|  |  |  |
| --- | --- | --- |
| **14** | **PROGRAMMABLE ELECTRICAL MEDICAL SYSTEMS (PEMS)** |  |
| 14.1 | Requirements in 14.2 to 14,12 not applied to pems when it provides no functionality necessary for basic safety or essential performance, or |  |  |
|  | - when application of risk management showed that failure of pess does not lead to unacceptable risk………………………………..: |  |  |
|  | risk management file contains an assessment of risks associated with the failure of the pess:(ISO 14971 Cl. 5.2-5.5, 6) |  |  |
|  | Requirements of 14.13 not applied to pems intended to be incorporated into an it network |  |  |
|  | When the requirements of 14.2 to 14.13 apply, the requirements of IEC 62304:2006 and IEC 62304:2006/amd1:2015 clause 4.3, 5, 7, 8 and 9 apply for the development or modification of software of each pess |  |  |
|  | Software development process for Software Classification applied in accordance with Clause 4.3 and 4.4 of IEC 62304:2006 and IEC 62304:2006/amd1:2015…………………………..: |  |  |
|  | Software development process applied according to Clause 5 of IEC 62304:2006 and IEC 62304:2006/amd1:2015……………………: |  |  |
|  | Software development process for Software risk management applied according to Clause 7 of IEC 62304:2006 and IEC 62304:2006/amd1:2015………………………….: |  |  |
|  | Software development process Configuration Management applied according to Clause 8 of IEC 62304:2006 and IEC 62304:2006/ amd1:2015…………………………………………: |  |  |
|  | Software development process for Software Problem Resolution applied according to Clause 9 of IEC 62304:2006 and IEC 62304:2006/amd1:2015…………………………..: |  |  |
| 14.2 | Documents required by Clause 14 reviewed, approved, issued and revised according to a formal document control process………………: |  |  |
| 14.3 | Risk management plan required by 4.2.2 includes reference to pems validation plan  |  |  |
| 14.4 | A pems development life-cycle including a set of defined milestones has been documented  |  |  |
|  | At each milestone, activities to be completed, and verification methods to be applied to activities have been defined |  |  |
|  | Each activity including its inputs and outputs defined, and each milestone identifies risk management activities that must be completed before that milestone |  |  |
|  | Pems development life-cycle tailored for a specific development by making plans detailing activities, milestones |  |  |
|  | Pems development life-cycle includes documentation requirements |  |  |
| 14.5 | A documented system for problem resolution within and between all phases and activities of pems development life-cycle has been developed and maintained  |  |  |
| **14.6** | **Risk management process** |  |
| 14.6.1 | Manufacturer considered hazards associated with software and hardware aspects of pems including those associated with the incorporating pems into an it-network, components of third-party origin, legacy subsystems when compiling list of known or foreseeable hazards……………………………..: |  |  |
|  | risk management file includes known or foreseeable hazards associated with software, hardware, incorporation of the pems into an it-network, components of 3rd party origin and legacy subsystems………………………………:(ISO 14971 Cl. 5.3) | RMF Reference to specific hazards:(ISO 14971 Cl. \_\_) |  |
| 14.6.2 | Suitably validated tools and procedures assuring each risk control measure reduces identified risk(s) satisfactorily provided in addition to pems requirements in Clause 4.2.2…: |  |  |
|  | risk management file documents the suitability of tools and procedures to validate each risk control measure…………………………………:(ISO 14971 Cl. 7.1) | RMF Reference to specific risks:(ISO 14971 Cl. \_\_) |  |
| 14.7 | A documented requirement specification for pems and each of its subsystems (e.g. for a pess) which includes essential performance and risk control measures implemented by that system or subsystem………………………:(ISO 14971 Cl. 7.2) | RMF Reference to specific risk controls:(ISO 14971 Cl. \_\_) |  |
| 14.8 | An architecture satisfying the requirement is specified for pems and each of subsystems …..:(ISO 14971 Cl. 7.2) | RMF Reference to specific risk controls:(ISO 14971 Cl. \_\_) |  |
| 14.9 | Design is broken up into sub systems and descriptive data on design environment documented………………………………………: |  |  |
| 14.10 | A verification plan containing the specified information used to verify and document functions implementing basic safety, essential performance, or risk control measures……..:(ISO 14971 Cl. 7.2) | RMF Reference to specific risk controls:(ISO 14971 Cl. \_\_) |  |
|  | – milestone(s) when verification is to be performed for each function |  |  |
|  | – selection and documentation of verification strategies, activities, techniques, and appropriate level of independence of the personnel performing the verification |  |  |
|  | – selection and utilization of verification tools |  |  |
|  | – coverage criteria for verification |  |  |
|  | The verification performed according to the verification plan and results of the verification activities documented |  |  |
| 14.11 | A pems validation plan containing validation of basic safety & essential performance : |  |  |
|  | The pems validation performed according to the pems validation plan with results of pems validation activities and methods used for pems validation documented  |  |  |
|  | The person with overall responsibility for pems validation is independent  |  |  |
|  | All professional relationships of members of pems validation team with members of design team documented in risk management file (ISO 14971 Cl. 7.2) | RMF Reference to specific risk controls:(ISO 14971 Cl. \_\_) |  |
| 14.12 | Continued validity of previous design documentation assessed under a documented modification/change procedure |  |  |
|  | Software Classification for Software changes applied in accordance with Clause 4.3 and 4.4 of IEC 62304:2006 and IEC 62304:2006/ amd1:2015…………………………………………: | Software Class:\_\_ |  |
|  | Software Process for Software changes applied according to Clause 5 of IEC 62304:2006 and IEC 62304:2006/ amd1:2015 : |  |  |
|  | risk management for Software changes applied according to Clause 7 of IEC 62304:2006 and IEC 62304:2006/ amd1:2015 : |  |  |
|  | Configuration management of software changes applied per Clause 8 of IEC 62304:2006 and IEC 62304:2006/ amd1:2015……………………: |  |  |
|  | Problem resolution for Software changes applied according to Clause 9 of IEC 62304:2006 and IEC 62304:2006/ amd1:2015 : |  |  |
| 14.13 | For pems incorporated into an it-network not validated by the pems manufacturer, instructions made available for implementing the connection include the following…………………: |  |  |
|  | a) Purpose of the pems connection to an it-network |  |  |
|  | b) required characteristics of the it-network |  |  |
|  | c) required configuration of the it-network |  |  |
|  | d) technical specifications of the network connection, including security specifications |  |  |
|  | e) intended information flow between the pems, the it-network and other devices on the it-network, and the intended routing through the it-network |  |  |
|  | f) a list of hazardous situations resulting from failure of the it-network to provide the required characteristics(ISO 14971 Cl. 5.2-5.5, 6, 7.1, 7.2) | RMF Reference to specific hazardous situations:(ISO 14971 Cl. \_\_) |  |
|  | **accompanying documents for the responsible organization include the following:** |  |
|  | – statement that connection to it-networks including other equipment could result in previously unidentified risks to patients, operators or third parties |  |  |
|  | – Notification that the responsible organization identify, analyse, evaluate and control these risks |  |  |
|  | – Notification that changes to the it-network could introduce new risks that require additional analysis |  |  |
|  | - Changes to the it-network include: - changes in network configuration - connection of additional items - disconnection of items - update of equipment - upgrade of equipment |  |  |
|  |  |  |  |
|  | **Attachment - Software – IEC 62304:2006+AMD1:2015** | — |
| **4.3** | **[A, B, C] Software safety classification** | — |
|  | a) The manufacturer assigns to each software system a software safety class according to the risk of harm to the patient, operator, or other people resulting from a hazardous situation to which the software system can contribute in a worst-case-scenario |  |  |
|  | The software system is software safety class A if: | — |
|  | – the software system not contribute to a hazardous situation; or |  |  |
|  | – the software system contribute to a hazardous situation which does not result in unacceptable risk after consideration of risk control measures external to the software system |  |  |
|  | The software system is software safety class B if: | — |
|  | – the software system contribute to a hazardous situation which results in unacceptable risk after consideration of risk control measures external to the software system and the resulting possible harm is non-serious injury |  |  |
|  | The software system is software safety class C if: | — |
|  | – the software system contribute to a hazardous situation which results in unacceptable risk after consideration of risk control measures external to the software system and the resulting possible harm is death or serious injury |  |  |
|  | For a software system initially classified as software safety class B or C, the manufacturer has implemented additional risk control measures external to the software system and subsequently has assigned a new software safety classification to the software system |  |  |
|  | c) The manufacturer documents the software safety class assigned to each software system in the risk management file |  |  |
|  | d) When a software system is decomposed into software items, and when a software item is decomposed into further software items, such software items inherit the software safety classification of the original software item (or software system) unless the manufacturer documents a rationale for classification into a different software safety class |  |  |
|  | A rationale explains how the new software items are segregated so that they may be classified separately |  |  |
|  | e) The manufacturer documents the software safety class of each software item if that class is different from the class of the software item from which it was created by decomposition |  |  |
|  | f) When applied to a group of software items, the manufacturer uses the processes and tasks which are required by the classification of the highest-classified software item in the group unless the manufacturer documents in the risk management file a rationale for using a lower classification |  |  |
|  | g) Class C requirements apply for each software system, until a software safety class is assigned  |  |  |
| **4.4** | **[A, B, C] Legacy software** | — |
|  | Clauses 5 through 9 have applied to demonstrate the compliance of legacy software |  |  |
|  | As alternative, clauses 4.4.2 through 4.4.5 have applied to demonstrate the compliance of legacy software |  |  |
| 4.4.2 | [A, B, C] Risk management activities | — |
|  | The manufacturer: |  |
|  | a) assesses any feedback, including post-production information, on legacy software regarding incidents and / or near incidents, both from inside its own organization and / or from users |  |  |
|  | b) performs risk management activities associated with continued use of the legacy software  |  |  |
|  | Considering the following aspects: |  |
|  | – integration of the legacy software in the overall medical device architecture |  |  |
|  | – continuing validity of risk control measures, implemented as part of the legacy software |  |  |
|  | – identification of hazardous situations associated with the continued use of the legacy software |  |  |
|  | – identification of potential causes of the legacy software contributing to a hazardous situations |  |  |
|  | – definition of risk control measures for each potential cause of the legacy software contributing to a hazardous situations |  |  |
| 4.4.3 | [A, B, C] Gap analysis |  |
|  | Based on the software safety class of the legacy software, the manufacturer performs a gap analysis of available deliverables against those required according to 5.2, 5.3, 5.7, and Clause 7 |  |  |
|  | a) The manufacturer assesses the continuing validity of available deliverables |  |  |
|  | b) Where gaps are identified, the manufacturer evaluates the potential reduction in risk resulting from the generation of the missing deliverables and associated activities |  |  |
|  | c) Based on this evaluation, the manufacturer determines the deliverables to be created and associated activities to be performed |  |  |
|  | Software system test records are the minimum deliverables to be created |  |  |
| 4.4.4 | [A, B, C] Gap closure activities |  |
|  | a) The manufacturer establishes and executes a plan to generate the identified deliverables |  |  |
|  | Objective evidences have used to generate required deliverables without performing activities required by 5.2, 5.3, 5.7 and Clause 7 |  |  |
|  | b) The plan addresses the use of the problem resolution process for handling problems detected in the legacy software and deliverables in accordance with Clause 9 |  |  |
|  | c) Changes to the legacy software have performed in accordance with Clause 6. |  |  |
| 4.4.5 | [A, B, C] Rationale for use of legacy software |  |
|  | The manufacturer documents the version of the legacy software together with a rationale for the continued use of the legacy software  |  |  |

|  |  |  |
| --- | --- | --- |
| **5** | **SOFTWARE DEVELOPMENT PROCESS** | **—** |
| **5.1** | **Software development planning** | — |
| 5.1.1 | [A, B, C] The manufacturer establishes a software development plan (or plans) for conducting the activities of the software development process appropriate to the scope, magnitude, and software safety classifications of the software system to be developed. |  |  |
|  | The software development life cycle model is either fully defined or be referenced in the plan (or plans). |  |  |
|  | The plan addresses the following: |  |
|  | a) the processes to be used in the development of the software system |  |  |
|  | b) the deliverables (includes documentation) of the activities and tasks |  |  |
|  | c) traceability between system requirements, software requirements, software system test, and risk control measures implemented in software |  |  |
|  | d) software configuration and change management, including soup configuration items and software used to support development |  |  |
|  | e) software problem resolution for handling problems detected in the medical device software, deliverables and activities at each stage of the life cycle |  |  |
| 5.1.2 | [A, B, C] The manufacturer updates the plan, as appropriate, as development proceeds  |  |  |
| 5.1.3 | [A, B, C] Software development plan reference to system design and development |  |
|  | a) As inputs for software development, system requirements are referenced in the software development plan by the manufacturer |  |  |
|  | b) In the software development plan, the manufacturer includes or references procedures for coordinating the software development with the system development necessary to satisfy 4.1 (such as system integration, verification, and validation) |  |  |
| 5.1.4 | [C] Associated with the development of software items of class C, in the software development plan are included or referenced: |  |
|  | a) standards |  |  |
|  | b) methods |  |  |
|  | c) tools |  |  |
| 5.1.5 | [B, C] The manufacturer includes or references in the software development plan, a plan to integrate the software items (including soup) and performs testing during integration |  |  |
| 5.1.6 | [A, B, C] In the software development plan, the following verification information are included or referenced: |  |
|  | a) deliverables requiring verification |  |  |
|  | b) the required verification tasks for each life cycle activity |  |  |
|  | c) milestones at which the deliverables are verified |  |  |
|  | d) the acceptance criteria for verification of the deliverables |  |  |
| 5.1.7 | [A, B, C] In the software development plan the manufacturer includes or references a plan to conduct the activities and tasks of the software risk management process, including the management of risks relating to soup |  |  |
| 5.1.8 | [A, B, C] In the software development plan the manufacturer includes or references information about the documents to be produced during the software development life cycle |  |  |
|  | For each identified document or type of document the following information has included or referenced: |  |
|  | a) title, name or naming convention |  |  |
|  | b) purpose |  |  |
|  | c) procedures and responsibilities for development, review, approval and modification |  |  |
| 5.1.9 | [A, B, C] The manufacturer includes or references software configuration management information in the software development plan |  |  |
|  | The software configuration management information includes or references: |  |
|  | a) the classes, types, categories or lists of items to be controlled |  |  |
|  | b) the software configuration management activities and tasks |  |  |
|  | c) the organization(s) responsible for performing software configuration management and activities |  |  |
|  | d) their relationship with other organizations, such as software development or maintenance |  |  |
|  | e) when the items are to be placed under configuration control |  |  |
|  | f) when the problem resolution process is to be used |  |  |
| 5.1.10 | [B, C] The items to be controlled include tools, items or settings, used to develop the medical device software, which could impact the medical device software |  |  |
| 5.1.11 | [B, C] The manufacturer plans to place configuration items under documented configuration management control before they are verified |  |  |
| 5.1.12 | [B, C] In the software development plan the manufacturer includes or references a procedure for: |  |
|  | a) identifying categories of defects that may be introduced based on the selected programming technology that are relevant to their software system |  |  |
|  | b) documenting evidence that demonstrates that these defects do not contribute to unacceptable risk |  |  |
| **5.2** | **Software requirements analysis** | — |
| 5.2.1 | [A, B, C] For each software system of the medical device, the manufacturer defines and documents software system requirements from the system level requirements |  |  |
| 5.2.2 | [A, B, C] As appropriate to the medical device software, the manufacturer includes in the software requirements: |  |
|  | a) functional and capability requirements |  |  |
|  | b) software system inputs and outputs |  |  |
|  | c) interfaces between the software system and other systems |  |  |
|  | d) software-driven alarms, warnings, and operator messages |  |  |
|  | e) security requirements |  |  |
|  | f) user interface requirements implemented by software |  |  |
|  | g) data definition and database requirements |  |  |
|  | h) installation and acceptance requirements of the delivered medical device software at the operation and maintenance site or sites |  |  |
|  | i) requirements related to methods of operation and maintenance |  |  |
|  | j) requirements related to IT-network aspects |  |  |
|  | k) user maintenance requirements |  |  |
|  | l) regulatory requirements |  |  |
| 5.2.3 | [B, C] The manufacturer includes risk control measures implemented in software in the requirements as appropriate to the medical device software |  |  |
| 5.2.4 | [A, B, C] The manufacturer re-evaluates the medical device risk analysis when software requirements are established and update it as appropriate |  |  |
| 5.2.5 | [A, B, C] The manufacturer ensures that existing requirements, including system requirements, are re-evaluated and updated as appropriate as a result of the software requirements analysis activity |  |  |
| 5.2.6 | [A, B, C] The manufacturer verifies and documents that the software requirements: |  |
|  | a) implement system requirements including those relating to risk control |  |  |
|  | b) do not contradict one another |  |  |
|  | c) are expressed in terms that avoid ambiguity |  |  |
|  | d) are stated in terms that permit establishment of test criteria and performance of tests  |  |  |
|  | e) can be uniquely identified |  |  |
|  | f) are traceable to system requirements or other source |  |  |
| **5.3** | **Software architectural design** |  |
| 5.3.1 | [B, C] The manufacturer transforms the requirements for the medical device software into a documented architecture that describes the software’s structure and identifies the software items |  |  |
| 5.3.2 | [B, C] The manufacturer develops and documents an architecture for the interfaces between the software items and the components external to the software items (both software and hardware), and between the software items |  |  |
| 5.3.3 | [B, C] If a software item is identified as soup, the manufacturer specifies functional and performance requirements for the soup item that are necessary for its intended use |  |  |
| 5.3.4 | [B, C] If a software item is identified as soup, the manufacturer specifies the system hardware and software necessary to support the proper operation of the soup item |  |  |
| 5.3.5 | [C] The manufacturer identifies any segregation between software items that is necessary for risk control, and states how to ensure that such segregation is effective |  |  |
| 5.3.6 | [B, C] The manufacturer verifies and documents that: |  |
|  | a) the architecture of the software implements system and software requirements including those relating to risk control |  |  |
|  | b) the software architecture is able to support interfaces between software items and between software items and hardware |  |  |
|  | c) the medical device architecture supports proper operation of any soup items |  |  |
| **5.4** | **Software detailed design**  |  |
| 5.4.1 | [B, C] The manufacturer subdivides the software until it is represented by software units |  |  |
| 5.4.2 | [C] The manufacturer documents a design with enough detail to allow correct implementation of each software unit |  |  |
| 5.4.3 | [C] The manufacturer documents a design for any interfaces between the software unit and external components (hardware or software), as well as any interfaces between software units, detailed enough to implement each software unit and its interfaces correctly |  |  |
| 5.4.4 | [C] The manufacturer verifies and documents that the software detailed design: |  |
|  | a) implements the software architecture |  |  |
|  | b) is free from contradiction with the software architecture |  |  |
| **5.5** | **Software unit implementation** |  |
| 5.5.1 | [A, B, C] The manufacturer implements each software unit |  |  |
| 5.5.2 | [B, C] The manufacturer establishes strategies, methods and procedures for verifying the software units |  |  |
|  | Where verification is done by testing, the test procedures are evaluated for adequacy |  |  |
| 5.5.3 | [B, C] The manufacturer establishes acceptance criteria for software units prior to integration into larger software items as appropriate, and ensures that software units meet acceptance criteria |  |  |
| 5.5.4 | [C] When present in the design, the manufacturer includes additional acceptance criteria as appropriate for: |  |
|  | a) proper event sequence |  |  |
|  | b) data and control flow |  |  |
|  | c) planned resource allocation |  |  |
|  | d) fault handling (error definition, isolation, and recovery) |  |  |
|  | e) initialisation of variables |  |  |
|  | f) self-diagnostics |  |  |
|  | g) memory management and memory overflows |  |  |
|  | h) boundary conditions |  |  |
| 5.5.5 | [B, C] The manufacturer performs the software unit verification and documents the results |  |  |
| **5.6** | **Software integration and integration testing** |  |
| 5.6.1 | [B, C] The manufacturer integrates the software units in accordance with the integration plan  |  |  |
| 5.6.2 | [B, C] The manufacturer verifies that the software units have been integrated into software items and/or the software system in accordance with the integration plan and retains records of the evidence of such verification |  |  |
| 5.6.3 | [B, C] The manufacturer tests the integrated software items in accordance with the integration plan and documents the results |  |  |
| 5.6.4 | [B, C] For software integration testing, the manufacturer addresses whether the integrated software item performs as intended |  |  |
| 5.6.5 | [B, C] The manufacturer evaluates the integration test procedures for adequacy |  |  |
| 5.6.6 | [B, C] When software items are integrated, the manufacturer conducts regression testing appropriate to demonstrate that defects have not been introduced into previously integrated software |  |  |
| 5.6.7 | [B, C] The manufacturer: |  |
|  | a) documents the test result (pass/fail and a list of anomalies) |  |  |
|  | b) retains sufficient records to permit the test to be repeated |  |  |
|  | c) identifies the tester |  |  |
| 5.6.8 | [B, C] The manufacturer enters anomalies found during software integration and integration testing into a software problem resolution process |  |  |
| **5.7** | **Software system testing** |  |
| 5.7.1 | [A, B, C] Establish tests for software requirements | — |
|  | a) The manufacturer establishes and performs a set of tests, expressed as input stimuli, expected outcomes, pass/fail criteria and procedures, for conducting software system testing, such that all software requirements are covered |  |  |
|  | b) The manufacturer evaluates the adequacy of verification strategies and test procedures. |  |  |
| 5.7.2 | [A, B, C] The manufacturer enters anomalies found during software system testing into a software problem resolution process |  |  |
| 5.7.3 | [A, B, C] When changes are made during software system testing, the manufacturer: |  |
|  | a) repeats tests, performs modified tests or performs additional tests, as appropriate, to verify the effectiveness of the change in correcting the problem |  |  |
|  | b) conducts testing appropriate to demonstrate that unintended side effects have not been introduced |  |  |
|  | c) performs relevant risk management activities as defined in 7.4 |  |  |
| 5.7.4 | [A, B, C] Evaluate software system testing |  |
|  | The manufacturer evaluates the appropriateness of verification strategies and test procedures |  |  |
|  | The manufacturer verifies that: |  |
|  | a) all software requirements have been tested or otherwise verified |  |  |
|  | b) the traceability between software requirements and tests or other verification is recorded |  |  |
|  | c) test results meet the required pass/fail criteria |  |  |
| 5.7.5. | [A, B, C] In order to support the repeatability of tests, the manufacturer documents: |  |
|  | a) a reference to test case procedures showing required actions and expected results |  |  |
|  | b) the test result (pass/fail and a list of anomalies) |  |  |
|  | c) the version of software tested |  |  |
|  | d) relevant hardware and software test configurations |  |  |
|  | e) relevant test tools |  |  |
|  | f) date tested |  |  |
|  | g) the identity of the person responsible for executing the test and recording the test results |  |  |
| **5.8** | **Software release for utilization at a system level** |  |
| 5.8.1 | [A, B, C] The manufacturer ensures that all software verification activities has been completed and the results evaluated before the software is released |  |  |
| 5.8.2 | [A, B, C] The manufacturer documents all known residual anomalies |  |  |
| 5.8.3 | [B, C] The manufacturer ensured that all known residual anomalies have been evaluated to ensure that they do not contribute to an unacceptable risk |  |  |
| 5.8.4 | [A, B, C] The manufacturer documented the version of the medical device software that is being released |  |  |
| 5.8.5 | [B, C] The manufacturer documents the procedure and environment used to create the released software |  |  |
| 5.8.6 | [B, C] The manufacturer ensures that all software development plan (or maintenance plan) activities and tasks are complete along with the associated documentation |  |  |
| 5.8.7 | [A, B, C] For at least a period of time determined as the longer of: the life time of the medical device software as defined by the manufacturer or a time specified by relevant regulatory requirements, the manufacturer archives: |  |
|  | a) the medical device software and configuration items |  |  |
|  | b) the documentation |  |  |
| 5.8.8 | [A, B, C] The manufacturer establishes procedures to ensure that the released medical device software can be reliably delivered to the point of use without corruption or unauthorised change |  |  |
|  | These procedures address the production and handling of media containing the medical device software including as appropriate: |  |
|  | – replication |  |  |
|  | – media labelling |  |  |
|  | – packaging |  |  |
|  | – protection |  |  |
|  | – storage |  |  |
|  | – delivery |  |  |
| **7** | **SOFTWARE RISK MANAGEMENT PROCESS** | **—** |
| **7.1** | **Analysis of software contributing to hazardous situations** | — |
| 7.1.1 | [B, C] The manufacturer identifies software items that could contribute to a hazardous situation identified in the medical device risk analysis activity of ISO 14971  |  |  |
| 7.1.2 | [B, C] The manufacturer identifies potential causes of the software item identified above contributing to a hazardous situation |  |  |
|  | The manufacturer considers potential causes including, as appropriate: |  |
|  | a) incorrect or incomplete specification of functionality |  |  |
|  | b) software defects in the identified software item functionality |  |  |
|  | c) failure or unexpected results from soup |  |  |
|  | d) hardware failures or other software defects that could result in unpredictable software operation |  |  |
|  | e) reasonably foreseeable misuse |  |  |
| 7.1.3 | [B, C] If failure or unexpected results from soup is a potential cause of the software item contributing to a hazardous situation, the manufacturer evaluates as a minimum any anomaly list published by the supplier of the soup item relevant to the version of the soup item used in the medical device to determine if any of the known anomalies result in a sequence of events that could result in a hazardous situation |  |  |
| 7.1.4 | [B, C] The manufacturer documents in the risk management file potential causes of the software item contributing to a hazardous situation  |  |  |
| **7.2** | **Risk control measures** | — |
| 7.2.1 | [B, C] For each case documented in the risk management file where a software item could contribute to a hazardous situation, the manufacturer defines and documents risk control measures in accordance with ISO 14971 |  |  |
| 7.2.2 | [B, C] If a risk control measure is implemented as part of the functions of a software item, the manufacturer: |  |
|  | a) includes the risk control measure in the software requirements |  |  |
|  | b) assigns to each software item that contributes to the implementation of a risk control measure a software safety class based on the risk that the risk control measure is controlling |  |  |
|  | c) develops the software item in accordance with Clause 5 |  |  |
| **7.3** | **Verification of risk control measures** | — |
| 7.3.1 | [B, C] The implementation of each risk control measure documented in 7.2 is verified, and this verification is documented |  |  |
|  | The manufacturer reviewers the risk control measure and determines if it could result in a new hazardous situation |  |  |
| 7.3.3 | [B, C] The manufacturer documents traceability of software hazards as appropriate: |  |
|  | a) from the hazardous situation to the software item |  |  |
|  | b) from the software item to the specific software cause |  |  |
|  | c) from the software cause to the risk control measure |  |  |
|  | d) from the risk control measure to the verification of the risk control measure |  |  |
| **7.4** | **Risk management of software changes** | — |
| 7.4.1 | [A, B, C] The manufacturer analyses changes to the medical device software (including soup) to determine whether: |  |
|  | a) additional potential causes are introduced contributing to a hazardous situation |  |  |
|  | b) additional software risk control measures are required |  |  |
| 7.4.2 | [B, C] The manufacturer analyses changes to the software, including changes to soup, to determine whether the software modification could interfere with existing risk control measures |  |  |
| 7.4.3 | [B, C] The manufacturer performs relevant risk management activities defined in 7.1, 7.2 and 7.3 based on these analyses |  |  |

|  |  |  |
| --- | --- | --- |
| **8** | **SOFTWARE CONFIGURATION MANAGEMENT PROCESS** | **—** |
| **8.1** | **Configuration identification** | — |
| 8.1.1 | [A, B, C] The manufacturer establishes a scheme for the unique identification of configuration items and their versions to be controlled according to the development and configuration planning specified in 5.1 |  |  |
| 8.1.2 | [A, B, C] For each soup configuration item being used, including standard libraries, the manufacturer documents: |  |
|  | a) the title |  |  |
|  | b) the manufacturer |  |  |
|  | c) the unique soup designator |  |  |
| 8.1.3 | [A, B, C] The manufacturer documents the set of configuration items and their versions that comprise the software system configuration |  |  |
| **8.2** | **Change control** | — |
| 8.2.1 | [A, B, C] The manufacturer changes configuration items identified to be controlled according to 8.1 only in response to an approved change request |  |  |
| 8.2.2 | [A, B, C] The manufacturer implements the change as specified in the change request |  |  |
|  | The manufacturer identifies and performs any activity that needs to be repeated as a result of the change, including changes to the software safety classification of software systems and software items |  |  |
| 8.2.3 | [A, B, C] The manufacturer verifies the change, including repeating any verification that has been invalidated by the change and taking into account 5.7.3 and 9.7 |  |  |
| 8.2.4 | [A, B, C] The manufacturer maintains records of the relationships and dependencies between: |  |
|  | a) change request |  |  |
|  | b) relevant problem report |  |  |
|  | c) approval of the change request |  |  |
| 8.3 | [A, B, C] The manufacturer retains retrievable records of the history of controlled configuration items including system configuration |  |  |

|  |  |  |
| --- | --- | --- |
| **9** | **SOFTWARE PROBLEM RESOLUTION PROCESS** | **—** |
| 9.1 | [A, B, C] The manufacturer prepares a problem report for each problem detected in the medical device software |  |  |
|  | Problem reports include a statement of criticality (for example, effect on performance, safety, or security) as well as other information that may aid in the resolution of the problem (for example, devices affected, supported accessories affected) |  |  |
| 9.2 | [A, B, C] The manufacturer: |  |
|  | a) investigates the problem and if possible identify the causes |  |  |
|  | b) evaluates the problem’s relevance to safety using the software risk management process  |  |  |
|  | c) documents the outcome of the investigation and evaluation |  |  |
|  | d) creates a change request(s) for actions needed to correct the problem, or document the rationale for taking no action |  |  |
| 9.3 | [A, B, C] The manufacturer advises relevant parties of the existence of the problem, as appropriate |  |  |
| 9.4 | [A, B, C] The manufacturer approves and implements all change requests, observing the requirements of the change control process  |  |  |
| 9.5 | [A, B, C] The manufacturer maintains records of problem reports and their resolution including their verification |  |  |
|  | The manufacturer updates the risk management file as appropriate  |  |  |
| 9.6 | [A, B, C] The manufacturer performs analysis to detect trends in problem reports |  |  |
| 9.7 | [A, B, C] The manufacturer verifies resolutions to determine whether: |  |
|  | a) problem has been resolved and the problem report has been closed |  |  |
|  | b) adverse trends have been reversed |  |  |
|  | c) change requests have been implemented in the appropriate medical device software and activities |  |  |
|  | d) additional problems have been introduced |  |  |
| 9.8 | [A, B, C] When testing, retesting or regression testing software items and systems following a change, the manufacturer includes in the test documentation: |  |
|  | a) test results |  |  |
|  | b) anomalies found |  |  |
|  | c) the version of software tested |  |  |
|  | d) relevant hardware and software test configurations |  |  |
|  | e) relevant test tools |  |  |
|  | f) date tested |  |  |
|  | g) identification of the tester |  |  |

| **Attachment**  | **Software - Mapping of required evidence and manufacturer documents** |  |
| --- | --- | --- |
| Standard Clause | Deliverables | Title | Revision # | Date |
| 4.3 | Software safety classification document |  |  |  |
| 4.3 | Specification of risk control measures external to software system |  |  |  |
| 4.3 | Rationale of classification for decomposed software system |  |  |  |
| 4.4.2 | Risk management activities for legacy software |  |  |  |
| 4.4.3 | Gap analysis for legacy software |  |  |  |
| 4.4.4 | Gap closure plan for legacy software |  |  |  |
| 4.4.5 | Rationale for use of legacy software |  |  |  |
| 5.1.1 | Software development plan |  |  |  |
| 5.1.3 | Software requirements reference to software design and development document |  |  |  |
| 5.1.4 | Development standards, methods and tools records for class C software |  |  |  |
| 5.1.5 | Software integration and integration testing plan |  |  |  |
| 5.1.6 | Software verification plan |  |  |  |
| 5.1.7 | Software risk management plan |  |  |  |
| 5.1.8 | Document management procedures |  |  |  |
| 5.1.9 | Software configuration management procedures |  |  |  |
| 5.2 | Software system requirements specification |  |  |  |
| 5.2.3 | Specification of risk control measure implemented in software |  |  |  |
| 5.3 | Software system architecture design specification |  |  |  |
| 5.3 | Software item architecture design specification |  |  |  |
| 5.4 | Software item detailed design specification |  |  |  |
| 5.4 | Software unit detailed design specification |  |  |  |
| 5.5.1 | Software unit implementation records |  |  |  |
| 5.5.2 | Software unit verification process |  |  |  |
| 5.5.3 | Software unit acceptance criteria  |  |  |  |
| 5.5.5 | Software unit verification records |  |  |  |
| 5.6.1 | Software unit integration process |  |  |  |
| 5.6.2 | Software unit integration records |  |  |  |
| 5.6.4 | Software unit integration testing records |  |  |  |
| 5.6.5 | Evaluation of software unit integration test |  |  |  |
| 5.6.6 | Software unit regression testing process |  |  |  |
| 5.6.7 | Software unit regression testing records |  |  |  |
| 5.6.8 | Software problem resolution process |  |  |  |
| 5.7 | Software system testing process |  |  |  |
| 5.7 | Software system testing records |  |  |  |
| 5.8 | Software system release process |  |  |  |
| 5.8 | Software system release record |  |  |  |
| 5.8 | Statement of known residual anomalies |  |  |  |
| 7.1 | Software hazard analysis process |  |  |  |
| 7.1 | SOUP anomaly lists |  |  |  |
| 7.2 | Risk control process |  |  |  |
| 7.3 | Risk control verification process |  |  |  |
| 7.4 | Risk management of software change process |  |  |  |
| 8.1 | Configuration identification record |  |  |  |
| 8.2 | Change control process |  |  |  |
| 8.2 | Records for traceability of change |  |  |  |
| 9 | Software problem resolution process |  |  |  |
| 9 | Software problem resolution records |  |  |  |
| **Supplementary information:** |