Suomen Automaatioseuran turvallisuusjaosto (ASAF)
Teemasarja
Toiminnallinen turvallisuus – uusittu standardisarja
SFS-EN IEC 61508

Uusittujen ohjelmistostandardien IEC 61508-3 ja EN 50128 vertailua

VR Track Oy
Janne Peltonen
Insinöörit-ekonomit talo, Itä-Pasila, 7.11.2011

VR TRACK

Teemat

Uusitut ohjelmistostandardit - soveltamisalat

Ohjelmiston kehittämisen elinkaarimallit

Standardin IEC 61508-3 tekniikat ja toimenpiteet

Standardin EN 50128 tekniikat ja toimenpiteet

Lainattua

- “An ingredient that gives maximum play to the planning, measurement, and control elements is consistent and vigorous discipline.” (M.E.Fagan, Design and code inspections to reduce errors in program development, 1976)

IEC 61508-3 : 2010 yleiskatsaus

- IEC 61508 Ed.2.0 : 2010 – SÄHKÖISTEN / ELEKTRONISTEN / OHJELMOITAVIEN ELEKTRONISTEN TURVALLISUUTEEN LIITTYVIEN JÄRJESTELMIEN TOIMINNALLINEN TURVALLISUUS – *Osa 3: Ohjelmistovaatimukset*
  - Kuva 1 – IEC 61508-sarjan kokonaisrakenne
  - Kappale 6 - Lisävaatimukset turvallisuuteen liittyvän ohjelmiston hallintaan
  - Kappale 7 - Ohjelmiston turvallisuuden elinkaaren vaatimukset

- Velvoittavat osat
  - Liitteineen noin 45s. (Suomenkielinen teksti)
  - Velvoittavat liitteet A ja D sekä opastavat liitteet B, C, E, F ja G
  - Dokumentointi, toiminnallisen turvallisuuden hallinta ja arviointi - viite osaan IEC 61508-1
  - Turvaväylien vaatimukset, viite IEC 61508-2 kohtaan 7.4.11

IEC 61508-3 : 2010
Velvoittavat standardiviitteet

- IEC 61508-1: 2010, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements
- IEC 61508-2: 2010, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
- IEC 61508-4: 2010, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations
- IEC Guide 104:1997, The preparation of safety publications and the use of basic safety publications and group safety publications
- ISO/IEC Guide 51:1999, Safety aspects – Guidelines for their inclusion in standards

EN 50128 : 2011 yleiskatsaus

- EN 50128 : 2011 – *Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems*
  - The main changes with respect to the previous edition:
    - requirements on software management and organization, definition of roles and competencies; deployment and maintenance have been added; a new clause on tools has been inserted, based on EN 61508-2:2008; tables in Annex A have been updated

- Korvaa ohjelmistostandardin EN 50128 : 2001
  - Standardiin IEC 61508-3 nähden rinnakkainen kehityslinja

- Velvoittavat osat
  - Liitteineen noin 87s. (Englanninkielinen teksti)
  - Velvoittavat liitteet A ja B sekä opastavat liitteet C, D, ZZ

IEC 61508-3 : 2010
Velvoittavat standardiviitteet

- IEC 61508-1: 2010, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements
- IEC 61508-2: 2010, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
- IEC 61508-4: 2010, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations
- IEC Guide 104:1997, The preparation of safety publications and the use of basic safety publications and group safety publications
- ISO/IEC Guide 51:1999, Safety aspects – Guidelines for their inclusion in standards

EN 50128 : 2011
Velvoittavat standardiviitteet

- EN 50126-1:1999 Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Basic requirements and generic process
- EN 50129:2003 Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling
- EN ISO 9000 Quality management systems – Fundamentals and vocabulary (ISO 9000)
- EN ISO 9001 Quality management systems – Requirements (ISO 9001)
- ISO/IEC 90003:2004 Software engineering – Guidelines for the application of ISO 9001:2000 to computer software
- ISO/IEC 9126 series Software engineering – Product quality

IEC 61508-3 : 2010 sovellusala

Standardisarjan IEC 61508 tämä osa

- a) on tarkoitettu käytettäväksi vasta standardien IEC 61508-1 ja IEC 61508-2 perusteellisen ymmärtämisen jälkeen
- b) on sovellettavissa mihin tahansa ohjelmistoon, joka muodostaa osan turvallisuuteen liittyvästä järjestelmästä tai jota käytetään standardien IEC 61508-1 ja IEC 61508-2 soveltamisalaan kuuluvan turvallisuuteen liittyvän järjestelmän kehittämiseen. Tällaista ohjelmistoa kutsutaan turvallisuuteen liittyväksi ohjelmistoksi (mukaan lukien käyttöjärjestelmät, järjestelmäohjelmisto, tietoliikenneverkkojen ohjelmistot, ihminen-kone-käyttöliittymätoiminnot ja kiinteä ohjelmisto sekä sovellusohjelmisto)
- c) esittää erityiset tukityökaluille soveltuvat vaatimukset, joita käytetään turvallisuuteen liittyvän järjestelmän kehittämiseen ja konfigurointiin standardien IEC 61508-1 ja IEC 61508-2 soveltamisalueella
- d) edellyttää, että ohjelmiston toteuttamat turvatoiminnot ja ohjelmiston systemaattinen kyvykkyys on määritetty
- e) määrittelee turvallisuuden elinkaaren vaiheisiin liittyvät vaatimukset sekä toimenpiteet, joita on sovellettava turvallisuuteen liittyvän ohjelmiston suunnittelun ja kehittämisen aikana (ohjelmiston turvallisuuden elinkaarimalli). Näihin vaatimuksiin kuuluu sovellettavat tekniikat ja toimenpiteet, jotka on jaettu luokkiin vaadittavan systemaattisen kyvykkyyden mukaisesti, jotta vältettäisiin ja hallittaisiin ohjelmiston viat ja vikaantumiset

IEC 61508-3 : 2010 sovellusala

Standardisarjan IEC 61508 tämä osa

- f) esittää vaatimukset järjestelmän turvallisuuden ohjelmisto-osuuksien kelpuutukseen liittyville tiedoille, jotka on toimitettava sähköisen/elektronisen/ohjelmoitavan elektronisen järjestelmän integrointia toteuttavalle organisaatiolle
- g) esittää vaatimukset niiden tietojen ja menettelytapojen valmisteluun, jotka koskevat ohjelmistoa, ja jota käyttäjä tarvitsee turvallisuuteen liittyvän sähköisen/elektronisen/ohjelmoitavan elektronisen järjestelmän käyttöä ja ylläpitoa varten
- h) esittää vaatimukset, jotka sen organisaation on täytettävä, joka toteuttaa turvallisuuteen liittyvän ohjelmiston muutokset
- i) esittää yhdessä standardien IEC 61508-1 ja IEC 61508-2 kanssa vaatimukset aputyökaluille kuten kehitys- ja suunnittelutyökaluille, kääntäjille, testi- ja virheenjäljitystyökaluille sekä konfiguraation hallinnan työkaluille
- j) tätä standardia ei sovelleta lääkintälaitteisiin, jotka ovat standardisarjan IEC 60601 mukaisia.

EN 50128 : 2011 sovellusala

- It is within the scope of EN 50126-1 and EN 50129 to define the process of specifying the safety functions allocated to software.
- This European Standard specifies those measures necessary to achieve these requirements.
- As decomposition of the specification into a design comprising safety-related systems and components takes place, further allocation of safety integrity levels is performed. Ultimately this leads to the required software safety integrity levels.
- The current state-of-the-art is such that neither the application of quality assurance methods (so-called fault avoiding measures and fault detecting measures) nor the application of software fault tolerant approaches can guarantee the absolute safety of the software. There is no known way to prove the absence of faults in reasonably complex safety-related software, especially the absence of specification and design faults.

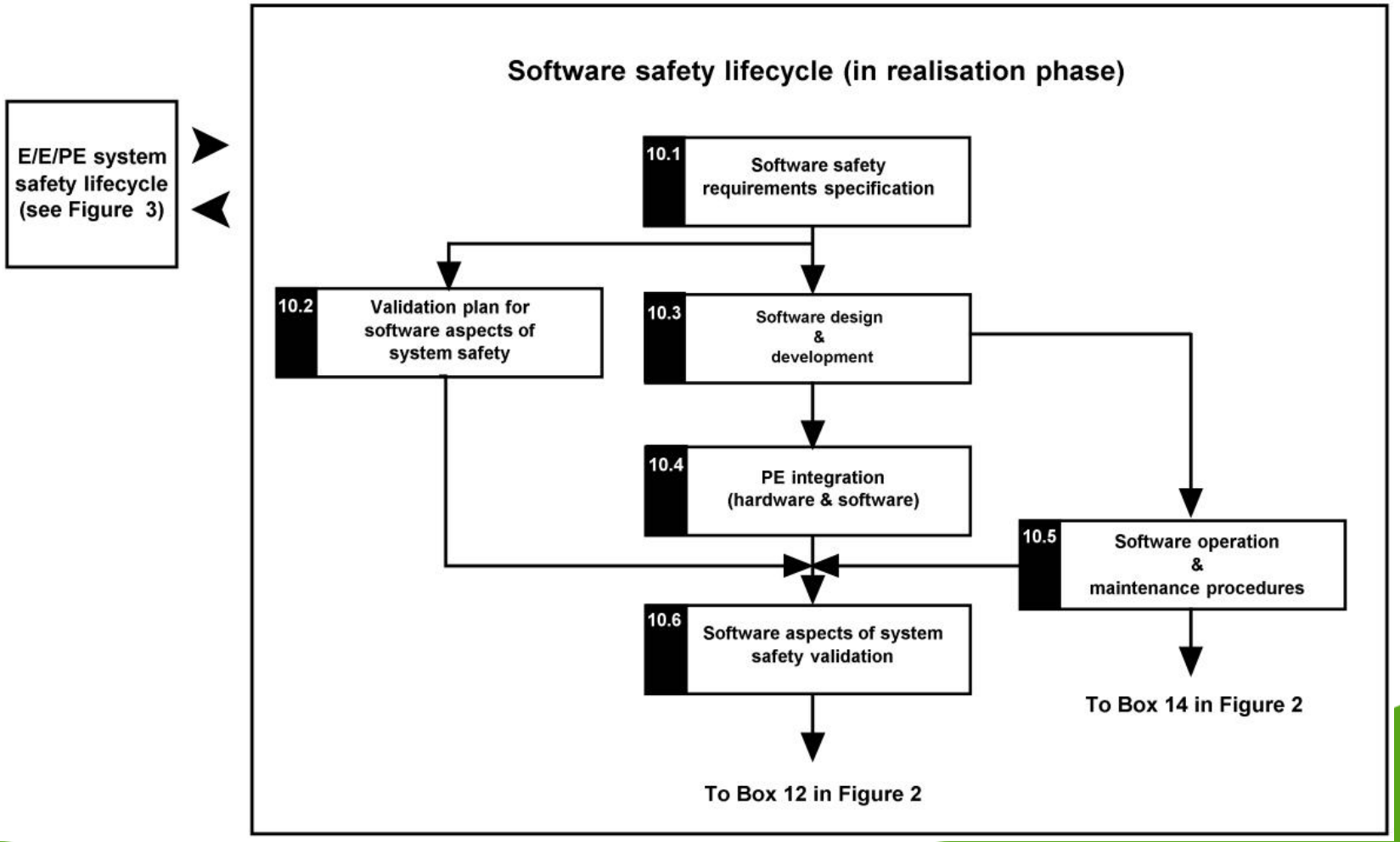
EN 50128 : 2011 sovellusala

- 1.1 This European Standard specifies the process and technical requirements for the development of software for programmable electronic systems for use in railway control and protection applications. It is aimed at use in any area where there are safety implications. These systems can be implemented using dedicated microprocessors, programmable logic controllers, multiprocessor distributed systems, larger scale central processor systems or other architectures.
- 1.2 This European Standard is applicable exclusively to software and the interaction between software and the system of which it is part.
- 1.3 This European Standard is not relevant for software that has been identified as having no impact on safety, i.e. software of which failures cannot affect any identified safety functions.
- 1.4 This European Standard applies to all safety related software used in railway control and protection systems, including
  - application programming,
  - operating systems,
  - support tools,
  - firmware.
- Application programming comprises high level programming, low level programming and special purpose programming (for example: Programmable logic controller ladder logic).

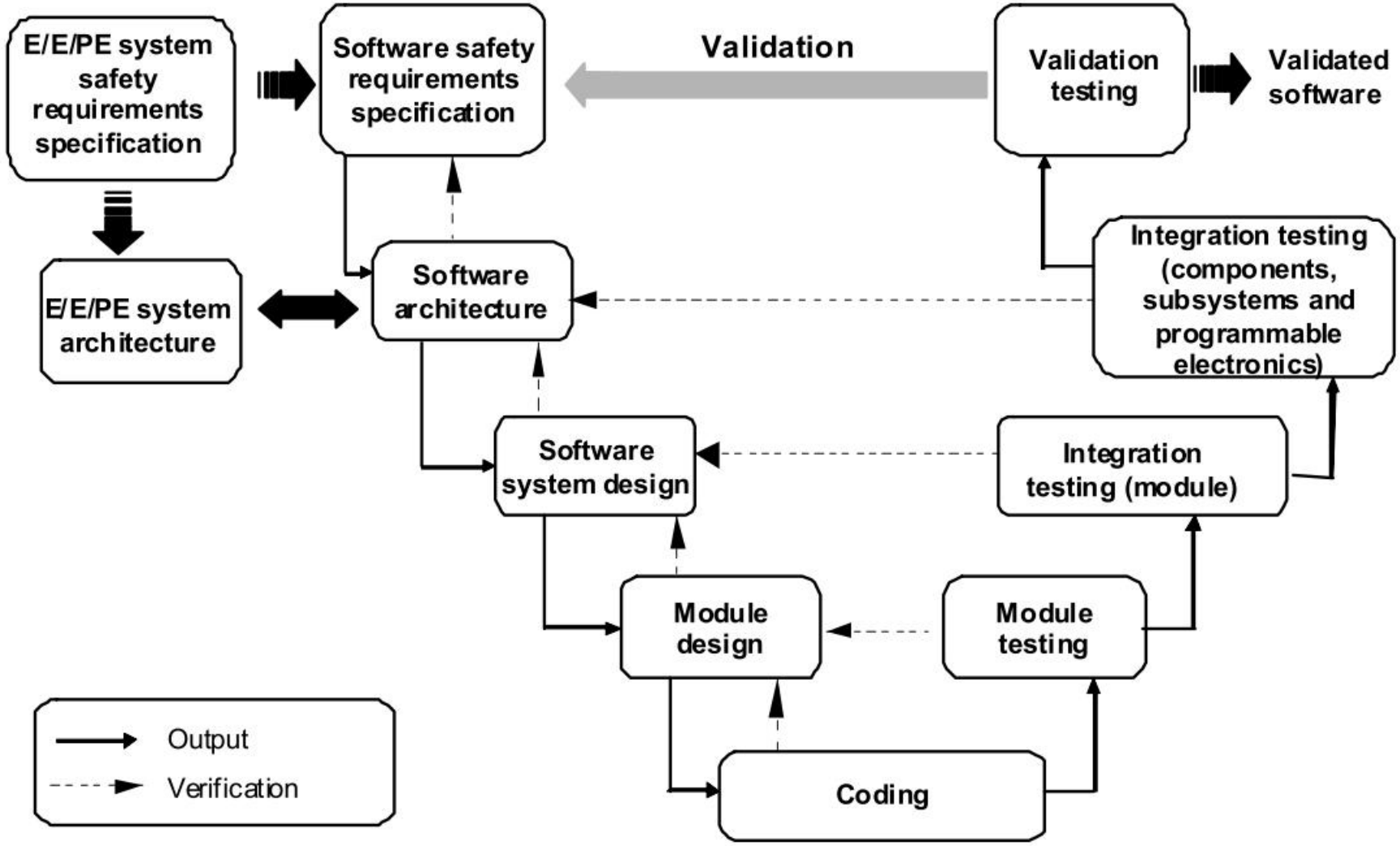
EN 50128 : 2011 sovellusala

- 1.5 This European Standard also addresses the use of pre-existing software and tools. Such software may be used, if the specific requirements in 7.3.4.7 and 6.5.4.16 on pre-existing software and for tools in 6.7 are fulfilled.
- 1.6 Software developed according to any version of this European Standard will be considered as compliant and not subject to the requirements on pre-existing software.
- 1.7 This European Standard considers that modern application design often makes use of generic software that is suitable as a basis for various applications. Such generic software is then configured by data, algorithms, or both, for producing the executable software for the application. The general Clauses 1 to 6 and 9 of this European Standard apply to generic software as well as for application data or algorithms. The specific Clause 7 applies only for generic software while Clause 8 provides the specific requirements for application data or algorithms.
- 1.8 This European Standard is not intended to address commercial issues. These should be addressed as an essential part of any contractual agreement. All the clauses of this European Standard will need careful consideration in any commercial situation.
- 1.9 This European Standard is not intended to be retrospective. It therefore applies primarily to new developments and only applies in its entirety to existing systems if these are subjected to major modifications. For minor changes, only 9.2 applies. The assessor has to analyse the evidences provided in the software documentation to confirm whether the determination of the nature and scope of software changes is adequate. However, application of this European Standard during upgrades and maintenance of existing software is highly recommended.

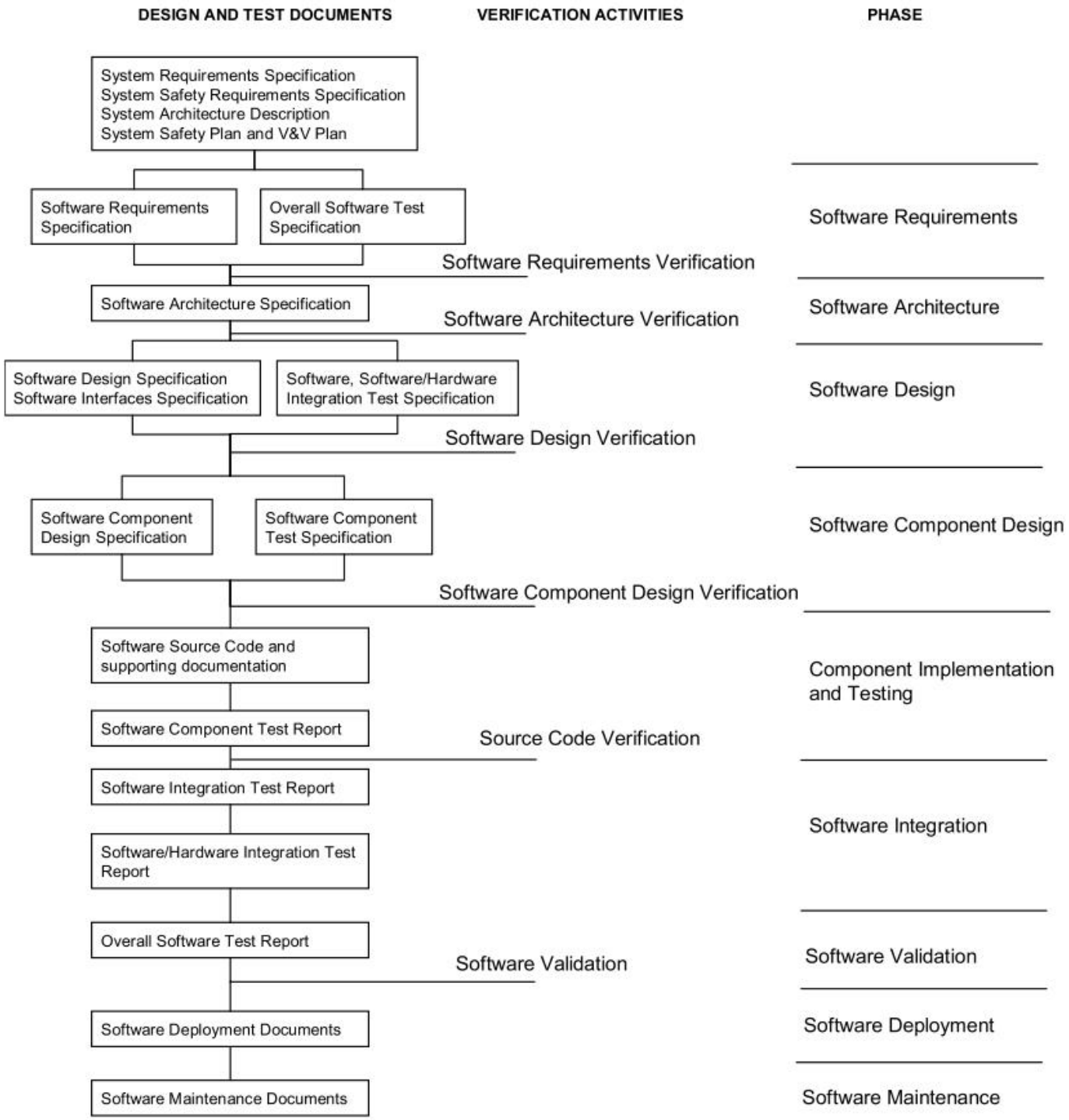
IEC 61508-3 : 2010
Ohjelmiston turvallisuuden elinkaari



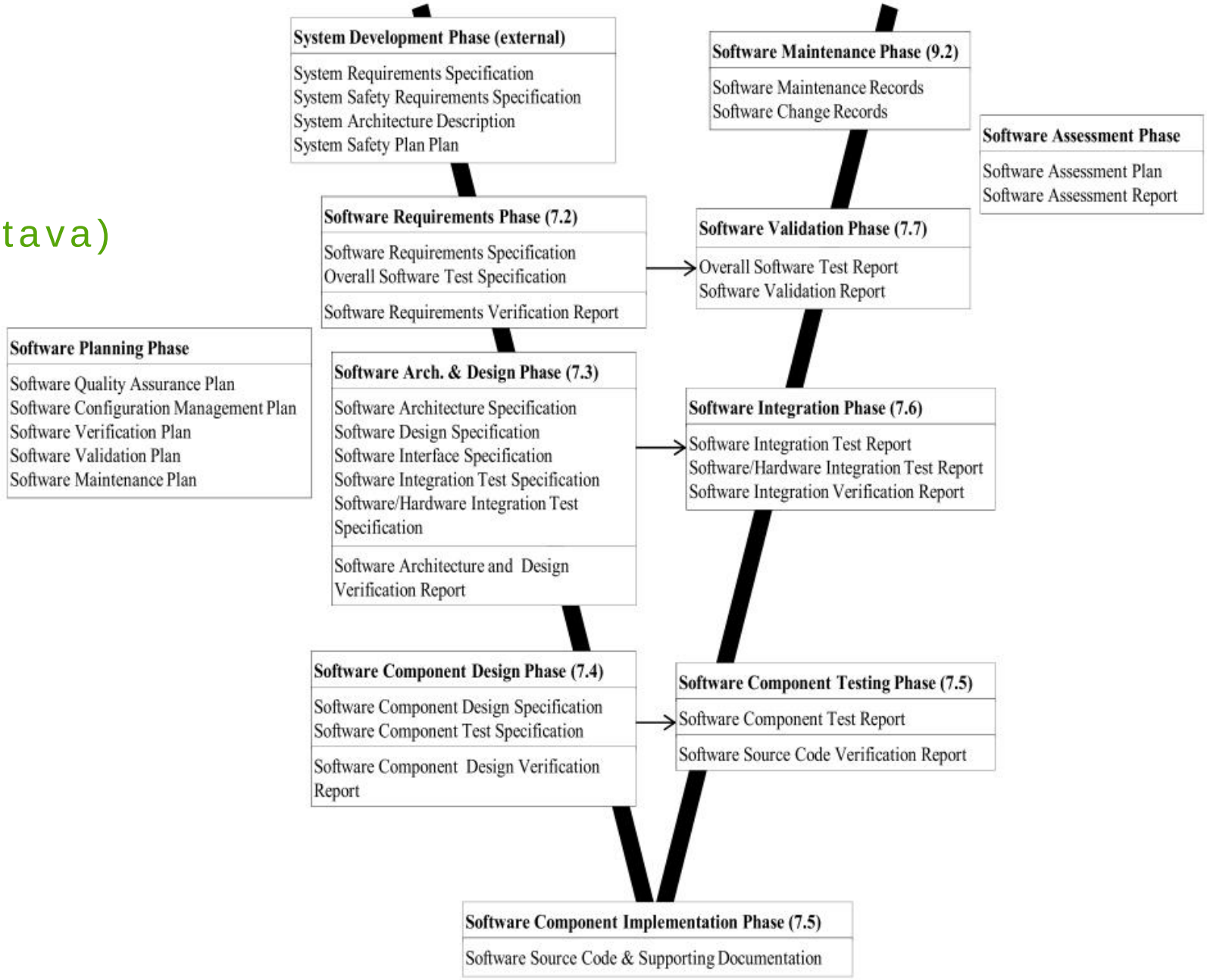
IEC 61508-3 Ohjelmiston systemaattinen kyvykkyys ja ohjelmiston kehittämisen elinkaari (V-malli)



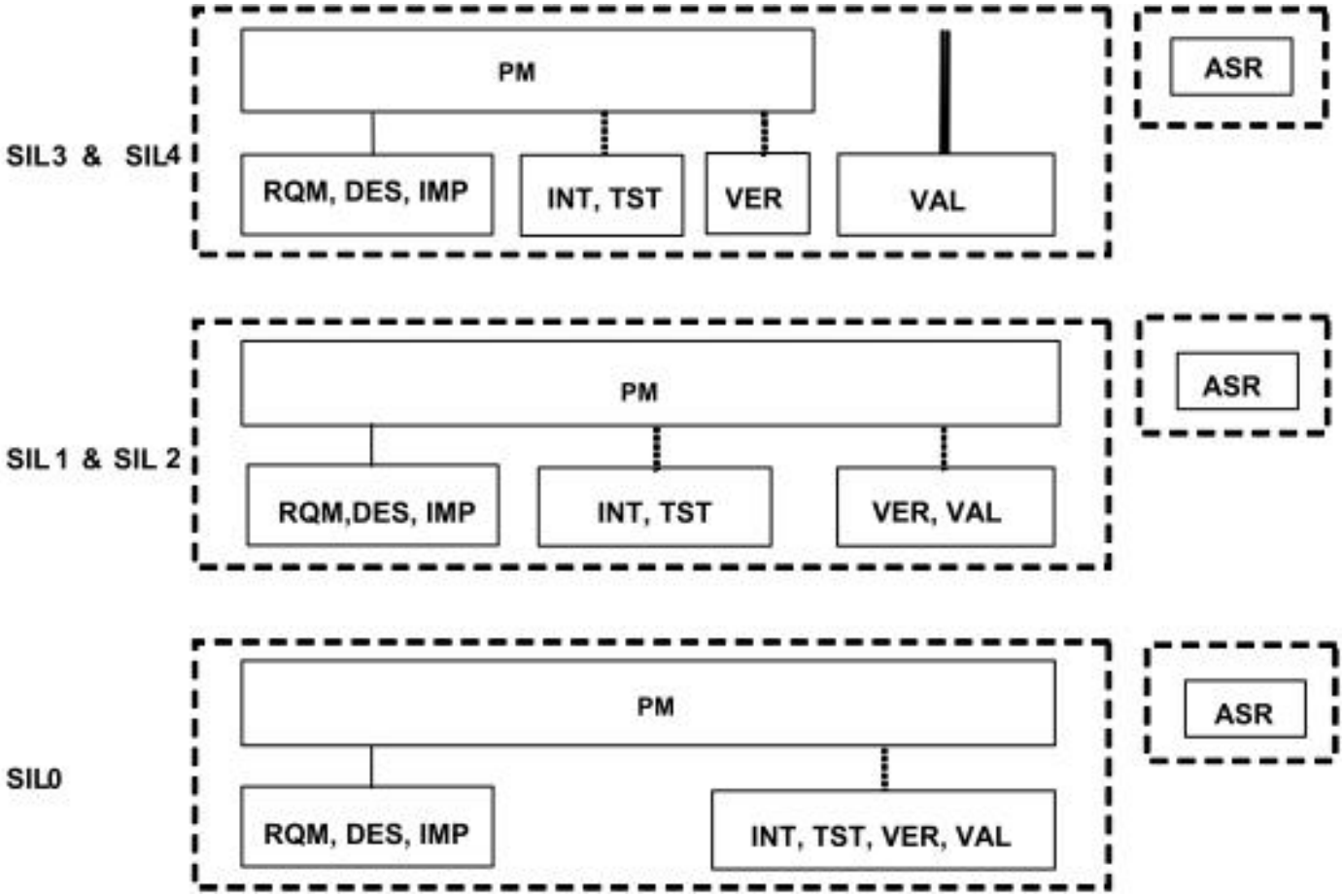
EN 50128 Ohjelmiston kehittämisen elinkaari 1 (havainnollistava)



EN 50128 Ohjelmiston kehittämisen elinkaari 2 (havainnollistava)



EN 50128 Ohjelmiston kehittämisen suositeltava organisaatiorakenne



Key

	can be the same person
	can be the same organization
———	shall report to the Project Manager
.....	can report to the Project Manager
	shall not report to the Project Manager

PM	Project Manager	**ASR**	Assessor
RQM	Requirements Manager	**INT**	Integrator
DES	Designer	**TST**	Tester
IMP	Implementer	**VER**	Verifier
		VAL	Validator

NOTE For the role of the Configuration Manager, see Table B.10, there are no independence requirements

Ohjelmiston toiminnallisen turvallisuuden arviointi

- IEC 61508-3 : 2010 Software functional safety assessment
  - ”To investigate and arrive at a judgement on the software aspects of the functional safety achieved by the E/E/PE safety-related systems”

- EN 50128 : 2011 Assessment
  - “Process of analysis to determine whether software, which may include process, documentation, system, subsystem hardware and/or software components, meets the specified requirements and to form a judgement as to whether the software is fit for its intended purpose. Safety assessment is focused on but not limited to the safety properties of a system”

- Uusittu EN 50128 : 2011 ei esitä tekniikoita ja toimenpiteitä toiminnallisen turvallisuuden arviointiin
  - Vanha EN 50128 : 2001 esittää enemmän tekniikoita ja toimenpiteitä arviointiin kuin IEC 61508-3 : 2010

- EN 50128 : 2011 huomioi selkeästi EN ISO 9001 vaatimustenmukaisuuden

Aiemmin kehitetyt ohjelmistot

- IEC 61508-3 : 2010
  - Pre-Existing Software Elements and Packages – compliance routes
    - Route 1_S: compliant development. Compliance with the requirements of this standard for the avoidance and control of systematic faults in software;
    - Route 2_S: proven in use. Provide evidence that the element is proven in use. See 7.4.10 of IEC 61508-2;
    - Route 3_S:assessment of non-compliant development. Compliance with 7.4.2.13.
  - Provide a safety manual that gives a sufficiently precise and complete description of the element to make possible an assessment of the integrity of a specific safety function that depends wholly or partly on the pre-existing software element.
  -
- EN 50128 : 2011
  - Generic Software : software which can be used for a variety of installations purely by the provision of application-specific data and/or algorithms
  - Pre-Existing Software : pre-existing software all software developed prior to the application currently in question is classed as pre-existing software including
    - COTS (commercial off-the-shelf) and open source software,
    - software previously developed
  - EN 50129 : Generic Product / Generic Application / Specific Application

- Molemmat standardit asettavat erityisiä vaatimuksia eri kohdissa

IEC 61508-3 : 2010 turvallisuuskäsikirja – lisävaatimuksia ohjelmiston elementeille

- ’Turvallisuuskäsikirja vaatimustenmukaisille tuotteille’ vaatimukset esitetään standardissa IEC 61508-2
  - määritellään turvallisuuteen liittyvät tiedot, jotka käyttäjän on saatava
  - ennalta kehitettyjen ohjelmistojen osalta IEC 61508-3 esittää lisävaatimuksia
  - jos turvallisuuden arviointi estyy tietojen saatavuuden takia, standardin vaatimuksia ei täytetä!

- Vaatimukset mahdollistavat ohjelmistokomponenttien kierrätyksen
  - kaikkien ohjelmistokehittäjien on esitettävä täsmennetyt ohjelmiston kuvaukset ja tiedot väittäessään ohjelmiston olevan IEC 61508 vaatimusten mukainen
  - aiemmin kehitettyjen ohjelmistokomponenttien arviointi

- IEC 61508-3 velvoittava liite D määrittelee tiedot ja perustelut, jotka tulee käsitellä ohjelmistoelementin turvallisuuskäsikirjassa

- Vastaavia käsitteitä standardissa EN 50128 : 2011
  - Software Release and Deployment Plan
  - Software Deployment Manual
  - Release Notes

IEC 61508-3 : 2010
Tekniikat ja toimenpiteet

- Liite A (velvoittava) – Ohje tekniikoiden ja toimenpiteiden valintaan
  - vahvasti suositeltu (HR), suositeltu (R), ei suositusta (-), ehdottomasti ei suositeltu (NR) tietylle eheystasolle
  - ei tarkasti määriteltyä dokumentaatiokehystä
  - ennalta määritellyt vaihtoehtoisten tekniikoiden ja toimenpiteiden ryhmät
  - tekniikat ja toimenpiteet toiminnallisen turvallisuuden arviointiin

- Liite B (opastava) – Yksityiskohtaiset taulukot

- Liite C (opastava) – Ohjelmiston systemaattisen kyvykkyyden ominaisuudet
  - opastusta tekniikoiden ja toimenpiteiden valintaan
  - täydentää liitteiden A ja B taulukoita

- Liite F (opastava) - Tekniikat, joilla saavutetaan ohjelmistoelementtien välinen erillisyys yhdessä tietokoneessa

EN 50128 : 2011
Tekniikat ja toimenpiteet

- Liite A (velvoittava) – Criteria for the Selection of Techniques and Measures
  - pakollinen (M), vahvasti suositeltu (HR), suositeltu (R), ei suositusta (-), ehdottomasti ei suositeltu (NR) tietylle eheystasolle
  - tarkasti määritelty dokumentaatiokehys
  - ennalta määritellyt tekniikoiden ja toimenpiteiden hyväksyttävät yhdistelmät eheystasoittain
  - ei tekniikoita ja toimenpiteitä toiminnallisen turvallisuuden arviointiin

- Liite B (velvoittava) – Key software roles and responsibilities
  - täsmentää roolit ja tehtävät ohjelmiston kehittämisessä

- Liite D (opastava) – Bibliography of techniques

VR TRACK

Ohjelmiston vaatimusmäärittely ja arkkitehtuuri - esimerkki

- IEC 61508-3 : 2010
  - Määrittely: formaalit ja semi-formaalit menetelmät, eteen-/taaksepäin jäljitettävyys, tietokoneavusteiset määrittelytyökalut
  - Arkkitehtuuri: 27 eri tekniikkaa, joista 4:ään vaihtoehtoisten tekniikoiden ryhmään kuuluvat 16 tekniikkaa

- EN 50128 : 2011
  - Määrittely: formaalit menetelmät (matemaattiset), mallinnus, rakenteellinen metodologia, totuustaulukot
  - Arkkitehtuuri: 23 eri tekniikkaa, joista eheystasoille 3 ja 4 ennalta määritelty 2 vaihtoehtoista 5 eri tekniikan ryhmää ja eheystasoille 1 ja 2 ennalta määritelty 4 eri tekniikan ryhmä

VR TRACK

Ohjelmointikielet

- IEC 61508-3 : 2010 taulukko A.3 ’support tools and programming languages’ edellyttää soveltuvia ohjelmointikieliä ja kääntäjiä
  - myös koodausstandardeja edellytetään vaatimuksissa

- EN 50128 : 2011 taulukko A.15 ’textual programming languages’ asettaa suosituksia/rajoituksia käytettäville tekstimuotoisille ohjelmointikielille (esim. ADA, Pascal, C/C++, C#, Java, jne.) ja taulukko A.16 ’diagrammatic languages for application algorithms’ huomioi sovellusohjelmoinnin

KIITOS!