IAEA
International Atomic Energy Agency

Development of FPGA-based Computer Security Controls for Advanced PWRs

Ahmed S. Ibrahim

Nuclear Power Plants Authority
Cairo, EGYPT

International Conference on Nuclear Security 2020
10 – 14 February, 2020, VIC

Outline of the Presentation

1 Introduction

2 Compliance with IAEA Guidelines

3 Conceptual Approach to Advanced PWR

4 Summary

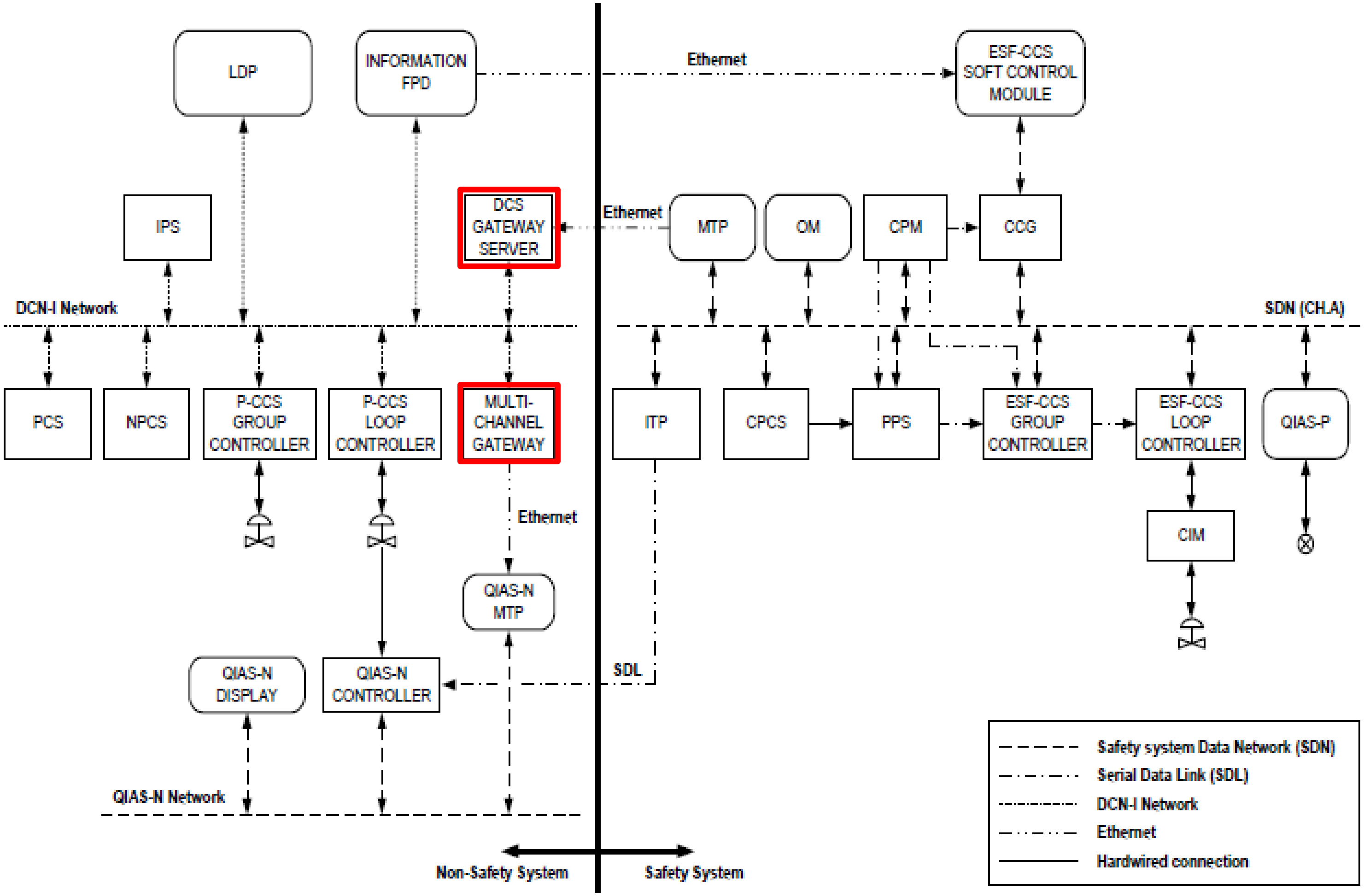
1 Introduction

- In advanced PWR reactors like Korean APR1400 and Russian VVER-1200, I&C systems are computer-based.

- Such computer-based systems encompass safety I&C systems network for NPP reactor protection, and non-safety I&C systems network for NPP normal operation.

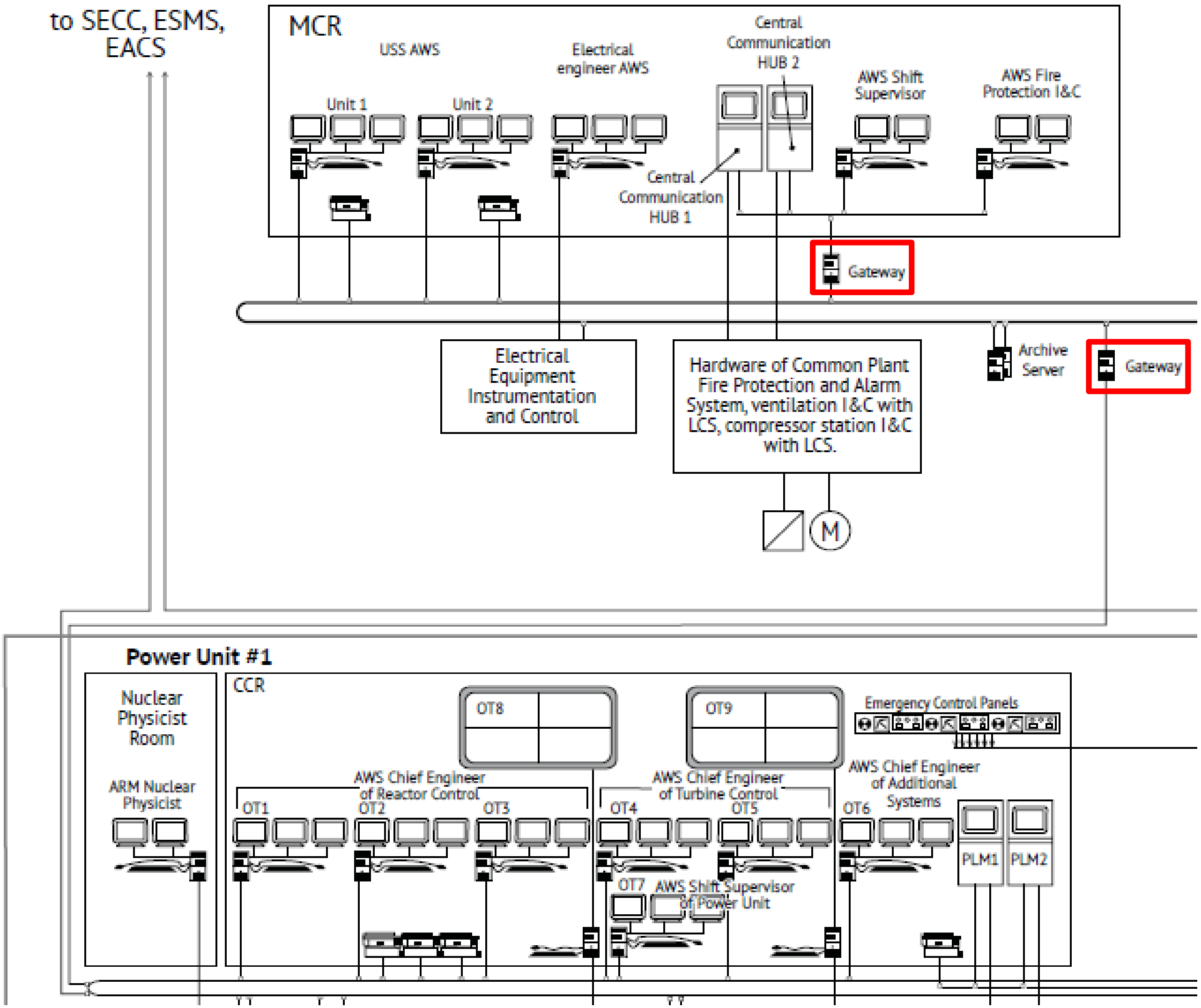
- Computer-based redundant gateway devices are serving as network security perimeters allowing data exchange between I&C systems networks with different protocols and interconnections.

APR1400 Data Communication Block Diagram



Reference: APR1400 Design Control Document Tier 2, Chapter 7 I&C, www.nrc.gov

VVER-1200 I&C System Overview Architecture


to SECC, ESMS, EACS
MCR
USS AWS
Unit 1
Unit 2
Electrical engineer AWS
Central Communication HUB 2
Central Communication HUB 1
AWS Shift Supervisor
AWS Fire Protection I&C
Gateway
Electrical Equipment Instrumentation and Control
Hardware of Common Plant Fire Protection and Alarm System, ventilation I&C with LCS, compressor station I&C with LCS.
M
Archive Server
Gateway
Power Unit #1
Nuclear Physicist Room
ARM Nuclear Physicist
CCR
OT8
OT9
Emergency Control Panels
AWS Chief Engineer of Reactor Control
OT1
OT2
OT3
AWS Chief Engineer of Turbine Control
OT4
OT5
AWS Chief Engineer of Additional Systems
OT6
PLM1
PLM2
OT7
AWS Shift Supervisor of Power Unit

Reference: Professional Solutions on Automation, I&C based on Leningrad NPP-2, rasu.ru

Gateways Functionality

- Such gateways are mainly designed to handle:
  - Data exchange between I&C Safety System and Safety-related systems (i.e., I&C system for Normal Operation Related to Safety);
  - Data exchange between I&C Safety System and Non-safety systems (i.e., I&C system for Normal Operation); and
  - Data exchange of various I&C systems with database servers.

- Gateways also provide a computer security perimeter between I&C Safety and Non-safety data communication networks.

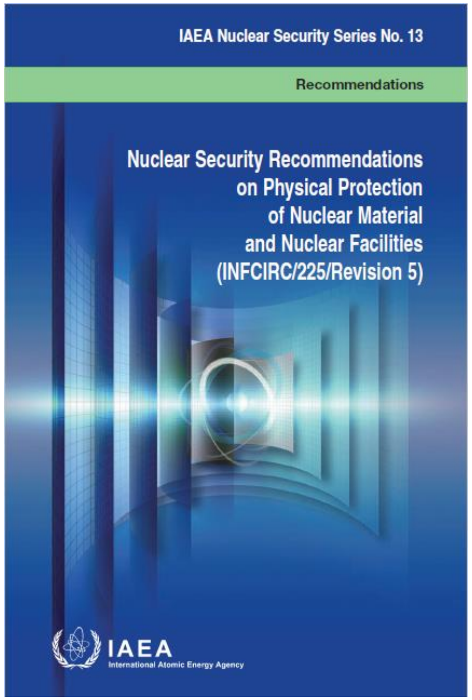
- Potential cyberattacks or malicious actions, if initiated from the non-safety systems network, may compromise the gateways availability or data integrity.

2 Compliance with IAEA Guidelines

- IAEA NSS no. 13 “*Nuclear security recommendations on physical protection of nuclear material and nuclear facilities (INFCIRC/225/revision 5*)” states that:

  “5.18. The operator should assess and manage the physical protection interface with safety activities in a manner to ensure that they do not adversely affect each other and that, to the degree possible, they are mutually supportive.”

  “5.19. Computer based systems used for physical protection, nuclear safety, and nuclear material accountancy and control should be protected against compromise (e.g. cyber attack, manipulation or falsification) consistent with the threat assessment or design basis threat.”

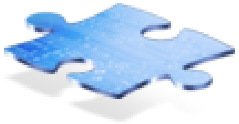


IAEA Nuclear Security Series No. 13

Recommendations

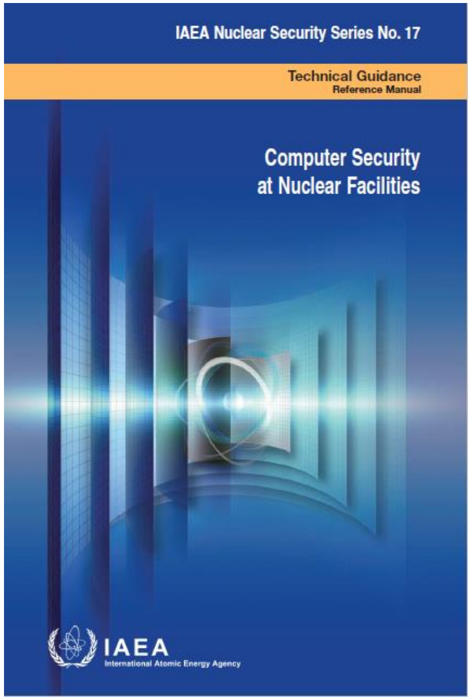
Nuclear Security Recommendations
on Physical Protection
of Nuclear Material
and Nuclear Facilities
(INFCIRC/225/Revision 5)

IAEA
International Atomic Energy Agency



- IAEA NSS no. 17 “*Computer Security at Nuclear Facilities*”, Section 5.4 *Computer System Classification* states that:

> “*Computer functions of prime concern are control and data processes associated with safety and security. Other computer functions may be a concern in terms of support to these functions, of possible compromise of security through secondary or indirect effects or of overall plant productivity.”*



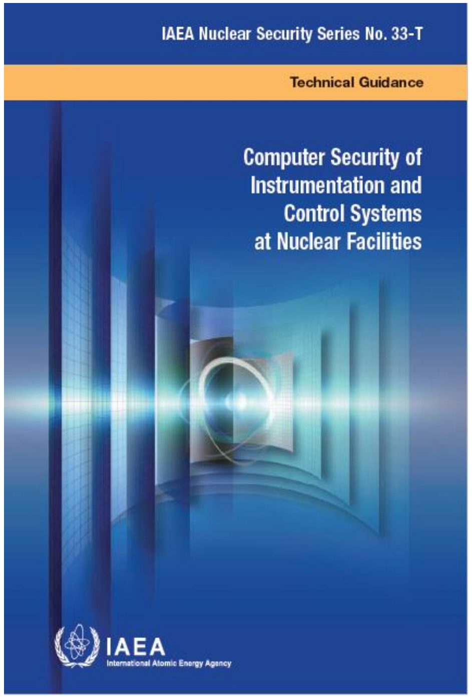
IAEA Nuclear Security Series No. 17

Technical Guidance
Reference Manual

Computer Security
at Nuclear Facilities

IAEA
International Atomic Energy Agency

- IAEA NSS no. 33-T "*Computer Security of Instrumentation and Control Systems at Nuclear Facilities*" states that:
  - *"3.43. The implementation of computer security measures should not adversely affect the essential safety functions and performance of the I&C system."*
  - *"3.44. Neither the normal nor the abnormal operation of any computer security measure should adversely affect the ability of an I&C system to perform its safety function."*
  - *"3.46. Computer security measures that protect the human–system interface should not adversely affect the operator's ability to maintain the safety of the facility. The operator should also consider adverse effects such as the interception and modification of process data sent to the human–system interface (e.g. spoofing) with the aim of preventing or delaying the operator from actuating a safety function (e.g. manual trip)."*



IAEA Nuclear Security Series No. 33-T

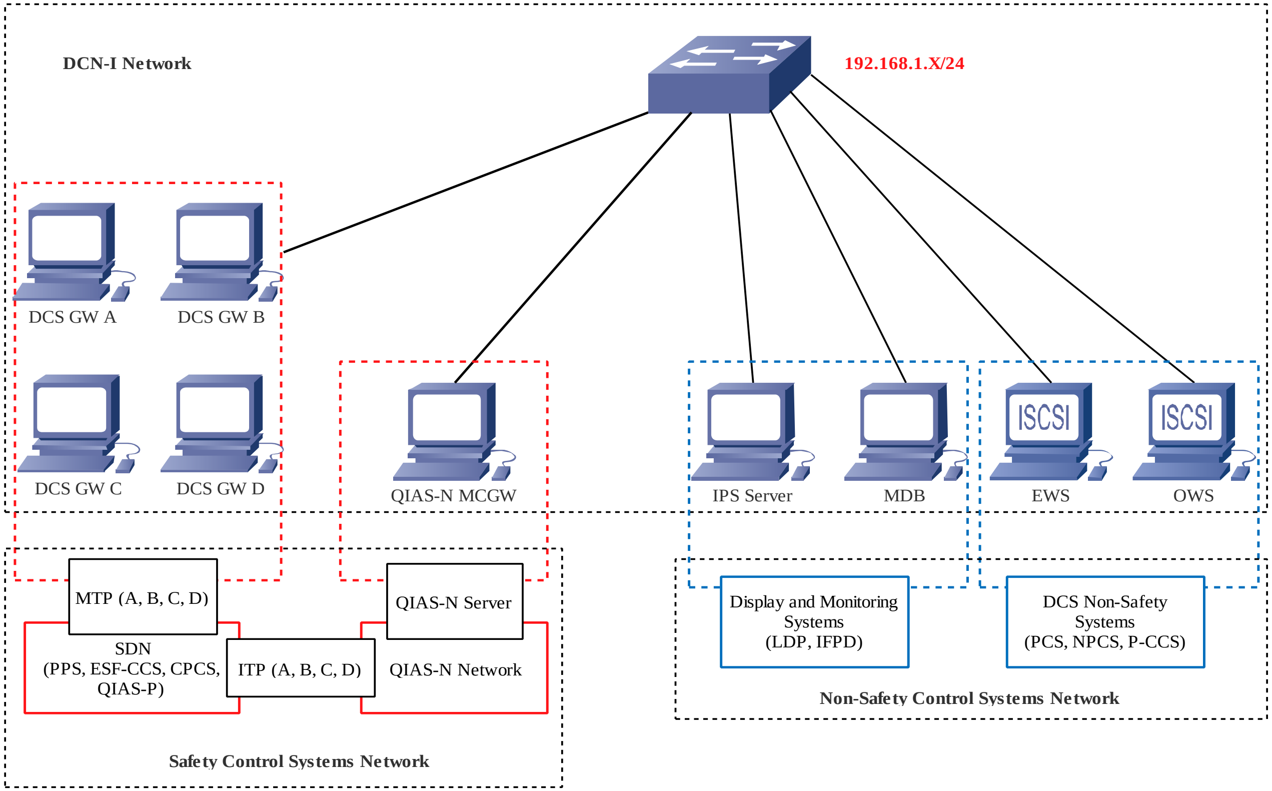
Technical Guidance

Computer Security of
Instrumentation and
Control Systems
at Nuclear Facilities

IAEA
International Atomic Energy Agency

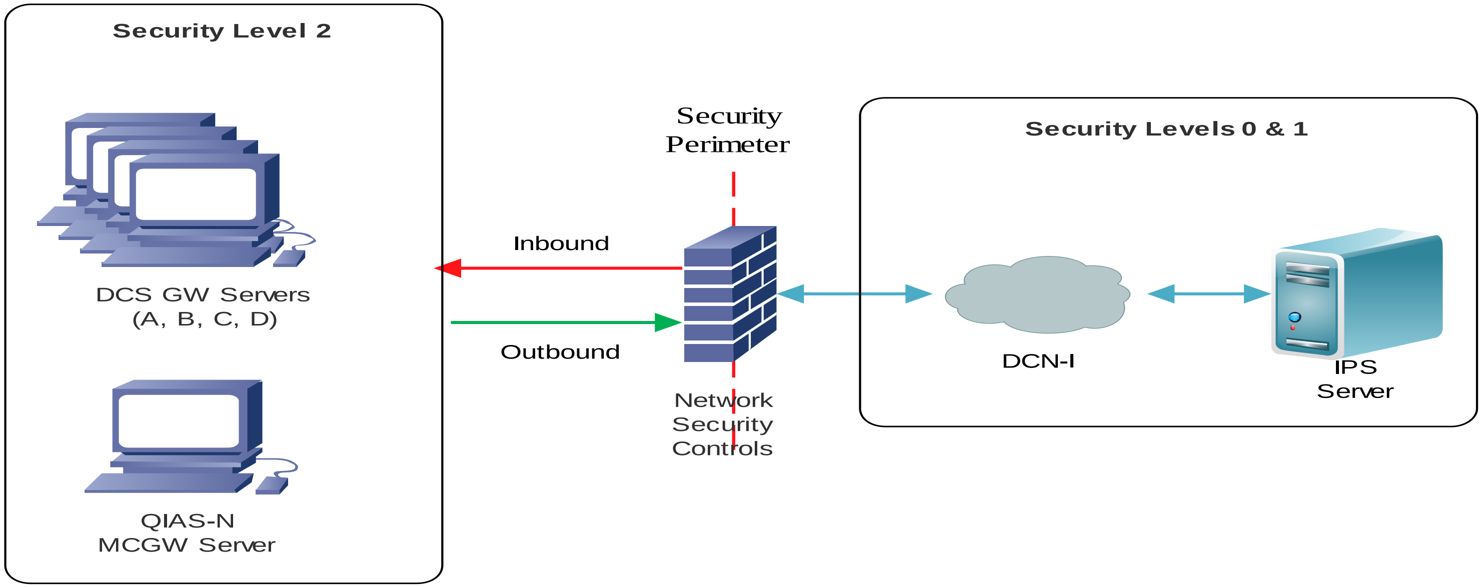
3 Conceptual Approach to Advanced PWR

The current data communication network architecture does not implement security controls between the Non-safety side and the redundant safety-channel gateway devices.



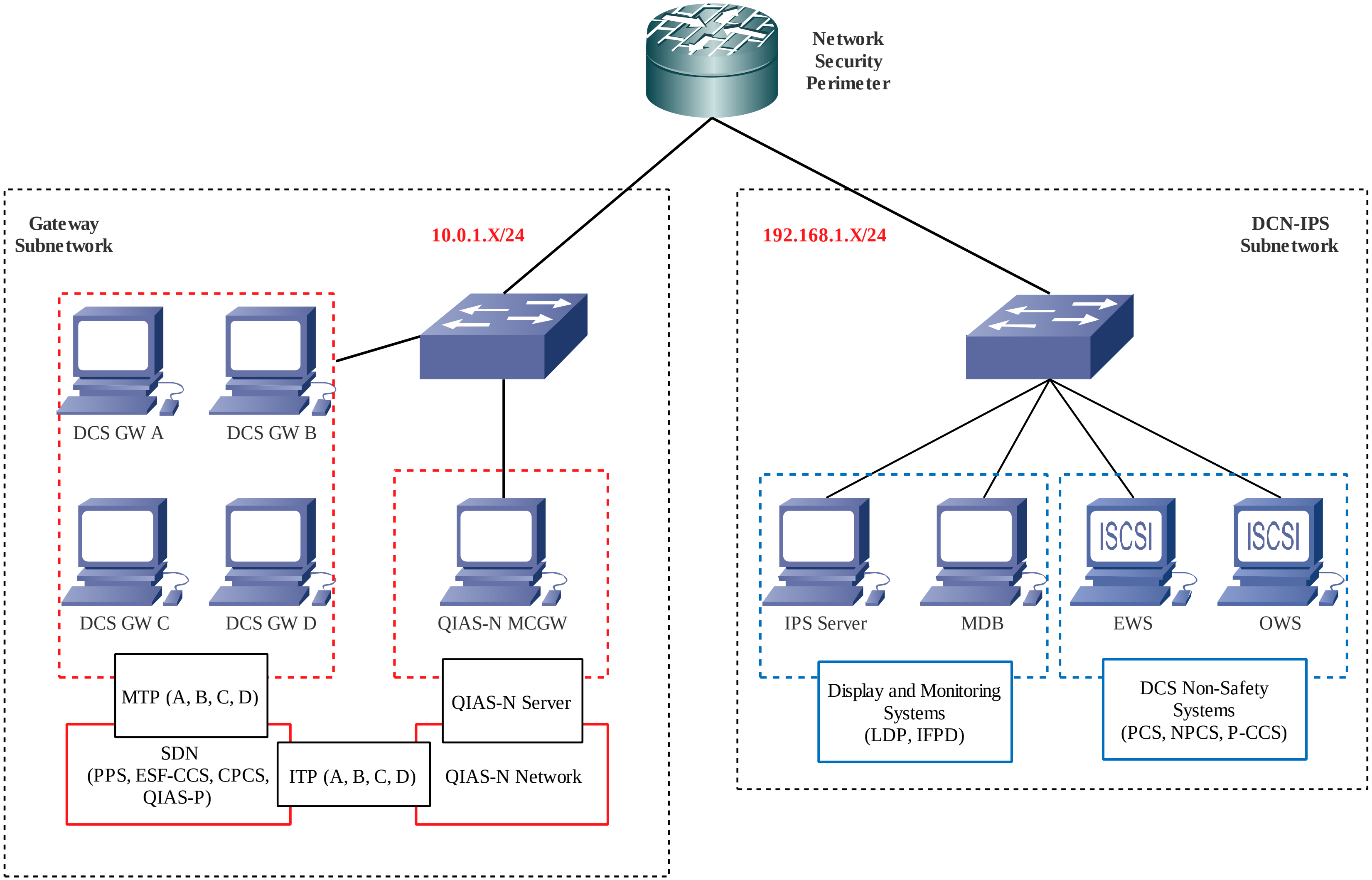
Reference: APR1400 Design Control Document Tier 2, Chapter 7 I&C, www.nrc.gov

Conceptual Design Approach to Computer Security

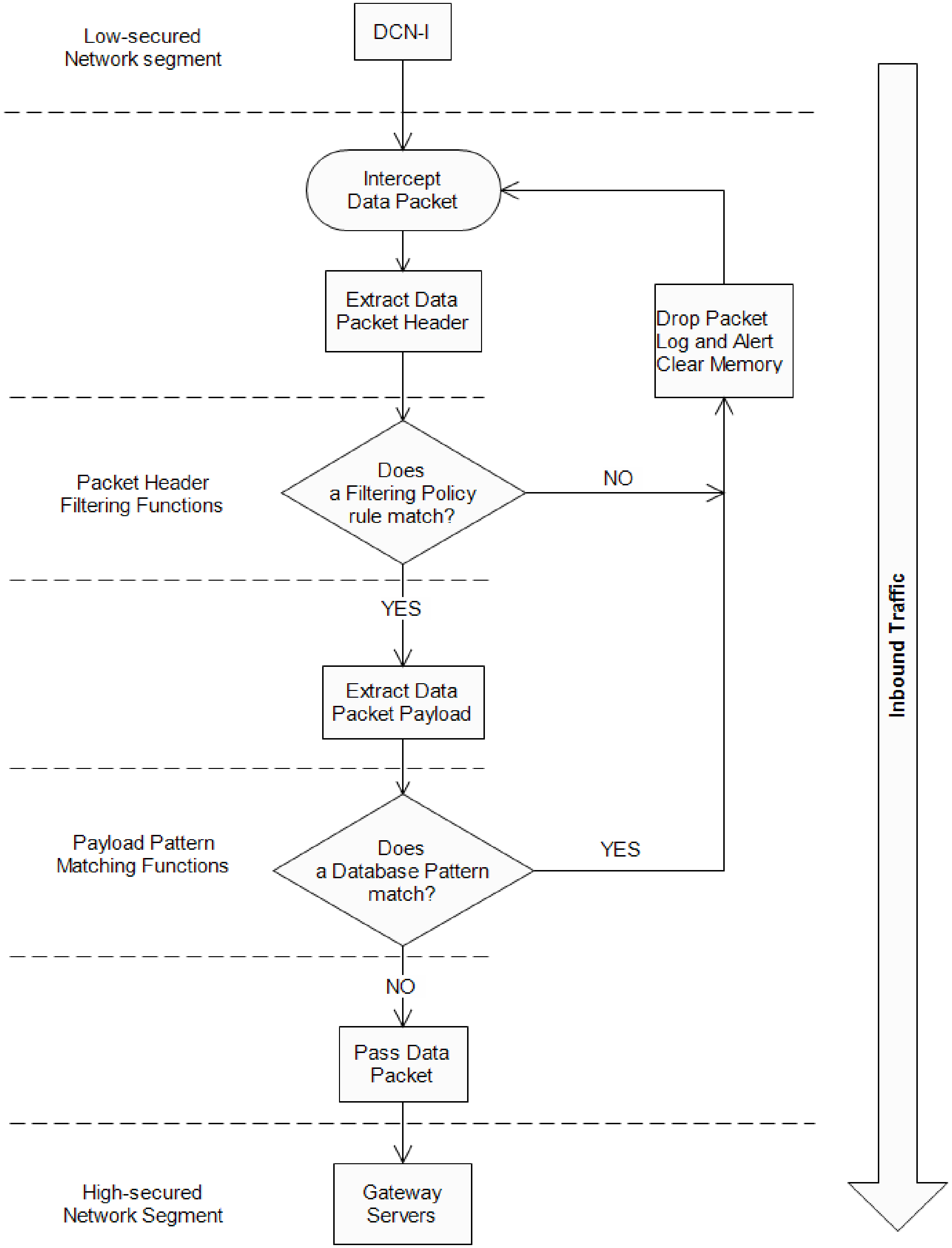


- Establishing a computer security perimeter as an FPGA-based network security controller between the DCN-I Subnet and DCS safety-channel gateway servers Subnet is to implement security controls for controlling and managing the inbound data traffic.

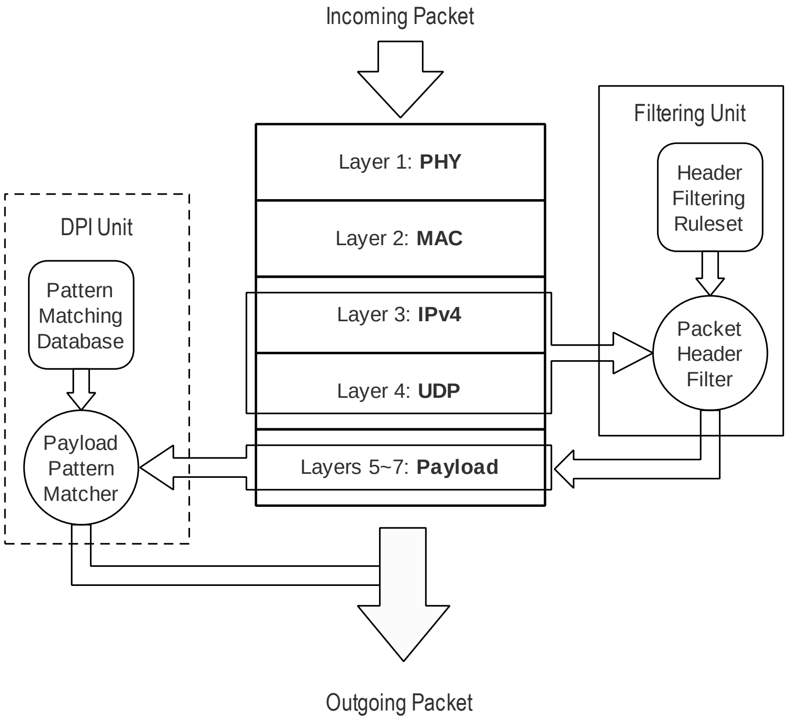
Re-architected Data Network

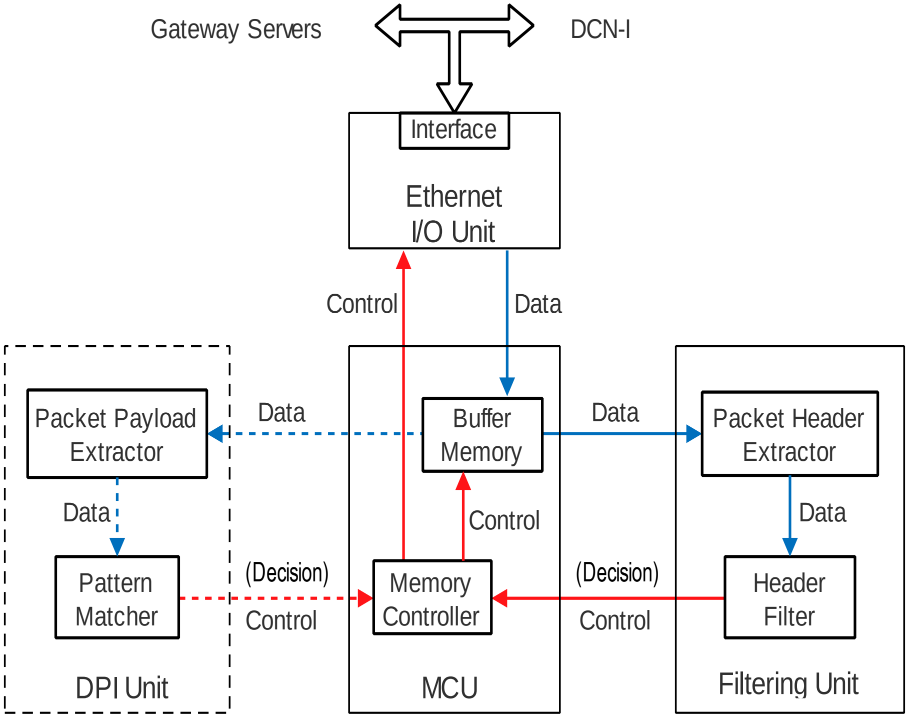


Design Flowchart

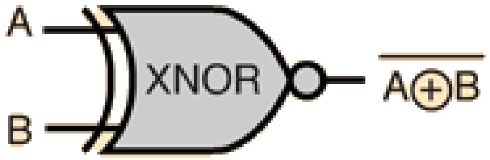


Design Block Diagram

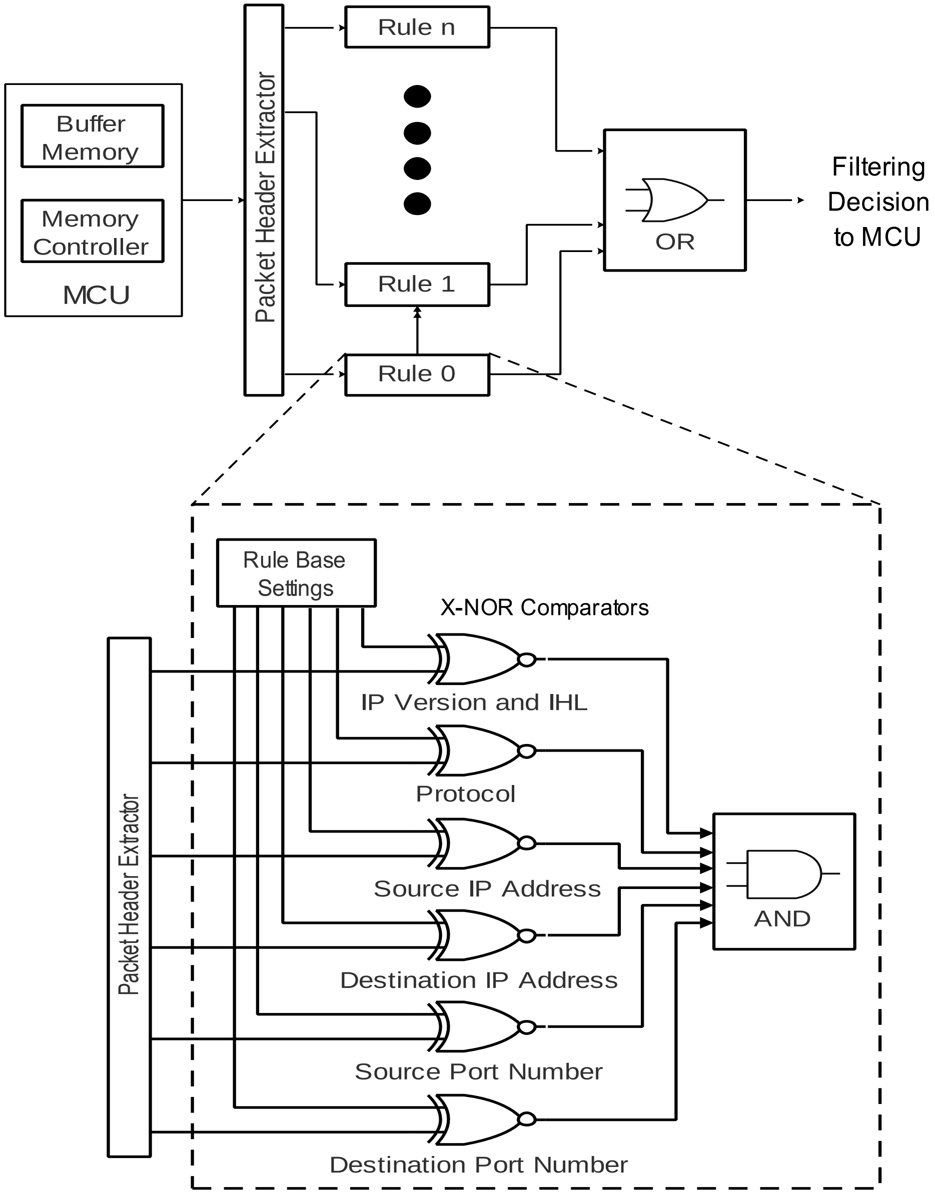




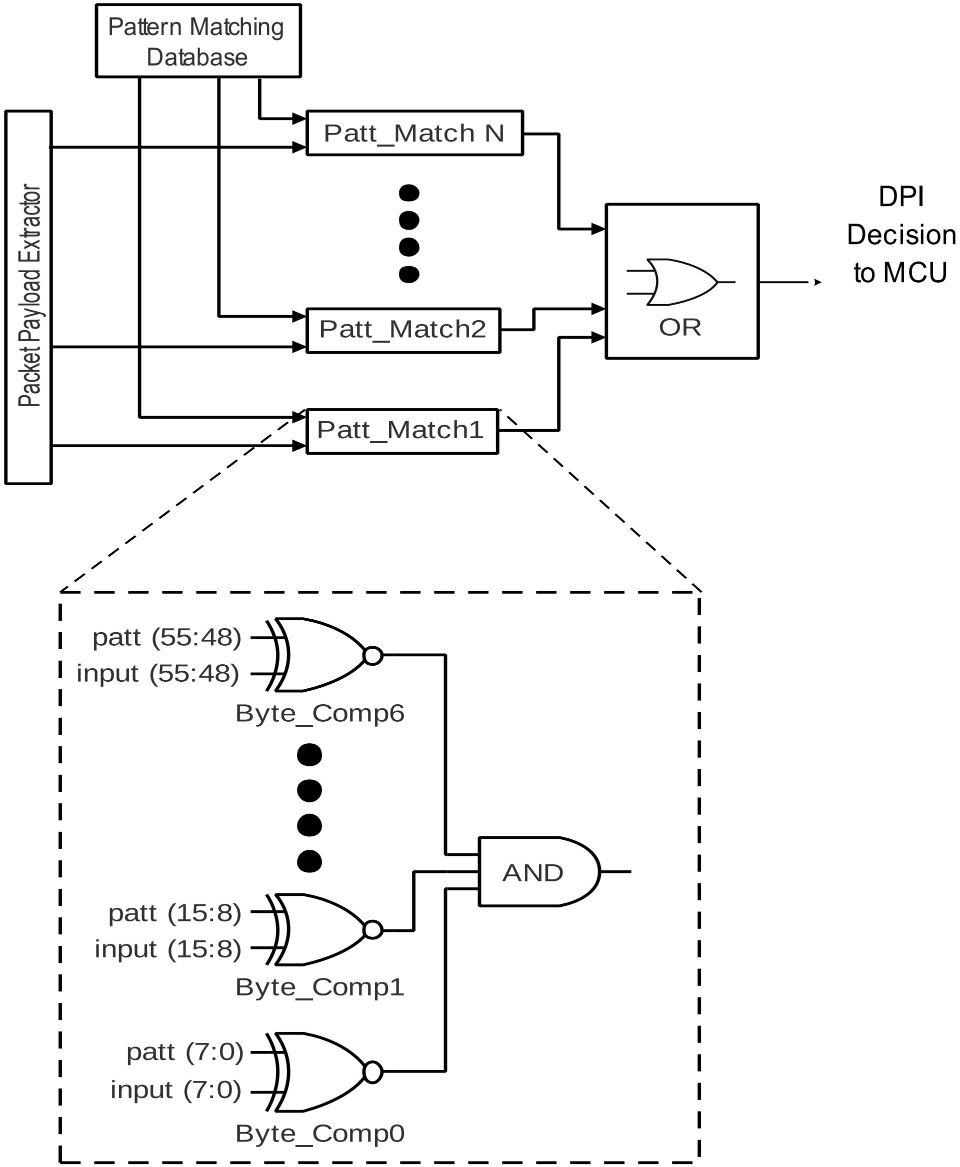
Packet Filtering Block Diagram



A	B	Out
0	0	1
0	1	0
1	0	0
1	1	1



Pattern Matching Block Diagram



4 Summary

- The human-system interface shall be protected by computer security measures that not adversely affect the safety functions of NPP I&C systems.

- The conceptual approach introduces FPGA-based solution to protect the gateway devices against potential cyberattacks or malicious actions. Such approach aims at improving and strengthening the interface between nuclear safety and security.

- Further work needed to develop the use of modern digital technologies like FPGAs in the field of nuclear safety and security.

Thank you for your attention!