

PRODUCT & QUALITY ASSURANCE FOR SPACE PROJECTS

NATALIA AURICCHIO – INAF /OAS-BOLOGNA

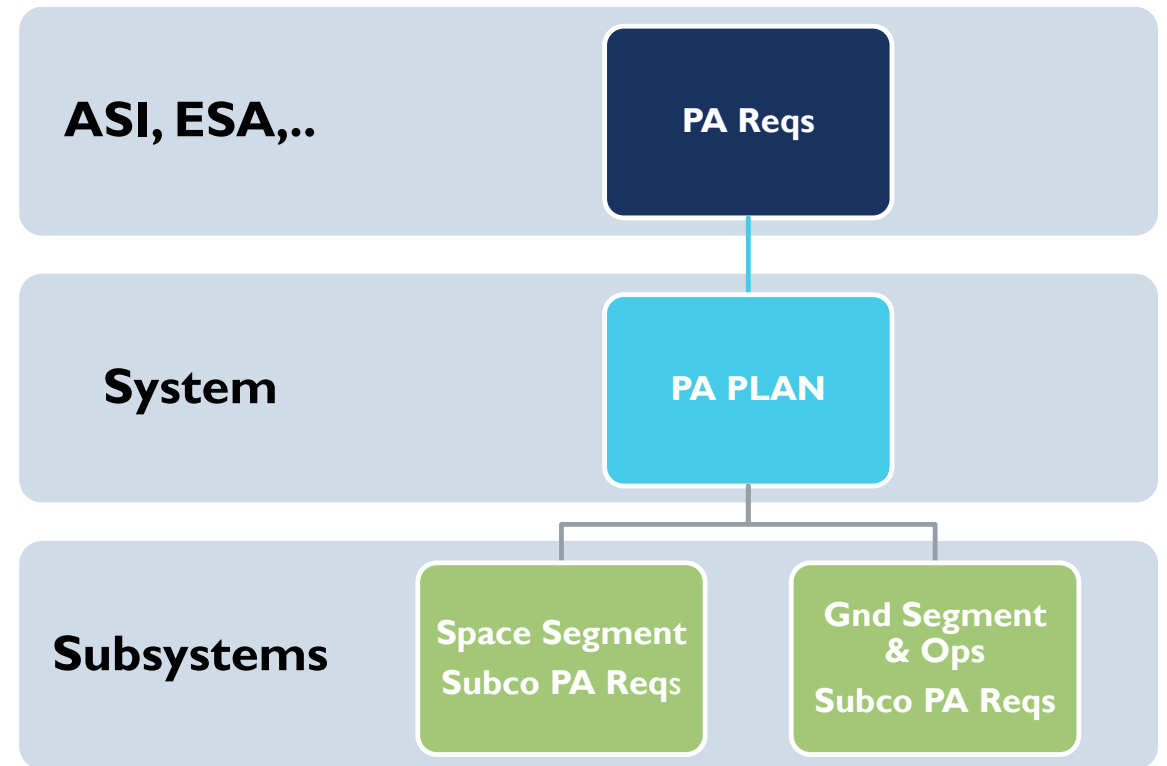


OUTLINE

- ❖ **ECSS standard**
- ❖ **Product & Quality Assurance**
- ❖ **NCR**
- ❖ **SW Product Assurance**

ECSS STANDARD: EUROPEAN COOPERATION FOR SPACE STANDARDIZATION (I)

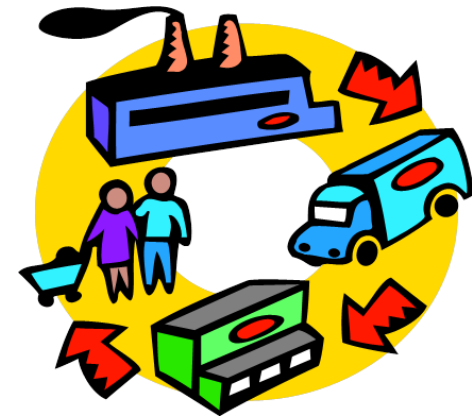
- ECSS is a consistent and coherent set of standards for the procurement of a generic space product.
- ECSS Standards shall NOT be used in isolation, it is an interrelated set of standards
- The supplier, at any level, is responsible for demonstrating compliance with the project requirements, including compliance to ECSS Requirements, subject to **tailoring**: the process of adapting the requirements to the project specificities



Requirement tailoring process flow-down

ECSS STANDARD: EUROPEAN COOPERATION FOR SPACE STANDARDIZATION (II)

- The ECSS Standards and requirements to be made applicable at each level of the customer–supplier chain are influenced by the type and phase of the project involved, as well as by the type of business agreement to be used for managing the project.



PROJECT/MISSION LIFE CYCLE

MISSION PHASES



Concept Exploration
Preliminary Design
Detailed Design
Production
Operations

Phase **A**
Phase **B**
Phase **C**
Phase **D**
Phase **E**

PA activity

- Ex ante: **analysis**
- In Itinere: **surveillance**
- Ex post: **recovery/lesson learnt**

DISPOSAL

ECSS STANDARD: EUROPEAN COOPERATION FOR SPACE STANDARDIZATION (III)

- **Standardization needs & objectives in Space Projects**
 - **Competitiveness**
 - **Efficiency**
 - **Knowledge**
 - **Education**

WHAT IS PRODUCT ASSURANCE?

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 degree of **quality** in a **product** (ECSS-S-ST-00-01C, Glossary of terms)

Product assurance disciplines

- Quality Assurance
- Dependability
- Safety
- EEE Components
- Materials/processes
- SW PA

PRODUCT ASSURANCE MANAGEMENT

- Product Assurance management is a multidisciplinary activity to ensure that a PA programme is planned, implemented and managed, throughout all phases and coordinated with all actors.
- It addresses the Product Assurance Plan (PAP).

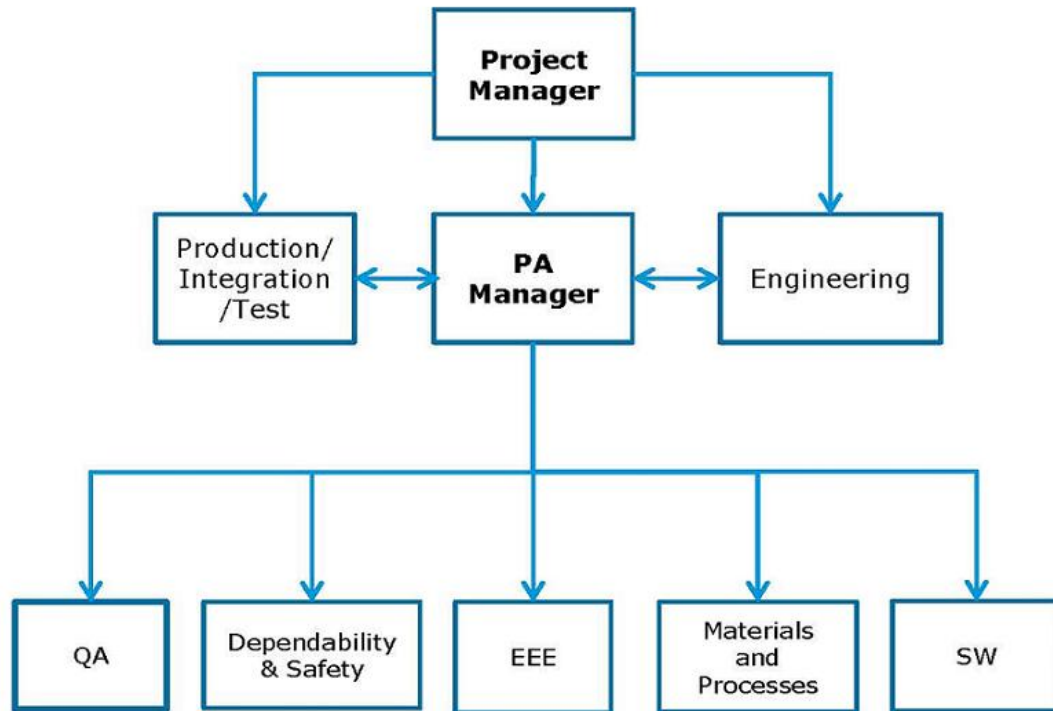
PA PLAN content (ECSS-Q-ST-10 Annex A):

- PA organization, responsibilities and authority, resources, PA interfaces & processes
- PA implementation procedures, including:
 - PA management
 - PA reporting
 - PA audits
 - Critical items
 - Risk mgmt. interfaces
 - Document & data control
 - Quality records
 - PA contribution to CC
 - NCRs
 - Alerts management
- QA processes & procedures
- Dependability (Q30) processes & procedures
- Safety (Q40) processes & procedures (or refer to the Safety plan)
- EEE components (Q60) processes & procedures
- MMP&P (Q70) processes & procedures
- SW PA (Q80) processes & procedures
- Specific PA process & procedures relevant to the organization, not covered above

QA PLAN content (ECSS-Q-ST-20 Annex A):

- QA processes and procedures including training and certification
- Design and verification QA activities and processes (including qualification)
- Procurement QA activities and processes
- Manufacturing, assembly and integration (MAI) QA activities, including:
 - MAI Planning, processes & workmanship
 - MMP&P and equipment control
 - CCCP (Cleanliness & cont. control plan)
 - Inspection
 - Records
 - ESD protection programme
- Testing QA activities and processes
- Acceptance & delivery QA activities (including among others EIDP & Delivery Review Board)
- QA specific activities, including:
 - Critical items
 - NCRs
 - Alert management
 - Authority media
 - Traceability
 - Metrology and calibration
 - Handling and storage
 - Statistical quality control

PA/QA ORGANIZATION



- Ideal organization
- QA and other PA disciplines are managed by PAM

WHAT IS QUALITY ASSURANCE?

- Part of quality management focused on providing confidence that quality requirements will be fulfilled

[ISO 9000:2005]

- “Quality is never an accident it's always the result of high intention, sincere effort, intelligent direction and skillful execution; it represent the wise choice of many alternatives.”

“The bitterness of poor quality lingers long after the sweetness of low price is forgotten.”

(John Ruskin, 19th century)

PA VERSUS QA

PA Manager tasks

- Define and maintain the PA plan
- Responsibility for coordinating, planning and controlling the PA activities
- Present the PA status
- Management and control of PA actions
- Participation in System/subsys reviews
- Management of non-conformances
- Internal and external PA audits/inspection management.
- Cooperation in risk assessment and configuration activities.
- Presentation and control of the RFD/W status

Quality Assurance tasks

- Record all the activities for traceability
- Review and approval of step-by-step procedure including inspections
- Packing, marking and labelling
- Visual inspections, KIP/MIP
- Incoming inspections & Outgoing inspection
- Control the personnel training status
- Ensuring proper handling according to procedure
- Maintain ESD, cleanliness and contamination control
- Maintain NCR system

NONCONFORMANCE CONTROL SYSTEM

ECSS-Q-ST-10-09C

- This Standard defines the requirements for the control of nonconformances
- The Standard applies to all deliverable products and supplies, at all the levels, which fail to conform to project requirements
- This Standard is applicable throughout the whole project lifecycle as defined in ECSS-M-ST-10
- Describes the approach to the identification and processing of nonconforming items, which can be performed at each customer/supplier level

- According to ECSS-S-ST-00-01C:
- **nonconformance:** non-fulfilment of a requirement
- **Anomaly:** any deviation from the expected situation. An anomaly justifies an investigation that might lead to the discovery of a nonconformance or a defect.

NON-CONFORMANCES: INVESTIGATING ROOT CAUSES

- For each non conformity there is a **root cause**
 - ❑ Root cause must be removed by **corrective action**
 - ❑ Causes are **preventable**
 - ❑ Prevention is always **cheaper**
- Non-conformances shall be classified as **Major** or **minor** based on severity of their consequences. Classification of Non-conformances shall not be based on their consequences on cost and schedule.

NON-CONFORMANCES: CORRECTIVE ACTIONS & DISPOSITION

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

Disposition

- **Return to supplier**
- **Use-as-is**
- **Rework**
- **Repair**
- **Scrap**

NONCONFORMANCE PROCESSING: NRB (HW/SW)

- The **internal NRB** investigates the causes and consequences of the nonconformance and classifies the nonconformance either as minor or Major.
- Major nonconformances are submitted to the **Customer NRB**.
- Multiple internal or customer NRBs can be held before the NCR is closed out.
- During internal as well as customer NRB, corrective actions are determined to eliminate the causes of the NCs.
- The NRB shall be the sole technical authority for the treatment of nonconformances
- The internal/Customer NRB shall include, at least, **core members** from the following areas: Project PA, Engineering, Additional members, or experts, depending on the NCR subject.
- The customer NRB shall decide on the need to perform additional analyses, complementary investigations to assess the cause and consequences of a nonconformance and to support its disposition.
- The NCR can be considered closed when all agreed dispositions / actions have been successfully implemented and verified.

SW PRODUCT ASSURANCE

Definitions

- A **Software Product** is a set of computer programs, procedures, documentation, and their associated data.
- **Software Product Assurance (SPA)** is the totality of activities, standards, controls, and procedures in the lifetime of a software product which establish confidence that the delivered software product, or software affecting the quality of the delivered product, conforms to Customer requirements

SPA Objective

- SPA Objective: «To provide adequate confidence to the Customer and to the Supplier that the developed or procured/reused software satisfies its requirements throughout the system lifetime»
 - ❖ In particular, that the software performs properly and safely in its operational environment
- SPA consists of:
 - ❖ Assurance of process (Software Process Assurance).
 - ❖ Assurance of product quality (Software Product Quality Assurance)

ECSS-Q-ST-80C and **ECSS-E-ST-40C** should always be applied together to specify all processes for Space Software Development.

ECSS-Q-ST-80C

Structure

Software product assurance programme implementation	
5.1 Organization and responsibility	5.5 Procurement
5.2 Software product assurance programme management	5.6 Tools and supporting environment
5.3 Risk management and critical item control	5.7 Assessment and improvement process
5.4 Supplier selection and control	

Software process assurance	
6.1 Software development life cycle	
6.2 Requirements applicable to all software engineering processes	
6.3 Requirements applicable to individual software engineering processes or activities	

Software product quality assurance	
7.1 Product quality objectives and metrication	
7.2 Product quality requirements	
7.3 Software intended for reuse	
7.4 Standard ground hardware and services for operational system	
7.5 Firmware	

Reqs, Expected Outputs, Files, Reviews



Requirement



Expected Output



File



Documents



Review

SOFTWARE PRODUCT ASSURANCE PROGRAMME IMPLEMENTATION

Software problems

- Detailed content of software problem report (SPR)
- Interface with nonconformance
- Verify correct implementation of SPR procedures
- Identification, classification, segregation, reporting, review, analysis, disposition of NCRs
- Corrective and preventive actions

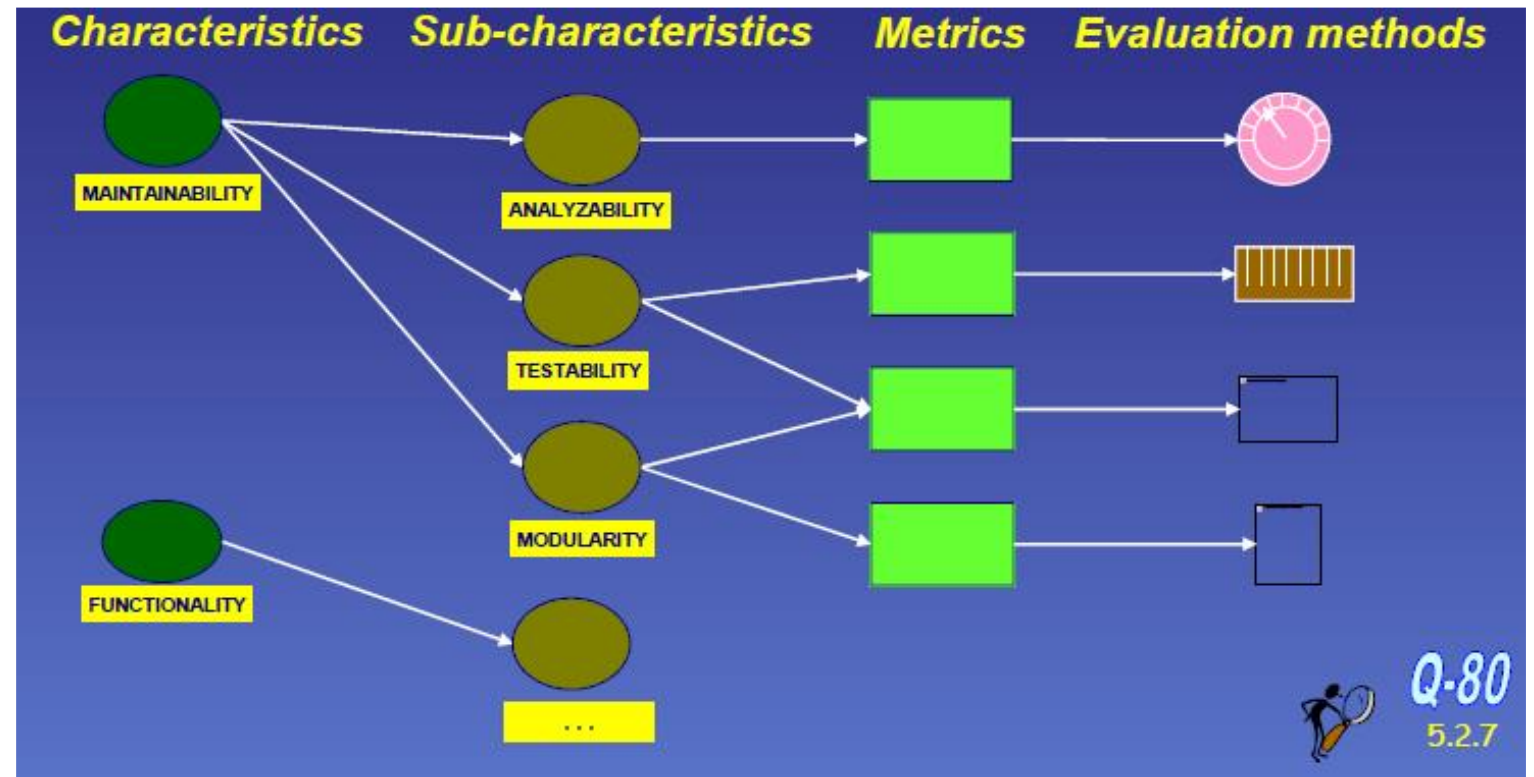
NCR

- For software nonconformance handling:
ECSS-Q-ST-10-09 shall apply
- SPA and SW engineering must be represented in the **Nonconformance Review Board** (NRB).

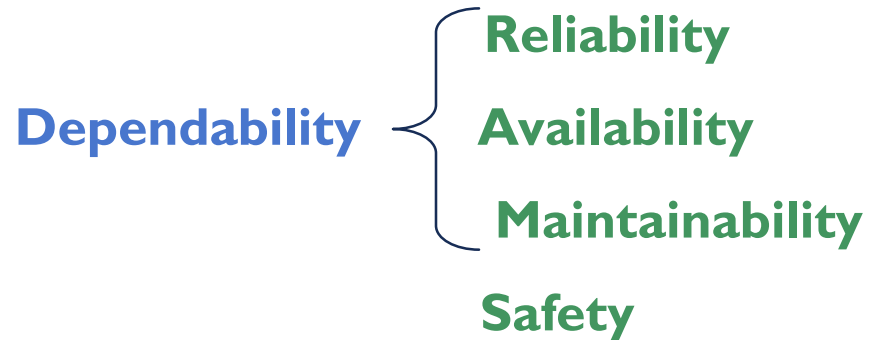
QUALITY REQUIREMENTS AND QUALITY MODELS

■ SW Quality characteristics:

- Functionality
- Reliability
- Maintainability
- Reusability
- Suitability for safety
- Security
- Usability
- Efficiency
- Portability
- Software development effectiveness



SOFTWARE PROCESS ASSURANCE



- Studies have been carried out on methods, techniques, and procedures in order to specify SW RAMS requirements, and how to perform V&V against them.

SOFTWARE DEPENDABILITY AND SAFETY

NAME	LEVEL	DEPENDABILITY (ECSS-Q-30)	SAFETY (ECSS-Q-40)
CATASTROPHIC	1		<ul style="list-style-type: none"> Loss of life, life-threatening or permanently disabling injury or occupational illness. Loss of an interfacing manned flight system Severe detrimental environmental effects. Loss of launch site facilities. Loss of system
CRITICAL	2	COMPLETE LOSS OF MISSION	<ul style="list-style-type: none"> Temporarily disabling but not life-threatening injury, or temporary occupational illness. Major detrimental environmental effects. Major damage to public or private properties. Major damage to interfacing flight systems, Major damage to ground facilities.
MAJOR	3	MAJOR MISSION DEGRADATION	
MINOR OR NEGLIGIBLE	4	MINOR MISSION DEGRADATION OR ANY OTHER EFFECT	

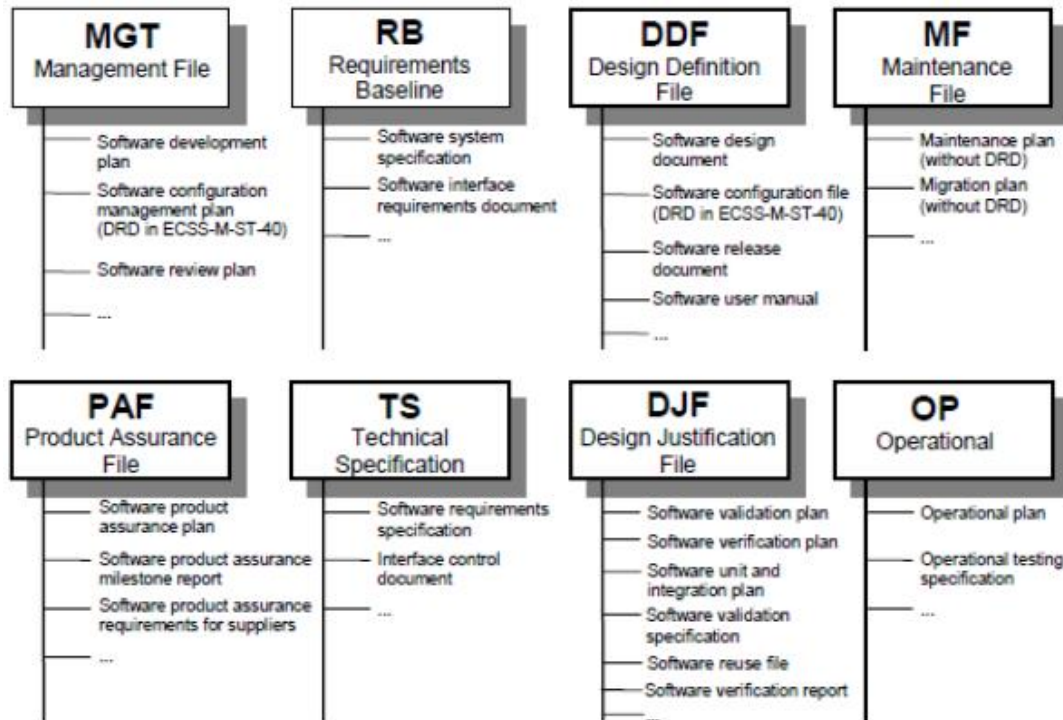
Software criticality categories

Cat.	Definition
A	Software that if not executed, or if not correctly executed, or whose anomalous behaviour can cause or contribute to a system failure resulting in Catastrophic consequences .
B	Software that if not executed, or if not correctly executed, or whose anomalous behaviour can cause or contribute to a system failure resulting in Critical consequences .
C	Software that if not executed, or if not correctly executed, or whose anomalous behaviour can cause or contribute to a system failure resulting in Major consequences .
D	Software that if not executed, or if not correctly executed, or whose anomalous behaviour can cause or contribute to a system failure resulting in Minor or Negligible consequences .

SOFTWARE PRODUCT QUALITY ASSURANCE

- Software Product Quality Assurance comprises the measures taken to obtain a SW product that meets the specified quality requirements:
 - ❖ Definition of SW quality requirements
 - ❖ Definition of a Metrication Programme
 - ❖ Production of detailed documentation for design and test planning and reporting
 - ❖ Definition of specific requirements for software intended for reuse
 - ❖ Careful selection of hardware, services and firmware for ground equipment

SOFTWARE DOCUMENTATION



- **Annex B** and **Annex C** specify the DRD's (Document Requirements Definitions) for SPA specific documents:
 - ❖ **SPAP**: Software Product Assurance Plan
 - ❖ **SPAMR**: Software Product Assurance Milestone Report

EXPECTED OUTPUT VERSUS REVIEWS

File	DRL Item	SRR	PDR	CDR	QR	AR	ORR	File	DRL Item	SRR	PDR	CDR	QR	AR	ORR	
PAF	Software product assurance milestone report (SPAMR)	√	√	√	√	√	√	PAF	Software product assurance milestone report (SPAMR)	√	√	√	√	√	√	
	Statement of compliance with test plans and procedures			√	√	√	√		Statement of compliance with test plans and procedures				√	√	√	√
	Records of training and experience								Records of training and experience							
	(Preliminary) alert information								(Preliminary) alert information							
	Result of pre-award audits and assessments, and of procurement sources								Result of pre-award audits and assessments, and of procurement sources							
	Software process assessment plan								Software process assessment plan							
	Software process assessment records								Software process assessment records							
	Review and inspection reports								Review and inspection reports							
	Receiving inspection reports	√	√	√	√				Receiving inspection reports	√	√	√	√			
	Input to product assurance plan for systems operation								√	Input to product assurance plan for systems operation						