Safety & Security

IT 융합 정보보호학과
김 그 린

greenkim@konkuk.ac.kr

2015. 10. 30

Table of Contents

1. Introduction 2

1.1 Concepts 3

1.2 Principles 4

1.3 Methodology 4

1.4 Standards 5

2. Profiling of Security Requirements 5

2.1 Regulatory Security Background 5

2.2 Security Regulatory Interdependencies 6

3. Safety-Critical System's Attributes 7

4. Safety and Security Interrelation 8

4.1 The Principle of unity of safety and security assessment 8

4.2 Safety and Security lifecycle model of FPGA-based I&Cs 10

5. Security Assessment Technique 11

5.1 GAP-analysis technique 11

5.2 IMECA(Intrusion Modes and Effect Criticality Analysis)-analysis technique 11

5.3 Security informed safety approach 12

6. Case Study 12

6.1 Regulatory Requirements 12

6.2 V-Model of FPGA-Based SCI&C 13

6.3 Features of Assessment 13

6.4 Criticality Matrix 14

7. Conclusion 15

1. Introduction

Program Logic Device들과 FPGA(Field Programmable Gate Arrays)는 특히 safety-critical I&Cs(Instrumentation and control systems)의 개발과 구현에 널리 사용된다. NPP(Nuclear Power Plant) I&C와 같은 중요한 영역에서의 응용프로그램들에 의하여 확인 된 바, FPGA 기반 시스템이 마이크로프로세서(소프트웨어 등)기반 시스템에 비해 상대적으로 장점이 있다는 것에는 반박할 여지가 없다. 하지만, I&Cs에서의 FPGA 사용은 safety를 확보하는 측면에서 특정 위험을 초래한다. FPGA를 사용한 I&C 프로젝트는 소프트웨어와 하드웨어 구성요소를 모두 포함하는 복잡한 솔루션이라고 할 수 있다. FPGA 기반 I&C의 safety에 대한 전반적이고 정확한 평가는 security 특성을 고려하지 않고는 불가능하다.

Safety-critical 시스템은 NPP를 위한 I&C를 포함하여, 다양한 형태로 다양한 분야의 산업에 널리 사용된다. 위에서 말한 바와 같이 I&C 시스템은, 종종 safety-critical한, 주어진 역할을 수행하기 위해 끊임없이 서로 상호작용하는 소프트웨어와 하드웨어로 구성된 복잡한 시스템이라고 할 수 있다. 특정 기술 관점에서 FPGA 기술은 SCI&C(Safety-critical Instrumentation and control systems)를 구현하기 위한 하나의 트렌드로 자리잡고 있으며, 결과적으로 이러한 시스템을 설계하고 구현하고 유지하는 측면에 있어 새로운 문제를 야기하고 있다. 특히, NPP I&Cs와 FPGA 기반 I&Cs 와 관련된 주요 문제 중 하나는 security 보장을 요구하는 것과 표준에 따른 개발 및 구현된 시스템이 요구사항에 맞는지 증명하는 데에 있다.

safety 영역에서, 시스템으로부터의 이점과 시스템의 기능은 발생가능성을 내포한 사고적 결함(harm)과 균형을 이루어야 한다. 반면 security 영역은 가능한 악의적 결함(harm)으로부터 이를 생각해보아야 한다. 이 두 가지 영역을 구분하는데 쓰이는 전형적인 방법은 다음과 같다.

- "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" (Piertre-Camnbacedes and Chaudet. 2010)

두 가지 영역에 공통되는 것은 harm의 잠재로부터 생긴 risk라고 할 수 있으며, 이는 가능성(probability)과 심각성(severity)으로 설명될 수 있다. 시스템 개발 및 구현에 걸쳐서 risk를 식별하고, 분석하고, 평가하고 가능한 한 많은 관련(relevant) risk를 다루는 것은 중요하다. 더불어, safety는 특별히 의도치 않은 hazards에 대해 다루고, security는 의도된 threats에 대해 다룬다고 이야기된다. (또한, security는 악의적 risk를 야기하는 의도적인

공격을 다루고, safety는 사고적(accidental) risk를 야기하는 의도치 않은 행동이나 실패(behavior or failures)에 대해 다룬다고도 이야기할 수 있다.) 의도된, 의도치 않은 측면에 대하여 다루는 것에는 많은 차이점이 있지만, 이를 위해 hazards와 threats를 식별하는 기술은 같은 principle을 기반으로 두고 있다고 말할 수 있다. Safety 관점에서 부합하는(corresponding) hazards에 대한 식별을 위해 environment에서 harm은 식별되어야 하며, security 관점에선 corresponding hazards가 식별되는 것이 중요하다.

과거, safety와 security는 별도의 지침을 따랐다. 하지만 이러한 양상엔 변화가 생겼으며, stakeholder들은 "If it's not secure, It's not safe"라고 주장하기 시작하였다. safety와 security를 결합하는 것은 새로운 개념은 아니지만, 간단한 개념이라고 볼 수는 없다. 위에서 말한 바와 같이, 시스템이 safe하기 위해선, 반드시 secure해야한다. 이 말이 성립하지 않으면, 사람에게 해를 끼치거나 피해를 입힐 수 있다고 간주되는 safety critical system은 공격자로 하여금, 광범위한 피해와 극심한 공포를 초래할 것이며, 이러한 시스템은 악의적 공격의 타겟이 될 것이다. 원칙적으로, safety와 security를 통합하는 것은 간단해야 한다. safety와 security 모두 good process, 위험 분석의 중요성, 검증의 필요성과 정당성을 강조하는 정교한 엔지니어링 문화를 가지고 있다. 하지만 이러한 유사점은 피상적이며, 대규모 시스템 구축 경험에서 알 수 있듯 실제로 구현할 시에는 상당한 어려움을 지니고 있다.

1.1 Concepts

Safety와 security 사이의 공통점은 다른 개념과 용어들을 사용하여 불분명하게 이야기된다. 실제로, safety와 security 커뮤니티 내부와, 커뮤니티 간의 용어에는 상당한 차이가 있다. 따라서 각각의 도메인의 주요 개념에 대하여 이해를 공유하기 위해서, 공용어와 일반적인 ontology(언어로 표현된 개념 간 연간 관계 지식이 드러나는 망)을 설립할 필요가 있다.

Basic Concepts and Taxonomy of Dependable and Secure Computing에 따른, safety와 security의 정의는 다음과 같다.

- 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"

넓은 의미에서 safety는 시스템으로부터 환경을 보호하는 것에 대해 다루는 반면, security는 환경으로부터 시스템을 보호하는 것에 대해 이야기한다. Safety와 security는 dependability의 종류 중 하나로 볼 수 있으며, 전체 시스템에 미치는 영향을 파악하고, 잠재적 failure를 식별하기 위해서 유사한 기술을 사용한다. 이로 인해, safety와 security의 초점일 다르고, 요구 사항이 충돌하는 경우가 생길 수도 있지만, safety와 security 방법 간에는 상당한 공통 부분이 존재하게 된다. 특히, safety와 security사이의 가장 큰 차이점 중 하나는 secure 시스템은 운영 부분, 디자인 및 구조적 방법을 통하여 진화하는 위협과 환경 변화에 대해 대응할 수 있어야 한다. 이러한 변화에도 불구하고, system이 safe하고 secure할 수 있기 위해선 변화에 resilient해야한다.

1.2 Principles

safety와 security의 원칙은 중첩되는 부분이 많지만, 중요성(emphasis)과 잠재적 충돌 측면에서는 상당한 차이점을 지니고 있다. 예를 들어, 독립적인 다수의 barrier에 의존하는 defense in depth는 safety와 security 모두에 걸쳐 중요한 architecture principle이지만, safety 관련 고려 사항은 safety barrier의 독립성과 효율성에 대해 다룰 가능성이 높다. Safety 시스템 관점에서 economy of mechanism, 최소 권한 및 심리적 수용과 같은 security principle은 쉽게 허용될 것이다. Complete mediation과 end-to-end arguments와 같은 다른 principle들은 시스템의 퍼포먼스와 구조에 상당한 영향을 미칠 수 있다. 특히, safety 시스템이 calibration 및 유지 보수를 위한 작동 변화를 지원하기 위해 설계되어 있더라도, 시스템의 security는 쉽게 변경할 수 없는 것에 의존하지 않아야 한다고 주장하는 복구 principle의 용이성은 safety 시스템의 구조에까지 영향을 미칠 수 있다. 또한, 시스템의 lifetime 동안의 위협의 변화는 초기에 적절하다고 생각된 컨트롤에 대한 제고가 필요함을 의미한다. 이 것은 20~40년 정도의 수명을 가진 embedded safety system의 lifecycle과 구조에 대해 의미를 지닌다. 미래의 위협의 불확실성을 감안할 때, 시스템은 적용 가능하게 설계되어야 하며, safety 관점에서 필요할 때보다 빠르게 대체 되어야 한다. 이는 특히, 이미 진행 중인 대형 인프라 프로젝트에 대하여 구조적이고 비용적 측면에서 상당한 의미를 지닌다.

1.3 Methodology

위험 평가는 safety와 security 분석의 기본적인 단계이지만, 위협 기본 모델은 다르다.

시스템의 safety와 security에 대한 위협을 평가하기 위한 통합된 방법이 필요하다. Security 고려 사항은 safety case에 상당한 영향을 미칠 수 있다. 예를 들어 security 위협에 대한 대응, 새로운 취약점 발견, 보호 매커니즘 강도의 감소 등에 대한 영향 분석이 필요할 수 있다. 이러한 것들은 설계의 resilience를 특별히 강조한다. 또한, safety incident 동안의 잠재적인 공격과, 이러한 공격이 악의적 활동을 제공할 수 있는 기회가 될 것이라는 것을 고려할 필요가 있다. 만약 시스템이 공격을 받고 있거나, 컨트롤 시스템에 대한 어떤 security 공격이라도 일반적으로 타당하지 않은 fail-safe state에 도달할 수 있다는 가정이 있다면 fail-safe state는 생각되었던 것보다 안전하지 않을 수 있다. 더불어, society의 상태와 능력에 대한 가정은 바뀔 수 있다. (예를 들어, 주요 security 사건 도중 safety incident를 관리하는 것처럼).

1.4 Standards

Safety 표준은 이미 "hazard, risk 분석 단계 동안 악이 있거나 권한을 가지지 않는 행동이 고려되어야 한다"는 것을 요구하고 있다. 하지만 security informed safety에 대한 표준 프레임워크는 현재의 경우보다 명확해져야 할 필요가 있다. 특히, 특정 영역과 일반적인 safety와 security 표준과의 관계가 명확해야 하고, 용어적 개념적 차이가 해결되어야 한다.

2. Profiling of Security Requirements

2.1 Regulatory Security Background

SCI&C의 개발 프로세스의 한계와 요구사항에 대하여 규정한 원자력 산업관련 safety 규제와 표준이 다수 존재한다. 이러한 규제 및 표준은 secure한 개발 및 구현 환경과 관련된 요구사항에서부터 시스템의 보안 특징에 이르기까지 다양한 양상을 띄고 있으며, SCI&Cs의 라이프사이클 모델에 적절한 security활동을 추가하는 것은 여전히 문제로 남아 있으며, 규제 및 표준들은 다음과 같다.

- RG(Regulatory Guide) 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 기준을 포함하고 있다.
- RG 5.71-2010 "Cyber security programs for nuclear facilities" : 10 CFR 73.54

"Protection of digital computer and communication systems and networks"의 실제 구현을 위한 지침으로 NPP의 유지 및 구현을 위한 security 활동과 방법에 대해 설명한다. 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 구현되어야 한다.

- IEEE Std. 603-1991
- IEEE Std. 7-4.3.2-2003

2.2 Security Regulatory Interdependencies

Fig. 1은 US NRC(Nuclear Regulatory Commission) 산하의 보안 양상 관련 규제 간 상호 의존의 개발 다이어그램(developed diagram of regulations interdependencies for the security aspect)을 보여준다.

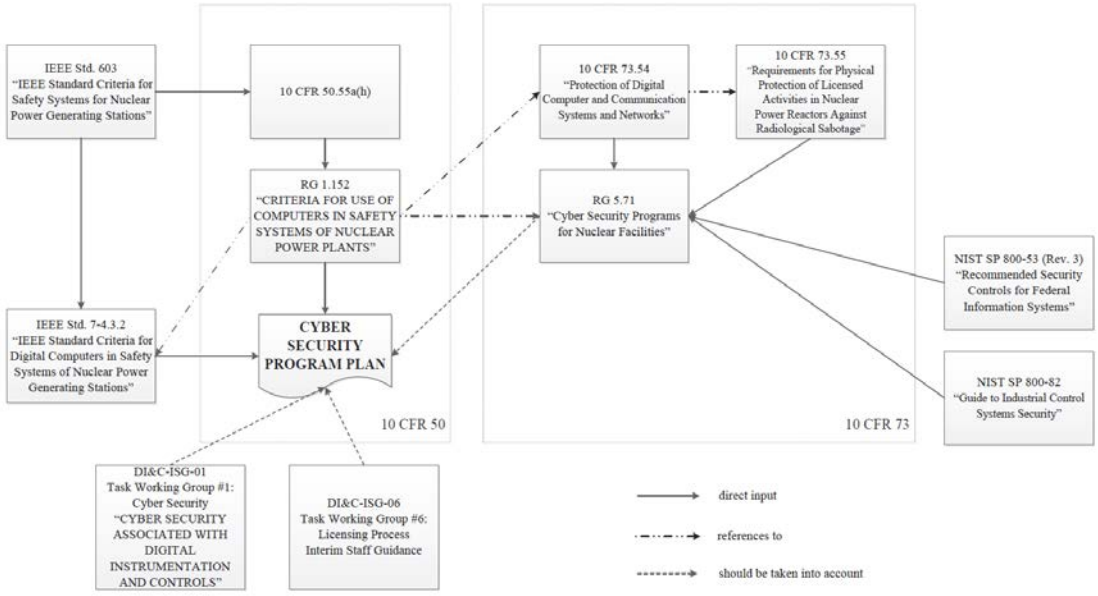

Fig.1. Regulations interdependencies for the security aspect under US NRC requirements

10 CFR 60, Appendix B에 대해 security 관점에서의 준수를 위해서, SCI&C를 위한 secure 한 개발과 구현 환경이 설립되어야 한다. 이를 위한 방안 중 하나는 적절한 Cyber Security Program Plan에 의해 규제되는 Cyber Security Program을 설립하고 유지하는 것이다.

이러한 문서들은 SCI&C를 위한, 개발 단계를 따르는 구체적인 security assurance

process들에 대한 설명을 포함하고 있어야 한다: 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 필요로 한다. 이를 위한 취약성 평가 프로세스는 다른 방법으로 수행될 수 있다.

3. Safety-Critical System's Attributes

I&C가 지닌 다양한 속성들 중 가장 중요한 것은 dependability(the ability to deliver required services(perform functions) that can justifiably be trusted)라고 할 수 있다. Dependability는 safety 와 security를 포함한 first-order 속성의 set으로 분해(decompose) 될 수 있는 복잡한 속성이다. I&C의 safety는 사용자와 environment에 대한 비극적인 결과의 부재를 보장한다. 국제적으로 저명한 문서들의 관점에서 Cyber security는 다음을 보장하는 보호 매커니즘으로 정의된다.

- 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

현재 복잡한 I&C에 대하여 safety와 security에 대한 통합된 접근 방법은 존재하지 않는다. Safety와 security 영역의 전반적인 방법론적 장치는 I&C로 하여금 safety를 평가하고 보장할 수 있게 만들어 줄 것으로 보여진다. 이러한 장치는 기존의 접근 방식 및 전문가의 경험(safety와 security의 분리된 분석)을 기반으로 해야 할 것이다. 하지만, safety와 security 모두에 있어 general하고 private 한 특징에 대한 할당이 우선적으로 고려되어야 할 것이다. ISO/IEC 15408에 따르면. Security는 위협으로부터 자산을 방어하는 것과 관련이 있다. (위협은 잠재적으로 안전하게 할 수 있는 자산의 남용에 기초하여 분류된다.). 모든 종류의 위협은 고려되어야 한다. (특히, 악의적이든 아니든 사람의 행동과 관련하여서). 다음의 Fig. 1.은 ISO/IEC 15408에서 제시하는, high-level의 security 개념과 그들의 관계에 대하여 보여준다. I&C에 영향을 줄 수 있는 영역은 빨간색 점으로 표시되어 있다.

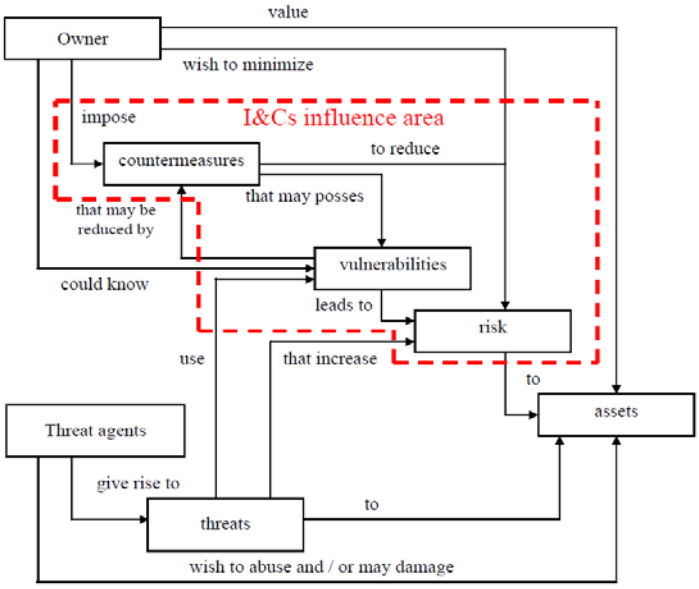

Fig. 2. Security concepts and relationships according to ISO/IEC 15480 series

이 영역은 I&C의 security의 보안에 대해 평가하고 보장할 수 있는 프레임에 대해 구체화되어 있으며, 다음의 요소를 포함하고 있다.

- countermeasures for risk reduction : 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 분석과 safety분석의 차이점은 분석이 수행되는 자산에 기초한다. safety 분석은 중요한 OCM(objects of control and management)에 기초하고, security 분석은 information 자산에 기초한다. 이 상호 관계에 대한 적절한 표현은 Fig. 2. 를 통해 확인할 수 있다. I&Cs의 자산 및 safety 기능에 따라 safety를 security로, safety를 security로 바꾸는 "흐름"이 수행된다. information 자산을 위하여 security가 고려되며, 이 경우 safety는 safety 무결성 보장을 목표로 한다.

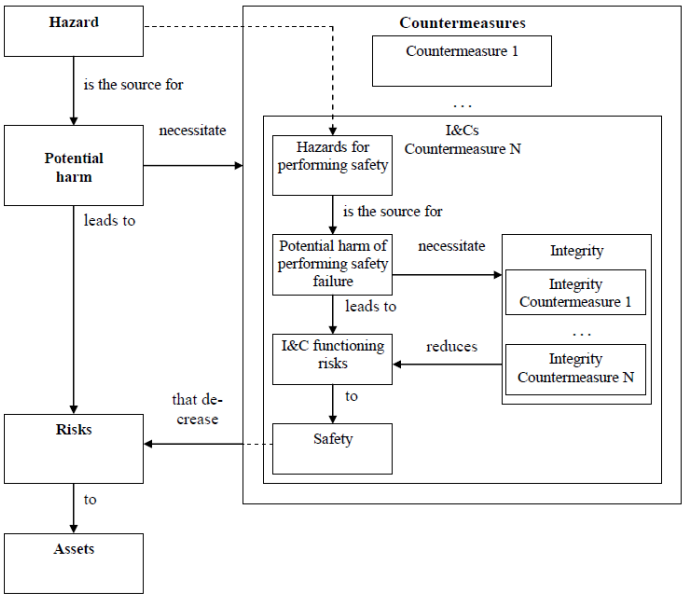

Fig. 3. The structure of objects which are used during safety analysis : integration of level of assets and I&Cs

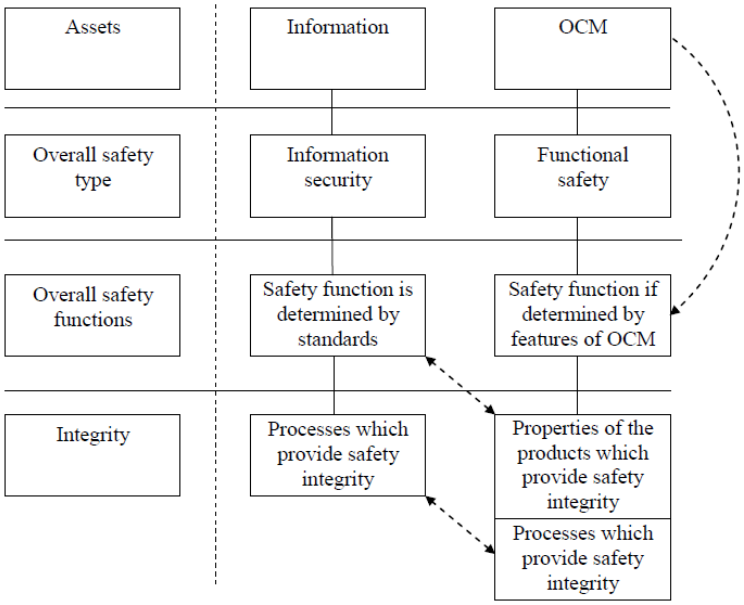

Fig. 4. Safety and security cross influence

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

Safety-critical한 FPGA 기반 I&Cs의 security를 평가하기 위하여, 환경 및 개발 도구에 대한 제어를 포함한 개발 프로세스를 보고하기 위한 전략과 lifecycle에 대한 구체화가 필요하다. 여기서 lifecycle 모델이란 시스템의 개발 및 동작에 대한 위상을 포함하는 구조적이고 체계적이 모델이다. 이상적으로, input 단계들에 대하여 성공적으로 구현되어야 개발 lifecycle의 각 단계의 output을 검증하는 것이 가능하다.

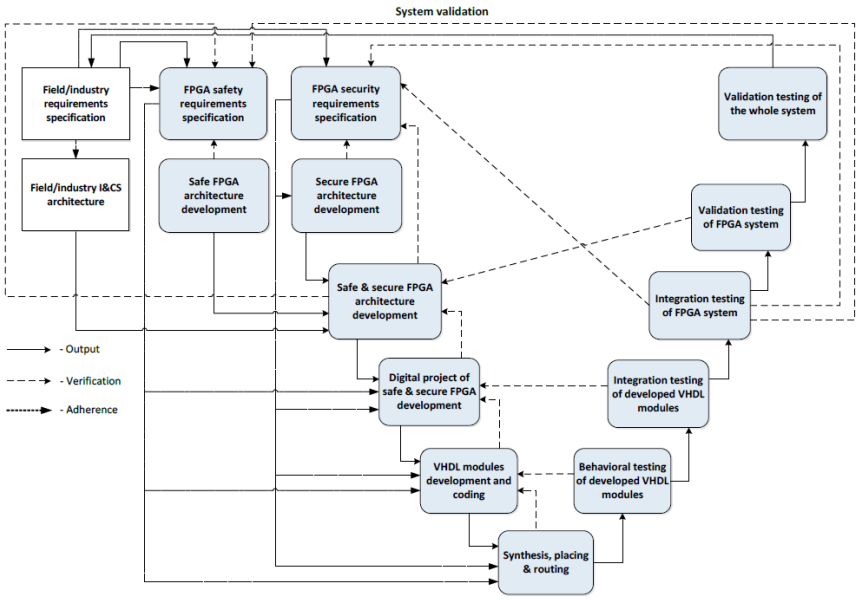

Fig. 5. Safety and security lifecycle model of FPGA-based I&Cs

Fig. 4의 두 직사각형은 FPGA 개발 라이프사이클 기반 프로젝트와 직접적으로 연관되어 있지 않다. 하지만 그들은 시스템 개발 동안 규제 측면에서의 역할을 수행한다. 모서리가 둥근 직사각형은 개발 라이프사이클의 단계와 직접적으로 관련된 활동을 묘사한다. 각기 다른 화살표가 라이프사이클 활동에서의 다른 종류의 관계를 나타내는데, safety와 security 준수 사항의 경우 점선으로 나타내어진다.

중요한 과제 중 하나는 critical 시스템의 safety와 security 요구사항과 critical I&Cs의 safe, security 모두 혹은 각각의 아키텍처를 제공하기 위한 비용과의 균형을 맞추는 것이다. I&Cs의 분명하고 정확한 safety, security 요구사항에 대한 명세에 숨어있는 약점은 safety와 security의 요구사항이 모순되는 상황을 피하고, 시스템이 적절하게 동작할 수 있다는 것을 보장하기 위하여 safety와 security 요구사항이 충돌하는 상황에서의 사고 제도에 대해 시스템을 평가하기 위한 방향으로 개발되고 있다.

5. Security Assessment Technique

5.1 GAP-analysis technique

보안 평가에 있어서 가장 중요한 원칙은 최종 제품 및 제품 개발 과정 간의 불일치성과 발생하는 문제들에 대한 결정으로 이루어진 process-product 접근 방식을 사용하는 것이다. 이에 대한 기본적인 개념 중 하나는, I&C 시스템의 lifecycle의 모든 프로세스마다의 discrepancy에 대해 결정하고 이를 통해 제품의 이상(취약성과 같은)을 발견하거나 제품에 존재하는 이상을 제거할 수 없다는 것을 결정하는 GAP의 개념이다. I&C 시스템의 고려사항에 따라 각각의 GAP은 모든 discrepancy에 대해 결정하는 하나의 양식으로 나타나게 된다. 정형화된 설명은 GAP에의해 식별된 discrepancy의 set으로 이루어져야 한다.

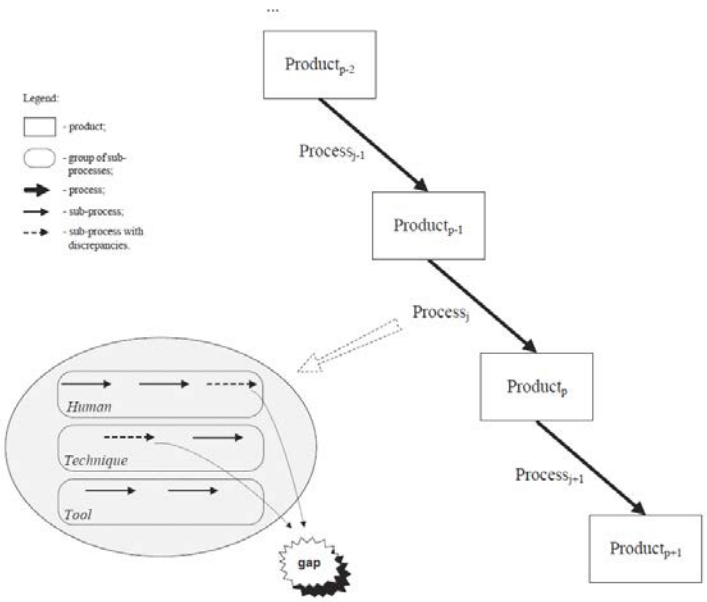

Fig. 6. GAP-analysis technique

5.2 IMECA(Intrusion Modes and Effect Criticality Analysis)-analysis technique

IMECA 분석법은 Security에 적용하기 위하여 FMECA(Failure Modes, Effects and Criticality Analysis)를 실제로 개선한 것이라고 볼 수 있다. 식별된 각각의 GAP들은 단일 로컬 IMECA 표로 표현되고, GAP 내의 각각의 discrepancy는 하나의 행들로 표현될 수 있다. 로컬 IMECA 표는 FPGA와 I&C 자체의 process-product 특징에 대해 나타낸다. 각 GAP에 대하여 GAP 분석에 의해서 식별된 취약성들은 포함한 별도의 표가 생성되며 모든 테이블들은 일반(general) IMECA 테이블로 결합된다.

5.3 Security informed safety approach

구조화된 Safety에 기초하여, "The impact that Security might have on and existing safety case"를 전제로 수행되는 접근 법이다. FPGA 기반 I&C의 Safety와 Security에 관한 평가 및 보장의 문제는 다음과 같이 연구되었다.

- 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

RG 1.152-2011의 I&C의 Secure한 개발 및 구현 환경 설립에 대해 다음과 같이 언급한다.

- 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

이러한 행동에 대한 해석은 시스템에 대한 의도치 않은 접근을 불가능하게 하고, 시스템 동작 동한 적절하지 못한 행동으로부터 보호할 수 있는 보호 디자인의 적용을 포함한다.

6.2 V-Model of FPGA-Based SCI&C

SCI&C의 개발 lifecycle의 V-Model을 고려하는 것은 FPGA 기반 I&C에서 필수 요소라고 할 수 있다. 좌측에 하강하는 부분은 개발 활동과 상응하며, 우측에 상승하는 부분은 Verification 활동과 상응한다.

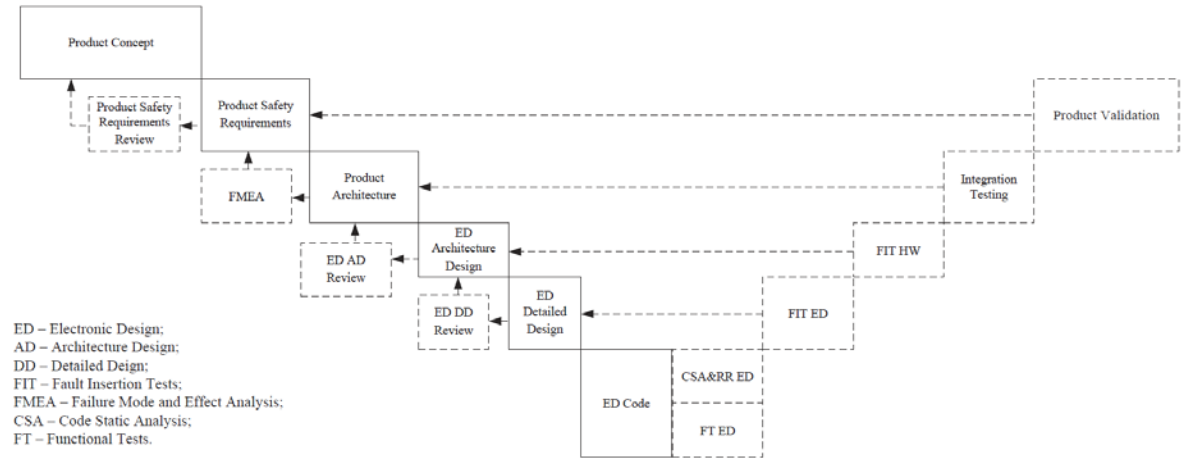

Fig. 7. Development Lifecycles for FPGA-based SCI&C

6.3 Features of Assessment

보안 측면은 concept부터 system retirement에 이르기까지 SCI&C의 모든 lifecycle 각각에서 고려되어야 한다. 그것들은 분리되어있지만 복합적이라고 볼 수 있다. 제품 구조 개발 활동 구현에서의 가능한 gap 중 하나는 앞서 언급한 중요한 Safety 요구사항의 의도한/의도치 않은 가능성에 있다. 다른 gap 은 SCI&C 에서 사용되는 특정 기술과 연관된 가능성 있는 취약성의 이기적인 이용으로 표현될 수 있다. 아래의 표는 FPGA-based I&C 에서 가능한 공격의 일부를 나타낸다.

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

성공적인 cyber 공격 위험을 감소시키기 위해 다음과 같은 세가지 절차가 사용된다.

- 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

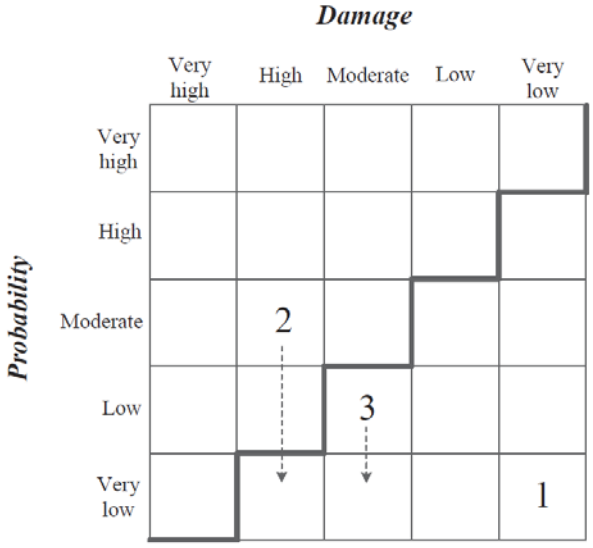

Figure 5. Criticality matrix

Fig. 8. Criticality matrix

Criticality matrix는 위의 그림과 같다. matrix내의 숫자들은 IMECA 표의 적절한 row number를 나타낸다. Cyber security assurance 관점에서, related damage는 상수이기 때문에, risk를 감소시키기 위해선 공격 발생확률을 줄여야 한다. 굵은 선으로 표시된 부분을 기점으로 아래 부분은 수용할 수 있는 정도의 위험을 의미한다. Numbered row의 확률 감소 케이스는 화살표가 달린 점선으로 표시된다. FPGA-based NPP I&C에서 위와 같은 확률 감소는 다음과 같은 경우에 가능하다.

- 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

보통의 경우, Safety critical I&C 시스템은 서로 다른 기능을 가진 서로 다른 기술 기반의 구성요소들의 상호작용으로 구성되어있기에, 이에 대한 security 분석 및 평가는 여전히 어렵다. 따라서, 다양한 I&C 속성들의 interference와 사용된 모든 기술의 특징을 포함한 모든 구체적인 세부 사항을 고려할 필요가 있다.

앞서 제시한 접근 방식들은 gap 개념과 IMECA 기술, 사람, 적용 기술 및 도구와 연관된 개발 프로세스에 대한 분석에 에 기반하여 제시되었다. 이는 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 보여진다. 따라서 이를 위한 보다 상세한 요구사항과 gap에 대한 분석 및 countermeasure들에 대한 연구가 필요할 것으로 보여진다.

이와 관련된 다른 연구로는 risk assessment와 safe와 secure 모두를 추구하는 실제 시스템에서의 security-informed safety justification을 바탕으로 methodology를 개발하고, 이러한 methodology를 구현한 도구를 개발 중인 연구가 있다.

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