Space System Verification Approach Based on MEAL and Mission Risk Posture

Oscar Gonzalez[1], Raymond L. Ladbury[2], Yuan Chen[3], Dwayne. R. Morgan[4], Christopher M. Green[2], Daniel E. Yuchnovicz[3], George L. Jackson[2]

[1]Formerly with NASA Goddard Space Flight Center, Greenbelt, MD 20771

[2]NASA Goddard Space Flight Center, Greenbelt, MD 20771

[3]NASA Langley Research Center, Hampton, VA 23681

[4]NASA Wallops Flight Facility, Wallops Island, VA 23337

To be presented by Raymond Ladbury at the 31st Aerospace Testing Seminar, Los Angeles, CA, October 22-25, 2018.

Abbreviations and Definitions

CMOS—Complementary Metal Oxide Semiconductor

COTS—Commercial Off The Shelf

e-—electron

ELDRS—Enhanced Low Dose Rate Sensitivity

LOC—Loss of Crew

LOM—Loss of Mission

MEAL—Mission Environment Applicaton and Lifetime

NESC—NASA Engineering and Safety Center

p+— proton

TRL—Technology Readiness Level (1-9)

V&V—Verification and Validation

Radiation Effects Threats

Prompt Effects:

SEB—Single-Event Burnout

SEE—Single-Event Effect

SEFI—Single-Event Functional Interrupt

SEGR—Single-Event Gate Rupture

SEL—Single-Event Latchup

SET—Single-Event Transient (SET)

SEU—Single-Event Upset

Cumulative Effects:

DDD—Displacement Damage Dose

TID—Total Ionizing Dose

Outline

- Motivation
- Verification approach based on MEAL and risk posture for space systems
    - MEAL - Mission, Environment, Application, and Lifetime
    - Risk and risk posture
- Verification performed at part-, board- and box-level, and risks
- Approach applications on
    - Flight heritage verification
    - Commercial off the shelf (COTS) verification
    - Radiation effect verification

Motivation: To *rectify common misunderstandings about verification*

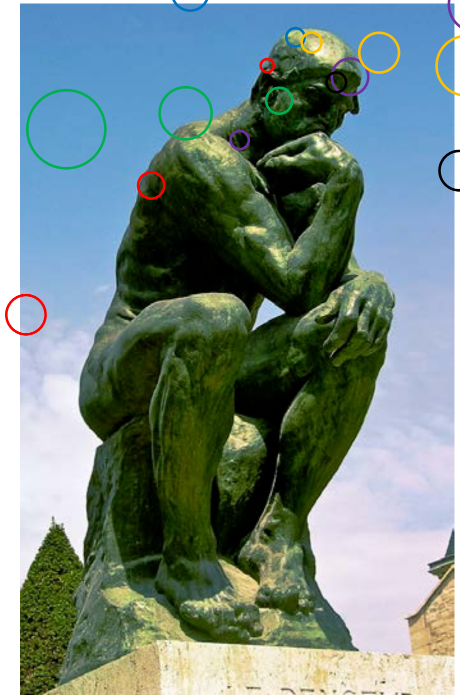
Verification not needed beyond manufacturer's data on COTS technologies

Flight heritage allows omission of critical verification steps

It is not important to understand the verification process including capabilities, advantages and limitations at different integration level

Cost/budget/schedule pressures are adequate reason to deviate from accepted qualification and screening procedures

One size fits all



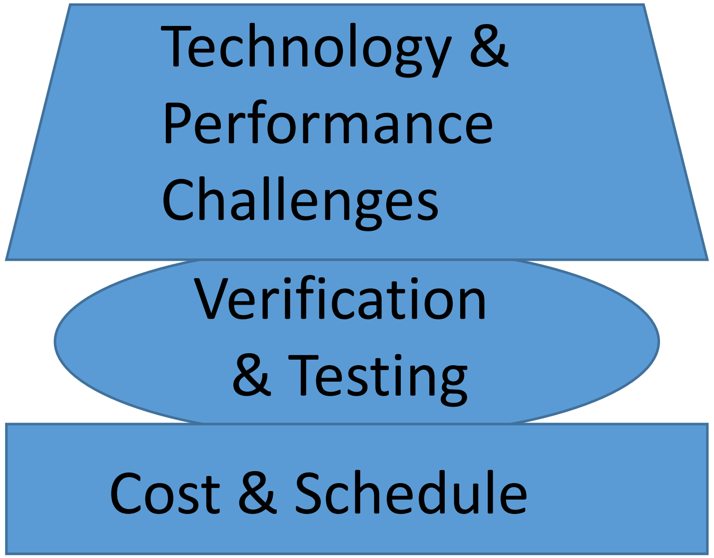
New technologies have sufficient reliability built-in and so require no additional screening or qualification

Photo by Andrew Horne (talk) - Own work (Original text: I (AndrewHorne (talk)) created this work entirely by myself.), Public Domain, https://commons.wikimedia.org/w/index.php?curid=15582363

Background: Verification Basics and Challenges

- Space missions face increasing challenges, whether the mission is human exploration, science or communications
  - Performance demands are increasing and becoming difficult to meet without using state-of-the-art components
  - Testing and verification are becoming more difficult and challenging as components & systems get more complicated
  - Technologies are being pushed to their physical limits

- Verification—proving through test, analysis, inspection, and/or demonstration that a product provides its required *function* while meeting performance requirements
- Verification must yield understanding of performance under worst-case conditions to evaluate margins to failure in the application
- Verification tests, etc. carried out at each level have different capabilities, advantages and limitations
  - Omitting a step carries different risks depending on level of integration as well as MEAL



<u>Part-Level</u>

Goodness of parts
Margins to failure
Failure Symptoms
Failure probabiities
⋮

<u>Board-Level</u>

Part Interactions
Circuit Margins
Realistic circuit errors/failures
⋮

<u>System/Box-Level</u>

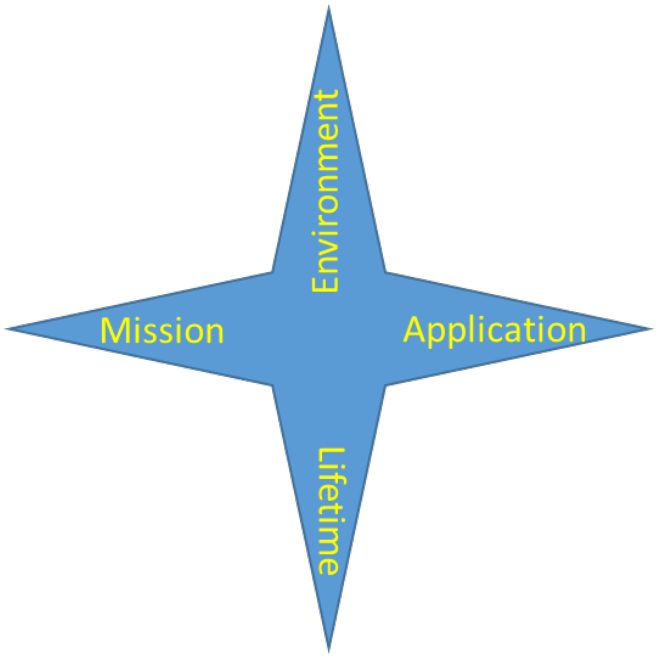
System Interactions
Workmanship
System-level errors
⋮

Definition of MEAL

Environment: relevant ambient conditions the system would experience during the life cycle to accomplish the mission (e.g., thermal effects, electromagnetics effects, electrostatic effects, radiation effects, etc.).

Mission: Ultimate goal or objective of the effort. Identifies type/kind of mission.

- Helps define environment/application related requirements
- Expected progression, beginning to end
- Risk posture/acceptable risks
- Cost, schedule &required performance



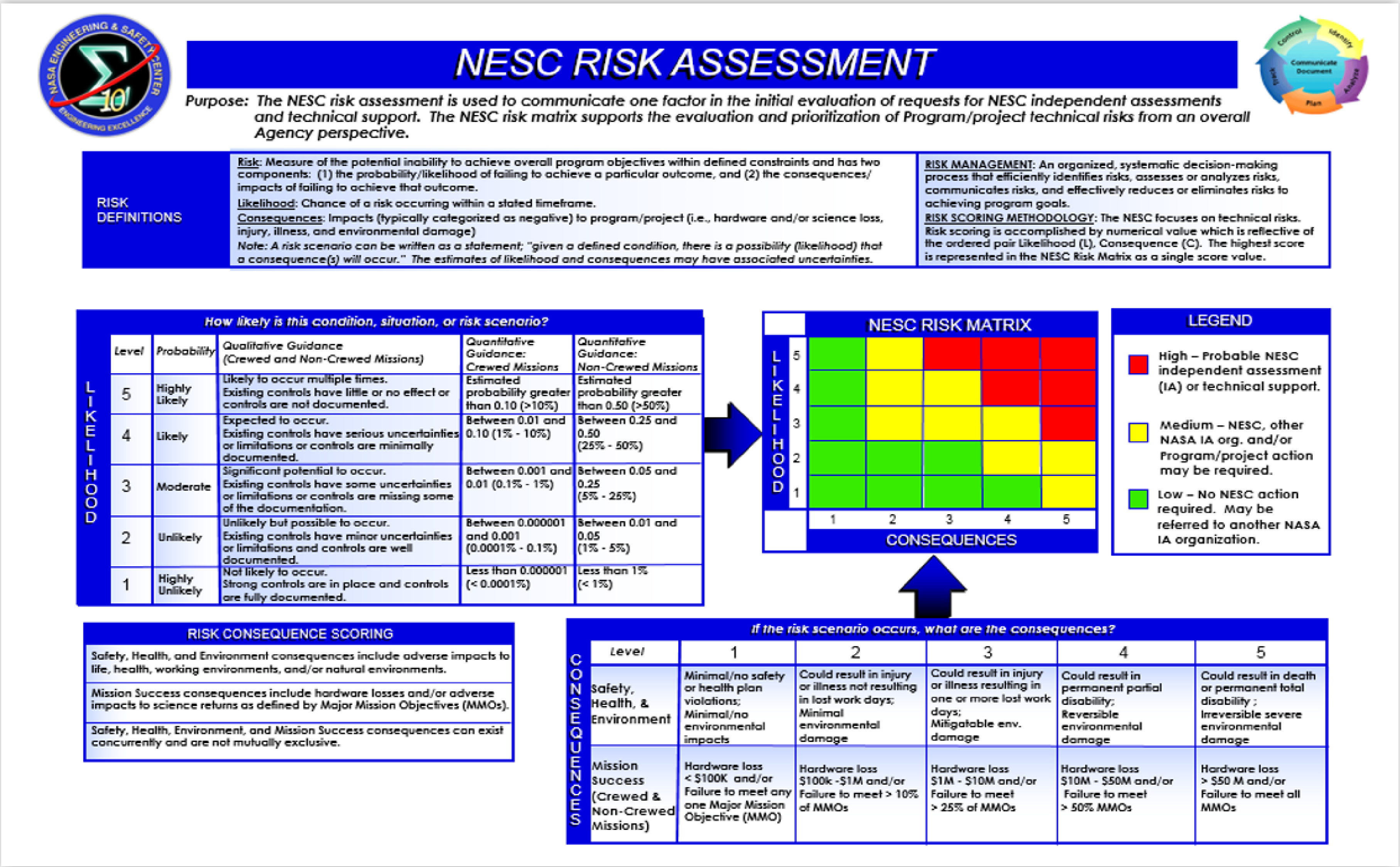
Application: Specific function(s) to be executed to meet mission goals.

- Includes architecture, parts, technologies, redundancy & other mitigation…
- How parts, circuits, subsystems interface to/interact with each other

Lifetime: The total time during which the system must perform its intended functions, including subcomponent manufacturing, systems development, system implementation, system execution/operations, and retiring of the system to accomplish the mission.

Risk and Risk Posture

- No single risk matrix for all NASA missions
- Projects develop own matrix based on MEAL and their requirements
- Human Exploration Risks
  - Health/Safety: Loss of Crew(LOC)
  - Technical: Loss of Mission (LOM)
  - Programmatic: Cost/Schedule
- Robotic Exploration
  - Health/Safety: LOM
  - Technical: LOM
  - Programmatic: Cost/Schedule



NESC RISK ASSESSMENT

Purpose: *The NESC risk assessment is used to communicate one factor in the initial evaluation of requests for NESC independent assessments and technical support. The NESC risk matrix supports the evaluation and prioritization of Program/project technical risks from an overall Agency perspective.*

RISK DEFINITIONS

Risk: Measure of the potential inability to achieve overall program objectives within defined constraints and has two components: (1) the probability/likelihood of failing to achieve a particular outcome, and (2) the consequences/ impacts of failing to achieve that outcome.
Likelihood: Chance of a risk occurring within a stated timeframe.
Consequences: Impacts (typically categorized as negative) to program/project (i.e., hardware and/or science loss, injury, illness, and environmental damage)
Note: A risk scenario can be written as a statement; "given a defined condition, there is a possibility (likelihood) that a consequence(s) will occur." The estimates of likelihood and consequences may have associated uncertainties.

RISK MANAGEMENT: An organized, systematic decision-making process that efficiently identifies risks, assesses or analyzes risks, communicates risks, and effectively reduces or eliminates risks to achieving program goals.
RISK SCORING METHODOLOGY: The NESC focuses on technical risks. Risk scoring is accomplished by numerical value which is reflective of the ordered pair Likelihood (L), Consequence (C). The highest score is represented in the NESC Risk Matrix as a single score value.

How likely is this condition, situation, or risk scenario? (LIKELIHOOD)

Level	*Probability*	*Qualitative Guidance (Crewed and Non-Crewed Missions)*	*Quantitative Guidance: Crewed Missions*	*Quantitative Guidance: Non-Crewed Missions*
5	Highly Likely	Likely to occur multiple times. Existing controls have little or no effect or controls are not documented.	Estimated probability greater than 0.10 (>10%)	Estimated probability greater than 0.50 (>50%)
4	Likely	Expected to occur. Existing controls have serious uncertainties or limitations or controls are minimally documented.	Between 0.01 and 0.10 (1% - 10%)	Between 0.25 and 0.50 (25% - 50%)
3	Moderate	Significant potential to occur. Existing controls have some uncertainties or limitations or controls are missing some of the documentation.	Between 0.001 and 0.01 (0.1% - 1%)	Between 0.05 and 0.25 (5% - 25%)
2	Unlikely	Unlikely but possible to occur. Existing controls have minor uncertainties or limitations and controls are well documented.	Between 0.000001 and 0.001 (0.0001% - 0.1%)	Between 0.01 and 0.05 (1% - 5%)
1	Highly Unlikely	Not likely to occur. Strong controls are in place and controls are fully documented.	Less than 0.000001 (< 0.0001%)	Less than 1% (< 1%)

LEGEND

High – Probable NESC independent assessment (IA) or technical support.
Medium – NESC, other NASA IA org. and/or Program/project action may be required.
Low – No NESC action required. May be referred to another NASA IA organization.

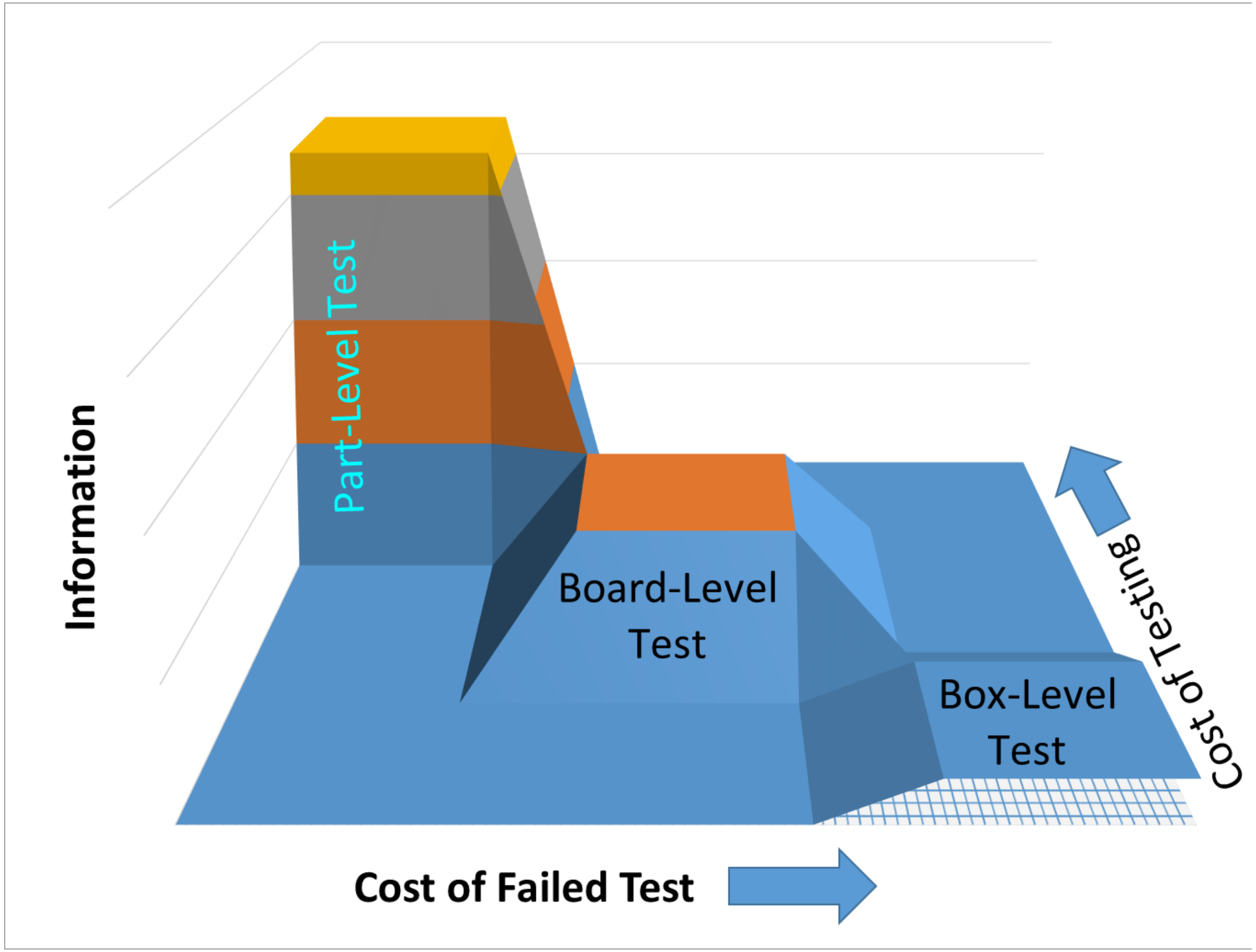
RISK CONSEQUENCE SCORING

Safety, Health, and Environment consequences include adverse impacts to life, health, working environments, and/or natural environments.
Mission Success consequences include hardware losses and/or adverse impacts to science returns as defined by Major Mission Objectives (MMOs).
Safety, Health, Environment, and Mission Success consequences can exist concurrently and are not mutually exclusive.

If the risk scenario occurs, what are the consequences? (CONSEQUENCES)

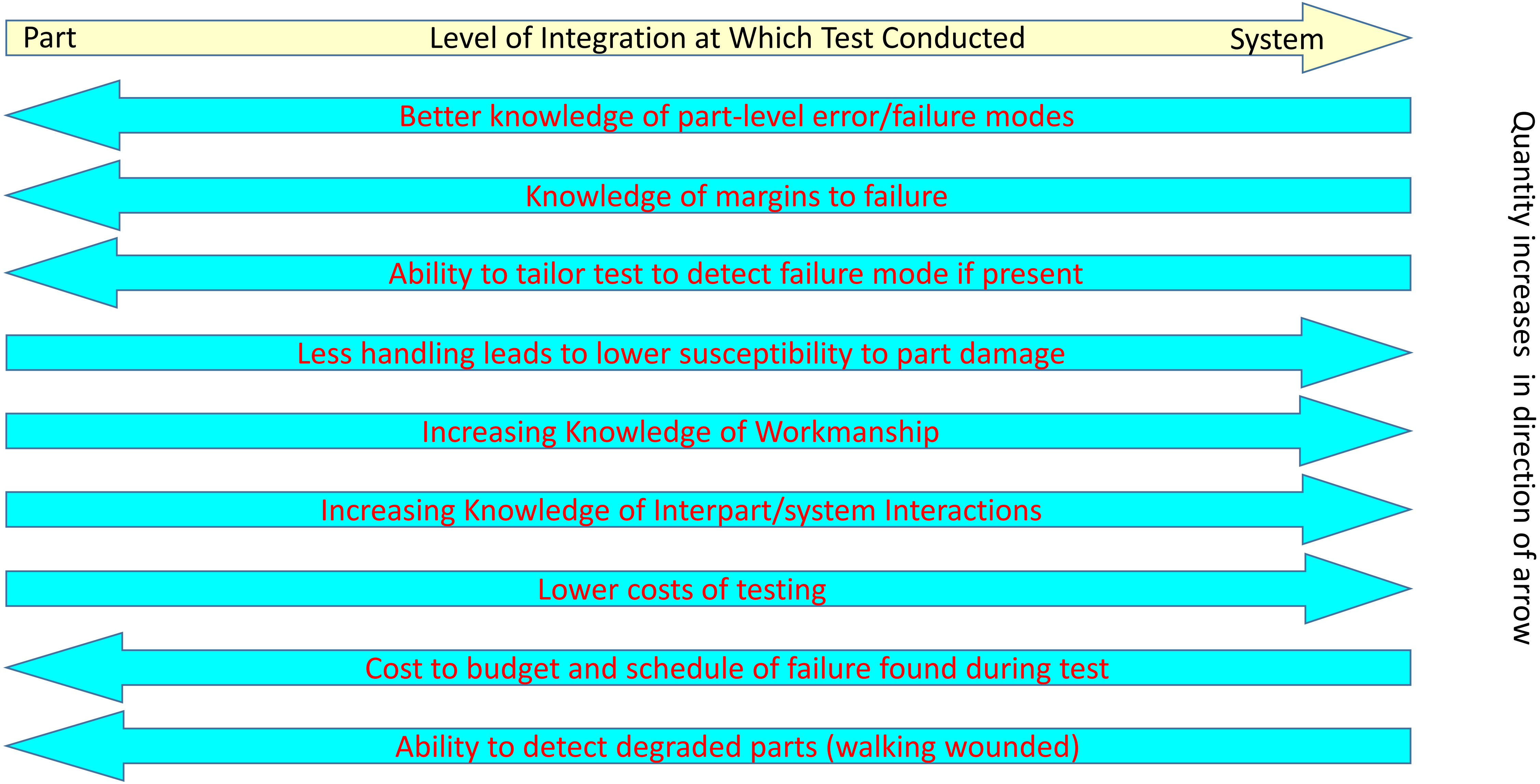
Level	1	2	3	4	5
Safety, Health, & Environment	Minimal/no safety or health plan violations; Minimal/no environmental impacts	Could result in injury or illness not resulting in lost work days; Minimal environmental damage	Could result in injury or illness resulting in one or more lost work days; Mitigatable env. damage	Could result in permanent partial disability; Reversible environmental damage	Could result in death or permanent total disability ; Irreversible severe environmental damage
Mission Success (Crewed & Non-Crewed Missions)	Hardware loss < $100K and/or Failure to meet any one Major Mission Objective (MMO)	Hardware loss $100k -$1M and/or Failure to meet > 10% of MMOs	Hardware loss $1M - $10M and/or Failure to meet > 25% of MMOs	Hardware loss $10M - $50M and/or Failure to meet > 50% MMOs	Hardware loss > $50 M and/or Failure to meet all MMOs

Cartoon: Results of Testing at Various Levels of Integration



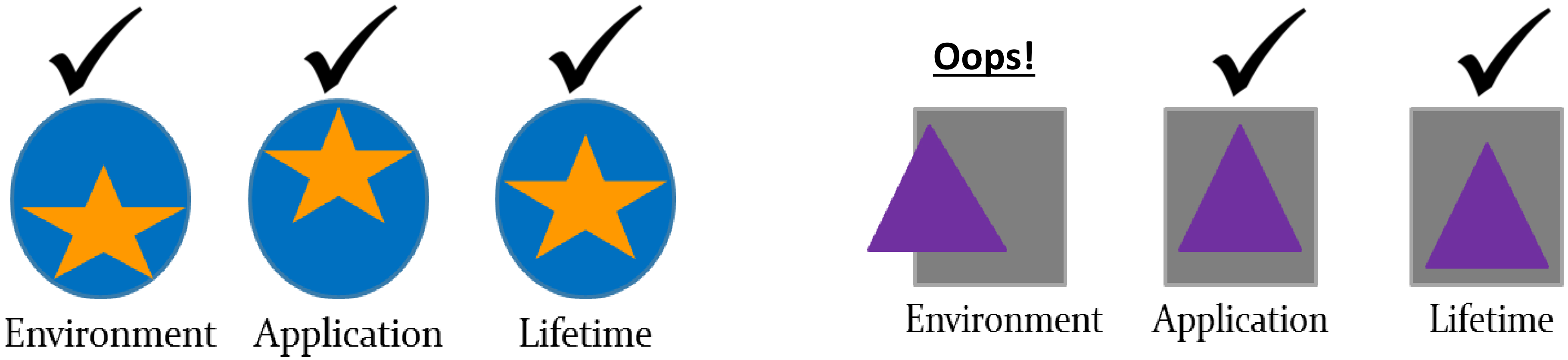
- Part-Level Testing
  - Testing many parts is expensive
  - Not all part failures manifest @system level
  - Tests can be tailored to technology and failure mode (improves failure detection)
  - Yields Failure margins as well as levels
- Board-Level testing
  - Many part-tests consolidated to 1 board test
    - Board serves as test hardware
  - Failures detected likely relevant for system
  - Yields info on part interactions/workmanship
  - Yields little detail on failures or margins
  - Cost of remediation high if failures detected
  - Some failures not detected at board level
- Box/Subsystem/System-Level Testing
  - Trends from part- to-board-level continue
    - Lower testing costs
    - Less Information, higher remediation costs
- Some tests not possible at all levels

Testing Trends vs. Level of Integration



MEAL-based Verification for Flight Heritage (I)

- Provides steps to qualify any design and helps assess whether "heritage design" is suitable for the given mission.
- Heritage mission's characteristics must bound those of the new mission:
  - Environment
  - Application
  - Lifetime
- If not realized, technology regresses to appropriate TRL for the new mission
  - Must be certified/verified to the predicted conditions of new mission.



MEAL-based Verification for Flight Heritage (II)

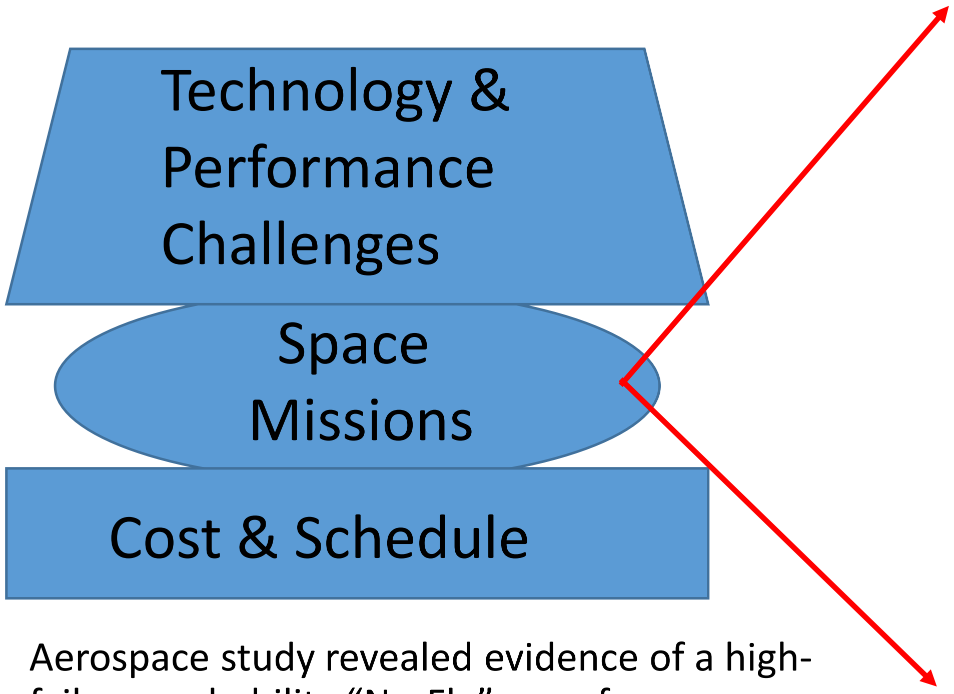
		Description	Mission Examples				
			(a)	Environment Application Lifetime (b)	Environment Application Lifetime (c)	Environment Application Lifetime (d)	Environment Application Lifetime (e)
			New Technology	Proposed New Mission MEAL (mission environment, application and expected lifetime) is equal or a subset of the previously flown mission MEAL, including identical concept, form fit, design, interfaces, etc.	Proposed New Mission application and expected lifetime is equal or a subset of the previously flown mission, including identical concept, form fit, design, interfaces, etc., but with an environment outside the previously flown mission.	Proposed New Mission MEAL is equal or a subset of the previously flown mission MEAL, but with different application implementation (i.e. different design outside the previously flown like mechanical, thermal &/or electrical)	Design previously flown but different application, environment and lifetime (where the original application does not envelope the new application)
	TRL #	Description as stated on 7120.5C					
Concept	1	Basic principles observed and reported	V&V	Previous Data Available	Previous Data Available	Previous Data Available	Previous Data Available
Concept	2	Technology concept and/or application formulated	V&V	Previous Data Available	Previous Data Available	Previous Data Available	V&V
Concept	3	Analytical and experimental critical function and/or characteristic proof-of-concept	V&V	Previous Data Available	Previous Data Available	Previous Data Available	V&V
Implementation – Ground	4	Component and/or breadboard validation in laboratory environment	V&V	Previous Data Available	Previous Data Available	V&V	V&V
Implementation – Ground	5	Component and/or breadboard validation in relevant environment	V&V	Previous Data Available	V&V	V&V	V&V
Implementation – Ground	6	System/subsystem model or prototype demonstration in a relevant environment	V&V	Previous Data Available	V&V	V&V	V&V
Implementation – Space	7	System prototype demonstration in the real environment	V&V	V&V	V&V	V&V	V&V
Implementation – Space	8	Actual system completed and "flight qualified" through test and demonstration	V&V	V&V	V&V	V&V	V&V
Implementation – Space	9	Actual system "flight proven" through successful mission operations	V&V	V&V	V&V	V&V	V&V
		Comments:	Must undergo through the entire TRL process	Must verify system/subsystem under relevant environment (acceptance verification test)	Must validate component &/or Breadboard under relevant environment.	Must validate component &/or Breadboard under laboratory environment.	Must be treated as the new technology

Notes:

V&V	Must be validated and verified as per TRL Definitions and descriptions.
Previous Data Available	Validation data available from previously flown/validated system. Requires Verification at all levels of implementation.

COTS Parts: Why, Why Not, MEAL and Test Integration Level

One Approach: Use More COTS



Lower part cost
Faster delivery
Better Performance

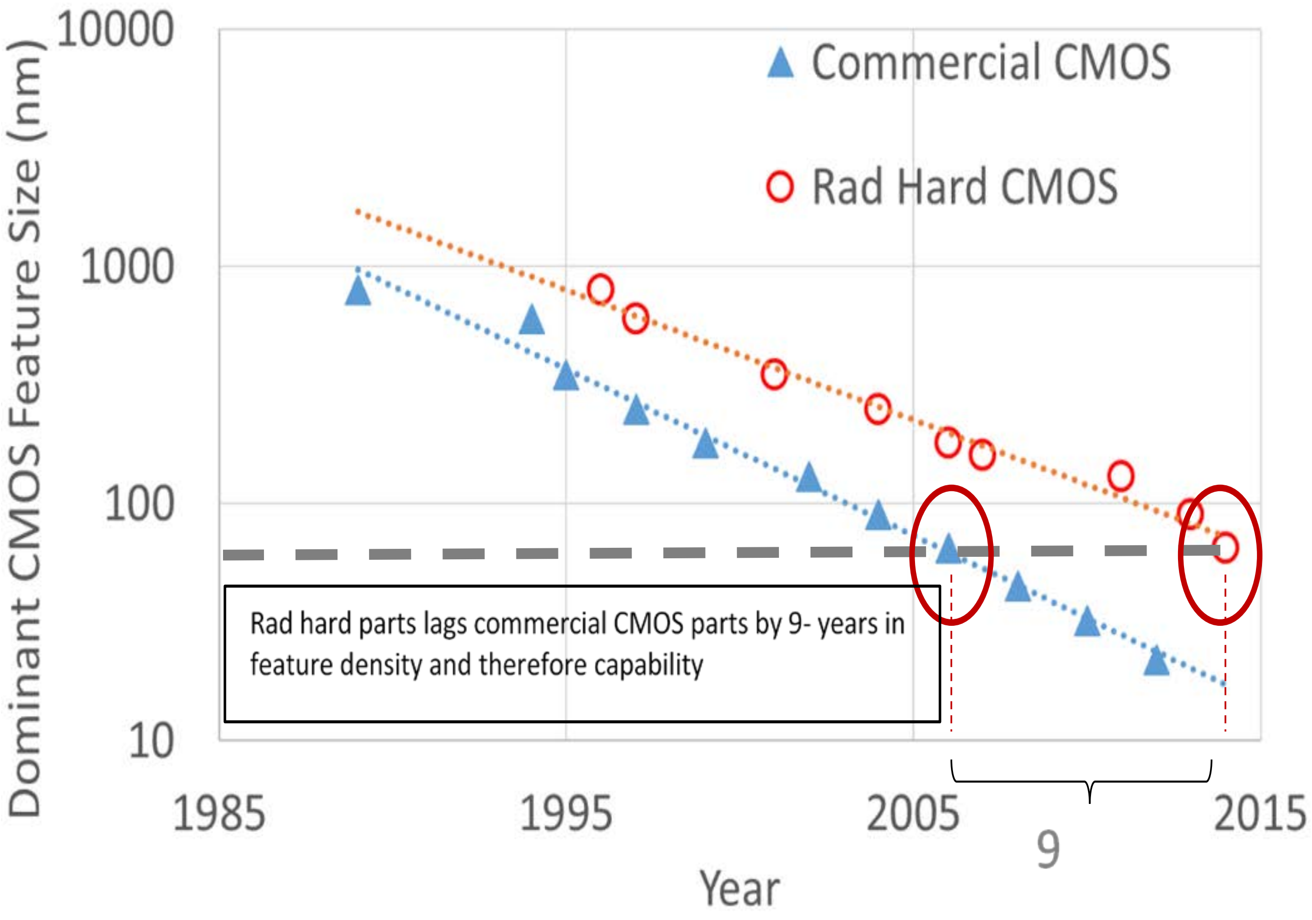
Not designed for space
Harder to test
No radiation data
Costlier qualification
Longer qualification times
Faster obsolescence
May make system more complex

- Aerospace study revealed evidence of a high-failure probability “No-Fly” zone for “complex” missions where cost and schedule were too aggressive.*

- Part-level testing
  - Most effective but takes longer
  - Requires complicated test gear
  - A few tests of complex state-of-the-art COTS parts breaks the bank
- Board-level testing
  - Inclusion of several complex COTS parts may make system too complex for comprehensive test
  - Board can serve as test hardware, but yields limited understanding
  - Less costly
- Box/Subsystem/System-level test
  - Still lower costs, but also less understanding
- For COTS, part-level testing is important, but may be costlier, more complicated and take longer

*William F. Tosney, “What the U.S. Space Industry Learned the ‘Hard Way’ and Why it’s ‘Back to Basics”

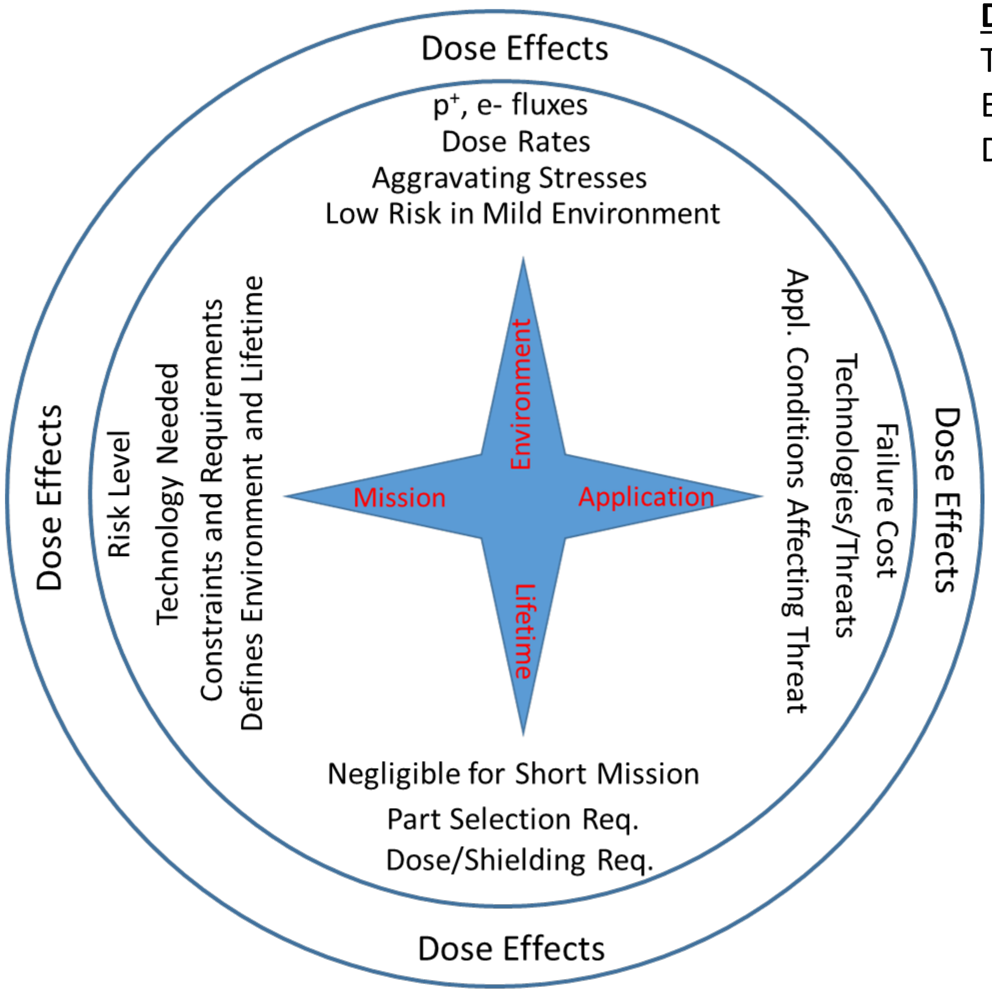
Pressure to Use COTS Is Increasing



- Moore's Law applies to both commercial and radiation hardened technologies
  - Commercial doubling time~18 months
  - Rad Hard doubling time ~24 months
- Increased density only 1 measure of progress
  - New semiconductor materials
    - Until 2000, only 8 elements used in semiconductors; count is now >40
  - New device topologies
    - FINFETS, Nanowires…
  - New methods of integrating technologies
    - System In a Package (SIP)
    - Much harder to test
- Radiation hardening efforts expensive
- Space qualified hardware likely to be
  - Bulkier, slower than commercial
  - More limited choices of technology

Radiation Effects: Here Thar Be Dragons!!!

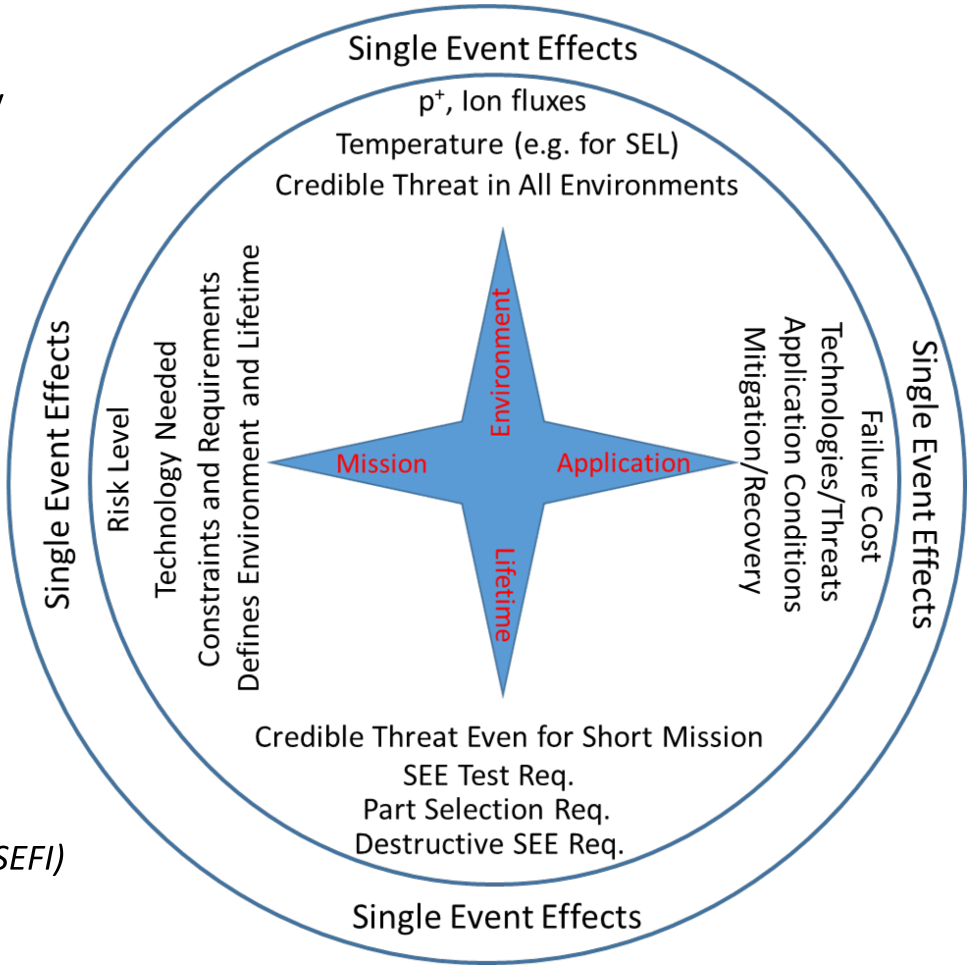
Cumulative Effects of Radiation



Dose Effects Include:
Total-Ionizing Dose
Enhanced Low-Dose-Rate Sensitivity
Displacement Damage Dose

SEE Include:
Nondestructive
Single-Event Transient (SET)
Single-Event Upset (SEU)
Single-Event Functional Interrupt (SEFI)
Destructive
Single-Event Latchup (SEL)
Single-Event Gate Rupture (SEGR)
Single-Event Burnout (SEB)

Prompt Effects of Radiation



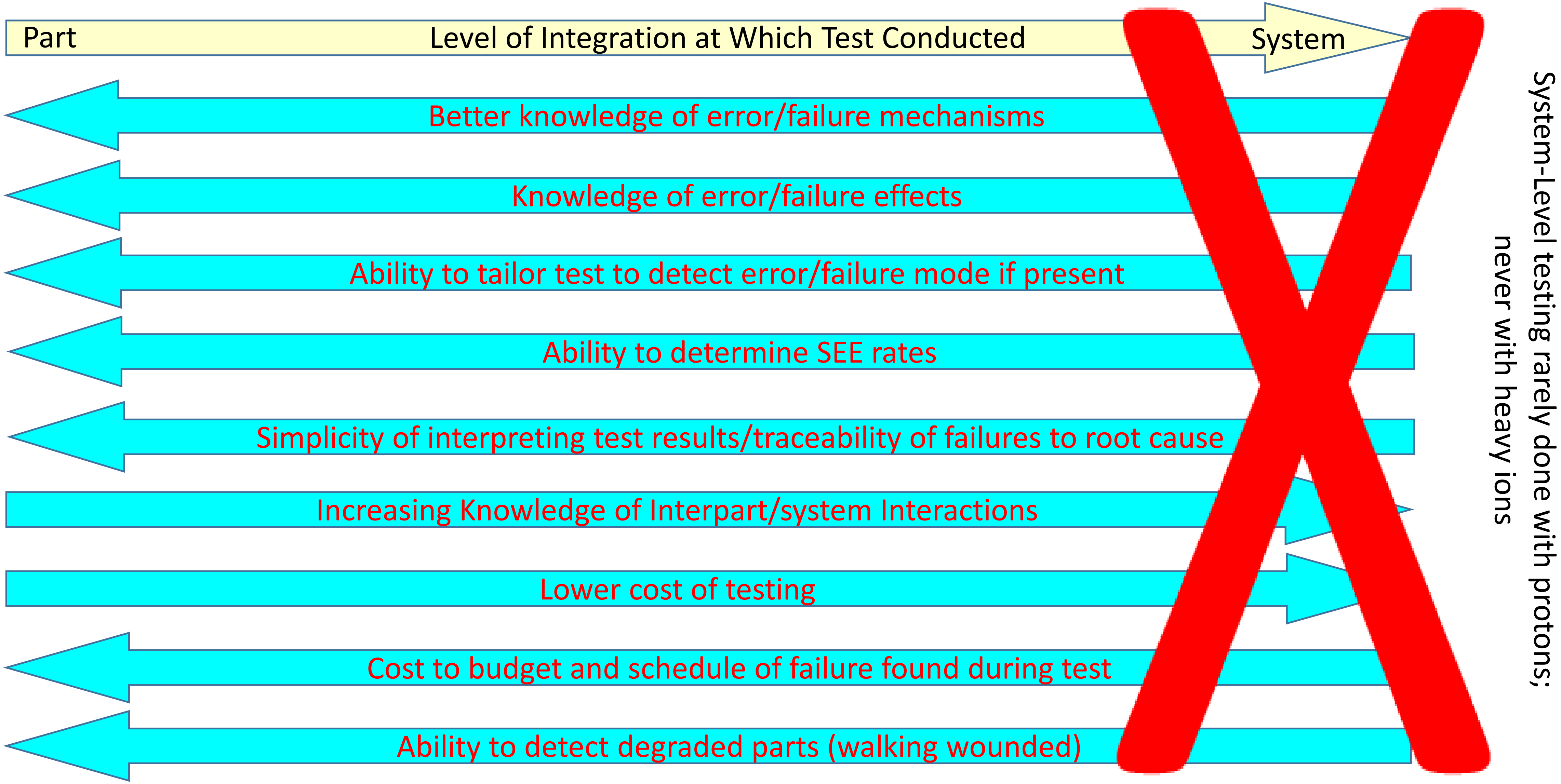
Dose Effect Testing Trends vs. Level of Integration

Part — Level of Integration at Which Test Conducted → System

- ← Better knowledge of part-level error/failure modes
- ← Knowledge of margins to failure
- ← Ability to select dose rate, temperature, bias, etc. based on part technology
- ← Ability to select appropriate sample size based on project risk posture, part history/technology
- → Ability to test to flight-like conditions
- → Increasing Knowledge of Interpart/system Interactions
- → Lower cost of testing (if board/box has ELDRS parts, board/box test cost increased somewhat)
- ← Ability to test parts to appropriate dose levels (board/box limited by weakest part)
- ← Cost to budget and schedule of failure found during test
- ← Ability to detect degraded parts (walking wounded)

Quantity increases in direction of arrow

SEE Testing Trends vs. Level of Integration



Summary

- Verification testing at different levels of integration provides different types of information
  - Part-level testing provides the most specific information on part performance and failure modes
  - Board/box/system-level testing are best for part/system-level interactions; yield limited part information
- Omitting testing at a given level has consequences for performance/cost/schedule
  - Omitting part-level testing saves test cost, but severely impacts cost/schedule if failure subsequently found
  - Modeling part performance from system test or system performance from part data is challenging
- Verification based on Project MEAL and risk posture provides flexible approach
  - Adaptable to any mission—tailorable rather than one-size-fits-all
  - Suggests approaches/strategies for all phases of the mission
  - Matches information required to mitigate risk to the appropriate level of integration for the test
  - Ensures risk in mission design commensurate with project risk posture
- Applications
  - Ensures technology heritage is appropriate for all aspects of MEAL for the TRL claimed
  - Provides framework for assessing risks of using COTS technologies
  - Provides a lens for evaluating testing/data for performance in radiation environment—risks unique to space missions