두산중공업

설계해석용 소프트웨어의 원자력시설용 컴퓨터 소프트웨어의 품질보증요건 적용 방안

두산중공업 품질보증팀 윤종석 과장

목차

DOOSAN

검토 배경

1. 해석용 SW와 관련하여 ASME 2019년 NCA 4000 요건 개정에 따라 Subpart 2.7 원자력시설에 사용되는 소프트웨어 요건 적용이 요구됨
   → 해석용 SW의 개발, 취득(구매), 운영, 유지 및 폐기 시 I&C SW와 동일한 요건 적용 필요

2. 이에 기존 사용 전/사용 중 확인 외에 소프트웨어의 종류(개발/구매) 구분 및 종류에 따른 요건이 세분화 됨에 따라 추가 절차 수립/운영방안을 위해 검토 수행

3. 검토 결과 공유 및 해외 사업 적용 사례 공유를 통해 협회에 건의 사항 및 사업계 전반의 의견 수렴 필요사항을 공유 하기 위함

해석용 SW 관련 ASME 2019ED 개정 사항

해석용 SW와 관련하여 ASME 2019년 NCA 4000 요건 개정(Subpart 2.7 요건 만족이 요구됨)
→ 해석용 SW의 개발, 취득, 운영, 유지 및 폐기 시 I&C SW와 동일한 요건 적용 필요

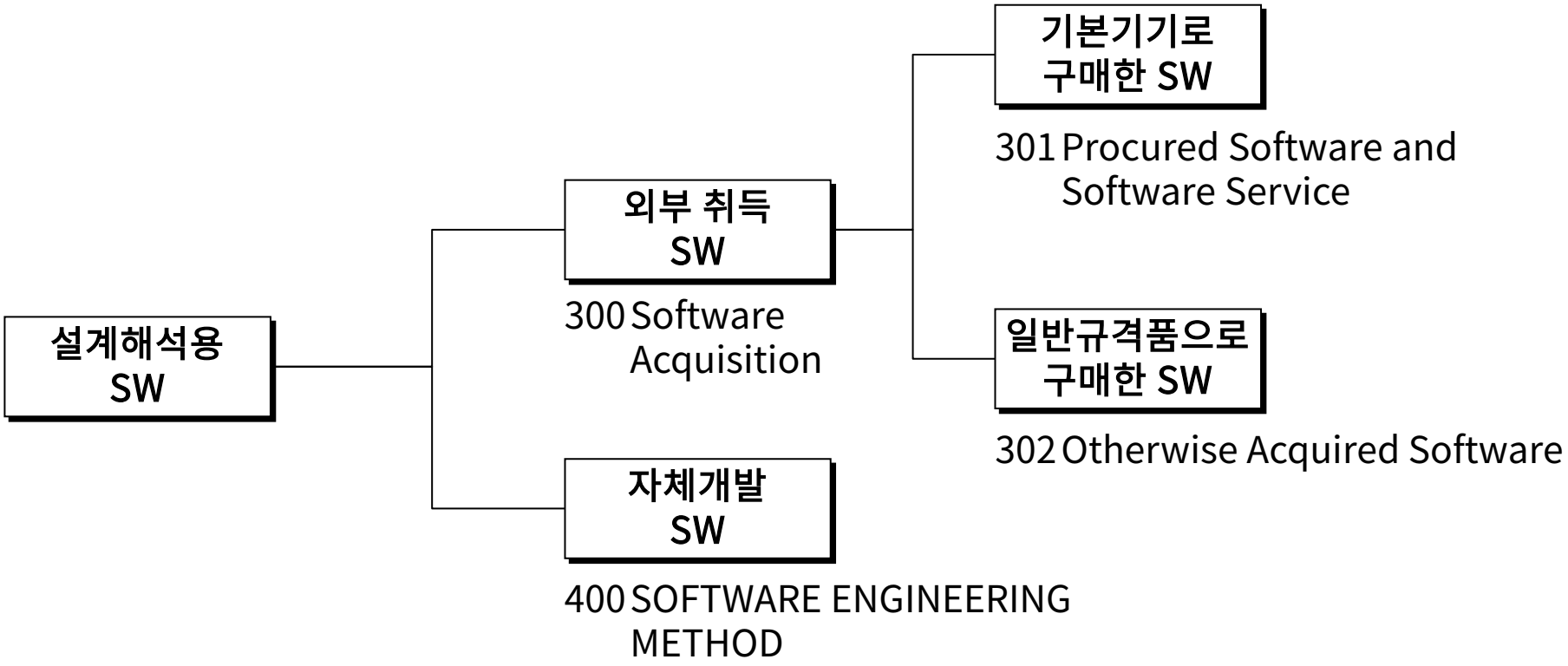
NCA-4134.3 Design Control.
*(a)*The provisions of NQA-1, Requirement 3, shall apply.
(b) Measures shall be established to ensure that applicable requirements of the Design Specifications and of this Section for items are correctly translated into specifications, drawings, procedures, and instructions.
(c) Design documents shall be verified for adequacy and compliance with the Design Specification and this Section.
(d) Computer programs used for design analysis shall meet the requirements of NQA-1, Part II, Subpart 2.7.
(e) Paragraph 601, Configuration Management of Operating Facilities, is not applicable.

SUBPART 2.7
Quality Assurance Requirements for Computer Software for Nuclear Facility Applications

100 GENERAL
Subpart 2.7 provides requirements for the acquisition, development, operation, maintenance, and retirement of software. ~

ASME NQA-1 Subpart 2.7 구조

Subpart 2.7에서 SW는 두가지 형태[1)외부구매, 2)자체개발]로 구분하며 이에 따른 적용 요건 항목은 아래와 같으며 200 공통사항 및 400 번 일부 항목(Acceptance Test 일부요건)은 외부 취득 SW에도 적용



외부취득 소프트웨어-기본기기(NQA-1 Part I 요건 적용)로 구매

외부로부터 구매한 소프트웨어는 NQA-1 Part I 요건을 만족하여 구매 및 수락되어야 함

301 Procured Software and Software Services
Part I, Requirements 4 and 7 for items and services shall be applied to the procurement of software and software services. The Purchaser shall be responsible for the appropriate requirements of this Subpart upon acceptance of the software or related item (e.g., programmable device). Procurement documents shall identify requirements for Supplier's reporting of software errors to the Purchaser and, as appropriate, the Purchaser's reporting of software errors to the Supplier.

기본기기로 구매→Part I 요건 4 및 요건 7을 만족한 구매

- 요건 4를 만족한 구매문서 작성, 검토 및 변경 관리
  - 공급 범위, 기술 & 품질요건, 접근권한, 문서화, 불일치사항 관리
  - 적절한 인원의 검토 등
- 공급업체에 대한 평가 및 승인업체 등록
  - 계약요건에 따라 필요 시 평가를 위해 현지실사 필요
- 공급된 SW 수락을 위해 다음 중 1개 이상의 확인 필요
  - 품질확인서 접수 및 확인 (구매품목 식별, 적용 요건 명시, 해당 시 만족하지 못한 구매요건 명시, 공급자 서명, 확인서 운영 절차 명시, 주기적 공급자 수행 확인(감사, 독립검사 또는 확인시험) 등)
  - 공장확인 (주기적 모니터링, 입회 또는 관찰)
  - 인수검사
  - 설치 후 시험

외부취득 소프트웨어-일반규격품으로 구매

NQA-1요건을 만족한 구매/수락을 못하는 경우 **1) CGID 절차 적용** 또는 **2)개별 해석결과 확인을 통한 검증 중 1가지 방법 적용**

302 Otherwise Acquired Software

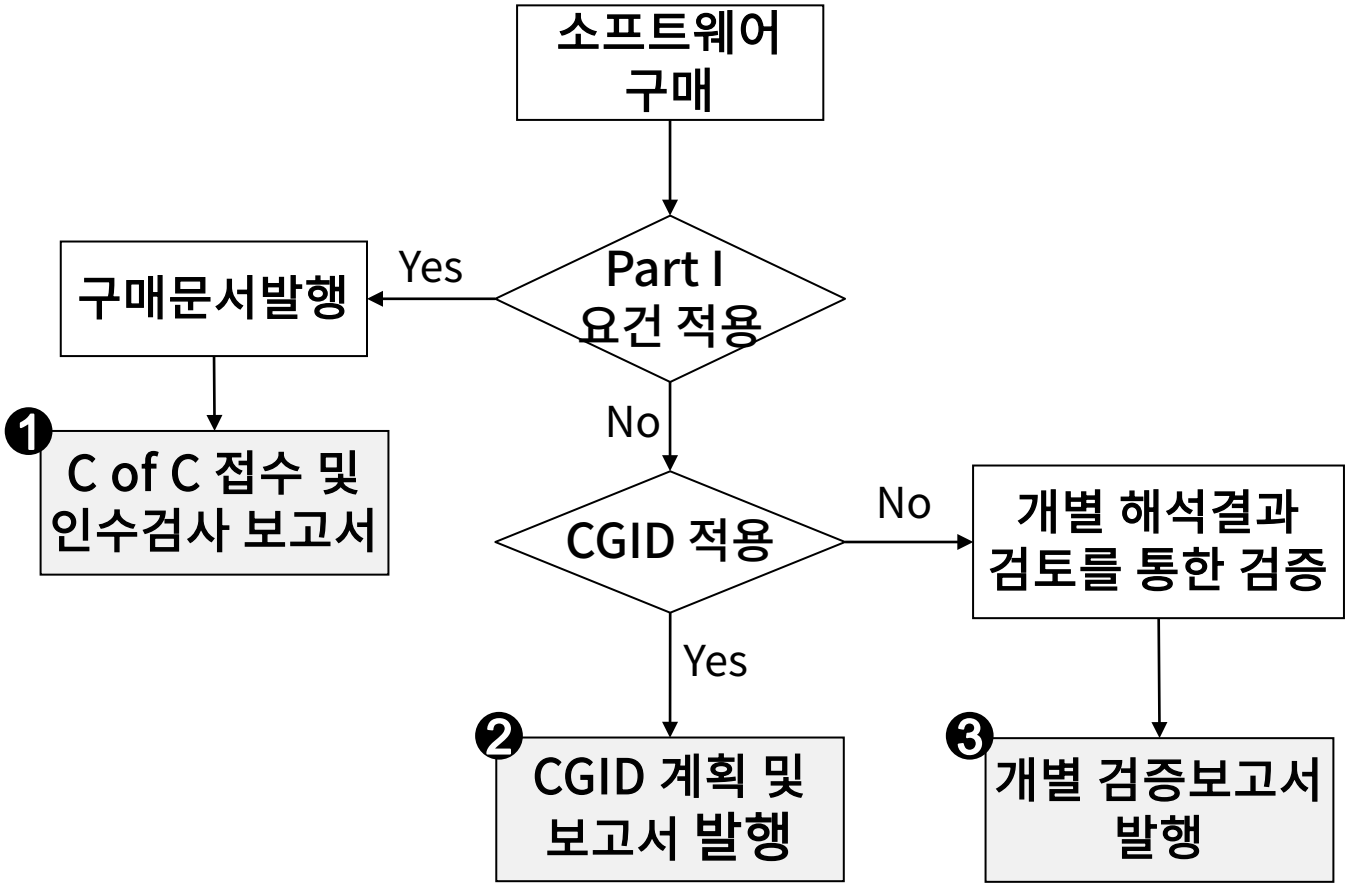
Part I, Requirement 7, and Part II, Subpart 2.14, Quality Assurance Requirements for Commercial Grade Items and Services, shall be applied to acquired software that has not been previously approved under a program consistent with Part I of this Standard for use in its intended application. This includes computer programs not obtained using the procurement requirements of Part I, such as freeware, shareware, and computer programs from corporate repositories. Otherwise acquired computer programs whose results are verified with the design analysis for each application as specified in Part I, Requirement 3, para. 401 are excluded from the requirements of Part II, Subpart 2.14.

CGID를 적용하는 경우 **1) 필수특성 선정, 2) 사용하는 시험계획 및 시험케이스 및 3) 사용지침서를 포함한 Dedication 절차 문서화** 필요

Otherwise acquired computer programs shall be identified and controlled during the dedication process. The dedication process shall be documented and include the following:
(a) identification of the capabilities and limitations for intended use as critical characteristics
(b) utilization of test plans and test cases as the method of acceptance to demonstrate the capabilities within the limitations
(c) instructions for use (e.g., user manual) within the limits of the dedicated capabilities
The dedication process documentation and associated computer program(s) shall establish the current baseline. Subsequent revisions of the software shall be dedicated in accordance with this section.

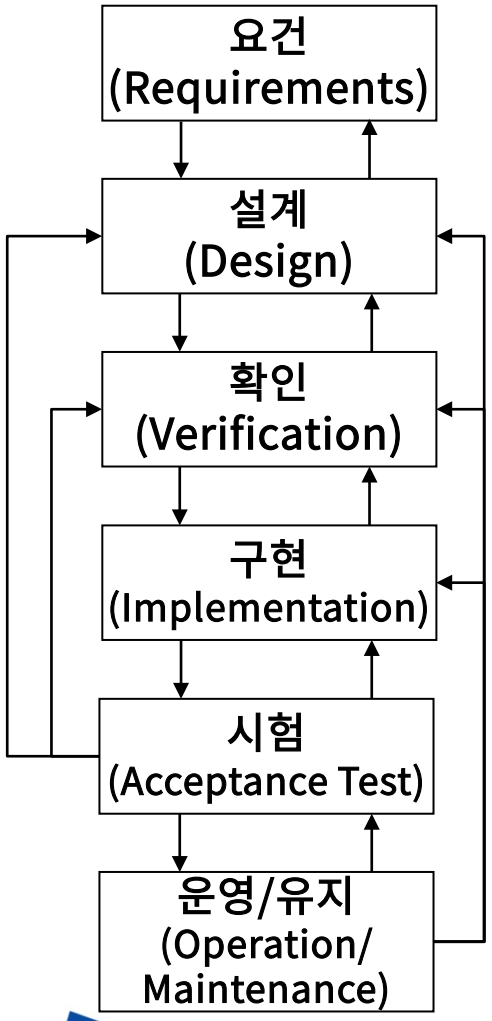
외부취득 소프트웨어-업무 Flow 종합

구매하는 소프트웨어의 경우 다음 업무 Flow에 따라 **3가지 중 1가지 결과물이 문서화 되고 기록관리** 돼야함



자체개발 소프트웨어-소프트웨어 개발 절차

Subpart 2.7의 400 항이 소프트웨어 자체개발 시 적용 해야 하는 요건으로 이를 반영한 운영 및 기록관리 절차가 수립되어야 함



401 Software Design Requirements
- 소프트웨어 설계 전 적용 요건에 대한 문서화→설계시방서 검토

402 Software Design (NQA-1 2015 이전 판의 요건 3 설계관리 내용 이동)
- 설계 계획 및 결과 문서화
- 요건단계 또는 구현단계와 연계하여 문서화 가능

402.1 Software Design Verification
- 원설계를 수행하지 않은 인원/조직이 수행
- 설계 검토, 대체계산, 개발 중 시험 중 1개 이상의 방법으로 수행(복합적으로 수행 가능)

403 Implementation
- 설계계획 및 결과를 실현하기 위한 코딩 및 구현된 프로그램의 통합 및 논리화
- 구현 결과에 대한 확인(Verification) 수행

404 Acceptance Testing
- 시험은 개발된 컴퓨터 프로그램의 적절성을 확인하기 위해 수행
- 공장시험, 현장설치 후 시험, 사용 중 시험을 포함

405 Operation, 406 Maintenance
- 운영: 사용이력, 접근관리, 문제보고, 사용 중 시험, 형상변경 관리 절차 문서화 및 이행
- 보수: 사용자 요구, 설계 요건 변경, 운영환경 변경, 문제 발견에 따른 수정 등 변경 관리 절차 수립 및 이행

소프트웨어 형상관리 (Configuration Management)

형상관리는 소프트웨어 개발, 구매 및 운영 중 관리대상 형상의 변경 유무를 확인하고 변경에 대한 추적, 영향을 확인하는 것으로 1) 관리 대상 형상 식별, 2) 형상 변경 관리, 3)형상 현황 관리 요건이 있음

203 Software Configuration Management
Software configuration management includes, but is not limited to, configuration identification, change control, and configuration status control. Configuration items shall be maintained under configuration management until the software is retired.

형상식별은 다음 세가지 방법을 위한 라벨링 체계를 이행

1) 각 형상품목에 대한 고유의 식별
2) 형상품목 변경의 식별은 개정 별로 식별
3) 사용 가능한 개정된 소프트웨어의 각 형상을 고유 식별할 수 있는 기능을 제공

203.1 Configuration Identification. A labeling system for configuration items shall be implemented that
(a) uniquely identifies each configuration item
(b) identifies changes to configuration items by revision
(c) provides the ability to uniquely identify each configuration of the revised software available for use

소프트웨어 형상관리 (Configuration Management)

형상변경 관리 절차는 변경 요청의 시작, 평가 및 조치, 구현 전 변경 관리 및 승인, 재시험 요건 및 시험결과 승인을 포함해야 함

(a) The software configuration change control process shall include
(1) initiation, evaluation, and disposition of a change request
(2) control and approval of changes prior to implementation
(3) requirements for retesting (e.g., regression testing) and acceptance of the test results

소프트웨어 기준선의 파트로 형상항목은 문서화, 소스/목적/백업 프로그램 및 지원소프트웨어를 포함해야 함
→소프트웨어 개발 시 포함되어야 하는 형상항목

(b) A software baseline shall be established at the completion of each activity of the software design process. Approved changes created subsequent to a baseline shall be added to the baseline. A baseline shall define the most recently approved software configuration. Configuration items to be controlled as part of the baseline shall include, as appropriate
(1) documentation (e.g., software design requirements, instructions for computer program use, test plans, and results)
(2) computer program(s) (e.g., source, object, backup files)
(3) support software

소프트웨어 변경은 문서화되고 변경사항, 변경 사유 및 영향을 받는 기준선의 식별을 포함해야 함

(c) Changes to software shall be formally documented. The documentation shall include
(1) a description of the change
(2) the rationale for the change
(3) the identification of affected software baselines

소프트웨어의 기준선은 소프트웨어 자체, 설치 하드웨어 및 운영시스템을 포함

소프트웨어 형상관리 (Configuration Management)

형상항목의 현황은 유지되고 변경은 제안되고, 승인되나 이행되지 않은 변경 현황을 유지하는 것을 포함하여 관리되야 함

203.3 Configuration Status Control. The status of configuration items resulting from software design shall be maintained current. Configuration item changes shall be controlled until they are incorporated into the approved product baseline. The controls shall include a process for maintaining the status of changes that are proposed and approved but not implemented. The controls shall also provide for notification of this information to affected organizations.

문제보고 및 시정조치 (Problem Reporting and Corrective Action)

하기 내용을 반영한 소프트웨어 문제 보고 및 시정조치 절차 수립 필요

소프트웨어 문제 보고 관련 절차는 문제에 대한 평가 절차, 조치 책임 정의를 포함해야 함
해당 문제가 소프트웨어 에러인 경우 아래사항에 대한 적절한 방법을 제공해야 함
(1) 에러가 적절한 소프트웨어 엔지니어링 요소와 어떻게 관련되는지
(2) 에러가 과거 및 현재 사용 중인 컴퓨터 프로그램의 영향 정도는 얼마인지
(3) 시정조치가 과거 개발 활동에 영향을 어떻게 미치는지
(4) 사용자에게 식별된 에러, 영향, 에러 회피방법, 시정조치 이행 지연에 대해 알림
시정조치 절차는 Part I 요건 16의 적절한 요건에 따라야 함

204 Problem Reporting and Corrective Action
(a) Method(s) for documenting, evaluating, and correcting software problems shall
(1) describe the evaluation process for determining whether a reported problem is an error or other type of problem (e.g., user mistake)
(2) define the responsibilities for disposition of the problem reports, including notification to the originator of the results of the evaluation
(b) When the problem is determined to be an error, the method shall provide, as appropriate, for
(1) how the error relates to appropriate software engineering elements
(2) how the error impacts past and present use of the computer program
(3) how the corrective action impacts previous development activities
(4) how the users are notified of the identified error, its impact, and how to avoid the error, pending implementation of corrective actions
The problem reporting and corrective action process shall address the appropriate requirements of Part I, Requirement 16.

폐기 (Retirement)

소프트웨어 생산에 대한 지원을 종료하고 소프트웨어의 일상 사용을 예방하기 위한 식별 등 관리 절차 필요

407 Retirement
During retirement, support for the software product is terminated, and the routine use of the software shall be prevented.

지원 소프트웨어 (Software Tools & System Software)

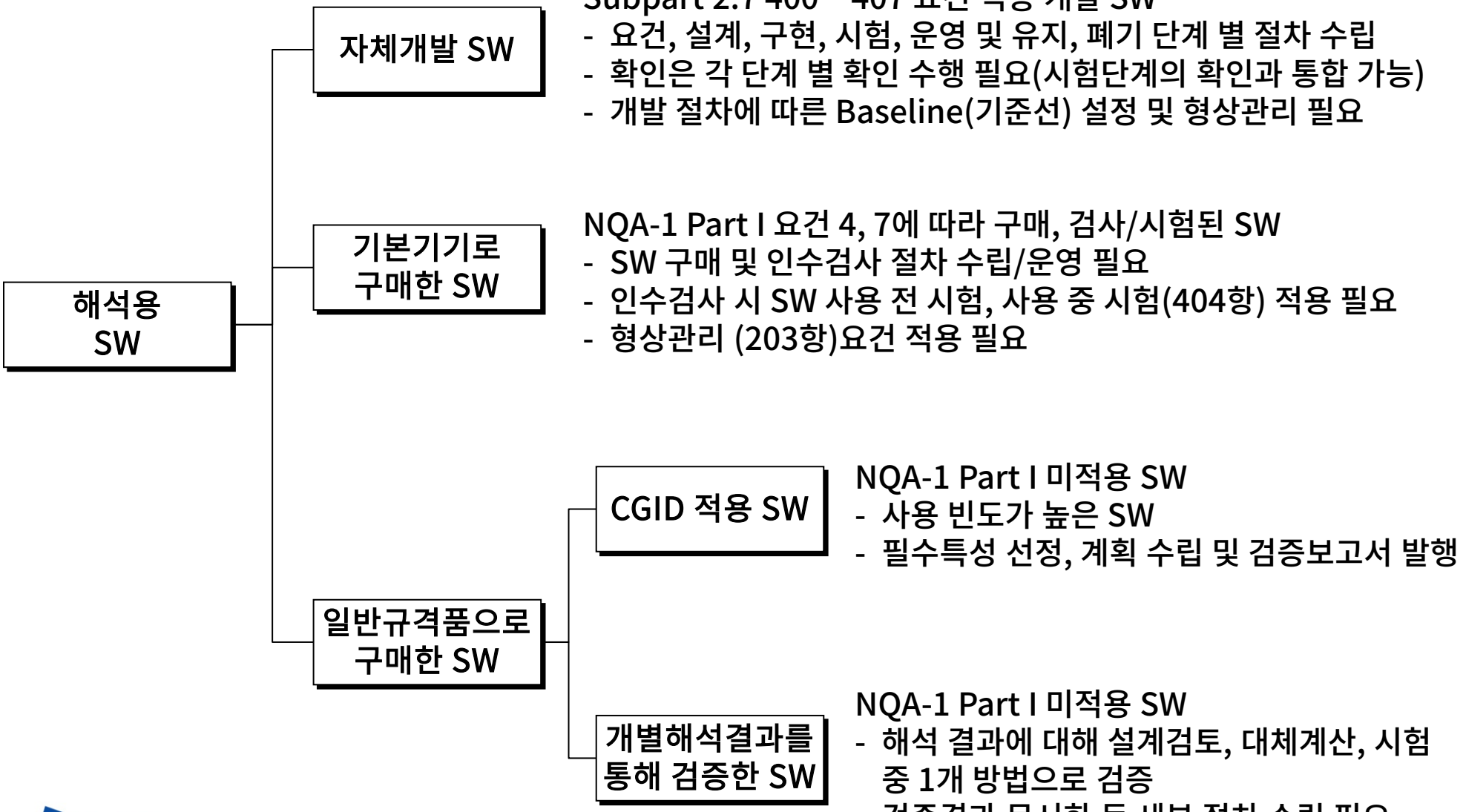
소프트웨어 성능에 영향을 미치는 소프트웨어 툴(개발도구)는 평가, 검토, 시험 및 합격 되어야 하고 소프트웨어 개발 주기의 파트로 형상관리 대상

601 Software Tools
Software tools shall be evaluated, reviewed, tested, and accepted for use and placed under configuration control as part of the software development cycle of a new or revised software product. Software tools that do not affect the performance of the software need not be placed under configuration control.

시스템 소프트웨어는 소프트웨어 개발 주기의 파트로 사용을 위해 평가, 검토, 시험 및 합격 되어야함. 시스템 소프트웨어는 형상관리 대상

602 System Software
System software shall be evaluated, reviewed, tested, and accepted for use as part of the software development cycle of a new or revised software product. System software shall be placed under configuration change control.

해석용 소프트웨어 관리 요건 요약



결론 및 건의 사항

◆ 결론

1. 해석용 소프트웨어의 입수 경로에 따른 차등화된 절차 수립 및 적용 필요
   (1) 취득한 경우
      - NQA-1 요건 4, 7을 적용하여 기본기기로 구매
      - 일반규격품을 구매하여 Dedication 수행
      - 개별 설계결과 검토를 통한 확인
   (2) 개발한 경우
      - 소프트웨어 개발 절차 수립
      - 수립된 절차에 따라 개발 수행 및 결과물 문서화
2. 입수 경로와 관계 없이 모든 해석용 소프트웨어에 대한 형상관리, 폐기 절차 수립 및 이행 필요
3. 지원소프트웨어에 대해 형상관리 항목으로 포함 및 관리 필요

◆ 건의사항

1. ASME NQA-1 개정사항 국내 도입을 위한 협회 차원의 검토 및 Guide 제시
2. 사업계 전반에서 사용하는 해석용 프로그램(ANSYS)의 기본기기 구매 방안 검토