2021

통합 소프트웨어 프로세스 관리 지침

GC-34-K

한 국 선 급

“통합 소프트웨어 프로세스 관리 지침”의 적용

1. 별도로 명시하지 않는 한, 이 지침은 2021년 7월 1일 이후 통합 소프트웨어의 프로세스 관리에 대하여 인증을 받고자 하는 선박에 적용한다.

2. 2020년판 지침에 대비 개정사항 및 그 적용일자는 아래와 같다.

적용일자 : 2021년 7월 1일 (건조계약일 기준)

제 1 장 일반사항

제 1 절 일반사항

- 101.의 6항을 추가함.

제 4 장 프로젝트 프로세스

제 1 절 관리 프로세스

제 2 절 지원 프로세스

- 제 4 장 프로젝트 프로세스의 세부요건이 관련 국제 규격의 개정 사항을 반영하여 전면 개정함.

차 례

제 1 장 총칙

제 1 절 일반사항

101. 적용

1. 이 지침은 소프트웨어 개발과 관련된 컴퓨터 기반 제어 시스템의 검토 및 검사를 통해 우리선급이 적용하는 절차와 기준을 제시한다. 이 지침의 목적은 시스템의 성능에 부정적으로 영향을 미칠 수 있는 소프트웨어 관련 사고를 줄이기 위한 것이다.
2. 이 지침은 통합 컴퓨터 기반 제어 시스템의 설계, 개발 및 유지보수를 위한 소프트웨어 개발 프로세스의 공학적 관리를 위한 방법을 규정한다.
3. 선박 또는 해양구조물에서 이 지침에 제시된 절차와 기준을 만족하면 부기부호 ISPM이 부여 될 수 있다.
4. 이 지침은 제어 시스템의 소프트웨어 측면을 강조한다. 하드웨어, FMEA (Failure Mode and Effect Analysis) 및 컴퓨터 기반 제어 시스템의 보안 기준은 우리선급이 발행한 기타 규칙, 안내서 및 기타 표준에 나와 있다. 이 지침에 제공된 것 외에도 다른 기준을 만족해야 한다.
5. 이 지침에 제공된 절차와 기준은 컴퓨터 기반 시스템의 설계, 구현 및 유지보수에서 소프트웨어 개발 프로세스의 공학적 관리를 위해 모범 사례를 기반으로 구조화된 프로세스이다. 이 지침의 프로세스 및 기준 준수는 컴퓨터 기반 제어 시스템의 안전성, 접근성, 신뢰성 및 유지 보수성을 높이기 위한 것이다.
6. 제어 이외의 목적으로 설치된 소프트웨어(예. 감시, 관리)가 제어시스템의 성능에 영향을 미치는 경우, 이 지침에서 제시하는 절차와 기준에 따라 개발 하여야 한다. *(2021)*

102. 용어의 정의

용어의 정의는 여기에 별도로 정하는 경우를 제외하고는 **선급 및 강선규칙**에 따른다.

1. **소프트웨어 제품**(Software Product)이라 함은 일련의 컴퓨터 프로그램, 절차 및 관련된 문서와 데이터를 말한다.
2. **적응 보수**(Adaptive Maintenance)라 함은 소프트웨어 제품을 변경하거나 변경되는 환경에서 사용할 수 있도록 인도 후 수행하는 소프트웨어 제품 수정을 말한다.
3. **예외적인 사항**(Anomaly)이라 함은 검증 프로세스 동안에 발견된 운용의 오류를 말한다.
4. **결과물**(Artifact)이라 함은 소프트웨어 개발 동안 생산된 유형 제품 또는 부산물을 말한다. 일부 결과물은 소프트웨어의 기능, 아키텍처 및 설계를 설명하는 것을 돕는다. 나머지 결과물은 프로젝트 계획, 사업 사례 및 위험성 평가와 같은 개발 프로세스 자체에 관여한다. 결과물로 여겨지는 것들의 대부분은 소프트웨어 문서들이다.
5. **변경관리**(Change Control)라 함은 소프트웨어 형상 관리(Software Configuration Management, SCM) 프로세스의 한 부분으로서 변경을 관리하는 것이다.
6. **폐회로 검증**(Closed Loop Verification)이라 함은 컴퓨터 기반 통합 시스템의 입력 및 출력이 다른 통합 구성 요소와의 상호 작용을 최소화하여 시뮬레이션 하는 것을 말한다. V&V는 통합 제어 시스템 소프트웨어 응답을 평가하기 위해 프로그램의 레지스터 값을 변경해야 할 수도 있다. 소프트웨어 코드와 기능의 종합적인 이해도는 간단한 시스템으로 이 옵션을 제한한다.
7. **완전성**(Completeness)이라 함은 필요한 기능의 완전한 구현이 제공되는 소프트웨어 상태를 말한다.
8. **구성요소**(Component)라 함은 시스템을 구성하는 부분들 중 하나를 말한다. 구성요소는 하드웨어 또는 소프트웨어가 될 수 있고 다른 구성요소로 세분화 될 수 있다. “모듈”, “구성요소”, 그리고 “단위”라는 용어는 종종 문맥에 따라 서로 다른 방식으로 상호 교환적으로 사용되거나 서로 하위 요소라고 정의되는 경우가 많다. 이 용어들의 관계는 아직 표준화 되지 않았다.
9. **포괄성**(Comprehensibility)이라 함은 이해될 수 있는 품질을 말한다.
10. **계획 오류**(Concept Error)라 함은 SRS 및 SDS와 비교할 때 ConOps 해석에 오류가 있거나 기능의 의도된 목적이 올바르게 설명되지 않은 경우 소프트웨어 모듈이 의도한 기능을 제대로 수행하지 못하게 되는 것을 말한다.
11. **운용 계획서**(Concept of Operations)라 함은 ConOps가 제안된 시스템의 특성을 그 시스템을 사용할 개인의 관점에서 기술한 문서를 말한다. 그것은 모든 이해관계자에게 양적 및 질적 시스템 특성을 전달하기 위해 사용된다.
12. **형상 항목**(Configuration Item)이라 함은 형상 관리를 위해 지정되고 형상 관리 프로세스에서 단일 독립체로 취급되는 하드웨어, 소프트웨어 또는 둘 모두를 통합한 것이다.
13. **일관성**(Consistency)이라 함은 설계 및 구현 기술, 부기부호의 통일성을 말한다.

14. **수정 유지보수**(Corrective Maintenance)라 함은 인도 후 발견된 결함을 수정하기 위해 수행하는 소프트웨어 제품의 빠른 수정을 말한다.
15. **정확성**(Correctness)이라 함은 추적성, 일관성 및 완전성이 제공되는 소프트웨어 상태를 말한다.
16. **경미한 결함**(Cosmetic Defects)라 함은 주로 데이터의 표시나 레이아웃과 관련 있는 것을 말한다. 그러나 데이터 손상 및 잘못된 값의 위험은 없다.
17. **심각한 결함**(Critical Defects)이라 함은 매우 심각한 결함으로, 이미 중지되었거나 컴퓨터 기반 제어 시스템의 작동을 중지시킬 수 있는 것을 말한다. 심각한 결함은 EUC의 안전하지 않은 작동이 가능한 결함이기도 하다.
18. **결함**(Defect)이라 함은 소프트웨어 코딩 오류를 말한다.
19. **결점**(Deficiency)이라 함은 소프트웨어가 ConOps, SRS 및 SDS에 열거된 기능을 수행하지 않는 경우를 말한다.
20. **퇴화**(Degraded)라 함은 제어 시스템 또는 연결된 장비의 구성요소 또는 일부가 명세서에 따라 작동 하지 않는 것을 말한다.
21. **긴급 유지보수**(Emergency Maintenance)라 함은 시스템 작동을 유지하기 위해 계획되지 않은 수정 유지보수를 하는 것을 말한다.
22. **에뮬레이터**(Emulator)라 함은 다른 시스템을 사용하여 한 시스템의 기능을 복제하는 것을 말한다. 두 번째 시스템은 첫 번째 시스템처럼 "동작"하는 것을 말한다.
23. **중요용도**(Essential Services)라 함은 선박의 추진, 조타 및 안전에 필수적인 용도를 말한다. 중요용도는 일차중요용도와 이차중요용도로 구분되며 정의 및 예는 선급 및 강선규칙 **6편 1장 101. 4항**을 따른다.
24. **실패**(Failed)라 함은 통합 소프트웨어 제어 시스템 또는 연결된 장비의 상당 부분이 정상적으로 작동하지 않는 것을 말한다.
25. FMECA(Failure Modes, Effects and Criticality Analysis)라 함은 결과의 심각성에 대해서 위험 분석이 고장 모드의 확률을 도표로서 사용되는 것을 말한다. 분석은 상대적으로 높은 확률 및 결과의 심각성과 함께 고장 모드를 강조한다.
26. **펌웨어**(Firmware)라 함은 하드웨어 장치와 컴퓨터 명령 및 해당 장치에서 읽기 전용 소프트웨어로 존재하는 데이터의 결합을 말한다.
27. **유연도 매트릭스**(Flexibility Matrix)라 함은 프로젝트 정의 및 작업 계획 동안 범위, 일정 및 자원에 관한 절충 분석을 용이하게 하는 방법을 말한다.
28. **기능**(Function)이라 함은 제어 중인 장비의 목적(즉, 유압 동력 장치, 윈치, 전원 관리 시스템)을 말한다.
29. **하드웨어**(Hardware)라 함은 컴퓨터 소프트웨어 또는 데이터를 처리, 저장 또는 전송하는 데 사용되는 물리적 장비를 말한다.
30. **하드웨어 인 더 루프**(Hardware-In-the-Loop)라 함은 통합 시스템의 프로그램이 기본 하드웨어(CPU 또는 컨트롤러 하드웨어)에서 실행되고 있으며, 시뮬레이션이 별도의 기계에서 실행되고 있는 것을 말한다. 두 개의 시스템 사이의 인터페이스는 시험을 위해 개발되었다. 시뮬레이션은 중앙 제어 시스템의 프로그래밍을 검증하고 고무된 결과를 문서화하는 물리적 실제 설계 동적 시스템을 포함하기에 충분한 정확도가 있어야 한다. 시뮬레이션 프로그램에서 수학적 모델로 나타난다.
31. **인간 기계 인터페이스**(Human Machine Interface)라 함은 디스플레이 및 운영자 입력 장치를 말한다.
32. **기기 장치**(Instrumentation)라 함은 사용량 측정 또는 오류 식별을 제공하는 소프트웨어 속성을 말한다.
33. **무결성 수준**(Integrity Level)이라 함은 소유자 및/또는 사용자가 컴퓨터 기반 기능에서 다양한 고장의 결과가 소프트웨어에 미치는 영향에 따라 부여하는 번호를 말한다. 여기서 무결성 레벨 0은 기능 실패의 결과에 거의 영향을 미치지 않고, 무결성 레벨 3은 기능 실패의 결과에 크게 영향을 미친다.
34. **상호운용성 시험**(Interoperability Testing)이라 함은 수정된 시스템이 다른 유형의 시스템과 정보를 교환하고 해당 정보를 사용하는 기능을 유지하는지 확인하기 위해 수행되는 것을 말한다.
35. **주요 결함**(Major Defects)이라 함은 심각한 결함으로 시스템을 정지 시키지는 않지만 성능을 심각하게 저하 시키거나 의도하지 않은 동작 또는 잘못된 데이터 전송을 유발하는 것을 말한다.
36. **사소한 결함**(Minor Defects)이라 함은 낮은 수준의 기능 장애를 일으킬 수 있거나 초래하는 결함을 말한다. 이러한 결함으로 인해 데이터 대기 시간이 발생하지만 필수 또는 IL2 또는 IL3 기능에는 영향을 미치지 않는다. 장애가 발생하더라도 통합 시스템과 기능은 계속 작동한다. 일부 기능의 이러한 중단 또는 비 가용성은 IL1 기능에 대해 제한된 시간 동안 허용 될 수 있다. 경미한 결함은 짧은 시간 동안 허용되는 방식으로 일부 중요 데이터 값이 손상 될 수 있다.
37. **적당한 결함**(Moderate Defects)이라 함은 소프트웨어 기능이 SRS 및 SDS에 지정된 것과 다르게 작동하여 운영 설명서가 변경 될 수 있는 것을 사소한 결함이라고 한다. 소유자는 그러한 영향과 각 변화의 위험성을 검토해야 한다.

38. **수정 요청서(Modification Request)**라 함은 다양한 문제 보고 문서(예 : 사고 보고서, 문제 보고서) 및 형상 변경 제어 문서(예 : 소프트웨어 변경 요청서(SCR))와 관련된 양식을 포함하는 일반적인 용어를 말한다.
39. **모듈화(Modularity)**라 함은 매우 독립적인 모듈 구조를 말한다.
40. **고유 시스템용 컴퓨터(Modularity)**라 함은 프로그램이 설치 될 하드웨어에서만 실행되는 것을 말한다.
41. **비 고유 시스템용 컴퓨터(Non-native Computer)**라 함은 프로그램이 에뮬레이터를 사용하여 대상 하드웨어의 에뮬레이션을 이용하여 실행하는 것을 말한다.
42. **작동불가(Nonoperational)**라 함은 작동하지 않거나 사용할 준비가 되지 않은 것을 말한다.
43. **정상(Normal)**이라 함은 제어 시스템, 연결된 구성 요소, 관련 입력 및 출력 모듈이 작동하는 것을 말한다.
44. **작동(Operational)**이라 함은 (1) 의도된 환경에서 사용할 수 있는 시스템 또는 구성요소에 대한 사항. (2) 의도된 환경에 설치된 시스템 또는 구성요소에 대한 사항. (3) 시스템 또는 구성요소가 사용되는 환경에 대한 사항. (IEEEE 규격 610, 1990, IEEE 표준 컴퓨터 사전, IEEE 표준의 컴파일) 컴퓨터 용어집)
45. **소유자(Owner)**라 함은 자금을 제공하고 프로젝트를 시작하는 조직이다.
46. **패키지(Package)**라 함은 하드웨어, 소프트웨어, 센서, 조립 기기의 배선 및 부속품을 말한다.
47. **동료 평가(Peer Review)**라 함은 유능하거나 같은 분야의 전문가로 간주되는 다른 사람들이 문서 또는 개발자의 작업을 면밀히 조사하는 프로세스를 말한다.
48. **완전 유지보수(Perfective Maintenance)**라 함은 인도 후 소프트웨어 제품을 수정하여 성능 또는 유지 보수성을 향상시키는 것을 말한다.
49. **단위 시험(Unit Testing)**이라 함은 모듈의 시험 가능한 가장 작은 부분을 검증하는 방법을 말한다. 개별 장치를 먼저 시험 한 다음 모듈 내 다른 장치와 함께 시험하여 적절한 상호 작용 및 결과를 평가한다. 모듈이 입증되면 모듈 간 상호 작용을 시험 할 수 있다.
50. **검증 및 확인(V&V)**이라 함은 통합 소프트웨어 프로그램의 검증 및 확인을 말한다.
51. **검증 및 확인 조직(V&V Organization)**이라 함은 소프트웨어를 폐쇄루프 (특별히 고려하는 경우), 와 Software-In-the-Loop(SIL, Hardware-In-the-Loop(HIL) 또는 이 세 가지 방법의 조합을 통해 소프트웨어 요구사항 명세서(SRS) 와 통합 소프트웨어 설계 명세서(SDS)에서 정의된 사항을 확인한다. 검증 및 확인 조직은 시스템 통합 조직의 일부이거나 소유자의 요청에 따라 독립적 일 수 있다.
52. **확인(Validation)**이라 함은 소프트웨어가 운용계획서에 설명된 대로 의도된 용도를 충족하는지 확인하는 것을 말한다.
53. **검증 가능성(Verifiability)**이라 함은 검사 또는 조사를 통해 검증, 입증 또는 확인할 수 있는 소프트웨어의 기능을 말한다.
54. **검증(Verification)**이라 함은 SRS 및 SDS에 설명된 대로 소프트웨어 성능을 입증하는 것을 말한다. 또한 특정 활동의 개발 제품이 해당 활동의 요건을 준수하는지 여부를 결정한다.
55. **버전 관리(Version Control)**라 함은 SCM 프로세스의 일부로서 만들어진 자산 버전의 관리를 말한다.
56. **바이러스 정의(Virus Definition)**라 함은 안티바이러스 프로그램에 의해 사용된 컴퓨터 바이러스 특징의 데이터베이스를 말한다.

103. 동등효력

이 지침에 만족하지 않거나 적용할 수 없는 대체 설계 및 신기술의 동등효력에 대해서는 **선급 및 강선규칙 1편 1장 105.**를 따른다.

104. 제외사항

우리 선급은 이 지침에 명시되지 않은 기타 기술적인 특성 및 허가받지 않은 상용 제품의 사용에 대하여는 책임을 지지 아니한다. ⚓

제 2 장 시험 및 검사

제 1 절 일반사항

101. 일반 사항

1. 지침은 통합 소프트웨어 프로세스 관리 부기부호(ISPM)와 관련된 제어 시스템의 분류를 유지하기 위한 요구 사항이다. 적용 가능한 경우, 요구사항은 우리선급 규칙 및 / 또는 지침에 명시된 규정에 추가하여 선박 또는 설비에 적용할 수 있다.
2. 시운전 날짜는 검사원이 ISPM 부기부호를 부여 받은 선박 또는 설비에 대해 임시 선급 증서를 발행한 날짜가 된다.

102. 통합 소프트웨어 품질 관리 부기부호(ISPM)에 대한 검사

1. 검사 간격 및 유지보수 매뉴얼/기록

(1) ISPM 부기부호와 관련된 모든 연차 및 정기 검사는 선박 또는 설비의 정기적인 선급 검사로서 동일한 시간 및 간격으로 수행하여 동일한 인증 날짜로 기록한다.

(2) ISPM 부기부호와 관련된 통합 소프트웨어에 대한 연차 검사는 최초의 인증 검사가 시행되는 매년 1년마다 3개월 이내에 검사원이 수행하여야 한다. ISPM 부기부호와 관련된 통합 소프트웨어에 대한 정기 검사는 초기 인증 검사로부터 5년 이내에 그리고 그 이후 5년 간격으로 수행하여야 한다.

(3) 유지보수 및 교정 기록을 보관하여 검사원이 입회 시 검토 할 수 있도록 하여야 한다. 검사원은 연차 및 정기 검사의 범위와 내용을 수립하기 위해 유지보수 기록을 검토한다. 소프트웨어 시스템 구성 요소의 서비스 수명 동안 유지보수 기록은 지속적으로 업데이트 하여야 한다.

(a) 소유자는 IL3 소프트웨어 모듈이 ISPM 부기부호로 제어 시스템에 개조되거나 설치 될 때마다 우리선급에 통보해야한다. 우리선급은 IL3 소프트웨어 모듈의 수정 또는 설치를 통보 한 후 선박을 검사 할 수 있다.

2. 연차 검사

연차 검사 시 검사원은 다음에 대한 검증을 포함하는 소프트웨어 및 하드웨어가 통합된 검사를 수행한다.

(1) 변경 관리 절차가 준수되고 있음을 확인한다.

(2) 제어기기 레지스트리 검사

(가) 마지막 검사 이후에 변경된 제어기기 식별

(나) 변경된 각 장비 항목 기록

(다) 변경된 장비에서 관리되는 모든 소프트웨어 리스트

(라) 변경으로 인해 영향을 받는 모든 문서 식별

(마) 각 문서 변경 사항 기록

(바) 레지스트리에 나열되지 않은 변경 사항 기록

(3) 소프트웨어 레지스트리 검사

(가) 검사 이후 변경된 모든 제어 소프트웨어를 식별

(나) 각 소프트웨어 항목 변경 사항 기록

(다) 변경된 장비에서 관리되는 모든 소프트웨어 검사

(라) 변경된 장비에 대한 소프트웨어 변경 사항을 기록

(마) 변경 사항의 영향을 받는 모든 문서 식별

(바) 모든 변경된 문서를 소프트웨어 레지스트리에 기록

(사) 레지스트리에 나열되지 않은 소프트웨어 변경 사항을 기록

(4) 통합 제어 시스템의 하드웨어 레지스트리 검토

(가) 관련 소유자/사용자 및 공급업체 직원을 인터뷰하고 지원 문서를 검토하여 소프트웨어 변경관리를 얼마나 밀접하게 준수하는지 평가한다.

(나) 가능한 결점을 확인하고 프로세스 개선을 권고한다.

(5) 바이러스 및 악성 소프트웨어 검사 기록 검토.

3. 정기 검사

정기 검사는 연차 검사에 열거된 모든 품목을 검사원이 만족하도록 포함하여야 한다.

103. 수정, 손상 및 수리

1. 선박 또는 설비의 ISPM 부기부호에 영향을 미치는 소프트웨어 시스템의 변경을 수행하고자하는 경우, 변경에 대한 세부 사항을 제출하여 승인을 받아야하며, 검사원이 만족할 만큼 작업을 수행해야한다.
2. 선박 또는 설비의 ISPM 부기부호에 영향을 미치는 제어 시스템이 무결성 레벨에 영향을 줄 수 있는 손상을 입은 경우 우리선급에 통보하고, 무결성 등급을 다시 평가 받아야 한다.
3. 제어 시스템이 예기치 않은 고장이 발생하고 검사원의 입회 없이 수리 또는 교체한 경우, 고장의 세부 사항은 가능한 한 손상된 부분을 포함하여 다음 선급 검사 중 검사원의 검증을 위해 선내에 남겨 두어야한다. 고장이 부적절하거나 부적절한 유지 보수의 결과로 간주되는 경우 유지보수 매뉴얼을 수정하고 승인을 위해 다시 제출하여야 한다. ⚓

제 3 장 소프트웨어 프로세스

제 1 절 일반사항

101. 일반사항

1. 이 절에서는 소프트웨어의 성공적인 개발 및 전환을 목표로 하는 단계 및 관리 방법의 개요를 보여준다. 소프트웨어 개발 생명주기 (Software Development Life Cycle, 이하 SDLC) 5단계, 관리 프로세스, 지원 프로세스가 있다.
2. 이 지침에 설명된 SDLC는 최소한의 허용 가능한 프로세스이다. 마일스톤은 프로세스의 각 단계에서 이행해야할 항목들이 체계적으로 처리되고 있으며, 문서가 기능들의 의미와 의도를 충분히 전달하는 것을 확인하여야 하는 사항을 의미한다. 마일스톤의 사항은 각 단계가 끝나기 전에 충족하여야 한다.

제 2 절 이해관계자의 역할과 책임

201. 일반사항

1. 이해관계자 요구사항의 목적은 정의된 환경에서 사용자 및 기타 이해관계자들이 필요로 하는 서비스를 제공할 수 있는 시스템의 요구사항을 정의하는 데 있다. 시스템의 생명주기를 통하여 시스템과 연관을 갖는 이해관계자 또는 이해관계자 집단을 식별하고, 그들의 필요, 기대 및 욕구를 식별한다. 이 공동의 요구사항 세트는 시스템과 운용 환경과의 의도된 상호작용을 표현하며, 또한 각 운용 서비스 결과의 유용성을 확인하는 대조 기준이 된다.
2. 통합 소프트웨어의 개발 및 전환에는 다양한 조직이 필요하다. SDLC의 각 프로세스에는 여러 요건들과, 활동 그리고 산출물을 포함하며, 그 과정에서 다양한 조직이 요건 및 활동을 수행 한다.
3. 이 지침은 활동에 따라 책임을 조직에 할당하여 수행한다고 가정하며, 활동의 할당은 각 단계별 이해관계자 조직의 역할 및 산출물을 명확히 한다.
4. 이해관계자는 프로젝트의 성공에 관심이 있는 조직을 일컫는다. 통합 소프트웨어 SDLC 프로세스의 이해 관계자는 202.를 통해서 정의하며, 그 책임과 역할은 경우에 따라 결합 할 수 있다. (예를 들어, 소유자(Owner)는 사용자(User)가 될 수 있고, 초기 개발단계에서는 선박 건조업체(제조자 또는 조선소)가 될 수 있다.)
5. 프로젝트 일정을 유지하기 위해서 이해관계자 간의 상호 작용, 정보의 흐름 및 정보의 적시성을 관리하여야 한다.

202. 이해관계자의 역할

1. 소유자 (Owner)

소유자는 통합 소프트웨어를 획득하거나 조달하는 이해관계자로서, 자금을 제공하고 프로젝트를 시작하는 조직이다. 통합 소프트웨어를 사용하는 목적을 달성하고자 개발자에게 요구사항을 제시하고, 각 단계별 산출물과 요구사항 충족여부를 판단한다.

2. 시스템 통합 조직(System Integrator 이하 SI)

시스템 통합 조직은 통합 시스템의 개발을 담당 한다. 선택된 ISPM 시스템에 따라 복수의 시스템 통합 조직이 있을 수 있다. 시스템 통합 조직은 담당하는 제어 시스템의 전문가이며, 장비가 연결된 제어 시스템의 요건에 대한 통합 인식을 가진다. 시스템 통합 조직은 통합 시스템의 설계, SRS & SDS 작성, 공급자 관리, 통합 및 소유자의 허가와 제어 시스템 소프트웨어의 확인을 담당 한다. 소유자는 ConOps의 개발을 위해 필요에 따라 시스템 통합 조직으로부터 정보를 요청할 수 있다. 소유자는 SI를 선정하여 통합 시스템의 확인을 수행 하거나, 소유자가 독립적인 제3자 검증을 요구할 수 있다. SI 또는 선박 건조업체 조직은 SI 활동을 제 3자에게 위임 할 때 책임을 양도 할 수 없다. 프로젝트 규모가 시스템 통합 조직을 보증하지 않는다면 소유자, 사용자 또는 사용자가 선택한 공급자 조직이 이러한 책임을 수행해야 한다.

(1) 시스템 통합 조직은 현재 ISO 9001을 보유하거나 CMMI 레벨2 이상이어야 한다.

(2) 기타 소프트웨어 품질 관리 시스템은 우리선급에 의해 특별히 고려 할 수 있다. 시스템 통합 조직과 조선소는 공급자가 확인 요건과 활동을 미리 알 수 있도록 안내할 것을 권장한다.

3. 사용자 (User)

통합 소프트웨어 사용 기간 동안 전환된 통합 소프트웨어로부터 혜택을 얻는 개인 또는 집단으로, 시스템의 운영 및 유지보수 단계를 담당 한다. 유지보수의 책임은 시스템의 생명주기 동안 개선, 업그레이드 및 교체 또는 새로운 구성 요소

가 시스템에 추가 되는 경우에 안정적인 작동이 지속되게 한다.

4. 품질관리자(V&V)

품질관리자는 시스템 통합 조직으로부터 소유자의 만족기준인 품질기준을 전달받아 소프트웨어를 페쇄루프 (특별히 고려하는 경우)와 Software-In-the-Loop(SIL) 또는 Hardware-In-the-Loop(HIL) 혹은 이 세 가지 방법의 조합을 통해 소프트웨어 요구사항 명세서(SRS) 와 통합 소프트웨어 설계 명세서(SDS)에서 정의된 요구사항을 확인한다. 검증 및 확인 조직은 시스템 통합 조직의 일부이거나 소유자의 요청에 따라 독립적 일 수 있다.

5. 선박 건조업체 (Shipbuilder)

선박 건조업체는 조선소를 의미한다. 시스템 통합 조직과 계약을 체결하거나, 104.의 SI 조직에 관한 사항을 충족한다면 조선소 내에 부서는 선박 건조업체가 될 수 있다. 선박 건조업체는 ISPM 제어 시스템이 설치되면 통합 확인 활동을 수행한다. 통합 활동에는 ISPM 제어 시스템에 연결된 장비 간의 통신(통합 확인)확인을 포함한다. 선박 건조업체는 계약에 따라 소유자가 원하는 ISPM 제어시스템의 전환(공급)할 책임이 있다.

6. 선급 (Class Society 이하 CS)

우리선급은 이해관계자가 이 지침을 준수하도록 SI와 독립적으로 ISPM 제어 시스템 개발 중에 작성된 문서를 검토한다. 다만, IL2 또는 IL3의 등급이 받은 제어 시스템의 확인 시험은 우리선급의 입회하에 진행한다. 선박 건조업체 또는 소유자가 수행하는 통합 검증 시험은 우리선급의 입회하에 진행한다.

7. 공급자 (Supplier)

프로세스 동안에 개발 업무를 수행하는 조직으로 통합 소프트웨어의 구성 요소 또는 소프트웨어의 계약된 공급자이다. 개발자는 시스템 통합 조직 또는 선박 건조업체가 할당한 구체적인 범위와 일정에 따라서 개발자는 공급하는 시스템 패키지의 규격 및 제약 조건을 제공하여야 한다. IL2 및 IL3 공급 장비의 공급자 검증은 우리선급에 확인되어야 한다.

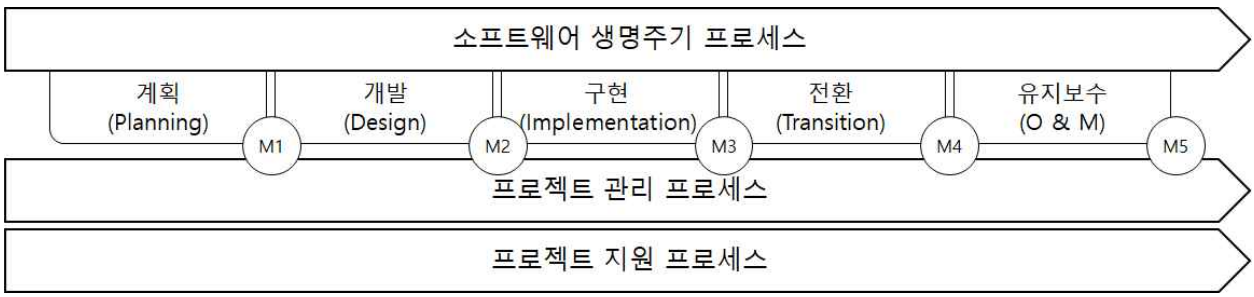
(1) 공급자 조직은 현재 ISO 9001을 보유하거나 CMMI 레벨2 이상이어야 한다.

(2) 기타 소프트웨어 품질 관리 시스템은 필요시 소프트웨어 적합성 인증 지침을 따라야 한다.

제 3 절 ISPM 프로세스

301. 일반사항

이 절에서는 개발 생명주기 프로세스의 5단계와 프로젝트 지원 프로세스 및 프로젝트 관리 프로세스에 대해 간략하게 설명한다.



302. 소프트웨어 개발 생명주기 (SDLC)

1. 소프트웨어 개발 생명주기는 컴퓨터 기반 제어 시스템의 개념수립부터 폐기에 이르기까지 소프트웨어 개발을 위한 일련의 공학적인 계획을 일컫는다. 마일스톤(또는 단계 게이트)은 SDLC의 각 단계 내 또는 경계와 관련이 되며 특정 단계 산출물의 제공과 관련이 있다.
2. 소프트웨어 개발 생명주기는 다음과 같다.

(1) 계획 단계 (Planning)

프로젝트의 방향과 업무 범위를 결정하고 통합 시스템을 상세하게 정의하기 위해 다음의 활동을 수행한다.

(가) 안전성 검토

(나) 무결성 수준(IL) 평가

(다) 초기 통합 시스템의 구성요소

(라) 주요 검증 방법
(마) ConOps 작성

(2) 개발 단계 (Design)
시스템 통합 조직의 개발자와 프로그래머가 ConOps에 정의된 기능에 대해 시스템 아키텍처를 고려하여 소프트웨어를 구성하는데 사용할 수 있는 문서를 작성한다.

(3) 구현 단계 (Implementation)
SRS 및 SDS의 요건 및 사양을 기능 통합 시스템 코드로 변환하고, 작동하도록 한다. 확인 및 검증 활동은 커미셔닝(Commissioning) 및 해상 시운전 활동에 걸쳐서 계획 단계에서 선정한 검증 방법에 따라 품질관리자는 검증 계획을 작성하고 시뮬레이터를 설정하여야 한다.

(4) 전환 단계 (Transition)
완성된 소프트웨어의 검증 후, 통합 시스템을 소유자 및 사용자로 전환하는 데 필요한 모든 작업이 완료되어야 한다. 소프트웨어는 소유자가 선택한 하드웨어에 설치되고 지원 서비스가 제공되며 시스템 통합 조직은 모든 문서를 소유자와 사용자에게 제출하여야 한다.

(5) 유지 보수 (Operation & Maintenance) 단계
예정되거나 예정되지 않은 업그레이드 및 문제 해결 활동을 포함한 운영 및 유지보수 활동을 다루며 폐기 활동을 포함한다.

303. 프로젝트 프로세스

프로젝트 관리 프로세스(계획, 평가 및 통제)는 모든 관리 활동의 핵심이다. 이들 프로세스는 한 프로젝트 또는 한 프로세스를 관리하기 위한 일반적인 접근법을 제시한다. 한 조직 전체로부터 한 생명주기프로세스 및 그 태스크까지의 전 범위에 걸쳐 진행되는 모든 과업의 관리에서 프로젝트 지원 프로세스는 모두 명백하다. 이 표준에서 프로젝트는 계획, 실행, 평가 및 통제와 관련된 프로세스를 표현하기 위한 정황으로 사용된다.

1. 프로젝트 관리 프로세스

프로젝트 관리 프로세스는 다음 프로세스로 구성된다.

(1) 프로젝트 계획 프로세스
(2) 프로젝트 평가 및 통제 프로세스

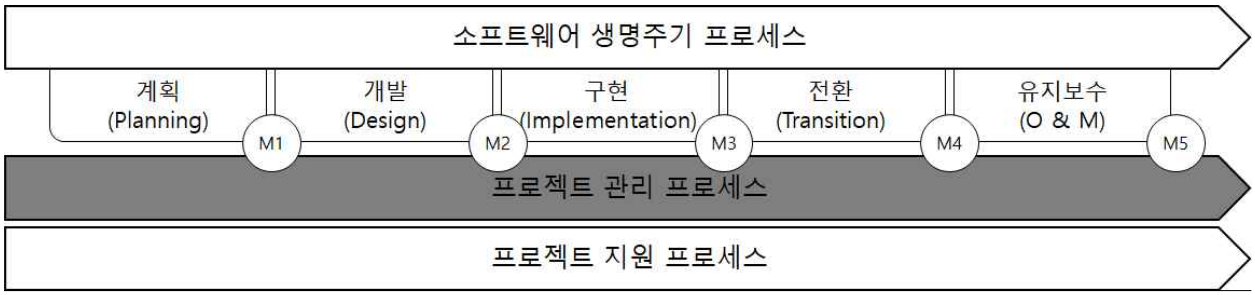
2. 프로젝트 지원 프로세스

프로젝트 지원 프로세스는 다음 프로세스로 구성된다.

(1) 의사결정 관리 프로세스
(2) 위험 관리 프로세스
(3) 형상 관리 프로세스
(4) 정보 관리 프로세스
(5) 측정 프로세스 ⚓

제 4 장 프로젝트 프로세스

제 1 절 관리 프로세스



101. 일반사항

프로젝트 관리 프로세스는 다음으로 구성된다.

1. 프로젝트 계획 프로세스
2. 프로젝트 평가 및 통제 프로세스

102. 프로젝트 계획 프로세스

1. 일반사항

(1) 프로젝트 계획 프로세스의 목적은 효과적이고 실천 가능한 프로젝트 계획을 수립하고 이를 조정하는데 있다.

(2) 이 프로세스는 프로젝트 관리 활동과 기술 활동의 범위를 결정하고, 프로세스 결과물, 프로젝트 인도 품목, 프로젝트 소요 자원을 포함하여 프로젝트를 수행하기 위한 일정 계획을 작성한다.

(3) 프로젝트 계획 프로세스 외의 프로세스에서 수립한 내용을 받아 통합한다.

2. 활동

계획 프로세스는 적용 가능한 조직의 정책 및 절차에 따라 다음 활동을 수행해야 한다.

(1) 프로젝트 정의

(가) 프로젝트 목표 및 제약사항을 식별한다.

(a) 목표 및 제약사항에는 성능 및 다른 품질 속성, 비용, 일정 및 이해관계자 만족이 포함된다.

(b) 각 목표는 적절한 프로세스와 활동을 선택하고, 조정 및 이행할 수 있도록 충분히 상세하게 식별되어야 한다.

(나) 계약에 따라 정해진 프로젝트의 범위를 설정한다.

(a) 프로젝트 범위는 사업의 의사 결정 기준을 충족시키고, 프로젝트를 성공적으로 완수하는 데 필요한 모든 관련 활동들을 포함한다.

(b) 프로젝트는 전체 시스템 생명주기 중에서 하나 또는 그 이상의 단계를 책임 질 수도 있다.

(c) 계획에는 프로젝트 계획을 유지하고, 프로젝트를 평가하고 통제하는데 필요한 적절한 행동이 포함된다.

(다) 조직에서 정의한 생명주기 모델을 활용하여, 단계들로 구성된 하나의 생명주기 모델을 정의하고 유지한다.

(2) 프로젝트 및 기술 관리 계획

(가) 관리 목표 및 기술 목표와 이에 따른 작업 추정량을 바탕으로 프로젝트 일정 계획을 작성하고 유지한다.

(a) 프로젝트를 적기에 완료하는 데 필요한 활동들의 기간, 관계, 의존성 및 순서, 채용된 자원, 마일스톤 및 위험 관리를 위한 예비 일정 등에 대한 정의를 포함한다.

(나) 생명주기단계의 의사결정 시점에서 프로젝트 성과 기준을 정의한다.

(a) 프로젝트의 내부 검토 주기는 시스템의 긴요성, 일정 계획, 기술적 위험 등을 고려하여 관련 조직의 정책에 따라 정한다.

(다) 프로젝트 비용을 정의하고 예산을 계획한다.

(a) 비용 산정은 프로젝트 일정, 예상되는 노동량, 기반 시설 비용, 조달 품목, 획득된 서비스, 예상되는 생명주기 지원 시스템, 위험관리를 위한 예비 예산 등을 바탕으로 한다.

(라) 프로젝트 조직의 역할, 책임, 성과 및 권한을 정의한다.

(a) 프로젝트 조직 편성, 인원의 획득, 구성원의 기술 개발 등을 정의하는 일이 포함된다.
(b) 설계 권한, 안전 권한, 자격 및 인증 부여 권한 등과 같은 권한 설정은 법적 책임을 갖는 역할의 지정과 담당자의 지명을 포함한다.

(마) 프로젝트에 필요한 기반 시설과 서비스를 정의한다.
(a) 기반 시설 및 서비스의 각 항목별로 요구되는 용량 또는 역량과 그 가용성 및 할당을 포함한다.
(b) 기반 시설에는 설비, 도구, 통신 및 정보 기술 자산도 포함된다.
(c) 각 생명주기 단계에 필요한 생명주기 지원 시스템에 대한 요구사항도 포함한다.

(바) 프로젝트 외부에서 공급이 필요한 자원 및 생명주기 지원 시스템의 서비스에 대한 획득을 계획한다.
(a) 필요에 따라 입찰 권유, 공급자 선정, 수락, 계약 행정 및 계약 종료에 대한 계획을 포함한다.

(사) 검토 계획을 포함하여 프로젝트, 기술 관리 및 수행에 대한 계획을 작성하고 공지한다.

(3) 프로젝트 착수
(가) 프로젝트 수행 권한을 부여한다.
(나) 프로젝트 수행을 위해 필요한 자원을 요청하고 승인을 받는다.
(다) 프로젝트 목표 및 기준을 만족하기 위하여 프로젝트 계획에 따라 진행한다.

3. 산출물

(1) 프로젝트 관리 계획서
(2) 프로젝트 계약관리 계획서
(3) 프로젝트 변경관리 계획서
(4) 프로젝트 통제 계획서
(5) 소프트웨어 개발 계획서
(6) 문서화 계획서

103. 프로젝트 평가 및 통제 프로세스

1. 일반사항

(1) 프로젝트 평가 및 통제 프로세스의 목적은 다음과 같다.
(a) 프로젝트 계획 프로세스에서 통합된 전략들이 실현가능한지 평가한다.
(b) 기술적인 성과 및 프로세스 성과를 포함한 프로젝트 상태를 결정하는 것이다.
(c) 프로젝트의 재정 한도에서 기술 목표를 만족시키기 위하여 업무 성과가 계획 및 일정을 명확히 준수할 수 있도록 프로젝트 계획 실행을 인도하기 위한 것이다.

(2) 이 프로세스는 주기적으로, 주요 시점에서 요구사항, 계획 및 사업 전반적 목표에 대한 진척도 및 성과를 평가한다. 프로세스 성과가 목표치에서 심각하게 벗어나 있는 경우 이 정보를 관리자에게 전달하여 적절한 조치를 취할 수 있도록 한다.

(3) 이 프로세스는 다른 기술 관리 프로세스 또는 기술 프로세스에서 식별된 성과 차이 및 변동을 바로잡기 위해 프로젝트 활동들에 대하여 적절한 방향 수정 활동을 포함한다.

(4) 필요시 방향 수정의 범위는 계획 재작성을 포함한다.

2. 활동

프로젝트 평가 및 통제 프로세스를 적용하는 프로세스에서는 조직의 관련 정책과 수행 절차에 따라 다음 활동을 하여야 한다.

(1) 프로젝트 평가 및 통제 계획
(가) 프로젝트 평가 및 통제 방법을 정의한다.
(a) 계획된 평가 방법 및 평가 시점 그리고 규정된 기술 검토 및 프로젝트 관리 등을 포함하여 예상하는 프로젝트 평가 및 통제 활동을 식별한다.

(2) 프로젝트 평가
(가) 프로젝트의 목표와 계획이 프로젝트 상황과 일관성이 있는지를 평가한다.
(나) 프로젝트 목표 달성 적합성과 타당성을 결정하기 위해서 프로젝트 목표에 대비하여 관리 및 기술 계획을 평가한다.
(다) 해당 프로젝트의 비용, 일정 및 품질의 예상과 실제의 차이를 결정하기 위해 계획에 대비하여 프로젝트 상태를 평가한다.
(라) 프로젝트 팀의 구조, 역할, 역할에 대한 책임, 성과책임 및 권한의 적절성을 평가한다.

(a) 평가에는 구성원의 역량이 프로젝트 역할 수행에 적합한지에 대한 평가도 포함한다.
(b) 자원 사용의 효율성, 프로젝트의 성취도 등과 같이 가능한 한 객관적인 척도를 사용한다.

(마) 프로젝트의 지원 기반 시설에 대하여 적절성과 가용성을 평가한다.
(a) 기반시설은 인프라, 인력, 재원, 시간 또는 기타 관련 항목이 포함된다.
(b) 조직의 내부적 동의 여부에 대한 확인을 포함한다.

(바) 측정된 성과와 마일스톤 완료 여부를 사용하여 프로젝트 진도를 평가한다.
(a) 평가는 업무량, 물자 사용량, 서비스 비용 및 기술적 성능 그리고 가격 적정성(affordability) 등과 같은 다른 기술적 데이터도 수집하고 평가한다.
(b) 평가 결과를 설정된 프로젝트 성과 척도와 비교한다.
(c) 요구사항에 대비하여 시스템이 적절하게 개발되고 있는지를 결정하기 위한 효과도 평가를 포함한다.
(d) 생명주기 지원 시스템이 필요할 때 서비스를 제공할 수 있는지 그 준비 상태에 대한 평가도 포함한다.

(사) 요구되는 관리 및 기술 검토, 심사와 검사를 수행한다.
(a) 프로젝트 마일스톤 또는 생명주기의 다음 단계로 진척 여부를 결정하기 위해 수행한다.
(b) 프로젝트 목표 및 기술 목표의 충족 여부를 확신하기 위해 수행한다.
(c) 이해관계자로부터 피드백을 받기 위해 수행한다.

(아) 핵심 프로세스와 신기술을 검토한다.
(a) 프로젝트 계획에 따른 기술 성숙도와 적용 현황을 식별하고 평가하는 것을 포함한다.

(자) 측정 결과를 분석하고 적절한 시정사항을 권고한다.
(a) 잠재적인 문제를 포함하여 모든 관심사항별로 계획된 목푯값과의 편차, 변동 또는 바람직하지 않은 경향을 식별하여 수정 및 예방 활동에 필요한 적절한 시정사항을 권고하기 위해 측정 결과를 분석한다.
(b) 측정 결과 분석은 결과물의 품질을 나타내는 결함 밀도 또는 프로세스 반복성(repeatability)을 나타내는 여러 변수별 측정값 분포 등과 같이 적합한 경향을 나타내는 통계적 분석을 포함한다.

(차) 평가 상태 및 결과를 기록 및 제공한다.
(a) 기록 및 제공하여야 하는 사항은 협약서, 정책서 또는/및 절차를 포함하는 지침서에 명시한다.

(카) 프로젝트에서 프로세스 수행 내용을 감시한다.
(a) 프로세스 감시는 프로젝트 목푯값에 대비하여 프로세스 측정값과 측정값의 경향성 검토 등에 대한 분석을 포함한다.

(3) 프로젝트 통제

(가) 식별된 문제를 해결하는 데 필요한 시정조치를 한다.
(a) 시정조치는 주로 프로젝트 성과 또는 기술적 진척도가 계획된 목푯값을 달성하지 못한 경우에 수행한다.
(b) 수정, 예방 및 문제 해결 활동을 포함한다.
(c) 프로젝트 또는 기술적 성취도가 계획된 목푯값을 초과 달성한 경우 또는 기반시설이 부적절하거나 가용할 수 없는 경우에는 일반적으로 계획을 수정하거나 인력, 도구 및 기반 구조 자산을 재할당한다.
(d) 프로젝트의 비용, 일정 및 기술적 범위에 영향을 미칠 수 있다.
(e) 시정조치로 인해 소프트웨어 생명주기 프로세스의 수행 내용을 변경 할 수 있다.
(f) 필요한 활동의 적합성과 적시성을 확인하기 위하여 기록하고 검토하여야 한다.

(나) 프로젝트 재계획이 필요한 부분에 대해 재계획을 시작한다.
(a) 프로젝트 목표 또는 제약사항이 변경되거나 가정이 틀린 것으로 드러난 경우에는 프로젝트 재계획을 시작한다.
(b) 필요한 경우 시스템 통합조직과 공급자 간의 계약을 변경 할 수도 있다.

(다) 시스템 통합조직 또는 공급자의 요청에 따라 프로젝트 비용, 일정, 품질에 대한 계약 변경이 필요할 때 프로젝트에 대한 변경 조치를 시작한다.
(a) 공급에 관한 조건 및 조항을 수정하는 것부터 새로운 공급자의 선정을 시작하는 것을 포함된다.

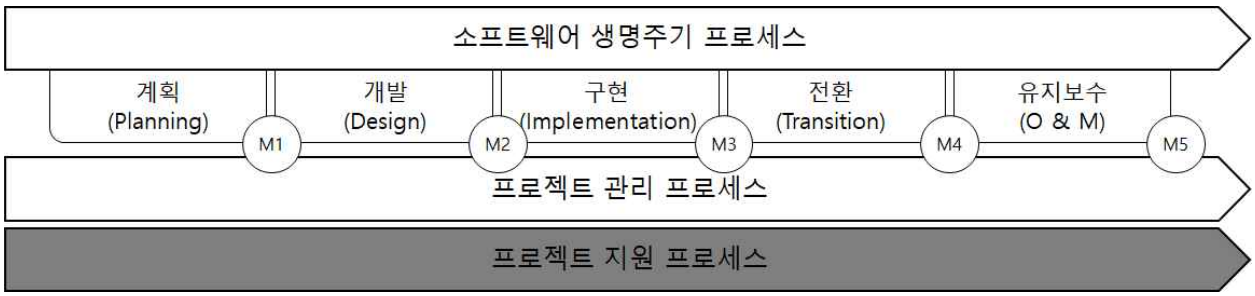
(라) 기준을 충족한 경우, 다음 마일스톤 또는 다음 이벤트로 진행하도록 프로젝트에 권한을 부여한다.
(a) 마일스톤 완료 기준 충족 여부에 대한 합의를 위해 프로젝트 평가 및 통제 프로세스를 활용한다.

3. 산출물

(1) 프로젝트 상태 평가
(2) 품질 보증 수행
(3) 프로젝트 팀 평가

(4) 프로젝트 진척 평가
(5) 관리 및 기술적 검토, 검사 수행
(6) 주요 프로세스/신기술 관찰
(7) 데이터 분석 및 권고
(8) 주기적 보고서 제공
(9) 프로젝트 통제 계획서
(10) 프로젝트 변경 보고서
(11) 요구사항 상태 보고서
(12) 프로젝트 진척 보고서

제 2 절 지원 프로세스



201. 일반사항

프로젝트 지원 프로세스는 다음으로 구성된다.

1. 의사결정 프로세스
2. 위험 관리 프로세스
3. 형상 관리 프로세스
4. 정보 관리 프로세스
5. 측정 프로세스

202. 의사결정 관리 프로세스

1. 일반사항

(1) 의사결정 관리 프로세스의 목적은 생명주기의 어느 시점에서든 의사 결정을 수행하기 위하여, 일련의 대안을 객관적으로 식별, 특성화 및 평가하기 위한 구조화된 분석 프레임워크를 제공하고 가장 유익한 조치 방안을 선택하는 것이다.

(가) 소프트웨어 생명주기 동안 발생하는 의사 결정 요청에 대응하고, 프로젝트 또는 기술적 쟁점사항을 해결하기 위하여 의사 결정 관리 프로세스를 적용한다.

(나) 프로세스를 통해 상황에 적합하며 바람직한 대안을 식별하고 선정한다.

(다) 활용한 가정 및 의사결정 근거 등과 같은 주요 연구 결과를 정리하여 의사 결정자에게 전달하고 미래의 의사결정을 위해 기록한다.

2. 활동

의사 결정 프로세스를 적용하는 프로젝트에서는 조직의 관련 정책과 수행 절차를 준수하면서 다음 활동을 수행하여야 한다.

(1) 의사 결정 준비

(가) 의사결정 관리 전략을 수립한다.

(a) 의사결정 관리 전략은 의사결정에 대한 책임과 권한의 식별 및 할당, 의사결정 범주 및 우선순위 선정방안의 식별을 포함한다.

(b) 의사결정은 효과도 평가의 결과로, 기술적 절충 분석의 결과, 해결이 필요한 문제, 수용 한계를 초과하는 위험에 대한 대응 행동, 새로운 기회의 출현, 생명주기의 다음 단계로 진행하기 위한 승인 등에 의해 발생할 수 있다.

(c) 의사결정 분석 에 적용하는 형식성 및 엄격성 수준의 결정은 조직 또는 프로젝트 지침을 준수한다.

(나) 의사 결정의 필요성과 환경을 식별한다.

(a) 문제 또는 기회와 이들을 해결할 여러 대안 조치 방안을 기록 및 분류하고, 기록하고 보고한다.

(다) 경험과 지식을 활용하기 위해 의사결정과 관련된 이해당사자들을 참여시킨다.

(a) 분석과 의사 결정 과정에 필요한 전문성을 식별하는 것이 좋다.

(2) 의사결정 정보 분석

(가) 각 의사결정 항목에 대하여 의사 결정 전략을 선택하여 선언한다.

(a) 문제 또는 기회의 해결에 필요한 대안 평가에 사용되는 데이터 및 시스템 분석 항목과 그 수행 강도를 결정한다.

(나) 바람직한 결과와 측정 가능한 성공 기준을 식별한다.

(a) 대안 선정 기준의 항목별 가중치를 결정하고, 모든 정량화 가능한 기준에 대한 기대값과 한계값을 결정한다.
(다) 대안과 절충 영역(trade space)을 식별한다.
(a) 대안이 다수 존재하는 경우에는 보다 상세한 시스템 분석을 위해 정성적으로 선별하여 대안을 관리 가능한 수로 줄인다.
(b) 정성적인 선별은 위험, 비용, 일정 및 규제 영향과 같은 요소에 대한 평가를 기반으로 한다.
(c) 절충 영역은 비용 및 성능에 대한 허용 범위로써, 비용 제약 조건에서 최고 성능을 내는 대안을 찾거나, 허용 성능 범위 내에서 최저 비용의 대안을 찾는 방법을 사용한다.
(라) 대안 선정 기준에 따라 각 대안을 평가한다.
(3) 의사 결정 수행 및 관리
(가) 각 의사 결정 항목별로 선호하는 대안을 결정한다.
(a) 대안을 선정 기준에 따라 정량적으로 평가한다.
(b) 선정된 대안은 일반적으로 관련 의사 결정에 대한 최적화 또는 개선 기회를 제공한다.
(나) 결론, 의사 결정 근거 및 가정을 기록한다.
(다) 의사 결정을 기록, 추적, 평가 및 보고한다.
(a) 조직의 절차 또는 계약에 정해진 바에 따라 문제와 기회 그리고 그 처리 결과를 기록하여, 조직이 경험으로부터 교훈을 배우고 심사에 대응할 수 있도록 한다.
(b) 의사 결정의 기록, 추적, 평가 및 보고를 통해 조직은 부정적인 경향이 호전되고, 기회의 이점을 확보하였으며, 문제가 효과적으로 해결되었음을 확인할 수 있다.

203. 위험 관리 프로세스

1. 일반사항

(1) 위험 관리 프로세스의 목적은 지속적으로 위험을 식별, 분석, 처리 및 감시하는 데 있다.
(2) 위험 관리 프로세스는 제품 및 서비스 시스템의 생명주기 전반에 걸쳐 지속적으로 그리고 체계적으로 위험에 대처하는 프로세스이다.
(3) 시스템의 획득, 개발, 유지보수 또는 운영과 관련된 위험을 다루는 데 활용 할 수 있다.

2. 활동

위험관리 프로세스를 적용하는 프로젝트에서는 조직의 관련 정책과 수행절차를 준수하면서 다음 활동을 수행하여야 한다.

(1) 위험관리 계획
(가) 위험관리 정책을 정의한다.
(a) 위험관리 정책은 공급망에 있는 모든 공급자의 위험관리 프로세스를 포함하며, 이 위험이 다음 단계로 어떻게 전이되는지를 포함한다.
(나) 위험 관리 프로세스의 적용 상황을 정의하고 기록한다.
(a) 기록에는 이해관계자의 인식, 위험 범주 그리고 기술 목표와 관리 목표에 대한 설며, 가정 및 제약사항을 포함한다.
(b) 위험 범주에는 시스템과 관련된 여러 기술 영역을 포함시켜 시스템 생명주기 동안 발생 가능한 위험을 용이하게 식별할 수 있도록 한다.
(c) 위험관리 프로세스의 적용 상황을 정의하고 기록하는 목적은 포괄적인 위험 목록을 작성하는 것이다.
(d) 위험 목록을 활용하여 프로젝트 목적 달성과 관련 있는 사건을 생성, 개선, 예방, 저하, 촉진 또는 지연시킨다,
(e) 위험의 한 유형인 기회는 시스템 또는 프로젝트에 잠재적 이점을 제공한다.
(f) 기회를 추구할 경우 예상하는 이익을 달성하지 못하는 위험이 발생할 수도 있다.
(g) 위험에는 기회로부터 얻어지는 이익을 획득하지 못하는 위험뿐만 아니라 기회를 추구하지 못하는 위험까지 포함한다.
(2) 위험 프로파일 관리
(가) 위험이 허용될 수 있는 위험 한계를 특정 조건과 함께 정의
(나) 위험 프로파일을 구축 및 유지한다. 위험 프로파일은 다음과 같은 사항으로 구성된다.
(a) 위험 프로파일 기록(위험 관리 상황)
(b) 각 위험 항목별로 위험 한계, 발생 확률 그리고 발생 시 영향을 포함하는 위험 상태에 대한 기록
(c) 이해관계자가 제공한 위험 기준에 기초한 각 위험의 우선 순위

(d) 위험 상태에 따른 위험관리 요청 활동
(e) 각 위험 항목별로 위험 상태의 변화가 있는 경우 위험 프로파일에 반영 및 최신화
(f) 위험 프로파일로부터 도출된 위험 우선순위에 따라 위험을 해결하기 위한 자원 배분
(다) 이해관계자의 필요에 따라 주기적으로 관련 위험 프로파일을 제공

(3) 위험 분석
(가) 위험관리 정황에 서술된 범주별로 위험을 식별한다.
(a) 위험은 일반적으로 다양한 분석과 준비 상태 평가 그리고 적정성 연구를 통해 식별한다.
(b) 위험은 생명주기 초기에 식별되어 시스템의 활용, 지원 및 용도 폐기까지 지속될 수 있다.
(c) 추가적으로 시스템의 각종 측정값에 대한 분석을 통해 위험을 식별할 수도 있다.
(나) 식별된 위험별로 발생확률과 발생 시 영향을 추정한다.
(다) 위험별로 해당 위험 한계에 대한 위험 수준을 평가한다.
(라) 위험 한계를 벗어난 각 위험에 대하여, 추천 조치 전략을 정의하고 문서화하고 측정한다.
(a) 위험 조치 전략은 위험 제거와 위험 발생 빈도 감소 또는 위험 발생으로 인한 영향 심각도의 감소와 위험 감수를 포함하며, 이 외에도 가능한 방안을 포함한다.
(b) 위험 처리는 위험 증가를 감수하고 기회를 추구하는 것도 포함한다.
(c) 처리 대안의 효과를 알 수 있도록 관련 척도를 정의한다.

(4) 위험 조치
(가) 위험을 조치하기 위한 추천 대안을 식별한다.
(나) 위험을 수용 가능한 수준으로 경감시키기 위해 이해관계자가 결정한 위험조치 대안을 실시한다.
(다) 위험한계를 초과하는 위험을 이해관계자가 수용할 경우, 이 위험은 우선순위가 높은 항목이며, 지속적으로 조사하여 더 이상 추가적인 위험 조치 활동이 필요한지를 결정해야 한다.
(라) 위험 조치가 선택되면, 이 장의 **1절 103. 2항**의 평가 및 통제 활동에 따라 관리 활동을 수행해야 한다.

(5) 위험 감시
(가) 모든 위험 및 위험 관리 상황에 대한 변화 여부를 지속적으로 감시하며, 그 상태가 변할 경우 위험을 평가한다.
(나) 위험 조치의 효과를 평가하기 위해 위험 평가 척도를 정의하고 측정 결과를 감시한다.
(다) 생명주기에 걸쳐 새로운 위험과 원인을 지속적으로 감시한다.

204. 형상 관리 프로세스

1. 일반사항

형상 관리 프로세스의 목적은 생명주기 전반에 걸쳐 시스템 요소 및 형상을 관리하고 통제하는데 있다. 형상관리는 또한 제품과 해당 제품에 대한 정의한 형상 간의 일관성을 관리한다.

2. 활동

프로젝트는 형상 관리 프로세스를 적용하는 프로젝트에서는 조직의 관련 정책과 수행 절차를 준수하면서 다음과 같은 활동을 수행하여야 한다.

(1) 형상 관리 계획
(가) 형상 관리 전략을 정의한다.
(a) 형상 관리 전략의 세부 내용은 다음 사항을 포함한다.
(i) 역할, 책임, 성과 책임 및 권한
(ii) 형상 항목에 대한 저장 등의 처분, 접근, 배포 및 변경 통제 관련 내용
(iii) 수립할 필수 베이스라인
(iv) 무결성, 보안성 및 안전성 규정을 충족하는 저장 위치 및 조건, 저장 매체를 포함한 기타 환경
(v) 형상 베이스라인을 포함하여 진화하는 형상을 유지 관리하고 제어하기 위한 기준 또는 이벤트
(vi) 형상 정의 정보의 무결성 및 보안성을 지속적으로 평가하기 위한 감사 전략 및 책임
(vii) 계획된 형상 통제 위원회, 정기 및 비상 변경 요청, 변경 관리 절차 등을 포함한 변경 관리 방안
(b) 형상 관리 전략은 일련의 시스템 통합조직, 공급자 및 공급망 조직 전반에 걸쳐 형상 관리 관련 조직 간 조정 방식을 포함한다.
(나) 형상 항목, 형상 관리 산출물 및 데이터에 대한 저장 및 검색 방법을 정의한다.

(2) 형상 식별 수행
(가) 형상 관리가 필요한 시스템 요소 및 정보 항목을 형상 항목으로 식별한다.

(a) 형상 항목은 특별히 주의하여 취급한다.
(b) 형상 항목은 일반적으로 고유 식별자를 할당받으며, 검토 및 형상 감시의 대상이 된다.
(c) 형상 통제 대상은 일반적으로 요구사항, 제품 및 시스템 요소, 정보 항목 및 베이스라인을 포함한다.
(나) 계층 구조(hierarchy)를 포함하여 시스템 정보 구조를 식별한다.
(다) 시스템, 시스템 구성 요소 그리고 정보 항목 식별자의 구조를 구축한다.
(a) 식별자를 활용하여 형상 통제 대상 항목의 규격을 포함한 기록 정보를 명확하게 추적할 수 있도록 한다.
(라) 생명주기 전반에 걸쳐 베이스라인을 정의한다.
(a) 베이스라인은 진화하는 시스템 요소의 지정된 시간 또는 정의된 상황에서의 형상 상태를 식별한 것이다.
(b) 베이스라인은 제품형상의 다음 변경을 위한 검토의 기준이 된다.
(마) 베이스라인 수립을 위해 시스템 통합조직과 공급자가 협의한다.
(a) 협의과정에서 프로젝트 평가 및 통제 프로세스를 활용한다.

(3) 형상 변경 관리 수행

형상 변경 관리는 설정된 베이스라인에 대한 변경을 관리하는 절차와 방법을 수립하여 수행한다.
(가) 형상 변경 요청 및 편차 허용 요청을 식별하고 기록한다.
(나) 형상 변경 요청 및 편차 허용 요청을 조정, 평가 및 처리한다.
(a) 제안된 변경에 의한 영향 평가, 즉 프로젝트 계획, 위험, 품질에 대한 영향 평가를 포함한다.
(b) 이 영향 평가 결과에 따라 변경 및 허용 요청의 수용 및 거부를 결정한다.
(다) 형상 변경 요청 및 편차 허용 요청과 승인된 베이스라인의 변경사항을 추적 관리한다.
(a) 추적, 일정 및 형상 변경 내용을 포함한다.
(b) 모든 변경사항과 의사 결정 근거를 기록한다.

(4) 형상 상태 정보 개발
(가) 시스템 요소, 베이스라인 및 배포에 대한 형상 관리 상태 정보를 개발하고 유지 관리한다.
(a) 형상 상태 통계는 시스템 생명주기 전반에 걸쳐 시스템 요소에 관한 결정을 내리는 데 필요한 관리 제품의 상태 데이터를 제공한다.
(b) 하나의 형상 상태는 다른 형상 상태와 순방향 및 역방향 추적이 가능하여야 한다.
(나) 형상 관리 데이터를 수집, 저장 및 보고한다.

(5) 형상 평가
(가) 형상 관리 감시의 필요성을 식별하고 감사 일정 계획을 수립한다.
(나) 형상 제품이 형상 요구사항을 충족시키는지 검증한다.
(다) 승인된 형상 변경 내용의 적용 여부를 감사한다.
(라) 시스템이 기능 베이스라인에 정의된 기능 및 성능 규격을 충족시키는지 평가한다.
(마) 시스템이 운용 정보 항목 및 형상 정보 항목을 준수하는지 평가한다.
(바) 형상 감사 결과와 이에 따른 이행 활동 내용을 기록한다.

(6) 형상 배포 통제
(가) 시스템 배포와 인도물을 승인한다.
(a) 배포의 목적은 제약이 있는 또는 없는 상태에서 특정 목적을 위해 시스템 사용 권한을 승인하는 데 있다.
(b) 배포는 일반적으로 일련의 변경사항을 포함한다.
(c) 배포 승인을 위해서는 일반적으로 검증 및 확인된 변경사항에 대한 수락 활동을 수행한다.
(나) 시스템 배포와 인도물을 추적 관리한다.
(a) 필요한 경우 모든 시스템 요소의 마스터 사본은 시스템 수명 동안 유지한다.

205. 정보 관리 프로세스

1. 일반사항

(1) 정보 관리 프로세스의 목적은 지정된 당사자들에게 정보를 생성, 수집, 확인, 변형, 보관, 검색, 분배 및 폐기하는 데 있다.

(2) 정보 관리를 통해 모호하지 않고, 완전하고, 검증 가능하며, 일관성 있고, 수정 가능하며, 추적 가능하고, 표현할 수 있는 정보를 지정된 이해관계자에게 제공하는 것을 계획, 실행 및 통제한다.

(3) 프로세스는 기술 정보, 프로젝트 정보, 조직 정보, 계약 정보 및 사용자 관련 정보를 포함한 지정된 정보를 관리한다. 이러한 정보는 조직, 시스템, 프로세스 또는 프로젝트의 데이터 기록에서 파생될 수 있다.

2. 활동

프로젝트는 정보 관리 프로세스를 적용하는 프로젝트에서는 조직의 관련 정책과 수행 절차를 준수하면서 다음과 같은 활동을 수행하여야 한다.

(1) 정보 관리 준비

(가) 정보 관리 전략을 정의한다.

(a) 동일한 주제에 대한 정보가 생명주기의 다른 지점에서, 다른 사용자를 위해 서로 다른 방식으로 개발될 수 있다.

(나) 관리 대상 정보 항목을 정의한다.

(a) 관리 대상 정보 항목에는 시스템 생명주기 동안 관리되어야 하고, 그 후 정의된 기간 동안 유지되어야 하는 정보를 포함한다.

(b) 관리 대상 정보 항목을 정의할 때는 조직의 정책, 계약 또는 법률에서 정의한 정보 항목 요구를 반영한다.

(다) 정보 관리를 위한 권한과 책임을 지정한다.

(a) 법률, 보안 및 사생활 보호와 같은 제한조건 또는 강제조건이 적용되는 정보는 조건에 맞춰서 식별한다.

(b) (a)의 조건에 해당되는 정보 품목의 지식을 갖고 있는 인원에게는 그들의 책임과 의무를 알려준다.

(라) 정보 유지 관리 활동을 정의한다.

(마) 정보 유지보수 활동을 정의한다.

(a) 정보 유지 관리 활동은 저장된 정보의 상태 검토를 무결성, 유효성 및 가용성 관점에서 수행한다.

(2) 정보 관리 수행

(가) 정보 항목을 수집, 개발 또는 변환한다.

(a) 정보 표준에 적합하도록 정보를 검토, 확인 및 편집하는 작업도 포함한다.

(나) 정보 항목과 저장 기록 및 정보 상태 기록을 유지한다.

(a) 정보 항목은 무결성, 보안성 및 개인 정보 보호 요구사항에 따라 유지 관리한다.

(b) 정보 항목의 상태(예 : 버전 설명, 발행일 또는 유효 기간, 배포 기록, 보안 분류)를 유지한다.

(c) 정보를 변환하는 데 사용된 원천 데이터 및 도구는 결과 문서와 함께 형상 관리 프로세스를 준수하는 형상 통제 대상이 된다.

(다) 정보 및 정보 항목을 지정된 이해관계자에게 게시 및 배포하고 접근 권한을 제공한다.

(a) 합의된 일정이나 정해진 상황에 따라 규정된 양식으로 정보를 지정된 당사자들에게 제공한다.

(b) 필요시 정보 항목에는 인증, 조직 역량 인가, 면허 또는 등급 평가에 필요한 공식 문서를 포함한다.

(라) 지정된 정보를 기록 보존한다.

(a) 감사, 지식 보관 및 프로젝트 종료 등의 목적에 따라 기록 보존을 수행한다.

(마) 조직의 정책, 보안 요구사항에 따라 불필요한 정보, 미 검증 정보, 무가치한 정보를 폐기한다.

206. 측정 프로세스

1. 일반사항

측정 프로세스의 목적은 객관적인 데이터와 정보를 수집, 분석 및 보고하여 효과적인 관리를 지원하고 제품, 서비스 및 프로세스의 품질을 입증하는 것이다.

2. 활동

측정 프로세스를 적용하는 프로젝트에서는 조직의 관련 정책과 수행 절차를 준수하면서 다음 활동을 수행하여야 한다.

(1) 측정 준비

(가) 측정 전략을 정의한다.

(나) 측정과 관련된 조직의 특성을 서술한다.

(다) 정보의 수요를 식별하고 우선순위를 정한다.

(라) 정보의 수요를 충족시키는 척도를 선정 및 규정한다.

(마) 데이터 수집, 분석, 접근 및 보고 절차를 정의한다.

(바) 정보 결과물 및 측정 프로세스를 평가하기 위한 기준을 정의한다.

(사) 측정에 필요한 서비스와 지원 시스템을 식별하여 측정 계획에 반영한다.

(2) 측정 수행

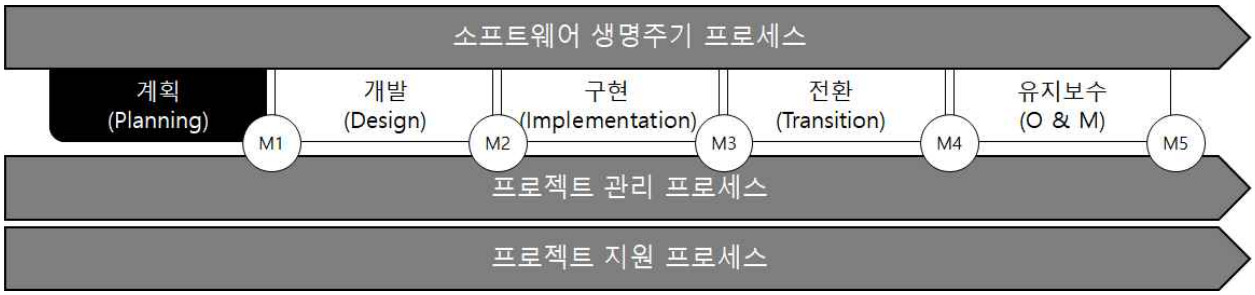
(가) 데이터 생성, 수집, 분석 및 보고를 위한 절차를 관련 프로세스와 통합한다.

(나) 데이터를 수집, 저장 및 검증한다.

(다) 데이터를 분석하여 정보 항목을 개발한다.
(라) 결과를 기록하고 사용자에게 전달한다.
(a) 측정 분석 결과는 의사 결정을 지원하고 시정 조치, 위험 관리 및 개선을 지원하기 위해 적시에 사용될 수 있도록 관련 이해관계자에게 보고한다.
(b) 결과는 의사 결정 프로세스 참가자, 기술 및 관리 검토 참여자, 제품 및 프로세스 개선 프로세스 책임자 등으로 이들에게 측정 분석 결과를 보고한다. ⚓

제 5 장 소프트웨어 생명주기 프로세스

제 1 절 계획 프로세스



101. 일반사항

1. 계획 프로세스는 소프트웨어 생명주기 전반에 걸쳐 통합 소프트웨어와 관련이 있는 이해관계자를 식별하고, 그들의 필요와 요구를 식별한다.
2. 계획 프로세스는 이해관계자의 필요와 요구를 고려하여, 안전 검토 및 무결성 레벨 평가가 가능하도록 충분한 세부사항으로 통합 소프트웨어를 정의한다.
3. 계획 프로세스는 개발 단계를 시작하기 위해 시스템 통합 조직에서 필요한 아키텍처, 표준, 설명 및 요건을 포함하는 ConOps를 완성하는 것을 목적으로 하고, 통합 소프트웨어의 구성 요소 인 HMI (Human Machine Interfaces) 및 패키지와 연결된 통합 시스템의 공급자를 식별하여야 한다.
4. 계획 프로세스는 기능에 대해서 무결성 레벨 (IL)을 정하고, 이 무결성 레벨(IL)은 개발 프로세스에서 적합한 소프트웨어 모듈에 적용한다.

102. 활동

계획 프로세스 동안 이해관계자를 파악하고, 통합 소프트웨어 구성을 위한 요구사항을 파악 및 평가 하게 된다. 이 프로세스의 활동은 IEEE 12207-1-2008 Second Edition, 2008-02-01, IEEE 시스템 및 소프트웨어 엔지니어링 - 소프트웨어 생명주기 프로세스를 참조하여 개발되었으며 다음과 같다.

No.	활동 Activity
소유자	
1	역할과 책임 지정, 소유자 관련 부서원, 사용자, 시스템 통합 조직 구분
2	소유자의 팀원 할당
3	전체 프로젝트 및 일반적인 시스템 요건 업데이트
4	통합 제어 시스템에 대한 변경관리 절차 개발
5	SDLC를 이용한 개발 프로세스 추적
6	업무의 조정, 갈등 해결 방법 설계
7	통합 시스템 구성요소 식별
8	ARMS 고려
9	안전성 검토 관리, 결과 문서 제공
10	무결성 수준 정의 제공
11	통합 시스템으로부터 필수적인 시스템의 독립적인 운영 수단
12	ISPM 제어 시스템의 모든 기능에 무결성 번호 할당
13	확인 방법 선택
14	공급업체 패키지에 대한 V&V 보고서 및/또는 V&V 계획 포함
15	검토에 대한 ConOps 개발 및 제공
16	ConOps 검토의 강화된 의견의 보고서
17	권고된 매트릭스
18	계획단계에서 시스템 통합 조직에게 지원 정보 제공
19	통합 시스템의 생명주기 관리 선택
20	개발 단계로 진행하기 위헌 권한 부여
사용자	
1	사용자의 팀원 할당
2	사용자의 팀원에게 역할과 책임 할당
3	업무의 조정, 충돌 해결 방법과 함께 소유자 지원
4	최소 요구사항 및 설계 수립 지원
5	안정성 검토 회의에 참석
6	무결성 수준 할당 회의에 참석
7	정보요구와 함께 소유자 및 시스템 통합 조직 지원
8	ConOps 검토
9	통합 시스템의 구성요소 설명서 제공
10	정상상태, 성능 저하 또는 고장 조건 동안 기능 활동의 설명서 제공

No.	활동 Activity
시스템 통합 조직	
1	소유자의 요건 수집
2	시스템 통합 조직의 선임 기술 직원 할당
3	현재 ISO9001 또는 CMMI 레벨 2 인증서 제공
4	SDLC를 이용한 개발 프로세스 추적
5	하위 공급업체 제약사항 수집
6	업무의 조정, 충돌 해결 방법 설계
7	기본적인 통합 모델이 개발된 경우 조직에게 제공
8	모든 통합 시스템 기능을 식별하여 사용자를 도움
9	시스템 요건 분석
10	안전성 검토 회의 참석
11	무결성 할당과 함께 소유자 도움
12	시스템 통합 아키텍처 설계
13	하드웨어에 대한 노후화 계획
14	소프트웨어에 대한 노후화 계획
15	선택된 검증 방법 검토
16	ConOps 검토
공급자	
1	요구하는 조직에게 기기 제한 또는 제약사항 제공
2	ISPM 제어 시스템에 연결된 패키지에 대한 V&V 보고서
3	ISPM 제어 시스템에 연결된 패키지에 대한 V&V 계획
4	현재 ISO 9001 인증서 제공
5	기본적인 통합 모델 검토. 설계에서 기본적인 모델 사용

102. 계획 프로세스 개발

1. 설계업무의 조정, 식별 및 갈등 해결 방법 (공급 업체에 대한 통합 시스템)을 문서화하여야 한다. 사용된 표준, 안전, 보안 및 인적 요소를 문서화 하여야 한다. 위의 요인을 분석 한 결과로 만들어진 문서는 형상 관리를 하는 것이 좋다.
2. 기본적인 통합 모델은 통합 소프트웨어에서 관련 소프트웨어 모듈 간의 통신을 위한 공통 기반을 제공하여, 이해관계자 사이의 문제를 식별하고 해결책을 결정하는 데 도움이 된다.
   (1) SI는 프로젝트 전반에 걸쳐 사용되는 기본적인 통합 모델을 정의하고 계획 단계 초기에 모든 이해 관계자와 공급업체에 기본적인 통합 모델을 제공하는 것이 좋다.

103. 통합 모델 요구사항 분석

1. SI는 통합 모델의 요구사항을 분석하여야 한다. 통합 소프트웨어의 요구사항 분석은 ConOps 개발을 위한 활동으로 통합 소프트웨어의 전체적인 요구사항을 정하고 관련된 타협에 초점을 둔다.
2. 다음의 사항들이 문서화 되어야 한다.
   (1) 기능 요구사항, 전체 시스템의 특성;
   (2) 접근성
   (3) 신뢰성
   (4) 유지 보수성
   (5) 안전성
3. 접근성, 신뢰성, 유지 보수성 및 안전성 (ARMS 또는 RAMS)에 대한 추가 고려 사항은 다음과 같다.

(1) 보안
(2) 인적 요소 엔지니어링 인터페이스 요건
(3) 설계 제약
(4) 자격 요건

4. 통합 모델 요구사항은 다음을 고려하여 평가하여야 한다.
(1) 추적성
(2) 일관성
(3) 테스트 가능성
(4) 운영 및 유지 보수 실행 가능성 (ARMS)

104. 통합 모델 아키텍처 설계

1. 통합 모델 아키텍처 설계는 ConOps 개발을 위한 활동이다. 통합 모델 아키텍처 설계 활동을 통해서 시스템의 최상위 아키텍처가 생성된다. 이 아키텍처는 그룹화를 식별하고 가능하게 한다. 권장하는 그룹화 구성은 다음과 같다.
(1) 하드웨어
(2) 소프트웨어
(3) 수동 조작 항목
2. 모든 소프트웨어 요구사항은 추적성 매트릭스에 표시하는 것이 좋다.
3. 통합 모델 아키텍처 평가 시 권장하는 기준은 다음과 같다.
(1) 추적성
(2) 일관성
(3) 적합성
(4) 실행 가능성

105. 리스크 관리

필수 기능 및 안전 기능과 같은 중요한 기능을 용이하게 식별하기 위해서 정의 된 기능에 대한 안전성 검토를 수행하여야 한다. ANSI / ISA-84 및 IEC61508 프로세스에서 무결성 레벨 (IL) 평가를 위해 사용 된 기술을 필요시 사용할 수 있다. 안전성 검토는 다른 안전성 및 작동 가능성의 검토, 하드웨어 FMEA 또는 소프트웨어 FMECA와 결합 될 수 있습니다.

1. 안전성 검토 및 신기술

(1) SIS 안전 시스템
통합 되거나 통합되지 않은 SIS 안전 시스템은 안전 무결성 레벨 (SIL) 평가를 위해 ANSI / ISA-84 또는 IEC61508을 준수해야한다.
(가) 안전 시스템에 ANSI / ISA-84 또는 IEC61508을 사용하는 경우 IL 평가는 SIS 기능에 적용되지 않는다.
(나) 이 지침은 SIL (IEC61508 또는 ANSI / ISA-84에 따라) 또는 IL (ISPM에 따라) 번호를 정하기 위한 절차를 제공하지 않는다.

(2) 안전성 검토
안전성 검토는 통합 시스템 및 관련 패키지, 유닛 및 연결된 장비에서 수행하여야 한다. SI, 소유자, 사용자, 선박 건조업체 및 우리 선급의 입회하에 안전성 검토를 하는 것을 권고한다.

(3) ConOps 검토
(가) SI 및 사용자는 ConOps를 검토하여야 한다. 검토 의견 및 권장 사항들은 문서화 되어야한다. SI가 ConOps를 개발 한 경우 소유자 및 사용자는 ConOps를 검토하여야 한다.
(나) 검토 의견은 우리선급에 제출하여야 한다.

(4) 신기술 또는 검증되지 않은 기술
새로운 또는 검증되지 않은 기술은 추가적인 위험을 수반 할 수도 있다. 신기술은 하드웨어, 기계 장비, 인터페이스 프로토콜 또는 소프트웨어 모듈 코딩 일 수 있다.
(가) 새로운 필수 시스템 또는 필수 기능은 최소한 IL2의 무결성 레벨을 부여 하여야 한다.
(나) 새로운 SIS 기능은 IL3의 최소 무결성 레벨을 부여 하여야 한다.
(다) 새로운 비 필수 시스템 및 비 SIS 기능은 적어도 IL1의 무결성 레벨을 부여 하여야 한다.

2. 무결성 레벨 (IL) 평가

무결성 레벨 (Integrity Level, IL)은 기능이 작동하지 않은 경우의 결과를 바탕으로 평가하여야 한다. 무결성 수준은 기능이 시스템 작동에 있어 얼마나 중요한지를 나타낸다. IL 번호는 소유자 및/또는 사용자가 기능이 페일 세이프 상황을 포함하여 정해진 대로 작동하기를 원하는 신뢰도를 나타낸다. IL 번호는 사용자 및 SI의 의견을 고려하여, 국제 및 국가 표준, 선급 협회의 요건을 유의하여 소유자를 지정하여야 한다. 무결성 레벨은 성능에 대해 기대되는 신뢰도 및 고장 결과의 심각성으로부터 파생된다.

(1) IL 평가는 다음을 따른다.
  (가) 안전상의 결과
  (나) 환경적 결과
  (다) 사업적인 영향 (선택사항)

(2) 기능은 안전성 및 환경의 범주에서 평가하여야 한다. 사업적인 영향은 선택 사항으로 간주한다. 사업적인 영향은 선택적이며 우리선급에 의해 검토되지 않는다. IL 지정을 위해 기능을 평가할 때 잠재적인 안전성 및 환경적 영향이 고려하여야 한다. 무결성 레벨의 지정은 회사의 위험 허용범위 및 잠재적인 사업의 영향으로 증가 할 수 있다.

(3) 4 개의 무결성 레벨 (IL)이 있다. 각각은 안전, 환경 또는 비즈니스 결과에 거의 또는 전혀 영향을 미치지 않는 것으로 간주하는 IL0에서 안전성, 환경 또는 비즈니스 문제에 중대한 영향을 미칠 수 있는 IL3까지 점점 더 심각한 결과를 야기한다. ISPM 제어 시스템은 소프트웨어 기능의 가장 높은 IL을 적용한다. IL0에서 IL2로 매겨진 기능들로 구성된 제어 시스템과 IL3인 한 개의 소프트웨어 기능이 있는 제어 시스템에는 IL3으로 모든 기능들에 지정하여야 한다. 다만 위험성 분석 결과에 따라 다른 기능들에 대해 상위 IL을 요구하지 않을 경우, ISPM 제어 시스템 내의 모든 기능에 IL3 등급을 할당하지 않을 수도 있다.

(4) 중요 시스템 및 기능 :
  (가) 중요 시스템 및 기능은 IL2 또는 IL3으로 지정된다. 중요 시스템은 정당성, 이중화 등을 고려하여 IL1을 할당받을 수 있다.
  (나) SIS는 IEC61508 또는 ANSI/ISA 84, IMO 및 소유자의 비 SIS 기능 또는 시스템에 대한 선택적 요구에 의해 IL3으로 지정하여야 한다. SIS 시스템은 정당성, 이중화 등을 고려하여 IL2 를 할당받을 수 있다.
  (다) 소프트웨어 기능을 이용하는 ESD 시스템은 IL3이어야한다. ESD 시스템은 정당성, 이중화 등을 고려하여 IL2를 할당받을 수 있다.
  계획 단계에서 IL 할당의 구현은 개별 기능과 시스템 전체를 정밀 조사할 수 있다. IL 할당의 목표는 안정적인 통합 시스템을 제공하는 것입니다. 위험성은 일정, 하드웨어 및/또는 소프트웨어 노후화 그리고 소프트웨어 개발의 신뢰성(품질)을 포함하여야 한다. 할당된 IL은 기능의 소프트웨어 모듈 (코드)에 적용하여야 한다.

(5) 전체적인 통합 시스템의 IL은 ISPM 제어 시스템에 의해 제어되는 기능 중 할당 된 가장 높은 IL 번호와 동일하게 적용하여야 한다.

(6) 소유자와 사용자는 기능의 IL 평가에 사용된 기준을 우리선급에 제공하여야 한다. 소유자와 사용자는 위에서 사용된 용어를 회사의 위험 허용 범위에 맞춰 개선할 수 있다.

표 1 무결성 레벨

IL	잠재적인 결과		
	안전	환경	사업적인 영향
0	경미한 정도(1)	경미한 정도(1)	운영상 경미한 영향. 지원 프로세스 시스템에는 영향을 줄 수 있지만 기본 프로세스 시스템에는 영향을 미치지 아니 함.
1	사소한(2) 안전사고로 이어질 수 있다.	사소한(2) 환경사고로 이어질 수 있다.	중요하지 않은 시스템의 유지보수 정지로 이어질 수 있다. 주요 프로세스는 계속 작동 한다.
2	짧은 시간 내에 심각한 손상, 시간 손실, 사고 또는 인명 손실이 발생 할 수 있음.	중요한(3) 환경 영향	주요 시스템의 정지. 장시간 동안 수리
3	즉각적이고 치명적인(4) 시간 손실 또는 다수의 인명 손실	치명적(4) 환경 영향	상당한 수리 시간 또는 조선/해양 자산의 손실
(비고) (1) 경미한 정도 : 업무용이 아닌 시스템의 정지 또는 성능 저하 (2) 사소한 : 시간 손실, 선박 또는 유닛 성능 저하 또는 일부 재정적 손실 또는 사회적 손실. (3) 중요한 : 영구적인 손상 또는 다중 시간 손실, 업무상 중요한 시스템 피해 또는 심각한 재정적 손실 또는 사회적 손실. (4) 치명적인 : 인명 손실, 자산 손실, 시스템 안전 또는 보안 상실 또는 광범위한 재정적 손실 또는 사회적 손실.			

3. IL 할당 기능 문서 요건

(1) IL0

일반적으로 필수적이지 않고 상대적으로 중요하지 않은 기능을 제어하고 감시한다. 사용자가 중요 결정을 내리는 데 정보를 이용하지 않고, 안전성이나 중요하고 필수적인 소프트웨어 모듈의 알고리즘(소프트웨어 모듈)에서 데이터를 사용하지 않는 중요하거나 필수적인 기능을 모니터링 한다.

(가) 그 기능의 운영상 또는 정상 상태(성능 저하 또는 고장 조건에는 필요하지 않음)에 대한 설명은 ConOps에 명시되어야 한다.

(나) 사용자가 필수적이거나 중요한 결정을 내리기 위해 HMI에 표시되는 데이터는 IL0가 아니다. 이 데이터는 사람의 경험과 지식이 프로세스의 안전한 작동을 위해 사용되는 시추 작업에 적용될 수 있다.

(다) 인터페이스 설명

이중화 실행 시스템에 간섭하지 않고 테스팅, 복구 및 재시작에 대한 ARMS 요건을 지정하여야 한다.

(2) IL1

일반적으로 필수적이지 않은 기능의 모니터링 및/또는 제어 :

(가) 기능의 정상 운전 상태에 대한 설명을 ConOps에 명시하여야 한다.

(나) 고장 조건 및 상태에 대한 설명을 ConOps에 명시하여야 한다.

(다) 인터페이스에 대해 설명 하여 한다.

(라) 이중화 실행 시스템에 간섭하지 않고 테스팅, 복구 및 재시작에 대한 ARMS 요건을 지정하여 한다.

(마) 시스템이 이중화되는 경우 이중화 운영 구성 요소 또는 부품에 간섭받지 않고 테스팅, 수리 및 재시작에 대한 요건을 지정하여 한다.

(바) 교체 구성 요소 또는 부품을 가진 ARMS에 대해 노후화 위험이 정의되고 옵션이 선택된다.

(3) IL2

필수적이고 중요한 시스템과 기능 :

(가) 기능의 정상적인 상태에 대한 설명을 ConOps에 명시하여야 한다.

(나) 기능의 저하 조건 및 상태에 대한 설명을 ConOps에 명시하여야 한다.

(다) 고장 조건 및 상태에 대한 설명을 ConOps에 명시하여야 한다.

(라) 인터페이스 설명하여야 한다.

(마) 시스템이 이중화되는 경우 이중화 운영 구성 요소 또는 부품에 간섭받지 않고 테스팅, 수리 및 재시작에 대한 요건을 지정하여야 한다.

(바) 이중화 운영 구성 요소 또는 부품에 간섭받지 않고 테스팅, 수리 및 재시작 요건을 지정하여야 한다.
(사) 대체 구성 요소 또는 부품을 가진 ARMS에 대해 노후화 위험이 정의되고 옵션이 선택된다.

(4) IL3

필수, SIS 및 중요한 시스템 및 기능 :

(가) 정상 상태 요건에 대한 설명은 ConOps에 명시되어야한다.
(나) 기능의 저하 조건 및 상태에 대한 설명은 ConOps에 명시하여야 한다.
(다) 고장 조건 및 상태에 대한 설명은 ConOps에 명시하여야 한다.
(라) 인터페이스 설명
(마) 시스템이 이중화되는 경우 이중화 운영 구성 요소 또는 부품에 간섭받지 않고 테스팅, 수리 및 재시작에 대한 요건을 지정하여야 한다.
(바) 이중화 운영 구성 요소 또는 부품에 간섭받지 않고 테스팅, 수리 및 재시작 요건을 지정하여야 한다.
(사) 대체 구성 요소 또는 부품을 가진 ARMS에 대해 노후화 위험이 정의되고 옵션이 선택 된다.

4. 소프트웨어 품질 관리

(1) 소유자는 따라야 할 확인 방법을 지정해야 한다. 통합 시스템 소프트웨어의 확인에는 세 가지 옵션이 있다. V&V 단계에서 시스템 소프트웨어는 최소한 SRS 및 SDS에 지정된 대로 작동하여야 한다. 소유자가 선택한 방법이 가능한 경우 IL2 및 IL3 기능을 확인하는 경우 세 가지 확인 방법 모두를 사용할 수 있다.
(가) 페루프 검증
(나) 소프트웨어 인 더 루프 검증
(다) 하드웨어 인 더 루프 검증

(2) 확인 방법의 선택은 기능 및 관련 소프트웨어 모듈의 복잡성, 기능의 무결성 레벨 및 통합할 공급자 패키지의 수량에 대한 고려가 포함된다. 시뮬레이션의 개발은 소프트웨어 개발의 종결이 아니라 통합 시스템 소프트웨어 개발과 병행하여 수행된다.

5. 노후화 계획

(1) SI는 통합 시스템을 위한 높은 수준의 하드웨어 노후화 계획을 제공하는 것이다. 접근성, 신뢰성, 유지 보수성 및 안전성 (ARMS)은 계획을 수립 할 때 고려하여야 한다.

(2) SI는 통합 시스템 소프트웨어에 대한 높은 수준의 소프트웨어 노후화 계획을 제공하는 것이다.

106. 운용 계획서 (Concept of Operations 이하 ConOps)

ConOps는 소유자 (소유자가 개발하지 않은 경우), 선박 건조업체, 사용자, SI (SI가 개발하지 않은 경우) 및 우리선급에 의해 검토되어야 한다. ConOps는 106. 1.에 나열된 정보를 포함해야 한다. 계약 당사자와의 계약 또는 기타 계약에 따라 기간을 검토한다.

1. 일반적인 주제

(1) 프로젝트의 전반적인 범위와 목표

(2) 공급자 패키지(해당되는 경우)
(가) 제조업체 또는 SI 또는 공급자의 부품 번호
(나) 모델 번호(가능한 경우)
(다) 인터페이스 프로토콜
(라) 제약

(3) 기능 설명 :
(가) RD 단계 문서를 개발하기에 충분한 세부 사항.
시스템 통합 조직은 "충분히"라는 단어를 입력 할 수 있다. 공통적이고 잘 이해된 기능에 대해 세부 사항은 한 줄의 진술로 "충분한" 할 수 있다.
(나) 모든 기능은 설명과 할당된 무결성 레벨 (IL0 ~ IL3)을 가져야한다.
(다) 페일 세이프 (fail safe) 상태.

(4) 휴먼 머신 인터페이스의 번호 및 설명은 다음을 포함해야 한다 :
(가) 제조자
(나) 모델 번호 또는 SI 또는 공급자의 부품 번호(가능한 경우)
(다) 인터페이스 프로토콜
(라) 제약사항

(5) 인터페이스의 번호 및 설명 (데이터 수집, SCADA 시스템 ...) :
(가) ISPM 제어 시스템에 대한 네트워크 또는 직접 연결의 수량
(나) 인터페이스 네트워크, 제어 시스템 및 / 또는 장비의 인터페이스 프로토콜
(다) 인터페이스 네트워크, 제어 시스템 및 / 또는 장비의 제약사항
(6) 주요 확인 방법

2. 프로젝트 범위의 정의

사용자로부터 의견을 가진 소유자는 ConOps에 통합 시스템의 목적과 범위를 명시해야 한다.

3. 통합 시스템 주요 구성 요소 및 경계

(1) 주요 패키지 또는 구성 요소는 높은 무결성 레벨에서 예비 선정되어야한다. 이 시점에서 SI 및 / 또는 소유자는 ConOps를 충족시키기 위해 다른 공급자로 부터 인터페이스 또는 연결된 장비 패키지가 필요하다는 것을 알고 있다. Dynamic Positioning System은 Vendor Xyz로부터 Power Management System과 인터페이스 할 것이다. 인터페이스 또는 연결된 장비 및 HMI의 목록이 ConOps에 포함된다.

(2) 제어 시스템 구성 요소 이중화는 중복 제어 시스템이 동일한 소프트웨어를 실행하는 경우 기능의 무결성 레벨을 낮추지 않는다. 여기에는 통합 시스템과 연결된 구성 요소가 포함된다. 소프트웨어에 결함이 있는 경우 주요 및 백업 제어 시스템이 동일한 코드를 실행하고 있기 때문에 제어중인 기능 및 관련 연결된 구성 요소 또는 장비가 고장 날 수 있다.

(3) 이중화가 두 가지 기술 (PLC 제어 및 다른 제어 수단 또는 제어된 셧다운, 기계적, 유압 등)로 구성되는 경우 IL 번호를 낮출 수 있다.

4. 제약사항

(1) 제약사항은 운영 문서의 개념에서 확인되고 기술되어야한다. 여기에는 다음이 포함될 수 있다.
(가) 공급자의 패키지 제약사항
(나) 적용될 현재 존재하는 기술, 신기술
(다) 소프트웨어 제한 (알고있는 경우)
(라) 공급자 패키지 (기능)의 네트워크 또는 연속적인 통신 제한 (알고 있는 경우)
(마) 예상된 소프트웨어 기능 위험 평가
공급자의 패키지는 통합 시스템에 대한 추가적인 하드웨어 모듈에 대해 요구를 이끄는 9600 BPS에서 Modbus를 사용하여 통신 할 수 있어야 한다. 프로세스 제어 그룹은 입증되지 않은 소프트웨어 모듈 (퍼지 로직, 모델 예측 제어)을 사용하여 고급 제어를 제안 할 수 있지만 위험은 소유자에 의해 너무 높게 판단되어 보다 단순하고 입증 된 제어를 사용하게 된다.

(2) 공급자의 제약은 필요에 따라 완화되어야한다.

107. 산출물

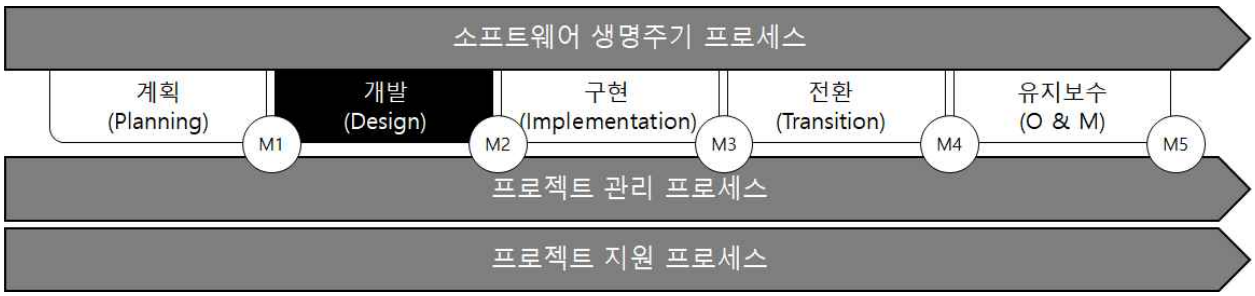
1. 계획 프로세스의 주요 산출물은 105.에 따른 ConOps이며, 소유자는 필요한 경우 ConOps 개발을 위해 SI 또는 선박 건조업체로부터 정보를 요청할 수 있다. ConOps는 적어도 다음의 사항을 포함하여야 한다.
(1) SDLC에서 사용하기 위한 기능의 추적성을 제공하고 기능을 식별.
(2) 안전성 검토의 권고 사항을 기능 설명 및 ConOps에 포함(해당되는 경우).
(3) 각 기능별 무결성 레벨을 할당
(4) 통합 시스템의 구성 요소를 식별
(5) 경보 관리 방침을 정의
2. ConOps에서는 이후 SDLC 단계에서 기능, 활동 및 산출물이 추적 가능하도록 하는 것이 좋다.
3. 기능 및 인터페이스의 정의에 대한 설명은 공급자의 자료와 함께 ConOps의 중요한 부분이다.

108. 계획 프로세스 마일스톤 (M1)

1. 통합 시스템의 구성 요소가 식별된다.
2. 안전성 검토 보고서가 제출된다.
3. ConOps는 안전 검토, FMEA 등으로 업데이트 된다. (승인 된 권장 사항)
4. 무결성 수준은 기능에 할당된다.
5. 변경 관리 절차 (MOC)가 ConOps에 적용된다.
6. 잠재적인 하청 업체와 협의.

7. ISPM 제어 시스템의 주요 V & V 방법 선택
8. 공급자의 V&V 계획은 IL2 또는 IL3 ISPM 제어 시스템 패키지에 대해 제공되고 예외사항은 ConOps에 명시된다. V & V 보고서는 개발 단계에서 인도 될 수 있다. 개발을 시작하기 위해 IL2 및 IL3 시스템에 대한 모든 공급 업체에 V & V 보고서를 작성할 필요는 없다.
9. 패키지와 연결된 IL1 ISPM 제어 시스템 대한 공급 업체의 V & V 보고서는 제공되며 예외사항은 ConOps에 명시된다. 확인 IL2 및 IL3 기능은 우리선급에 의해 입증되고 V & V 보고서는 ConOps 개발 시점에 제공되지 않을 수 있다. V & V 보고서는 개발 단계에서 인도 될 수 있다. 개발을 시작하기 위해 IL2 및 IL3 시스템에 대한 모든 공급 업체에 V & V 보고서를 작성할 필요는 없다.
10. 업데이트된 통합 시스템의 프로젝트 및 전체 일정이 완료된다.
11. 하드웨어 및 소프트웨어 노후화 계획은 ConOps에 포함된다.
12. ARMS 고려 사항은 ConOps에 명시되어 있다.
13. 설계 고려 사항 타협은 완료되고 ConOps에 포함된다.
14. ConOps는 사용자, SI 및 우리선급에 의해 검토 되었다. 계약 당사자와의 계약 또는 기타 계약에 따라 기간을 검토한다.
15. 연결된 공급자의 장비 목록.

제 2 절 개발 프로세스



201. 일반사항

1. 개발 프로세스는 통합 제어 소프트웨어의 사양, 아키텍처 및 통합 제어 소프트웨어의 설계에 중점을 둔다.
2. 개발 프로세스는 ConOps를 이용하여 시스템 특징과 관련된 지침을 제공한다. 개발 프로세스 초기에 마무리 된 원칙 및 품질 기준에 따라 ConOps의 내용은 소프트웨어의 사양, 아키텍처 및 세부적인 설계를 위한 지침으로 사용된다. 개발 프로세스의 산출물들은 통합 제어 소프트웨어 구현의 기초가 된다.
3. 새로운 제약 사항이 식별되면, 문서화되고 소유자와 논의하여야 한다. 제약 조건의 완화는 문서화되고 ConOps는 변경 관리 (Management of Change, MOC) 절차에 따라 업데이트하여야 한다. 개발 단계의 문서들은 ConOps를 바탕으로 검토되고 소유자의 승인에 따라 검증 인수 문서가 된다.

202. 활동

개발 프로세스에서는 시스템 레벨 설명 및 설계에서 소프트웨어 레벨 사양, 아키텍처 및 설계로 옮겨가게 된다. 이 프로세스에서 프로그래머(coder)는 모델링 관계를 정리하여, 소프트웨어 코드화 준비를 두 가지 문서를 통해서 마친다. 개발 프로세스의 활동은 IEEE 12207-1-2008 Second Edition, 2008-02-01, IEEE 시스템 및 소프트웨어 엔지니어링 - 소프트웨어 생명주기 프로세스를 참조하여 개발되었으며 다음과 같다.

No.	활동
소유자	
1	변경관리에 따라 ConOps 업데이트. SRS 및 SDS와 함께 우리선급에 제공
2	SRS 및 SDS 검토 및 승인
3	FMECA에 참석
4	추가된 기능 또는 공급업체의 패키지에 대한 안전성 검토
5	구현단계로 진행하기 위한 권한부여
사용자	
1	SRS 및 SDS 검토
2	소유자 및 SI 활동 지원
시스템 통합 조직	
1	시스템 통합 조직 팀원 할당
2	개발된 경우, 기본적인 통합 모델을 업데이트, 공급업체에게 전달
3	SRS에서 기능의 개선 및 상세화
4	SDS에서 기능의 개선 및 상세화
5	ConOps로부터 운영상 및 비운영상에 대한 V&V 시나리오 추가
6	내부 기능은 ConOps 및 안전 검토를 통해 추적 가능
7	공급업체의 패키지에 대한 V&V 계획 및/또는 V&V 보고서
8	소프트웨어 제어 시스템 FMECA 회의 참석
9	소프트웨어 제어 시스템 FMECA 보고서 제공
10	기능적인 FMECA 및 검토로부터 의견에 따라 SRS 및 SDS 업데이트 및 승인
11	공급업체의 패키지 문서화
12	표준 보고서와의 차이
13	SRS 발행
14	SDS 발행
15	통합 SRS 및 SDS 검토 보고서 제공
공급자	
1	SI 활동 지원
2	이전에 제공되지 않은 경우, 현재 ISO 9001 인증서 제공
3	소프트웨어 FMECA 회의 참석
품질관리자	
1	V&V 계획 초안

203. 소프트웨어 요구사항 분석

1. 이해관계자의 요구사항은 희망하는 서비스에 대한 요구사항 중심의 이해관계자 표현을, 그러한 서비스를 제공할 제품에 대한 기술적 표현으로 변환하기 위해 분석을 수행한다. 이 프로세스는 제약사항의 허용 범위 내에서 이해관계자의 요구사항을 만족시키는 통합 소프트웨어에 대한 표현(representation)을 구축하며, 어떤 특정 구현 방법을 암시하지 않는다. 그 결과는 시스템이 이해관계자 요구사항을 만족하려면 어떤 특성을 얼마나 보유해야 하는지 개발자의 관점에서 명시한, 측정 가능한 시스템 요구사항이 설정된다.
2. 소프트웨어 요구사항 분석 과정에서 기능들은 소프트웨어 모듈로 분리된다. 소프트웨어 모듈의 사양은 기능적 성능(functional capability) 및 기능수행 세부사항을 포함한다. 그 밖에 다음의 사항들을 고려하여야 한다.
   (1) 소프트웨어 모듈 외부의 인터페이스

(2) 자격 요건
(3) 안전 및 환경 사양
(4) 운영 및 유지 보수
(5) 보안 요건
(6) 인적 요소 (인간 공학)
(7) 사용자 문서화

204. 소프트웨어 아키텍처 설계

1. 아키텍처 설계의 목적은 다음에 따라 통합 소프트웨어 요구사항을 만족하는 해결방안을 찾는데 있다.
(1) 해결방안의 영역을 분할하고 정의하되 일련의 관리가 가능하고, 개념적이며, 궁극적으로 실현 가능한 규모의 분리된 문제의 집합체로 표현한다.
(2) 시스템의 기술적 요구사항 및 상업적 요구사항과 그 위험 즉, 요구사항 전체와 일관된 상세 수준에서 하나 이상의 구현전략을 식별하고 탐색한다.
(3) 이로부터 아키텍처 설계 해결방안을 정의하는데, 시스템을 구성할 일련의 시스템 요소에 관한 요구사항의 형태로 표현한다.
(4) 수행 결과로 규정된 설계 요구사항은 구현된 시스템을 검증할 근거가 되며, 조립 및 검증 전략을 구상하기 위한 기초가 된다.
2. 소프트웨어 아키텍처 설계 활동 중에 시스템 통합 조직은 다음의 활동을 수행하여야 한다.
(1) 소프트웨어 요구사항을 각 소프트웨어 모듈에 대해 소프트웨어 구성요소를 식별하는 최상위 아키텍처로 변환
(2) SRS의 각 요건을 하나 이상의 소프트웨어 모듈에 할당
(3) 추적성 매트릭스에 요구사항 및 소프트웨어 모듈을 문서화
(4) 소프트웨어 모듈의 아키텍처를 문서화
(5) 개발
(가) 최상위 외부 인터페이스 설계
(나) 모든 데이터베이스를 위한 최상위 설계
(다) 사용자 문서의 초안 작성
(라) 사전 시험 요건
3. 소프트웨어 아키텍처 설계는 IEEE 12207 표준에서 권장하는 기준을 따르는 것을 권장한다.
(1) 소프트웨어 항목 요구사항에 대한 추적성
(2) 소프트웨어 항목 요구사항과의 외부적 일관성
(3) 소프트웨어 구성품 간의 내부적 일관성
(4) 사용된 설계 방법과 표준의 적절성
(5) 상세설계의 실현 가능성
(6) 운영 및 유지보수의 실현 가능성

205. 리스크 관리 (Risk Management)

개발 프로세스에서는 위험성, 프로젝트 및 운영에서 두 가지 주요 측면이 있다.

1. 프로젝트 위험 관리
일정, 역량 및 소프트웨어 품질과 관련된 잠재적 문제를 프로젝트 관리자에게 안내하기 위해 개발 단계에서는 매트릭스를 수집, 측정 및 관리하는 것을 권장한다. 지표의 자료들은 소프트웨어 품질을 관리하기 위해 시스템 통합 조직이 내부적으로 이용한다.
2. 운영 위험 관리
운영상의 위험은 안전성 검토, 고장 모드 영향 및 중요성 분석(FMECA) 및 기타 검토를 통해 식별한다. 신기술은 개발 단계에서 식별되어 나타날 수 있다.
3. 공급자 패키지 문서
공급자의 패키지 문서는 전체적인 계획을 고려하여야 한다.
4. 소프트웨어 제어 시스템 FMECA
FMECA은 단일 소프트웨어 모듈의 고장으로 인해 다른 소프트웨어 모듈의 고장 또는 제어 시스템의 손실이 발생하지 않도록 하는 것을 목적으로 한다.

(1) ISPM 제어 시스템에 IL2 및 IL3이 할당된 경우에는 소프트웨어 중심의 기능적인 FMECA를 하여야 한다.
(2) 제어 시스템 FMECA는 추적성 매트릭스의 관련 기능에 소프트웨어 모듈의 추적성을 제공하여야 한다.
(3) IL2 및 IL3의 제어 시스템 FMECA는 그 기능에 영향을 미칠 수 있는 통합 제어 시스템과의 인터페이스를 포함하여 수행하여야 한다.
(4) FMECA 권고 사항에 따라 SRS 및 SDS를 업데이트하여야 한다.

5. 새롭거나 입증되지 않은 기술

새롭거나 입증되지 않은 기술은 추가적인 위험성을 수반한다. 신기술은 하드웨어, 기계 장비, 인터페이스 프로토콜 또는 소프트웨어 모듈 코딩 일 수 있다.

6. 개발 단계에 추가된 새로운 기능

(1) 소유자는 ConOps를 업데이트하여야 한다.
(2) 새로운 기능에 대한 안전성 검토를 하고, 그 결과는 문서화하여야 한다.
(3) 소프트웨어 제어 시스템 FMECA 후에 기능이 추가된 경우, 새로운 기능 및 관련 소프트웨어 모듈로 인한 모든 위험성을 해소하기 위해 FMECA를 수행하여야 한다.

206. 소프트웨어 요구사항 명세서(SRS) 및 소프트웨어 설계 명세서(SDS)

1. 소프트웨어 요구사항 명세서(Software Requirement Specification 이하 SRS)

ISPM SRS는 정해진 환경에서 정의된 기능을 수행할 수 있도록 특정 소프트웨어 제품, 프로그램 또는 프로그램 집합의 통합을 위한 명세서이다. SRS는 소유자, 사용자 조직 및 우리선급에 의해 검토되어야 한다. 계약 당사자와의 계약 또는 기타 계약에 따라 기간을 검토한다. SI는 SRS에 SI의 소프트웨어 기능 소유 정보 또는 지적 재산권의 포함여부에 관한 재량권을 가진다. SI는 기술적인 용어에서 기능을 설명하여야 한다.

(가) 기능성 : 최상위 용어에서 제어 시스템과 소프트웨어의 목적
(나) 외부 인터페이스 : 소프트웨어에서 사용자와의 상호작용 (사용자 인터페이스), 시스템 실행 하드웨어, 외부 인터페이스 시스템 지원 하드웨어 및 외부 인터페이스 시스템 지원 소프트웨어
(다) 성능 : 응용 프로그램, 복구 또는 재부팅 시간이 충분히 빠른 경우 제어 시스템의 가용성, 탐색 속도
(라) 속성 : 코드의 재사용성, 유지 보수성, 보안성 등을 고려
(마) 설계 제약 사항 : 이 구현 단계에 부과 된 제약 사항
(바) 기타 : 소프트웨어 구현, 실행 하드웨어, 구현에 사용 된 소프트웨어 언어, 데이터베이스 무결성 정책, 리소스 제한, 운영 환경 등에 적용되는 표준

2. 소프트웨어 설계 명세서(Software Design Specification 이하 SDS)

ISPM 통합 SDS는 시스템의 통합 구성 요소 설계를 설명한다. 일반적인 내용으로 시스템 또는 구성 요소 아키텍처, 제어 논리, 데이터 구조, 입출력 형식, 인터페이스 설명 및 알고리즘이 포함된다. SDS는 소유자, 사용자 및 우리선급에 의해 검토되어야 한다. 계약 당사자와의 계약 또는 기타 계약에 따라 기간을 검토한다. SI는 SDS에 SI의 소프트웨어 기능적인 소유 정보 또는 지적 재산권의 포함여부에 관한 재량권을 가진다. SI는 기능을 자세히 설명하여야 한다.

(1) 통합 소프트웨어 상세 설계 프로세스

소프트웨어 상세 설계는 개발 단계에서 소프트웨어 요구사항 분석을 시작으로 구현 단계의 전체에 걸쳐서 수행한다. 소프트웨어 통합 상세 설계는 소프트웨어 모듈의 소프트웨어 구성 요소 통합이 코딩 될 단위 통합 소프트웨어로 구성된 하위 수준으로 다듬는 활동이다. SDS는 개발 단계에서 작성되어, SI 개발자들(코드 작성자)이 소프트웨어가 수행해야 할 작업의 정확한 특성을 명확하게 이해할 수 있도록 한다.

(2) 소프트웨어의 세부 설계 및 시험 요건은 IEEE 12207 표준에서 권장하는 다음 기준을 사용하여 평가하여야 한다.

(가) 소프트웨어 항목의 요건에 대한 추적성
(나) 아키텍처 설계와의 외부 일관성
(다) 소프트웨어 구성 요소 (모듈, 프로그램) 간의 내부 일관성
(라) 사용된 설계방법 및 표준의 적합성
(마) 타당성 테스트
(바) 운영 및 유지 보수의 타당성

207. 산출물

1. 소프트웨어 요구사항 명세서 (SRS)

SRS는 206.의 1항의 사항을 고려하여 적어도 다음을 포함하여야 한다.

(1) 소프트웨어 요구사항 분석 활동의 결과
(2) 작업 프로세스 흐름 다이어그램
(3) 기준 및 표준
(4) 관련 기능을 가진 소프트웨어 모듈은 필요한 기능을 구성하는 하위 소프트웨어 모듈로 재구성
(5) 사전 시험 요건
(6) 기능 시험 요건
(7) 최상위 외부 인터페이스 사양
(8) 기능은 ConOps에서 추적 가능하여야 한다.

2. 소프트웨어 설계 명세서 (SDS)

SDS는 206.의 2항의 사항을 고려하여 적어도 다음을 포함하여야 한다.
(1) 모든 데이터베이스의 최상위 설계
(2) 내부 및 외부 인터페이스 설계
(3) 사용자 문서의 사전 설계
(4) 소프트웨어 아키텍처 설계 평가
(5) 소프트웨어 설계 제약사항
(6) 기능은 ConOps에서 추적 가능하여야 한다.

3. 품질관리자가 수립한 개발 초기 V & V 계획

4. 표준 보고서의 변화(변화가 발생할 경우)

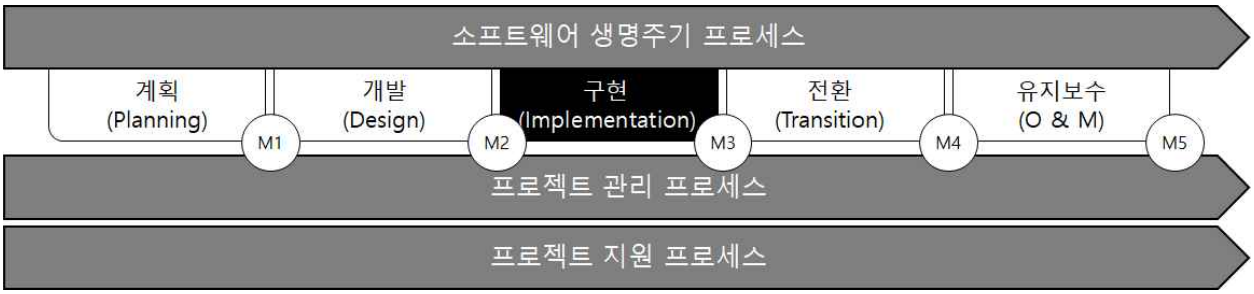
208. 문서 유지보수

SRS 및 SDS는 소유자, 사용자 조직 및 우리선급에 의해 ConOps와의 일관성에 대해 검토하여야 한다. 계약 당사자와의 계약 또는 기타 계약에 따라 기간을 검토한다.
(1) SI는 제어 시스템 FMECA의 검토 의견에 따라 SRS 및 SDS를 업데이트 하여야 한다.

209. 개발 프로세스 마일스톤 M2

일부 개발 프로세스 활동은 구현 단계로 확장된다.
1. 통합 시스템 구성 요소 간의 인터페이스 또는 통합을 명확하게 정의하여야 한다.
2. 기능 구성 요소에 대한 자세한 설명을 완료하여야 한다.
3. SRS 및 SDS가 ConOps 문서와 일관성 있게 완료하여야 한다.
4. 계획 범위에 따라 무결성 수준을 정렬하여야 한다.
5. 소프트웨어 및 전체 프로젝트 일정을 업데이트 하여야 한다.
6. 소유자로부터 구현 단계로 진행하기 위한 권한
7. 표준 보고서의 변동
8. SDS 및 SRS 발행 (구현 단계를 위해 발행)

제 3 절 구현 프로세스



301. 일반사항

1. 구현 프로세스는 SRS와 SDS를 통해서 규정된 통합 소프트웨어를 현실화하고, 아키텍처 설계와 일치하도록 소프트웨어 요소를 조립하는 것을 목적으로 한다. 이 프로세스를 통해 SRS 및 SDS의 모든 기능이 통합 소프트웨어에서 만족스럽게 동작하고, 계획 프로세스에서 구상한 운용 환경에서 사용 목적을 달성하는지 객관적으로 입증한다.
2. 구현 프로세스는 구현된 통합 소프트웨어가 정의된 요구사항에 불만족 할 경우, 교정 작업을 하는데 필요한 정보를 제공하고, 이해관계자의 요구사항과 비교하여 교정 활동을 수행한다. 교정이 완료된 통합 소프트웨어는 이해관계자가 확인한다.

302. 활동

구현 프로세스에서는 SRS 및 SDS 세분화, 소프트웨어 모듈 코딩, COTS 제품 구성의 통합을 통해 통합 소프트웨어를 구현하고, 확인 및 검증 계획을 수립하여 단위 테스트, 통합 테스트 및 소프트웨어 시스템 수준 수락 테스트를 수행한다. 구현 프로세스의 활동은 ISO/IEC/IEEE 12207 First Edition, 2017-11, 「시스템 및 소프트웨어 엔지니어링 - 소프트웨어 생명주기 프로세스」와 ISO/IEC/IEEE 15288 First edition 2015-05-15, 「시스템 및 소프트웨어 엔지니어링 - 소프트웨어 생명주기 프로세스」를 참조하여 개발되었으며 다음과 같다.

No.	활동
소유자	
1	변경관리 정책에 대한 변경 요청관리
2	추적성 위험
3	계획에 대한 프로젝트 진행 모니터링
4	시스템 통합 조직 활동 지원
5	시스템 통합 조직의 전체적인 시험 결과 검토
6	SRS 및 SDS에 대하여 업데이트 검토 및 승인
7	SRS 및 SDS에서 업데이트에 대한 ConOps 검토
8	프로그래밍이 90% 완성되면 ConOps 재발행
9	V&V 계획 검토
10	소유자의 V&V 검증 활동 참석 권고.
11	IL2가 할당된 기능에서 보통 결함이 발견되면 제안 된 해결 방법에 대해 안전 검토를 수행해야 한다. IL3가 할당된 기능에는 해결 방법이 허용되지 않는다.
12	결함 등급 검토
13	V & V 보고서 검토
14	V & V 계획 검토 및 승인

No.	활동
사용자	
1	변경관리에 대한 변경 요구사항 관리
2	SI 활동 지원
3	전체적인 시험 결과의 검토
4	ConOps에 대해 업데이트 검토
5	SRS 및 SDS에 대해 업데이트 검토
6	V&V 계획 검토
7	사용자의 V & V 활동 참석 권고
8	V&V 계획
9	V&V 보고서
10	V&V 조직에 의해 결함 등급에 대한 정보 제공
시스템 통합 조직	
1	이해관계자, 공급업체 및 하도급 업체 사이에 문제에 대한 모니터링.
2	하도급 업체에게 계약서 발행
3	하도급 업체 모니터링
4	코딩의 동료 검토
5	개발 활동의 관리
6	변경관리(요구사항 변경) 검토 및 착수
7	검토에 대한 통합 시험 결과 제공
8	보고서 완료 예상
9	공개된 문제를 지적하여 제공 가능한 요약보고서
10	업데이트된 또는 현재의 SRS 및 SDS 제공
11	소유자가 요청한 일정 업데이트 발행
12	V&V 계획 검토
13	표준과의 불일치 보고서
14	V&V 검증 활동의 참석
15	검증 시험을 통과한 후 소프트웨어의 잠김 상태 전환
16	IL2가 할당된 기능에서 보통 결함이 발견되면 제안 된 해결 방법에 대해 안전 검토를 수행해야 한다. IL3가 할당된 기능에는 해결 방법이 허용되지 않는다.
17	코딩 결함 수정
18	V&V 조직의 결함 순위를 정하기 위한 정보 제공
공급자	
1	변경관리(요구사항 변경) 검토 및 착수
2	계약된 패키지 장비 및 관련 소프트웨어 개발 및 인도
3	요구된 문서 개발 및 제공
4	예외적인 사항 식별을 지원하기 위해 요청된 정보 제공

No.	활동
품질관리자	
1	승인된 SRS 및 SDS 변경사항 모니터링 및 포함
2	V&V 계획
3	검토 중/검토 후에 V&V 계획 발행, 구현 동안 발행
4	계획에 대한 V&V 형상관리를 모니터링 하는 V&V의 프로젝트 관리
5	시뮬레이션 소프트웨어 개발
6	시뮬레이터 소프트웨어 또는 형상관리 동료검토
7	모든 V&V 계획 의견으로부터 통합 보고서 생성
8	시뮬레이션 검증
9	시뮬레이션 형상관리 동등검토. 동등검토 이후에
10	의견에 대한 V&V 계획 제공 및 승인된 V&V 계획 제공
11	V&V 계획 실행
12	V&V 계획으로부터 편차 유의
13	발견 된 모든 예외사항에 대한 V&V 보고서를 작성하고 다른 검토자의 의견 통합.
14	바이러스 스캔의 결과
15	시뮬레이터는 필요에 따라 통합 시스템, 신호, 소프트웨어 인터록 및 알람에 연결된 구성요소 데이터(모니터링 및 제어) 명령들을 포함해야 한다.
16	중간 V&V 보고서 생성
17	IL2가 할당된 기능에 대해 제안된 보통결함 해결방법의 안전 검토 지원
18	결함 순위
선급	
1	V&V 계획 검토
2	지침 준수에 대한 통합 조직 및 하도급업체 모니터링
3	독립적인 설계 검토 수행
4	ConOps, SRS 및 SDS 검토
5	V&V 계획 검토
6	V&V 계획을 실행 시 V&V 조직을 모니터링
7	중간 V&V 보고서 검토
8	최종 V&V 보고서 검토
9	바이러스 스캔의 결과 검토
10	결함 순위에 대한 정보 제공
11	확인 입증

1. 시스템 통합 조직은 구현단계에서 다음에 따라 관리한다.
   (1) 소유자는 코드를 작성하기 전에 SRS, SDS에서 식별된 오류 또는 설명을 수정, 검토 및 승인하여야 한다.
   (2) SI는 SI가 개발한 모든 소프트웨어 모듈이 검토되고 단위 테스트를 거쳤음을 증명하는 문서를 제공하여야 한다.
   (3) 통합 소프트웨어의 단위 모듈이 검토되고 나면 형상 관리 하에 배치되고 베이스라인 프로젝트에 통합하여야 한다.
   (4) 모든 개별 소프트웨어 모듈이 성공적으로 통합된 후, 소프트웨어가 SRS 및 SDS의 요건을 충족하는지 확인하기 위해 종합적인 소프트웨어 시스템 레벨의 SI 통합 테스트를 하여야 한다.
   (5) 소유자 및/또는 사용자는 시스템 통합 조직 및/또는 계약자의 소프트웨어 개발 활동에 대하여 주기적으로 검토하여야 한다. 검토 결과에 대하여 우리선급에 이를 통보 하여야 한다.

303. 소프트웨어 코딩 및 시험

이 활동은 사용자 맞춤형 소프트웨어 모듈의 개발 및 라이브러리 모듈 사용, COTS 제품 통합 및 인터페이스로 구성된다. SI는 모델, 다이어그램 및 기능 사양, SRS 및 SDS를 사용하여 소프트웨어 아키텍처를 완성한다. 프로그래머는 SRS, SDS를 바탕으로 사양 내용의 소프트웨어 모듈 코드로 만들고 소프트웨어 개발 순서를 설정한다. 그리고 개별 소프트웨어 모듈의 내부 테스팅이 수행된다,

1. IL2 및 IL3이 할당된 기능에 관여하지 않는 SI의 프로그래머는 통합 소프트웨어 모듈 코드의 동료 평가(Peer review)를 하여야 한다. 동료 평가자는 표준 방법을 사용하여, 다음 사항에 대하여 통합 소프트웨어 모듈을 평가하여야 한다.
   (1) 정확성(Correctness) : SRS, SDS에 있는 기능이 정확하게 동작 한다.
   (2) 완전성(Complete) : 누락된 기능이 없다.
   (3) 명료성(Coherent) : 논리는 명확하고 불필요하게 복잡하지 않다.
   (4) 유지보수성(Maintainability) : 소스 코드 로직은 읽기 쉽고 주석이 작성 된다. COTS 구성의 경우 통합, 레지스터 및 구성에 대한 명확한 정보를 기록하여야 한다.
   (5) 효율성(Efficient) : 수용 할 수 없는 성능 지연 현상(performance bottleneck)이 없어야 한다.
2. SI는 최종 세부 설계, 코딩 및 단위/데이터베이스 테스트 중에 다음 사항을 고려하여 평가 결과를 문서화하는 것을 권고한다.
   (1) 소프트웨어 항목의 요건 및 설계에 대한 추적성
   (2) 소프트웨어 항목의 요건 및 설계에 대한 일관성
   (3) 단위 요구 사항 간의 일관성, 표준 통합 모델
   (4) 단위 테스트 범위
   (5) 소프트웨어 통합 및 테스트의 타당성
   (6) 운영 및 유지 보수의 타당성

304. 소프트웨어 통합

이 활동은 달성해야 할 통합 테스트의 레벨을 자세히 설명하는 통합 계획을 개발 한다. 테스트 계획은 개발 된 코드가 이전 단계에서 개발 된 요건, 아키텍처 및 사양의 준수여부를 확인하는 것을 목적으로 한다. 통합 계획은 V & V 계획의 한 부분이다.

1. 통합 계획은 시험 요건, 절차, 데이터, 책임 및 일정을 포함할 것을 권고한다.
2. 각 요구사항은 일련의 시험 종류, 시험 사례 및 시험 절차에 의해 통합 시험을 진행하여야 한다.
3. 각 시험 사례는 문서화 하여야 하고, SRS, SDS의 요구사항에서 추적 할 수 있어야 한다.
4. 다음의 기준에 따라 SI는 통합 계획, 시험 결과 및 사용자 문서를 평가하여야 한다.
   (1) 시스템 요건에 대한 추적성
   (2) 시스템 요건의 일관성
   (3) 단위 요건 간의 일관성
   (4) 소프트웨어 항목의 요건에 대한 테스트 적용 범위
   (5) 사용된 시험 표준 및 방법의 적합성
   (6) 예상 결과에 대한 적합성
   (7) 소프트웨어 자격 테스트의 타당성
   (8) 운영 및 유지 보수의 타당성

305. 소프트웨어 통합 테스트

SI는 동료 평가나 다른 방법을 통해 SRS, SDS 요구사항(기능 및 통합 요건)에 대해 내부적으로 모든 소프트웨어 모듈을 시험하여야 하며, 소프트웨어 모듈이 베이스 라인에 통합할 때마다 소프트웨어의 나머지 부분과 올바르게 상호 작용하는지 확인하기 위해 통합 테스트를 수행하는 것이 좋다.

1. 다음 기준을 사용하여 소프트웨어의 상세 설계 및 시험 요건을 평가하는 것이 좋다.
   (1) 소프트웨어 항목 요건의 테스트 범위
   (2) 예상 결과에 대한 적합성
   (3) 소프트웨어 인수 시험의 타당성
   (4) 운영 및 유지 보수의 타당성

306. 문서 유지보수

ConOps, SRS 및 SDS의 업데이트 사항은 소유자, 사용자 조직 및 우리선급에서 검토하여야 한다. ConOps 는 소유자의 승인을 받아야 한다. 종합적인 시험 결과는 소유자, 사용자이 검토하여야 한다. 계약 당사자와의 계약 또는 기타 계약에 따라 기간을 검토한다.

307. V & V 계획

V & V 계획은 현재 SRS 및 SDS의 V & V 요건을 따른다.

1. V & V 계획 설명

V & V 계획은 소프트웨어 V & V 노력의 목적, 목표 및 범위를 설명한다. 계획은 현재의 SRS 및 SDS에 열거 된 요건을 따르는 것이다.

(1) 표준, 관례 및 협약을 만족시킨다.
(2) 시나리오는 현재 SRS 및 SDS에 추적 가능해야한다.
(3) V & V 계획에는 소프트웨어가 소프트웨어 시스템 요구 사항을 충족한다는 증거를 수집하는 프로세스가 포함되어야한다.
(4) 현재 SRS 및 SDS에 열거된 요건의 의도를 쉽게 이해하기 위해 ConOps를 검토하는 것이 좋다.
(5) V & V 계획은 시험 활동의 범위, 접근 방식, 자원 및 일정을 지정하는 문서이다.
(6) 시험 설계는 소프트웨어 모듈에 대한 시험 방법의 세부 사항을 규정한 문서이다.
(7) V & V 계획은 테스트 실행을 위한 일련의 작업을 지정하는 문서이다.
(8) 결과를 문서화하고 V & V 보고서를 작성하여야 한다.

2. V & V 계획 승인

소유자, 사용자 및 SI 조직과 우리선급은 V & V 계획을 검토해야한다. 소유자와 우리선급은 검토자의 의견을 수렴하여 V & V 계획을 승인하여야 한다. 계약 당사자와의 계약 또는 기타 계약에 따라 기간을 검토한다.

308. V & V 방법

1. 소프트웨어의 주요 확인 방법은 다음과 같다.
   (1) 페루프 검증 (특별히 고려된 경우)
   (2) 소프트웨어 인 더 루프 검증
   (3) 하드웨어 인 더 루프 검증
2. V & V 단계의 최소 목표는 SRS 및 SDS에 명시된 대로 소프트웨어 성능을 확인하는 것이다. 시뮬레이션은 제어 시스템 소프트웨어를 테스트하기에 충분한 정확도를 가져야한다.
3. 시뮬레이션은 필요한 경우 통합 된 시스템의 코드를 확인하고 SRS 및 SDS에 명시된 대로 이해 관계자에게 제어 시스템 소프트웨어를 명확하게 보여주기 위해 연결된 구성 요소의 데이터 (모니터링 및 제어), 통합 시스템과의 명령, 신호, 소프트웨어 인터록 및 경보를 포함한다. 의도는 통합된 제어 시스템을 확인하는 것이고, 연결된 구성요소의 소프트웨어는 확인할 필요가 없다.

4. 페루프 검증

컴퓨터 기반 통합 시스템의 입력 및 출력은 다른 통합 구성 요소의 최소 상호 작용과 함께 시뮬레이션 된다. 페루프 확인은 통합 시스템 소프트웨어 응답을 평가하기 위해 프로그램의 레지스터 값을 변경해야 할 수 있다. 소프트웨어 코드와 그 기능에 대한 포괄적인 이해가 요구되며 이는 어플리케이션을 단순한 시스템으로 제한한다. 페루프 검증을 수행하기 전에 우리선급의 특별 고려 사항 및 사전 승인이 필요하다. SI, 소유자 및 사용자는 이러한 폐쇄 루프 검증 요구 사항이 충족되었다는 문서를 제공해야 한다.

(1) 페루프 검증 방법의 요건 :
   (가) 단순 통합 또는 독립형 컴퓨터 기반 시스템.
   (나) 3개 이하의 통합 구성 요소
   (다) 소수의 복잡한 기능과 관련된 복잡한 소프트웨어 모듈.
   (라) 통합 시스템이 필수 또는 안전 기능을 제어하지 않는다. 필수 또는 안전 기능이 시스템에서 모니터링 되고 이 데이터가 사람의 의사 결정에 사용되는 경우 페루프 테스트는 적절하지 않을 수 있다.
   (마) IL1 기능은 안전 또는 환경 영향을 초래하지 않는다.

(바) 시스템에 IL2 또는 IL3 기능이 없다.

5. 소프트웨어 인 더 루프 검증

제어 시스템 소프트웨어가 비 고유시스템용 컴퓨터에서 실행되고 시뮬레이션이 동일하거나 별도의 컴퓨터에서 실행되고 있다. 충분한 정확도를 가져야하며 실제 시스템을 포함하여 필요한 범위 내에서 통합 시스템의 코드를 확인하고 자극 결과를 문서화해야한다. 시뮬레이션의 정확도는 현재 SRS 및 SDS에 대한 제어 시스템 소프트웨어의 확인을 허용하기에 충분해야한다.

6. 하드웨어 인 더 루프 검증

(1) 통합 시스템의 프로그램은 사용 가능한 구성 요소 및 시뮬레이션 컴퓨터와 제어 시스템의 메인보드와의 통신을 위해 인터페이스 카드가 있는 네이티브 하드웨어 (CPU)에서 실행된다.

(2) 시뮬레이터는 제어 시스템의 인터페이스 카드에 연결된 별도의 컴퓨터 하드웨어에서 실행된다.

(3) 시뮬레이터는 통합 시스템의 구성 요소를 에뮬레이팅하는 것을 지원한다.

(4) 시뮬레이션은 충분한 정확도를 가져야하며 실제 시스템을 포함하여 필요한 범위 내에서 통합 시스템의 코드를 확인하고 자극 결과를 문서화하여야 한다.

(5) 시뮬레이션의 정확도는 현재 SRS 및 SDS에 대한 제어 시스템 소프트웨어의 확인을 허용하기에 충분하여야 한다.

309. 바이러스 및 기타 악성 소프트웨어에 대한 검사

V & V 조직은 모든 V & V 활동을 수행하기 전에 제어 시스템 소프트웨어에서 바이러스 검사를 실행하는 것이고 소유자, 사용자, SI 및 우리선급에게 스캔 결과를 보고하여야 한다.

1. V & V 조직은 바이러스 검사 프로그램에서 사용할 수 있는 최신 바이러스 정의를 사용하고 있다고 명시하여야 한다.
2. 바이러스 검사 보고서에 바이러스 정의 번호 또는 식별자를 제공한다.
3. SI는 SI의 컴파일된 소프트웨어가 잠재적인 악성으로서 바이러스 스캐닝 프로그램에 의해 탐지된 스크립트를 포함하는 경우 명시하여야 한다.
   (1) SI는 스크립트가 탐지된 악성 소프트웨어의 이름 또는 유형 (스파이웨어, 트로이 목마 등) 및 여러 보고된 사례를 제공한다. 이것은 유지보수 단계에서 잠재적으로 다른 악성 소프트웨어의 식별을 가능하게 한다.
4. SI, 공급업체 또는 하위 공급업체가 제어 시스템에 바이러스 백신 소프트웨어를 제공하는 경우 소유자 보안 계획과의 충돌은 소유자와 SI, 공급업체 또는 하위 공급업체 간에 해결되어야 한다.
   (1) 안티 바이러스 소프트웨어가 제어 시스템에 설치되어있는 경우 SI, 공급업체 또는 하위 공급업체는 바이러스 정의가 선내 어떻게 그리고 언제 업데이트되는지에 대한 세부사항을 제공하는 것을 권고한다.

310. 구현 프로세스의 V & V

1. V & V 조직은 구현 단계에서 다음 활동을 수행하는 것이다.

(1) V & V 조직은 V & V 계획을 상세화해야 한다. 상세화된 V & V 계획은 소유자, 사용자, SI가 검토를 한다. 검토가 완료된 V & V 계획 보고서는 우리선급에 제출하여야 한다.

(2) V & V 조직은 V & V 계획을 동료 평가한다.

(3) V & V 조직은 구현 단계에서 시뮬레이터를 구성하여야 한다.

(4) 시뮬레이터를 프로그램 한다.

(5) 시뮬레이터 프로그램을 검증한다.

311. 시뮬레이션의 V&V 검토

1. 시뮬레이터는 SRS 및 SDS에 명시된 대로 통합 시스템의 코드를 확인하고 이해 관계자에게 제어 시스템 소프트웨어를 명확하게 보여주기 위해 필요한 경우 통합 시스템, 신호, 소프트웨어 인터록 및 경보와 연결된 구성 요소 데이터 (모니터링 및 제어) 명령을 포함한다.
2. 시뮬레이션은 충분한 정확도를 가져야하며 실제 동적 시스템과 효과를 합리적으로 포함시켜 통합 시스템의 코드를 확인해야 하고 V & V 조직은 확인 결과를 문서화한다.
3. 합리적인 것은 제어 시스템 소프트웨어 기능과 프로그래밍을 테스트할 수 있는 충분한 정확도를 제공하는 동시에 소프트웨어가 SRS 및 SDS에 따라 작동하고 있다는 충분한 피드백을 V&V 조직에 제공하는 것으로 정의된다.
4. 타당성은 SI의 입력과 함께 V&V 조직에 의해 결정된다.
5. 시뮬레이션의 V & V 동등평가

확인 전에 시뮬레이션 구성은 V & V 조직에 의해 다음 사항에 대한 동등 평가를 거쳐야 한다.

(1) 현재 추적성 매트릭스를 사용하여 요건에 대한 추적성.
(2) 시뮬레이션의 타당성
(3) 선박 건조업체, 소유자 및 우리선급에게 보고서를 제공해야 한다.

312. 결함

SI는 V&V, 소유자 조직으로부터의 정보를 바탕으로 결점이 제어 시스템 코드 결함, 시뮬레이션 코드 결함 또는 계획 오류 인지 여부를 결정해야 한다.

1. 무결성 레벨 및 결함 카테고리

표2는 결함 또는 오류 수정에 대한 요건과 권장 사항이 포함되어 있다.

313. 확인 및 검증 보고서 (V & V 보고서)

1. 보고서는 현재 SRS 및 SDS에 설명된 각 기능의 합격 또는 불합격에 대한 추적 가능한 부기부호를 사용하여 V & V 조직에 의해 생성된다. 이 보고서에는 다음 내용이 포함된다.
(1) 소프트웨어 모듈에서 발견된 이상.
(2) 결함, 오류 또는 이상의 원인(알려진 경우)
(3) 결함, 오류 또는 이상이 기능에 미치는 영향 및 다른 기능에 영향을 미친 경우.
(4) 시뮬레이션 설계, 시뮬레이션 시나리오, 시뮬레이션 절차 및 시뮬레이션 결과.
(5) V & V 계획과의 차이. 함수 식별자를 포함 시키려면 편차가 있는 위치와 편차가 있는 이유.
(6) 권장 사항

314. V & V 보고서의 검토

소유자와 사용자는 어떤 개념 에러를 식별하기 위해 V&V 보고서를 검토하고 그들을 해결한다. SI는 코딩 결함을 수정하고 우리선급은 V&V 보고서를 검토한다. 계약 당사자와의 계약 또는 기타 계약에 따라 기간을 검토한다.

315. 산출물

1. 구현 프로세스의 산출물은 세부 코드 사양 및 IL2 및 IL3이 할당된 기능에 대한 단위 시험 결과, 통합 계획 및 전반적인 통합 소프트웨어 시험 결과를 포함한다. 단, 이 때 실제 코드를 문서에 포함할 필요는 없다.
2. 적어도 구현 프로세스는 아래의 산출물을 가져야 한다.
(1) 시험 계획의 결과에 대한 통합 보고서. IL2 및 IL3 결과를 포함
(2) 완성된 통합 소프트웨어 모듈 코드
(3) 검증 조직에 의한 V & V 업데이트된 계획
(4) 업데이트된 ConOps 발행
(5)업데이트된 SRS 및 SDS 발행
(6) 통합된 V & V 보고서 요약
(7) 시뮬레이션 동료 평가 보고서

316. 위험성 관리

1. 위험 관리는 프로젝트 및 운영상의 위험성을 포함한다.
(1)프로젝트 위험성 관리
매트릭스를 수집하는 것을 권고한다.
(2) 운영상 위험성 관리
운영상의 위험성은 안전성 검토, FMECA 및 프로세스 초기에 수행된 검토사항을 다룬다. 신기술이 구현 단계에서 식별되어 나타날 수 있다.
(3) 소프트웨어 제어 시스템 FMECA
(가) 제어 시스템 FMECA는 추적성 매트릭스의 관련 기능에 소프트웨어 모듈의 추적성을 제공하여야 한다.
(나) 제어 시스템 FMECA은 는 구현 단계에서 변경된 기능에 대해 통합 시스템에서 전체적으로 수행하여야 한다.
(다) IL2 및 IL3의 제어 시스템 FMECA는 그 기능에 영향을 미칠 수 있는 통합 제어 시스템과의 인터페이스

를 포함하여 수행하여야 한다.

(4) 새롭거나 입증되지 않은 기술

새롭거나 입증되지 않은 기술은 추가적인 위험성을 수반한다. 신기술은 하드웨어, 기계 장비, 인터페이스 프로토콜 또는 소프트웨어 모듈 코딩 일 수 있다.

표 2 IL 레벨 및 결함 카테고리, 요건 및 권장 사항(소유자에 의해 결함 수정 요구 가능)

IL	요구사항 및 권고사항				
결함 분류	경미한 결함[1]	낮은 결함[2]	보통 결함[3]	주요 결함[4]	치명적인 결함[5]
0	D	D	D	R	R
1	D	D	D (Review)	R	R
2	R (Essential)	R (Essential)	R (Essential)	R	R
3	R (Essential)	R	R	R	R

(비고)

D : 수정 연기 가능

D (Review) : 수정 연기 가능 (소유자 및 사용자의 결과 및 리스크 검토)

R (Essential) : 필수 기능인 경우 수정 및 재시험이 필요하며, IL 결과만 비즈니스와 관련된 경우 지연될 수 있다. 필수 기능이 아닌 경우. 소유자 및 사용자의 결과 및 위험성 검토

R : 수정 및 재시험 요구

1) 경미한 결함이라 함은 주로 데이터의 표시 또는 레이아웃과 관련된 결함이다. 그러나 데이터 손상 및 잘못된 값의 위험은 없다. 시스템에서 필수 또는 안전 기능이 모니터링 되고 이 데이터가 인간의 의사 결정에 사용되는 경우 경미한 등급이 적절하지 않을 수 있다. 기능의 IL 등급에 따라 소프트웨어 모듈은 소유자 및 사용자의 허가 하에 배포될 수 있다. HMI 그래픽 색상은 외관 결함이 아닐 수 있다.

2) 낮은 결함이라 함은 낮은 수준의 기능 장애를 일으킬 수 있거나 초래 한 결함. 이러한 결함으로 인해 데이터 대기 시간이 발생할 수 있지만 필수, 안전 또는 IL2 또는 IL3 기능에는 적용되지 않는다. 장애가 발생하더라도 통합 시스템과 기능은 계속 작동한다. 일부 기능의 이러한 중단 또는 비 가용성은 IL1 기능에 대해 제한된 기간 동안 허용 될 수 있다. 작은 결함은 짧은 기간 동안 허용 할 수 있는 방식으로 일부 중요하지 않은 데이터 값의 손상을 일으킬 수 있다. IL2 또는 IL3 할당 기능에 할당 된 필수 또는 SIS 기능을 수정해야한다. 비 필수 및 비 SIS IL2 또는 IL3 할당 기능은 소유자의 옵션으로 수정해야한다. 기능이 할당된 IL0 또는 IL1은 소유자 옵션에서 수정해야한다.

3) 보통결함이라 함은 소유자 및 사용자에게 수용 가능한 해결방법이 있는 주요 결함을 말한다. 이러한 결함은 데이터 대기 시간을 초래할 수 있지만 필수 또는 IL2 또는 IL3 기능에는 적용되지 않는다. 고장이 발생하더라도 통합 시스템과 기능은 계속 작동한다. 일부 기능의 이러한 중단 또는 비 가용성은 IL1 기능에 대해 제한된 기간 동안 허용 될 수 있다. 중간 정도의 결함은 짧은 기간 동안 허용 할 수 있는 방식으로 일부 비 중요 데이터 값을 손상시킬 수 있다. 운영 매뉴얼의 변경을 보통 결함이라고 한다. 소유자는 그러한 변경의 영향과 위험을 검토해야한다. IL2 또는 IL3 할당 기능에서 보통 결함이 발견되면 통합 조직은 소유자, 사용자 및 통합 조직과 관련된 제안된 해결 방법에 대한 안전성 검토를 용이하게 하는 것입니다. 안전 검토 회의를 우리선급에 통보해야한다. 안전 검토 보고서를 IA와 우리선급에 제공해야 한다. IL0 및 IL1 기능에 대해 안전 검토를 수행하는 것이 좋다.

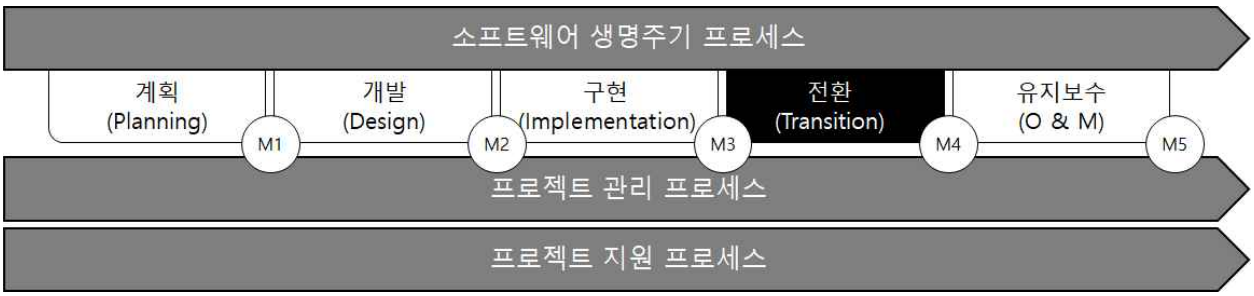
4) 주요 결함이라 함은 심각한 결함으로, 시스템을 정지 시키지는 않지만 성능을 심각하게 저하 시키거나 의도하지 않은 동작 또는 잘못된 데이터 전송을 유발한다. 모든 치명적 결함을 수정하고 제어 시스템을 다시 테스트해야 한다.

5) 치명적인 결함이라 함은 매우 심각한 결함으로, 이미 컴퓨터 기반 제어 시스템의 작동을 정지 했거나 정지시킬 수 있다. 치명적 결함은 제어되는 장비 (EUC)의 위험한 작동이 가능한 결함이다. 모든 치명적 결함을 수정하고 제어 시스템을 다시 테스트해야 한다.

317. 구현 프로세스 마일스톤 M3

1. 코드 개발을 완료한다.
2. 통합 및 SI 테스트를 완료한다.
3. 기능 시험 전략 및 계획과 시험 결과의 조정은 추적성 매트릭스를 기준으로 검토되고 확인하여야 한다.
4. SI는 전환 단계를 위해 통합 시스템 프로그램을 배포한다.
5. V & V 계획을 완료한다. (V & V 조직에 의해 개발됨)
6. 시뮬레이션을 완료한다. (V & V 조직에 의해 검증됨)
7. 확인이 완료되고 제어시스템 소프트웨어의 SRS 및 SDS 요건이 충족된다.
8. V & V 보고서가 작성되어 이해 관계자에게 전달된다.
9. 소프트웨어를 배포하기 전에 소프트웨어는 바이러스에 대해 검사된다.
10. 소유자는 소프트웨어가 현재 ConOps를 충족하는 것으로 확인한다. 여기에는 프로젝트 진행 과정에서 변경된 개념이 포함된다.
11. ConOps에서 정해진 대로 모든 구성 요소와 하위 시스템은 업데이트 된다.

제 4 절 전환 프로세스



401. 일반사항

1. 전환 프로세스는 이해관계자의 요구사항에 규정된 서비스를 운용 환경 내에서 제공할 수 있는 능력을 확립하고, 소유자 및 사용자가 구현된 통합 소프트웨어가 요구사항을 충족시키는 것을 확인한다.
2. 전환 프로세스에서 사용자는 통합 소프트웨어의 작동 및 유지 보수에 대한 책임을 진다. SI는 매뉴얼, ConOps, SRS 및 SDS 등을 포함한 최종 문서를 사용자 및 소유자에게 전달하여야 한다.

402. 활동

전환 프로세스에서는 통합 소프트웨어를 사용자에게 공급 및 설치하고, 사용자는 설치된 통합 소프트웨어가 SDS에 맞게 동작하는지 확인하며, 소유자는 유지보수(Maintenance) 계획을 수립해야 한다. 전환 프로세스의 활동은 ISO/IEC/IEEE 12207 First Edition, 2017-11, 「시스템 및 소프트웨어 엔지니어링 - 소프트웨어 생명주기 프로세스」와 ISO/IEC/IEEE 15288 First edition 2015-05-15, 「시스템 및 소프트웨어 엔지니어링 - 소프트웨어 생명주기 프로세스」를 참조하여 개발되었으며 다음과 같다.

No.	활동
소유자	
1	인수단계 이후 변경 관리를 사용자로 이전.
2	운용 메뉴얼 검토
3	유지보수 계획 수립
4	유지보수 계획 검토
사용자	
1	신규/ 수정된 통합 소프트웨어 설치
2	설치된 통합 소프트웨어의 초기화, 실행, 종료 시험
3	통합 소프트웨어 유지 보수 관리자 식별
4	O&M 계획 검토
시스템 통합 조직	
1	운영 메뉴얼 개발
2	통합 소프트웨어 유지 보수 관리자 식별
3	운용 매뉴얼, ConOps, SRS 및 SDS 등 소유자 및 사용자에게 제공
4	통합 소프트웨어 업데이트 변경 관리
5	소유자 및 사용자에게 교육 훈련 제공
6	통합 소프트웨어 운영 시험
7	통합 소프트웨어 배포

403. 유지보수 계획서 및 운영 매뉴얼

1. SI는 운영 매뉴얼을 개발하여 소유자 및 사용자에게 제공하여야 한다. 운영 메뉴얼은 통합 소프트웨어 유지 보수 관리자를 식별하여야 한다.
2. 소유자 및/또는 사용자는 가능한 경우 SI, 공급 업체 및 하위 공급 업체의 문서를 활용하여 유지보수 계획을 수립하여야 한다. SI는 유지보수 계획서 작성에 필요한 사항을 소유자 및 사용자에게 제공하여야 한다. 사용자는 소유자가 수립한 유지보수 계획을 검토하는 것이 좋다.
3. 유지보수 계획서에는 다음의 사항을 포함하는 것을 권고한다.
   (1) 시스템 소프트웨어의 유지 보수를 담당하는 이해 관계자를 식별한다.
   (2) 유지 보수의 구성 요소를 정의 한다.
   (3) 계획된 운영 및 유지 보수가 발생하는 곳을 식별한다.
   (4) 특정 운영 및 유지 보수가 발생 시기를 정의한다.
   (5) SI는 시스템의 유지 보수를 위한 교육 기간 및 과정을 권장 하여야 한다.
   (6) 수행 할 유지 보수 활동을 설명한다.
   (7) 건전성 및 성능 모니터링을 위해 수행할 점검 및 수집할 데이터를 설명한다.
   (8) 시스템 건전성 및 성과를 보고하는 일정을 포함하여 유지보수 효과성을 관리하기 위한 피드백을 제공한다.
   (9) SI가 제공하여야 하는 모든 문서를 지정한다.
   (10) 구성 변경, 수리 및 업그레이드에 따른 시스템 시험 및 형상 설명서 업데이트를 다룬다.
   (11) 소프트웨어의 예상 수명과 폐기시 대체, 업그레이드 및 폐기를 구체적으로 다룬다.
   (12) 소유자 또는 사용자는 운영 및 유지 보수에 필요한 인적 자원, 시설 및 도구를 식별할 것을 권고한다.
   (13) 계획은 개별 안전, 보안 및 소프트웨어 / 펌웨어 형상 관리 계획을 참조하고 소유자는 SI가 제공하지 않은 필요한 문서 목록을 추가하여야 한다.

404. 유지보수 항목 검토

1. 이해관계자는 완전성 및 다음의 유지보수 프로세스 진입을 기준으로 항목들을 검토하여야 한다. 검토하여야 하는 항목들은 다음과 같으며, 이러한 모듈이 누락 되었거나 불완전한 경우 유지보수 프로세스를 시작하지 않는 것을 권고한다.

(1) 제어 장비 레지스트리
(2) 변경 관리(Management of Change 이하 MOC) 정책
(3) 변경 관리(MOC) 절차
(4) 선박 소프트웨어 레지스트리
(5) 소프트웨어 형상 관리 계획서
(6) 소프트웨어 변경 제어 절차

405. 변경 관리(MOC) 정책

1. MOC 정책은 통합 소프트웨어 완전성을 결정하기 위해 사용자에 의해 검토되는 것을 권고한다. 검토 기록은 우리선급의 검토를 위해 선박에 보관되어야 한다.
2. 소프트웨어의 변경 관리는 설치 승인을 위해 소유자 또는 사용자의 MOC 절차를 따르는 것이다. SI는 내부적으로 소프트웨어 업데이트에 대한 변경 관리를 유지 한다. 소유자 및/또는 사용자는 MOC에 따라 신규 또는 업데이트 된 소프트웨어를 설치할 수 있다.
3. 사용자는 적어도 다음 항목 및 활동에 대한 변경 관리 (MOC) 정책을 검토하여야 한다.
   (1) MOC 프로세스 내의 다양한 역할과 책임에 대한 정의
   (2) IL2 및 IL3 구성 요소의 변경에 대한 소프트웨어 검증을 위한 프로세스
   (3) MOC에서 검토 및 정의된 마일스톤 및 생명주기
   (4) 변경 프로세스 평가는 프로세스의 일부로 수행되어야 한다.
   (5) 공식적인 승인 절차를 정의한다.
   (6) 소유자 또는 사용자는 새로운 제한사항 및 공정 안전성 업데이트를 위해 MOC를 지켜야 한다. 변경 사항은 기록하여야 한다.
   (7) 공식적인 선박 또는 해양플랜트의 통보는 소유자 또는 사용자의 MOC 절차의 일부가 되어야 한다.
   (8) 사용자는 자산의 MOC 정책 내에서 소프트웨어 변경 사항을 관리하여야 한다.
   (9) 사용자는 ISPM 제어 시스템에서 추가, 갱신 또는 삭제 된 IL2 및 IL3 기능을 우리선급에 통보해야한다.
   (10) 소프트웨어 변경, 업데이트, 삭제 또는 새 기능은 하위 시스템을 포함한 제어 시스템의 범위에 미치는 영향에 대해 검토하는 것을 권장한다.

406. 소프트웨어 레지스트리

1. 레지스트리는 최소한 다음의 정보를 포함하여야 한다.
   (1) 파일 크기
   (2) SI 또는/그리고 공급업자에게 제공될 경우 백업의 물리적 위치
   (3) 제어 시스템 및 구성 요소, HMI, 서버 등에 대한 복구 절차의 위치
   (4) 최근 소프트웨어를 설치한 날짜

407. 제어 장비 레지스트리

1. 레지스트리에는 적어도 다음의 정보를 포함하여야 한다.
   (1) 설치되어 있는 제어 장비
   (2) 무결성 레벨
   (3) 제어장비의 추적 가능한 고유 태그
   (4) 상호작용을 하는 소프트웨어 모듈

408. 소프트웨어 형상 관리 계획

1. 소유자와 사용자는 적어도 다음에 따라 소프트웨어 형상 관리 계획을 검토하는 것을 권고한다..
   (1) 소프트웨어 형상 관리 활동을 계획하여야 한다.
   (2) 모든 소프트웨어 작업 자산은 식별하고 통제하며 사용할 수 있어야 한다.
   (3) 식별된 소프트웨어 작업 자산에 대한 모든 변경이 관리하여야 한다.
   (4) 모든 이해 관계자에게 소프트웨어 베이스 라인의 상태 및 내용을 통보 한다.
   (5) 소프트웨어 요구사항의 변경을 제어하기 위한 메커니즘을 사용하여야 한다.

(6) 소프트웨어 설계의 변경을 제어하기 위한 메커니즘을 사용하여야 한다.
(7) 코드 변경을 제어하는 메커니즘을 사용하여야 한다.
(8) 메커니즘은 유지 관리 프로세스에서 소프트웨어 도구의 형상 관리에 사용된다.
(9) 회귀 테스트 라이브러리는 유지보수사항의 수락을 위해 포함되어야 한다.
(10) 소프트웨어 형상 관리 계획은 소유자/사용자의 MOC 절차의 일부일 수 있다.

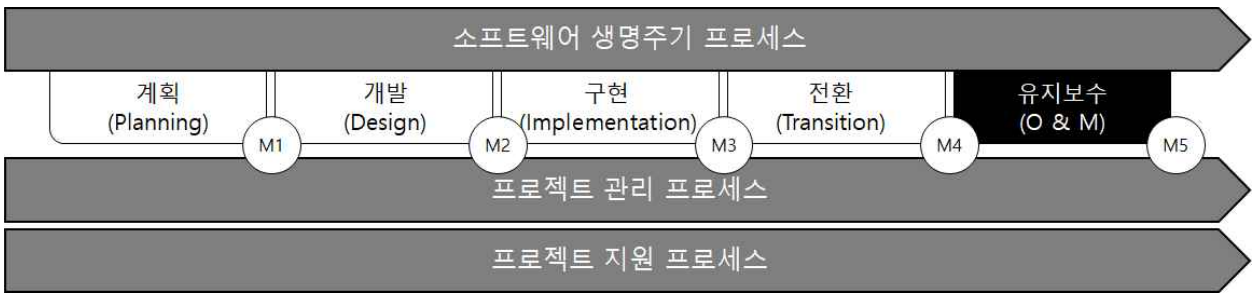
409. 바이러스 및 기타 악성 소프트웨어 검사

1. 통합 소프트웨어의 설치 전에 모든 소프트웨어 코드, 실행 파일 및 선박에 설치하는 데 사용되는 물리적인 매체에 바이러스 및 악의적인 소프트웨어가 있는지 검사하여야 한다.
2. 검사 결과는 문서화되어 소프트웨어 레지스트리에 보관된다.

410. 전환 프로세스 마일스톤 M4

1. 작동 매뉴얼 제공
2. 운영 관리 계획 개발
3. 제어시스템 소프트웨어 승인
4. 선박 건조업체, 소유자, 사용자 및/또는 SI에 의해 선박 소프트웨어 레지스트리 갱신
5. 선박 건조업체, 소유자, 사용자 및/또는 SI에 의해 제어 장비 레지스트리 갱신
6. 시운전 시험.
7. 소유주로부터 O & M 단계로 진행하는 권한 부여

제 5 절 유지보수 프로세스



501. 일반사항

1. 유지보수 프로세스는 예정된 업그레이드와 예기치 않은 업그레이드 그리고 문제 해결 활동을 포함한 모든 유지보수 활동을 다룬다. 이 프로세스는 ISPM 통제 시스템의 폐기 활동까지 적용 할 수 있다.
2. 유지보수 프로세스는 통합 소프트웨어를 사용하고, 그 능력이 지속되도록 한다. 최종적으로는 통합 소프트웨어의 가동을 중단하고, 해체 및 제거하여 통합 소프트웨어가 설치된 환경을 원래 상태 또는 소유자 또는 사용자가 수락 가능한 상태로 복원한다.

502. 활동

유지보수 프로세스의 활동은 사용자와 그의 지시에 따라 공급자(들)의 책임 하에 이루어진다. 통합 소프트웨어는 소유자가 수락하여 사용자에게 제공되는 등 전환 프로세스 후, 소유자 또는 사용자는 SI, 공급 업체 및 하위 공급 업체가 제공한 정보 및 문서를 바탕으로 통합 소프트웨어의 성능을 관찰한다. 유지보수 프로세스의 활동은 ISO/IEC/IEEE 12207 First Edition, 2017-11, 「시스템 및 소프트웨어 엔지니어링 - 소프트웨어 생명주기 프로세스」와 ISO/IEC/IEEE 15288 First edition 2015-05-15, 「시스템 및 소프트웨어 엔지니어링 - 소프트웨어 생명주기 프로세스」를 참조하여 개발되었으며 다음과 같다.

No.	활동
소유자	
1	변경관리 절차 개발 및 관리. 변경관리 요구사항 관리
2	노후화 모니터링
3	O&M 계획 검토
4	변경관리 검토
5	O&M 계획 개발, 검토를 위해 발행 한 다음 구현을 위해 발행.
사용자	
1	시스템 소프트웨어의 변경사항은 통제된 방식으로 관리 된다.
2	소프트웨어 변경의 영향이 시스템 전체에 미치는 영향을 검토해야 한다.
3	업그레이드 또는 코드 변경 후에 검증 시험 수행(통합 조직은 동등 검토를 수행 할 수 있다.)
4	사용자 일정에 대한 정기적인 소프트웨어 감사 수행
5	O&M 계획 업데이트 (필요시)
6	O&M 계획 검토
7	ISPM 통합 소프트웨어 레지스터 유지관리
8	제어기기 레지스트리 유지관리
9	노후화에 대한 모니터링
시스템 통합 조직	
1	운영 매뉴얼 개발

1. 조직의 제약사항과 관련된 운영상의 문제점을 식별하고 분석한다.
(1) 서비스를 제공하는 시스템의 능력을 관찰하고, 문제점을 분석하기 위해 기록하고, 교정 활동, 조정 활동, 적응 활동, 예방 활동을 취하고, 회복된 능력을 확인한다.
(2) 이 프로세스는 시스템 요소 또는 폐기물을 법률, 협약, 조직의 제약사항 및 이해관계자 요구사항에 따라 환경적으로 건전한 방식으로, 재생, 저장, 파괴한다. 요구된 경우에는 조작자, 사용자의 건강 및 환경의 안전을 감시할 수 있도록 기록을 유지하여야 한다.

503. 바이러스 및 기타 악성 소프트웨어 검사

운용 중인 통합 소프트웨어에 바이러스 및 악의적인 소프트웨어가 있는지 정기적으로 검사하여야 한다. 검사 결과는 문서화되어 소프트웨어 레지스트리에 보관된다.

504. 통합 제어 시스템 유지 보수

1. 예정된 업그레이드 - 새로운 기능

통합 제어 시스템의 새로운 기능 업그레이드는 대개 중요한 컴퓨터 시스템의 교체, 주요 시스템 기능의 추가 또는 교체에 따른 것이다. 알려진 특성과 유닛에 대한 중요한 영향으로 인해 이러한 업그레이드는 초기 시스템통합과 같은 방식으로 관리한다. 새로운 제어 시스템 기능을 사용하려면 이전의 SDLC 단계에서 프로세스 및 산출물을 업데이트하여야 한다. SDLC의 활동들은 프로젝트의 범위에 맞게 축소 될 수 있다. 중요한 업그레이드와 사소한 업그레이드의 구분은 제어 시스템의 단위 및 적용에 따라 다르다.

(1) 프로젝트 관리
예정된 새 기능에 대한 프로젝트 관리 계획을 세운다.
(2) 개념 단계
(가) 기존 ConOps를 검토하고 새로운 기능을 반영하여 업데이트
(나) 모든 새로운 기능을 정의
(다) 새로운 기능의 안전성 검토.
(라) 기능의 고장으로 인한 결과를 검토하고 다른 조직 및 그룹으로부터의 입력으로 새로운 무결성 레벨을 지정

(마) 새로운 기능에 대한 검증 방법은 가급적 원래 검증에 사용한 방법과 동일하게 적용
(바) 모든 추적 성 매트릭스를 업데이트

(3) 요구 사항 및 설계 단계
(가) 새로운 기능을 반영하여 기존 SRS를 업데이트
(나) 새로운 요구사항을 반영하여 기존 SDS를 업데이트
(다) 모든 기존의 성능, 안전성, 데이터베이스 및 보안 요구 사항을 업데이트하고 표준, 인간 공학적 고려 사항 및 기능을 준수하십시오.
(라) 모든 새로운 상업용 기성품 (COTS) 패키지에 대한 새로운 통합 테스트를 정의한다.

(4) 개발 단계
(가) 새로운 기능을 지원하는 통합 코드를 개발
(나) SI는 SRS 및 SDS에 따라 개발 단계에 명시된 모든 수준의 테스트를 완료하여야 한다.

(5) 확인, 검증 (V & V) 단계
(가) 검증 계획 (V & V 계획)을 업데이트하고 검증 방법에 대한 시뮬레이션 구성.
(나) 업데이트 된 V & V 계획 수행.
(다) 통합 시스템을 소유자 및 사용자로 전환.

(6) 전환 단계
(가) 설치하고자 하는 하드웨어에 소프트웨어 설치.
(나) 모든 지원 서비스를 기능적으로 테스트.
(다) O & M 단계에서 모든 문서 업데이트.

2. 예기치 않은 업그레이드

(1) 기기 제조업체가 제어 시스템에 대한 하드웨어, 펌웨어 또는 소프트웨어 업그레이드를 배포하거나 컴퓨터 하드웨어 제조업체가 일련의 수정 사항을 배포 할 때 예기치 않은 업그레이드가 발생한다.
ISPM 제어 시스템 또는 무결성 레벨 IL0 ~ IL3를 가진 소프트웨어 기능은 업그레이드의 경우 다음 단계를 통해 업그레이드를 수행하여야 한다.
(가) 잠금 / 태그 아웃과 관련된 안전 절차를 따른다.
(나) 하드웨어 / 소프트웨어를 업그레이드 할 때 제조업체의 지침을 따른다.
(다) 소프트웨어 및 제어 장비 레지스트리를 사용하여 업그레이드된 하드웨어/소프트웨어와 상호 작용하는 모든 하드웨어/소프트웨어 모듈을 식별한다.
(라) 적어도 SI는 모든 식별된 하드웨어/소프트웨어 대해 소프트웨어 코드를 검토하거나 회귀 테스트를 수행하여야 한다.
(마) 모든 시험을 통과되면 업그레이드된 하드웨어 / 소프트웨어를 작동 상태로 만든다.
(바) 테스트가 실패한 경우 업그레이드를 시도하기 전에 공급자에 문의하여 이전 버전의 하드웨어 / 소프트웨어로 시스템을 반환한다.
(사) 모든 문서 갱신.

(2) IL2 또는 IL3 소프트웨어 기능이 업그레이드하는 경우 소유자 또는 사용자는 가능한 “예정된 업그레이드” 절차를 따라야한다.

(3) 중요하거나 사소한 업그레이드는 결정된 대로 IL2 및 IL3 ISPM 제어 시스템에 대해 “예정된 업그레이드” 절차에 따라 수행하여야 한다. ConOps, SRS & SDS를 업데이트하기 위해 최소한 504.의 1항 (1), (2)에 정의 된 프로세스를 따라야 한다.

(4) IL0 및 IL1 ISPM 제어 시스템의 경우 504.의 2항 (1) (가) ~ (바) 또는 소유자의 재량에 따라 504.의 1항을 준수하는 것을 권고한다.

505. 시스템 폐기

제어 시스템의 폐기 또는 교체는 다음에 따라 폐기 또는 교체 계획을 고려하여야 한다.

1. 폐기 또는 교체 활동 중에 제어 및 모니터링이 감소되거나 제거된다. 폐기 계획은 제거 및/또는 교체 중 장비 및 프로세스에 대한 안전장치를 고려하여야 한다.
2. 교체되는 제어 시스템은 ISPM 부기부호를 부여받은 제어 시스템의 기능에 영향을 미쳐서는 아니 된다.

506. 유지보수 프로세스 마일스톤 M5

1. 통합 제어 시스템 폐기. ⚓

인 쇄 2021년 3월 24일
발 행 2021년 4월 1일

통합 소프트웨어 프로세스 관리 지침

발행인 이 형 철
발행처 한 국 선 급
부산광역시 강서구 명지오션시티 9로 36
전화 : 070-8799-7114
FAX : 070-8799-8999
Website : http://www.krs.co.kr

신고번호 : 제 2014-000001호 (93. 12. 01)