Product/Quality Assurance, verification, validation

David Berghmans
Acting PA/QA responsible for P3SC development at ROB

PROBA-3 SOC development is

- an ESA/PRODEX funded activity
- a part of the PROBA-3 Ground Segment
- subject to ESA reviewing (SRR, PDR, CDR, QAR)

ECSS[*] standards apply

[*] European Cooperation for Space Standardisation


ECSS-Q-ST-80C Rev.1
15 February 2017

EUROPEAN COOPERATION
ECSS
FOR SPACE STANDARDIZATION

Space product assurance

Software product assurance

ECSS Secretariat
ESA-ESTEC
Requirements & Standards Division
Noordwijk, The Netherlands

PROBA-3 SOC is not mission critical
&
Resources are scarce

“Tailoring” of PA/QA requirements ongoing

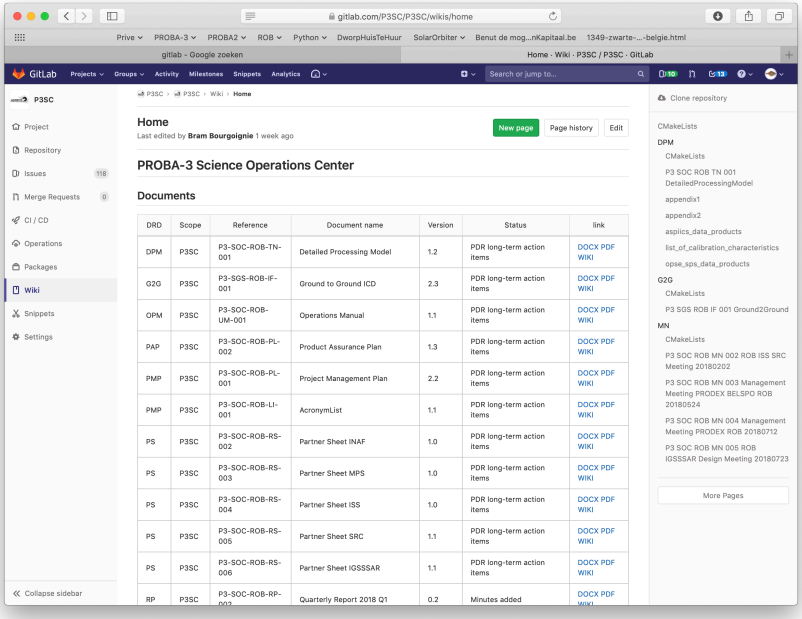
Some PA/QA related processes

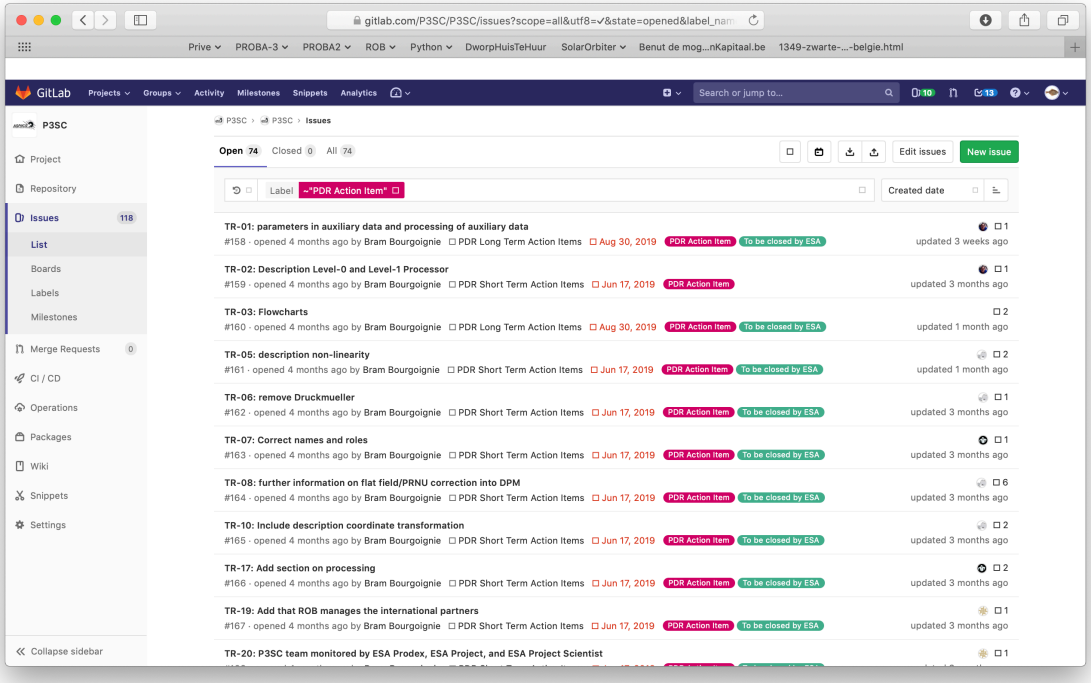
- configuration management
- document handling
- risk registry
- verification/validation

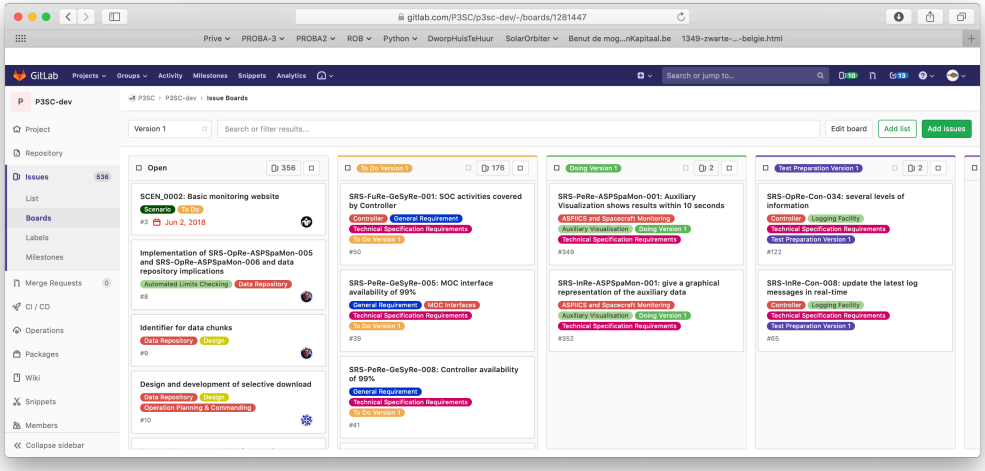
ROB PA/QA overview does not look into internal processes of partners

[*] European Cooperation for Space Standardisation

Configuration Management

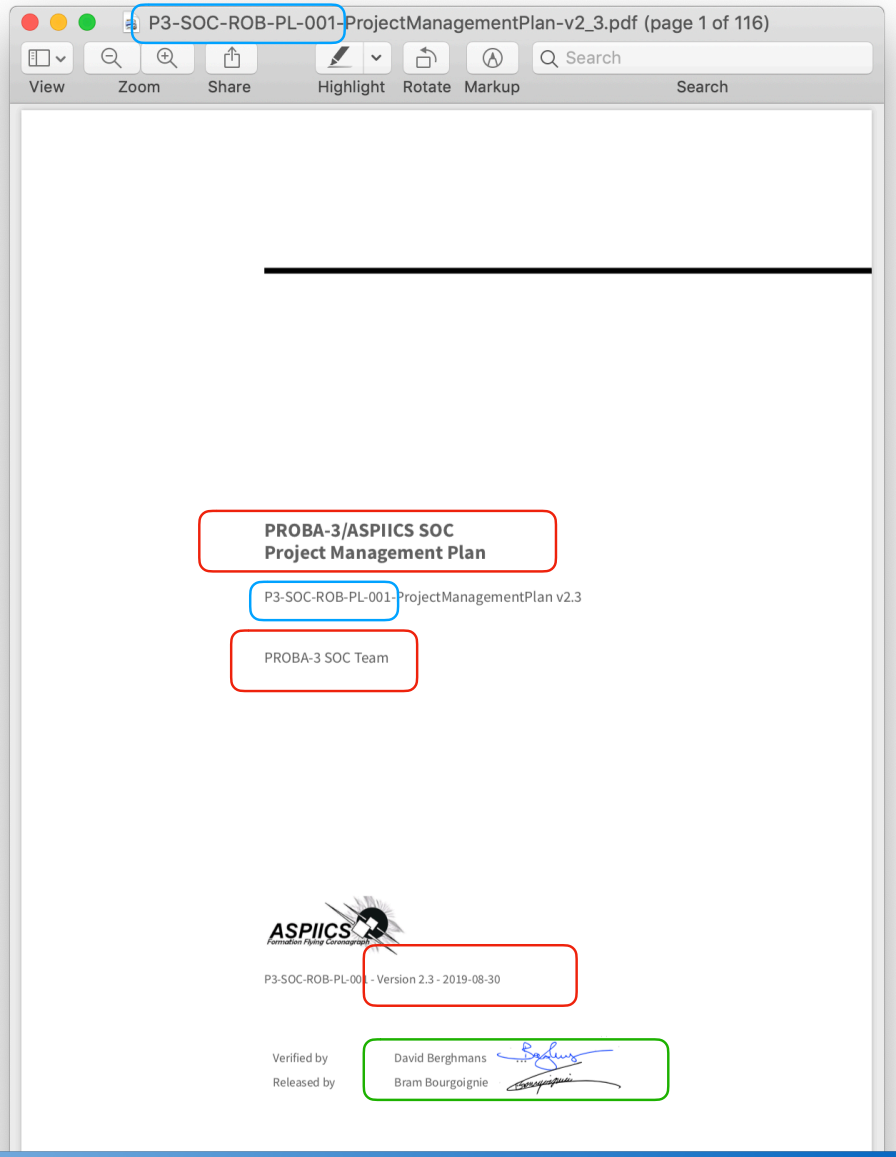






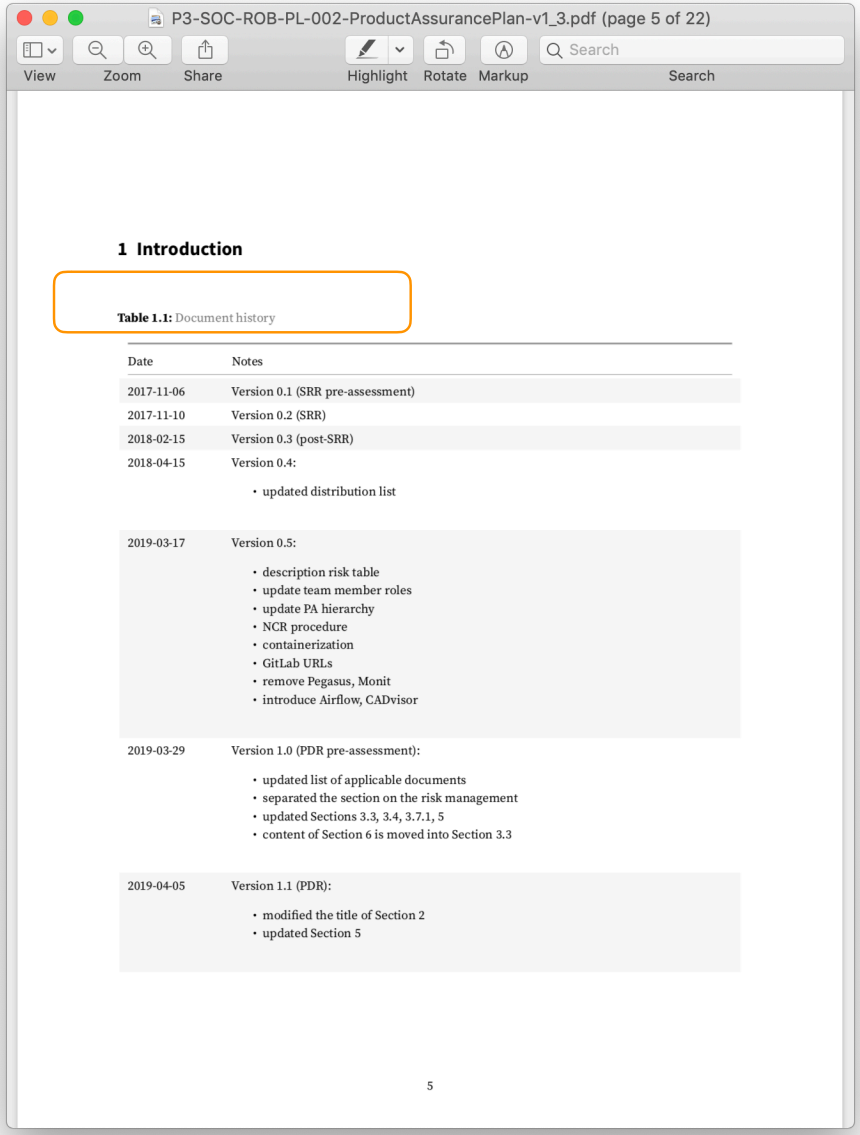
Document Handling

- file-name starts with a formatted document code
  P3-SOC-[institute]-[type]-[number]-[title]-v[version]
- front page with title, author, version & date
- a release document cannot be “draft”
- review documents have to signed
-



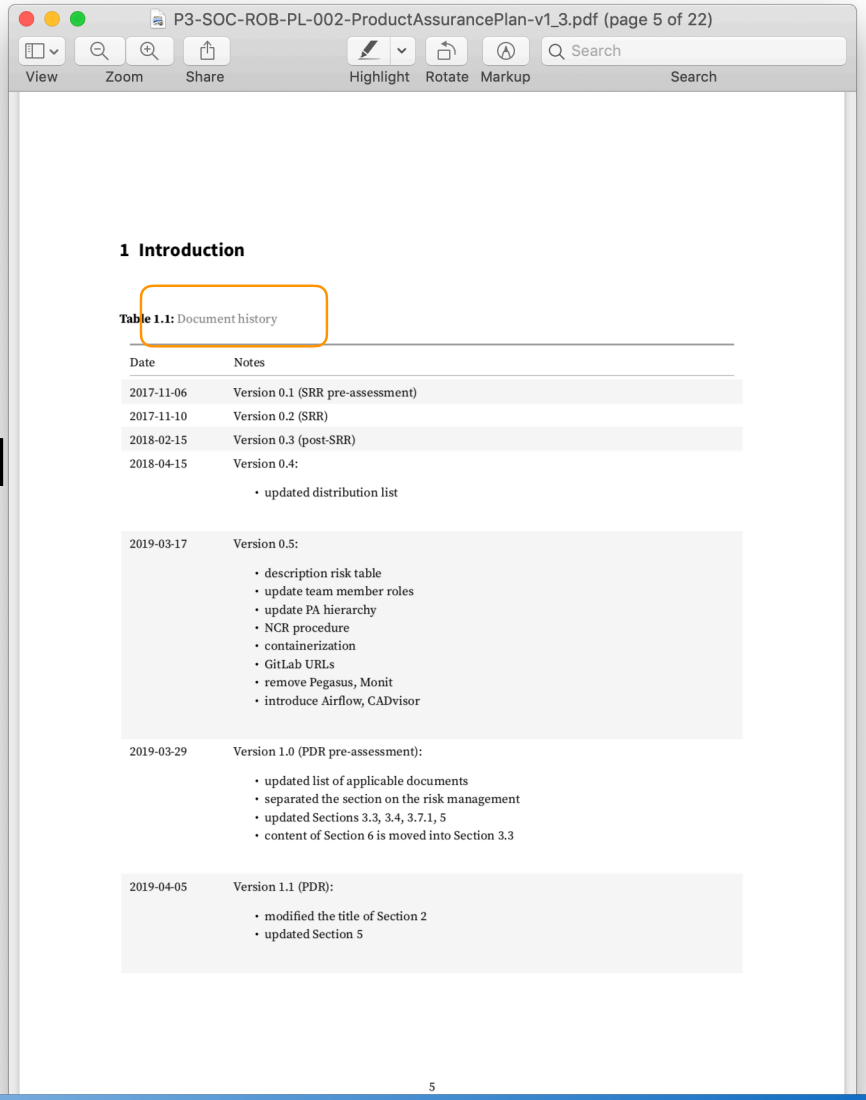
Document Handling

- file-name starts with a formatted document code
  P3-SOC-[institute]-[type]-[number]-[title]-v[version]
- front page with title, author, version & date
- a release document cannot be “draft”
- review documents have to signed
- detailed document history



Project Documents

- file-name starts with a formatted document code
  P3-SOC-[institute]-[type]-[number]-[title]-v[version]
- front page with title, author, version & date
- a release document cannot be “draft”
- review documents have to signed
- detailed document history


P3-SOC-ROB-PL-002-ProductAssurancePlan-v1_3.pdf (page 5 of 22)

View Zoom Share Highlight Rotate Markup Search

1 Introduction

Table 1.1: Document history

Date	Notes
2017-11-06	Version 0.1 (SRR pre-assessment)
2017-11-10	Version 0.2 (SRR)
2018-02-15	Version 0.3 (post-SRR)
2018-04-15	Version 0.4: • updated distribution list
2019-03-17	Version 0.5: • description risk table • update team member roles • update PA hierarchy • NCR procedure • containerization • GitLab URLs • remove Pegasus, Monit • introduce Airflow, CADvisor
2019-03-29	Version 1.0 (PDR pre-assessment): • updated list of applicable documents • separated the section on the risk management • updated Sections 3.3, 3.4, 3.7.1, 5 • content of Section 6 is moved into Section 3.3
2019-04-05	Version 1.1 (PDR): • modified the title of Section 2 • updated Section 5

5

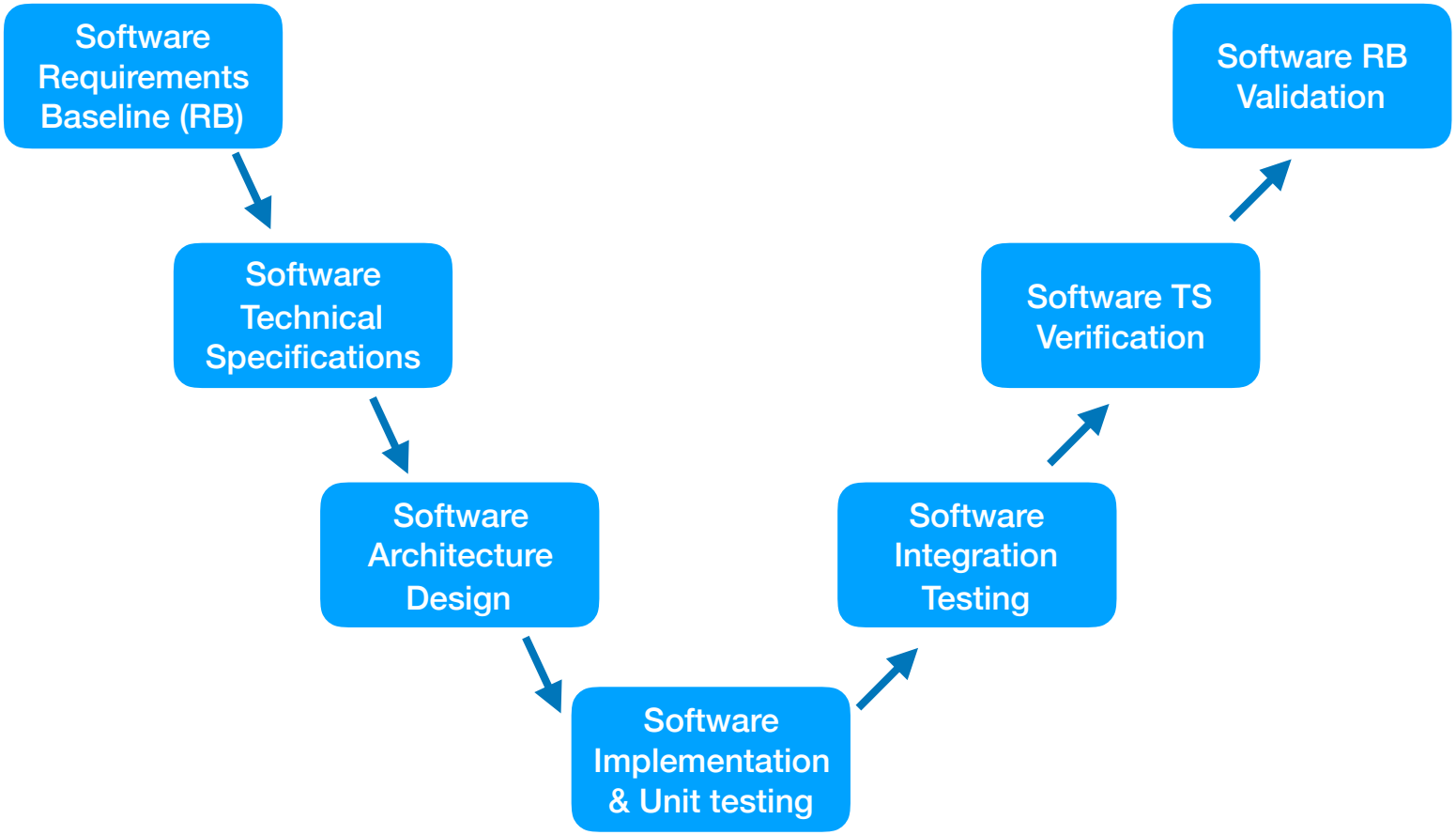
Risk register

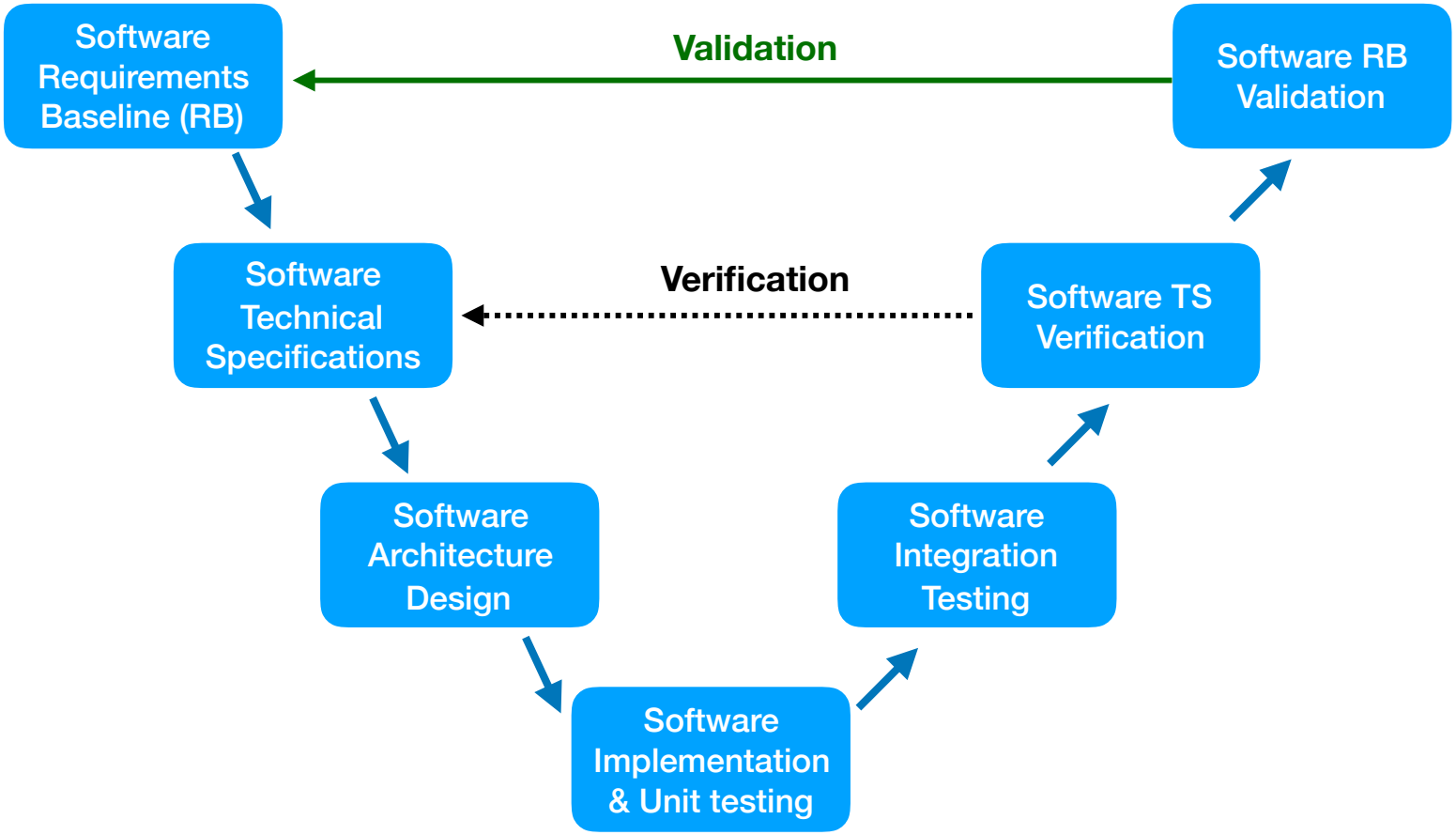
L=5: certain
L=4: probable

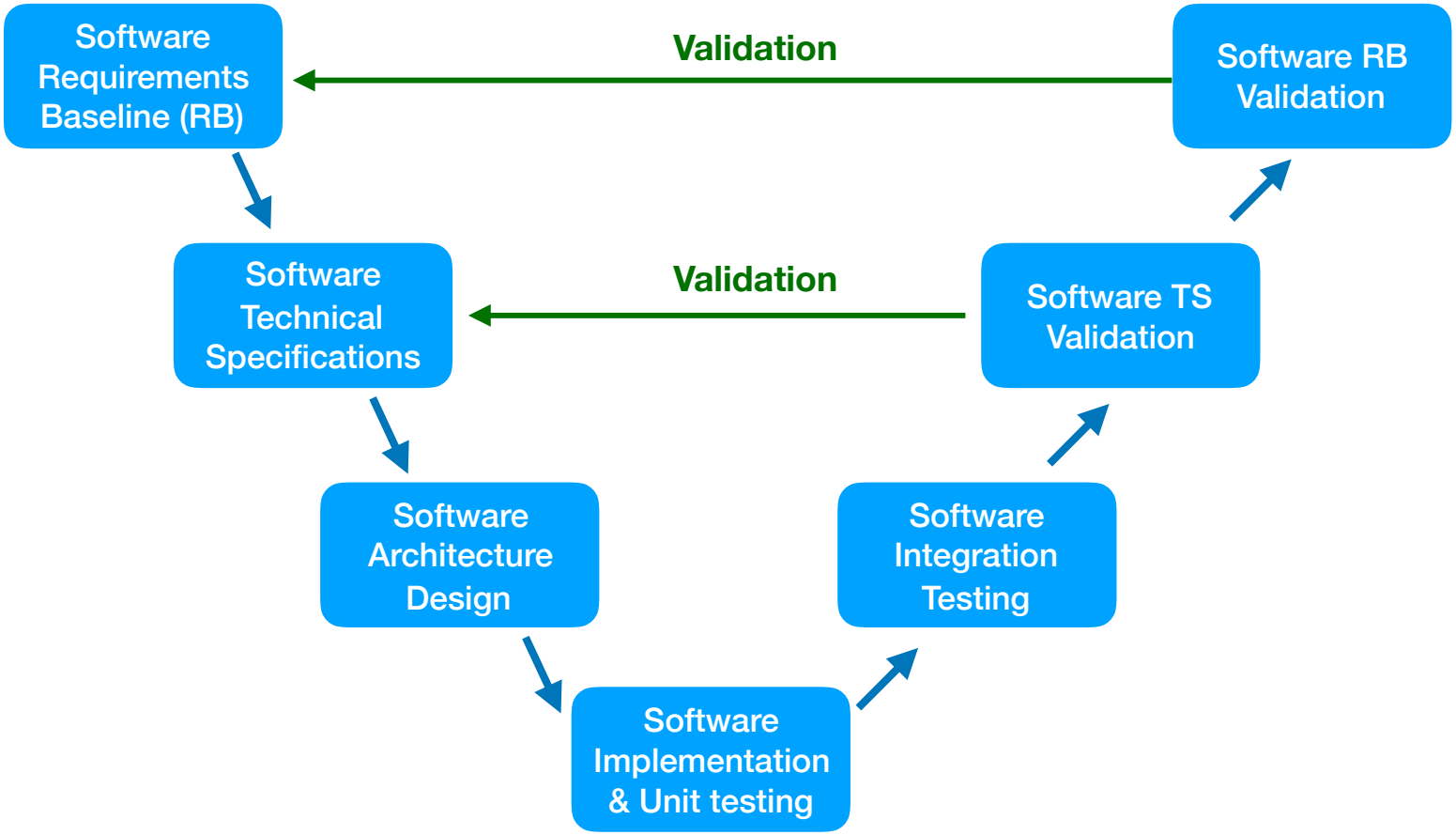
S=3: major
S=2: significant

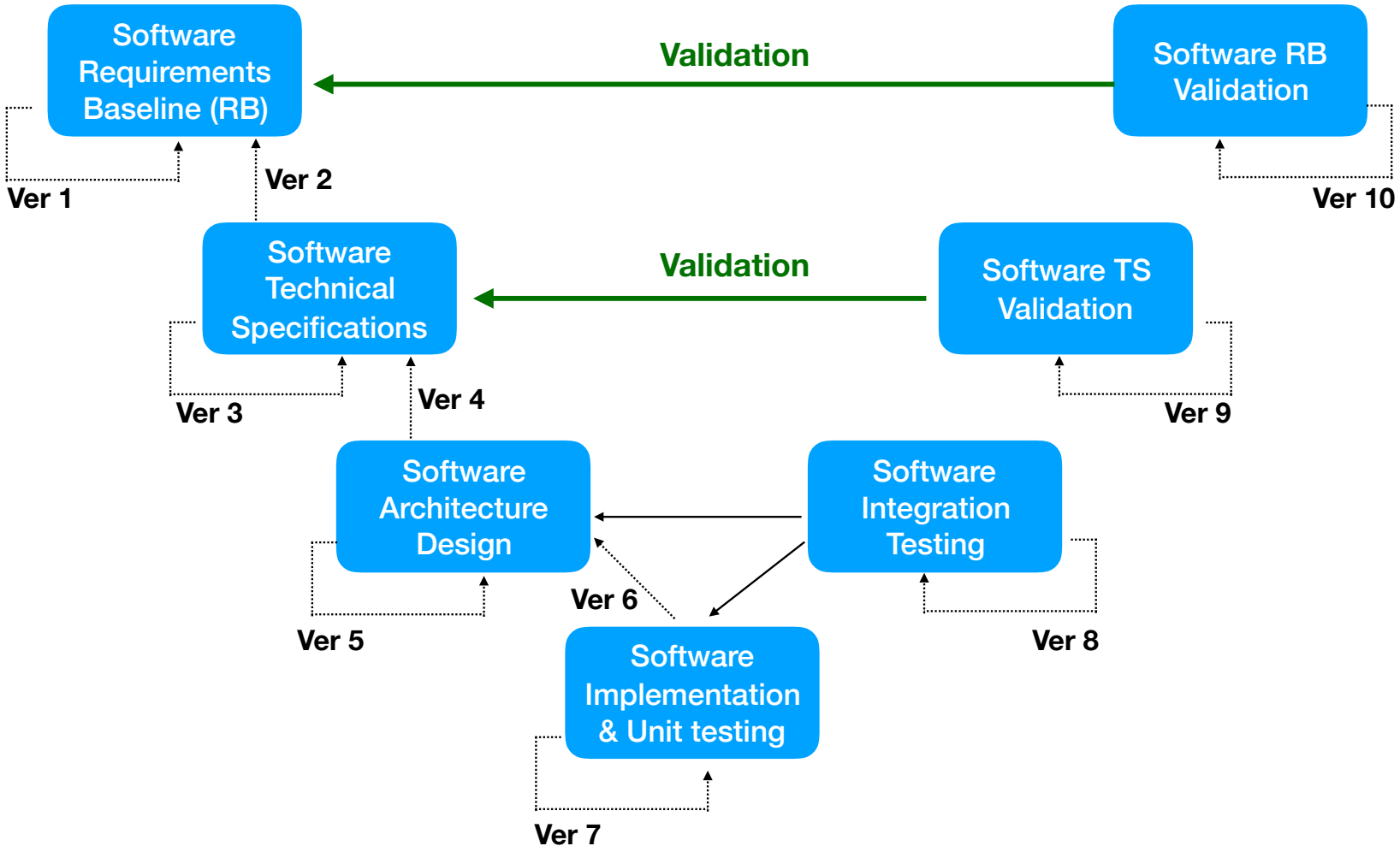
Risk ID	Risk title	Affected Subsystems	Likelihood, Severity, RI	Mitigation
R1	Remaining TBDs in MOC/SOC IRD	SOC data repository structure depends on details of interchanged data	L=2, S=3, RI=6	Develop on the basis of assumtions
R2	Delays in Project ICD	Delay in specific subsystems: Data Repository, Operations Planning & Instrument Commanding, and MOC Support Software & Products	L=4, S=3, RI=12	For the time being we can focus on other work but this is becoming increasingly hampering as planning needs to be reorganized.
R3	Developments by international partners not usable	Various partner contributions	L=3, S=2, RI=6	Enhanced monitoring develop in-house instead
R4	Unsurmountable documentation workload	Delay in all subsystems	L=5, S=3, RI=15	Focus on the actual technical work
R5	Grafana not integratable with data repository subsystem	Delay in ASPIICS and Spacecraft Monitoring System	L=2, S=2, RI=4	Add ASPIICS and spacecraft monitoring data in Prometheus
R6	MIB not available	Delay in Auxiliary Data Processors subsystem	L=2, S=1, RI=2	Manually write parsers for the auxiliary data
R7	Complexity of the Data Repository	Delay in the Data Repository subsystem	L=2, S=2, RI=4	Simplify the required functionality of the Data Repository, reduce the generalisation of the Data Repository subsystem
R8	Future evolution of used open source tools	Delay in all subsystems	L=2, S=2, RI=4	Make changes to the code of the open source tool if needed, use older version or in the worst case replace the open source tool
R9	Complexity of the interoperability of the workflows	Workflow manager	L=3, S=2, RI=6	Run the system non-optimally resulting in longer processing times
R10	Delays in planning and testing	Delay in all subsystems	L=5, S=2, RI=8	Delay documentation workload

Validation & Verification


Software Requirements Baseline (RB)
Software Technical Specifications
Software Architecture Design
Software Implementation & Unit testing
Software Integration Testing
Software TS Verification
Software RB Validation


Software Requirements Baseline (RB)
Validation
Software RB Validation
Software Technical Specifications
Verification
Software TS Verification
Software Architecture Design
Software Integration Testing
Software Implementation & Unit testing


Software Requirements Baseline (RB)
Validation
Software RB Validation
Software Technical Specifications
Validation
Software TS Validation
Software Architecture Design
Software Integration Testing
Software Implementation & Unit testing


Software Requirements Baseline (RB)
Validation
Software RB Validation
Ver 1
Ver 2
Ver 10
Software Technical Specifications
Validation
Software TS Validation
Ver 3
Ver 4
Ver 9
Software Architecture Design
Software Integration Testing
Ver 6
Ver 5
Ver 8
Software Implementation & Unit testing
Ver 7

Conclusions

- Tailoring of “ECSS Software Product Assurance” underway
- Contributed documents will be inspected for traceability
- “Verification and Validation Plan” VVP, becomes just “Validation Plan” covering both checking against RB and TS
- New document “Verification Plan”, to check completeness and correctness of information flows between development cycles