원전 소프트웨어 사이버보안과 안전

SW 안전 국제 컨퍼런스 2016

김태효

taihyo.kim@formalworks.com

주식회사 포멀웍스

2016.11.29

목차

I. 원전 사이버보안 활동 배경

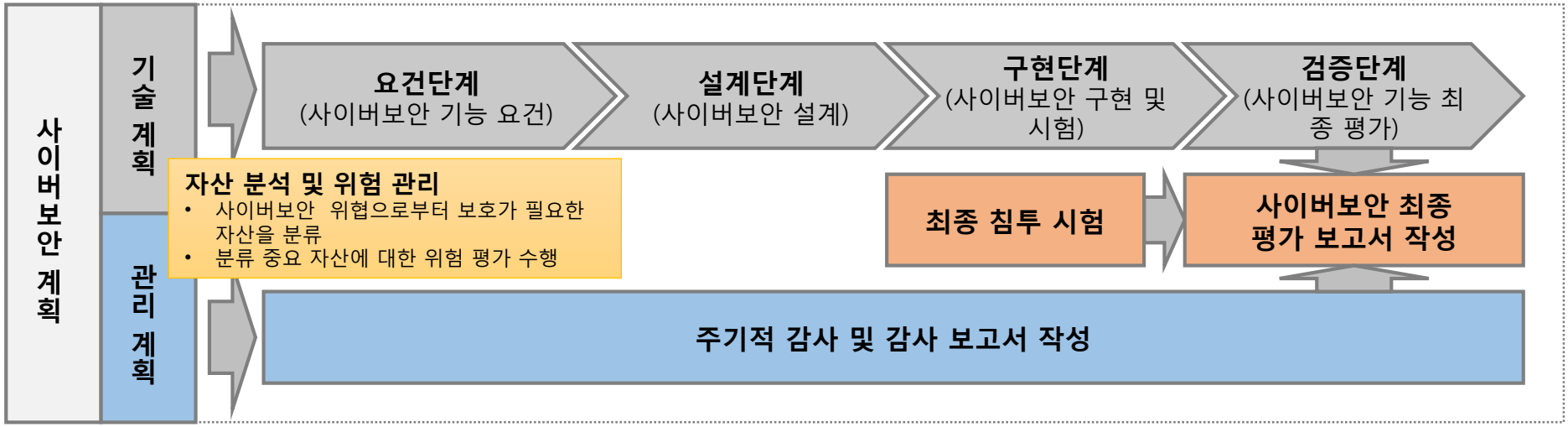
원전 사이버보안 초기 적용 사례

1. 초기 사이버보안 활동 개요

- USNRC R.G. 1.152 Rev02 기반 초기 PLC 제어기기 사이버보안 활동 수행 (2009년~)
- **초기 사이버보안 활동 수행 경험 및 현재 방법론 수립의 동기 공유**

초기 사이버보안 활동 요약

- USNRC R.G. 1.152 Rev02의 사이버보안 요건을 만족하기 위하여 NIST SP 특별 보고서 등을 참고하여 활동 계획을 수립



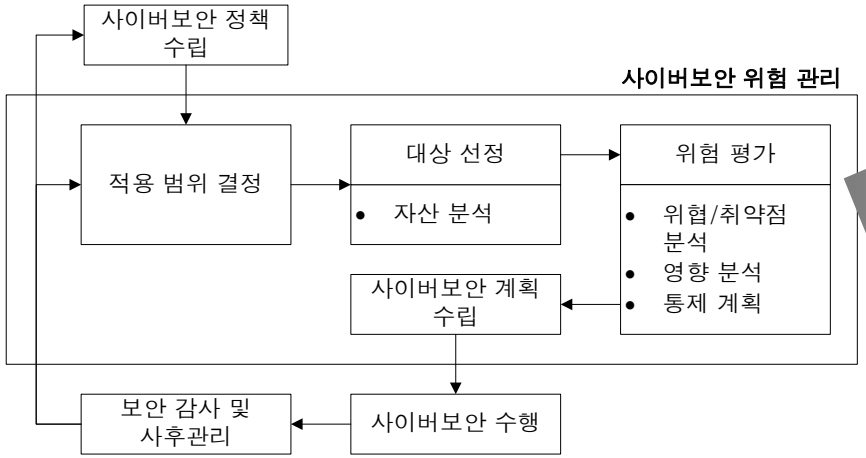
사이버보안 기술 계획 수행
일반 기능요건과 동일한 방법으로 개발 진행

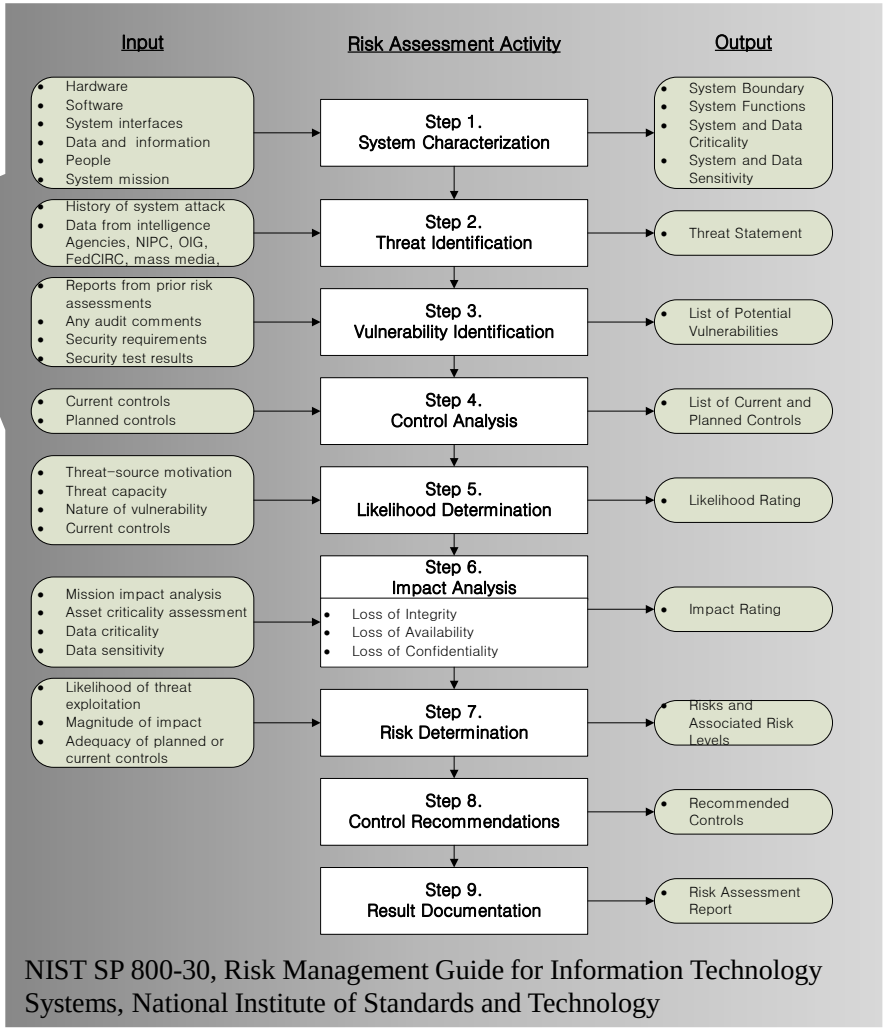
사이버보안 관리 계획 수행
주기적 감사를 수행하여 감사 보고서 작성

사이버보안 최종 평가
기술 계획: 단계 별 검증보고서 평가
관리 계획: 감사 결과 평가
최종 침투 시험: 독립 침투 시험

2. 원전 사이버보안 위험 관리 프로그램

사이버보안 위험 관리 단계





NIST SP 800-30, Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology

❖ **적용 범위**
- 사이버보안 활동의 적용 대상 정의

❖ **대상 선정 / 자산 분석**
- 사이버보안 대상이 되는 정보 자산을 파악

❖ **보안 위험 평가**
- 정보 자산에 영향을 줄 수 있는 위협과 취약점을 파악

❖ **사이버보안 계획의 수립**
- 통제 계획을 바탕으로 하여 계획을 수립

3. 사이버보안 위험 평가 결과

관리적 대응 방안 필요 항목

➢ 각 자산 별 필요 관리적 대응 조치 도출

➢ 관리적 계획 수립
- 개인 PC 통제 계획
- 네트워크 통제 계획
- 데이터 백업 통제 계획
- 문서 통제 계획
- 보안 구역 및 사무실 통제 계획
- 서버 운용 통제 계획
- 인력 통제 계획
- 통신 통제 계획
- …

➢ 이후 주기적인 사이버보안 감사를 통하여 관리적 계획이 유지되는 지 평가

기술적 대응 방안 필요 항목

➢ 각 자산 별 필요 기술적 대응 조치 도출

➢ 기술적 대응 필요 항목 도출
- PLC 제어기기 모듈의 해킹/크래킹에 의한 파괴
- PLC 제어기기 모듈에 대한 침입
- PLC 제어기기 모듈에 대한 시스템 공격 (DDoS)
- PLC 제어기기 모듈의 Hijacking
- PLC 제어기기 모듈의 악의적인 위/변조
- PLC 제어기기 모듈에 올바르지 않은 데이터 입력
- PLC 제어기기 모듈에 대한 비인가 접근
- …

➢ **필요 설계 반영 사항 도출 후 설계 반영**
- E.g. 작성한 응용 프로그램 파일의 변경 여부를 확인 등

4. 최종 사이버보안 평가

사이버보안 침투 시험 구성 및 결과

구분	정의	위협 행위자	공격목표	예상피해
외부침투	PLC 제어기기에 대한 정보를 가지고 있지 않은 공격자에 의한 침투시도	PLC 제어기기에 대한 정보를 알지 못하는 악성코드 작성 및 배포자	정보수집	PLC 제어기기 및 Eng. SW의 구조 및 구성 정보에 대한 유출
내부침투	PLC 제어기기에 대한 운영경험을 가지고 있거나 인터넷 등을 통해 PLC 제어기기 매뉴얼 및 Eng. SW 등을 입수하여 PLC 제어기기의 구조 및 운영관련 정보를 습득한 공격자에 의한 침투시도	PLC 제어기기에 대한 운영 기술을 보유하고 있는 악성코드 작성 및 배포자	원자로 안전계통 마비	PLC 제어기기 배치 후 이상 동작 / 원자로 안전 계통 긴급상황 발생
Stuxnet 유사침투	Eng. SW모듈변경을 통해 PLC에 대한 접근을 시도하는 형태의 Stuxnet 과 유사한 방법에 의한 침투시도			

➢ **초기 사이버보안 대응 노력에도 불구하고 최종 단계에서 1) 미대응 취약점, 2) 대응 수준 미흡 취약점 발견!!!**

5. 사이버보안 체계 재수립

초기 사이버보안 적용 경험과 개선 방안

체계적인 사이버보안 방법론

- 각 활동 단계 별로 필요한 세부 활동 및 산출물에 대한 참고 문헌이 부재
  - ✓ RG 5.71 등 발행 이전, 참고 문헌에 예시 부족
- 일반 사이버보안 컨설팅의 산출물을 원전 소프트웨어 인허가에 활용 한계

➔ **새로운 원전 사이버보안 방법론 수립**

체계적인 사이버보안 위험 평가 기법

- 모의 해커의 수준에 따라서 침투 시험 결과 상이
- 취약점 분석 커버리지 수준에 대한 의구심
  - ✓ Completeness?
- 모의 해커는 상세 침투 방법 및 시험 항목 등을 비공개

➔ **체계적이고 문서화가 가능한 사이버보안 위험 평가 방법론 (Attack Tree 기반) 수립**

초기 침투 시험

- 문서 기반 사이버보안 평가는 한계를 가짐
  - ✓ 고급 침투 기법에 대한 지식 부족, 대응 수준에 대한 적절성 결정이 어려움
- 최종 단계의 침투 시험 실패 시 과도한 비용 소요
  - ✓ PLC 제어기기의 경우 최종 평가 개선 사항 반영을 위하여 1년 이상의 설계 변경 및 V&V 활동이 추가로 소요됨

➔ **초기 예비 사이버보안 침투 시험 수행 후 통제 항목 도출**

II. 원전 제어시스템 사이버보안 평가 프로그램

공격 트리 기반 체계적인 사이버보안 평가 프레임워크

1. 개요

원전 사이버보안 대응 체계 구축 활동 및 특징

수행 대상

- 안전등급 사용 단위 기기 (PLC 제어기기와 개발 도구, Industrial PC 및 QNX OS 등) 및 계통
- 안전 계통과 연결성을 갖는 비안전 계통

주요 수행 활동

- 잠재 취약점에 대한 점검 (침투 시험, 문서기반의 평가 포함)
- 취약점에 따른 원전의 위협 평가
- 모의 침투를 통한 실제 침투 시나리오 가능성 평가
- 원전에 대한 실재 위협을 완화하기 위한 대응 방안 도출 및 구현

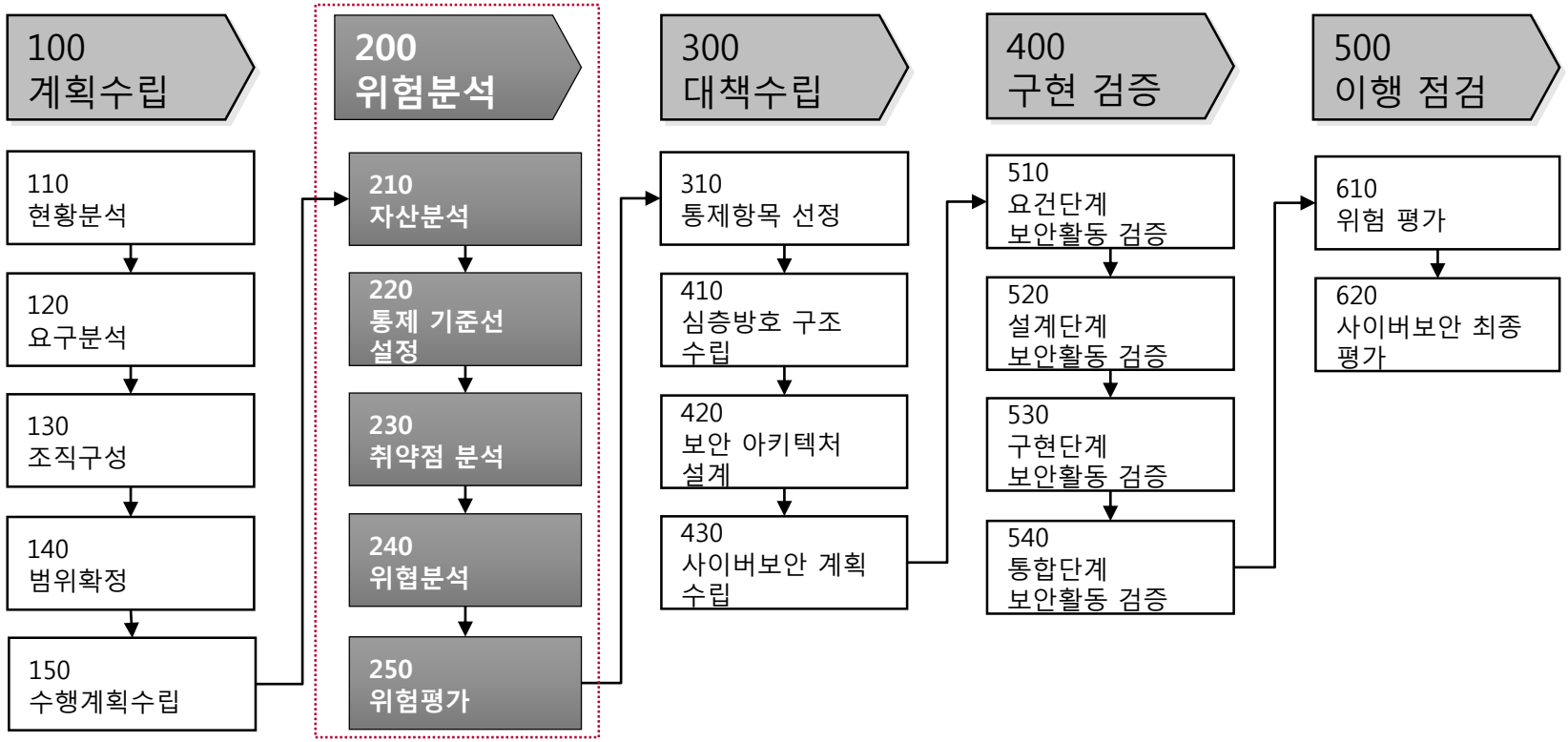
특장점

- 기술 표준 및 현재 알려진 취약점에 대한 점검 완료
- 보안 전문가의 모의 침투를 통한 잠재 취약점 추가 점검
- 취약점에 대한 원전 위협 여부 평가 체계 구축 및 체계적인 운용 방안 개발

2. 원전 사이버보안 방법론 개요

- 국내 원전 사이버보안 활동을 위한 체계적인 방법론을 수립
- 포멀웍스-안랩의 원자력 제어 시스템 사이버보안 평가 방법론(NUSAF) 중 위험분석 단계를 적용하여 사이버보안 평가를 수행

NUSAF™ 방법론 수행 활동 개요



※ NUSAF™(Nuclear Security Assessment Framework) : 포멀웍스-안랩 제어 시스템 사이버 보안성 평가 방법론 (FASAF™ : Formalworks-Ahnlab Security Assessment Framework) 를 원자력 제어 시스템 분야에 적합하게 수정한 평가 방법론

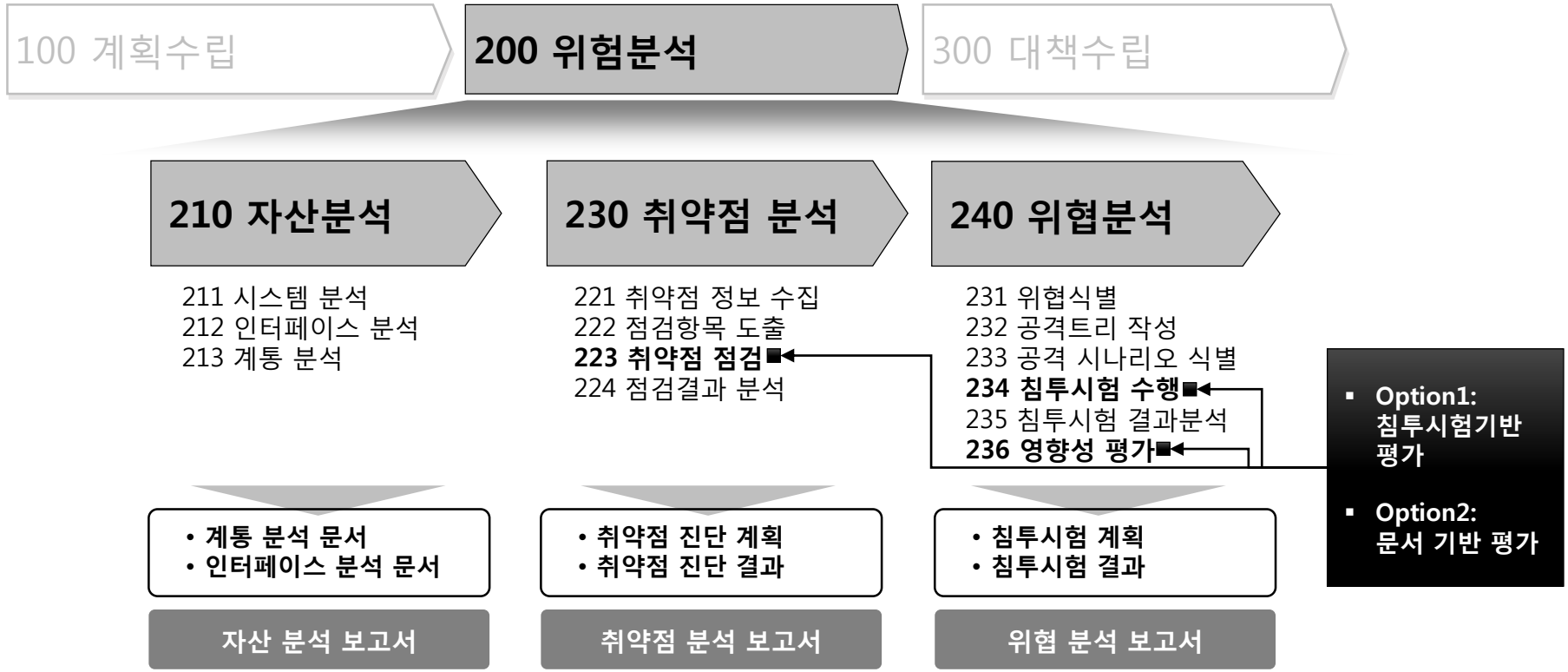
3. 사이버보안 위험 분석

➢ 원전 사이버보안 활동에서는 보안 위험을 체계적으로 관리하기 위하여

NUSAF 방법론 기반 보안 위험 분석(Security Risk Analysis)을 수행

사이버보안 활동 방법론의 위험 분석

➢ 각 단위 장비 및 계통에 대하여 1)자산 분석, 2)취약점 분석, 3)위협 분석을 수행



4. 사이버보안 위험 분석 절차 및 운용

원전 사이버보안 위험 분석

1. 자산 분석

- 대상의 개요, 주요기능 및 구성, 영향도, 의존성 등을 분석
- 대상의 네트워크 인터페이스 및 영향도, 의존성 등을 분석
- 대상 계통에 대한 특성, 연계 정보 등을 분석

2. 취약점 분석

- 대상과 관련된 취약점 정보를 수집
- 대상 별 취약점 점검 항목을 도출
- 도출된 **점검항목 및 침투 시험 기반의 취약점 평가**

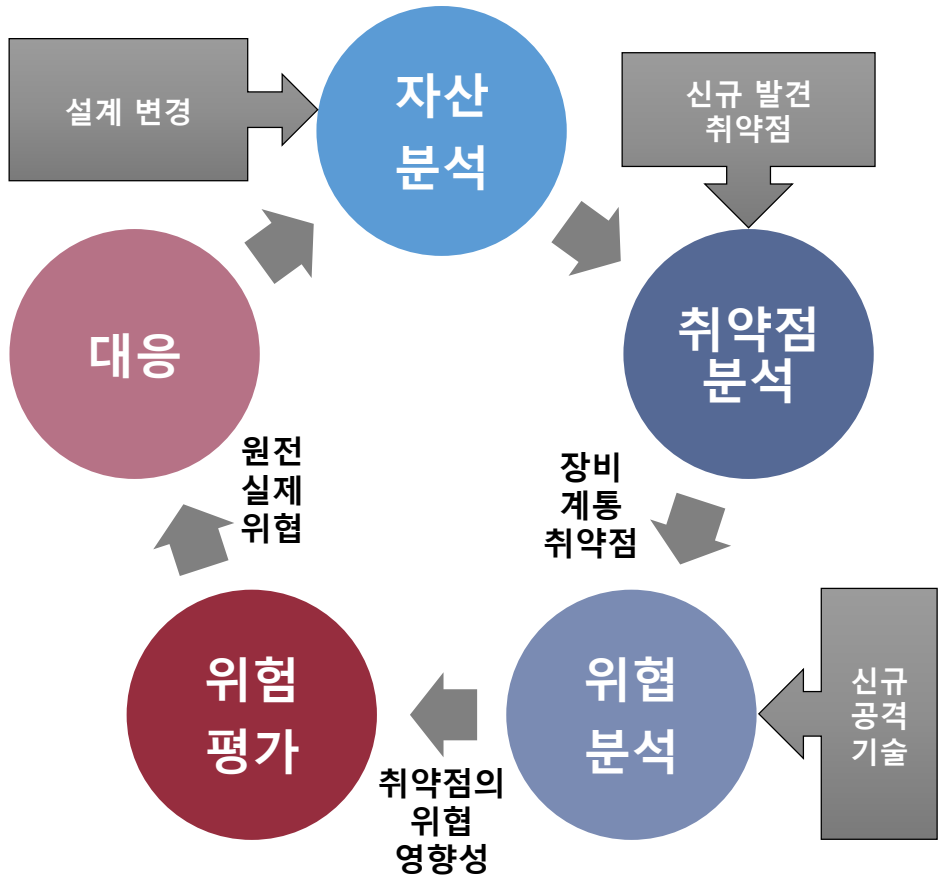
3. 위협 분석

- 대상에 대해 알려진 사이버보안 위협을 식별
- 식별된 위협을 기반으로 공격 트리(Attack Tree) 작성
- 작성된 공격 트리를 기반으로 공격 시나리오를 식별
- **작성된 시나리오를 기반으로 모의 침투를 수행**

4. 위험 평가

- 발견 취약점 및 성공 공격 시나리오에 대하여 **원전에 대한 실제 위협 가능성 평가**
- 각 위협에 대한 영향도 및 심각도 평가

사이버보안 위험 분석 체계 운용

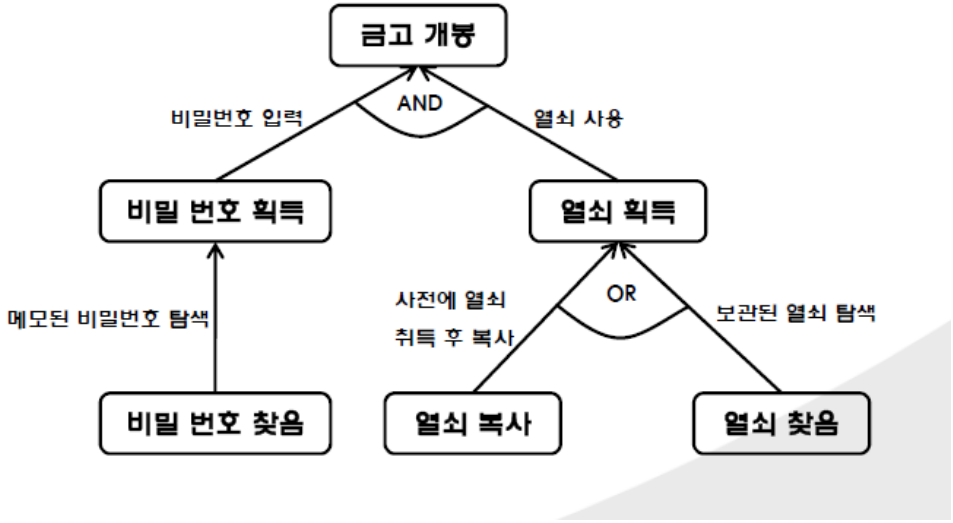


5. 사이버보안 위험 분석 예시

A. 공격 트리 기반 침투 시험

※ Attack Tree

- 시스템에 대한 공격에 대하여 목표에 도달하기 위한 행위들을 트리 형태로 가시화 한 형태
- 하나의 루트 노드와 자식 노드로 구성
- 최하위 노드로부터 루트 노드까지의 하나의 경로의 조건을 만족할 경우 공격이 성사됨

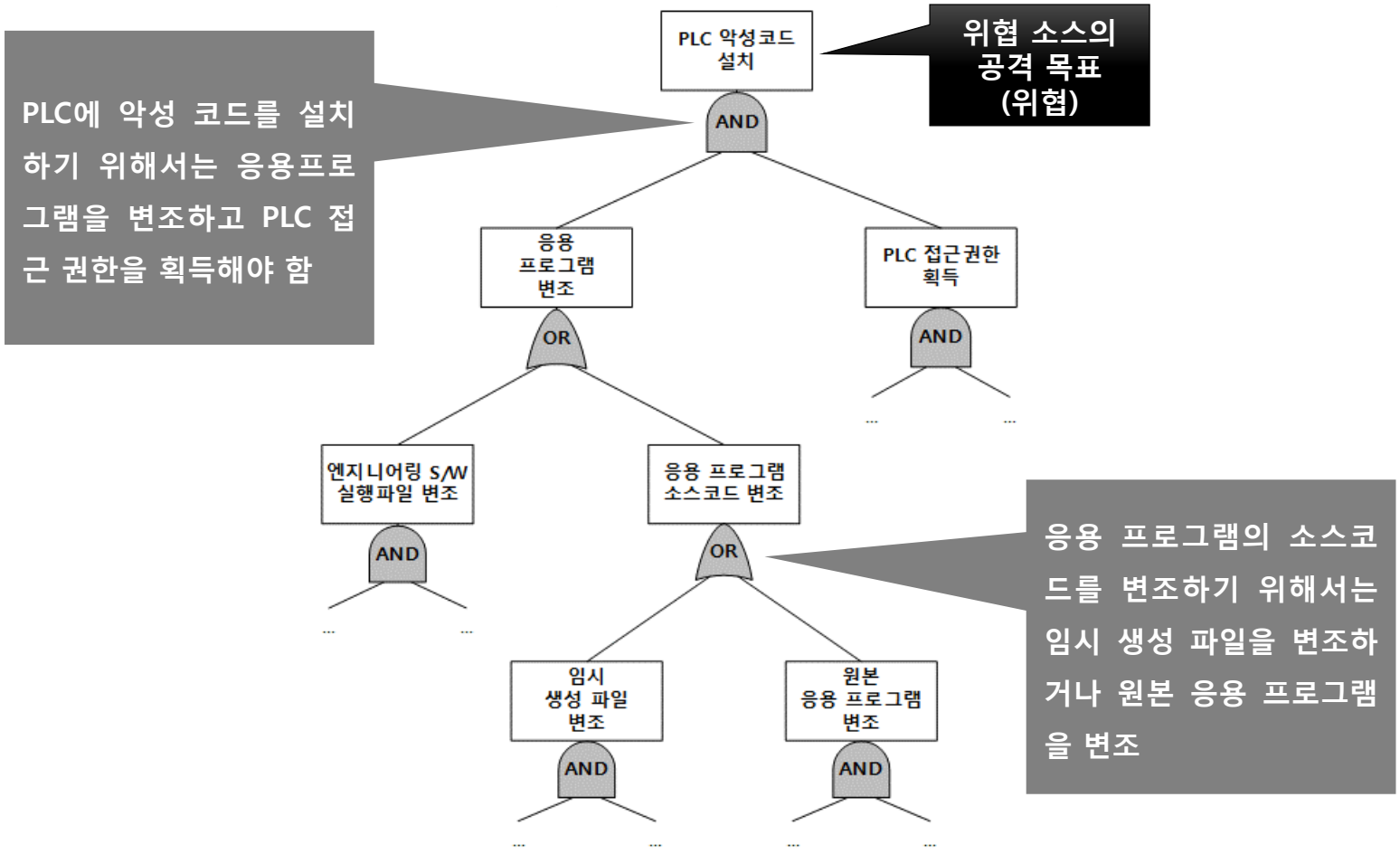


- 각 노드의 하위 간선(edge)은 노드의 조건을 만족하기 위한 행위를 명시
  - AND-decomposition : 하위 간선의 명시된 동작이 모두 행해져야 상위 노드 의 조건을 만족
  - OR-decomposition : 하위 간선의 명시된 동작 중 하나가 행해지면 상위 노드의 조건을 만족

5. 사이버보안 위험 분석 예시

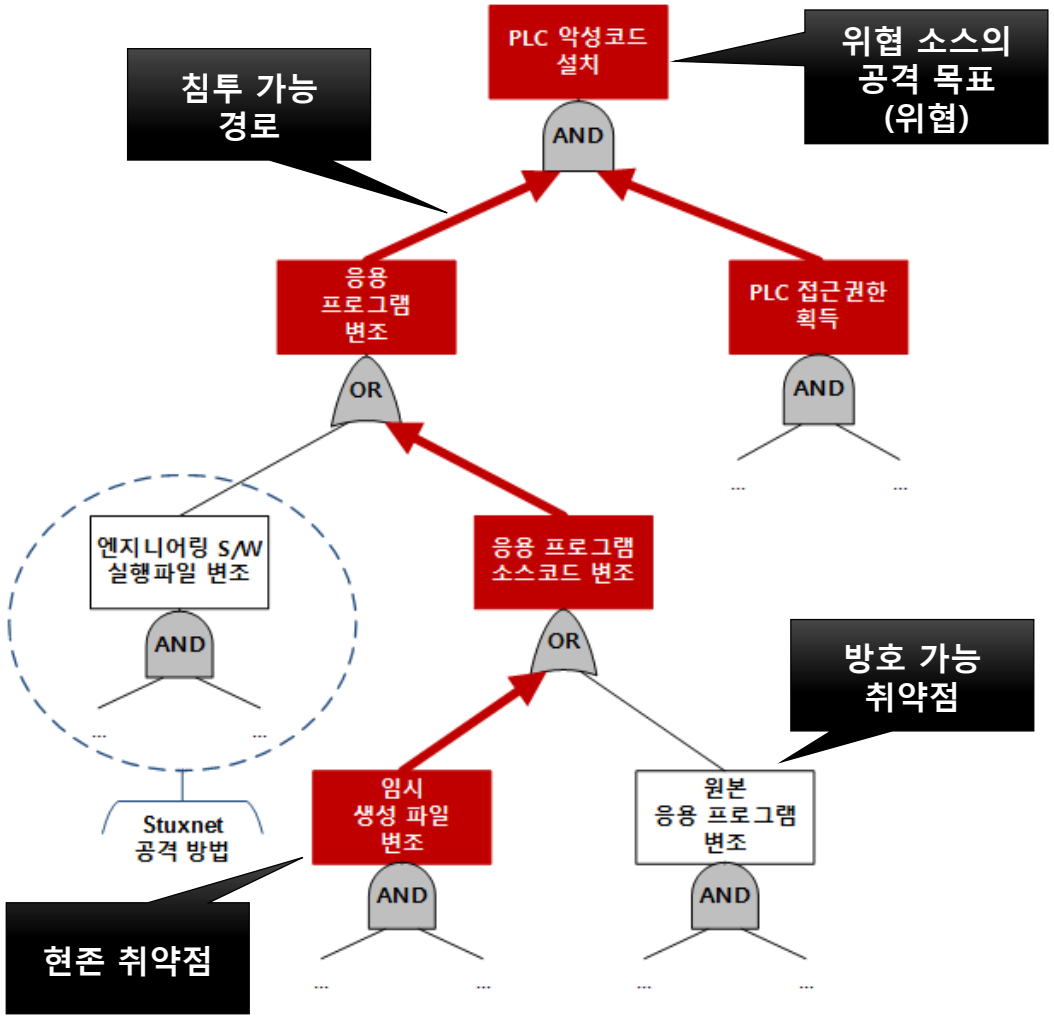
B. PLC 제어기기 공격 트리 예시

➢ 점검항목을 기반으로 공격 트리를 통해 대상 시스템에 대한 공격 시나리오를 표현



5. 사이버보안 위험 분석 예시

C. PLC 제어기기 악성 코드 설치에 대한 취약점의 위협 분석 예시



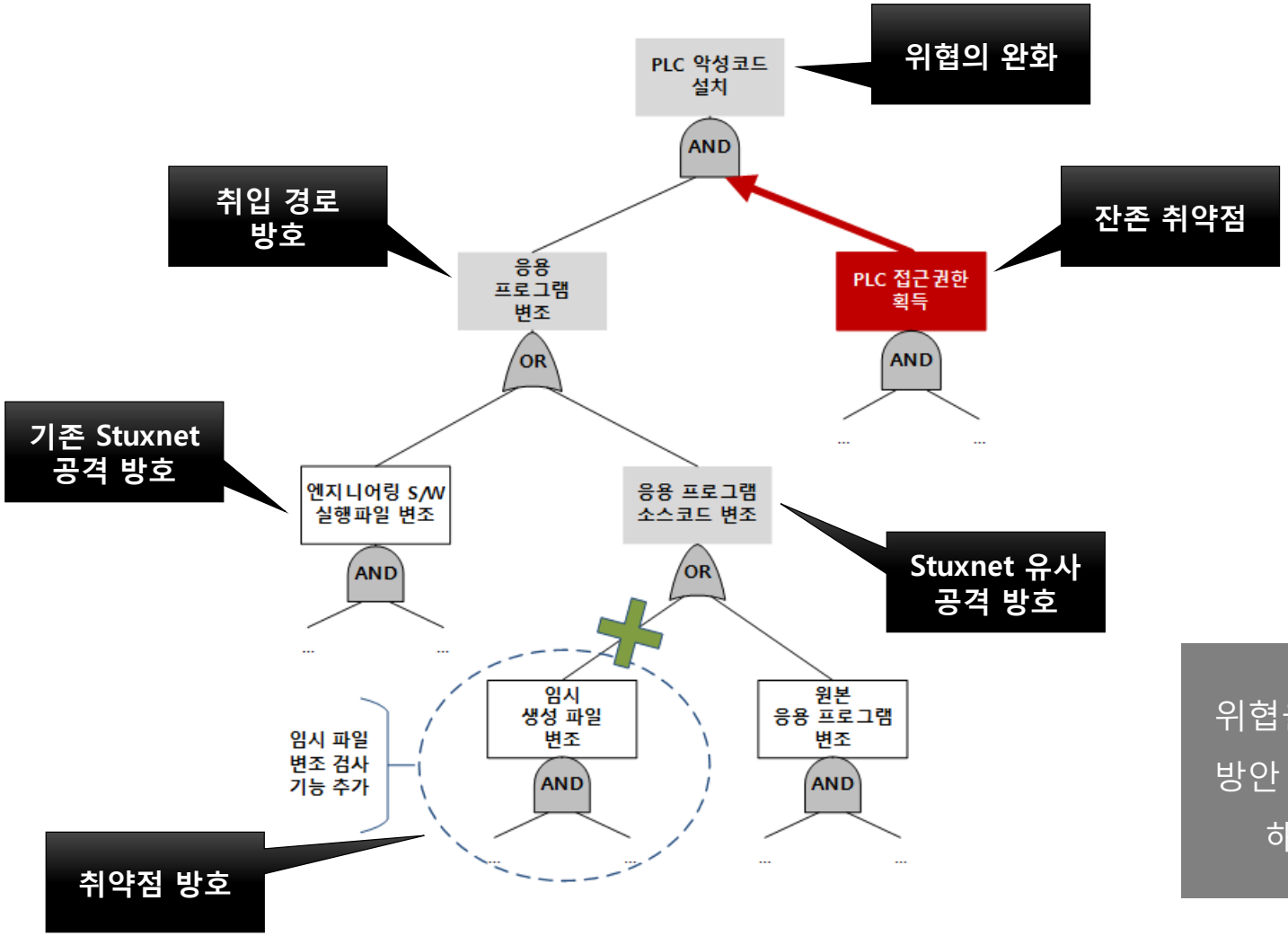
구분	정의	위협 행위자	공격 목표	예상 피해
외부 침투	원전 정보를 가지고 있지 않은 공격자에 의한 침투시도	악성코드 작성 및 배포자	정보 수집	원전 구조 및 구성 정보에 대한 유출
내부 침투	운영경험을 가지고 있거나 구조 및 운영관련 정보를 습득한 공격자에 의한 침투시도	운영 기술을 보유하고 있는 악성코드 작성 및 배포자	원자로 안전계통 마비	운영 후 이상 동작 / 원자로 안전 계통 긴급상황 발생
Stuxnet 유사침투	최신 공격 기술을 이용한 자동화된 웜 바이러스			

※ *예시의 평가 결과는 취약점들을 이용하여 악성 코드를 설치 오동작을 일으킬 수 있는* ***위협이 존재함 (공격 목표 달성 = 원전에 대한 실재 위협)***

※ ***침투 가능 경로의 취약점을 보완 대응****하여 위협의 해소 및 완화 필요*

5. 사이버보안 위험 분석 예시

D. 체계적인 사이버보안 취약점 방호 예시



위협을 해결할 수 있는 방안 중 가장 효율적인 해결 방안 도출!

6. 사이버보안 위협의 대응

- 모의 침투 시험의 결과를 통하여 추가 설계 취약 사항 발견
- 신규 취약점에 대한 대응 방안 수립 및 설계 반영

PLC 대응 방안의 반영 예시

모의 침투 시험을 통하여 보완 필요 개선 과제 도출

Eng. SW 관련 취약점 사항	PLC 관련 취약점 사항

개선 과제에 따라 대응 방안 도출 및 반영

Eng. SW 관련 보안 설계 반영	PLC 관련 보안 설계 반영

신규 취약점 대응 방안 적용

- 원전 사이버 보안은 실재 위협에 대한 취약점을 중심으로 대응
  - 실재 위협 관련 취약점
    - ❖ 각 공격 경로가 공격 목표에 도달 불가능 하도록 조치
    - ❖ 여러 개의 대응 방안이 가능한 경우 효과 적인 기술을 적용
  - 비위협 취약점
    - ❖ 장기적 관점에서 개선 과제 도출
    - ❖ 필요한 경우 가능성 고려 추가 대응
    - ❖ 성능 또는 안전 기능 영향성을 고려하여 대응 여부 결정
- 잔존 취약점의 경우 관리적 방법과 연계하여 방호

7. 위협 모델 기반 사이버보안 대응 체계 특징

➢ **체계적인 위협 평가 체계가 없다면**

취약점 = 위협

➢ **취약점이 위협과 관련 되는지 여부에 대한 평가 불가**

- 몇 개 발견? 몇 개 수정? 몇 개 대응?
- 일반 IT의 프로그램 Patch : 정말 필요한 Patch 일까?

발견된 취약점이 수정되면 안전한가?

➢ **단순 취약점 분석으로는 향후 취약점 발견 시 이에 대한 보안 평가가 비효율적임**

Attack Tree 기반 사이버보안 대응 체계

7. 위협 모델 기반 사이버보안 대응 체계 특징

사이버보안 상시 대응 체계

➢ **원전 사이버보안 활동은 기본적 평가 이외에 상시 신규 취약점 위험 평가 체계를 구축함**

➢ **신규 취약점 발견 시**

- 공격 목표 달성 여부 상시 확인
- **가동 원전에 활용 가능**

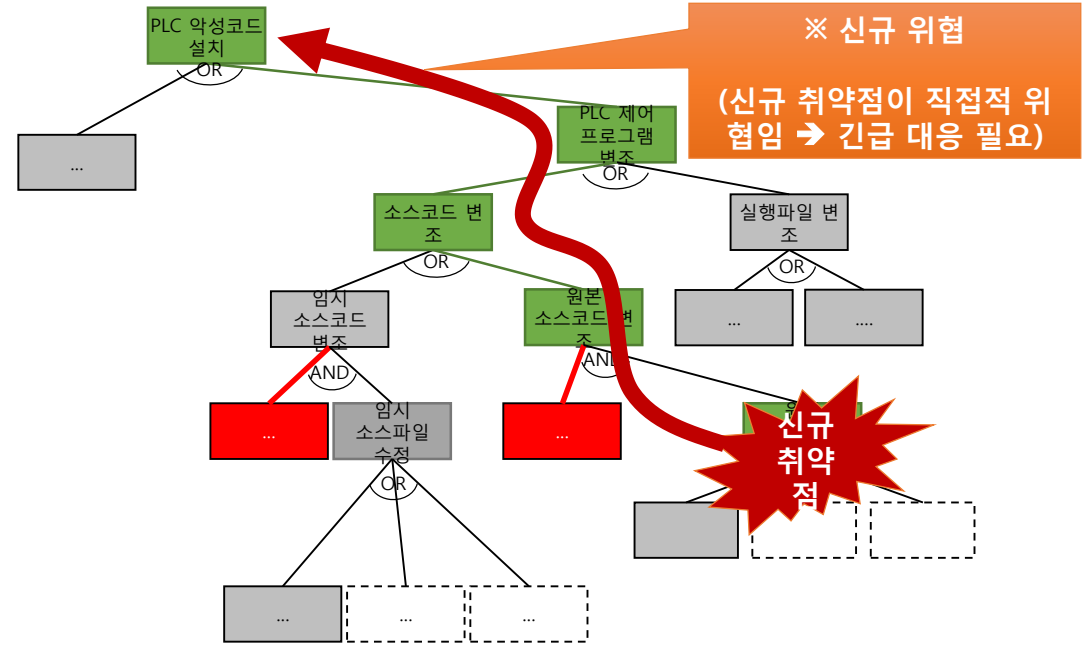
➢ **직접적 위협 ➔ 긴급 대응**

- 다음 유지 보수 기간에 즉시 반영

➢ **비위협 ➔ 장기 대응**

- 우선 순위 기반의 효과적 대응 적용 (장기 계획 수립)

신규 취약점 발견 시 영향 가능성 평가 예시



체계적인 원전 사이버보안 위험 평가 방법론

III. 원전 소프트웨어 개발과 V&V

소프트웨어 시스템 시험의
요구사항 커버리지 적용 사례

1. 사이버보안 위협의 대응

사이버보안 침투 시험 결과의 대응 예시

[SRS-xxx] [ST-xxx]	PLC 엔지니어링 도구는 프로젝트를 구성하는 파일을 읽어 만든 해쉬 값과 프로젝트 저장 시에 생성된 해쉬 값을 비교하여 프로젝트 파일의 위변조 여부를 판단한다.	
	Case 1	해쉬 값이 일치
	Case 2	해쉬 값이 불일치
	Case 3	해쉬 값을 비교 불가
	….	…

사이버보안 침투 시험

모의 해킹의 결과 단순한 해쉬 값을 통하여 위변조 여부를 파악하고 있는 것이 노출되어 해커가 위변조 후 해쉬 값도 함께 변조

➔ 복잡하고 해쉬 값 생성 알고리즘을 사용하여 방호

➔ 사이버보안 요건이 존재하나 미흡한 대응 사례

추가적인 보안 요구사항 또는 요구사항 변경으로 인하여 설계 변경 사례 존재

모의 해킹의 결과 프로젝트 파일 뿐 아니라 임시로 생성되는 파일의 위변조를 통하여 침입이 가능함

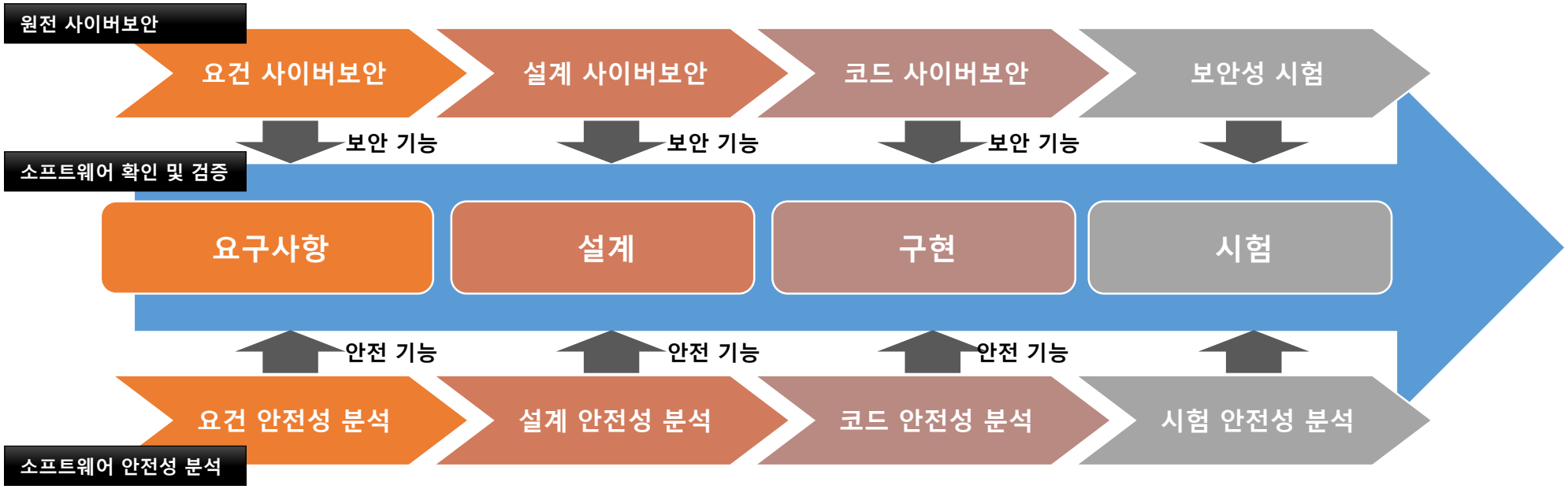
➔ 내부적으로 생성되는 임시파일의 위변조 검사 기능이 필요

➔ 추가 사이버보안 요건 발생 사례

2. 원전 설계·검증 활동의 구성 및 통합

원전 소프트웨어 개발

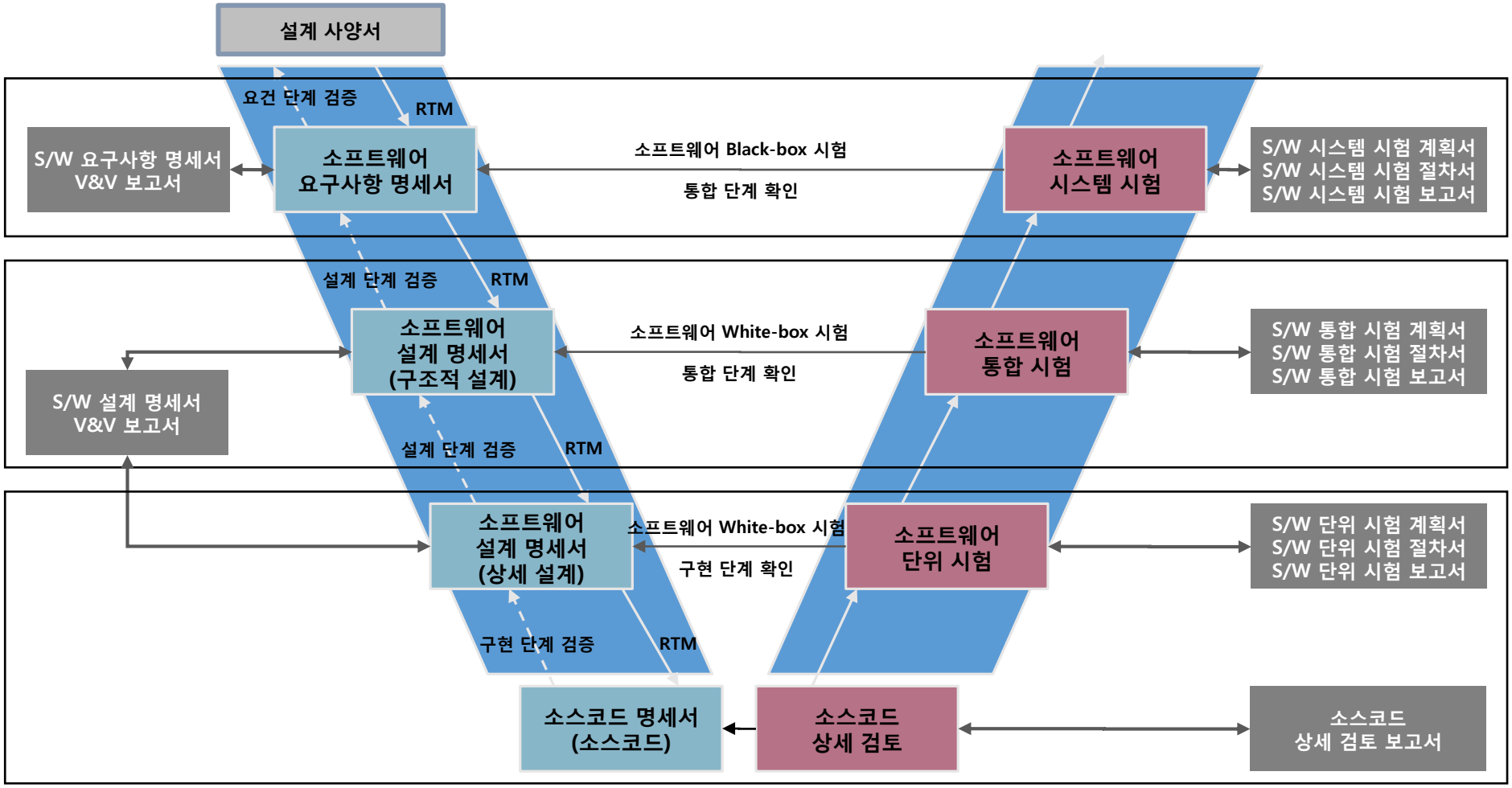
- 소프트웨어 안전을 중심으로 사이버보안성도 동시에 확보해야 함
  - 안전성분석: IEEE Std. 1228
  - 사이버보안: USNRC R.G. 1.152 Rev02 ➔ RG 1.152 Rev03(SDOE) & RG 5.71(Cybersecurity)
- 소프트웨어 품질을 확보하기 위하여 단계별 확인 및 검증을 수행
  - 소프트웨어 확인 및 검증: IEEE Std. 1012
  - 소프트웨어 개발 생명 주기: IEEE Std. 1074



3. 원전 소프트웨어 V&V 개요

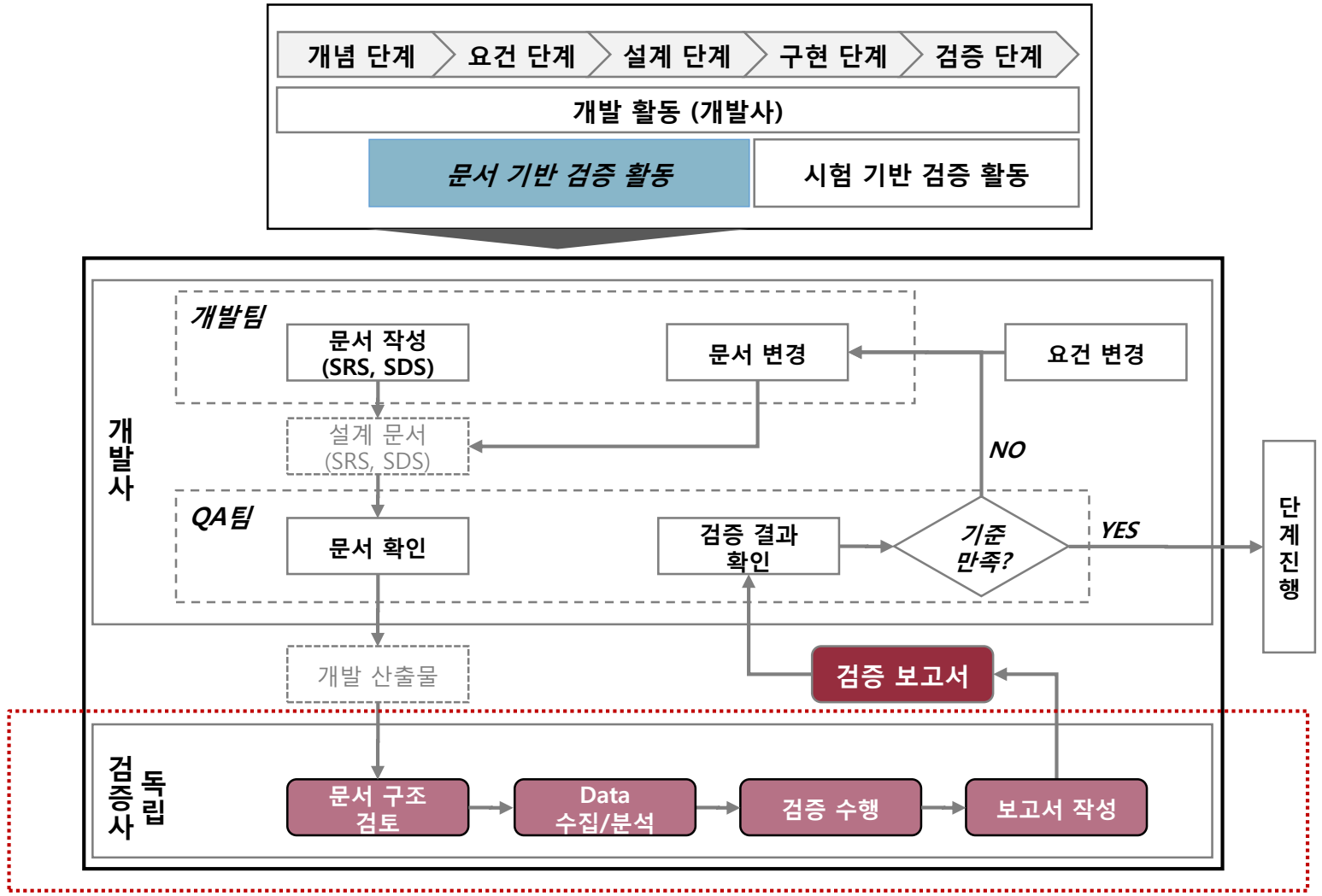
소프트웨어 확인 및 검증 활동 요약

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



4. 문서 기반 검증

문서 기반 검증 절차 예시



4. 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**

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*

5. 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 명세서의 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

5. 소프트웨어 요구사항 명세

요구사항 명세서 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

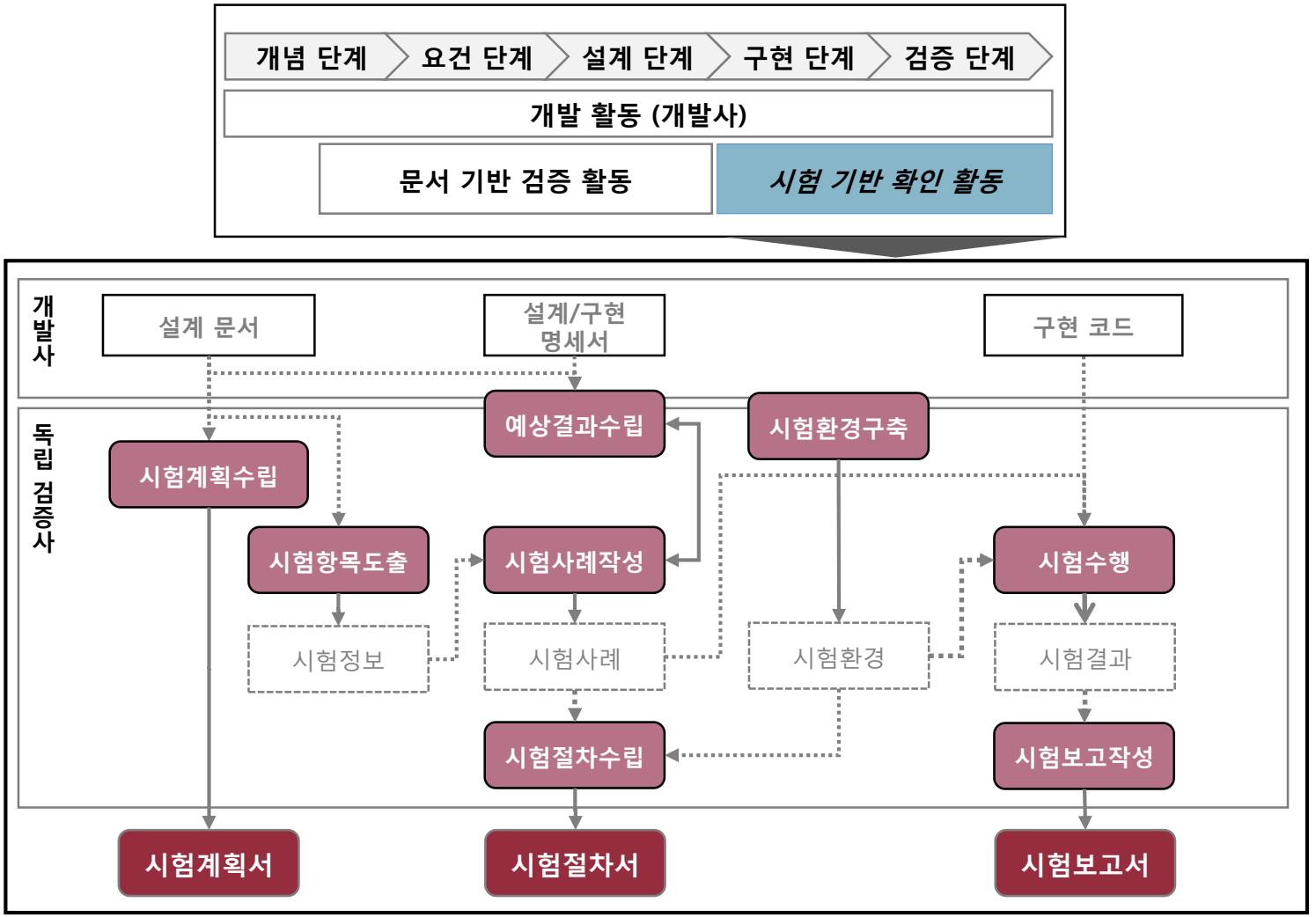
…
…
…

Completeness & Consistency!

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

6. 소프트웨어 시스템 시험

시험 기반 검증 절차 예시



6. 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**

6. 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	…	…	…	…	…	…	…

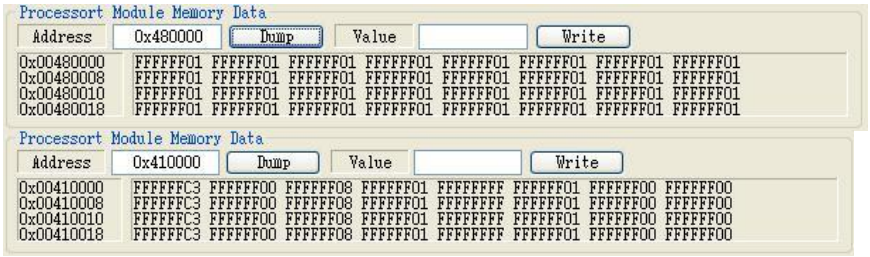
- Master(정상) / Slave (비정상)
  - 어플리케이션 계속 실행 설정
  - LED만 표시 후 계속 수행
- Master(정상)/Slave (비정상)
  - 어플리케이션 계속 실행 설정 없음
  - Fail-Safe 상태로 전이
- 슬레이브 모드에서 발생한 경우는 비정상 상태
- 정상 수행
- …
- …
- …

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

6. 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 마 다 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	

7. 시스템 시험의 수행 및 환경

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

제어 소프트웨어 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)
- 인허가 또는 기술 표준 만족을 위해 체계적인 요구사항 명세서 (SRS) 작성 및 V&V 활동 필요
- 제품의 품질을 위한 높은 수준의 확인 및 검증을 요구

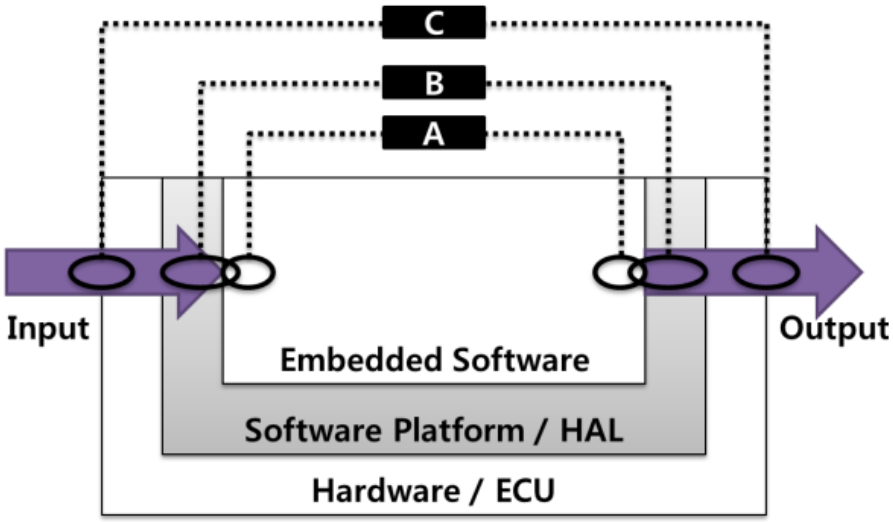
시험 관리의 체계화

7. 시스템 시험의 수행 및 환경

- 입출력 인터페이스 위치에 따라서 다양한 환경 구성이 가능
- 임베디드 시스템의 특성 상 하드웨어 제약에 의존적

소프트웨어 시스템 시험 환경 구성의 종류

- **소프트웨어 경계 및 시스템 아키텍처에 따라서 다양한 수준의 인터페이스 활용 가능**
- **입출력 제어 및 모니터링 위치에 영향**
- **임베디드 시스템의 환경적 제약에 의존적**



A. 온-칩-디버거 환경

- **소프트웨어의 내부 상태를 모두 접근 가능**
- 개발 환경과 유사 환경 활용

B. 플랫폼 지원 테스트 도구 환경

- **소프트웨어 플랫폼/HAL 또는 소프트웨어 입출력 인터페이스 활용**
- 별도의 입출력 장비 불필요

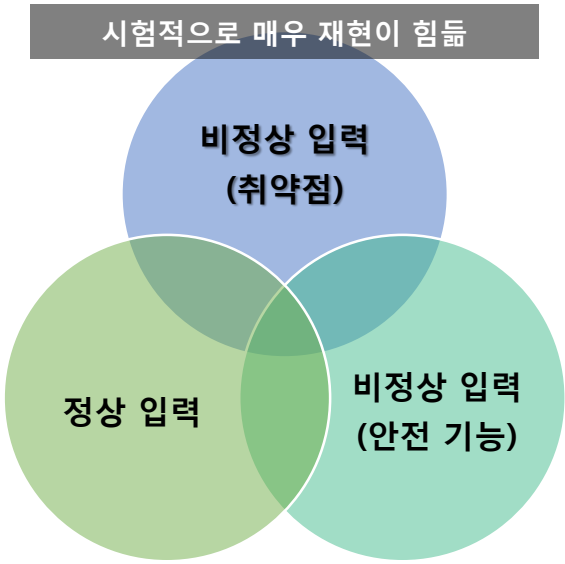
C. 하드웨어 테스트 환경

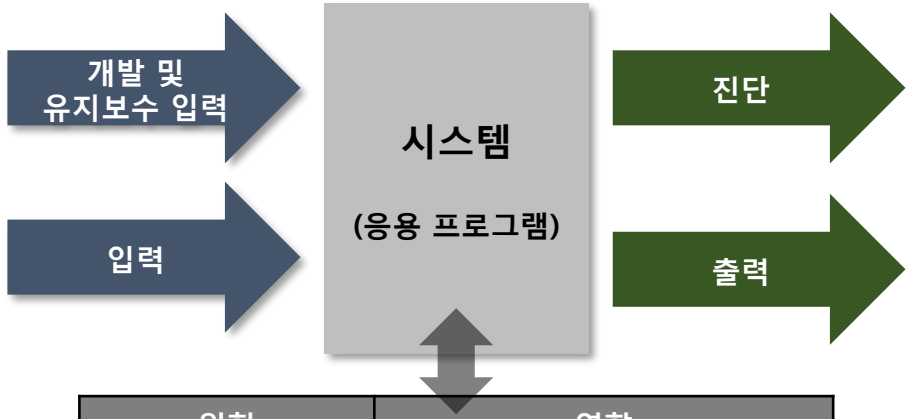
- **하드웨어 입출력 신호 외부 제어 및 모니터링**
- 소스코드 또는 별도 소프트웨어 인터페이스가 없는 최종 제품에 적용 가능

7. 시스템 시험의 수행 및 환경

사이버보안 요건과 테스팅

[SRS-xxx] [ST-xxx]	PLC 엔지니어링 도구는 프로젝트를 구성하는 파일을 읽어 만든 해쉬 값과 프로젝트 저장 시에 생성된 해쉬 값을 비교하여 프로젝트 파일의 변조 여부를 판단한다.	
	Case 1	해쉬 값이 일치
	Case 2	해쉬 값이 불일치
	Case 3	**해쉬 값을 비교 불가**
	….	…





위협	영향
오류	진단 및 출력 불가
위변조	의도하지 않은 출력
시간적 위반	결정론적 동작의 방해

IV. 요약

원전 사이버보안 대응 체계와 V&V

1. 위협 모델 기반 원전 사이버보안 대응 체계 특징

- 현재 기술 수준에 따른 평가 수행 및 대응 방안 반영
- 체계적인 평가 방법론을 수립하여 향후 취약점 발견에 따른 위협 평가 및 대응 체계 구축

단순 취약점 점검과 사이버보안 대응 체계 비교

단순 취약점 점검 (IT or 일반 보안 평가)

단순 취약점 점검

- ✓ 점검 항목에 따른 case-by-case 시험 수행
- ✓ 원전 영향성에 대한 평가 미흡

취약점 = 위협

모든 취약점에 대한 방호 필요

- ✓ 취약점의 영향 가능성 평가 불가
- ✓ E.g. MS Windows update (필요성 평가 불가)

원전 사이버보안 대응 체계 (상시 운용 체계)

체계적인 취약점 분석 및 위협 영향 분석

- ✓ 취약점과 위협간의 관계를 체계적으로 관리
- ✓ 원전 영향성을 기반으로 상시 관리 가능

취약점=위협+비위협

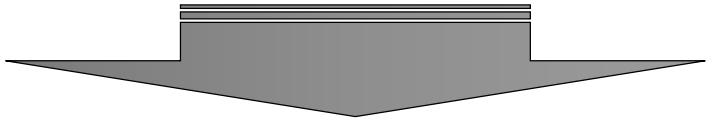
직접적 위협 취약점에 대한 방호

- ✓ 영향에 따른 우선순위 기반 대응 가능
- ✓ 효과적인 대응 적용 가능

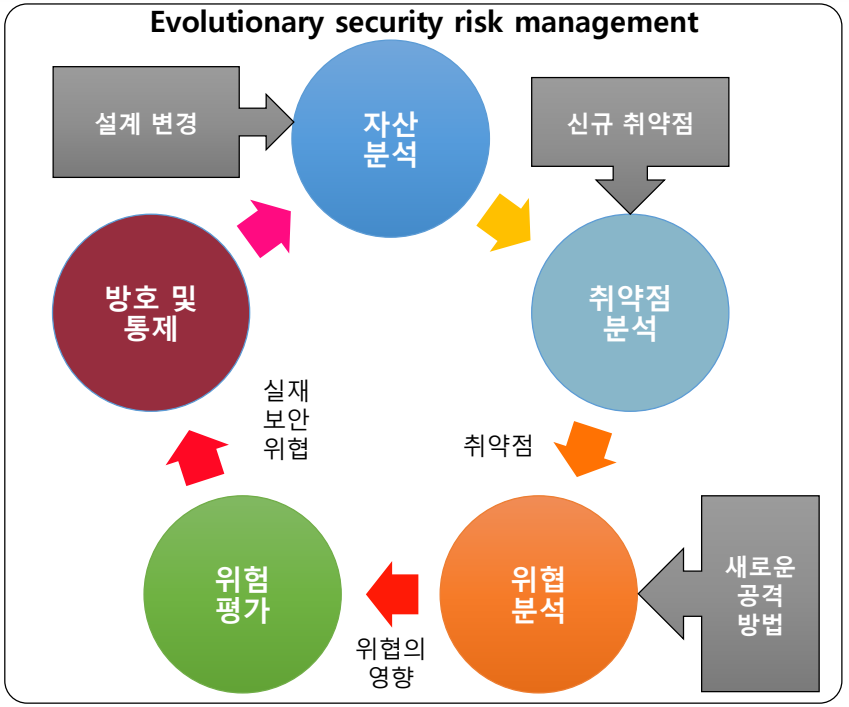
2. 사이버보안 상시 관리 체계

➢ **사이버보안 : 평가에서 위험 관리로!**

- 사이버보안은 전체 생명주기 동안 유지되어야 함
- 새로운 취약점 및 위협을 적절하게 통제하여야 함



➢ **설계 변경, 신규 취약점, 새로운 공격 기법 등을 고려한 체계적인 사이버보안 위험 관리 방법론을 수립하여 제공**



설계 단계

사이버보안 평가 및 설계

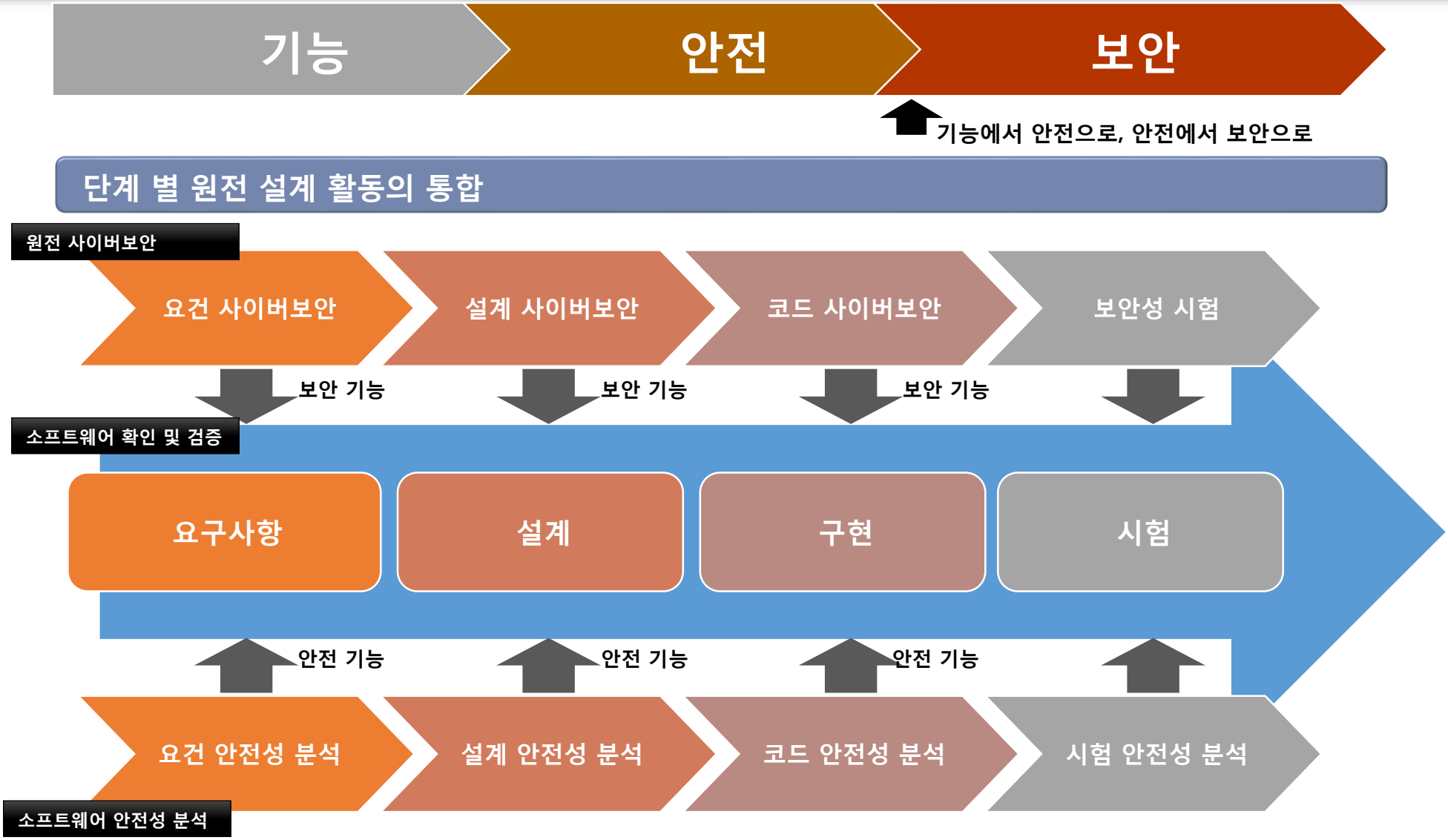
➢ 알려지거나 유사한 공격에 대하여 엄밀한 사이버보안 요구사항을 도출하고 구현

운영 단계

체계적인 운영 절차

➢ 현재 알려지지 않은 공격에 대하여 attack-tree 위협 분석을 통하여 사이버보안을 유지

3. 개발, 사이버보안, 안전, 확인 및 검증



감사합니다.

http://www.formalworks.com