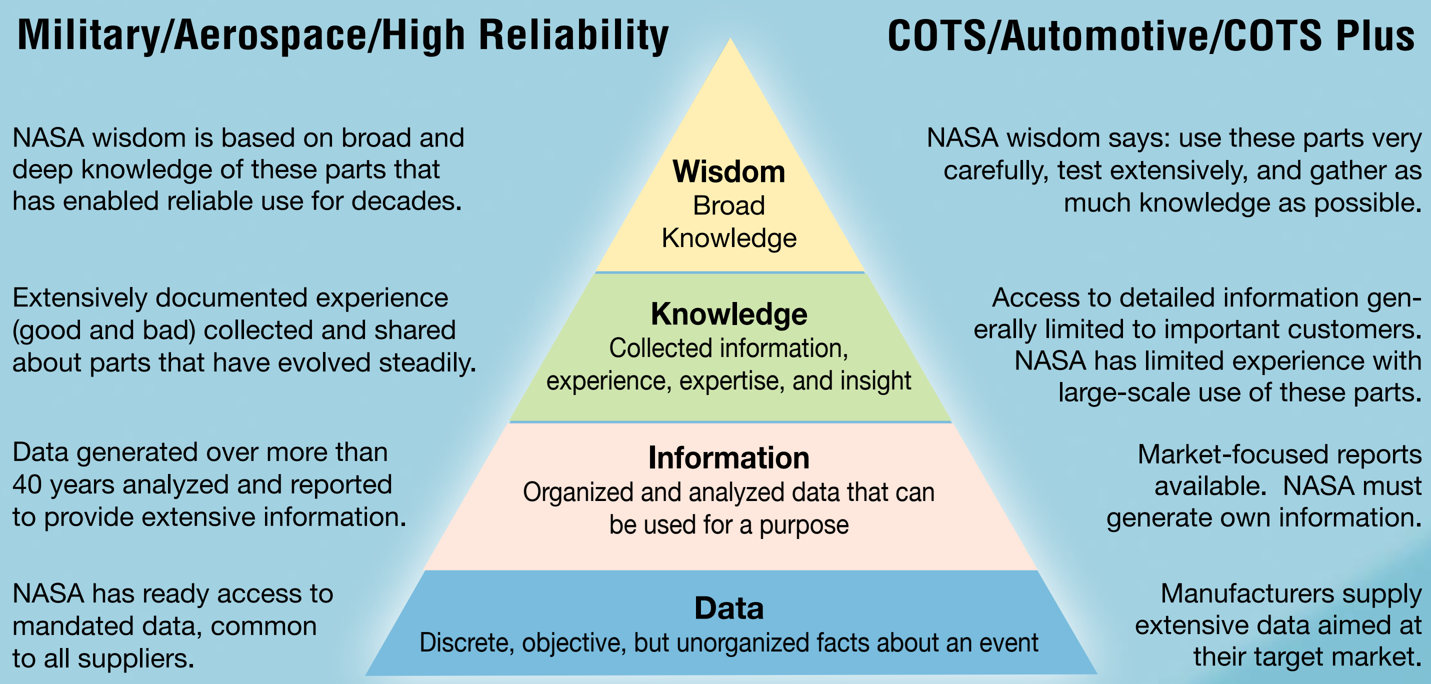

COTS Components in Spacecraft Systems: Understanding the Risk

NASA's Commercial Crew Program (CCP) is stimulating efforts within the private sector to develop and demonstrate safe, reliable, and cost-effective space transportation capabilities to the International Space Station. One initiative involved investigating the possible use of commercial grade electronic parts in launch vehicle and spacecraft designs. The CCP was interested in data that would help frame the technical, cost, and schedule risk trades associated with the use of electrical, electronic, and electromechanical (EEE) parts of a lower grade than traditionally used in most NASA safety-critical applications.

The fundamental question

The fundamental question is "Can commercial-off-the-shelf EEE parts with limited screening be used in crewed flight hardware systems?" The terms "commercial-off-the-shelf parts," or "COTS," and "screening" are broadly defined and not applied consistently. Automotive, commercial aviation, medical, and safety conscious consumer electronics industries engage in assurance processes within their supply chain to establish a basis for the quality and reliability of the EEE parts used in their products before assembling them into critical applications. These assurance processes, with inspections and tests possibly performed on a sample basis depending on criticality, are intended to identify defects and abnormalities that serve as warning signs of a potential for premature failure, reduced performance, and safety.

Parts screening approaches

There is a wide spectrum of approaches to parts screening. At one end of the spectrum, EEE parts used in critical space systems in general are subjected to 100% parts-level inspections and testing to provide high assurance of quality and reliability. At the other end of the spectrum are commercial catalog parts that have not been subjected to any testing other than those established by the manufacturer. An NESC team analyzed two COTS parts screening approaches: one that employs only card-level testing coupled with box-level and system-level testing versus the traditional approach of screening at the parts level prior to card, box and system-level testing. The team concluded that there are fundamental concerns with replacing parts-level screening and qualification with card and box-level or system-level testing only.

Assembling COTS EEE parts on circuit boards for space applications without proper parts-level qualification or additional screening could result in assembling good parts along with any weak parts (parts containing latent defects and infant mortals and/or parts not suitable for the application) into flight hardware, with the questionable assumption that board-, box-, and system-level testing can effectively identify parts that might fail during the anticipated mission lifetime. Proper parts-level qualification is essential to: 1) ensure the part technology, design, and construction is capable of predictable and required performance in the space environment and 2) identify parts that function properly in terrestrial applications but may not perform safely in the more extreme space radiation, vacuum, vibration, and thermal environments found in spaceflight applications. Card-level, box-level, and system-level testing cannot replicate accelerated failure factors that voltage, current, and temperature stresses can provide during parts-level screening prior to installation on a circuit board.

Commercial parts use at NASA

NASA has successfully used commercial parts in spacecraft for specific and sometimes mission-critical applications throughout the Agency's history. This has been achieved by careful selection, qualification, and screening. The level of screening required for commercial parts to ensure they will work successfully is highly dependent on the mission, intended application, environment, mission duration, and part technology. The level of screening is quite well characterized in existing NASA parts documents such as EEE-INST-002. NASA flies non-MIL (non-military) grade parts when the required functionality and/or performance is not available in MIL parts. If a MIL part can be used, they are preferred.

Initial qualitative analysis indicates significant differences in reliability and safety can result between screened MIL parts and unscreened commercial parts. Parts quality, architecture (including the selection of like or diverse backup systems), and mission duration are inseparable variables that must be traded in a mission design. One system architecture could use lower grade parts for short-duration missions (a few minutes to a few days) and possibly exhibit acceptable analytical system reliability. That same architecture may not provide the analytical reliability required for long-duration missions (a few weeks to many months) when using lower grade parts. Parts quality dominates system reliability in long-duration missions where environmental effects like space radiation and single event upsets are more likely to occur. A system design for long-duration missions is an example where NASA would typically employ in critical applications high reliability space-qualified military grade parts or use highly screened and qualified COTS parts.

Alternative approaches

Any alternative approach for the use of COTS EEE parts in critical applications other than those that have proven successful, such as described in EEEINST-002 or similar NASA documents, requires a firm basis for substantiation. Any approach based on architecturally similar redundancy and card-level, box-level, and system-level testing alone is not sufficient to enable widespread use of unscreened parts acquired from commercial catalog distributors in critical applications. To reduce the likelihood that parts failures result in unacceptable mission risk, standard practice dictates designers to: 1) develop and implement a systems engineering-oriented mission assurance program to address EEE parts derating, qualification, traceability, and counterfeit control, and demonstrate how it mitigates the risks associated with EEE parts applications, and 2) provide data supporting the effectiveness of the proposed screening approach, ensuring part failure rates are adequately bounded. □

Important definitions

COTS: An assembly or part designed for commercial applications for which the item manufacturer or vendor solely establishes and controls the specifications for performance, configuration, and reliability (including design, materials, processes, and testing) without additional requirements imposed by users and external organizations. For example, this would include any type of assembly or part from a catalog without any additional parts-level testing after delivery of the part from the manufacturer.

COTS Plus: A COTS part supported by test data available to end users establishing random failure rate assumptions, performance consistent with the manufacturers data sheet and methods to exclude infant mortal parts, parts with latent defects, weak parts, or counterfeit parts. For example, automotive electronics council-certified or compliant automotive parts are one type of COTS Plus.

Parts Qualification: Sample-based mechanical, electrical, and environmental tests at the piece parts level intended to verify that materials, design, performance, and long-term reliability of parts on the same production line are consistent with the specification and intended application until a major process change.

Parts Screening: A series of tests and inspections at the piece parts level intended to remove nonconforming and/or infant mortal parts (parts with defects that are likely to result in early and/or cluster failures) and thus increase confidence in the reliability of the parts selected for use.

Reference NASA/TM-2014-218261