무기체계 사이버보안 발전방향

2018. 12. 12.

국방과학연구소

김 현 숙

국 방 과 학 연 구 소
AGENCY FOR DEFENSE DEVELOPMENT

목 차

목 차

무기체계 사이버 위협 사례

- 2011년 이란이 RQ-170(미 UAV) 해킹, 탈취
- 2016년 이란이 역공학으로 복제 생산한 UAV 공개

연합뉴스

이스라엘 "시리아서 격추된 이란 드론은 미국제 '모조품'"

기사입력 2018/02/12 16:05 송고

미제 MQ-170 '센티넬 역설계해 개발 제작…다양하게 '복사'

무기체계 사이버 위협 사례

북한 무수단 미사일 시험발사 실패

- 2014년부터 지속된 미국의 미사일 방어 전략, 'Left of Launch(발사 직전 교란)' 으로 북 미사일 발사 방해

朝鮮日報 2017년 3월 6일 월요일 A04면 종합

北 무수단 발사 잇단 실패 뒤엔… 美 'Left of Launch' 작전 있었다

(발사 직전 교란)

사이버 공격으로 미사일 발사前 무력화… 작년 8발 중 7발 실패

"오바마 행정부는 2014년 초 북한 핵·미사일 기술의 진전을 늦추기 위해 'Left of launch(발사 직전 교란)'라 불리는 사이버·전자전 능력 증강에 나섰다. 실제 북한의 미사일 개발은 곧 헌저한 속도로 실패하기 시작했다."

미 오바마·트럼프 행정부의 북핵·미사일 대응 고민을 다룬 뉴욕타임스(NYT)의 4일 보도에 따르면 미국의 대(對)북한 사이버·전자 공격은 상당한 성과를 거둔 것으로 보인다. 북한이 작년에 발사한 증거리 무수단 미사일에 대부분 심각한 것이 사이버 공격의 결과라는 것이다. NYT는 "미 당국자들은 이를 통해 북한의 미국 본토 타격용 핵미사일 실전 배치를 수년간 늦췄다고 믿고 있다"고 보도했다.

◇오바마의 선택은 대북 사이버 공격

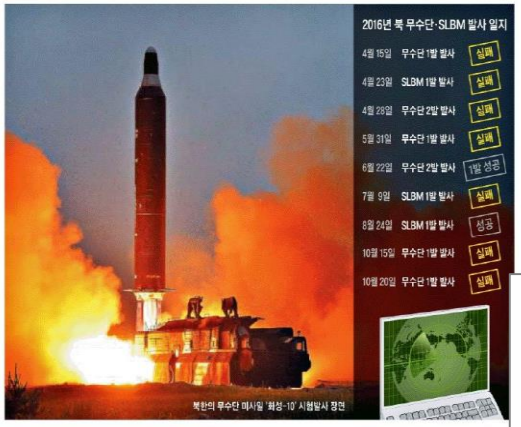
NYT에 따르면 오바마 행정부가 북한의 핵·미사일 위협에 결정적 경각심을 갖게 된 계기는 2013년 2월 12일 북한의 3차 핵실험이다. 핵실험 며칠 후 미 국방부 악성코드 심고 전자기파 공격

‡Left of Launch(발사 직전 교란)

악성코드, 전자기파 등으로 미사일 통제 시스템을 교란해 미사일을 발사 전에 무력화하는 개념. 직역하면 '발사의 왼편'인데, 이는 미사일 요격 단계를 '발사 준비→발사→상승→하강'으로 나눌 때 '발사' 보다 왼쪽에 있는 '발사 준비' 단계에 공격을 가하기 때문에 붙은 이름이다.

거리 3000km의 무수단을 발사한 것은 이때가 처음이다. 미국 괌 기지에 대한 핵 공격 능력을 과시함으로써 김정은 체제의 위대성을 선전하고 전통적 국제 체제로 어수선한 내부 결속을 다지려 했던 것으로 보인다.

하지만 미사일은 발사 수초 만에 상승 단계에서 공중 폭발했다. 이를 시작으로 같은 해 10월까지 북한은 총 6차례에 걸쳐 무수단을 8발 발사했지만 이 중 '부분적 성공'으로 평가받는 것은 6월 22일 발사한 2발 중 1발뿐이다. 나머지 7발은 대부분 발사 직후 폭발하거나 발사와 동시에 폭발해 발사 차량까지 깨끗하게



dongA.com

2017-03-06 03:00:00 편집

프린트 담기

오바마 정부때 '발사의 왼편' 작전 실행… 전자파-해킹기술로 北미사일 발사 방해

[美, 전술핵 한반도 재배치 검토]"北 발사실험 잇단 실패로 실제 효과… 최근 신형미사일 성공후 효용 논란"

"안보 위협이 계속 증가하는 현재, (기존 미사일방어체계는) 비용 면에서 지속 가능하지 않다."

무기체계 사이버 위협 원인

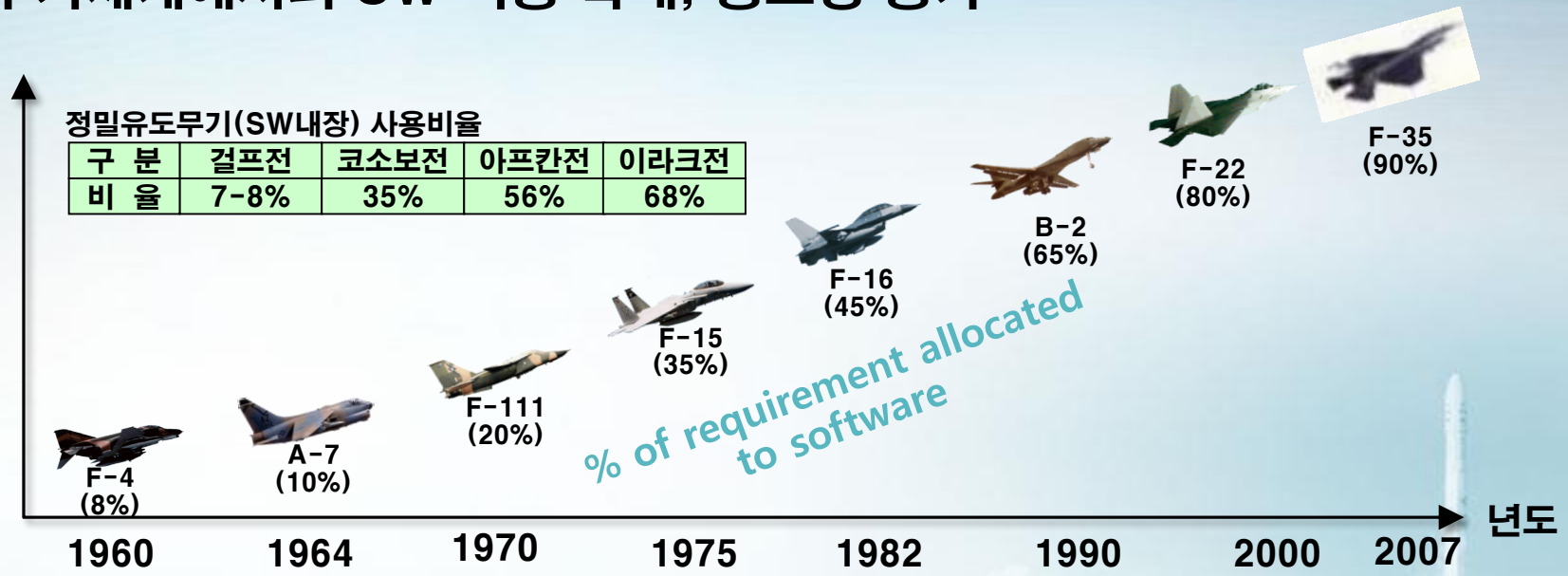
- **무기체계 SW의 취약점(vulnerability)이 공격 대상**
- **무기체계 사이버 위협 상황 예**
  - 정보수집 장비에서 정보 탈취 및 誤정보 주입
  - 무기체계 내장형 SW에 악성코드 삽입
  - 무기체계의 제어권을 탈취하여 기능 마비 및 誤작동 유발

무기체계 사이버보안의 필요성

무기체계에서의 SW 비중 확대, 중요성 증가

정밀유도무기(SW내장) 사용비율

구 분	걸프전	코소보전	아프칸전	이라크전
비 율	7-8%	35%	56%	68%



K1A1전차('97년)	K9자주포('99년)	K2 전차('07년)
3만 라인	12만 라인	62만 라인
		

※ 출처: 무기체계 SW 발전방안(방사청, 2012.4.)

무기체계 사이버보안의 필요성

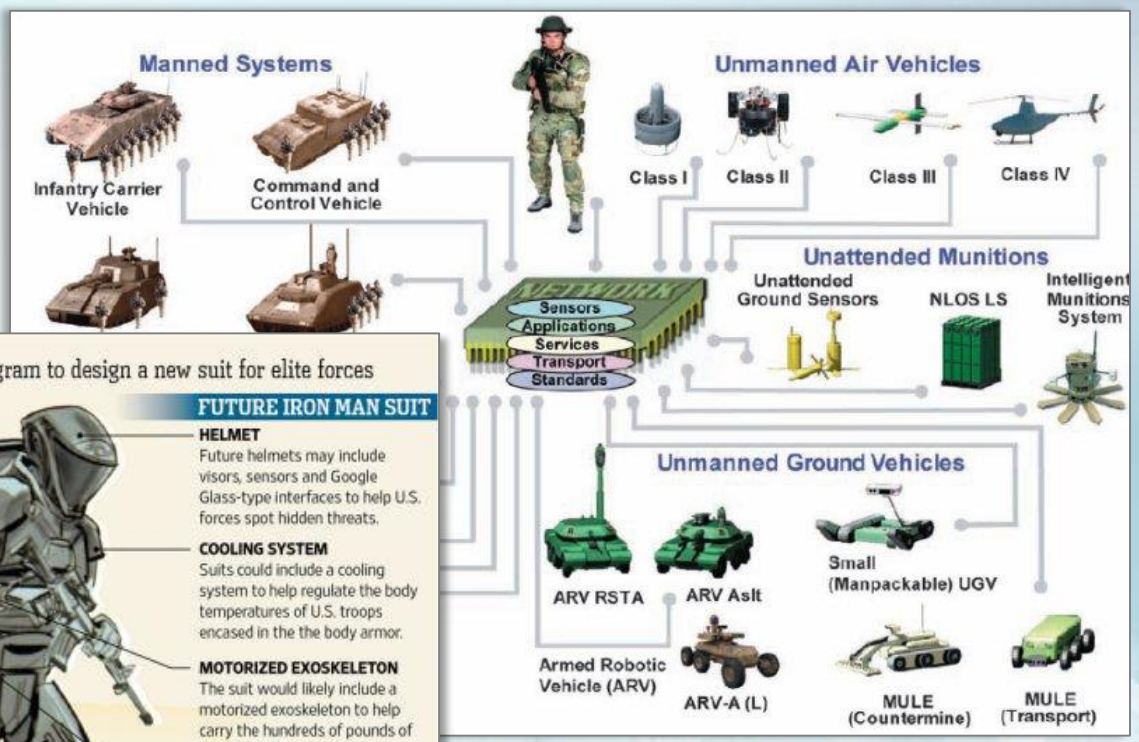
무기체계 내장형 SW 활용 현황

구분	무기체계 내장형 SW 관리 대상	운용 체계
육군	19개 체계, 172종 (전력화 예정 포함)	원격사격통제체계, 소형정찰용 UAV, 사단정찰용 UAV, 차기열상감시장비, 차기전자전장비, 차기군단정찰용 UAV, TICN, 방공C2A체계 등
해군	92종	한국형구축함전투체계, 이지스전투체계, 대형수송함전투체계, 지휘무장통제체계, 해상이동위성통신체계, 연합해상작전통신체계, 함내지휘통신체계 장비 등
공군	16개 체계, 755종	전투기, 국산기 등의 C4I/통신, 감시/정찰, 항공전자/임무컴퓨터, 화력, 방호 등

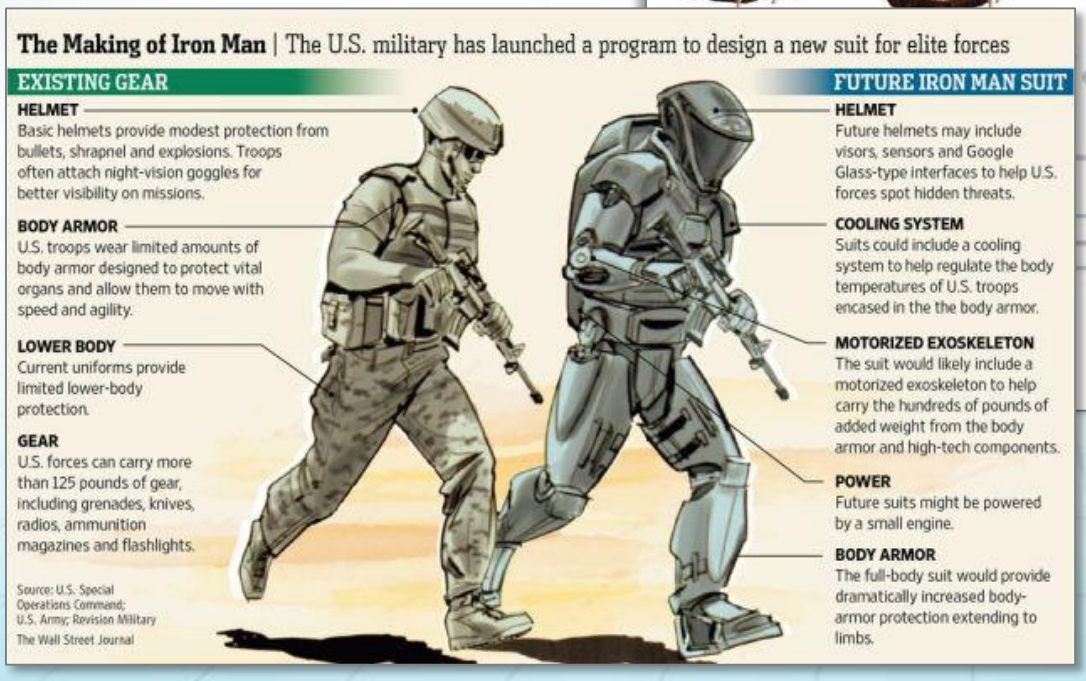
※ 출처: 무기체계 내장형 SW 관리 현황(국방부, 2016.2.)

무기체계 사이버보안의 필요성

- **무기체계 SW 간 연결성 확대**



[FCS, U.S. DoD]



[TALOS program, DARPA]

국내 무기체계 SW 사이버보안

전자신문

2018년 06월 20일 수요일 001면 종합

실전 배치된 軍 무기체계 SW '보안 무방비'

정보보호인증센터, 무기체계 SW 보안 검증…"기본도 안지켜"
소스코드 내 암호키 노출돼 해커가 계정획득 후 정보 탈취 우려
악성코드 발견돼도 오작동 일으킬라 치료 못하고 그대로 운영

김인순 insoon@
보안 전문기자

군이 사용하고 있는 무기 체계 소프트웨어(SW) 보안이 위험 수준인 것으로 드러났다. 무기 체계 SW 소스 코드와 주석문, 설정 파일 내 관리자 계정 다. 전체 기능 90%가 SW로 구현되는 등 무기 체계 내 SW 비중과 중요성은 높다.

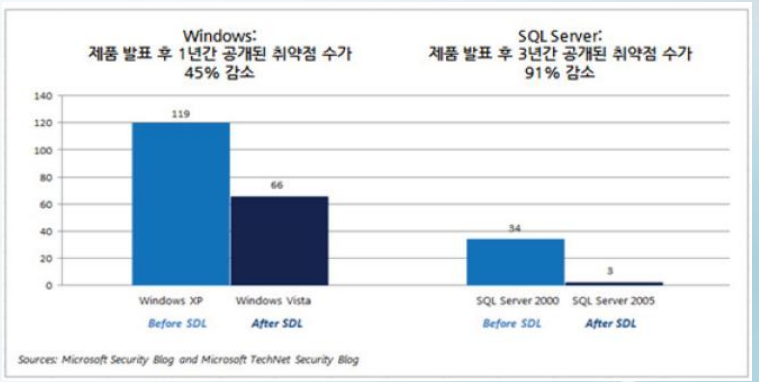
기무사 정보보호인증센터 관계자는 "두 번에 걸친 시범 검증에서 무기 체계에 쓰인 소스 코드 내 암호키가 그대로 들어있고, 취약한 암호 알고리즘이 사용된 사례를 발견했다"면서 "해코드에 감염되는 사례가 많다"고 설명했다. 이 관계자는 "무기 체계에서 악성코드가 발견돼도 치료할 수 없는 구조"라면서 "악성코드 치료로 무기 체계가 오작동을 일으킬 수 있다"고 덧붙였다.

군은 무기 체계 전용 백신을 개발·배포하는 1차 조치만 취했다. 전용 백신은 PC나 무기 체계에 설치하지 않고 USB나 CD에서 실행하는 휴대형이다. 무기 체계 내 악성코드 감염 여부만 탐지하고 치료는 하지 않는다. 사이버 위협을 안고 무기 체계를 운영하는 상황이다.

목 차

안전한 소프트웨어 개발 방법론

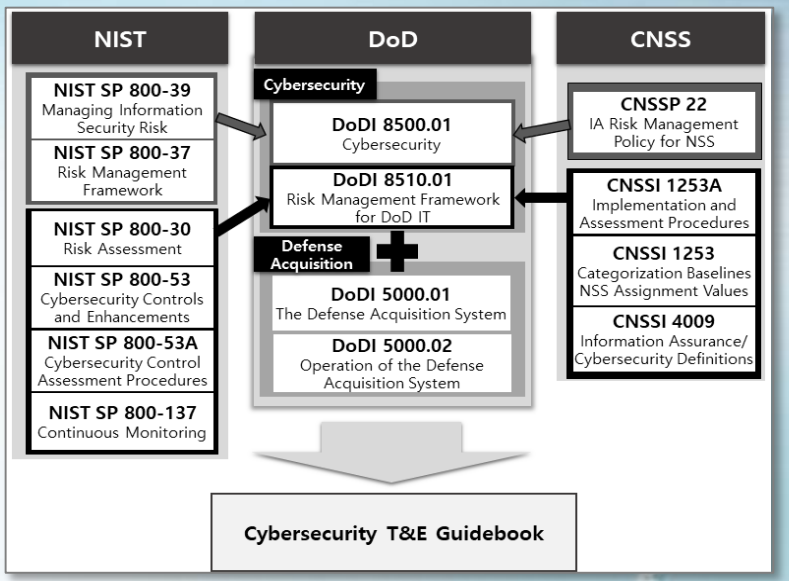
- SDL(Security Development Lifecycle)
  - 마이크로소프트에서 개발, 소프트웨어 개발단계에서 수행해야할 보안활동을 정의
  - 2004년에 실제 제품 개발에 적용, 시스템 취약점 급감
    - 요구사항 분석 : 보안 요구사항 작성
    - 설계 : 위협 모델링
    - 구현 : 보안코딩, 정적분석, 보안 코드리뷰
    - 시험 : 보안테스트, 동적분석, 침투테스트
    - 출시(양산) : 최종 보안점검
    - 유지보수 : 제품 보안 이슈 대응



1. Training	2.Requirements	3.Design	4.Implementation	5.Verification	6.Release	7.Response
1. Core security training	2. Establish Security Requirements	5. Establish Design Requirements	8. Use Approved Tools	11. Perform Dynamic Analysis	14. Create an Incident Response Plan	17. Execute Incident Response Plan
	3. Create Quality Gates/Bug Bars	6. Perform Attack Surface Analysis / Reduction	9. Deprecate unsafe Functions	12. Perform Fuzz Testing	15. Conduct Final Security Review	
	4. Perform Security and Privacy Risk Assessments	7. Use Threat Modeling	10. Perform Static Analysis	13. Conduct Attack Surface Review	16. Certify Release and Archive	

美 사이버보안과 획득 생명주기의 통합

- 미 국방부는 무기체계에 사이버보안을 실현하기 위해 국방획득체계, 위험관리프레임워크, 사이버보안 시험평가체계 통합
- 무기체계 내 전반적인 사이버보안을 다루기 위해 사이버보안 시험평가 프로세스 수행. 이는 국방획득체계 중 소요분석 단계부터 생산, 배치 단계까지 연속으로 진행되며 시스템 공학 및 RMF 프로세스 통합하여 진행

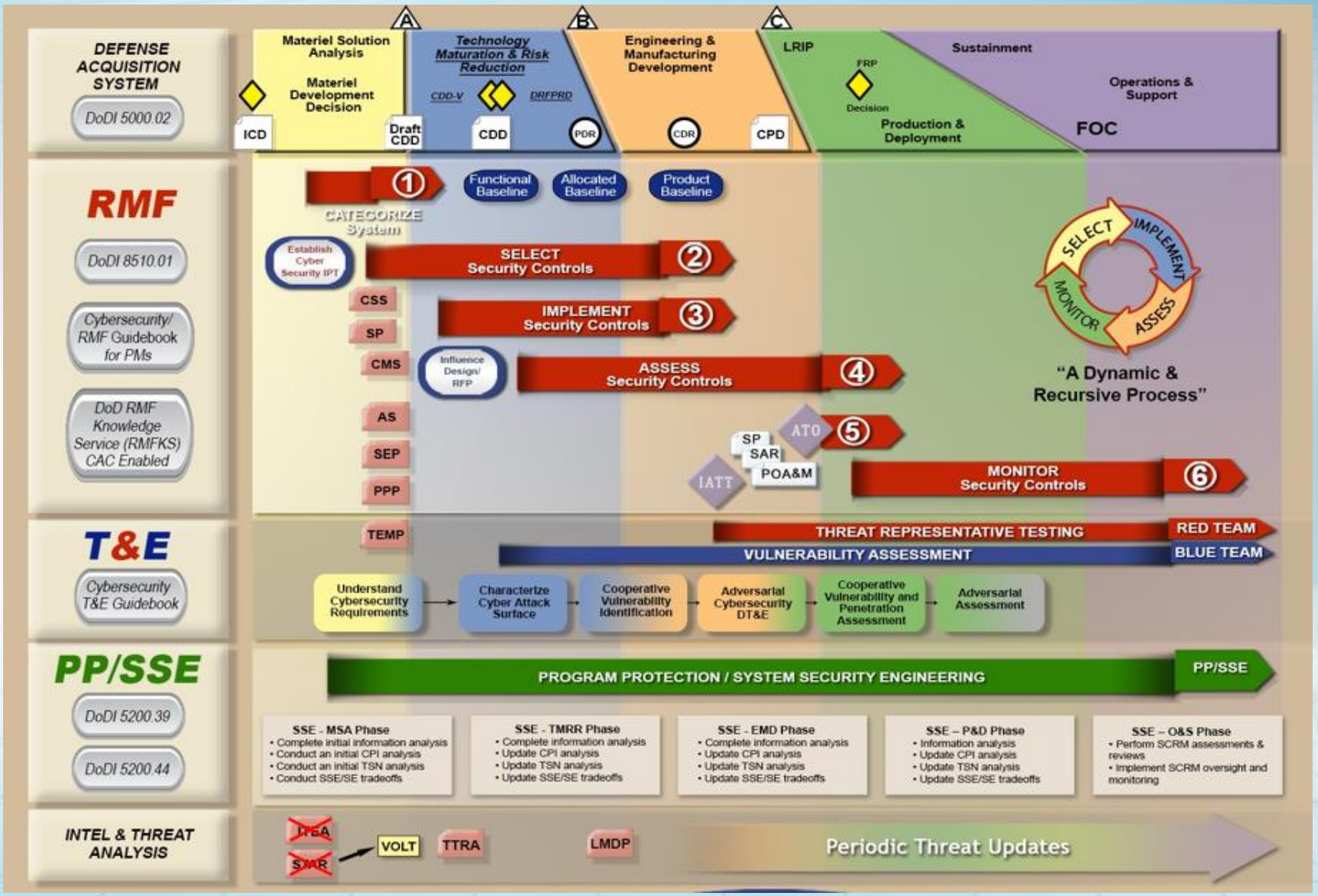


[미국 사이버 보안 문서간의 관계]

분류	제목	내용
DoDI 5000.02	Operation of the Defense Acquisition System	All the information systems planning to purchase or develop by DoD must be confirmed if information assurance strategy related to standard and structure are in agreement with DoD's policy
DODI 8510.01	Risk Management Framework for DoD Information Technology	Guidelines are provided for RMF for DoD IT and related cyber security policy establishment
DoDI 8500.01	Cybersecurity	General Guidelines are provided for protection and defence of DoD IT

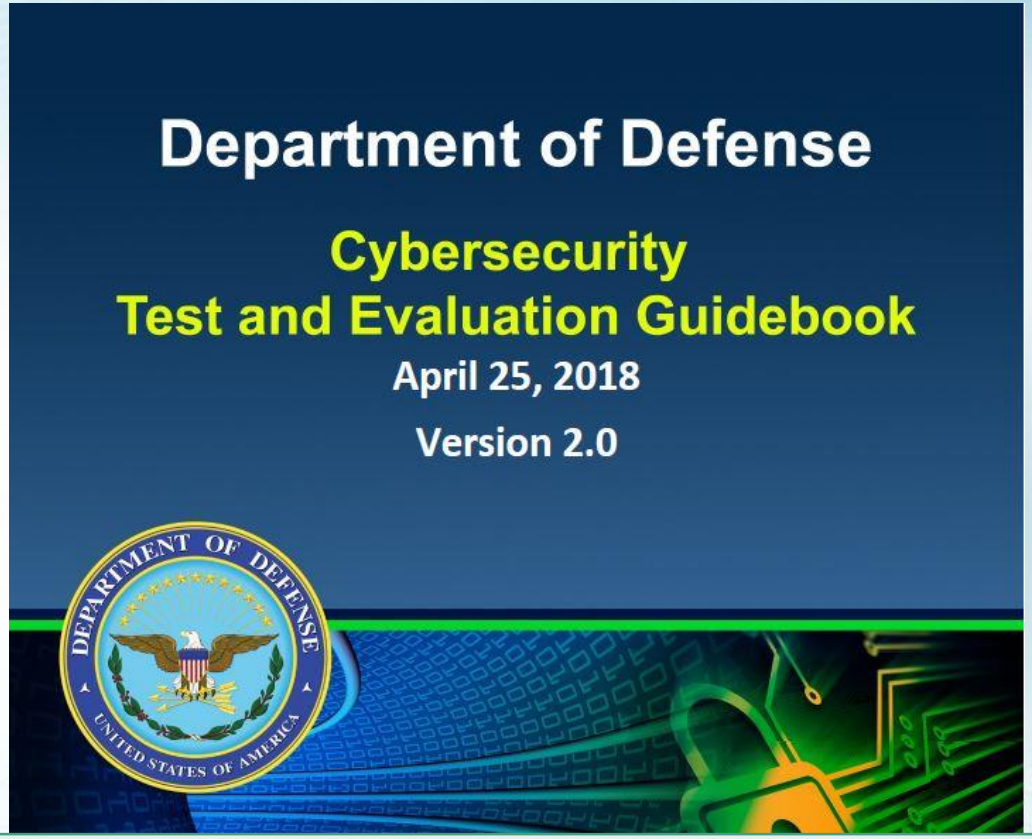
[미 국방 주요 사이버 보안 가이드라인]

美 사이버보안과 획득 생명주기의 통합



14

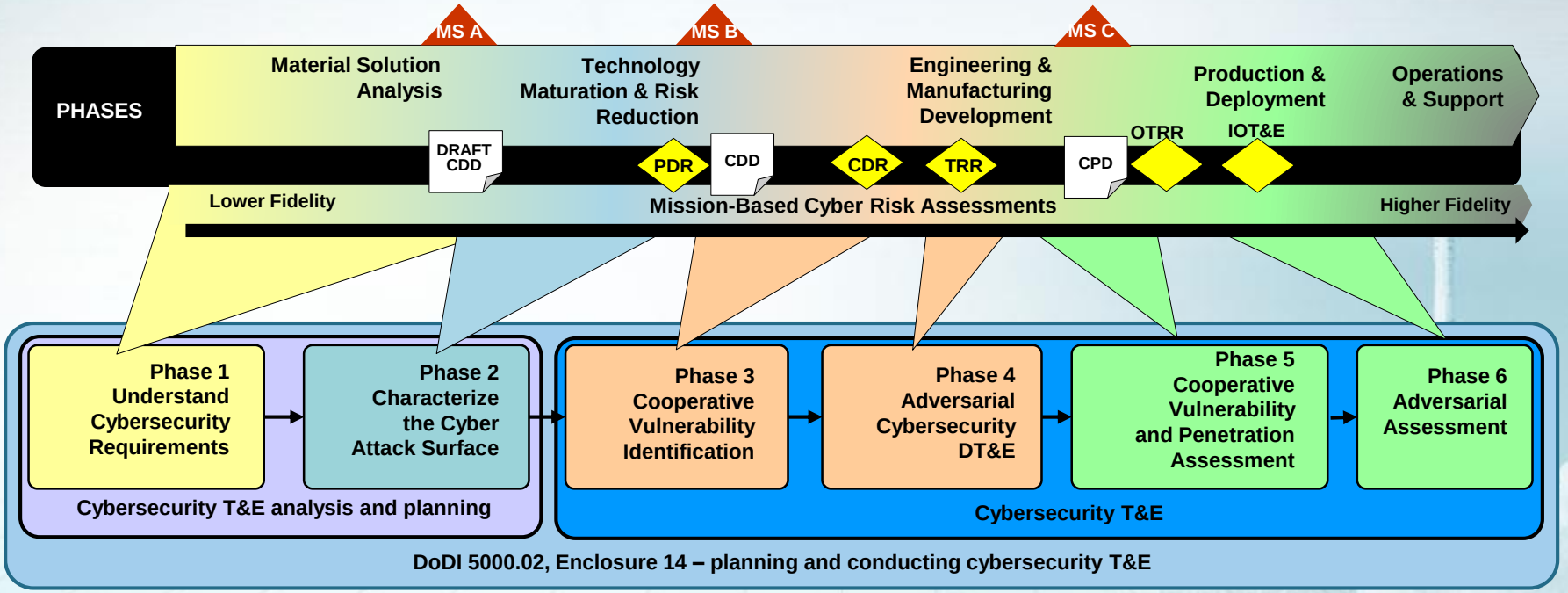
美 사이버보안과 획득 생명주기의 통합



- ❖ 구체적인 사이버보안 시험평가 계획, 분석, 실행지침 제공
- ❖ 사이버보안 시험평가 활동 : 획득 절차에 포함, 시험평가기본계획(TEMP)에 반영
- ❖ 모든 DoD 획득 프로그램 및 시스템에 적용

美 사이버보안과 획득 생명주기의 통합

- 사이버보안 T&E 단계는 DoDI 500.02 획득 수명주기에 맞추어 수행
- 사이버보안 T&E 단계와 획득 수명주기와의 관계



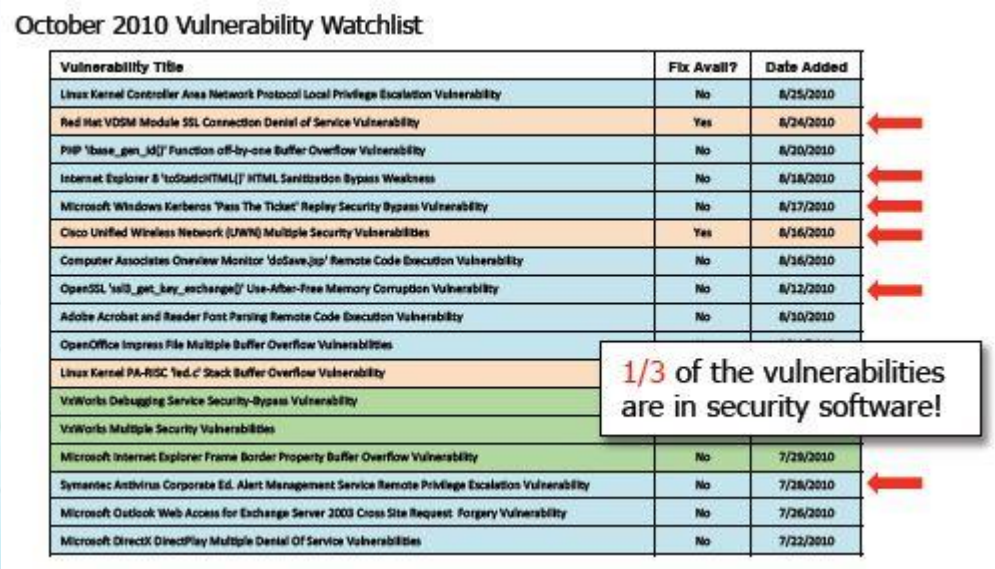
CDD : Capabilities Development Document
CDR : Critical Design Review
CPD : Capabilities Production Document
IOT&E : Initial Operational Test & Evaluation
OTRR : Operational Test Readiness Review
PDR : Preliminary Design Review
TRR : Test Rediness Review
DT&E : Development Test & Evaluation

美 사이버보안과 획득 생명주기의 통합

- 사이버보안 T&E 단계
  - 1단계 사이버보안 요구사항 이해 : 가능한 모든 대상 시스템 관련 문서를 살펴보고 사이버보안 요구사항 이해
  - 2단계 공격 접점 특성 분석 : 공격자가 시스템을 악용할 수 있는 취약점 및 공격방법 식별
  - 3단계 협업을 통한 취약점 식별 : 시험, 분석, 수정, 재시험 과정을 통해 시스템 개발 전반에 걸쳐 사이버보안 취약점을 식별
  - 4단계 적대적 사이버보안 개발시험평가 : 이전 사이버보안 시험평가 단계에서 산출된 취약점 분석평가보고서, 보안평가 보고서, 개발시험평가 산출물을 활용하여 대상 시스템의 시험평가를 수행
  - 5단계 협업을 통한 취약점 평가 및 침투 평가 : 취약점이 발생할 수 있는 환경을 임의로 구축하여 시험평가 진행. 이를 통해 대상 시스템에 적용된 사이버보안 정도 파악
  - 6단계 적대 평가 : 공인된 취약점 침투 테스트팀이 이전 사이버보안 시험평가 단계에서 도출된 사이버위협에 대한 대응방안 평가

고신뢰 소프트웨어 개발

- 필요성
  - 망분리를 통한 통제시스템 구축, 데이터보호를 위한 암호화 방식의 한계
    - Stuxnet, RQ-170 등 사례
  - 바이러스 검사, 침입탐지시스템, 패치인프라 등
    - 알려진 보안취약점에 대하여만 방어, 제로데이 공격에 취약
  - 새로운 접근 방식 필요



고신뢰 소프트웨어 개발

- 각 단계 산출물의 안전함을 수학적으로 검증하거나 보안이 검증된 개발방법 사용
- 호주 NICTA(국립정보통신기술연구소)의 seL4 마이크로커널
- 미국 DARPA의 HACMS(High-Assurance Cyber Military Systems) 프로그램
  - Hack_Free 드론 개발

목 차

안전한 무기체계 SW 확보

- 운영단계의 취약점 제거 비용은 개발단계에서 보다 60~80배의 비용 소요(IBM)

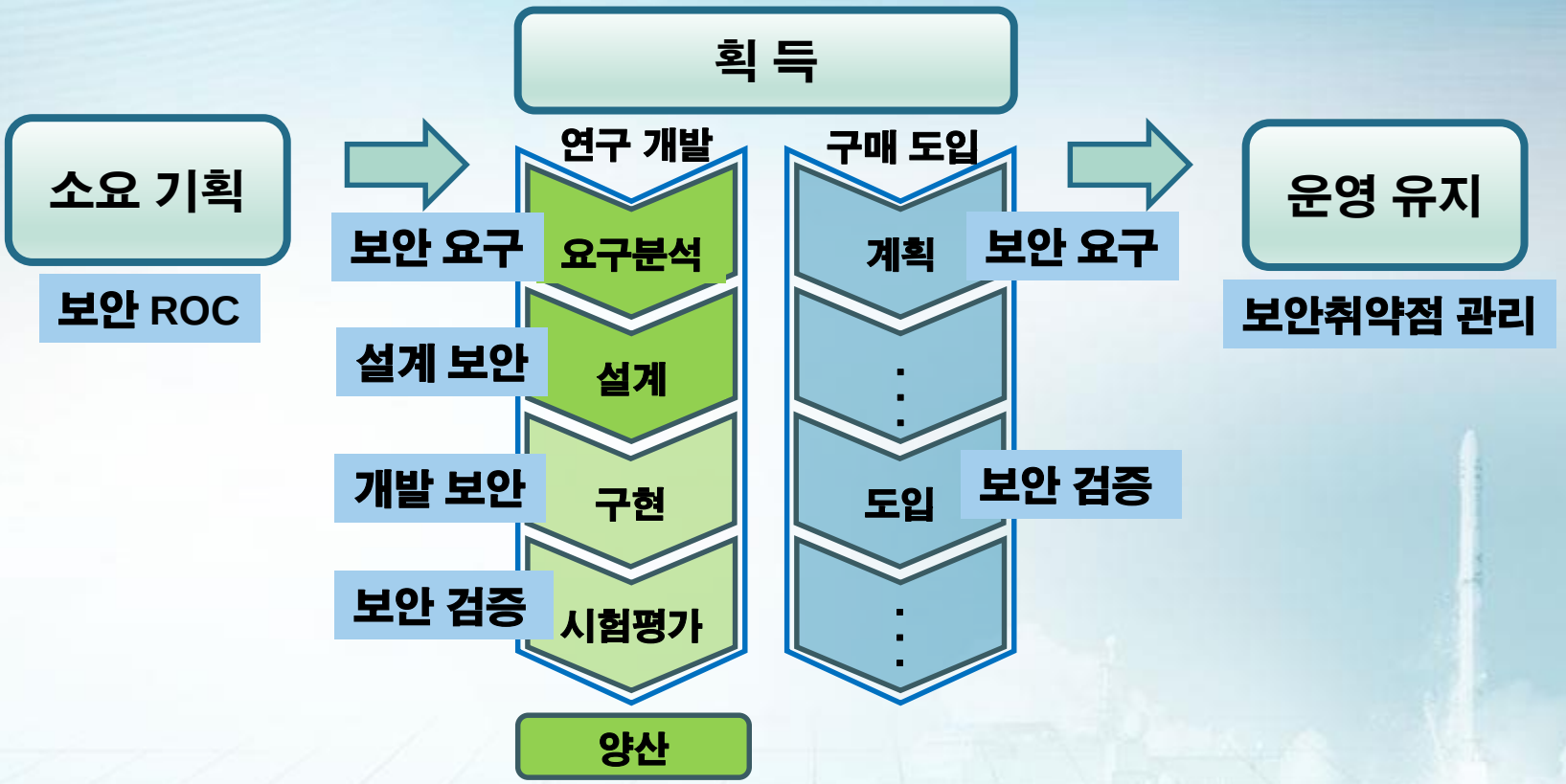
※ 출처: 국방SW발전 포럼 및 동계워크샵, 2015.2.

- **안전한 무기체계 SW**를 확보하기 위하여 공급사슬 전체에 대한 위험 관리 방안 필요

무기체계 SW를 잘 만들자!!!

무기체계 획득 전 단계에서
보안성 강화 노력 필요

무기체계 획득 프로세스와 사이버보안 활동의 연계




기동무기체계

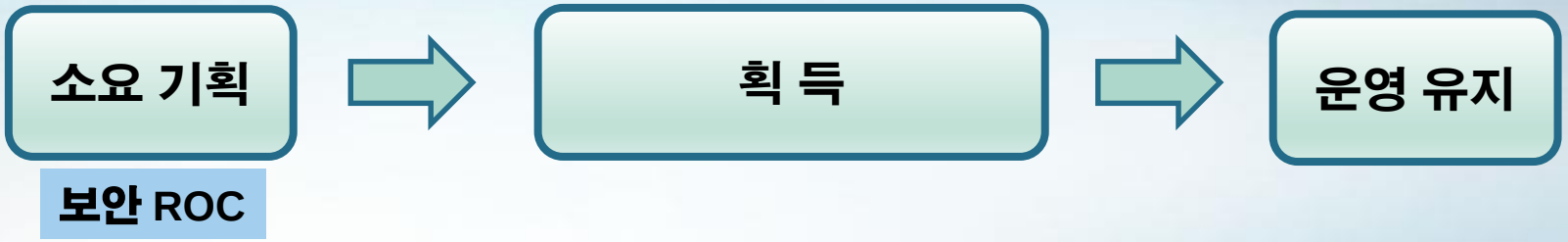

유도무기체계


감시정찰무기체계


함정전투체계

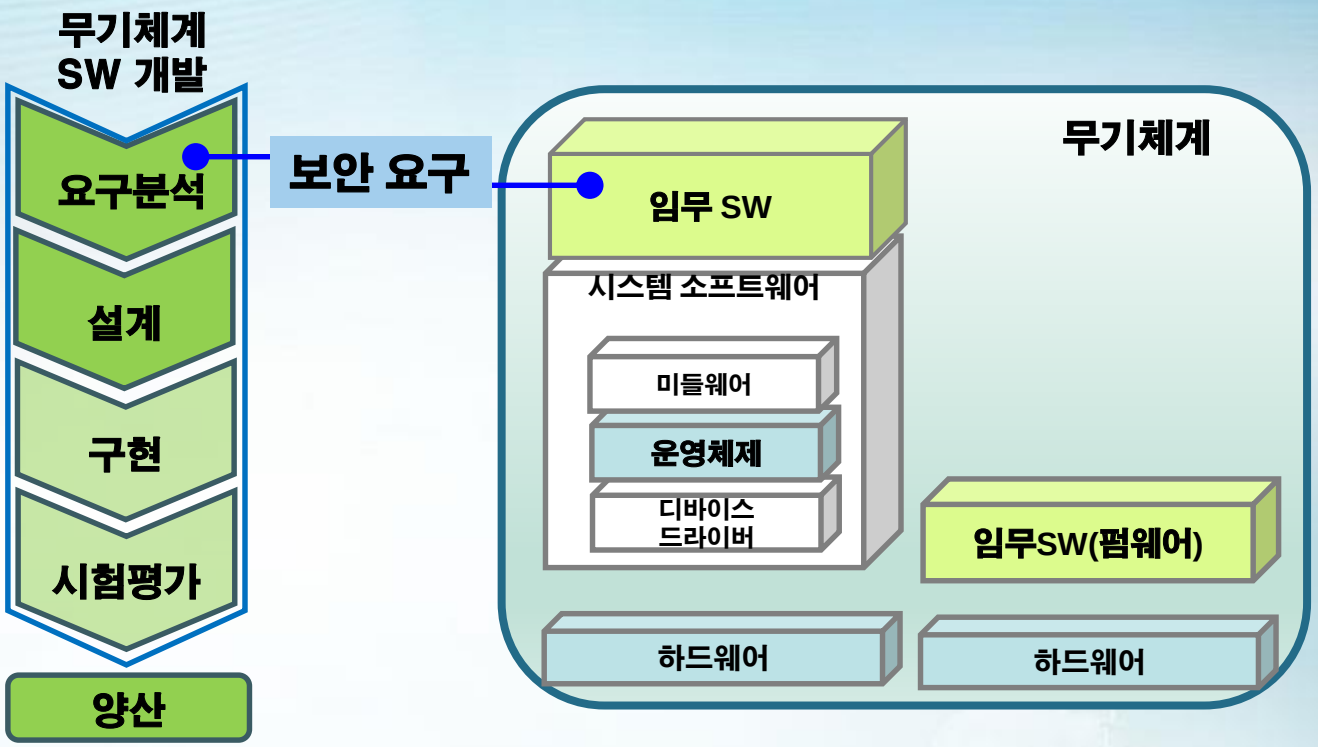

항공무기체계

무기체계 SW 개발간 보안성



- 소요 기획 단계 보안성
  - 보안 관련 ROC 언급 필요
    - 체계의 작전운용능력에 필요한 보안 요구사항 명시
    - 장기 전력소요서
    - 중기 전력소요서

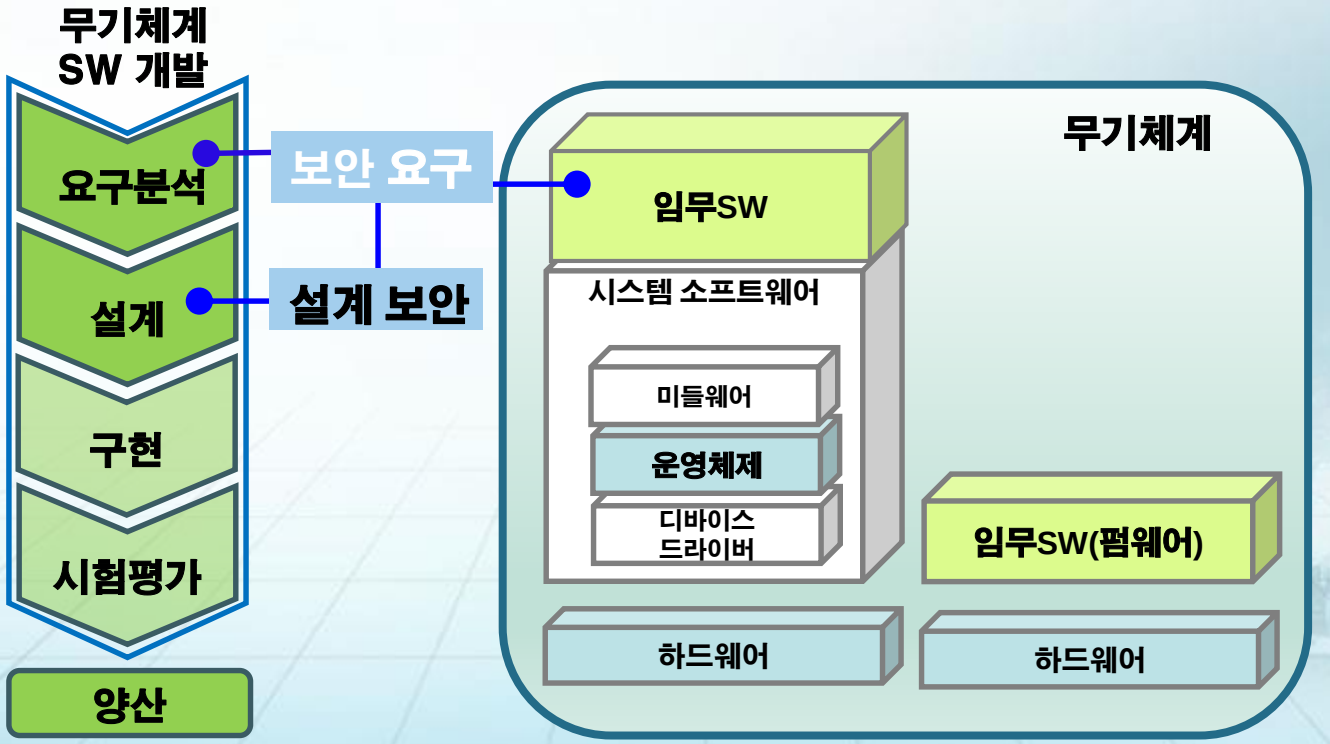
무기체계 SW 개발간 보안성



- 요구분석 단계 : 보안 요구
  - 보안 항목 요구사항 식별
  - 관리해야 할 데이터 식별 : 데이터의 보안등급(기밀성, 무결성, 가용성) 정의

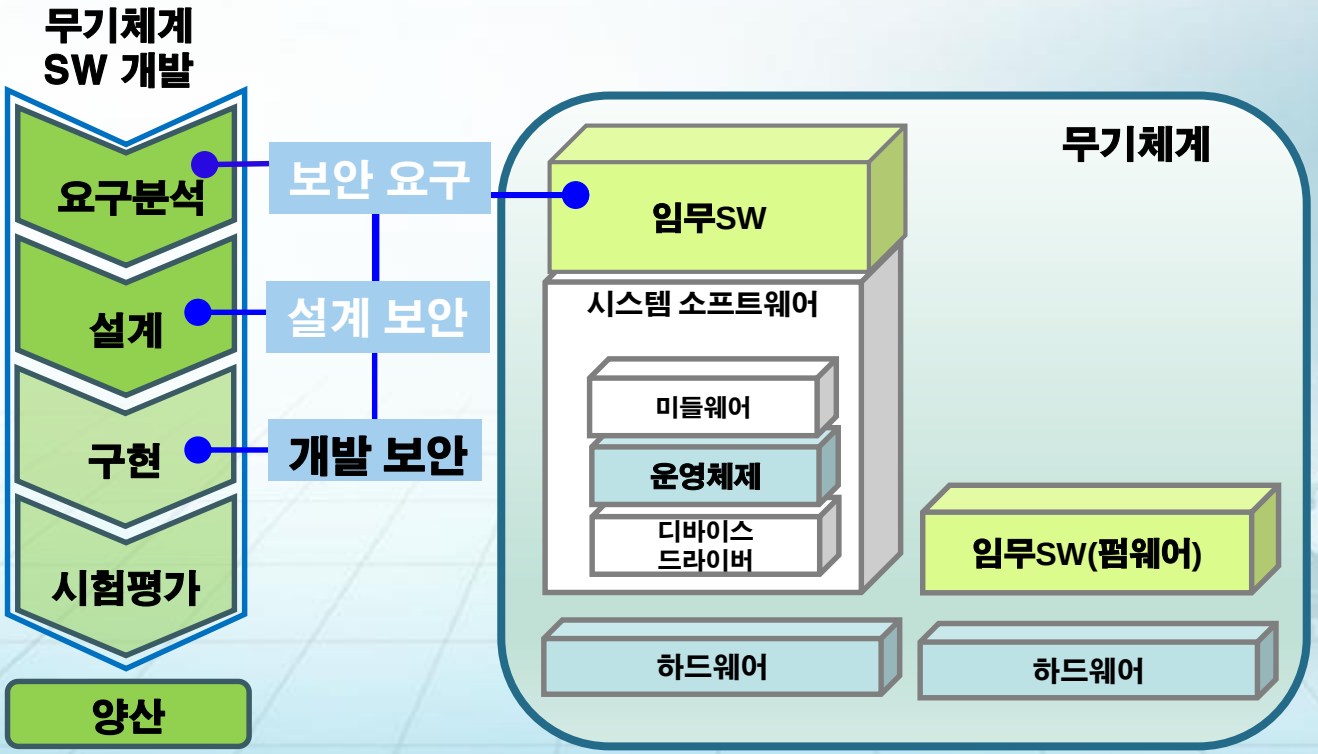
무기체계 SW 개발간 보안성

- 설계 단계 : 설계 보안
  - 체계의 위협 도출하는 위협모델링 수행
  - 도출된 위협이 제거될 수 있도록 설계



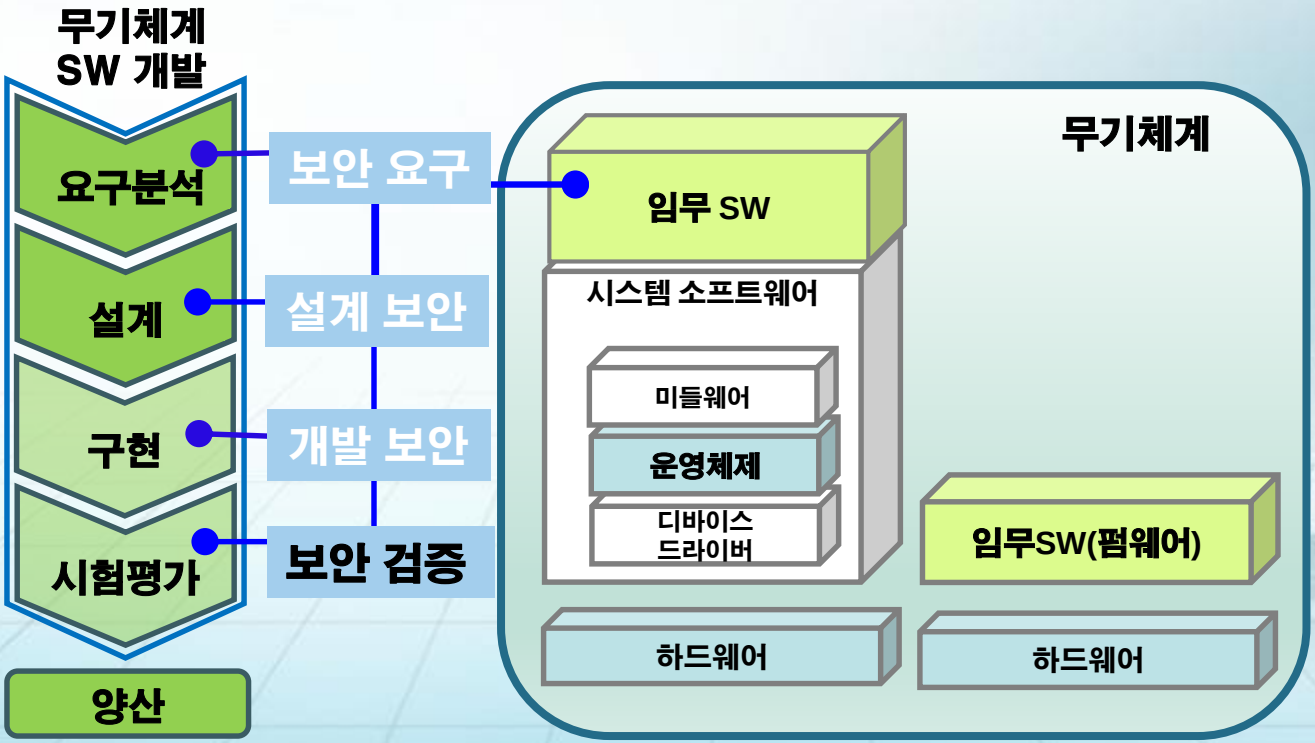
무기체계 SW 개발간 보안성

- 구현 단계 : 개발 보안
  - 시큐어코딩 표준 준수
  - 소스코드 보안약점 진단(정적 코드분석)
  - 단위테스트를 통해 보안취약점 사전 제거

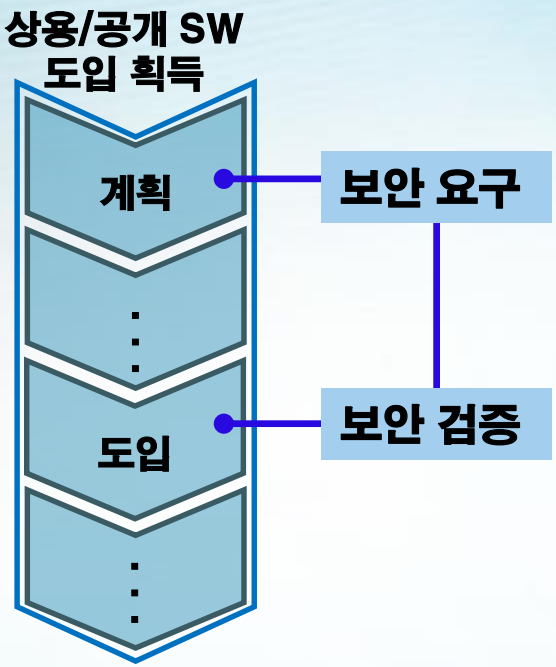


무기체계 SW 개발간 보안성

- 시험평가 단계 : 보안 검증
  - 코드 보안성 검토
  - 동적 분석
  - 모의침투 테스트



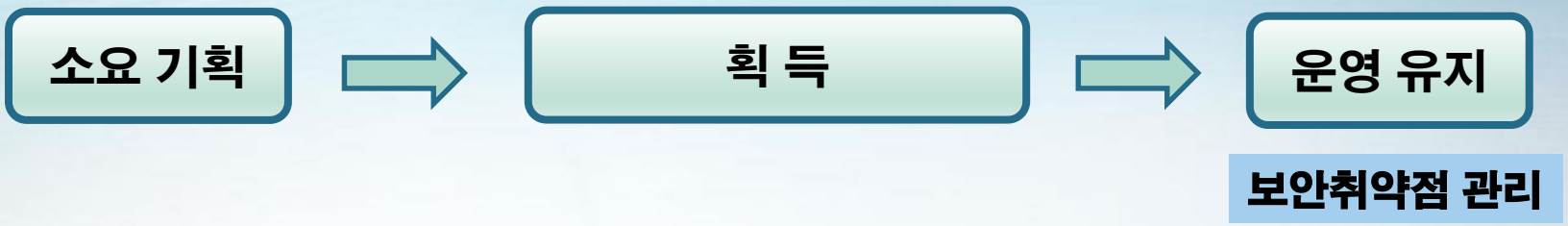
무기체계 SW 개발간 보안성



- 구매/도입 보안성
  - 계획 단계
    - 보안 항목 요구사항 식별
    - 관리해야 할 데이터 식별
      - 보안등급(기밀성, 무결성, 가용성) 정의
  - 도입 단계
    - 계획 단계 요구사항 기능 확인
    - 보안취약점/악성기능 분석/검증
      - 모의침투 테스트
      - 정적/동적 분석

❖ (미)소프트웨어 보증 요구
- 도입절차에 명시
  - 계획단계(요구조건 결정) → 계약단계(소프트웨어 보증 요구사항 포함)
- 상용 및 공개 소프트웨어 보안평가 항목 보유, 평가

무기체계 SW 개발간 보안성

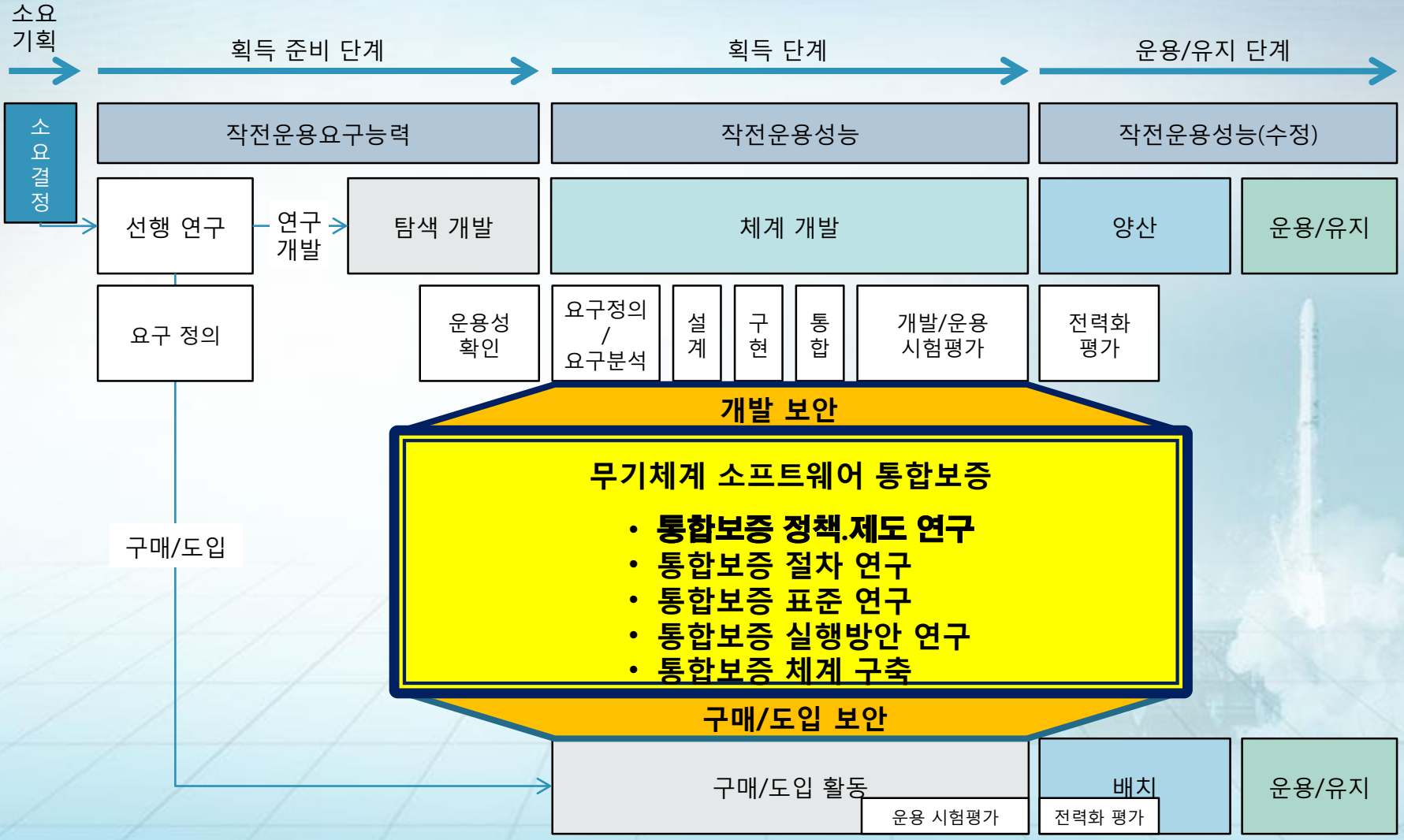


- 운영 유지 단계
  - 보안취약점 관리
    - 보안사고에 대한 관리
    - 보안취약점 수집, 저장
    - 사이버 위협 유형 분석
    - 시스템 통합 보안

❖ 국가 소프트웨어 보안취약점 데이터베이스 구축/운용
  - 미국(NVD), 중국(CNVD), 일본(JVN)

안전한 무기체계 SW 개발/획득

무기체계 SW 통합보증



안전한 무기체계 SW 개발/획득

SW 보증 정책·제도 및 개발절차

분류	미국		한국	
SW 보증 정책 제도 및 개발 절차	연방정보보안관리법 FISMA	연방정부 정보시스템 보안을 위해 기관별 보안절차 개발 및 실행토록 하는 법률	국방전력발전업무훈령	무기체계/전력지원체계 소요·획득·운영유지를 포함하는 전력증강 관련 업무의 기본절차 규정
	대통령 행정명령 EP 13636	국방 등 16개 국가주요기반시설에 대한 사이버보안 프레임워크 표준모델 및 규정	국방정보화업무훈령	국방정보화사업추진, 정보화 기반기술의 적용 등에 관한 절차·기준·원칙을 정하는 것을 목적으로 함
	상무부 국가기술표준원(NIST) 표준기술	국방 등 16개 기관에서 사용할 보안 관련 기준, 기술 및 가이드에 관한 표준 및 체크리스트, 매뉴얼	방위사업관리규정	방위력개선·군수품조달 및 방위산업육성 등 방위사업을 효율적으로 추진하기 위하여 필요한 절차 등을 규정
	미 국방성 지침 DoDI	전 생명주기에서 정보보증 정책의 실행을 위한 지침	무기체계 SW 개발 지원에 관한 규정	무기체계 SW 개발 활성화, 품질 향상, 국방 SW 산업 발전을 추진하기 위한 규정
	국방정보체계국 지침 DISA ASD STIG	국방관련 SW,어플리케이션 개발시 보안생명주기, 운영 유지보수, 획득, 평가에 관련한 지침	무기체계 SW 개발 및 관리 매뉴얼	방위력개선사업으로 획득되는 무기체계 SW의 체계적인 개발 및 관리를 위한 프로세스와 산출물 작성 표준을 규정함. SW 신뢰성/보안성 시험 평가 기준을 명시
	ISO/IEC/IEEE 15288 ISO/IEC/IEEE 12207 등	보안성 확보를 위한 정보시스템 개발생명주기 프레임워크, 보안성 확보를 위한 SW 개발 생명주기 국제표준 등	국방CBD방법론	국방정보체계의 개발 프로세스에 대한 산출물 표준을 제시
비고	• 미국과 비교할 때 SW 보증과 관련된 정책·제도 및 SW 개발절차 상의 보안활동 정의 미흡 • 정보시스템 및 내장형 SW를 포함한 무기체계 SW에 대하여 신뢰성 외에 보안성 확보 필요 • 보안 검증을 위해 필요한 추가 활동과 새로운 방식의 보안검증 방안이 필요			

안전한 무기체계 SW 개발/획득

SW 보증을 위한 조직 및 활동

단계	기 획	교 육	요구사항	설 계	구 현	확 인	획득/운영	폐 기
추가 활동	레드팀 선정 사용도구 선정 보안요구사항 도구 검토	보안 교육	위험 분석 코딩규칙 선정 시험도구 선정	위험 분석	시큐어코딩 정적분석	보안정적시험 보안동적시험 침투테스트	보안DT/OT 운영 보안시험	보안 폐기

조직/활동

교육조직	운용조직 (레드팀)	관리조직		연구개발조직	
		보안취약점 관리	통합보증SW 관리	기술연구	정책연구
SW 보안	위험 분석	보안취약점 DB관리	무기체계 임베디드SW DB	테스트케이스	통합보증평가방안연구
위험분석 기술	시험도구 선정	보안취약점 분석	무기체계 임베디드SW 형상관리	훈련시나리오	통합보증정책제도연구
시큐어코딩	코딩규칙 선정	보안약점 DB관리		SW취약점점검체계	성과분석정책연구
보안성시험기술	보안동적시험	보안약점 분석		훈령장	
교육커리큘럼	보안정적시험			보안정적분석도구	
	침투테스트			보안동적분석도구	
	보안DT/OT			코딩규칙	
	운용무기 보안시험			보안취약점 평가체계개발	
				시큐어디자인	

목 차

맺음말

- 사이버전의 공격 대상 및 목적이 확대되고, 네트워크 중심의 작전환경으로 변화됨에 따라
  - 무기체계의 보안성 훼손이 기반체계의 실패로 이어질 수 있음
  - 부차적인 속성이던 소프트웨어 보안이 핵심 소프트웨어 요구사항이 됨
  - 무기체계 소프트웨어의 사소한 보안취약점이 전장에서의 전투능력 상실로 이어짐
- 무기체계 소프트웨어의 보안취약점 최소화를 위해서는 소프트웨어 개발단계에서의 반복적이고 지속적인 보안 활동이 필요함
- 무기체계 획득 프로세스와 사이버보안의 연계성을 높이고
- 무기체계 사이버보안을 체계적으로 검증할 수 있는 통합보증체계(기술, 도구, 제도절차 등) 필요

감사합니다.

Q&A