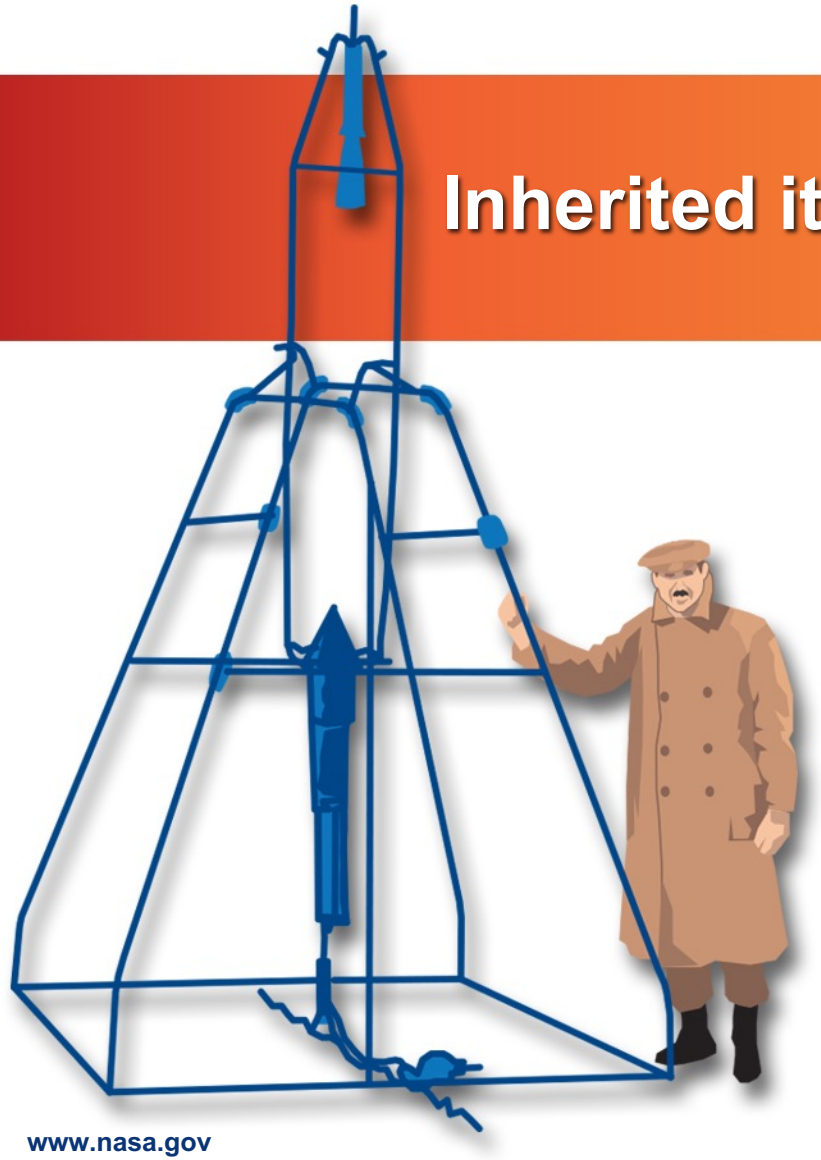
National Aeronautics and Space Administration



Inherited items process 2.0

Dr. Jesse Leitner
Chief SMA Engineer
NASA GSFC
Jesse.Leitner@nasa.gov
321-352-7966

SAFETY and MISSION ASSURANCE
DIRECTORATE Code 300

SMA
SAFETY and MISSION ASSURANCE
NASA Goddard

Outline

- Inherited items process overview
- Phased approach
- Comparison to traditional piece-part approach
- Related items

Inherited items process overview

- Application: products that are inherited and currently built, COTS, to be built-to-print, or otherwise cannot be changed
- Purpose of process: Most such items are built to to different standards and/or level of oversight is disruptive to the development
- The reason for our traditional requirements:
  - Based on one-of-a-kind developments
  - Since there is no basis for reliability, reliability is assured as a by-product of quality measures, piece-part controls, and reliability analyses

- Process has been based on an inherited item risk assessment (I2RA), which is linked to the established reliability of the item combined with what has changed
  - Flight history of the item
  - Changes in item or development process from prior flights
  - Changes in the environment
  - Lifetime comparisons
  - Flight anomalies that affect lifetime
  - Vendor performance and capabilities for the same or similar items

Inherited Items Process 2.0 breakdown

- Process will be divided into two phases
  - Phase 1 is mandatory and is entirely handled within SMA
    - SMA will determine promptly which items are inherited and determine which path will be used for the product based on Code 300 policy (*designated products*)
    - Only (and all) SMA items in the project MAR are affected
      - Project may choose to use the process for items outside of the MAR at their discretion, and we (300) will support as requested
    - Phase 1 products will be based on basic principles (next chart)
      - The Phase 1 SMA approach (contract items) will be delivered within 1 week of obtaining limited information (subsequent charts). This will be denoted the “Phase 1a” report.
      - The Phase 1 final assessment (Phase 1b) will be delivered based on workload and priority, but does not affect contracts
    - Any holdups will necessitate the inclusion of the Code 300 chief engineers (SMA CE, 370 CE, Asst Director/Technical)
  - Phase 2 is optional and may include or require participation from engineering, with potential for multiple products
    - Overall risks of using the product
    - Identification of special operational considerations
    - Those needed for compliance to COTS and inherited items elements of NPR 8735.2
- Products used outside of their datasheets, qualification ranges, or known capabilities will prompt a special actions process involving systems engineering and will not be considered designated products
- The SC CRAE is now the SMA technical authority (under the CSO) for all standard components, with overarching responsibility for SMA for the items

Basic Phase 1 principles

(apply to products used within their bounds and qualification ranges)

- Changing processes for a proven product is unlikely to improve, but more likely to degrade the product
- Changing processes for a proven product is most often not possible to do and doing so or attempting to do so will not only increase risk, but will substantially increase cost and development time
- GMIPs inserted into a standard build only cause a distraction from the standard build process and should only be attempted if there is a history of quality escapes that have entailed mission risk that GMIPs have caught for the product. Review of records for common standard components has not revealed any such escapes.
- Changing parts or part screening practices for a proven design or system will add both risk and cost to the system and likely will not be feasible
- Reliability analyses are needed only if a design is unproven
- The MAR requirements can be categorized as safety, quality, or reliability, but the purpose of quality requirements is to achieve reliability
  - Established standard products are already proven reliable and thus should not be assessed from a piece-part, one-of-a-kind design perspective

Determination of Applicability
(Phase 1 is automatically applied as standard SMA policy)

- Standard or reused product has history in multiple missions and/or indicates noncompliance(s) in MAR compliance matrix
- The process is requested
- Item built to print either to different standards or has inability to apply government surveillance
- Item already existing
- The SC CRAE as the TA over standard products has right to refusal upon initial review

Applicable items will be denoted *designated products*

First steps

- CSO or designee constructs product list based on applicability
  - CSO will ask the following question to the developer SMA lead: "Do you have any products that either already exist or for which it is not reasonable to flow down requirements from the MAR because they are standardized, commercially procured on fixed price contracts, or are commercial-off-the-shelf?" Positive response items will be initially declared designated items.
- CSO or applicable HQE verify product datasheet/spec sheet compliance to project application levels (will not hold up Phase 1 deliverables), e.g.
  - 38V limit on product and 32V +/- 3V application voltage
  - max current 5A on product with application current 3A
  - product used within temperature limits, product proven in same environment for comparable lifetime

  If there are violations, they must be addressed upon discovery, see "Special Cases"
- Standard component CRAE is member of the project SMA team responsible for data collection by interface with contractor SMA representatives
  - The role is analogous to that of a parts engineer, materials and processes engineer, or quality engineer

Specific requests: Parts

- Parts that have been changed from previous designs
- Specialized or custom parts that have been historically produced by one manufacturer but changed to another. Examples:
  - Custom Presidio M123-inspired capacitor now produced by AVX
  - JANS Microsemi MOSFET replaced with Wolfspeed SiC MOSFET
  - Very low ESL Kemet MLCCs replaced with Vishay very low ESL MLCCs
- Any general, but major, changes in parts practices
  - Changes in BGA or CGA approach

These do not affect Phase 1a product

Short-term overall requests

- On-orbit failure (catastrophic) time(s) and cause if known
- Major environmental differential from past experience
- Longest achieved lifetime in similar orbit

This is not intended to identify every anomaly that may have been tied to the component, but rather to address its overall reliability based largely on whether the item has failed or seriously degraded. Operational anomaly details are pertinent to the Phase 2 process, if selected. The results do not affect the Phase 1a product.

Specific requests: Printed Circuit Boards and workmanship

- Change in spec (other than moving to current rev)
  - Switch from Class 3 to Space Addendum
  - Changes in the board design
    - Layout
    - Routing
    - Added or removed reference designators
- Change to HDI design or changing HDI features
  - Microvias or via-in-pad that weren't present before
  - Additional board layers
- New major special restrictions on board materials
  - Switch to halogen free
- Major changes in soldering approach
  - Switch to lead-free solder

These do not affect Phase 1a product

Materials and Processes

- Major materials approach changes
  - Full switch to ROHS compliance
- Switch to additive manufactured items

These do not affect Phase 1a product

GMIP criteria (no vendor info needed except flight history)

- For standard components with at least 10 past flights, minimum 1 at required mission lifetime and no prior instances of NASA catching quality escape that involved risk that vendor QA missed
  - No GMIPs
- For standard components that have had at least three prior NASA projects with no identified instances of NASA catching quality escape that involved risk that vendor QA missed
  - No GMIPs
- When standard component history is not sufficient or available, vendor history of 10 past similar products with similar lifetimes no identified instances of NASA catching quality escape that involved risk that vendor QA missed
  - No GMIPs
- COTS inherited items (not be confused with COTS parts inside): no GMIPs. Lack of past reliability history will be used to establish risk.
- Other commercial fixed-price procurements: closeout photos on internal boards. Project decides if they want to wait for approval after review or not.
- Cost plus contracts with limited prior history or quality escapes caught only by NASA, GMIPs as negotiated.

These are guidelines subject to SC CRAE interpretation and tailoring

Reliability analyses

- Reliability analyses are needed when a system does not have proven reliability
- Reliability analyses are only required when
  - There is no established history
  - There is a major change in some element that has to be propagated through the system to characterize risk

Special cases

- An unestablished COTS (or otherwise unchangeable) product is in the system
  - This will be common to have some in Class D, sub-Class-D, and in technology demonstration missions in general
  - When such products are used, the risk should be characterized based on other products from the supplier and fault-tolerance in the system (This would apply only to Phase 2)
    - For Class D and below, and tech demos, it will often mean flying with acknowledged elevated risk
    - For Class A - C missions, such products should be avoided for critical components providing critical functions (i.e., no backup to maintain the function)
  - If available, a reliability analysis of the product may be used to better characterize the risk
- Use of product in a new and challenging environment that is outside of the datasheet/qualification bounds
  - Primarily this would involve a new radiation environment or using the product at extremes (e.g. temperature) that it wasn't designed for.
  - In some sense, this is no longer an inherited item, it is a new item that requires qualification, although the phase 2 process can be used to determine to what extent a new qualification is required
- Item will be no longer be a *designated product* upon discovery that either case applies

Timeline

- Phase 1 SMA approach (Phase 1a) memo must be complete before contracts are let by the government or the prime for the inherited items.
  - Ideally, once designated items are identified, process should begin
  - When possible, complete the bulk of the process before any contracts are awarded for items that are specifically identified in the proposal or existing in hand
  - Goal - no more than one week for completion of Phase 1a SMA approach for any item, even when items are processed in parallel, but Phase 1a product completed before pertinent contracts are let
    - Phase 1 complete assessment (1b) completed based on workload and priority (not needed for contracts)
- Phase 2 process, when selected, will be on a longer and adjustable timeline, driven by needs, constraints, and information availability

Inherited items process is an SMA implementation per Code 300 policy

- Designated items fall under SC CRAE, all other items are covered by the other discipline areas
- Does not require engineering inputs
  - Identifying ”overall risk of using the item” would be an optional part only in Phase 2
- Similar information needed for waivers, so waiver process will always be a much greater burden, with no value added
- Entire Phase 1 process can be handled within Code 300
  - If project SMA cannot obtain items such as flight history either internally or by requests to contractors, then the same risk would apply in a waiver process.
  - Such items are needed to understand risk
- If engineering would be involved in waiver process, then they have the option of being involved in inherited items process in the same way.

In what instance is engineering involvement required?

- When there is a major change in one of the key discipline areas such that circuit details are needed to characterize risk
  - Reliability analyses may provide enough information to assess such risks
- Such major changes will almost always entail a significant engineering change in the item that would not affect the implementation of SMA requirements, and thus would be resolved over time as part of a qualification or qualification by similarity process
  - Thus, these types of changes would not affect the SMA approach (Phase 1a) memo (SMA relief recommendations)

Phase 1 product

- SMA approach memo (phase 1a) produced in about 1 week (prior to need for contracts), which includes
  - GMIPs approach
  - Parts approach
  - Printed circuit boards approach
  - Materials approach
  - Workmanship approach
  - Reliability analysis approach
- Full Phase 1 assessment report (phase 1a and phase 1b) delivered based on priority and workload, which includes
  - Any determinations of risk from the initially-provided data set
    - Differences in environment or usage outside of datasheet or design limits, or proven lifetimes in comparable environments
  - Any specific recommendations to the project for follow-up
  - Possible recommendation for Phase 2

Phase 2 product

- Provides the full set of background information
  - Select elements of the commodity usage guidelines
- Might address some items outside of SMA-driven risks
- Considers the most mature set of information
- Can be used to address COTS/inherited elements of NPR 8735.2, Hardware Quality Assurance Program Requirements for Programs and Projects

Externally performed I2RAs

- We will work with partners and developers and encourage them to use or form their own process
- Main points to agree upon:
  - What are the thresholds required for processes such as GMIPs
  - The content and construct of a risk statement, should be consistent with GPR 7120.4, Risk Management

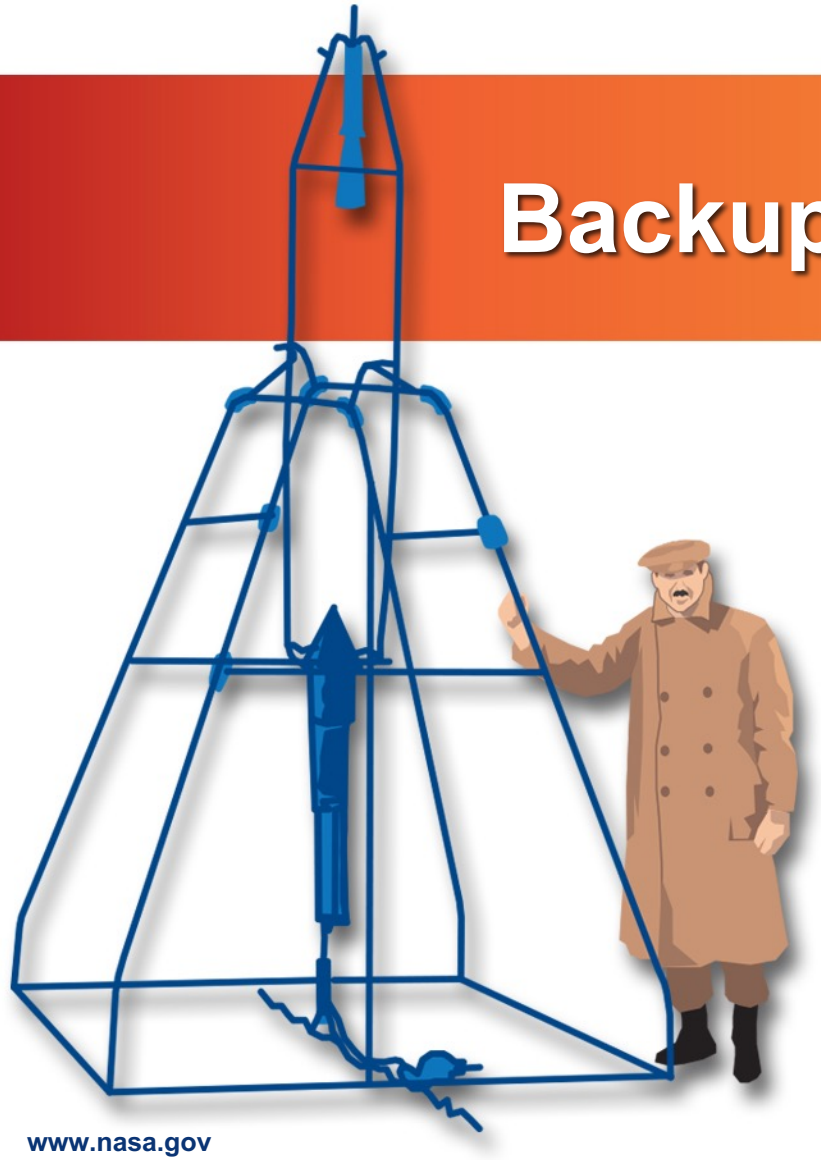
Technical authority

- The standard components CRAE is the defined SMA technical authority (under the CSO) for all designated products.
  - This includes all aspects of quality, reliability, parts, materials, and processes
  - Similar to MPCB CRAE's TA over bare printed circuit boards, lead parts engineer's TA over EEE parts, or MPE's TA over materials and processes that are not in designated items.

Summary

- Inherited items 2.0 is based on the principle that a manufacturer whose products have proven reliability can be trusted to deliver standard products without outside interference in their processes.
- Standard and COTS components that are established as reliable are now called out as a specific commodity analogous to parts, materials, and printed circuit boards.
- Standard and COTS components determined to be designated items will be under the Standard Components CRAE as the technical authority and the responsible SME within each project's SMA program.
- A designated item follows an alternative path within a project's SMA program via the Inherited Items process.
- Phase 1 of the process is mandatory. Phase 1a will provide all necessary input to establish basic SMA requirements in contracts.
- Phase 2 of the process is optional and based on providing a holistic risk picture for the product and aid to obtain compliance to NPR 8735.2.

National Aeronautics and Space Administration



Backup

SAFETY and MISSION ASSURANCE
DIRECTORATE Code 300

SMA
SAFETY and MISSION ASSURANCE
NASA Goddard

www.nasa.gov

National Aeronautics and Space Administration

Ceramic Capacitor Problem RCA

Safety and Mission Assurance

Jesse Leitner, Chief Engineer

April 2021

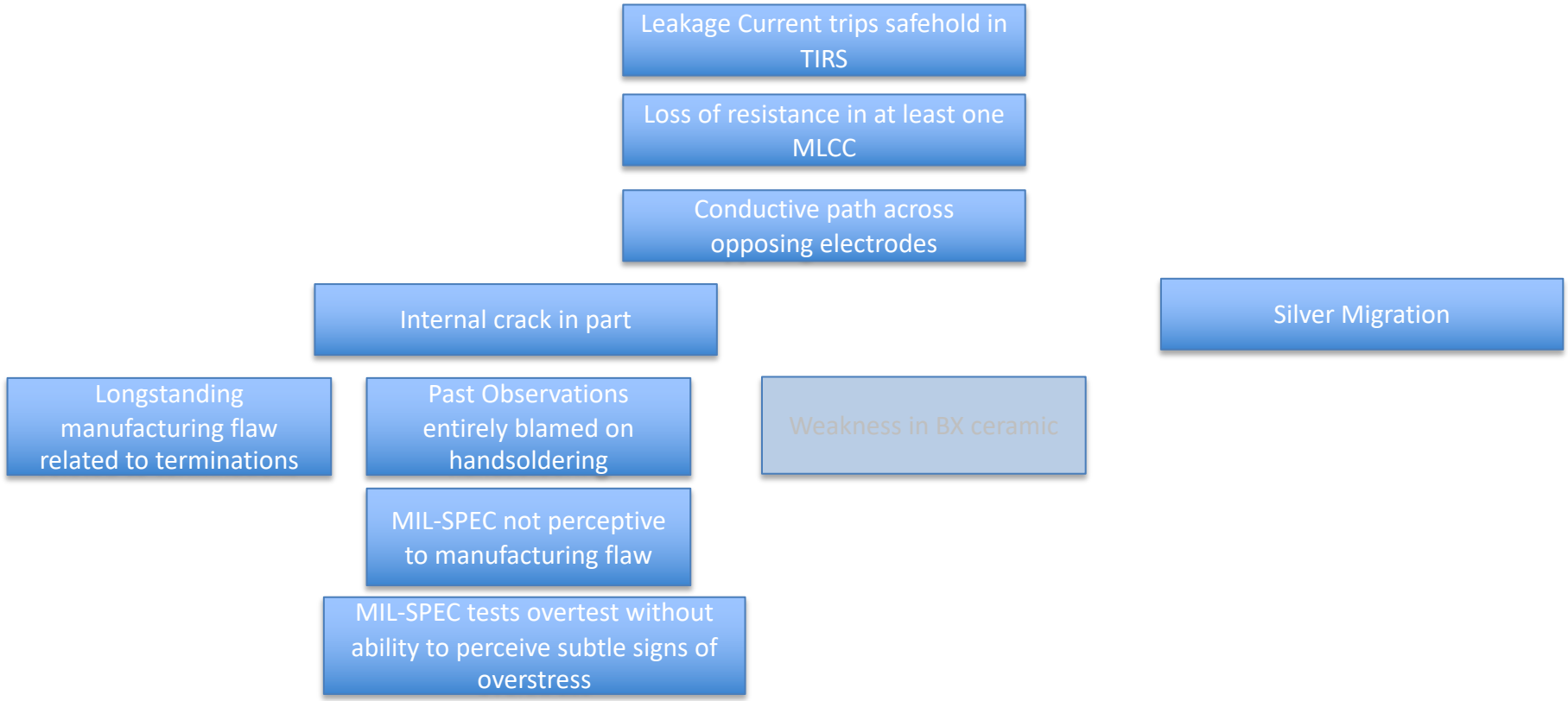
SAFETY and MISSION ASSURANCE DIRECTORATE Code 300

SMA SAFETY and MISSION ASSURANCE NASA Goddard

Hearts, minds, and culture

- When mission success has prevailed and processes have remained the same for decades, it is hard for people to conceive that change is in order
  - Not everyone understands that in almost every significant field continuous improvement and the perpetual need to do more with less are essential
  - In some cases we don't recognize or appreciate the changing world around us or that we may be in process of being surpassed.
- Change has been a long haul, especially for Class B national asset missions because for practices that have long been perceived as critical for mission success, a "money is no object" approach has been taken with the perception that the risk and financial impacts of those processes are as simple as "essential to reliability" and "a small percentage of the budget"
  - In some cases, no amount of data, analysis, and overall evidence are sufficient to change the culture
  - Of course there is a comfort that if I do what we've always done and we fail, then I am covered, but if I am part of a change that is perceived as trying to save a few pennies, then I will be blamed
  - Some change will have to be forced through and stakeholders, customers, and developers must all contribute to the change.

Fault Tree from H6-A-19-01



Root Cause: MIL-SPEC Level 1 Assurance is neither necessary nor sufficient to assure parts to be good for use. Additionally, in some cases, weaker parts may be overtested without knowing overtest has caused overstress

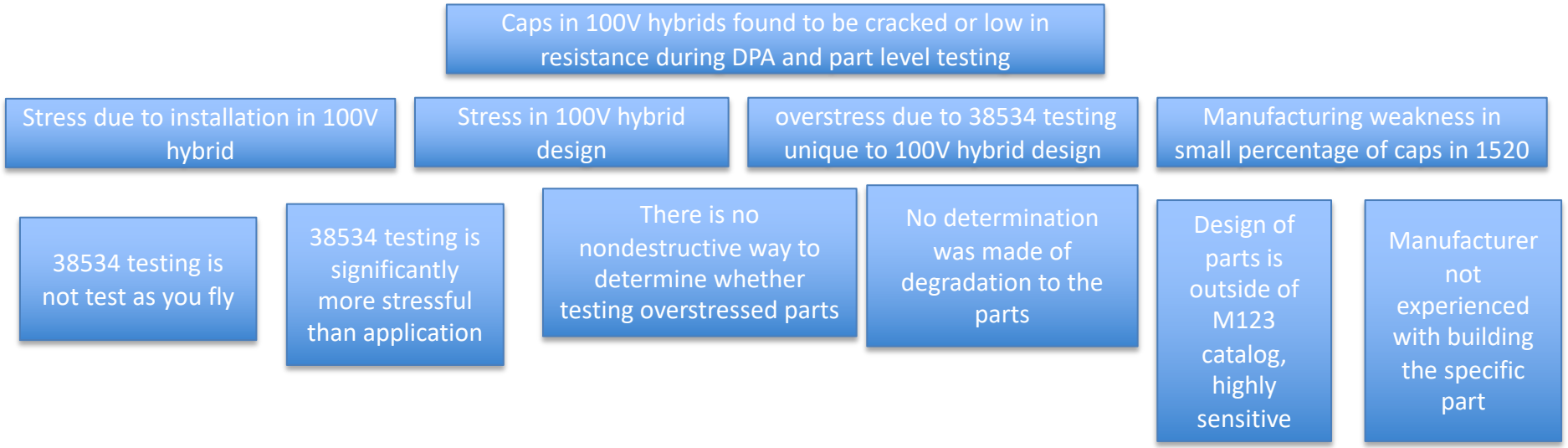
Lessons Learned

- Manufacturer knew of problem for years but was not aware that the problem could materialize without the use of manual soldering or touch-up.
- Manufacturer placed greater emphasis on meeting the MIL-SPECs over product quality because customer expectations and contractual documentation are focused on meeting MIL-SPECs
  - Government and industry believed MIL-SPECs were assurance of product quality and part reliability

Lessons:

1. Over-reliance on testing approaches that are neither necessary or sufficient for success can lead to enormous and broad problems
2. Manufacturers are best tuned to identify processes needed to assure reliability of components based on their own manufacturing processes, experiential observations, and usage

Fault Tree from RWA cap problem



Root Causes:

1. The use of MIL SPEC screening and qualification processes for part designs (both the capacitor and hybrid) that were not within the intended performance range of the MIL SPECs used
2. False confidence created that one reputable vendor's successful use of a mismatched screening and qualification process with a specialized part design implies that another reputable vendor would have the same results
3. MIL-SPEC Level 1 Assurance used as sole determinant of parts being good to use, but is neither necessary nor sufficient to assure parts to be good for use. Additionally, in some cases, weaker parts may be overtested without knowing overtest has caused overstress

Lessons Learned

- RWA manufacturer has certainly demonstrated a working process that has withstood the test of time. However, there may have been at least a semblance of luck that the capacitor manufacturer for years has been able to produce this specialized part robustly enough to withstand the M123 and 38534 (after being installed into the hybrid) screening processes uniformly across the lot (This is actually Presidio's forte).
- Hindsight is 20/20 – the burn-in failure of the two 100v hybrids should have set off more flares. While it may well not have meant that the parts are unusable, it should have indicated that some aspect of the design, testing, or manufacture required further study

Lessons:

1. Over-reliance on testing approaches that are neither necessary or sufficient for success can lead to enormous and broad problems
2. Be sure that multiple discrepancies in part testing give rise to not only a characterization of usability of parts, but also their ability to withstand the tests and overall effectiveness of the tests