98- o -2-09V

SAFETY AND PRODUCT ASSURANCE FOR JEM

Norikazu Hara
21st International Symposium on Space Technology and Science
Japan Manned Space Systems Corporation
1-29-6, Hamamatsu-cho, Minato-ku, Tokyo 105, JAPAN
(E-mail: nhara@jamss.co.jp)

Abstract

Since Japan decided to participate in the Space Station Freedom Program with Japanese Experiment Module (JEM) program, National Space Development Agency of Japan (NASDA) who is responsible for the JEM development and operations has conducted the Safety and Product Assurance (S&PA) activities for all her manned space programs. This paper describes purpose, organization, and background of the JEM S&PA activities first. Then JEM S&PA requirements are summarized somewhat in detail for the purpose of introducing contents of JEM S&PA activities. It is stressed that some fundamental technical terms used in the S&PA field should be redefined systematically and uniquely.

1. Introduction

The S&PA activities are a set of activities to be done for achieving a mission successfully. To achieve a mission without a failure requires that mission items be developed and operated as intended by the mission planners. For the items to be developed as intended, the items should be designed and manufactured properly. Reliability assurance activities ensures that the items are designed properly; Quality Assurance (QA) activities ensures that the items are manufactured properly. In addition, the safety assurance activities are stressed for manned space programs. For the development of computer software, Software Product Assurance (SPA) is performed to account for the differences from hardware. These four assurance activities are not mutually exclusive but intertwined and should be conducted in harmony. In other words, the largest merit of this new concept, S&PA, is to eliminate the overlapped requirements and setting the common viewpoint by cross-checking the management activities which had been conducted separately.

2. Purpose of JEM Safety and Product Assurance

The purpose of S&PA activities in the JEM Program is to safely achieve the specified objectives of the program. For this reason, all activities under the JEM program can be considered as S&PA activities. Accordingly, all persons involved in the JEM program must perform their responsibilities with understanding that they perform S&PA roles. However, we could divide various work necessary for a program into two group of categories, indispensable work and assurance work. Indispensable work contains design, strength analysis, drawing, manufacture, test, operation, etc.

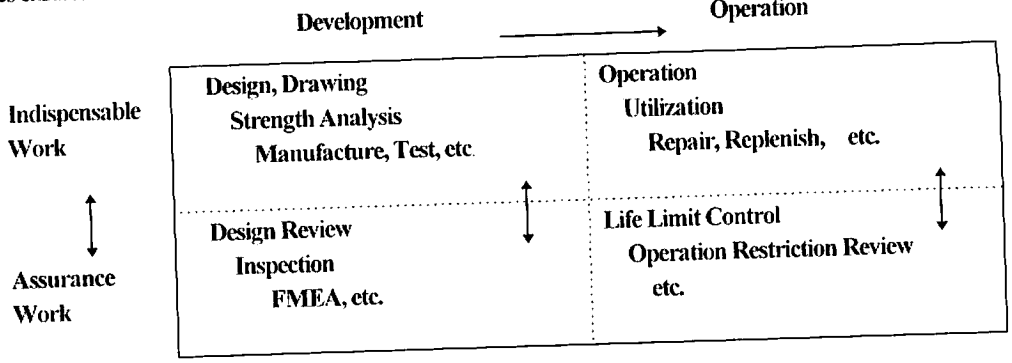

Fig.1 Concept of the Assurance Work

Assurance work may contain reviews, inspection, failure analyses, etc. and which can be defined as the work which are needed for achieving the mission successfully. The latter group of work would be unnecessary if the mission success were disregarded. The latter work is called S&PA activities in narrow sense of the word, there is not clear boundary between two categories, though. Fig. 1 shows the concept of the assurance work.

3. Organization for JEM S&PA

The management organization for S&PA activities should be independent from the development or operation organization because S&PA covers too wide range of activities for a development or operation organization to conduct without omission by their own management. If they were busy or with insufficient fund, some of activities could apt to be ignored.

In NASDA, the Space Station Safety and Product Assurance office which is responsible for JEM S&PA management has been placed under the Reliability Assurance Department which is independent from JEM development departments. Generally speaking, quality assurance department in JEM contractors are responsible for the management of S&PA. Fig.2 shows organization for JEM S&PA in NASDA.

4. Background of JEM S&PA

Many NASA documents have been playing a role of textbooks for the space development activities of NASDA. NASDA has interpreted and implemented NASA documents as faithfully as possible. For the International Space Station (ISS) program, all International Partners (IPs) should proceed with their programs using same criteria and having the same sense of values as NASA, while NASA incorporates opinions of the IPs to establish overall safety plans and requirements.

Based on the international agreements such as Intergovernmental Agreement (IGA) and Memorandum Of Understanding (MOU), NASDA has established various domestic documents which meet or exceed the SSP 30000 Program Definition and Requirements Document (PDRD) established by NASA. In 1989 NASDA firstly issued the NASDA-ESPC-1088 "JEM Safety and Product Assurance Requirements," which corresponds to the PDRD Section 9, Product Assurance Requirements. Then NASDA prepared CR-99302 "JEM S&PA Plan" for the overall JEM S&PA activities.

NASDA-ESPC-1088 has been used for the JEM contractors who develop JEM hardware and software. The NASDA-ESPC-1088 has been updated through the meet or exceed coordination with NASA even during the transitional

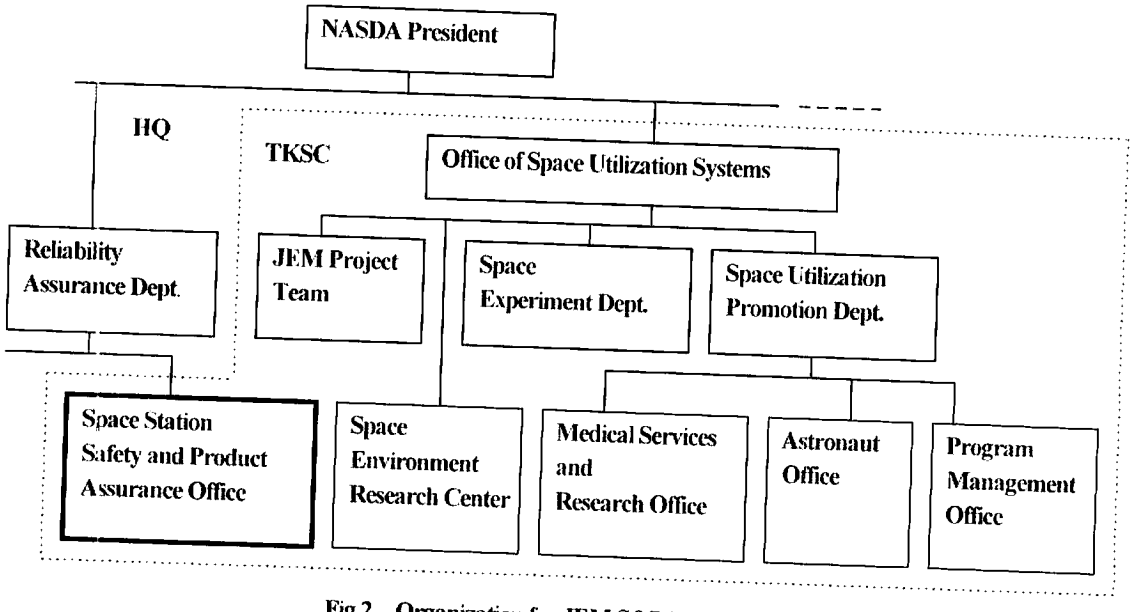

Fig.2 Organization for JEM S&PA in NASDA

phase from the Freedom Program to the ISS Program. Its current version is D.

The highest document but under MOU between NASA and NASDA became SSP 50030 for ISS era. As NASA phased out all of the PDRD, NASA prepared the draft of SSP 50145 as the bilateral document in place of PDRD Section 9 between NASA and NASDA. NASDA gave many comments and opinions to NASA so that NASDA-ESPC-1088 would be compatible with the new SSP 50145. Finally both NASA and NASDA mutually agreed that the execution of this document was necessary for the effective and safe integration of the JEM into the International Space Station. Fig.3 shows documents tree for JEM S&PA.

5. Contents of JEM S&PA

NASDA-ESPC-1088 was derived from NASDA-SPC-1177A "Reliability Program Provision" and NASDA-SPC-558 "Quality Assurance Program Provision" which had been applied to NASDA's unmanned programs being supplemented with the SSP 30000 Section 9. NASDA-SPC-1177A and NASDA-SPC-558 are now superseded by NASDA-STD-17 and NASDA-STD-16 respectively. NASDA-ESPC-1088 consists of safety assurance requirements, reliability and maintainability assurance requirements, quality assurance requirements, and software products assurance requirements. It can be said that the following three requirements are common for all above four assurance.

- To clarify the organization
- To plan the activities
- To conduct with documents

These requirements might be matters of course needless to specify in a document. Other many requirements specified in the NASDA-ESPC-1088 may be also matters of course by seeing them from a deferent angle.

NASDA has issued another S&PA requirements document, NASDA-ESPC-1681, which is the simplified version from NASDA-ESPC-1088 for the development of JEM payload, such as equipment for experiment installed into JEM. The requirements of Software Product Assurance (SPA) is not specified in the NASDA-ESPC-1681.

What should be done for the successful JEM operation has not been specified in the NASDA-ESPC-1088 in detail. These are currently studied and will be included in the 1088 or another document will be settled for the JEM Operational Safety and Product Assurance after discussion with NASA.

The introduction of contents of NASDA-ESPC-1088 means naturally summary of JEM S&PA activities being conducted so far. The following shows rather detail excerpt of the document including some comments by the author.

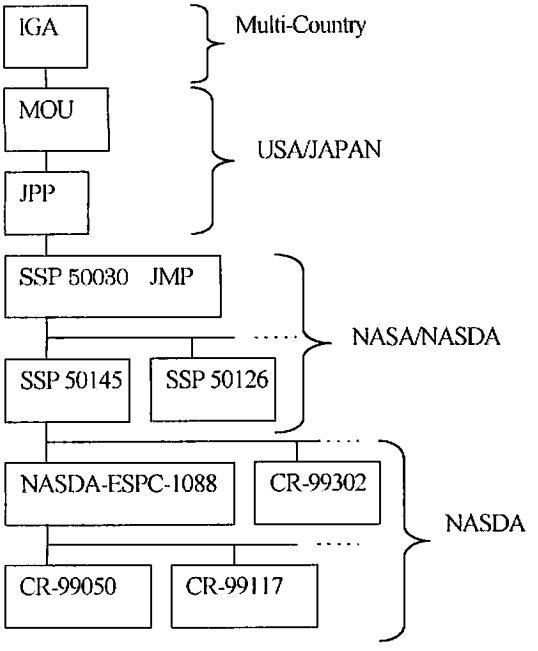

Fig.3 Document Tree Related JEM S&PA

5.1 S&PA General Requirements

General requirements consists of the description of the principle for S&PA activities and common requirements for S&PA. S&PA management shall be implemented for conducting JEM Program.

1) Principles for Safety and Product Assurance Activities

This clause includes Philosophy of safety and product assurance activities, and Basis of activities. S&PA activities shall be conducted according to the philosophy described in this clause.

2) Common Requirements for Safety and Product Assurance.

The followings are specified here as the common requirements for S&PA.

- S&PA activities, management details and schedule shall be clarified.
- S&PA program plans shall be prepared and maintained.

- S&PA management documents such as verification plan which are listed in the appendix of the NASDA-ESPC-1088 shall be established.
- S&PA management organization shall be functionally independent of the organizations for design, development, operation, utilization, etc.
- S&PA personnel shall participate in milestone reviews.
- S&PA management activities for suppliers are also necessary.
- S&PA management documents and data shall be prepared for rapid retrieval.
- Reporting on S&PA activities is necessary.
- Internal audit shall be conducted to ensure that S&PA activities meet the contract requirements.
- S&PA manager shall be sufficient knowledgeable.
- Designated NASDA representatives shall be accepted.
- Verification plans shall be evaluated from the S&PA viewpoint.
- Control procedures shall be established for NASDA and International Partner Furnished Equipment (NFE/IGFE).
- S&PA requirements shall be applicable for software also. In addition, requirements specific to software which is described as the Software Product Assurance shall be satisfied.
- Deviation and waiver shall be applied in accordance to NASDA-STD-1.

5.2 Safety Assurance

For safety assurance, the following four items are specified.

1) Safety Management

The key points of requirements for safety management are to identify hazards and to evaluate the risk. Therefore, it is necessary to establish the effective method to do them. That is, the organization for safety management shall be clear and the safety program plan shall be settled, and the safety reviews shall be conducted as planned. In addition, Mishap reporting and investigation, Safety training and certification, and Waivers and deviations, are specified.

2) System Safety

To minimize risk through the life cycle of JEM, system safety in accordance with NHB 1700.1(V1-B) shall be implemented, where the life cycle means from design phase to operation phase. In other words,

a) firstly, the hazards shall be identified

b) secondly proper design and performance requirements shall be developed, documented and implemented

c) thirdly an overall risk assessment shall be performed by conducting safety analysis.

To identify hazards Fault Tree Analysis (FTA) , Failure Mode Effect Analysis (FMEA), and other analysis shall be performed lest a hazard should be overlooked. The Critical Item List (CIL) generated from FMEA should be used for the cross check.

To conduct proper design safety technical requirements are available. The design requirements for control of the hazard identified are safety technical requirements. In the NASDA-ESPC-1088 the system safety technical requirements are specified by referring the NASDA-ESPC-840, KHB 1700.7B and SSP 50005.

At present NASA has issued the following requirements documents used for the safety reviews by the NASA panels, Payload Safety Review Panel (PSRP), Safety Review Panel (SRP), and Ground Safety Review Panel (GSRP).

a) PSRP's criteria document for the Payload of the Space Shuttle: NSTS 1700.7B

b) SRP's criteria documents for the Space Station Elements: NSTS 1700.7B Addendum, SSP 50021, and SSP 50038B

c) GSRP's criteria document for the launch site safety operation: KHB 1700.7B

For the JEM development Japan has followed the NASA safety policy by making JEM design satisfy the safety technical requirement documents above mentioned. However, to review the safety of JEM by Japanese government level a review policy document for JEM safety was issued by the Subcommittee for the Safety Assessment of the Space Activities Commission (SAC) in April 1996. Fortunately this document is compatible with NASA safety requirement documents. In the world of civil aviation the Federal Aviation Regulation (FAR) issued by the Federal Aviation Administration (FAA) is de fact standard of the safety technical requirements for the development and operation of the civil aircraft. In the space world it is to be desired that only and one document corresponding to the FAR is established as the world wide standard.

Safety analysis means the study for degree of severity of the mishap in the hazard and probability of occurrence of the mishap. The technical safety requirements are design requirements for control hazard identified. Safety analysis shall be performed in accordance with SSP 30309.

Hazardous conditions, causes, effects, controls, and verification methods shall be identified and documented on hazard report per CRS-94013. Safety analysis results which show the degree of the risk due to the cause identified are written in the document called Hazard Report. This is considered the primary part of the Safety Assessment Report (SAR).

In addition, Hazard elimination and control, Hazard report closure criteria, Human engineering, Specifications and procedure review, Ground Support Equipment safety, Review of changes, Review of flight and ground hardware failures, Evaluation of ground and flight test results, and Evaluation of mission operational activity are specified.

3) Industrial Safety

The contractor shall observe industrial regulations for ground operations.

4) Test Operations Safety

To evaluate the safety margins on testing, to review the testing facilities, etc. are specified.

5.3 Reliability and Maintainability Assurance

Reliability and Maintainability (R&M) assurance requirements are statement of work which are mainly imposed on the design phase. These were mainly derived from NASDA-SPC-1177A In this section the following four items are specified.

1) General Requirement

R&M activities shall be regarded as indispensable elements.

- R&M tasks shall be defined.
- The effective implementation of R&M requirements shall be assured.
- R&M characteristics shall be evaluate through analysis, test, etc.
- Trade-off studies shall be conducted for the optimum availability.

2) R&M Assurance Management

- R&M program plan shall be prepared and maintained.
- R&M assurance shall be required also for the supplier who manufacture the critical items.
- For the R&M verification requirements shall be settled and implemented.
- Qualification test shall be conducted for the verification of the design and its evaluation on R&M shall be conducted.

3) R&M Engineering

Reliability engineering and Maintainability engineering are close but different field of engineering by nature.

a) Reliability Engineering requirements

- Reliability design criteria shall be established.
- Design specification shall be prepared for the each contract end items.
- Reliability failure tolerance assurance shall be established and implemented.
- Reliability analyses and trend studies shall be conducted.
- The block diagram shall be prepared for the reliability prediction.
- Parts stress analysis shall be implemented.
- Worst case analysis (WCA) shall be conducted.
- Trend analysis shall be conducted.
- Special analyses such as sneak analysis shall be identified and implemented in the R&M Program Plan.
- A system for preparing, maintaining and controlling Failure Modes and Effects Analyses (FMEA) shall be established according to SSP 30234 and CR-99144.
- Critical Item List (CIL) items shall be controlled in accordance with CRS-94020.
- Reliability and maintainability data shall be prepared and maintained in accordance with CR-99146.
- Reports on the identification and status of Limited Life Items (LLIs) shall be prepared, submitted and maintained in accordance with CR-99145 and CRS-94020.
- A measure shall be prepared for elimination of human induced failures including those occurring in design process.
- Design reviews shall be conducted in the contractors. The contractor shall be participated in the suppliers design reviews. Design change control shall be implemented.
- The contractor shall analyze the suspected nonconformance. The contractor shall report, remedy and prevent recurrence of the nonconformance.
- The contractor shall standardize and control design practice and fabrication processes.
- The software shall be controlled in accordance with the software product assurance requirements specified in the following chapter.
- The critical category shall be referred SSP 30234.

b) Maintainability engineering requirements

Maintenance concept, Maintenance plan, Maintainability design criteria, Maintainability analysis and trade studies,

Tool requirements, Orbital Replacement Unit (ORU) Placement, Problem reporting and corrective action, Maintainability analysis, and Maintainability assessment, demonstration, and data collection are specified. Some detail requirements are as follows.

- ORU maintenance activity shall be based on the EVA or IVA maintainability design criteria.
- Maintainability analysis shall be conducted.
- Optimum ORU configuration shall be designed and maintainability analysis/trade study shall be conducted.
- Maintenance tools shall be confirmed.
- ORU positioning and accessibility shall be considered.
- Maintainability shall be considered for PRACA also.
- Maintainability predictions shall be prepared, submitted, and maintained in accordance with CR-99147.
- Preventive maintainability analysis shall be conducted for minimum system down time.
- Emergency maintenance analysis shall be conducted.
- Consistent with the maintenance concept, the quantities of spares shall be analyzed.
- ORU level maintainability information shall be prepared, submitted and maintained in accordance with CR-99146.
- Maintainability assessment, demonstration, and data collection shall be conducted.
- As the maintainability demonstration, the ORU shall be removed and exchanged.

4) Material, Process, and Parts Controls

Materials and processes shall be selected, applied, and controlled in accordance with CR-99117. A material and process program plan shall be prepared and approved. If materials or processes do not comply with CR-99117, a Material Usage Agreement (MUA) must be approved.

For the Electrical, Electronic, and Electromechanical (EEE) parts the S&PA activities shall be implemented in accordance with this paragraph and CR-99050. For the mechanical parts the S&PA activities shall be implemented in accordance with CRS-94010. The some detail requirements for the material and process are as follows.

- For the usage of the material which is not included in the Material Selection List (MSL), the MUA shall be submitted to NASDA for review.
- Material and process specifications shall be controlled and critical one shall be submitted to NASDA for review.
- Material and process shall be qualified.
- Material Identification and Usage List (MIUL) shall be prepared.
- Nondestructive Inspection (NDI) Plan are specified.

Some of detail management requirements for the EEE parts are as follows.

- EEE parts for criticality other than 3 hardware shall be selected from the Grade 1 Parts.
- EEE parts for criticality 3 hardware shall be selected from Grade 1 or 2 Parts.
- For the Non-standard EEE Parts which is not listed in the CR-99051 or SSP 30423, the JEM Non-standard Part Approval Requests (JNSPARs) shall be submitted in accordance with CR-99050.
- Ionizing radiation test for some of EEE parts shall be conducted according to SSP 30513.
- For Electrostatic Discharge (ESD) susceptible parts the control plan for the handling shall be developed and implemented based on CR-99287.
- EEE parts shall be controlled with EEE parts specifications.
- The parts shall be qualified by the EEE parts level when the qualification data is not available.
- For the EEE parts procurement pre-award survey plan, pre-award survey report, Destructive Physical Analysis (DPA) plan, and DPA report shall be prepared. In addition source inspection shall be conducted.
- As-designed EEE parts list and as-built EEE parts list shall be prepared.
- EEE parts application reviews shall be conducted. The de-rating based on CR-99291 and radiation data validation shall be reviewed.
- Nonconformance of EEE parts shall be controlled as required.
- All EEE parts shall have trace-ability data.
- Waiver or deviation for non-compliant parts shall be submitted to NASDA for approval.
- Mechanical parts shall be controlled in accordance with CRS-94010.

5.4 Quality Assurance

This requirements came mainly from NASDA-SPC-558 and included design controls as ISO 9001 does. However, design controls should be included in the previous reliability assurance section as a S&PA document. In this section the concept of Quality Assurance (QA) could be limited to production management. There are thirteen items here as the QA requirements. The followings are extracts of these requirements.

1) Concept of quality assurance activities, Quality assurance program plan, Quality status report, Training, and Quality assurance organization confirmation items at reviews are specified.

2) Technical document shall be established. Documents contents, Document reviews, and drawing system are also specified. Change control system shall be established.

3) The identification and data retrieval system shall be developed and maintained for articles and materials.

4) The QA activities regarding procurement shall be planned, implemented, and maintained. The contractor QA department shall participate in the selection of suppliers. Receiving inspection shall be conducted.

Above are essences from General and Receiving inspection. In addition, Procurement document, Contractor quality assurance activities at supplier, Subcontractor supervision by NASDA, Receiving inspection records, Supplier rating system. Coordination with supplier-conducted inspections and tests, and nonconformance information notification are specified.

5) Fabrication processes shall be controlled and the fabrication tasks shall be recorded.

Above is an essence from Fabrication operations. In addition, Article and material controls, Cleanliness control, Special process controls, Workmanship standards, and Control of temporary installations are specified.

6) The inspection and tests necessary to ensure that the article conform to the requirements in contracts, drawings, and specification shall be planned and implemented.

For the above, Inspection and test planning, Test specifications, Inspection and test procedures, Designation of representatives and quality assurance activities, Inspection and test performance, Records of inspections and tests, and Roles of contractor quality assurance department in test perfonmances are specified in detail.

7) A documented nonconformance processing system shall be established and maintained.

For the above, Identification and isolation of non-conforming articles, Documentation of non-conformance, Cause investigation and analysis, Preliminary Reviews (PRs), Material Review Board (MRB), Confirmation of disposition implementation, Corrective actions, Supplier material review board, Statistical analysis of non-conformance, and Utilization of NASDA articles are specified.

8) The records of each article shall be prepared, maintained, and updated to continuously control history of articles.

9) The metrology control system shall be established. For this, Receiving of measurements equipment and Evaluation of special measurement equipment, Measurement accuracy, Calibration accuracy, Calibration controls, Environmental conditions, Handling, storage, and transportation, Remedial actions, and Fabrication jigs and tools used for inspections are specified.

10) The status of inspection or processes for all articles and materials shall be identified. For this Stamp control system is specified.

11) The procedure for operations including handling, storing, packaging, and shipping the articles and materials shall be established and documented. Measures against electrostatic discharge or vibration shall be implemented. An Acceptance Data Package (ADP) for each end item article and material shall be prepared and maintained according to CRS-94021.

For the above, Handling, Storage, Preservation, Marking and labeling, Packaging, Packing, and Shipping are specified in detail.

12) Statistical process control shall be utilized if it is effective for controlling fabrication and inspection operations.

For this, Sampling inspection is specified referring MIL-STD-105D and MIL-STD-414.

13) Contractor's responsibility and Unsuitable NASDA and international partner property are specified.

5.5 Software Product Assurance

The requirements of Software Product Assurance (SPA) are specified separately in this section because of its inherent nature. The followings are essences of these requirements.

1) SPA activities shall be planned, managed, and integrated in conjunction with other S&PA organization's management.

2) Standards and procedural controls shall be established and implemented. Audits, evaluations and reviews shall be accomplished. Procedures shall be followed. All assurance activities shall be performed as scheduled.

3) Configuration identification, configuration status accounting, configuration verification, and configuration change control shall be performed for software.

4) All nonconformance shall be documented after software unit testing.

5) Software fault analysis shall be performed for software which supports critical functions. The result shall be

documented in accordance with CRS-95005.

6) Software safety analysis shall be performed in accordance with SSP 30309.

7) Software development standards shall be established and implemented.

8) Software trade studies shall be implemented.

9) Software shall be integrated for the software-to-hardware interfaces, software-to-software interfaces, and software-to-users interfaces, according to SSP 30459.

10) It shall be verified that the software products were developed according to an approved process. It shall be verified that all software product are present, complete, current and controlled. It shall be validated that the software products meet all of the applicable requirements.

11) Equivalent Independent Verification and Validation (IV&V) shall be conducted.

12) A security control plan shall be developed and maintained.

6. JEM S&PA Data Base

Looking at the rapid progress of the computer technology, NASDA has established a S&PA information system, S&PA Data Exchange (SPADE) system using the Hypertext and Internet technology. All the persons involved in the JEM program including NASA personnel can access the JEM S&PA data whenever they need as long as the password is obtained in advance. This system is already in operation and S&PA data is being accumulated. Currently SPADE accumulates the following data sets.

1) JEM Problem Reporting and Corrective Action (J-PRACA) for the non-conformance information.

2) JEM Material and Process Technical Information System (J-MAPTIS) for Material Usage Agreement (MUA), Material Identification and Usage List (MIUL), JEM Material Selection List (JEM-MSL), Flammability, Odor, and Off-gas Test Data.

3) JEM EEE Parts Information Management System (J-EPIMS) for the JEM Approved Parts List (JEM-APL), JEM Non-Standard Parts Approval Request (JNSPAR), As Designed Parts List (ADPL).

In Addition, JEM FMEA/CIL, JEM ORU, JEM Hazard Report, JEM Payload, JEM LLI, JEM Reliability, Availability and Maintainability program (JRAM), JEM EEE Parts Application Stress ratio calculation program (JEM EPAS), and S&PA Vocabulary are included.

The data category in the SPADE is being reviewed for the JEM operational phase. The recent technology, such as PDF format of Acrobat, will be incorporated for better convenience. Thus, SPADE system will be improved continuously.

7. Definitions for fundamental terminology

As mentioned above, S&PA activities are somewhat complicated and simplification of S&PA requirements would be desired. One of the reasons for complexity is that the integration of four assurance activities is incomplete. In this respect, what we should improve first is to have one and only definitions for at least fundamental terminology used in S&PA, such as "hazard," "risk," "safety," "criticality," " failure," "fault." Those definitions sometimes vary even among NASA documents. As the one of examples, let us look at the "risk".

The definition of the "risk" may be self-evident because it is a very popular word in the world. However, fairly differences are found among documents.

"As applies to safety, exposure to the chance of loss of injury or loss. It is a function of the possible frequency of occurrences of an undesirable event, of the potential severity of the resulting consequences, and of the uncertainties associated with the frequency and severity."

— NHB 1700.1(V1-B)

"The chance (qualitative) of loss of personal, loss of system, or damage to or loss of equipment property"

— NHB 5300.4(1D-2)

"Exposure to the chance of injury or loss. It is a function of the possible frequency of occurrence of an undesirable event and the potential severity of the resulting consequences."

— SSP 30309E

NASDA adopts the definition in NHB 5300.4(1D-2) for NASDA-ESPC-1088.

All of the NASA's definitions, accordingly including NASDA's definition, have a defect. That is, risk has the significant meaning when it is compared by height, high or low. Two dimensional value cannot be compared as it is. We need a transfer function or an evaluation equation from two dimension to one dimension. In the NASA definition, SSP 30309E, only the word, "a function," is used but there is no definition for the function.

Not limiting to space development field and generally speaking, the risk is defined the product of the probability of

the occurrence and the severity if it happened. As the generalization, the risk is properly defined as the expectation value of the severity, where probability density function is the expression for the occurrence of the event versus the severity of the event. The reason for not using expectation in NASA definition may be explained by the confusion in the definition for probability in real world. Some NASA documents use "Likelihood of Occurrence" and others use "Frequency of Occurrence" in place of the "Probability" It must be pointed out that risk has the dimension of the "value", whatever unit is used.

Though we see different definitions for even "safety" also among NASA documents, "safety" should be defined as "the state where risk is acceptably low." Accordingly "unsafe" is the opposite concept of "safe" and defined as "the state where risk is unacceptably high." Acceptable limit may be different from the background of the society. However, there is no gray zone between safe and unsafe for decision makers. Especially, manned space program must be conducted always under the decision of safe and should not be conducted on risky situation.

8. Definition of Probability in real world

Recently, under the severe environment of space development budgets, quantitative risk assessment has been spotlighted again to manage space programs effectively. For example, an IAA report, "Risk as a Resource" by Greenfield/NASA shows this tendency. Therefore most important item is to review the definition of "probability" used in the engineering field, although its mathematical definition is completely clear.

It is important how to define the probability in the real world for application of mathematical probability theory where the abstract probability is defined with the axiom. Although there are many ways of defining real world probability which satisfy the axiom, three of them are recognized essential. These are limit of relative frequency, a priori definition as a ratio of favorable to total number of alternatives, and degree of belief.

The relative frequency definition is also called von Mises's approach and this definition is broadly used in the engineering field so far, although the existence of the limit of relative frequency is a hypothesis and cannot be proved. People try to estimate the probability with available data. When they need exact expression for this estimation, they introduce confidence level. The accuracy of estimation can be expressed by the level of confidence. This is logically true, but not rational because we do not have reasonable basis for the selection of confidence level value at all. This definition is easy to understand and there is almost no claim where the laws of large numbers govern. However, there is no basis for the only one time event in real world as von Mises says by himself.

The classical definition is also called Laplace's approach and broadly adopted by physicists. This definition is criticized on the "equally likely." This criticism in this definition may be cleared by the integrating to the next definition.

The degree of belief definition is called Savage's approach. In this definition the provability is the value assigned to the degree of belief on the proposition. When the degree of belief can be assigned in the distribution form as the density from 0 to 1, the probability should be defined that the expectation value of the density of belief of the probability. The probability is assigned from the information about the proposition. When we have no information about the proposition, we assign the value a priori based on the principle of equally likely as the same way of classical definition. After we see the data a posteriori probability can be calculated with Bayes' Theorem. This probability is also called subjective probability, because different value would be assigned by the two people if they had different information about the proposition. Of cause if they showed their data each other and if they saw same data, they would assign same value for the probability. This definition is the right interpretation of the probability especially for evaluation of risk.

References

1) (IGA), November, 1988
2) (MOU), March, 1989
3) Joint Program Plan, (JPP)
4) SSP 30000 "Program Definition and Requirements Document", (PDRD) Section 9 Safety and Product Assurance Requirement
5) SSP 30309E "Safety Analysis and Risk Assessment Requirements Document International Space Station Alpha Program", October 28, 1994
6) SSP 30234 "Instructions for Preparations of Failure Modes and Effects Analysis and Critical Items List for

Space Station"
7) SSP 30459 "International Space Station Interface Control Plan"
8) SSP 30513 "Space Station Ionizing Radiation Environment Effects Test and Analysis Techniques"
9) SSP 50005 "International Space Station Flight Crew Integration Standards"
10) SSP 50021 "Safety Requirements Document International Space Station", December 12, 1995
11) SSP 50030 "NASA/NASDA Joint Management Plan", March 25, 1994
12) SSP 50038B "Computer-Based Control System Safety Requirements International Space Station Program", November 17, 1995
13) SSP 50126 "NASA/NASDA Bilateral Data Exchange Agreement (BDEA), Lists and Schedules"
14) SSP 50145 "NASA/NASDA Bilateral Safety and Product Assurance Requirements", August 7, 1995
15) NHB 1700.1(V1-B) NASA Safety Policy and Requirements Document, June 1993
16) KHB 1700.7B "Space Shuttle Payload Ground Safety Handbook", September 1, 1992
17) NSTS 1700.7B "Safety Policy and Requirements For Payloads Using the Space Transportation System", January 1989
18) NSTS 1700.7B ADDENDUM "Safety Policy and Requirements For Payloads Using the International Space Station", December 1995
19) MIL-STD-105D "Sampling Procedures and Tables for Inspection by Attributes"
20) MIL-STD-414 "Sampling Procedures and Tables for Inspection by Variables for Percent Defective"
21) ISO 9001 "Quality Systems-Model for Quality, Assurance in Design/Development, Production, Installation and Servicing"
22) IAA-97-IAA.6.2.06 "Risk as a Resource", M. Greenfield, October 6-10, 1997
23) "Space Shuttle Probabilistic Risk Assessment", Joseph R. Fragola, ESREL'96 - PSAM-III, June 24-28 1996, Crete, Greece
24) "Introduction To Probability and Statistics from a Bayesian Viewpoint", D.V.Lindley, 1965
25) "Probability, Statistics, and Truth", Von Mises, R., Dover. New York, 1957.
26) Title 14 of the U.S. Code of Federal Regulations Federal Aviation Regulations

NASDA Documents: (Japanese)
1) NASDA-STD-1B "Configuration Management Provision", October 6, 1997
2) NASDA-STD-16 "Quality Assurance Program Provision", July 21, 1994
3) NASDA-STD-17 "Reliability Program Provision", March 18, 1997
4) NASDA-SPC-558 "Quality Assurance Program Provision" (disuse)
5) NASDA-SPC-1177A "Reliability Program Provision" (disuse)
6) NASDA-ESPC-840G "JEM System Specification"
7) NASDA-ESPC-1088D "Safety and Product Assurance Requirements for Japanese Experiment Module (JEM) Attached to the Space Station" October 18, 1995
8) NASDA-ESPC-1681 "Japanese Experiment Module (JEM) Payload Safety and Product Assurance Requirements", June 21, 1995
9) CR-99117 "JEM Material and Process Requirements"
10) CR-99144 "JEM FMEA/CIL Preparation"
11) CR-99145 "JEM Limited Life Item List Preparation"
12) CR-99146 "JEM ORU Data Preparation"
13) CR-99147 "JEM Maintainability Prediction Data Preparation"
14) CR-99050 "JEM EEE Parts Control Plan"
15) CR-99051 "JEM Approve Parts List"
16) CR-99287C "ESD Management Requirements for the EEE Parts", October 31, 1997
17) CR-99302 "JEM Safety and Product Assurance Plan"
18) CRS-94010 "JEM Mechanical Parts Control"
19) CRS-94020 "JEM Special Control Item Control Requirements"
20) CRS-94021 "JEM Acceptance Data Package (ADP) Preparation"
21) CRS-95005 "Software Fault Analysis Procedure"
22) R SOP-20A "Handling Procedures for Parts Data"

Other Document: (Japanese)
1) "Nuclear Safety", Prof. Syunsuke Kondo, dohbun-syoin
2) "Basic Guideline for Safety Assessment to Japanese Experiment Module (JEM) Attached to the Space Station", Safety Assessment Sub-Committee of Space Activities Commission, April 24, 1996