

Cyber Security at NPP

김의섭

IEC 62645

- **Main Focus**

- 이 IEC 표준은 특히 컴퓨터 보안 프로그램과 컴퓨터 기반 시스템에 대한 공격 방지 및 영향을 최소화하기 위한 시스템 개발 프로세스에 대한 요구 사항의 문제에 초점을 맞춤.

- **Main Goal**

- 목표는 국가 별 요구 사항을 개발하고 적용 할 수 있는 내 프레임 워크를 정의하는 표준을 제공하는 것입니다.

- **Primary Objective**

- The primary objective of this standard is **to define adequate programmatic measure for the prevention of malicious or misguided acts** which could lead to an accident.

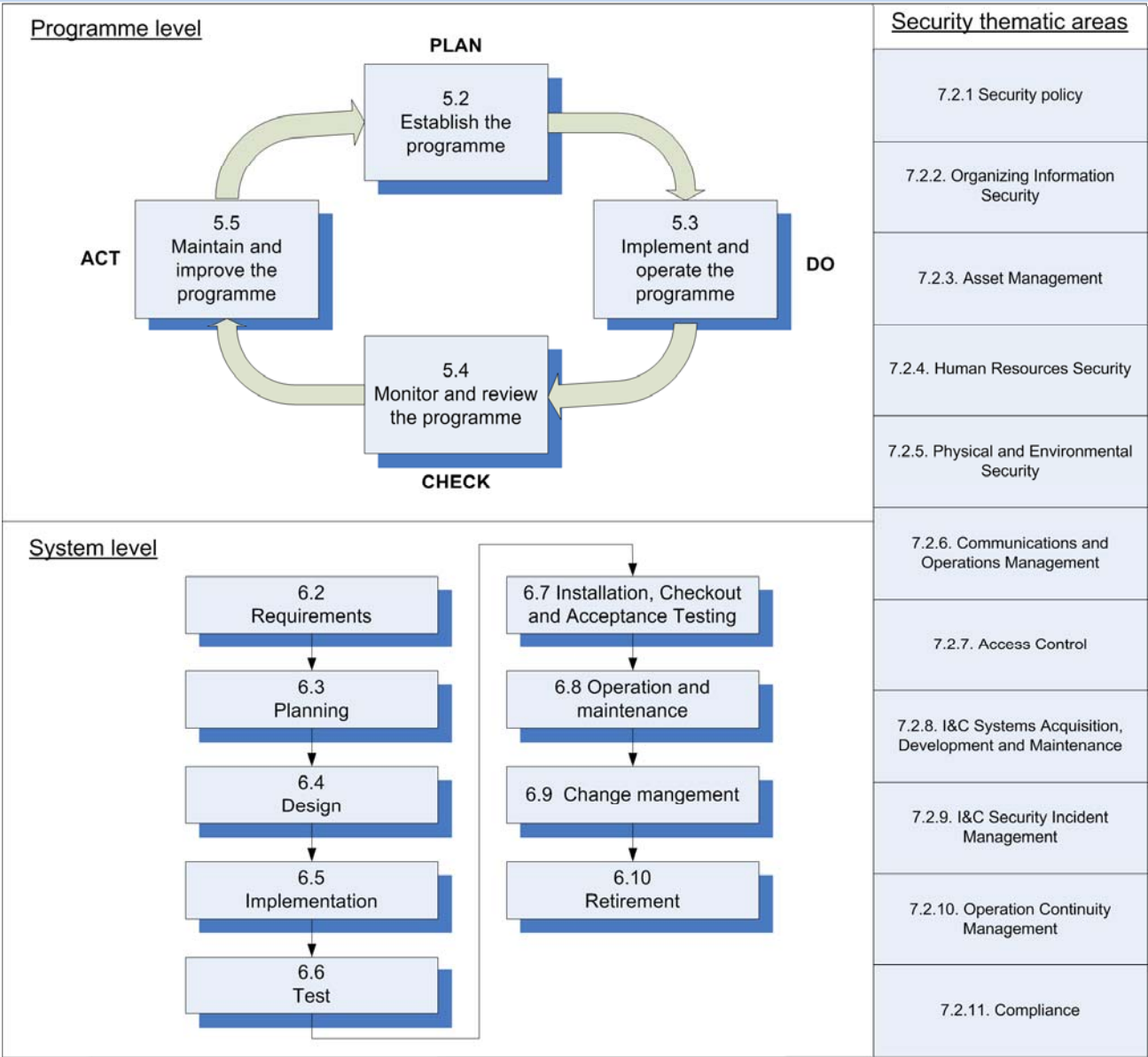
- **Excluded**
 - **non-malevolent** actions and events such as accidental failures, human errors and natural events.
 - site **physical** security and room access control and site security surveillance systems
- **Application**
 - This standard is limited to security of **I&C systems used in a an NPP.**
 - This standard is intended to be used
 - for modernizing existing NPP,
 - for designing new nuclear power plants (NPP),
 - for initial system design and
 - for modifying existing systems throughout the digital system life cycle.

- Cyber attack Story
 - NPP에서 점점 **digital technology** 사용이 늘어나면서 **new vulnerabilities** 가 생겨나고 있다.
 - Not important to safe 한 곳 뿐만 아니라 important to safe 한 곳 까지 다양하게 사용되고 있다.
 - 따라서 **plant safety, equipment or performance** 에 영향을 주게 된다.
 - 본 Standard 는 **establishes requirements and provides guidance**
 - For the **development and management** of computer **security programmes** at NPPs

- Cyber attack Story
 - Computers are also used **to store important and sensitive data**, where any malfunctions could lead to the loss of important data or the unauthorized release of sensitive information.
 - Ex (아주 아주 중요한 정보)
 - 손으로 쓴 장부 -> Physical Security
 - Computer에 저장 정보 -> **Cyber Security**
 - The **complexity of these computer systems** makes it difficult to identify comprehensively the potential threats to the nuclear power plants.

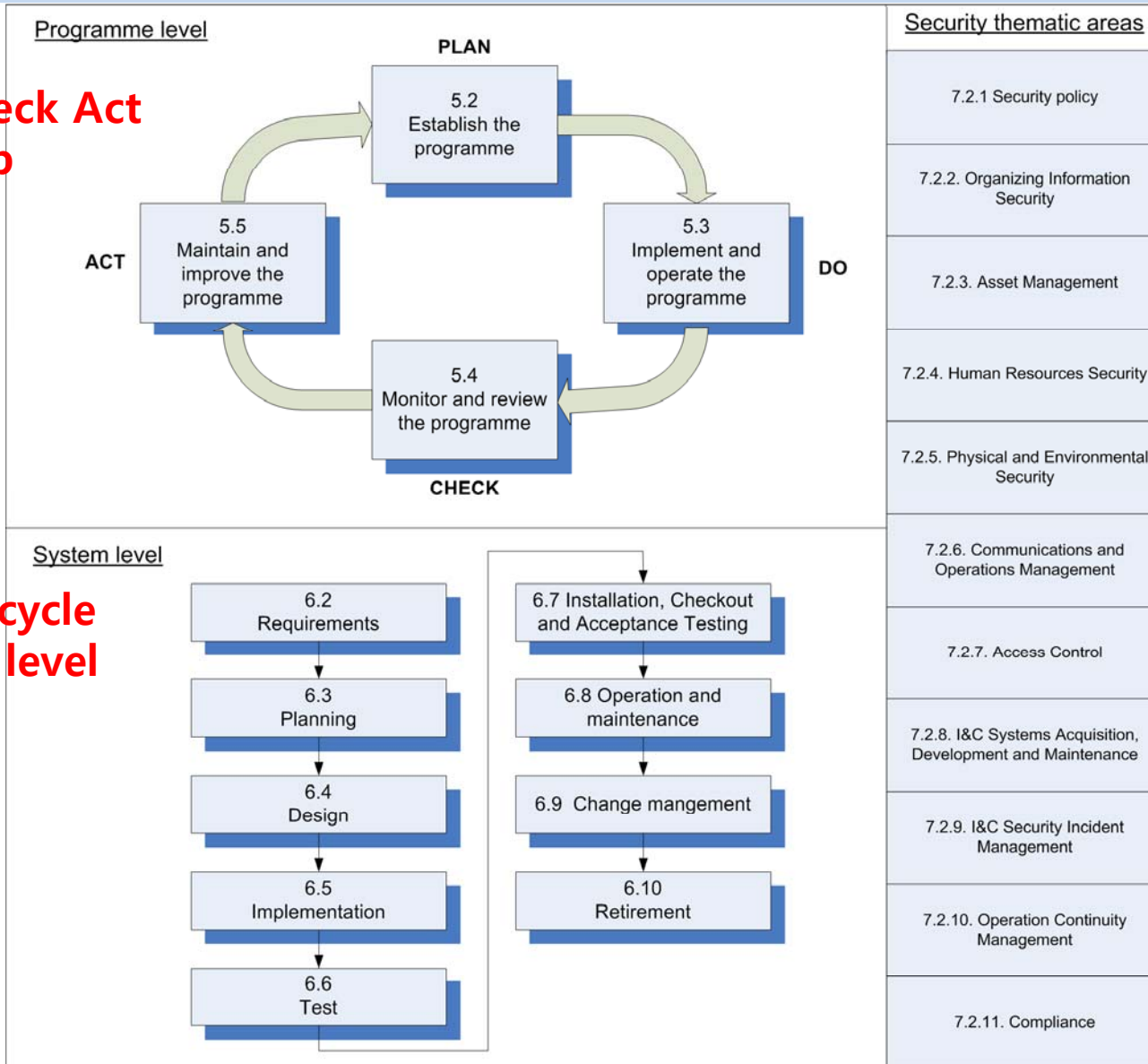
- Cyber attack Story
 - **Experience shows** that computer systems without proper protection from cyber attack can become unavailable or unable to fulfil their intended function or manipulated to fulfil functions other than the ones they are required to fulfil, and must be protected throughout the **whole life cycle**.
 - **Computer-based systems (hardware and software)** must be secure as reasonably possible from digital risks.
 - The consideration of **hardware** shall include **physical access** control and access control of data communication paths (**Example: modems, connectivity to external networks, data links**).
 - Security of computer-based **software** relates to the **ability to prevent unauthorized, undesirable, and unsafe intrusions** throughout the life cycle of the computer-based system.

Framework



Framework

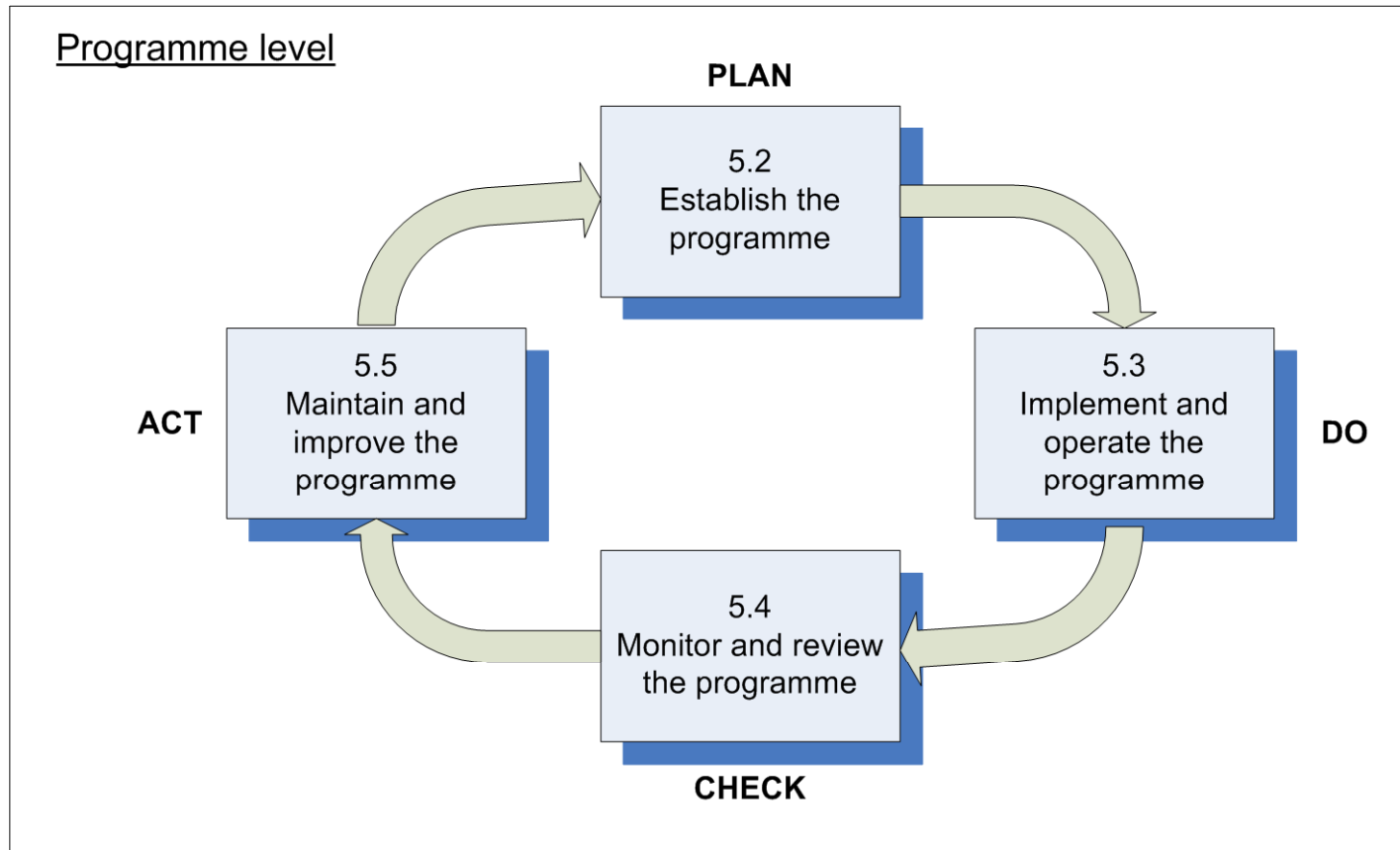
Plan Do Check Act (PDCA) loop



특정 부분에 대한 control

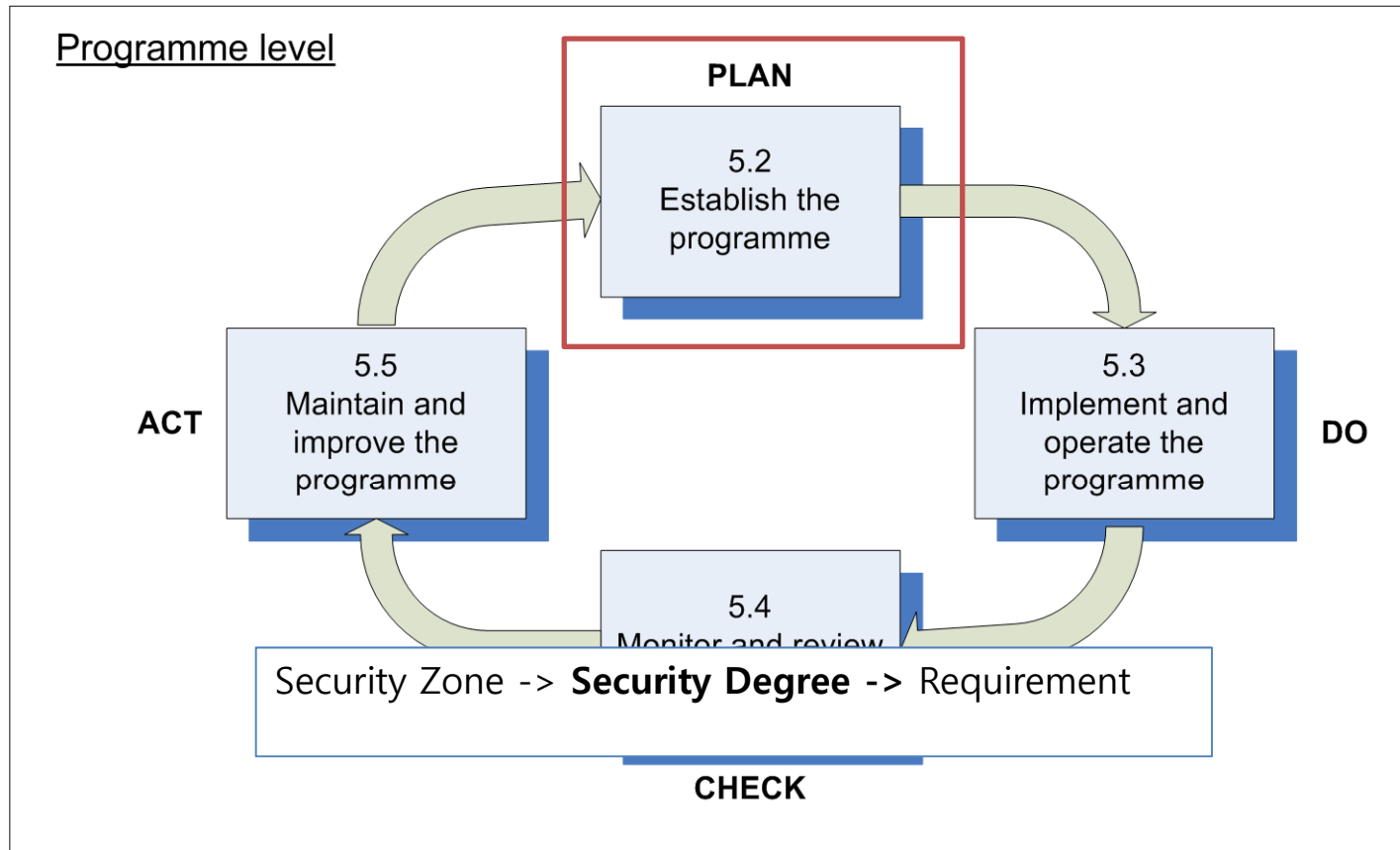
security life-cycle on a system level

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



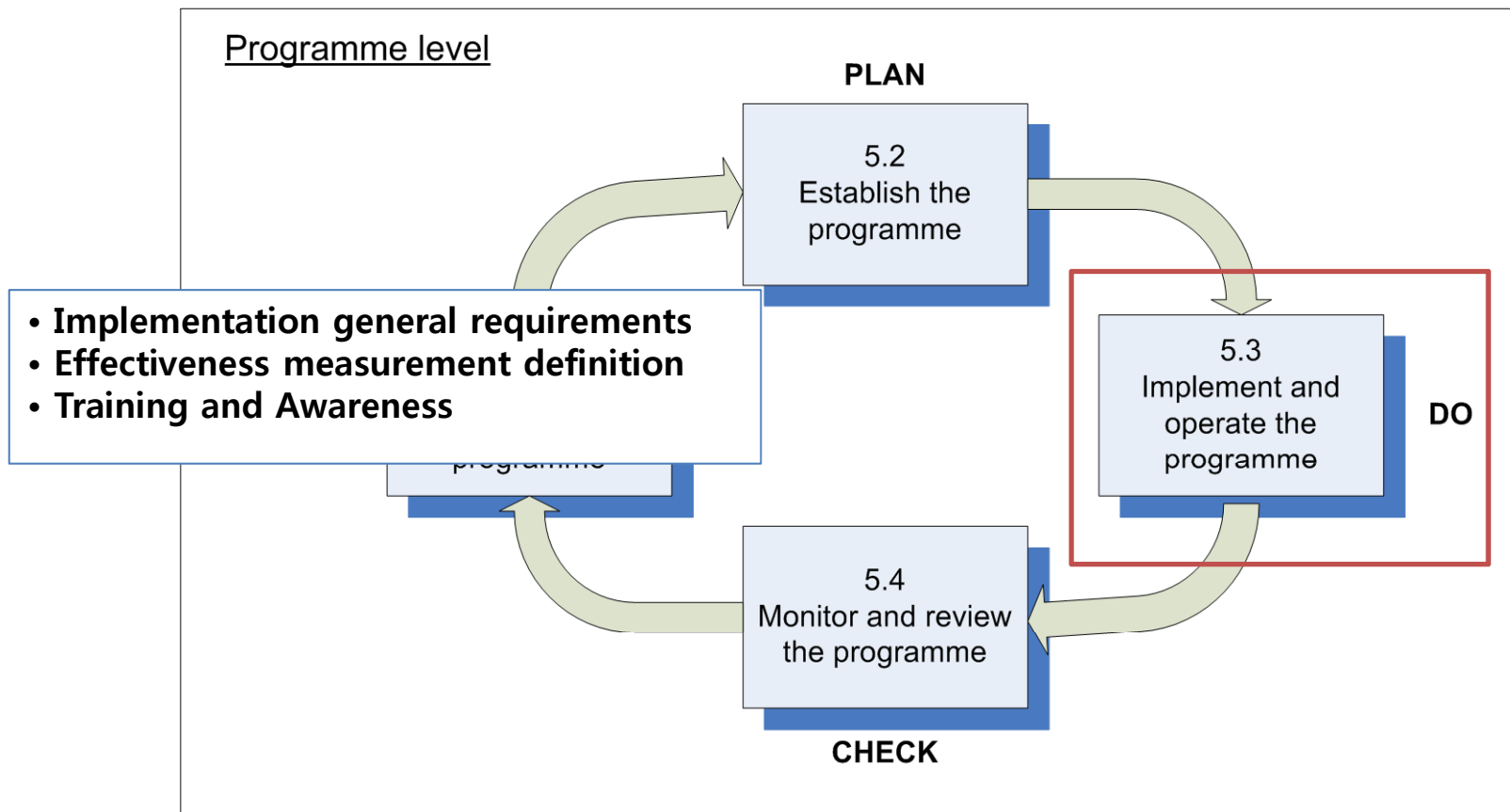
1. Plan(계획): 과거의 실적과 미래의 예측을 통해 계획을 책정한다.
2. Do(실시, 실행): 실제 계획에 따라 실행한다.
3. Check(점검, 평가): 계획대로 실행되고 있는지 확인한다.
4. Act(처리, 개선): 실행이 계획대로 되지 않은 부분을 조사해 개선한다.

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



1. Plan(계획): 과거의 실적과 미래의 예측을 통해 계획을 책정한다.
2. Do(실시, 실행): 실제 계획에 따라 실행한다.
3. Check(점검, 평가): 계획대로 실행되고 있는지 확인한다.
4. Act(처리, 개선): 실행이 계획대로 되지 않은 부분을 조사해 개선한다.

5.3 Implement and operate the programme

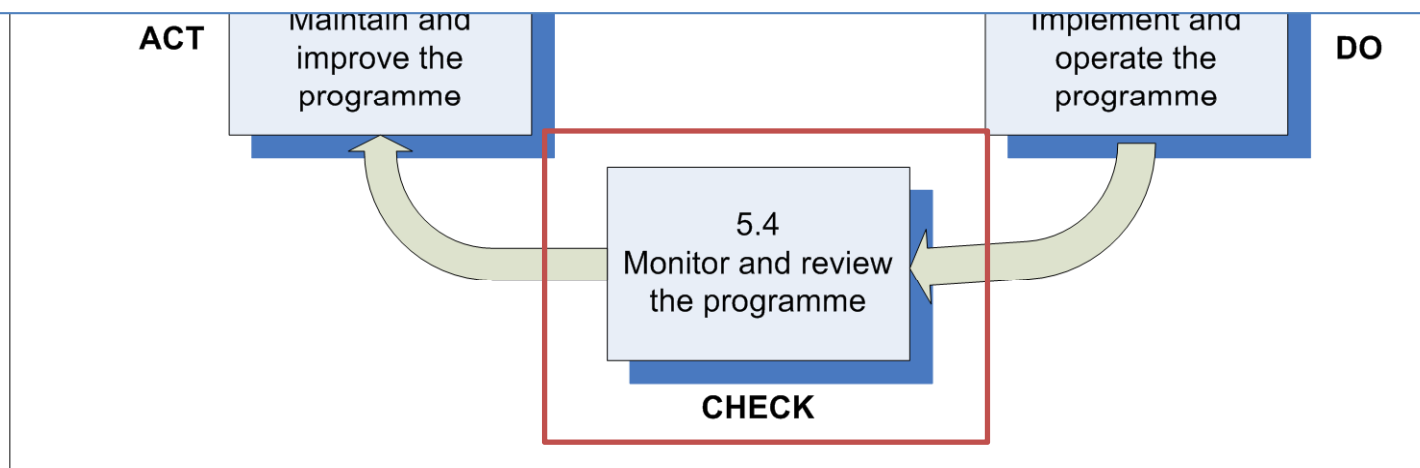


1. Plan(계획): 과거의 실적과 미래의 예측을 통해 계획을 책정한다.
2. Do(실시, 실행): 실제 계획에 따라 실행한다.
3. Check(점검, 평가): 계획대로 실행되고 있는지 확인한다.
4. Act(처리, 개선): 실행이 계획대로 되지 않은 부분을 조사해 개선한다.

5.4 Monitor and review the programme

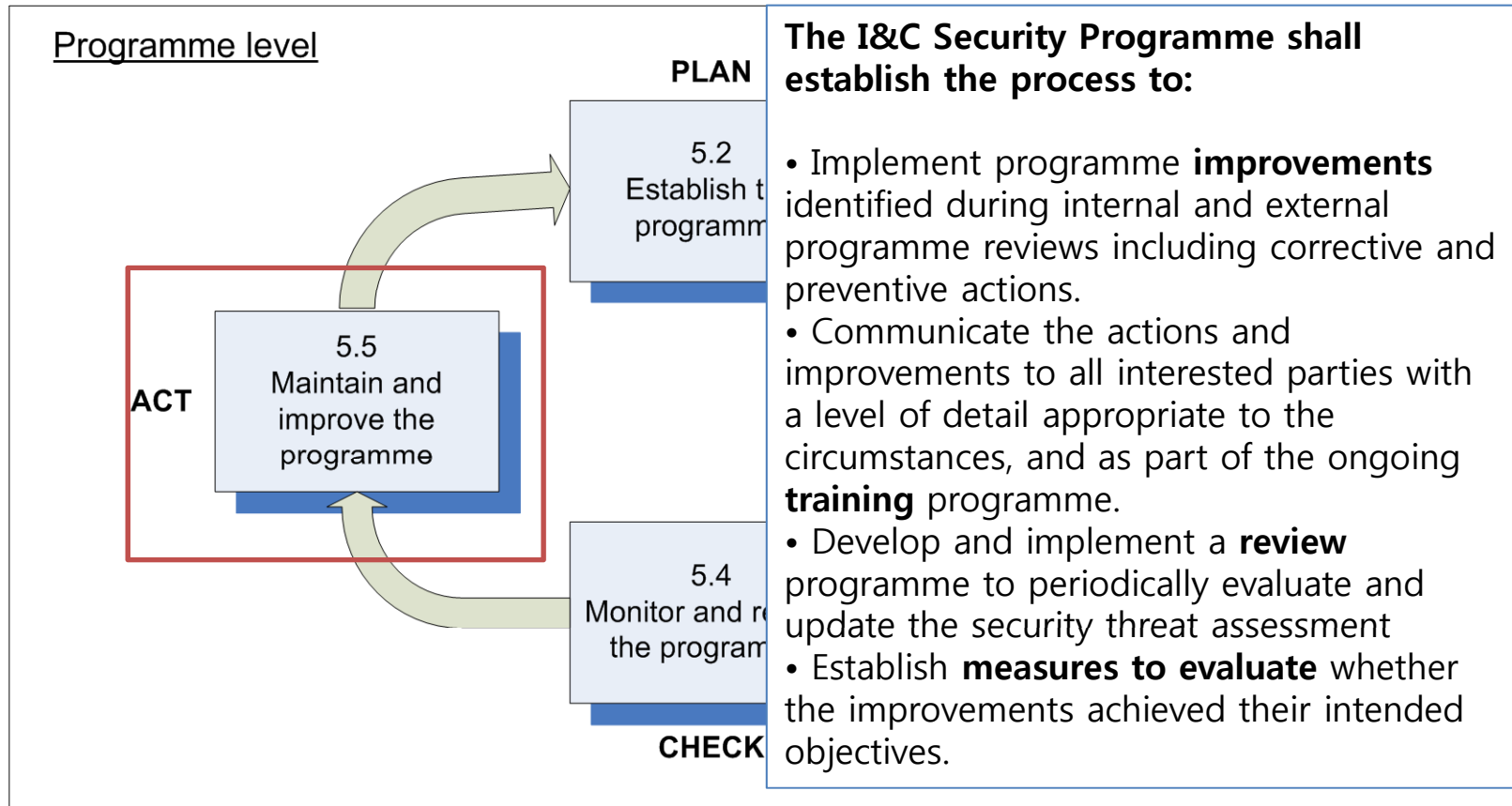
To conduct period security program reviews.

- **Develop and implement a review programme** that addresses the purpose, scope, roles, responsibilities, requirements and management commitment associated with reviewing elements of the I&C Security Programme for effectiveness.
- **Develop and implement procedures** to facilitate and maintain the review programme including required frequency of the reviews, and qualifications of individuals performing the reviews.



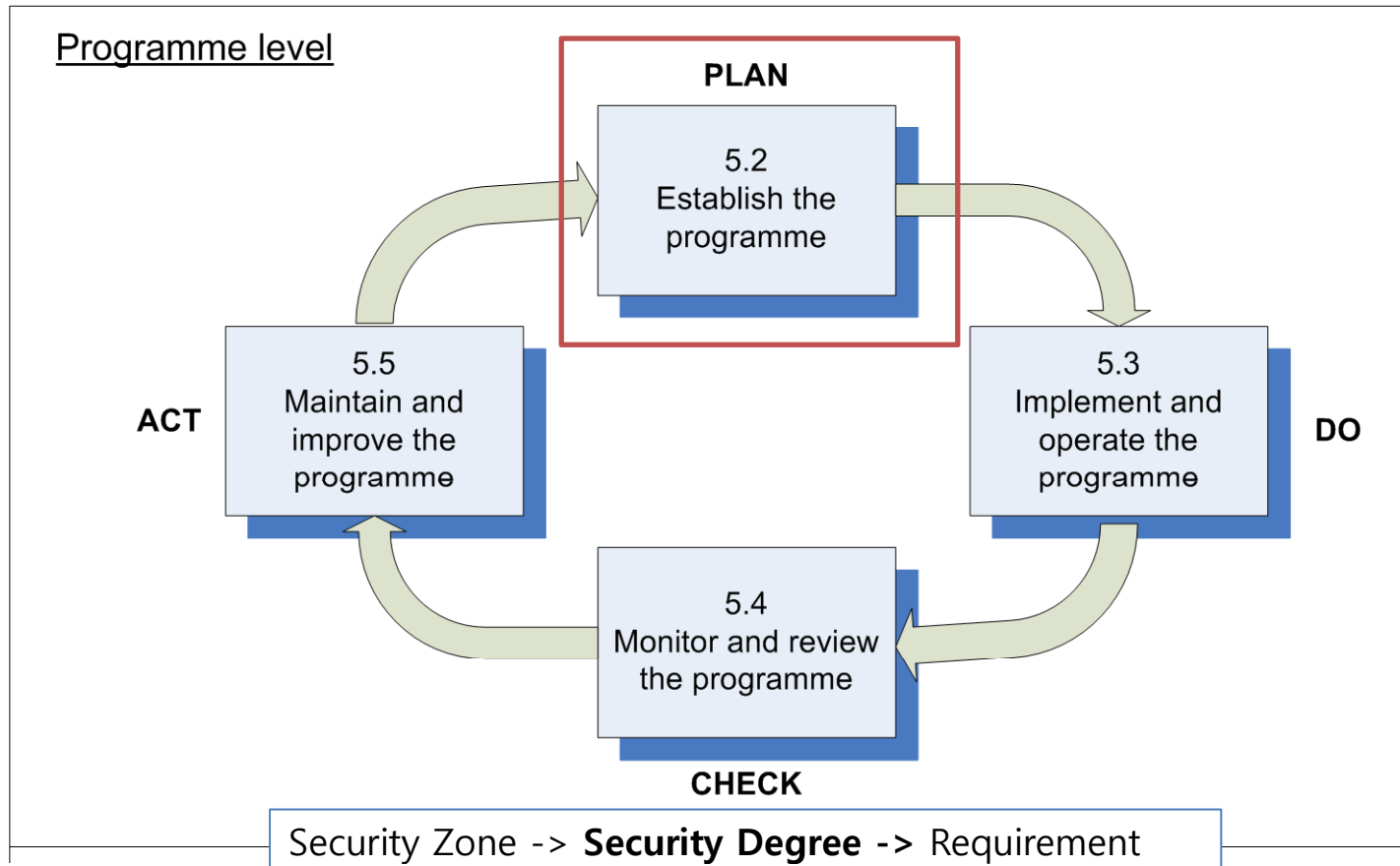
1. Plan(계획): 과거의 실적과 미래의 예측을 통해 계획을 책정한다.
2. Do(실시, 실행): 실제 계획에 따라 실행한다.
3. Check(점검, 평가): 계획대로 실행되고 있는지 확인한다.
4. Act(처리, 개선): 실행이 계획대로 되지 않은 부분을 조사해 개선한다.

5.5 Maintain and improve the programme



1. Plan(계획): 과거의 실적과 미래의 예측을 통해 계획을 책정한다.
2. Do(실시, 실행): 실제 계획에 따라 실행한다.
3. Check(점검, 평가): 계획대로 실행되고 있는지 확인한다.
4. Act(처리, 개선): 실행이 계획대로 되지 않은 부분을 조사해 개선한다.

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



1. Plan(계획): 계획 수립한다.
2. Do(실시, 실행): 실제 계획에 따라 실행한다.
3. Check(점검, 평가): 계획대로 실행되고 있는지 확인한다.
4. Act(처리, 개선): 실행이 계획대로 되지 않은 부분을 조사해 개선한다.

5.2 Establish the programme



- 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**
- 5.2.4 Management approval

5.2.3 Graded approach to I&C security and risk assessment



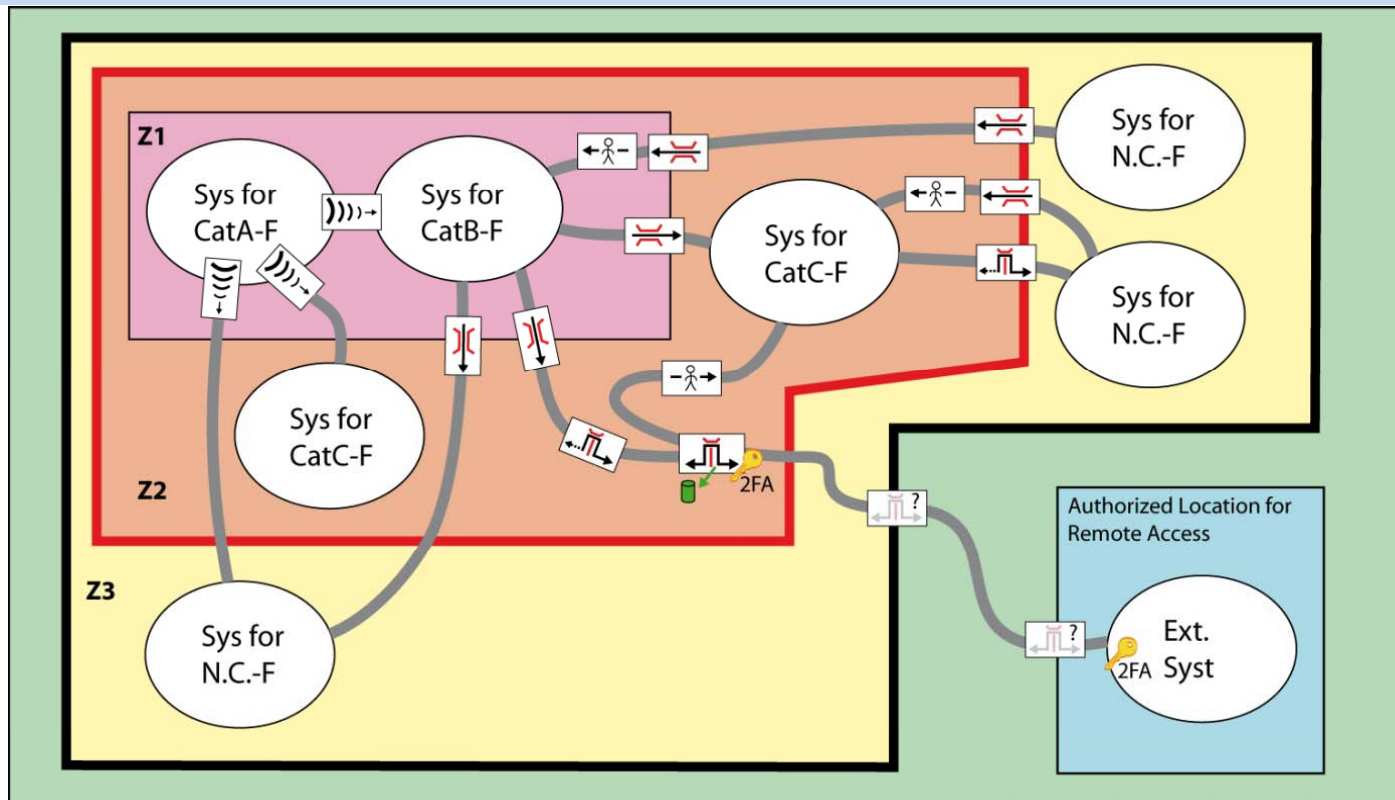
- I&C security shall be based on a graded approach.
 - Security degree , Security level
 - S1, S2 .. S5







- Security Zones -> Degree -> Requirement

5.2.3 Graded approach to I&C security and risk assessment

- **Security Zones** -> Degree -> Requirement
- Security Zones
 - A possible practical implementation of the graded approach is to categorize computer systems into **logical zones**, where graded protective principles are applied for each security zone.
 - security zones are practical implementations of security degrees. They are not limited in number.
 - **different I&C systems** may have **similar impacts on plant** safety or performance, so that they are attributed the **same security degree**. Nevertheless, they may be implemented in **different security zones so that a cyber-attack does not jeopardize** them at the same time, or for administrative or other sorts of constraints.
 - I&C systems grouped in a given security zone have the same security degree.
 - every I&C system is useful to the plant, even if it only processes functions with potential delayed impact on performance. Hence it is secured in an adapted way and, if isolated, may be the single device of a specific security zone

Appendix A

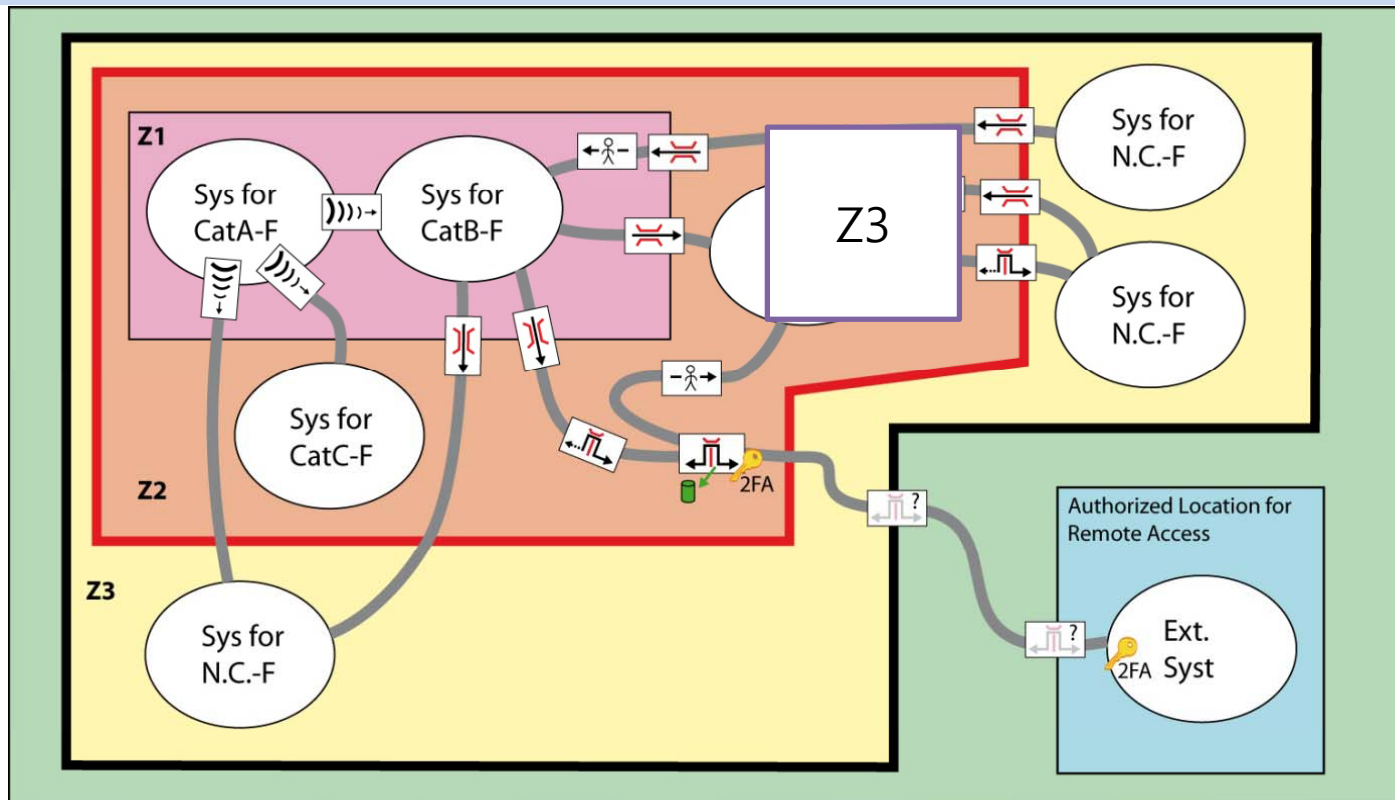


-  Stateless unidirectional data transfer (Broadcasting)
-  Data transfer with manual authorization, verification and approval.
-  Remote Access Application Level Gateway for arbitrary data transfer with strong 2-factor user authentication and session content logging.
-  Sender initiated unidirectional data transfer with protection filter
-  Unidirectional data transfer upon request with protection filter (Application Level Gateway)
-  Data Communication Gateway with unknown protection level

© F.Dafelmair 2011, TÜV SÜD Industrie Service GmbH

Example Graded Approach with Zone Applications

Appendix A



-)))> Stateless unidirectional data transfer (Broadcasting)
- |> Sender initiated unidirectional data transfer with protection filter
- |> Data transfer with manual authorization, verification and approval.
- |> Unidirectional data transfer upon request with protection filter (Application Level Gateway)
- |> 2FA Remote Access Application Level Gateway for arbitrary data transfer with strong 2-factor user authentication and session content logging.
- |> ? Data Communication Gateway with unknown protection level

© F.Dafelmair 2011, TÜV SÜD Industrie Service GmbH

Example Graded Approach with Zone Applications

5.2.3 Graded approach to I&C security and risk assessment

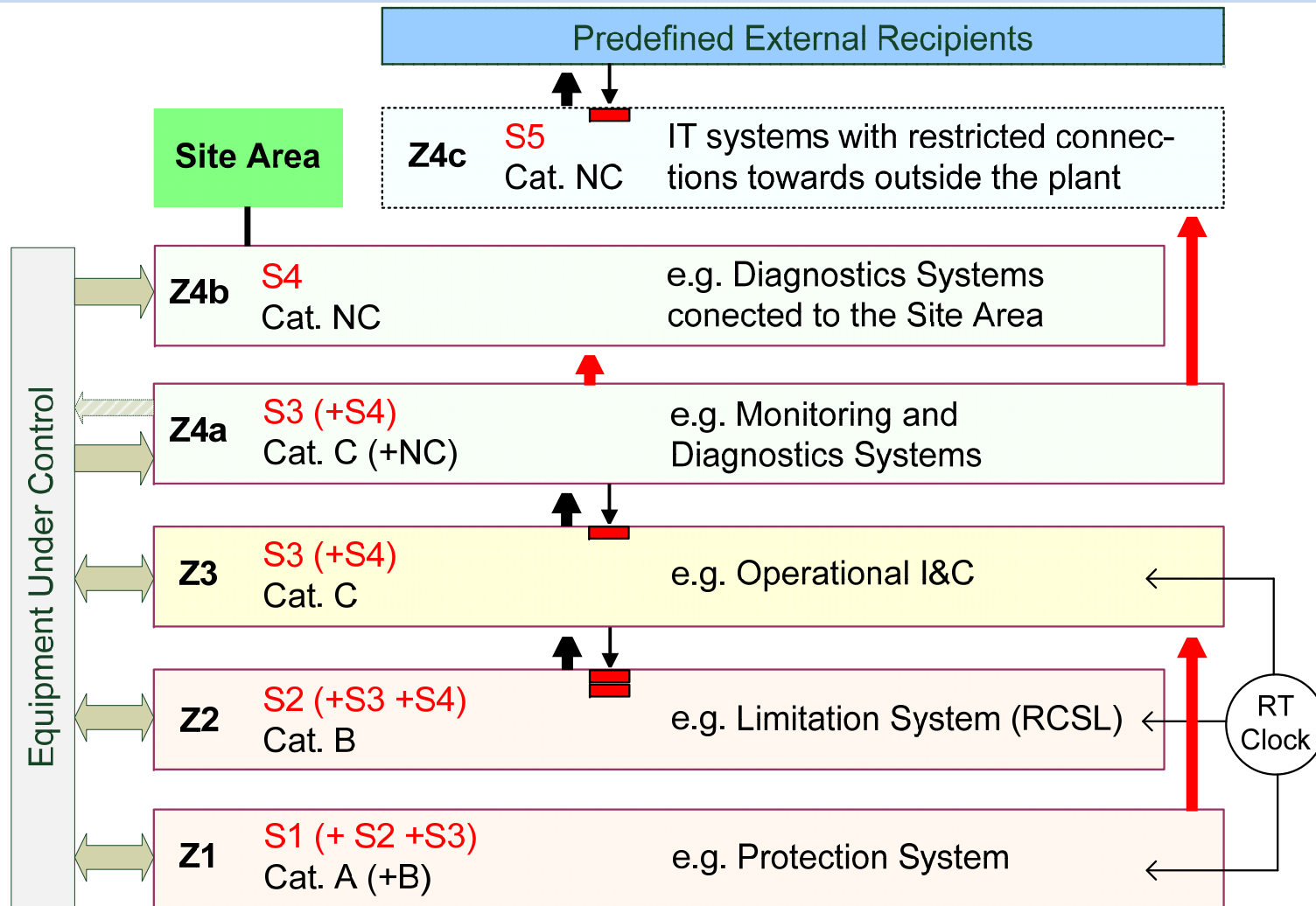


- Security Zones -> **Degree** -> Requirement
- Link between safety categories, safety classes and security degrees
 - The security graded approach described in this standard aims at defending the **plant safety and performance** against cyber threats, built on a consequence-based analysis
- Description of the security degrees and associated assignment criteria
 - S1, S2 and S3
 - **I&C systems are not the final target** of a cyber-attack, they are only vectors which, if not correctly secured, allow plant equipment to be targeted. Hence, successful cyber-attacks regarding I&C systems may have consequences on **population, plant personnel, environment and equipment**. Only three degrees are necessary to feature such conceptual consequences.

5.2.3 Graded approach to I&C security and risk assessment

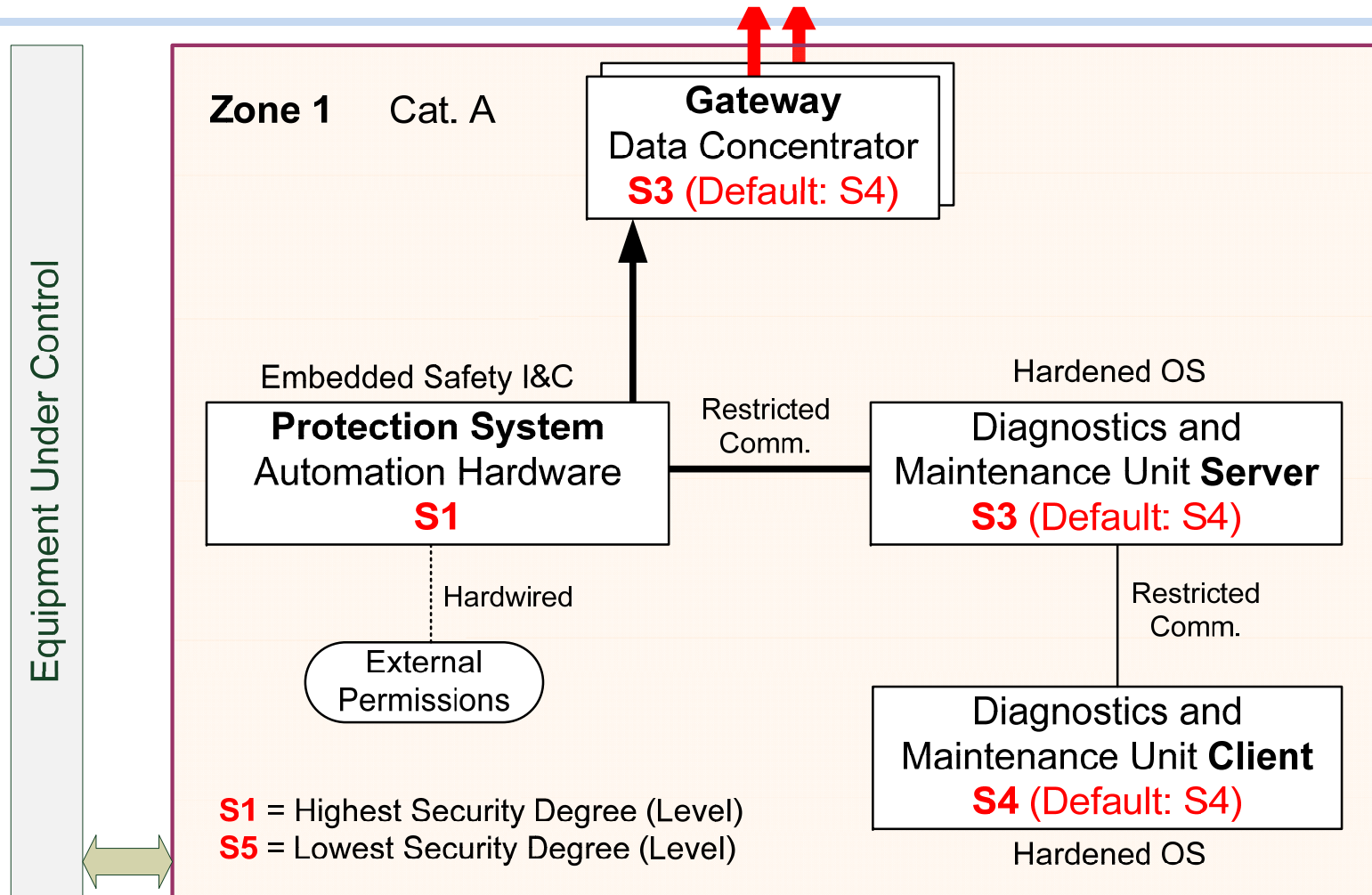
- category A functions -> Security degree S1
- category B functions -> Security degree S2
- Real-time operation -> security degree S2
- operation and maintenance -> security degree S3.

Appendix A



Example Security Zone Model and Security Degrees

Appendix A



Example Security Zone Model and Security Degrees - Assignment of Increased Security Degrees

5.2.3.3 Assignment of technical requirements



- Security Zones -> Degree -> **Requirement**
- 5.2.3.3.4 Degree S1 additional requirements
- 5.2.3.3.5 Degree S2 additional requirements
- 5.2.3.3.6 Degree S3 additional requirements

5.2.3.3 Assignment of technical requirements

- **Degree S1 additional requirements**
 - a. For S1 systems, networked links shall be authorized only with other S1-graded systems or with S2-graded systems.
 - b. Communications should be oriented from S1-graded systems towards S2-graded systems
 - c. Data transmission from a S2-graded system to a S1-graded system shall be restricted to the maximum extent. Only unavoidable transmissions (e.g., permissives) shall be authorized on a case-by-case basis and supported by a complete justification and security risk-analysis.
 - d. Any data transmitted from a S2-graded system to a S1-graded system shall be secured by adapted static provisions (e.g., format and time-window controls).
 - e. Software upgrade and configuration change of S1-graded systems shall be possible only locally (by means of local interlock, e.g. keys) and only for one channel at time. Bidirectional data transfer between I&C equipment of highest security degree and a dedicated service station shall be performed using as dedicated data connection which is decoupled from the I&C data transfer network used for online plant safety functions. This dedicated data connection shall be secured by technical, organizational and administrative means.
 - f. Entering communication into I&C systems, either from outside the plant or from IT systems, shall be prevented. Exception may be implemented only for managing security equipment in case there is no qualified personnel on site to manage them.
 - g. There shall be provisions against hidden functions in the system software (e.g., software code verification).
 - h. Compliance with clauses 5.7 and 12.2 of IEC 60880 shall be required for S1-graded systems.
 - i. Alarms of the anomaly detection system should be analyzed promptly and carefully and appropriate measures should be taken.

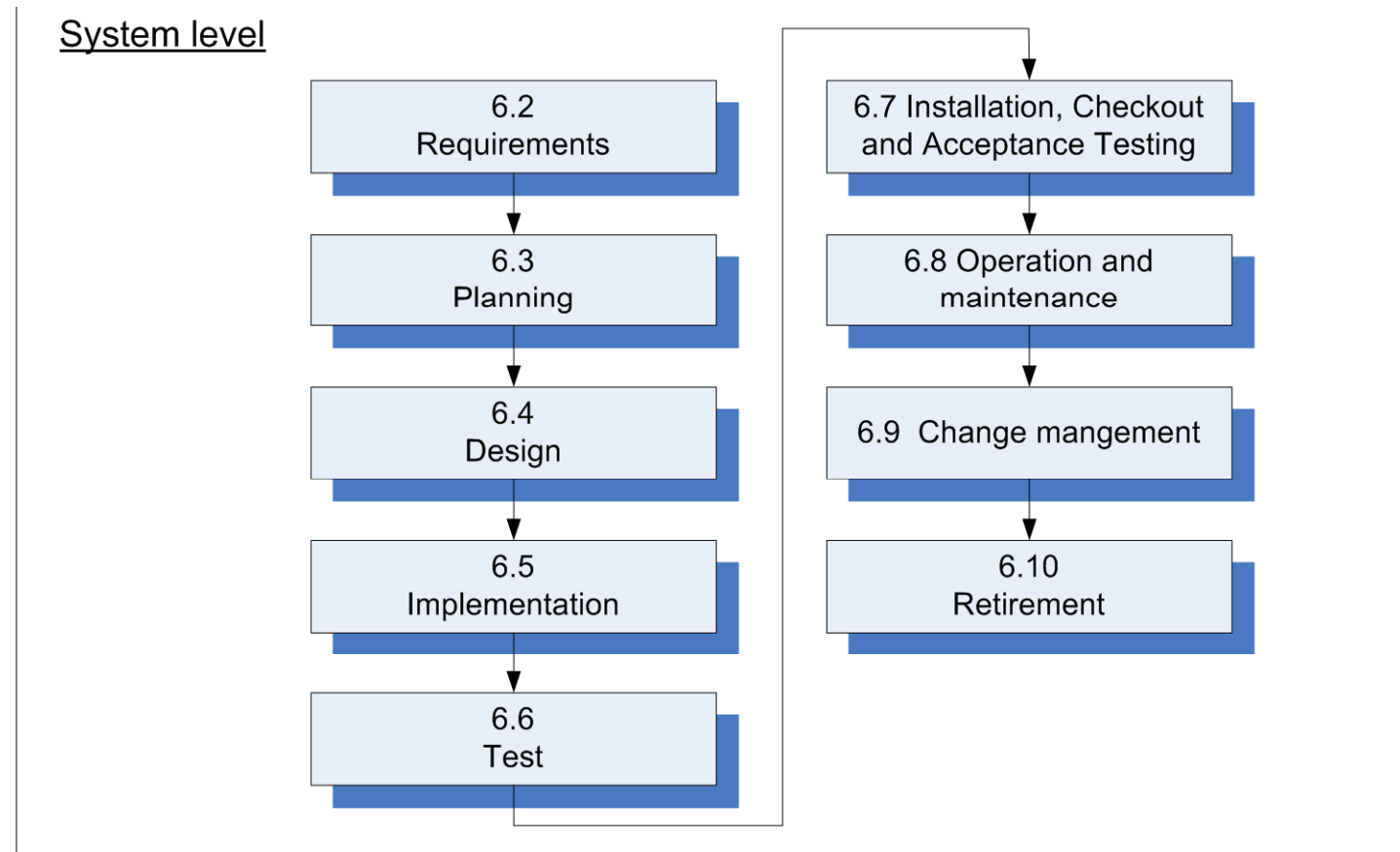
5.2.3.3 Assignment of technical requirements

- **Degree S2 additional requirements**
 - Communications should be one-way from S2-graded systems towards S3-graded systems
 - Data transmission from a S3-graded system to a S2-graded system shall be restricted to the maximum extent and justified on a case-by-case basis.
 - Software upgrade and configuration change of a S2-graded system shall not be possible from a S3-graded system.
 - Software upgrade and configuration change of S2-graded systems shall be done only one channel at time.
 - Access to S2-graded systems shall be strictly limited to prevent access from unauthorized persons. This shall be enforced by physical protection measures (incl. locked cabinet, zone access control), monitored by alarms in control room, and covered by appropriate organizational and administrative measures.
 - Communications initiated by IT systems (i.e., non I&C systems) towards I&C systems shall be justified and controlled on a case by case basis. Any direct remote communication from outside the plant shall be preventedg) Design measures shall limit access to programmable zones of S2-graded systems (by efficient user authentication) and prevent from any unauthorized creation of new access to these zones.
 - Alarms of the anomaly detection system should be analyzed promptly and appropriate measures should be taken.

5.2.3.3 Assignment of technical requirements

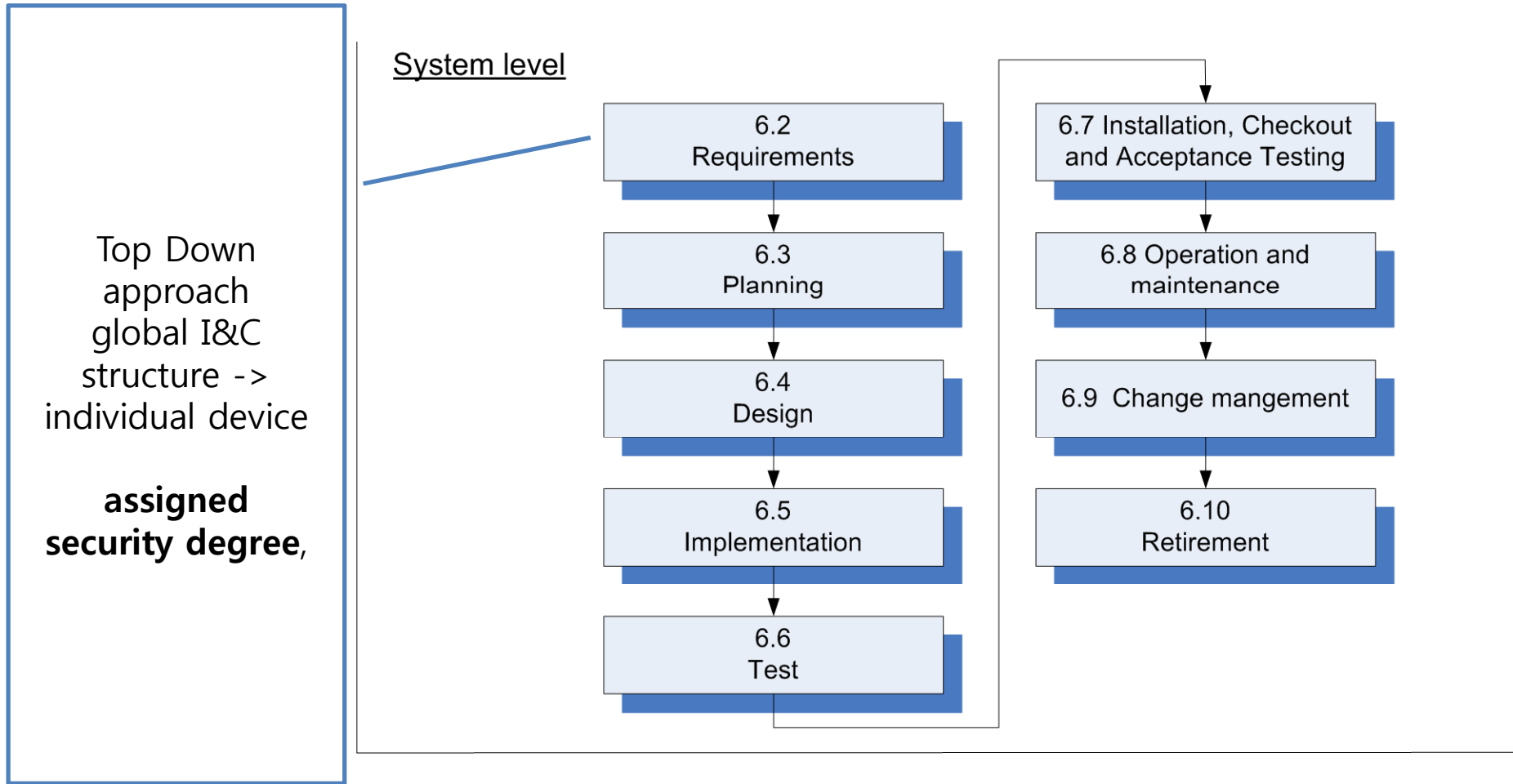
- **Degree S3 additional requirements**
 - Remote access from outside the plant technical buildings which could influence the I&C system functions shall be justified on a case-by-case basis and shall not compromise security and safety requirements associated to the system.
 - S3-graded systems shall be physically protected against unauthorised access. Access control shall include reliable identification of personnel.
 - Security logs should be checked periodically for systems performing category C functions. e) Alarms of the anomaly detection system should be analyzed and appropriate measures should be taken.

6. Life Cycle Implementation for I&C system security



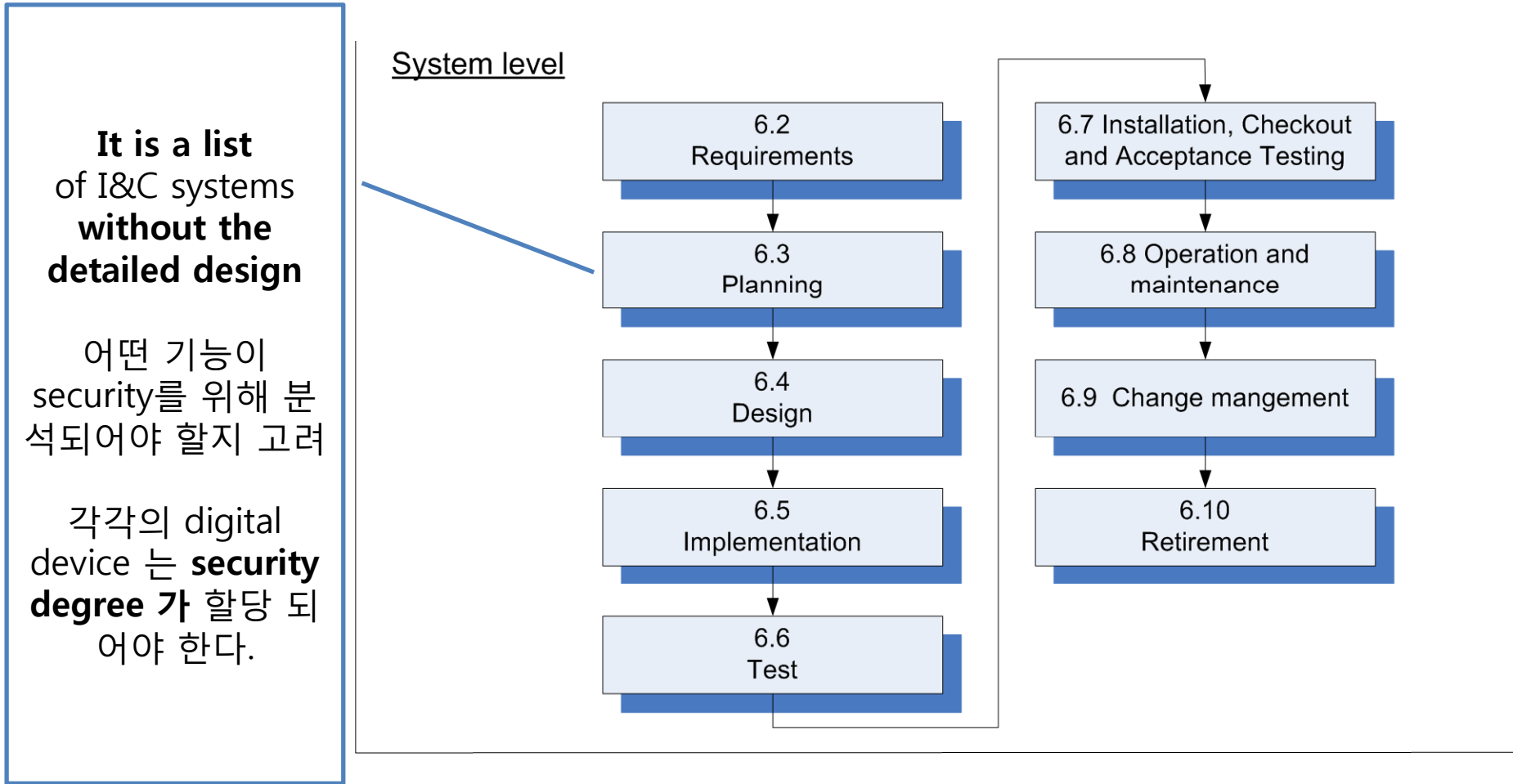
The following clauses provide an **overview of the documents and tasks** that should be included in the I&C security life cycle process on a system level.

6. Life Cycle Implementation for I&C system security



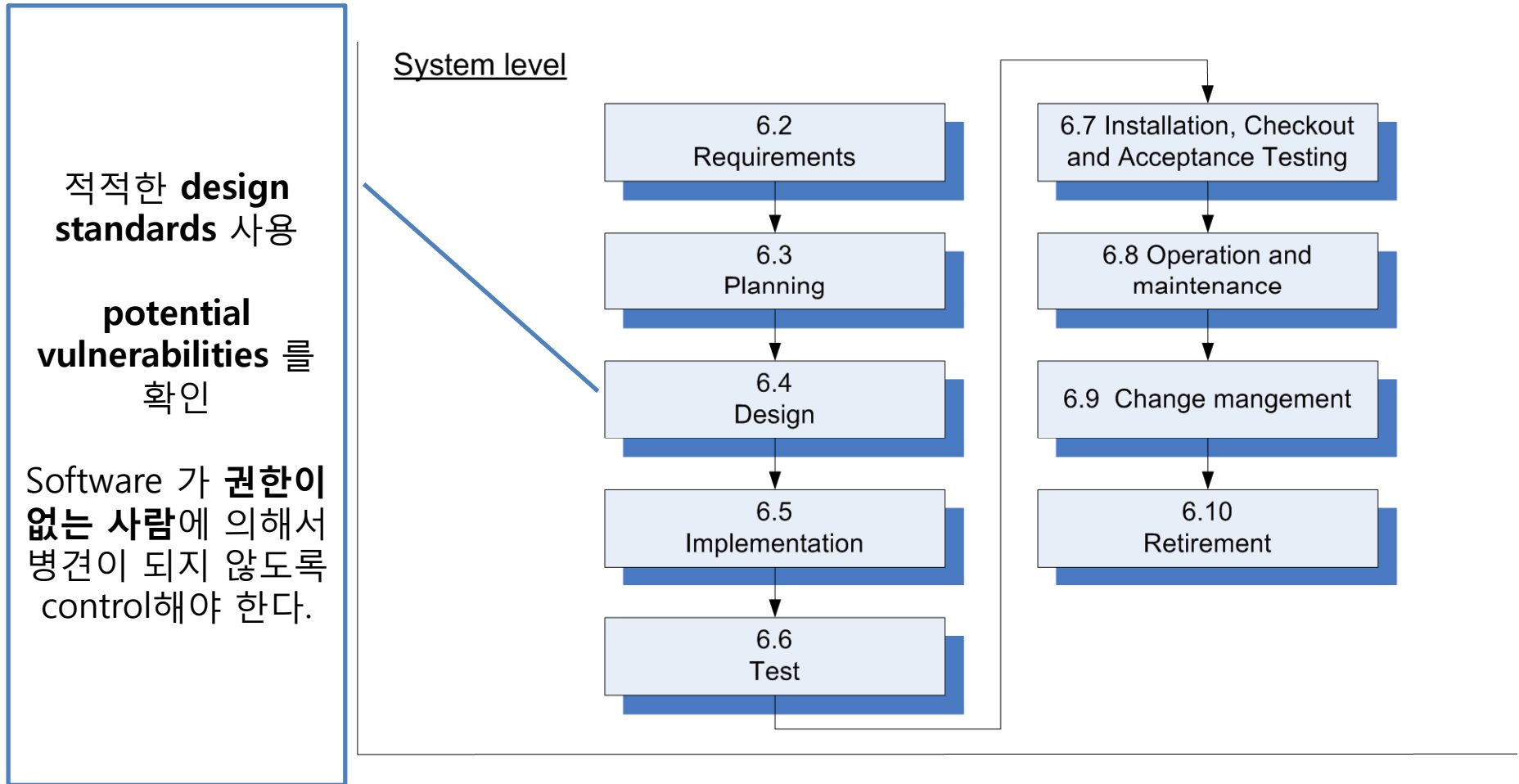
The following clauses provide an **overview of the documents and tasks** that should be included in the I&C security life cycle process on a system level.

6. Life Cycle Implementation for I&C system security



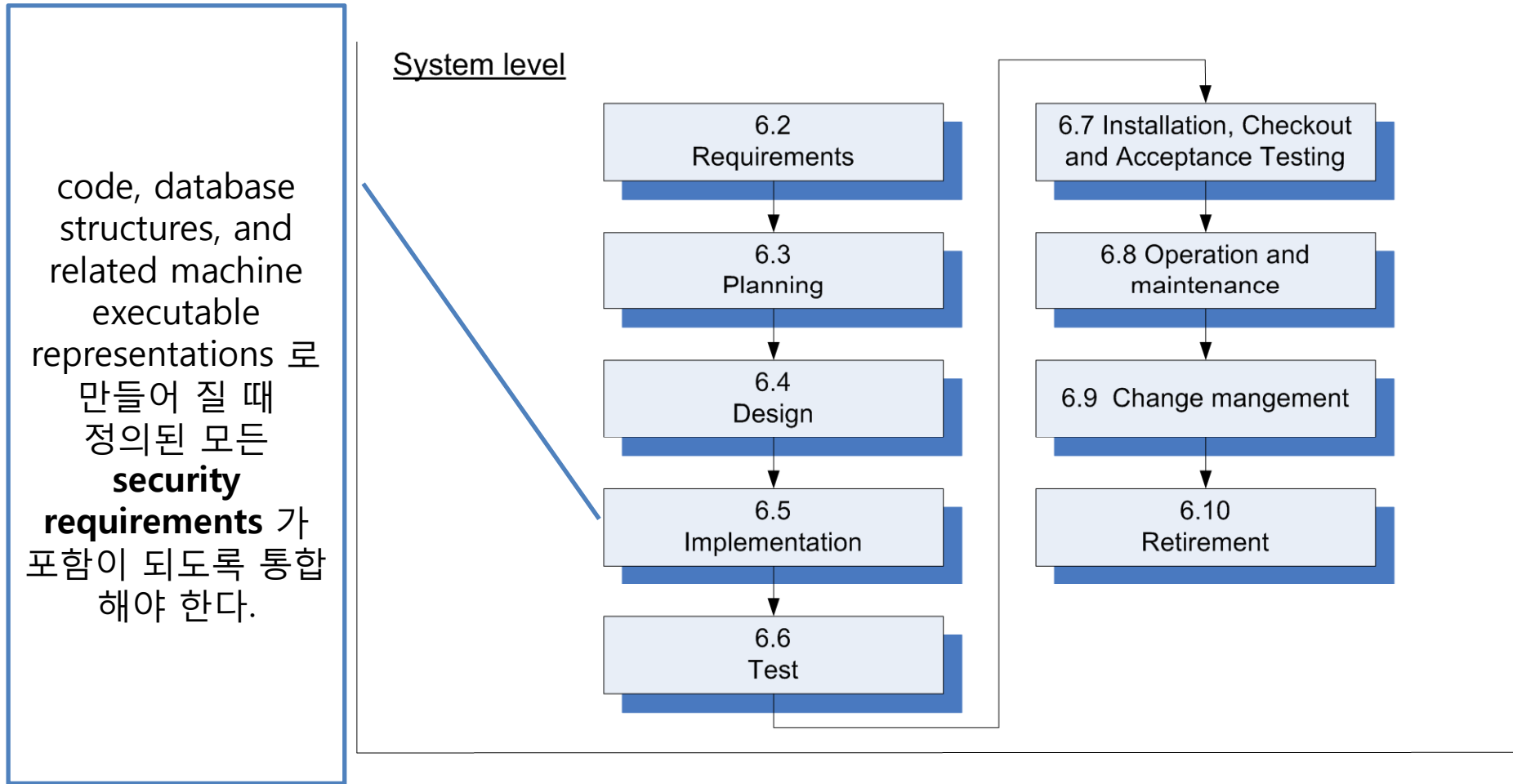
The following clauses provide an **overview of the documents and tasks** that should be included in the I&C security life cycle process on a system level.

6. Life Cycle Implementation for I&C system security



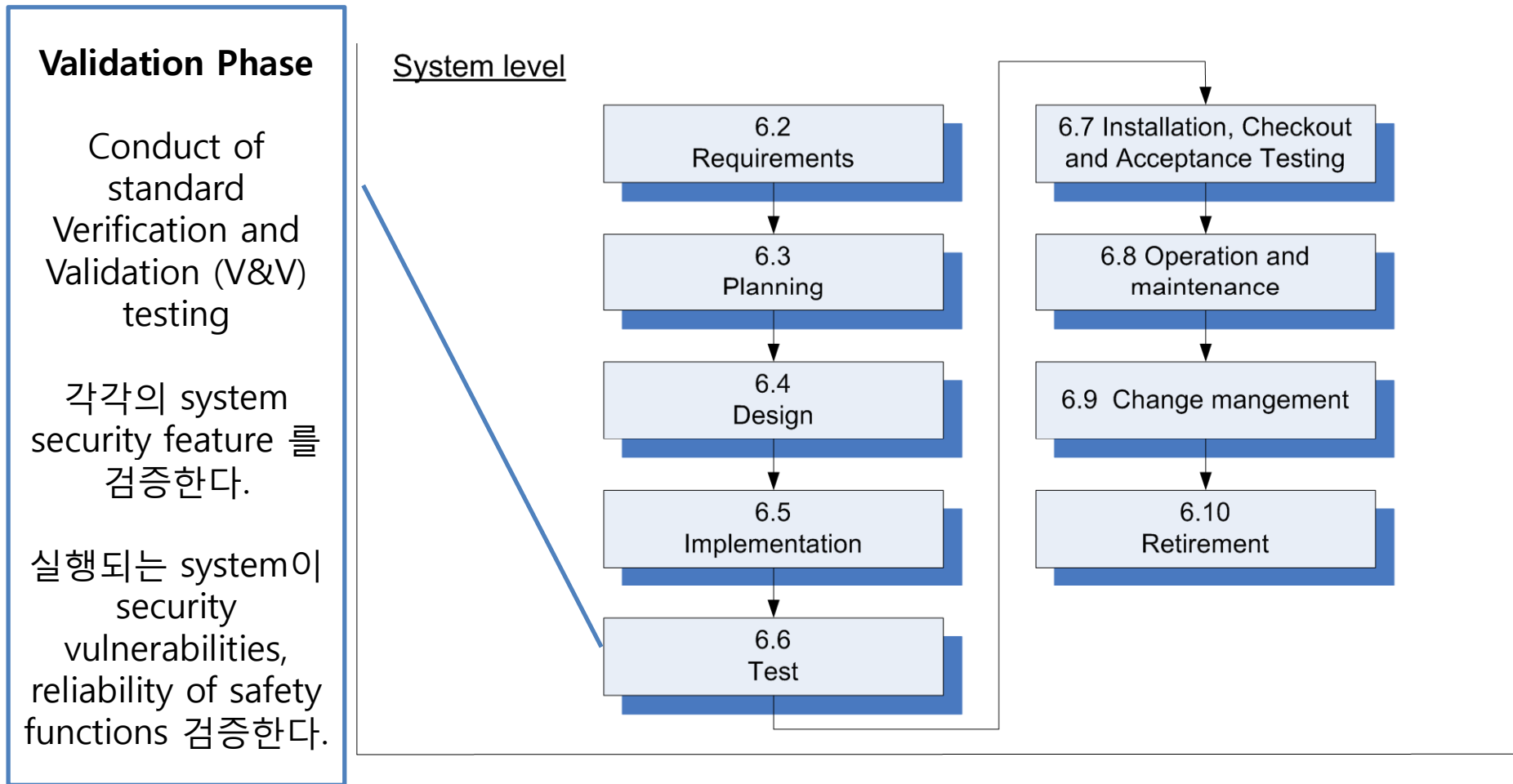
The following clauses provide an **overview of the documents and tasks** that should be included in the I&C security life cycle process on a system level.

6. Life Cycle Implementation for I&C system security



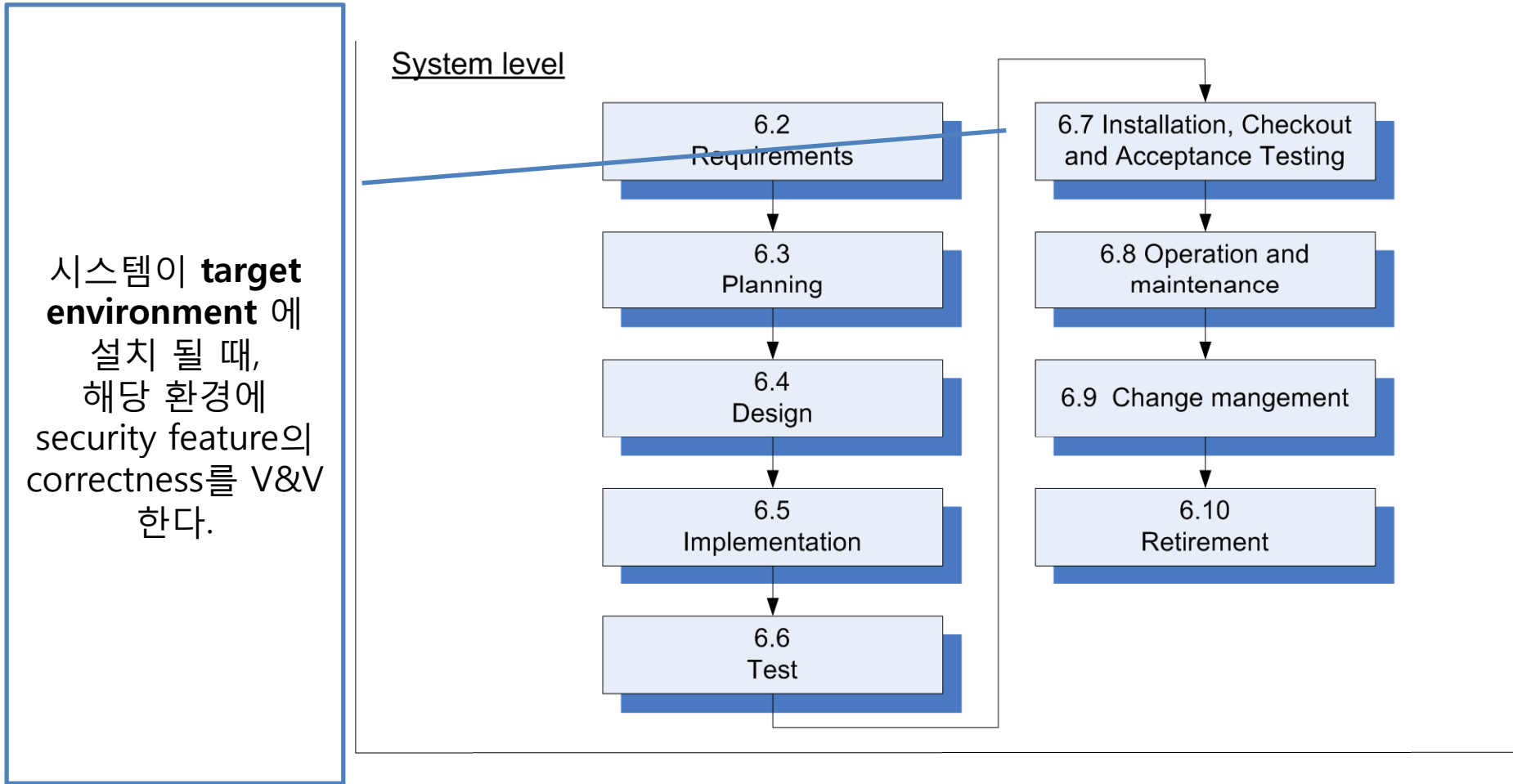
The following clauses provide an **overview of the documents and tasks** that should be included in the I&C security life cycle process on a system level.

6. Life Cycle Implementation for I&C system security



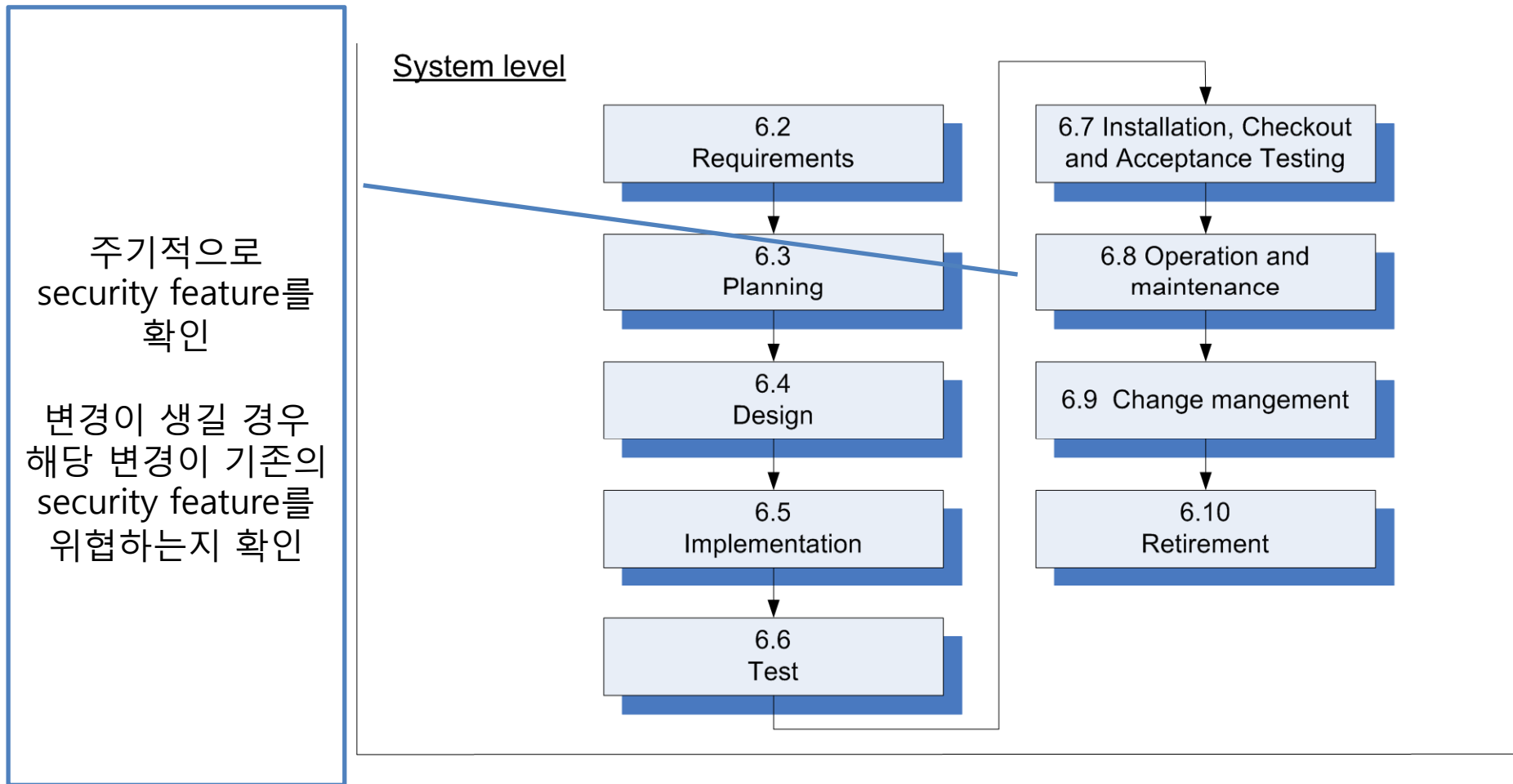
The following clauses provide an **overview of the documents and tasks** that should be included in the I&C security life cycle process on a system level.

6. Life Cycle Implementation for I&C system security



The following clauses provide an **overview of the documents and tasks** that should be included in the I&C security life cycle process on a system level.

6. Life Cycle Implementation for I&C system security



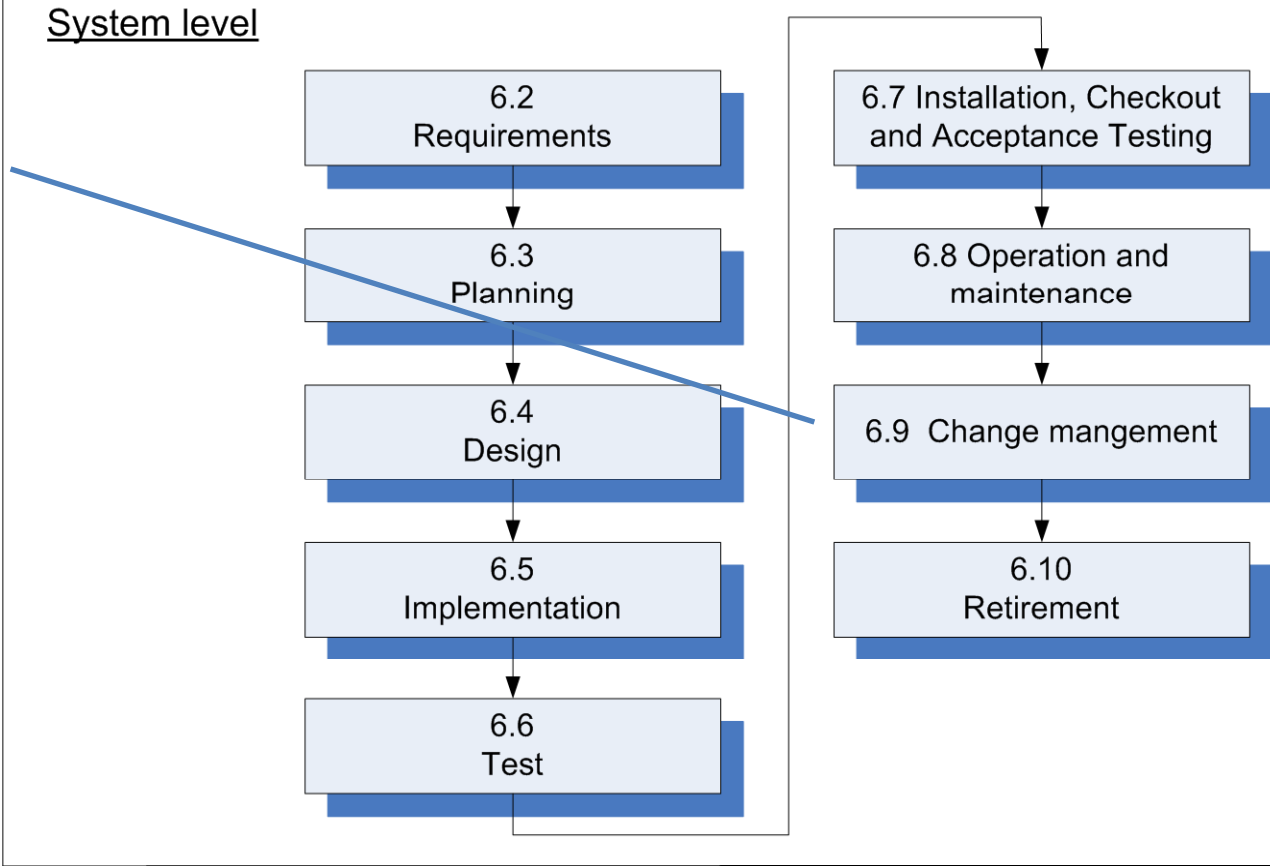
The following clauses provide an **overview of the documents and tasks** that should be included in the I&C security life cycle process on a system level.

6. Life Cycle Implementation for I&C system security

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

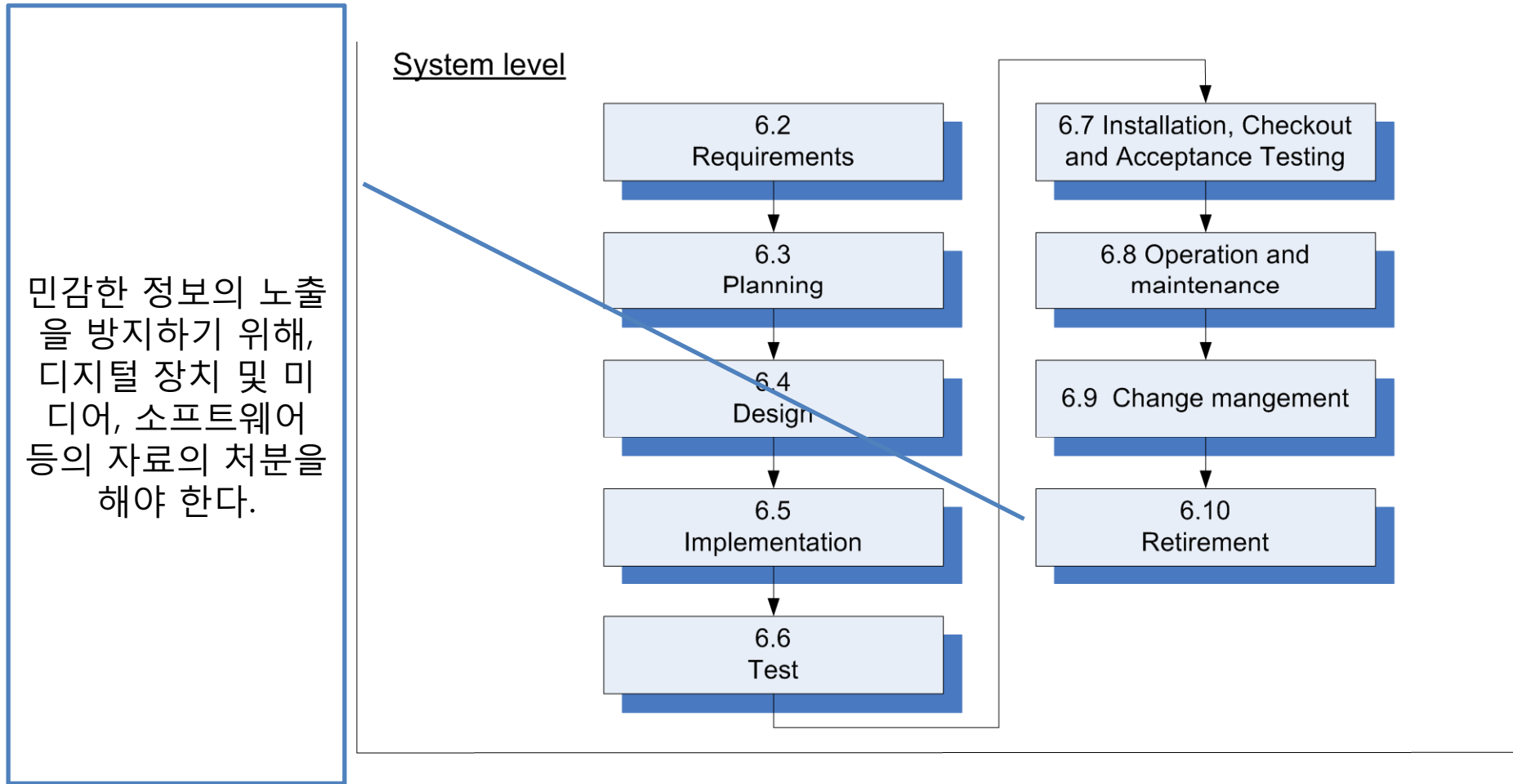
변경에 대한 review 와 testing을 해야 한다.

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



The following clauses provide an **overview of the documents and tasks** that should be included in the I&C security life cycle process on a system level.

6. Life Cycle Implementation for I&C system security



The following clauses provide an **overview of the documents and tasks** that should be included in the I&C security life cycle process on a system level.

6.2 Requirements Phase

- A **top-down approach**,
 - global I&C structure -> individual device
 - Specifications shall be written in order to cover the **global I&C structure** from a functional point of view, before addressing functional **sub-structures and their interfaces**.
- A **security degree**, as defined in clause 5.2.3.2, and associated security requirements shall **be assigned** to each functional sub-structure

6.3 Planning Phase



- 6.3.1 Identification and Classification of Digital Devices
 - Each I&C system within the plant or facility design shall be identified.
 - **It is a list** of I&C systems **without the detailed design** or component selections
 - This list shall be used to evaluate **what functional areas need to be analysed and secured.**
 - Each digital device shall **be assigned to a security degree.**
- 6.3.2 Communication Pathways
 - As part of this process, the system **boundaries** should be defined and a system **map** established.
 - Enforce and **document assigned authorizations** for controlling the flow of information, within and **between interconnected systems** in accordance with their assigned security degrees

6.4 Design Phase



- To address control over
 - (1) physical and logical access to the I&C system functions,
 - (2) use of I&C systems, and
 - (3) data communication with other I&C systems.
- The **designer should ensure** that the software code design complies with **appropriate design standards**, to address **potential vulnerabilities** that can be introduced as part of the design process.
- Access to all software entities placed under configuration control shall be subject to **adequate controls** to ensure that **software is not modified by unauthorized persons** and that the security of the software is maintained.

6.5 Implementation Phase



- This subclause is focused on implementation of the secure design for creation of secure hardware and software.
- In the implementation phase, hardware and software shall be integrated per the system design into code, database structures, and related machine executable representations, including all defined security requirements.

6.6 Validation Phase



- Conduct of standard **Verification and Validation (V&V)** testing per **required standards shall be performed for appropriately specified security requirements** for safety systems and important to safety systems.
- Additionally, **testing** shall verify the I&C security design of the hardware architecture, external communication devices and configurations **for unauthorized pathways and system integrity.**

6.7 Installation and Acceptance Testing Phase



- The installation and acceptance testing for specified security requirements shall comply with this standard and the plant-specific Policy and Procedures, as well as the plant digital system security programme, as applicable. **In installation and acceptance testing**, the system shall be installed and tested in the **target environment to verify and validate** the correctness of the I&C system security features and the appropriate incorporation to the system.

6.8 Operation and Maintenance Phase



- During the operational and maintenance phase, the **periodic security audits** of security features under configuration and control shall be performed. Prior to any system modification or maintenance, the affected components shall be evaluated to confirm that all protective feature and design elements will remain functional. After such modifications or maintenance are performed, any temporarily disabled security protective features and controls shall be restored and security functionality verified.

6.9 Change Management

- Change management processes shall follow plant procedural, regulatory and/or licensing commitments, as applicable, for maintaining both compliance basis and configuration control. When required (e.g. major evolution, technological shift), changes shall follow the same review and testing process for I&C security as with the original approval process that was applied to the system or component. **A risk assessment shall be performed before any modifications are made that could affect a security feature.**

6.10 Retirement Phase



- The I&C system retirement phase shall be primarily the responsibility of the plant management.
- An effective continuing programme shall address the **retirement lifecycle phase**. Procedure(s) shall be in place to address proper retirement of digital devices and disposal of media and resident software in a controlled manner, **to avoid disclosure of sensitive information**. In addition, security aspects for the preparation of a system for retirement such as the dual operation of both the current and new system – if needed – should be addressed.

7. Security controls

- 5장과 6장에서 제시되었던 보안 프로그램의 프레임에서 security feature를 다루기 위해 원자력 I & C 환경에서 고려해야 할 특정 사항을 제공.
- eleven security thematic = ISO/IEC 27000 series
- This is due to the fact that this clause only aims at **providing a complementary perspective** on security controls for NPPs, not to add new recommendations or requirements to the standard.
- It does not aim at providing a detailed or exhaustive list of security controls.

<u>Security thematic areas</u>
7.2.1 Security policy
7.2.2. Organizing Information Security
7.2.3. Asset Management
7.2.4. Human Resources Security
7.2.5. Physical and Environmental Security
7.2.6. Communications and Operations Management
7.2.7. Access Control
7.2.8. I&C Systems Acquisition, Development and Maintenance
7.2.9. I&C Security Incident Management
7.2.10. Operation Continuity Management
7.2.11. Compliance

7. Security controls

- **7.2.1 Security Policy**
 - The objective of this subclause is to provide plant management direction and support for I&C security in accordance with **business requirements, safety considerations, and plant performance** while being compliant with all applicable **national laws and regulations**.
 - Plant management shall set a **clear** policy direction in line with overall security requirements (**including corporate security policy, physical security, and data security**) through the issue, implementation and management of an organizational wide security policy.

Security thematic areas
7.2.1 Security policy
7.2.2. Organizing Information Security
7.2.3. Asset Management
7.2.4. Human Resources Security
7.2.5. Physical and Environmental Security
7.2.6. Communications and Operations Management
7.2.7. Access Control
7.2.8. I&C Systems Acquisition, Development and Maintenance
7.2.9. I&C Security Incident Management
7.2.10. Operation Continuity Management
7.2.11. Compliance

7. Security controls

- **7.2.2 Organizing Security**
 - The objective of this subclause is to manage security of I&C systems within the facility.
 - **A management framework shall be established** to initiate and control the implementation of **a cyber security programme** within the plant during I&C platform.
 - **The framework** shall take into account the **different knowledge base, threat issues and operational considerations** that differentiate I&C systems and their associated experts.
 - 국가 및 국제 기관 등 외부 보안 전문가 및 그룹의 설립
 - 지속적인 협력은 보안 관리 프로세스의 중요한 부분

Security thematic areas
7.2.1 Security policy
7.2.2. Organizing Information Security
7.2.3. Asset Management
7.2.4. Human Resources Security
7.2.5. Physical and Environmental Security
7.2.6. Communications and Operations Management
7.2.7. Access Control
7.2.8. I&C Systems Acquisition, Development and Maintenance
7.2.9. I&C Security Incident Management
7.2.10. Operation Continuity Management
7.2.11. Compliance

7. Security controls

- **7.2.3 Asset Management**

- All assets shall be accounted for and have a responsible owner.
- **Owners** should be identified for all assets and the responsibility for maintenance and operational compliance of appropriate controls should be assigned.
- **Owner** should be responsible for maintaining compliance of asset with the national regulations and ensuring that asset and respective controls are properly identified, evaluated and maintained as per system security plan.
- **Owner** should be responsible for proper evaluation of asset's risk component and overall level of vulnerability as discussed in Clause 5 and ensuring that appropriate and effective measures are utilized for asset protection.
- **Owner** should also be responsible for ensuring that new and emergent threats do not impact the required operation of asset – to the degree required by the system risk assessment.

<u>Security thematic areas</u>
7.2.1 Security policy
7.2.2. Organizing Information Security
7.2.3. Asset Management
7.2.4. Human Resources Security
7.2.5. Physical and Environmental Security
7.2.6. Communications and Operations Management
7.2.7. Access Control
7.2.8. I&C Systems Acquisition, Development and Maintenance
7.2.9. I&C Security Incident Management
7.2.10. Operation Continuity Management
7.2.11. Compliance

7. Security controls

- **7.2.4 Human Resources Security**

- The objective of this subclause is to ensure that **employees, contractors** and **authorized third parties** understand their responsibilities, are suitable and qualified for the roles they are considered for and/or assigned, and to minimize the risk of **theft, fraud, misuse** or intentional **sabotage** of facility.

- 채용하기 전에 미리 설명과 서약
- 지속적인 training과 교육 프로그램 구성
- 불법행위에 대한 공식적인 절차 구성
- 인전 협정서에 사인
- 지속적인 신뢰성 프로그램
- 고용 종료 시 지속적인 보안 동의서에 대한 사인

Security thematic areas
7.2.1 Security policy
7.2.2. Organizing Information Security
7.2.3. Asset Management
7.2.4. Human Resources Security
7.2.5. Physical and Environmental Security
7.2.6. Communications and Operations Management
7.2.7. Access Control
7.2.8. I&C Systems Acquisition, Development and Maintenance
7.2.9. I&C Security Incident Management
7.2.10. Operation Continuity Management
7.2.11. Compliance

7. Security controls

- **7.2.5 Physical and Environmental Security**

- 인가되지 않은 물리적 접근, 손상, I & C 시스템에 영향을 미칠 수 있는 간섭 등
- 물리적 보안 지침, 핵 시설의 핵심 및 / 또는 민감한 구성 요소 등은 다양한 방법을 통해 보호되어야 한다.
- 경계와 입구 / 출구 컨트롤 등 물리적 통제를 해결해야 한다.

<u>Security thematic areas</u>
7.2.1 Security policy
7.2.2. Organizing Information Security
7.2.3. Asset Management
7.2.4. Human Resources Security
7.2.5. Physical and Environmental Security
7.2.6. Communications and Operations Management
7.2.7. Access Control
7.2.8. I&C Systems Acquisition, Development and Maintenance
7.2.9. I&C Security Incident Management
7.2.10. Operation Continuity Management
7.2.11. Compliance

7. Security controls

- **7.2.6 Communications and Operations Management**
 - **Responsibilities and procedures for management and operation** of the facility shall be established
 - The safe and reliable operation of a nuclear power facility require detailed and accurate **operational procedures** for the facility.
 - These existing procedures should be tied into the **computer security requirements**.
 - establishment of trusted domain
 - 이동식 매체의 보호/관리
 - 원격 접속 관리
 - Logging
 - monitoring

<u>Security thematic areas</u>
7.2.1 Security policy
7.2.2. Organizing Information Security
7.2.3. Asset Management
7.2.4. Human Resources Security
7.2.5. Physical and Environmental Security
7.2.6. Communications and Operations Management
7.2.7. Access Control
7.2.8. I&C Systems Acquisition, Development and Maintenance
7.2.9. I&C Security Incident Management
7.2.10. Operation Continuity Management
7.2.11. Compliance

7. Security controls

- **7.2.7 Access Control**

- The objective of this subclause is to **control logical access** to facilities I&C systems' information and operation.
- **Security degree**, as defined in Subclause 5.2.3.2, should be the basis for required levels of access control.
- 액세스 제어, 정보 보급 및 권한 부여를 위해 계정 설정 정책뿐만 아니라 운영 액세스 제약 조건을 고려

<u>Security thematic areas</u>
7.2.1 Security policy
7.2.2. Organizing Information Security
7.2.3. Asset Management
7.2.4. Human Resources Security
7.2.5. Physical and Environmental Security
7.2.6. Communications and Operations Management
7.2.7. Access Control
7.2.8. I&C Systems Acquisition, Development and Maintenance
7.2.9. I&C Security Incident Management
7.2.10. Operation Continuity Management
7.2.11. Compliance

7. Security controls

- **7.2.8 I&C Systems Acquisition, Development and Maintenance**
 - The objective of this subclause is to ensure systems are **developed and maintained** in an **appropriate and secure manner** commensurate to their security degree.
- D
- Systems should have **cyber security** elements **considered** and designed in from the **requirements** stage.
 - **Designers and developers** shall have **established and verified secure development methodologies** in place throughout the development lifecycle of a system.
- M
- Prior to any patches and/or **upgrades**, system functionality should be verified to ensure that such patch or upgrade **will not impact the safety function** of the system.
 - Any **graded approach** to recommendations and requirements during development, operation and maintenance should be based upon assigned security degree.

Security thematic areas
7.2.1 Security policy
7.2.2. Organizing Information Security
7.2.3. Asset Management
7.2.4. Human Resources Security
7.2.5. Physical and Environmental Security
7.2.6. Communications and Operations Management
7.2.7. Access Control
7.2.8. I&C Systems Acquisition, Development and Maintenance
7.2.9. I&C Security Incident Management
7.2.10. Operation Continuity Management
7.2.11. Compliance

7. Security controls

- **7.2.9 I&C Security Incident Management**

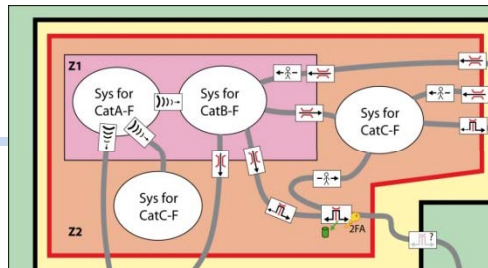
- I&C 시스템과 관련된 보안 이벤트를 식별하고 적시에 완화시킬 수 있도록 확인
- 공식화된 event 보고 및 대응 절차 있어야 한다.
- 모든 시스템 사용자는 cyber-event에 대한 대응절차 등을 훈련 받아야 한다.
- 식별된 cyber-event는 바로 기록해 두어야 한다.
- 외부자료(다른 도메인의 cyber-event)를 이용하여 지속적으로 monitoring 해야 한다.

Security thematic areas
7.2.1 Security policy
7.2.2. Organizing Information Security
7.2.3. Asset Management
7.2.4. Human Resources Security
7.2.5. Physical and Environmental Security
7.2.6. Communications and Operations Management
7.2.7. Access Control
7.2.8. I&C Systems Acquisition, Development and Maintenance
7.2.9. I&C Security Incident Management
7.2.10. Operation Continuity Management
7.2.11. Compliance

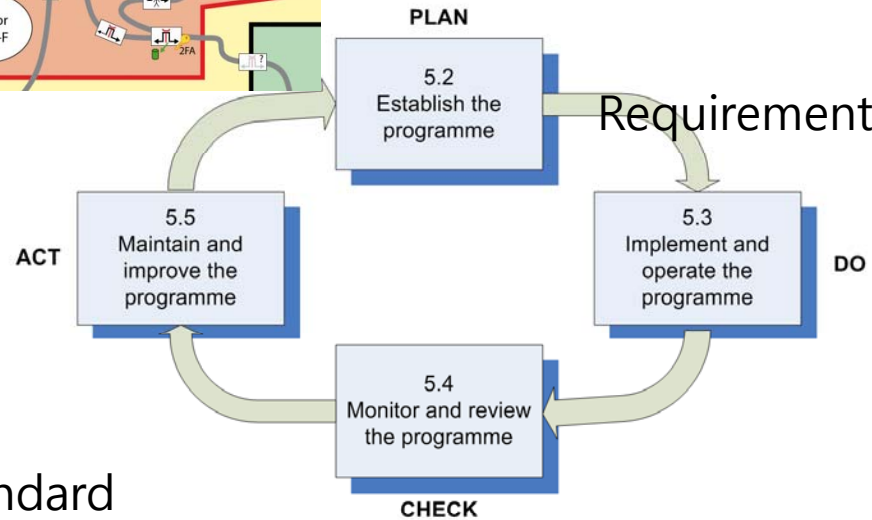
7. Security controls

- **7.2.10 Operation Continuity Management**
 - 목적은 악의적인 행동으로 인해 I&C 시스템이 중단되는 것을 막고 적시 재개를 할 수 있게 하는 것.
 - Processes to support operation **continuity** management with regards to cyber security and the impact of malicious events should be **integrated** into the facilities existing operation continuity programmes.
- **7.2.11 Compliance**
 - 목적은 law, statutory, regulatory, security requirements에 어긋나는 점이 없는 지 확인 하는 것.

Security thematic areas
7.2.1 Security policy
7.2.2. Organizing Information Security
7.2.3. Asset Management
7.2.4. Human Resources Security
7.2.5. Physical and Environmental Security
7.2.6. Communications and Operations Management
7.2.7. Access Control
7.2.8. I&C Systems Acquisition, Development and Maintenance
7.2.9. I&C Security Incident Management
7.2.10. Operation Continuity Management
7.2.11. Compliance



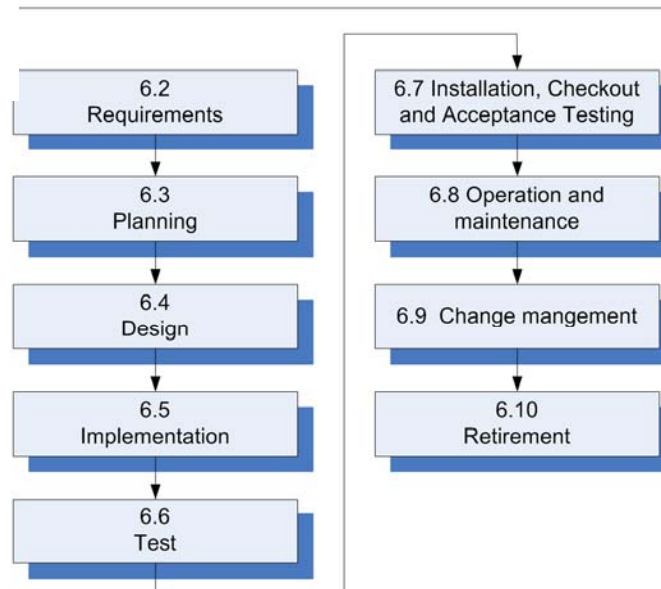
Degree



Security thematic areas

7.2.1 Security policy
7.2.2. Organizing Information Security
7.2.3. Asset Management
7.2.4. Human Resources Security
7.2.5. Physical and Environmental Security
7.2.6. Communications and Operations Management
7.2.7. Access Control
7.2.8. I&C Systems Acquisition, Development and Maintenance
7.2.9. I&C Security Incident Management
7.2.10. Operation Continuity Management
7.2.11. Compliance

아직 미완성 standard
5장, 6장, 7장의
연관관계가 조금 부족



NUCLEAR REGULATORY 5.71

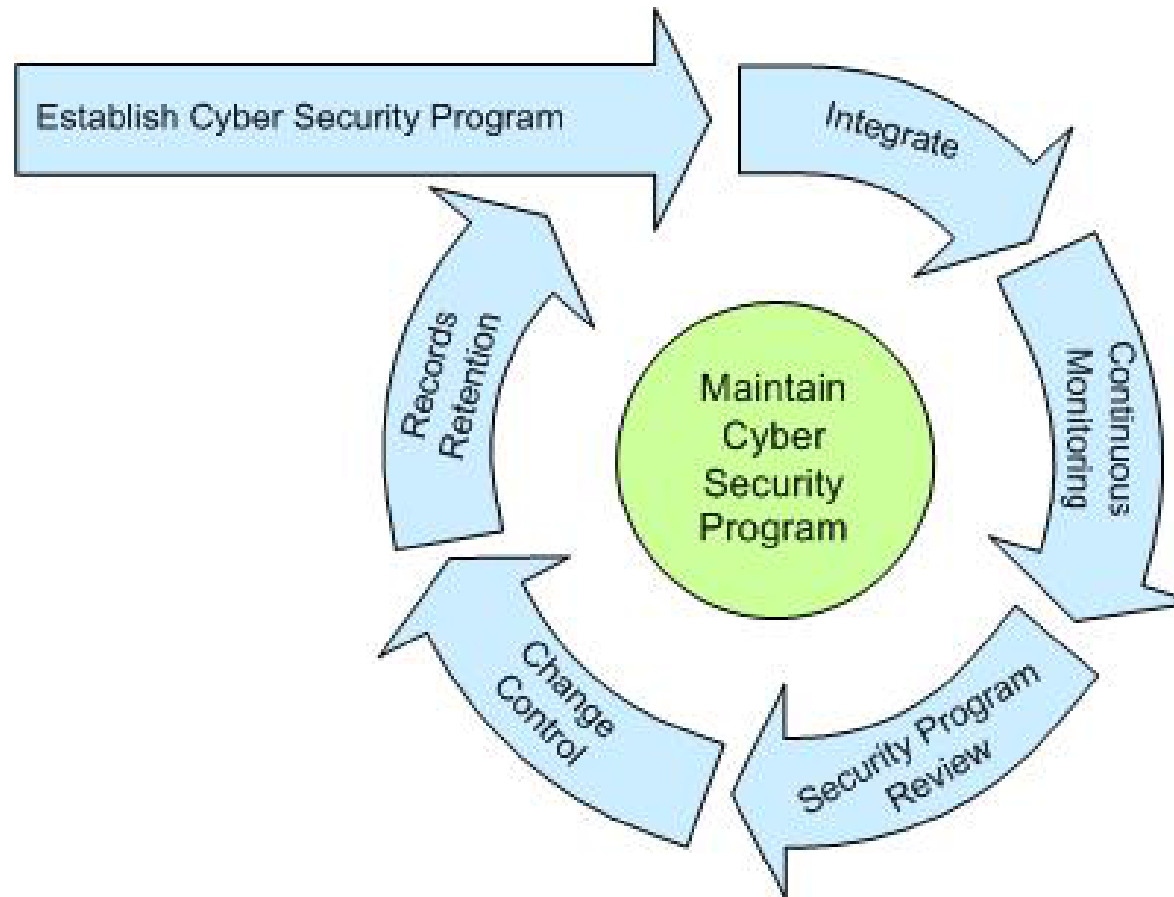
RG 5.71



- **Title 10 CFR 73.54**
 - “**Protection of Digital Computer and Communication Systems and Networks**” 2009
 - a licensee must provide **high assurance** that digital computer and communication systems and networks are adequately protected against **cyber attacks**, up to and including the DBT.
- **NRC Regulatory Guide 5.71**
 - “**Cyber Security Programs for Nuclear Facilities,**” 2010

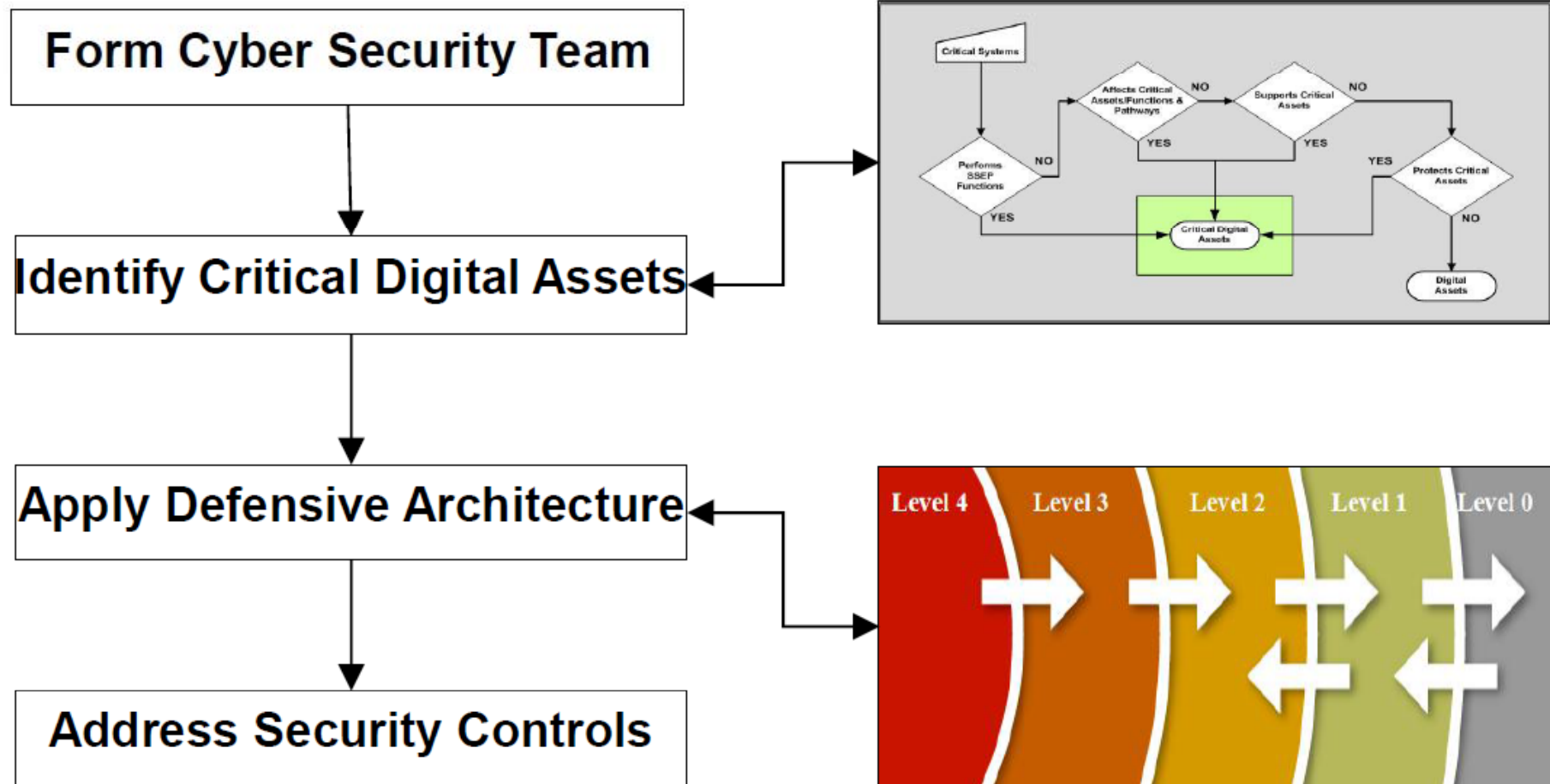
RG 5.71

- The process of establishing, implementing, and maintaining the cyber security program.



Security life cycle process

RG 5.71



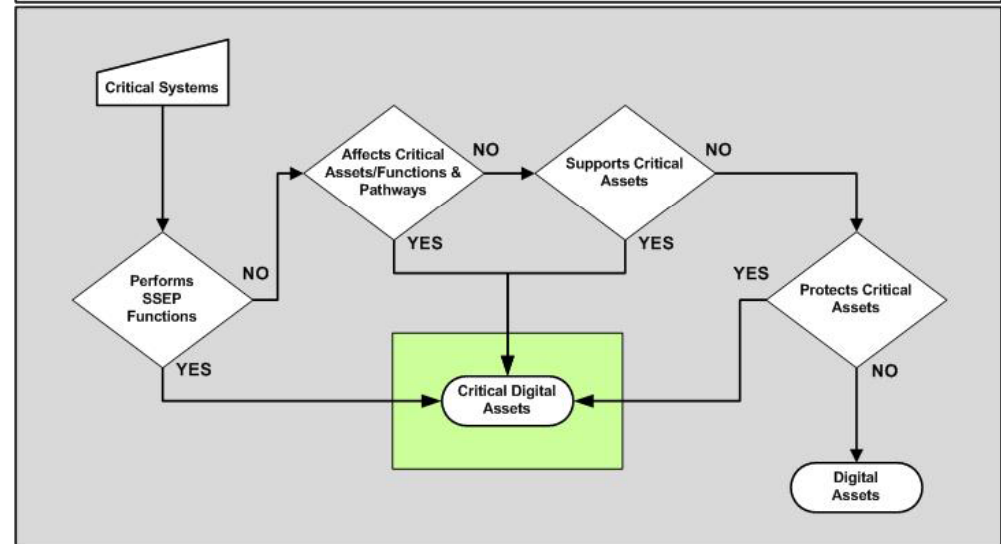
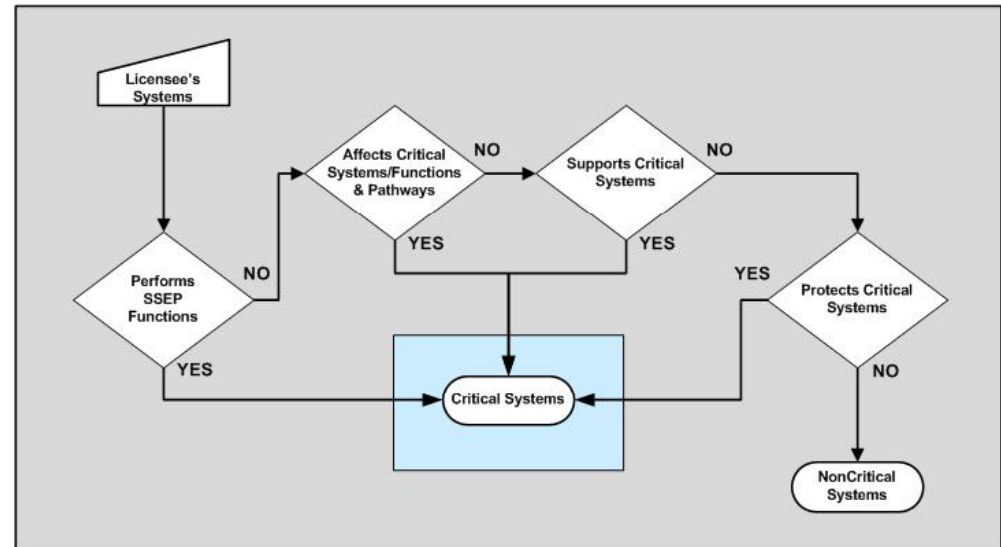
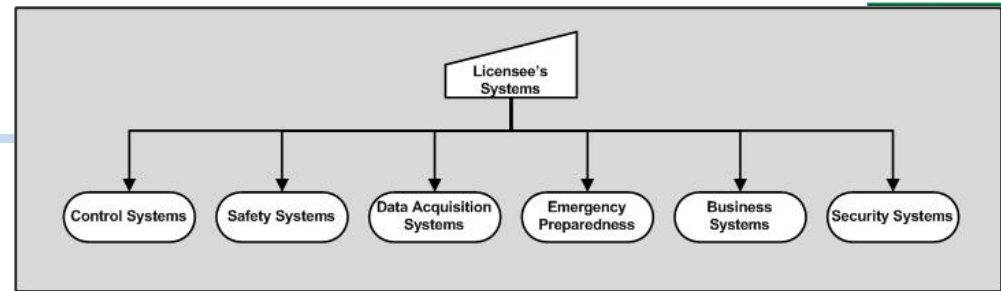
RG 5.71



- Form a Cyber Security Team
 - **Senior Plant Manager** will be designated as the “Cyber Security Program Sponsor”
 - **Cyber Security Program Manager** will oversee the Cyber Security Program
 - **Cyber Security Specialists** protecting CDAs from cyber threats
 - **Cyber Security Incident Response Team** that will include representatives from physical security, operations, engineering, IT and other organizations
 - Other plant staff will also have cyber security roles

RG 5.71

- Identification of Critical Digital Assets
- A typical nuclear power plant **contains hundreds of individual systems** that contribute to the overall operation, safety, and security of the facility.
- Safety, security, and emergency preparedness(SSEP)
- Critical Asset(CA)
- Critical Digital Assets(CDAs).



RG 5.71

- Security Defensive Architecture

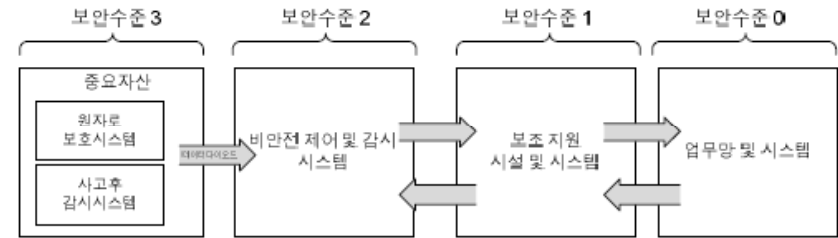


그림 1. 다중방호 구조의 예



- Level 4: Vital Area
- Level 3: Protected Area
- Level 2: Owner-Controlled Area
- Level 1: Corporate Accessible Area
- Level 0: Public Accessible Area



데이터 흐름

RG 5.71



- Security Controls
 - Technical Control
 - Operation Control
 - Management Control

Technical Control

- Technical controls are safeguards or protective measures that are executed through **nonhuman mechanisms** contained within the hardware, firmware, operating systems, or application software.
 - **access** control rights (i.e., which individuals and processes can access what resources)
 - and access control **privileges** (i.e., what these individuals and processes can do with the resources accessed)
 - system hardening (i.e., the identification and removal of unnecessary system services, communication pathways, data storage capabilities, and insecure communication protocols)
 - management of CDAs (i.e., establishing, activating, modifying, reviewing, disabling, and removing accounts)
 - auditing of CDAs (i.e., at least annually or immediately upon changes in personnel responsibilities or major changes in system configurations or functionality)
 - separation of duties (i.e., through assigned access authorizations)

Operational Control

- Operational controls are protective measures typically performed by humans rather than by automated means.
 - Media Protection
 - USB, ... X
 - Personnel Security
 - CDA에 개인 혼자 X
 - System and Information Integrity
 - CDA에 관련된 정보는 integrity 해야 한다.
 - Maintenance
 - Physical and Environmental Protection
 - Incident Response
 - Contingency Planning/Continuity of SSEP Functions
 - Awareness and Training
 - Configuration Management

Management Control



- Management controls are those that concentrate on the management of risk and the security policy environment.
 - Continuous Monitoring and Assessment
 - Ongoing Assessments of Security Controls
 - Effectiveness Analysis of Security Controls
 - Vulnerability Scans and Assessments

 - Change Control

- 감사합니다...