	2.B.1.A Determine reliability	2.B.1.B Estimate reliability Da	2.B.1.C Support design trade	2.B.1.D Plan and perform life	2.B.1.E Track and monitor	4.A.1.A Design to facilitate o	4.A.1.B Design to minimize	4.A.1.C During design, consid	4.A.1.D Use standardization	4.A.1.F Perform maintainability	4.A.1.G Provide demonstration	4.A.2.A Identify and optimize the	4.A.2.B Incorporate fault	4.A.2.C Develop test-point-design	4.A.3.D Design-in self-diagnostics	4.A.3.A Design the system to	4.A.3.B Design for physical and	4.A.3.C Incorporate modular	4.A.4.A Establish capabilities and	4.A.4.B Periodically analyze test	4.A.4.C Periodically review and	4.A.4.D Ensure availability of data
Acceptance Test Plan								■																													
Demonstration Testing																	■																				
Design Requirement Verification Matrix																						■															
Failure Trending Analysis																		■																			
I&T Reports																											■										
Inspection Criteria							■																														
Maintainability Demonstration																									■	■			■	■				■			
Performance Trending Analysis																		■																			
Regression Testing	■																																				
Reliability Growth Modeling																		■																			
Results of demonstration test																													■								
Test Results												■																									
Testability demonstration plan and results																													■	■	■	■					
Verification and Validation Testing	■																																				

Test Activities

Assurance Objectives *unaddressed* by MBSE:

- Track, address, and trend issues via a closed loop problem resolution process
- Select appropriate quality components and materials
- Use standardization to limit the number of feasible design options and encourage the use of common items, procedures, processes, tools, etc
- Periodically review and update maintenance strategy and activities

…

"Process" related, only indirectly support by MBSE

Also need more work on assurance of MBSE itself (models, processes, infrastructure)

Jet Propulsion Laboratory
California Institute of Technology

jpl.nasa.gov