**Introduction**

This European Standard is part of a group of related standards. The others are EN 50126-1:1999 "*Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Basic requirements and generic process*” and EN 50129:2003 "*Railway applications –Communication, signalling and processing systems – Safety related electronic systems for signalling*".

e) plan, monitor and control the technical and managerial activities necessary to translate the System Safety Requirements Specification into a Safety-Related System of a validated safety integrity.

검증된 안전 무결성의 안전관련 계통에 대한 “시스템 안전 요구사항 명세서”로 변환하는데 필요한 기술적이고 관리적인 활동을 계획, 모니터링 합니다.

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.

안전관련 계통 및 기기를 포함하는 설계사양의 명세서로 분해가 이루어지도록 안전무결레벨이 추가적으로 할당되어 수행되어 진다. 이는 궁극적으로 요구되어진 소프트웨어 SIL로 이르게 된다.

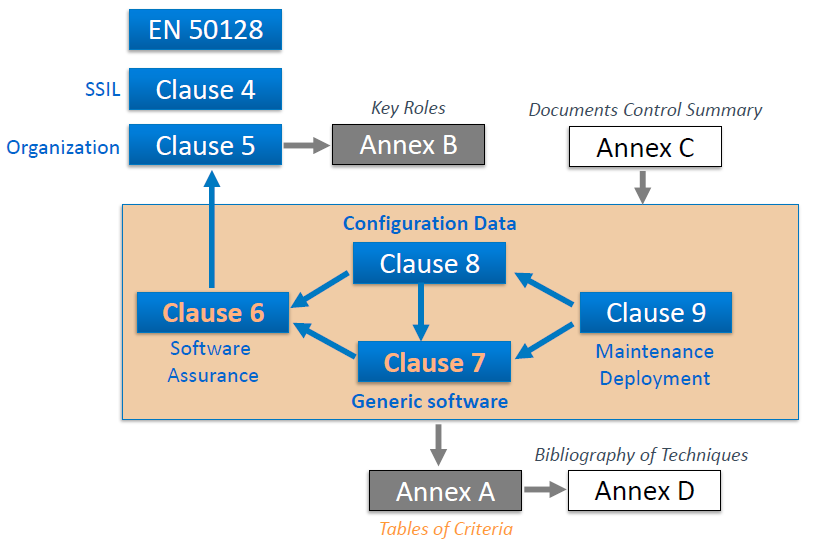
The current state-of-the-art is such that neither the application of quality assurance methods (so-called fault avoiding measures and fault detecting measures) nor the application of software fault tolerant approaches can guarantee the absolute safety of the software. There is no known way to prove the absence of faults in reasonably complex safety-related software, especially the absence of specification and design faults.

현재의 최신 기술은 A도 아닌 B도 아닌 소프트웨어의 절대 안전을 보장할 수 있는 것이다. 상당히 복잡한 안전관련 소프트웨어의 결함 부재를 증명하기 위해 알려진 방법은 없다. 특히 명세서나 설계결함의 부재는 없다.

The principles applied in developing high integrity software include, but are not restricted to

아래의 사항은 높은 무결의 소프트웨어를 개발하는데 적용되지만 아래의 내용으로 한정시키지 않는다.

**EN50128:2011문서구조**

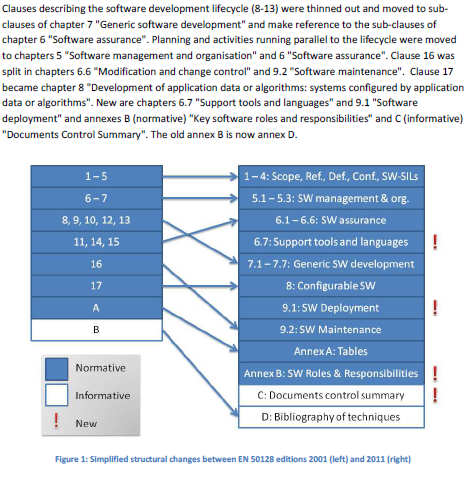


**변경된 내용(EN 50128:2001->2011)**

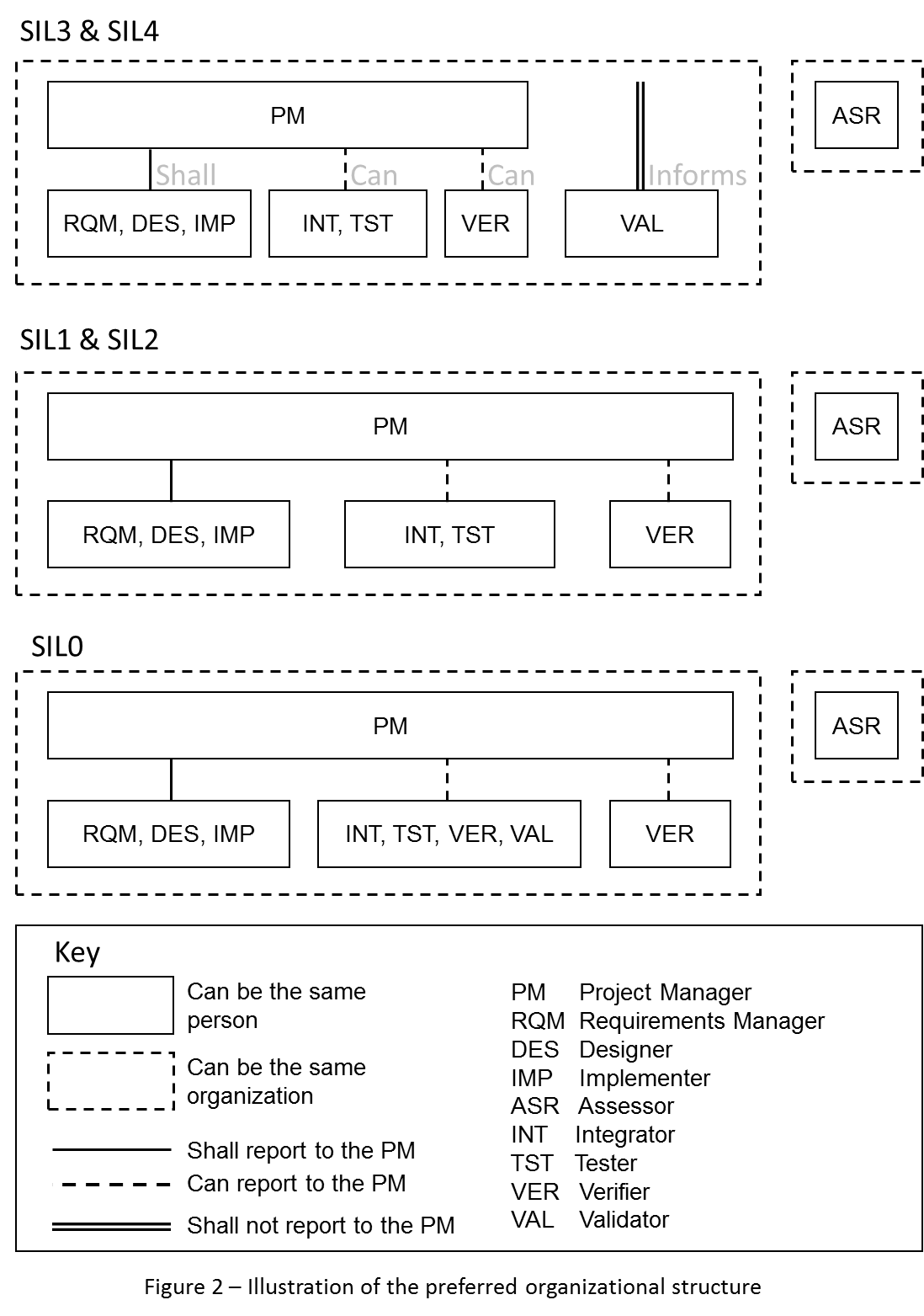
Clauses describing the software development lifecycle (8 clauses of chapter 7 "Generic software development" and make reference to the sub chapter 6 "Software assurance". Planning and activities running parallel to the lifecycle were moved to chapters 5 "Software management and o

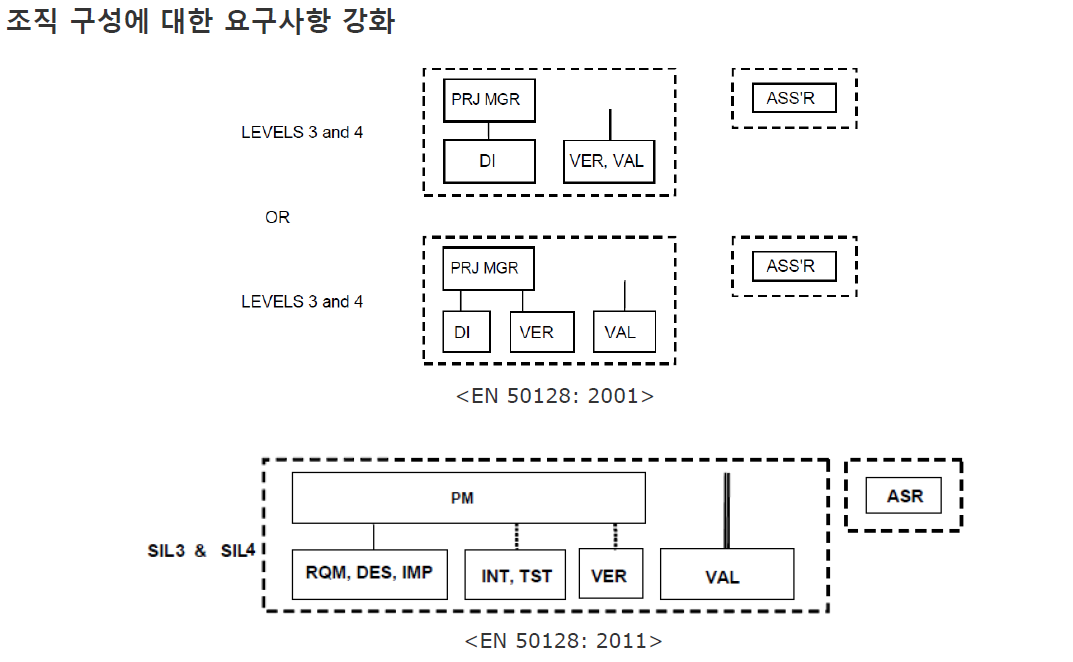
split in chapters 6.6 "Modification and change control" and 9.2 "Software maintenance". Clause 17

became chapter 8 "Development of application data or algorithms: systems configured by application data or algorithms". New are chapters 6.7 "Support tools and languages" and 9.1 "Software deployment" and annexes B (normative) "Key software roles and responsibilities" and C (informative) "Documents Control Summary". The old annex B is now annex D.

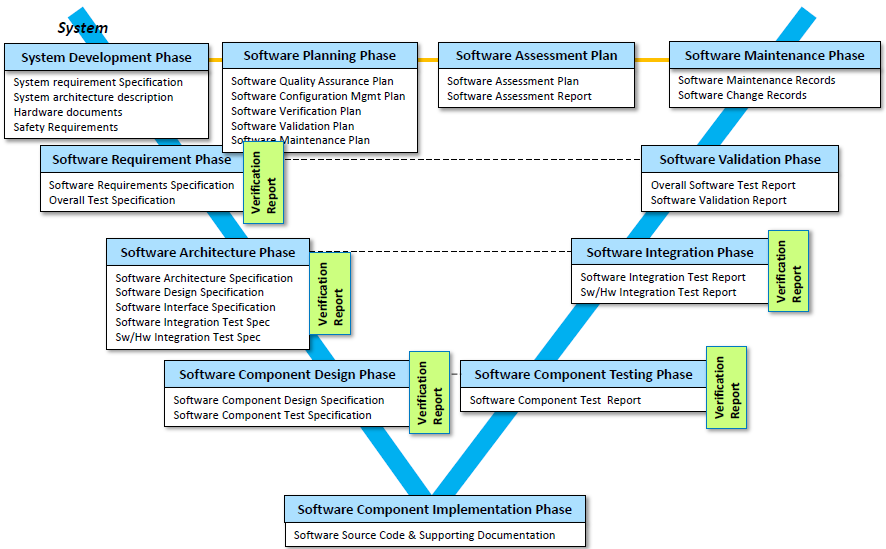


**5. Software management and organization**

**5.1 Organisation, roles and responsibilites**



**EN50128 : 2011 V-Cycle**



**6. Software assurance**

**6.1 Software testing**

**6.1.1 Objective**

6.1.1.1 The objective of software testing, as performed by the Tester and/or Integrator, is to ascertain the behaviour or performance of software against the corresponding test specification to the extent achievable by the selected test coverage.

**6.1.2 Input documents**

1) All necessary System, Hardware and Software Documentation as specified in the Software Verification Plan

**6.1.3 Output documents**

1) 전체의 소프트웨어 시험 명세서(Overall Software Test Specification)

2) 전체의 소프트웨어 시험 보고서(Overall Software Test Report)

3) 소프트웨어 통합 시험 명세서(Software Integration Test Specification)

4) 소프트웨어 통합 시험 보고서(Software Integration Test Report)

5) 소프트웨어/하드웨어 통합 시험 명세서(Software/Hardware Integration Test Specification)

6) 소프트웨어/하드웨어 통합 시험 보고서(Software/Hardware Integration Test Report)

7) 소프트웨어 구성 시험 명세서(Software Component Test Specification)

8) 소프트웨어 구성 시험 보고서(Software Component Test Report)

**6.1.4 Requirements**

6.1.4.4 Each **Test Specification** **shall document** the following:

a) 시험 목적(test objectives)

b) 시험 케이스, 시험 데이터 그리고 시험 예상 결과(test cases, test data and expected results)

c) 수행될 시험의 유형(types of tests to be performed)

d) 시험 환경, 도구, 구성 및 프로그램(test environment, tools, configuration and programs)

e) 시험 완료 판단의 기준(test criteria on which the completion of the test will be judged)

f) 기준 및 완료할 수 있는 시험 범위의 등급(the criteria and degree of test coverage to be achieved)

g) 시험과정에 참여하는 요원의 역할과 책임(the roles and responsibilities of the personnel involved in the test process)

h) 시험사양이 적용되는 요구사항(the requirements which are covered by the test specification)

i) 소프트웨어 시험 장비의 선택과 사용(the selection and utilisation of the software test equipment)

6.1.4.5 A **Test Report shall be produced** as follows:

a) 시험보고서에서는 테스터 이름, 시험결과와 시험명세서에서 시험 목적 및 시험 기준을 충족하였는지의 여부를 기재한다. 실패의 경우 문서화하고 요약한다.

the Test Report shall mention the Tester names, state the test results and whether the test objectives and test criteria of the Test Specification have been met. Failures shall be documented and summarized;

b) 되도록이면 후속 분석을 위하여 기계판독 가능한 형식으로 시험 케이스와 결과는 기록되어야 한다.

test cases and their results shall be recorded, preferably in a machine-readable form for subsequent analysis;

c) 만일 실행 가능하면 시험은 반복적으로 그리고 자동방법으로 이루어져야 한다.

tests shall be repeatable and, if practicable, be performed by automatic means;

d) 자동 시험실행을 위한 시험 스크립트는 확인되어져야 한다.

test scripts for automatic test execution shall be verified;

e) 관련 모든 항목은 문서화 되어져야 한다.

the identity and configuration of all items involved (hardware used, software used, equipment used, equipment calibration, as well as version information of the test specification) shall be documented;

f) 시험 범위와 시험 종료의 평가가 제공되고 시험절차에서의 편차도 기록되어야 한다.

an evaluation of the test coverage and test completion shall be provided and any deviations noted.

**6.2 Software verification**

|  |  |  |  |
| --- | --- | --- | --- |
| **Objective** | The objective of software verification is to examine and arrive at a judgment based on evidence that output items (process, documentation, software or application) of a specific development phase fulfil the requirements and plans with respect to completeness, correctness and consistency. These activities are managed by the Verifier. | | |
| **Input documents : 1** | | **Output documents : 3** | **Requirements : 13** |
| All necessary System, Hardware and Software Documentation. | | 1) Software Verification Plan  2) Software Verification Report(s)  3) Software Quality Assurance Verification Report |  |

|  |
| --- |
| **Requirements** |
| 6.2.4.1 **Verification** shall be documented by at least a **Software Verification Plan** and one or more (process related) **Verification Reports**.  6.2.4.2 A **Software Verification Plan** **shall be written**, under the responsibility of the **Verifier**, on the basis of the necessary documentation.  6.2.4.5 The **Software Verification Plan** shall document all the **criteria, techniques and tools** to be used in the verification process.  The **Software Verification Plan** shall include **techniques and measures** chosen from **Table A.5, Table A.6, Table A.7 and Table A.8**.   * Table A.5 : Verification and Testing * Table A.6 : Integration * Table A.7 : Overall Software Testing * Table A.8 : Software Analysis Techniques.   The selected combination shall be justified as a set satisfying **4.8, 4.9 and 4.10.**   |  | | --- | | 4.8. 표에서 해당하는 기술 또는 계측방법이 **강력한 권고(HR)**인 경우에는 이론적으로 해당 기술이 **소프트웨어 품질 인증 계획** 또는 소프트웨어 품질 인증 계획과 관련된 참조 문건에 **상세하게 기록되어 있지 않으면 사용할 수 없다**. **하지만 해당 표에서 제공하는 기술들이 검증된 기술들의 조합인 경우에는 그 기술을 사용**할 수 있다.  4.9. 표에 존재하지 않는 기술이나 계측방법이 요구되는 경우에는 요구사항을 상세하게 만족해야 하며, 소프트웨어 품질 인증 계획 문서 또는 소프트웨어 품질 인증 계획과 관련된 참고문헌상의 각 조항의 목적에 부합됨을 증명해야 한다.  4.10. **요구 사항의 만족은 각 조항의 요구 사항을 대상**으로 하며, **각각의 기술과 측정 방법은** 이 표준 및 객관적인 증거 그리고 시험을 근거로 한 입증에 따른 **검사 항목 문서를 바탕으로 상세히 평가된 표를 만족**해야 한다. |   6.2.4.6 The Software Verification Plan shall describe the activities to be performed to ensure correctness(정확성) and consistency(일괄성) with respect to the input to that phase. These include reviewing, testing and integration.  6.2.4.7 **In each development phase** it shall be shown that the **functional, performance and safety requirements** are met.  6.2.4.8 The **results of each verification** shall be retained in a **format defined** or **referenced in the Software Verification Plan**.  6.2.4.9 The **Software Verification Plan** shall address the following:  a) the selection of verification strategies and techniques (to avoid undue complexity in the assessment of the verification and testing, preference shall be given to the selection of techniques which are in themselves readily analysable);  b) selection of techniques from Table A.5, Table A.6, Table A.7 and Table A.8;  c) the selection and documentation of verification activities;  d) the evaluation of verification results gained;  e) the evaluation of the safety and robustness requirements;  f) the roles and responsibilities of the personnel involved in the verification process;  g) the degree of the functional based test coverage required to be achieved;  h) the structure and content of each verification step, especially for the Software Requirement Verification (7.2.4.22), Software Architecture and Design Verification (7.3.4.41, 7.3.4.42), Software Components Verification (7.4.4.13), Software Source Code Verification (7.5.4.10) and Integration Verification (7.6.4.13) in a way that facilitates review against the Software Verification Plan. |

| **구분** | **clause** | **단계** | **Input documents** | **Output documents** |  |
| --- | --- | --- | --- | --- | --- |
| **6. Software assurance** | **6.1** | **Software testing** | All necessary System, Hardware and Software Documentation as specified in the Software Verification plan | 1) Overall Software Test Specification  2) Overall Software Test Report  3) Software Integration Test Specification  4) Software Integration Test Report  5) Software/Hardware Integration Test Specification  6) Software/Hardware Integration Test Report  7) Software Component Test Specification  8) Software Component Test Report |  |
| **6.2** | **Software verification** | All necessary System, Hardware and Software Documentation. | 1) Software Verification Plan  2) Software Verification Report(s)  3) Software Quality Assurance Verification Report |  |
| **6.3** | **Software validation** | All system, hardware and software documentation as specified in this European Standard. | 1) Software Validation Plan  2) Software Validation Report  3) Software Validation Verification Report |  |
| **6.4** | **Software assessment** | 1) System Safety Requirements Specification  2) Software Requirements Specification  3) All other documents necessary to carry out the assessment process. | 1) Software Assessment Plan  2) Software Assessment Report  3) Software Assessment Verification Report |  |
| **6.5** | **Software quality assurance** | All the documents available at each stage of the lifecycle. | 1) Software Quality Assurance Plan  2) Software Configuration Management Plan, if not available at system level  3) Software Quality Assurance Verification Report |  |
| **6.6** | **Modification and change control** | 1) Software Quality Assurance Plan  2) Software Configuration Management Plan  3) All relevant design, development and analysis documentation  4) Change Requests  5) Change impact analysis and authorisation | 1) All changed input documents  2) Software Change records (see 9.2.4.11)  3) New Configuration records |  |
| **6.7** | **Support tools and languages** | Tools specification or manual. | Tools validation report (when needed see 6.7.4.4 or 6.7.4.6) |  |
| **7. Generic software development** | **7.2** | **Software requirements** | 1) System Requirements Specification  2) System Safety Requirements Specification  3) System Architecture Description  4) External Interface Specifications (e.g. Software/Software Interface Specification, Software/Hardware  Interface Specification)  5) Software Quality Assurance Plan  6) Software Validation Plan | 1) Software Requirements Specification  2) Overall Software Test Specification  3) Software Requirements Verification Report |  |
| **7.3** | **Architecture and Design** | 1) Software Requirements Specification | 1) Software Architecture Specification  2) Software Design Specification  3) Software Interface Specifications  4) Software Integration Test Specification  5) Software/Hardware Integration Test Specification  6) Software Architecture and Design Verification Report |  |
| **7.4** | **Component design** | 1) Software Design Specification | 1) Software Component Design Specification  2) Software Component Test Specification  3) Software Component Design Verification Report |  |
| **7.5** | **Component implementation and testing** | 1) Software Component Design Specification  2) Software Component Test Specification | 1) Software Source Code and supporting documentation  2) Software Component Test Report  3) Software Source Code Verification Report |  |
| **7.6** | **Integration** | 1) Software/Hardware Integration Test Specification  2) Software Integration Test Specification | 1) Software Integration Test Report  2) Software/Hardware Integration Test Report  3) Software Integration Verification Report |  |
| **7.7** | **Overall Software Testing / Final Validation** | 1) Software Requirements Specification  2) Overall Software Test Specification  3) Software Verification Plan  4) Software Validation Plan  5) All Hardware and Software Documentation including intermediate verification results  6) System Safety Requirements Specification | 1) Overall Software Test Report  2) Software Validation Report  3) Release Note |  |
| **8. Development of application data or algorithms: systems configured by application data**  **or algorithms** |  |  | 1) Software Requirements Specification of generic software  2) Software Architecture Specification of generic software  3) Application conditions of the generic software and application tools  4) User manuals of the generic software and application tools | 1) Application Preparation Plan  2) Application Requirements Specification  3) Application Architecture and Design  4) Application Test Specification  5) Application Test Report  6) Application Preparation Verification Report  7) Source Code of Application Data/Algorithms  8) Application Data/Algorithms Verification Report |  |
| **9. Software deployment and maintenance** |  |  | All design, development and analysis documents relevant to the deployment. | 1) Software Release and Deployment Plan  2) Software Deployment Manual  3) Release Notes  4) Deployment Records  5) Deployment Verification Report |  |