KU 건국대학교 KONKUK UNIV.

Security vs Safety

김 그 린

greenkim@konkuk.ac.kr

KU 건국대학교 KONKUK UNIV.

Table of Contents

1. Introduction

1.1 Concepts

1.2 Principles

1.3 Methodology

1.4 Standards

1. Introduction (1/3)

- Program Logic Device, FPGA는 I&C의 개발, 구현에 널리 사용
  - FPGA를 사용한 I&C 프로젝트는 종종 Safety-critical 하며, 소프트웨어와 하드웨어 구성요소를 모두 포함하는 복잡한 솔루션
  - NPP I&C 등에서 확인 된 바, 마이크로세서(소프트웨어 등)기반 시스템에 비해 상대적으로 장점이 많음
  - But, I&C에서 FPGA 사용은 safety 확보 측면에서 특정 위험을 초래
  - FPGA 기반 I&C의 safety에 대한 평가를 위해선 security 특성 고려가 필요
  - NPP I&C와 관련된 주요 문제 중 하나는 security 보장을 요구하는 것과 표준에 따른 개발 수행 및 구현된 시스템이 요구사항에 맞는 가를 보장하는 것

% FPGA (Field Programmable Gate Arrays)
% NPP (Nuclear Power Plant)
% I&C (Instrumentation and control system)
% SCI&C(Safety-critical Instrumentation and control systems)

1. Introduction (2/3)

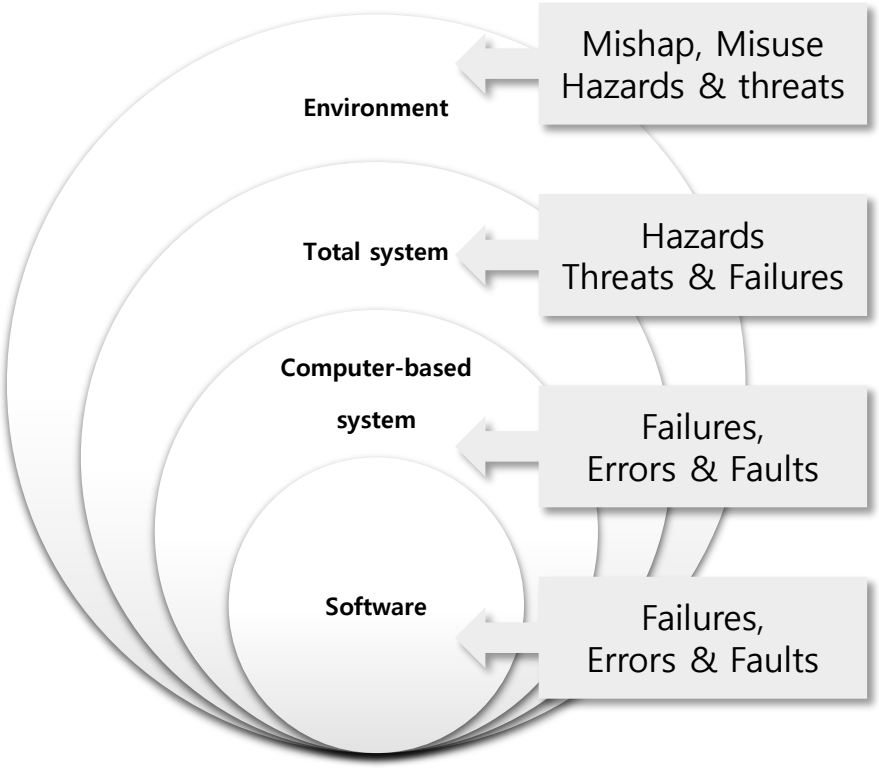
- Safety 영역에서, 시스템의 이점과 기능은 발생가능성을 지닌 사고적 결함(harm)과 균형을 이루어야 하고, Security 영역은 악의적 결함(harm)과 균형을 이루어야 함

"Security is concerned with the risks originating from the environment and potentially impacting the system, whereas safety deals with the risk arising from the system and potentially impacting the environment"

From Piertre-Camnbacedes and Chaudet. 2010

- Safety, Security 영역의 공통점은 harm의 잠재로부터의 risk라고 할 수 있으며, 이를 식별, 분석, 평가하고 다루는 것이 중요
  - Safety는 의도치 않은 hazards에 다루고, Security는 의도적인 threats에 대해 다룸
  - Safety는 accidental risk를 야기하는 의도치 않은 행동이나 실패에 대해 다루고, Security는 악의적 risk를 야기하는 의도적인 공격에 대해 다룸

Cf. A layered view of computer-based systems



Harm	is the "Physical injury or damage to the health of people or damage to property or the environment" (IEC, 2008)
Hazard	is a "potential source of harm" (IEC, 2008)
Threat	is the "potential cause of an incident which may result in harm to a system or organization" (ISO, 2005)
Failure	is a "termination of the ability of a functional unit to provide a required function or operation of a functional unit in any way other that as required" (IEC, 2008)
Error	is the "discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition" (IEC, 2008)
Fault	is the "abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function" (IEC, 2008)

From Comparing risk identification techniques for safety and security requirements

1. Introduction (3/3)

- 과거 Safety와 Security는 별도의 지침을 따라왔음, 하지만 이러한 양상에 변화가 생겼으며, Stakeholder들은 “if it’s not secure, it’s not safe”라고 주장
  - 위의 말이 성립하지 않으면, 사람에게 해를 끼치거나 피해를 입힐 수 있다고 간주되는 safety critical system은 공격자로 하여금, 광범위한 피해와 극심한 공포를 초래 및 악의적 공격대상으로 자리잡을 가능성 내포
  - Safety와 Security를 결합하는 것은 새로운 개념은 아니지만, 간단하지 않음
  - Safety와 Security 모두 good process, 위험 분석의 중요성, 검증의 필요성과 정당성을 강조하는 정교한 엔지니어링 문화를 가지고 있음
  - Safety와 Security가 지니고 있는 유사점은 피상적이며, 실제로 구현 시 많은 어려움이 있음

1.1 Concepts

- Safety와 Security의 공통점은 다른 개념 및 용어를 통해 불분명하게 제시
  - 실제로 Safety와 Security 커뮤니티 내 ·외부의 용어에는 상당한 차이가 있으며, 이해를 위해 공용어 및 일반적인 ontology를 설립할 필요성 내포

· safety : absence of catastrophic consequences on the user(s) and the environment
· security : a composite of the attributes of confidentiality, integrity and availability, requiring the concurrent existence of 1) availability for authorized actions only 2) confidentiality, and 3) integrity with "improper" meaning "un authorized"

From Basic Concepts and Taxonomy of Dependable and Secure Computing

- 넓은 의미에서 Safety는 시스템으로부터 환경을 보호하는 것에 다루는 반면, Security는 환경으로부터 시스템을 보호하는 것을 이야기 함
  - Safety와 Security는 dependability의 종류 중 하나로 볼 수 있으며, 유사한 기술 및 방법을 사용, 이로 인해 Safety와 Security의 초점이 다르고 요구 사항 충돌 가능

1.2 Principles

- Safety와 Security의 Principle들은 중첩된 부분이 많지만 중요성과 잠재적 충돌 측면에서 차이점을 지님
  - Defense in Depth의 경우, 두 요소에 걸쳐 모두 중요한 architecture principle이지만 safety 관련 고려사항은 safety barrier의 독립성과 효율성이 중요 (매커니즘의 효율성, 최소 권한, 심리적 수용과 같은 security principle은 쉽게 허용)
  - 복구 principle의 용이성은 Safety 시스템이 calibration 및 유지 보수를 위한 작동 변화를 지원하기 위해 설계되어 있더라도, 시스템의 security는 쉽게 변경할 수 없는 것에 의존하지 않아야 한다고 주장
- 시스템의 lifetime 동안의 위협의 변화는 초기에 적절했던 컨트롤의 제고 필요
  - 불확실성을 감안할 때, 시스템은 적용 가능하게 설계 되어야 하고, safety 관점에서 필요할 때 보다 빠르게 대처할 수 있는 방향으로 진행되어야 함

1.3 Methodology

- 위험 평가(Risk assessment)는 Safety와 Security 분석의 기본 단계이지만, 이 둘의 위협 기본 모델(Underlying threat model)에는 차이가 있음
  - 시스템의 Safety와 Security에 대한 위협을 평가하기 위한 통합된 방법이 필요
  - Security의 고려 사항은 Safety case에 상당한 영향을 미칠 수 있음
  - Security 위협에 대한 대응, 새로운 취약점 발견, 보호 메커니즘 강도의 감소 등에 대한 영향 분석 필요
  - Safety incident 동안 잠재적인 공격과, 이러한 공격이 악의적 활동을 제고할 수 있는 기회가 될 것이라는 고려 필요

1.4 Standards

- Safety 표준은 이미 “hazard, risk 분석 단계 동안 악의를 가지거나, 권한을 가지지 않는 행동이 고려되어야 한다”라고 요구
  - 표준 프레임워크는 현재 보다 더욱 명확해져야 할 필요성 존재
    - Security-informed safety :
  - 특정 영역 및 일반적 영역의 Safety와 Security 표준과의 관계가 명확해야 하고, 용어적, 개념적 차이의 문제의 해결 필요

2. Profiling of Security Requirements

2.1 Regulatory Security Background

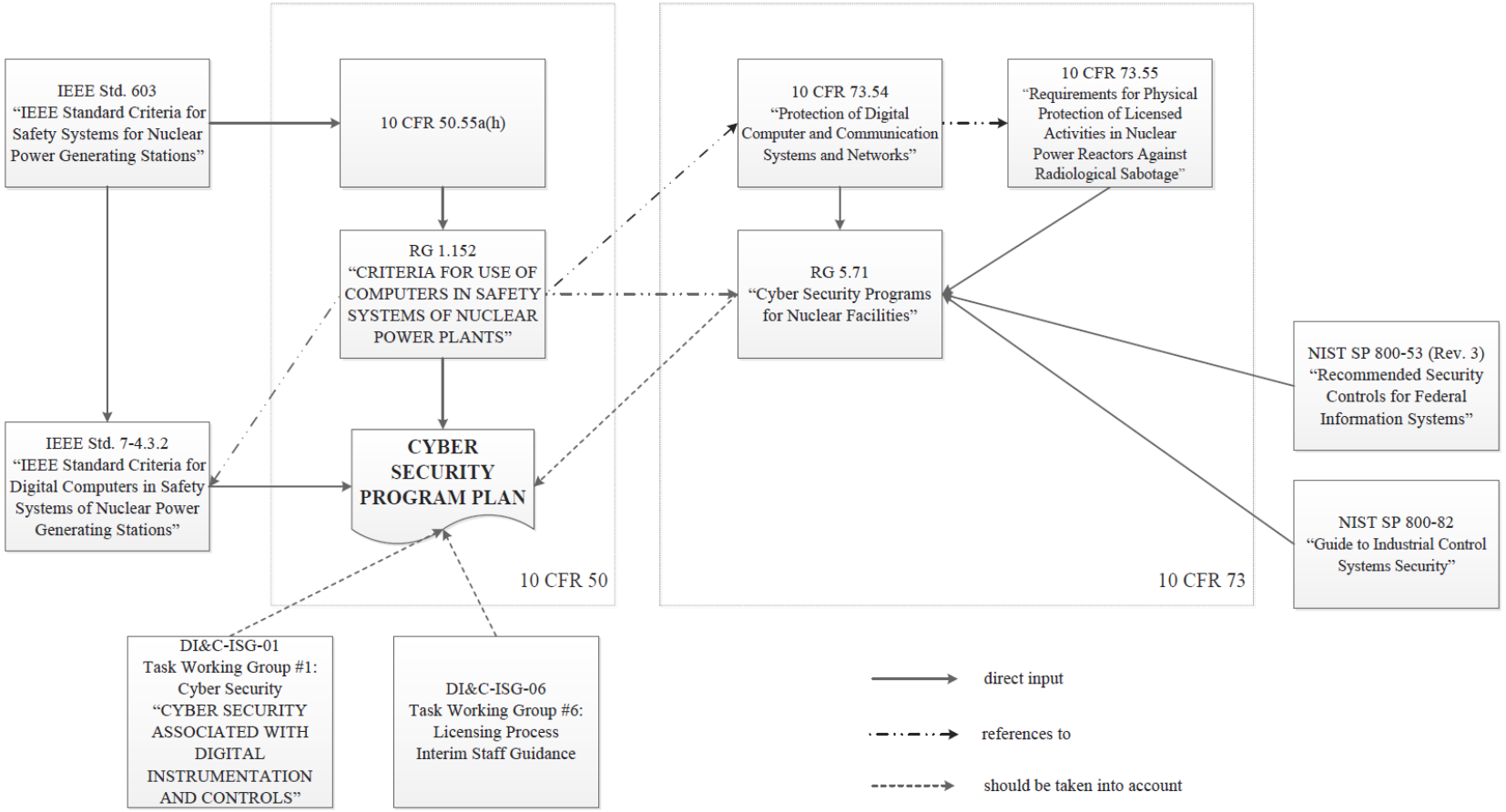
2.2 Security Regulatory Interdependencies

2.1 Regulatory Security Background

- SCI&C의 개발 프로세스의 한계와 요구 사항에 대하여 규정한 원자력 산업관련 safety 규제와 표준이 다수 존재
  - 이러한 규제 및 표준은 Secure한 개발 및 구현 환경과 관련된 요구사항에서부터 시스템 보안 특징에 이르기까지 다양한 양상을 지님
  - SCI&Cs의 라이프사이클 모델에 적절한 Security 활동을 추가하는 것은 여전한 문제

RG 1.152-2011	• Criteria for use of computers in safety systems of nuclear power plants • digital I&C를 위한 secure한 개발 및 구현 환경의 설립에 대한 규제 기준 포함
RG 5.71-2010	• Cyber security programs for nuclear facilities • 10 CFR 73.54 "Protection of digital computer and communication systems and networks"의 실제구현을 위한 지침 • NPP의 유지 및 구현을 위한 security 활동과 방법에 대해 설명 • But, 하지만, SCI&C의 라이프사이클과 관련된 구체적인 프로세스는 제공하지 않는다. 이로 인해, RG 5.71-2010에 적합한 security 통제는 I&C 개발 동안 추가적으로 계획, 설계 필요
IEEE Std. 603-1991	
IEEE Std. 7-4.3.2-2003	

2.2 Security Regulatory Interdependencies (1/2)



<Regulations interdependencies for the security aspect under US NRC requirements>

2.2 Security Regulatory Interdependencies (2/2)

- 10 CFR 60, Appendix B에 대해 security 관점에서의 준수를 위해서, SCI&C를 위한 secure한 개발과 구현 환경 설립 필요
  - 이를 위한 방안 중 하나는 적절한 Cyber Security Program Plan에 의해 규제되는 Cyber Security Program을 설립하고 유지하는 것
  - 개발 단계를 따르는 구체적인 security assurance process들에 대한 설명을 포함하고 있어야 함

Namely the set of activities, including measures and controls taken to establish a secure environment for development of the digital SCI&C against undocumented, unneeded and unwanted modifications, as well as a protective actions taken against a predictable set of undesirable acts that could challenge the integrity, reliability or functionality of a I&C during operations.

- Secure한 개발 및 구현 환경 설립 프로세스는, secure한 개발과 개발 환경 및 I&C의 reliability를 경감시킬 지 모르는, 각 단계에서의 잠재적인 취약성을 식별하고 경감시키는 개발프로세스를 요구

3. Safety-Critical System's Attributes

- I&C가 지닌 다양한 속성들 중 가장 중요한 것은 Dependability
  - Dependability : the ability to deliver required services(perform functions) that can justifiably be trusted
  - Dependability는 Safety와 Security등을 포함한 속성의 set으로 분해 가능
  - I&C의 safety 는 사용자와 Environment에 대한 비극적 결과의 부재를 보장
- 국제 문서들은 Cyber security가 다음을 보장하는 보호 매커니즘이라 정의

Confidentiality	the property that information is not made available or disclosed to unauthorized individuals, entities or processes
Integrity	Protection of the accuracy and completeness of the information and methods or processing
Authenticity	the confidence that the information comes from the correct source and/or the system trust the source code
Availability	Access to information and associated assets of authorized users as needed
Reliability	Entities involved in the processing, or communication, should not be able to refuse to exchange data

4. Safety and Security Interrelation

4.1 The principle of unity of safety and security assessment

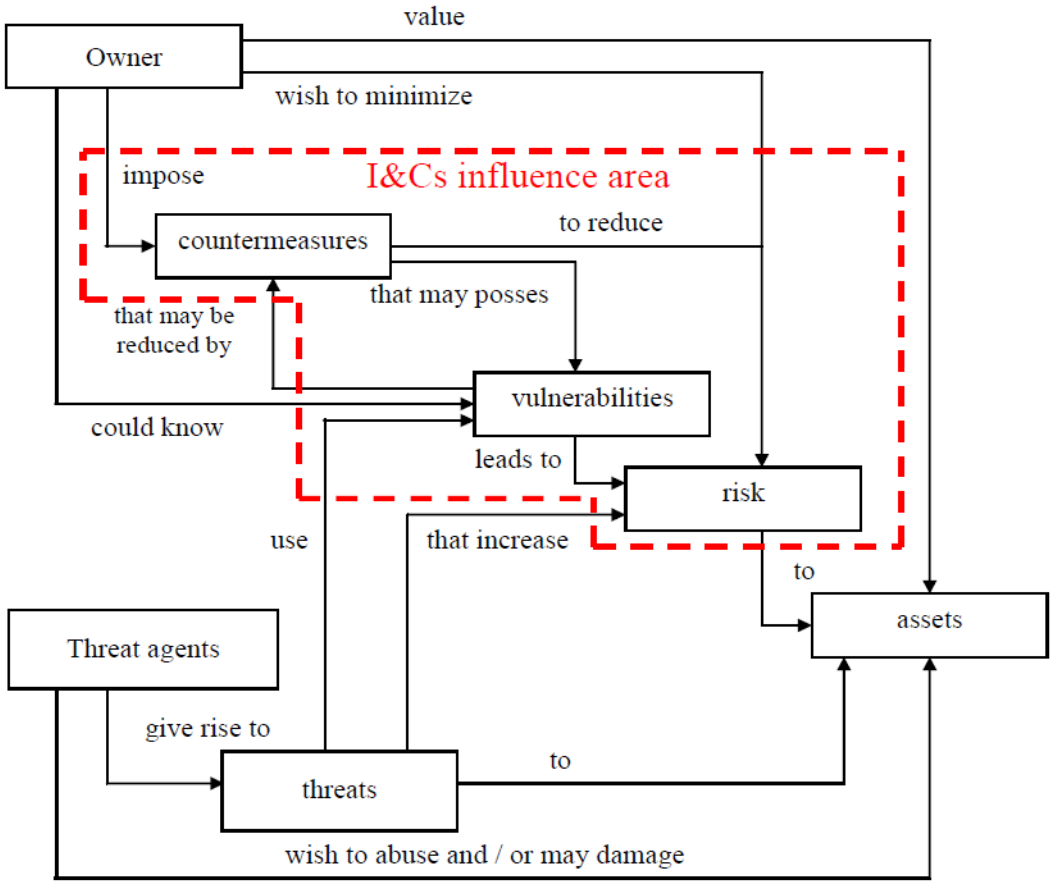
4.2 Safety and Security lifecycle model of FPGA-based I&Cs

4.1 The principle of unity of safety and security assessment (1/3)

- 지금까지는 복잡한 I&C에 대해서 Safety와 Security에 대한 통합적인 접근 방법이 존재 하지 않음
  - Safety와 Security 영역의 전반적인 방법론적 장치는 I&C로 하여금 Safety를 평가하고 보장할 수 있게 만들어 줄 것
  - 이러한 장치는 기존의 접근 방식 및 전문가의 기반으로 구축되어야 함

- ISO/IEC 15480에 따르면, Security는 위협으로부터 자산을 방어하는 것과 관련
  - 악의적이든, 그렇지 않든 사람의 행동과 관련하여 모든 종류의 위협은 고려되어야 함

4.1 The principle of unity of safety and security assessment (2/3)

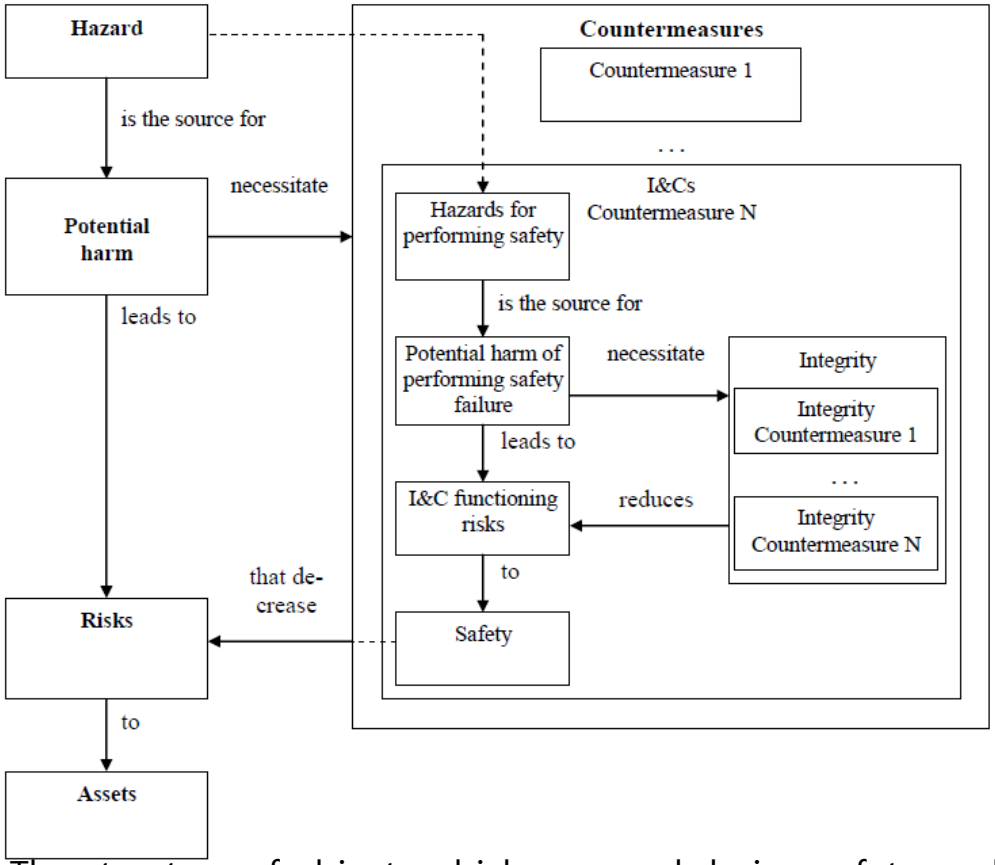


countermeasures	because some I&Cs could be one of the such countermeasures, e.g. I&Cs important to safety
vulnerabilities	because from the one side I&Cs aimed at vulnerabilities elimination and from the other they could have vulnerabilities itself
risks	from the one side I&Cs, as countermeasures itself, aimed to decreasing the risks, and from another they could produce additional risks to the system

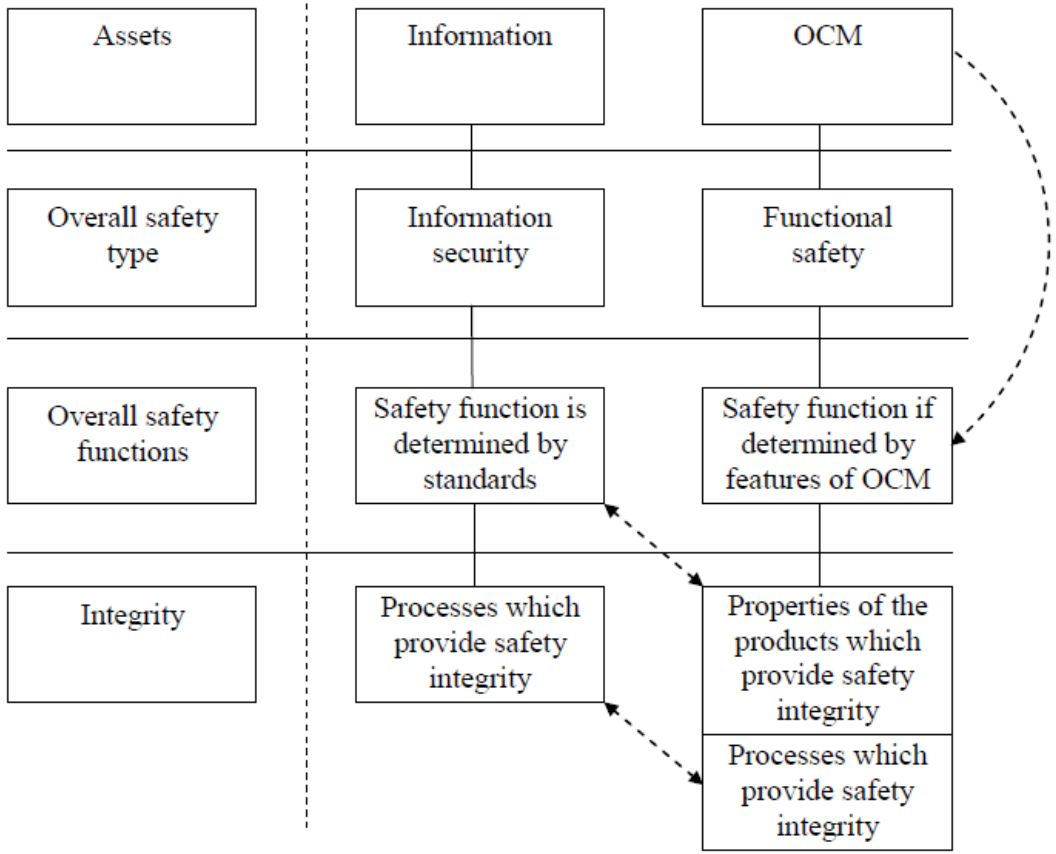
<Security concepts and relationships according to ISO/IEC 15480 series>

4.1 The principle of unity of safety and security assessment (3/3)

- Security 분석과 Safety 분석의 차이점은 수행되는 자산에 기초



<The structure of objects which are used during safety analysis: integration of level of assets and I&Cs>

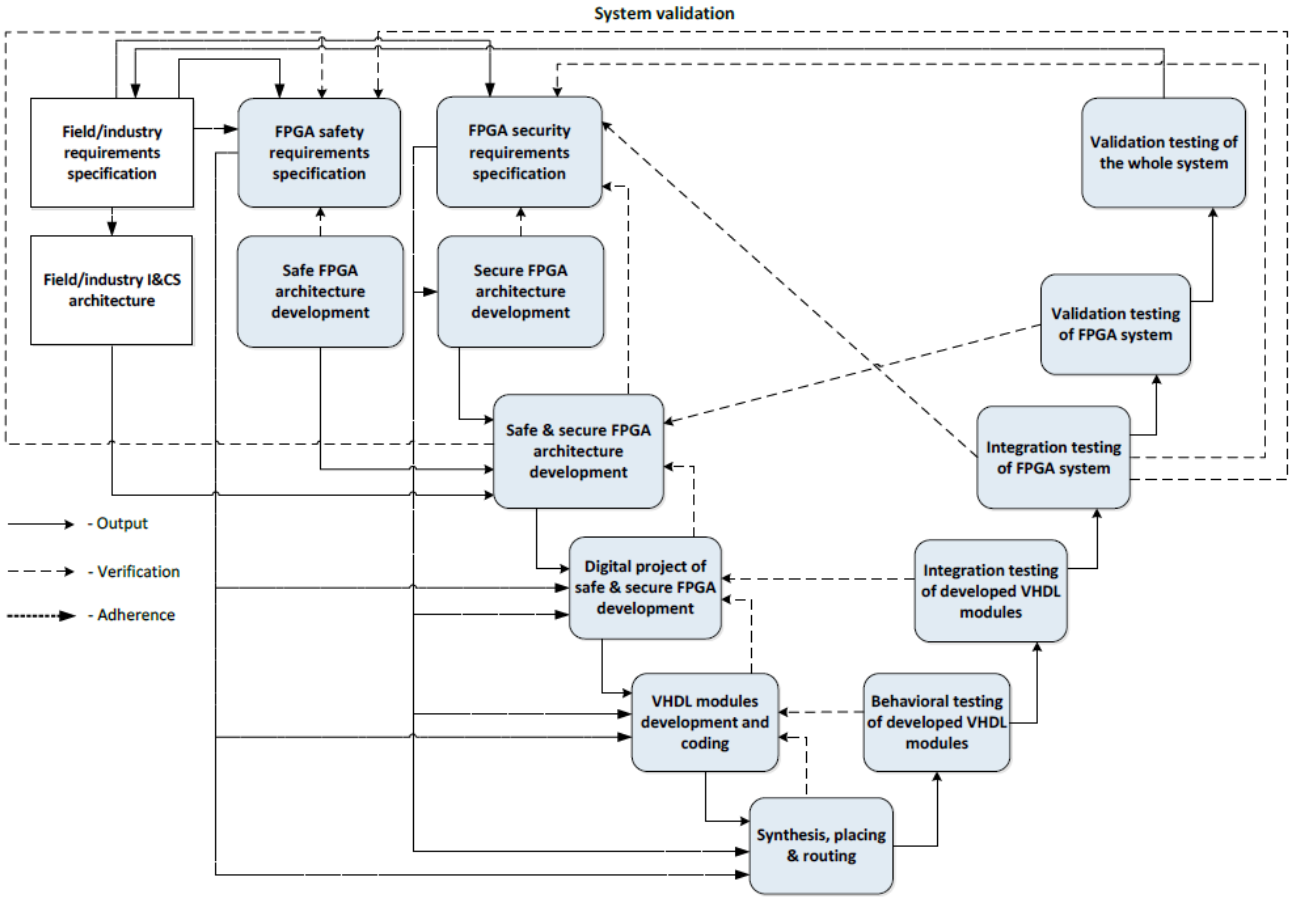


<Safety and security cross influence>

4.2 Safety and Security lifecycle model of FPGA-based I&Cs (1/2)

- Safety-critical한 FPGA 기반 I&Cs의 Security를 평가하기 위하여 다음이 필요
  - 환경 및 개발 도구에 대한 제어를 포함한 개발 프로세스를 보고하기 위한 전략
  - lifecycle에 대한 구체화
    - lifecycle 모델 : 시스템의 개발 및 동장에 대한 위상을 포함하는 구조적, 체계적인 모델
    - Input 단계들에 대한 성공적인 구현이 되어야 개발 lifecycle의 각 단계의 output을 검증 하는 것이 가능
- 시스템의 Safety와 Security 요구사항과 각각의 아키텍처를 제공하기 위한 비용과 균형을 맞추는 것이 중요
  - Safety, Security 요구사항에 대한 명세에 숨어 있는 약점은 Safety와 Security 요구사항이 모순되는 상황을 피하고, 이러한 상황이 발생해도 사고 제도에 대한 시스템을 평가할 수 있는 방향으로 개발되고 있다.

4.2 Safety and Security lifecycle model of FPGA-based I&Cs (2/2)



<Safety and security lifecycle model of FPGA-based I&Cs>

- 두 직사각형은 직접 연관되어 있진 않지만 시스템 개발 동안 규제측면에서 역할을 수행
- 모서리가 둥근 직사각형은 개발 라이프사이클 단계와 직접적으로 관련된 활동을 묘사
- 각기 다른 화살표가 라이프 사이클 활동에서의 다른 종류 관계를 나타냄
  - Safety와 Security 준수 사항의 경우 점선으로 표시

5. Security Assessment Technique

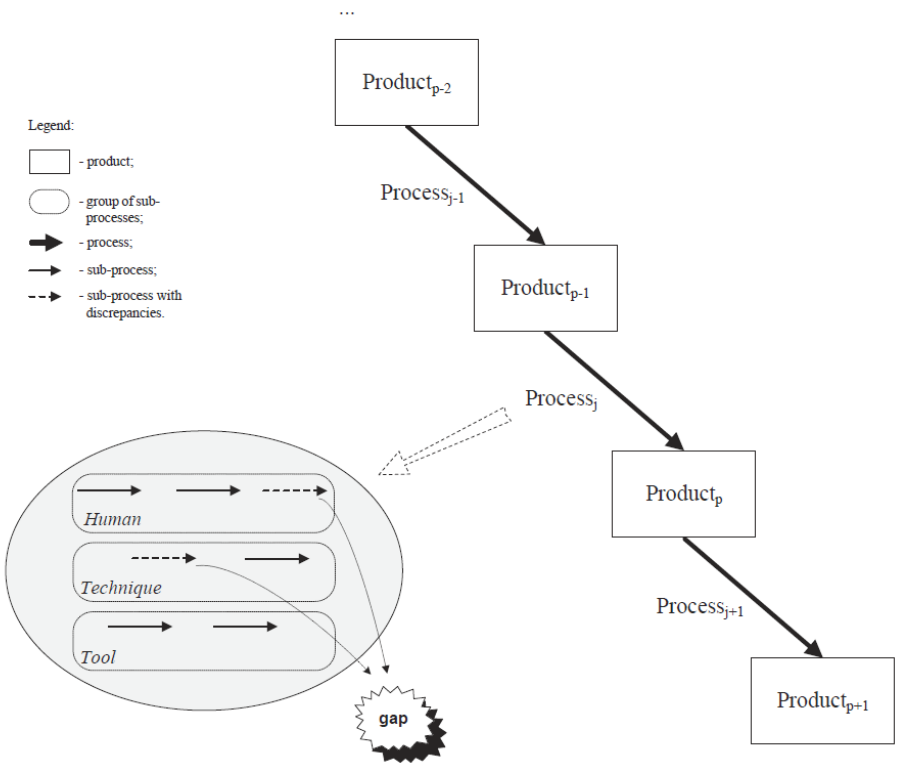
5.1 GAP-analysis technique

5.2 IMECA-analysis technique

5.3 Security informed safety approach

5.1 GAP-analysis technique

- I&C 시스템 lifecycle의 모든 프로세스 마다 discrepancy에 대해 결정, 이를 통해 이상을 발견하거나, 이상을 제거할 수 없다는 것을 결정하는 GAP 개념을 사용할 수 있음



<GAP-analysis technique>

5.2 IMECA-analysis technique

- Security 적용하기 위하여 FMECA를 실제로 개선 한 것
- 식별된 GAP들은 단일 로컬 IMECA 표로 표현되며, GAP 내의 각각의 discrepancy는 하나의 행들로 표현
- 각 GAP에 대한 GAP 분석에 의해 식별된 취약성들을 포함한 별도의 표를 생성하며, 모든 테이블은 general IMECA 테이블로 결합

% IMECA : Intrusion Modes and Effect Criticality Analysis
% FMECA : Failure Modes, Effects and Criticality Analysis

5.3 Security informed safety approach

- 구조화된 Safety에 기초하여, “The impact that Security might have on and existing safety case”를 전제로 수행되는 접근법
- FPGA 기반 I&C의 Safety와 Security에 관한 평가 및 보장의 문제
  - consideration of possible vulnerabilities that may occur in the components due to any anomalies in the earlier phases of the life cycle
  - development of the product security threat models
  - ranging of identified vulnerabilities in accordance with their criticality and severity
  - determination of both sufficient and cost-effective countermeasures either to eliminate identified (or even possible) attacks, vulnerabilities and threats or make them difficult (or even impossible) to exploit by an attacker

6. Case Study

6.1 Regulatory Requirements

6.2 V-Model of FPGA-Based SCI&C

6.3 Features of Assessment

6.4 Criticality Matrix

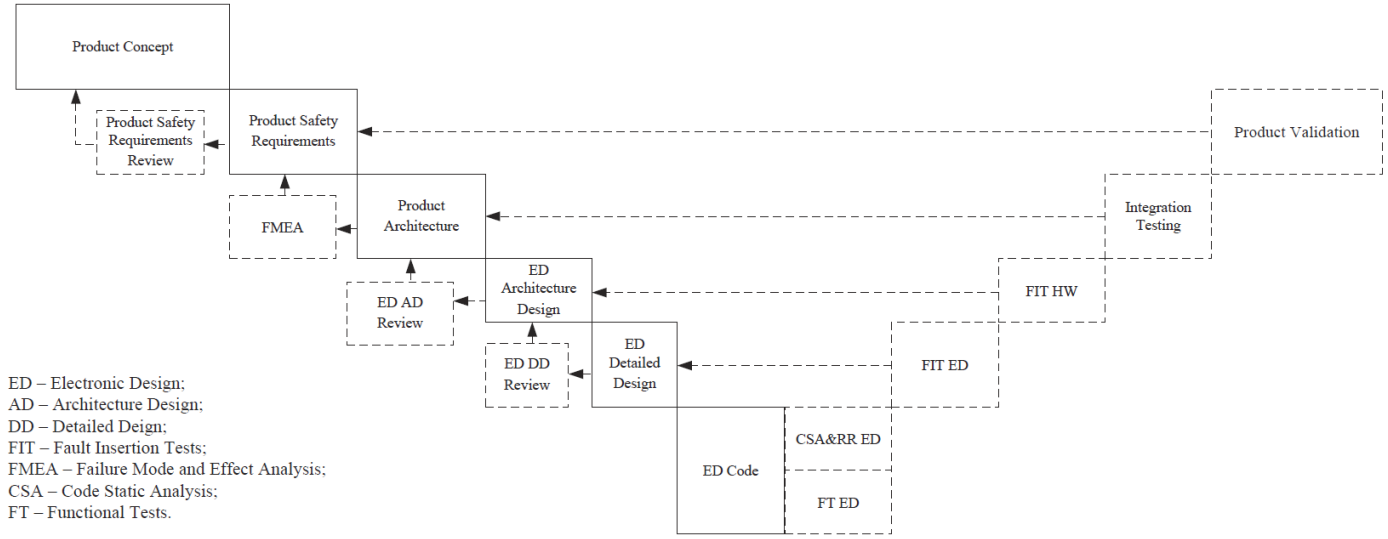
6.1 Regulatory Requirements

- RG 1.152-2011의 I&C의 secure한 개발 및 구현환경 설립
  - Measures and controls taken to establish a secure environment for development of the I&C against undocumented, unneeded and unwanted modifications
  - Protective actions taken against a predictable set of undesirable acts (e.g. inadvertent operator actions or the undesirable behavior of connected systems) that could challenge the integrity, reliability, or functionality of a SCI&C during operations

- 시스템에 대한 의도치 않은 접근을 불가능하게 하고, 시스템 동작 동한 적절하지 못한 행동으로부터 보호할 수 있는 보호 디자인의 적용을 포함

6.2 V-Model of FPGA-Based SCI&C

- SCI&C의 개발 lifecycle의 V-Model 고려는 FPGA 기반 I&C에서 필수 요소
- 좌측에 하강하는 부분은 개발 활동과 상응하며, 우측에 상승하는 부분은 Verification 활동과 상응



<Development Lifecycles for FPGA-based SCI&C>

6.3 Features of Assessment (1/2)

- 보안 측면은 concept부터 system retirement에 이르기까지 SCI&C의 모든 lifecycle 각각에서 고려되어야 함

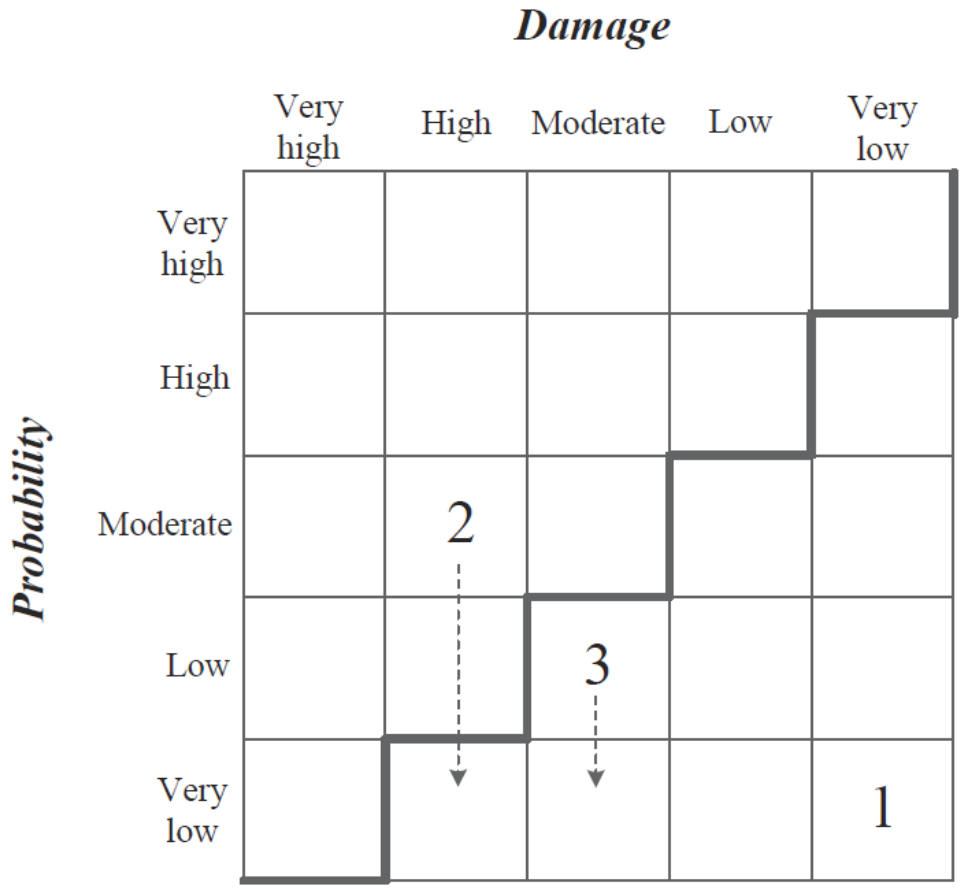
TABLE I. RESULTS OF IMECA FOR FPGA ATTACKS

Row No.	Attack mode	Attack nature	Attack cause	Occurrence probability	Effect severity	Type of effects	Countermeasures
1	Black Box Attack	Active	Simple logic of electronic design	Very low	Very low	Reverse engineering of logic by adversary	Complication of electronic design logic
2	Readback Attack	Active	Absence of chip security bit and/or availability of physical access to chip interface (for example, JTAG)	Moderate	High	Obtaining of secret information by adversary	The use of security bit Application of physical security controls
3	Physical Attack	Active	Absence of monitoring of physical parameters (voltage, temperature, clock frequency) of environment and chip	Low	Moderate	Obtaining of information concerning patented algorithms by adversary	Decreasing memory retention effect Monitoring of physical parameters (voltage, temperature, clock frequency) of environment and chip

6.3 Features of Assessment (2/2)

- 성공적인 Cyber 공격 위험을 감소시키기 위해 다음의 세가지 절차가 수행
  - Creation of criticality matrix based on results of proposed approach
  - Selection of a set of applicable appropriate countermeasures based on recommendations of the specific regulations
  - Choice of a subset of specific countermeasures in order to decrease risks of intrusion into FPGA-based SCI&C to acceptable value and to minimize costs for their purchase, implementation and maintenance

6.4 Criticality Matrix



<Criticality Matrix>

- matrix내의 숫자들은 IMECA 표의 적절한 row number를 나타냄
  - Cyber security assurance 관점에서, related damage는 상수이기 때문에, risk를 감소시키기 위해선 공격 발생확률을 줄여야 함
  - Numbered row의 확률 감소 케이스는 화살표가 달린 점선으로 표시
  - By, implementation of certain process countermeasures during implementation of development processes or specific countermeasures during operation and maintenance stage on the basis of results of proposed approach application

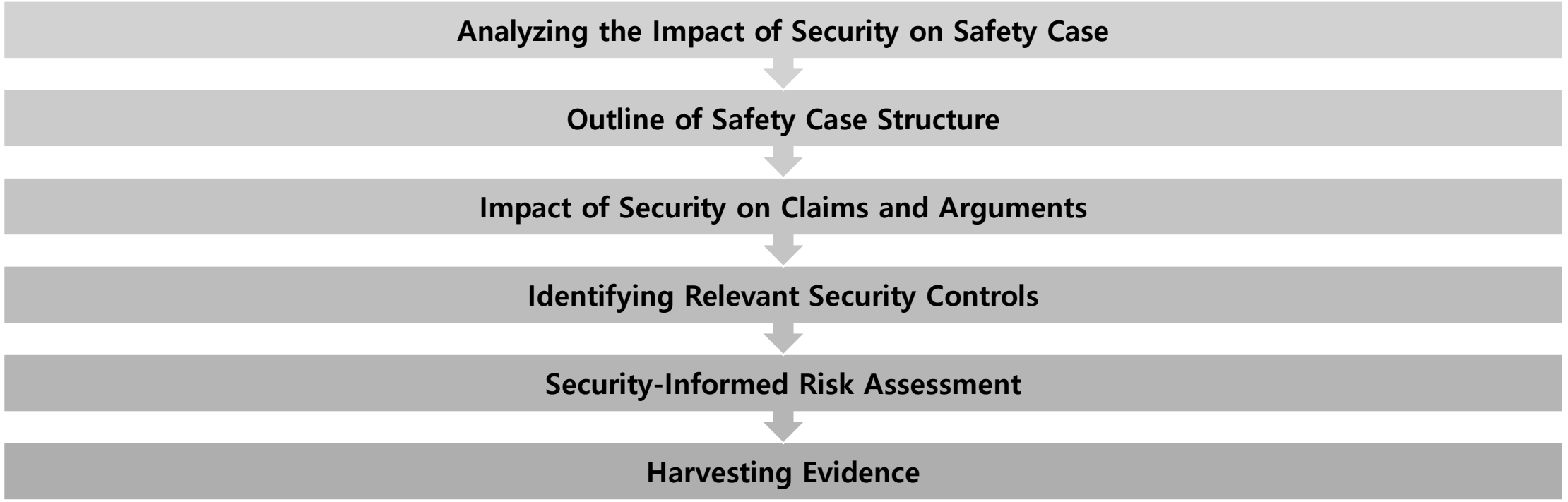
7. Conclusion

- Safety critical I&C 시스템은 서로 다른 기능을 가진 서로 다른 기술 기반의 구성요소들의 상호작용으로 구성되어있기에, 이에 대한 security 분석 및 평가는 어려우며, 다양한 I&C 속성들의 interference와 사용된 모든 기술의 특징을 포함한 모든 구체적인 세부 사항에 대한 고려가 필요

- 제시한 접근 방식들은 gap 개념과 IMECA 기술, 사람, 적용 기술 및 도구와 연관된 개발 프로세스에 대한 분석에 에 기반하여 제시
  - 잠재적으로 이상을 초래할 수 있을지 모르는 모든 프로세스의 discrepancies에 대해 보여주는 process-product 모델을 고려하였기 때문에, I&C의 다양한 측면의 평가에 적용할 수 있을 것으로 보여짐
  - 이를 위한 보다 상세한 요구사항과 gap에 대한 분석 및 countermeasure들에 대한 연구가 필요할 것으로 보여짐

Cf. Related Works

- risk assessment와 safe와 secure 모두를 추구하는 실제 시스템에서의 security-informed safety justification을 바탕으로 methodology를 개발하고, 이러한 methodology를 구현한 도구를 개발 중인 연구



References

- [1] Christian Raspotnig, Andres Opdahl. "Compareing risk identification techniques for safety and security requirements". Jan 2013
- [2] Algirdas Avizienis, Jean-Claude Laprie, Brian Randell, Carl Landwehr. "Basic Concepts and Taxonomy of Dependable and Secure Computing". Jan 2004.
- [3] Vyacheslav Kharchenko, Oleg Illiashenko, Eugene Brezhnev, Artem Boyarchuk, Vladimir Golovanevskiy. "Security Informed Safety Assessment of Industrial FPGA-Based Systems". Jun 2014
- [4] Robin Bloomfield, Robert Stroud. "Security-Informed Safety "If it's not secure, it's not safe"". Jan 2014.
- [5] Robin Bloomfield, Kateryna Netkachova, Robert Stroud. "Security-Informed Safety : If It's Not Secure, It's Not Safe". Oct 2013.
- [6] Robin Bloomfield, Jay Lala. "Safety-Critical Systems: The Next Generation". Aug 2013
- [7] V. Kharchenko, A. Kovalenko, O. Siora, V. Sklyer. "Security Assessment of FPGA-based Safety-Critical Systems: US NRC Requirements Context". Jul 2015

KU 건국대학교 KONKUK UNIV.

Q & A

THANK YOU