Software crítico para sistemas espaciales

2024/25

Master Universitario en Enxeñaría Aeroespacial

Arno Formella
Miguel Ramón González Castro
Manuel Pérez Cota

Departamento de Informática
Universidade de Vigo

24/25

¿por qué estándares?

- no hace falta reinventar de nuevo lo ya descubierto
- simplifican re-usabilidad, adaptabilidad, e interconectividad
- simplifican el trabajo en equipos y entre entidades diferentes
- simplifican el trabajo en paralelo con diferentes provedores
- aumentan la confianza en los productos (se asume que evitar errores está incluido en las recomendaciones)
- garantizan cierta compatibilidad y longevidad
- aumentan la velocidad en el desarrollo (una vez superado la primera barrera de aprendizaje)
- permiten competición en mercados interconectados (ejemplos: televisión, teléfono, ofimática)
- son en la mayoría de los casos negociados entre competidores, así se presentan neutrales y amplios

desafíos de estándares

- limitán hasta cierto punto la innovación (ejemplo: televisión en EE.UU., un estándar temprano, pero no bueno para el rápido avance de la techología posible)
- un cambio en el estándar puede provocar problemas con la compatibilidad
- incluso en caso de necesidad de un posible estándar las organizaciones pueden entrar en discusiones eternas sin resolver (ejemplo: USB via Apple)
- es difícil especificar un estándar sin considerar una implementación real, pero una norma debe ser abstracta para permitir diferentes soluciones
- software y hardware evolucionan muy deprisa, estándares a veces no van a la par (ejemplo: navigadores y entretenimiento en el software de los coches)

organizaciones nacionales e internacionales

ISO: Organización Internacional de Normalización (International Organization for Standardization). Sus normas especifican requerimientos para garantizar que los productos y/o servicios cumplen con su objetivo.

IEC: Comisión Electrotécnica Internacional (International Electrotechnical Commission). Sus normas son documentos técnicos que ayudan a diseñadores y fabricantes a garantizar la seguridad.

IEEE: Instituto de Ingenieros en Eléctrica y Electrónica (Institute of Electrical and Electronic Engineers). Sus normas tienen como fin unificar la forma de presentar trabajos escritos a nivel internacional.

organizaciones internacionales

UNE: Una Norma Española.
Sus normas se crean en los Comités Técnicos de Normalización (CTN) de la Asociación Española de Normalización y Certificación (AENOR) e incluyen adaptaciones españolas de normas internacionales.

ESA: Agencia Europea del Espacio
(European Space Agency)

tres pilares de la calidad

QM: Quality Management o Gestión de la Calidad. Es el concepto más amplio, ya que incluye planificación y estrategia. Considera la cadena de valor de un proyecto, proceso o producto de forma completa.

QA: Quality Assurance o Aseguramiento de la Calidad. Se centra en proporcionar confianza en que se cumplirán los requisitos de calidad. Se enfoca de manera proactiva en los procesos y sistemas.

QC: Quality Control o Control de la Calidad. Se centra en el cumplimiento de los requisitos de calidad. Se enfoca ‘de manera reactiva en las partes del sistema y los productos.

lista de estándares (seguro que faltan algunos...)

los siguientes estándares se pueden mirar en el ámbito de calidad de software:

- ISO 9000 (familia), ISO/IEC/IEEE 90003, ISO 10005, CMMI, ISO/IEC/IEEE 12207, ISO 14000 (familia)
- ISO/IEC 5055, ISO/IEC 20246, *ISO 23081*, ISO/IEC 25000 (familia), ISO/IEC/IEEE 29119, *ISO/IEC 29138*, ISO/IEC 33000 (ISO 15504), IEC 61508, IEEE 730 IEEE 830
- ECSS

los estándares se revisan y se sustituyen, por eso, hay que estar atento a las versiones más recientes

ISO 9000 e ISO/IEC/IEEE 90003

ISO 9000: familia de normas

- para la implementación de un método o Sistema de Gestión de la Calidad (SGC),
- supone la acreditación de la capacidad para satisfacer los requisitos de calidad
- aporta así una serie de requisitos genéricos y aplicables a cualquier organización
- 9000: fundamentos y vocabulario, 9001: sistema de gestión de calidad, 9004: duía de gestión de calidad

ISO/IEC/IEEE 90003: desarrollo de software, guía para la aplicación del estándar ISO 9001 a software

ISO 10005 y CMMI

ISO 10005: guía para estructurar y gestionar un plan de calidad

CMMI: *Capability Maturity Model Integration*

- proporciona un marco de referencia para evaluar y mejorar la madurez de los procesos en el desarrollo de software
- se centra en áreas como la gestión de proyectos, de la calidad, de la configuración, o de los riesgos, entre otros
- una organización puede estar evaluada (*appraised*) en cumplir con tal modelo

ISO/IEC/IEEE 12207 e ISO 14000

ISO 12207: modelos de ciclos de vida del software.

- proporciona un estándar para observar los procesos de ciclo de vida del software
- desde la idea inicial hasta la retirada del software
- está ligado al estándar ECSS-E-40 (que veremos un poco más en detalle)

ISO 14000: familia de normas

- es aplicable a todas las organizaciones
- supuestamente voluntariamente se está buscando reducir los impactos en el medio ambiente
- y cumplir con la legislación nacional e internacional en materia ambiental
- tiene un homólogo para el espacio en el estándar ECSS-U-20

ISO/IEC 5055 e ISO/IEC 20246

ISO 5055: Software Quality Standards

- se establece tipos de debilidades críticas de software
- que se deben inspeccionar y medir en el código
- fijándose en los criterios de seguridad, confianza, eficiencia de rendimiento y mantenibilidad
- (veremos unos detalles más en adelante)

ISO/IEC 20246: Ingeniería de Software (sustituye a IEE 1028)

- marco genérico para revisiones de productos de trabajo
- utilizable por cualquier organización para la gestión, desarrollo, pruebas y mantenimiento de sistemas y software
- contiene un proceso genérico con actividades, tareas, técnicas de revisión y plantillas de documentación que se aplican durante la revisión

ISO 23081 e ISO/IEC 25000

ISO 23081: gestión y preservación de documentos y de información digital

- establece un marco para la creación, gestión y uso de metadatos
- como gestionar documentos
- y explica los principios por los que se debe regir

ISO/IEC 25000: Software product Quality Requirements and Evaluation, SQuaRE

- familia de normas que define un marco de referencia para la calidad del producto de software
- evalúa en 8 áreas: adecuación funcional, fiabilidad, usabilidad, eficiencia, compatibilidad, seguridad, mantenibilidad y portabilidad

ISO/IEC/IEEE 29119

ISO/IEC/IEEE 29119: Software and systems engineering – Software testing

- norma para la documentación de pruebas
- enfoca a la relación de las pruebas con las metodologías de desarrollo y el ciclo de vida
- describe el papel de las pruebas en la gestión de la calidad y cómo parte de la verificación y validación
- menciona las pruebas estáticas y dinámicas
- pone de manifiesto la imposibilidad de realizar pruebas exhaustivas sobre un producto
- destaca la importancia de realizar las pruebas por terceras partes independientes
- define cómo diseñar estrategias, gestionar, priorizar y enfocar las pruebas
- marca la necesaria distinción entre niveles, tipos y técnicas de diseño de pruebas

ISO/IEC 29138 e ISO/IEC 33000

ISO 29138: Information technology – User interface accessibility

- a pesar de ser una norma para realizar interfaces para usuarios con accesibilidad reducida
- es buena guía para realizar interfaces para cualquier usuario
- (os disteis cuenta que los teclados de números son diferentes: cajeros, teclado, móviles, etc.)

ISO 33000: Calidad de los procesos de desarrollo de software (sustitue la ISO 15504) o SPICE (Software Process Improvement and Capability Determination).

- enfoca en la evaluación de la calidad de los procesos
- busca conocer la evolución en el tiempo
- sugiere un seguimiento y determinar posibles estrategias de mejora

IEC 61508

IEC 61508: seguridad funcional de sistemas E/E/EP

- es una norma internacional para la seguridad funcional de equipos equipos eléctricos, electrónicos y electrónicos programables (E/E/EP)
- cubre todo tipo de sistemas cuales incorporan dispositivos E/E/EP
- el objetivo es cubrir los posibles riesgos creados cuando fallan las funciones realizadas
- se base en dos conceptos
  - ciclo de vida de seguridad
  - niveles de integridad de seguridad (*safety integrity level* (SIL))
- a partir de este estándar han surgido varios estánderes más específicos en diferentes ámbitos, entre ellos partes del ECSS para espacio y la ISO 26262 para automóviles

IEEE 730 e IEEE 830

IEEE 730: estándar para planes para asegurar la calidad de software
(*Standard for Software Quality Assurance Plans*)

- define qué es software de alta calidad
- propone una elaboración de un Plan de Aseguramiento de la calidad de software (SQAP)
- proporciona los requisitos mínimos para el aseguramiento de la calidad del software

IEEE 830: prácticas recomendadas para elaborar requisitos de software
(*Recommended Practice for Software Requirements Specifications*)

- un poco antiguado pero da buenas pistas como realizar un documento de requisitos de software
- incluye plantillas para elaborar documentación
- (se puede comparar en partes con las ECSS)

familia de normas ISO/IEC 25000

ISO/IEC 25000: conocida como SQuaRE (*System and Software Quality Requirements and Evaluation*)

- es una familia de normas que tiene por objetivo la creación de un marco de trabajo común para evaluar la calidad del producto software
- es el resultado de la evolución de otras normas anteriores
  (entre otras ISO/IEC 9126 e ISO/IEC 14598)
- está compuesta por cinco divisiones

familia de normas ISO/IEC 25000

ISO/IEC 2500n – División de Gestión de Calidad

las 2500n definen todos los modelos, términos y definiciones comunes referenciados por las otras normas de la familia 25000 y están formadas por:

ISO/IEC 25000: guía para SQuaRE (*Guide to SQuaRE*)

- contiene el modelo de la arquitectura de SQuaRE
- aclara la terminología de la familia, un resumen de las partes, los usuarios previstos y las partes asociadas
- incorpora modelos de referencia

ISO/IEC 25001: planificación y gestión (*Planning and Management*)

- establece los requisitos y orientaciones para gestionar la evaluación y la especificación de los requisitos del producto software

ISO/IEC 2501n – División de Modelo de Calidad

las 2501n presentan modelos de calidad detallados incluyendo características para calidad interna, externa y en uso del producto software y están formadas por:

ISO/IEC 25010: *system and software quality models*

- describe el modelo de calidad para el producto software y para la calidad en uso
- presenta las características de calidad frente a las cuales evaluar el producto software

ISO/IEC 25012: *data quality model*

- define un modelo general para la calidad de datos
- es aplicable a aquellos datos que se encuentran almacenados de manera estructurada y forman parte de un sistema de información.

ISO/IEC 2502n – División de Medición de Calidad

las 2502n incluyen un modelo de referencia de la medición de la calidad del producto, definiciones de medidas de calidad (interna, externa y en uso) y guías prácticas; está formada por:

ISO/IEC 25020: *measurement reference model and guide*

- presenta una explicación introductoria y un modelo de referencia común a los elementos de medición de la calidad
- proporciona una guía para que los usuarios seleccionen o desarrollen y apliquen medidas propuestas por normas ISO

ISO/IEC 25021: *quality measure elements*

- define y especifica un conjunto recomendado de métricas base y derivadas que puedan ser usadas a lo largo de todo el ciclo de vida del desarrollo software

ISO/IEC 2502n – División de Medición de Calidad

ISO/IEC 25022: *measurement of quality in use*

- define específicamente las métricas para realizar la medición de la calidad en uso del producto

ISO/IEC 25023: *measurement of system and software product quality*

- define específicamente las métricas para realizar la medición de la calidad de productos y sistemas software

ISO/IEC 25024: *measurement of data quality*

- define específicamente las métricas para realizar la medición de la calidad de datos

ISO/IEC 2503n – División de Requisitos de Calidad

las 2503n ayudan a especificar requisitos de calidad que pueden ser utilizados en el proceso de elicitación de requisitos de calidad del producto software a desarrollar o como entrada del proceso de evaluación y está formada por:

ISO/IEC 25030: requisitos de calidad (*quality requirements*)

- provee de un conjunto de recomendaciones para realizar la especificación de los requisitos de calidad del producto software

ISO/IEC 2504n – División de Evaluación de Calidad

las 2504n incluyen normas que proporcionan requisitos, recomendaciones y guías para llevar a cabo el proceso de evaluación del producto software y están formadas por:

ISO/IEC 25040: *evaluation reference model and guide*

- propone un modelo de referencia general para la evaluación
- considera las entradas al proceso de evaluación, las restricciones y los recursos necesarios para obtener las correspondientes salidas

ISO/IEC 25041: *evaluation guide for developers, acquirers and independent evaluators*

- describe los requisitos y recomendaciones para la implementación práctica de la evaluación del producto software desde el punto de vista de los desarrolladores, de los adquirentes y de los evaluadores independientes

ISO/IEC 2504n – División de Evaluación de Calidad

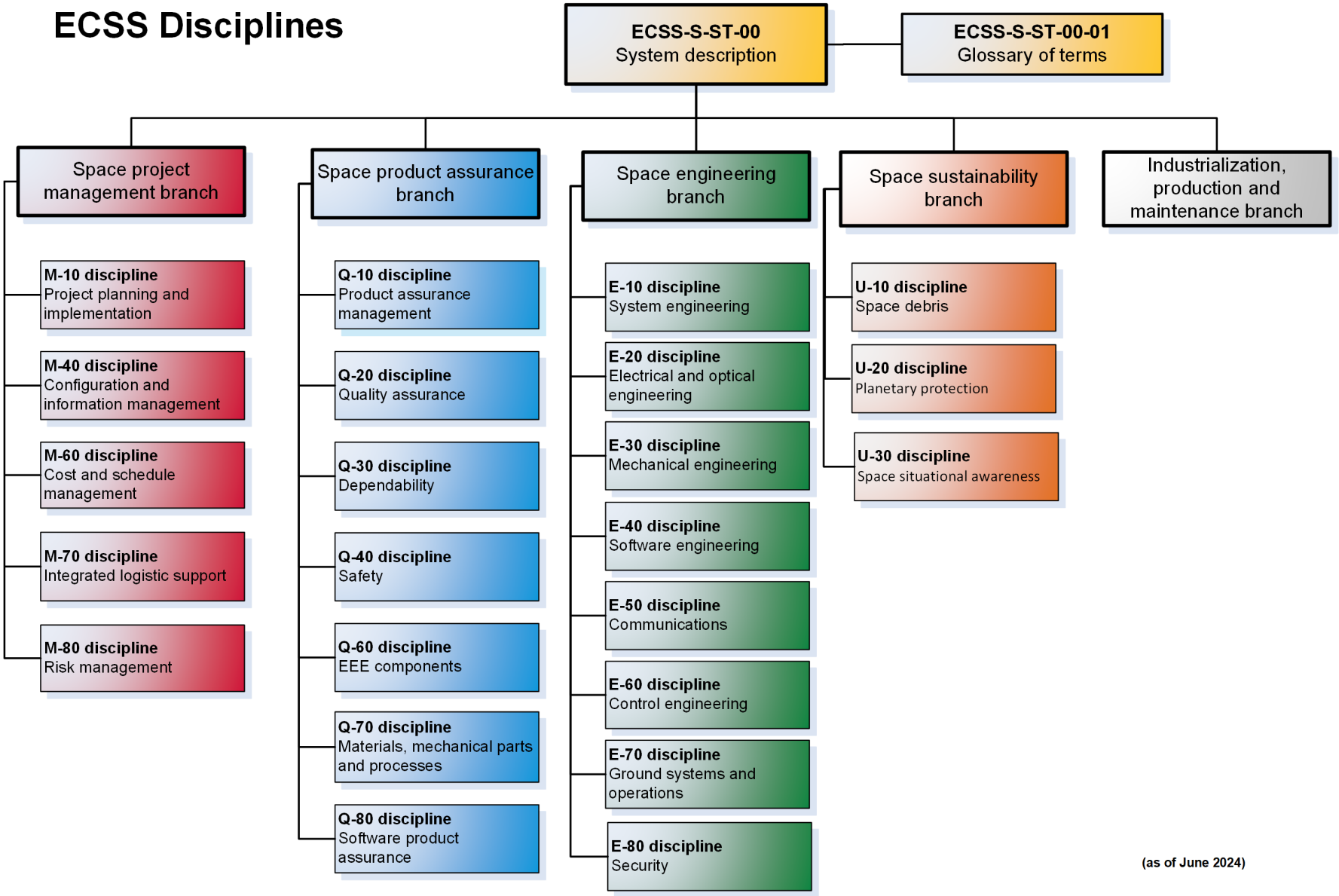
ISO/IEC 25042: *evaluation modules*

- define lo que la Norma considera un módulo de evaluación y la documentación, estructura y contenido que se debe utilizar a la hora de definir uno de estos módulos

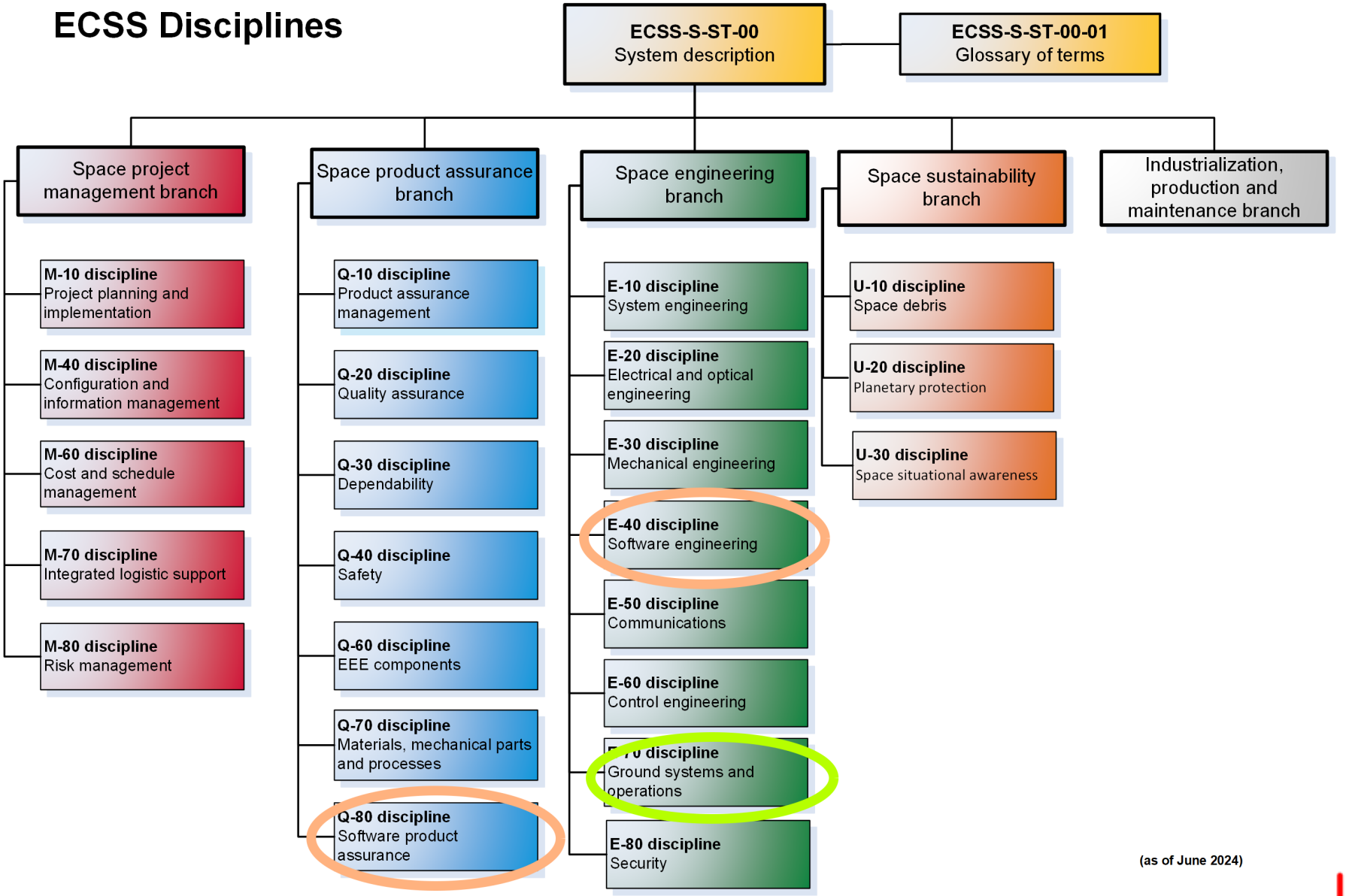
ISO/IEC 25045: *evaluation module for recoverability*

- define un módulo para la evaluación de la subcaracterística eecuperabilidad (*ecoverability*)

ECSS estándar: árbol de documentos



ECSS estándar: árbol de documentos



ECSS estándar: ramas principales

el estándar ECSS consta de tres ramas principales:

- **M**-documentos, tratan aspectos de la gestion del proyecto
- **E**-documentos, tratan aspectos de la ingeniería del proyecto
- **Q**-documentos, tratan aspectos de la garantía de calidad del proyecto

ECSS estándar: documentos principales

todos los documentos del estándar se puede acceder gratuitamente en la página web de ECSS

los documentos más importantes en relación con el desarrollo de software son:

Number	Title
ECSS-M-ST-10	project planning and implementation
ECSS-M-ST-40	configuration and information management
ECSS-E-ST-10	system engineering general requirements
ECSS-E-ST-40	software engineering
ECSS-E-ST-70	ground systems and operations
ECSS-E-HB-40	software engineering handbook
ECSS-Q-ST-80	software product assurance

ECSS estándar: fases

todas las misiones (proyectos) de la ESA se ejecutan en las siguientes fases:

- Phase 0 (*idea/needs-identification/feasibility-study*)
- Phase A (*feasibility*)
- Phase B (*preliminary definition*)
- Phase C (*detailed definition*)
- Phase D (*qualification and production*)
- Phase E (*operations/utilization*)
- Phase F (*disposal*)

Nota que en cualquier momento se puede abandonar la misión, por no ser factible, por falta de recursos o dinero, por falta de soluciones o producción, etc.

ECSS estándar: relación software

el estándar ECSS es

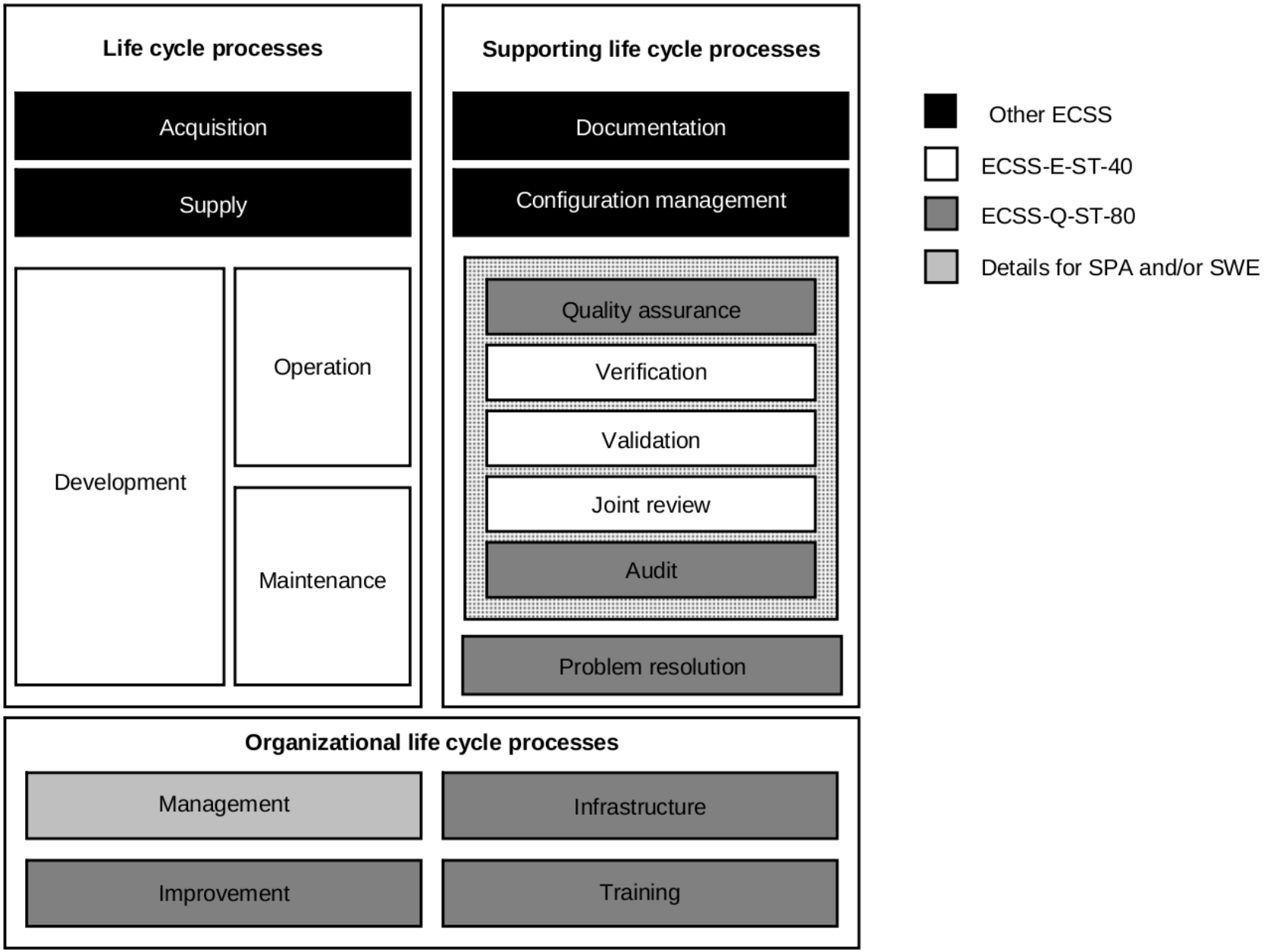
- modelo de procesos
- que no describe ningún ciclo de vida de software en particular
- sino, se puede implementar cualquier ciclo de vida para el desarrollo de software o modelo de ingeniería
- imprecindibles serán siempre
  - las revisiones (incorporando todas las partes involucradas)
  - la generación de documentación adecuada

ECSS estándar: revisiones

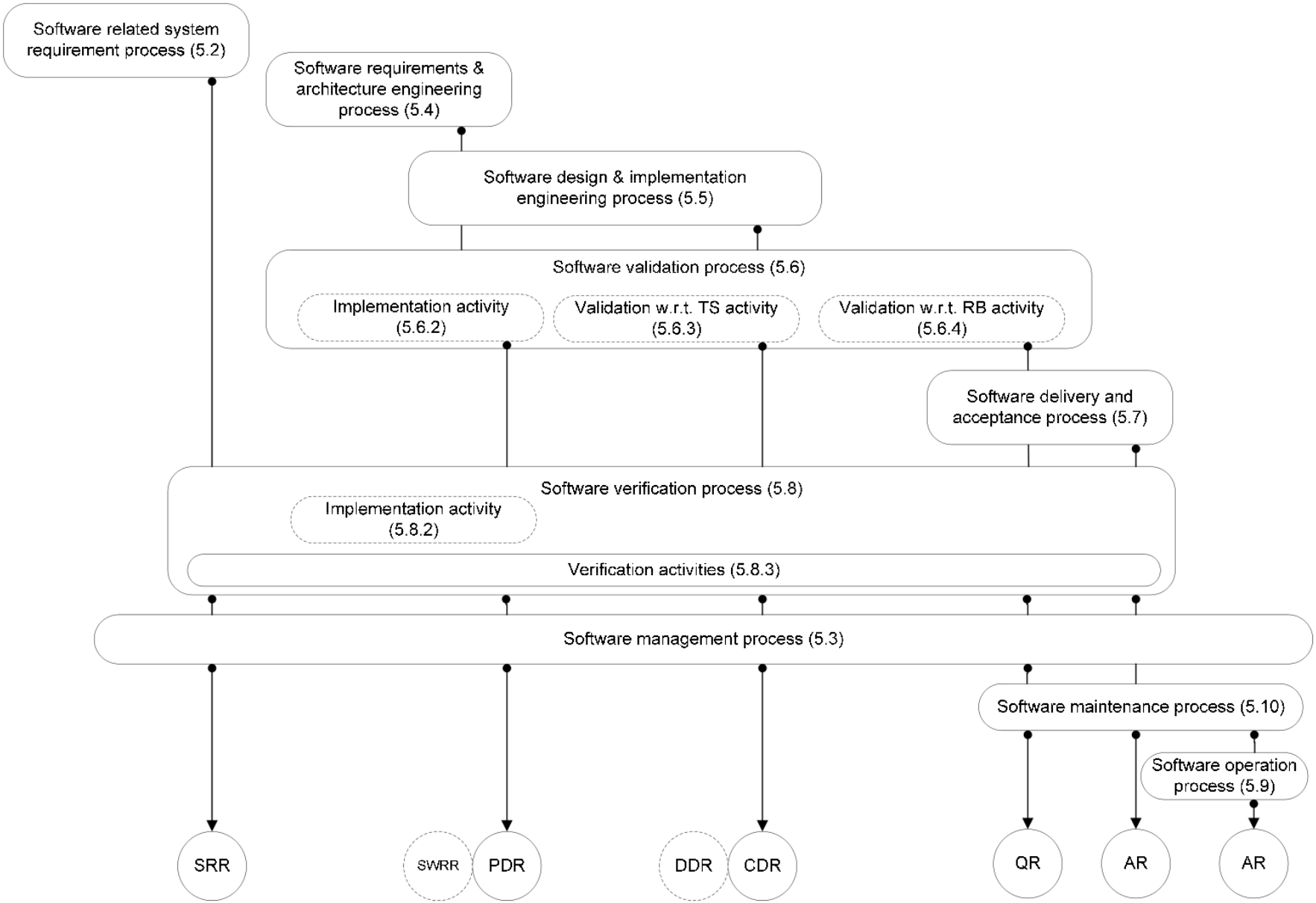
- las revisiones son los puntos principales de interacción
- sincronizan los procesos de ingeniería de software
- las revisiones relevantes para el software son:
  - *system requirements review* (SRR)
  - *preliminary design review* (PDR)
  - *critical design review* (CDR)
  - *qualification review* (QR)
  - *acceptance review* (AR)
  - *operational readiness review* (ORR)

como definidos en ECSS-M-ST-10

ECSS estándar



ECSS estándar



ECSS estándar: resumen de documentos I

File	Document	DRD	SRR	PDR	CDR	QR	AR	ORR
SMF	sw management file							
	sw development plan	SDP						
	sw review plan	SRevP						
	sw configuration management plan	SCMP						
SSF	sw specification file							
	sw system specification	SSS						
	interface requirements document	IRD						
	sw requirements specification	SRS						
	interface control document	ICD						
DDF	design definition file							
	sw design document	SDD						
	sw configuration document	SCD						
	sw release document	SRelD						
	sw user manual	SUM						

ECSS estándar: resumen de documentos II

File	Document	DRD	SRR	PDR	CDR	QR	AR	ORR
DJF	design justification file							
	sw verification plan	SVerP						
	sw verification report	SVR						
	sw validation plan	SValP						
	sw validation specification with respect to TS	SVS						
	sw validation report with respect to TS							
	sw validation specification with respect to RB	SVS						
	sw validation report with respect to RB							
	sw re-use document	SRD						
	independent sw verification and validation plan							
	independent sw verification and validation report							
	sw unit test plan	SUITP						
	sw unit test report							
	sw integration test plan	SUITP						
	sw integration test report							
	sw acceptance test plan							
	sw acceptance test report							
	sw installation plan							
	sw installation report							

ECSS estándar: resumen de documentos III

File	Document	DRD	SRR	PDR	CDR	QR	AR	ORR
PAF	product assurance file							
	sw product assurance plan	SPAP						
	sw product assurance milestone report	SPAMR						
MF	maintenance file							
	sw maintenance plan							
	sw maintenance report							
OPF	operational file							
	sw operation support plan							
	sw operational testing results report							

dentro de un proyecto es importante

- requisitos de la gestión del software
  (*software management requirements*)
- requisitos de ingeniería de software
  (*software engineering process requirements*)
  - incluyendo verificación, verificación, verificación y validación, validación, validación
- requisitos de documentación de todo
  (*software documentation and work product requirements*)

- Antoine de Saint Exupery:
  A goal without a plan is just a wish.
- Lord Kelvin:
  If you cannot measure it, you cannot improve it.
- anonymous:
  The devil is in the details.

¿que falta en los estándares (en mi opinión)?

- requisito que toda la información esté guardada con su historial en un repository
- requisito de evitar cualquier duplicación de información
- el control de versiones debe estar automatizado
- requisito para (hiper)enlazar la documentación
- requisito que todos los documentos deben tener la fecha de su última modificación en la primera página y en los metadatos
- requisito que documentos obsoletos deben estar marcados como tales y sus nuevas versiones deben estar enlazados, por ejemplo, anteponiendo una nueva portada (e hiperenlaces)