# Communication Architecture and Security Issues for Distribution Automation Systems

July 8, 2008

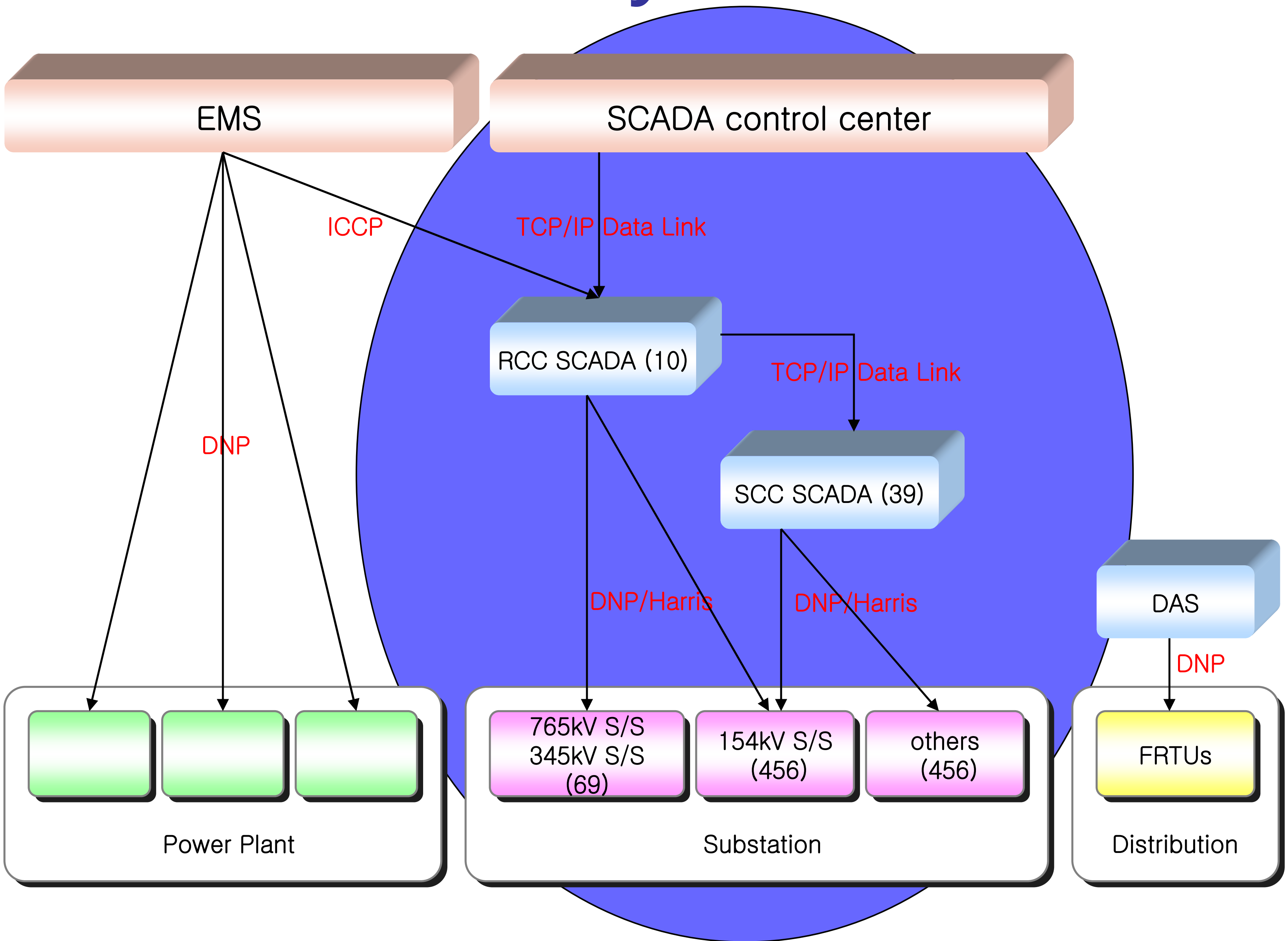
Myongji University

Sugwon Hong

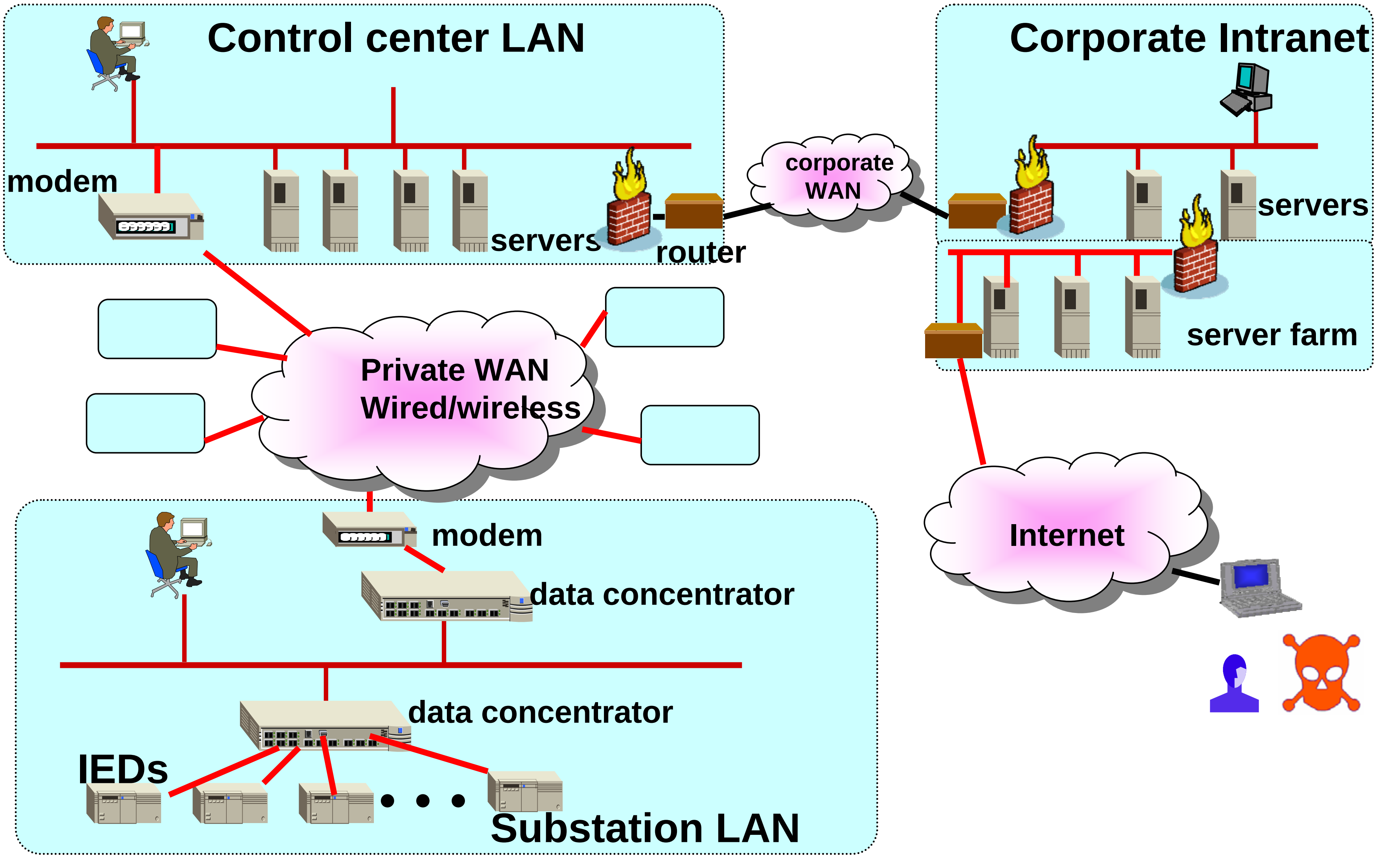
# In this presentation

- Communication networks for the SCADA system and distribution automation system.
- Security Issues
  - Cyber threats
  - Security protocols
- Comments

# KEPCO SCADA system



# SCADA network



# Conventional wisdom

- There are two reasons why cyber security risks in the SCADA system are claimed to be facts not myths.
  - One is that the SCADA system doesn't reside on a physically separate, standalone network.
  - The other is that the SCADA network is more relying on the open standard communication protocols, especially TCP/IP.

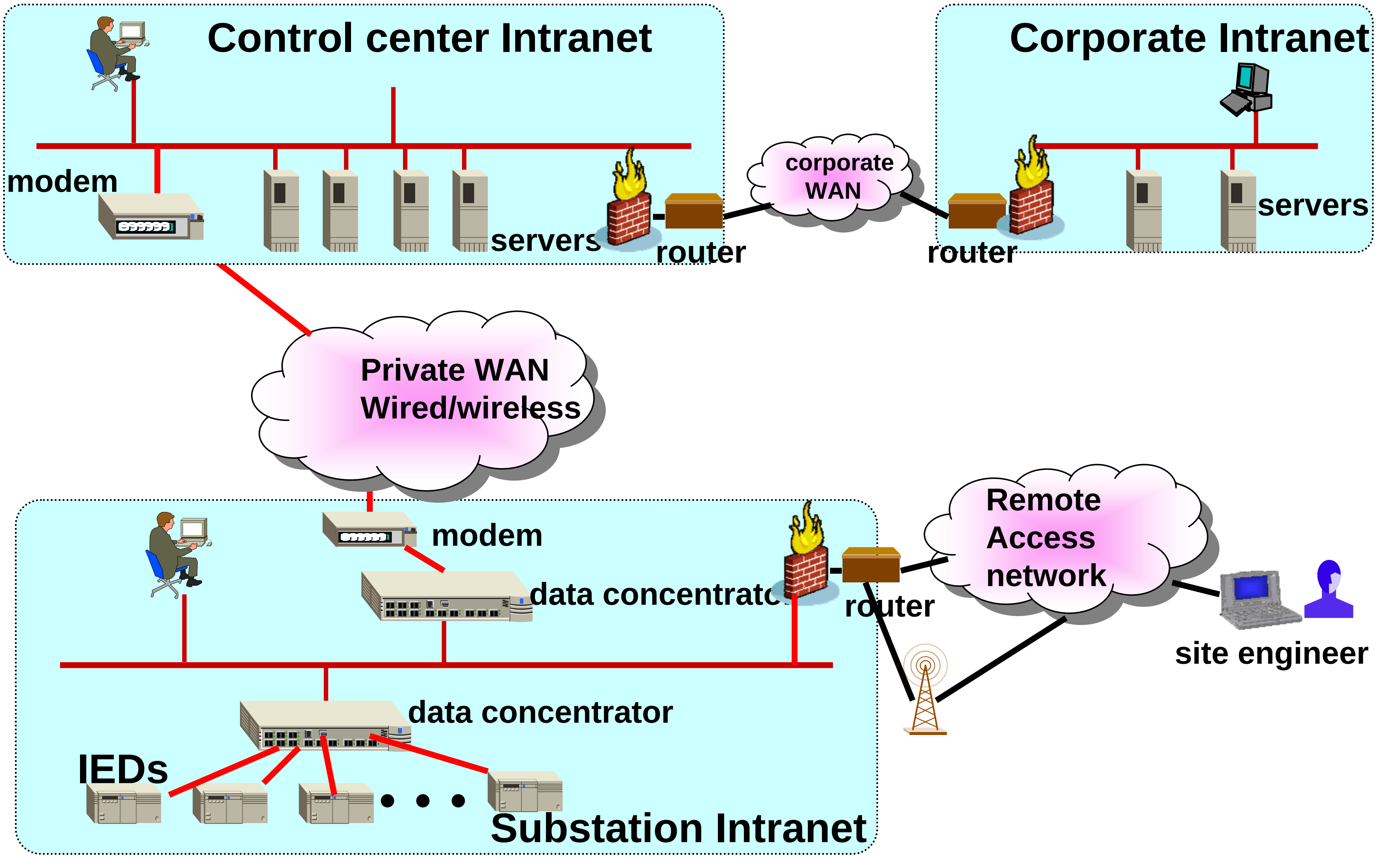
# Caveat

- "The distinct trend within the industry is to link the systems to access control center data necessary for business purposes. One utility interviewed considered the business value of access to the data within the control center worth the risk of open connection between the control center and the corporate network." (Kevin Poulsen, Security focus 2003-08-19)
- Even if we are fully aware of the risks when the network is based on TCP/IP and is connected to Internet, can we really claim that it is worth taking the risks?

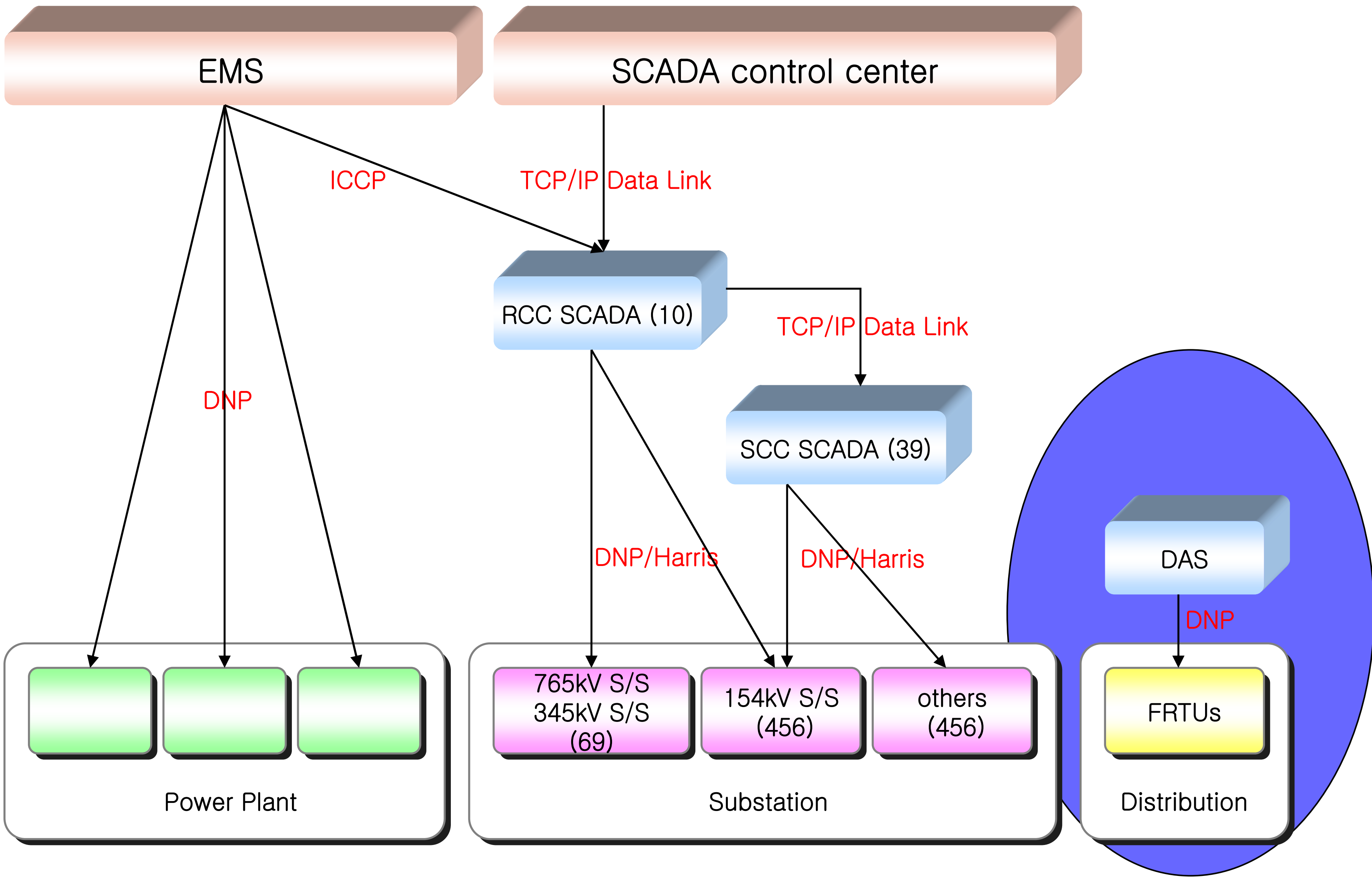
# Originally SCADA is not an isolated network

- Even before the interconnection between SCADA network and Internet is becoming common, devices in the SCADA system can be accessed from outside.
- However, the access is only permitted to privileged personnel.
- It means that internal attackers could penetrate the system from outside.

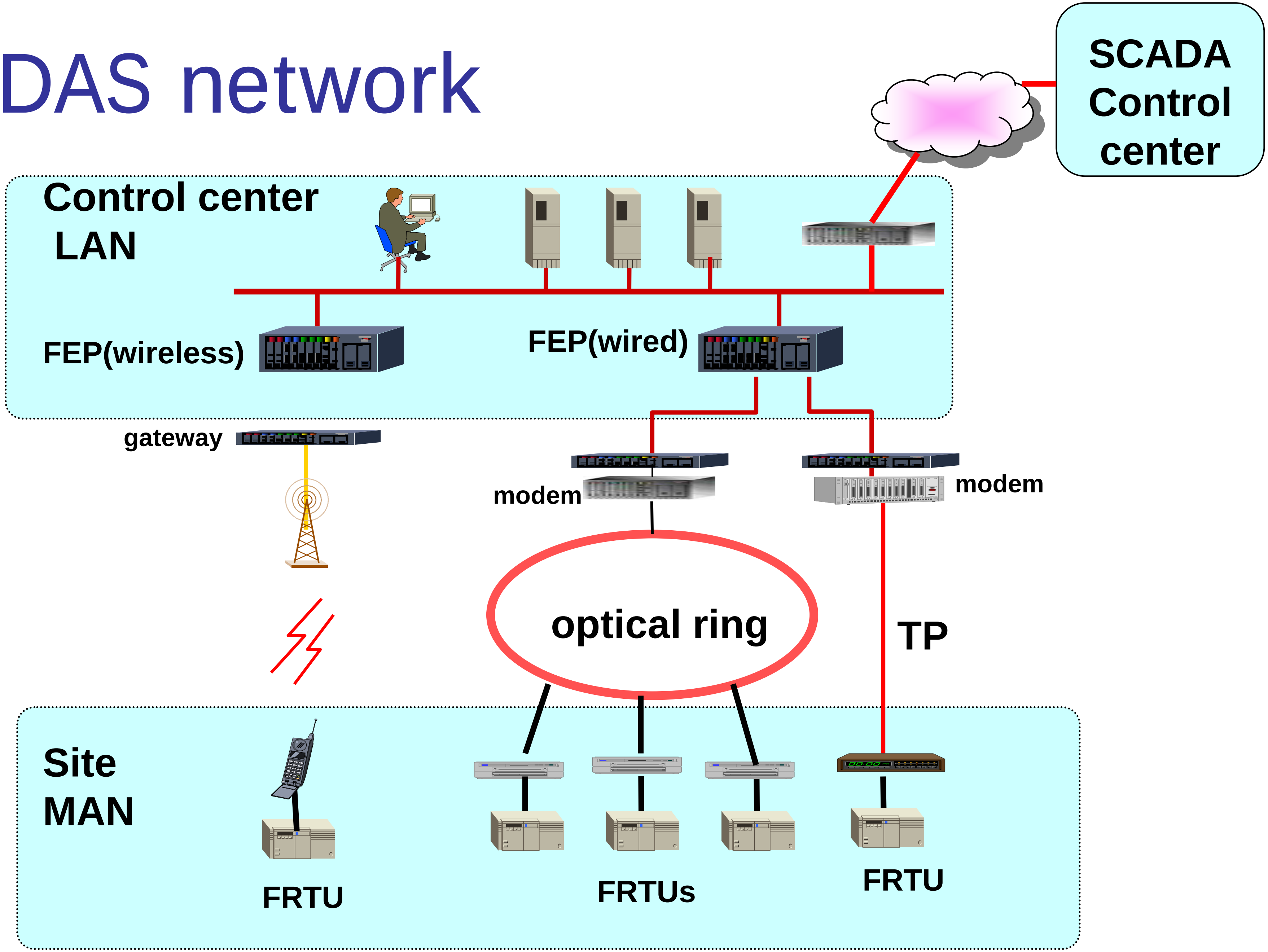
# SCADA network



# KEPCO SCADA system



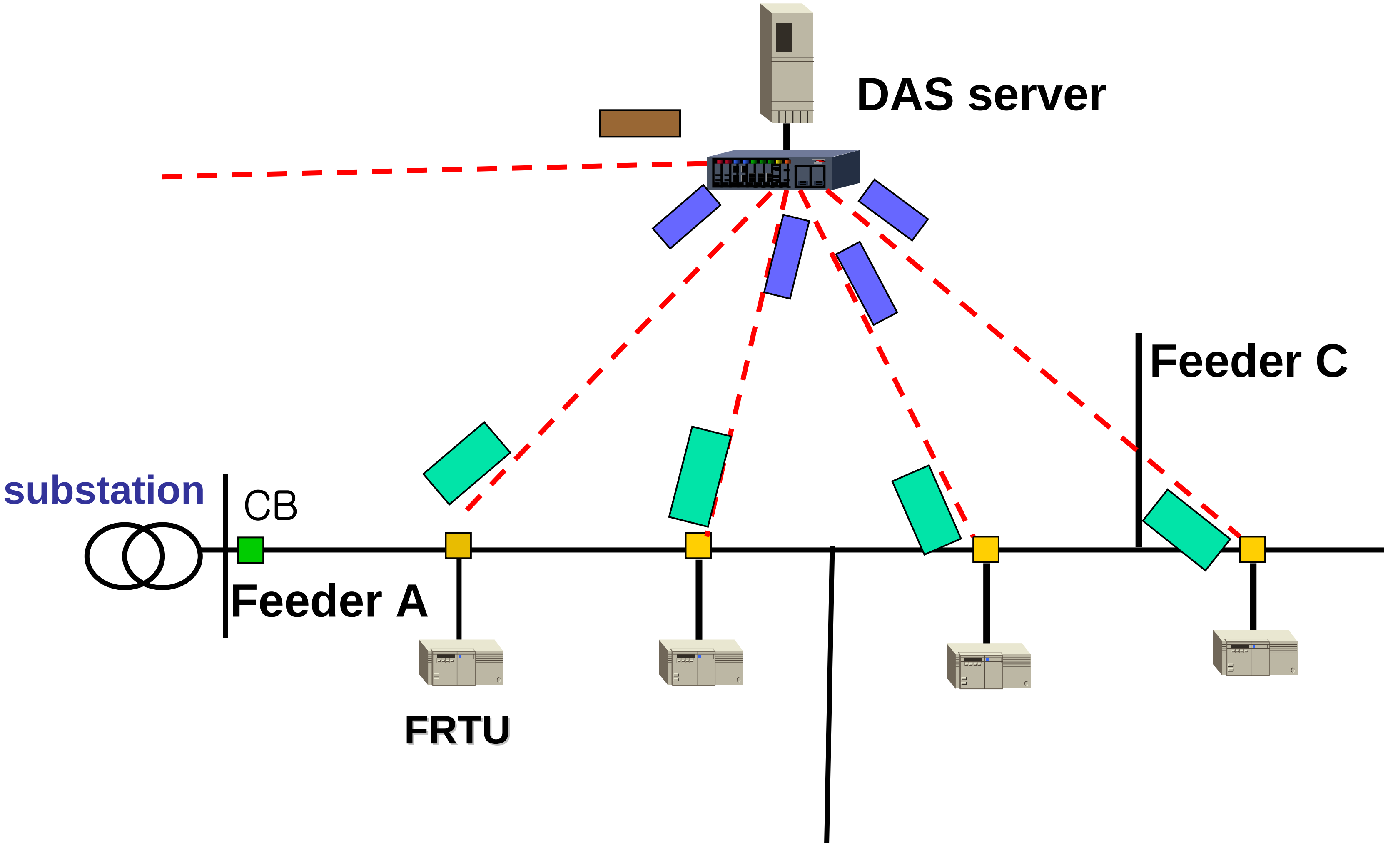
# DAS network


SCADA Control center
Control center LAN
FEP(wireless)
FEP(wired)
gateway
modem
modem
optical ring
TP
Site MAN
FRTU
FRTUs
FRTU

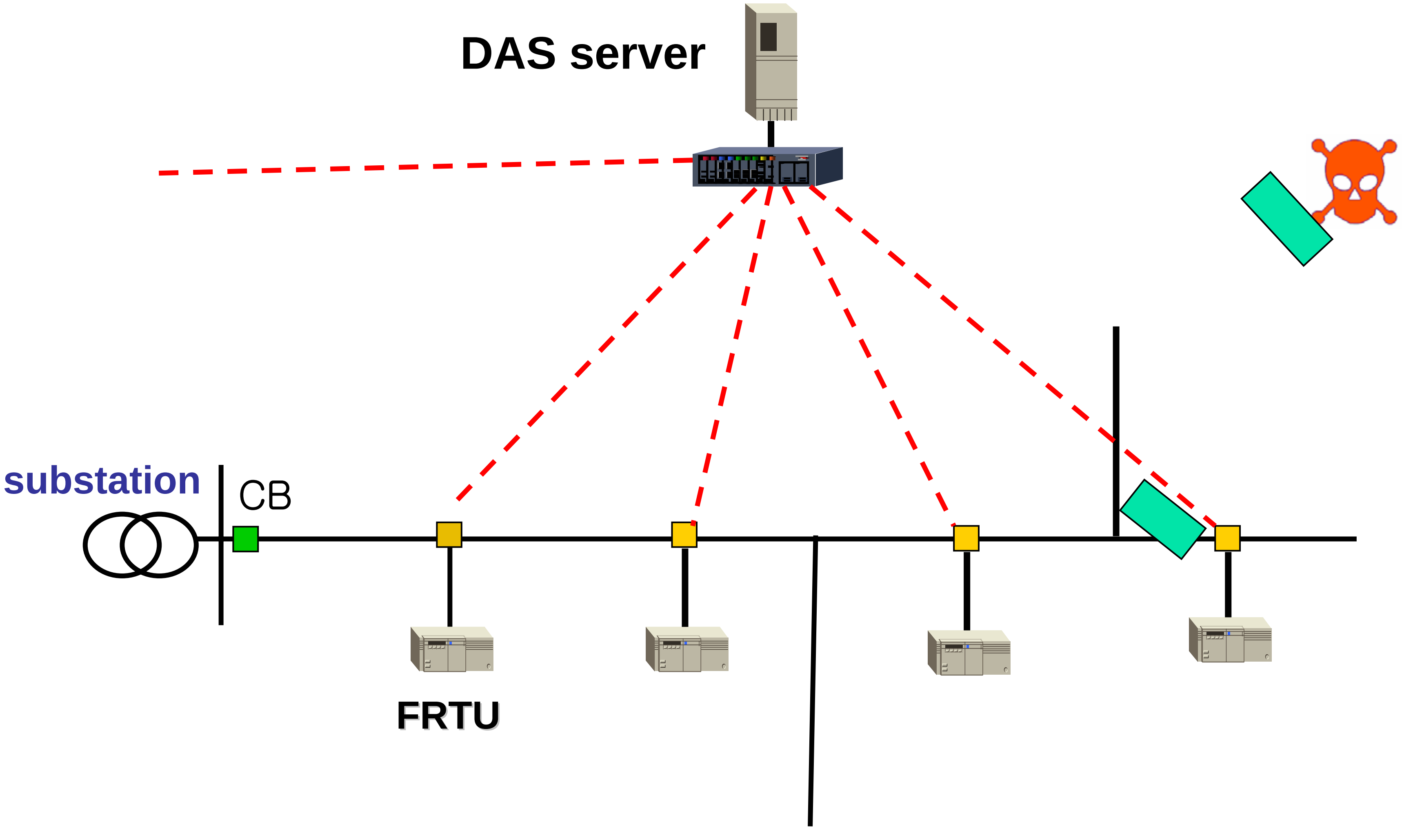
# DAS network is more vulnerable

- FRTUs are spread in wide area networks.
  - A single distribution system consists of approximately 100 to 500 FRTUs depending on the geographic size(5-20km).
- FRTUs are located in unattended remote sites.
- Unlike the IEDs in the SCADA system, FRTUs are not located in protected sites.

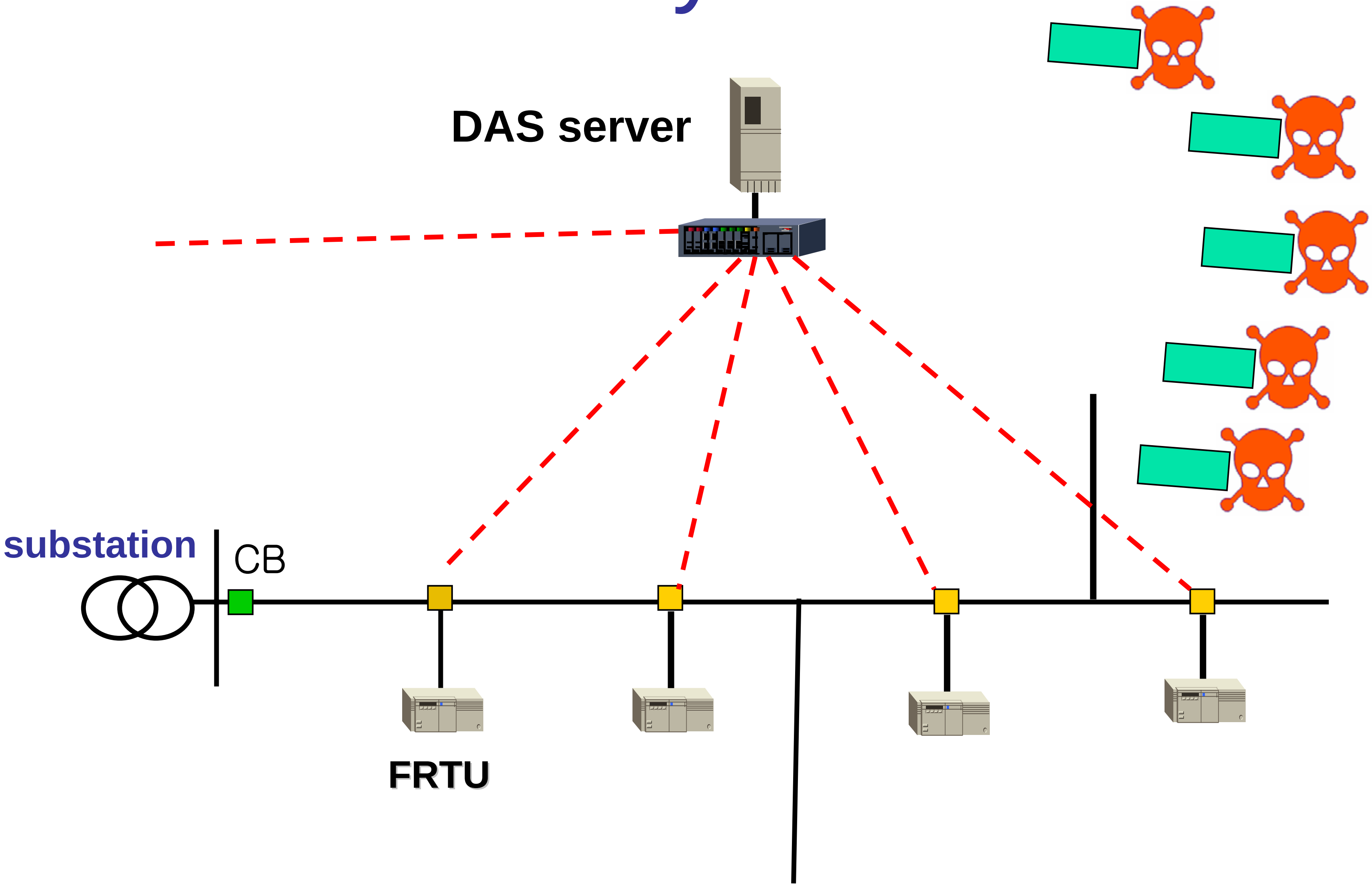
# What kinds of cyber attacks?



# What kinds of cyber attacks?



# What kinds of cyber attacks?



# Basic attacker model

- Passive attackers
  - Eavesdropping
- Active attackers
  - Data injection
  - Data modification
  - Replay
  - Server breakdown: DDOS
- Attacker access
  - External attacker
  - Internal attacker

# Basic Security requirements

- Confidentiality (privacy, secrecy)
  - Keep data hidden from unintended receiver
- Data integrity
  - Ensure data is correct, i.e., prevents unauthorized or improper change
- Data authentication
  - Ensure that data originates from claimed sender
- Entity authentication (identification)
  - Verify the identity of another participant
- Availability
  - Maintain service no matter what happens

# Observation(1)

- Normally data confidentiality is not important in the operations of the DAS network. In some cases, however, messages can deliver highly sensitive information such as secret keys which should be known to only two communication nodes. In this case we need to protect the message contents from eavesdropping.
- The most dangerous attacks are to cause FRTUs to fail to work properly.
  - alter the contents of the messages exchanged between the server and FRTUs and then to deliver this false messages to the FTRUs.
  - create bogus messages and inject them in the communication channel.
  - catch some messages and deliver the messages afterwards. This replay attacks can also make FRTUs to lead malfunctions.

# Observation(2)

- As long as the DAS server is in the protected (or isolated) location, availability requirement is secondary.
- For most operations, authentication of control actions (message contents and owner) is far more important than any other security requirements in order to prevent from malfunction of FRTUs.

# What happened in real world?(1)

- The most referenced one is the Maroochy water breach in Australia in 2000.
  - Attacker access: insider (disgruntled former consultant)
  - Where
    - Outside the system
  - Active attack
    - Inject false data to terminal devices by radio link

# What happened in real world?(2)

- The slammer worm penetrated a private computer network at Ohio’s Davis-Besse nuclear power plant in January 2002.
- The worm began by penetrating the unsecured network of the company’s contractor, then squirmed through a T1 line bridging that network and the company corporate network. The T1 line was one of multiple ingresses into the business network that completely bypassed the plant’s firewall.
- This is typical backdoor from the Internet to the corporate internal network that was not monitored by company personnel.

# What happened in real world?(3)

- The Blaster worm may have contributed to the cascading effect of the Aug. 14 blackout in northeastern US (2003).
- Blaster degraded the performance of several communication lines linking key data centers used by utility companies to manage the power grid.
- The inability of critical control data to be exchanged quickly across the grid could have hampered the operators' ability to prevent the cascading effect of the blackout.
- The Blaster worm exploits RPC DCOM on Windows platform and infect a host. Then the infected host will begin SYN flooding on port 80 using spoofed source address. – DOS attack

# What’s wrong?

- The kernel of the problem is that some companies’ servers are based on Windows 2000 or XP OS and rely on commercial data links, including the Internet and wireless systems for exchanging information.
- Windows had security flaws.
- Engineers didn’t realize how dangerous the Internet was.
- So a solution is simple.
  - Stop connection everything to the ‘net.

# Basic Cryptographic Primitives(1)

- Asymmetric (public-private key)
  - Diffie-Hellman key agreement
    - Requires authentic key from other party
  - Public-key encryption
    - Requires authentic key from other party
  - Digital signature
    - Generates signature by private key
    - Provides authenticity of message contents and owner

# Basic Cryptographic Primitives(2)

- Symmetric (shared-key)
  - Block cipher
  - Stream cipher
  - Keyed hash function
    - Generates message authentication code (MAC)
    - Provides authenticity of message contents and owner
- Unkeyed symmetric
  - One-way hash function
  - Cryptographic hash function

# Comparison Symmetric and Asymmetric Crypto

- Symmetric crypto
  - Need shared secret key
  - 80 bits key for high security (year 2010)
  - ~1,000,000 ops/s on 1GHz processor
  - >100x speedup in HW
- Asymmetric crypto
  - Need authentic public key
  - 2048 bits key (RSA) for high security (year 2010)
  - ~1000 encry/s, ~100 decrpt/s (RSA)
  - ~10x speedup in HW

# Security Protocol Wish List

- We use the basic crypto primitives to design higher-level security protocols.
- Efficient protocol
  - Low computation overhead
  - Low communication overhead
- As little trust as necessary
- As few assumptions as necessary

# The gist of the protocol proposed in this paper

- goal:
  - Efficient protocol
    - FRTUs are limited in resources (computing power, bandwidth).
  - Provide message integrity
  - Provide message owner's authenticity
  - Prevent replay attack
- Use keyed hash function using MD5
- Trust requirement
  - Every FRTUs trusts the DAS server from the beginning.
- Key distribution
  - The DAS server distribute shared keys to FRTUs periodically in secure way.

# A few things to be noted(1)

- Is cyber security real?
  - Yes, especially in distribution system.
- Why did cyber breaches happen so far?
  - The system is connected to the ‘net.
  - They didn’t realize how dangerous the Internet world is.
- Keep the SCADA system isolated as possible as you can.
  - We are not facing not just script kids, but government-funded professionals.
  - Nothing is almost impossible to hackers these days.
  - Just don’t do it if that web-based or internet-based business is a fad is the main reason.

# A few things to be noted(2)

- Nonetheless the cyber threat is here and now.
  - Even SCADA system is exposed to access from outside, not to mention DAS system.
  - More importantly, it is very difficult to protect against insider attacks.
  - Remember to find out where the vulnerable points are.
  - Security-awareness and risk assessment is the important first step.
- Are security measures costly?
  - Yes, very costly in the sense of transition.
  - Imagine that we have to implement security measures to tens of thousands of FRTUs. The situation may be same as in IEDs.
  - Therefore, the security adaptation will be a slow evolutionary process, not a revolutionary process.
  - But technologically security measures have been well established in corporate networks for many years.