Conceptual Design Approach to Implementing Hardware-based Security Controls in Data Communication Systems

Authors

Ahmad Salah Ibrahim, Jaecheon Jung

KEPCO International Nuclear Graduate School

Presented by

Ahmad Salah Ibrahim

Outline of the Presentation

1 Introduction

2 Methodology

3 Conclusion

4 Further Work

1 Introduction

- Data communication systems in APR1400 mainly encompass safety systems data network (SDN) and non-safety systems data communication and information network (DCN-I).

- Unidirectional gateways and data diodes are serving as network security zones allowing data transfer from the safety to the non-safety networks and block the reverse communication path.

- A computer-based gateway server is to transfer safety parameters data to MCR for monitoring and display.

- Potential cyberthreats or malicious actions, if initiated from DCN-I network, may compromise the gateway server availability or data integrity.

- The main objective of this work is to implement network cybersecurity access controls to maintain the data availability and integrity for monitoring and display processes in the MCR.

- Design is systematically approached by conducting reverse and re-engineering processes.

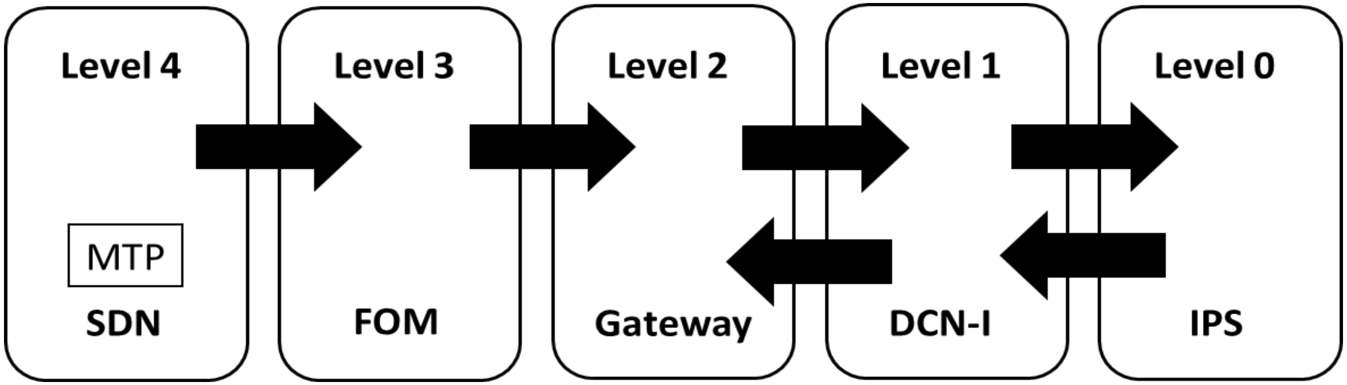
2 Methodology

Stakeholders Needs and Problem Definition

- **K-URD, Ch. 10, Sections 4 and 5**: Requirements for data availability and reliability (integrity) for computer-based facilities (e.g., MCR operators aid)
- **ICS-CERT**: In 2015, received and responded to 295 cyber incidents. 22 of these incidents were observed as high-level intrusion that infected critical systems.
- **Problem**: Loss of View (LOV) may result from a potential denial-of-service (DoS) attack.
- **Needs**: A robust gateway server against cybersecurity issues to maintain monitoring and display data transmission.

Regulatory Requirements

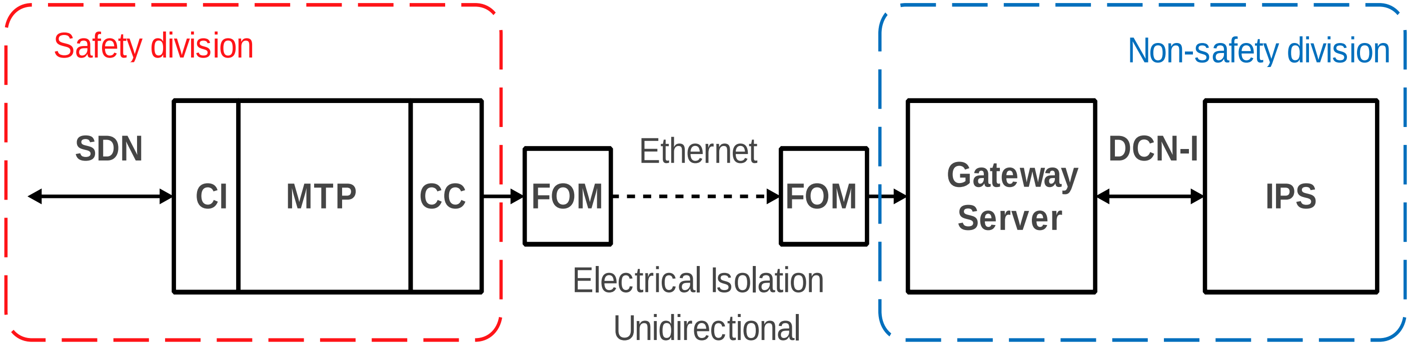
U.S.NRC 10 CFR 73.54 and RG-5.71



- Safety-related systems, if compromised, would adversely impact the safety functions, are allocated at levels 4 and 3 (Only one-way communication)

- Digital I&C safety systems are physically protected from any cyberattack may be initiated from the non-safety network.

- The current data network architecture does not implement security access controls between DCN-I and the redundant safety channels gateway servers.
- Gateway server data traffic depends on cyclic redundancy check (CRC) algorithm for data error detection and correction.



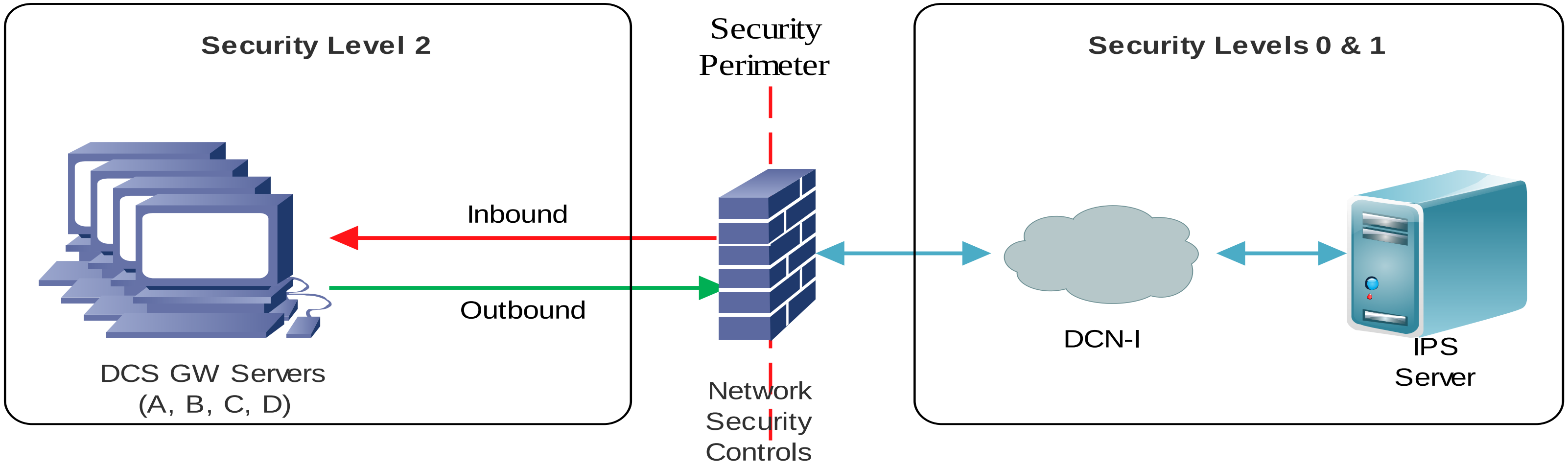
CI: Communication interface card
CC: Communication card (Ethernet)
FOM: Fiber-optic Modem

System Requirements

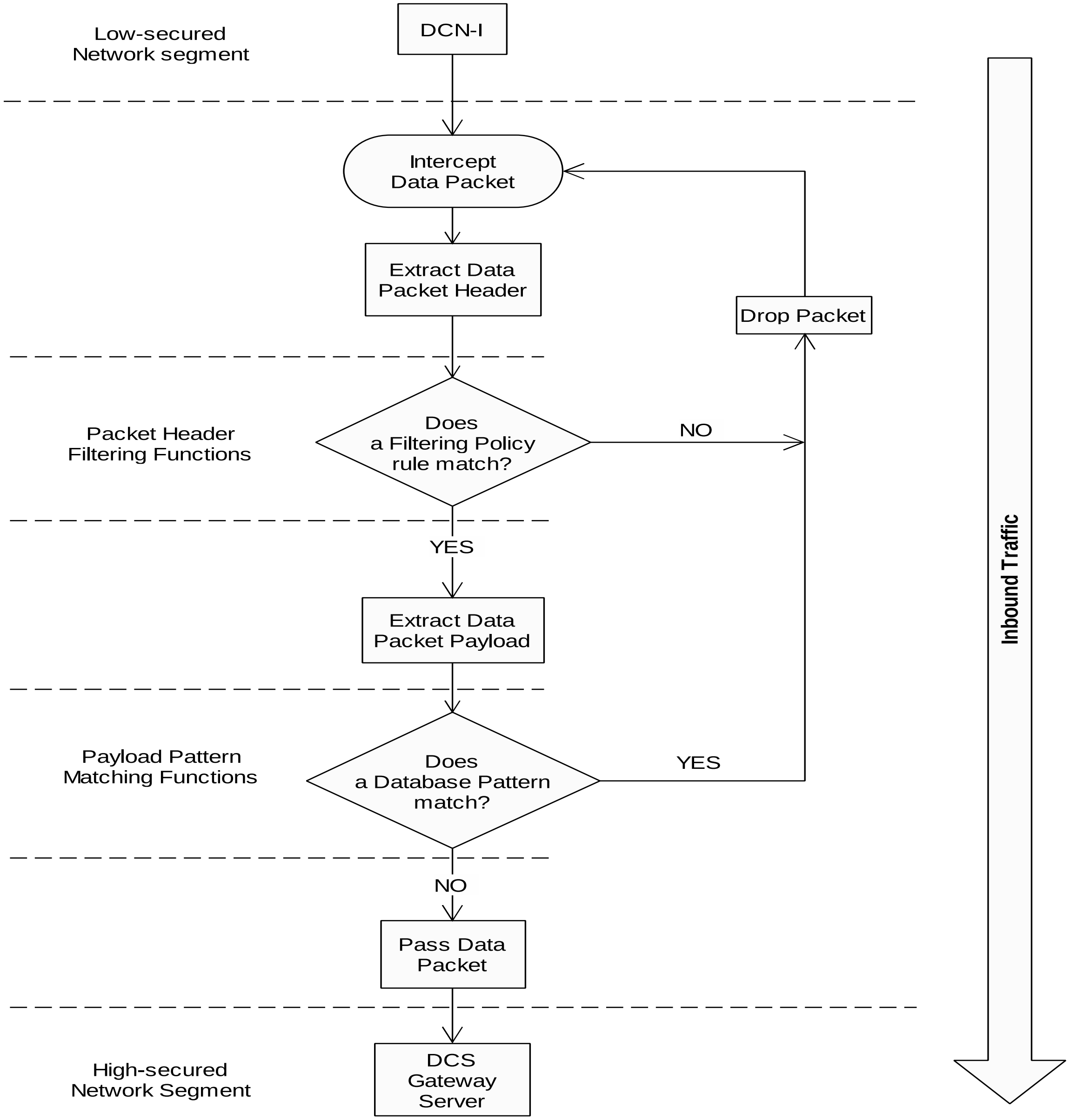
- **NEI 08-09 Standard**: Real-time malicious code protection mechanisms are established at security boundary device entry and exit points on the network to detect and eliminate malicious code resulting from:
  - Data communication between systems.
  - Exploitation of systems vulnerabilities.

- **NERC-CIP-005 Standard**: Both firewall filtering functions and NIDS/NIPS functions are used to implement security devices between zones.

Design Concept



- Establishing a Security perimeter between the DCN-I Subnetwork and redundant safety channels gateway servers to implement cybersecurtiy access controls to control and manage the inbound data traffic (On-demand traffic).



Low-secured Network segment

DCN-I

Intercept Data Packet

Extract Data Packet Header

Drop Packet

Packet Header Filtering Functions

Does a Filtering Policy rule match?

NO

YES

Extract Data Packet Payload

Payload Pattern Matching Functions

Does a Database Pattern match?

YES

NO

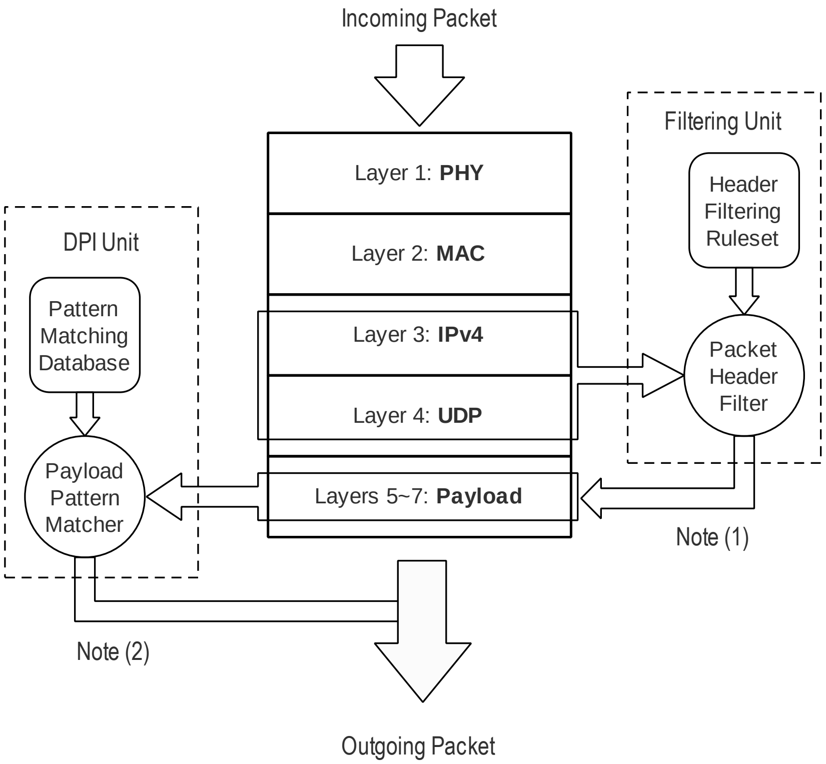
Pass Data Packet

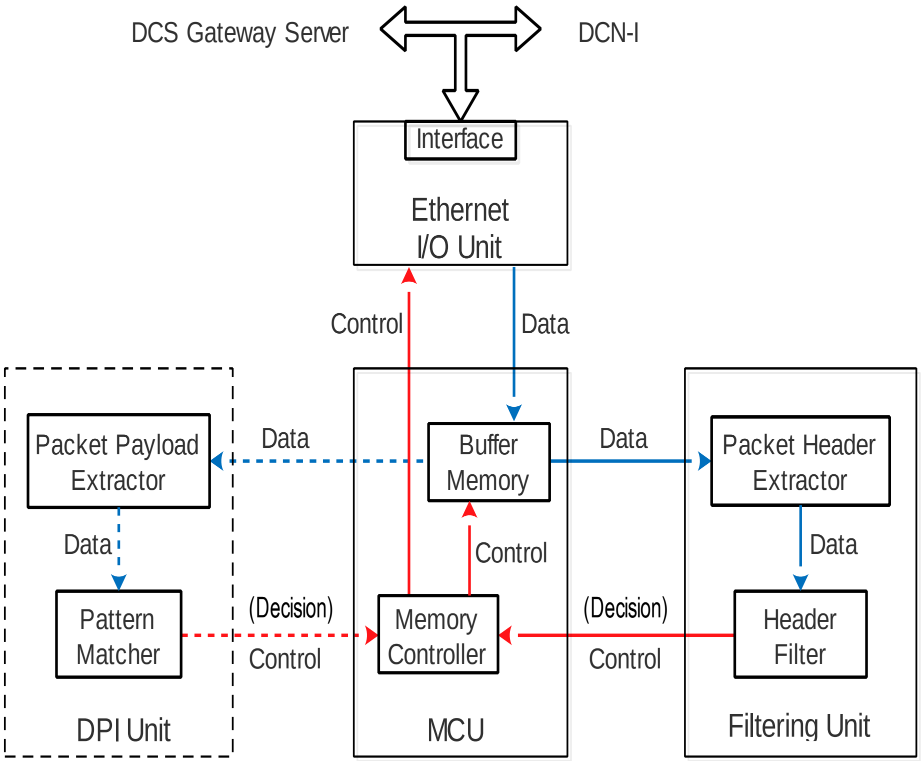
High-secured Network Segment

DCS Gateway Server

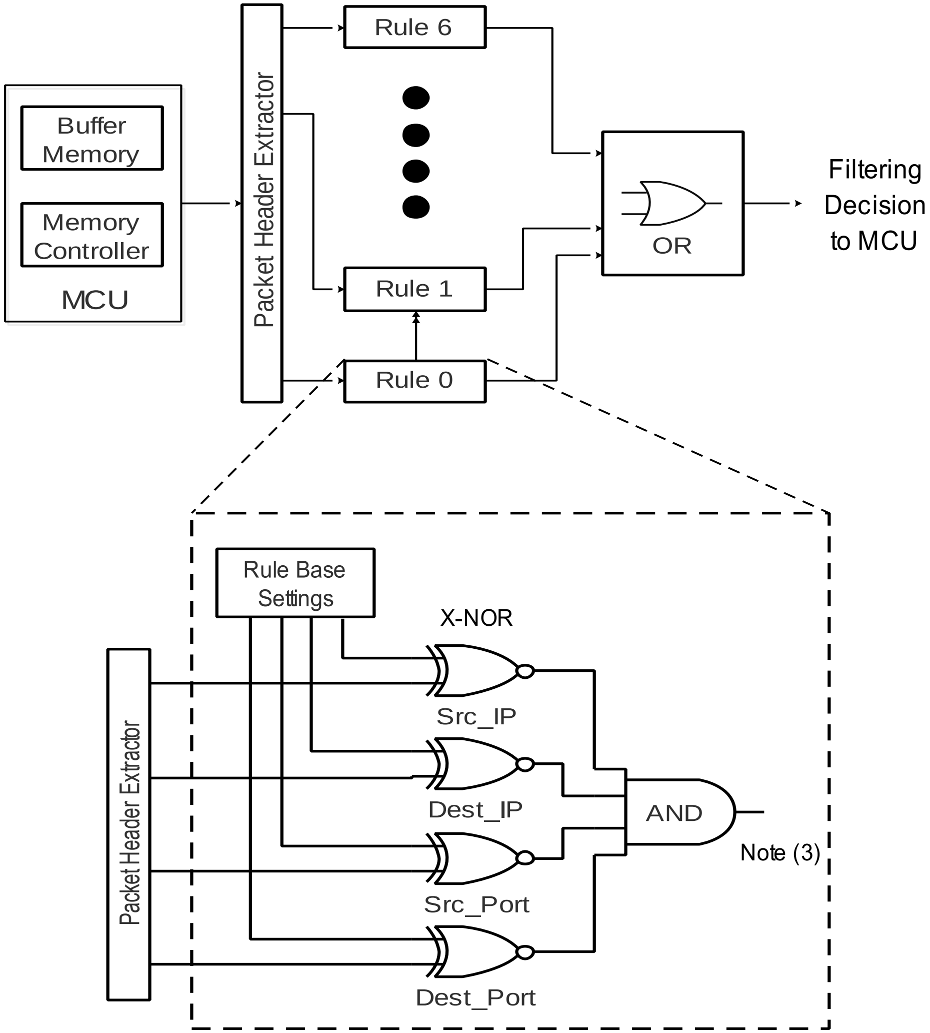
Inbound Traffic

Security Controls Block Diagram

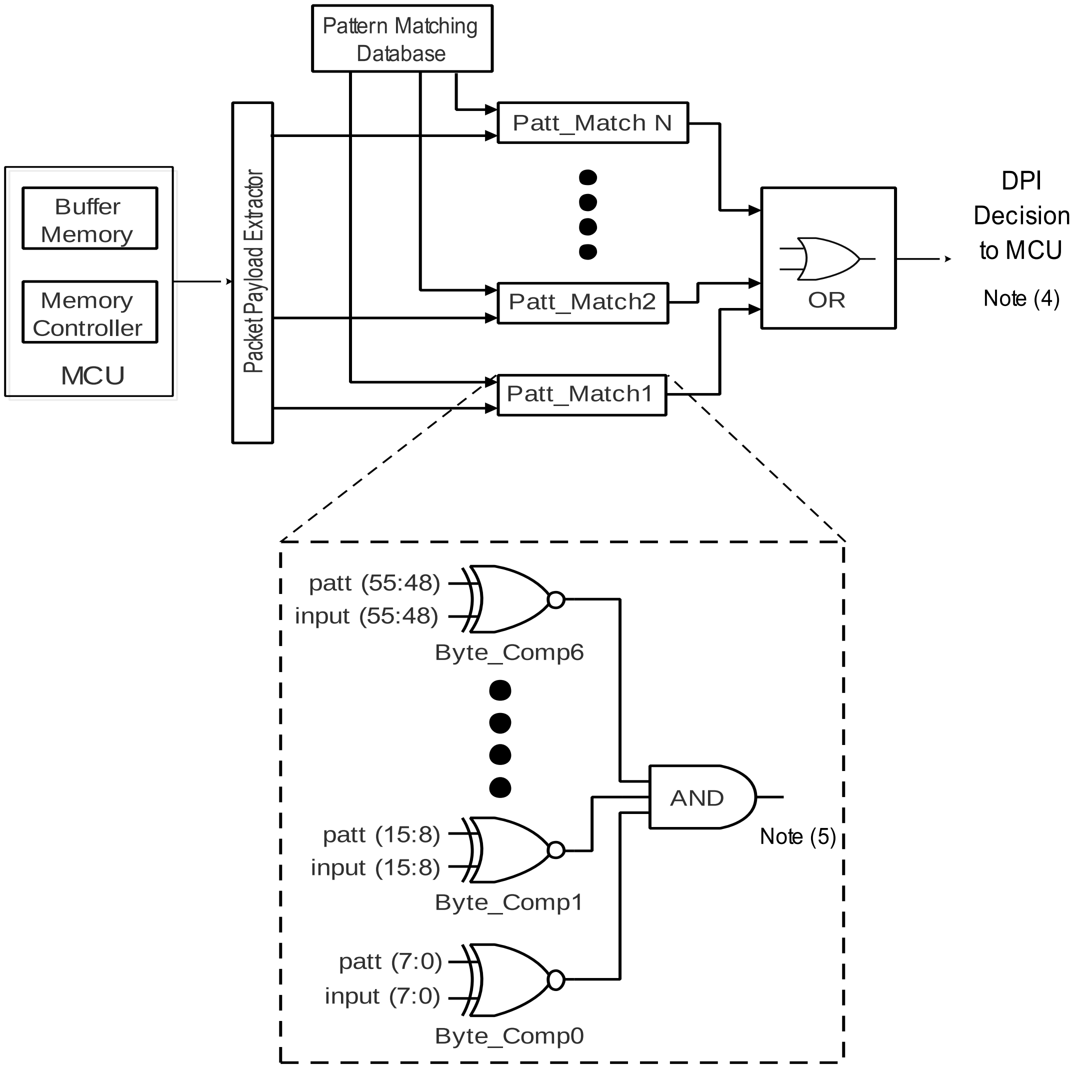




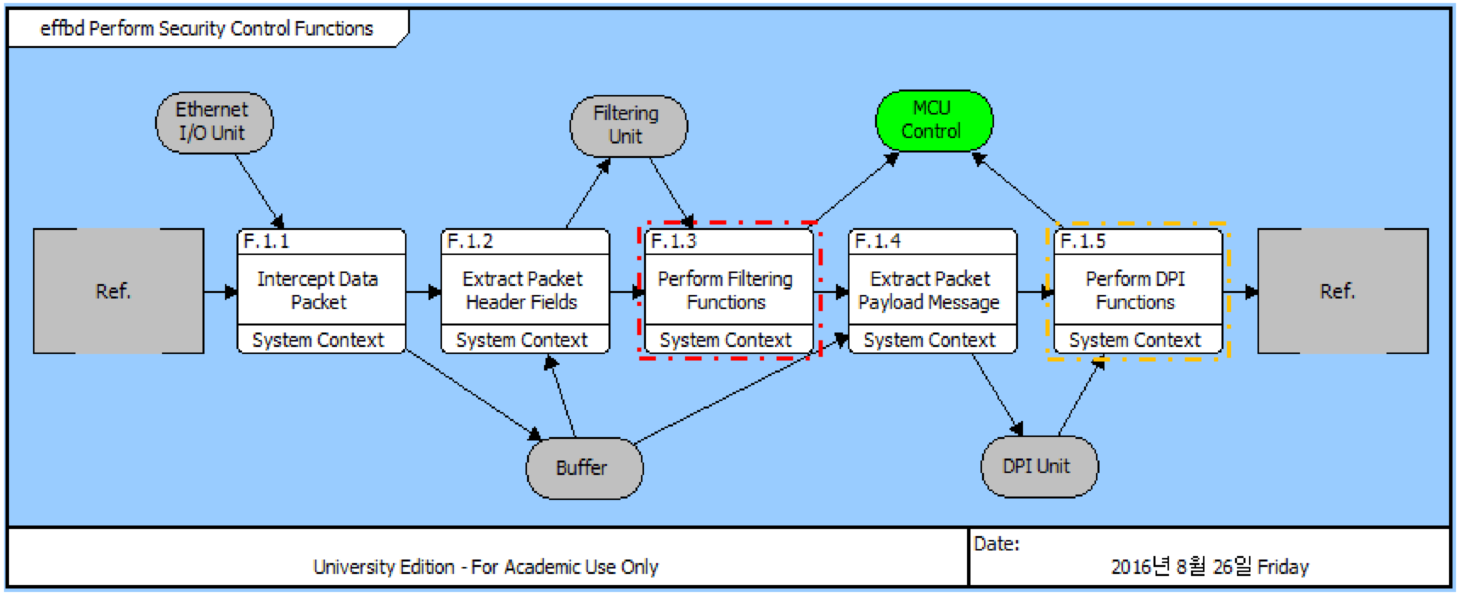
Packet Filtering Block Diagram



Pattern Matching Block Diagram



Functional Flow – EFFBD Model



effbd Perform Security Control Functions

Ethernet I/O Unit

Filtering Unit

MCU Control

Ref.

F.1.1 Intercept Data Packet System Context

F.1.2 Extract Packet Header Fields System Context

F.1.3 Perform Filtering Functions System Context

F.1.4 Extract Packet Payload Message System Context

F.1.5 Perform DPI Functions System Context

Ref.

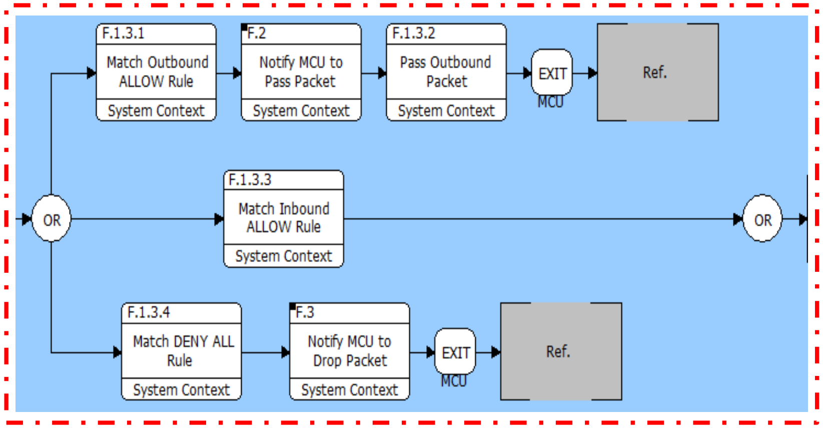
Buffer

DPI Unit

University Edition - For Academic Use Only

Date:

2016년 8월 26일 Friday



F.1.3.1 Match Outbound ALLOW Rule System Context

F.2 Notify MCU to Pass Packet System Context

F.1.3.2 Pass Outbound Packet System Context

EXIT MCU

Ref.

OR

F.1.3.3 Match Inbound ALLOW Rule System Context

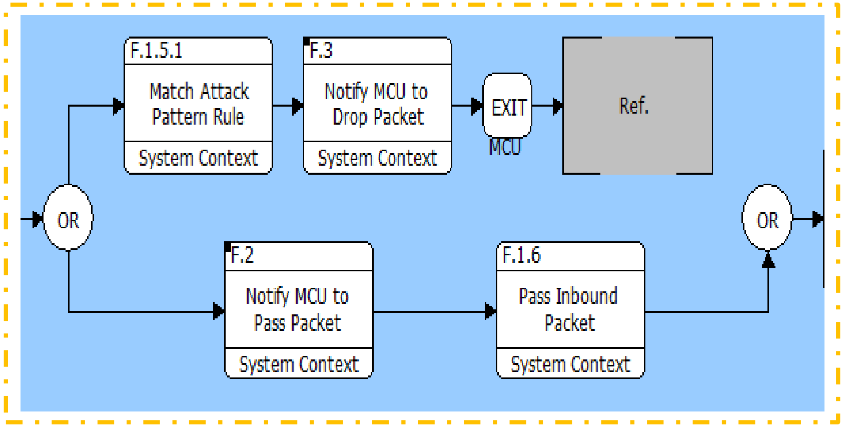
OR

F.1.3.4 Match DENY ALL Rule System Context

F.3 Notify MCU to Drop Packet System Context

EXIT MCU

Ref.



F.1.5.1 Match Attack Pattern Rule System Context

F.3 Notify MCU to Drop Packet System Context

EXIT MCU

Ref.

OR

F.2 Notify MCU to Pass Packet System Context

F.1.6 Pass Inbound Packet System Context

OR

3 Conclusion

- Design concept of hardware-based cybersecurity controls is defined and functionally modelled in this work.
- Design is systematically approached by conducting reverse and re-engineering processes to define the design requirements and concept. Known cyberattacks patterns are the limitation for this study.
- Data system availability and integrity are the measures for this study.
- Hardware-based security controls are to provide robustness and immunity for targeted data systems against potential cyberattacks or malicious actions.
- Data packet filtering and deep inspecting functional flow is verified by EFFBD modelling.

4 Further Work

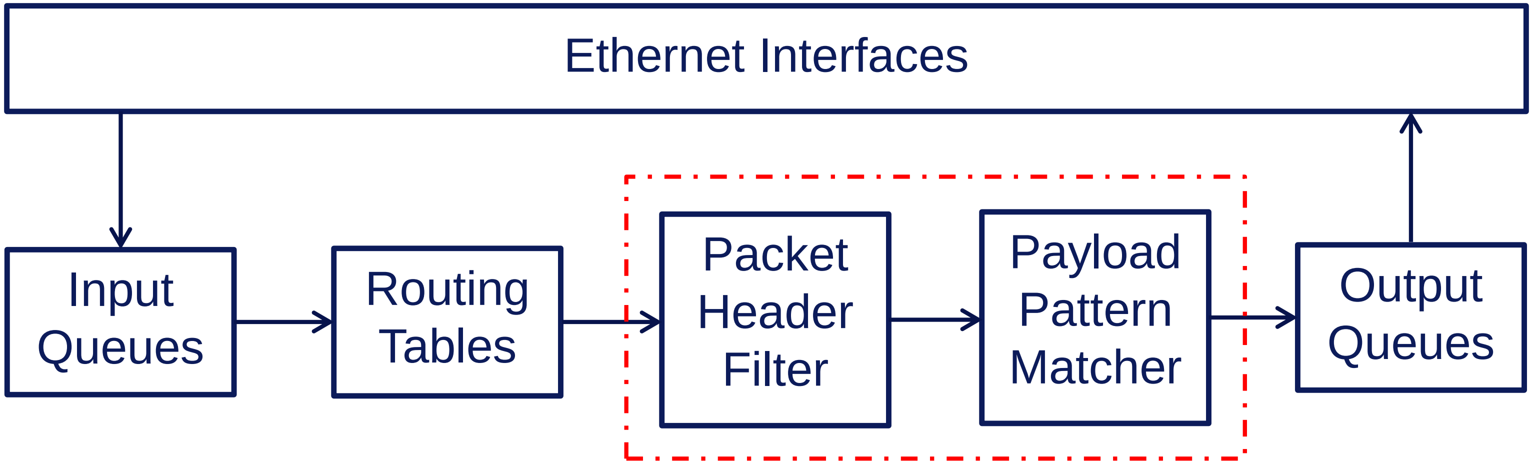
Design verification (In progress…)

- Data packet filtering and DPI functions are being verified by testing and simulation using Xilinx ISE ModelSim Simulator.
- Verification depends mainly on schematic design to model and simulate the cybersecurity control functions.

Design Validation

- Design will be validated by configuring an FPGA board using HDL code and test it in a network-based environment.
- Denial-of-Service (DoS and DDoS) attack is one of the major cyberthreats to data systems availability and integrity.

- NetFPGA technology is recommended to accomplish the V&V of this design.
- The reference code can be reconfigured and the Filtering/DPI functional modules can be inserted between the routing tables outputs and output queues.



Thank you for your attention