ECSS: Friend or Foe?

ECSS from Space to Ground

Andrea Balestra – INAF@OAPd

What’s in here

An overview of ECSS

Bridging Space to Ground

A possible Way Forward

ECSS What…

- The European Cooperation for Space Standardization is an initiative established to develop a coherent, single set of user-friendly standards for use in all European space activities.
- Standards state what has to be done, not how (e.g. they do not tell you the coding standard to use).
- ECSS applies to space projects, either from ESA or any Space Agency, and also to space-related research projects. It does not apply, in principle, to not-space projects

… and Why?

- There were ESA standards before (i.e. PSS):
- Software had a well-developed set of standards, with its renown (?) PSS-05-0.
- But these standards were not coordinated: Different concepts, approaches and terminology.
- There were also different standards in place (CNES, DLR, etc.).
- A standard was needed for the total system:
- Homogeneity was sought across Space Organizations (Agencies, Industry). How? Seeking compliance with internationally recognized standards (e.g. ISO/IEC 12207 for software).

How is ECSS organized?

ECSS has four major Branches (or Series):

- ECSS-M: Space Project Management
  - Policy and principles to provide a uniform approach to a number of generic, managerial disciplines.
- ECSS-E: Space Engineering
  - Policy and principles addressing a broad range of key Space engineering disciplines.
- ECSS-Q: Space Product Assurance
  - Policy and general principles (QA, Safety, and RAM), and specific disciplines (SW, materials, etc.).
- ECSS-U: Space Sustainability
  - Policy and principles governing planetary and space protection.

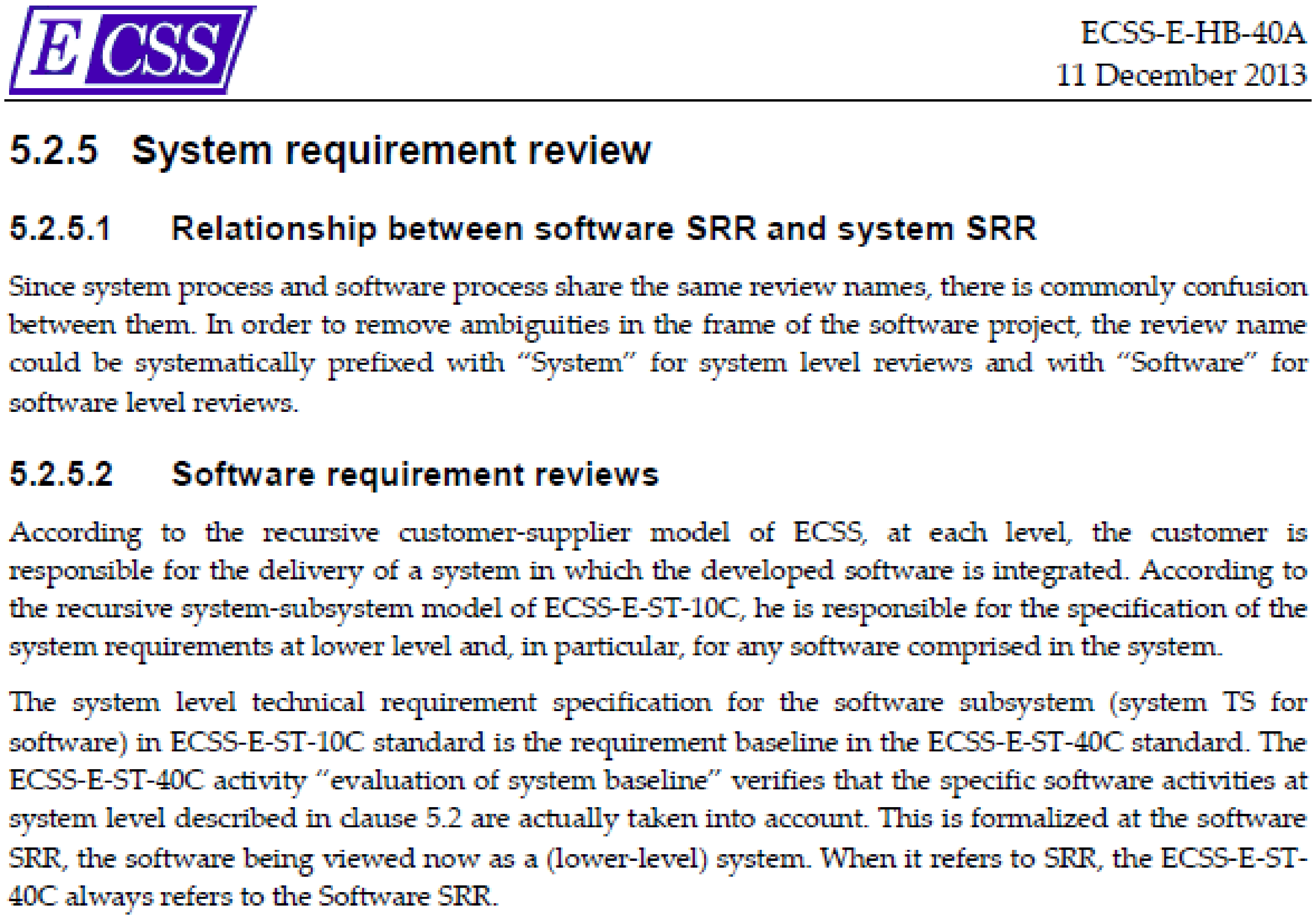
ECSS document types

- There are three types of ECSS documents:
- Standards (ST)
- Handbooks (HB)
- Technical Memoranda (TM)

ECSS Handbooks

- The Handbooks are non-normative documents. They provide background information, orientation, advice, or recommendations:
  - Advice on how to do something, and useful information about a subject.
  - Related to one specific discipline, technique, technology, process, or activity.
  - Contain the best knowledge and practices on the subject.
  - They do not contain requirements. They are usually considered reference documents.
  - However, a Customer may transform them to normative (on project basis).
- E.g.
  - ECSS-E-HB-32-26A: Spacecraft mechanical loads analysis handbook
  - ECSS-E-HB-40A: Software engineering handbook

Handbook example



ECSS-E-HB-40A
11 December 2013

5.2.5 System requirement review

5.2.5.1 Relationship between software SRR and system SRR

Since system process and software process share the same review names, there is commonly confusion between them. In order to remove ambiguities in the frame of the software project, the review name could be systematically prefixed with "System" for system level reviews and with "Software" for software level reviews.

5.2.5.2 Software requirement reviews

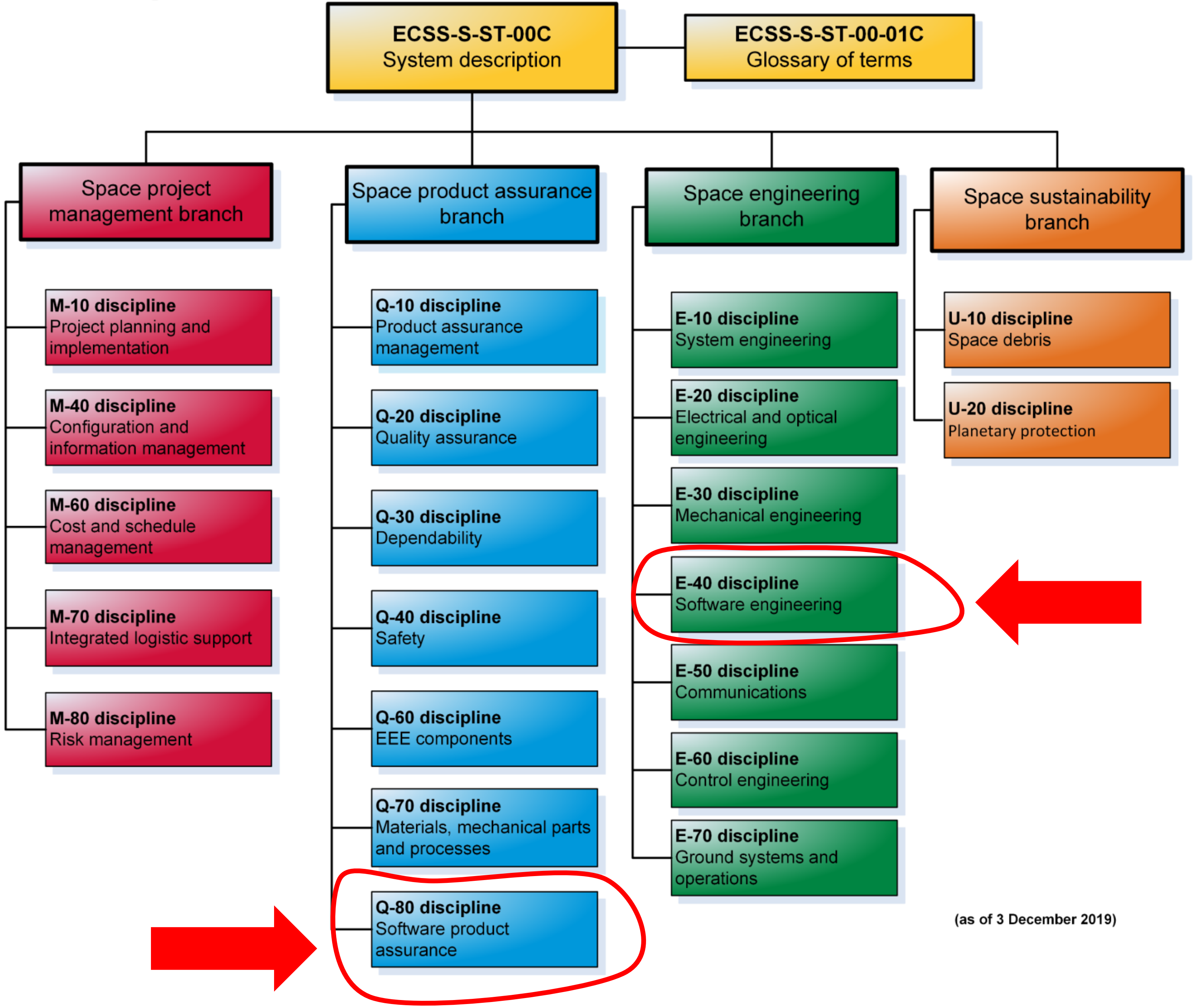
According to the recursive customer-supplier model of ECSS, at each level, the customer is responsible for the delivery of a system in which the developed software is integrated. According to the recursive system-subsystem model of ECSS-E-ST-10C, he is responsible for the specification of the system requirements at lower level and, in particular, for any software comprised in the system.

The system level technical requirement specification for the software subsystem (system TS for software) in ECSS-E-ST-10C standard is the requirement baseline in the ECSS-E-ST-40C standard. The ECSS-E-ST-40C activity "evaluation of system baseline" verifies that the specific software activities at system level described in clause 5.2 are actually taken into account. This is formalized at the software SRR, the software being viewed now as a (lower-level) system. When it refers to SRR, the ECSS-E-ST-40C always refers to the Software SRR.

ECCS Technical Memoranda

- ECSS Technical Memoranda:
  - Provide useful information on a specific subject.
  - May be broader in scope than Handbooks.
  - Are prepared to record and present non-normative data that are:
  - Not relevant
  - or
  - Not yet mature for being published as Standard or Handbook.
- TM’s can’t be transformed into normative.

ECSS Disciplines



ECSS-S-ST-00C
System description

ECSS-S-ST-00-01C
Glossary of terms

Space project management branch

- **M-10 discipline** Project planning and implementation
- **M-40 discipline** Configuration and information management
- **M-60 discipline** Cost and schedule management
- **M-70 discipline** Integrated logistic support
- **M-80 discipline** Risk management

Space product assurance branch

- **Q-10 discipline** Product assurance management
- **Q-20 discipline** Quality assurance
- **Q-30 discipline** Dependability
- **Q-40 discipline** Safety
- **Q-60 discipline** EEE components
- **Q-70 discipline** Materials, mechanical parts and processes
- **Q-80 discipline** Software product assurance

Space engineering branch

- **E-10 discipline** System engineering
- **E-20 discipline** Electrical and optical engineering
- **E-30 discipline** Mechanical engineering
- **E-40 discipline** Software engineering
- **E-50 discipline** Communications
- **E-60 discipline** Control engineering
- **E-70 discipline** Ground systems and operations

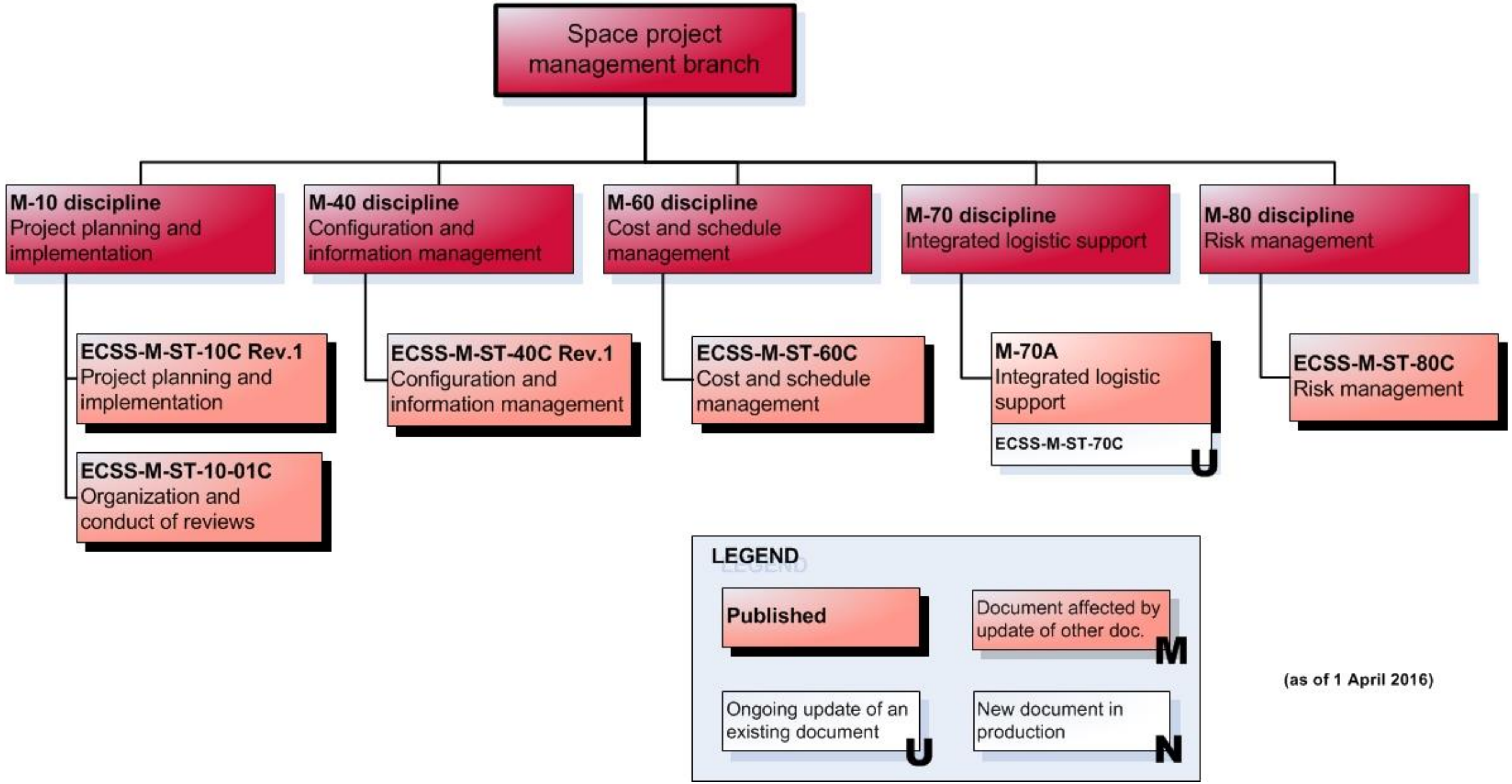
Space sustainability branch

- **U-10 discipline** Space debris
- **U-20 discipline** Planetary protection

(as of 3 December 2019)

ECSS Standards

Management branch



Space project management branch

M-10 discipline
Project planning and implementation

- **ECSS-M-ST-10C Rev.1**
  Project planning and implementation
- **ECSS-M-ST-10-01C**
  Organization and conduct of reviews

M-40 discipline
Configuration and information management

- **ECSS-M-ST-40C Rev.1**
  Configuration and information management

M-60 discipline
Cost and schedule management

- **ECSS-M-ST-60C**
  Cost and schedule management

M-70 discipline
Integrated logistic support

- **M-70A**
  Integrated logistic support
  ECSS-M-ST-70C U

M-80 discipline
Risk management

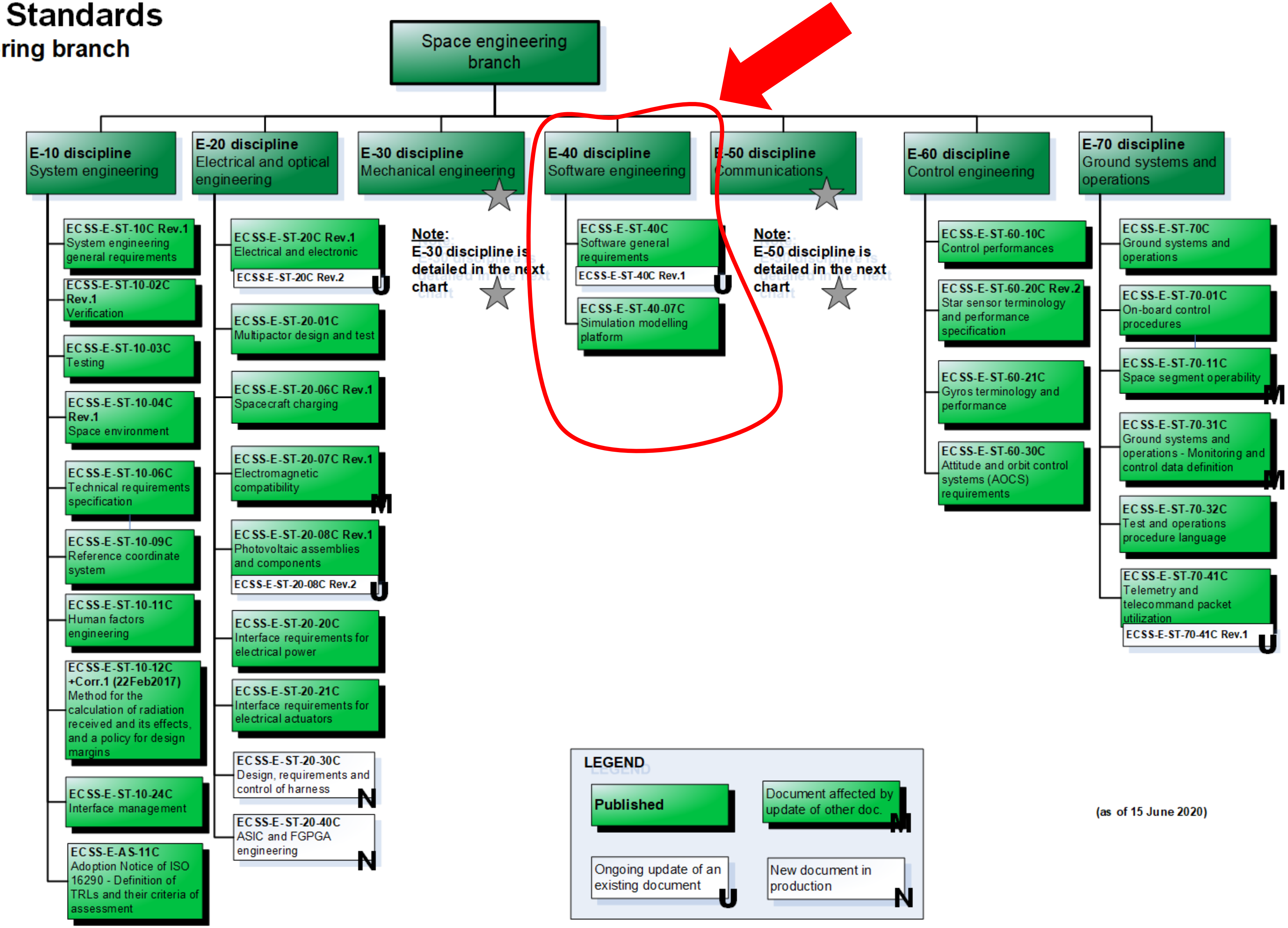
- **ECSS-M-ST-80C**
  Risk management

LEGEND

- Published
- Document affected by update of other doc. M
- Ongoing update of an existing document U
- New document in production N

(as of 1 April 2016)

ECSS Standards
Engineering branch



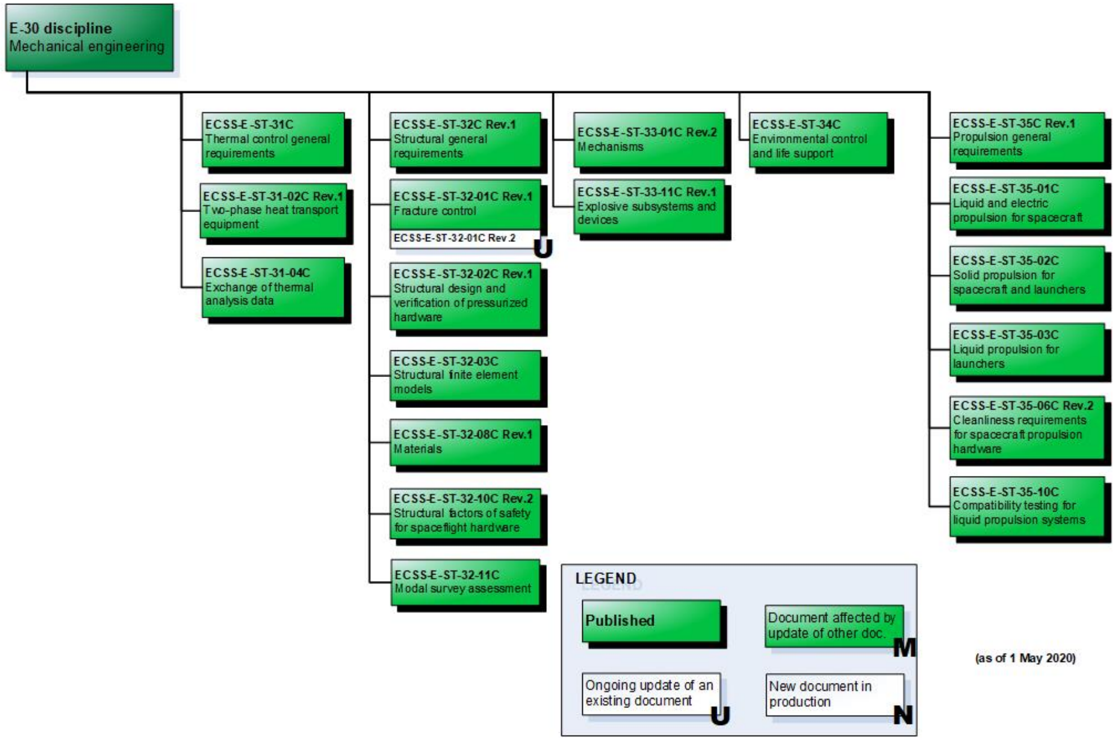
Space engineering branch

- **E-10 discipline** System engineering
  - ECSS-E-ST-10C Rev.1 System engineering general requirements
  - ECSS-E-ST-10-02C Rev.1 Verification
  - ECSS-E-ST-10-03C Testing
  - ECSS-E-ST-10-04C Rev.1 Space environment
  - ECSS-E-ST-10-06C Technical requirements specification
  - ECSS-E-ST-10-09C Reference coordinate system
  - ECSS-E-ST-10-11C Human factors engineering
  - ECSS-E-ST-10-12C +Corr.1 (22Feb2017) Method for the calculation of radiation received and its effects, and a policy for design margins
  - ECSS-E-ST-10-24C Interface management
  - ECSS-E-AS-11C Adoption Notice of ISO 16290 - Definition of TRLs and their criteria of assessment
- **E-20 discipline** Electrical and optical engineering
  - ECSS-E-ST-20C Rev.1 Electrical and electronic — ECSS-E-ST-20C Rev.2 U
  - ECSS-E-ST-20-01C Multipactor design and test
  - ECSS-E-ST-20-06C Rev.1 Spacecraft charging
  - ECSS-E-ST-20-07C Rev.1 Electromagnetic compatibility M
  - ECSS-E-ST-20-08C Rev.1 Photovoltaic assemblies and components — ECSS-E-ST-20-08C Rev.2 U
  - ECSS-E-ST-20-20C Interface requirements for electrical power
  - ECSS-E-ST-20-21C Interface requirements for electrical actuators
  - ECSS-E-ST-20-30C Design, requirements and control of harness N
  - ECSS-E-ST-20-40C ASIC and FPGA engineering N
- **E-30 discipline** Mechanical engineering ★
  - **Note**: E-30 discipline is detailed in the next chart ★
- **E-40 discipline** Software engineering
  - ECSS-E-ST-40C Software general requirements — ECSS-E-ST-40C Rev.1 U
  - ECSS-E-ST-40-07C Simulation modelling platform
- **E-50 discipline** Communications ★
  - **Note**: E-50 discipline is detailed in the next chart ★
- **E-60 discipline** Control engineering
  - ECSS-E-ST-60-10C Control performances
  - ECSS-E-ST-60-20C Rev.2 Star sensor terminology and performance specification
  - ECSS-E-ST-60-21C Gyros terminology and performance
  - ECSS-E-ST-60-30C Attitude and orbit control systems (AOCS) requirements
- **E-70 discipline** Ground systems and operations
  - ECSS-E-ST-70C Ground systems and operations
  - ECSS-E-ST-70-01C On-board control procedures
  - ECSS-E-ST-70-11C Space segment operability M
  - ECSS-E-ST-70-31C Ground systems and operations - Monitoring and control data definition M
  - ECSS-E-ST-70-32C Test and operations procedure language
  - ECSS-E-ST-70-41C Telemetry and telecommand packet utilization — ECSS-E-ST-70-41C Rev.1 U

LEGEND

🟩 Published	🟩 Document affected by update of other doc. M
Ongoing update of an existing document U	New document in production N

(as of 15 June 2020)



E-30 discipline
Mechanical engineering

- **ECSS-E-ST-31C** Thermal control general requirements
- **ECSS-E-ST-31-02C Rev.1** Two-phase heat transport equipment
- **ECSS-E-ST-31-04C** Exchange of thermal analysis data

- **ECSS-E-ST-32C Rev.1** Structural general requirements
- **ECSS-E-ST-32-01C Rev.1** Fracture control
  ECSS-E-ST-32-01C Rev.2 U
- **ECSS-E-ST-32-02C Rev.1** Structural design and verification of pressurized hardware
- **ECSS-E-ST-32-03C** Structural finite element models
- **ECSS-E-ST-32-08C Rev.1** Materials
- **ECSS-E-ST-32-10C Rev.2** Structural factors of safety for spaceflight hardware
- **ECSS-E-ST-32-11C** Modal survey assessment

- **ECSS-E-ST-33-01C Rev.2** Mechanisms
- **ECSS-E-ST-33-11C Rev.1** Explosive subsystems and devices

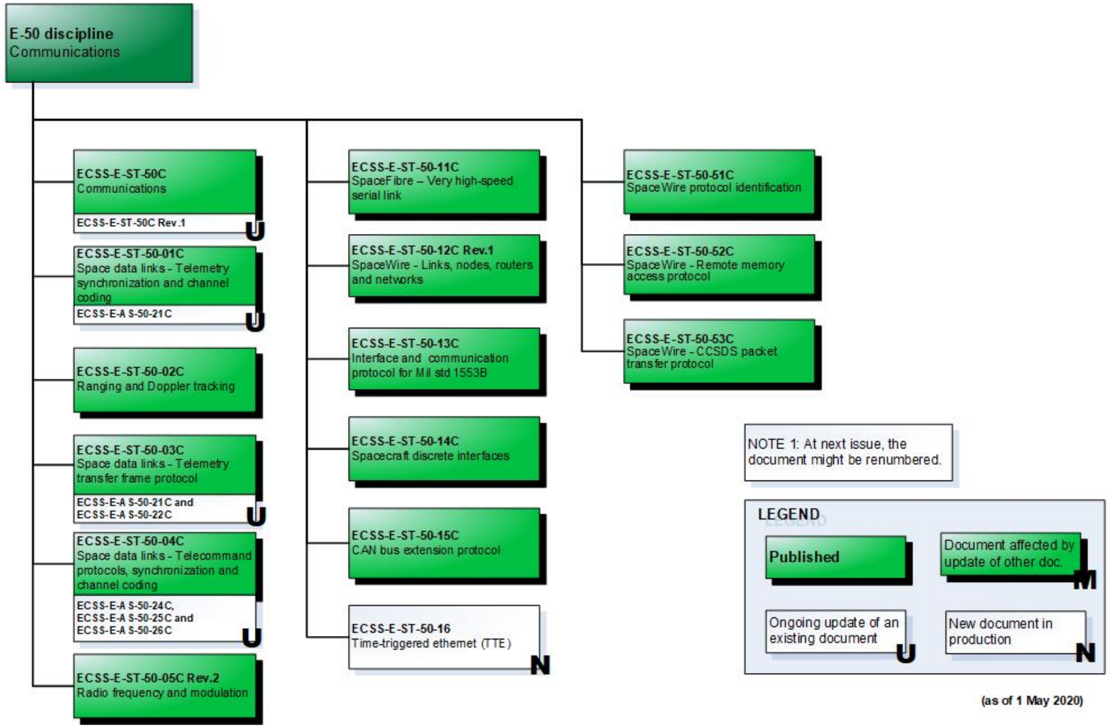
- **ECSS-E-ST-34C** Environmental control and life support

- **ECSS-E-ST-35C Rev.1** Propulsion general requirements
- **ECSS-E-ST-35-01C** Liquid and electric propulsion for spacecraft
- **ECSS-E-ST-35-02C** Solid propulsion for spacecraft and launchers
- **ECSS-E-ST-35-03C** Liquid propulsion for launchers
- **ECSS-E-ST-35-06C Rev.2** Cleanliness requirements for spacecraft propulsion hardware
- **ECSS-E-ST-35-10C** Compatibility testing for liquid propulsion systems

LEGEND

- 🟩 **Published**
- Document affected by update of other doc. M
- Ongoing update of an existing document U
- New document in production N

(as of 1 May 2020)



E-50 discipline
Communications

- **ECSS-E-ST-50C** Communications
  ECSS-E-ST-50C Rev.1 U
- **ECSS-E-ST-50-01C** Space data links - Telemetry synchronization and channel coding
  ECSS-E-AS-50-21C U
- **ECSS-E-ST-50-02C** Ranging and Doppler tracking
- **ECSS-E-ST-50-03C** Space data links - Telemetry transfer frame protocol
  ECSS-E-AS-50-21C and ECSS-E-AS-50-22C U
- **ECSS-E-ST-50-04C** Space data links - Telecommand protocols, synchronization and channel coding
  ECSS-E-AS-50-24C, ECSS-E-AS-50-25C and ECSS-E-AS-50-26C U
- **ECSS-E-ST-50-05C Rev.2** Radio frequency and modulation

- **ECSS-E-ST-50-11C** SpaceFibre – Very high-speed serial link
- **ECSS-E-ST-50-12C Rev.1** SpaceWire - Links, nodes, routers and networks
- **ECSS-E-ST-50-13C** Interface and communication protocol for Mil std 1553B
- **ECSS-E-ST-50-14C** Spacecraft discrete interfaces
- **ECSS-E-ST-50-15C** CAN bus extension protocol
- **ECSS-E-ST-50-16** Time-triggered ethernet (TTE) N

- **ECSS-E-ST-50-51C** SpaceWire protocol identification
- **ECSS-E-ST-50-52C** SpaceWire - Remote memory access protocol
- **ECSS-E-ST-50-53C** SpaceWire - CCSDS packet transfer protocol

NOTE 1: At next issue, the document might be renumbered.

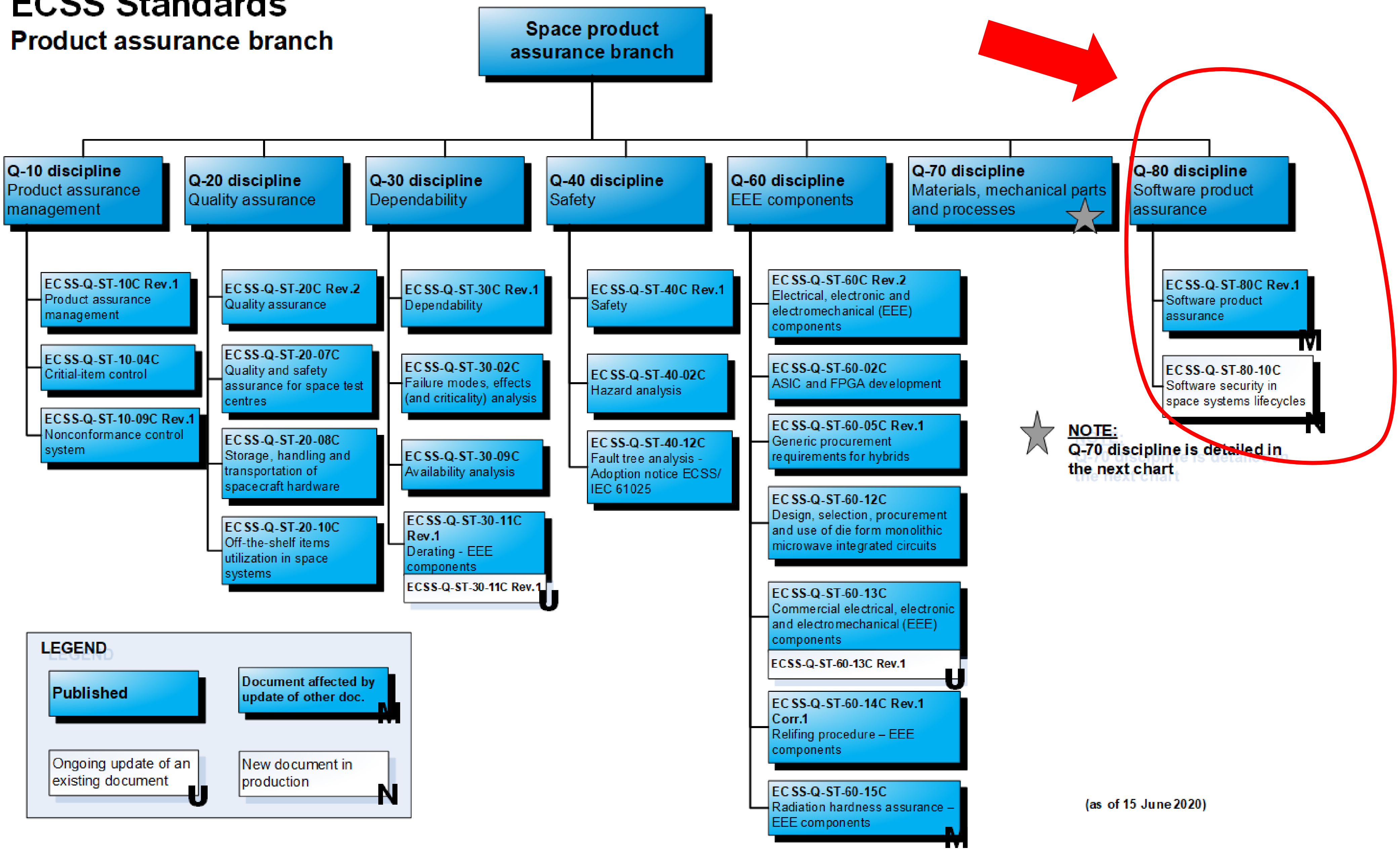
LEGEND

- 🟩 **Published**
- Document affected by update of other doc. M
- Ongoing update of an existing document U
- New document in production N

(as of 1 May 2020)

ECSS Standards

Product assurance branch



Space product assurance branch

Q-10 discipline Product assurance management
- ECSS-Q-ST-10C Rev.1 Product assurance management
- ECSS-Q-ST-10-04C Critial-item control
- ECSS-Q-ST-10-09C Rev.1 Nonconformance control system

Q-20 discipline Quality assurance
- ECSS-Q-ST-20C Rev.2 Quality assurance
- ECSS-Q-ST-20-07C Quality and safety assurance for space test centres
- ECSS-Q-ST-20-08C Storage, handling and transportation of spacecraft hardware
- ECSS-Q-ST-20-10C Off-the-shelf items utilization in space systems

Q-30 discipline Dependability
- ECSS-Q-ST-30C Rev.1 Dependability
- ECSS-Q-ST-30-02C Failure modes, effects (and criticality) analysis
- ECSS-Q-ST-30-09C Availability analysis
- ECSS-Q-ST-30-11C Rev.1 Derating - EEE components
- ECSS-Q-ST-30-11C Rev.1 U

Q-40 discipline Safety
- ECSS-Q-ST-40C Rev.1 Safety
- ECSS-Q-ST-40-02C Hazard analysis
- ECSS-Q-ST-40-12C Fault tree analysis - Adoption notice ECSS/ IEC 61025

Q-60 discipline EEE components
- ECSS-Q-ST-60C Rev.2 Electrical, electronic and electromechanical (EEE) components
- ECSS-Q-ST-60-02C ASIC and FPGA development
- ECSS-Q-ST-60-05C Rev.1 Generic procurement requirements for hybrids
- ECSS-Q-ST-60-12C Design, selection, procurement and use of die form monolithic microwave integrated circuits
- ECSS-Q-ST-60-13C Commercial electrical, electronic and electromechanical (EEE) components
- ECSS-Q-ST-60-13C Rev.1 U
- ECSS-Q-ST-60-14C Rev.1 Corr.1 Relifing procedure – EEE components
- ECSS-Q-ST-60-15C Radiation hardness assurance – EEE components M

Q-70 discipline Materials, mechanical parts and processes ★

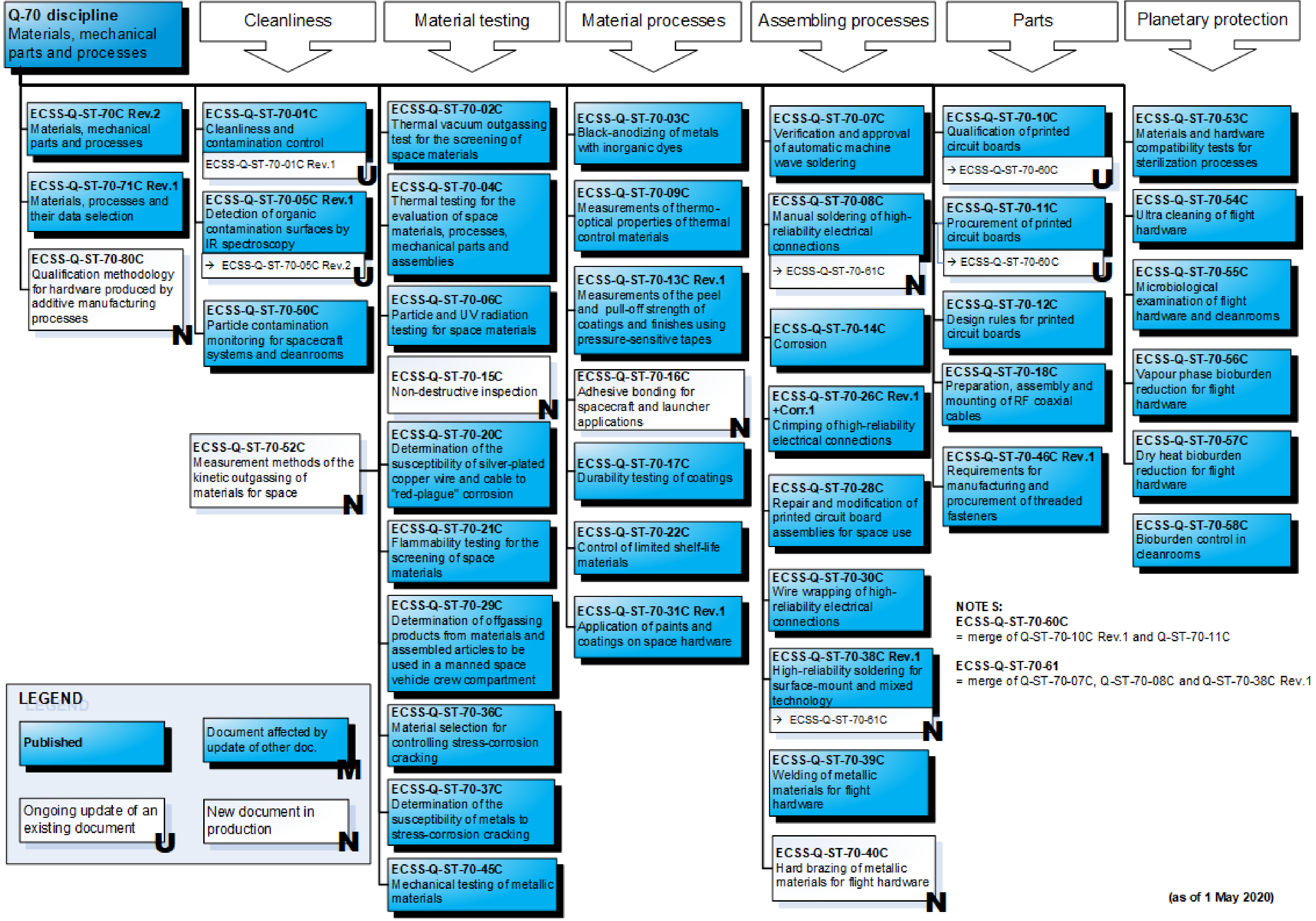
Q-80 discipline Software product assurance
- ECSS-Q-ST-80C Rev.1 Software product assurance M
- ECSS-Q-ST-80-10C Software security in space systems lifecycles N

★ **NOTE:**
Q-70 discipline is detailed in the next chart

LEGEND

Published	**Document affected by update of other doc.** M
Ongoing update of an existing document U	New document in production N

(as of 15 June 2020)



Q-70 discipline
Materials, mechanical parts and processes

- **ECSS-Q-ST-70C Rev.2** Materials, mechanical parts and processes
- **ECSS-Q-ST-70-71C Rev.1** Materials, processes and their data selection
- **ECSS-Q-ST-70-80C** Qualification methodology for hardware produced by additive manufacturing processes N

Cleanliness

- **ECSS-Q-ST-70-01C** Cleanliness and contamination control → ECSS-Q-ST-70-01C Rev.1 U
- **ECSS-Q-ST-70-05C Rev.1** Detection of organic contamination surfaces by IR spectroscopy → ECSS-Q-ST-70-05C Rev.2 U
- **ECSS-Q-ST-70-50C** Particle contamination monitoring for spacecraft systems and cleanrooms
- **ECSS-Q-ST-70-52C** Measurement methods of the kinetic outgassing of materials for space N

Material testing

- **ECSS-Q-ST-70-02C** Thermal vacuum outgassing test for the screening of space materials
- **ECSS-Q-ST-70-04C** Thermal testing for the evaluation of space materials, processes, mechanical parts and assemblies
- **ECSS-Q-ST-70-06C** Particle and UV radiation testing for space materials
- **ECSS-Q-ST-70-15C** Non-destructive inspection N
- **ECSS-Q-ST-70-20C** Determination of the susceptibility of silver-plated copper wire and cable to "red-plague" corrosion
- **ECSS-Q-ST-70-21C** Flammability testing for the screening of space materials
- **ECSS-Q-ST-70-29C** Determination of offgassing products from materials and assembled articles to be used in a manned space vehicle crew compartment
- **ECSS-Q-ST-70-36C** Material selection for controlling stress-corrosion cracking
- **ECSS-Q-ST-70-37C** Determination of the susceptibility of metals to stress-corrosion cracking
- **ECSS-Q-ST-70-45C** Mechanical testing of metallic materials

Material processes

- **ECSS-Q-ST-70-03C** Black-anodizing of metals with inorganic dyes
- **ECSS-Q-ST-70-09C** Measurements of thermo-optical properties of thermal control materials
- **ECSS-Q-ST-70-13C Rev.1** Measurements of the peel and pull-off strength of coatings and finishes using pressure-sensitive tapes
- **ECSS-Q-ST-70-16C** Adhesive bonding for spacecraft and launcher applications N
- **ECSS-Q-ST-70-17C** Durability testing of coatings
- **ECSS-Q-ST-70-22C** Control of limited shelf-life materials
- **ECSS-Q-ST-70-31C Rev.1** Application of paints and coatings on space hardware

Assembling processes

- **ECSS-Q-ST-70-07C** Verification and approval of automatic machine wave soldering
- **ECSS-Q-ST-70-08C** Manual soldering of high-reliability electrical connections → ECSS-Q-ST-70-61C N
- **ECSS-Q-ST-70-14C** Corrosion
- **ECSS-Q-ST-70-26C Rev.1 +Corr.1** Crimping of high-reliability electrical connections
- **ECSS-Q-ST-70-28C** Repair and modification of printed circuit board assemblies for space use
- **ECSS-Q-ST-70-30C** Wire wrapping of high-reliability electrical connections
- **ECSS-Q-ST-70-38C Rev.1** High-reliability soldering for surface-mount and mixed technology → ECSS-Q-ST-70-61C N
- **ECSS-Q-ST-70-39C** Welding of metallic materials for flight hardware
- **ECSS-Q-ST-70-40C** Hard brazing of metallic materials for flight hardware N

Parts

- **ECSS-Q-ST-70-10C** Qualification of printed circuit boards → ECSS-Q-ST-70-60C U
- **ECSS-Q-ST-70-11C** Procurement of printed circuit boards → ECSS-Q-ST-70-60C U
- **ECSS-Q-ST-70-12C** Design rules for printed circuit boards
- **ECSS-Q-ST-70-18C** Preparation, assembly and mounting of RF coaxial cables
- **ECSS-Q-ST-70-46C Rev.1** Requirements for manufacturing and procurement of threaded fasteners

Planetary protection

- **ECSS-Q-ST-70-53C** Materials and hardware compatibility tests for sterilization processes
- **ECSS-Q-ST-70-54C** Ultra cleaning of flight hardware
- **ECSS-Q-ST-70-55C** Microbiological examination of flight hardware and cleanrooms
- **ECSS-Q-ST-70-56C** Vapour phase bioburden reduction for flight hardware
- **ECSS-Q-ST-70-57C** Dry heat bioburden reduction for flight hardware
- **ECSS-Q-ST-70-58C** Bioburden control in cleanrooms

NOTES:
ECSS-Q-ST-70-60C
= merge of Q-ST-70-10C Rev.1 and Q-ST-70-11C

ECSS-Q-ST-70-61
= merge of Q-ST-70-07C, Q-ST-70-08C and Q-ST-70-38C Rev.1

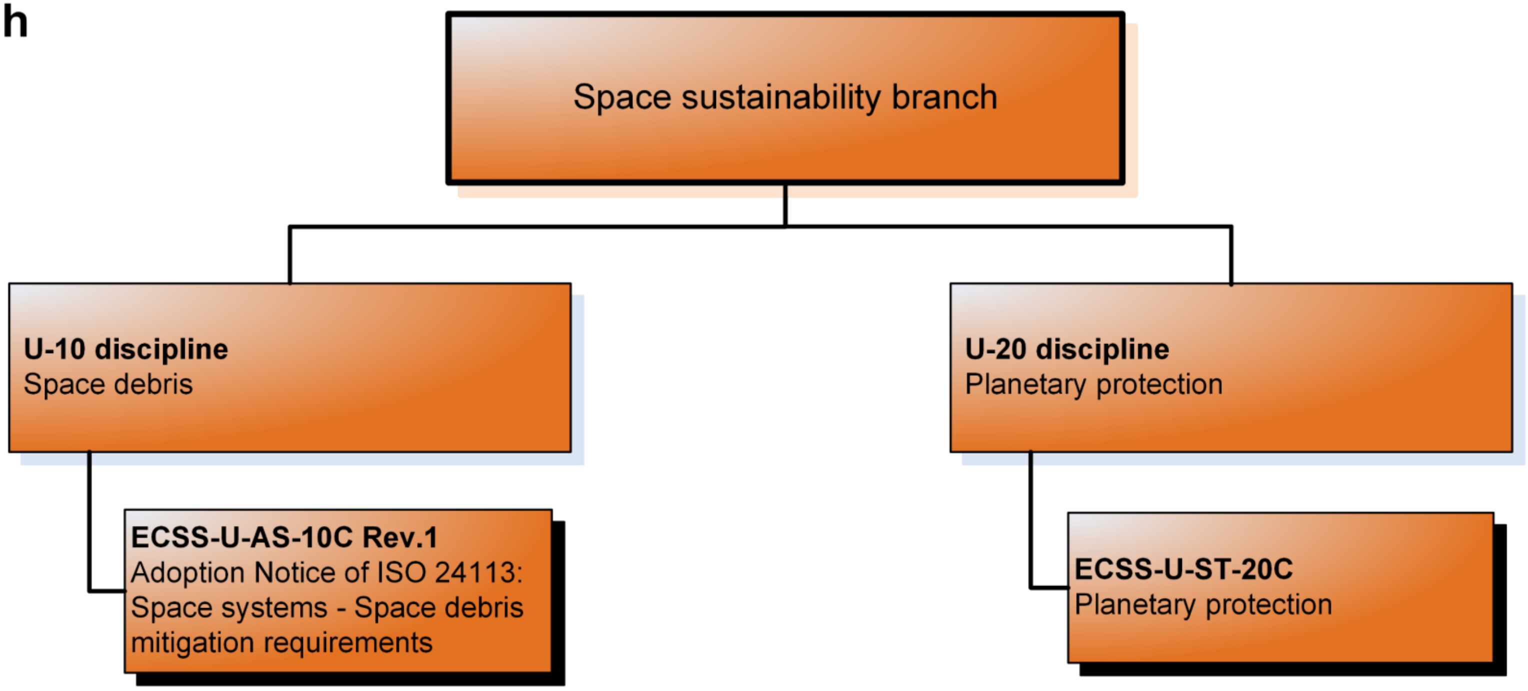
LEGEND

Published	Document affected by update of other doc. M
Ongoing update of an existing document U	New document in production N

(as of 1 May 2020)

ECSS Standards

Sustainability branch



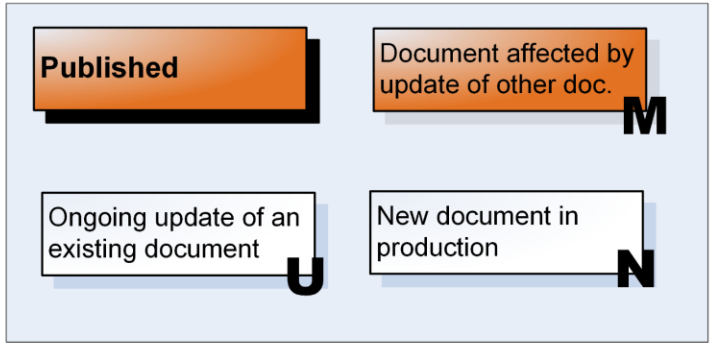
Space sustainability branch

U-10 discipline
Space debris

ECSS-U-AS-10C Rev.1
Adoption Notice of ISO 24113: Space systems - Space debris mitigation requirements

U-20 discipline
Planetary protection

ECSS-U-ST-20C
Planetary protection



Published

Document affected by update of other doc. **M**

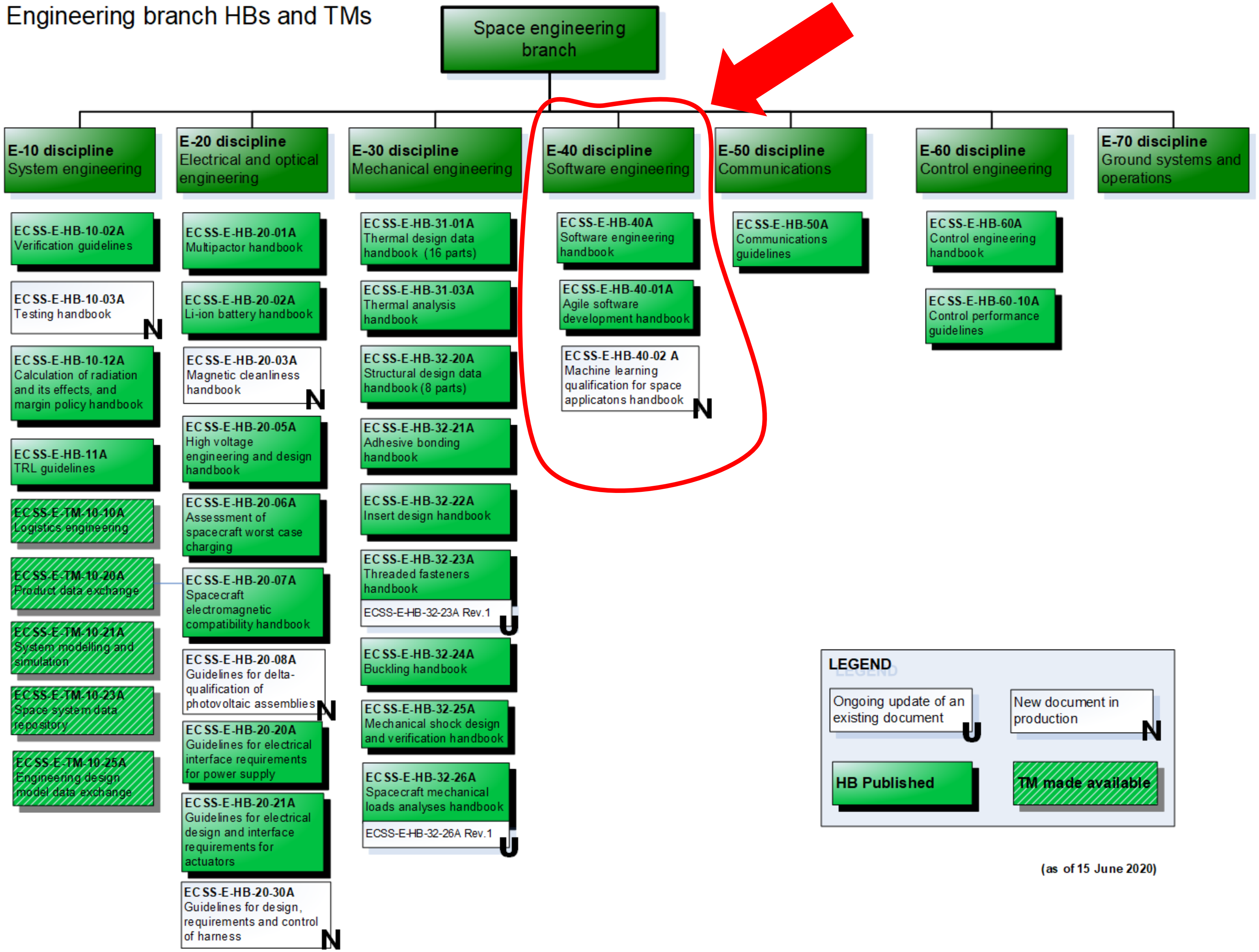
Ongoing update of an existing document **U**

New document in production **N**

(as of 3 December 2019)

ECSS Handbooks and Technical memoranda

Engineering branch HBs and TMs



Space engineering branch

E-10 discipline System engineering
- ECSS-E-HB-10-02A Verification guidelines
- ECSS-E-HB-10-03A Testing handbook N
- ECSS-E-HB-10-12A Calculation of radiation and its effects, and margin policy handbook
- ECSS-E-HB-11A TRL guidelines
- ECSS-E-TM-10-10A Logistics engineering
- ECSS-E-TM-10-20A Product data exchange
- ECSS-E-TM-10-21A System modelling and simulation
- ECSS-E-TM-10-23A Space system data repository
- ECSS-E-TM-10-25A Engineering design model data exchange

E-20 discipline Electrical and optical engineering
- ECSS-E-HB-20-01A Multipactor handbook
- ECSS-E-HB-20-02A Li-ion battery handbook
- ECSS-E-HB-20-03A Magnetic cleanliness handbook N
- ECSS-E-HB-20-05A High voltage engineering and design handbook
- ECSS-E-HB-20-06A Assessment of spacecraft worst case charging
- ECSS-E-HB-20-07A Spacecraft electromagnetic compatibility handbook
- ECSS-E-HB-20-08A Guidelines for delta-qualification of photovoltaic assemblies N
- ECSS-E-HB-20-20A Guidelines for electrical interface requirements for power supply
- ECSS-E-HB-20-21A Guidelines for electrical design and interface requirements for actuators
- ECSS-E-HB-20-30A Guidelines for design, requirements and control of harness N

E-30 discipline Mechanical engineering
- ECSS-E-HB-31-01A Thermal design data handbook (16 parts)
- ECSS-E-HB-31-03A Thermal analysis handbook
- ECSS-E-HB-32-20A Structural design data handbook (8 parts)
- ECSS-E-HB-32-21A Adhesive bonding handbook
- ECSS-E-HB-32-22A Insert design handbook
- ECSS-E-HB-32-23A Threaded fasteners handbook
  - ECSS-E-HB-32-23A Rev.1 U
- ECSS-E-HB-32-24A Buckling handbook
- ECSS-E-HB-32-25A Mechanical shock design and verification handbook
- ECSS-E-HB-32-26A Spacecraft mechanical loads analyses handbook
  - ECSS-E-HB-32-26A Rev.1 U

E-40 discipline Software engineering
- ECSS-E-HB-40A Software engineering handbook
- ECSS-E-HB-40-01A Agile software development handbook
- ECSS-E-HB-40-02 A Machine learning qualification for space applicatons handbook N

E-50 discipline Communications
- ECSS-E-HB-50A Communications guidelines

E-60 discipline Control engineering
- ECSS-E-HB-60A Control engineering handbook
- ECSS-E-HB-60-10A Control performance guidelines

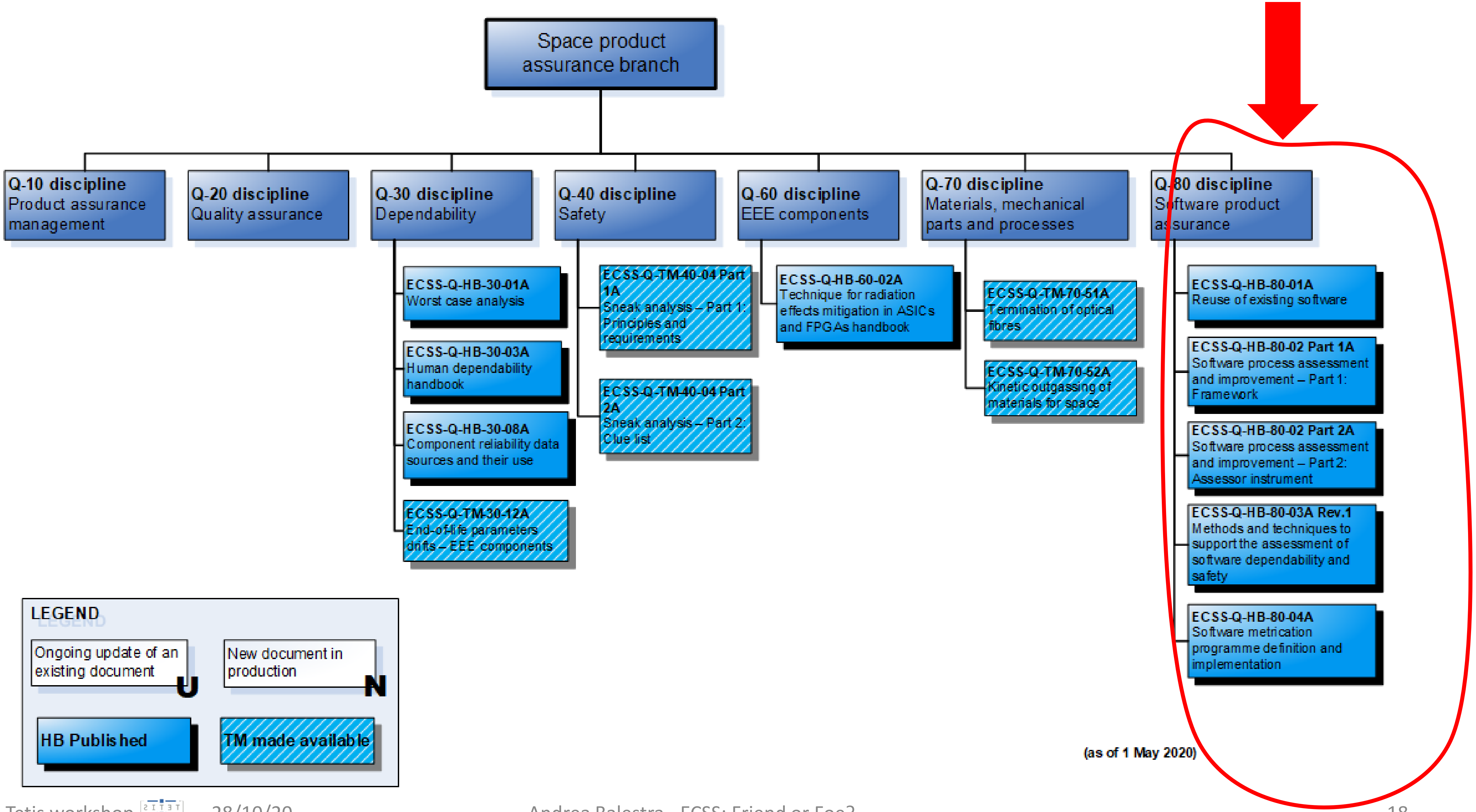
E-70 discipline Ground systems and operations

LEGEND
- Ongoing update of an existing document U
- New document in production N
- HB Published
- TM made available

(as of 15 June 2020)

ECSS Handbooks and Technical memoranda

PA branch HBs and TMs



Space product assurance branch

Q-10 discipline
Product assurance management

Q-20 discipline
Quality assurance

Q-30 discipline
Dependability

- **ECSS-Q-HB-30-01A** Worst case analysis
- **ECSS-Q-HB-30-03A** Human dependability handbook
- **ECSS-Q-HB-30-08A** Component reliability data sources and their use
- **ECSS-Q-TM-30-12A** End-of-life parameters drifts – EEE components

Q-40 discipline
Safety

- **ECSS-Q-TM-40-04 Part 1A** Sneak analysis – Part 1: Principles and requirements
- **ECSS-Q-TM-40-04 Part 2A** Sneak analysis – Part 2: Clue list

Q-60 discipline
EEE components

- **ECSS-Q-HB-60-02A** Technique for radiation effects mitigation in ASICs and FPGAs handbook

Q-70 discipline
Materials, mechanical parts and processes

- **ECSS-Q-TM-70-51A** Termination of optical fibres
- **ECSS-Q-TM-70-52A** Kinetic outgassing of materials for space

Q-80 discipline
Software product assurance

- **ECSS-Q-HB-80-01A** Reuse of existing software
- **ECSS-Q-HB-80-02 Part 1A** Software process assessment and improvement – Part 1: Framework
- **ECSS-Q-HB-80-02 Part 2A** Software process assessment and improvement – Part 2: Assessor instrument
- **ECSS-Q-HB-80-03A Rev.1** Methods and techniques to support the assessment of software dependability and safety
- **ECSS-Q-HB-80-04A** Software metrication programme definition and implementation

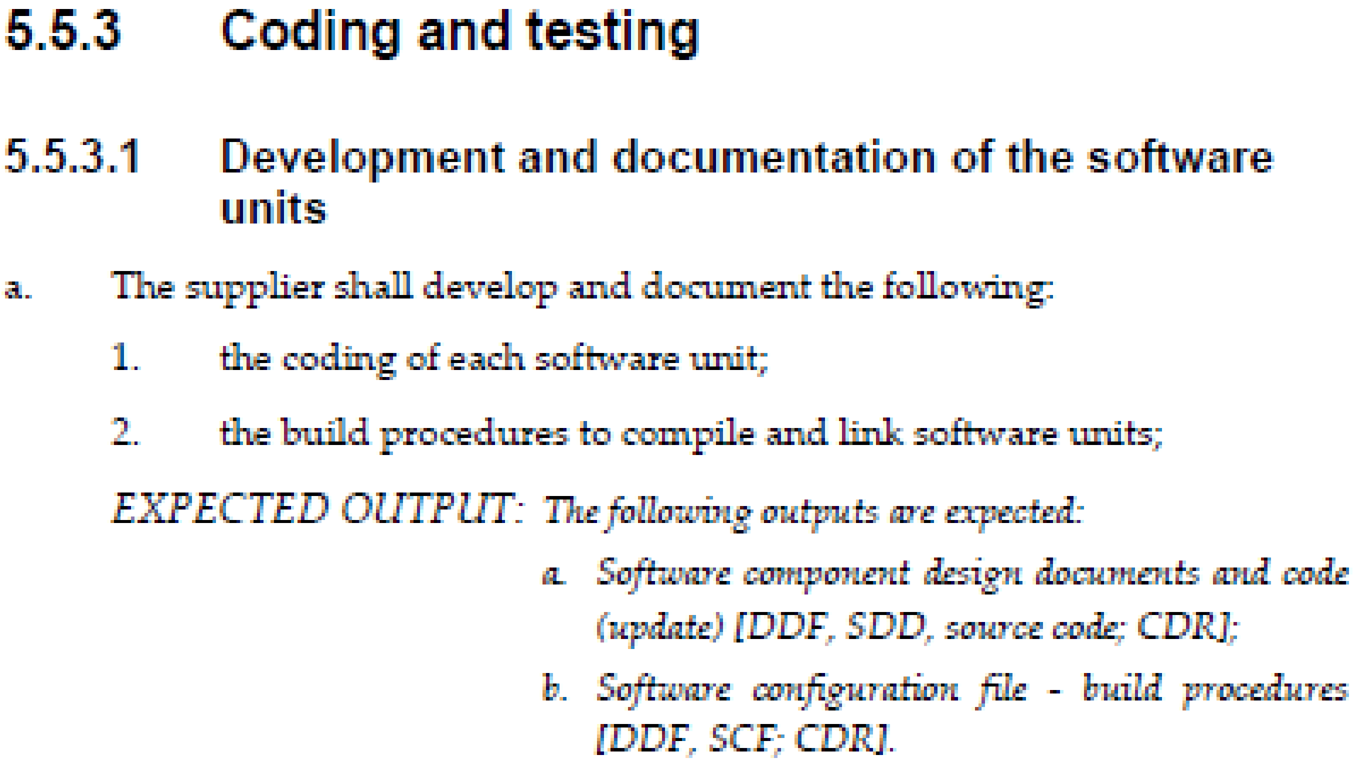
LEGEND

Ongoing update of an existing document U	New document in production N
HB Published	▨ TM made available

(as of 1 May 2020)

ECSS and Software

- ECSS-E-40C for SW Engineering
- Here an example of how it looks like
- No “rocket science” ;) but definitions/procedures that may well apply to any software project.
- Of course in the standard you have also templates for the documents.



5.5.3 Coding and testing

5.5.3.1 Development and documentation of the software units

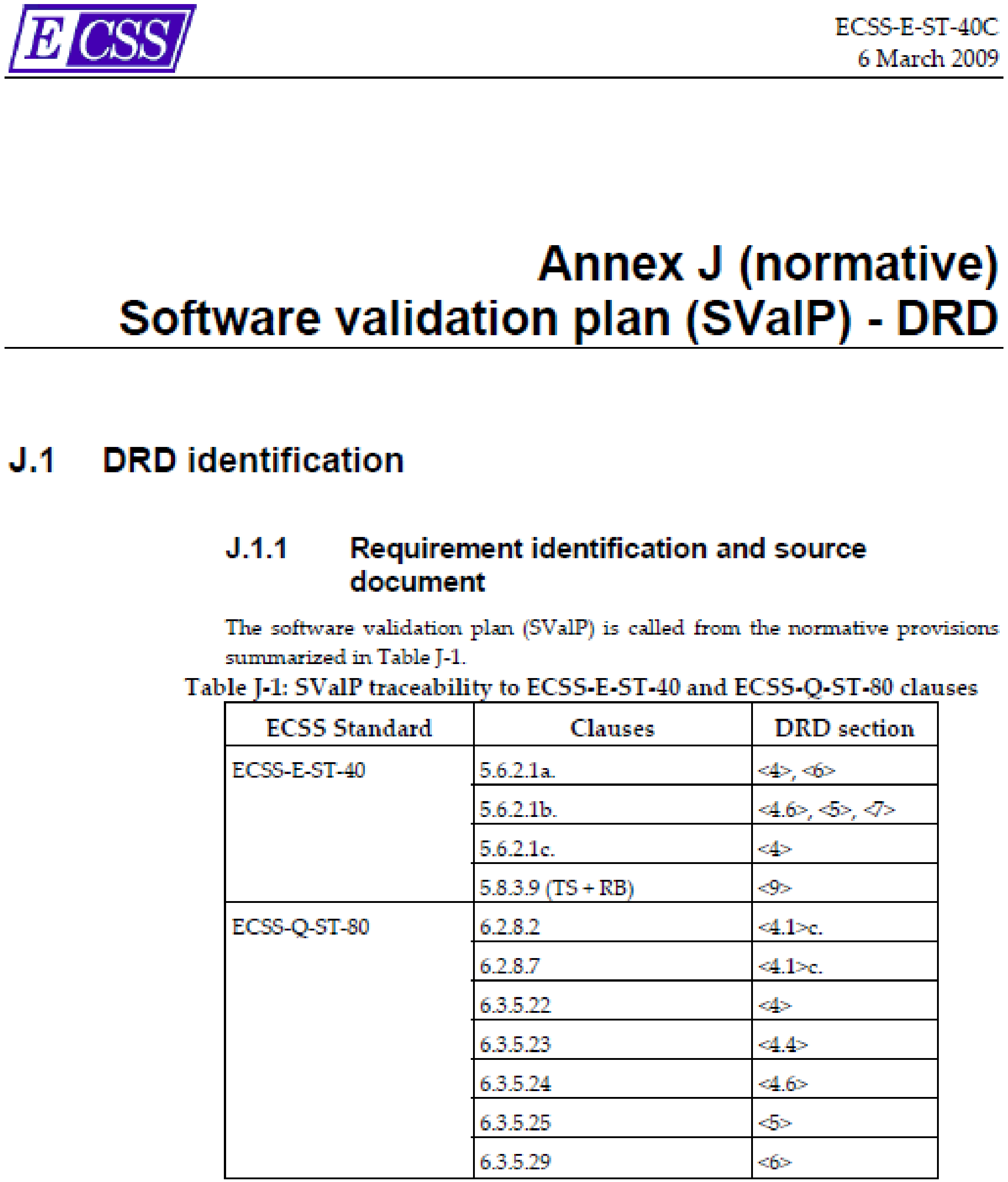
a. The supplier shall develop and document the following:

1. the coding of each software unit;
2. the build procedures to compile and link software units;

EXPECTED OUTPUT: The following outputs are expected:

a. Software component design documents and code (update) [DDF, SDD, source code; CDR];

b. Software configuration file - build procedures [DDF, SCF; CDR].



ECSS-E-ST-40C
6 March 2009

Annex J (normative)
Software validation plan (SValP) - DRD

J.1 DRD identification

J.1.1 Requirement identification and source document

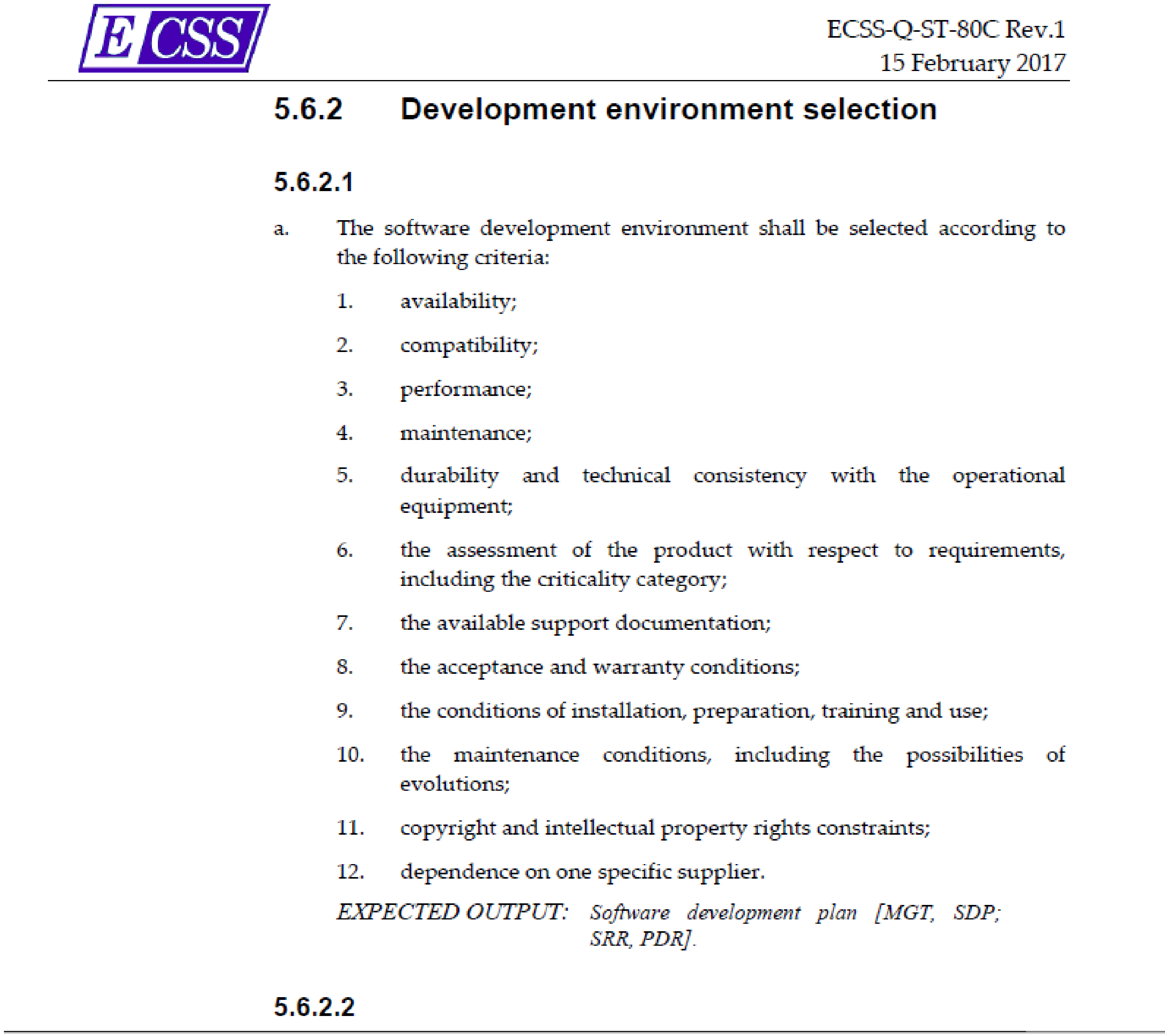
The software validation plan (SValP) is called from the normative provisions summarized in Table J-1.

Table J-1: SValP traceability to ECSS-E-ST-40 and ECSS-Q-ST-80 clauses

ECSS Standard	Clauses	DRD section
ECSS-E-ST-40	5.6.2.1a.	<4>, <6>
	5.6.2.1b.	<4.6>, <5>, <7>
	5.6.2.1c.	<4>
	5.8.3.9 (TS + RB)	<9>
ECSS-Q-ST-80	6.2.8.2	<4.1>c.
	6.2.8.7	<4.1>c.
	6.3.5.22	<4>
	6.3.5.23	<4.4>
	6.3.5.24	<4.6>
	6.3.5.25	<5>
	6.3.5.29	<6>

ECSS and Software

- ECSS-Q-80C for SW PA/QA
- Again, no “rocket science” ;) but a sensible list of criteria.



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

5.6.2 Development environment selection

5.6.2.1

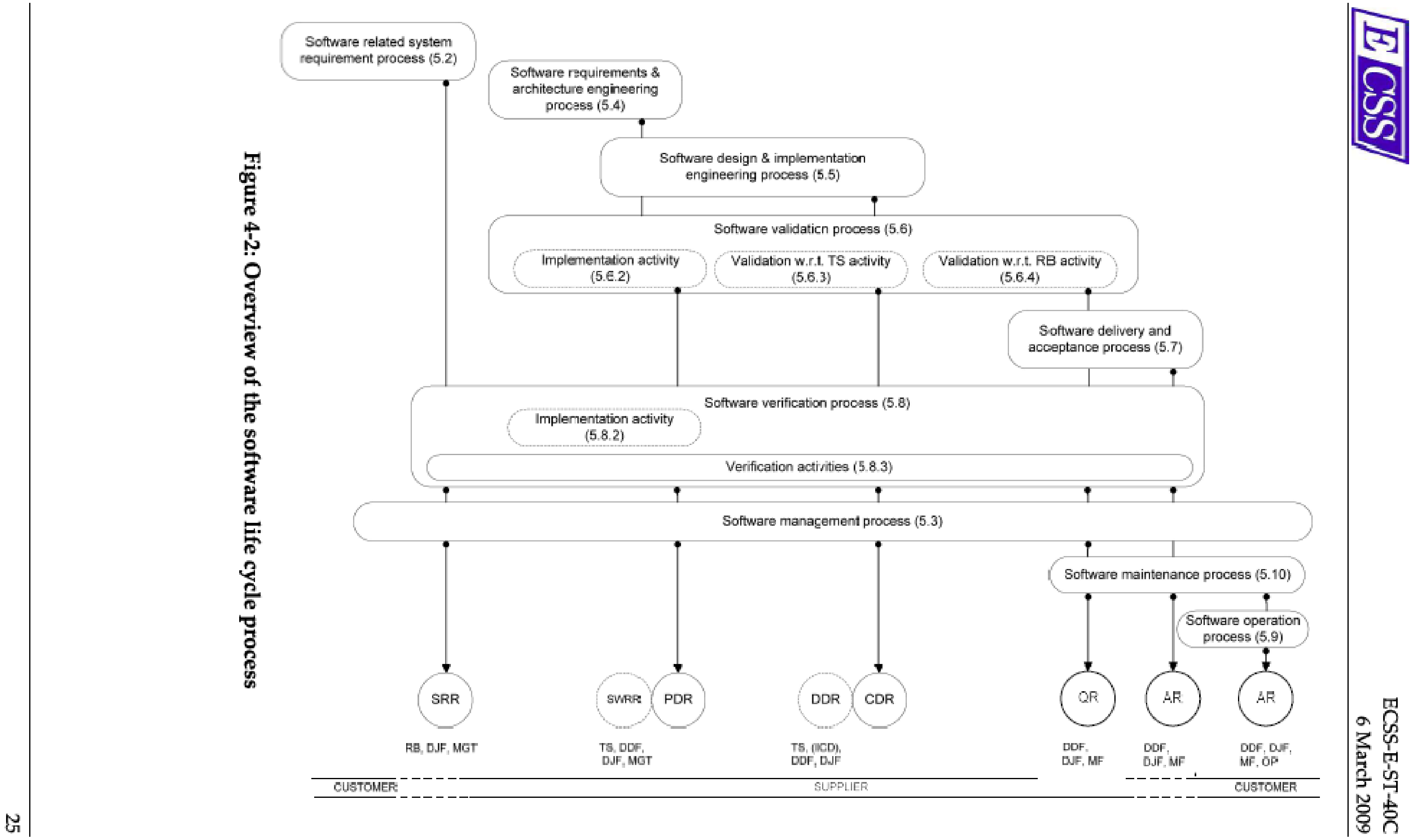
a. The software development environment shall be selected according to the following criteria:

1. availability;
2. compatibility;
3. performance;
4. maintenance;
5. durability and technical consistency with the operational equipment;
6. the assessment of the product with respect to requirements, including the criticality category;
7. the available support documentation;
8. the acceptance and warranty conditions;
9. the conditions of installation, preparation, training and use;
10. the maintenance conditions, including the possibilities of evolutions;
11. copyright and intellectual property rights constraints;
12. dependence on one specific supplier.

EXPECTED OUTPUT: Software development plan [MGT, SDP; SRR, PDR].

5.6.2.2

Lifecycle according to ECSS



ECSS-E-ST-40C
6 March 2009

Software related system requirement process (5.2)

Software requirements & architecture engineering process (5.4)

Software design & implementation engineering process (5.5)

Software validation process (5.6)

Implementation activity (5.6.2)

Validation w.r.t. TS activity (5.6.3)

Validation w.r.t. RB activity (5.6.4)

Software delivery and acceptance process (5.7)

Software verification process (5.8)

Implementation activity (5.8.2)

Verification activities (5.8.3)

Software management process (5.3)

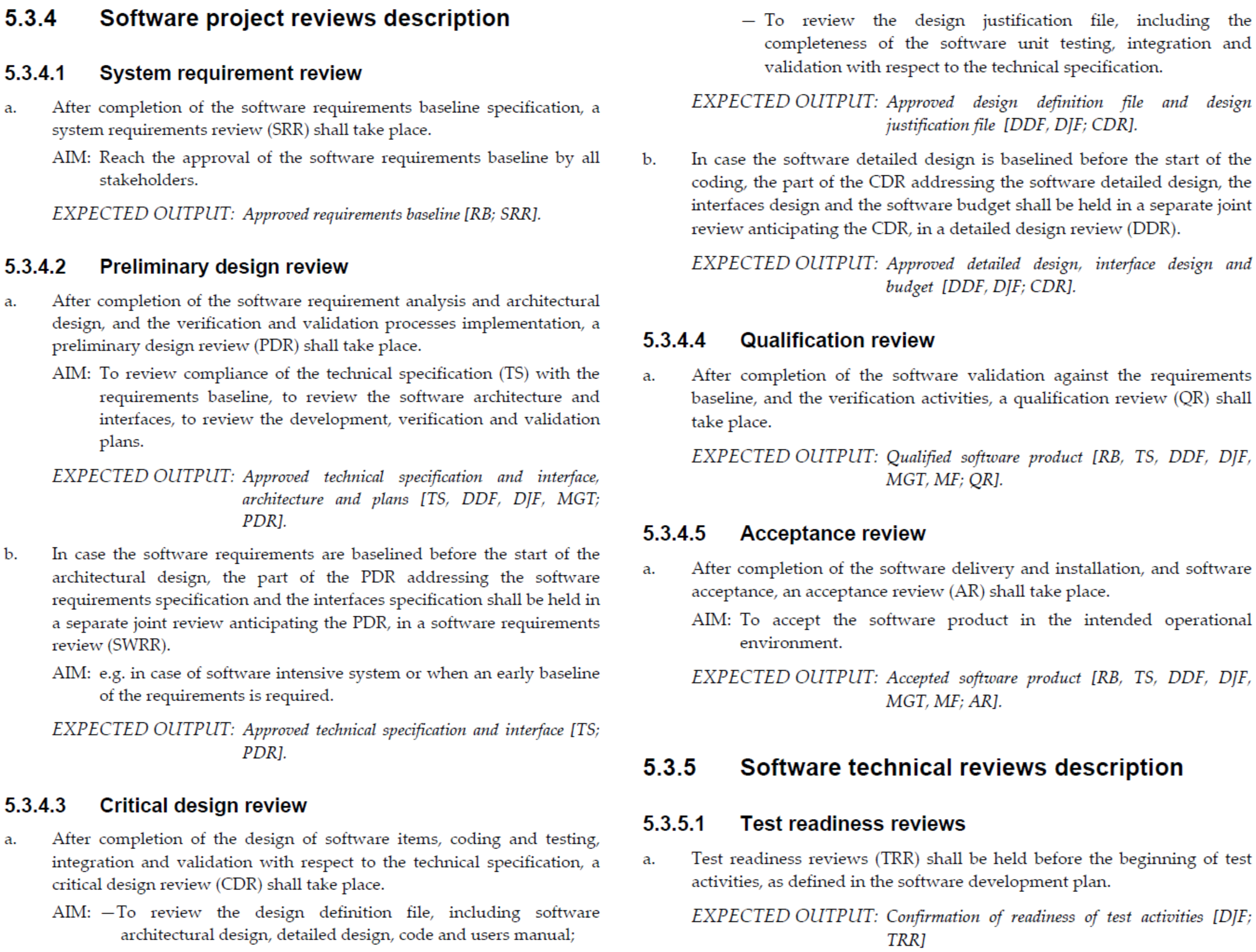
Software maintenance process (5.10)

Software operation process (5.9)

Figure 4-2: Overview of the software life cycle process

25

ECSS Reviews



5.3.4 Software project reviews description

5.3.4.1 System requirement review

a. After completion of the software requirements baseline specification, a system requirements review (SRR) shall take place.

AIM: Reach the approval of the software requirements baseline by all stakeholders.

EXPECTED OUTPUT: *Approved requirements baseline [RB; SRR].*

5.3.4.2 Preliminary design review

a. After completion of the software requirement analysis and architectural design, and the verification and validation processes implementation, a preliminary design review (PDR) shall take place.

AIM: To review compliance of the technical specification (TS) with the requirements baseline, to review the software architecture and interfaces, to review the development, verification and validation plans.

EXPECTED OUTPUT: *Approved technical specification and interface, architecture and plans [TS, DDF, DJF, MGT; PDR].*

b. In case the software requirements are baselined before the start of the architectural design, the part of the PDR addressing the software requirements specification and the interfaces specification shall be held in a separate joint review anticipating the PDR, in a software requirements review (SWRR).

AIM: e.g. in case of software intensive system or when an early baseline of the requirements is required.

EXPECTED OUTPUT: *Approved technical specification and interface [TS; PDR].*

5.3.4.3 Critical design review

a. After completion of the design of software items, coding and testing, integration and validation with respect to the technical specification, a critical design review (CDR) shall take place.

AIM: — To review the design definition file, including software architectural design, detailed design, code and users manual;

— To review the design justification file, including the completeness of the software unit testing, integration and validation with respect to the technical specification.

EXPECTED OUTPUT: *Approved design definition file and design justification file [DDF, DJF; CDR].*

b. In case the software detailed design is baselined before the start of the coding, the part of the CDR addressing the software detailed design, the interfaces design and the software budget shall be held in a separate joint review anticipating the CDR, in a detailed design review (DDR).

EXPECTED OUTPUT: *Approved detailed design, interface design and budget [DDF, DJF; CDR].*

5.3.4.4 Qualification review

a. After completion of the software validation against the requirements baseline, and the verification activities, a qualification review (QR) shall take place.

EXPECTED OUTPUT: *Qualified software product [RB, TS, DDF, DJF, MGT, MF; QR].*

5.3.4.5 Acceptance review

a. After completion of the software delivery and installation, and software acceptance, an acceptance review (AR) shall take place.

AIM: To accept the software product in the intended operational environment.

EXPECTED OUTPUT: *Accepted software product [RB, TS, DDF, DJF, MGT, MF; AR].*

5.3.5 Software technical reviews description

5.3.5.1 Test readiness reviews

a. Test readiness reviews (TRR) shall be held before the beginning of test activities, as defined in the software development plan.

EXPECTED OUTPUT: *Confirmation of readiness of test activities [DJF; TRR]*

Ground and Space SW: Is there still a difference nowadays?

- Maybe not as in the past. Cost, Complexity, Engineering effort, Consortia size have become comparable. ELT and its instruments, SKA, CTA can compare to Euclid, Athena etc. on all those aspects.
- But yes, there are differences, e.g.:
  - ✓ Changing software after launch could be extremely expensive, or even impossible while a ground mission in some nice location is always possible. This leads to much more stringent checks and conditions on space SW (not to mention that in some cases lives may be at stake).
  - ✓ Software used for space may be outdated due to space qualification constraints (e.g. operating systems).
- What about joining forces?

Would ECSS be “usable” for ground software?

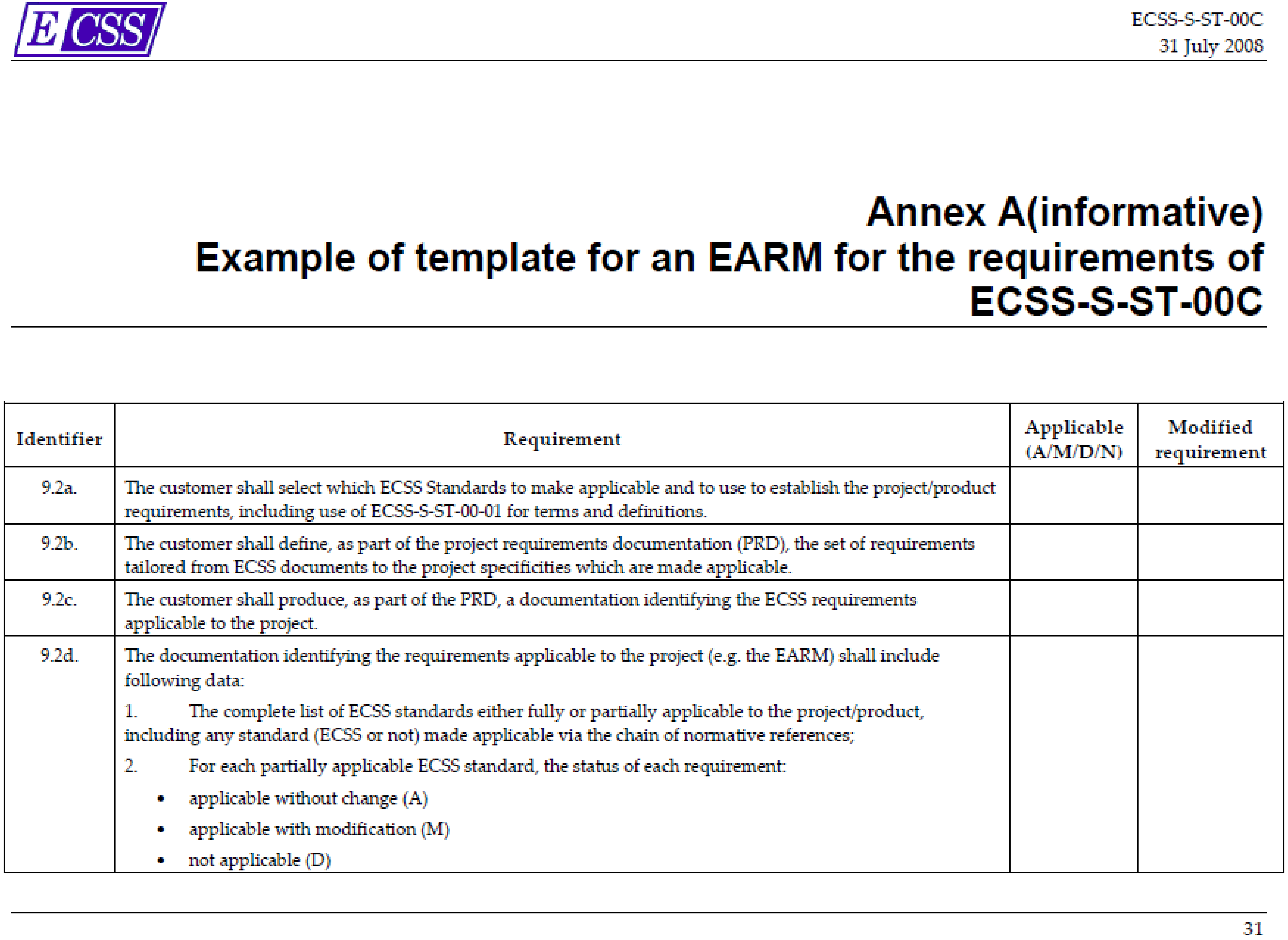
- Overkill? E.g.:
  - Typical review à la ESO < 10 documents
  - Typical review à la ECCS >(>) 10 documents
- Clash with other standards (e.g. ESO)?
  - In practice, mapping ECSS to ESO is quite simple.
  - Also, ESO is currently exploring the possibility to use ECSS standard and is using it as reference in PA/QA for SW.
  - PA/QA for control SW in Maory is done according to ECSS.
- Point is that the “structure” that a standard like ECSS gives to the SW development and review process is extremely useful.
- The “reinvent the wheel syndrome” every time we tackle a new project (unless it’s an ESA project of course ;)) would be avoided as a “TODO” list would be there. Also, common structure, naming etc. would make jumping from one project to the other easier.
- Tailoring of the documents may reduce the amount of documents and requirements solving the overkill/complexity issue.

Tailoring

- **What is a tailoring? (In ECSS glossary words)**

  The ECSS-E40-Part 1B standard defines a set of requirements for developing software in the scope of a space system project. It was defined by the European Cooperation for Space Standardization committee. But because these requirements cover a wide range of applications, some of them may not be applicable for small, low-cost projects. The selection process of the appropriate requirements for a particular project is called a *tailoring*. To be accurate, a tailoring must follow a certain number of rules and generally has to be done with the help of a standard expert. (…)

Of course there is an ECSS standard procedure also for tailoring…



ECSS-S-ST-00C
31 July 2008

Annex A(informative) Example of template for an EARM for the requirements of ECSS-S-ST-00C

Identifier	Requirement	Applicable (A/M/D/N)	Modified requirement
9.2a.	The customer shall select which ECSS Standards to make applicable and to use to establish the project/product requirements, including use of ECSS-S-ST-00-01 for terms and definitions.		
9.2b.	The customer shall define, as part of the project requirements documentation (PRD), the set of requirements tailored from ECSS documents to the project specificities which are made applicable.		
9.2c.	The customer shall produce, as part of the PRD, a documentation identifying the ECSS requirements applicable to the project.		
9.2d.	The documentation identifying the requirements applicable to the project (e.g. the EARM) shall include following data: 1. The complete list of ECSS standards either fully or partially applicable to the project/product, including any standard (ECSS or not) made applicable via the chain of normative references; 2. For each partially applicable ECSS standard, the status of each requirement: • applicable without change (A) • applicable with modification (M) • not applicable (D)		

31

But see also the ECSS Handbook on SW Engineering…

Question: MBSE and ECSS?

- In addition to tailoring, MBSE could be the next step in bridging space and ground control SW. MBSE ('S' for both Systems and Software) is "environment neutral" being used for both space and ground projects.
- MBSE ('S' for Software) used for e.g. Euclid (NISP & VIS) and Plato.
  - Tools: Rhapsody, DOORS, Enterprise Architect, UML.
- MBSE ('S' for Systems) used for e.g. Maory and Mavis.
  - Tools: Cameo, SysML.
  - Integration with PA/QA activities (BOM, FMECA etc.)
- I suppose there also initiatives in SKA, CTA, ASTRI...
- ESA carries on also an MBSE initiative based on Capella/Arcadia and TASTE, used on several missions.
- ECSS and MBSE have then been integrated by ESA in the context of Euclid and Plato projects with a solution based on DOORS, Enterprise Architect, SysML and a handful of DBs.

Answer: Why not?

- MBSE could give the framework where ECSS structure can be implemented. E.g. Reviews, Verification Matrixes, Requirement flow down, Design etc. possibly up to the “Holy Graal”: Code Generation.
- Documents could be generated but, as we want a paperless world, the model should be the unique “Source of Truth”. ECSS would live there in the model.
- There is a long way in homogenizing tools, languages and methodologies, with a visionary view on MBA (Model Based Architecture) i.e. integrating models from other domains (Mechanics, Electronics…).
- Work is ongoing.

The End

Domanden?