11TH INTERNATIONAL CONFERENCE
ON CRITICAL INFORMATION
INFRASTRUCTURES
SECURITY

10-12 October 2016
UIC HQ Paris

CRITIS
2016

# Security Validation for Data Diode with Reverse Channel

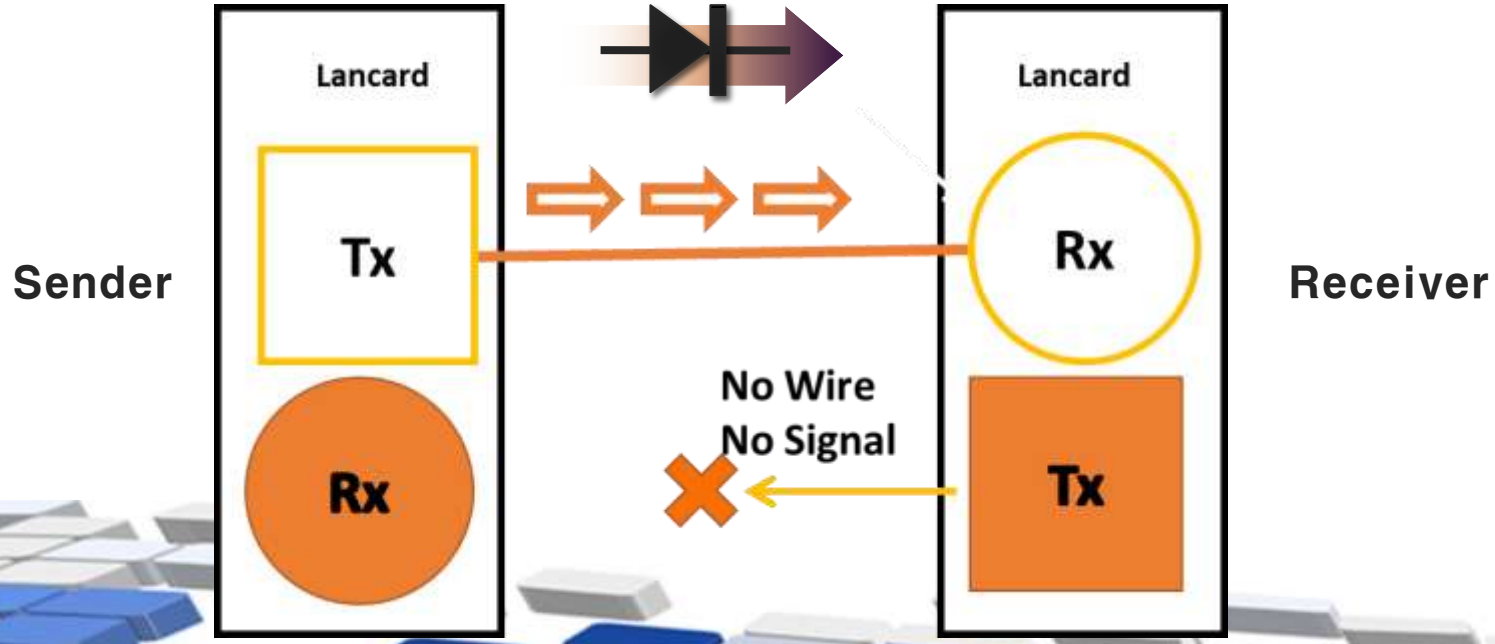
**Jeong-Han Yun**, Yeop Chang, Kyoung-Ho Kim,
and Woonyon Kim

*National Security Research Institute, Korea*

NSR
National Security Research Institute

# Data diode

- Data diode or Unidirectional security gateway
  - No line to send data reversely
  - Bug safe: Vulnerability is less critical than that of firewalls
  - Mistake safe: Configuration error is less critical than that of firewalls
- It is recommended in many ICS security guidelines



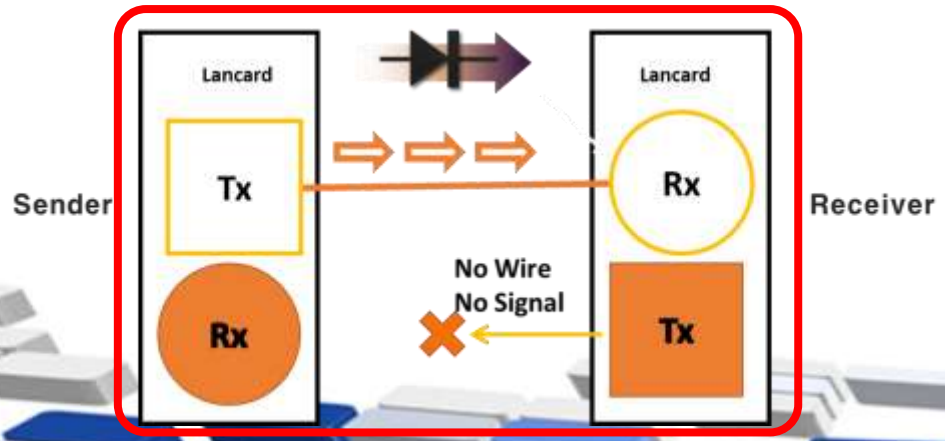

Owl

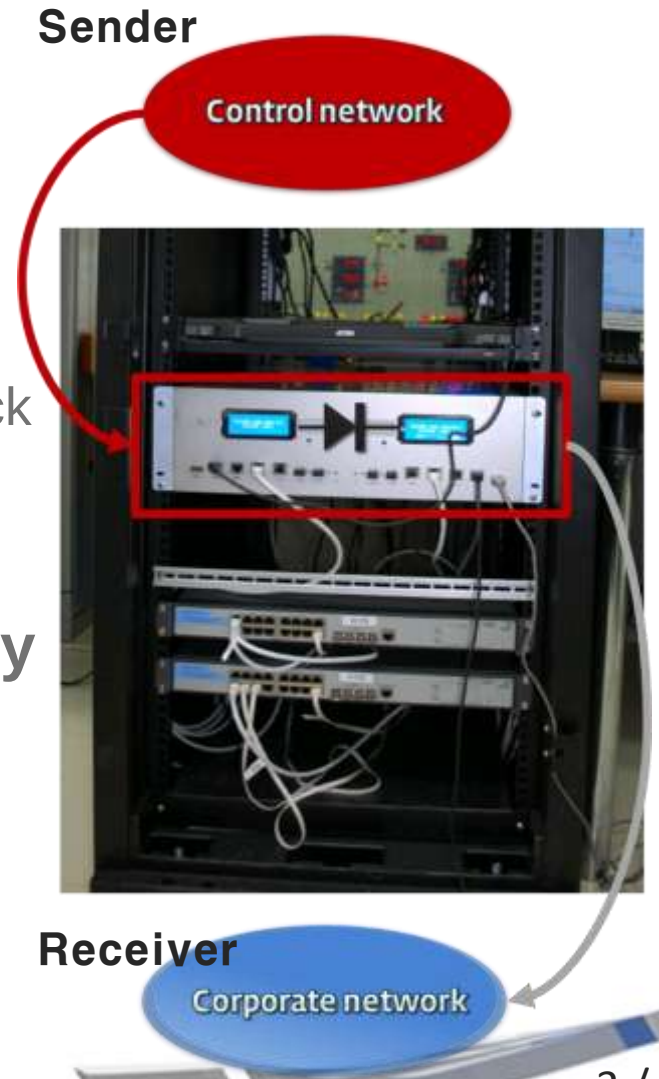
Waterfall

NNSP

# We implemented a data diode

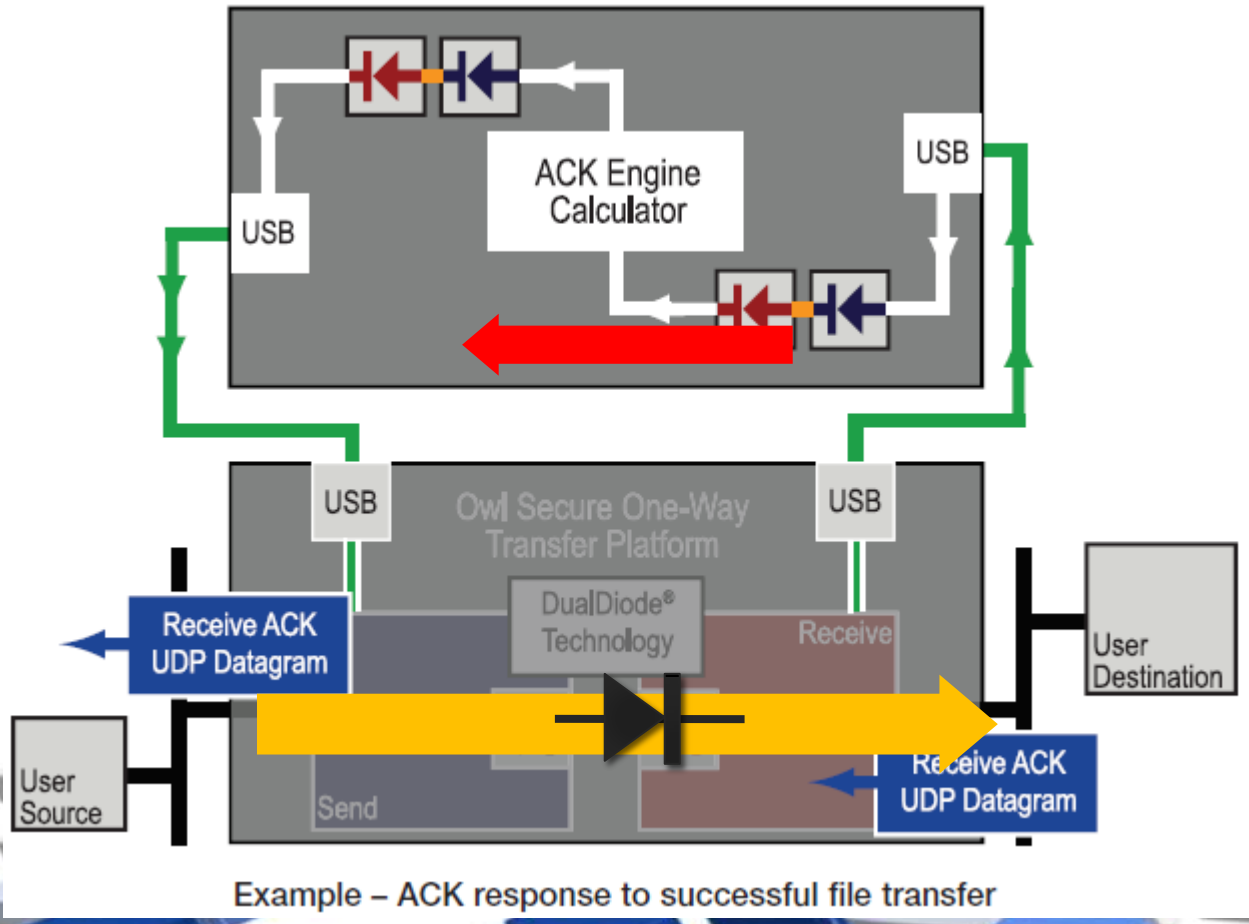
- Some critical infrastructures cannot apply data diodes
  - Dislike to open internal information to other companies
  - Not enough money
- Field operators complained
  - Uncertain : Sender cannot sure data transfer success due to No-Ack
  - Inconvenient : Sender cannot check status of receivers
  - Inflexible : Receiver cannot request anything (when and what)
- To solve all the complaints, **reverse channel is necessary**



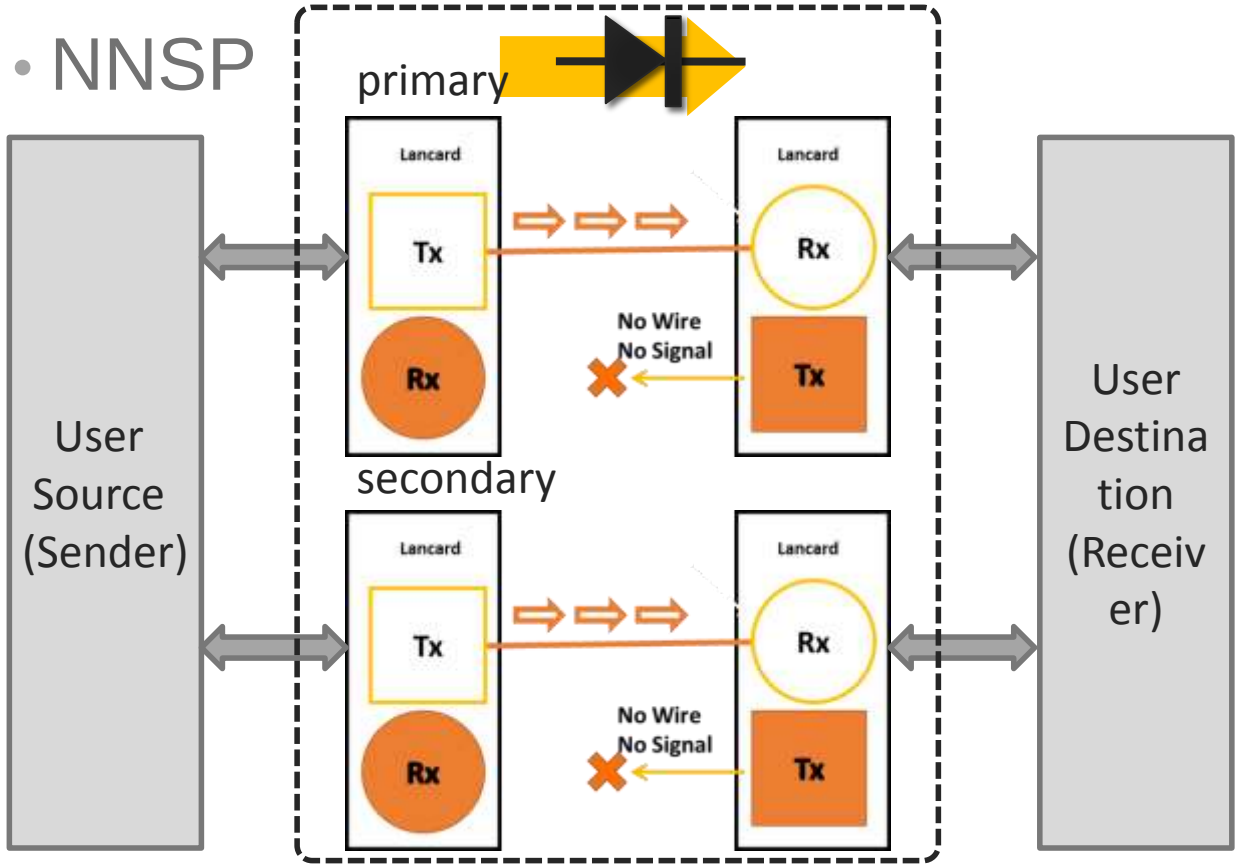
# Data diode with reverse channel

- Owl Secure Ack Engine




Example – ACK response to successful file transfer

- NNSP



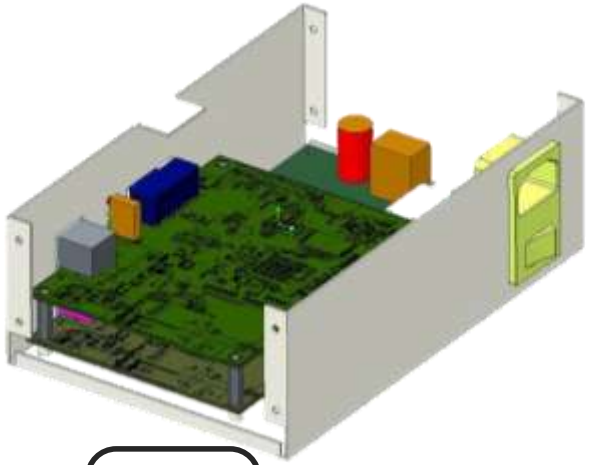

Send data through primary line.
If received data has problems, primary line is disconnected
Retransmit data (buffer) through secondary line

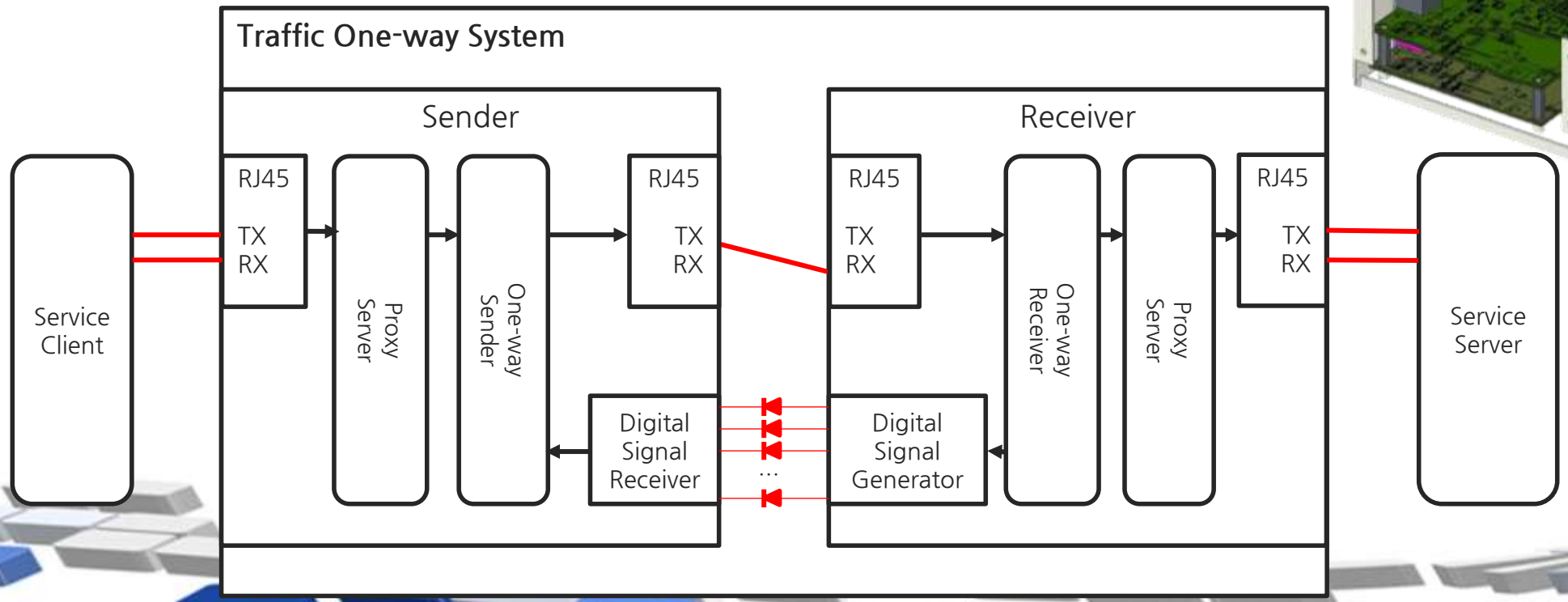
# Data diode with reverse channel? Conflict

- **Data diode with reverse channel** can be used for critical infrastructure?
- We need more detail security analysis
  - ICS security guidelines just say ‘hardware-based data diode’
  - Each area of critical infrastructure has different security level and characteristic
  - If data diode with reverse channel may satisfy security requirements of an area?
- In our work,
  - We implement a data diode with reverse channel
  - We propose its security requirements on an application environment
  - And we validate the requirements by unit/integration/system testing

# TOS : Light data diode with reverse channel

- TOS : Traffic One-way System
  - Cut the Sender's RX line for one-way data transmission
  - Embedded board, ARM 720MHz, 100 Mbps
  - Reverse channel : 8 digital lines

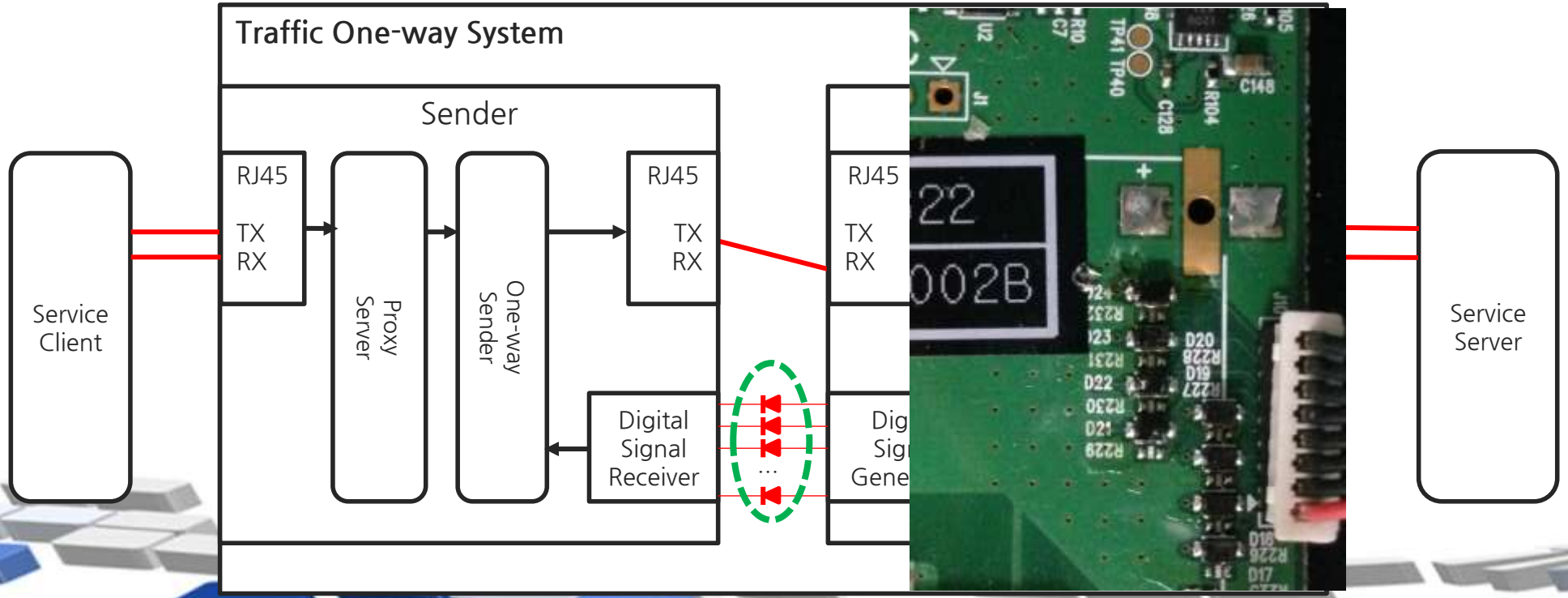




# Reverse Channel

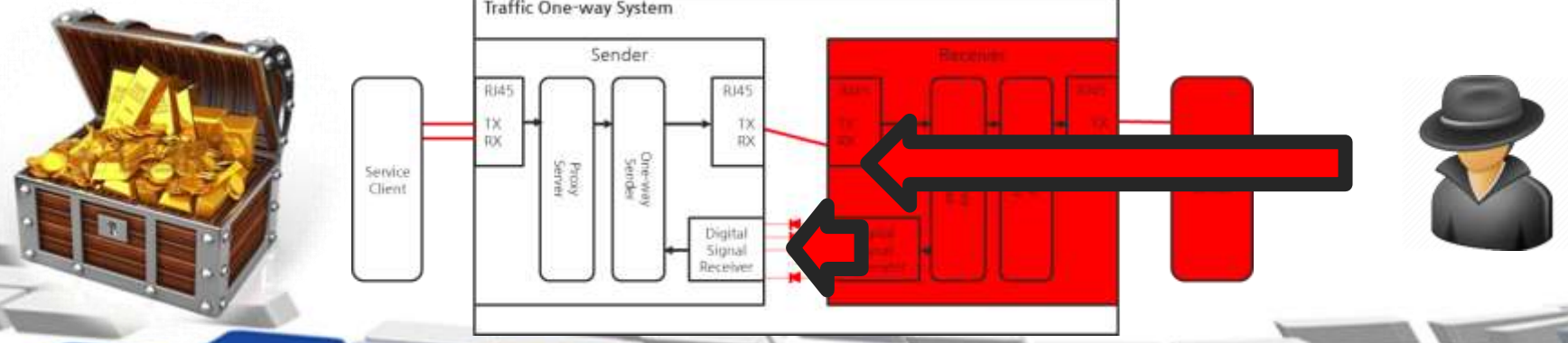
- One-way : Diode installed
- Functions
  - Data acknowledgement
  - Monitoring Receiver's status

| Pin No. | Description (System code) | Pin No. | Description (Error code) |
|---|---|---|---|
| 1 | Rx Node power-on/off | 5 | Storage is available |
| 2 | Rx Node network status | 6 | Storage is almost full |
| 3 | Feedback | 7 | Same file exists already |
| 4 | N packet acknowledgment | 8 | Reserved |

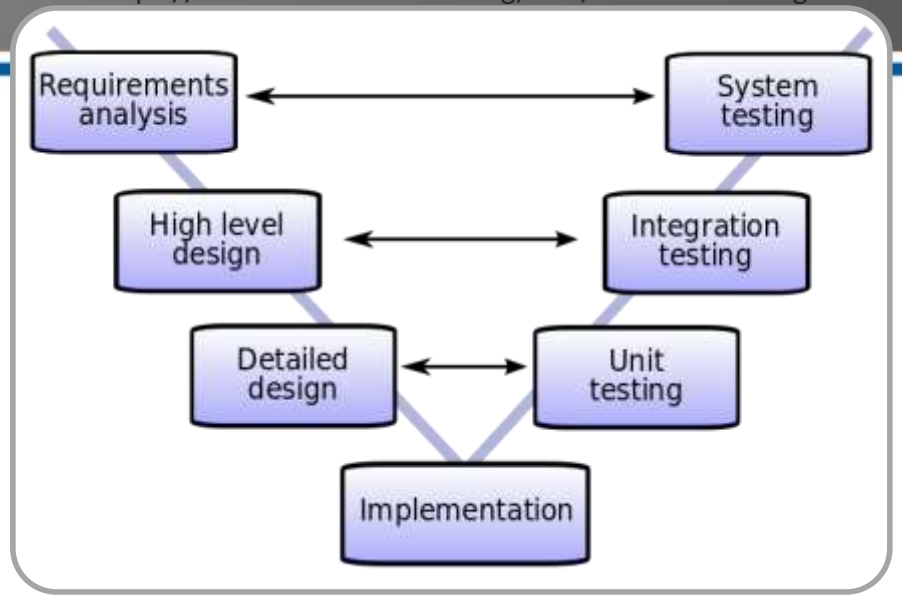


# Application Environment

- Assumptions
  - TOS locates in a safe place
  - TOS must block remote attacks from outside (receiver) network
- Attacker
  - 1. The attacker cannot physically access TOS
  - 2. The attacker can access to the TOS receiver over the network
  - 3. The attacker can take control of the TOS receiver
- Security requirements of TOS
  - 1. (Data) When the sender receives information from the TOS reverse channel, the sender does not store the information in the files
  - 2. (Command) Although any information is sent through the TOS reverse channel, the sender performs only the predefined functions of sender (Section 3.2 in our paper)

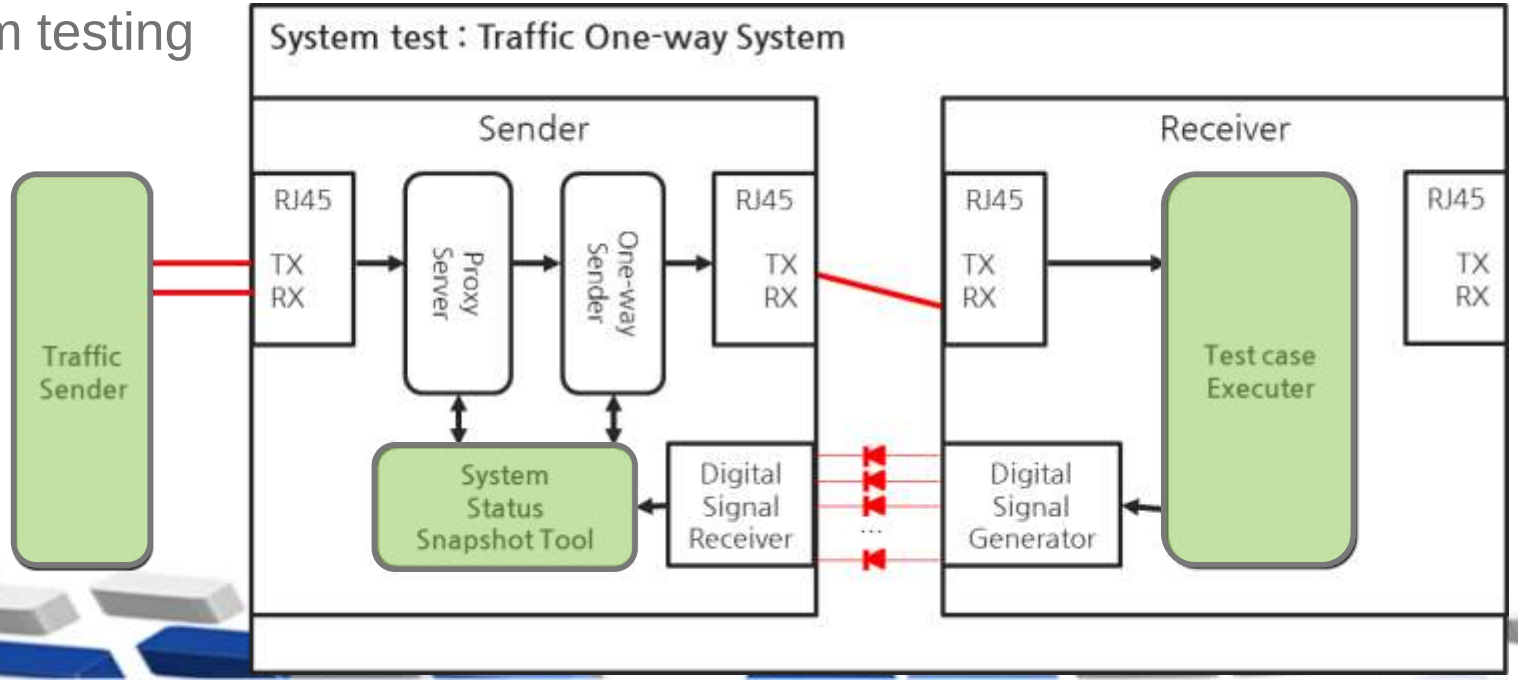


https://commons.wikimedia.org/wiki/File:V-model.svg



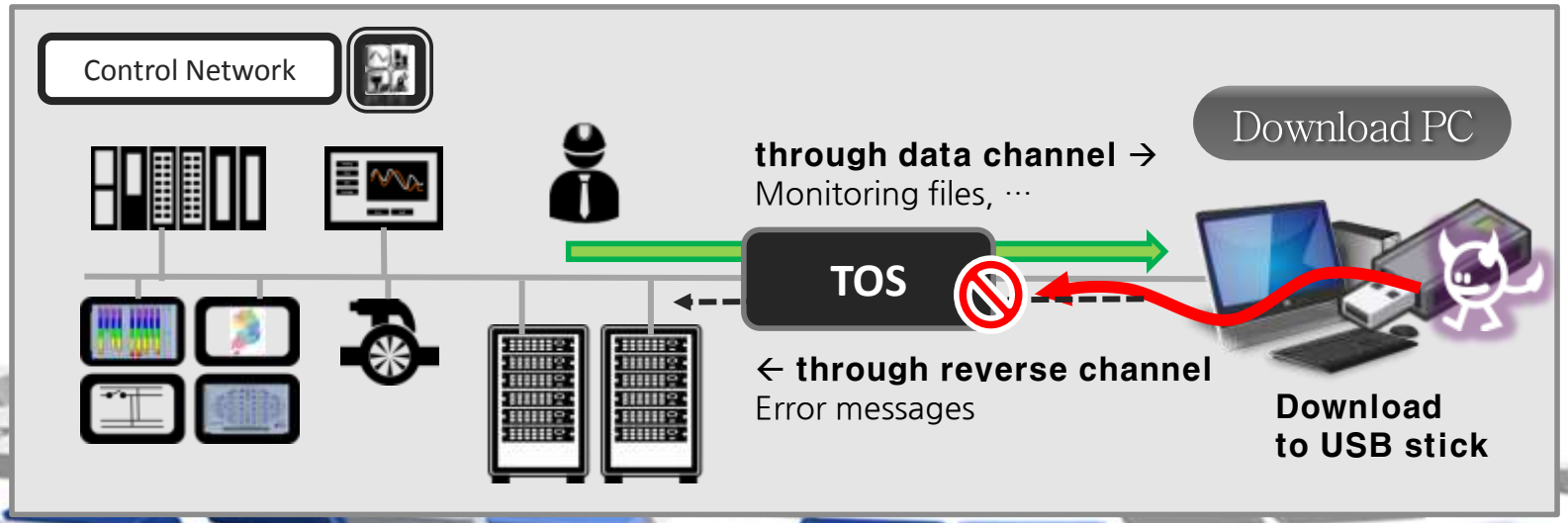

# Validation

- Unit / integration testing
  - Code spec : Code review, design specification
  - Test case generation for 100% statement/branch coverage
- System testing
  - Using pairwise-generation technique to cover all possible situations
  - 3 days random testing



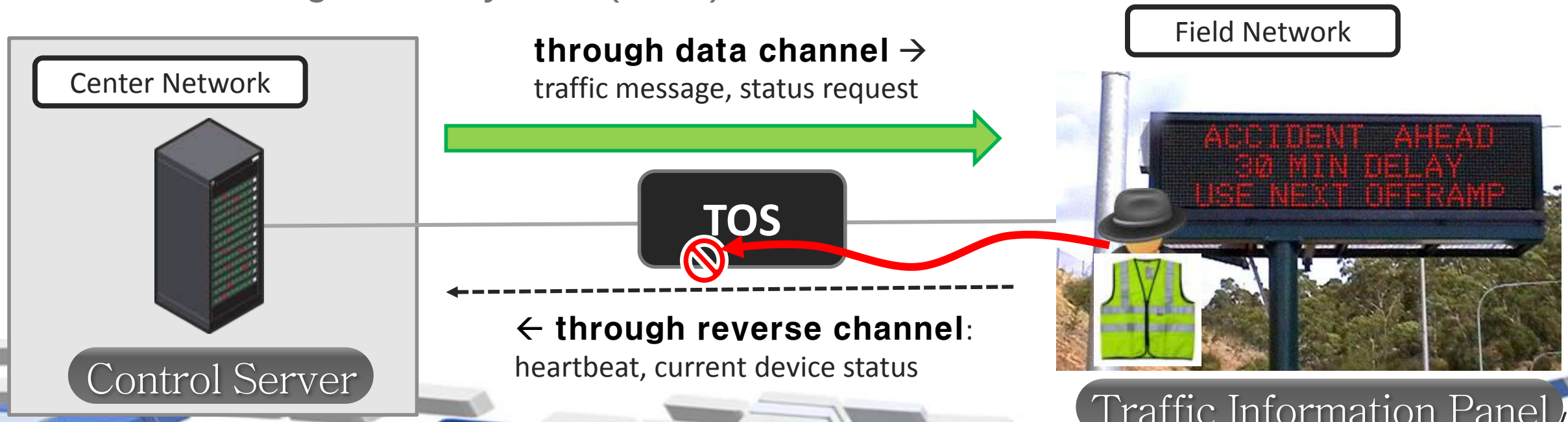
# Field test : Safe USB memory usage

- Motivation
  - Operator should occasionally move files of a control system to business network
  - Portable device is forbidden in the control system
  - SW-based media security solution cannot be installed to control system
- File download through USB memory stick
  - Although USB memory stick is compromised, the malware cannot penetrate the rest
  - Running on two sites



# Application for Data Sender

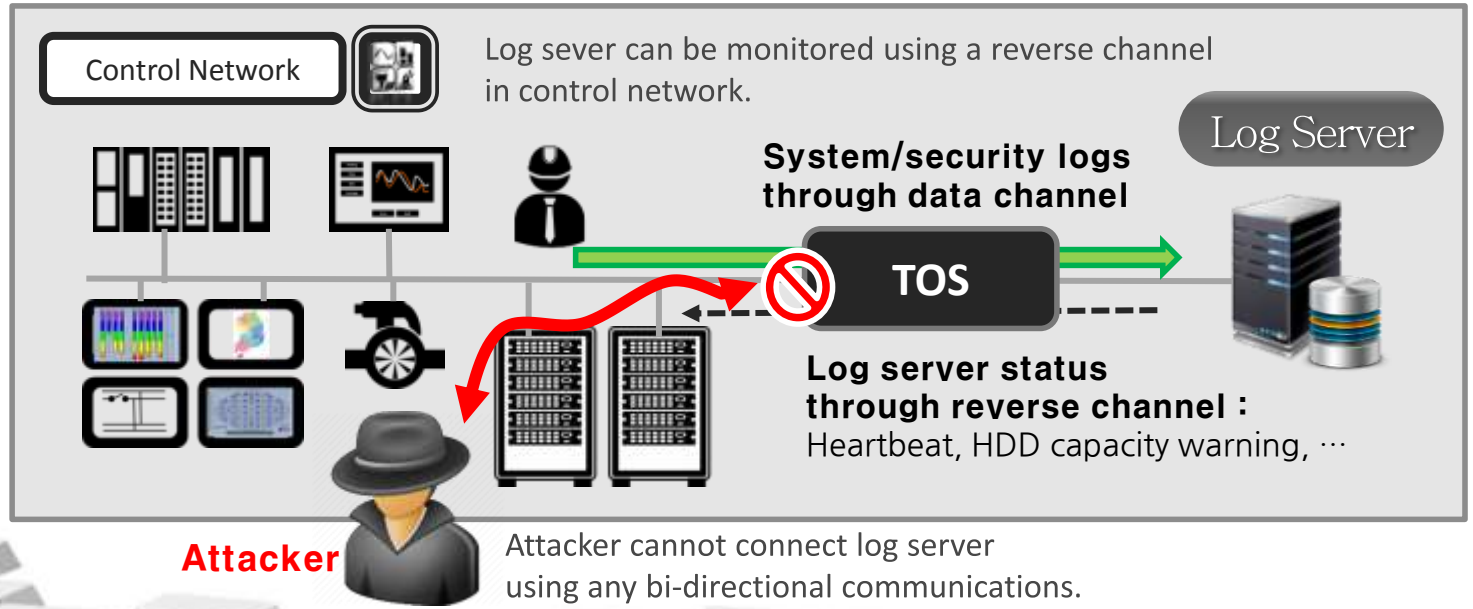
- Variable Message System (VMS)
  - Manager sends messages to field panels
  - Manager can check predefined information : the status of field panels
  - Attacker in field cannot penetrate center network
- Patch Management System (PMS) is a similar case




http://www.roadtraffic-technology.com/projects/adelaide-crafers-highway/adelaide-crafers-highway1.html

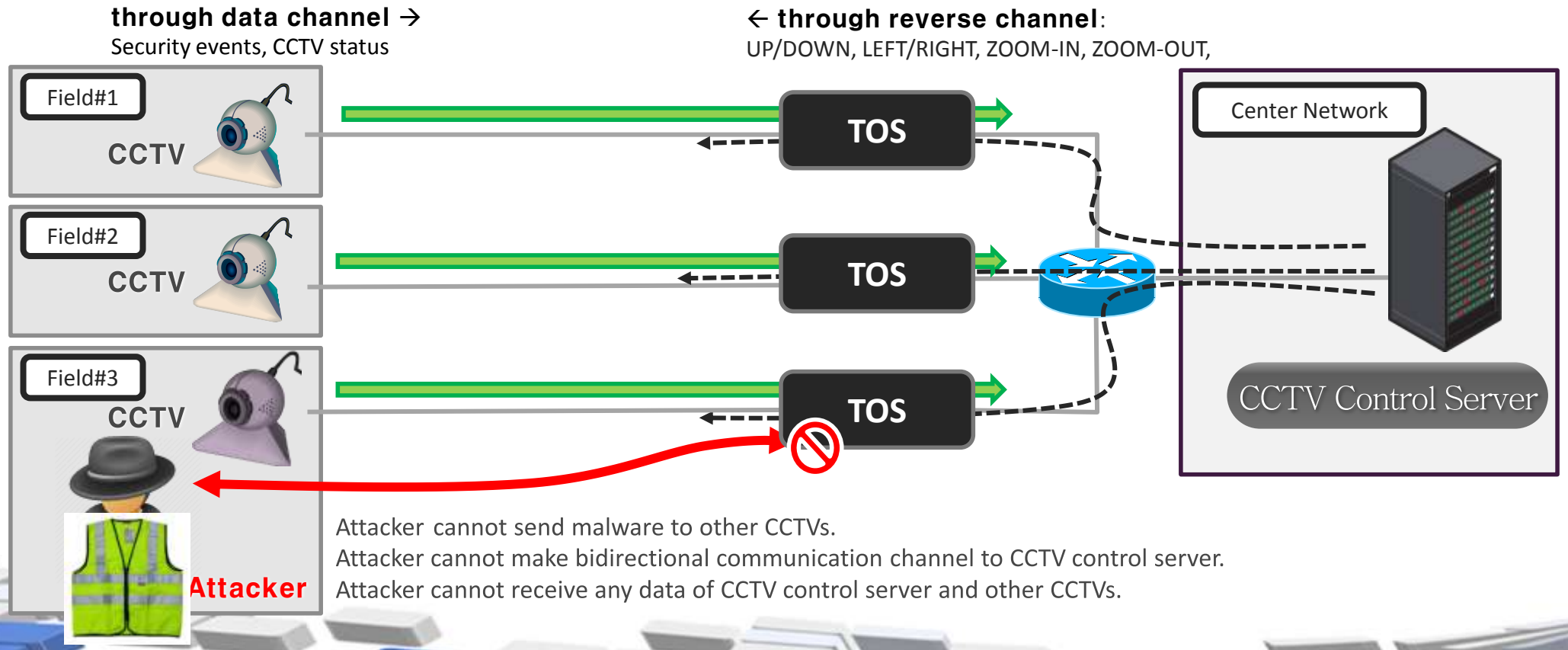
# Application for Data Receiver

- Log server
  - In control network, log server only receives log data from all systems
  - Manager in control network can check the log server status
  - Manager (or attacker) cannot modify existing logs
    - Logs can be used for auditing



# Application for Data Receiver

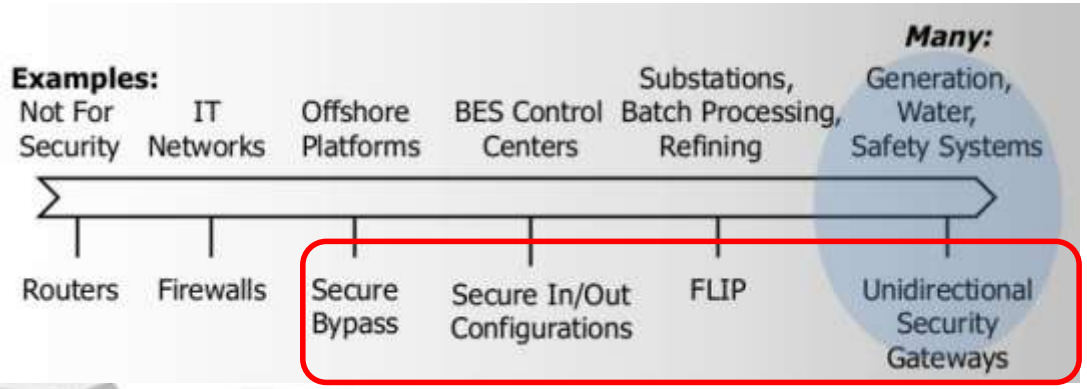
- CCTV
  - Attacker in field cannot penetrate control server and other field devices




Attacker cannot send malware to other CCTVs.
Attacker cannot make bidirectional communication channel to CCTV control server.
Attacker cannot receive any data of CCTV control server and other CCTVs.

# Conclusion

- Physical one-way data transfer is a powerful security solution, but
  - Uncertain : Sender cannot sure data transfer success due to No-Ack
  - Inconvenient : Sender cannot check status of receivers
  - Inflexible : Receiver cannot request anything (when and what)
- Restrictive reverse channel can be applied to some areas
  - Strong and user-friendly solution in an application environment
  - Needs specific security requirements and validation for each part in critical infrastructures




**Variants of data diode**

http://www.slideshare.net/dgpeters/8-ginter114-30733484