Workshop on Planetary Missions
The challenge of Product Assurance

F. Panin

9 January 2018

Content

- What is Product Assurance?
- The PA disciplines
  - Quality Assurance
  - Safety
  - Dependability
  - Materials and process(MMPP) control
  - Component (EEE) control
  - Software PA
- The space standards system
- Specifics to planetary explorations
- Additional notes

What is Product Assurance ? (1/5)

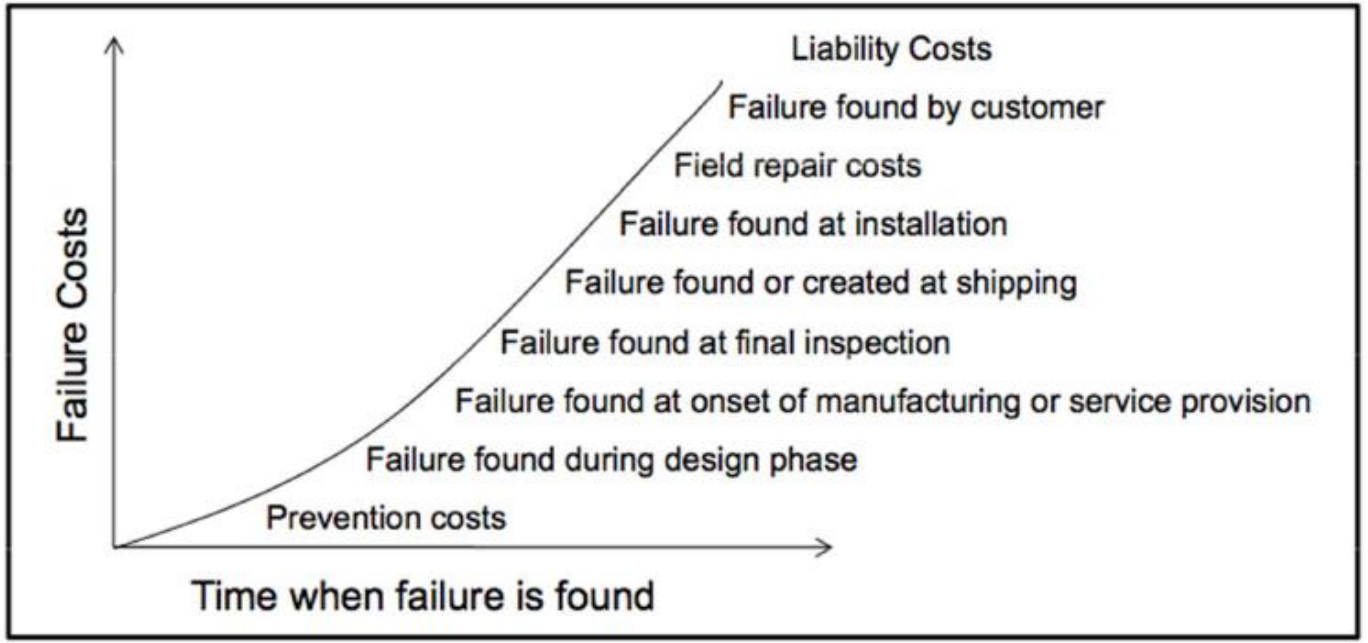
- PA is the amalgam that covers a number of specialist disciplines, often linked with each other:
  - Quality Assurance
  - Safety and Dependability
  - Materials and process control
  - Component control
  - Software PA
- The primary objective of Product Assurance is to ensure that a given space product will perform as required till end of life, in a reliable and safe way, for a given mission.
- A product can be a piece part (e.g. a bolt or a resistor) or an entire spacecraft
- PA applies to all mission phases, from initial mission definition, to the design and development, till production, operations and disposal (mission termination).

What is Product Assurance ? (2/5)

- Planetary missions for scientific exploration are one-off, high budget enterprises that takes at least a decade to develop from initial studies to launch. Operations also can extend to a decade. This justifies a full “commitment to quality”, to ensure mission success and maximum science return.
- PA places emphasis on the identification of potential problems, not only during the mission, but all along the entire procurement till delivery.
- PA contribution to the resolution of problems after their occurrence, is essential
- It is easy to show, that preventing problems is much more cost- and schedule-effective than resolving problems.

What is Product Assurance ? (3/5)

The importance of prevention



What is Product Assurance ? (4/5)

- PA practices and methodologies are based on lessons that have been learned from past experiences, specifically from problems that have actually occurred and their corresponding solutions.
- Experience of relevance is twofold:
  - Ground problems → impact on activities (and associated cost and schedule)
  - On orbit failures / anomalies → impact on performance or life

➔ In essence, PA is good engineering based on experience that is put into practice in a structured and documented manner → need for standardization

➔ Disclaimer: a proper coverage of PA would take far longer than this presentation, that only touches on some key points

What is Product Assurance ? (5/5)

The identification and control of Critical Items (CIs) is a key to prevent problems.

A CI is any potential threat to:

- performance,
- procurement,
- manufacturing, assembly, integration, testing (MAIT),
- safety,
- storage, transport,
- etc

The identification of CIs and their control through implementation of specific actions (with associated deadlines) is part of the PA program of work.

Quality Assurance (1/5)

- Quality Assurance (QA) is a broad domain that includes among other:
  - Documentation and Data Control
  - Traceability and Logbook
  - Metrology and Calibration
  - Non-Conformance Control System
  - Quality Control and Inspections
  - Alerts
  - Selection and surveillance of procurement sources
  - Handling, Storage and Preservation (see 6.4.7)
- End objectives is providing evidence that quality is achieved to the required level.
- Quality characteristics that should be design drivers → the "ilities":

  Producibility, Inspectability; Testability; Repeatability; Operability

Quality Assurance (2/5)

- Non-Conformance control is a fundamental (and recurrent) activity throughout the MAIT phases.
- An item is found “non-conformant” e.g. “Not OK” during inspection, or failure during testing
- A Non-Conformance Report (NCR) is generated to describe the problem
- The issue is discussed with the Customer in a Non Conformance Review Board (NRB)
- The issue is investigated till the root cause is found. This allows deciding on what to do with the item:
    - Use as is
    - Rework (to bring it to the required state: e.g. remove material found in excess)
    - Repair (to restore the functionality and performance)
    - Scrap

Quality Assurance (3/5)

- Non-Conformances and their associated investigation are a key element of the design and development process, as one understand the limitations of the design (and associated implementation) and how to improve it, for the specific application (as opposed to R&D) → “success through failure”

Quality Assurance (4/5)

Tethered Satellite System-1 (TSS-1)

- Joint NASA and ASI mission flown in 1992, aboard the Space Shuttle Atlantis from 31 July to 8 August
- **Mission was to deploy 20 Km of tether**, to verify tether dynamics and its physics
- The tether got **initially stuck at 78 m**, after deployment **continued up to 256 m**, where the effort finally ended
- A **protruding bolt** from a **late-stage modification** of the deployment reel system, jammed the deployment mechanism and prevented deployment to full extension
- Despite this issue, the basic concept of long gravity-gradient stabilized tethers was demonstrated
- Also voltage and current measurements were made, although too low (due to the short tether length) to run most of the experiments

NASA artist's rendering of TSS-1 tethered to the space shuttle

Quality Assurance (5/5)

The NOAA N-PRIME spacecraft mishap

NOAA: National Oceanic and Atmospheric Administration;

Sept 2003: Spacecraft fell during handling at the Lockheed Martin facility of Sunnyvale, CA

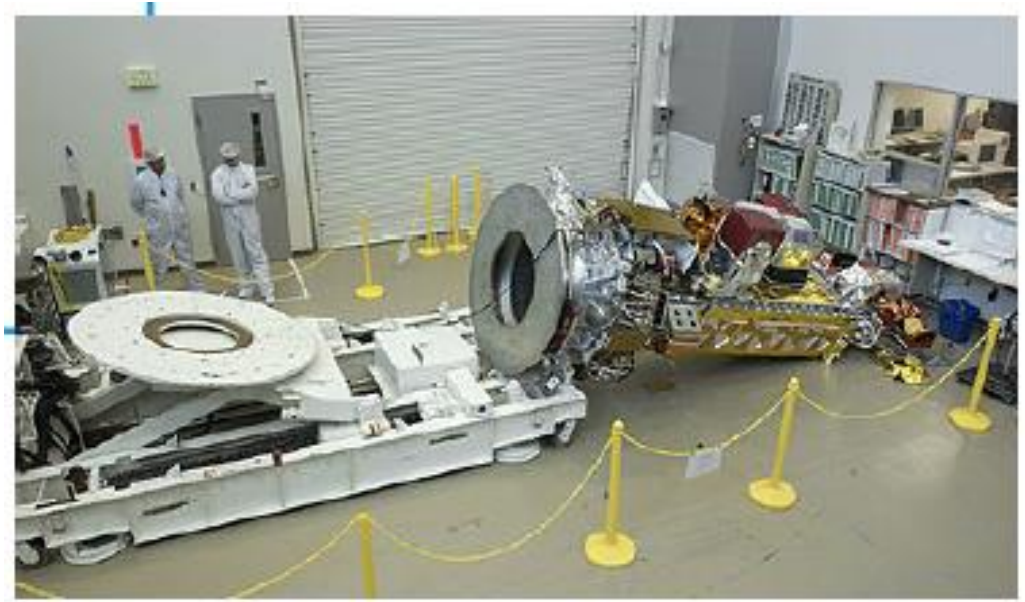
Cart is common with DMSP spacecraft;

DMSP crew started working on the NOAA cart by removing the 24 mounting bolts;

Then they decided to use DMPS cart – but did not document the bolt removal to the NOAA crew!

NOAA crew started their shift by turning the spacecraft….

➔ Root cause: gross violation of procedure



Impact: 290 M US$; launch delayed for years

Dependability (1/3)

Dependability is the capability of providing the required functionalities with a performance level sufficient to achieve the mission objectives. It encompasses:

- Reliability: the ability of performing a required function under given conditions for a given time interval → paramount for planetary missions
- Availability: the ability to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval → important but secondary for planetary missions
- Maintainability: the ability to be retained in, or restored to, a state in which a required function is performed, when maintenance is performed → not relevant

Also, there is a tight link with Safety → "RAMS" in PA jargon.

Dependability (2/3)

Dependability (alias reliability for planetary missions) focuses on failure modes, their effects (local and on the system/ mission) and on the reduction of their consequences.

Considering dependability since early design phases is fundamental for robust design and operations.

All possible failure modes and the corresponding effects are identified. Failure modes are systematically analyzed depending on the severity of their consequences.

The need for functional redundancy (failure tolerance), failure detection methods, and failure recovery are established, through analyses:

- Failure Modes and Effects Analysis (FMEA)
- Reliability analysis: indicators e.g. failure rate and Mean Time To Failure (MTTF)

Dependability (3/3)

Example: Spacecraft Main Engine

The ME plays a key role in the long and intricate journey involved with an interplanetary mission: several burns are needed at precise points along the mission.

It is a critical element from a reliability perspective, as the system cannot afford a redundancy due to mass limitations.

- Rigorous process in ME design and testing → high effort in all PA aspects (one example for all: material and process control)
- At system level: analysis of ME failures and performance degradation, to explore alternative (fall back) ways to perform the mission in the case of ME failure or performance degradation

➔ JAXA Hayabusa journey for asteroid sample return: successful landing in Australia despite several AOCS and propulsion failures

Safety (1/3)

Safety relates to:

- People e.g. injuries during ground operations
- Ground facilities e.g. explosion during propellant loading
- Launcher e.g. unwanted deployment during launch
- Spacecraft
- Environment e.g. pollution resulting from launch crash

At system level, safety assurance applies both before and after delivery of the spacecraft to the Launcher Authority. For the former phase the applicable national and international safety regulations apply, for the latter phase additional safety rules apply depending on the launch range.

A safety hazard is “an existing or potential condition that can result in a mishap”.

Examples: a charged battery, a folded antenna ready to deploy, a loaded propellant tank are safety hazards due to their stored energy; an under-designed structural element (insufficient margins)

Safety (2/3)

A safety program is developed in a structured way:

The system design and operations are analyzed vis-à-vis a number of safety hazard groups: structural integrity/ mechanical, thermal, electrical/ electromagnetic, radiation, chemical etc.

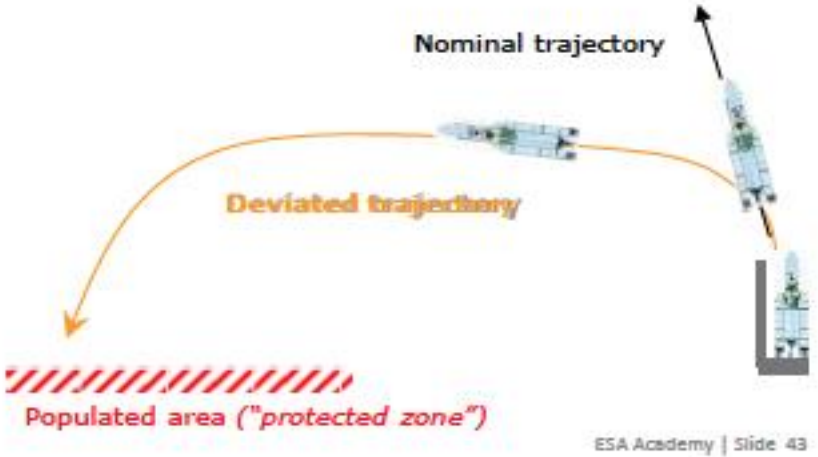
A safety (or hazard) analysis is developed that shows how the identified safety hazards are controlled, through “inhibits”. The number of inhibits that is required depends on the severity of the hazard consequences (e.g. catastrophic, critical)

The verification of the inhibits becomes part of the overall system verification.

Safety (3/3)

Incident of the "Long-March" Chinese Roket

On February, 14th of 1996, 22 seconds after take-off of the new Long-March 3B launcher, a failure in the guidance system occurs, resulting in a dramatic crash onto a village located 3 kilometers from the launch pad …



Materials and processes (1/5)

- Materials, Mechanical Parts, and Processes (MMPPs)

- The control of MMPP is paramount to ensure reliable operation during the mission. This control involves:
  - selection criteria,
  - specific technical requirements,
  - evaluation/ validation/ qualification testing,
  - procurement and receiving inspection,
  - documentation control

- Bottom line is to show that materials are fit for purpose over the mission life

Materials and processes (2/5)

- Materials used in a spacecraft:
  - Metals (e.g. structures, pipework, cables)
  - Polymers (e.g. adhesives, paints, bonding, insulation)
  - Composites (e.g. structures, antennas)
  - Glasses (e.g. optics)
  - Ceramics (e.g. optics, mirrors, insulators)

Materials and processes (3/5)

- Aspects to be considered for material selection:
  - Vacuum → outgassing testing needed to confirm material stability and control contamination
  - Thermal cycling → testing needed to confirm material stability
  - Radiation resistance → testing needed to confirm material stability
  - Galvanic (electrochemical) compatibility
  - Corrosion (including stress corrosion cracking) → testing needed to confirm material stability
  - Wear resistance / tribology aspects → testing needed to confirm material suitability

➔ The above involves a lot of testing, in turn resulting in a cost effort and need for careful planning (also due to limitation in adequate facilities)

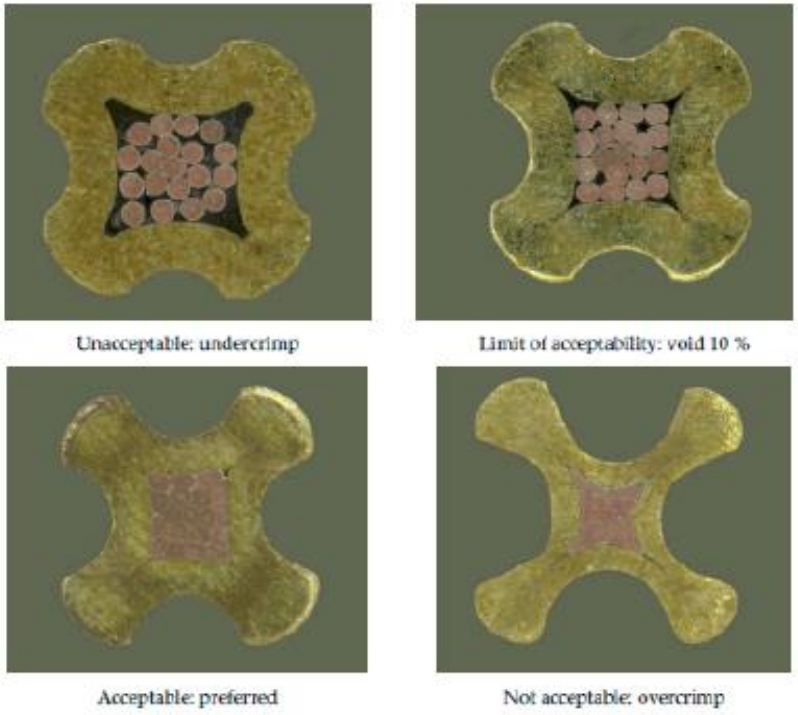
- Some materials are prohibited for use in space:
  - cadmium, zinc as they sublimate;
  - pure tin as it develops whiskers;
  - beryllium as it promotes cancer when inhaled during machining
- Specifics apply to Printed Circuit Boards (PCBs)

Materials and processes (4/5)

- Processes used in a spacecraft:
  - Bonding
  - Coating/ painting
  - Plating
  - Cleaning
  - Composite manufacturing
  - Welding/ brazing
  - soldering
  - Machining/ forming
  - Heat treatment
  - Other … other ... other specific to the application
- A specific process is the assembly of components onto PCBs (Surface Mount Technology)
- Operators and inspectors need to be trained and certified

Materials and processes (5/5)

Example of critical process – crimping



Components (1/4)

- Electrical, Electronic, Electromechanical (EEE) “parts”:

  Capacitors, resistors, crystals, filters, fuses, relays, heaters, thermistors, diode/ transistors, magnetics, …., switches, ..., wires and cables → but not solar cells!

- The control of EEE components is paramount to ensure the reliable operation of a space unit employed in a spacecraft. This control involves:
  - selection criteria and requirements,
  - evaluation/ qualification testing
  - screening, lot acceptance testing
  - procurement and receiving inspection
  - documentation control
- For large missions where a suite of instruments are used, usually ESA adopts the services of a Coordinated Component Procurement Agent (CPPA)

Components (2/4)

- Derating of components is essential to ensure reliability. Derating is the reduction of component mechanical, thermal, and electrical stresses below the rating values specified by the manufacturer.
- This allows lowering failure rates, extending life, and improving end-of-life (EOL) performance
- Derating rules applies to voltage, current, power, temperature for the various components types
- The environmental factors already seen for MMPP apply to components, but radiation effects plays a key role for interplanetary explorations. Additionally, moisture resistance is necessary.
- Component failure mechanism breakdown:

  50% - assembly on PCB / 30% - operation / 15% - design / 5% - processing

Components (3/4)

- Component quality (reliability) is in three classes (1 to 3) with different level of assurance in their performance. Planetary missions use the highest level.
- Space qualified qomponents come with a lot-specific Certificate of Compliance (CoC) against the applicable specification/ requirements. This is a commitment by the manufacturer, and also a warranty against problems after delivery.
- A commercial component is always “subject to changes without notice” (change in processes, design, materials, testing) and the commitment / support by the manufacturer is limited. In addition, data sheet parameters may be incomplete or loosely defined to safeguard production yield.
- The ESA policy is that the use of commercial components is allowed only to fill gaps in specific applications, not as a replacement of qualified components when these are available. Commercial components must be up-screened to class 1

Components (4/4)

Space Radiation Blamed for Phobos-Grunt Crash

Topic: **Phobos-Grunt spacecraft**

The recent crash of Russia's Mars probe was caused by a glitch in the onboard computer system under the impact of space radiation, Federal Space Agency head Vladimir Popovkin said on Tuesday.

14:52 31/01/2012 © RIA Novosti

VORONEZH, January 31 (RIA Novosti)

Tags: Phobos-Grunt, Roscosmos, NASA, Vladimir Popovkin, Voronezh, Russia

- **Nature – Feb. 2012**

Failed Mars probe Russia's Phobos-Grunt spacecraft, which failed to escape Earth orbit in its attempt to reach Mars's moon Phobos last year, was doomed by electronics components not certified for use in space, which in turn led to a computer glitch, according to an official analysis commissioned by the country's space agency, Roscosmos. Its main conclusions were released on 3 February. Once the craft reached orbit, **two electronics chips suffered radiation damage (which they had not been designed to withstand), causing two processors to reboot and crashing the on-board computer program**

The space standard system (1/2)

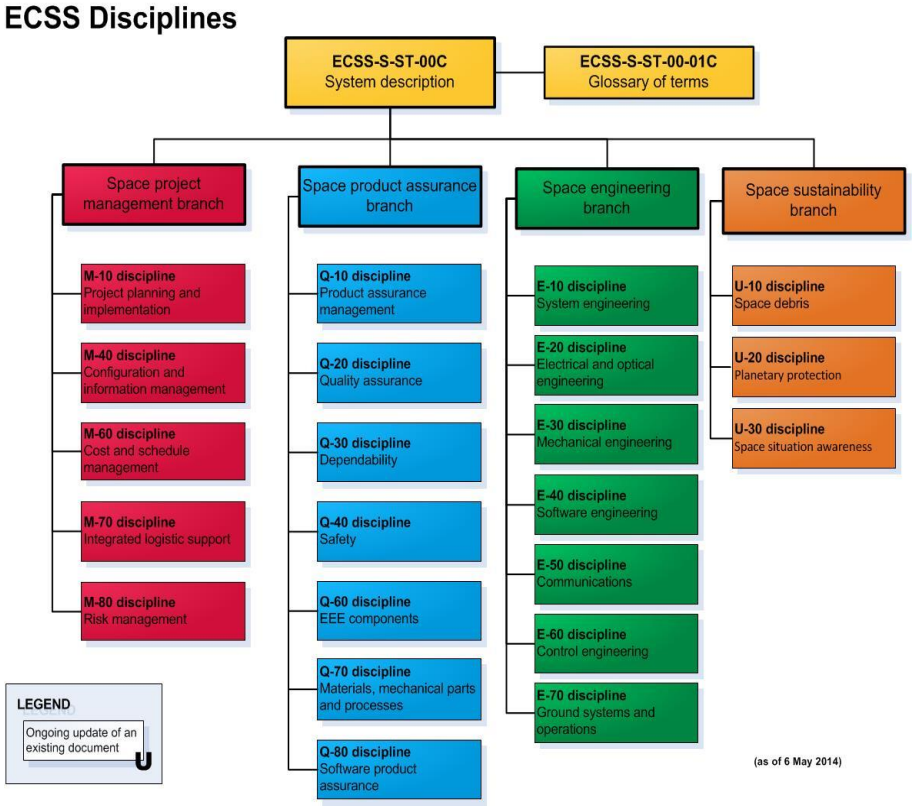
The European Cooperation for Space Standardization(ECSS) is an effort by ESA, the national space agencies and industrial partners.

The ECSS system is a comprehensive, multidisciplinary set of standards that cover engineering, management and PA.

Standards need to be tailored by ESA to suit the constraints affecting each procurement (from unit to entire spacecraft), and also to match the mission objectives and class (risk policy).

Standards embody past experience, and are based on the history of failures and successes of past missions. They are aimed at providing the highest assurance of successful results, both on ground during procurement phases, as well as during actual on orbit operations. Deviations from standards constitute a risk.

The space standards system (2/2)



Specifics to planetary exploration (1/1)

In addition to the usual environmental factors:

- Vacuum (no convection for heat transfers; outgassing)
- Mechanical loads (high levels at launch; zero-g afterwards → deployment → on ground testing)

Long interplanetary cruises imply one of more of:

- Odd thermal exposures: not a simple thermal cycling between two extremes, but a sequence of phases with different ranges; min and max temperature may be extremely low or high e.g. -240C or > +500C)
- Radiation levels → Radiation Hardness Assurance adds to PA disciplines
- Mechanism actuation at late mission phases (need for long life, friction issues)

Science instruments are in general sensitive to contamination (particulate/ molecular) → impact on material choice, need for analyses, testing and verifications

Additional notes (1/2)

- Suggested reading:
  - “To engineer is human: the role of failure in successful design”, Petroski
  - “Design for the real world”, Papanek

- Suggested course:
  - “Space system development: lessons learned” by Aerospace Engineering Associates

Additional notes (2/2)

- For reflection:
  - "PA stands for Preventive Approach" ….. or "Problem Avoidance"
  - "I wish I had never to say: I told you" *PA Manager mantra*
  - "Everything an be accepted, but one has to face the consequences"
  - "Never say: this is not my responsibility" *unknown*
  - "Confidence is the feeling you have before you fully understand the situation" *Mark Twain*
  - "Test as you fly, fly as you test" *too many to name*
  - "In God we trust, all others must bring data" *Edwards Deming*
  - "A man without reliability is utterly useless" Confucius
  - "Product Assurance is not rocket science, but it makes rockets fly" *Roberto Ciaschi*
  - "Your best teacher is the array of mistake you have made" *unknown*
  - "Without a standard there is no logical basis for making a decision or taking an action" *Joseph Juran*
  - "Faster, better, cheaper: pick two" *unknown, following failures resulting from this approach*