IEC 62645

김의섭, 서영주

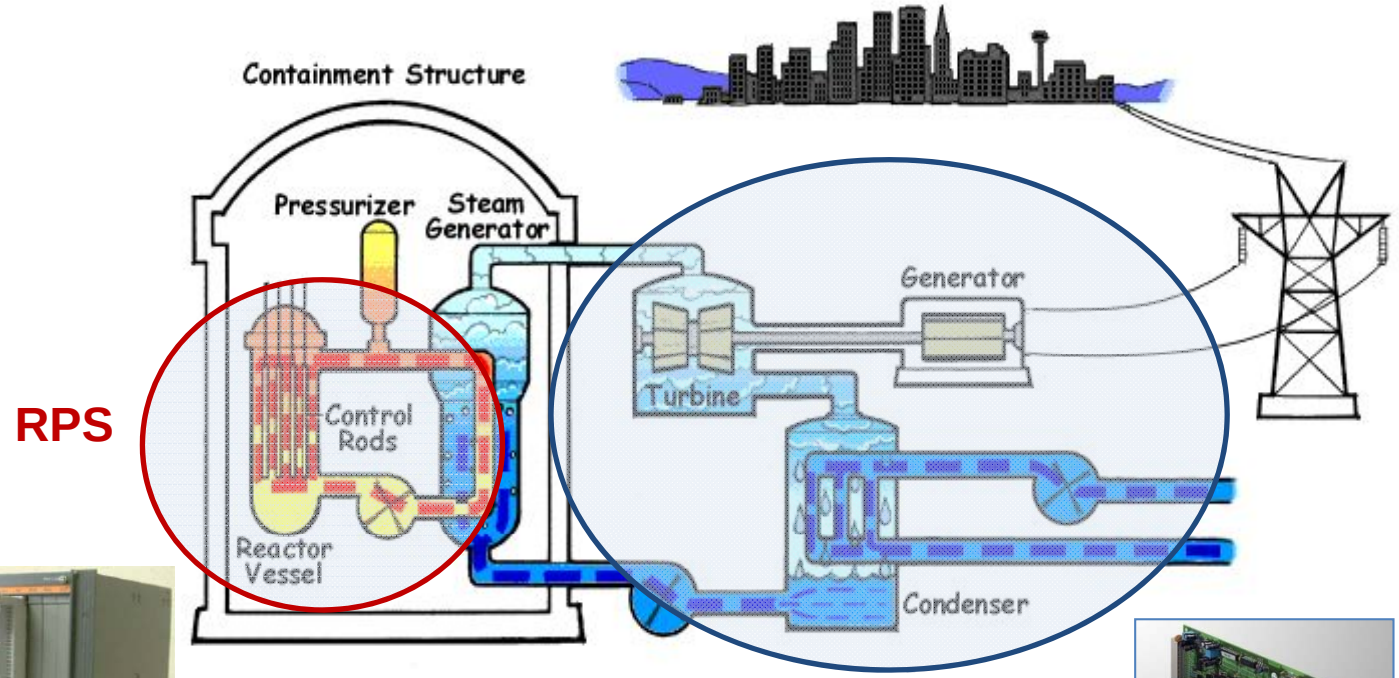
목차

- 1. Overall
- 2. Application
  - 5장 – Plan -Do-Check-ACT
  - 6장 – Security Development Life Cycle
  - 7장 – Control
- 3. CMMI
- 4. Conclusion

OVERALL

Overall

- Target
  - KNICS (Korea Nuclear Instrumentation & Control System)
    - RPS (Reactor Protection System)
    - ESF-CCS (Engineering Safety Features Component Control System)



PLC
(Programmable Logic Controller)

DCS
(Distributed Computing System)

KNICS (Korea Nuclear Instrumentation & Control System)

원전의 사고를 방지하거나 완화시키는 기능
원전 특성으로 인한 고유한 기능

설계부터 구현까지 엄격한 절차와 검증 필요

안전 관련 변수를 감지, 미리 설정된 위험 상태의 접근 여부를 판단. **위험 판단** 시 사고 상태로 진전 되는 것을 막기 위하여 **원자로를 정**지시키거나 사고 시 이를 **완화 시키기 위한 제반 기기의 작동을** 개시 하고 감시

계측제어 계통
온도, 압력 등의 공정변수들을 감지 및 처리하여 관련 계통에 변수 데이터를 제공

BOP 계통
이차측의 계측, 감시 제어에 요구되는 제반 기능을 수행하는 수많은 계통으로 구성

일반 산업 분야와 마찬가지로 플랜트 운전에 요구되는 계측, 에어, 감시 및 정보처리 기능

원전 운전을 위한 제반 제어 행위를 수행하는 **제어계통**

원전 전체의 상태 정보를 수집, 처리, 분석하고 경보와 화면 정보 제공하는 **정보 계통**

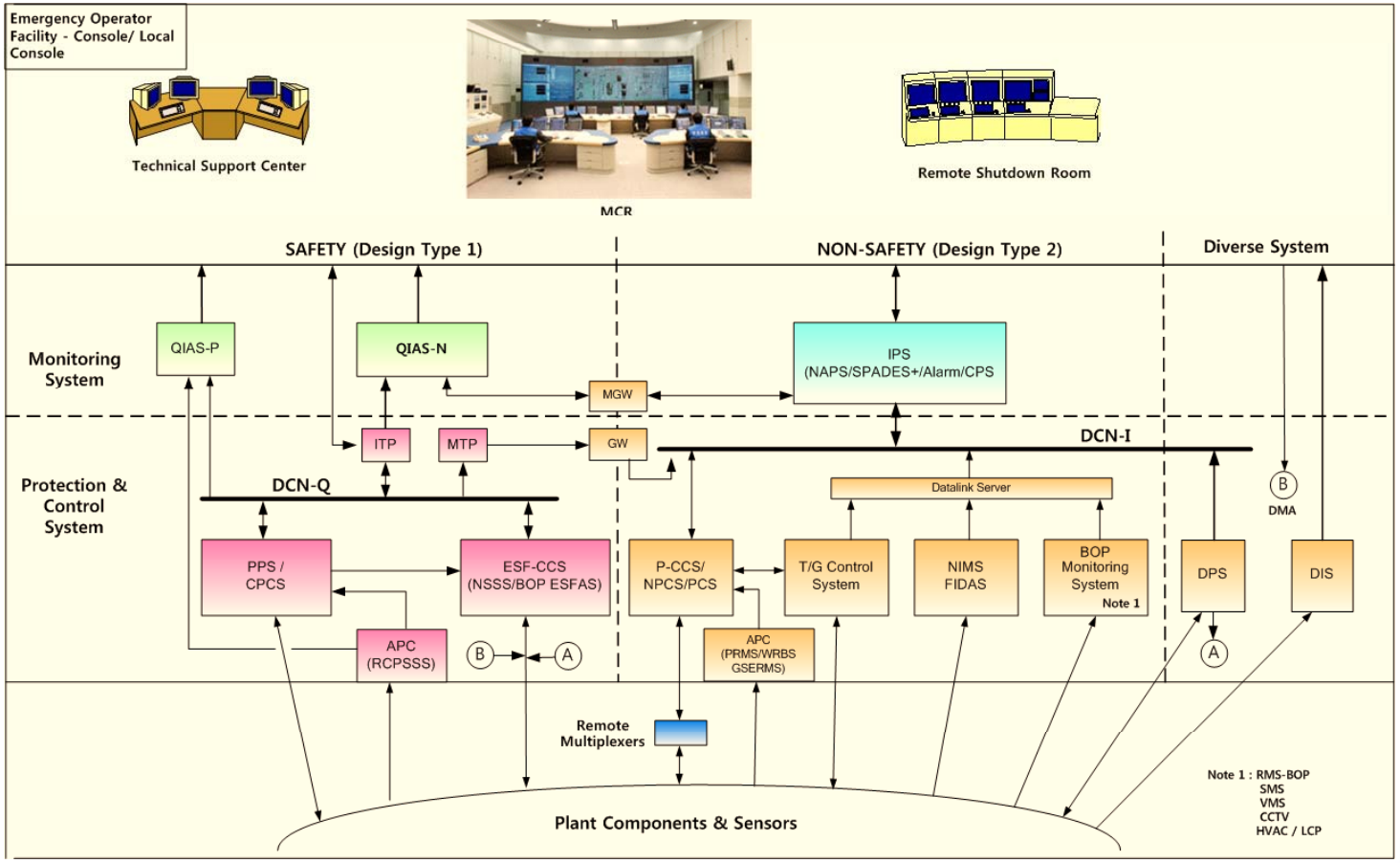
특정기능의 판단 및 감시를 위하여 데이터를 수집하고 처리하는 **감시계통**

현장 변수를 감지하고 처리하여 각 계통에 공급하는 **계측계통**

각종 **BOP 계통**

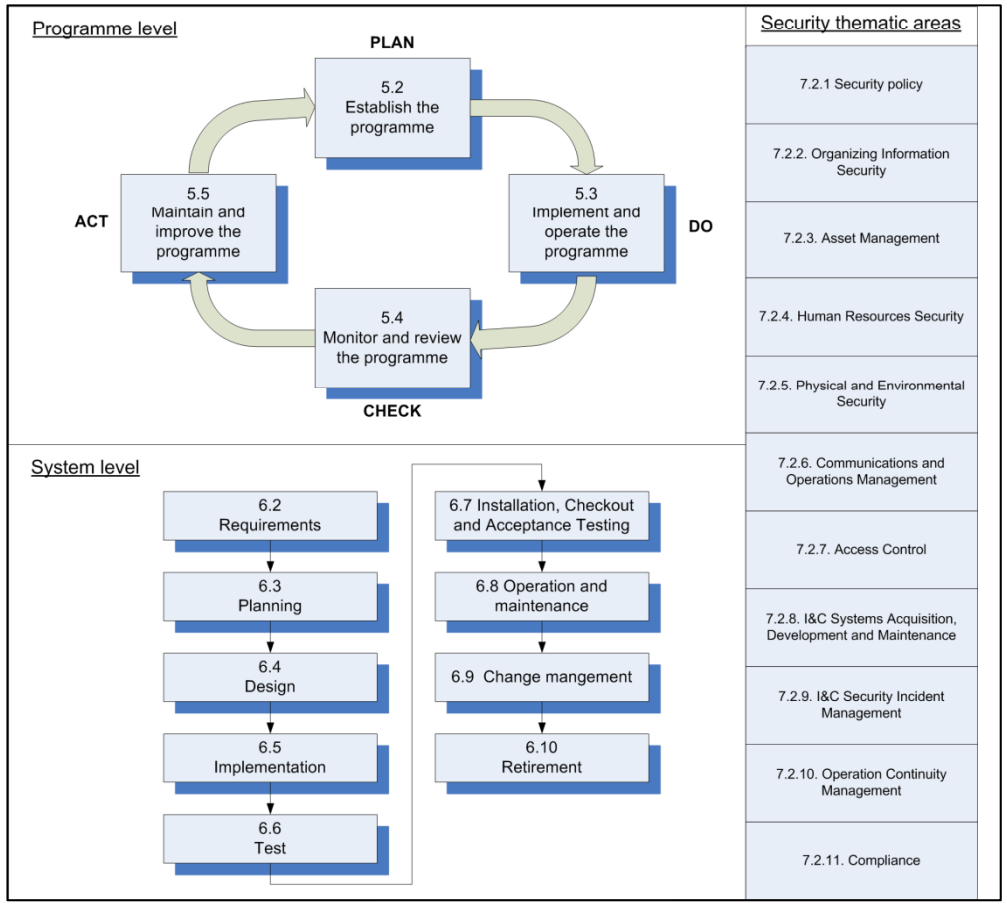
Overall

- Target
  - KNICS (Korea Nuclear Instrumentation & Control System)
  - 한국 원자력 발전소 계측제어 시스템



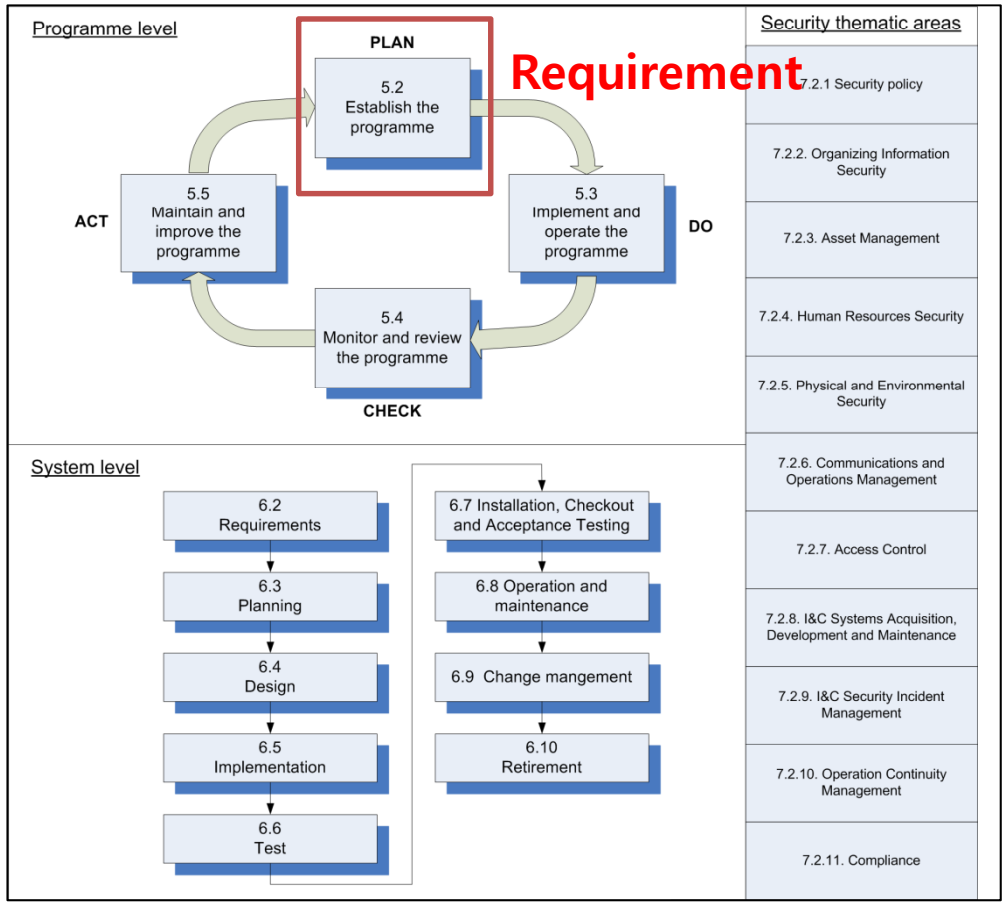
Overall

- Standard
  - IEC 62645
    - Nuclear power plants - Instrumentation and control systems - **Requirements for security programmes** for computer-based systems



Overall

- Standard
  - IEC 62645
    - Nuclear power plants - Instrumentation and control systems - **Requirements for security programmes** for computer-based systems



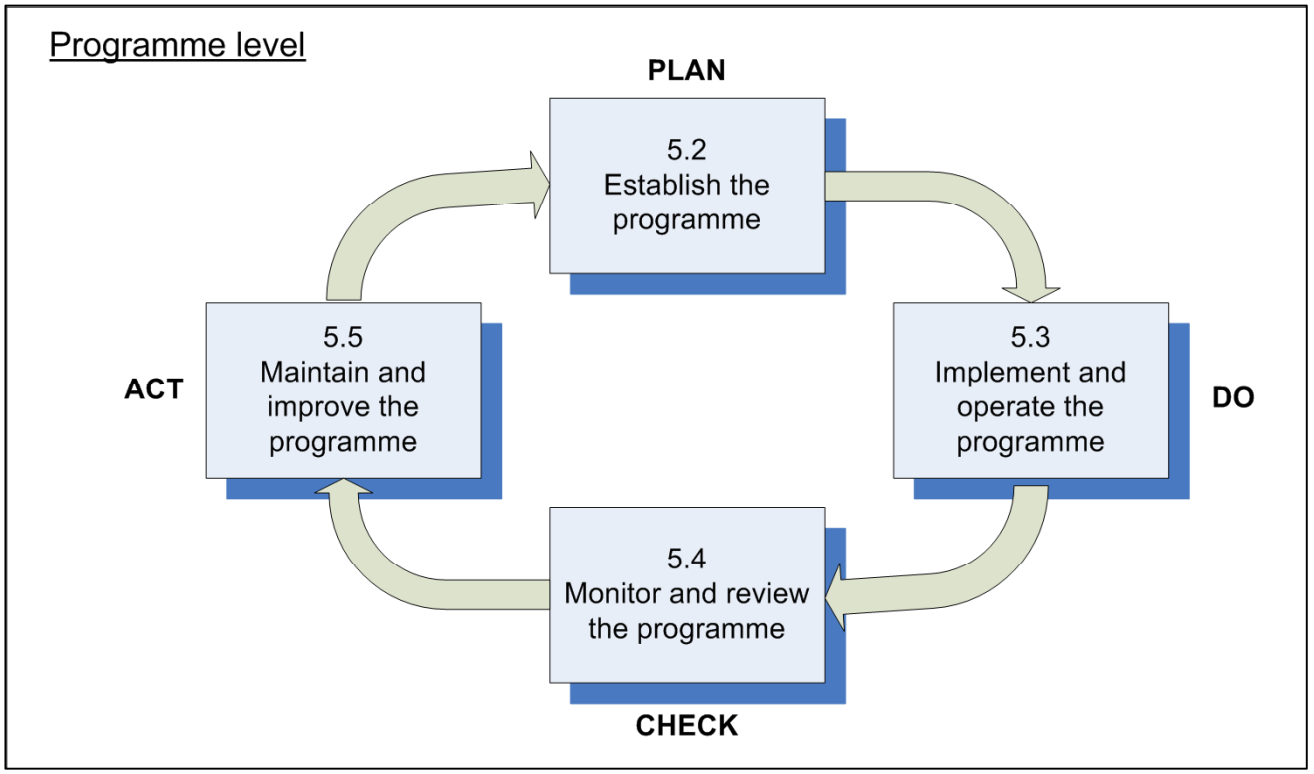
Overall

- IEC 62645
  - 소프트웨어 개발과 관련된 기본적인 사항은 **IEC 61513**을 따른다.
  - 개발 소프트웨어의 카테고리별 추가사항은 **IEC 60880, 62138**을 따른다.
  - 주 목표는 사고를 일으킬 수 있는 악의적인 행동을 막을 수 있는 프로그램을 개발 하는 것.
  - **Security**와 관련된 사항들은 **ISO/IEC 27000**대의 표준을 참고할 수 있지만 NPP의 특징들 때문에 직접적으로 적용할 수 있는 것은 아니다.

5장, 6장, 7장

APPLICATION

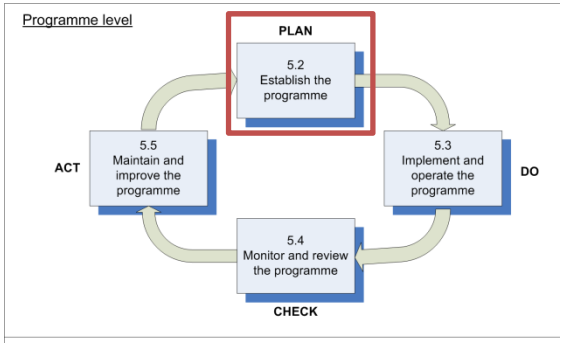
5장. Establishing and managing a nuclear I&C security programme



5.1

5.2 Establish the programme

- Description
  - 5.2.1 Defining security policy
  - 5.2.2 Defining the programme scope and boundaries
  - 5.2.3 graded approach to I&C security and risk assessment
    - 5.2.3.1 Security Zone
    - 5.2.3.2 Degree
    - 5.2.3.3 Assignment of technical requirements
  - 5.2.4 Management approval



5.2.1 Defining security policy

- Description
  - Defining security policy
  - The I&C Security Policy shall:
    - be **defined in terms of the characteristics** of the nuclear power plant's organization, its location, national regulatory requirements, digital I&C assets and technology, risk of system exploitation;
    - include a **framework** for setting objectives and establishes an overall sense of direction and principles for **action** with regard to digital I&C **security**;
    - take into account **legal** and **regulatory requirements**, as well as **contractual security obligations**;
    - ensure security requirements are applied through all levels of supply chain for all life cycle activities
    - align with the nuclear facility's strategic risk management context in which the establishment and maintenance of the I&C Security Programme will take place;
    - establish criteria against which risk will be evaluated including consideration of the outcomes from digital I&C system exploitation; and
    - have been **approved** by management.

5.2.1 Defining security policy

- Detailed solution
  - Security policy를 작성한다.
    - **사용되는 용어의** 해설 : 다른 표준들이나 산업에서 관련 자료를 찾는다.
    - Digital I&C security와 관련된 개발 **프레임워크 포함** : 해당 사항을 목적으로 한 프레임워크는 현재 존재하지 않는 것 같으므로 PSA(Probabilistic Safety Assessment)와 같은 risk assessment framework 등을 채택하고 security와 관련된 요구사항들을 추가로 집어넣는 방향으로 진행한다.
    - 거래처를 법적 규제 및 요구사항을 따르고 보안 의무를 따르는 곳으로 선정함 : security policy와 관련된 법적 규제 및 요구사항을 파악하고 해당 요건을 만족하는 곳만 거래처로 선정한다.
    - Security requirement는 모든 단계의 supply chain의 공급 레벨에 대해 적용됨을 보장해야 한다. : supply chain의 각 단계마다 security requirement가 보장되는지를 확인해서 문서화 한다.
    - I&C security programme은 핵시설의 전략적 리스크 관리 상황에 맞추어서 일어나야 함 : 전략적 리스크 관리 상황과 그에 맞는 security programme의 대응 관계를 문서화 한다.
    - establish criteria against which risk will be evaluated (see 5.2.2) including consideration of the outcomes from digital I&C system exploitation : IEC 60880이나 62138의 기준을 따른 피해 규모를 보고 리스크에 대한 기준을 세운다.

5.2.2 Defining the programme scope and boundaries

- Description
  - Defining the programme scope and boundaries
    - Security programme의 scope와 boundary에 들어가는 부분만 적용 대상으로 처리한다.
      - 주 목표는 사고를 일으킬 수 있는 악의적인 행동을 막기 위한 프로그램에 따른 판단 정의이므로 악의적인 행동이 아닌 경우에 대해서는 security programme에 포함되지 않는다.
      - 시스템의 완전성에 영향을 줄 수 있는 비인가 상태의 수정이나 정보, 데이터 또는 I & C 기능으로의 전달 또는 필요한 서비스의 성능을 손상시킬 수 있는 자원 간섭 등이 포함된다.

5.2.1 & 5.2.2

- Task
  - Defining security policy
    - Domain 용어집 문서화
    - Domain 관련된 규제, 규약, 표준 조사 및 문서화
    - Security 관련된 연구 현황 조사 및 문서화
    - Security 관련 계약서 문서화
  - Defining the programme scope and boundaries
    - location,
    - national regulatory requirements,
    - digital I&C assets and technology,
    - risk of system

- Solution
  - 직접 작성 및 관련 기관에 자료 요청

5.2.3.1 Security Zone

- Description
  - The application of a **zone** model should comply with the following guidelines:
    - Each zone comprises systems that have the same or comparable degree of security and importance for safety;
    - Systems belonging to one zone have similar demands for protective measures;
    - Different computers systems belonging to one zone build a trusted area for internal communication within that zone;
    - Network equipment (switches, cables, etc.) is located in a security zone consistent with those of the interconnected I&C systems;```
    - Zone borders require decoupling mechanisms for data flow built on zone dependent policies;
    - Zones can be partitioned into sub-zones to improve the configuration.

5.2.3.1 Security Zone

- Task
  - Security Zone 구성 (문서화)

- Solution
  - System에 관한 개발 설계, 요구 사항 문서 필요
  - Security zone 을 나눌 수 있는 기준 작성
  - Security zone 을 나눌 수 있는 process 개발 및 조사
  - 나누어진 Security zone 에 대한 assessment 방법 개발 및 조사
  - 문서화

5.2.3.2 Degree

- Task
  - Security degree 할당 (system, tool)

- Solution
  - Safety 요구사항 참조
    - 다른 표준 (61513, 61226 and 61513)을 참조.
      - 이미 만들어진 safety level (Category A, B, C Function)를 이용
        - » Ex) Category A Function -> S1
      - Safety level을 정하는 analysis 를 참조
  - Degree를 줄 수 있는 기준, process, assessment 작성
  - 또한, 개발에 사용되는 tool에 대해서도 security degree를 할당
    - Security에 인정받은 tool 조사, 인증 과정 진행
  - 문서화

5.2.3.3 Assignment of technical requirements

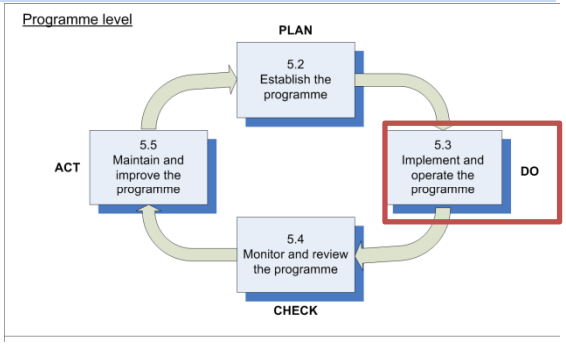
- Task
  - Technical requirement 할당 (문서화)

- Solution
  - Programm에 대한 security degree 할당이 선행
  - 등급별 제공하는 requirement를 할당
  - Programm에 대한 요구사항 문서 요청 및 작성
  - 추가적인 security requirement는 assessment activity를 통해 구현
    - vulnerability assessment
    - attack scenario analysis(including the country-specific design basis threat (DBT))
      - 관련자료 요청 및 조사, 작성

5.2.3.3 Assignment of technical requirements

- Detailed Solution
  - 어느 정도의 **신뢰성을** 보장할 수 있는 **디자인 방법**이 정의되어야 한다.
    - 기존에 있는 Security와 관련된 디자인 방법을 채택하거나 없을 경우에는 61513등의 개발 방법론을 기본으로 62645에서 도출된 요구사항을 만족시키는 방향으로 한다.
  - 기존에 개발된 소프트웨어를 사용할 경우에는 시스템의 **취약성을 최소화** 해야 한다
    - 60880 등 다른 표준에서 카테고리별로 pre-developed software의 검증에 대한 항목이 있으니 해당 내용을 따르는지 확인 후 사용한다.
  - 소프트웨어 security 분석은 소프트웨어나 시스템의 QA 계획이나 security 계획을 고려해야 한다.
    - Security에 대한 분석을 하기 전에 해당 소프트웨어에 대한 QA 계획 또는 security 계획이 존재하는지 확인 후 분석을 시작한다. 없을 경우 해당 부분에 대한 계획을 먼저 수립한다.
  - 데이터 연결은 덜 중요한 security degree의 시스템과 이루어져야 한다.
    - Security degree를 나눈 상태에서 높은 등급의 security degree를 가진 시스템은 외부 혹은 차이가 심한 등급의 시스템에서 직접 데이터를 받지 않는 형태로 설계한다.
  - 소프트웨어나 파라미터의 **변경사항 추적**
    - SVN, CVS 등의 도구를 사용하여 변경사항이 있을 경우 해당 정보를 기록으로 남긴다.
  - 소프트웨어 기능이나 메모리에 대한 유저의 접근 제한
    - 논리적인 사용자 등급의 부여가 가능할 경우 이를 통해서 접근 제한. 불가능할 경우 인가 받은 사용자만 해당 작업을 수행할 수 있도록 한다.
  - 시스템의 V&V 과정 동안 적절한 테스트 케이스를 통해 security function의 효과를 보일 것
    - ISO/IEC 27000번 대의 표준 및 카테고리 별 표준을 참고로 하여 효율적인 테스트 케이스의 도출을 함을 전제로 함. V&V 과정은 61513 또는 60880 등의 내용을 따르며 여기에 추가로 정의된 security에 대한 V&V도 수행하며 이 결과를 문서화하여 security function의 효과를 보인다.
  - **사용자의 접근이 허가되기 전에 효과적인 인증 절차를 제공하기 위한 기술적인 방법이 있어야 한다.**
    - 사용자의 인증에 대한 부분은 NPP의 특수성이 크게 반영되지 않을 것이므로 ISO/IEC의 고려사항을 따른다.

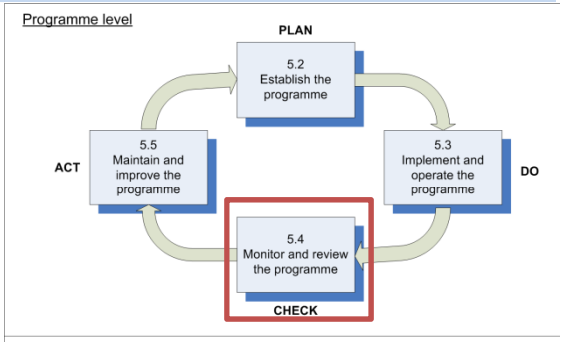
5.3 Implement and operate the programme



- 2. Do
  - 1. 구현
    - Security requirement 가 잘 반영이 되도록 구현
  - 2. 실행
    - cyber attack에 관해 지속적인 관리, update
    - 관련 사람들에 대한 Training

- Solution
  - Security requirement가 잘 구현 되었는지 Metric 작성을 통해 확인
    - Metric 구성
  - Cyber attack에 대한 지속적인 조사
  - Training 과정 개설, 지속적인

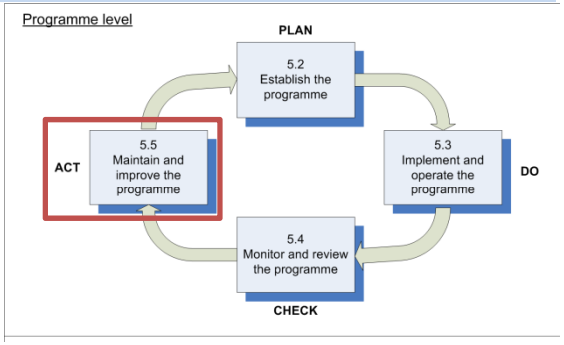
5.4 Monitor and review the programme



- 3. Check
  - Monitor and review the programme
  - To conduct period security program reviews.

- Solution
  - Reviewing 할 요소를 작성
  - Monitor, review 할 수 있는 program, procedure를 작성

5.5 Maintain and improve the programme

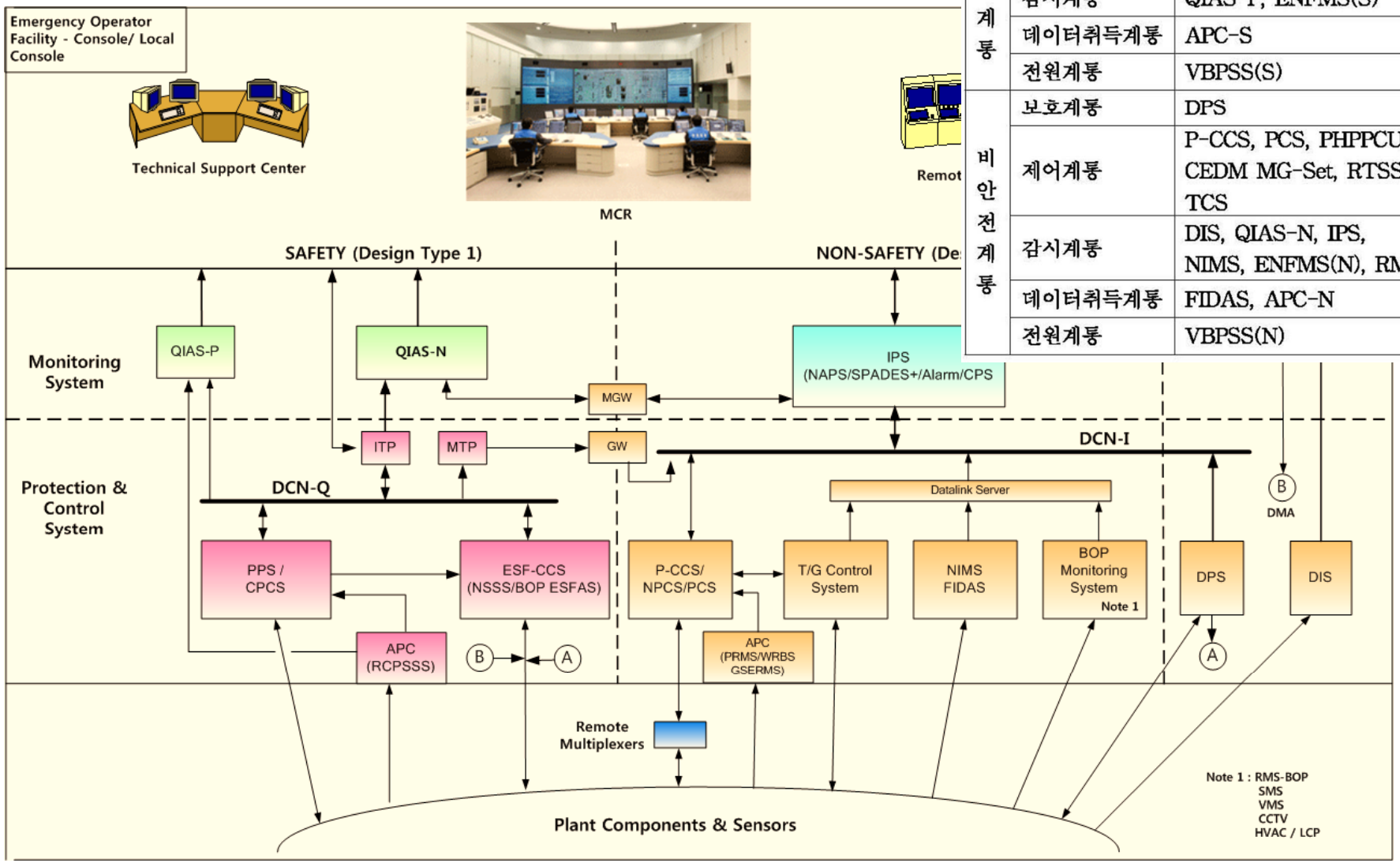


- 4. ACT
  - internal and external programme reviews
  - ongoing training programme
  - periodically evaluate and update the security threat assessment
  - measures to evaluate whether the improvements achieved their intended objectives

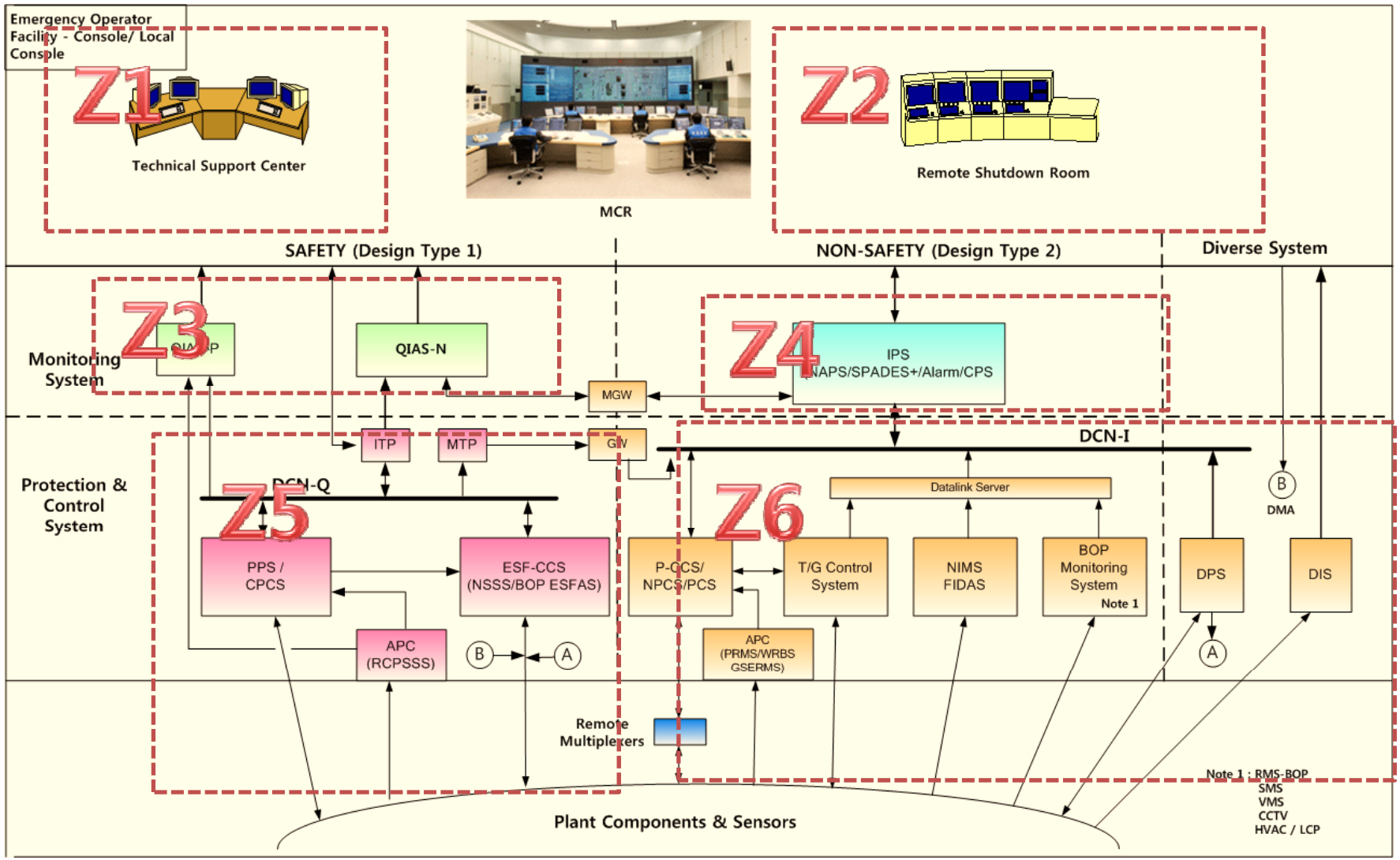
- Solution
  - 지속적인 security threat를 조사
  - ongoing training programme 계획 수립
  - Update에 대한 Improvements 를 확인할 수 있는 기준, process등을 확립

Graded approach to I&C security and risk assessment

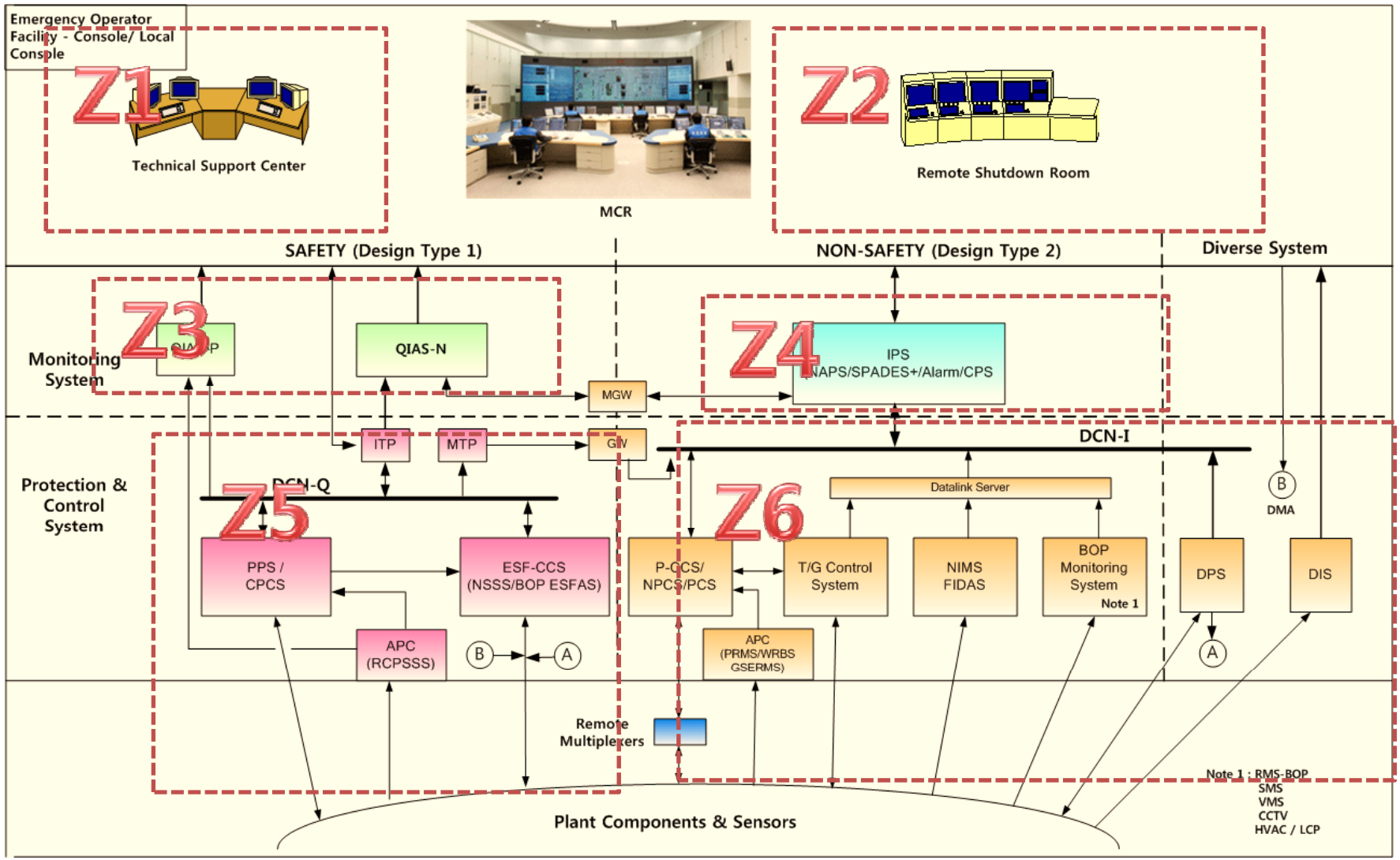
안전계통	보호계통	PPS, CPCS, ESF-CCS, MTP/ITP
	감시계통	QIAS-P, ENFMS(S)
	데이터취득계통	APC-S
	전원계통	VBPSS(S)
비안전계통	보호계통	DPS
	제어계통	P-CCS, PCS, PHPPCU, CEDM MG-Set, RTSS, TCS
	감시계통	DIS, QIAS-N, IPS, NIMS, ENFMS(N), RMS
	데이터취득계통	FIDAS, APC-N
	전원계통	VBPSS(N)

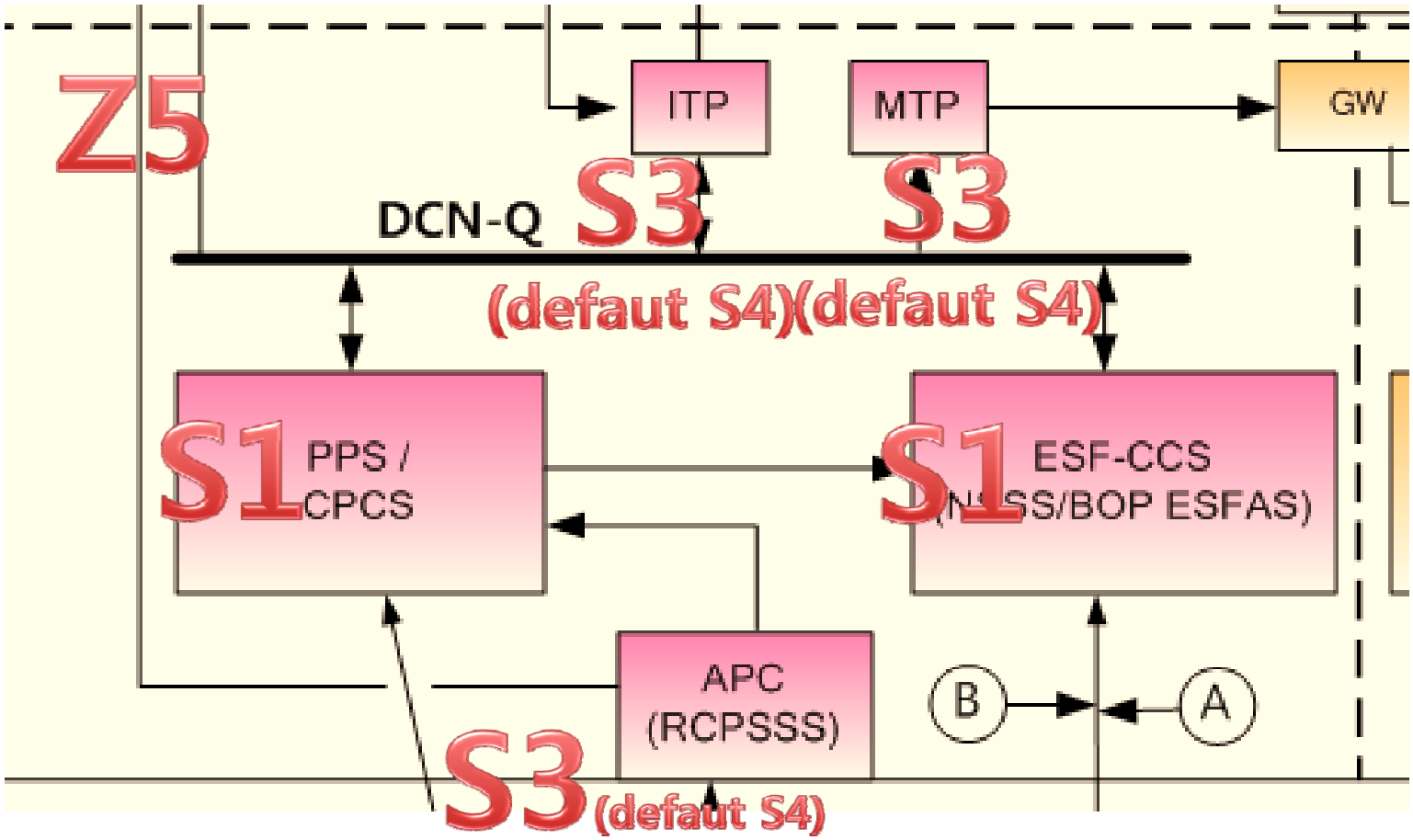


Graded approach to I&C security and risk assessment

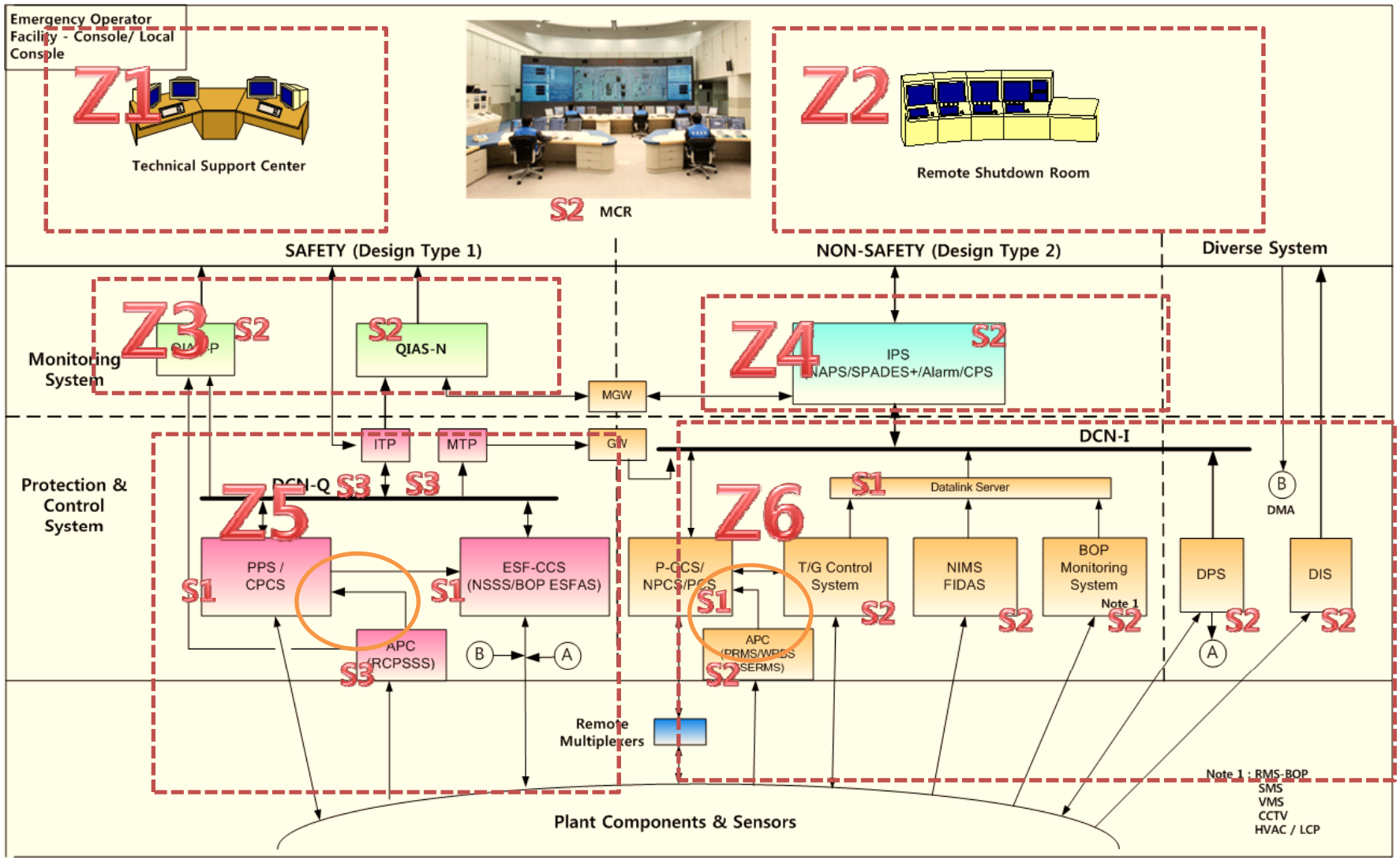


Graded approach to I&C security and risk assessment




Z5
ITP
MTP
GW
DCN-Q
S3
S3
(defaut S4)(defaut S4)
S1
PPS /
CPCS
S1
ESF-CCS
SS/BOP ESFAS)
APC
(RCPSSS)
B
A
S3
(defaut S4)

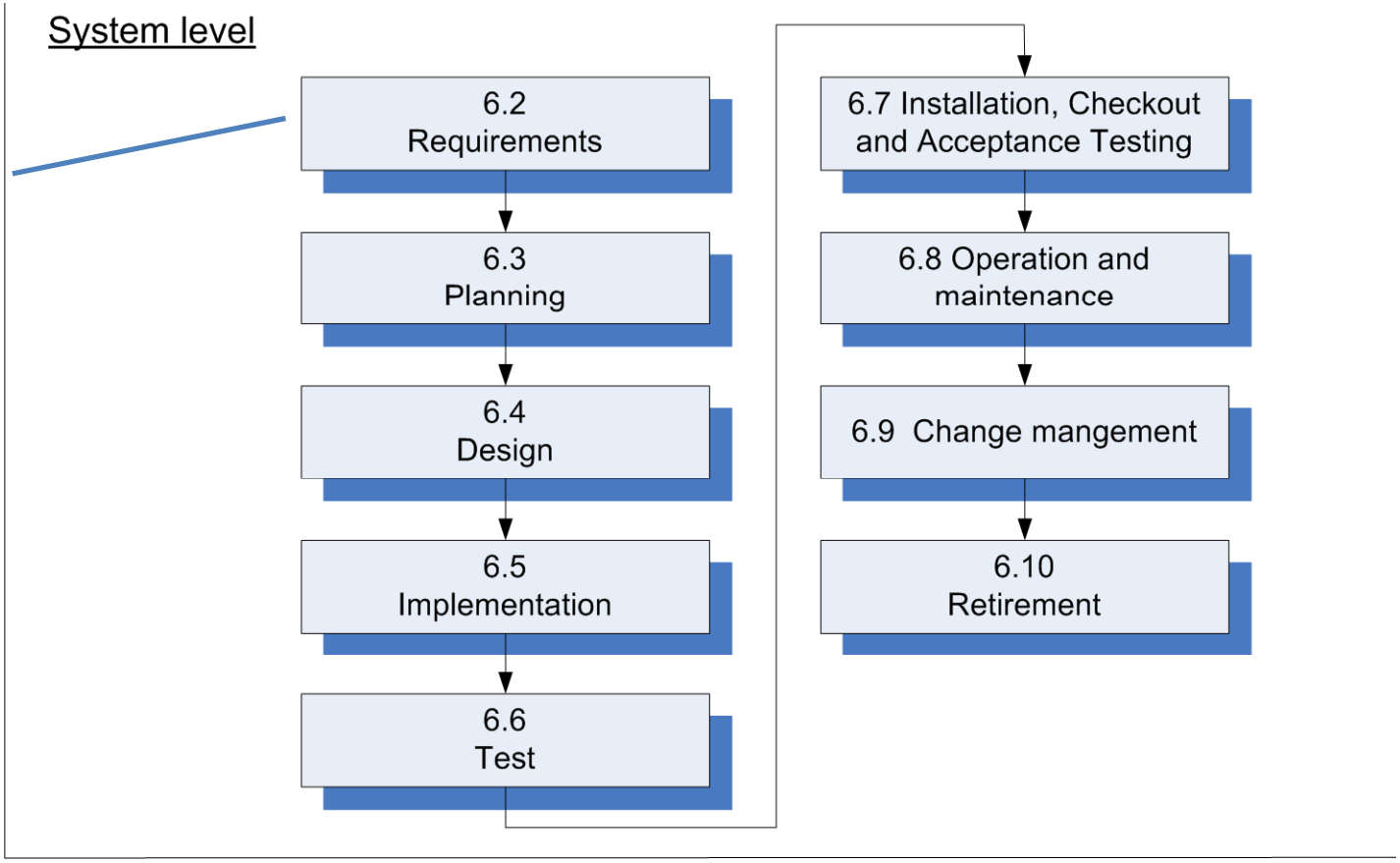
Graded approach to I&C security and risk assessment



6. Life Cycle Implementation for I&C system security

A security degree 에 의해 할당된 requirement 가 잘 반영 되었는지 확인 해야 한다.

적절한 방법 필요

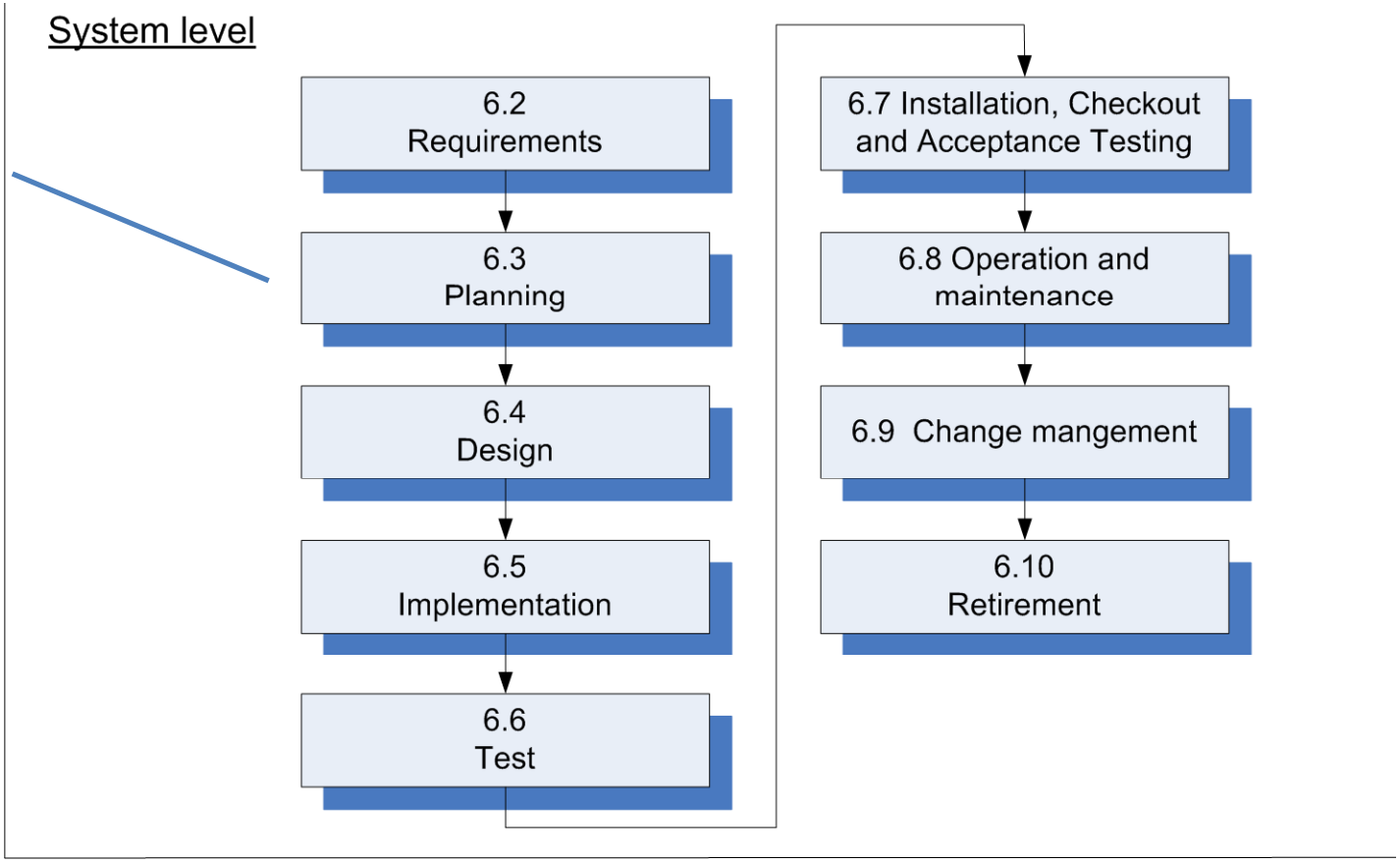


6. Life Cycle Implementation for I&C system security

추가적으로 어떤 기능이 security를 위해 분석 되어야 할지 요소인지 analysis 해야 한다.

각각의 digital device 간의 pathways에 대한 vulnerabilities, security risk 평가 해야한다.

적절한 방법 필요

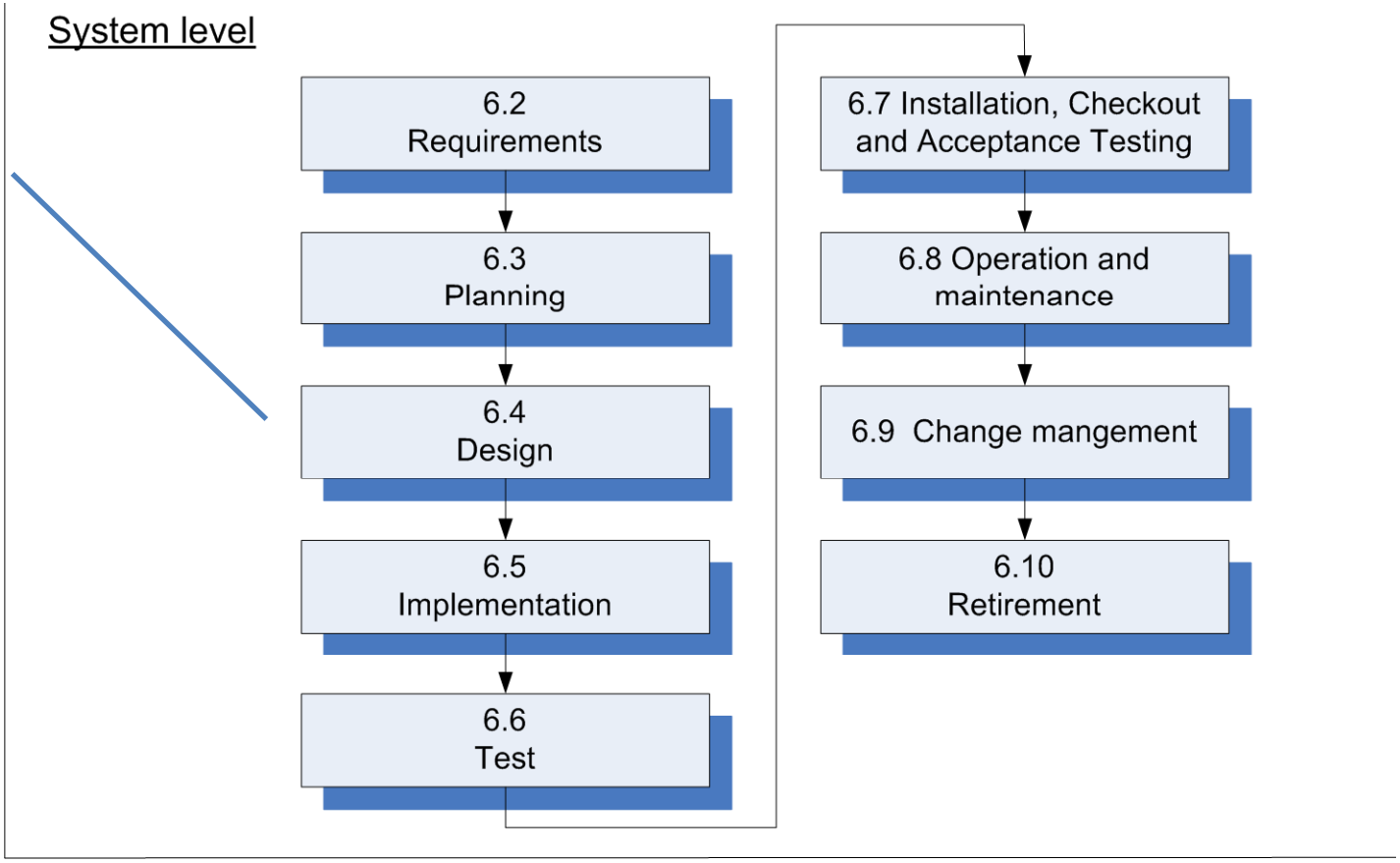


6. Life Cycle Implementation for I&C system security

requirements 에서 정의된 item에 대해 configuration management 를 해야 한다.

The requirements shall be translated into specific design criteria.

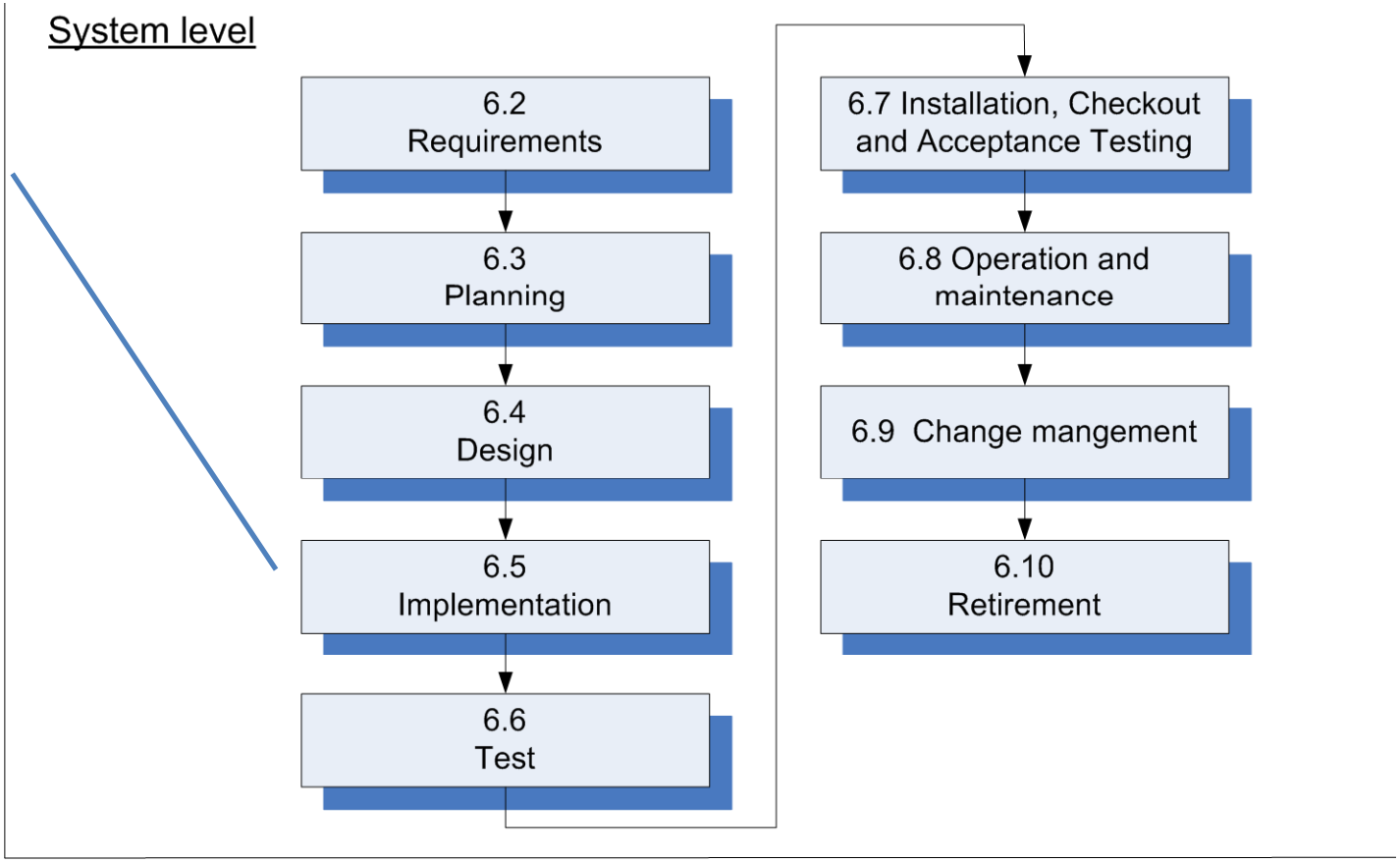
적절한 방법 필요



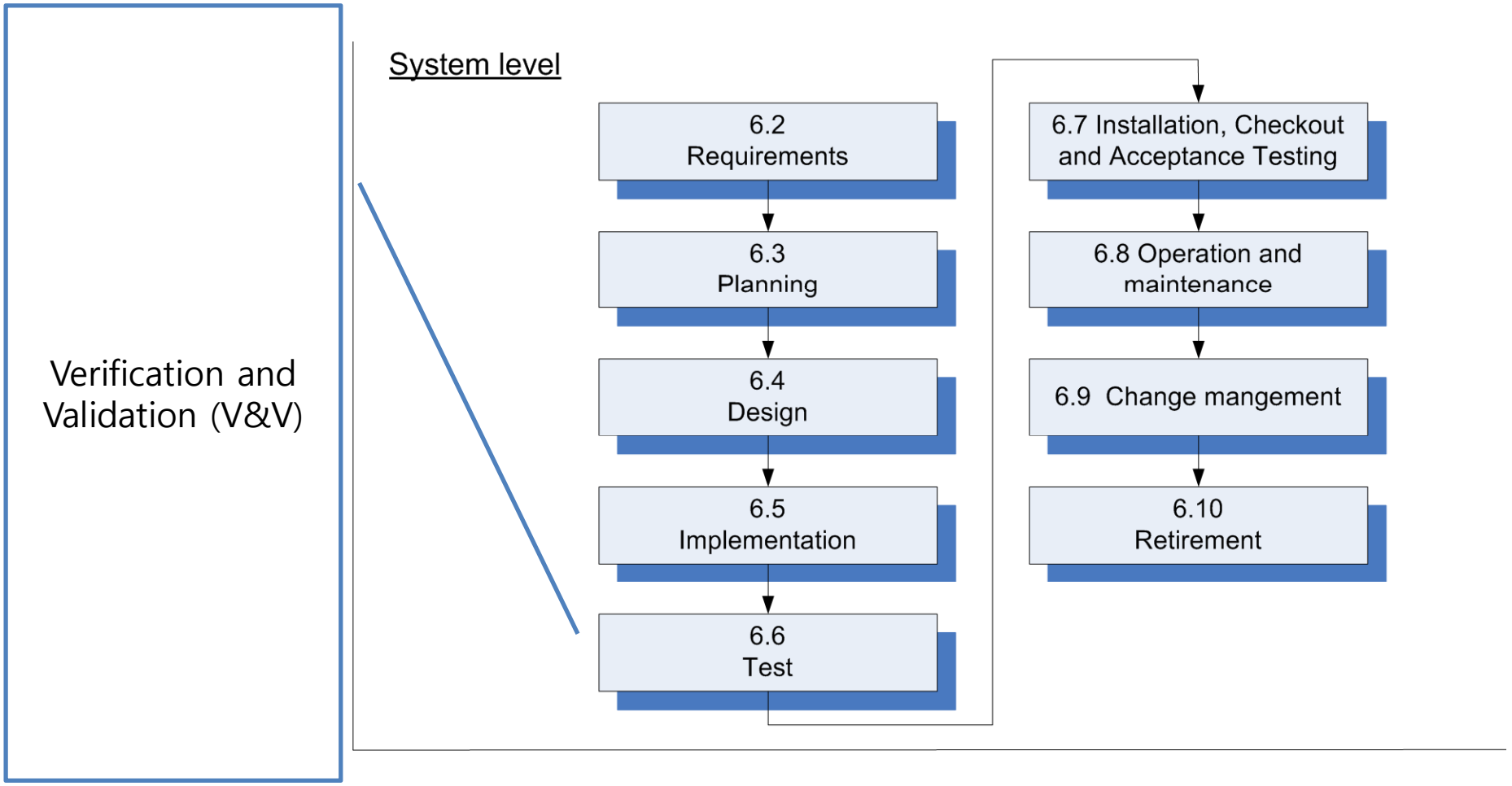
6. Life Cycle Implementation for I&C system security

code, database structures, and related machine executable representations 로 만들어 질 때 정의된 모든 **security requirements** 가 포함이 되도록 통합 해야 한다.

확인할 수 있는 방법 필요

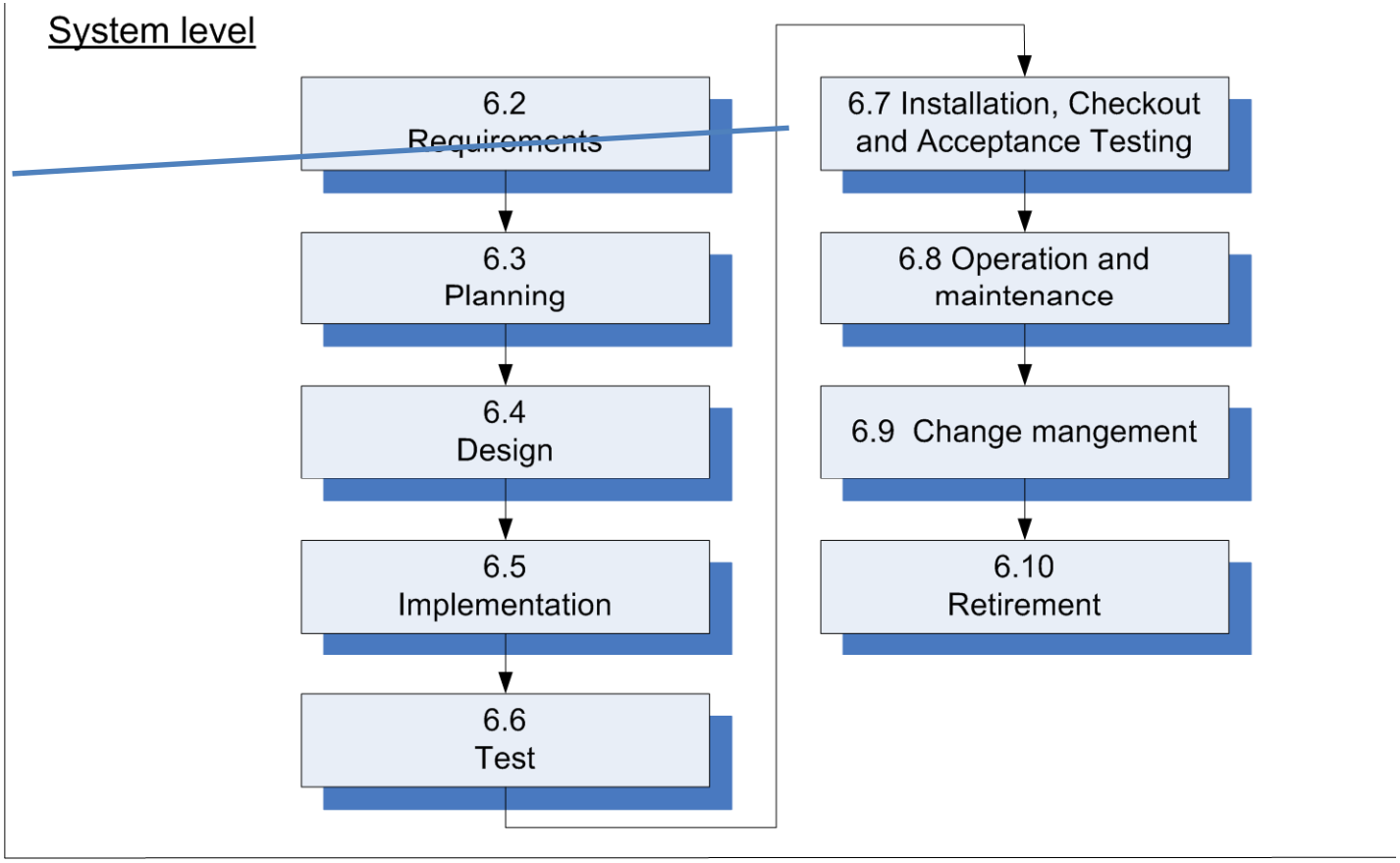


6. Life Cycle Implementation for I&C system security



6. Life Cycle Implementation for I&C system security

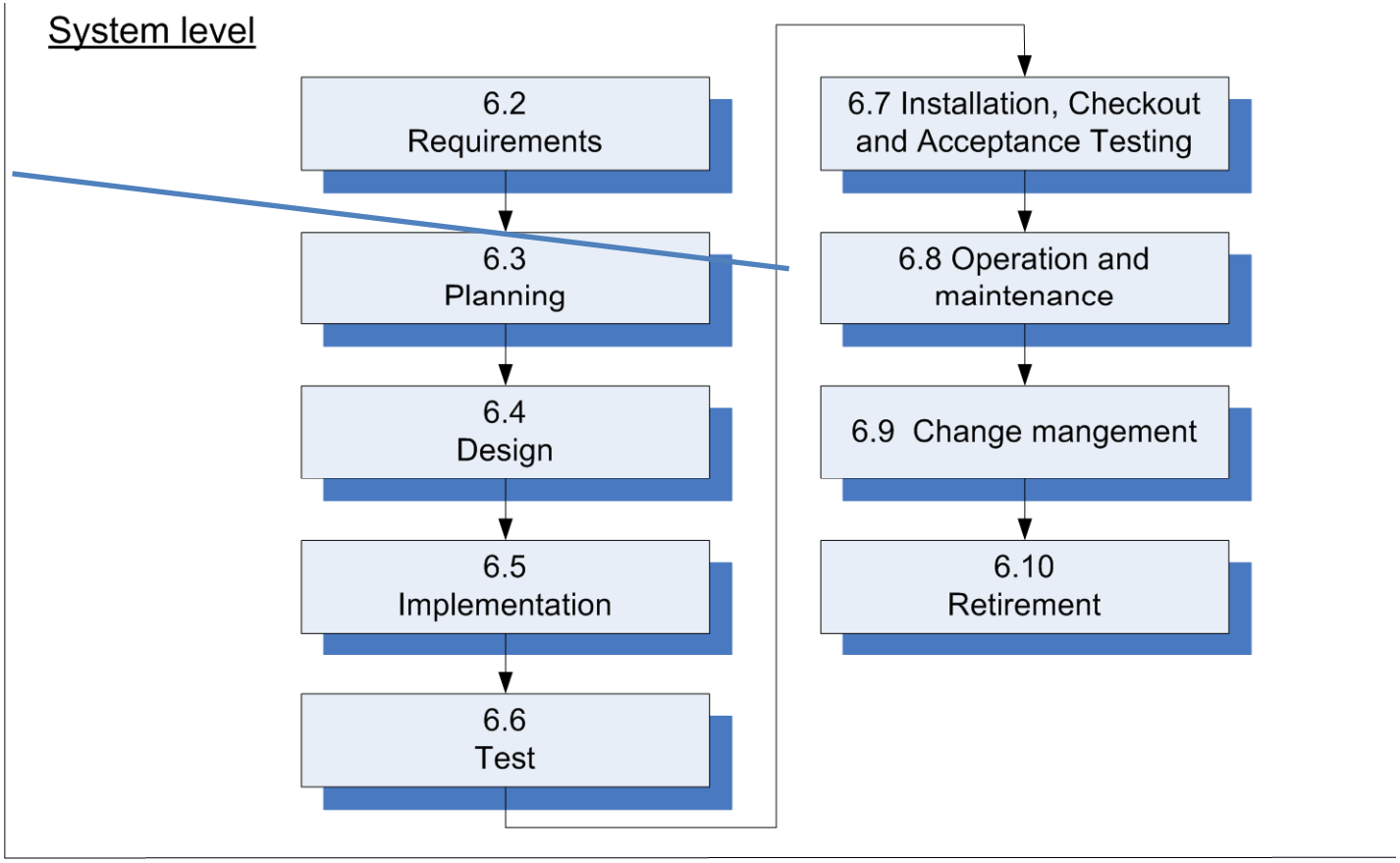
시스템이 **target environment** 에 설치 될 때, 해당 환경에 security feature의 correctness를 V&V 한다.



6. Life Cycle Implementation for I&C system security

주기적으로 security feature를 확인

변경이 생길 경우 해당 변경이 기존의 security feature를 위협하는지 확인

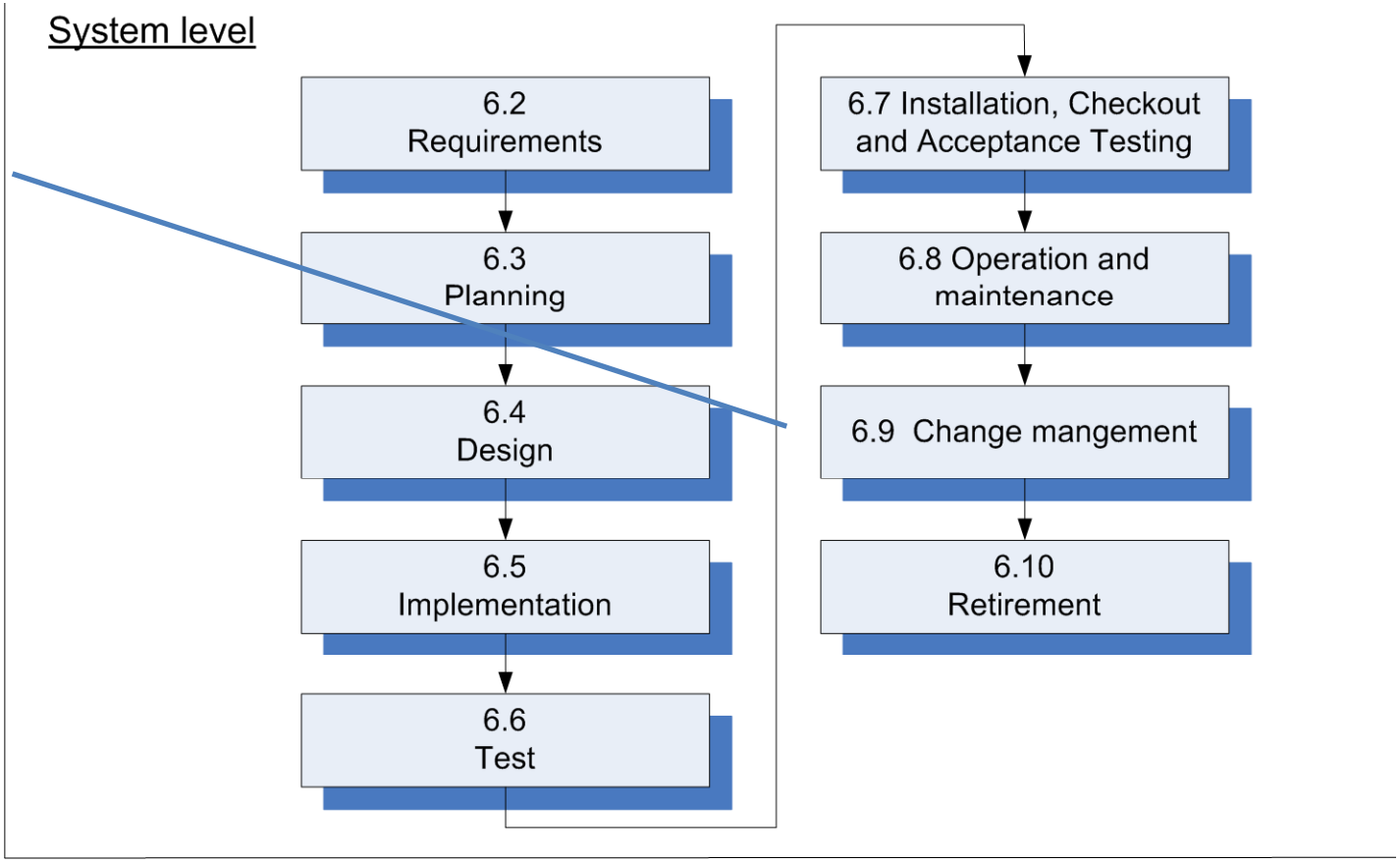


6. Life Cycle Implementation for I&C system security

변경을 할 경우 반드시 plant procedural, regulatory and/or licensing commitments 를 따라야 한다.

변경에 대한 review 와 testing을 해야 한다.

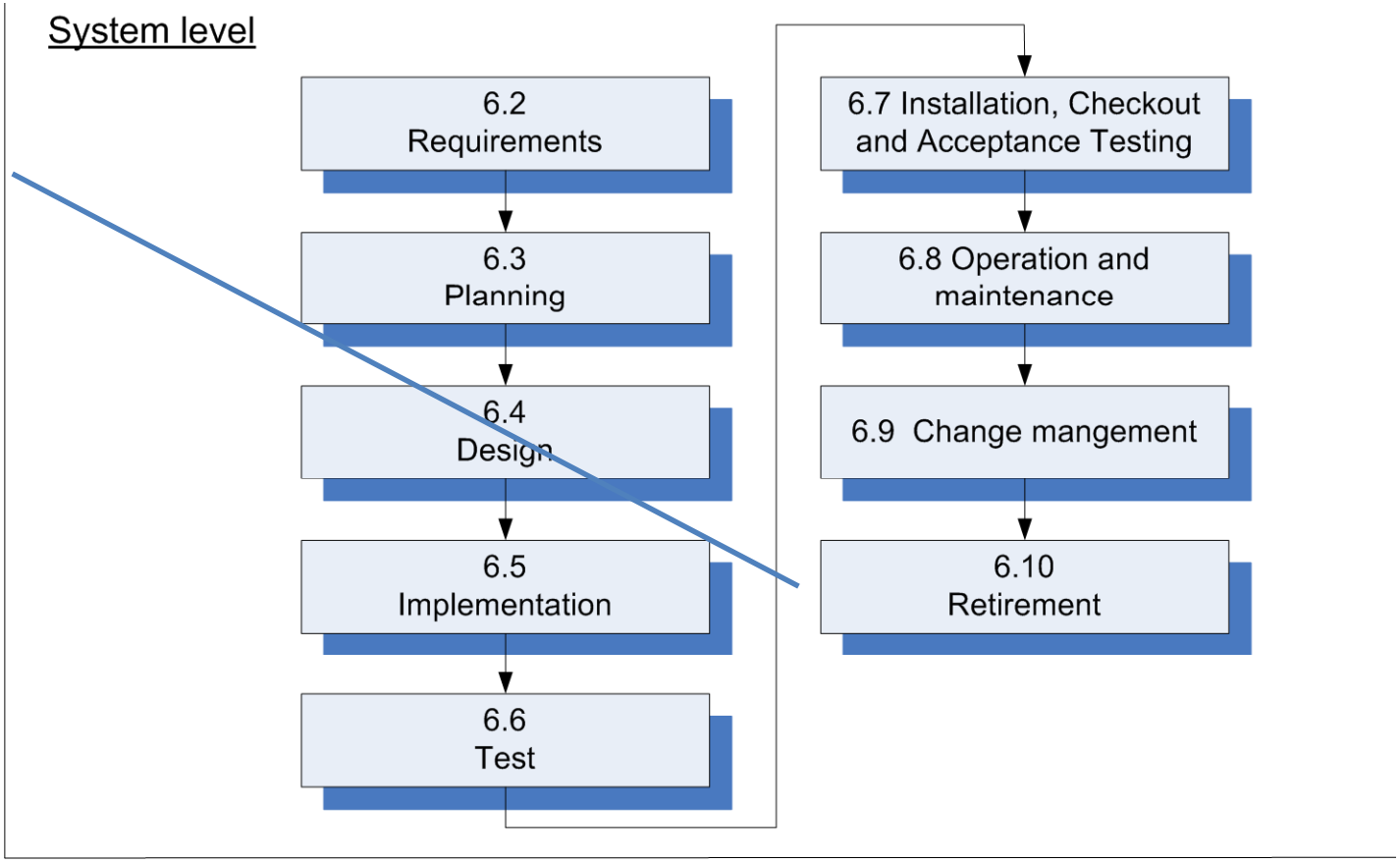
변경을 하기 전에 반드시 security feature에 대해서 risk assessment를 수행해야 한다.



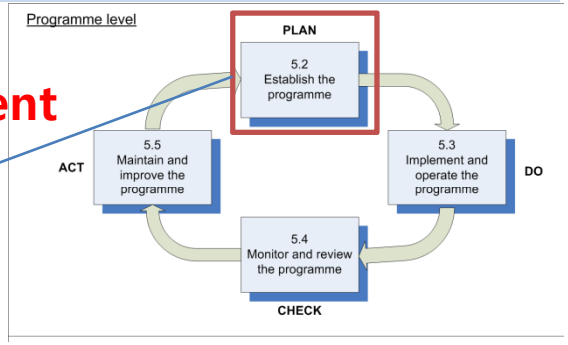
6. Life Cycle Implementation for I&C system security

민감한 정보의 노출을 방지하기 위해, 디지털 장치 및 미디어, 소프트웨어 등의 자료의 처분을 해야 한다.

적절한 방법...



그래서 6장은



Requirement

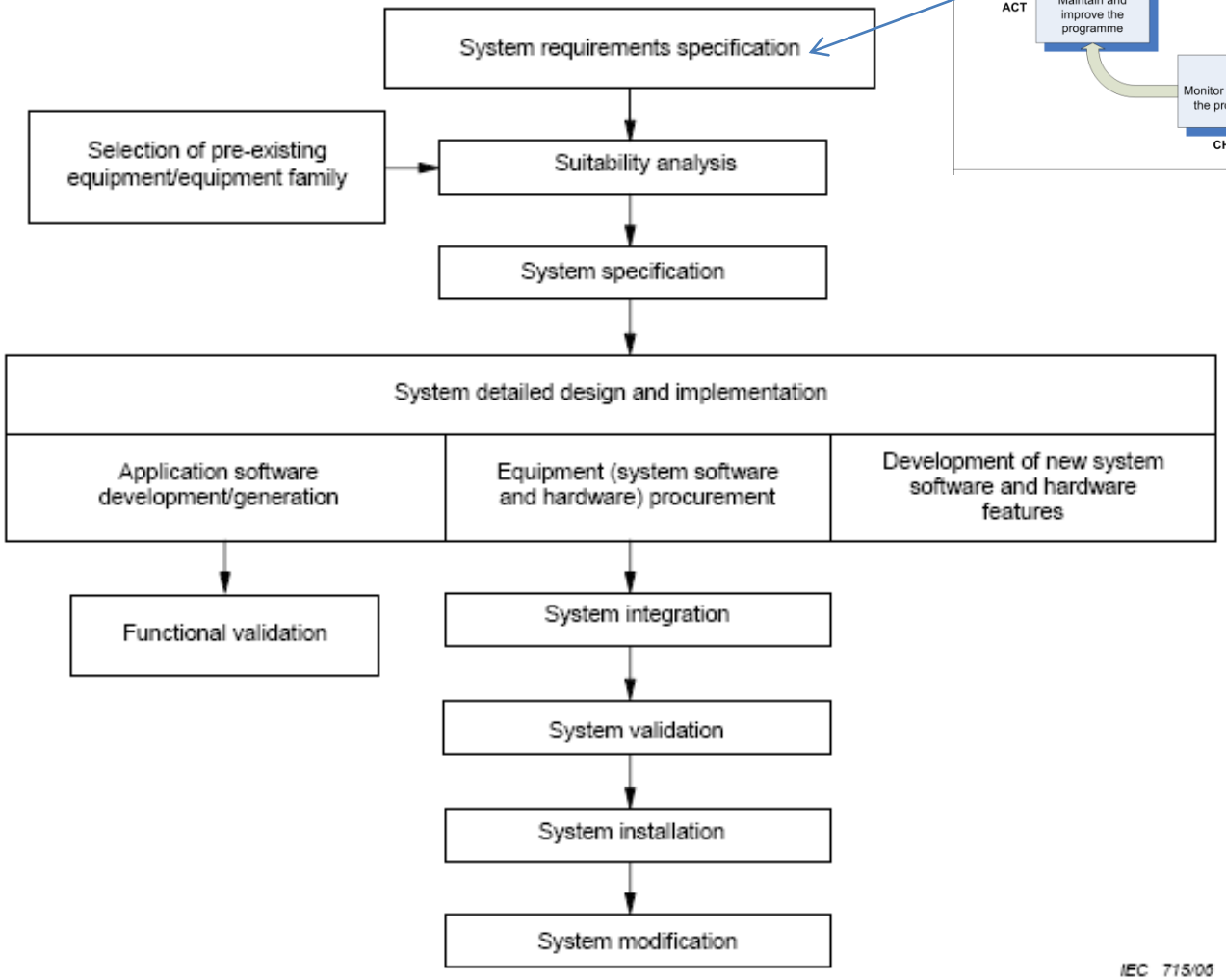
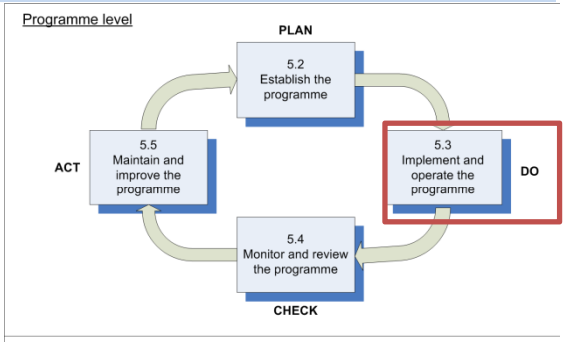


Figure 1 – Activities of the system safety lifecycle (as defined by IEC 61513)

- 각 개발 단계에 Security Requirement가 잘 반영이 되어 개발 되고 있는지.
- 할당된 security requirement가 system의 safety에 영향을 주고 있지 않은지
- Security requirement를 trace할 수 있는지

등을 고려하여
Safety Development를
진행 해야 한다.



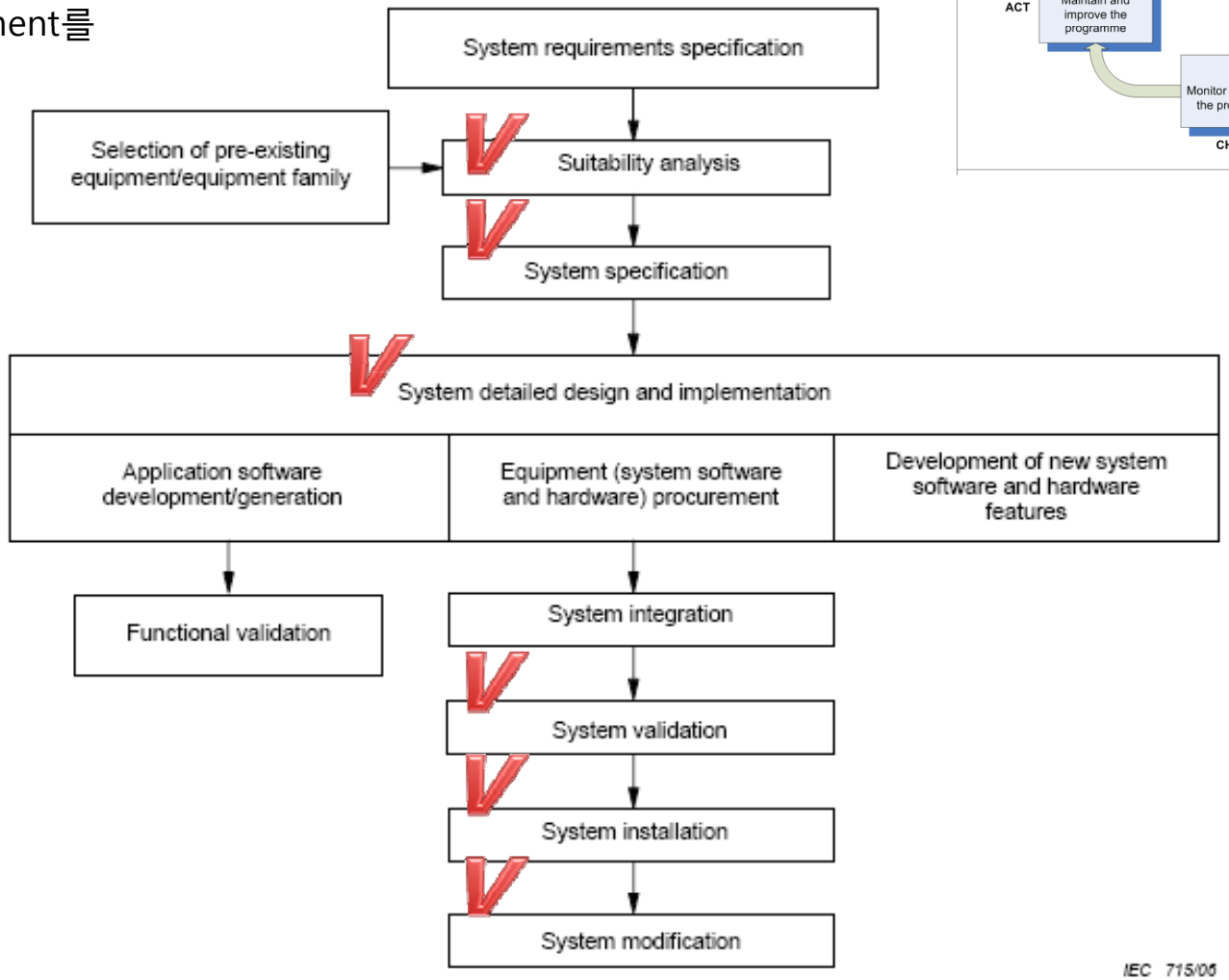


Figure 1 – Activities of the system safety lifecycle (as defined by IEC 61513)

Capability Maturity Model Integration

CMMI

CMMI

- 개념
- 목적
- 레벨 별 의미
- 실천 항목(PA)
- 실제 적용
- CMMI 심사

CMMI의 개념

- Capability Maturity Model Integration

- 조직의 개발 능력이 얼마나 성숙했는지를 보기 위한 것.

CMMI의 목적

- 프로세스 개선!

- 실천항목을 제시하고, 이의 준수를 요구함을써 개발 프로세스를 개선하려고 한다.
- 이를 통해 제품 품질을 높이고자 하는 것이다.

- 단순한 개선된 프로세스의 존재뿐이 아닌, 그 프로세스가 몸으로 익어진 상태(내재화; institutionalization)을 원한다.

- 이렇게 내재화가 되어 조직원 전부가 해야 할 것을 당연히 여기게 되었을 때 조직이 성숙했다고 한다.

CMMI의 레벨별 의미

- Level 1 : 관리되지 않는.
- Level 2 : 관리되는(Managed)
- Level 3 : 표준화된 프로세스에 의해(Defined)
- Level 4 : 정략적으로(Quantitively Managed)
- Level 5 : 지속적인 프로세스 개선(Optimized)

- 상위 레벨은 하위레벨을 만족한다.
  - 예 : Level3일 경우 Level2도 역시 만족한다.

CMMI 실천 항목(Process Area)

- PA(Process Area) : 실천 영역
  - 실제로 취하여야 하는 실천항목을 영역 별로 구분해 놓았다.

- Level 별로 요구하는 실천영역이 있다.
  - Level 1 : 0개
  - Level 2 : 7개
  - Level 3 : 11개
  - Level 4 : 2개
  - Level 5 : 2개

- 성숙도 Level 3일 경우 18개(Level2 7개+Level3 11개)의 실천영역에 대한 실천항목을 모두 만족시킨것을 의미한다.

- 어떤 분야에 대항하는 CMMI인지에 따라 PA의 내용이 약간씩 다름
  - CMMI for Development
  - CMMI for Services
  - CMMI for Acquisition

- 각 실천 항목들에 대해 Practice들이 있음.

- V 1.2와 1.3간에 차이가 조금 있음.

PA(Process Area) 리스트

Level	약어	Process Name	프로세스 명	목적 혹은 의미
Level 2	1. REQM	Requirements Management	요구사항 관리	요구사항을 관리하자
	2. PP	Project Planning	프로젝트 계획 수립	프로젝트 계획을 수립하자.
	3. PMC	Project Monitoring and Control	프로젝트 감시 및 통제	프로젝트가 잘되고 있는지 파악하고 조정하자.
	4. SAM	Supplier Agreement Management	공급업체 계약 관리	공급업체를 잘 관리하자.
	5. MA	Measurement and Analysis	측정 및 분석	모든 활동을 측정하고 분석하자.
	6. PPQA	Process and Product Quality Assurance	프로세스 및 제품 품질보증	모든 활동과 프로젝트 산출물을 점검하자.
	7. CM	Configuration Management	형상 관리	모든 결과물들을 형상관리하자.
Level 3	8. RD	Requirements Development	요구사항 개발	요구사항을 개발하자.
	9. TS	Technical Solution	기술 솔루션	적절한 기술 솔루션을 선택하자.
	10. PI	Product Integration	제품 통합	배포를 위해 제품을 제대로 통합하자.
	11. VEL	Verification	검증	원 목적대로 제대로 만들었는지 점검하자.
	12. VAL	Validation	확인	요구사항이 적절한지 점검하자.
	13. OPF	Organizational Process Focus	조직 프로세스 중점 관리	프로세스를 개선하자.
	14. OPD	Organizational Process Definition	조직 표준 프로세스 정의	프로세스를 정의하자.
	15. OT	Organizational Training	조직 교육 관리	교육시키자.
	16. IPM	Integrated Project Management	통합 프로젝트 관리	복수의 프로젝트들을 통합적으로 관리하자.
	17. RSKM	Risk Management	위험관리	위험을 관리하자.
	18. DAR	Decision Analysis and Resolution	의사결정분석 및 해결	제대로 의사결정을 하자.
Level 4	19. OPP	Organizational Process Performance	조직 프로세스 성과	프로세스 성능의 정량적 이해
	20. QPM	Quantitative Project Management	정량적 프로젝트 관리	프로젝트의 성과를 정량적으로 평가
Level 5	21. OPM	Organizational Performance Management	조직 성과 관리	조직 성과의 수준을 관리
	22. CAR	Causal Analysis and Resolution	원인분석 및 해결	결과에 대한 원인 분석 및 성능 향상

PA 영역의 분류

- 프로세스 관리(Process Management)
- 프로젝트 관리(Project Management)
- 공학(Engineering)
- 지원(Support)

PA 영역의 분류 – 프로세스 관리(Process Management)

- 프로세스 관리(Process Management)
  - 프로세스 관리 프로세스 영역은 프로세스를 정의하고 계획하고 전개하고,적용하고,감시하고,조정하고, 평가하고 측정하고 개선하기 위한 프로젝트 간의 활동을 포함한다.

PA 영역의 분류 – 프로세스 관리(Process Management)

Level	약어	Process Name	프로세스 명	목적 혹은 의미
Level 2	1. REQM			
	2. PP			
	3. PMC			
	4. SAM			
	5. MA			
	6. PPQA			
	7. CM			
Level 3	8. RD			
	9. TS			
	10. PI			
	11. VEL			
	12. VAL			
	13. OPF	Organizational Process Focus	조직 프로세스 중점 관리	프로세스를 개선하자.
	14. OPD	Organizational Process Definition	조직 표준 프로세스 정의	프로세스를 정의하자.
	15. OT	Organizational Training	조직 교육 관리	교육시키자.
	16. IPM			
	17. RSKM			
	18. DAR			
Level 4	19. OPP	Organizational Process Performance	조직 프로세스 성과	프로세스 성능의 정량적 이해
	20. QPM			
Level 5	21. OPM	Organizational Performance Management	조직 성과 관리	조직 성과의 수준을 관리
	22. CAR			

PA 영역의 분류 – 프로젝트 관리(Project Management)

- 프로젝트 관리(Project Management)
  - 프로젝트 관리 프로세스 영역은 프로젝트를 계획하고 감시하고 통제하는 것과 관련된 프로젝트 관리활동들을 다룬다.

PA 영역의 분류 – 프로젝트 관리(Project Management)

Level	약어	Process Name	프로세스 명	목적 혹은 의미
Level 2	1. REQM	Requirements Management	요구사항 관리	요구사항을 관리하자
	2. PP	Project Planning	프로젝트 계획 수립	프로젝트 계획을 수립하자.
	3. PMC	Project Monitoring and Control	프로젝트 감시 및 통제	프로젝트가 잘되고 있는지 파악하고 조정하자.
	4. SAM	Supplier Agreement Management	공급업체 계약 관리	공급업체를 잘 관리하자.
	5. MA			
	6. PPQA			
	7. CM			
Level 3	8. RD			
	9. TS			
	10. PI			
	11. VEL			
	12. VAL			
	13. OPF			
	14. OPD			
	15. OT			
	16. IPM	Integrated Project Management	통합 프로젝트 관리	복수의 프로젝트들을 통합적으로 관리하자.
	17. RSKM	Risk Management	위험관리	위험을 관리하자.
	18. DAR			
Level 4	19. OPP			
	20. QPM	Quantitative Project Management	정량적 프로젝트 관리	프로젝트의 성과를 정량적으로 평가
Level 5	21. OPM			
	22. CAR			

PA 영역의 분류 – 공학(Engineering)

- 공학(Engineering)
  - 엔지니어링 프로세스 영역은 개발과 엔지니어링 Disciplines 간의 공유되는 유지보수 활동을 다룬다. 엔지니어링 프로세스 영역은 또한 소프트웨어 공학과 시스템 공학을 하나 제품 개발 프로세스로 통합하고, 제품 기반 프로세스 개선 전략을 지원한다.

PA 영역의 분류 – 공학(Engineering)

Level	약어	Process Name	프로세스 명	목적 혹은 의미
Level 2	1. REQM			
	2. PP			
	3. PMC			
	4. SAM			
	5. MA			
	6. PPQA			
	7. CM			
Level 3	8. RD	Requirements Development	요구사항 개발	요구사항을 개발하자.
	9. TS	Technical Solution	기술 솔루션	적절한 기술 솔루션을 선택하자.
	10. PI	Product Integration	제품 통합	배포를 위해 제품을 제대로 통합하자.
	11. VEL	Verification	검증	원 목적대로 제대로 만들었는지 점검하자.
	12. VAL	Validation	확인	요구사항이 적절한지 점검하자.
	13. OPF			
	14. OPD			
	15. OT			
	16. IPM			
	17. RSKM			
	18. DAR			
Level 4	19. OPP			
	20. QPM			
Level 5	21. OPM			
	22. CAR			

PA 영역의 분류 – 지원(Support)

- 지원(Support)
  - 제품 개발 및 유지보수를 지원하는 활동을 다룬다. 다른 프로세스들이 제대로 수행될 수 있도록 하는 프로세스들이다. 일반적으로 지원 프로세스 영역은 프로젝트를 목표로 하며,조직에 대해 좀 더 일반적인 프로세스들이다. 예를 들어 PPQA는 프로세스의 객관적 평가와 모든 프로세스 영역에서 정의되는 작업 산출물을 제공하기 위한 모든 프로세스 영역에 사용될 수 있다. 모든 PA들에서 사용할 수 있는 기능들을 제공하며, 몇몇 일반 실행(generic practice) 들을 구현하는 것을 도와준다.

PA 영역의 분류 – 지원(Support)

Level	약어	Process Name	프로세스 명	목적 혹은 의미
Level 2	1. REQM			
	2. PP			
	3. PMC			
	4. SAM			
	5. MA	Measurement and Analysis	측정 및 분석	모든 활동을 측정하고 분석하자.
	6. PPQA	Process and Product Quality Assurance	프로세스 및 제품 품질보증	모든 활동과 프로젝트 산출물을 점검하자.
	7. CM	Configuration Management	형상 관리	모든 결과물들을 형상관리하자.
Level 3	8. RD			
	9. TS			
	10. PI			
	11. VEL			
	12. VAL			
	13. OPF			
	14. OPD			
	15. OT			
	16. IPM			
	17. RSKM			
	18. DAR	Decision Analysis and Resolution	의사결정분석 및 해결	제대로 의사결정을 하자.
Level 4	19. OPP			
	20. QPM			
Level 5	21. OPM			
	22. CAR	Causal Analysis and Resolution	원인분석 및 해결	결과에 대한 원인 분석 및 성능 향상

실제 적용

- 실제로 프로젝트를 진행할 땐 전사표준 프로세스(OSSP)를 가지고 각 프로젝트에 맞게끔 다듬는다.

- OSSP : Organizational Software Standard Process

- OSSP에는 표준적인 프로세스와 산출물 예제가 있다.
- 이러한 프로세스를 프로젝트에 맞도록 수정하고,
- 산출물을 프로젝트에 맞도록 수정한다.

- 그리고 프로젝트가 종료된 후에 프로젝트 결과물을 가지고 각 조직에 맞도록 다시 OSSP를 개선해 나간다.

CMMI 심사

- gap 분석 : 현재의 상태와 goal과의 차이를 파악한다.
- Readiness Review : 심사준비가 되었는지 파악하고.
- Appraisal : 실제 심사
  - 모든 실천영역에 대한 실천항목에 대하여 증거의 여부를 파악한다.
  - 증거와 더불어 간접증거를 파악하고 인터뷰를 통해 이를 검증한다.
  - 증거의 목록을 PIID라 한다.

- 모든 영역의 모든 실천항목에 대하여 충분한 실천에 대한 직접증거와 간접증거로 인정되어야만 그 성숙도가 인정된다.
- Carnegie Melon의 SEI(Software Engineering Institute)에서 주관

62645 - CMMI

- 정부기관 및 기업들은 프로젝트 참여나 제품공급에 대한 전제조건으로 지원업체의 CMMI 레벨3 기준을 기본으로 요구한다.
- 한국 원자력 연구원에서 CMMI 인증을 받았다는 내용은 찾아보지 못했음.
- 레벨 4, 5에 해당하는
  - **Organizational Process Performance**
  - **조직 프로세스 성과**
  - **Quantitative Project Management**
  - **정량적 프로젝트 관리**
  - **Organizational Performance Management**
  - **조직 성과 관리**
  - **Causal Analysis and Resolution**
  - **원인분석 및 해결**
- 의 내용은 표준에서 요구하는 사항과 직접적인 연관이 있다고는 생각되지 않음.
- Safety의 요구사항들을 만족시키기 위한 V&V 및 risk management등은 level 3에 대부분 포함 됨.
- IEC 62645에 대해 직접적인 CMMI 레벨을 명시해놓은 문서는 없음.

CONCLUSION

Conclusion

- IEC 61513, 60880의 safety development life cycle이 바탕
- IEC 62645는 위 표준의 development life cycle에 Security적인 부분을 추가하고 있다.
- **Safety > Security**
  - Security 의 degree도 safety 결과(영향도)로 결정되는 부분이 있다.