Quality Assurance for Space Projects

by

T. Sgobba and J. M. Carranza

IAASS Quality Assurance Course September 2007
These handouts are released for general instruction purpose only. These handouts are not meant to take any precedence on applicable project requirements, documents and definitions.
QA Course Outline

◆ Course Introduction
  – The space environment
  – Some key concepts in systems development
  – Considerations on failures and causes
  – What is Product Assurance?

◆ Concepts, Techniques and Standards : part I
  – Introduction
  – Basic values and principles
  – QA Main elements/techniques: part I
  – Standards evolution
QA Course Outline (cont’d)

- Concepts, Techniques and Standards: part II – H/W
  - QA Main elements/techniques: part II
  - QA during project phases
  - ECSS-Q-20B

- Special Techniques – H/W
  - Statistical techniques
  - Cost of Quality
  - Alert Systems

- Concepts, Techniques and Standards: part II – S/W
  - Basic concepts
  - Space SW standards
  - SW Process Capability Assessment
Course Introduction

Before starting!
The space environment
Launch environment

- Accelerations & vibrations
- Acoustic noise
- Shock
- Rapid depressurisation
## Space environment

<table>
<thead>
<tr>
<th>Orbit</th>
<th>LEO (low earth orbit)</th>
<th>GEO (geostationary orbit)</th>
<th>Planetary missions and Deep Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Altitude</td>
<td>200 tot 800 km</td>
<td>36000 km</td>
<td>n.a.</td>
</tr>
<tr>
<td>Temperature</td>
<td>-100°C to +100 °C 16 cycles/day</td>
<td>-150 °C to +120 °C 1 cycle /day</td>
<td>-180 °C to +260 °C</td>
</tr>
<tr>
<td>Vacuum</td>
<td>10^-4 to 10^-9 mbar</td>
<td>10^-9 to 10^-10 mbar</td>
<td>to 10^-14 mbar</td>
</tr>
<tr>
<td>Plasma</td>
<td>Dense cold plasma Aurora</td>
<td>Hot Plasma</td>
<td>Thin plasma</td>
</tr>
<tr>
<td>Radiation</td>
<td>hv [X-ray (V)UV, Vis, IR]</td>
<td>Van Allen belts (partial)</td>
<td>Cosmic Rays</td>
</tr>
<tr>
<td></td>
<td>Particles (98 % e^-, 2% p^+, Van Allen Belts)</td>
<td>Solar particle events</td>
<td>Solar particle events</td>
</tr>
<tr>
<td>Impacts</td>
<td>Micrometeorites / Debris</td>
<td>Micrometeorites/ Debris</td>
<td>Comets Meteoroids</td>
</tr>
<tr>
<td>Atmosphere</td>
<td>Atomic Oxygen</td>
<td>n.a.</td>
<td>Planets (reactive gasses)</td>
</tr>
</tbody>
</table>

Note: Internal boxes temperature typically cycling from -10°C to +60°C
Space environment and its effects

**ENvironments**

- Galactic Cosmic Rays
- Energetic Solar Events
- Radiation Belt Particles
- Hot Plasmas
- Ionospheric Plasma
- Residual Atmosphere (Atomic Oxygen)
- Meteoroids & Space Debris

**(increasing charged-particle energy)**

**Effects**

- Upsets to electronics
- Payload interference
- Radiation hazards
- Damage to components
- Electrostatic discharge
- Parasitic currents...
- Chemical erosion of surfaces
- Puncture of surfaces

IAASS Quality Assurance Course  September 2007
Some key concepts in systems development
Definition of system

System
A set of interrelated components which interact with one another in an organised fashion toward a common purpose

or better

A composite, at any level of complexity, of personnel, procedures, materials, tools, equipment, facilities and software. The element of this composite entity are used together in the intended operation or support environment, to perform a given task or achieve a specific production, support or mission requirement (MIL-STD-882)
Related definitions

- **Project**
  The design, development and operation of one or more systems

- **Program**
  A related series of projects that continue over a period of time, which are designed, or are in support of, a focused scientific or technical goal, and which are characterised by: design, development and operations of systems
Hierarchical system terminology

Example of terminology (NASA scheme):

- **System**
  - **Segment**
    - **Element**
      - **Subsystem**
        - **Assembly**
          - **Sub-Assembly**
            - **Part**

Schemes are not used rigidly. Projects often establish their own terminology or delete some layers. From the SE point of view a segment, element, or subsystem is a system in its own right.
Definition of system engineering

System engineering

The application of scientific and engineering efforts to:

- transform an operational need into a description of system performance parameters and a system configuration
- integrate related technical parameters and insure compatibility of all physical, functional, and program interfaces
- integrate safety, reliability, human factors into the total engineering effort (MIL-STD-499)
Three system engineering key concepts

- Configuration
- V-Cycle
- Project Life-Cycle
Configuration related definitions

**Configuration**
The functional and physical characteristics of a product as set forth in technical documentation and achieved in the product

**Configuration Identification**
The activities of determination of the product structure, selection of configuration items, documenting their physical and functional characteristics including interfaces and subsequent changes
Configuration related definitions (cont’d)

**Configuration Baseline**
Configuration (documentation) of a product, *formally established at a specific point in time*, which serves as reference for further activities.

**Configuration Control**
Configuration (change) control is the means to assess and record changes to the functional and physical characteristics of a product, monitor such changes during preparation, review, approval and implementation.
Design and verification cycle: the V-cycle

- Mission Requirements, System Concept
- System Specification, System Verification Plan
- CI Specification, CI Verification Plan
- “Build-to” Documents, Inspection Plan
- Fabricate, Assemble and Code
- Integrate System, perform System Verification
- Assemble CI, perform CI Verification
- Inspect to “build-to” Documents
- Demonstrate and Validate the System
- Integration and Verification Sequence
- Decomposition and Definition Sequence
Project Life-Cycle

Categorisation of everything that should be done to accomplish a project in distinct “Phases” separated by “Control Gates” for GO / NO GO decisions.
Project Life-Cycle

MISSION NEED DETERMINATION

- Concept Exploration  Phase A
- Preliminary Design   Phase B
- Detailed Design      Phase C
- Production          Phase D
- Operations          Phase E

DISPOSAL
Phase A : Concept Exploration

- **Purpose:**
  Determine technical feasibility and compatibility with overall plans

- **Major Activities:**
  - Prepare “Mission Requirements”
  - Develop top-level requirements
  - Identify project constraints and system boundaries
  - alternative design concept (risk, cost, schedule, technologies)

- **Baseline:** Mission Requirements

- **Control Gate:** Mission Definition Review (MDR)
Phase B: Preliminary Design

- **Purpose:** Establish the overall system design and technologies

- **Major Activities:**
  - Establish system requirements and verification requirements
  - Establish a baseline design solution and concept of operations
  - Establish a verification approach
  - Prepare a “Design and Development Plan”
  - Prepare a “Product Assurance Plan”
  - Initiate Configuration Management
Phase B: Preliminary Design (cont’d)

- **Baseline:**
  - System Specification
  - System architecture and concept of operations
  - “Design to Specifications” at all levels
  - Plans (Design&Development, PA etc.)

- **Control Gates:**
  - System Requirements Review (SRR)
  - System Preliminary Design Review (PDR)
  - Lower-level PDRs
  - Safety Review Phase 1
Phase C: Detailed Design

Purpose:
Complete the design of the system

Major Activities:
- Finalise/refine verification plans
- Prepare “Build-to” specifications, drawings, technical lists,
- Prepare interface control documents
- Prepare manufacturing, assembly and integration plans
- Update analyses
Phase C: Detailed Design (cont’d)

- **Baseline:**
  - “Build-to” specifications, drawings, technical lists,
  - Verification Plans
  - Manufacturing- Assembly-Integration Plans
  - “As designed” Configuration Data (CIDL)

- **Control Gates:**
  - System Critical Design Review (CDR)
  - Lower-level CDRs
  - Safety Review Phase 2
Phase D: Production

**Purpose:**
Manufacture, assembly and integrate lower level items to create the system. Demonstrate that system requirements are met.

**Major Activities:**
- Develop verification procedures at all levels
- Fabricate (or code) the items
- Integrate lower level items and perform verifications
- Perform system verifications (qualification + acceptance)
- Prepare operations and maintenance manuals
- Finalise “Integrated Logistics Support Plan”
- Prepare operational procedures and initiate training
Phase D: Production (cont’d)

- **Baseline:**
  - “As-build” Configuration Data (ABCL)
  - Command sequences, telemetry validation, ground data processing
  - On-board procedures (when applicable)
  - Manuals (operator, user, maintenance)
  - Hazard Reports and Safety Compliance Data

- **Control Gates:**
  - Manufacturing Readiness Reviews (MRR)
  - Test Readiness Reviews (TRR)
  - Qualification and Acceptance Reviews (QR/AR)
  - Safety Reviews Phase 3
Phase E: Operations

- **Purpose:**
  Operate the system

- **Major Activities:**
  - Training (operators, maintainers, astronauts)
  - Conduct mission(s)
  - Maintain, reconfigure and upgrade the system
  - Dispose of the system
Phase E: Operations (cont’d)

- **Baseline:**
  - Modification and changes
  - Problem and failure reports

- **Control Gates:**
  - Operation Readiness Reviews (ORR)
  - System upgrade reviews
  - Decommissioning review
Considerations on failures and causes
Space insurance claims…lift-off

Billion

$1.4
1.2
1.0
0.8
0.6
0.4
0.2
0

1980 '82 '84 '86 '88 '90 '92 '94 '96 '98 '00

IAASS Quality Assurance Course  September 2007
Space insurance claims…lift-off (cont’d)

Contributing factors:

◆ Increased number of commercial satellites on orbit.

◆ Significant increase of satellites technical complexity. Average payload power almost tripled from 2.3 kW in 1996 to 6.3 kW in 2001.

◆ Trend to shorten the time from contract award to launch, puts pressure on manufacturers to perform less rigorous analyses/tests. Average production time from 45 months in 1996 to 33 months in 2001.

Space insurance claims…lift-off (cont’d)

Below the distribution per S/S of anomalies experienced by satellites launched in the period 1990-2001. Only anomalies with impact on mission included (i.e. no loss of redundancies or minor mission interruption)

(Data source: AAS 03-071, Robertson/Stoneking NASA GSFC)
Space insurance claims…lift-off (cont’d)

“A large number of satellites anomalies are observed on the first day of the mission. After reaching 10% of a satellite design life, the anomaly failure rate declines precipitously and continues to decline thereafter. ...This indicates that design flaws and latent manufacturing defects have a greater effect on mission success than materials contamination or fatigue/overstress. The standard spacecraft integration and test process already invests significant effort to expose design flaws and physical defects before launch. The fact that some mission critical faults get through shows that this effort is not excessive...”

(From AAS 03-071, Robertson/Stoneking NASA GSFC)
Space systems failures causes

IAASS Quality Assurance Course

2000 1960

February 2007

IAASS Quality Assurance Course September 2007
Space systems failures causes (cont’d)

“...if there is any surprise in the synoptic results it is the prominence of manufacturing, production and assembly...a strong cautionary note to those seeking to marginally hold down production costs by cutting quality assurance, inspection, audit...”*

* FAILURE SPACE: A Systems engineering look at 50 Space System Failure
What is Product Assurance?
Product assurance disciplines

- Quality Assurance
- Reliability
- Safety
- Materials
- EEE Components
- Configuration Management
Product assurance definitions

- **Product Assurance:**
  A discipline devoted to the study, planning and implementation of activities intended to assure that the design, controls, methods and techniques in a project result in a satisfactory level of quality in a product (ECSS-P-001A)

- **Mission Assurance:**
  Mission assurance provides confidence to the project and sponsors that the mission will be successfully completed through its planned support activities, standardised processes, and monitored project milestones. Mission assurance brings a set of specialised disciplines to support the project team environment (NASA)
European product assurance space standards

- **OLD**: ESA Procedures Standards and Specifications (PSS)

- **NEW**: European Cooperation for Space Standardisation (ECSS)
Concepts, Techniques and Standards

Part I
Introduction
What is Quality?

- In technical usage, *quality* can have two meanings:
  - (1) *the characteristics of a product or service that bear on its ability to satisfy stated or implied needs*
  - (2) *a product or service free of deficiencies."

- It is also defined as:
  - *Quality of design*
  - *Product conformance*
  - *Quality of performance*
Product Conformance

Traditional QA deals mainly with means and practices to achieve and ensure achievement of:

**PRODUCT CONFORMANCE:**

Product conformance relates to the fidelity with which the product conforms to the design.
POOR QUALITY IS COSTLY!

Companies that measure their “poor quality” costs for the first time are usually shocked at what they find.

Reducing “poor quality” costs has been compared by J.M. Juran to mining gold (Gold in the Mine), because it may translate directly into increased profits and higher production capacity (Hidden Plant).
What is a quality system?

Product quality depends on many variables. The processes, organisation, resources and procedures that manufacturers and suppliers use to control these variables to produce a product of consistent quality which meets defined specifications is called a *QUALITY SYSTEM*.

* The definition as formulated applies specifically to the manufacturing environment.
The four QS controlled elements

- **PERSONNEL**: to perform or supervise the production tasks
  [Competence, training, identification, motivation, attributes]

- **MATERIAL**: on which to apply production processes (component, sub-assembly, etc.)
  [Type, condition, capability, quantity, identification]

- **MEANS**: tools, equipment and facilities required to perform the task
  [Type, condition, capability, identification, location, environment]

- **DOCUMENTATION**: input/output (specifications, drawings, records, reports, orders, etc.)
  [Content, control, condition, identification, distribution]
Quality system as business strategy

There are companies, in particular SMEs, which enforce QA rules only when required by the customer. Such companies miss the strategic business value of the Quality System for:

- competitiveness improvement
- product improvement
- organisational continuity/growth
- personnel motivation
Quality system as assurance technique

- The ability not only to achieve Quality (meet or exceed customer requirements/expectations) but to demonstrate that an effective system is in place and maintained for that purpose

- For the European Union (as for any organisation having regulatory responsibilities for safety), the implementation of a Quality Assurance system by a company is a pre-condition for valid certification assessment of their products compliance to relevant norms

- Safety and high reliability required by space systems has made QA systems implementation mandatory during any project phase (design, manufacturing and operations)
Quality assurance

QUALITY ASSURANCE

METHOD
(to obtain)

- write what you do
- do as written
- prevent mistakes
- learn from mistakes

OBJECTIVE
(to demonstrate)

- perform verifications
- prove verifications

QUALITY

IAASS Quality Assurance Course
“Quality assurance is the planned and systematic activities implemented within the quality system and demonstrated as needed to provide adequate confidence that an entity will fulfill requirements for quality”.

(ISO-Vocabulary)
Evolution of quality system concepts

Major changes of focus:
- from *external quality* to *internal quality*
- from *product/service improvement* to *process improvement*
- from *second-party certification* to *third-party certification*
From artisan to quality control

- **small workshop**: proprietor knowing everything - customer in touch
  - proprietor training workmen and checking the end product
  (good product quality - optimum quality costs)

- **larger workshop**: division of work - intermediate merchants
  - intermediate supervisors - end product checked by supervisors
  (poor external quality - high quality costs)

- **factories**: larger quantities and use of machines
  - work "atomisation" and quantity incentives
  - managers and intermediate supervisors - end product
  checked by independent inspectors
  (good external quality - poor internal quality - high quality costs)
From artisan to quality control (cont’d)

- **evolving factories**-long management chain-industrial engineering functions-sales management-ubiquitous independent inspectors-inspector supervisors-Inspection Department (good external quality-good internal quality-high inspection costs)

- **modern factories**-management driving quality-quality planning-marketing functions-preventive quality approach-limited number of inspectors-Quality Control Department (QC engineering etc.) (good product quality-optimum quality costs)

"Quality control is operational techniques and activities that are used to fulfill requirements for quality. It involves techniques that monitor a process and eliminate causes of unsatisfactory performance at all stages of the quality loop". (ISO-Vocabulary)
Statistical quality control

- Statistical Quality Control was initially the application of statistical techniques and economical considerations to acceptance sampling (pioneered by H. Dodge and H. Romig of Bell Telephone Labs).

- The purpose was to avoid the cost of 100% lot inspection, while lowering the customer’s risk to receive a defective product, and the manufacturer’s risk to reject a good one.
Statistical process control

- Statistical Process Control (SPC) is an analytical tool invented by W.A. Shewhart of the Bell Telephone Labs to assess, monitor and control manufacturing processes.

- SPC is applicable to areas in which a large number of parts are being produced or a process is being repeated many times.

Notes:
- The term Statistical Quality Control includes nowadays statistical process control and statistical acceptance sampling.
- SPC cannot be applied to software products because all copies of software are exactly identical.
Total quality management (TQM)

- By the 1980s the idea was advancing that quality leadership could be achieved only by applying the entire array of quality tools and techniques **to all functions and all levels of a company**. This approach was called *Total Quality Management* or TQM. (In Japan it is called *Company-wide Quality Control*).

- “Total quality management is the management approach of an organization, centered on quality, based on the participation of all of its members, and aiming at long-term success through customer satisfaction and benefits to all members of the organization and to society”.

  (ISO-Vocabulary)
TQM: process model for quality

A process is defined as a “set of interrelated or interacting activities which transforms inputs into outputs”
Total quality management (cont’d)

- TQM objectives are well defined in practical terms by the “Malcom Baldrige National Quality Award” criteria published by the U.S. National Institute for Standards and Technology (NIST):

  - leadership
  - information/analysis
  - strategic quality planning
  - human resource development/management
  - management of process quality
  - quality and operational results
  - customer focus and satisfaction
Best practices

- Global competition encourages companies to seek out and emulate best practices

- *Best practices* refers to choosing working methods that has been found to be the most effective and efficient
What is ISO 9000?

- ISO is the International Organisation for Standardisation, founded in 1946 to promote the development of international standards. ISO is composed of member bodies from over 90 countries.

- In 1987, the ISO published the first issue of a series of five international standards (ISO 9000, 9001, 9002, 9003 and 9004), developed by ISO Technical Committee (TC) 176 on quality systems. The ISO 9000 standards were intended to be advisory in nature and for use in two-party contractual situations.

- Quality system registration (certification) involves the assessment and periodic audit by a third-party (quality system registrar).
Basic values and principles
Quality assurance: basic values and principles

- Integrity
- Independence
- Prevention/Improvement
- Objective Evidence
- Identification/Traceability
- Segregation
Integrity

- Personal integrity:
  - professional
  - physical

- Documentation integrity:
  - technical
  - physical
Personal integrity: professional

- Fraud and collusion related to quality are not uncommon. In most cases, quality frauds are the results of ignorance or greed of managers. Sometimes irregularities and frauds are not committed for personal interest but to overcome what could seem a temporary contingency harmful to the company.

Key principles and methods currently applied to government procurement are traceable to the recommendations of the famous Truman Committee which investigated in U.S. a vast number of quality frauds which took place before and during WW II. Some basic QA practices (e.g. Certificate of Conformity signature, quality records) are meant to discourage frauds and help their investigation if the need arises.
Personal integrity: professional (cont’d)

On April 5, 2000, US President Clinton signed into law the Wendell H. Ford Aviation Investment and Reform Act for the 21st Century. Section 506 of the Act, titled Prevention of Frauds Involving Aircraft or Space Vehicle Parts in Interstate or Foreign Commerce, substantially increased the criminal penalties for false statements related to quality of parts (up to life sentence in case of accident!)

The law is meant basically to better fight the growing market of counterfeit aircraft parts, but it applies also to space hardware.

[Recent cases reported by NASA-OIG: press releases 2003-002 NASA Subcontractor sentenced in parts testing scheme; press release 2003-017 New Indictment in counterfeit parts scheme]
Personal integrity: professional (cont’d)

- Exposure of the QA personnel itself to potentially dangerous situations of collusion

“Within the daily range of activity there are many pressures to test the integrity of the inspector... dangerous is the situation posed when there is a potential rejection on a vendor. Here the person pleading for a “break” is often an influential individual well supplied with funds for entertainment or other forms of influence”

(J.M. Juran-Quality Control Handbook)
“Flinching”. This term describes the tendency of inspectors to falsify the results of inspection of borderline product (excess of reading at maximum of specified value and not beyond).

Incorrect use of QA stamps, as for example “lending” of personal QA stamps

Willful errors or negligence. These are instances when it is to personal advantage or convenience of the inspector to falsify the results of an inspection
Personal integrity: professional (cont’d)

- The QA function must be vigilant, enforce the practical means and exercise the authority to prevent the occurrence of questionable practices

"...The real remedy is by creating and maintaining an atmosphere of respect for the facts as the ethical foundation of the QA function..."

(J.M. Juran - Quality Control Handbook)
Personal integrity: professional (cont’d)

Inspection/certification companies find sometimes appropriate to issue a specific policy statement regarding integrity, as the following example:

“STATEMENT OF INTEGRITY

...For over a hundred years, we have been building our reputation as the world leader in independent, reliable and high quality verification, testing and certification services. The cornerstone of this reputation is integrity. Our integrity is our asset. It is our balance sheet, it defines us to ourselves, our customers, our shareholders and to the world.... Nothing, not client wishes, nor revenue growth, nor profitability, nor instructions from above, is more important than integrity.”

(From the “Statement of Integrity” of SGS of Geneva)
Personal integrity: physical

- Some QA jobs rely on good physical conditions for their correct accomplishment, for example vision integrity.

Personnel performing nondestructive inspections (NDI) are therefore subjected to periodical eye exam as per norms (e.g., MIL-STD-410)
Documentation integrity: technical & physical

- Errors can occur due to use of:
  - unreleased draft documents
  - obsolete documents
  - defaced documents
Documentation integrity: technical & physical

- Documents must be released and modified through formal procedures.
- A “Documents Master List” must be continually updated/maintained and made available to document users.
- Obsolete documents must be promptly removed from all point of use, or clearly identified (e.g. “OBsolete” red ink stamp).
- Document users must be forbidden to alter or deface released documents (by adding personal notes, work instructions, etc.).
Independence

“State or quality of being independent; freedom from the influence, control, or determination of another or others”
(Webster’s Dictionary)

Placement of QA in the organisation should foster independence, but independence must be first of all a professional attitude of QA engineers and managers

Acceptance determination of products shall not be influenced by cost and schedule considerations!
Identification/traceability

- Materials
- Personnel
- Measurements
- Design requirements/verifications
For critical products the conformity certification is of little value without materials traceability.

It must be possible using the product identification (e.g., P/N, DWG/N + S/N, Lot Nr, CI Nr) to trace all the objective data which demonstrate conformity to the design documentation.

Traceability is achieved during manufacturing and storage by means of a continuous chain of tagging, marking and identification verifications.
Personnel traceability: stamps and signatures

- Certain operations or decisions to be valid must be performed by personnel specifically trained/certified and/or authorised:
  - inspectors
  - certified welders
  - project controllers
  - manufacturing engineers
  - Test engineers
  - MRB members
  - CCB members, etc

- Traceability is ensured through issuance and use of inspection and other stamps, or signatures, which are **formally controlled**
Measurements traceability

- A measure is by definition the comparison to a reference standard.

- To ensure the accuracy of a measurement it must be possible to relate it to national or international standards through an unbroken chain of comparison.
Design requirements/verifications traceability

- The paramount consideration in writing a design requirement is its technical essence, verifiability and traceability.

- Design requirements of a product (H/W or S/W) are linked hierarchically and logically to system level requirements following the product-tree structure. Three types of requirements exist:
  - direct/requirement: a lower level requirement the satisfaction of which totally satisfies the higher level requirement
  - partial/requirement: a lower level requirement that meets the system level requirement but does not itself totally satisfy the higher level requirement
  - derived/requirement: a lower level requirement necessary at the lower level to allow the subsystem or equipment to meet a higher level requirement
Design requirements/verifications traceability (cont’d)

- Design requirements identification (by progressive number) and traceability is necessary to ensure design completeness/consistency

- Traceability of design requirements to relevant verifications (test, analysis, inspection, review of design) is essential to completely prove that customer requirements are met
Objective evidence

- If it isn’t written down it does not exist
- If it isn’t written down it didn’t happen
- If it isn’t written down it is subjective

Objective evidence are data such as:
- laboratory analyses
- test reports
- shop-travelers
- NCR’s

Objective data must be archived for a pre-defined time
Prevention

The continuous change of denominations for the quality systems and the additions of new tools should not confuse about what was and still is the prime concept of quality management: PREVENTION

- Prevention of chronic troubles
- Prevention of re-occurrence
- Prevention activities and methods

"Once the idea of such prevention is grasped, the label used to describe it (quality control, quality improvement, prevention, etc) is unimportant ..."

(Juran’s Quality Control Handbook)
Prevention of chronic troubles

- Sporadic spike
- Old quality control zone
- New quality control zone
- Quality improvement
- Cost of poor quality
Human error prevention

- Human errors are frequently caused by lack of training, inadequate information or automatic conduct, less frequently by pure negligence. **Knowledge and skills are the foundation of quality.**

“Making a violin requires a variety of tools, since each piece of wood has its own unique gifts that must be brought out by precise tapping, flexing and shaping. So too with European craftsmanship. As this special report has shown, each art requires special tools from lathes to lasers and **special people** to wield those instruments...”

*(TIME Magazine, August 20, 2001)*
Steps of a quality improvement process

A quality improvement process includes the following steps:

- assess current state and problems
- define preferred state
- identify barriers and root causes
- develop improvement solutions
- implement solutions
- monitor results
Segregation

- Segregation is meant to prevent the inadvertent/unauthorised use of materials, equipment and documents such as:
  - incoming materials not yet inspected
  - nonconforming materials
  - materials undergoing re-lifing tests
  - out-of-calibration measurement equipment
  - scrapped materials (waiting disposal)
  - obsolete design documents (waiting disposal)

- Segregation areas will be secured and accessible only to authorised personnel
QA Main Elements/Techniques
(Part I)

<<>>
QA main elements/techniques: part I

- Organisation
- Manual, Procedures, Plans and Records
- Audits
- Nonconformance Control
Organisation

This is the story of four people: EVERYBODY, SOMEBODY, ANYBODY and NOBODY.
There was an important job to be done and EVERYBODY was asked to do it.
EVERYBODY assumed that SOMEBODY would do it.
ANYBODY could have done it but NOBODY did it.
SOMEBODY got angry about that because it was EVERYBODY’s job.
EVERYBODY thought ANYBODY ought to do it, but NOBODY realised EVERYBODY wouldn’t do it.
Finally, ANYBODY blamed EVERYBODY for not helping NOBODY and SOMEBODY wisely concluded that NOBODY is the most helpful person in the company.
Organisation

Good organisation means:

- clear responsibilities and authorities
- well defined management system
- adequate communication lines
- quality function independence
Organisation: clear responsibilities/authorities

- defined company organisation structure
- written job descriptions
- no conflicting responsibilities
- no overlap of duties
- responsibilities commensurate to authority
- adequate competence and abilities
- adequate positions
Organisation: defined management system

- defined way of operation of each organisation unit
- defined functional interfaces with other units
- defined external interfaces
Organisation: adequate communication lines

- communication methods
- information flow (internal external)
- open attitude
Quality function placement: example

Higher Manager

- Production Manager
  - Inspection
- Quality Manager
  - QC Engineering
- Other Managers
  - Quality Assurance
Quality function placement: example
Quality function placement: example

Higher Manager

Quality Manager

Production Manager  Project Manager A  Project Manager B

QC/Insp  PA/QA  PA/QA
Quality function placement: example

Higher Manager

Production Manager  Technical Manager  Other Managers

Insp  QC/QA
ESA-Product Assurance and Safety function

TEC Directorate

Q Department

Quality/Depend/Safety Materials Components

ESA Director General

Directorates

Departments

Project Divisions

Project PA Manager

IAASS Quality Assurance Course September 2007
NASA-Safety and Mission Assurance function

IAASS Quality Assurance Course

September 2007
QA main elements/techniques: part I

- Organisation
  - Manual, Procedures, Plans and Records
- Audits
- Nonconformance Control
Quality system documentation

Hierarchy of Documentation

- **Document Contents**
  - Describes the policies, standards, organizations, responsibilities, and documentation that make up the quality system.
  - Describes the key processes and activities that implement the quality system.
  - Defines how the requirements of each project or product will be addressed within the quality system.
  - Provides detailed descriptions of specific tasks, if required for consistent conformance to requirements.
  - Demonstrates operational conformance to quality system requirements.

- **Structure of Quality System Documentation**
  - Quality Manual
  - Documented Procedures
  - Quality Planning Documents
  - Work Instructions
  - Quality Records
Quality manual

A Quality Manual is a compilation of company policies and requirements meant to guide day-to-day practices, in particular to:

- make customers and employees aware of the company’s quality philosophy and standards
- establish responsibilities of each organisational unit
- provide written guidance and instructions for quality
- serve as the basis from which audits are performed
The *Quality Manual* is prefaced by a quality policy statement of the Company’s chief executive.

The company operating policy is described in several functional areas, such as subcontracting, design control, process control, procurement control, inspections, tool and gage control, training, packaging/shipping etc. It will also describe in general terms how decisions will be made regarding conformance and product suitability.

The *Quality Manual* is divided into sections based either on functional or organisational areas.
Quality procedures: the six honest serving men

The beginning of Rudyard Kipling’s poem “The Elephant Child” goes as follows:

“I keep six honest serving men
(they taught me all I knew).
Their names are What and Why and When
and How and Where and Who”

These six words—what, why, when, how, where and who—are the six points that every procedure should address to provide a clear and focused content.
Quality procedures: short and concise

Procedures should be as short and concise as possible (i.e., ideally no more than five pages). Inclusion of flow-diagrams is always encouraged to summarise the sequence of steps.
QA plans

In general, a plan is a method or strategy for achieving an objective.

The QA plan is the contractor’s management strategy for fulfilling the specific quality requirements of a contract.

ISO 8402:
“Document setting out the specific quality practices, resources, and sequence of activities relevant to a particular product, project or contract”
- The quality plan usually references parts of the supplier’s quality manual applicable to the specific case
- The quality plan may be called “quality program plan” or “quality assurance plan” depending on the scope
To be meaningful, the QA Plan must build on a pre-established company quality (management system) manual. The reason being that project schedule is usually incompatible with the time required to start a quality system from “zero”.
QA plans (cont’d)

Basic QA plan content:

- organisation: charts, functional roles and responsibilities
- compliance matrix to customer requirement cross-referencing to in-house applicable procedures
- requirements made applicable to sub-contractors
- project-wide procedures
- approach to surveillance of subcontractors
- chart identifying relationship between QA tasks and project milestones
Work instructions

In some cases, it is necessary to provide step-by-step instructions to the work force for specific activities. It is beneficial to separate this type of instruction from the more generalised procedures.
Quality records

- Quality records are documents which are maintained to provide objective evidence of activities performed or results achieved demonstrating:
  - conformance to specified requirements
  - effective operation of the quality system

A freshly minted test procedure is not a quality record, but it becomes a quality record when filled in with the results of the test.

A minimum retention period must be defined and documented. Periods of 5 to 7 years are commonly used.
Quality records (cont’d)

- Examples of Quality Records:
  - Inspection and test records
  - Shop-travelers (after completion)
  - Nonconformance records
  - Calibration records
  - Audit plan
  - Audit results/reports
  - Training/certification records
  - Identification and traceability records
  - Special processes records
  - Preventive actions records
QA main elements/techniques: part I

- Organisation
- Manual, Procedures, Plans and Records
- Audits
- Nonconformance Control
What is an audit?

An audit is an independent examination of **objective evidence** performed by competent personnel, to determine whether or not the auditee

- is able to achieve its policies and objectives, and/or
- is capable to fulfil its contractual and legal obligations; and
- is effectively implementing a QA system

It is also the true and fair presentation of the results of such examination. When conducting an audit, it is vital constantly to remember that one’s aim is

**FACT FINDING NOT FAULT FINDING**

Obviously, there will be occasions when faults will be found, but that is a fact!
Audits

- System audit
- Compliance audit
- Process audit
- Product audit
System audit

Documented activity performed to verify, by examination and evaluation of objective evidence, that applicable elements of the quality system are suitable and have been developed, documented, and effectively implemented in accordance with specified requirements.

A system audit probes whether or not there is an organisation and a quality assurance system in existence and assesses their adequacy to meet the requirements invoked by a contract.

It is advantageous to conduct a systems audit well in advance of the actual starting of an activity. System audits are akin to readiness reviews.
Compliance audit

The compliance audit investigates whether or not the QA system is implemented. The auditor will scrutinise the objective evidence that should be generated by the implementation of the system. The auditor checks that the auditee works to the letter of the QA procedures.

Compliance audit must not be confused with an “inspection”. The latter is concerned with product acceptance and release for further processing. The former concerns itself with verifying that the QA system is implemented satisfactorily.
Process audit

Analysis of elements of a process and appraisal of completeness, correctness, or conditions
Product audit

Quantitative assessment of conformance to required product characteristics
Internal audit

- Internal audits are not performed in a single shot. At start of each year an Internal Audit Plan is drawn up. Each area of the company will be audited at least once annually.

- The objective is to ascertain if all personnel who have duties and responsibilities in accordance to the Quality Manual (or PA Plan), understand and satisfactorily perform their duties and responsibilities.

- The audit of the QA/QC organisation is considered accomplished by customer’s audits, third party maintenance of certification checks (if any), MIP’s.
External audit

- Preparation
- Performance
- Conclusions
- Report
- Follow-up
Audit preparation and performance

- Pre-audit Questionnaire and visit
- Audit team selection
- Audit notification
- Opening meeting
- Audit performance
- Debriefing meeting
- Report and follow-up
Pre-audit questionnaire and visit

- To collect basic information about the company to be audited
- To ensure no misunderstanding about audit scope and objectives
- To obtain the QA Manual (including compliance matrix w.r.t. audit baseline)
- To Identify the reference documentation
- To visit the facilities
Audit team selection

- It includes at least an audit team leader
- If necessary one or more additional auditor because of areas of expertise (e.g. S/W PA, RAMS, CM)
- Project QA representative (if a project audit)
Audit notification

- A reasonable time before the audit (e.g. agreement on dates 2 months before the audit, formal notification 1 month before audit)

- Notification in writing and including:
  - scope/baseline of audit
  - schedule
  - name of lead auditor
  - draft agenda
Opening meeting

- Introduction of attendants:
  - meeting the management
  - meeting counterparts

- Presentation of audit agenda (team leader):
  - summarise audit scope and procedure
  - finalise detail agenda (splinters if any)

- Presentation of the company and logistics:
  - assigned rooms
  - documentation access
Performance of audit

- Investigate by means of audit checklist:
  - use audit checklist as guide
  - not all questions are to be asked
  - adapt the wording to your counterpart
  - adapt the sequence of questions to circumstances (locations) “to be re-inquired”

- Look for **OBJECTIVE EVIDENCE** (trace of facts, such as reports, signatures, certificates):
  - statements are not sufficient (it may be useful to note them_”we are told that...”_ and
  - feelings are not sufficient
    to conclude on conformance to requirements
Performance of audit (cont’d)

If you identify a non conformance or deficiency:

- confirm it with your counterpart. Questions to be answered by “yes” or “no”, note explanations
- determine if it is of a systematic nature in view of conclusions

REMINDER:
In the conduct of the audit keep in mind that the Customer/Supplier relationship of the past that operated in an adversarial environment is becoming ancient history.
Debriefing meeting:

- meeting with the management of audited organisation
- each auditor presents his Observations Sheets (OS)
- provide clarifications
- collect signatures (if not yet done), as recognition that each reported observation is as verbally indicated during the audit
- audit team leader presents opinion on the audit results
- request formal response to each observation
Audit report

- Audit Report:
  - purpose of the audit
  - requirements baseline
  - audit team members
  - audit agenda
  - personnel contacted
  - summary of results
  - Observations Sheets
  - recommendations on each OS
Audit follow-up

- Obtain written response for each OS
- Evaluate response:
  - proposed corrective actions
  - proposed schedule
- Agree and formalise corrective actions and schedule
- Follow-up visits to verify close-out of corrective actions
- Formal audit closure
Audit terminology

Observation
An observation is made every time a total absence of arrangements to meet an important requirement or arrangements which are clearly inadequate is found. Observations are also made when lack of implementation of Quality Manual or procedures is revealed. The term “Non-Compliance” is also often used as synonym.

Recommendation
A Recommendation describes an acceptable solution to an observation. A recommendation should be written when it considered helpful to speed-up the achievement of agreement on a corrective action.
QA main elements/techniques: part I

- Organisation
- Manual, Procedures and Plans
- Audits

- Nonconformance Control
Non-conformance procedure

Usual elements of a nonconformance reporting (NCR)* procedure:

- Forms definition for internal/external reporting

- Initiator responsibilities (is anybody authorised to issue a report or only inspectors/QA?)

- Processing/meetings (formal meeting often only in special cases)

- Responsibility for investigation of causes, preventive actions definition/concurrence and tracking

*often called SPR (S/W Problem Report) for S/W products

IAASS Quality Assurance Course

September 2007
Non-conformance procedure (cont’d)

- Material Review Board responsibilities and membership (by name)

- Serial or parallel NCR distribution distribution (e.g., next higher level+customer)

- Interfaces with Configuration Control function (issuing of waivers)

- Disposition implementation. [Repair: to be treated as any manufacturing operation (written instructions) except for very simple cases]

- Segregation of non-conforming product
Non-conformances: disposition

- **Return to supplier**: Only applies to non-conforming procured items
- **Use-as-is**: The non-conformance is acceptable at the status
- **Rework**: Re-application of process will eliminate the non-conformity
- **Repair**: It is basically a modification that will allow use of the item
- **Scrap**: The item is not acceptable at the status or recoverable

Dispositions **Use-as-is** and **Repair** may require issuing a waiver.
Nonconformance processing: example

- PREPARES DISCREPANCY NOTICE (DN)
- SEGREGATION

- QA CONDUCTS PR
- DN CONFIRMATION
- OR MINOR REWORK
- PROMOTION TO MRB

- NCR PREPARATION
- NOTIFIES OF FORTHCOMING MRB
- ASSESSES CUMULATIVE EFFECT OF PREVIOUS NCRs

- CUSTOMER PARTICIPATION FOR MAJOR NCR
- MRB DETERMINES DISPOSITION

- CUSTOMER (ANY LEVEL)

- VERIFIES CORRECT IMPLEMENTATION OF DISPOSITION (after implementation)

- CONDUCTS CCB
- DISPOSITIONS AND APPROVES WAIVER
- CONTRACTUAL AUTHORIZATION TO PROCEED WITH WAIVER

- WAIVER NUMBERING
- SCHEDULES CHANGE BOARD (if needed)

- PREPARES SUPPORTING DATA AND DESCRIPTION / JUSTIFICATION FOR WAIVER

IAASS Quality Assurance Course September 2007
Non-conformances: investigating root causes

Root cause is the real reason for a nonconformity. It is possible that symptoms of the problem are identified as the cause, and it is the symptoms that are treated rather than the cause.

A defect attributed to operator error may not be the real reason if the operator has not been trained, had inadequate work instructions, or was working with a poor design.

- For each non-conformity there is a root cause
- Causes are preventable
- Prevention is always cheaper
Non-conformances: corrective actions

Corrective actions shall be aimed to prevent recurrence:

- Determine and document action to remove root causes
- Plan corrective actions (what, who and when)
- Identify interim actions

A *Corrective Actions System* should be in place to:
- summarise and collect nonconformances data (including costs)
- determine need/effectiveness of corrective actions
- initiate QIP (Quality Improvement Project) when appropriate
The Material Review Board

Purpose of the MRB is to provide an organised review of non-conforming product. The MRB is chaired by QA with members from Engineering and other specialists teams (e.g. Materials, S/W)

Members of the MRB have collective responsibility and specific responsibility. Specific responsibility relate to the field of specialisation.

Specific responsibility of the QA function in the MRB is to:

- investigate root causes to identify corrective/preventive actions
- ensure that remedial actions are properly implemented
- ensure that the process is correctly followed and records kept
Standards Evolution
Quality Assurance: standards evolution

- ISO standards
- Military standards
- Space standards:
  - NASA standards
  - European standards
## Where does ISO 9000 come from?

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>1963</td>
<td>MIL-Q-9858 updated to RevA</td>
</tr>
<tr>
<td>1968</td>
<td>NATO adopts MIL-Q-9858A as AQAP-1</td>
</tr>
<tr>
<td>1970</td>
<td>U.K. MoD adopted AQAP-1 as DEF/STAN 05-8</td>
</tr>
<tr>
<td>1979</td>
<td>BSI (British Standards Institution) develops the first commercial quality management standard, BS 5750</td>
</tr>
<tr>
<td>1987</td>
<td>ISO created ISO 9000 standards from BS 5750</td>
</tr>
</tbody>
</table>
The ISO 9000 (1994) series

- The ISO 9000 (1994) series was composed of five standards:
  
  **ISO 9000**  Guidelines for selection and use of 9001, 9002, 9003
  
  **ISO 9001**  Standard for organisations involved in design, production, and service
  
  **ISO 9002**  Standard for organisations involved in production
  
  **ISO 9003**  Standard for organisations involved in final inspection and test
  
  **ISO 9004**  Guidelines for quality management
ISO 9001(1994) compared to “traditional” QA

ISO 9001 (1994)

- Management Review
- Contract Review
- Servicing

Quality Assurance (Traditional)

Design Assurance (Basic Principles)
Cross reference table of ISO 9001, 9002 and 9003

<table>
<thead>
<tr>
<th>ISO Clause and Title</th>
<th>Quality Assurance Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1 Management Responsibility</td>
<td>◯</td>
</tr>
<tr>
<td>4.2 Quality System</td>
<td>◯</td>
</tr>
<tr>
<td>4.3 Contract Review</td>
<td>◯</td>
</tr>
<tr>
<td>4.4 Design Control</td>
<td>◯</td>
</tr>
<tr>
<td>4.5 Document Control</td>
<td>◯</td>
</tr>
<tr>
<td>4.6 Purchasing</td>
<td>◯</td>
</tr>
<tr>
<td>4.7 Control of Customer-supplied Product</td>
<td>◯</td>
</tr>
<tr>
<td>4.8 Product Identification and Traceability</td>
<td>◯</td>
</tr>
<tr>
<td>4.9 Process Control</td>
<td>◯</td>
</tr>
<tr>
<td>4.10 Inspection and Testing</td>
<td>◯</td>
</tr>
<tr>
<td>4.11 Inspection, Measuring, and Test Equipment</td>
<td>◯</td>
</tr>
<tr>
<td>4.12 Inspection and Test Status</td>
<td>◯</td>
</tr>
<tr>
<td>4.13 Control and Non-conforming Product</td>
<td>◯</td>
</tr>
<tr>
<td>4.14 Corrective Action</td>
<td>◯</td>
</tr>
<tr>
<td>4.15 Handling, Storage, Package and Delivery</td>
<td>◯</td>
</tr>
<tr>
<td>4.16 Quality Records</td>
<td>◯</td>
</tr>
<tr>
<td>4.17 Internal Quality Audits</td>
<td>◯</td>
</tr>
<tr>
<td>4.18 Training</td>
<td>◯</td>
</tr>
<tr>
<td>4.19 Servicing</td>
<td>◯</td>
</tr>
<tr>
<td>4.20 Statistical Techniques</td>
<td>◯</td>
</tr>
</tbody>
</table>

שיוף: ◯  Comprehensive Requirement, ◯ ◯  Less Comprehensive Than 9001 and 9002, NA  Element Not Present.
New format of ISO 9001(2000)  
“Quality management systems - Requirements”

- None of the ISO 9001(1994) requirements have been removed, they have been reorganised in five main sections:
  - Quality Management System (QMS)
  - Management Responsibility
  - Resource Management
  - Product Realisation
  - Measurement, Analysis and Improvement

- ISO 9002 and 9003 cancelled. ISO 9001 is used instead by excluding certain requirements
Basic terminology modifications

ISO 9000(1994)
- SUBCONTRACTOR
- SUPPLIER
- CUSTOMER

ISO 9000(2000)
- SUPPLIER
- ORGANISATION
- CUSTOMER
ISO 9001(2000):
Clause 4 - Quality Management System (QMS)

- Demonstrate continuous improvement in QMS effectiveness
- Define processes for QMS application throughout the organisation
- Documents demonstrate effective planning
## 4.1 QMS - General Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>4.1 – The organization shall establish, document, implement &amp; maintain a Quality Management System and continually improve its effectiveness in accordance with the requirements of this standard</strong></td>
<td>Explicitly defined by the standard itself</td>
</tr>
<tr>
<td></td>
<td>a) identify the <strong>processes</strong> needed for the QMS and their application;</td>
</tr>
<tr>
<td></td>
<td>b) determine their sequence and interaction;</td>
</tr>
<tr>
<td></td>
<td>c) determine criteria and methods for their effective operation and control;</td>
</tr>
<tr>
<td></td>
<td>d) ensure the availability of resources &amp; information for their operation and monitoring;</td>
</tr>
<tr>
<td></td>
<td>e) measure, monitor and analyse processes, and</td>
</tr>
<tr>
<td></td>
<td>f) implement action necessary to achieve planned results and continual improvement.</td>
</tr>
<tr>
<td><strong>4.1 - Ensure control of outsourced processes that affect product conformity.</strong></td>
<td>Accept responsibility for outsourced processes.</td>
</tr>
<tr>
<td></td>
<td>Identify needed controls in contract(s).</td>
</tr>
<tr>
<td></td>
<td>Establish acceptance process of outputs.</td>
</tr>
</tbody>
</table>
## 4.2 QMS - Documentation Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>4.2.1, 4.2.2</strong> – QMS documentation shall include:</td>
<td>Draft, review, approve and release policies, manual, procedures and other QMS documents. Provide necessary training and communication. Lead implementation. Maintain and adapt QMS to changing circumstances.</td>
</tr>
<tr>
<td>†Quality Policy &amp; Quality Objectives</td>
<td></td>
</tr>
<tr>
<td>†Quality Manual</td>
<td></td>
</tr>
<tr>
<td>†Documented Procedures</td>
<td></td>
</tr>
<tr>
<td>†Other documents needed for effective control of processes</td>
<td></td>
</tr>
<tr>
<td>†Records</td>
<td></td>
</tr>
<tr>
<td><strong>4.2.3</strong> - Documents required by the QMS shall be controlled</td>
<td>Prepare document control procedure.</td>
</tr>
<tr>
<td>Draft, review, approve &amp; authorise documents.</td>
<td></td>
</tr>
<tr>
<td>Release only approved documents.</td>
<td></td>
</tr>
<tr>
<td>Control changes &amp; version.</td>
<td></td>
</tr>
<tr>
<td><strong>4.2.4</strong> – Records shall be established &amp; maintained to:</td>
<td>Prepare &amp; apply procedure addressing records identification, storage, protection, retrieval, retention time &amp; disposition.</td>
</tr>
<tr>
<td>†Provide evidence of conformity</td>
<td></td>
</tr>
<tr>
<td>†Show effective QMS operation</td>
<td></td>
</tr>
<tr>
<td>Create and control records identified in procedures</td>
<td></td>
</tr>
</tbody>
</table>
ISO 9001(2000):
Clause 5 - Management Responsibility

- Customer requirements must be defined and fulfilled
- Quality policy provides framework for objectives and is measurable
- Effectiveness of QMS is communicated
## 5.1 Management Commitment

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1 Top management shall provide evidence of its commitment to develop &amp; implement the QMS and continually improve its effectiveness, by: a) Communicating to the organization importance of meeting customer &amp; legal requirements b) Establishing the Quality Policy c) Establishing Quality Objectives d) Conducting management reviews e) Ensuring resources are available</td>
<td>Communicate vision and leadership whereby Quality is considered a key success factor. Be involved visibly (to staff) in QMS definition, operation &amp; maintenance. Not only implement what is required by the standard (a through e), but link it to the actual way of managing the work. As a ultimate proof of commitment, provide the resources needed for QMS development, implementation and maintenance, with proper priority.</td>
</tr>
</tbody>
</table>
5.2 Customer Focus

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Implementation</th>
</tr>
</thead>
</table>
| **5.2** – Top management shall ensure that *customer requirements are determined and met with the aim of enhancing customer satisfaction* (See also 7.2.1 and 8.2.1) | For each product & service:  
- Explicitly identify its customers  
- Document the associated customer requirements, even if not formally imposed by the customer (see 7.2.1)  
- Constantly verify compliance to requirements  
- Monitor perceived customer satisfaction and define a process to improve it (see 8.2.1) |
## 5.3 Quality Policy

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>5.3</strong> – Top management shall ensure that the Quality Policy is:</td>
<td>Define the purpose = mission of the organization (implied in 5.3.a).</td>
</tr>
<tr>
<td>a) Appropriate to the purpose of the organization</td>
<td>Establish &amp; promulgate Quality Policy.</td>
</tr>
<tr>
<td>b) Includes commitment to comply with requirements and continually improve</td>
<td>Translate Quality Policy into concrete Quality Objectives</td>
</tr>
<tr>
<td>QMS effectiveness</td>
<td>Inform all staff of Quality Policy &amp; Objectives, so that each one understands</td>
</tr>
<tr>
<td>c) Provides framework to establish &amp; review quality objectives</td>
<td>how their work is affected.</td>
</tr>
<tr>
<td>d) Is communicated &amp; understood within the organization</td>
<td>Measure performance &amp; achievement of objectives.</td>
</tr>
<tr>
<td>e) Is reviewed for continuing suitability</td>
<td>Periodically review and update Quality Policy &amp; Objectives.</td>
</tr>
</tbody>
</table>
## 5.4 Planning

### Requirement

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Implementation</th>
</tr>
</thead>
</table>

5.4.1 – Top management shall ensure Quality Objectives, [including product requirements - see 7.1 a)] are established at relevant functions and levels within the organization. The quality objectives shall be measurable and consistent with the Quality Policy

- Establish Quality objectives, in line with Quality Policy,
- Flow the company’s Quality Objectives through the entire organisation, down to individual objectives.
- Measure performance & achievement of objectives
- Improve implementation & effectiveness

5.4.2 – Top management shall ensure that:

- Planning of QMS is carried out
- Its integrity is maintained when changes are made

- Develop and operate the QMS in accordance with clearly defined logic and established plans.
- Implement controlled change process & review QMS changes for impacts
# 5.5 Responsibility, Authority & Communication

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>5.5.1</strong> – Top management shall ensure that responsibilities and authorities are defined &amp; communicated within the organization</td>
<td>Publish and maintain documented definition of responsibilities &amp; authorities. Inform all interested parties.</td>
</tr>
<tr>
<td><strong>5.5.2</strong> – Top management shall appoint member of management … with responsibility and authority to a) ensure QMS processes are established, implemented, maintained b) report to top management on QMS performance and improvement needs c) ensure awareness of customer requirements throughout the Organization</td>
<td>Delegate authority needed to fulfil quality responsibilities Involve Quality Manager in Top Management decisions &amp; processes Provide access to information &amp; people needed by Quality Manager</td>
</tr>
</tbody>
</table>
5.5 Responsibility, Authority & Communication (cont’d)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>5.5.3</strong> – Top management shall ensure that appropriate communication processes are established and that QMS effectiveness is communicated within the organization</td>
<td>Define internal communication processes and associated resources.</td>
</tr>
<tr>
<td></td>
<td>Implement communications processes.</td>
</tr>
<tr>
<td></td>
<td>Provide information to staff.</td>
</tr>
<tr>
<td></td>
<td>Promote communication of QMS, performance &amp; customer satisfaction</td>
</tr>
</tbody>
</table>
## 5.6 Management Review

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Implementation</th>
</tr>
</thead>
</table>
| **5.6.1** – Top management shall review the organization's QMS, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness. This shall include assessing improvement opportunities and the need for QMS changes, including Quality Policy and Quality Objectives | Perform formal Management Reviews, at regular intervals (typically, 2 times/ year) Quality Manager to prepare input data package covering:  
    ◆ Results of internal & external audits  
    ◆ Customer feedback  
    ◆ Process performance and product conformity  
    ◆ Status of preventive and corrective actions  
    ◆ Changes affecting QMS  
    ◆ Recommendations for improvement  
    Decide and act upon:  
    ◆ improvement of QMS effectiveness  
    ◆ improvement of product quality  
    ◆ resource needs & constraints  
    Follow-up decisions and actions |
ISO 9001(2000):
Clause 6 - Resource Management

- Establish competency needs
- Determine training effectiveness
- Infrastructure/working environment provided for
- Determine resources to:
  - Implement/maintain QMS
  - Continually improve
  - Meet customer objectives
### 6.0 Resource Management

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>6.1 –</strong> The organization shall determine &amp; provide <strong>resources</strong> to</td>
<td>Review resource needs &amp; constraints Allocate adequate resources for</td>
</tr>
<tr>
<td>✔️ implement / improve QMS</td>
<td>✔️ QMS operation, assessment &amp; control</td>
</tr>
<tr>
<td>✔️ meet customer requirements</td>
<td>✔️ Ensuring customer requirements are met</td>
</tr>
<tr>
<td><strong>6.2 – Human resources</strong>&lt;br&gt;6.2.1 – Personnel performing work affecting product quality shall be competent on the basis of appropriate education, training, skills &amp; experience</td>
<td>Identify categories of personnel who perform work affecting quality and associated competences. Review competence of individuals and define specific skills development plans. Define a process for assessing the competences needed by the organisation and their management. Keep records of all the above.</td>
</tr>
<tr>
<td>6.2.2 … Determine competences needed, satisfy these needs, ensure actions are effective &amp; keep records</td>
<td></td>
</tr>
</tbody>
</table>
## 6.0 Resource Management (cont’d)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Implementation</th>
</tr>
</thead>
</table>
| **6.3** – The organization shall determine, provide & maintain **infrastructure** needed to achieve product conformity to requirements. This includes, as applicable:  
  ◆ Buildings, workspace & utilities  
  ◆ Process equipment (HW&SW)  
  ◆ Support services (transport, etc.) | Identify infrastructure needs  
  Assess existing infrastructure capabilities  
  Acquire needed infrastructure |

| **6.4** – The organization shall determine & manage **work environment** needed to achieve product conformity to requirements | Identify needs for work environment  
  (temperature, humidity, cleanliness …) and associated controls  
  Assess existing work environment  
  Upgrade work environment as needed |
ISO 9001(2000):
Clause 7 - Product Realisation

- Quality objectives/product requirements set
- Customer requirements for delivery and post delivery determined
- Obligations related to product (e.g. statutory and regulatory determined)
- Product function and performance requirements defined
- Control of any customer intellectual property
7.1 Planning of Product Realization

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1 – The organization shall plan &amp; develop product realization processes,</td>
<td>Define rules for project and activity management, including risk management.</td>
</tr>
<tr>
<td>consistently with other QMS processes. This includes:</td>
<td>Prepare Project/Activity Management Plans (generic, specific) &amp; Quality Plans,</td>
</tr>
<tr>
<td>a) Defining product quality objectives &amp; requirements</td>
<td>incl:</td>
</tr>
<tr>
<td>b) Defining documents &amp; providing resources specific to the product</td>
<td>◆ product requirements</td>
</tr>
<tr>
<td>c) Defining verification, validation activities &amp; acceptance criteria</td>
<td>◆ Specific application of QMS processes</td>
</tr>
<tr>
<td>d) Determining quality records needed</td>
<td>◆ V&amp;V activities</td>
</tr>
<tr>
<td></td>
<td>◆ product acceptance criteria</td>
</tr>
<tr>
<td></td>
<td>◆ records needed to prove results</td>
</tr>
<tr>
<td></td>
<td>Provide resources needed to realise product</td>
</tr>
<tr>
<td></td>
<td>Measure performance &amp; achievements</td>
</tr>
<tr>
<td></td>
<td>Improve implementation &amp; effectiveness</td>
</tr>
</tbody>
</table>
# 7.2 Customer Related Processes

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Implementation</th>
</tr>
</thead>
</table>
| **7.2.1** – The org shall identify requirements related to the product:  
   a) Customer specified requirements  
   b) Unstated (implied) requirements  
   c) Statutory/regulatory requirements  
   d) Requirements of the organization | Identify and document all requirements related to the products, not only those stated by the customer, but also implied expectations, legal requirements and additional constraints imposed by internal policies and rules. |
| **7.2.2** - Review requirements before commitment for completeness, contractual implications, & organisational capability to deliver | Review for correctness & completeness. Ensure contractual implications agreed. Verify ability to deliver results as agreed. Keep records of all the above. |
| **7.2.3** - Communicate effectively with customer: product information, enquiries, contract changes & status, and customer feedback, including complaints | Establish customer communication processes  
Effect clear correct communications  
Follow up all customer communications. Keep appropriate records |
## 7.3 Design & Development

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set of requirements to ensure a well planned and controlled D&amp;D process,</td>
<td>For D&amp;D work define appropriate processes &amp; plans, addressing:</td>
</tr>
<tr>
<td>covering</td>
<td></td>
</tr>
<tr>
<td>7.3.1 – D&amp;D Planning</td>
<td>✦ D&amp;D logic</td>
</tr>
<tr>
<td>7.3.2 – D&amp;D Inputs</td>
<td>✦ interfaces, roles, responsibilities &amp; authorities</td>
</tr>
<tr>
<td>7.3.3 – D&amp;D Outputs</td>
<td>✦ D&amp;D inputs &amp; outputs</td>
</tr>
<tr>
<td>7.3.4 – D&amp;D Review</td>
<td>✦ review, verification and validation activities</td>
</tr>
<tr>
<td>7.3.5 – D&amp;D Verification</td>
<td>✦ Configuration control</td>
</tr>
<tr>
<td>7.3.6 – D&amp;D Validation</td>
<td></td>
</tr>
<tr>
<td>7.3.7 – Control of D&amp;D Changes</td>
<td></td>
</tr>
</tbody>
</table>
## 7.4 Purchasing

| Requirement                                                                 | Implementation                                                                 |
|                                                                           | Document process and procedure for external procurement (contracts, purchase orders). |
| 7.4.1 – The organization shall                                             | Define supplier control system, covering:                                       |
|   ◆ Ensure purchased product conforms to its requirements                   |   ◆ Evaluation of supplier capabilities (audits)                                 |
|   ◆ Apply appropriate type and extent of control to the supplier and       |   ◆ Feedback & records of suppliers performance                                 |
|     purchased product                                                      |   ◆ Supplier rating system, defining the required surveillance                  |
|   ◆ Evaluate & select suppliers based on ability to supply conforming      |                                                                           |
|     product                                                                |                                                                           |

IAASS Quality Assurance Course September 2007
### 7.4 Purchasing (cont’d)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Implementation</th>
</tr>
</thead>
</table>
| **7.4.2 – Purchasing information shall describe the product, including:**  
  a) Reqts for approval of product, procedures, processes & equipment  
  b) Reqts for personnel qualification  
  c) QMS requirements  
The org shall ensure adequacy of specified reqts prior to release | Standardise purchase documents and include appropriate quality / PA requirements.  
Review purchase documents to ensure correct / complete requirements.  
Quality representatives to be involved in critical procurements. |
| **7.4.3 – Implement inspections or other activities to ensure purchased product conforms to requirements** | Identify conformity verification activities, including: audits, inspections (at source; of incoming goods), tests etc.  
Assign responsibility for acceptance activities.  
Review results for acceptance. |
7.5 Production and Service Provision

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set of requirements to ensure a well planned and controlled production &amp; servicing process, covering</td>
<td>For work involving production &amp; servicing define appropriate processes &amp; plans, addressing:</td>
</tr>
<tr>
<td></td>
<td>◆ information / equipment needed</td>
</tr>
<tr>
<td></td>
<td>◆ processes &amp; validation criteria</td>
</tr>
<tr>
<td></td>
<td>◆ Monitoring of process performance</td>
</tr>
<tr>
<td></td>
<td>◆ Configuration Management</td>
</tr>
<tr>
<td></td>
<td>◆ Identification of products and its verification status</td>
</tr>
<tr>
<td></td>
<td>◆ System for authorized signatures</td>
</tr>
<tr>
<td></td>
<td>◆ responsibility and measures to ensure integrity of customer property</td>
</tr>
<tr>
<td></td>
<td>◆ Protection of product during handling, storage &amp; delivery</td>
</tr>
<tr>
<td></td>
<td>◆ Product packaging and marking.</td>
</tr>
</tbody>
</table>

7.5.1 – Control of production & service provision
7.5.2 – Validation of processes for production & service provision
7.5.3 – Identification & traceability
7.5.4 - Customer property
7.5.5 – Preservation of product
### 7.6 Control of Monitoring & Measuring Devices

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>7.6 – The organization shall:</strong></td>
<td>Define &amp; document processes for proper control of devices used to provide evidence of conformance of products, including:</td>
</tr>
<tr>
<td> … Determine monitoring &amp; measurements for products to be undertaken &amp; provide needed monitoring / measuring devices.</td>
<td> Define measurement needs</td>
</tr>
<tr>
<td> …Establish controlled monitoring / measuring processes</td>
<td> Provide measurement devices</td>
</tr>
<tr>
<td> Assess measurement validity when devices not conforming to requirements (uncalibrated) are used, and take actions accordingly on affected devices &amp; product</td>
<td> Establish calibration regime</td>
</tr>
<tr>
<td></td>
<td> Identify measurement controls</td>
</tr>
<tr>
<td></td>
<td> Ensure capable staff</td>
</tr>
<tr>
<td></td>
<td> Assess impacts of measurement done with out-of-calibration equipment</td>
</tr>
<tr>
<td></td>
<td> maintain database to monitor use and status of measuring equipment</td>
</tr>
</tbody>
</table>
ISO 9001(2000):
Clause 8 - Measurement, Analysis and Improvement

- Monitor customer perceptions on fulfilment of requirements
- Customer satisfaction data needed is defined and subsequently analysed
- Audits to verify compliance with planned arrangements, as well as QMS requirements and ISO 9001 (2000) requirements
- Audit frequency and methodology to take account of previous results
- Process defined for waiver approval and defect reporting to relevant authority
# 8.1 General

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>8.1</strong> – The organization shall plan &amp; implement monitoring, measuring, analysis &amp; improvement processes needed to:</td>
<td></td>
</tr>
<tr>
<td>a) Demonstrate product conformity</td>
<td>Define monitoring / measuring processes.</td>
</tr>
<tr>
<td>c) continually improve QMS effectiveness</td>
<td>Collect,analyse &amp; review data.</td>
</tr>
<tr>
<td></td>
<td>Identify improvement actions.</td>
</tr>
<tr>
<td></td>
<td>Implement improvements.</td>
</tr>
<tr>
<td></td>
<td>Measure effectiveness.</td>
</tr>
<tr>
<td></td>
<td>More specifically:</td>
</tr>
<tr>
<td></td>
<td>a) See 8.2.1, 8.2.4</td>
</tr>
<tr>
<td></td>
<td>b) See 8.2.2, 8.2.3</td>
</tr>
<tr>
<td></td>
<td>c) See 8.5</td>
</tr>
</tbody>
</table>
## 8.2 Monitoring & Measurement

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Implementation</th>
</tr>
</thead>
</table>
| **8.2.1 - Customer Satisfaction**  
The org shall monitor customer perception of whether the organization has met customer requirements. Determine methods to obtain and use this information | Define quality attributes for products & related customer satisfaction data.  
Define data collection methods.  
Collect & analyze data.  
Measure achievements, set targets for improvement & act accordingly. |
| **8.2.2 – Internal Audits**  
The org shall conduct internal audits at planned intervals to determine whether the QMS:  
- conforms to ISO 9001  
- is effectively implemented and kept | Train & certify auditors  
Define audit plan (typically, each area audited at least once a year).  
Conduct internal audits.  
Analyse results & assess effectiveness  
Identify & implement corrective actions |
### 8.2 Monitoring & Measurement (Cont’d)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Implementation</th>
</tr>
</thead>
</table>
| **8.2.3** – The organization shall apply suitable methods for monitoring and measurement of QMS processes | Define success criteria & related measures for QMS processes  
Collect & analyse performance data.  
Measure achievements, set targets for improvement & act accordingly. |
| **8.2.4** – The organization shall monitor and measure product characteristics to verify product requirements have been met | Define Project & Quality Plans, addressing product characteristics, acceptance criteria, verification methods … (see 7.1)  
Ensure requirements are met before releasing product.  
Collect & analyse data to verify results and trends. |
# 8.3 Control of Nonconforming Product

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Implementation</th>
</tr>
</thead>
</table>
| 8.3 – The organization shall ensure that nonconforming product is identified & controlled to prevent unintended use or delivery. Nonconforming product shall be dealt with by: a) Eliminating detected nonconformity b) Obtaining a waiver for use or release c) Precluding original intended use or application | Define controls and related responsibilities & authorities for dealing with nonconforming product in a documented procedure. Apply procedure, i.e.:  
- Identify & report nonconforming product  
- Assess nonconforming items to determine disposition  
- Act to eliminate causes of nonconformity  
- Obtain permission to release or use nonconforming product (if needed)  
- Segregation |
# 8.4 Analysis of Data

The organization shall determine, collect, analyse appropriate data to:
- demonstrate QMS suitability & effectiveness
- evaluate where continual improvement of the QMS can be made

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4 – The organization shall determine, collect, analyse appropriate data</td>
<td>Define data criteria &amp; collection processes.</td>
</tr>
<tr>
<td>to demonstrate QMS suitability &amp; effectiveness</td>
<td>Collect &amp; analyse performance data.</td>
</tr>
<tr>
<td>◆ evaluate where continual improvement of the QMS can be made</td>
<td>Measure achievements &amp; set targets.</td>
</tr>
<tr>
<td></td>
<td>Identify &amp; implement improvement actions.</td>
</tr>
<tr>
<td></td>
<td>Verify effectiveness of actions.</td>
</tr>
</tbody>
</table>
## 8.5 Improvement

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>8.5.1 – Continual Improvement</strong>&lt;br&gt;The organization shall continually improve QMS effectiveness</td>
<td>Establish improvement mechanism. Identify improvements opportunities. Initiate improvement projects. Assess results and act accordingly</td>
</tr>
<tr>
<td><strong>8.5.2 – Corrective Action</strong>&lt;br&gt;The organization shall eliminate causes of nonconformities to prevent <strong>recurrence</strong></td>
<td>Analyse nonconformities to identify trends and causes. Eliminate causes of nonconformities. Measure effectiveness of changes</td>
</tr>
<tr>
<td><strong>8.5.3 – Preventive Action</strong>&lt;br&gt;The organization shall eliminate causes of potential nonconformities to prevent <strong>occurrence</strong></td>
<td>Analyse all suitable data sources to identify potential nonconformities. Eliminate potential causes. Measure effectiveness of changes</td>
</tr>
</tbody>
</table>
Applying ISO 9001 to software

Software development, can only be successful if:

- specific methods and controls are in place from the start
- the development life cycle is made visible and manageable
- customer and supplier come together at the defined stages
Applying ISO 9001 to software (cont’d)

- ISO 9000-3 “Guidelines for the application of ISO 9001 to the Development, Supply, and Maintenance of Software” provides guidance on:
  - software “life-cycle” activities and reviews
  - requirements specification
  - plans (quality, CM, development, verification, test, maintenance)
  - release and maintenance procedures/records
  - specific support activities (CM and DM, purchasing quality records measurement, use of customer supplied s/w, training)
Applying ISO 9001 to software (cont’d)

- When looking for third party certification, it is important that the identified auditor is software knowledgeable and that he looks for good software development practices around key software processes.

- TickIT is a British industry specific standard for auditing software companies to the ISO 9001 standard using the ISO 9000-3 guidelines
Problems with ISO 9000

- Time required to write the manuals: 31
- High volume of paperwork: 27
- High Cost of implementation: 25
- Time required to complete implementation: 24
- High cost of maintain the standard: 19
- Lack of free advice: 18
- Lack of consistency between auditors: 18
- Time spent checking paperwork prior to audits: 16
- The vagueness of the standard: 12
- Difficulty interpreting the standard: 12

SOURCE: MANCHESTER BUSINESS SCHOOL
Reasons for seeking ISO 9000

- Future customers likely demand for ISO 9000: 78%
- Increase consistency of operations: 65%
- Maintain/improve market share: 61%
- Improve service quality: 61%
- Customer pressure: 58%
- ISO 9000 is a good ‘promotional tool’: 57%
- Make operations more efficient: 54%
- Improve product quality: 52%
- Proof of ‘TQM’: 34%
- Cost reductions: 22%

SOURCE: MANCHESTER BUSINESS SCHOOL
IAASS Quality Assurance Course
September 2007
Benefits resulting from ISO 9000

- Increased exports: 24%
- Increased market share: 49%
- Reduced costs: 50%
- More effective marketing: 52%
- Reduced wastage: 60%
- Increased productivity/efficiency: 60%
- Increased opportunity to win work: 62%
- A motivated workforce: 61%
- Improved customer satisfaction: 82%
- Improved management control: 83%

SOURCE: MORI

IAASS Quality Assurance Course
September 2007
ISO 9000 COSTS

- Internal resources
- ISO 9000 consultants (if required)
- Application fee
- Optional pre-assessment
- Assessment
- Maintenance of system
- Surveillance visits
## ISO 9000 Costs

<table>
<thead>
<tr>
<th>Company Size (Employees)</th>
<th>Internal Man Days</th>
<th>3rd Party Consultancy Man Days</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 50 people</td>
<td>1-2 p/wk - 6 months</td>
<td>20</td>
</tr>
<tr>
<td>&gt; 50 - &lt; 100 people</td>
<td>2 p/wk - 1 year</td>
<td>30 +</td>
</tr>
<tr>
<td>&gt; 100 - &lt; 250 people</td>
<td>2 p/wk - 2 years</td>
<td>40 +</td>
</tr>
<tr>
<td>&gt; 250 - &lt; 500 people</td>
<td>3 p/wk - 2 years</td>
<td>50 +</td>
</tr>
</tbody>
</table>
Quality Assurance: standards evolution

- ISO quality standards
- Military standards
- Space standards:
  - NASA standards
  - European standards
The fate of QA military standards

In the early nineties the U.S. DOD embarked on a new policy which can allow contractors to use their existing quality system standard (Performance-Based Contracting, Single Process Initiative)

In October of 1996, MIL-Q-9858A and MIL-I-45208A were cancelled

In February 1993, NATO canceled the AQAP 1-15 documents and adopted a new series of AQAP’s that incorporate the ISO 9000 series

Recently the so-called aerospace model of ISO 9001 (AS/EN 9100) has been introduced/adopted world-wide, which fills certain gaps in ISO 9001 with reference to the original MIL-Q-9858A.
Quality Assurance: standards evolution

- ISO quality standards
- Military standards
- **Space standards:**
  - NASA standards
  - European standards
**NASA-Mission Assurance**

Mission Assurance is defined by NASA as a set of specialised disciplines to support the project development.
QA standards at NASA

As for U.S. DOD Military Specifications also NASA Specifications are being phased out (NHB-5300.4/1-B/1-C), but certain NASA or Military unique standards may be maintained, some indefinitely.

The "hierarchy of choice" is:

- National or International Voluntary and Consensus Standards
- Corporate Standards
- NASA or Military Standards and Practices

The new NASA system is called “Advanced Quality System (AQS)”
NASA - Advanced Quality System (AQS)

NASA's goal is to eliminate unique processes/systems imposed on contractors shared with DOD or other Federal agencies, unless essential to ensure mission safety and reliability.

The new NASA business management model is based on three elements:

- baseline quality management system
- advanced risk mitigating practices
- program/project-unique risk mitigation measures
In 1998 NASA issued the Policy Directive NPD 8730.3 “NASA Quality Management System Policy (ISO 9000) and associated Management Instruction NMI 1270.3 to:

- implement an ISO 9000 based Quality System
- mandate ISO certification of all NASA Centers
- impose ISO standards as contractual requirements (when appropriate and beneficial)
- require suppliers third-party certification (when appropriate and beneficial)
ISO 9001 at NASA

- NASA centres became ISO certified by 1999. Within 3 years at the end of 2002 NASA changed policy from mandatory to optional requirement, following a US government initiative study (F2M: Freedom-to-Manage) which identified ISO 9001 as a barrier to lean management.

- The CAIB (Columbia Accident Investigation Board) heavily criticised ISO 9001 certification for degrading the QA function at the Kennedy Space Centre (several key safety inspections replaced by process sampling).

- NASA recently adopted ISO 9001(AS/EN 9100).
Instead of prescribing detailed contractual requirements, NASA emphasises the identification and selection of those offerors who propose effective advanced practices:

- Integrated Product/Process Development (IPPD)
- Identification and Control of Key Characteristics
- Design to Manufacturing Process Capability
- Design for Assembly/Manufacturing (DFA/M)
- “Robust” Design
- Geometric Dimensioning and Tolerancing (GD&T)
- Process Variability Reduction (PVR)
NASA advanced practices (cont’d)

◆ Process Variability Reduction (PVR)
◆ Use of stable, capable processes for product acceptance
◆ Control of variation in the measurement system
◆ Root cause, closed loop corrective action
◆ Deployment of AQS elements to subcontractors
◆ Continuous Improvement (CI)

NASA will base future procurements by increasing the rigor of contractors selection and placing more importance on past performance. In addition will place quality incentives tied to Advanced Quality metrics (e.g., Cost of Quality).

NASA unique measures

Many programs or projects will continue to have unique requirements for risk mitigation in assembly, manufacturing or operational environments.
QA standards in european space activities

- In 1965, CNES issued QA requirements for the satellite FR1
- In 1975, ESRO published a Product Assurance Manual (QRA-31)
- In 1981, ESA published a generic space QA standard, PSS-01-20
- In 1988, CNES issued a coherent series of space project management specification (SM) for the Ariane 5 development, including A-SM-50 for quality assurance
In 1990, the preparation of a common QA standard was started by ESA and CNES for the HERMES project (later cancelled).


In April 1996, the first European space QA standard was issued, ECSS-Q-20, which took to a certain extent into account in its formulation the ISO 9000 series.

At the end of 1999 the quality system at ESOC, the ESA space operation center, has been certified ISO 9001. ESRIN followed in 2001.
The dawn of a new aerospace world standard

- Using the ISO 9001/1994 standard as a baseline the aerospace industry developed a first consensus standard ARD9000 in 1996. One year later it was published by SAE as AS9000. In November 1999 the standard was issued as AS9100, to be managed by the IAQG.

- IAQG (International Aerospace Quality Group) was founded in December 1998 by leading aerospace companies. This organisation is dedicated “to establish and maintain a dynamic cooperation based upon trust between international aerospace companies on initiatives to make significant improvements in quality and reductions in cost throughout the value stream”.

- In August 2001 AS9100 Revision A was issued to align the standard to ISO 9001/2000.
The dawn of a new aerospace world standard (cont’d)

◆ AS9100 Rev.A:
  – Aerospace unique requirements not changed
  – ISO 9000/2000 incorporation results in eliminating some requirements from AS9100
  – Some requirements from ISO 9001/1994 were added back
  – AS9100 Rev. A contains 80 aerospace unique requirements, and 18 amplifications and notes.

◆ Most IAQG members have implemented AS9100 internally and are requiring it of their suppliers. Data on involved national accreditation bodies, approved certification/registration bodies and certified/registered suppliers is available to all stakeholders.

◆ In Europe AS9100 is baselined as EN9100, and in Japan as JISQ9100.
Concepts, Techniques and Standards

Part II – H/W
Main Elements/Techniques
(Part II – H/W)
QA main elements/techniques: part II

- Organisation
- Manual, Procedures, Plans and Records
- Audits
- Nonconformance Control
  - Inspections
- Training
- Qualifications/Certifications
Inspection

- What is an Inspection?
- Quality Characteristics
- Workmanship standards

- Inspection planning
- Information for Inspection
- Inspection types/techniques
- Mandatory Inspection Point (MIP)
- Degree of inspection

- Metrology and Calibration
What is an Inspection?

A basic QA function is that of deciding through inspections whether the product is conforming. Such inspections are generally called “acceptance” inspections or QA inspections and consist of:

a) Interpretation of the applicable technical documents
b) Measurement/assessment of the product
c) Comparison of a) and b)
d) Judgement as to conformance (a/r criteria)
e) Disposition of the product
f) Recording of data
Quality characteristics

A physical or chemical property, a dimension, a temperature, a pressure, or any other requirement used to define the nature of a product or a service is a *quality characteristics*
Classification of quality characteristics

- **Design (Functional) Characteristics**
  - ensure performance
  - ensure life/reliability
  - ensure safety
  - ensure interchangeability
  - ensure interfaces

- **Manufacturing (Non-Functional) Characteristics**
  - related to method of manufacturing
  - to facilitate manufacturing
  - to provide information for toolmaking
The great number and variety of quality characteristics makes often necessary to formally highlight their difference in importance so that right care is taken by all concerned. In particular for inspection:

- need for independent inspection
- need to record inspection results
- responsibility for acceptance of defects

Example of classification codes for dimensional characteristics:

- Critical
- Major
- Minor
- Other Not marked
Workmanship standards

“Something effected, made, or produced; the art or skill of a workman; the quality imparted to a thing in the process of making”

(Webster’s Dictionary)

Workmanship standards establish the standard for the appearance of a product (indicative of proper quality) and the basic techniques used in producing it.

ESA and NASA have produced workmanship standards in particular for electronics assembly techniques. A wider range of workmanship standards has been established by national and international standardisation organisations (ISO, DIN etc.).
## Workmanship standard (cont’d)

<table>
<thead>
<tr>
<th></th>
<th><strong>ESA</strong></th>
<th><strong>NASA</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Wire wrapping of high reliability electrical connections</td>
<td>ECSS-Q-70-30 [PSS-01-730]</td>
<td>NASA-STD-8739.4 [NHB5300.4(3G)]</td>
</tr>
<tr>
<td>Crimping of high reliability electrical connections</td>
<td>PSS-01-726</td>
<td>NASA-STD-8739.4 [NHB5300.4(3G)]</td>
</tr>
<tr>
<td>High reliability soldering for SMT and mixed technology</td>
<td>PSS-01-738</td>
<td>NASA-STD-8739.2 [NHB5300.4(3M)]</td>
</tr>
<tr>
<td>Fiber optic terminations, cable assemblies/install.</td>
<td>---</td>
<td>NASA-STD-8739.5</td>
</tr>
<tr>
<td>Staking and conformal coating of PCBs</td>
<td>---</td>
<td>NASA-STD-8739.1 [NHB5300.4(3J-1)]</td>
</tr>
<tr>
<td>Handsoldering of high reliability electrical connections</td>
<td>ECSS-Q-70-08 [PSS-01-708]</td>
<td>NASA-STD-8739.3 [NHB5300.4(3A-2)]</td>
</tr>
</tbody>
</table>
Workmanship standards: examples

**CONDUCTOR PATTERN**

**Scratches**

**MAGNIFICATION 5X**

**PREFERRED**
1. Conductor is clean and surface is unmarked.
2. No scratches or surface defects.

**ACCEPTABLE**
1. Scratch is not in contact area.
2. Scratch does not expose base metal to create corrosion problem.
3. Scratch may interfere with subsequent soldering operation.

**REJECT**
1. Scratch occurs at critical junction point of pad and conductor.
2. Cross-sectional area reduced more than 10%.
3. Cross-sectional area reduced more than 10%.
4. Metal foil is restricted to an undetermined degree.

---

**WELDING - FUSION**

**Crater**

**MAGNIFICATION 5X**

**PREFERRED**
1. No visible weld defects. Weld crater should be free from porosity and inclusions.
2. Weld crater should be filled and fused into adjacent weld bead.

**ACCEPTABLE**
1. Small clean crater does not exceed 1/10 the thickness of the parent metal in depth or 1X the weld bead in width.

**REJECT**
1. Crater has a pitted area in bottom without evidence of burn through, cracks or inclusions.
2. Crater has cracked the base metal and/or weld metal.
3. Depth of crater exceeds 1/10 the thickness of the parent metal.
4. Width of the crater is greater than the width of the weld bead.
Workmanship standards: examples

MACHINED AND SHEET METAL PARTS
Skin - Surface Condition

PREFERRED
1. Skin surface is smooth and even without wrinkles, dimples, scratches or other visible defects.
2. Skin assembly is straight along any longitudinal line or specified dimension.

ACCEPTABLE
1. Minor scratches, gouges or pits are not detectable by feel with the scratch detection tool.

NOTE: Scratch detection tool (plastic pick) should be held approximately 45° to skin surface with the needle surface in contact with the suspected area to "feel" scratches.

ACCEPTABLE MINIMUM
1. Minor marring marks and abrasions are visible only by reflected light and have an acceptable dimensional characteristic.
2. Small surface wave or dent does not break the skin surface nor does it exceed .006 inch in depth to any one inch length when measured along a longitudinal line.

REJECT
1. Defects, errors or pits are detectable by feel with the scratch detection tool.
2. Surface wave or dent exceeds .006 inch in depth for any one inch length when measured along a longitudinal line.
3. Straightness of the outer surface along a longitudinal line exceeds 0.013 inch overall.

SOLDER COVERAGE
Solder Cup - Minimum

PREFERRED
1. Solder flows the contours of the cup carry slot without overflow or timing spots on cup.

ACCEPTABLE
3. Less than optimum solder, however a smooth fillet is formed between cup and conductor.
2. Slight timing spot where soldering iron tip contacts side of cup is permitted.

ACCEPTABLE MINIMUM
1. Minimum solder. Connection is wetted.
2. Minimum solder fillet between cup and conductor.

REJECT
1. Insufficient solder. No solder fillet between cup and conductor.
Inspection planning

The plan for conducting the overall inspection points on a project is called *Inspection Plan*. Inspection points are usually identified through:

- contract requirements
- specifications/standards
- reliability and safety analyses (e.g., FMECA/CIL, PHA)
- quality concerns (e.g., interfaces)
- manufacturing constraints
- operational experience

Usually inspection and manufacturing plans are fully integrated.
Information for inspection

- Shop-travelers
- Drawings/engineering lists
- Workmanship standards
- Procurement specifications
- Purchase orders/sample plan
- Configuration Item Data List (CIDL)
- Delivery documentation
Inspection types/techniques

- Incoming inspection
- In-process inspection
- Self-inspection
- Final inspection
- Source inspection
- Non-destructive inspection
Incoming inspection

Inspections performed to assure the conformity of received items to purchase orders. Mandatory use of holding areas until acceptance.

Purchase Orders
- identify deliverable items and quality documents/records
- must be readily available at Incoming Inspection location

Incoming Inspection Instructions
- establish for group of items the verifications to be performed

Rejected materials
- usually processed for return to supplier
- sometimes processed via in-house MRB (impact on costs)
Incoming inspection (cont’d)

Use of suppliers data
Normally comprehensive inspections/testing must be performed to verify conformity of received items to relevant specifications. Such activities may be considered redundant (and therefore skipped) if relevant data are requested to the vendor, and the vendor’s Quality Assurance system has been audited/certified directly or by a reliable third party (e.g., ISO). The bottom line on use of suppliers data is to be cost effective without compromising the overall control of end-product conformance.

Shipping damages
Incoming items must be always examined for shipping damages.
Incoming inspection (cont’d)

Sometimes specific incoming inspections are anyhow performed to:

- prevent potentially severe schedule and cost impacts on the project due to late discovery
- comply with applicable standards (e.g., procurement of EEE)
- prevent warranty time expiration for costly item not of immediate use
In-process inspection

In-process inspection serve to provide early detection of nonconformances before items are completed or processed into higher assemblies.
Self-inspection

Consist of allowing performance of in-process inspection by the same operator who has performed the manufacturing operation. SI requires:

- written quality procedure
- trained/certified operators
- written specific instructions and a/r criteria
- quantitative record of results
- operator traceability
- sampling re-verifications by QA

Self-inspection of critical characteristics is allowed only for operations which will be directly or indirectly verified by QA at a later time.
Final inspection

Consist of inspecting the product and the manufacturing documentation at the time of production completion to verify:

- conformity to contract requirements (including as-designed/ as built)
- completion of all manufacturing activities (including inspection and testing)
- close-out of any previous NCR disposition
- correct marking, including serialisation (if applicable)
- complete/correct accompanying documents
Source inspection

- *Inspection performed by the customer’s QA to confirm product’s compliance to contractual requirements prior to shipment*

- Source inspection may also involve Engineering in a coordinated fashion for issues related to technical performance

- Acceptance at source: inspection and acceptance at supplier’s facility prior to shipment to the extent that no further inspection is required

- Source inspection is recommended for critical items when no incoming inspection is feasible at customer’s premises (e.g., due to lack of special equipment)
**Non-destructive inspection**

These are techniques used to inspect products for **internal defects** (porosity, impurities, inclusions, cracks, debonding etc.). These techniques require considerable operator skill (certification) in particular with for the **interpretation of results**.

The most commonly used techniques are:

- **Liquid penetrants**
- **Ultrasonic inspection**
- **Radiography**
Non-destructive inspection: liquid penetrants

Technique based on property of certain liquids with very low surface tension to penetrate cracks by capillary action. The penetrant can seep into cracks as small as 0.1 micron. Two types used:

- **fluorescent penetrant**, visible under ultraviolet light
- **visible penetrants**, using dyes usually red in color

LP process steps:
1) Part cleaned and dried, 2) LP brushed or sprayed, 3) Excess penetrant wiped off or washed away with water or solvents, 4) developing agent applied LP will seep back to surface and spread to the edges thus identifying location and size of defect
Non-destructive inspection: ultrasonic inspection

Ultrasonic beam travels through the part to be inspected. An internal defect interrupts the beam and reflects back a portion of the ultrasonic energy.

Ultrasonic waves generated by transducer that operate on the piezoelectrical principle using materials such quartz (usually 1-25 MHz)

Couplants (water, oil) are used to transmit the ultrasonic waves from the transducer to the test piece.
Non-destructive inspection: radiography

Method used to detect internal flaws, such as cracks and porosity

The principle involved is density differences. The metal surrounding a defect will appear denser and hence show up as lighter than the flaws on an x-ray film.

Radiation source an x-ray tube, visible permanent image made on x-ray film.
Mandatory Inspection Point (MIP)

- Mandatory Inspection Point (MIP): Activity performed by representatives of customer, prime contractor or their delegates, to verify that the operations of fabrication and control have been performed correctly.

- MIPs are performed at important stages of the fabrication process, in particular at points where following operations would make impossible the conformity assessment of previous operations.

- MIPs should be used not only as part of the product acceptance process, but also to spot-check certain relevant elements of the quality system.
MIP (cont’d)

- A MIP may take the form of:
  - **Inspection**: direct performance of an inspection (by customer)
  - **Witness**: watch a specific operation
  - **Results verification**: review of records
MIP (cont’d)

- Severity of identified defects should also be assessed:
  - minor
  - impact on following fabrication operations
  - impact on item qualification/acceptance
  - impact on system integration
  - mission failure
  - safety

- The identification of potential catastrophic defects undetectable until their occurrence in flight would require immediate high profile actions

- An inspection report should be issued for each MIP
MIP (cont’d)

Average results from a major space contractor: (acceptance up to 90% for experienced subcontractors; as low as 20% for inexperienced subs)
Degree of Inspection

- Redundant
- 100% Inspection
- Statistical sampling/sampling
- 1st/Last piece
- Audit
Metrology

- Measurement is basically a process of comparison, in which the quantity being measured is compared with another which has been selected as a unit (*Henry I of England decreed that the yard should be the distance from the tip of his own nose to the end of his own thumb when his arm was outstretched*).

- In 1960 the General Conference on Weights and Measures (CGPM) established the International System of Units (SI), based on the metrics system, for global use.

- A metrological *standard* is a physical object or a characteristic of a physical apparatus that represents the conceptual unit chosen to represent a particular measurable attribute.
Metrology classification

Measurements are made every day in trade, industry and scientific laboratories. They are classified based on the nature of the parameter being measured (physical or chemical), or based on the application of the results (legal, industrial or scientific):
Metrology classification by nature

- **Physical Metrology**
  Measurement of physical parameters such as mass, length, electric current, velocity, and viscosity

- **Chemical Metrology**
  Qualitative and quantitative analysis of substances used in the chemical, biological, medical, and environmental fields. Measurements made in metallurgical testing laboratories, pharmaceutical laboratories, and pathology laboratories fall under the purview of chemical metrology
Metrology classification by application

- **Legal metrology**
  Measurements made for the purpose of exchanging products as part of trade are fair and credible (e.g. market scales, gasoline pumps, taxi meters etc.)

- **Industrial metrology**
  Measurements made in industries and service organisations to check the conformance of products and services to their specifications

- **Scientific metrology**
  Measurements made in scientific laboratories (R&D laboratories, testing and calibration laboratories)
Metrology and calibration

A vast variety of gages and instruments are used in industry for measurement purpose (e.g. mechanical, electronic, optical, pneumatic).

The QA function is concerned with appropriateness, use, maintenance of such instruments (but not with their scientific development).

Calibration

*The set of operations which establish, under specified conditions, the relationship between values indicated by a measuring instrument and the corresponding standard or known values derived from the standard.*
Accuracy of measurement

Target analogy

- Precise but not accurate
- Accurate but not precise
- Accurate and Precise
Accuracy, precision and resolution

- **Accuracy**
  The degree of agreement of the measurement with the true value of that parameter. The difference between measured and true value is defined as error.

- **Precision**
  The ability of an instrument to repeat the same reading when making the same measurement in the same manner and under identical conditions.

- **Resolution**
  The smallest change in input necessary to produce the smallest detectable change in output of the instrument under test.
Maintaining accuracy

From the moment an instrument is put into use it begins to deteriorate in accuracy. The procedure for maintaining accuracy includes:

- Number each instrument
- Establish a “card” record for each instrument
- Establish a checking interval
- Provide for adherence to the checking schedule
- Keep record of the findings of the check
- Analyse the results to take corrective actions (if needed)
- Analyse the trends to modify the intervals (longer/shorter)
Checking interval

The initial checking interval is based on instrument manufacturer recommendation and company experience.
The checking interval is based on:

- Calendar
- Amount of use

Adherence to the checking system makes or breaks the system.
Level of standards

- **Primary Standards:**
  These standards (gage blocks, standard cells, standard electrical bridges) are certified (occasionally) by a national metrology institute. They are used *only* to check secondary standards.

- **Secondary Standards:**
  These standards are checked periodically against the primary standards. They are *not* used to measure the product but to check the shop standards.

- **Shop Standards:**
  These standards are used to check the product itself.
National and international (measurement) standards

- **Measurement Standard**
  A material measure, measuring instrument, reference material or system intended to define, realise, conserve or reproduce a unit or one or more known values of a quantity to serve as reference.

- **National Standard**
  A (measurement) standard recognised by an official national decision to serve, in a country, as the basis for fixing the value of all other standards of the quantity concerned.

- **International Standard**
  A (measurement) standard recognised by an international agreement to serve internationally as the basis for fixing the value of all other standards of the quantity concerned.
Traceability to national/international standards

**Traceability**

*The property of a result of a measurement whereby it can be related to appropriate standards, generally national or international standards, through an unbroken chain of comparison. (ANSI/NCSL Z540-1-1994)*

The purpose of requiring traceability is to ensure that measurements are accurate representations of the specific quantity subject to measurement, within the *uncertainty* of the measurement.

**Uncertainty**

*A parameter, associated with the result of a measurement, that characterises the dispersion of the values that could reasonably be attributed to the quantity subjected to measurement.*
Calibration records and certificates

- A record system will be maintained including the list of instruments under calibration control and records for each calibration performed (containing, at least, sufficient information to permit the repetition of the calibration, along with the identity of the performing technician).

- When calibrations are performed by an outside (accredited) Lab a Certificate of Calibration will be requested for each calibration. The certificate will present, in a clear, unambiguous and objective manner, all information necessary for the interpretation of the calibration results.

- When instruments are sent for external calibration, an official record of the shipment should be kept on file until the instrument is returned.
QA main elements/techniques: part II

- Organisation
- Manual, Procedures, Plans and Records
- Audits
- Nonconformance Control
- Inspection
- Training
- Qualifications/Certifications
Training

The existence of documented plans, procedures and specifications will not result in hardware quality if the skills of manufacturing personnel are not sufficient to execute the instructions.

Training in any area is based upon:

- familiarisation with written process specification/procedures
- practice procedure under instructor’s observation/support
- hardware test/inspection providing feedback on success

For some processes, this is all that is required, and records will simply note that the individual was given training on a certain date.
Training (cont’d)

Advanced training including testing are required for critical processes and special techniques such as:

- Welding
- Adhesive Bonding
- Electronics Assembly
- Conformal Coating
- NDI
- Metrology

Testing may be written, or an ability demonstration, or combination of written and demonstration. **Testing outcome must be quantified.**
## ESA skills training centers

<table>
<thead>
<tr>
<th></th>
<th>IdS Paris (F)</th>
<th>Highbury College Portsmouth (UK)</th>
<th>ZVE Oberpfaffenhofen (D)</th>
<th>IIS Genova (I)</th>
<th>Hytek Aalborg (DK)</th>
<th>IFE Oberpfaffenhofen (D)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hand Soldering Operator</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Hand Soldering Inspector</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Repair/Modif PCBs</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>RF Cable Assy</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Crimping Wire Wrapping</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>SMT</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Instructor</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Fiber Optic Termination</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

**IAASS Quality Assurance Course**

September 2007
Quality Assurance: main elements/techniques

- Organisation
- Manual, Procedures, Plans and Records
- Audits
- Nonconformance Control
- Training

* Qualifications/Certifications
Qualification/certifications

- Qualification
  - process qualification
  - product qualification

- Certification
  - quality system certification
  - product conformity certification
  - personnel certification
  - stamp warranty
Qualification and acceptance tests

- Formal tests provide confidence that the product will operate correctly for the duration of the mission.

- Formal tests are divided in two categories:
  - Qualification tests
  - Acceptance tests

- Qualification tests stress the product to levels beyond those expected during service to demonstrate that adequate margins exist in the design.

- Acceptance tests are less severe and are used to demonstrate the conformity of each product unit to the design.
Qualification and acceptance tests (cont’d)

- Qualification and acceptance tests are performed at every level in the product hierarchy (e.g. equipment, subsystems and system).

- The order in which tests are performed is important and it is based on the expected life cycle of the product plus a measure of experience.

- A typical qualification test sequence:
Qualification and acceptance tests (cont’d)

- Qualification test levels will envelope those expected under operating and non-operating conditions, including acceptance tests and ground activities, with margins.

- As example, the levels used during thermal qualification tests (rule of thumb +/- 10 °C)
Certificate of Conformity

“A document signed by an authorised party affirming that the supplier of a product or service has met the requirements of the relevant specifications, contract or regulation”
Personnel certification

- Certification is very similar to testing but the process is more formal. The testing process and standard for pass/fail must be documented.

- The certifying organisation may be:
  - the contractor
  - a space agency or a delegated organisation
  - a nationally recognised organisation

- Some skills must be practised on a regular basis in order to maintain the currency of the certification.

- Some certification may require annual medical eye exam.
Personnel certification: records

- Certification records will include at least:
  - location and date of training
  - certification process procedure
  - specification/procedure
  - grade/rating
  - instructor name
  - expiration date
  - periodic renewals
  - achieved job continuity
Personnel certification: re-certification

- Re-certification is required for one of the following reasons:
  - certification expiration
  - interruption of work
  - unsatisfactory performance
  - evolution of techniques
Stamp warranty

◆ **Stamp warranty** means that an inspector who signifies the status of an inspection or test by stamping:

◆ is qualified to determine that status

◆ personally saw or performed the activity as documented

◆ At the time of stamp release, the inspector will acknowledge in writing his full understanding of the rules for use of stamps
QA during Major Project Phases
(H/W)
Quality assurance during major phases

- Design and Verification
- Procurement
- Manufacturing
- Testing
- Acceptance/delivery
Design and verification

- Procedures for engineering documents
- Design/Development and Verification plans
- QA support to internal design review for:
  - producibility
  - repeatability
  - inspectability
  - testability
- QA review of design changes for quality impact
Design and verification: structured requirements

IAASS Quality Assurance Course

September 2007
Types of design requirements

- **Functional Requirements**
  *Tasks, actions or activities that must be accomplished by a system, without specifying how it has to be done*

- **Performance Requirements**
  *The extent to which a function must be executed, generally covered in terms of quantity, quality, coverage, timeliness or readiness*

- **Design Constraints**
  *Boundary conditions within which the designer must remain while allocating performance requirements and/or synthesizing system elements (safety, environmental, interface, technology etc.)*
Requirements for requirements

- Design requirements must be:
  - complete
  - consistent
  - unambiguous
  - verifiable
  - traceable

The QA function must ensure that design requirements are properly documented, and verifications consistently planned and thoroughly executed. Ensure that QUALITY is designed into the product.
Quality assurance during major phases

- Design and Verification
- Procurement
- Manufacturing
- Testing
- Acceptance/delivery
Procurement control

- Selection of procurement sources
- Control of purchase documents
- Surveillance of suppliers
Selection of procurement sources

The selection is usually based on the following criteria:

- certification/approval for specific items
- demonstrated capability (positive performance records)
- pre-award audit

Maintain a list of subcontractors and suppliers including records of supplies and performance data (e.g., % of defective items, NCRs)
Control of purchase documents

Procurement documents shall contain by statement or reference:

- technical description of the item/service to be procured
- QA requirements and deliverable/accompanying documents (e.g., CoC, ADP, interface data records)
- QA activities to be performed by the supplier
- planned activities at source (if any)

*Purchase Orders (PO) and Contracts shall be reviewed and formally approved by the QA function prior to release*
Surveillance of suppliers

QA surveillance of subcontractors and suppliers is performed through periodic audits and inspections (MIPs, source inspection, incoming inspection). In some special cases a resident inspector may be needed.
Quality assurance during major phases

- Design and Verification
- Procurement
- Manufacturing
- Testing
- Acceptance/ delivery
Manufacturing

- Materials and parts control
- Production equipment control
- Cleanliness and contamination control
- Control of manufacturing processes
- Control of manufacturing documents
Materials and parts control

- Control must be exercised to ensure that materials and parts released for manufacturing are:
  - correct /traceable
  - conforming
  - within their useful life (if life limited)

Ensure that shop-travelers always include materials and/or parts identity verifications as first operation.
Ensure limited-life materials tracking and labeling with expiration dates
Production equipment control

Control must be exercised to ensure that manufacturing tools are:

- conform to their drawings
- periodically checked (recurrent production)
- properly stored to prevent deterioration/damage
- identified
- inventory kept
Production equipment control (cont’d)

- With the increasing use of computer-aided manufacturing and inspection techniques, the relevant s/w need to be:
  - documented
  - tested and approved prior to use
  - configuration controlled
  - secured to prevent tampering and misuse

The QA function must have a primary and documented role in the validation and control of production tools, including any COTS software
Cleanliness and contamination control

- **Cleanliness levels**
  The required cleanliness levels of contamination-sensitive items will be indicated on specifications, drawings and procedures.

- **Contamination control plan**
  This is a plan identifying the control measures necessary to achieve the required level of cleanliness during manufacturing, testing, handling, packaging and storage of contamination-sensitive items.

- **Cleanliness of facilities**
  “Clean facilities” conditions and operations need to be controlled to ensure that their specified level of cleanliness is maintained.
Cleanliness and contamination control (cont’d)

- Clean rooms facilities instructions will cover:
  - entering/leaving (personnel and equipment)
  - cleaning methods and materials
  - preventive maintenance
  - control/recording of clean room parameters (pressure, humidity, temperature)
  - performance of particle counts
  - action in case of alarm (stop work, shield items)

The QA function has a primary role in enforcing compliance to the Contamination Control Plan and verification of clean-facilities.
Manufacturing processes

- **Process**
  *A sequence of pre-defined steps intended to achieve a goal or objective*

- **Manufacturing process:**
  - Special Process
  - Critical Process
  - Standard Process
Special process

*Special process* is a process in which the outcome cannot be adequately verified without destroying the manufactured part (e.g., heat treatment, bonding, welding). Special process require:

- qualification
- control of process parameters
- non-destructive inspection
- destructive testing (e.g., chemical analysis, tensile test) of representative samples/coupons
- periodic control of process equipment/materials
- training/certification of personnel
- records maintenance/archiving
Critical process

*Critical Process* is not necessarily the same as *Special Process*. A critical process may or may not be a special process and vice-versa. A critical process is one:

- which in case of failure can adversely affect performance or destroy a major part or system function
- the quality of which cannot be assessed solely by examining the end product
- which has caused problems previously
- with which the contractor has no experience
## Critical process: PSS and ECSS definitions

<table>
<thead>
<tr>
<th>DEFINITION</th>
<th>PSS-01-700</th>
<th>ECSS-Q-70A</th>
</tr>
</thead>
<tbody>
<tr>
<td>- A process that in the case of failure can adversely affect the performance or destroy a major part or function of the space system</td>
<td>YES</td>
<td>-</td>
</tr>
<tr>
<td>- The quality of which cannot be assessed solely by examining the end product</td>
<td>YES</td>
<td>-</td>
</tr>
<tr>
<td>- A process that has caused problems previously</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>- Where an ESA specification is available but is not being implemented</td>
<td>YES</td>
<td>-</td>
</tr>
<tr>
<td>- A process with which the contractor in charge of it has had no previous experience</td>
<td>YES</td>
<td>YES</td>
</tr>
</tbody>
</table>
Standard process

- *Standard process* is one that is well documented, has a previous history of use, is well understood and for which standard inspection procedures exist.
Manufacturing process control

- Emphasis on process control depends on the criticality of the process

- Each process must be covered by a *Process Specification*, including control methods, QA provisions and a/r criteria

- ESA requires delivery of a project *Process List* to verify that processes are properly specified and controlled. Each process will be classified as *standard/established* or *critical*
Control of manufacturing documents

- **Manufacturing documents**
  - identified/traceable to contract no./purchase order
  - include rev.status/date, release date
  - include item identification and configuration data
  - kept with product during manufacturing/inspection operations
  - include provisions for traceability of operators and inspectors

- **Manufacturing documents control**
  - QA concurrence to ensure adequacy and right placement of inspections (any later sequence change needs QA agreement)
  - Design Office approval for critical/special processes (any later sequence change requires Design Office approval)
Quality assurance during major phases

- Design and Verification
- Procurement
- Manufacturing
- Testing
- Acceptance/ delivery
Testing (qualification and acceptance)

- Test facilities and equipment
- Test reviews
- Test surveillance
- Test documentation:
  - test procedures
  - test reports
Test facilities and equipment

- Environmental tests at certified facilities
- Test equipment verifiable without application to the test article
- Test software validated/verified prior to use
Test reviews

Test Procedure/ Test Readiness

TRR

no

yes

authorisation

Test Performance

Test Report

PTR

TRR: Test Readiness Review
PTR: Post-Test Review
Test Reviews: TRR

- Test Readiness Review
  - test article configuration (as-required/as-built)
  - any open NCR for impact
  - test procedure (availability/approval)
  - test facility readiness
  - test procedure (availability/approval)
  - test equipment calibration status
  - protection of personnel and test article
Test Reviews: PTR

- Post-test Review
  - completeness of required data
  - deviations/modifications for proper authorisation
  - NCRs during test for proper disposition
  - test results compliance with requirements
  - grant authorisation for further tests/processing

Ensure that QA is represented in the boards established for reviewing test readiness and test results. Ensure QA surveillance during test.
Test surveillance

- Test surveillance is performed by QA in one of the following forms:
  - continuous witnessing
    (for tests requiring manual intervention)
  - observation
    (periodic monitoring)
  - data review
    (review recorded data)

- QA personnel has generally the authority to stop the test for safety reason or to prevent hardware damages
Test documentation

- Test procedure/report must include:
  - test article identification
  - test equipment and test set-up
  - characteristics and design criteria to be tested
  - data recording and pass/fail criteria
  - sequence of operations (including inspections)
  - measures to ensure safety
  - environmental conditions
  - test organisation (personnel/responsibilities)
  - test results and conclusions (for test reports)

Test procedures must be reviewed and approved by QA
Quality assurance during major phases

- Design and Verification
- Procurement
- Manufacturing
- Testing

* Acceptance/delivery
Acceptance/delivery

- **Acceptance Data Package**
  - data to support acceptance
  - documents/data to support further integration

- **Acceptance review**
  - formal acceptance review board, or
  - Delivery Review Board (DRB)

- **DRB responsibilities:**
  - assess conformity to contractual requirements
  - verify nonconformances closed-out
  - accompanying documentation complete
Acceptance/delivery

- QA is a member of the DRB
- QA will perform surveillance of packaging/labeling operations
- QA will ensure that accompanying documentation is included

*QA has a leading role in acceptance and delivery activities and must be directly involved in their performance*
ECSS-Q-20B
(issued 8 March 2002)
Requirements flow-down

ECSS Standards

SOW (tailored ECSS)

Allocated & Derived Rqts

Allocated & Derived Rqts

Allocated & Derived Rqts

ECSS Organisation

ESA Project

Prime Contractor

IAASS Quality Assurance Course

September 2007
ECSS-Q-20B

- QA Programme Management
- QA General Requirements
- QA Requirements for Design and Verification
- QA Requirement for procurement
- QA Requirements for Manufacturing/Assembly/Integr.
- Testing
- QA Requirements for Acceptance and Delivery
- Operations
- Annex A - GSE
- Annex B, C, D – DRDs (Logbook, EIDP, CoC)
### ECSS-Q-20B

#### ECSS-Q-20

<table>
<thead>
<tr>
<th>1. General</th>
<th><strong>Summary/remarks</strong></th>
</tr>
</thead>
</table>
| 2. Quality Assurance Programme | - Organisation  
- Quality Assurance Programme Plan  
- QA Status Reporting  
- Personnel Training and Certification  
- Quality Assurance Programme Audits  
- QA role in Configuration Management: ensure existence/implementation of CM requirements; QA as a member of CCB; “as-built” vs “as-designed” verifications  
- Critical Items Control: items for which major difficulties or uncertainties exist controlled to reduce risk |
| 3. Quality Assurance General Requirements | - Documentation and data control  
- Quality records  
- Stamp Control  
- Traceability  
- Metrology and Calibration  
- Non-Conformance control system  
- Alert system: participation to ESA AS: generation of alerts for items with multiple applications failing within specified design/usage limits; assessment of alerts from Customer  
- Handling, Storage, Preservation  
- Statistical Quality Control: SQC applications used for acceptance to be approved by Customer |
## ECSS-Q-20B

<table>
<thead>
<tr>
<th>ECSS-Q-20</th>
<th>Summary/remarks</th>
</tr>
</thead>
</table>
| 4. QA Requirements for Design and Verification | - Design and verification planning  
- Evaluation/qualification of new technologies and critical processes  
- Clear organisation interfaces between different groups  
- Design rules implemented to achieve producibility, repeatability, inspectability, testability, operability  
- Standards and procedures for maintenance of engineering drawings and specifications  
- Requirements verification and qualification process  
- Design changes |
| 5. QA Requirements for Procurement | - Selection of procurement sources  
- Record and list of Procurement Sources  
- Applicable requirements defined in procurement documents  
- Surveillance of procurement sources  
- Receiving inspection |
| 6. QA requirements for Manufacturing Assembly and integration | - Planning of MAI activities  
- Identification of MIPs  
- Adequate instructions (e.g. shop-travellers)  
- Identification of critical characteristics  
- QA responsibilities (approval of documents etc.)  
- Manufacturing Readiness Review  
- Control of processes  
- Critical processes  
- Statistical Process Control  
- Workmanship standards  
- Materials and Parts Control: only conforming items release; limited life items  
- Equipment control  
- Cleanliness and Contamination Control  
- Inspection |
<table>
<thead>
<tr>
<th>ECSS-Q-20</th>
<th>Summary/remarks</th>
</tr>
</thead>
</table>
| 7. Testing | - Test facilities  
            - Test equipment  
            - Test documentation  
            - Test reports  
            - Test performance monitoring  
            - Test reviews |
| 8. QA Requirements for Acceptance and Delivery | - Acceptance Data Package  
                                                - Delivery Review Board: to authorise shipment and certify conformity/completeness including documentation  
                                                - Preparation for delivery  
                                                - Delivery: shipping control, items properly preserved and packaged, accompanying documentation included |
| 9. Operations | - Quality of mission products  
                          - Validation and Qualification of Ground Support Segments  
                          - QA Plan for operations  
                          - Training and Operator Certification  
                          - Operations anomalies and Feedback corrective Loop; reporting of anomalies and problems  
                          - Deviations from procedures to be justified |
| Annex A: Ground Support Equipment | - Development and Configuration Control: depend on the criticality  
                                         - Production: as minimum ISO 9002 during MAIT  
                                         - Delivery/Maintenance |
Three Document Requirements Description (DRD) added:

» Annex B: Logbook CI historical record of integration and testing activities beginning with qualification/acceptance tests. It includes also configuration data (e.g. change records), quality data (e.g. NCRs), operating hours or cycles for limited life items (e.g., mating/demating of connectors), open works.

» Annex D: Certificate of Conformity

» Annex C: End Item Data Package
  Includes logbooks, CoC, procedures for product handling after delivery, loose items etc.
Beware of the “enemy” called bureaucracy!

Many companies write a huge binders full of procedures to fulfill the customer’s (or ISO standard’s) requirements regardless of whether the procedures do the company any good or make any practical sense. In such a case, engineers and personnel recognise that they are simply facing a bureaucratic exercise and ridicule the QA System.

THE PURPOSE OF A QA SYSTEM IS TO CREATE PROSPERITY

NOT

ENGENDER BUREACRACY
Special techniques - H/W
Statistical Techniques
Statistical techniques

- Statistical process control
- Statistical acceptance sampling
Statistical Process Control (SPC)

- Statistical Process Control is used to:
  - maintain a process within pre-defined limits (evaluate process performance and correct)
  - determine the process capability

- Statistical Process Control is based on the principle that:

  A PROCESS IS IN A STATE OF STATISTICAL CONTROL WHEN THE VARIATION OBSERVED IN ITS OUTPUT CAN BE ATTRIBUTED ONLY TO RANDOM CHANCE
Process performance and process capability

- **Process performance**
  Is the day-to-day behavior of a process including all random and assignable-cause effects

- **Process capability**
  Is an estimate of the best performance of which a process is thought to be capable, with all effects of controllable, assignable-cause variation removed

- **PERFORMANCE - CAPABILITY = POTENTIAL IMPROVEMENT**
Natural process variability

- **Natural Process Variability**
  Process variation is due to several causes (e.g. temperature variations, wearing, clearances, distortions, measurement error etc.). When each cause is held to its practical minimum the resultant process variability is called natural and follows a normal distribution.

![Normal Distribution](image-url)
Detecting assignable causes

Assignable causes are variations above the minimum. They can be detected by periodic sampling of the process and plotting data such that the time-history (i.e., in order of production sequence) is preserved.
Detecting assignable causes (cont’d)

- Most probably an assignable cause exist when there are:
  - one or more points outside \(+/-3\sigma\)
  - 2 or 3 successive points between \(2-3\sigma\) (same side)
  - 4 or 5 successive points beyond \(+/-1\sigma\) (same side)
  - 8 successive points in either \(1\sigma\) band
  - 8 successive rising and falling trends
Estimating process sigma

- Variation within a sample (e.g. 5 consecutive measurements in a short interval) reflect inherent process variability. The range “R” is the excursion between maximum and minimum values within the sample.

- Variation between samples reflect variation due to inherent process variability plus assignable causes (to the extent they may exist).

\[ \sigma' = \frac{\bar{R}}{d_2} \]

where \( \sigma' \) (sigma-prime) is an “estimated” value of \( \sigma \), \( \bar{R} \) is the average of \( R \), and \( d_2 \) is a correction factor depending on sample size.
Calculation of 3-sigma limits (subgroups)

- For $X$ chart:
  
  $\bar{X}$ chart:

  $\text{UCL} = \bar{X} + A_2 \times \bar{R}$

  $\text{LCL} = \bar{X} - A_2 \times \bar{R}$

- For $R$ chart:

  $\bar{R}$ chart:

  $\text{UCL} = \bar{R} \times D_4$

  $\text{LCL} = \bar{R} \times D_3$
Calculation of 3-sigma limits (single values)

- For X chart:

  \[ UCL = \bar{X} + I2 \times \bar{R} \]
  \[ LCL = \bar{X} - I2 \times \bar{R} \]

- A2, I2, D3, D4 are correction factors depending on subgroup size
<table>
<thead>
<tr>
<th>Subgroup Size (n)</th>
<th>d2</th>
<th>A2</th>
<th>D3</th>
<th>D4</th>
<th>L2</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1.128</td>
<td>1.880</td>
<td>0</td>
<td>3.267</td>
<td>2.88</td>
</tr>
<tr>
<td>3</td>
<td>1.693</td>
<td>1.023</td>
<td>0</td>
<td>2.574</td>
<td>-</td>
</tr>
<tr>
<td>4</td>
<td>2.059</td>
<td>0.729</td>
<td>0</td>
<td>2.282</td>
<td>-</td>
</tr>
<tr>
<td>5</td>
<td>2.326</td>
<td>0.577</td>
<td>0</td>
<td>2.114</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>2.534</td>
<td>0.483</td>
<td>0</td>
<td>2.004</td>
<td>-</td>
</tr>
<tr>
<td>7</td>
<td>2.704</td>
<td>0.419</td>
<td>0.076</td>
<td>1.924</td>
<td>-</td>
</tr>
<tr>
<td>8</td>
<td>2.847</td>
<td>0.373</td>
<td>0.136</td>
<td>1.864</td>
<td>-</td>
</tr>
<tr>
<td>9</td>
<td>2.970</td>
<td>0.337</td>
<td>0.184</td>
<td>1.816</td>
<td>-</td>
</tr>
<tr>
<td>10</td>
<td>3.078</td>
<td>0.308</td>
<td>0.223</td>
<td>1.777</td>
<td>-</td>
</tr>
</tbody>
</table>
Example: Calculation of 3-sigma limits (subgroups)

Characteristics: 0.60 +/- 0.003
**Process capability index**

\[ C_p = \frac{\text{tolerance width}}{\text{process capability}} = \frac{\text{USL-LSL}}{6\sigma'} \]

- **C_p** above **1.33**  
  Process **adequate**

- **C_p** below **1.00**  
  Process **inadequate**
Process control and capability

Process out of control but within specification

Process in control but out of specification
Cpk

- The capability index $C_p$ does not take into account the centering of the process. The ratio that reflects how the process is performing in terms of nominal center, or target value is $C_{pk}$

$$C_{pk} = \frac{Z(\text{min})}{3}$$

where $Z(\text{min})$ is the smaller of:

$$Z(\text{USL}) = \frac{\text{USL} - \bar{X}}{\sigma'}$$

or

$$Z(\text{LSL}) = \frac{\bar{X} - \text{LSL}}{\sigma'}$$
“Six-sigma”

- **Six-sigma** is a strategy developed by the Motorola Company to achieve in their processes:

  \[ \text{Cp} = 2 \]

- The main assumption is a “typical” centering error of +/- 1.5 sigma. It means passing from 66,807 defects per million (for +/- 3 sigma) to 3.4 defects per million (for +/- 6 sigma)
“Six-sigma” (cont’d)

- The *six-sigma* implementation steps are:
  - Identify critical characteristics (through marketing, engineering, R&D etc.)
  - Identify the product elements that influence the critical characteristics
  - Identify relevant process elements
  - Establish maximum tolerance for each product and process element
  - Determine actual capability

- The Motorola *Six-Sigma* quality initiative is also a motivational and training initiative
Statistical techniques

- Statistical process control

- Statistical acceptance sampling
Statistical acceptance planning

- Purpose of acceptance sampling is to avoid 100% inspection. Accept/reject entire lot based on the results of sample inspection.

- Single sampling plan:
  - \( N = \) lot size
  - \( n = \) sample size
  - \( c = \) acceptance number
  - \( d = \) number of defective items in sample
  - \( p = \% \) of defective items in lot

\[ d \leq c, \text{ lot accepted; otherwise rejected and controlled 100\%} \]
Producer’s and consumer’s risk

- **AQL** = (Acceptable Quality Level), the percentage of defective items in the lot that represents a “good quality level”. It should lead to acceptance most of the times (usually Pa=0.95)

- **LFTD** = (Lot Tolerance Fraction-Defective Level), the percentage of defective items in the lot that represents a “bad quality level”. It should lead to rejection most of the times (usually Pa=0.10)

- **α** = risk for the producer that lots at AQL are rejected probability

- **β** = risk for the consumer that lots at LFTD are accepted
A good sampling plan is one that effectively identifies the lots that can be accepted and those needing 100% inspection. A tool to support the selection is the *Operating Characteristic (OC) Curve*.

![Diagram of an Operating Characteristic (OC) Curve](image)

- **Pa**: Probability of acceptance
- **AQL**: Acceptable Quality Limit
- **LTFD**: Lot Tolerance for Rejection
- **n**: Sample size
- **c**: Acceptance number
- **1-α**: Significance level
- **β**: Probability of Type II error
- **p**: Fraction nonconforming
Double and multiple sampling plans

- **Double sampling**
  - number of defective < lower limit, accept
  - number of defective > upper limit, reject
  - number of defective between limits, take new sample
  - new accept/reject limits for the 2 samples

- **Multiple sampling**
  - steps 1, 2, 3, as above
  - continue sampling until accept or reject is achieved
MIL-STD-105

- Widely used for acceptance sampling by attribute since 1943
  - Cancelled Feb. 1995
  - Replaced by ANSI/ASQC Z1.4-1993

- Includes simple, double and multiple plans

- Includes normal, reinforced and reduced plans to deal with lots which are continuously received. Passing from normal to reinforced the acceptance number is reduced but sample size remains the same. Passing from normal to reduced, the sample size is reduced
Cost of Quality
Cost of Quality

COQ = PREVENTION + APPRAISAL + FAILURE COSTS, or

COQ = CONFORMANCE COST + NONCONFORMANCE COST

Quality cost measurements provide guidance to the quality management program much as the cost accounting system does for general management.
Cost of Quality: inspected-in quality

Total COQ vary with emphasis placed on prevention or appraisal. Inspected-in Quality, COQ as percentage of Total Cost: 25-40%
Cost of Quality: build-in quality

Build-in quality, COQ as percentage of Total Cost 5-10 %

- Prevention: 50%
- Appraisal: 40%
- Failure: 10%
Cost of Quality: prevention costs

Prevention cost is the cost allocated to prevent the occurrence or recurrence of nonconforming products:

- Quality planning
- Steps to ensure producible/robust design
- Metrology and calibration
- System audits
- Process capability evaluations
- Process qualifications
- Training
- Quality improvement projects
Cost of Quality: appraisal costs

Appraisal cost is the cost of judging the acceptability of products and to detect nonconformances. Appraisal costs are those associated with measuring, evaluating, or audit:

- Design reviews
- Incoming and source inspections
- In-process and final inspection/test
- Product and process audits
Cost of Quality: failure costs

Failure costs are costs resulting from nonconforming products. They are divided into internal costs incurred prior to product delivery, and external costs incurred after product delivery:

- Partial or full loss of the effort already expended
- Additional efforts to make the product acceptable
- Processing of customer reports
- Warranty claims
- Investigating causes
- Determining corrective actions
Cost of Quality: failure costs-scrap

- Cost of additional material to replace unusable material
- Labor cost for manufacturing of replacement material
- Labor cost for non-manufacturing personnel for actions coordination
- Productivity loss due to rescheduling of manufacturing activities
- Storage cost for extra inventory
Cost of Quality: failure costs-rework/repair

- Labor costs for manufacturing personnel performing rework/repair
- Labor cost for non-manufacturing personnel for actions coordination
- Productivity loss
- Costs of materials involved in repairing
- Costs of extra handling/transportation
- Cost of extra rework/repair inspection
- Administrative costs of waivers processing (for repairs)
New model of optimum quality costs

NEW

OLD

IAASS Quality Assurance Course  September 2007
Hidden quality costs

There is a “multiplier effect” between failure costs and “true failure costs”. Failure costs are the tip of an “iceberg”.

IAASS Quality Assurance Course

September 2007
Alert systems

by

P. Secchi
Alert systems

- What is an Alert?
- Types of Alert systems
- GIDEP
- NASA Part Advisories
- NASDA Alert System
- CNES Groupe d’Alertes
- ESA Alert System
What is an alert?

Alert
Alert is a report used to provide a prompt warning on failures and problems which may affect more than one user, or may re-occur in other projects, if no preventive actions are taken.

Alert report
The alert report will include a description of the observed problem, its cause, the actions to be taken to correct it and to prevent recurrence, comments from the manufacturer.
Types of Alert Systems

- Government systems

- Industry systems

IAASS Quality Assurance Course

September 2007
GIDEP
Government-Industry Data Exchange Program

- A co-operative activity between U.S. Government and industry participants, managed and funded by the U.S. Government

- Participating organisations:
  - US Government Agencies and Organisations (including NASA)
  - Industrial organisations producing parts, components and equipment for the government
GIDEP (cont’d)

GIDEP participants are provided electronic access to six major types data:

- Engineering data
- Failure experience data, including ALERTs, SAFE-ALERTs, Problem Advisories and Agency Action Notices
- Reliability and Maintainability data
- Metrology data
- Product information data
- Urgent data request
NASA Parts Advisories

- Intentionally called “Advisory” to distinguish them from GIDEP Alerts and TWX Alerts from other NASA Centers
- Original intention was a rapid “heads-up” warning vehicle
- Provides information and guidance but is not intended to require mandatory action – emphasis on flexibility
- To inform NASA of a significant risk, not to criticize a manufacturer
- First NASA Part Advisory is dated 08/29/90
The NASDA Alert system has been being established since 1974. Is operated by the Safety and Reliability Department (SRD) of NASDA. NASDA Alerts are called Reliability Technical Information (RTI). An RTI describes:

- observed failure/problem and its root cause
- measures to be taken to correct it and to prevent its recurrence

Over 100 RTIs have been issued so far.
CNES Groupe d’Alertes

- Started in 1989
- A Co-operation between CNES and French Space Industry
- Group meets every three months
- Report prepared and issued every three months
- “Anomalies” classified into three levels
- ESA receives CNES Alert Reports
- CNES is a registered user of the ESA Alert System
ESA Alert System

Operated by the ESTEQ TOS-QQ Division to:

◆ Facilitate exchange of information on problems experienced in ESA projects
◆ Eliminate or minimise their impacts
◆ Prevent recurrence on other projects
◆ Enhance competitiveness of European space industry by avoiding waste and mistakes
ESA Alert System (cont’d)

ESA Alerts cover failure related to:

- EEE parts
- mechanical parts
- pyrotechnic devices
- materials
- test equipment
- software used by several users
- equipment procured against a supplier’s specification
- commercial, aviation & military (CAM/COTS) equipment
ESA Alert System (cont’d)

ESA Alert System covers also problems with:

- safety
- manufacturing processes
- handling procedures
- standard test methods
- standard operational procedures
- software development & test methods and tools
- continuity of production of an item
Criteria to issue an ESA Alert

ESA Alerts are only issued when:

- the observed problem may apply to more than one project or organisation and
- the problem was observed while the item was applied within its specified limits and
- a preliminary investigation has provided evidence of the root cause of the problem and
- the problem is confirmed not to be of a random nature
Published ESA Alerts

ESA has published a total of 42 Alerts so far:

- 30 on EEE parts
- 5 on materials
- 3 on mechanical parts or mechanisms
- 1 on manufacturing processes
- 1 on test equipment
- 1 on flight equipment
- 2 on software product
ESA Alerts distribution

- ESA technical departments
- ESA Projects
- ESA contractors
ESA Alert focal point

- Co-ordinate Alert preliminary investigation
- Organise & support proceedings of ESA Alert Committee
- Publish Alerts on the web
- Follow-up of actions to be implemented by manufacturer
- Register new Users to the System
Alert co-ordinators

Alert co-ordinators are the interfaces between company and ESA. Large companies with different geographical locations have more than one Alert co-ordinator.
Technical experts role

- Review Preliminary Alert Information
- Assess failure/problem against criteria for issuing an alert
- Define recommended actions to:
  - to solve failure/problem
  - to prevent recurrence
- Assess:
  - Manufacturer’s response
  - Alert corrective actions
  - Feedback from users
- Recommend whether to issue Alert or not
ESA Alert System Web

Access restricted to registered participants only. It allows to:

- browse ESA Alerts
- search ESA Alerts
- request Access
- submit PAI on-line
- submit feedback/comments on-line

Have a look at: www.estec.esa.nl/qq/alerts
Concepts, Techniques and Standards

Part II – S/W

by

J. M. Carranza
Outline of the session

- Preliminary topics
- SW PA structure, concepts and techniques:
  - SW process assurance:
    - Configuration management
    - Verification and validation
    - System and SW Lifecycles
    - Process assessment and improvement
  - SW product quality assurance: Quality models and metrics
  - SW PA programme implementation:
    - SW safety
    - Organisation, Management and Planning
- Evolution of concepts
- European space SW standards
QA versus SW QA

- There is and should not be separation of the two
- SW QA is an aspect or a branch of QA
- Techniques used in SW QA are very much the same as those in the rest of QA
- Emphasis on techniques and methods is different in SW because of differences between essential properties of SW and HW
- However there is nothing special about SW QA only differences
Properties of SW

- SW is highly volatile and can be changed completely at the touch of a button ⇒ the myth that it is always possible (and cheaper) to correct in SW the HW problems
- All faults in SW are systematic. Therefore:
  - statistical control, etc. cannot be applied
  - statistical measurements are applicable in a limited fashion only
- Often there is no immediate direct relation between the apparent importance of the fault and the importance of the failure that it may produce
A few definitions (IEC)

**Fault**

Unplanned occurrence or defect in an item which may result in one or more failures of the item itself or of other associated equipment

[IEC 50 1992]

**Failure**

Termination of the ability of an item to perform a required function

[IEC 50 1992]
A few (working) definitions

**Fault**
*Defect introduced in the software through error or oversight in software specification, design, coding or maintenance*

**Failure**
*Malfunction in the software caused by a fault in the software or by propagation of a failure from another part of the system*

**SW Product Assurance**
*Union of SW Quality Assurance and SW Safety Assurance*
Characteristics of SW engineering

- Its implantation as an engineering discipline is weaker than in other engineering disciplines due to:
  - its relative “youth” as an engineering discipline compared to others
  - the very quick pace at which technology, techniques and methods evolve ⇒ need to adapt very quickly, lack of consolidation
- It is difficult to separate new from old: everything from dinosaurs to primates are alive and living together
- It is difficult to separate good from bad:
  - lack of historical information (experience) from technologies/methods/tools
  - high commercial pressure (rapidly evolving and aggressive tools market)
SW PA Concepts and Techniques
SW PA Concepts and Techniques

- **SW process assurance:**
  - **Structure of the SW PA discipline**
    - Configuration Management
    - Verification and validation
    - System and SW Lifecycles
    - Process Assessment and Improvement
- **SW product quality assurance:**
  - Quality Models and Metrics
- **SW PA programme implementation**
  - SW Safety
  - Organisation, Management and Planning
Structure of the SW PA discipline

**SW PA programme**

- Implementation

- "Everybody’s job"

- Supports

**SW process assurance**

- Supports

**SW product quality assurance**

- "SW PA people’s job"

"Everybody’s job" supports both SW process assurance and SW product quality assurance.
SW PA Concepts and Techniques

- SW process assurance:
  - Structure of the SW PA discipline
  - Configuration Management
  - Verification and validation
  - System and SW Lifecycles
  - Process Assessment and Improvement

- SW product quality assurance:
  - Quality Models and Metrics

- SW PA programme implementation:
  - SW Safety
  - Organisation, Management and Planning
Configuration management for S/W

- Configuration management in SW is the same as at the system level:
  - Configuration identification: how to identify items that are part of the project
  - Configuration control: concept of baselines
  - Change control: how to change in a controlled manner
  - Storage and handling: of configuration items
  - Status accounting: what is the state of the items
  - Configuration verification: is CM performing correctly
  - Traceability: not strictly CM but underlying topic
‘Internal’ and ‘external’ CM

- External CM links to system level CM:
  - Identification of formal Configuration Items
  - Links to system level change control
  - Interfaces to other domains, teams, organisations
- Internal CM:
  - Internal identification
  - Specific SW change control
  - Integrated in the daily work
- Formal Configuration Items set the boundary between ‘external’ and ‘internal’ CM
Configuration identification

- Volatility of SW allows very easy creation, deletion, modification AND DUPLICATION of SW items
- Volatility makes it important to know which items are part of the project and which are not ⇒ risk of introducing confusion (e.g. temporary artifacts)
- Difference with HW identification: duplicate items are still the same item (no serial number)
- SW systems are composed of many custom made components: complexity and lack of standardisation
- Configuration Item Identification must be planned before starting to create items
Configuration identification: hierarchy

- SW CM continues decomposition from system level identification
- Internal identification will probably follow a different convention than at system level

System Spacecraft
SC-0000-01

Subsystem A
SC-1000-01

Subsystem AOCS
SC-2000-01

Subsystem C
SC-3000-01

AOCS HW
SC-2100-01

AOCS SW
SC-2200-01
Configuration identification: types of items

◆ Three common types of internal configuration items:
  – SW artefacts: source code, data files, etc. ⇒ identification typically based on naming conventions although they can follow product tree as well
  – Tools: used to develop the SW
  – Documents: they can follow the product tree or they can have their own identification convention (e.g. reference numbers)

◆ Caution: identification of SW artefacts based on naming convention must avoid ambiguity. For example by:
  – Including context information in the name, e.g. AOCS_SafeMode
  – Including the relative pathname in the header of the file. Many CM tools will allow to make this automatic
Configuration control: baseline

- SW systems are very tightly coupled systems
- Consistency is critical: change in A requires change in B otherwise the system will not operate properly
- Baselines are **consistent** and **complete** sets of all items that make up the system or a part of it and allow co-ordination across the team
- Baselines have a well defined **purpose**
- Formal CI’s require formally defined baselines
A trivial example of a baseline: automatic train stop

Call and pass distance

Func A (v1): Calculate distance to end in yards

Func B (v3): Calculate braking distance (yards) and decide if to brake

Func A (v2): Calculate distance to end in cm

Func B (v4): Calculate braking distance (cm) and decide if to brake

Are valid baselines

May be not:

IAASS Quality Assurance Course

September 2007
Baseline evolution

- Baselines are created more often for SW than for HW systems
- Baselines must be planned according to their purpose
- Specially important baselines are:
  - Inputs to formal reviews
  - Outputs from formal reviews (often ignored)
  - Test baselines
  - Deliveries
- Baselines are configuration items
  ⇒ identification conventions should consider them specifically
Baselines along project lifecycle

Baselines grow along lifecycle as the project advances, for example:

- Customer starts project
- Preliminary Design Review
- Requirements
- Project Plans
- Requirements
- Technical Specification
Baselines along project lifecycle (cont’d)

- Project Plans
- Requirements
- Technical Specification
- Design
- SW components
- Test Plans, Specifications and Reports
Baselines along project lifecycle (cont’d)

Acceptance Review

- Project Plans
- Requirements
- …everything

SW deployment

- Software
- Operations Manual
- Maintenance Forms

Maintenance
Change control

- Complexity of SW makes it difficult to assess the impact of changes in one part of the system on another
- Individuals in a team may not be able to judge that impact
- Contractual implications may not be evident to developers
- Change control is a mechanism to allow a baseline to change into another avoiding above risks
- Key concepts:
  - entry of a configuration item under configuration control
  - authority to change (often not the developer)
  - check points in change implementation
  - all of the above adequately sized for the project
Change control is triggered by non-conformances, problem reports and change requests.

Software changes much faster than hardware \(\Rightarrow\) efficient change control procedure, normally separate from hardware procedure.

In system’s development, software change control will need formal interfaces to system’s non-conformance handling and system’s change requests.

One key point: once a configuration item is under change control, it is not the “property” of the author any more.
Nonconformance processing: example

- **QUALITY CONTROL** (or other authorised unit)
  - Prepares Discrepancy Notice (DN)
  - Segregation

- **PRELIMINARY REVIEW (PR)**
  - QA conducts PR
  - Disposition for SRP or minor rework
  - Promotion to MRB

- **QUALITY ASSURANCE**
  - NCR preparation
  - Notifies of forthcoming MRB
  - Assesses cumulative effect of previous NCRs

- **MATERIAL REVIEW BOARD (MRB)**
  - Customer participation for major NCR
  - MRB determines disposition

- **CUSTOMER (ANY LEVEL)**
  - Waiver number

- **CONFIGURATION MANAGEMENT**
  - Conducts CCB
  - Dispositions and approves waiver
  - Contractual authorization to proceed with waiver (note 5)

- **QUALITY ASSURANCE**
  - Waiver numbering
  - Schedules change board (if needed)
  - Prepares supporting data and description / justification for waiver

- **VERIFIES CORRECT IMPLEMENTATION OF DISPOSITION (after implementation)**

- **PREPARES SUPPORTING DATA AND DESCRIPTION / JUSTIFICATION FOR WAIVER**

IAASS Quality Assurance Course

September 2007
SW problem report processing: example

- Problem found (directly or system NCR)
- Create SPR (central record)
- Evaluation (CM/PM/QA)
- CCB disposition (PM/CM/QA)
- Implementation (CM/PM/QA)
- Verification
- CCB (can be PM/CM/QA)
- SPR closed (inform system level if needed)
- NCR to system level
- Implement

Do not implement
Storage, media

- CIs must be made available for use: libraries, views, etc.
- Each “library” must have a clear meaning: e.g. released version, latest version (live), etc.
- Clear definition of storage media, which type of media for each type of baseline:
  - Important to define how different baselines and libraries are stored: e.g.”live” versions on hard disk, release baselines on CD, documentation on CD or paper?
Storage

- Configuration Items are stored as:
  - Libraries: physical or on-line
  - Configuration tool repositories
  - Distribution media
- It is critical to know which is the master CI
- Usually at least the master is maintained with a configuration management tool (for on-line items)
- The repository is normally maintained by the tool and should be considered internal to the tool: not intended for human use ⇒ keep your hands off it
Libraries

- Although which is the master of a CI is important, multiple libraries can be useful
- An example:

  **Development:**
  - Internal to team
  - SW may fail

  **Stable:**
  - Shared with other development teams
  - SW may fail

  **Released:**
  - Copies of all released versions
  - Unchangeable

- Rules to go from one library to another must be defined: e.g. to Stable when unit tested; never back from Released, etc.
Storage, security

- CIs are worth money
- Physical security:
  - Access to physical media and equipment (also safety implications)
  - Protection against loss: well defined strategy for backup including storage of backup media: periodicity, scope; etc.
- Computer security: access through network? password protection? etc.
- Projects do suffer from attacks and accidents: complete software projects have evaporated
Handling and change authority

- Responsibilities and authorities for handling of items in libraries and change control must be specifically defined ⇒ roles and types of access, for example:

<table>
<thead>
<tr>
<th>Role</th>
<th>Create</th>
<th>Read</th>
<th>Modify</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW Engineer</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Tester</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System engineer</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration Manager</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Configuration verification

- On-going process
- Functional configuration audit:
  - All requirements covered
  - Verification and validation completed
  - NCRs, SPRs, etc. handled appropriately
  - Needed documentation available and up to date
- Physical configuration audit:
  - Consistent baseline
  - Physical media:
    » Correct content
    » Adequately labelled
Importance of traceability

- Baselines are not formed only by SW components. They may include also:
  - Specification (e.g. requirements)
  - Design
  - Verification items (test specifications, verification records, etc.)
  - Management documentation
  - User documentation, etc.
  - Development and verification tools
- Traceability is a fundamental tool to ensure completeness and also consistency of baselines
Traceability

- Traceability binds CIs into baselines
- Some important traces:

  - System specifications (or user requirements)
  - Software specifications (or software requirements)
  - Test specifications
  - Test reports
  - Code
  - Design
SW PA Concepts and Techniques

◆ SW process assurance:
  – Structure of the SW PA discipline
  – Configuration Management
  ✅ Verification and validation
  – System and SW Lifecycles
  – Process Assessment and Improvement

◆ SW product quality assurance:
  – Quality Models and Metrics

◆ SW PA programme implementation
  – SW Safety
  – Organisation, Management and Planning
Verification and validation: ISO definitions

**Verification**
Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled
[ISO 9000:2000]

**Validation**
Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled
[ISO 9000:2000]
Verification and validation: working definitions

Verification
Activity to ensure that the outputs of a process conform to its inputs (completeness, consistency, correctness)

Validation
Activity to ensure that a product or service is adequate for its intended use (use related)
Verification: phases

- Verification is not limited to testing
- Verification takes place at each phase of the software lifecycle:
  - requirements specification: formal review, etc.
  - design: walkthrough, review, modelling, etc.
  - coding: code review, inspection, unit testing, etc.
  - operation: non-regression testing, etc.
- Most verification activities are supported by traceability

Requirement X changes $\Rightarrow$ traceability helps identifying:
  Design components $Y_1, Y_2$ to change $\Rightarrow$ traceability helps identifying:
  Tests $Z_1, Z_2, Z_3$ to execute
Verification: scope

- Verification covers more than just the SW
- Items that should or may be verified are:
  - SW itself
  - documentation
  - implementation of processes
  - tools
  - infrastructure
Verification: techniques

- Different methods are used in SW
- The main ones are:
  - Testing
  - Review
  - Inspection, walkthrough
  - Audit
- Verification techniques may be intended for products (e.g. testing), processes (e.g. maturity assessments) or both (e.g. formal reviews)
Testing: planning

- Testing can take a lot of effort, therefore it is important to plan carefully:
  - What to test?
  - How to test?
  - When to test?
  - Where to test?
  - Who tests?
  - How well to test?
Testing: what to test?

- What to test depends on:
  - What the customer requires us to test +
    What the applicable standards mandate +
    What engineering good practice and common sense ask for
- What to test is expressed as a baseline: list of items and specific versions of each of them that will be the subject of testing
- Items to test are different at different levels:
  - Modules
  - SW sub-systems
  - Complete SW products
Testing: how to test, types of test?

- Testing can be aimed to test implementation, with specific knowledge of the internal logic ⇒ white box testing
- Testing can be aimed to test functionality at different levels, ignoring the internal logic ⇒ black box testing
- Black box testing can be of different types also:
  - nominal: test for normal conditions
  - back to back: same test on two or more versions of SW written with same specifications
  - interface: written on the basis of interface specifications
  - stress: test under extreme or abnormal conditions
  - statistical: test data selected according to statistical distribution
Testing: how to test, levels of test?

- Testing is performed at different levels
- Levels of testing have different targets and objectives:

<table>
<thead>
<tr>
<th>Level</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit</td>
<td>Source code units</td>
</tr>
<tr>
<td>Integration</td>
<td>Interfaces</td>
</tr>
<tr>
<td>System*</td>
<td>SW Specifications</td>
</tr>
<tr>
<td>Acceptance*</td>
<td>User or system specifications</td>
</tr>
</tbody>
</table>

*The different levels may have different names or be organised in slightly different ways (e.g. in ECSS terminology system and acceptance testing might translate into: validation against technical specifications and validation against requirements baseline).
Testing: unit testing

- It is structural testing (driven by design)
- It is the best level to ensure that:
  - Either all or a representative part of the software components is actually tested ⇒ structural coverage criteria
  - Unusual paths in the code, e.g. error handling or non-nominal conditions, are tested
- Unit testing requires significant effort but on the other hand it is the level for which more automation tools are available, e.g. test case generation, etc.
- Importance of defining what is a unit: small piece of code: class, single function, etc.
Testing: integration testing

- Integration testing is also structural testing
- When the SW architecture is built on several levels integration testing will happen at several levels too

Subroutines or classes

Integration testing

SW subsystems or applications

Integration testing

SW system
Testing: some key issues in integration testing

- Integration testing tests communication across interfaces ⇒ the subject of test must be identified ⇒ interfaces must be identified:
  - Explicitly: CI identification convention for interfaces
  - Implicitly: all public methods in a class
- At a low level integration, integration testing based on low level design
- At a high level integration (e.g. sub-systems), integration testing is based on interface specifications
- Sequence of integration is a critical part of planning integration tests:
  - What must be tested before what: schedule constraints
  - What will be stubbed and what not: development effort
Testing: system and acceptance testing

- Requirements-based testing

<table>
<thead>
<tr>
<th></th>
<th>System testing</th>
<th>Acceptance testing</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Involves</strong></td>
<td>Development organisation</td>
<td>Development organisation and customer</td>
</tr>
<tr>
<td><strong>Is normally based on</strong></td>
<td>Requirements or specifications produced by the development organisation</td>
<td>Customer requirements</td>
</tr>
</tbody>
</table>
Testing: when to test?

- Lower level testing can take place interleaved with implementation
- Detecting lower level faults at high level testing (late) is expensive

⇓

Levels of testing should be performed in sequence: testing activities need to be scheduled in sufficient detail

⇓

Higher level testing (validation) requires complete baselines, therefore it should only be performed after development and lower level testing have been performed
- Validation is in most cases contractually relevant: specific dates, customer involvement, formal
Testing: where to test?

- Test environment: platform + test tools
- Define test environment requirements independently from development environment requirements (although often it will happen that both are compatible and a single environment is sufficient).
- However it is a very common mistake to take for granted that the development environment is also the testing environment: twisting the first into the second often leads to:
  - Cost (time and money) for customer and supplier
  - Lower quality of product (poorer testing)
- Physical environment is also very important:
  - Target or simulator
  - Customer premises or factory environment (validation)
  - Etc.
Roles, responsibilities and competencies should be defined for each of the testing activities:

- Who supplies the SW baseline (developer at lower levels?, CM at higher levels?) and ensures that it is correct?
- Who performs the test (developer, separate tester)?
- Who decides/authorises when to start/stop/repeat/deviate (formal testing)?
- QA involvement?
- Customer (acceptance)?

Planning should detail who does what and when for all of the above and who is responsible for what.
Testing: who tests? (Cont’d)

- Testing is a separate activity from implementation
- There may be specific requirements for levels of independence in the testing and verification in general (Independent SW Verification and Validation):
  - no independence
  - 1st party ISVV: different people in the same team
  - 2nd party ISVV: different team in the same organisation/company
  - 3rd party ISVV: different organisation/company
- Good engineering practices may ask for independence even in the absence of formal requirements
- Level of independence will normally be proportional to level of criticality of software
Testing: how well to test?

- It is always possible to improve testing
- Deciding when to stop testing (other than running out of time) is not easy
- Goals must be set beforehand to ensure sufficient and uniform testing
- Goals for white box testing are typically based on structural coverage (statement, branch, path, etc.)
- Goals for black box testing will depend on its objective (e.g. software requirements, architectural design, etc.) and specific requirements (e.g. test specific non-nominal conditions)
- The mark of a good SW development manager is to avoid quality of testing being compromised by delays in implementation
Testing: specification

Although they may appear in other forms there are four types of artefacts used to specify tests and their results:

- Test design: what are we trying to achieve with a specific test; to be read by people and not always trivial (e.g. prove that train will stop at the right spot)
- Test case: specific set of conditions/data to be used in a specific execution of a test design (e.g. train at half load, running at 60 Km/h, etc.)
- Test procedure: the mechanism (test harness, procedure for operators, etc.) to execute tests
- Test report: the detailed result of the execution of a particular test case with a particular test procedure
Testing: specification (cont’d)

- Test designs drive the definition of the others
- These four artefacts do not need to map one to one: several test cases for a single design, same test procedure for several designs, same test case used in several designs, etc. ⇒ traceability again!
Testing: A typical scenario for specification

Objective: test response to loss of sun pointing
Way: simulate failure of attitude actuators and check response from AOCS

Test design

Test procedure

Detailed steps to inject faults in the target environment with a fault injection tool

Test cases:
- Failure of reaction wheel
- Failure of thruster

Test reports:
For each case/procedure

IAASS Quality Assurance Course

September 2007
Testing: verification

- Testing itself is subject to verification
- This will typically involve specific reviews of the test plan and test designs, cases and procedures
- It may involve additional verification: e.g. mutation testing
- Coverage and status of the testing must be controlled formally:
  - Verification Control Document
  - Coverage reports for structural testing
- In the ECSS standards test verification is called evaluation
Testing: baselines change

- Baselines are crucially important in SW testing
- Any level or type of testing starts from a properly controlled baseline ⇒ baseline identification (contents and versions of each item)
- Testing should be performed in well defined cycles, each cycle using a single baseline
- Problems found during formal testing are processed through the change control procedure once the CI is under formal configuration control
- Implementation of changes leads to a new baseline which is input to the next cycle of testing
- Do not give in to the temptation of changing along the way
Testing: baselines change (cont’d)

- Changes during testing are usually localised ⇒ testing should be adapted to the change ⇒ non-regression testing
- Non-regression testing should be performed from the lowest level up to the level at which the corresponding fault was found
- Traceability is an invaluable tool to define non-regression testing (e.g. which units do I test if a test for software requirement x failed)
- Dependencies between components, etc. must be taken into account
- Automate test where possible
Verification: inspections and walkthroughs

- Different types with different objectives:
  - Inspection: identify faults or non compliances (e.g. coding std.)
  - Walkthroughs: identify faults, bad coding practices, possible improvements

- Inspections are formal and involve specific roles:
  - Moderator: leader and chair of the inspection
  - Secretary: recording of inspection meetings (including defects)
  - Reader: guides the inspection through the inspection items
  - Inspector: identify and describe defects
  - Author: person who produced the inspected items

- Well known type of inspections is the Fagan inspection
Verification: other techniques

- Other verification techniques are very similar to general verification techniques:
  - Formal reviews: sometimes SW reviews integrated in system reviews
  - Audits
  - Peer or informal reviews: very important in SW, I cannot see my own mistakes
SW PA Concepts and Techniques

- SW process assurance:
  - Structure of the SW PA discipline
  - Configuration Management
  - Verification and validation
  - System and SW Lifecycles
    - Process Assessment and Improvement

- SW product quality assurance:
  - Quality Models and Metrics

- SW PA programme implementation
  - SW Safety
  - Organisation, Management and Planning
SW lifecycle models

- Abstract representations that allow to organise and plan SW development activities

- Common ones are:
  - Waterfall
  - Incremental
  - Evolutionary

- System development follows established lifecycle models too
System and SW levels

- Lifecycle models at system and SW level need not be the same
- Even if they are the same it is very unlikely that lifecycles will be synchronised
- SW lifecycle model selection is important and may be based, for example, on:
  - System lifecycle constraints
  - Contractual constraints
  - Project constraints
  - Technical aspects
Models: phases and milestones

- Most models are organised into phases connected by milestones
- Typical system milestones in space projects are:
  - System Requirements Review
  - Preliminary Design Review
  - Critical Design Review
  - Qualification Review
  - Acceptance Review
- SW models will have roughly similar milestones
- Synchronisation of phases and milestones between system and SW is a significant issue
Lifecycle synchronisation: rules of thumb

- Mapping and synchronisation of system and SW lifecycles must consider the exchange of inputs and outputs between both levels.
- Usually requirements for SW are taken from system, subsystem, equipment, etc. specifications (available at system PDR) \(\Rightarrow\) SW development starts with system PDR.
- Usually stable SW is required for system integration \(\Rightarrow\) SW CDR should take place in advance of integration (e.g. at system CDR).
- Detailed specification of SW may be needed to complete detailed design of system \(\Rightarrow\) SW CDR in advance of system CDR.
- Depending on project and contractual constraints the SW may need to be formally accepted before integration \(\Rightarrow\) SW AR in advance of system QR.
Synchronisation example: waterfall model

- **Preliminary Design**
  - SRR
  - PDR

- **Detail. Design**
  - PDR
  - CDR

- **Manufacturing, integration and testing**
  - QR
  - SRR
  - PDR

- **Requirements and Architectural Design**
  - PDR

- **Detailed Design, Implementation**
  - DDR

- **Integration Testing**
  - CDR

- **Testing Against SW Specifications**
  - CDR

- **Testing Against User Requirements**

*IAASS Quality Assurance Course September 2007*
SW PA Concepts and Techniques

- SW process assurance:
  - Structure of the SW PA discipline
  - Configuration Management
  - Verification and validation
  - System and SW Lifecycles
  - Process Assessment and Improvement

- SW product quality assurance:
  - Quality Models and Metrics

- SW PA programme implementation
  - SW Safety
  - Organisation, Management and Planning
Software process assessment

- Quality of software is directly related to the quality of the development processes carried out to produce the software
- Measuring the capability of the processes carried out by an organisation to develop software provides key information on the ability of that organisation to produce good quality software consistently
- SPiCE for Space (S4S) is a framework that allows measuring the capability of software development processes
Example: Motorola (2003)

Software Cost of Quality vs. Productive Work

- Creation Cost (Productive Work)
- Prevention Cost (Training, Prevention, …)
- Appraisal Cost (Test, Inspection, …)
- Cost of Poor Quality (Fixing, Retesting, …)

Motorola GSG
Average Creation = 62%

Best in Class
Creation = 82% (Raytheon)

Productivity (relative):
- Level 1: 1X
- Level 2: 1.4X
- Level 3: 2.2X
- Level 4: 2.9X
- Level 5: 3.4X

IAASS Quality Assurance Course
September 2007
Higher maturity leads to better predictability

Software Process Improvement Works!
Ferguson et al. (AIS Inc.), CMU/SEI-99-TR-027

IAASS Quality Assurance Course  September 2007
Higher quality & less need for rework

Findings from General Dynamics

Percentage of Rework

Level 2
Level 3
Level 4
Level 5

“How CMM Impacts Quality, Productivity, Rework, and the Bottom Line”
M. Diaz and J. King, Crosstalk, March 2002.
What is S4S?

- A method of evaluating space software development processes
- ISO/IEC 15504 (SPiCE) conformant
- Developed by ESA for the European space industry
- Can be tailored to different classes of critical software
ESA’s goals

- Encourage production of the best possible software products and services
- Develop customer-supplier relationships based on trust, not control
- Promote and disseminate best practice concepts proven across the software industry
- Widen supplier base to companies traditionally outside of the aerospace domain
S4S purposes

S4S may be used in three defined purposes:

- **Capability Determination**: Evaluate the maturity of current software processes within an organisation
- **Process Improvement**: Provide a solid basis for improving processes
- **ECSS Compliance**: Determine capability to comply with (European) space standards
Inputs to S4S

- ECSS Management, Engineering and Quality Standards for Space Software
- ISO/IEC 15504 (SPiCE): (Software) Process Assessment
What is ISO/IEC 15504?

- International standard for assessing software processes
- Developed in parallel with other software engineering standards (ex. ISO/IEC 12207)

Scope
  - Comprehensive
    » Processes include acquisition, supply, development, operation, maintenance and support
  - Modular
    » Can select which processes to assess
    » Each process is assessed on a scale of capability
SPICE: The Assessment Model

- Two-dimensional model for processes and process capability
  - Process Dimension
    » Process Categories
    » Processes (P1, ..., Pn)
  - Capability Dimension
    » Capability Levels (CL1, ..., CL5)
    » Process Capability Attributes.
- Each process receives a capability level rating.
Optimising
Quantitative measures used for continuous improvement process

Predictable
Metrics make process performance and results controllable

Established
Predefined processes are tailored for specific use, resources are managed..

Level 5  Optimizing
PA.5.1  Process Change
PA.5.2  Continuous Improvement

Level 4  Predictable
PA.4.2  Process Control

Level 3  Established
PA.3.1  Process Definition
PA.3.2  Process Resource

Level 2  Managed
PA.2.1  Performance Management
PA.2.2  Work Product Management

Level 1  Performed
PA.1.1  Process Performance

Level 0  Incomplete

Incomplete
Performance and results are incomplete, chaotic processes

Managed
Process and work products are managed, responsibilities identified.

Predictable
processes are intuitively performed, input and output work products are available

Performable
S4S: The Process Dimension

**ENGINEERING:**
- ENG.1 Requirements Elicitation
- ENG.2 System Requirements Analysis
- ENG.3 System Architecture Design
- ENG.4 Software Requirements Analysis
- ENG.5 Software Design
- ENG.6 Software Construction
- ENG.7 Software Integration
- ENG.8 Software Testing
- ENG.9 System Integration
- ENG.10 System Testing
- ENG.11 Software Installation
- ENG.12 Software and System Maintenance

**ACQUISITION:**
- ACQ.1 Acquisition Preparation
- ACQ.2 Supplier Selection
- ACQ.3 Contract Agreement
- ACQ.4 Supplier Monitoring
- ACQ.5 Customer Acceptance
- ACQ.6 Contract Maintenance

**SUPPLY:**
- SPL.1 Supplier Tendering
- SPL.2 Product Release
- SPL.3 Product Acceptance Support

**ENGINEERING:**
- ENG.1 Requirements Elicitation
- ENG.2 System Requirements Analysis
- ENG.3 System Architecture Design
- ENG.4 Software Requirements Analysis
- ENG.5 Software Design
- ENG.6 Software Construction
- ENG.7 Software Integration
- ENG.8 Software Testing
- ENG.9 System Integration
- ENG.10 System Testing
- ENG.11 Software Installation
- ENG.12 Software and System Maintenance

**OPERATION:**
- OPE.1 Operational Use
- OPE.2 Customer Support

**MANAGEMENT:**
- MAN.1 Organizational Alignment
- MAN.2 Organization Management
- MAN.3 Project Management
- MAN.4 Quality Management
- MAN.5 Risk Management
- MAN.6 Measurement
- MAN.7 Information Management

**REUSE:**
- REU.1 Asset Management
- REU.2 Reuse Program Management
- REU.3 Domain Engineering

**RESOURCE AND INFRASTRUCTURE:**
- RIN.1 Human Resource Management
- RIN.2 Training
- RIN.3 Knowledge Management
- RIN.4 Infrastructure

**PROCESS IMPROVEMENT:**
- PIM.1 Process Establishment
- PIM.2 Process Assessment
- PIM.3 Process Improvement

**SUPPORT:**
- SUP.1 Quality Assurance
- SUP.2 Verification
- SUP.3 Validation
- SUP.4 Joint Review
- SUP.5 Audit
- SUP.6 Product Evaluation
- SUP.7 Documentation
- SUP.8 Configuration Management
- SUP.9 Problem Resolution Management
- SUP.10 Change Request Management
- SUP.11 Safety and Dependability Assurance
- SUP.12 Independent Software Verification and Validation
## Example assessment results

<table>
<thead>
<tr>
<th>Process</th>
<th>Capability Level 1</th>
<th>Capability Level 2</th>
<th>Capability Level 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>CUS.1 Acquisition Process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CUS.1.1 Acquisition Preparation Process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CUS.1.2 Supplier Selection Process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CUS.1.3 Supplier Monitoring Process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CUS.1.4 Customer Acceptance Process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CUS.2 Supply Process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CUS.3 Requirements Elicitation Process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CUS.4 Operation Process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CUS.4.1 Operational Use Process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CUS.4.2 Customer Support Process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENG.1 Development Process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENG.1.1 System Requirements Analysis Process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENG.1.2 Software Requirements Analysis Process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENG.1.3 Software Design Process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENG.1.4 Software Construction Process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENG.1.5 Software Integration Process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENG.1.6 Software Testing Process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENG.1.7 System Integration and Testing Process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENG.2 System and Software Maintenance Process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SUP.1 Documentation Process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SUP.2 Configuration Management Process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SUP.3 Quality Assurance Process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SUP.4 Verification Process</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Differences between S4S and ISO 15504

In comparison with SPiCE, S4S has:

- **4 New Processes**
  - ACQ.6 Contract Maintenance
  - MAN.7 Information Management
  - SUP.11 Safety and Dependability Assurance
  - SUP.12 Independent Software Verification and Validation

- **Many lower level elements**
  (~40 new Base Practices, ~70 new Notes, ~30 new Work Products)
Performing a S4S assessment

Assessment Steps

- Initiation
  - define purpose, scope, context of assessment
- Planning
- Briefing
- Data Acquisition
  - through interviews and document examination
- Data Validation
- Process Rating
- Reporting
## Typical capability levels

<table>
<thead>
<tr>
<th>Component</th>
<th>Capability Level 1</th>
<th>Capability Level 2</th>
<th>Capability Level 3</th>
<th>Capability Level 4</th>
<th>Capability Level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENG.1.2 Software</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Managed</strong></td>
</tr>
<tr>
<td>Requirements</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Managed</strong></td>
</tr>
<tr>
<td>ENG.1.3 Software</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Managed</strong></td>
</tr>
<tr>
<td>Design</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Managed</strong></td>
</tr>
<tr>
<td>SUP.2 Configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Performed</strong></td>
</tr>
<tr>
<td>Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Managed</strong></td>
</tr>
<tr>
<td>SUP.3 Quality</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Managed</strong></td>
</tr>
<tr>
<td>Assurance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Managed</strong></td>
</tr>
<tr>
<td>MAN.2 Project</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Managed</strong></td>
</tr>
<tr>
<td>Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Managed</strong></td>
</tr>
<tr>
<td>MAN.4 Risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Managed</strong></td>
</tr>
<tr>
<td>Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Managed</strong></td>
</tr>
</tbody>
</table>
ISO 15504 Improvement Cycle

1. Examine organisation's needs
2. Initiate process improvement
3. Perform process assessment
4. Analyse results and derive action plan
5. Sustain improvement gain
6. Confirm the improvement
7. Implement improvement
8. Re-Assessment Request
9. Analysed assessment results
10. Approved action plan
11. Analyse results
12. Re-Assessment Request
13. Approved action plan

Improvement initiation
S4S
Preliminary improvement programme plan

Validated improvement results
Approved action plan
Implement improvements
Institutionalised improvements
Assessment results

IAASS Quality Assurance Course
September 2007
Motivations for process improvement

Why do you want to improve your processes?

- We need to improve the quality of our products
- We want to be better than our competitors
- We need more efficiency
- ... 
- My customer has asked me to do so!
S4S risk architecture

- R4S is an extension of S4S with a new Risk Dimension integrated in the method
- R4S addresses risks arising from inappropriate process management
- R4S is orientated to the risks involved in processes (from the S4S model)
Main issues

- Process orientated risks originate from the actual capability of a process not reaching the required capability.
- Process orientated risks are due to inadequate or insufficient management of the process performance.
- More than one process may contribute to one risk.
Elements of R4S

- In R4S the gap between the actual and required capability is analysed in detail (all process attributes)
- Risks are evaluated and classified according to their importance (acceptable, unacceptable, intermediate)
- R4S allows to identify actual management practices that need to be addressed in order to mitigate risks
- R4S differs from process improvement in that it does not try to reach a target capability but to correct those deficiencies that allow mitigation of the unacceptable process orientated risks
SW PA Concepts and Techniques

- SW process assurance:
  - Structure of the SW PA discipline
  - Configuration Management
  - Verification and validation
  - System and SW Lifecycles
  - Process Assessment and Improvement

- SW product quality assurance:
  - Quality Models and Metrics

- SW PA programme implementation
  - SW Safety
  - Organisation, Management and Planning
Metrics

- Metrics provide quantitative information on products or processes
- Metrics can be classified according to the entities from which they are extracted:
  - Process metrics
  - Product metrics
- Metrics can also be classified according to the entities to which they are addressed:
  - Project metrics
  - Organisation metrics
Metrics (cont’d)

- Project metrics: goals and associated reaction mechanisms to react to goals not being reached

- An example:
  - metric: cyclomatic complexity
  - goal: < 10
  - reaction: re-design module
Product metrics

- Product metrics measure the quality of the product
- Metrics should be defined on the basis of the most relevant properties of the specific SW being developed: Portability? Maintainability? Efficiency? Reliability?
- These properties are defined, in turn, on the basis of the quality requirements for the product
- Quality models are the mechanism to define a consistent and useful metrics program (e.g. ISO 9126, SPEC)
Their objective goes beyond the project ⇒ no immediate apparent benefit for the project

They rely on an organisation at a higher level than the project ⇒ metrics from different project must be collected and analysed

They have to be highly independent of technology (e.g. design complexity metrics from different models may not be comparable)

They are useful in the long term:
- Help define organisation strategy
- Improve development processes
- Etc.
Some metrics examples

- **Product metrics:**
  - code size: number of lines of code
  - design size: number of design components
  - code complexity: cyclomatic complexity
  - design complexity: depth of inheritance tree

- **Process metrics:**
  - actual effort against estimated effort
  - problems detected during system testing
  - rate of problems reported during operation
The SPEC Quality Model

- Developed by ESA for the space domain
- Its architecture is:

Goal property ➔ Property ➔ Property ➔ Metric ➔ Evaluation method
SPEC: an example

Goal property: reliability

Property: maturity

Metric: functional implementation stability

Definition: \( X = 1 - \frac{A}{B} \)

A: number of functions changed
B: number of specified functions

Evaluation method: CM report and specifications analysis
SW PA Concepts and Techniques

- SW process assurance:
  - Structure of the SW PA discipline
  - Configuration Management
  - Verification and validation
  - System and SW Lifecycles
  - Process Assessment and Improvement

- SW product quality assurance:
  - Quality Models and Metrics

- SW PA programme implementation
  - SW Safety
    - Organisation, Management and Planning
Safety definition (ECSS)

System state where an acceptable level of risk with respect to:
- fatality,
- injury or occupational illness,
- damage to launcher hardware or launch facilities,
- damage to an element of an interfacing manned flight system,
- the main functions of a flight system itself,
- pollution of the environment, atmosphere or outer space, and
- damage to public or private property
is not exceeded
Safety considerations

- SW cannot have adverse effects by itself since it is not a physical entity
- However it can cause systems to fail
- System failures can have adverse consequences of different severity
- Understanding how SW can lead to those failures is of paramount importance in space systems.
Safety and criticality: issues

- SW designs tend to be more and more complex every day
- It is not always obvious how relevant different SW components are to the performance of the more system critical functions
- Higher critical SW should be of higher quality to reduce risk of failure
- Availability or resources is limited

↓

- It is better to concentrate efforts on the most critical components

How do we do that?
Software classification: consequence severity

- The first step of classification is to define levels of severity of consequences of system malfunctions, for example:
  - **Catastrophic**: loss of life, permanent disability, loss of major elements
  - **Critical**: temporary disabling injury, use of emergency procedures
  - **Major**: loss of mission
  - **Minor**: degraded mission
  - **Negligible**: all other cases
- Severity levels may come from standard (above) but in some cases may need to be defined *ad hoc* ⇐ project requirements
- SW criticality classification is based *only* on the severity of consequences since SW faults are systematic ⇒ **different from HW!**
Criticality: system and SW

- Criticality of **SW** integrated in a system is always dependent on criticality of the **system** functions that it implements.
- The criticality of the functions at system level is analysed and the results of those analyses fed into similar analyses at SW level.
- There is feedback from SW to system level analyses including the analysis of HW and SW interaction.
- Criticality of functions is translated into criticality of software components: traceability again!!
- Concentrate resources (e.g. verification) on most critical components:
  - Design constraints, RAMS techniques, special methods
  - Special verification, testing, ISVV
Software safety analysis

- A given software function (and therefore all the components that implement it) is assigned the class for the worst possible consequence that a failure of that function may have on the system.
- How do we know what the worst possible consequence may be? ⇒ Safety Analyses

- There are many techniques with different purposes and views for safety analysis.
- Some common ones are:
  - Software Fault Tree Analysis
  - Software Failure Modes, Effects and Criticality Analysis
  - HW/SW Interaction Analysis
Software classification: classes

- Software classes are defined for each severity level:

<table>
<thead>
<tr>
<th>Consequence severity level</th>
<th>Software class</th>
<th>Safety (and dependability) impact</th>
<th>Dependability impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>A</td>
<td>Safety</td>
<td></td>
</tr>
<tr>
<td>Critical</td>
<td>B</td>
<td>(and dependability) impact</td>
<td></td>
</tr>
<tr>
<td>Major</td>
<td>C</td>
<td></td>
<td>Dependability impact</td>
</tr>
<tr>
<td>Minor</td>
<td>D</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Negligible</td>
<td>E</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Software Fault Tree Analysis

- Top-down inductive approach
- Starting from a set of top-level feared events, identify recursively their possible causes and combinations of causes at lower levels
- It is based on a system level technique called Fault Tree Analysis
- It consists of:
  - Identify top-level hazards
  - Diagnose recursively the causal events that lead to each top level hazard
  - Analyse the list of basic events sufficient to cause the top-level hazards (by analysing the tree of causal events)
SW Failure Modes, Effects and Criticality Analysis

- Deductive bottom-up approach
- Starting from the possible failure modes of low-level components and identifying their possible consequences at upper levels
- It is based on a system level technique called FMECA
- It consists of:
  - Identify the failure modes in each operating mode of the component for each component
  - Determine the effect of each failure mode on other components and the overall system
  - Determine the severity of each failure mode
HW/SW Interaction Analysis

- It consists of:
  - Examine systematically all HW/SW component interfaces in the system
  - Identify the failure modes of each of the interfacing HW components
  - Analyse, through a checklist, how the software reacts to the each of those failure modes.

- The technique may be reversed to analyse SW failure modes but this is less frequent.
SW PA Concepts and Techniques

- **SW process assurance:**
  - Structure of the SW PA discipline
  - Configuration Management
  - Verification and validation
  - System and SW Lifecycles
  - Process Assessment and Improvement

- **SW product quality assurance:**
  - Quality Models and Metrics

- **SW PA programme implementation**
  - SW Safety
  - Organisation, Management and Planning
SW PA organisation

- Explicitly identified SW PA organisation including interfaces to system level PA organisation:
  - Identified SW PA Manager
  - Responsibilities and authority
  - Reporting lines
- Allocated resources (including **ALL** PA activities, not only the SW PA Manager ones)
- Tools, for example:
  - NCR/SPR tools
  - Metrics collection and analysis
  - Process Assessment support
  - Audit support
SW PA planning

- SW PA activities must be explicitly planned ⇒ SW PA Plan either as a standalone document or as a section of System PA Plan

1. Applicable and reference documents
2. Software product assurance programme implementation
   2.1 Organization
   2.1 Relationships
   2.3 Responsibilities
   2.4 Resources
   2.5 Reporting
   2.6 Risk management
   2.7 Supplier selection and control
   2.8 Process assessment and improvement
SW PA planning

3. Software process assurance
   3.1 Lifecycle
   3.2 Project plans
   3.3 Dependability and safety
   3.4 Documentation and CM
   3.5 Reuse
   3.6 Individual processes and activities
   3.7 Procedures and standards
4. Software product quality assurance
5. Compliance to SW PA requirements

(Template compliant with ECSS standards)
Evolution of Concepts
Quality system evolution: the SW perspective

Artisan ➔ Team ➔ Defined methods ➔ Organization ➔ Quality system ➔ Best practices Standards ➔ Continuous process improvement
The evolution: SW “artisan”

- Individuals working independently even within a team are still common
- Often particularly able “artisans” will compensate resources or skills missing in the organisation
- “Artisans” carry with them essential skills an experience that is often impossible to replace
The evolution: SW team

- Most SW development projects require a team effort nowadays
- Teams are often formed by “artisans”
- Teams rely heavily on specific individuals, in particular the team leader
The evolution: defined methods

- Nowadays established methods and tools exist for all activities involved in SW development
- For example object orientated methods, modelling techniques, code generation tools, maintenance tools, etc., etc., etc.
- Proper use of those methods brings uniformity into SW development and allows communication across the team
- Build up of expertise in the use of methods ⇒ often it is more important expertise in a method than how “good” or “new” it is: e.g. many organisations used to stumble on their initial attempts at object orientation
The evolution: organisation

- Organisations are based on roles, not specific individuals
- This gives them a higher independence on staff turnover
- Roles allow separation of skills which facilitates training
- Roles and individuals can be mapped flexibly. This flexibility makes use of resources and skills more efficient
The evolution: QA system

- The QA system provides the framework that defines the roles, processes and methods used in the organisation
- In the case of SW development this is at least as important as in other engineering disciplines
- A generic QA system may not be enough for SW ⇒ a certain level of detailing and adaptation may be needed for SW
The evolution: best practices and standards

- National or international standards provide a common “vocabulary” for SW engineering (e.g. ISO 12207)
- They can be incorporated into the conception of the QA system allowing to map the organisation’s processes and methods directly to the standard allowing for automatic compliance
- Problem: “The nice thing about standards is that there are so many of them to choose from” ⇔ multiple customers/standards
- Standards are often a channel to promote best practices across industry
The evolution: best practices and standards (cont’d)

- In the case of some standards it is possible to obtain a certification
- The most common one is ISO 9001 under a number of SW or IT specific schemes
- TickIT is one example:
  - supported by UK and Swedish software industry
  - recognised by British government
  - provides assessment and certification services and also guidance
- ISO 9000-3: guidance on applying ISO 9001
The evolution: software process improvement

- Best practices of today may not be so tomorrow
- Methods, processes and their performance are always susceptible of improvement
- This improvement increases efficiency, maturity, reliability and competitiveness
- To improve a process or method it is necessary to be able to compare current and past performance ⇒ quantitative control (e.g. organisation metrics)
- Reliable improvement must be based on historical, objective data
The evolution: software process improvement (cont’d)

- Software Process Improvement must be institutionalised and an organisation-wide process in itself
- SPI must be supported by adequate organisation and resources
- SPI must be managed
- SPI must be promoted by higher management
- SPI has a cost and benefits
Major changes of focus

◆ From *individual* to *team*
◆ From *individual* to *role*
◆ From *product* to *process* but at the same time from *quality* assurance to *product* assurance
◆ However examples of all of the above steps of evolution co-exist nowadays in the market (dinosaurs and primates) ⇒ difficulty in differentiating them
Space SW Standards
Old ESA SW standards

- Previously ESA used the PSS series of standards
- Two documents in the series were the most relevant to software:
- ESA-PSS-05-0 was complemented by a set of guides, ESA-PSS-05-x
- They considered software only (no system)
New ECSS for SW

- New versions are available:
  - ECSS-E-40, Space Engineering – Software – Part 2B: Document requirements definitions (DRDs)
  - ECSS-Q-80B, Space Product Assurance - Software Product Assurance, 10 October 2003

- These new versions resolve a number of gaps between the previous versions A and adapt to evolution of SW engineering
Alignment with international standards

- The new versions of E-40 and Q-80 are based or aligned with a number of key international SW standards:
  - ISO/IEC 12207:1995 Information Technology - Software lifecycle processes
  - ISO 9126 Information Technology - Software product evaluation - quality characteristics and guidelines for their use
  - IEEE 612.10 - 1990 IEEE Standard glossary of software engineering terminology
  - IEEE 1062 - 1993 IEEE Standard recommended practices for software acquisition
The alignment of E-40 and Q-80 with international standards makes them:
- Internationally “readable” since they use recognised vocabulary and process models
- Simultaneous compliance with other standards easier
- Easier evolution in parallel with those standards
**SW ECSS: characteristics**

- The standards are based on the relation between SW and the system of which it forms part
- The standards are based on the concept of process as a set of activities that contribute to the development lifecycle: e.g. configuration management or design
- The standards are based on a customer-supplier model
- The model is recursive: the supplier may be the customer of next level suppliers
- The standards do not duplicate basic information which is general to the system, references are made instead to other ECSS standards: e.g. project management
Documentation

- Differently from ESA-PSS-05-0, documents are not dictated
- ECSS (SW) refers to eight collections of information:
  - Requirements baseline
  - Technical specification
  - Design definition file
  - Design justification file
  - Management file
  - Product assurance file
  - Maintenance file
  - Operational documentation
Documentation (cont’d)

- These collections contain all the work products of the project like plans, requirements document, design documents, technical documentation, reports, etc.
- ECSS-E-40 Part B provides DRD’s (expected contents) for some of the documents in the folders but not for all
SW processes

PRIMARY LIFE CYCLE PROCESSES
- Acquisition
- Supply
- Development
- Operation
- Maintenance

SUPPORTING LIFE CYCLE PROCESSES
- Documentation
- Configuration management
- Quality Assurance
  - Verification
  - Validation
  - Joint Review
  - Audit
- Problem Resolution

ORGANIZATIONAL LIFE CYCLE PROCESSES
- Management
- Improvement
- Infrastructure
- Training

IAASS Quality Assurance Course

September 2007
SW engineering

- Particular life-cycle models are not enforced but must include:
  - System engineering
  - Requirements engineering
  - Design engineering
  - Validation and acceptance
- The above engineering processes may overlap to some extent
- Major reviews mark the end of each of them:
  - System Requirements Review
  - Preliminary Design Review
  - Critical Design Review
  - Qualification Review
  - Acceptance Review
ECSS-E-40 requirements

- Requirements are established for the following processes:
  - System engineering processes related to SW
  - Software requirements engineering
  - Software design engineering
  - Software validation and acceptance
  - Software operations engineering
  - Software maintenance
  - Software verification and validation (supporting process)
ECSS-E-40 requirements (cont’d)

- Additional requirements exist for specific types of SW or development:
  - Space segment
  - Ground segment
  - SW reuse
  - Man-machine interfaces
  - Critical SW
ECSS-Q-80 requirements

- SW product assurance implementation:
  - Organisation, responsibilities, planning, management
  - Contractual aspects
  - Risk management and critical item control
  - Subcontractors, purchasing, tools, assessment and improvement

- Software process assurance:
  - Lifecycle
  - Software development processes

- Software product assurance:
  - Quality objectives and metrication
  - Product quality requirements
Clause 5.8.3.7

Verification of Test Specifications

The supplier shall demonstrate that the test requirements, test cases and test specifications cover all software requirements of the technical specification or the requirements baseline.

EXPECTED OUTPUT:

a. Traceability of the requirements baseline to the validations tests [DJF; QR, AR]

b. Traceability of the technical specification to the validations tests [DJF; QR, AR]
Clause 5.3.1.5 The supplier shall provide with his software assurance plan a compliance matrix documenting his compliance with the software product assurance requirements applicable for the project/contract.

EXPECTED OUTPUT:

Compliance matrix [PAF; SRR]
Quality Assurance in Test Center

Appendix I

by

Massimo Panicucci
Related Definitions

- **Test centre**
  A complete entity including the organization which provides, develops and operates test facilities for space project and applications including accompanied services

- **Test facility**
  Technical plant (test equipment and associated buildings) to provide specific simulated conditions for testing equipment for space projects and applications
Quality assurance in test center

- Test campaign general considerations
- Typical process
- Applicable standards
- Specific QA system requirements
- Main documents/records
- Customer’s QA responsibilities
- Safety
- European Coordinated Test Centres
Test campaign general considerations

- The article may remain in the test centre from few days to several months (case of complete spacecraft testing)

- Possible threats:
  - Contamination in clean rooms or during thermal test (molecular, particulate)
  - Shocks/high acceleration (lifting operations, anomalies during vibration, acoustic tests, etc)
  - Emergencies (fire/smoke, water damages)
Test campaign general considerations (cont’d)

♦ Performance of hazardous operations:
  – use of lasers,
  – pyrotechnics,
  – toxic fluids,
  – cryogenics
  – etc.

♦ Quality of test data/results (incorrect results = wrong predictions)

♦ Need for good planning and preparation: test delays may well affect the overall project schedule
Typical test process

- Long term planning
- Medium & short term planning
- Facility adaptation
- Facility preparation
- Test Item Preparation
- Test Item arrives
- Test campaign
- Test planning
- Test execution
- Post test activities
- FRR, TRR, ITR, PTR, LLR
Applicable QA standards

- Existing **ESA PSS-01-203** *Product Assurance requirements for Test Houses* replaced by an ECSS standard

- **ECSS-Q-20-07** *Quality assurance for Test Center* has been issued in the course of 2002. This standard refers to the requirements of ISO 9001 (2000) standard that are relevant to the mission of a typical space test centre and provides additional requirements specific of such application
Specific QA system requirements

Specific requirements have to be considered when establishing a Test Centre QA system, as:

- **Competence, awareness and training of personnel:**
  
  » A skills and competence’s matrix, or an equivalent method, to be used to identify the required competence profiles and the training requirements.
  
  » Personnel performing selected handling operations, such as lift and hoist operators, shall be trained and certified by an authorized body.
Specific QA system requirements (cont’d)

- **Cleanliness control:**
  
  » For a facility where spacecraft equipment is handled, the minimum cleanliness levels of the clean rooms for airborne particles is 100 000 (FED STD 209D) or M6.5 (FED STD 209E).

  » when deposited contamination levels need to be considered, the minimum levels are:
    
    ♦ particles: 225 parts per million /24h;
    
    ♦ molecular cleanliness: $10^{-7}$ g/cm²/168 h
Specific QA system requirements (cont’d)

– Other environmental controls:

In addition to the basic cleanliness control other environmental controls should be considered such as:

- inorganic contaminants control,
- temperature (22 +/- 3) °C; humidity (55 +/- 10) %
- pressure,
- light level,
- electromagnetic radiation,
- magnetic cleanliness,
- vibration,
- ionising radiation, acoustic environment.
Specific QA system requirements (cont’d)

- **Documented Procedures:**
  The test centre shall establish and maintain documented procedures to control/verify:
  - design of new test facilities;
  - modification of test facilities
  - software for operating test facilities;
  - operation of the test facilities;
  - test planning, test preparation, test performance and test related hardware and buildings
  - safe handling, storage, transportation, preservation and delivery
  - test specimen and associated test equipment (environmental conditions, safety/security etc.)
Specific QA system requirements (cont’d)

- **Configuration control of the test facilities:**

  » define parts of the test facilities under configuration control (as a minimum all systems used in the test process). Describe them by drawings and other documents as appropriate.

  » establish and maintain procedures for configuration identification, and for configuration change control.

  » modifications of the configuration by means of formal:
    - proposal for modification;
    - technical review board for evaluation of proposal;
    - system for update and review of drawings and documents
Specific QA system requirements (cont’d)

- **Control of test specimen:**
  
  » The test specimen shall be defined in its configuration on the test facility;
  
  » all interfaces between the test facility and test specimen shall be determined.
  
  » In case of a transfer of responsibility (for the test specimen) from the customer to the test centre, this transfer shall be contractually defined.
Specific QA system requirements (cont’d)

- **Maintenance activities control:**

  » Develop a maintenance plan, including type and extent of activities, resources needed and schedule for:
  
  - buildings,
  - test facilities,
  - test equipment
  - related software (upgrading etc.).
Specific QA system requirements (cont’d)

- **Monitoring and measurement of the test activities:**

  » A test centre representative shall participate to:
    - test readiness review (TRR);
    - post-test review (PTR).
  
  » For each test review the test centre shall define:
    - objectives;
    - input data;
    - outputs;
    - test centre’s tasks and responsibilities;
    - customer's tasks and responsibilities
Main TC controlled documents/records

- general facility operations and safety procedures
- test specific operations and safety procedures (in particular: Integrated Test Procedure)
- test reviews reports
- facility data reports
- test schedules
- site safety instructions
- accident/incident reporting
- Non-conformance reporting
- calibration of test equipment
- availability and maintenance of facilities
- facility certification and re-certification
Facility data report

- Sometimes called “test report” it contains:
  - all data required to document that the test has been performed according to applicable procedures.
  - all data required for correct test analysis and identification of the facility test configuration and the associated instrumentation, to permit post test evaluation and reproducible re-test, if necessary.
  - facility related NCRs occurred during the test, with the description of the dispositions taken.
The typical content of the test report is as follows:

- name and location of the test centre;
- customer’s name and address
- description and identification of the test specimen
- date of receipt of the test specimen
- date(s) of test(s) execution
- test specification or description of the method or procedure
- description of the sampling procedure, where relevant
- any deviations, additions to or exclusions from test specification
- any other information relevant to the specific test
Facility data report: typical content (cont’d)

- references to any non-conformances that occurred before and during the test campaign, including the dispositions taken
- measurements, examinations and derived results, supported by tables, graphs, sketches and photographs as appropriate
- a statement on measurement uncertainty, where relevant
- agreed confidentiality level
Customer’s QA responsibilities

- Customer’s responsibilities may be classified in the as:
  - Management and Organisation
  - PA and Safety Documentation
  - Operations
### Customer’s QA responsibilities (cont’d)

<table>
<thead>
<tr>
<th>Management and organisation</th>
<th>Test preparation</th>
<th>Test execution</th>
<th>Post-test activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify single point contact for PA&amp;S matters.</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Ensure attendance (and chairmanship) to formal Test Reviews.</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Ensure attendance to MRBs and failure investigation board.</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Attend safety briefing and training sessions, as required.</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
### Customer’s QA responsibilities (cont’d)

<table>
<thead>
<tr>
<th>Main PA&amp;S documentation</th>
<th>Test prep.</th>
<th>Test exec.</th>
<th>Post-test activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description of test item, support equipment (GSE) and required test fixtures.</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Definition of test objectives (mandatory and desirable).</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information on hazardous items.</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Statement of Compliance of test item/GSE to facility cleanliness requirements, including:</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>- list of external surface materials;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- samples of above materials;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- certificates of above material for contamination characteristics.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Customer’s QA responsibilities (cont’d)

<table>
<thead>
<tr>
<th>Main PA&amp;S documentation</th>
<th>Test prep.</th>
<th>Test exec.</th>
<th>Post-test activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Declared Material Lists completed as per PSS-01-700, if a thermal vacuum facility is used.</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificates of compliance of the MGSE (including lifting devices) to the relevant safety regulations.</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preparation of Test Item Readiness Review Report.</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Customer’s QA responsibilities (cont.d)

<table>
<thead>
<tr>
<th>Operations</th>
<th>Test prep.</th>
<th>Test exec.</th>
<th>Post-test activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Observe applicable safety, security, and access control rules.</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Specify for each staff involved in potentially hazardous operations the identity, the qualification, the work performed, the certification and the period of validity of the certification.</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Maintain and control the knowledge, skill, and physical ability of his personnel involved in hazardous activities. Monitor and renew of certifications.</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Observe airlock and clean rooms cleanliness and contamination control requirements.</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Customer’s QA responsibilities (cont.)

- The customer shall fill-in with a questionnaire (see details in the ECSS-Q-20-07), the aim of which is to identify and describe the possible hazardous operations during all testing activities.

- On test center request, the customer should provide any hardware certificate and training records which are required by law, e.g. pressure vessels, pyrotechnics, lifting devices.

- The Declared Material List (DML) shall consider the test item in the “test configuration”, i.e., including the test adapter and all connections (e.g. mechanical, electrical).
The test centre shall define and implement a safety programme to assure safety for all personnel as well as customer, the test specimen and the test facilities, including:

- identification of safety-critical functions, items and operations;
- hazard elimination, reduction, or control;
- safety risk analysis
- safety risk prevention measures
- acceptance of residual risk;
Safety (cont.)

The safety programme will also include:

» definition of safety provisions, equipment and resources
» training of personnel;
» preparation of associated safety and emergency procedures and instructions;
» systematic verification of safety requirements implementation
» planning of regular safety reviews
Safety (cont.)

- Safety preventive activities include:
  - systematic identification of “critical operations” expected during all the test phases, including maintenance.
  - performance of critical operations under surveillance of the QA staff or designated staff.
  - maintenance and inspection instructions, with respect to the safety critical items
  - implementation of customer’s specific safety requirements;
  - hazardous activities related to a specific test campaign. The test centre should gather information on the use of hazardous items and operations, requesting the customer to fill-in a questionnaire.
Safety: prevention (cont.)

- training and briefing rules to ensure that all employees and customer personnel are informed about the safety aspects of their working environment, the possible risks and the emergency procedures;
- a summary and description of hazardous activities of the facility;
- first aid management to ensure that sufficient test centre staff are adequately trained for first aid.
Safety documentation
The four European coordinated test facilities are:

- **ESTEC**:
  - Keplerlaan 1 2000AG Noordwijk (the Netherlands)
  - Contact person (ETS: Mr. K. Mueller)

- **IABG**:
  - Einsteinstrasse 20 85521 Ottobrunn (Germany)
  - Contact person: Mr. G. Vodermeier
European Coordinated Test Facilities (cont.)

- Intespace
  » Complexe Scientifique de Rangueil 18, Av. Edouard-Belin 31029 Toulouse CEDEX (France)
  » Contact person: Mr. J-C. Pasquet

- Centre Spatial de Liege
  » Parc Industriel du Sart Tilman Avenue du Pré-Aily B-4031 Angleur-Liege (Belgium)
  » Contact person: Mr. C. Jamar
Reliability

Appendix II: Basic Concepts
Reliability definitions

- **Reliability:**
  The probability that an item can perform its intended functions for a specific interval under stated conditions

- **Fault tolerance:**
  The designed in characteristics that maintains prescribed functions or services to users despite the existence of fault(s). Implemented by design redundancy and a fault detection and response capability

- **Fault avoidance:**
  An approach to increase system reliability by reducing the possibility of a failure by increasing the reliability of individual items (design margins, worst case design, screening, use of hi-rel components, derating, workmanship, formal inspections, acceptance testing, etc.)
Reliability definitions (cont’d)

- **Design redundancy:**
  More than one item to accomplish a function where more than one must fail before there is overall loss of the function.

  - **Hot redundancy** (active). Redundant elements fully energised. It is not necessary to switch in the redundant element or switch out the failed unit.
  - **Cold redundancy** (standby). Redundant elements are non-operative until they are switched into operation upon failure of primary element.
Reliability definitions (cont’d)

- **Functional redundancy:**
  The use of more than one means of accomplishing a function where more than one must fail before there is overall loss of the function

- **Failure mode:**
  How the failure is revealed. The abnormality of performance [of the item] which causes the item to be classified as failed

- **Failure propagation:**
  Failure mode that can propagate at interfaces (e.g., from spacecraft to payload or GSE and vice-versa)
Reliability definitions (cont’d)

- **Failure cause:**
  The IMMEDIATE REASON why an item failed

- **Failure mechanism:**
  The process or chain of events resulting in a particular failure mode

- **Single Failure Point**
  A single item of hardware, the failure of which would lead directly to loss of life, vehicle or mission
Designing reliable space systems

- Three basic approaches (generally in combination) are used to achieve a reliable space system:
  
  ✷ **FAULT AVOIDANCE**
  
  ✷ **FAULT TOLERANCE**
  
  ✷ **FUNCTIONAL REDUNDANCY**
Bathtub curve

I
INFANT MORTALITY

II
CONSTANT FAILURE RATE REGION

III
WEAROUT

failure rate, \( \lambda/10^6 \)

time, \( t \)

\[ R = e^{-\lambda t} \]

\[ MTBF = \frac{1}{\lambda} \]
Exponential distribution

- The failure rate of a complex system is usually considered to be constant (after burn-in and before wear-out).

- Reliability at MTBF:

  If MTBF = lifetime (operating time),

  \[ R = e^{-t/MTBF} = e^{-1} = 0.368 \approx 36.8\% \]

- Estimate of MTBF from test data:

  MTBF = (total test hours)/(total observed failures)
Reliability Block Diagrams SHOW THE SUCCESS LOGIC of the system by means of block diagrams.

Reliability Block Diagrams are used to make the overall system assessment of reliability.
Reliability calculation

- **Series:**

  \[ R_S = R_1 \cdot R_2 \cdot R_3 \ldots R_n \]

- **Parallel:**

  \[ R_P = 1 - (Q_1 \cdot Q_2 \cdot Q_3 \ldots Q_n) \quad \text{where} \quad Q_n = 1 - R_n \]

- **Complete system:**
  - Reduce system to simple series or parallel
  - Use failure rates (e.g., MIL-HDBK-217) and operating times
  - Calculate reliability of system
Reliability quantitative requirements/predictions

- In ESA projects, usually, quantitative reliability requirements are placed in the System Requirement Document as TARGET. In other words its validity is intended only for the purpose of DESIGN OPTIMISATION.

- For on-orbit maintainable systems (i.e. space stations) reliability predictions are used to support maintainability assessments and logistics planning.

- MIL-HDBK-217 reliability prediction methods widely used for electronic equipment: parts stress analysis, parts count analysis.
Effect of EEE components quality level

- The ESA standard payload computer (SPLC) for ISS is built with EEE components SCC level C or equivalent. The figure shows the predicted reliability by using the MIL-HDBK-217 parts count method, and the improvement that would be achieved by using higher reliability components such as SCC level B.
Reliability qualitative analysis

- **FMEA**
The Failure Mode and Effect Analysis (FMEA) is a structured qualitative analysis of a system, subsystem or equipment aimed to identify potential failure modes, their causes, and related effects on system operation. It includes a criticality classification based on severity of (worst) consequence.

- **FMECA**
An FMECA is basically an FMEA extended to include a quantitative Criticality Analysis (CA) for each failure mode. [Usually the analysis requested by ESA project is an FMEA although (erroneously) usually called FMECA]
Reliability consequence severity categories

The consequence of a failure on reliability is classified as:

- **MAJOR**
  - loss of mission

- **SIGNIFICANT**
  - degradation of mission objectives or performances

- **NEGLIGIBLE**
  - [all other cases]
## FMEA example

<table>
<thead>
<tr>
<th>Item</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>stop valve</td>
<td>controls gas flow; full-on/full-off (controlled by the controller)</td>
</tr>
<tr>
<td>controller</td>
<td>opens and closes gas valve (responds to temperature sensor)</td>
</tr>
<tr>
<td>press./temp.</td>
<td>senses water pressure/temperature</td>
</tr>
<tr>
<td>press./temp.</td>
<td>senses water pressure/temperature</td>
</tr>
<tr>
<td>sensor</td>
<td>prevents reverse flow if over-pressure</td>
</tr>
<tr>
<td>relief valve</td>
<td>opens when pressure $&gt; 100$ psig</td>
</tr>
<tr>
<td>pilot light</td>
<td>lights burner (always on)</td>
</tr>
<tr>
<td>burner</td>
<td>heats water (operated by gas valve)</td>
</tr>
<tr>
<td>tank</td>
<td>holds water (safe up to 100 psig)</td>
</tr>
<tr>
<td>faucet</td>
<td>releases water when needed</td>
</tr>
</tbody>
</table>
## FMEA example (cont’d)

<table>
<thead>
<tr>
<th>Item</th>
<th>Failure Mode</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stop Valve</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1) Fails closed</td>
<td>Burner off</td>
<td>No hot water</td>
</tr>
<tr>
<td>2) Fails open</td>
<td>Burner won’t shut off</td>
<td>Overheats, release valve releases pressure, may be scalded</td>
</tr>
<tr>
<td>3) Does not open fully</td>
<td>Burner not fully on</td>
<td>Water heats slowly or doesn’t reach desired temperature</td>
</tr>
<tr>
<td>4) Does not respond to controller-stays open</td>
<td>(same as 2)</td>
<td></td>
</tr>
<tr>
<td>5) Does not respond to controller-stays closed</td>
<td>(same as 1)</td>
<td></td>
</tr>
<tr>
<td>6) leaks through valve</td>
<td>Burner won’t shut off, burns at low level</td>
<td>Water overheats (possibly)</td>
</tr>
<tr>
<td>7) Leaks around valve</td>
<td>Gas leaks into room</td>
<td>Possible fire or gas asphyxiation</td>
</tr>
</tbody>
</table>
FMEA basic principles

- Iterated during the project life-cycle
- **Internal use.** Inside the design team to improve the design and to identify requirements for manufacturing/inspection and testing (focus on controlling the *causes*, focus on risk reduction)
- **External use.** To demonstrate to customer or regulatory body compliance with system requirements (e.g., failure tolerance, failure detection-isolation-and recovery FDIR) and identify deviations
- Can be used to support trouble-shooting during operations
- Can be used for products design as well as for processes
- Can be performed at any level. (*Failure effects* identified at one indenture level are interpreted as *failure modes* at the next higher level)
- **Not good** for evaluating the effect of combined multiple failures
# FMEA worksheet example

<table>
<thead>
<tr>
<th>ITEM</th>
<th>FUNCTION</th>
<th>FAILURE MODE</th>
<th>SUBSYSTEM OR OTHER SUBSYSTEMS</th>
<th>MISSION</th>
<th>FAILURE DETECTION</th>
<th>CORRECTIVE ACTION</th>
<th>Remarks/IFDWGS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. IPDU 11-1, 1, 2</td>
<td>+28 volt A internal conv. power from RU 2A</td>
<td>Open</td>
<td>No effect due to redundant power lines</td>
<td>No effect</td>
<td>Not detectable</td>
<td>Not required</td>
<td>III GC1371-040</td>
</tr>
<tr>
<td>2. IPDU 11-1, 1, 2</td>
<td>+28 volt A internal conv. power from RU 2A</td>
<td>Short to ground</td>
<td>Loss of internal conv. power, fuse blown</td>
<td>Loss of IPDU A analog and digital TLM, loss of power switching command capability on A side</td>
<td>Telemetry</td>
<td>Use FIRAS B side to retain cmd capability &amp; telemetry</td>
<td>II Same</td>
</tr>
<tr>
<td>3. IPDU 11, 3, 4</td>
<td>MTM&amp;C power from RU 2A</td>
<td>Open</td>
<td>No effect due to redundant power lines</td>
<td>No effect</td>
<td>Not detectable</td>
<td>Not required</td>
<td>III Same</td>
</tr>
<tr>
<td>4. IPDU 11, 3, 4</td>
<td>MTM&amp;C power from RU 2A</td>
<td>Short to ground</td>
<td>Power loss to MTM latch A, cal latch A, cal drive A, fuse blown</td>
<td>Degraded performance on A side due to cal loss</td>
<td>Telemetry</td>
<td>Continue operation on both sides in degraded mode</td>
<td>II Same</td>
</tr>
<tr>
<td>5. IPDU 11, 5, 5, 7</td>
<td>FIRAS +28V power from RU 2A</td>
<td>Open</td>
<td>No effect due to redundant power lines</td>
<td>No effect</td>
<td>Not detectable</td>
<td>Not required</td>
<td>III Same</td>
</tr>
</tbody>
</table>

IAASS Quality Assurance Course  
September 2007
The (reliability) Critical Item List (CIL) describes the design, test, inspection, or operational features that minimise the probability of failure for items not meeting project requirements for:

- **FAILURE TOLERANCE**
  (Including the case of credible common cause)

- **REDUNDANCY LOSS DETECTABILITY**

CIL approval by the customer is equivalent to granting a waiver on the basis of a *rationale for retention*
## Critical Item List (CIL) - rationale for retention

**Rationale for Retention Elements**

<table>
<thead>
<tr>
<th>Element</th>
<th>Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Design</strong></td>
<td>Identify design features that minimise the probability of occurrence of the failure causes</td>
</tr>
<tr>
<td><strong>Test</strong></td>
<td>Identify specific tests to detect the failure causes during Acceptance and Qualification tests</td>
</tr>
<tr>
<td><strong>Inspection</strong></td>
<td>Identify specific inspections points to ensure that failure causes are not inadvertently manufactured into the hardware</td>
</tr>
<tr>
<td><strong>Operational Use</strong></td>
<td>Any operational procedure to either prevent the occurrence of the failure mode or mitigate its effects</td>
</tr>
<tr>
<td><strong>Failure History</strong></td>
<td>Information related to test failures, flight failures, anomalies or problems to demonstrate a complete understanding of the failure mode and its effects</td>
</tr>
</tbody>
</table>
Fault-tree analysis

It is a graphical and logical representation which is developed by deductive logic from a top undesired event to all sub-events which must occur to cause it.

The Fault-Tree Analysis can be used for qualitative and quantitative evaluations:
- the qualitative evaluation can be used to verify compliance with failure tolerance requirements,
- the quantitative evaluation is based on insertion of failure rates into the fault tree structure and mathematical combination to yield probabilities.

The FTA can be performed at any time in the life of a system. It can be a very effective tool for accident or mishap investigation.
In this fault tree example, Event C represents a SPF.
Good luck!