Software Product Assurance

Emmanuel Lesser – Software PA Engineer

Block 4 – Software PA Across Processes

Who am I?

- SW PA Engineer in TEC-QQS
- Point of contact for Software Process Assessment and Improvement activities
- Point of contact for cybersecurity activities
- Support multiple ESA projects wrt SW PA, FPGA, Fault Management
- Run and support various research activities on process assessment, cybersecurity, machine learning and SW PA/Engineering
- Interest in quantum technologies for space systems, with a focus on security

ESA UNCLASSIFIED - For Official Use

Software Quality Requirements

- What is "quality"?

> Degree to which a set of characteristics of a product or process fulfils requirements
>
> [ECSS-S-ST-00-01C]

- To ensure software quality, suitable requirements must be specified
- Quality requirements shall be expressed in quantitative terms and constraints
- Quality models shall be used to specify the software quality requirements

Quality Model (I)

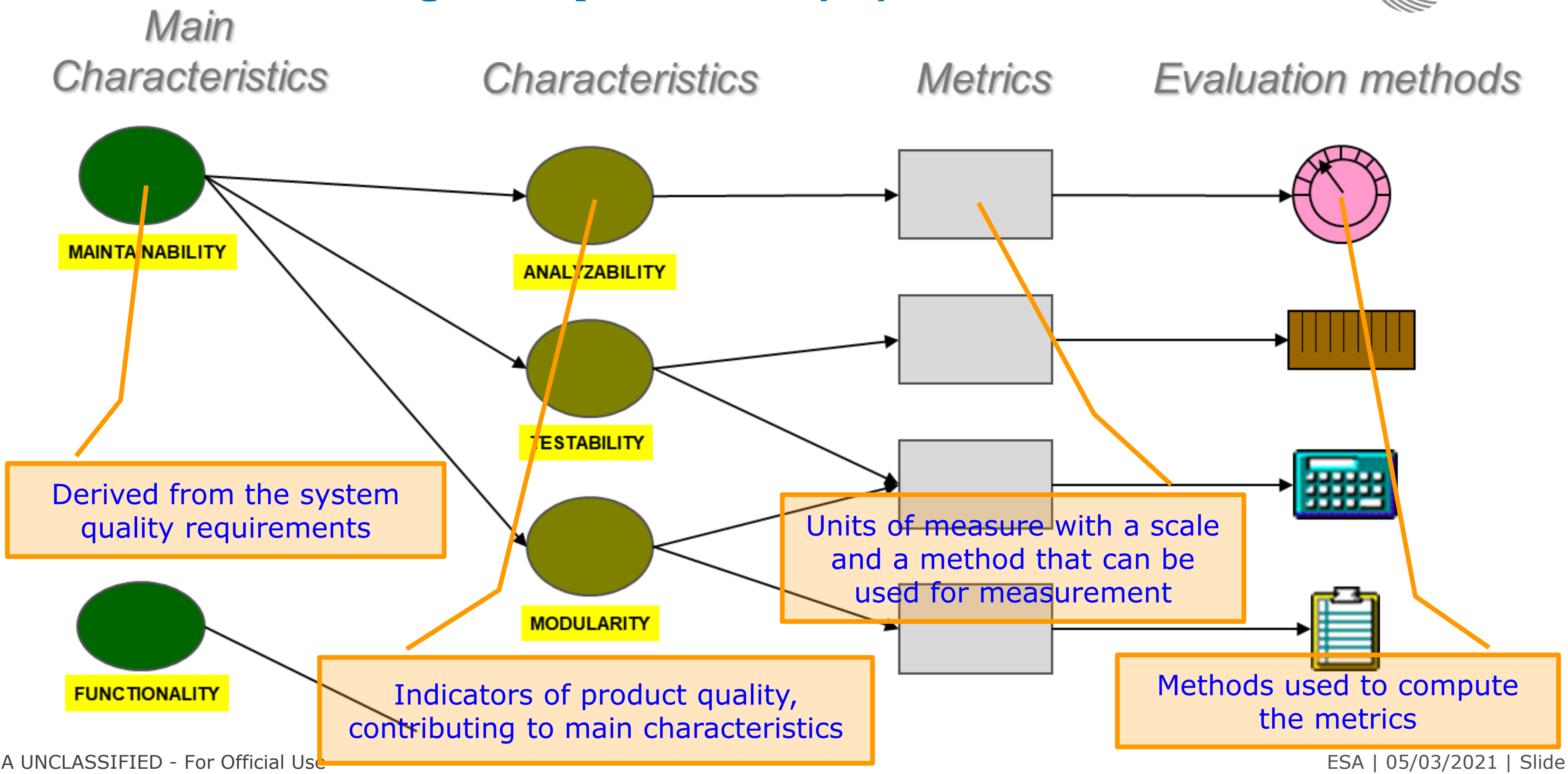
Set of characteristics and the relationships between them which provide the basis for specifying quality requirements and evaluating quality

[ECSS-Q-ST-80C]

- Defined e.g. in:
  - ISO 9126
  - ECSS-Q-HB-80-04

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

Quality Model (II)



Derived from the system quality requirements

Indicators of product quality, contributing to main characteristics

Units of measure with a scale and a method that can be used for measurement

Methods used to compute the metrics

Quality Model (III)

- A metrication programme shall be defined to verify the implementation of quality requirements
  - metrics to be collected
  - means to collect the metrics
  - target values
  - analyses to be performed (statistic, trends)
  - usage of metrics (corrective actions ⇨ see later)
  - schedule of collection

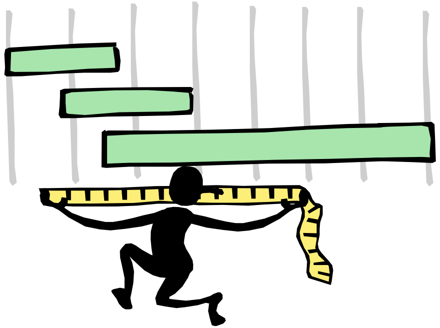
- Mandatory product metrics:
  - Size, complexity, fault density and failure intensity, test coverage

Quality Model (IV)

- Metrics are to be
  - Used to assess the quality of processes and products
  - Fed back to the development team and used to identify corrective actions

Collecting (product) metrics just at the end of the development is basically useless

- Metrics shall be reported upon as part of regular SW PA reporting
  - Both process and product



Product Quality Requirements (I)

- What do you think of the following requirement?

> In all modes, the CSW shall periodically perform the monitoring checks which are enabled in PUS service 12. When a parameter is detected out of limits for a consecutive number of times, a dedicated event report shall be generated (generated only once if the violation persists).

Product Quality Requirements (II)

- General requirements, not derived from quality model
- Software requirements shall be:
  - Correct
  - Unambiguous
  - Complete
  - Consistent
  - Verifiable
  - Traceable
- For each requirement, the method for verification and validation shall be specified.

Product Quality Requirements (III)

- Software shall be designed to facilitate testing
- Software with a long planned lifetime shall be designed with minimum dependency on the operating system and the hardware
- The test documentation shall cover:
  - Hardware and software configuration, test environment, tools and test software, personnel required and associated training requirements
  - Criteria for completion of each test and any contingency steps
  - Test procedures, data and expected results
- For any requirements not covered by testing, a verification report shall be drawn up

SW Process Assessment and Improvement (I)

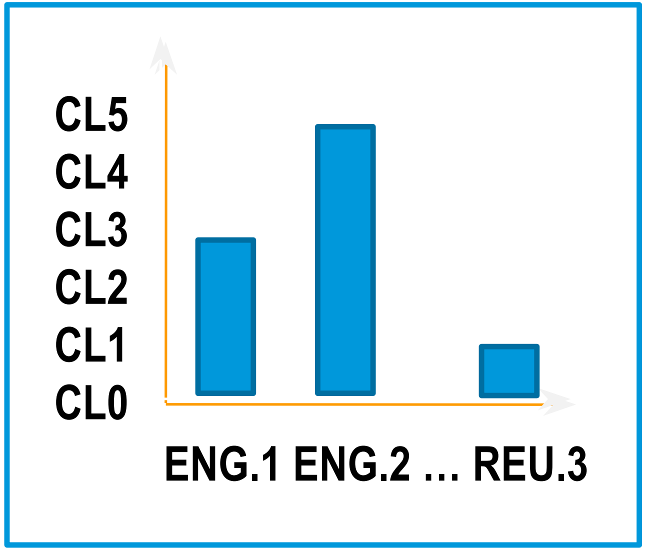
- The supplier shall monitor and control the effectiveness of the processes used during the development of the software
- Software product quality is highly influenced by the maturity of the processes used to acquire, develop and maintain the software.
- Evidence shall be provided that a process assessment and improvement process is in place
  - Records to be made available
  - Confidentiality is respected

SW Process Assessment and Improvement (II)

- The process assessment model and method used to perform software process assessment shall be documented
- Models and actual assessments shall comply with SPICE (ISO/IEC 33002)
  - But…CMMI model + SCAMPI A methods are OK
  - **ECSS-Q-HB-80-02** contains a method and a model which are conformant to ISO/IEC 15504
- Assessments shall be performed by skilled personnel
  - ISO/IEC 33002 ⇨ competent assessor
  - CMMI ⇨ SEI authorized lead appraiser

Process Assessment (I)

- S4S (SPICE for Space): Two-dimensional process assessment model
  - Process dimension
  - Capability dimension
- The process dimensions lists the processes that are within the scope of the current assessment
- The scope of assessments are tailored such that only relevant processes are included and assessed up to an agreed capability level, in-line with business-goals



Process Assessment (II)

PRIMARY LIFECYCLE PROCESSES

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

SUPPORTING LIFECYCLE PROCESSES

SUPPORTING:
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

ORGANIZATIONAL LIFECYCLE PROCESSES

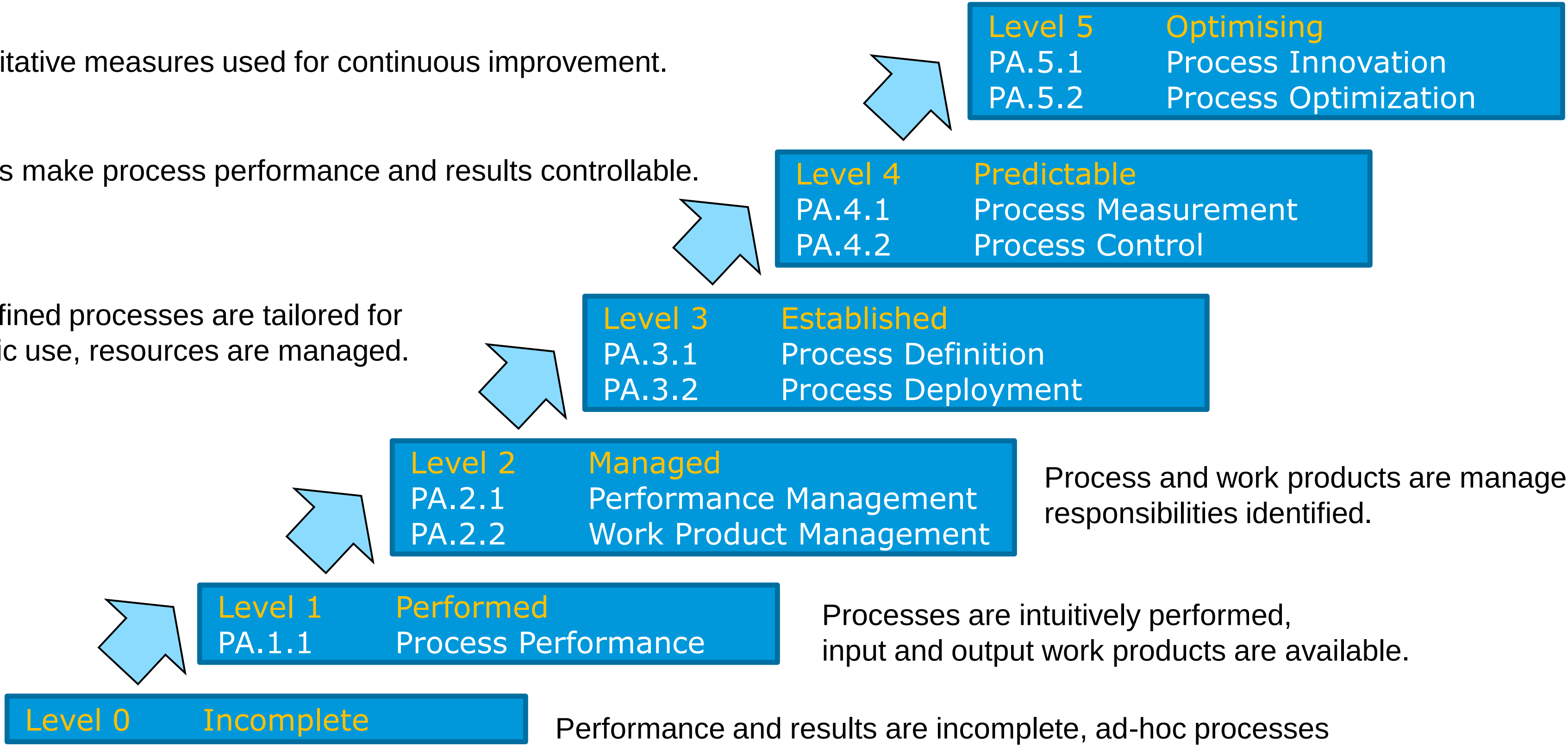
MANAGEMENT:
MAN.1 Organizational Alignment
MAN.2 Organizatioin Management
MAN.3 Project Management
MAN.4 Quality Management
MAN.5 Risk Management
MAN.6 Measurement
MAN.7 Information Management

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

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

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

Process Assessment (III)



Quantitative measures used for continuous improvement.

Level 5 Optimising
PA.5.1 Process Innovation
PA.5.2 Process Optimization

Metrics make process performance and results controllable.

Level 4 Predictable
PA.4.1 Process Measurement
PA.4.2 Process Control

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

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

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

Process and work products are managed, responsibilities identified.

Level 1 Performed
PA.1.1 Process Performance

Processes are intuitively performed,
input and output work products are available.

Level 0 Incomplete

Performance and results are incomplete, ad-hoc processes

Process Assessment (VI)

Audit

Focus: Requirements

Compliance / Non-compliance (Y/N)

Snapshot (is it compliant *now*?)

Straightforward (Success / Failure)

Improvement: Corrective actions

Common

Evidence-based (interviews, documents)

Confidential

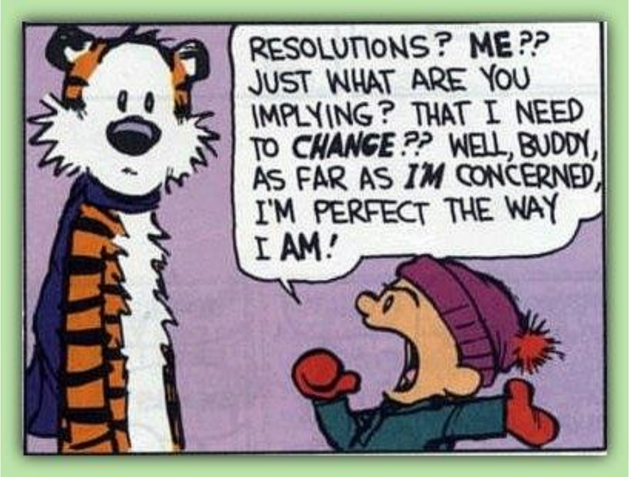
Focus on process (not people or technology)

Assessment

- Focus: Capability
- Rating: 0..100% achievement
- Projected (how capable is it?)
- Captures complexity (Effectiveness, Efficiency)
- Improvement: strengths, weaknesses, risks

Process Improvement

- The results of a process assessment are reported in detail in the Assessment Report. Identified gaps are described in detail
- The next step of the assessment & improvement cycle is an Improvement Workshop
- An Improvement Plan is implemented in 6 – 12 months (ideally)
- A delta-assessment is performed to complete the cycle. The organisation will now have achieved the target capability level.


RESOLUTIONS? ME?? JUST WHAT ARE YOU IMPLYING? THAT I NEED TO CHANGE?? WELL, BUDDY, AS FAR AS I'M CONCERNED, I'M PERFECT THE WAY I AM!

Approach for Very Small Entities (I)

Enterprise, organization, department or project having up to 25 people (VSE), but which is not part of (or belong to) an organization with standardized software processes or with demonstrated maturity for developing safety critical software in the space domain

[Draft ISO/IEC 29110-6-1]

Applying the whole S4S (ECSS-Q-HB-80-02) provisions to a VSE would most often correspond to an overkill

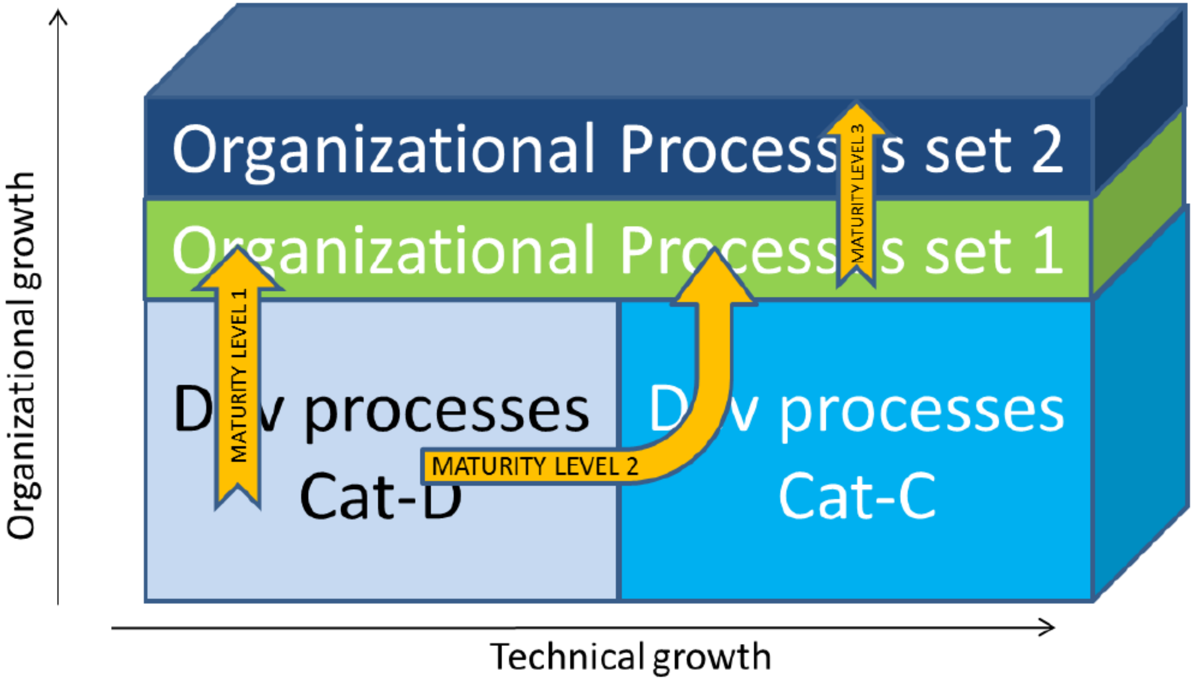
The assessment and improvement framework should be tailored to become feasible and affordable to a VSE

ISO/IEC 29110-6-1: simplified process and capability dimensions

Approach for Very Small Entities (II)

- ISO/IEC 29110-6-1 foresees a lighter approach to assessment conduct than S4S
- Assessment process similar to S4S: questionnaires, definition of scope, assessment plan, assessment, presentation of results, final assessment report
- Fully on-line – unless on-site is preferred by assessed organization
- Estimated assessment duration:
  - Maturity Level 1: 1-1,5 day
  - Maturity Level 2: 2 days
  - Maturity Level 3: 3–3,5 days

Approach for Very Small Entities (III)



ISO/IEC 29110-6-1 – Process Dimension

Development processes

Engineering processes

- ENG.1 Requirements elicitation (ECSS-Q-HB-80-02)
- SI Software Implementation (ISO/IEC 29110)
- ENG.8 Software testing (ECSS-Q-HB-80-02)

Management processes

- PM Project Management (ISO/IEC 29110)

Supporting processes

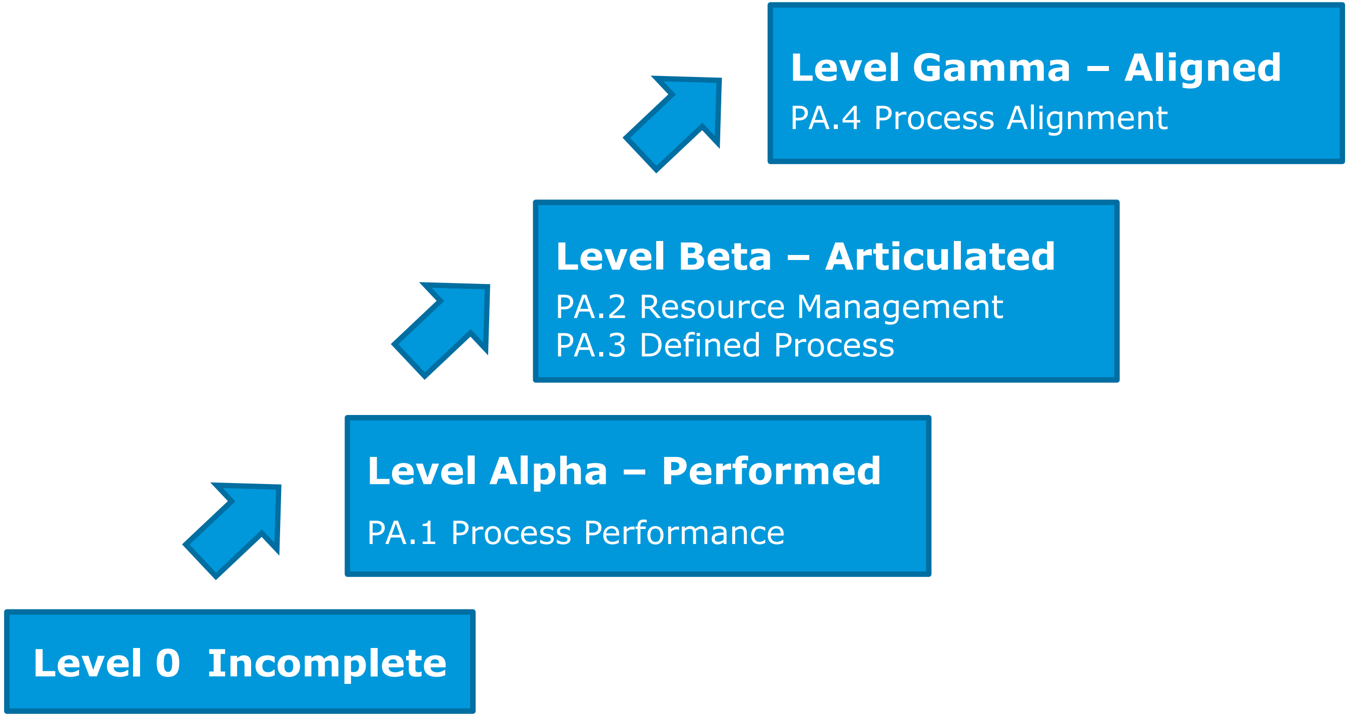
- SUP.1 Quality assurance (ECSS-Q-HB-80-02)
- SUP.2 Verification (ECSS-Q-HB-80-02)
- SUP.8 Configuration management (ECSS-Q-HB-80-02)
- SUP.9 Problem resolution management (ECSS-Q-HB-80-02)
- SUP.11 Safety and dependability assurance (ECSS-Q-HB-80-02)

Organizational processes

Organizational processes

- OM Organizational Management (ISO/IEC 29110)
- RM Resource Management (ISO/IEC 29110)
- PSM Process Management (ISO/IEC 29110)
- PPM Project Portfolio Management (ISO/IEC 29110)

ISO/IEC 29110-6-1 – Capability Dimension



Level Gamma – Aligned

PA.4 Process Alignment

Level Beta – Articulated

PA.2 Resource Management
PA.3 Defined Process

Level Alpha – Performed

PA.1 Process Performance

Level 0 Incomplete

Cybersecurity (I)

- Our missions and infrastructure must be resilient to cyber attacks
- This applies to the ground segment, space segment, software, hardware and data
- Cyber resilience must be ensured across the full supply chain

Cybersecurity (II)

- Cyber resilience is both a corporate and a project concern
- Corporate: policies, awareness, digital and physical security
- Project: top-down system approach, threat analysis, processes, secure coding, encryption, authenticity of COTS, certified (S)BOM, etc.

Cybersecurity (III)

- Safety and security impact each other!
  - From a security point-of-view: single-agent key distribution, single data copy, etc.
  - From safety/reliability point-of-view: Single-Point Failure!!
  - Radiation can impact encryption keys
  - and so on…

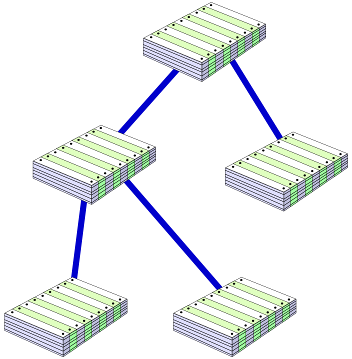
Cybersecurity (IV)

- Key-contributors to cyber security weaknesses in SW:
  - Poor source code maintainability
  - Technical debt
  - No static analysis (in toolchain)
  - Security not considered and integrated in the development life cycle from the start
  - One-dimensional strategy (e.g. considering only penetration resistance)
  - Compromises due to schedule or cost constraints

    ➔ Attacks happen on poor implementation of a good design!

Configuration Management (I)

- Configuration management is a Management discipline, addressed by ECSS-M-ST-40
  - PA should *only* provide support, but…
- A proper configuration management is key to the success of any software development and operations project



Configuration management is the process for establishing and maintaining a consistent record of a product’s functional and physical characteristics compared to its design and operational requirements

[ECSS-M-ST-40C]

Configuration Management (II)

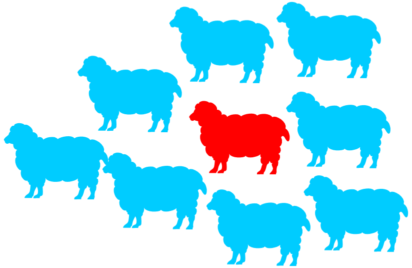
- Configuration management comprises:
  - Configuration identification
  - Change control
  - Configuration status accounting
  - Configuration verification and auditing
- Configuration changes are managed by a Configuration Control Board
  - At all project levels
- The CCB manages:
  - Change Requests and Change Proposals
  - Requests for Deviation and Requests for Waiver

Configuration Management (III)

- Specific CM aspects related to software:
  - It shall be possible to re-generate any software reference versions from back-ups
  - Procedures for branching and merging shall be defined
  - PA shall verify that only authorized changes are implemented in accordance with the CM plan
  - Methods and tools to protect software against corruption shall be identified and applied
  - A checksum-type key calculation shall be used for the delivered operational software

Nonconformances

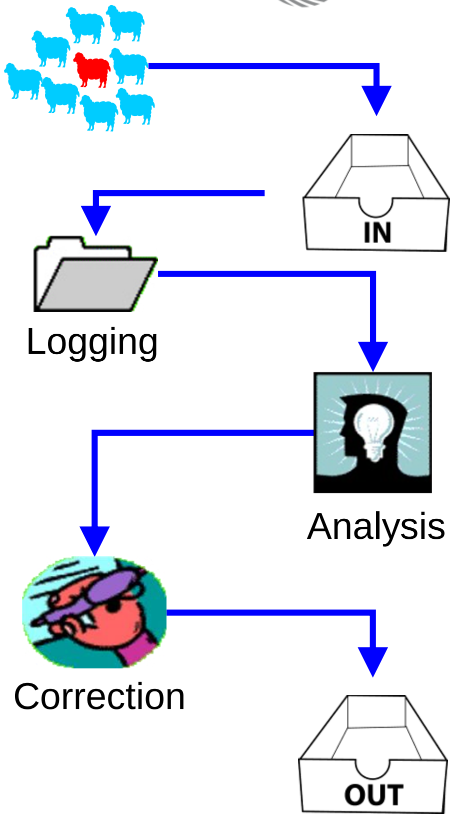
- Nonconformance = "non-fulfilment of a requirement"$_{\text{ECSS-S-ST-00-01}}$
- ECSS-Q-ST-10-09 defines requirements for nonconformance handling
  - System level
- Software suppliers are required to implement a nonconformance control system compliant with Q-10-09



- Software engineering and software product assurance are to be included in Nonconformance Review Boards
- The point in time, within the software life cycle, when the NCR procedure applies shall be specified

Software Problems

- Procedures shall be defined for the logging, analysis and correction of software problems
- SPRs shall contain sufficient information for their handling, even after long time
  - SW Item ID, problem description, recommended solution, final disposition, modifications implemented, test (re)-executed; anything else?
- The interface with the nonconformance control system shall be defined
  - I.e. the circumstances under which a software problem qualifies as a nonconformance



Alerts

> Formal notification to users, informing them of failures or nonconformance of items, already released for use or not, which could also be present on other items already delivered [e.g. items with identical design concept, materials, components or processes]
>
> "ECSS-S-ST-00-01

- Software suppliers are required to participate in the alert system organized by the customer (or other sources)
  - Notify customer about issues that could result in alerts
  - Investigate issues and recommend corrective actions for similar items
  - Assess incoming alerts for impact on the current project; identify and apply corrective actions
  - Distribute incoming alert information to possibly affected users within the project

ESA SW PA Workshop 2021

- Fully online event
- October 4 – 7, 2021
- 1 ECSS Training Day, 3 Workshop Days
- ECSS Training:
  - ✓ E-40: Software Engineering, including summary of upcoming changes
  - ✓ Q-80: Software Product Assurance
  - ✓ Agile methods

ESA SW PA Workshop 2021

- Workshop Topics:
  - ✓ Artificial Intelligence, Machine Learning and autonomy
  - ✓ Agile methods, including SAFe
  - ✓ Cybersecurity
  - ✓ Quantum technologies
  - ✓ SmallSats and CubeSats
  - ✓ FPGA development
  - ✓ SW PA
  - ✓ SW Engineering
  - ✓ …

ESA SW PA Workshop 2021

- Registration is **now open**
- Abstract Submission **until June 21**
- Workshop website: https://atpi.eventsair.com/software-pa-ws/

Disclaimer

This presentation is a property of the European Space Agency (ESA) or ESA's licensors. No part of this material may be reproduced, displayed, amended, distributed or otherwise used in any form or by any means, without written permission of ESA or ESA's licensors. Any unauthorised activity or use shall be an infringement of ESA's or ESA licensors' intellectual property rights and ESA reserves the right to defend its rights and interests, including to seek for remedies.