건설/가동중 원전 안전등급 소프트웨어 V&V 경험 공유

주식회사 포멀웍스

김 태 효

2020.7.8

Copyright © 2019 Formal Works Inc. All Rights Reserved

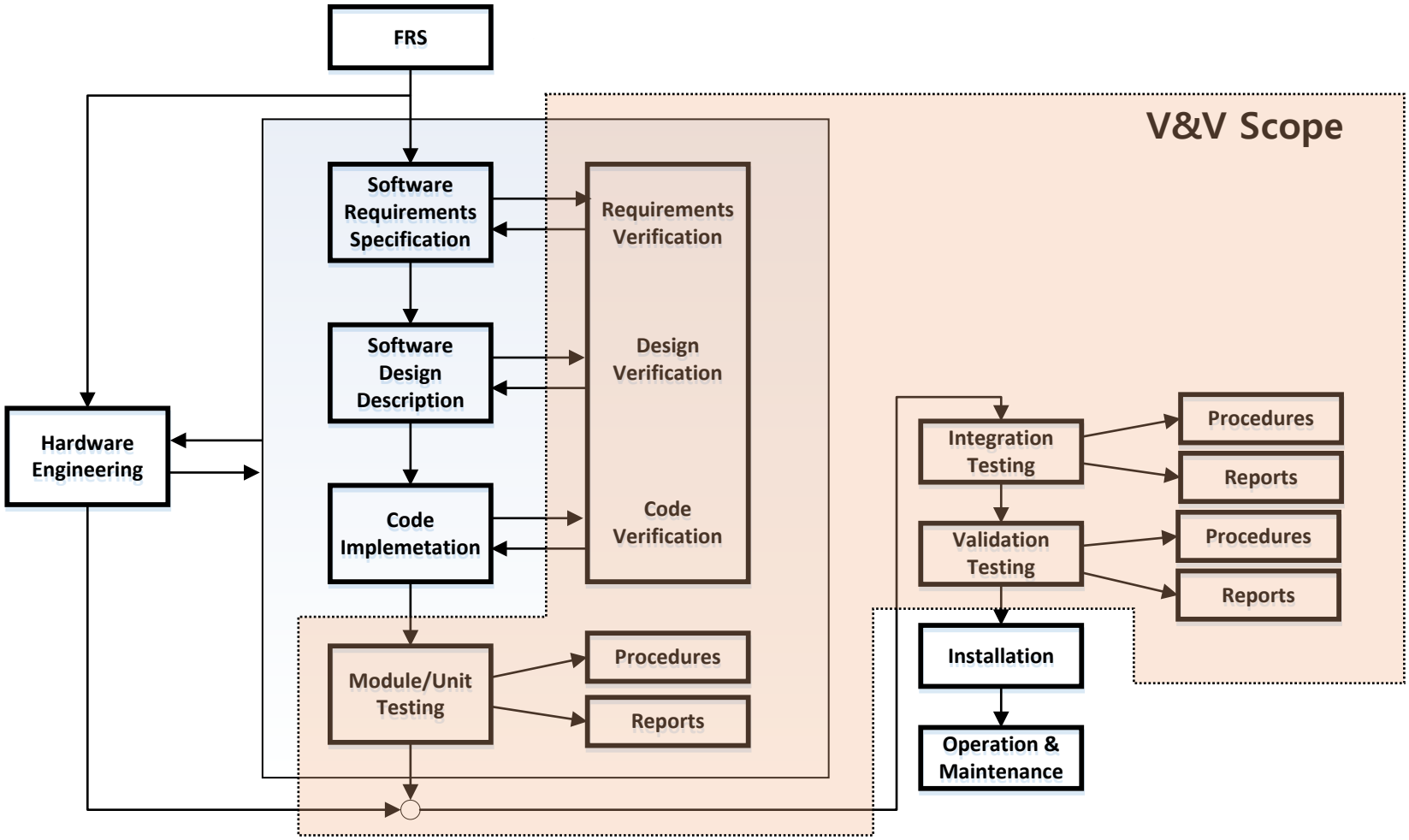
목차

I. 건설원전 소프트웨어 V&V 사례 연구

소프트웨어 요구사항 명세와 시스템 시험 사례 공유

1. 소프트웨어 V&V 개요

Software Engineering Process for I&C Systems

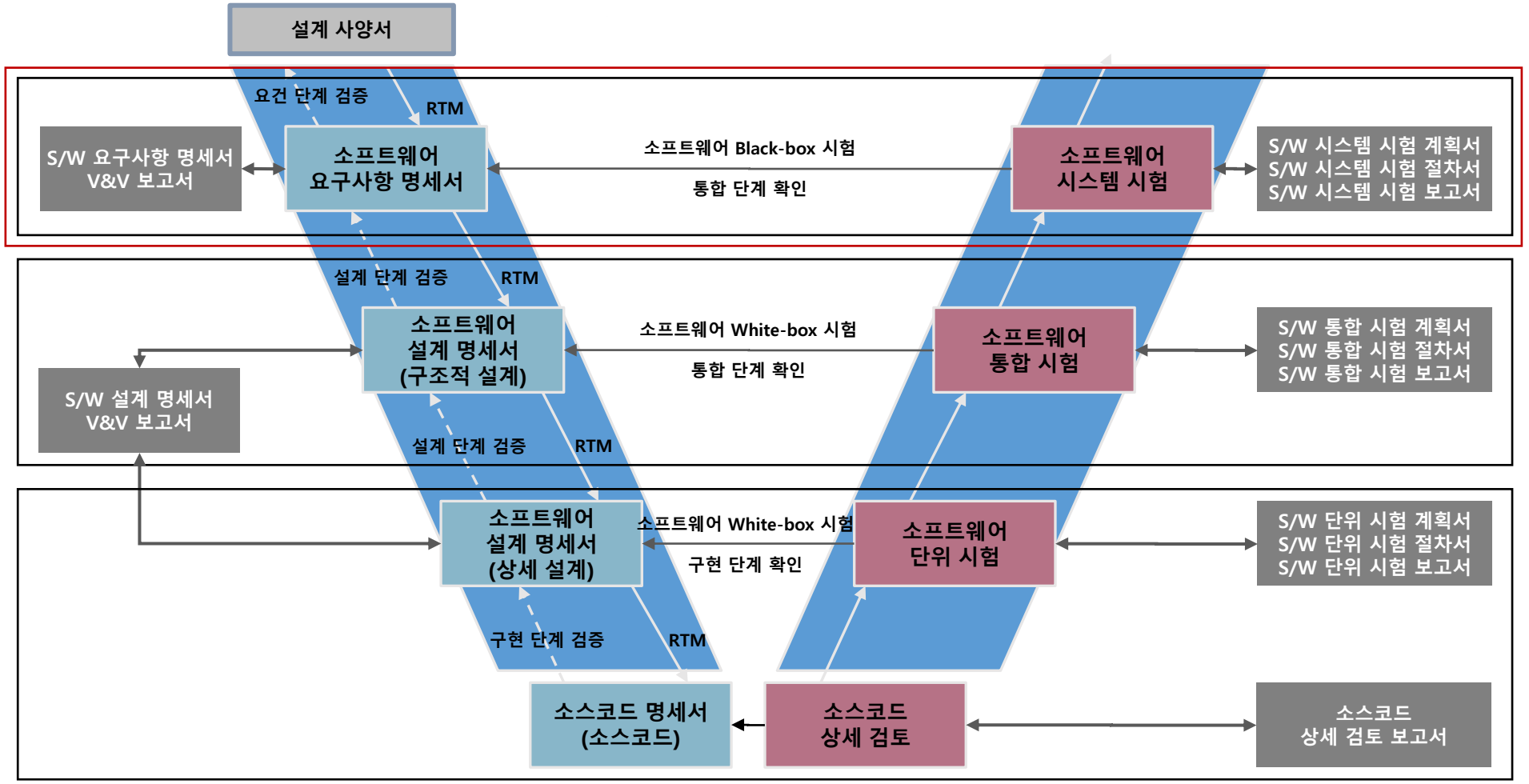


Copyright © 2019 Formal Works Inc. All Rights Reserved

1. 소프트웨어 V&V 개요

소프트웨어 확인 및 검증 활동 요약

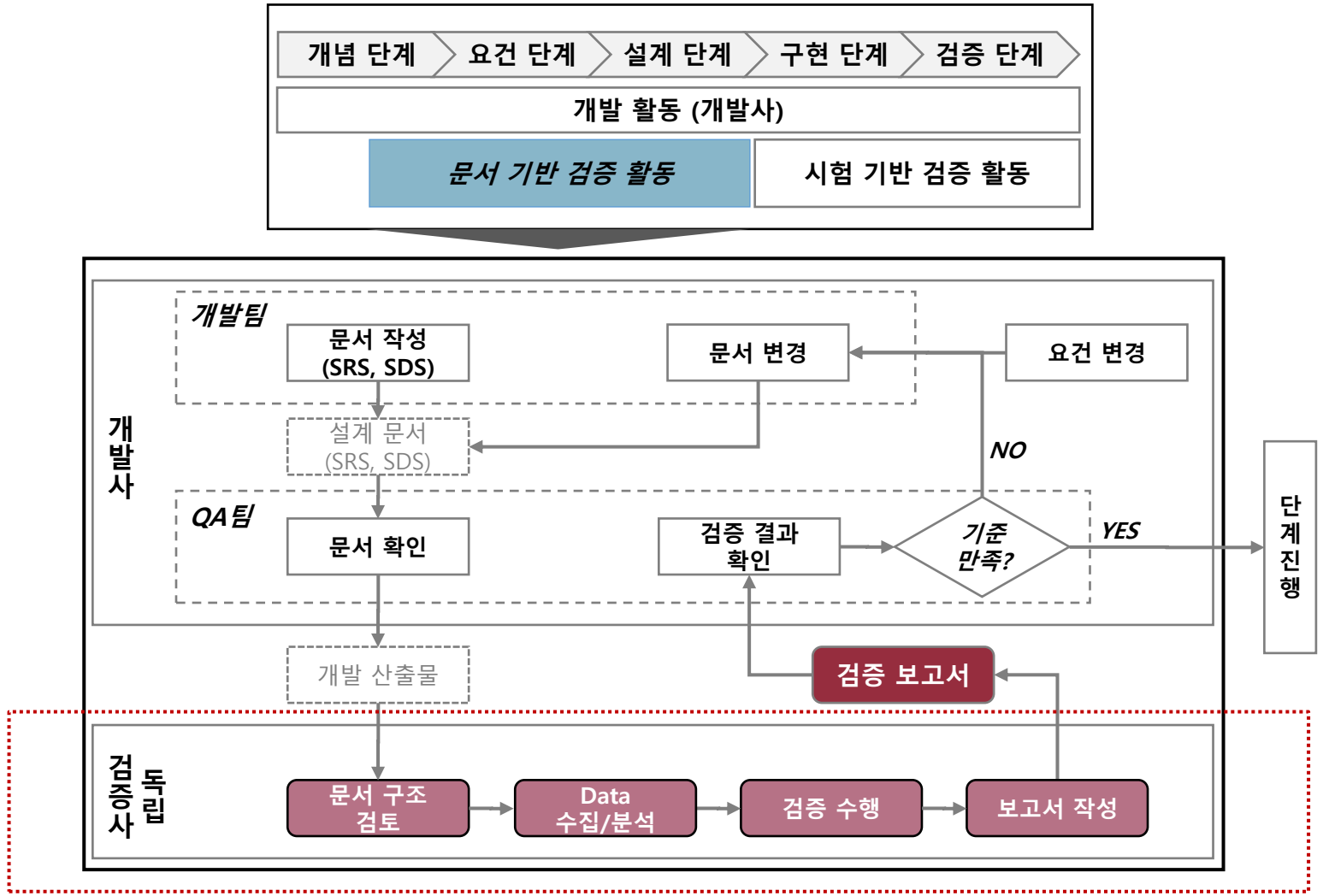
➢ 단계 별 개발 산출물에 대하여 IEEE Std. 1012 기반 확인 및 검증 활동을 수행



Copyright © 2019 Formal Works Inc. All Rights Reserved

2. 문서 기반 검증

문서 기반 검증 절차 예시



Copyright © 2019 Formal Works Inc. All Rights Reserved

2. 문서 기반 검증

➢ 문서 기반 검증은 소프트웨어 검증의 규제 지침 및 기술 표준을 기반으로 설계 문서에서 수집/분석한 정보가 각 **검증 특성을 만족하는지 확인하고 문서화**

원전 문서 기반 검증 활동 예시

➢ 기본 검증 특성
- BTP-14 및 IEEE Std. 1012를 위한 Checklist 기반 문서 검토

➢ 세부 검증 특성
- 추적성 세부 검증
  - ❖ [요건단계] 사양서 ↔ SRS
  - ❖ [설계단계] SRS ↔ SDS
- 완전성 및 일관성 세부 검증
  - ❖ [요건단계] 기능 ↔ 인터페이스
  - ❖ [설계단계] 기능 ↔ 데이터, 기능 ↔ 기능

SRS/SDS 검증

인허가 적합성 검토 (BTP-14)		상세 검증 (IEEE 1012)		
기능 특성	공정 특성	추적성	명세 평가	IF 분석
정확도	완전성	완전성	정확도	정확도
신뢰성	일관성	일관성	완전성	완전성
강인성	정확성	정확성	일관성	일관성
안전성	스타일		정확성	정확성
보안성	추적성		판독성	시험성
타이밍	검증성		시험성	

➔ *검증 특성 별 검증항목(Checklist)을 만족하는지 확인*

FORMAL WORKS S/W Development & Verification
Copyright © 2019 Formal Works Inc. All Rights Reserved

3. 소프트웨어 요구사항 명세

- 소프트웨어 확인 및 검증의 품질은 설계 문서의 품질에 따름
- 시험자 및 검증자의 판단보다 **설계 문서 기반의 확인 및 검증이 중요**

요구사항 명세서 작성 주안점

- 소프트웨어 시스템 시험 품질은 요구사항 명세서(SRS)의 품질과 직접적으로 연관됨
  - 3C + 1T
  - Completeness, Consistency, Correctness + Traceability
- 하나의 요구사항을 시험 가능한 세부 요구사항으로 분할하여 시험 항목 추출
  - 시험 가능한 시험 항목의 추출에 많은 노력 필요
    - ❖ 분할 가능한 요구사항 명세 필요 (e.g. Decision Table)
  - 엄밀한 요구사항 커버리지 측정 가능
- 정확한 인터페이스 요구사항 명세 필요
  - 시험의 입출력을 조작 및 모니터링 하기 위한 엄밀한 인터페이스 요구사항 정의 필요
    - ❖ 시험 입력 생성이 가능한 충분한 정보 필요 (type 정보 등)
- 인터페이스 요구사항에 기반한 기능 요구사항 명세 필요
  - 기능 요구사항을 인터페이스 (요구사항) 정의를 사용하여 명세

Copyright © 2019 Formal Works Inc. All Rights Reserved

3. 소프트웨어 요구사항 명세

설계 사양서 예시

설계 사양서	
절 번호	**사양**
3.2.1.12	참고문서 2.5.6절 진단 요건, 2.3.3.7절 고장 감지 및 복귀 요건, 2.4.6.5절 백업 및 이중화 요건 에 따라 이중화 프로세서모듈은 다음과 같은 진단 기능을 수행하며, ... **(G) 프로세서모듈 메모리 진단** ...
3.2.1.23	문제가 발생한 이중화 프로세서모듈은 ...

추적성 분석 (요구사항 명세 확인 및 검증 보고서)

설계 사양서		요구사항 명세서		검토 의견
절번호	**내용**	**절번호**	**내용**	
3.2.1.12	참고문서 2.5.6절 진단 요건, 2.3.3.7절 고장 감지 및 복귀 요건, 2.4.6.5절 백업 및 이중화 요건 에 따라 이중화 프로세서모듈은 다음과 같은 진단 기능을 수행하며, ... **(G) 프로세서모듈 메모리 진단** ...	**5.9.11**	**[R-9-11]** 마스터/슬레이브 정상 상태에서 클락틱의 발생에 따라 메모리 진단을 실시하여 메모리 에러 여부를 점검하여야 한다.	* 추적성을 만족함
3.2.1.23	문제가 발생한 이중화 프로세서모듈은 ...			

설계 사양서

- 3.2.1.12절 프로세서 모듈 메모리 진단
- 3.2.1.23절

소프트웨어 요구사항 명세서

- 5.9.11절 [R-9-11]

FORMALWORKS S/W Development & Verification
Copyright © 2019 Formal Works Inc. All Rights Reserved

3. 소프트웨어 요구사항 명세

기능 요건 작성 예시

[R-1] 마스터/슬레이브 정상 상태에서 클락틱의 발생에 따라 메모리 진단을 실시하여 메모리 에러 여부를 점검하여야 한다. …

(A) 입력: 클락틱, EXT_CON_REG_RUN, EXT_CON_REG_ERR, EXT_CON_REG_INI

(B) 출력: ERR_LED, LOCAL_CON_REG_FLT, BUS_RST

(C) 처리

입력		처리				출력			
클락틱	EXT_CON_REG_RUN, EXT_CON_REG_ERR, EXT_CON_REG_INI	조건1	조건2	조건 3	행위	ERR_LED	LOCAL_CON_REG_FLT	BUS_RST	
2ms 마다 발생 시	'EXT_CON_REG_RUN'이 1이 아니거나, EXT_CON_REG_ERR이 0이 아니거나, EXT_CON_REG_INI가 1이 아닌 경우'	메모리 에러 발생	마스터 모드로 동작중인 경우	사용자가 해당 에러 발생 시 계속 동작으로 설정한 경우	메모리 에러 발생 및 사용자 태스크 계속 실행	01	N/A	N/A	Master(정상) / Slave (비정상) 어플리케이션 계속 실행 설정 LED만 표시 후 계속 수행
				그 외의 경우	메모리 에러 에러 발생 및 사용자 태스크 중지, 마스터 Fail-Safe 상태로 전환	01	1	1	Master(정상)/Slave (비정상) 어플리케이션 계속 실행 설정 없음 Fail-Safe 상태로 전이
			슬레이브 모드로 동작 중인 경우	모든 경우	메모리 에러발생 및 슬레이브 비정상 상태로 진입	01	N/A	N/A	슬레이브 모드에서 발생한 경우는 비정상 상태
		그 외의 경우	모든 경우	모든 경우	N/A	N/A	N/A	N/A	정상 수행
	그 외의 경우	…	…	…	…	…	…	…	… … …

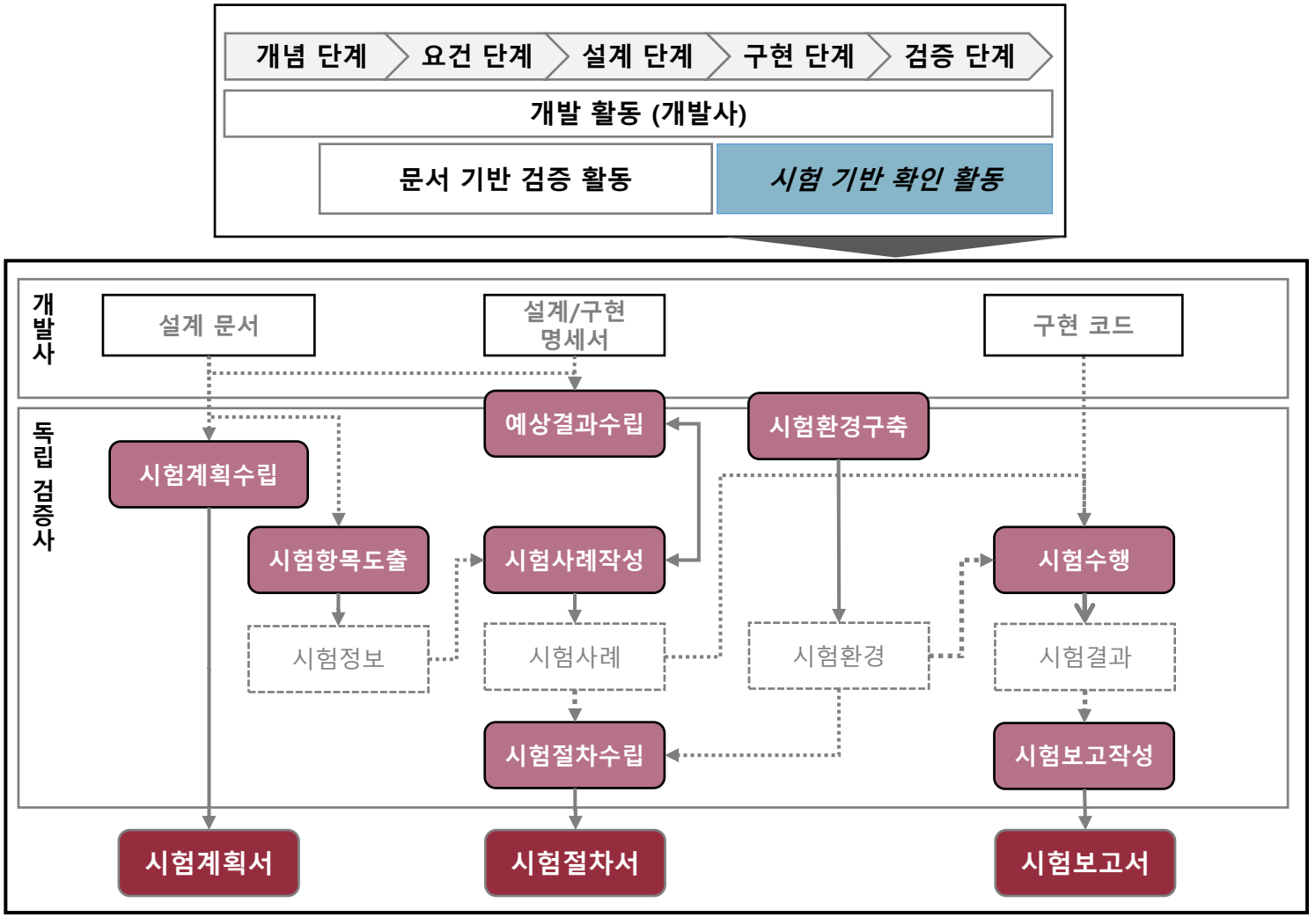
Completeness & Consistency!

(D) 기타: 코드나 상수 영역, Flash Memory 영역 중 데이터가 변하지 않는 메모리 영역에 대해서는 CRC 검사로 메모리 검사를 수행하며, …

Copyright © 2019 Formal Works Inc. All Rights Reserved

4. 소프트웨어 시스템 시험

소프트웨어 시험 절차 예시



Copyright © 2019 Formal Works Inc. All Rights Reserved

4. 소프트웨어 시스템 시험

- 소프트웨어 시험은 단위 시험, 통합 시험, 시스템 시험으로 구분하여 수행
- 각 시험 수준별로 확인 대상, 적절한 범위, 시험 기법, 커버리지 기준을 선정하여 진행

소프트웨어 시험의 종류 및 특징

테스팅 종류	테스팅 목적 (Testing Objectives)	테스팅 범위	테스팅 방법	테스팅 품질 측정 (Test Coverage)
단위 시험 (Software Unit Test)	소프트웨어의 구성 단위가 의도한대로 올바르게 동작하는 지 시험	함수	❖ 프로그램상의 function 각각에 대하여 White-box 시험 수행	Statement + Branch (Decision) + MCDC Coverage
통합 시험 (Software Integration Test)	소프트웨어의 구성 단위의 부분 통합들이 의도한대로 올바르게 동작하는지 시험	함수 집합	❖ Bottom-up 방식으로 함수들을 통합 ❖ 각 통합 부분에 대하여 함수 호출을 이용한 상호작용이 정확한지 White-box 시험 수행	Call Graph Coverage (+ Function Coverage)
시스템 시험 (Software System Test)	전체 소프트웨어 모듈이 의도한대로 올바르게 동작하는지 시험	**모듈의 전체 소프트웨어 부분**	❖ 소프트웨어 요구사항을 검사 가능하도록 세분화하고, ❖ 전체 모듈 소프트웨어에 대하여 Black-box 시험 수행	**Requirement Coverage**

Copyright © 2019 Formal Works Inc. All Rights Reserved

4. 소프트웨어 시스템 시험

시스템 시험 단계 및 특징

1. 시험 계획 수립

- 요구사항 명세서의 시험 가능 요구사항을 시험 특성으로 도출

2. 시험 항목 도출

- Black-Box 시험 기법에 따라 요구사항으로부터 시험 항목으로 도출
- 요구사항 입출력 및 구분된 처리에 따라 시험 항목 세분화

3. 시험 사례 작성

- 요구사항 커버리지 기준을 만족하도록 시험 사례 생성
- 외부 인터페이스 외의 입출력을 제어하는 시험은 비정상 상황 시험으로 별도 관리

4. 시험 환경 구축 및 절차 수립

- 시험 환경 구축 절차 기술
- 사례 별 시험 절차의 수립: 가능한 경우 공통 시험 수행 절차 수립

5. 시험 수행 및 시험 보고 작성

- 배치 환경 상에서 시험 사례 구동 : 가능한 경우 스크립트 작성으로 재연성 확보
- 개발 환경 수준에서 비정상 상황 시험 사례 구동
- 시험 결과 및 커버리지 정보 등의 보고 작성

Copyright © 2019 Formal Works Inc. All Rights Reserved

4. 소프트웨어 시스템 시험

기능 요건 작성 예시

[R-1] 마스터/슬레이브 정상 상태에서 클락틱의 발생에 따라 메모리 진단을 실시하여 메모리 에러 여부를 점검하여야 한다. …

(A) 입력: 클락틱, EXT_CON_REG_RUN, EXT_CON_REG_ERR, EXT_CON_REG_INI

(B) 출력: ERR_LED, LOCAL_CON_REG_FLT, BUS_RST

(C) 처리

입력		처리				출력		
클락틱	EXT_CON_REG_RUN, EXT_CON_REG_ERR, EXT_CON_REG_INI	조건1	조건2	조건 3	행위	ERR_LED	LOCAL_CON_REG_FLT	BUS_RST
2ms 마다 발생 시	‘EXT_CON_REG_RUN’ 이 1이 아니거나, EXT_CON_REG_ERR이 0이 아니거나, EXT_CON_REG_INI가 1이 아닌 경우’	메모리 에러 발생	마스터 모드로 동작중인 경우	사용자가 해당 에러 발생 시 계속 동작으로 설정한 경우	메모리 에러 발생 및 사용자 태스크 계속 실행	01	N/A	N/A
				그 외의 경우	메모리 에러 에러 발생 및 사용자 태스크 중지, 마스터 Fail-Safe 상태로 전환	01	1	1
			슬레이브 모드로 동작 중인 경우	모든 경우	메모리 에러발생 및 슬레이브 비정상 상태로 진입	01	N/A	N/A
		그 외의 경우	모든 경우	모든 경우	N/A	N/A	N/A	N/A
	그 외의 경우	…	…	…	…	…	…	…

- Master(정상) / Slave (비정상)
  - 어플리케이션 계속 실행 설정
  - LED만 표시 후 계속 수행
- Master(정상)/Slave (비정상)
  - 어플리케이션 계속 실행 설정 없음
  - Fail-Safe 상태로 전이
- 슬레이브 모드에서 발생한 경우는 비정상 상태
- 정상 수행
- …
- …
- …

(D) 기타: 코드나 상수 영역, Flash Memory 영역 중 데이터가 변하지 않는 메모리 영역에 대해서는 CRC 검사로 메모리 검사를 수행하며, …

Copyright © 2019 Formal Works Inc. All Rights Reserved

4. 소프트웨어 시스템 시험

- 요구사항 명세서의 각 세부 처리를 시험 항목으로 선정
  - 필요 시 예외 처리 및 기타 항목도 시험 항목으로 선정
- **Requirement Coverage**

시험 항목 예시

소프트웨어의 기능 요구사항에 대한 세부 요구사항

분류	기능 요구사항	세부 처리	예외처리	기타 사항
시스템 태스크의 진단 기능	[R-9-11]	[T1-L1] ~ [T1-L7]	N/A	[ETC01]

소프트웨어 시험 항목: 이중화 기능

시험 항목	기능 설명	세부 요구사항
[I-DUAL-04] 메모리 관련 동작	이중화 동작시 메모리 상태에 따라 해당 처리를 수행함	[R-9-11]-[T1-L4]
		[R-9-11]-[T1-L3]
		[R-9-11]-[T1-L1]
		[R-9-11]-[T1-L2]
		[R-9-11]-[T1-L7]
		[R-9-11]-[T1-L5]
		[R-9-11]-[T1-L6]

소프트웨어 시험 항목: 이중화 기능

시험 항목	기능 설명	세부 요구사항
[I-EX-MEM] 메모리 검사	메모리 검사 예외처리	[R-9-11]-[ETC01]

SRS 처리 내용

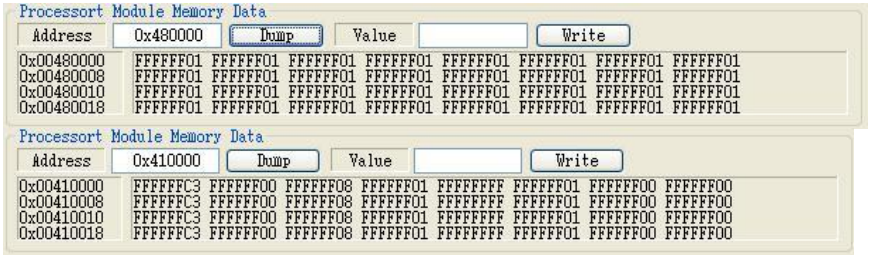
T1-L1	Master(정상)/Slave (비정상)
	어플리케이션 계속 실행 설정
	LED만 표시 후 계속 수행
T1-L2	Master(정상)/Slave (비정상)
	어플리케이션 계속 실행 설정 없음
	Fail-Safe 상태로 전이
T1-L3	슬레이브 모드에서 발생한 경우는 비정상 상태
T1-L4	정상 수행
T1-L5	...
T1-L6	...
T1-L7	...

FORMAL WORKS S/W Development & Verification
Copyright © 2019 Formal Works Inc. All Rights Reserved

4. 소프트웨어 시스템 시험

시스템 시험 사례 예시

입력		처리				출력		
클락틱	EXT_CON_REG_RUN, EXT_CON_REG_ERR, EXT_CON_REG_INI	조건1	조건2	조건 3	행위	ERR_LED	LOCAL_CON_REG_FLT	BUS_RST
2ms 마다 발생	'EXT_CON_REG_RUN' 이 1이 아니거나, EXT_CON_REG_ERR이 0이 아니거나, EXT_CON_REG_INI가 1이 아닌 경우'	메모리 에러 발생	마스터 모드로 동작중인 경우	그 외의 경우	메모리 에러 에러 발생 및 사용자 태스크 중지, 마스터 Fail-Safe 상태로 전환	01	1	1

[R-1]- [T1-L1]	시험 사례 설명	**마스터 모드에서 메모리 에러가 발생한 경우 에러 발생 및 Fail-Safe 상태로 전환하는지 시험한다.** ...
	선행 작업	* 시스템의 KEY 스위치를 RUN로, ROTARY 스위치를 8로 설정 * 시스템의 RST 버튼 선택 ...
	시험 입력	- 0x410001[0](**EXT_CON_REG_RUN**)=**0**, 0x410001[5:4](**EXT_CON_REG_ERR**)=**0**, 0x410001[7](**EXT_CON_REG_INI**)=**0**
	시험 기대값	- **ERR LED**: red, **LOCAL_CON_REG_FLT**(0x410000[6]) = 1, **BUS_RST**(0x480000[0]) = 1
	시험 절차	* CommTest2를 통해 다음 영역을 설정: 0xa02061(recv_global_run 관련 코드 영역) = 111 ...
	시험 결과	- **ERR LED**: red, **LOCAL_CON_REG_FLT**(0x410000[6]) = **1**, **BUS_RST**(0x480000[0]) = **1**
	결과	**Pass**
	이미지	

Copyright © 2019 Formal Works Inc. All Rights Reserved

4. 소프트웨어 시스템 시험

커버리지 예시 (절차서/보고서)

System Test : 초기화 기능 ST-1-1	
시험 항목	
ST-1-1-1-C1	통신 운용 소프트웨어는 전원 인가후 Hardware 설정, 타이머, 인터럽트 설정 …
ST-1-1-1-C2	통신 운용 소프트웨어는 전원 인가후 Hardware 설정, 타이머, 인터럽트 설정에서 오류가 발생하면, 오류를 보고하고, 초기화 …
ST-1-1-2-C1	통신운용 소프트웨어는 공유메모리(XC_DPM)의 모든 영역 초기화 완료 후, 정상 완료를 …
ST-1-1-2-C2	통신운용 소프트웨어는 공유메모리(XC_DPM)영역 초기화 도중 오류가 발생하면, …
ST-1-1-3-C1	…

커버리지					
	TC1	TC2	TC3	TC4	Coverage
ST-1-1-1-C1	-	Y	Y	Y	Covered
ST-1-1-1-C2	Y	-	-	-	Covered
ST-1-1-2-C1	-	-	Y	Y	Covered
ST-1-1-2-C2	-	Y	-	-	Covered
ST-1-1-3-C1	-	-	-	Y	Covered
결과	PASS	PASS	PASS	PASS	PASS
요약					
…					

Illustrative

시스템 시험 요약 (보고서)

시험 수행 결과						
시험 수행 결과 요약						
	성공율		전체 개수		통과 개수	
시험 사례	100%		34		34	
시험 항목	100%		63		63	
요구사항	100%				22	
수행 결과						
기능 상태	시험 항목	시험 사례	시험 수행	시험 성공	시험 실패	조치 완료
초기화 기능 [ST-1-1]	22	14	14	14	0	0
데이터 통신 기능 [ST-1-2]	24	12	12	12	0	0
자가진단 기능 [ST-1-5]	17	8	8	8	0	0
…	…	…	…	…	…	…
합계	**…**	**…**	**…**	**…**	**0**	**0**

Illustrative

Copyright © 2019 Formal Works Inc. All Rights Reserved

5. 시스템 시험의 수행 및 환경

- 임베디드 소프트웨어는 하드웨어와 밀접하게 연관되어 시험 환경의 구성이 어려움
- 분야 별로 다양한 특성을 가지므로 범용적인 환경 적용에 한계가 있음

임베디드 소프트웨어 시스템 시험의 특성 및 주요 이슈

하드웨어 의존성

- 분야/제품 별로 다양한 시험 환경 구성 필요
- 하드웨어 구성에 따른 입출력 제어의 어려움
- 실시간성으로 인한 입출력 제어의 어려움
- 소프트웨어와 시스템 요구사항 간의 연관성 등 분야/제품에 대한 높은 이해 필요

한정된 자원

- 시험 수행 성능 및 결과 기록 등의 문제
- 시험으로 인한 side effect 등 시험 영향 최소화 필요
- 자동화 등 일반적인 기법 적용이 어려움
- 시험 정보 관리 방안 필요

시험 환경 구성의 체계화

엄밀한 요구사항 확인

- 안전 중요 분야에 활용
  (인적 피해를 초래할 수 있는 안전 기능 등을 수행)
- 인증 또는 기술 표준 만족을 위해 체계적인 요구사항 명세서 (SRS) 작성 및 V&V 활동 필요
- 제품의 품질을 위한 높은 수준의 확인 및 검증을 요구

시험 관리의 체계화

Copyright © 2019 Formal Works Inc. All Rights Reserved

6. 요약

소프트웨어 시스템 시험 사례 연구 요약

요구사항 명세서

- ✓ Decision Table에 기반한 요구사항 명세를 기술하여 시험 가능성을 극대화 시킴
  - Completeness, Consistency, Correctness
- ✓ 시험 입력을 생성 가능하도록 명확한 인터페이스 요구사항 기술
- ✓ 기능 요구사항을 인터페이스 요구사항에 기반하여 명세

소프트웨어 시스템 시험

- ✓ 요구사항을 시험 가능한 시험항목으로 분할
- ✓ 각 상세 시험항목을 모두 커버하도록 사례 생성
  - 엄밀한 Requirement Coverage 측정
- ✓ 인터페이스 정의에 따른 입출력 조작 및 모니터링

Copyright © 2019 Formal Works Inc. All Rights Reserved

II. 가동원전 소프트웨어 V&V 사례 연구

현장설계변경(DCP)에 따른
소프트웨어 V&V 수행 방안

1. 설계 변경 소프트웨어 확인 및 검증

➢ IEEE Std. 1012에서는 소프트웨어 프로그램의 변경에 대하여 상세 활동을 입출력 산출물과 함께 기술

IEEE Std. 1012 소프트웨어 변경

➢ IEEE Std. 1012의 소프트웨어 변경 관련 주요 활동

- **소프트웨어 변경이 시스템이나 기존에 완료된 V&V 활동에 미치는 영향을 평가**
- 변경에 따른 영향에 대하여 V&V활동을 재수행하기 위한 계획을 수립
- 필요 시 변경 사항을 검증하기 위한 새로운 활동을 계획
- 설계 변경이 시스템 요건이나 기타 요건에 악영향을 주는 지 여부를 평가

➢ 문서화 요건

- 각 활동에 대한 보고서
- 개정된 확인 및 검증 계획
- 이상 상태 보고서 (Anomaly Report)

> ***<5.1.1 Activity: Management of the V&V effort>***...V&V management assesses each proposed change to the system and software, identifies the software requirements that are affected by the change, and plans V&V tasks to address the change. **For each proposed change, management assesses whether any new hazards or risks are introduced in the software or system development process, and identifies the impact of the change** on the assigned software integrity levels. ...Whenever necessary, the **V&V management determines whether a V&V task should be reperformed as a result of changes in the software program.**

Copyright © 2019 Formal Works Inc. All Rights Reserved

1. 설계 변경 소프트웨어 확인 및 검증

➢ IEEE Std. 1012에서 요구하고 있는 최소 활동은 SIL 4 등급에 대하여 전체 개발 단계의 검증을 고려함

IEEE Std. 1012 Table 2 - Minimum V&V tasks assigned to each SIL

➢ 개발 전 단계에 대하여 재검증이 고려되어야 함

Life cycle processes	Process: Acquisition (see 5.2)				Process: Supply (see 5.3)				Process: Development (see 5.4)																				Process: Operation (see 5.5)				Process: Maintenance (see 5.6)			
V&V activities	Activity: Acquisition support V&V (see 5.2.1)				Activity: Planning V&V (see 5.3.1)				Activity: Concept V&V (see 5.4.1)				Activity: Requirements V&V (see 5.4.2)				Activity: Design V&V (see 5.4.3)				Activity: Implementation V&V (see 5.4.4)				Activity: Test V&V (see 5.4.5)				Activity: Installation/ checkout V&V (see 5.4.6)				Activity: Operation V&V (see 5.5.1)				Activity: Maintenance V&V (see 5.6.1)			
Software integrity levels	Levels				Levels				Levels				Levels				Levels				Levels				Levels				Levels				Levels			
	4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1
Planning the interface between the V&V effort and supplier	X	X	X	X	X	X	X	X																																
Proposed/baseline change assessment									X	X	X		X	X	X		X	X	X		X	X	X		X	X	X		X	X	X		X	X	X		X	X	X	
Retirement assessment																																							X	X		
Risk analysis									X	X			X	X			X	X			X	X			X	X			X	X			X	X			X	X		

Copyright © 2019 Formal Works Inc. All Rights Reserved

1. 설계 변경 소프트웨어 확인 및 검증

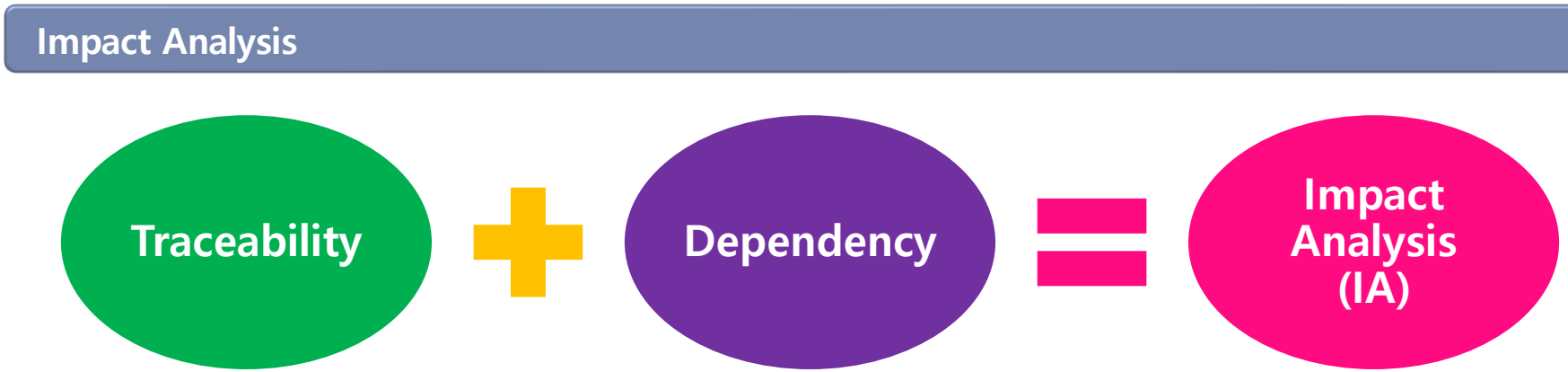
- 설계 변경 S/W의 체계적 검증 방안 수립 필요
- 인허가 적합성을 고려한 대응 체계 수립 필요

주요 활동

Copyright © 2019 Formal Works Inc. All Rights Reserved

2. 변경 영향 분석

➢ 변경 영향 분석(Change Impact Analysis)을 이용하여 설계 변경 부분에 따른 소프트웨어 검증 범위 도출



➢ Traceability: 요구사항, 설계, 코드, 시험들 사이의 관계

➢ Dependency: 모듈, 변수, 로직들 사이의 관계

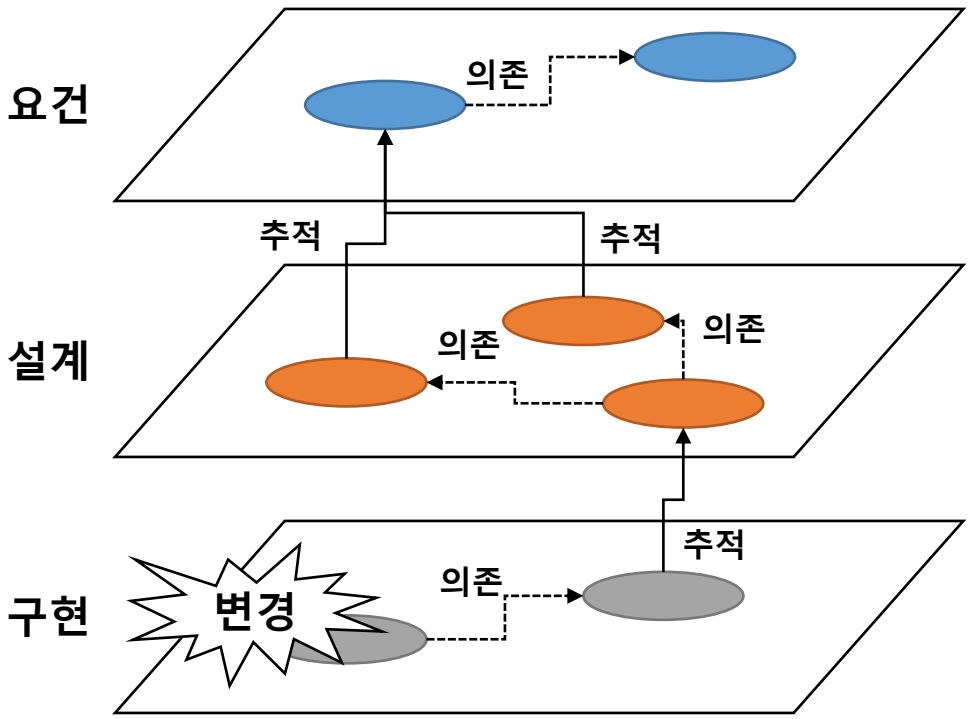
※ Impact Analysis를 위한 정적 코드 분석 및 동적 프로그램 분석이 존재하나, 전문가에 따른 비정형적 리뷰를 통한 활동도 사용됨

Copyright © 2019 Formal Works Inc. All Rights Reserved

2. 변경 영향 분석

- 의존성: 한 개발 단계 내에서 관련 부분을 도출
- 추적성: 개발 단계간의 관련 부분을 도출

변경에 따른 의존성 및 추적성 분석 예시



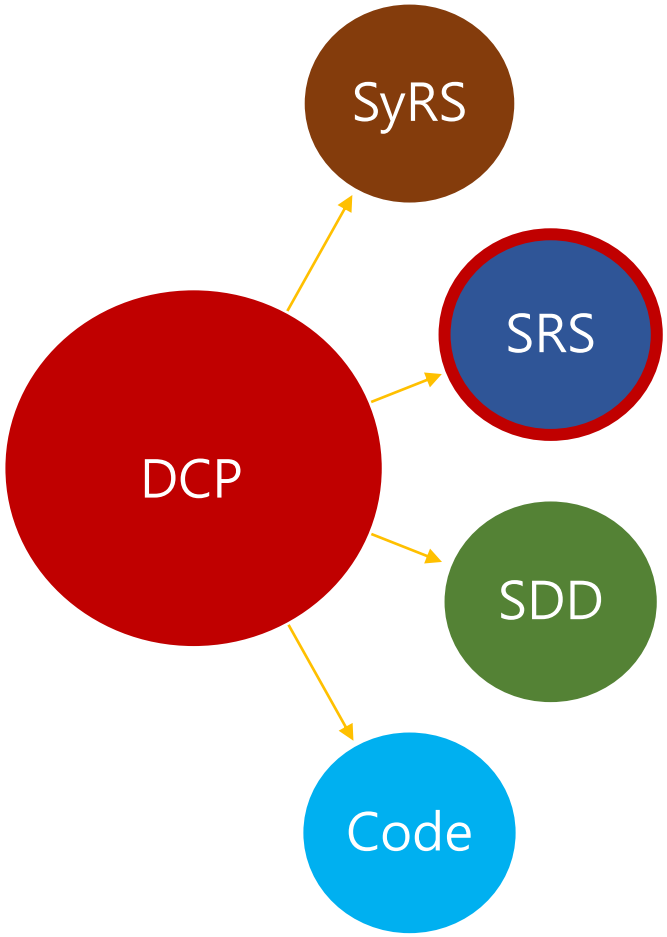
변경에 따른 의존성 및 추적성 분석

- **의존성에 따라서 단계 내 영향** 파악
- **추적성에 따라 단계 간 영향**을 파악
- 의존성 및 추적성을 **종합적으로 취합하여 영향 부분을 도출**
- **도출 영향 부분을 대상으로 확인 및 검증** 활동을 수행

Copyright © 2019 Formal Works Inc. All Rights Reserved

3. 변경 영향 분석 예시

SRS 영향 분석



...
7.7.3.1 Analog/Digital Inputs
R7731_5
Channel errors and the module error for each AI685 card within a LCC shall be connected to the EXMODERR Type Circuit for monitoring system health of the AI card at the MTP

R7731_9
Each LC shall monitor all DIs, hardwired to its cabinet, continuously at a CONTRM execution cycle time of less than or equal to one second(1 s)

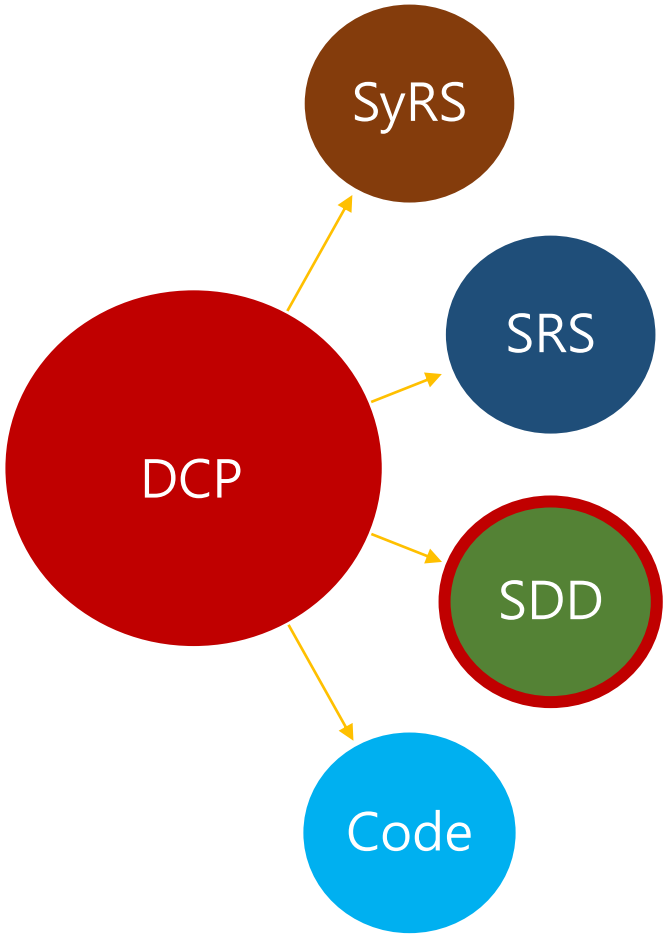
R7731_11
[Channel errors and the module error for each DI621 card within a LCC shall be connected to the EXMODERR Type Circuit for monitoring system health of the DI card at the MTP
...

Illustrative

Copyright © 2019 Formal Works Inc. All Rights Reserved

3. 변경 영향 분석 예시

SDD 영향 분석



Illustrative

…

2.4.9 Loop controller Feedback status and Alarm Outputs

The external sub-systems may further transmit LC feedback status and alarm outputs to other sub-systems such as …

…

5.2.5.7 Digital Output(DO) Module DO620 DS5257_3

Each DO620 slot position is defined on sheets 3 and 4 of the individual LCLDs

…

5.2.5.8 Analog Input(AI) Module AI685 DS5258_3

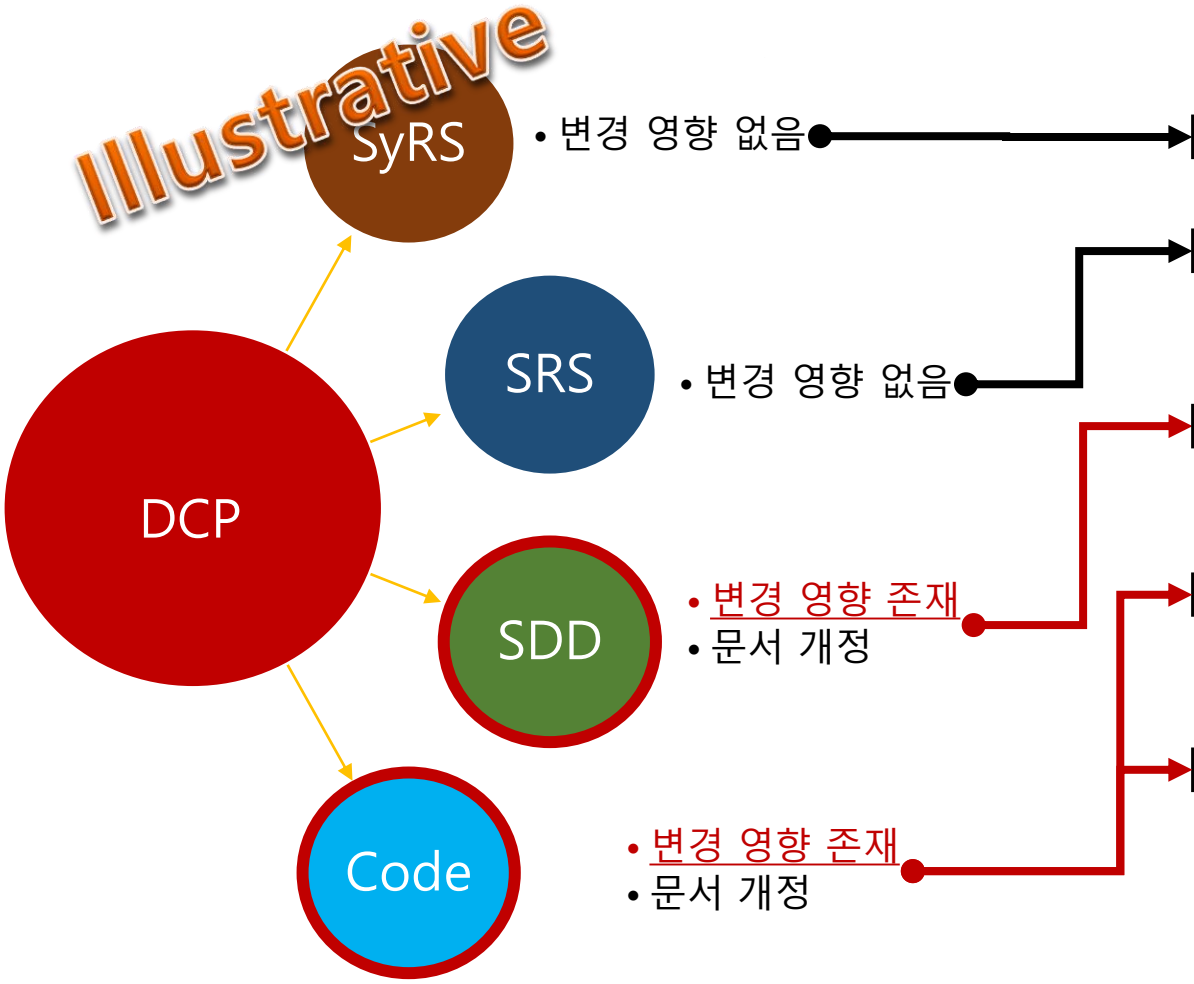
Each AI685 slot position is defined on sheets 3 and 4 of the individual LCLDs

…

Copyright © 2019 Formal Works Inc. All Rights Reserved

3. 변경 영향 분석 예시

변경 영향에 따른 문서 개정 예시



산출물	변경 전	변경 후
Concept Phase		
SyRS	Rev. 01	Rev. 01
Requirement Phase		
SRS	Rev. 01	Rev. 01
SRS V&V	Rev. 01	Rev. 01
Design Phase		
SDD	Rev. 01	**Rev. 02**
SDD V&V	Rev. 01	**Rev. 02**
Code Phase		
Code	Rev. 01	**Rev. 02**
Code V&V	Rev. 01	**Rev. 02**
Testing Phase		
Unit Test	Rev. 01	**Rev. 02**
Integration Test	Rev. 01	**Rev. 02**
System Test	Rev. 01	**Rev. 02**
…		

FORMALWORKS S/W Development & Verification
Copyright © 2019 Formal Works Inc. All Rights Reserved

4. 이슈

설계 변경 소프트웨어 확인 및 검증 이슈

기존 개발사에 의한 설계 변경

- 설계 원전 소프트웨어의 개정 과정과 동일한 절차 적용
- 일정 단축 및 효과적인 재수행에 대한 이슈
- 정확한 변경 영향에 대한 분석의 난이도
- 변경에 대한 부분 확인 + 불변경 부분에 대한 기능 유지 확인 중요

신규 개발사에 의한 설계 변경

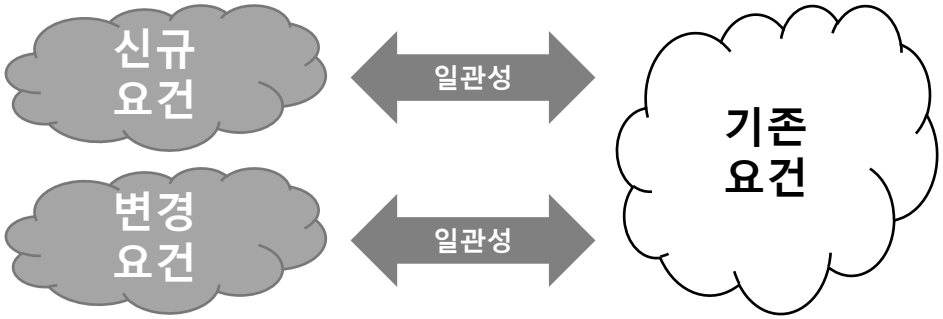
- 기존 설계 문서의 유무와 품질 이슈
- 기존 V&V 문서의 활용 가능성 여부 이슈
- 변경 영향에 대한 정확한 분석 이슈
- 재시험 범위 산정의 방법론 이슈

Copyright © 2019 Formal Works Inc. All Rights Reserved

4. 이슈

설계 변경 소프트웨어 확인 및 검증 이슈

- 기존 설계 문서의 유무와 품질 이슈
  - 설계 문서가 존재하지 않거나 설계 문서의 품질이 충분하지 않다면?
  - 일관성 문제 및 문서화 범위



- 기존 V&V 문서의 활용 가능성 여부 이슈 / 재시험 범위 산정의 방법론 이슈
  - 많은 경우 기존 V&V 문서에 대한 접근이 제한됨
  - V&V 세부 결과를 알 수 없을 때 어떤 범위로 어떻게 검증할 것인가?
  - **시험 사례의 재사용 또는 Regression Test 문제**

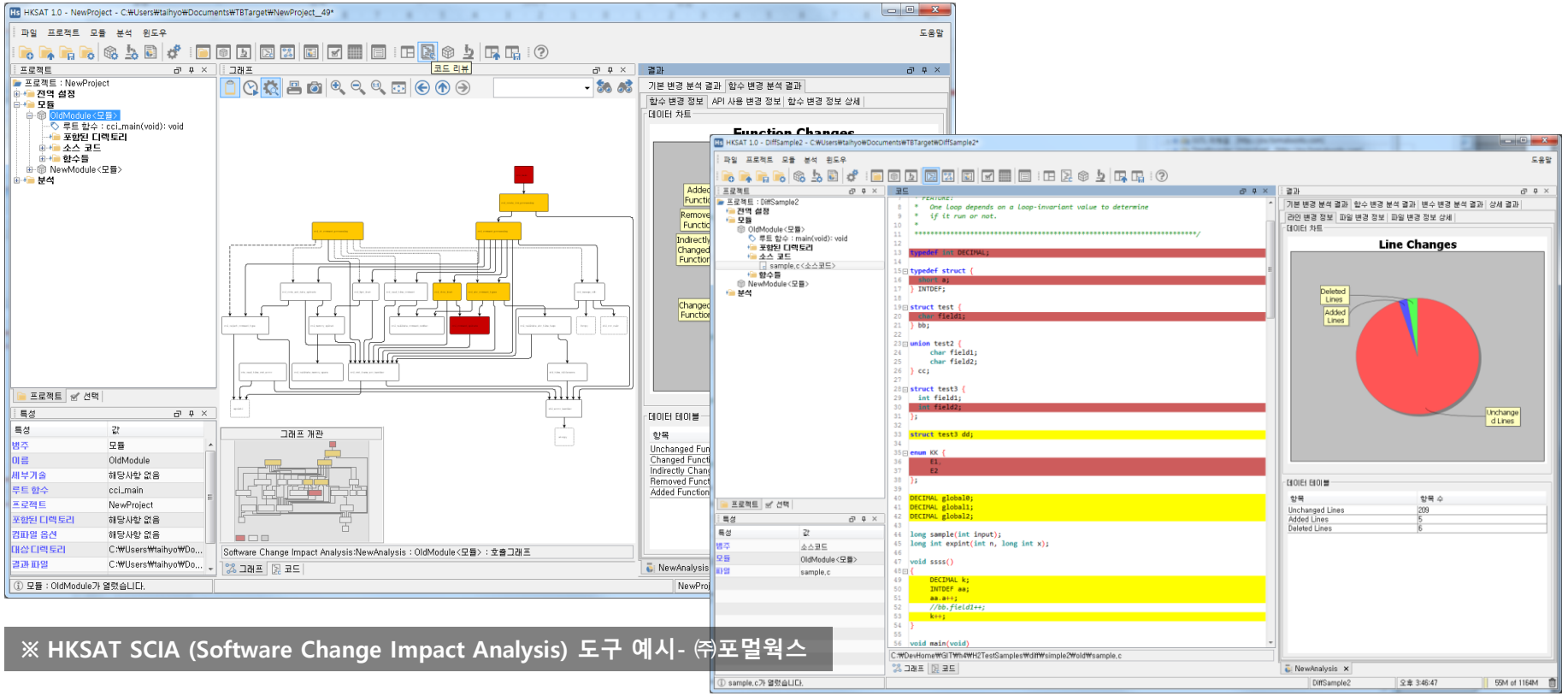
Copyright © 2019 Formal Works Inc. All Rights Reserved

4. 이슈

설계 변경 소프트웨어 확인 및 검증 이슈

➢ 변경 영향에 대한 정확한 분석 이슈

- 직접적인 변경 부분 뿐 아니라 간접적인 영향도 모두 파악 필요
  - ❖ Function Call, Pointer, Global Variable, …



※ HKSAT SCIA (Software Change Impact Analysis) 도구 예시- ㈜포멀웍스

Copyright © 2019 Formal Works Inc. All Rights Reserved

감사합니다.

taihyo.kim@formalworks.com
http://www.formalworks.com

Copyright © 2019 Formal Works Inc. All Rights Reserved