the Korean Nuclear Society Spring Meeting, 2018

Cyber Security for Direct CDA Life-cycle

May. 18. 2018

Kookheui Kwon

Cyber Security Division

Korea Institute on Nuclear non-proliferation and Control

KINAC

KOREA INSTITUTE OF NUCLEAR NONPROLIFERATION AND CONTROL

Contents

I Security in the SDLC

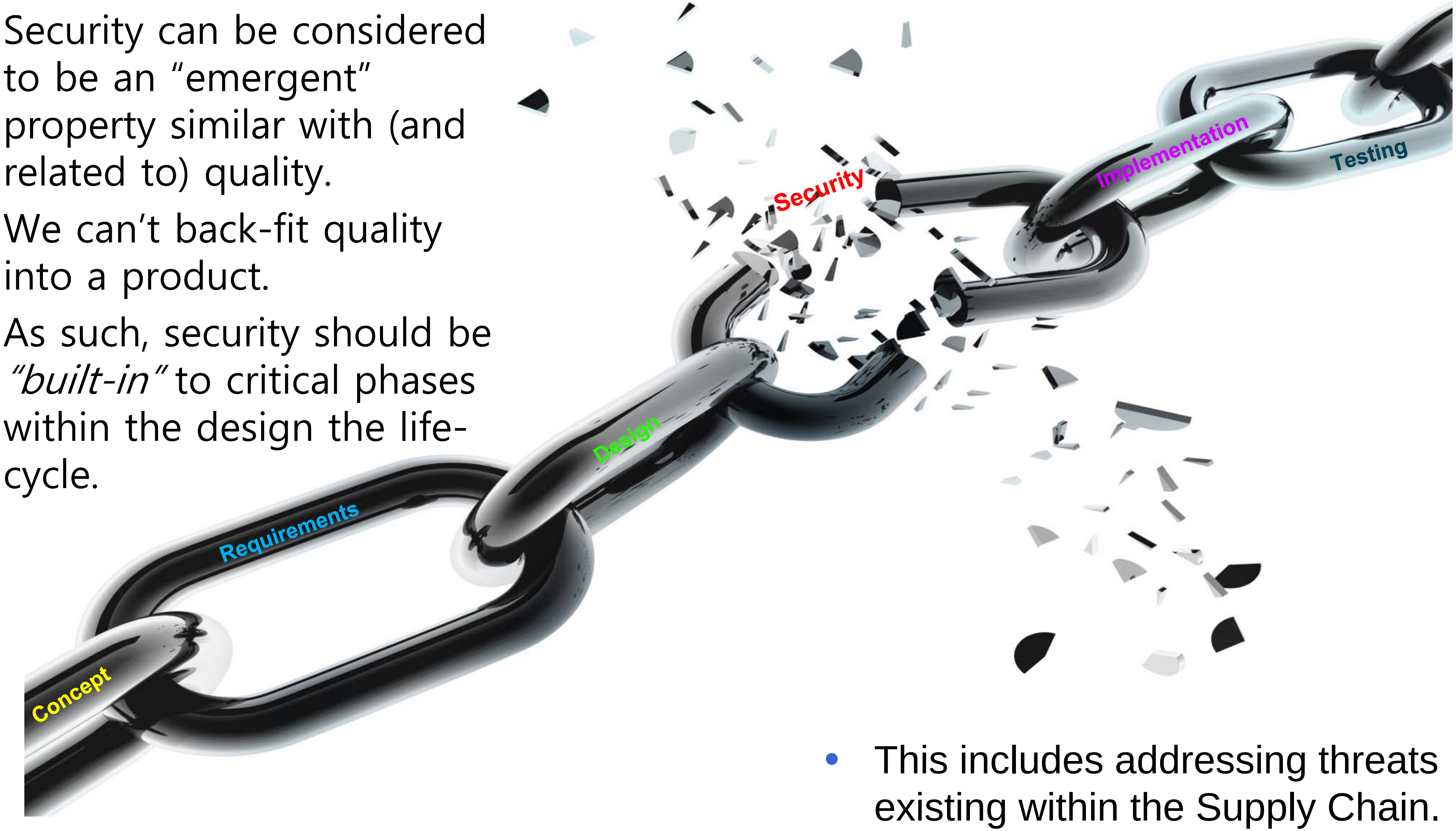
II Faced Issues

III Security Activities for Direct CDA Lifecycle

IV Summary

Security in the SDLC

- Security can be considered to be an “emergent” property similar with (and related to) quality.
- We can’t back-fit quality into a product.
- As such, security should be *“built-in”* to critical phases within the design the life-cycle.



- This includes addressing threats existing within the Supply Chain.

Security in the SDLC

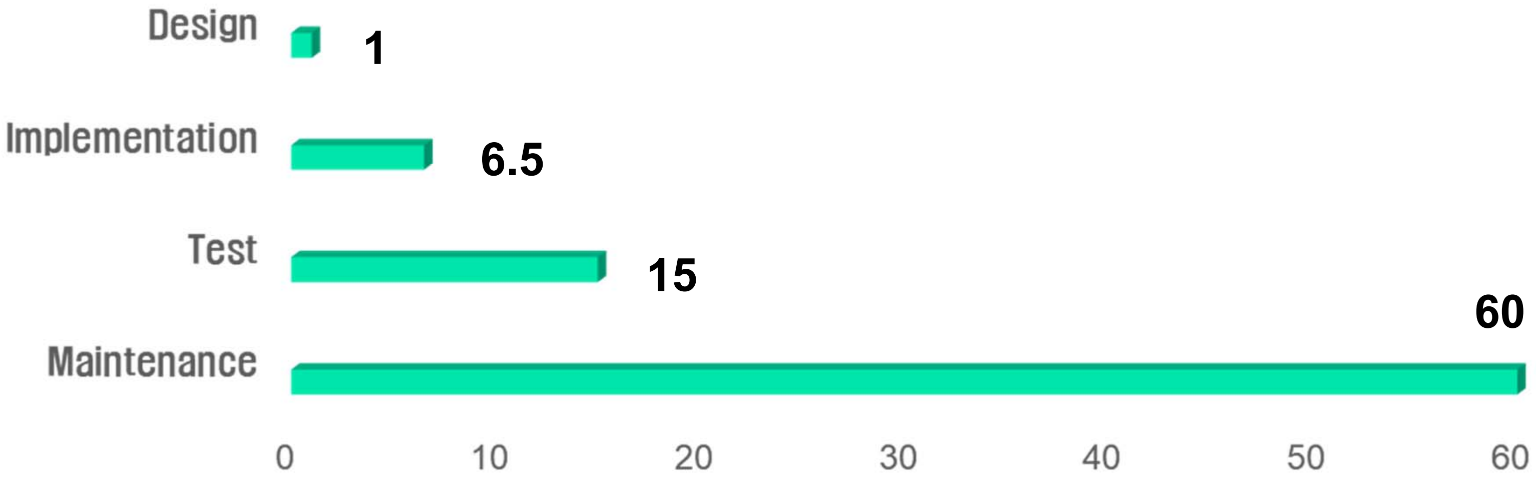
- **CMU S/W Engineering Center (2006)**

  - 70% of security vulnerabilities occur during the design process

- **Microsoft (2007)**

  - Applying SDL(secure development lifecycle) to the development phase reduces security vulnerabilities by 50 ~ 60%.

< Cost against Vulnerabilities >



Security in the SDLC – IAEA perspectives

- **NSS-13 (INFCIRC/225/Rev.5, 2011)**

  - Computer based systems used for physical protection, nuclear safety, and nuclear material accountancy and control should be protected against compromise(e.g. cyber attack, manipulation or falsification) consistent with the threat assessment or DBT

- **NSS-17 (TG for computer security, 2011)**

  - Risk management for nuclear cyber security should be done by system lifecycle including design, development, operation and maintenance.

- **NST036 (TG for com. security of I&C system, 2017/Q4)**

  - Describes the common and specific security requirements of the I&C system lifecycle
  - Describes requirements of Security evaluation, DID strategy, security by design, configuration management, security V&V, HW/SW security analysis, supply chain control, design change, media control, etc.

Security in the SDLC – domestic perspectives

▫ **DBT of cyber-attack**

- Classified that cyber attack can occur during design, development and supply
- Threat assessment and evaluation of facilities' cyber security system in every 3 years

▫ **Technical Security Issues**

- Effective Vulnerability Assessment and Removal
- Hard to apply & assess technical security controls during sys. operation
- Critical security issues made design change & process delay
- Consideration safety features(response time, system performance, HFE, etc.)

<u>Application of Security in the SDLC</u>

Faced Issues

- ❑ All CDAs should be considered all security requirements during development ?

- ❑ How will the RS-015 security requirements be applied to the development ?

Faced Issue – NEI 13-10, rev.6

- **Consequence-based Graded Approach**
- NRC endorsed this document as a way to satisfy RG 5.71
- It classifies CDAs that is not have an adverse impact on Safety and Security function as Non-direct CDAs, and it applies baseline security controls
- Non-Direct CDAs are required only the followings during development
  - Internal pre-operational testing
  - Malicious code scanning when possible
  - Calibration / configuration program

<table>
<tr><th>Direct CDA</th><th colspan="3">Non-Direct CDA</th></tr>
<tr><td rowspan="2">Cyber security Activities during development</td><td>Indirect</td><td>BOP</td><td>EP</td></tr>
<tr><td colspan="3">- Consideration of Baseline security controls
- Internal pre-operational testing
- Malicious code scanning when possible
- Calibration / configuration program</td></tr>
</table>

Faced Issue – RS-015 security req.

- **System and Service Acquisition**
  - Supply Chain Protection
  - Trustworthiness
  - Integration of Security Capabilities
  - Developer Security Testing
  - Applicant testing

- **Risk Management**
  - Threat and Vulnerability Management
  - Corrective Action Program

Pre-development security activities

- To analyze whether it is a CDA and Direct CDA through analysis of the function and the consequence
- classified by the security level according to the defense-in-depth strategy
- development with effective security requirements during life-cycle of the system considering communication network
- risk assessments taking into account the overall system architecture should be performed in advance

2.2.2 필수디지털자산의 식별

2.2.4 심층방호 전략

2.2.5 사이버 보안조치

Security activities during Development

❑ COMMON SECURITY ACTIVITIES

- **Configuration Management**

- Configuration changes including security configuration should be properly controlled
- Known vulnerabilities should be removed and recorded in accordance with configuration management procedures

- **Integrity Management**

- Physical and logical access controls should be properly performed and monitored.
- Only security-proven software, hardware, and development tools should be used and related files should be checked.
- The latest threat and vendor vulnerability information should be received and applied through assessment

3.1.4 개발자 보안 테스트
필수디지털자산 설계, 개발, 구현 및 운영 기간 동안 형상관리 수행

3.1.4 개발자 보안 테스트
시스템 개발자로 하여금 사이버보안 프로그램을 개발하여 시스템 납품과정에서 무결성 유지되었음을 보장
→ **2.2 시스템 및 정보의 무결성**

Security activities during Development

❑ COMMON SECURITY ACTIVITIES (계속)

- **Verification and Validation**

- The independent V&V for security requirements should be included in the system V&V program

- In particular, software V&V should include static source code vulnerability analysis, dynamic security testing.

- **Security Audit**

- An independent audit by CST in accordance with the cyber security program should be carried out.

3.1.4 개발자 보안 테스트
개발자로 하여금 확인 및 검증 수행을 통해 보안요건이 반영되었음을 보장, 소스코드 취약점 분석
3.2.1 위협 및 취약점 관리
보안테스트(침투테스트, 악의적 사용자테스트, 독립적인 V&V 등)

3.1.2 신뢰성 확보
개발자가 품질보증절차를 거치도록 요건을 개발, 이행 및 문서화

Security activities during Development

❑ Requirement Phase

- Risk assessments of the target CDA should be performed
- Analyzes whether security measures are applied
- The security requirements according to the assessment results are reflected in the req. specification
- In particular, a risk assessments program for pre-developed product is required.

2.2.5 사이버 보안조치
사이버 위험요소 평가를 통해 CDA를 보호를 위한 보안조치 적용

3.1.4 개발자 보안테스트
재사용 소프트웨어 및 상용품에 대한 보안검증 요구

Security activities during Development

❑ Design & Implementation Phase

- According to the security req. of the req. specification, the H/W and S/W of CDA are designed.
- Operational security measures should also be considered at the design phase for the operation and maintenance of CDA
- the results of the security design should be reflected in the design specification.
- At the implementation phase, the security design for H/W and S/W is applied and integrated
- Cyber security program for designer or manufacturer should be established in accordance with licensee's CSP.

2.2.5 사이버 보안조치
사이버 위험요소 평가를 통해 CDA를 보호를 위한 보안조치 적용

3.1.4 개발자 보안테스트
시스템 개발자로 하여금 사이버보안 프로그램을 개발하여 무결성 유지, V&V 및 다음 활동들을 통해 보안요건이 제품에 반영되었음을 보장

Security activities during Development

❑ **Test Phase**

- The test includes unit, integration, penetration, and malicious user testing.

- Check that security req. have been adequately implemented, and impact on safety functions.

❑ **Installation, Acceptance & Commissioning Phase**

- The security test and validation activities normally continue to the installation and commissioning phase

- these activities should be performed in a secure environment in accordance with the licensee's CSP

- Supply process control should be properly implemented

3.1.4 개발자 보안 테스트
다. S/W 테스트 결과
마. 보안요건에 따른 설계가 코드에 반영되었음을 보장하는 단위 테스트
3.2.1 위협 및 취약점 관리
바. 보안테스트(침투테스트, 악의적인 사용자 테스트, 독립 V&V 등) 수행

3.1.5 인수테스트
CDA 적용된 보안조치들이 인수테스트 시점에도 유효하며 제대로 기능하는지 확인
3.1.1 공급망 통제
공급받은 CDA의 무결성을 유지하고 공급과정으로부터 보호

Security activities during Operating

❑ **Operation Phase**

- Ongoing monitoring and effectiveness assessment
- Periodic security audit including system log, assess log, integrity, malicious code scanning
- Training in accordance with Cyber incident response plan

❑ **Maintenance & Modification Phase**

- Access control of the personnel, media, communications for CDA integrity
- assessment of the impact on the overall system security
- During the modification, V&V should be made through the same activities of SDLC

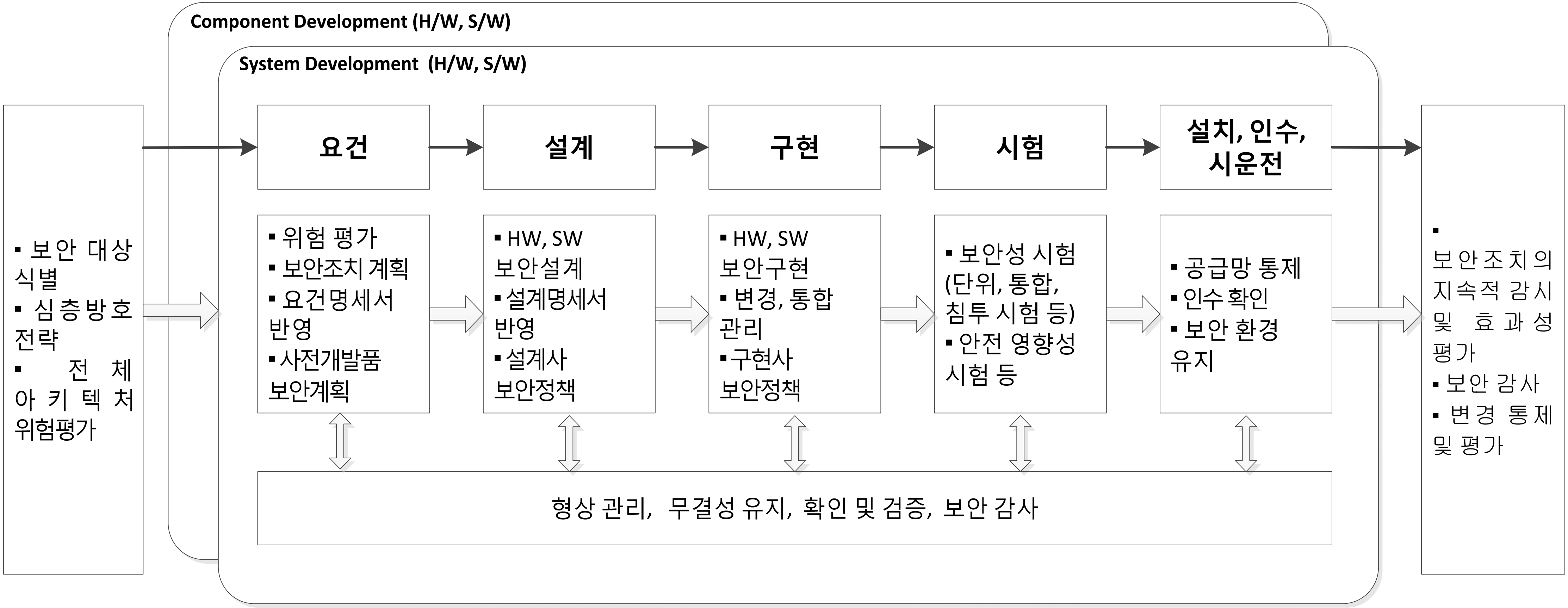
❑ **Retirement Phase**

2.4.1 지속적인 감시 및 평가

2.4.3 변경 통제

Summary

❑ Cyber Security for Direct CDA Lifecycle



Component Development (H/W, S/W)

System Development (H/W, S/W)

- 보안 대상 식별
- 심층방호 전략
- 전체 아키텍처 위험평가

요건

- 위험 평가
- 보안조치 계획
- 요건명세서 반영
- 사전개발품 보안계획

설계

- HW, SW 보안설계
- 설계명세서 반영
- 설계사 보안정책

구현

- HW, SW 보안구현
- 변경, 통합 관리
- 구현사 보안정책

시험

- 보안성 시험 (단위, 통합, 침투 시험 등)
- 안전 영향성 시험 등

설치, 인수, 시운전

- 공급망 통제
- 인수 확인
- 보안 환경 유지

형상 관리, 무결성 유지, 확인 및 검증, 보안 감사

- 보안조치의 지속적 감시 및 효과성 평가
- 보안 감사
- 변경 통제 및 평가

Questions ?

vivacita@kinac.re.kr