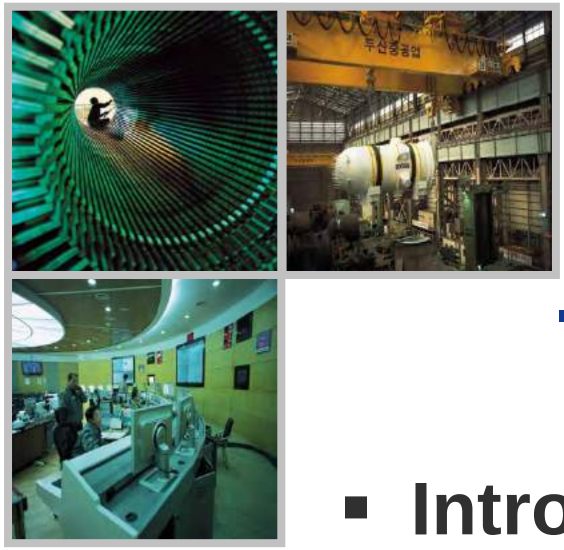
HF Controls

Cyber Security of HFC-FPGA Platform

Yin Guo
10/09/2018

Innovation Leadership Service



Presentation Outline

- Introduction
- Regulatory Requirements and Guides
- Cyber Security of HFC-FPGA Platform

Introduction

Cybersecurity

[U.S. NRC] RG1.152

Cyber Security refers to those measures and controls, implemented to comply with 10 CFR 73.54, to protect critical digital assets against malicious acts of an adversary up to and including the design basis threat, as defined by 10 CFR 73.1.

Introduction

Why Cyber Security is essential?

- ✓ Regulatory Compliance
  - ❖ Code of Federal Regulation
  - ❖ Regulatory Guide
- ✓ Increasing exposure to cyber threats
  - ❖ System Digitalization
  - ❖ Use of COTS
- ✓ Lesson and experience learnt from other industries
  - ❖ Bulk Power System
- ✓ ……

Introduction

North American Electronic Reliability Corporation (NERC) and Federal Energy Regulatory Commission (FERC)

- Project 2008-06 Cyber Security, Critical Infrastructure Protection (CIP) Standards
  - CIP-002-04 to CIP-009-04 and implementation plans, Jan. 2011

Electric Power Research Institute (EPRI)

- 1020110 Guidelines for Applying Security Measures to Meet Distribution Cyber Security Requirements, December 2010

International Society of Automation (ISA)

- ANSI/ISA-99.00.01-2007, “Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models”
- ANSI/ISA-99.02.01-2009 Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program

National Institute of Standard and Technology (NIST)

- Special Publications in the 800 series
  - SP 800-53, Rev.3, “Recommended Security Controls for Federal Information Systems”, August 2009
  - SP 800-82, “Guide to Industrial Control Systems (ICS) Security”, September 2008

Introduction-CFR

Code of Federal Regulations

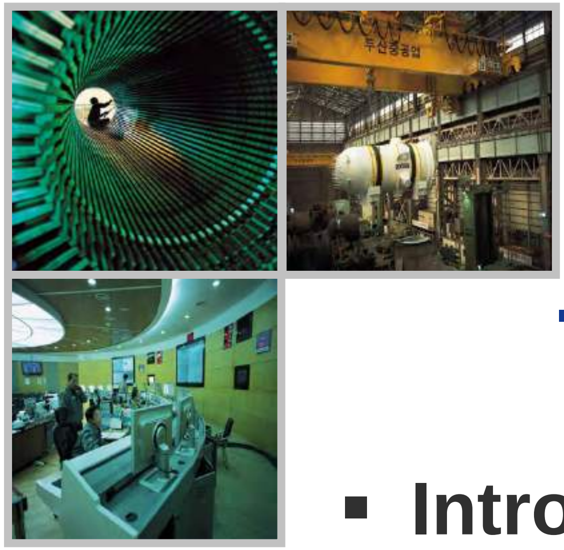
❖ **10 CFR Part 73, Physical Protection of Plant and Materials**

- *10 CFR Part 73.54 Protection of Digital Computer and Communication Systems and Networks*
- 10 CFR Part 73.55 Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage.
- **10 CFR Part 73.50 Requirements for Physical Protection of Licensed Activities**
- **10 CFR Part 73.1 Purpose and Scope**

Introduction-RG

United States Nuclear Regulatory Commission (USNRC)

- RG 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants”, Rev. 3, July 2011
- RG 5.71, “Cyber Security Programs for Nuclear Facilities”, January 2010.
- RG 1.168, “Verification, Reviews, and Audits for Digital Computer Software in Safety Systems of Nuclear Power Plants”, Section 3.7.C “Security Analysis”, Rev. 2, July 2013



Presentation Outline

- Introduction
- Regulatory Requirements and Guides
- Cyber Security of HFC-FPGA Platform

Regulatory Requirements

Code of Federal Regulations:

Design Basis Threats:
(10 CFR 73.1)

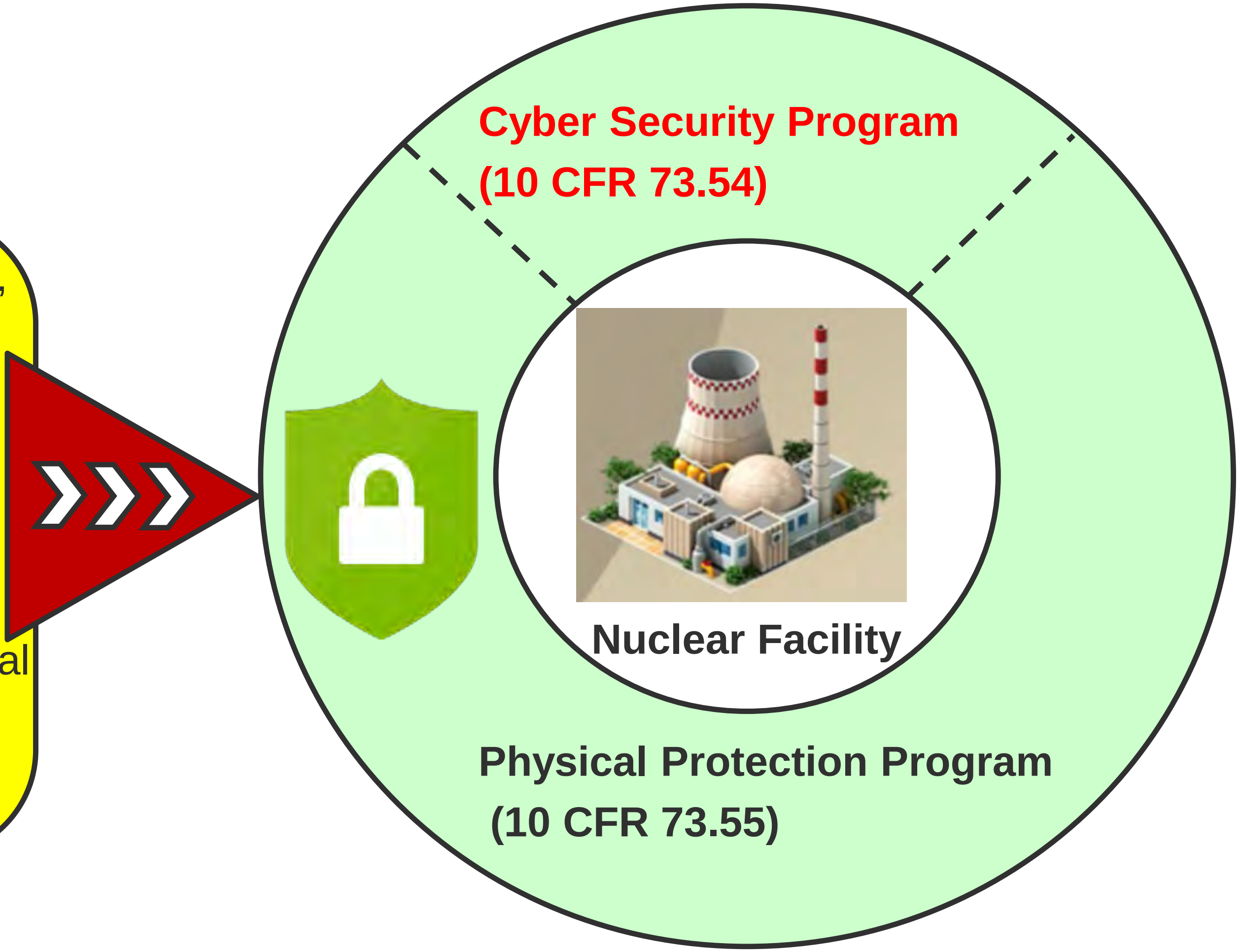
(1). A determined violent external assault, attack;

(2). An internal threat;

(3). A land vehicle bomb assault, which may be coordinated with an external assault;

(4). A waterborne vehicle bomb assault, which may be coordinated with an external assault;

(5). **A cyber attack**



Regulatory Requirements-10 CFR 73.54

10 CFR 73.54(a)

*The licensee shall provide high assurance that **digital computer and communication systems and networks** are adequately protected against cyber attacks, up to and including the design basis threat (DBT) as described in 10 CFR 73.1.*

- ***What kind of system shall be protected?** (10 CFR 73.54(a)(1))*

***Ans:** SSEP functions and support systems and equipment which, if compromised, would adversely impact SSEP functions*

- ***What kind of cyber attacks shall be considered?** (10 CFR 73.54(a)(2))*

***Ans:** (i) Adversely impact the integrity or confidentiality of data and/or software;*

(ii)Deny access to systems, services, and/or data; and

(iii)Adversely impact the operation of systems, networks, and associated equipment.

Regulatory Requirements 10 CFR 73.54

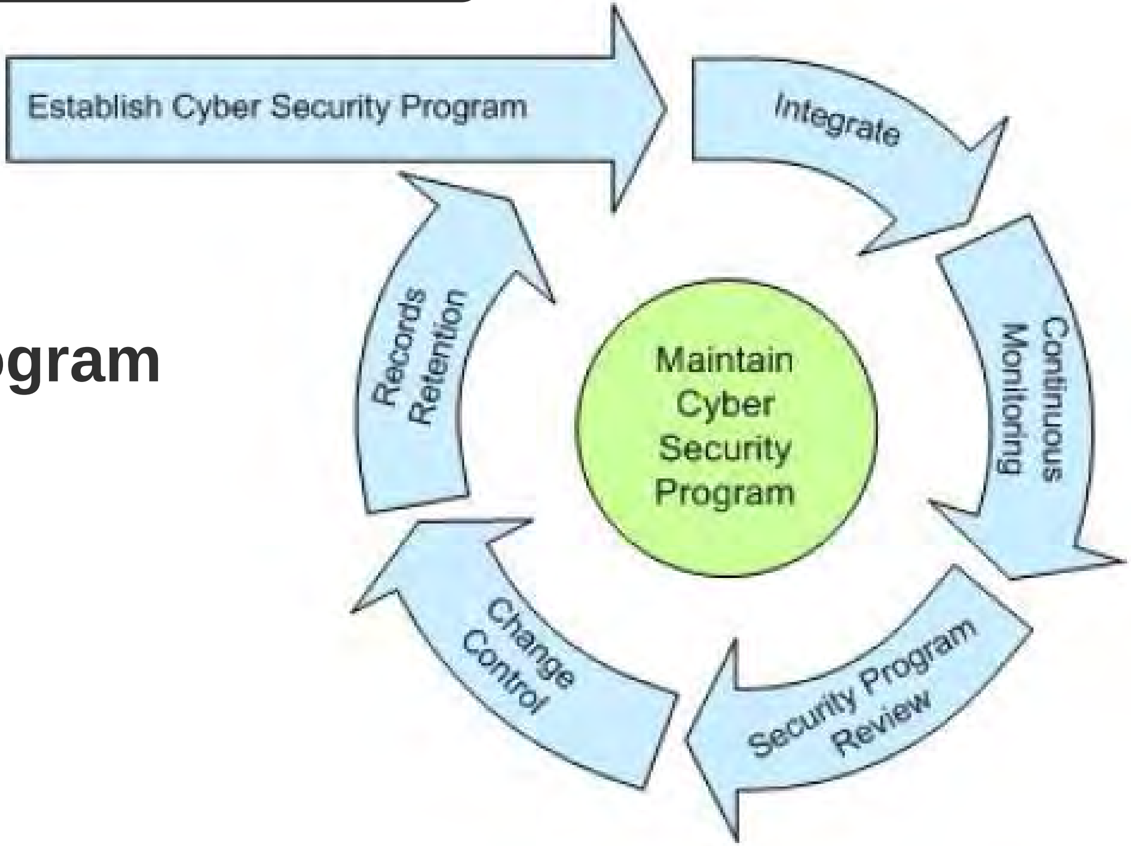
1	• Licensing Requirements	10 CFR 73.54(a)
2	• Cyber Security Program	10 CFR 73.54(b) 10 CFR 73.54(c) 10 CFR 73.54(d)
3	• Cyber Security Plan	10 CFR 73.54(e)
4	• Written Policy and implementing Procedures	10 CFR 73.54(f)
5	• Periodic Review	10 CFR 73.54(g)
6	• Records Retention	10 CFR 73.54(h)

Regulatory Guide 5.71

10 CFR 73.54 Protection of digital computer and communication systems and networks

RG 5.71 Cyber Security Program for Nuclear Facilities

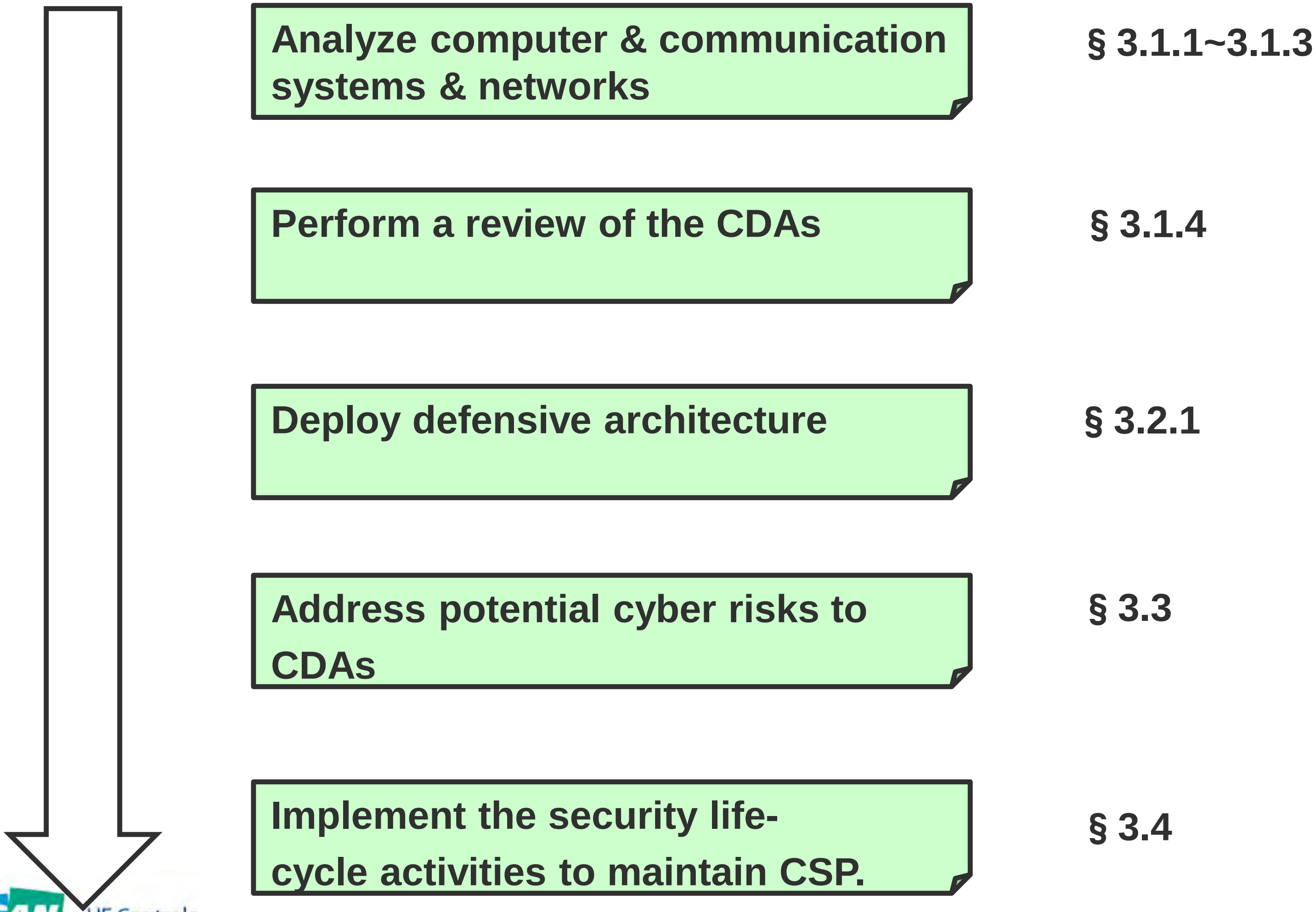
- ✓ **Cyber Security Program**
  - **- Establishment**
  - **- Implementation**
  - **- Maintenance**



Security Life Cycle Process

Regulatory Guide 5.71

Steps to Establish and Implement a Cyber Security Program



Analyze computer & communication systems & networks — § 3.1.1~3.1.3

Perform a review of the CDAs — § 3.1.4

Deploy defensive architecture — § 3.2.1

Address potential cyber risks to CDAs — § 3.3

Implement the security life-cycle activities to maintain CSP. — § 3.4

Regulatory Guide 5.71

- NRC categories security controls recommended by NIST SP 800 into 3 classes:
  - Technical

    Access Control; Audit and Accountability; System and Communication Protection;

    Identification and Authentication; System Hardening;

  - Operational

    Media Protection; Personnel Security; System and Information Integrity; Maintenance; Physical and Environmental Protection; Incident Response; Contingency Planning/Continuity of SSEP functions; Awareness and Training; Configuration Management;

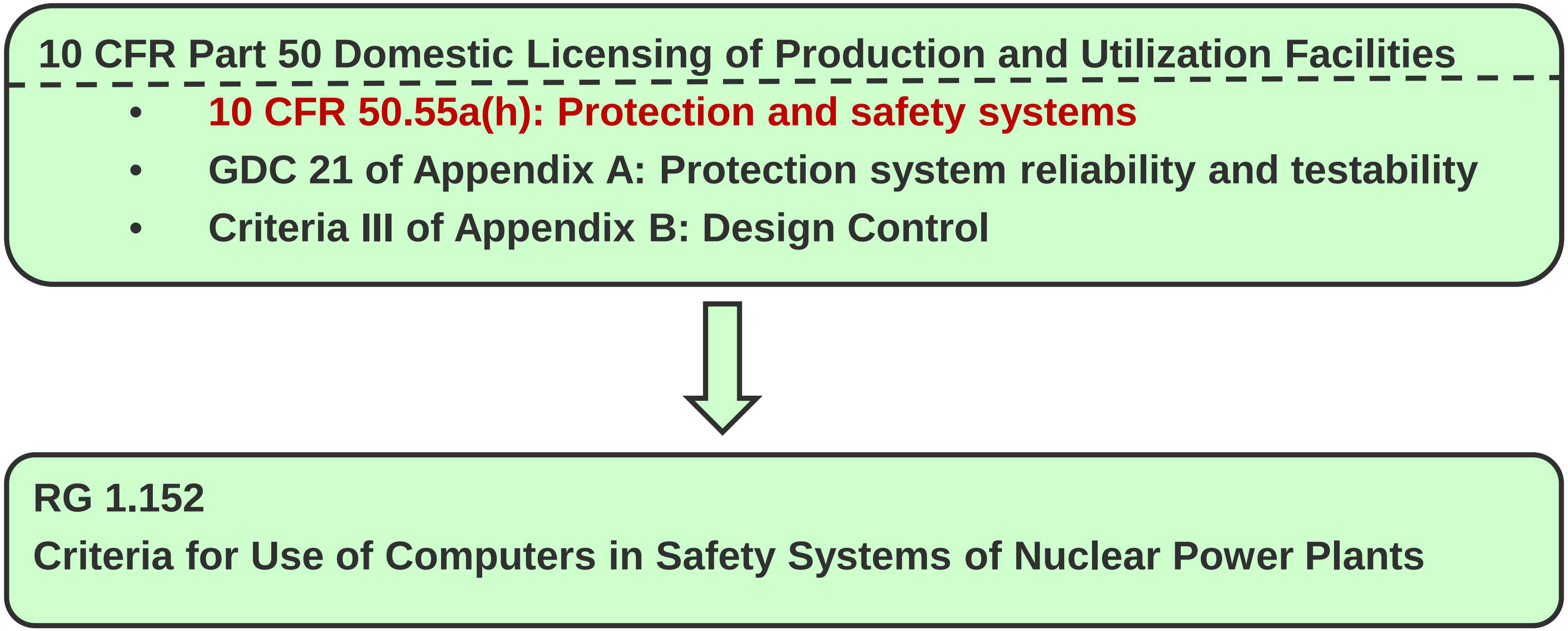
  - Management

    System and Service Acquisition

    Security Assessment and Risk Management

- Appendix A: Generic cyber security plan template
- Appendix B: Technical Controls
- Appendix C: Operational and Management Controls

Regulatory Guide 1.152



10 CFR Part 50 Domestic Licensing of Production and Utilization Facilities

- 10 CFR 50.55a(h): Protection and safety systems
- GDC 21 of Appendix A: Protection system reliability and testability
- Criteria III of Appendix B: Design Control

RG 1.152

Criteria for Use of Computers in Safety Systems of Nuclear Power Plants

- High Functional Reliability
- Design Quality
- A Secure Development and Operational Environment

Regulatory Guide 1.152

Secure Development and Operational Environment (SDOE) for the Protection of Digital Safety Systems

- **Establishment of SDOE**

1). Measures and controls taken to establish a secure environment for development of the digital safety system against undocumented, unneeded and unwanted modifications.

2). 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 digital safety system during operation.

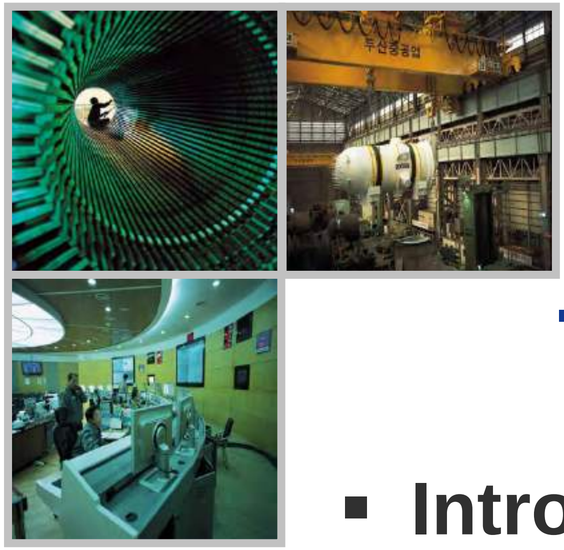
HFC Cyber Security Program

HFC Cyber Security Program

- More than 40 years operating history of HFC platform in power plant
- Lesson Learnt from USNRC Audits (Oct. 2009 and Dec. 2009)
- HFC has established, implemented and maintained a cyber security program in accordance with 10 CFR 73.54, RG 5.71 and RG 1.152

Implementation for new FPGA-based platform design

- Identify CDA
- Identify Vulnerability
    - Design
    - Process
    - Operation and Maintenance
- Countermeasures
- Implementation



Presentation Outline

- Introduction
- Regulatory Requirements and Guides
- Cyber Security of HFC-FPGA Platform

Cyber Security Analysis of FPGA-based Platform

FPGA-based platforms have characteristics that tend to increase the level of difficulty to be invaded

✓ **Directly implement the required I&C functions:**

Do not contain high-level, general-purpose components that could be easily diverted or hijacked for malicious purposes;

✓ **FPGA re-programming protection measures:**

Anti-fuse technology

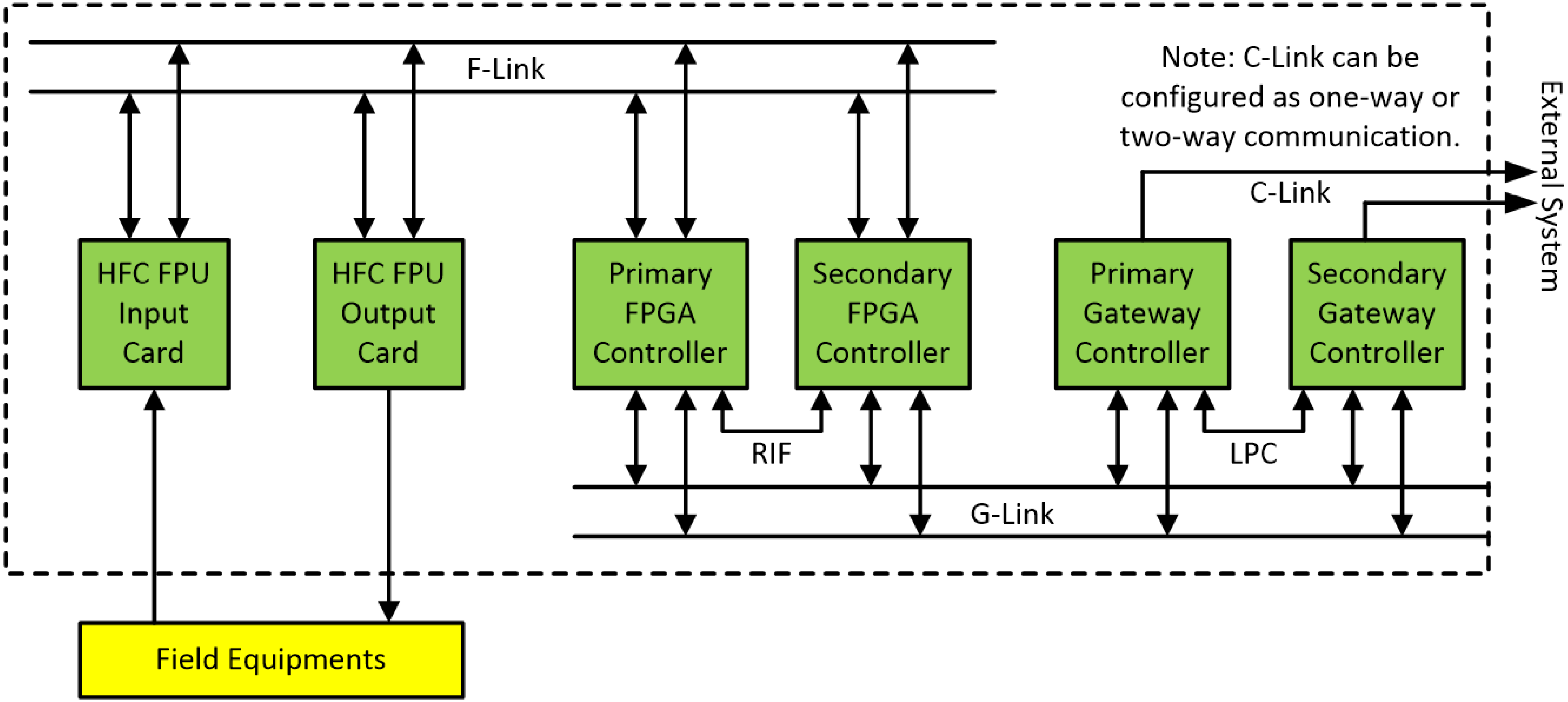
✓ **No operating system and peripheral software:**

Reduce overall complexity, and increase reliability

✓ **Separation of independent function:**

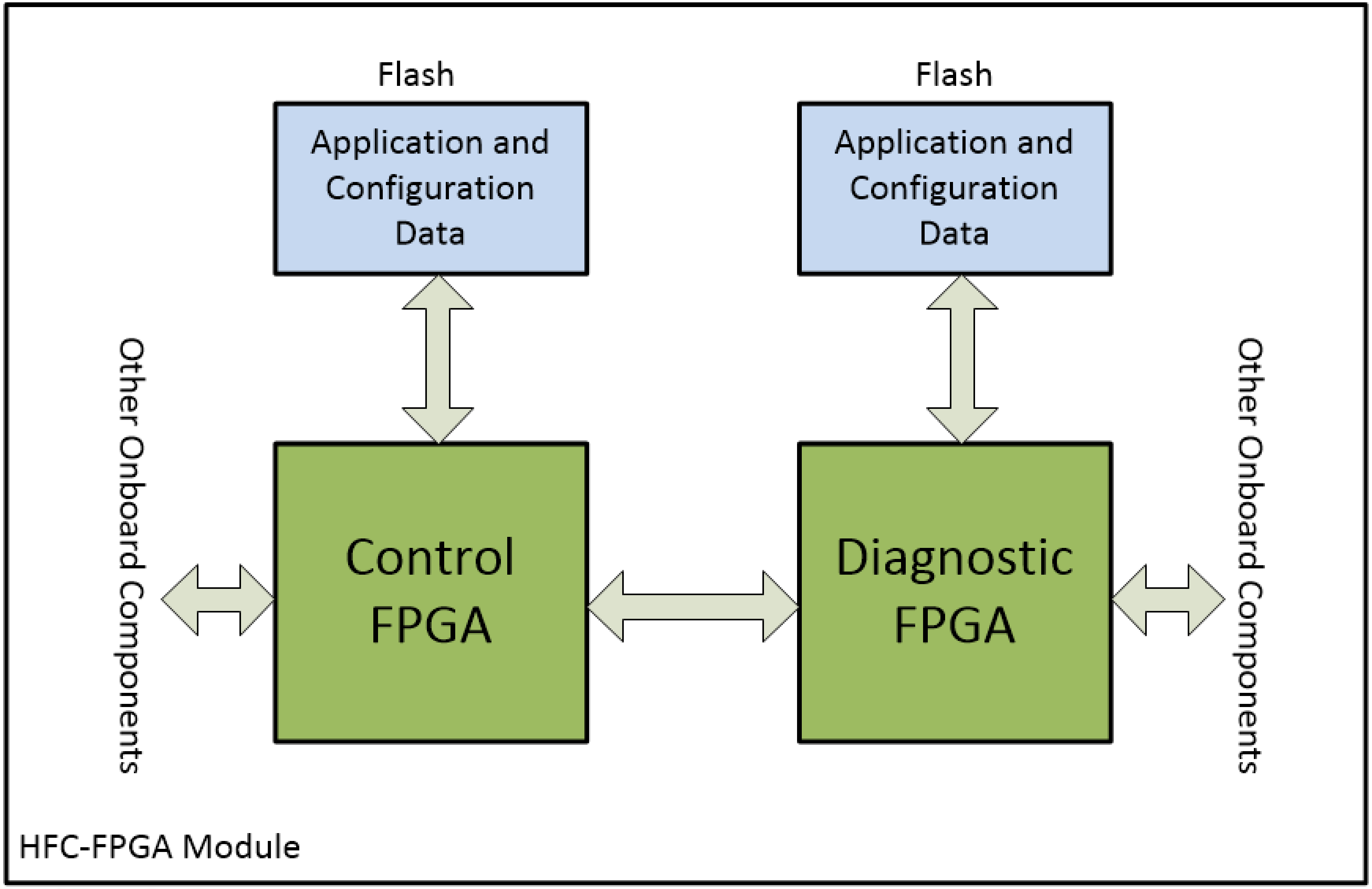
Prevent from failure postulating and separated function interfering with one another, facilitate verification, analysis, testing and ultimately, safety justification

HFC-FPGA Application


F-Link
Note: C-Link can be configured as one-way or two-way communication.
C-Link
External System
HFC FPU Input Card
HFC FPU Output Card
Primary FPGA Controller
Secondary FPGA Controller
Primary Gateway Controller
Secondary Gateway Controller
RIF
LPC
G-Link
Field Equipments

Example of HFC-FPGA based Platform Configuration

HFC-FPGA Application



HFC-FPGA Application

Design	Vulnerabilities	Security Design Features
Network	• Structure, protocol and data format, timing and sequence of Non-proprietary network is known to public	• HFC proprietary network structure –Hardcoded nodes and address • HFC proprietary communication protocol –Predefined data package length, format –Predefined timing and sequence –Integrity validation by CRC check • Communication link isolation and independence • Isolated with external network • Physical and logical access controls
Onboard Data	• Alteration to Application, configuration data, and FPGA load	• Download of FPGA build is only allowed in offline mode and security key is required • Only part of Application (e.g. setpoint) and configuration data can be updated online • Runtime security features –Runtime checking of any change in configuration data file –Protection of unauthorized updates of configuration data file • Physical and logical access controls

Cyber Security of HFC-FPGA Based Platform

HFC-FPGA Platform Development Process

Lifecycle	Critical Digital Assets	Vulnerabilities
Requirements	Requirements Documents	• Unauthorized updates to the documents • Uncontrolled version of documents
Design	Design Documents Test Documents	• Unauthorized updates to the documents • Uncontrolled versions of documents • Unnecessary/Unaddressed/Unwanted Designs/Functions
Implementation	FPGA Source Code Test Documents	• Unauthorized updates to the source code • Uncontrolled versions of source code • Unnecessary/Unaddressed/Unwanted source code
Test	FPGA build Test Documents	• Unauthorized updates to the build processing • Unauthorized release of source code • Unnecessary/Unaddressed executable functions

Cyber Security of HFC-FPGA Based Platform

Cyber Security Measures

Unauthorized change to CDAs in the development lifecycle

- -Access Control
  - -Physical Isolation of access Path
  - -Least privilege policy
  - -Account management
  - -Change control and change track
- -Identification and Authentication
  - -User identification and authentication
  - -Password requirements
  - -Device identification and authentication
- -Media Protection
  - -Media access
- -Personal Security
  - -Personnel termination or transfer
- -Physical and Environmental Protection
- -System Hardening

Cyber Security of HFC-FPGA Based Platform

Cyber Security Measures

Uncontrolled version of CDAs

- -Media Protection
- -Configuration Management
- -Configuration Change Control
- -Awareness and Training
- -Identification and Authentication

Unnecessary/unaddressed/unwanted functions/designs

- -Audit and Accountability
- -Configuration Change Control
- -Integrate cyber security program into the product lifecycle process

Summary

- HFC has established, implemented and maintained a cyber security program in accordance with the regulatory requirements and guide, and applicable industrial standards.

- The vulnerabilities identified in the HFC-FPGA platform design and development process were properly addressed.

Thank you for your attention!

DOOSAN HF Controls