Evaluation of Cyber Security Strategies for SCADA/ICS systems

Sep. 11, 2018

Sugwon Hong

Myongji University

Contents

- Major cyber security documents
- Network separation
- Communication message security
- Monitoring
- conclusion

Cyber Security Documents

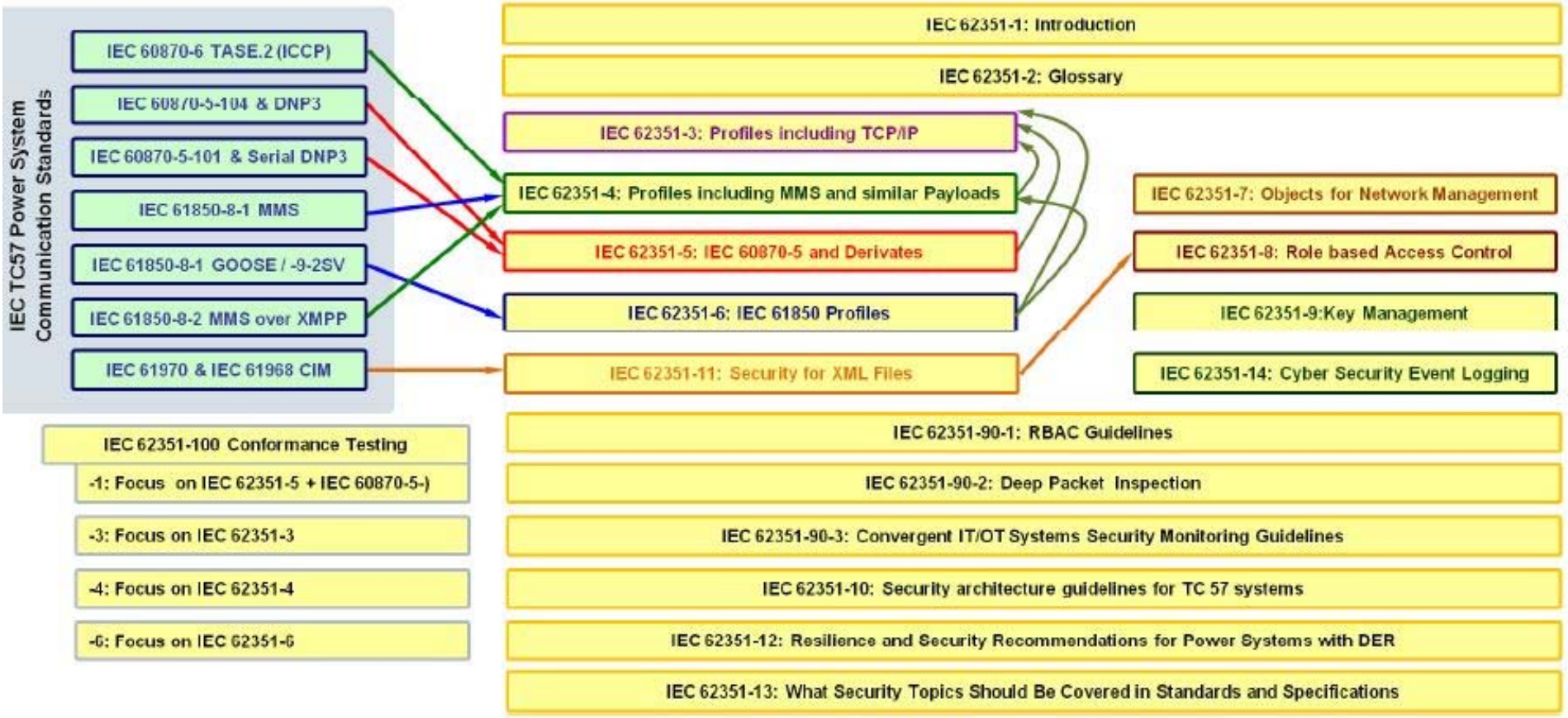
- NERC CIP(Critical Infrastructure Protection)
  - CIP2: Critical Cyber Asset Identification
  - CIP3: Security Management Control
  - CIP4: Personnel and Training
  - CIP5: Electronic Security Perimeters
  - CIP6: Physical Security of Critical Cyber Assets
  - CIP7: Systems Security Management
  - CIP8: Incident Reporting and Response Planning
  - CIP9: Recovery Plans for Critical Cyber Assets

- NIST IR 7628
  - "Guideline for Smart Grid Cyber Security: Vo1: Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements"
  - 7 domains (a high-level grouping of actors)
  - 46 actors (organization, building, individual, system, or devices)
  - Over 130 logical interfaces between these actors
  - Logical interfaces are grouped into 22 categories with a specific set of security requirements and priority values

- IEEE C37.240
  - "IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control System"
- IEEE 1686
  - "IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities"

- IEC 62351 (IEC TC 57 WG 15)
  - Originally, the standards address the security of the communication protocols defined by the IEC TC57 (IEC 60870-5, IEC 60870-6, IEC 61850, IEC 61970, IEC 61968).
  - So, IEC 62351-3,4,5,6 specify the security measures for specific communication protocols and services.
  - Recently, they extended their work scope.

IEC 62351 Standards



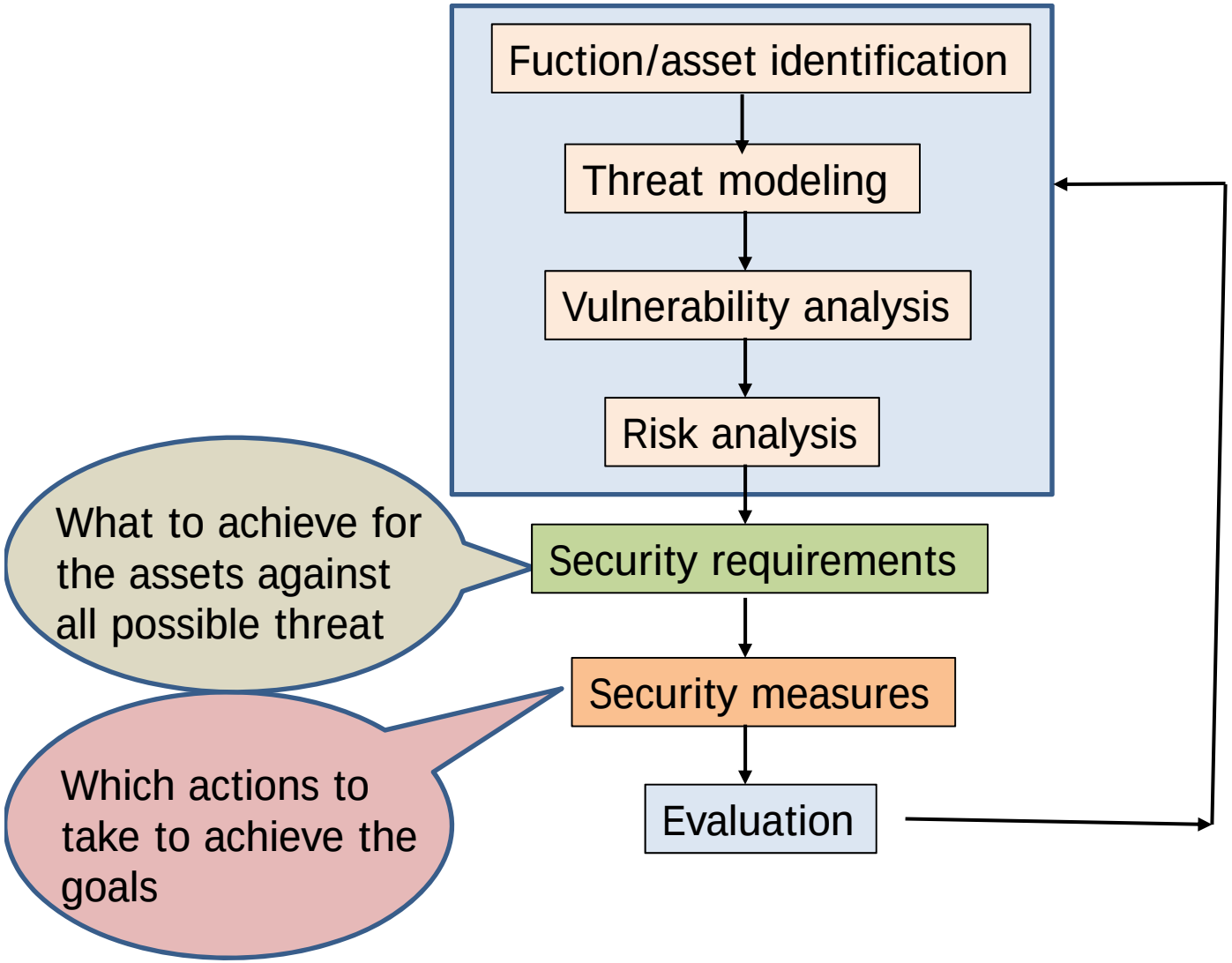
Cigre

- The Impact of Implementing Cyber Security Requirements using IEC 61850 (2010)
- Application and Management of Cybersecurity Measures for Protection and Control (2014)
- Framework for EPU operators to manage the response to a cyber-initiated threat to their critical infrastructure(2017)

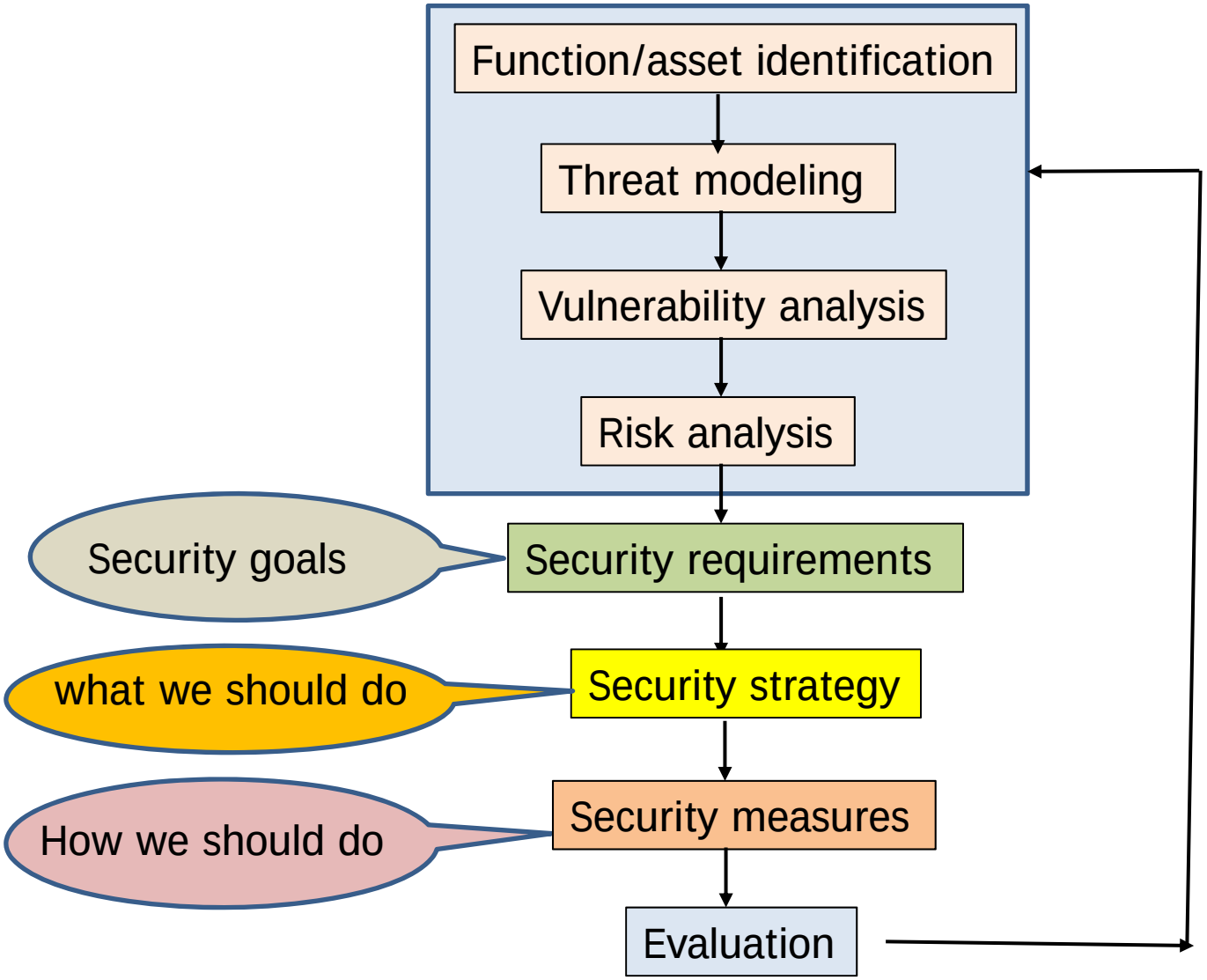
EPRI

- Network System Management: Implementation and Application of the IEC 62351-7 Standard (2014)
- Network System Management: End-System-Related IEC 62351-7 Object Definitions (2013)
- Network Security Management for Transmission Systems (2012)

Life Cycle of Security Steps



Life Cycle of Security Steps



Security Requirements

- 7 foundational requirements of ISA-62443-1-1 (IEC 62443)
  - Identification and authentication control of users(human, software processes, devices)
  - Use control: authorization
  - Data integrity
  - Data confidentiality
  - Restricted data flow
  - Timely response to event
  - Network resource availability

Three Security Strategies

- Network separation
  - Physical network separation
  - Logical network separation
- Communication message security
- Monitoring

Physical Network Separation(1)

- Physical network separation
  - This is the first line of defense in the context of an "air gap" which refer to the network that has no outside connections.
  - It has been considered "the" best weapon against cyber attacks.
  - Any IT devices outside can't connect into the SCADA network, crossing a physical gap.

Air Gap creed?

I've written about SCADA issue in the past, but one issue that I've consistently tried to emphasize is that critical control systems should never, ever interact nor interconnect with Internet systems in any way, shape, or form. There's a good reason for this, and it's always been referred to as the "Air Gap" principle."

(Paul Ferguson, Internet Security Intelligence Advanced Threats Research, Trend Micro, April 8, 2012)

Air Gap Myth

- But, currently the consensus is that the physical network separation is not achievable any more.
- Why?
  - In real life, in no cases can we find SCADA/ICS networks which are not connected with enterprise networks.
    - In many cases security is outweighed by business effectiveness, cost reduction, or other business conveniences.
    - In KEPCO, are SCADA control systems isolated from its enterprise networks?

- Firmware update, OS patches, new logic update to address design flaws, and other maintenance and support activities are highly likely to be implemented by remote access or by using laptops, and sometime by wireless.
- Attackers could be insiders.
  - Disgruntled, negligent employees, or traitors
- Current attacks are highly coordinated, concentrated, and enduring.
  - APT(Advanced Persistent Attacks)

Recent cyber incidents

- Recent cyber incidents speak volumes about its imperfection.
  - Stuxnet (2010)
  - Attack on Ukrainian electric distribution system (Dec. 2015)
  - Saudi Arabia Aramco (2016)
  - These incidents exemplify how APT(advanced persistence threat) is sophisticated enough to penetrate any strong walls of critical infrastructures.

Physical Network Separation

- Evaluation
  - Physical network separation still has validity, and should be the first design goal of SCADA/ICS network configuration.
    - ex, avoid unnecessary connections to SCADA networks, and disable unnecessary services unless the possible risks are fully understood.
  - Although the networks were believed to be physically separately in the past, actually they were not.
    - Past cyber incidents testified the fact.

Logical Network Separation(1)

- We should separate trust domains from not trust domains, and information should flow only over designated access points on which we enforce strict access controls.
- We have many handy tools(security measures) for logical(virtual) network separation.
  - Endpoint protection platform such as firewall, anti-virus, anti-spyware, behavioral blocking, IPS, IDS, HIDS, ACL(access control list), whitelisting, blacklisting, etc.

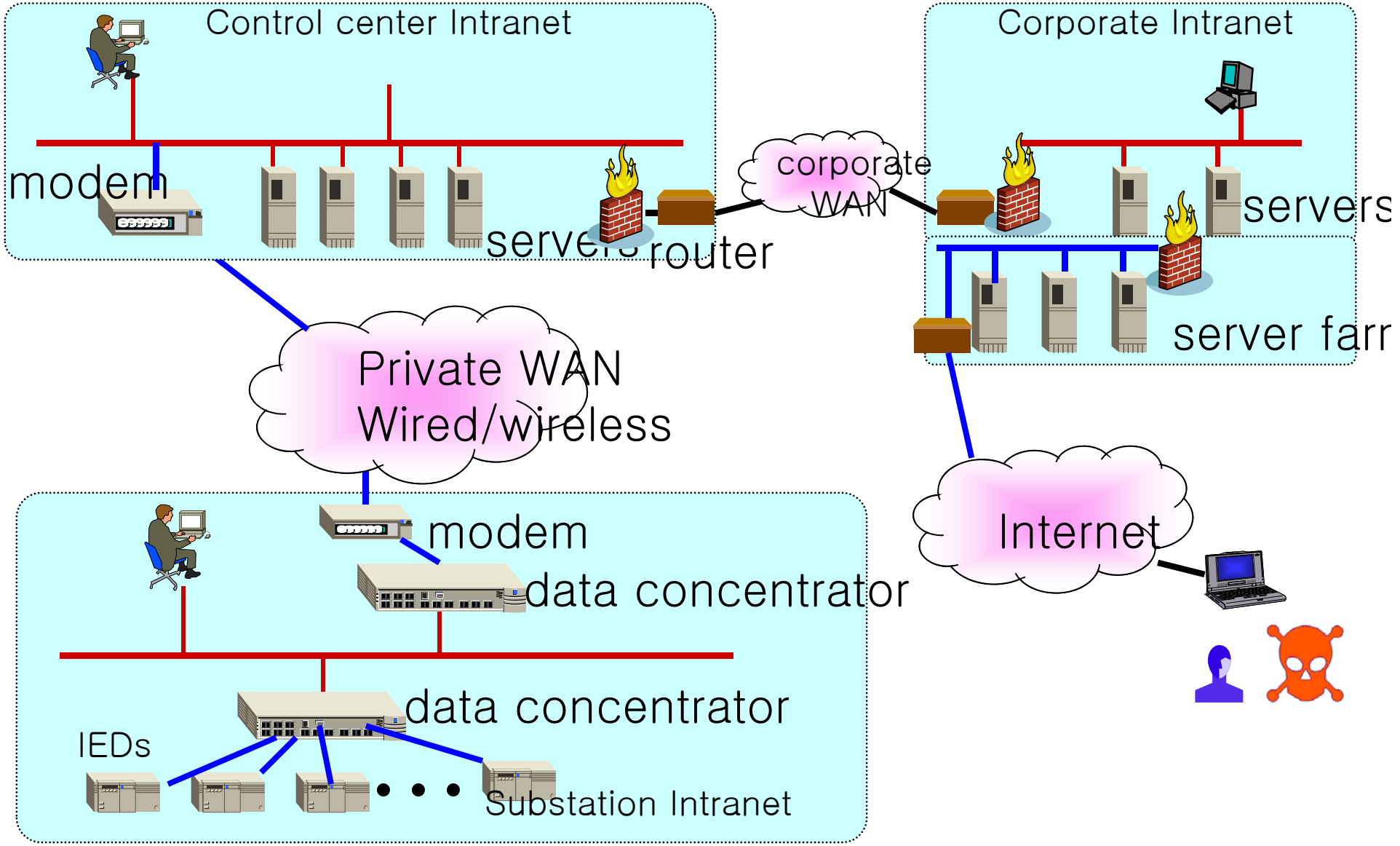
Logical Network Separation(2)

- Logical network separation is the “go-to” strategy that is being implemented in the current SCADA/ICS, and maybe it will continue to be so for a long time.
- Security can be stronger if we enforce stricter security policy over incoming flow into trust domains.
  - ex, remote access, USB usage
- This strategy aims at mostly attack prevention.

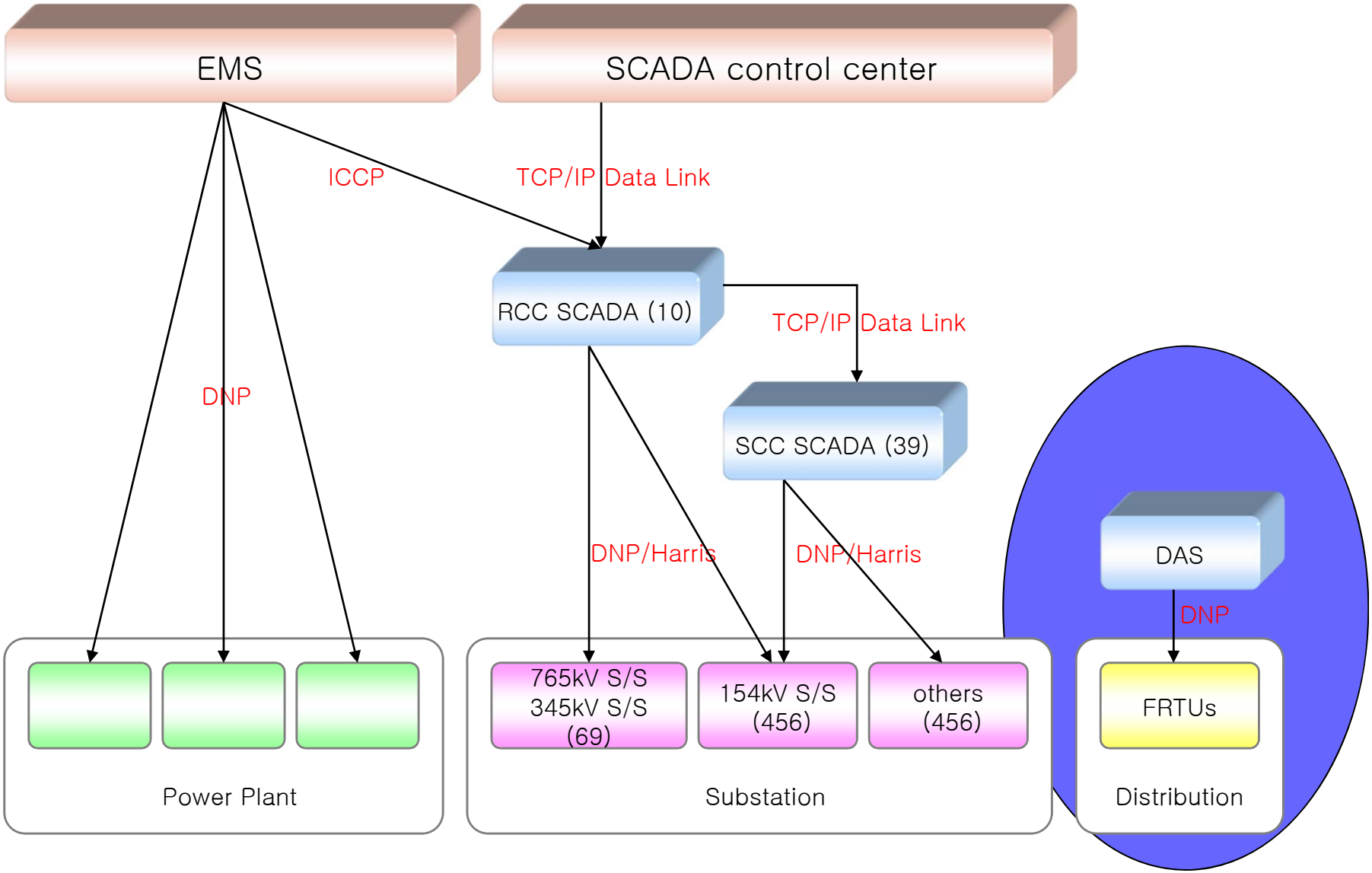
Defense in Depth

- Multi-layer defenses
  - A whole physical network is divided into several domain networks, depending on criticality of security levels.
  - Neighboring network domains have clearly defined security gateways, only on which all information flows are exchanged and strict security policing are enforced.
  - The primary goal is that as attackers try to penetrate deeper networks, it can reduces the probability of attack success, i.e., attacks are as isolated into a penetrated domain as possible, mitigating attack impacts.

SCADA network



KEPCO SCADA system



ISA/IEC 62443(formerly ISA-99)

- Divide the ICS network into security zones based on control function, and multiple separate zones are managed with “defense in depth” strategy.
  - core concept is “Zones and Conduits.”
  - security zone: grouping of logical or physical assets that share common security requirements

ISA/IEC 62443

- A conduit is a only path on which the flow of information is conducted between two zones.
  - Can provide the security functions that allow information to be exchanged securely between zones.
  - Consider all possible ways in which bad data are likely to deliver.

SCADA/ICS firewalls

- Look beyond traditional network layer firewalls towards firewalls that are capable of deep packet inspection of key SCADA and ICS protocols.

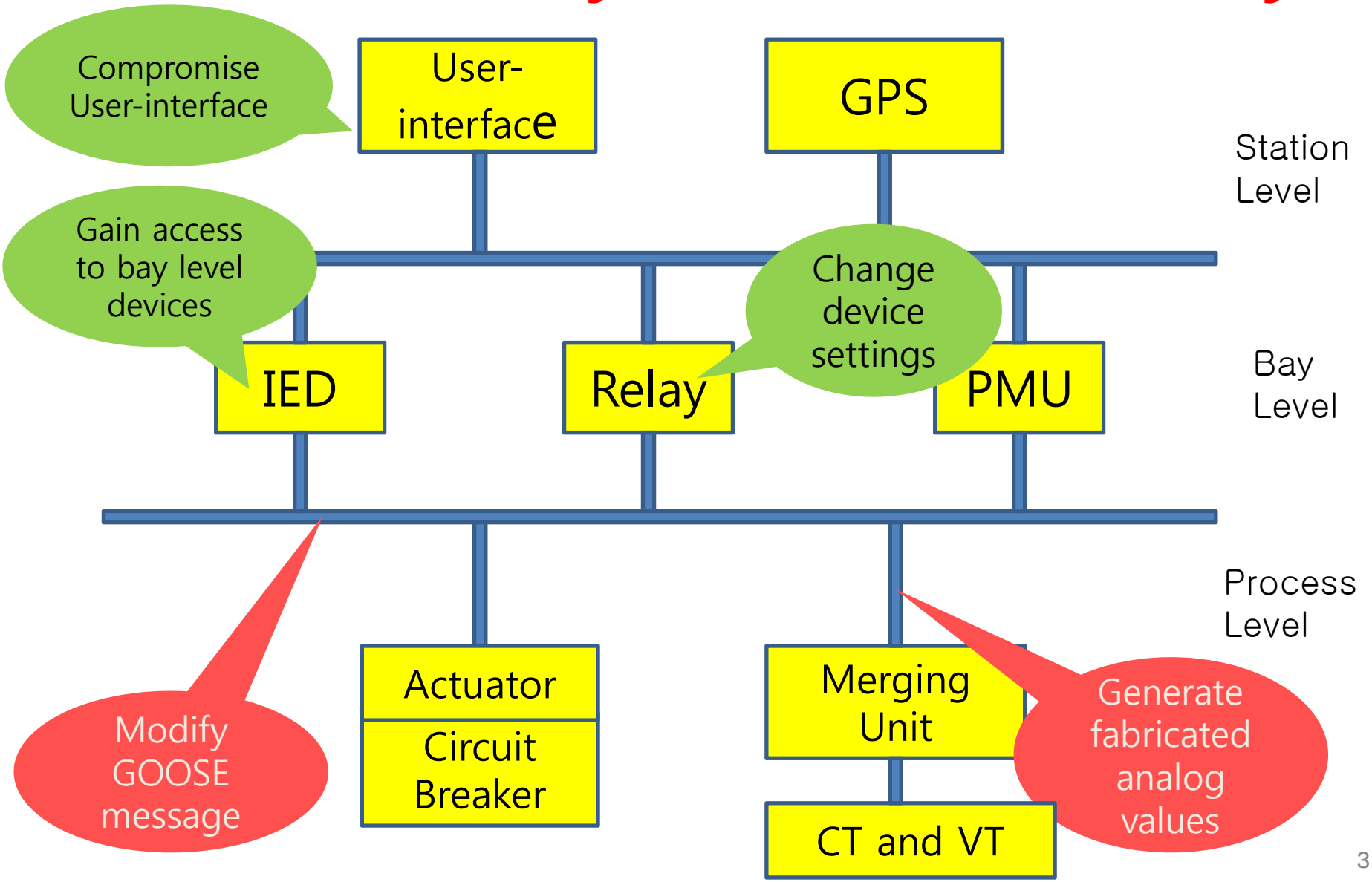
Communication message security(1)

- If intruders can penetrate into SCADA networks through multilayer of defense lines, the last line of defense should be the security at the level of communication message exchanged between users(devices) inside the network.
- The reason is that the ultimate goal of any serious attack will be disruption of control operations.

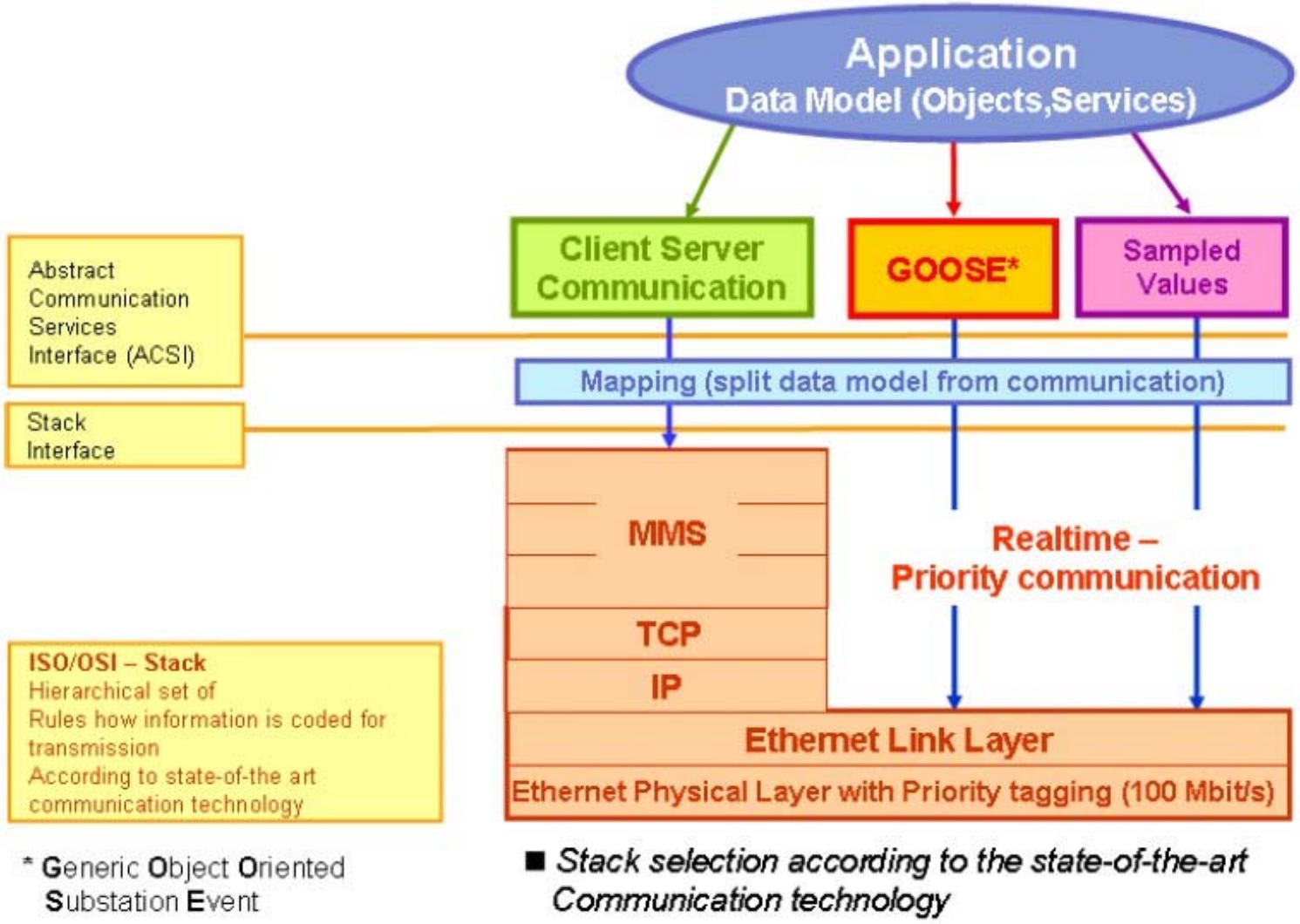
Communication message security(2)

- What should we do?
  - Messages should not be compromised (modified or falsified)
  - Messages should be sent by legitimate (authorized) users (devices)
  - Message contents should not be exposed to others.
- IEC TC57 addresses this issue.
  - IEC 62351 part 3,4,5,6 address security measures depending on service types and underlying communication protocols.

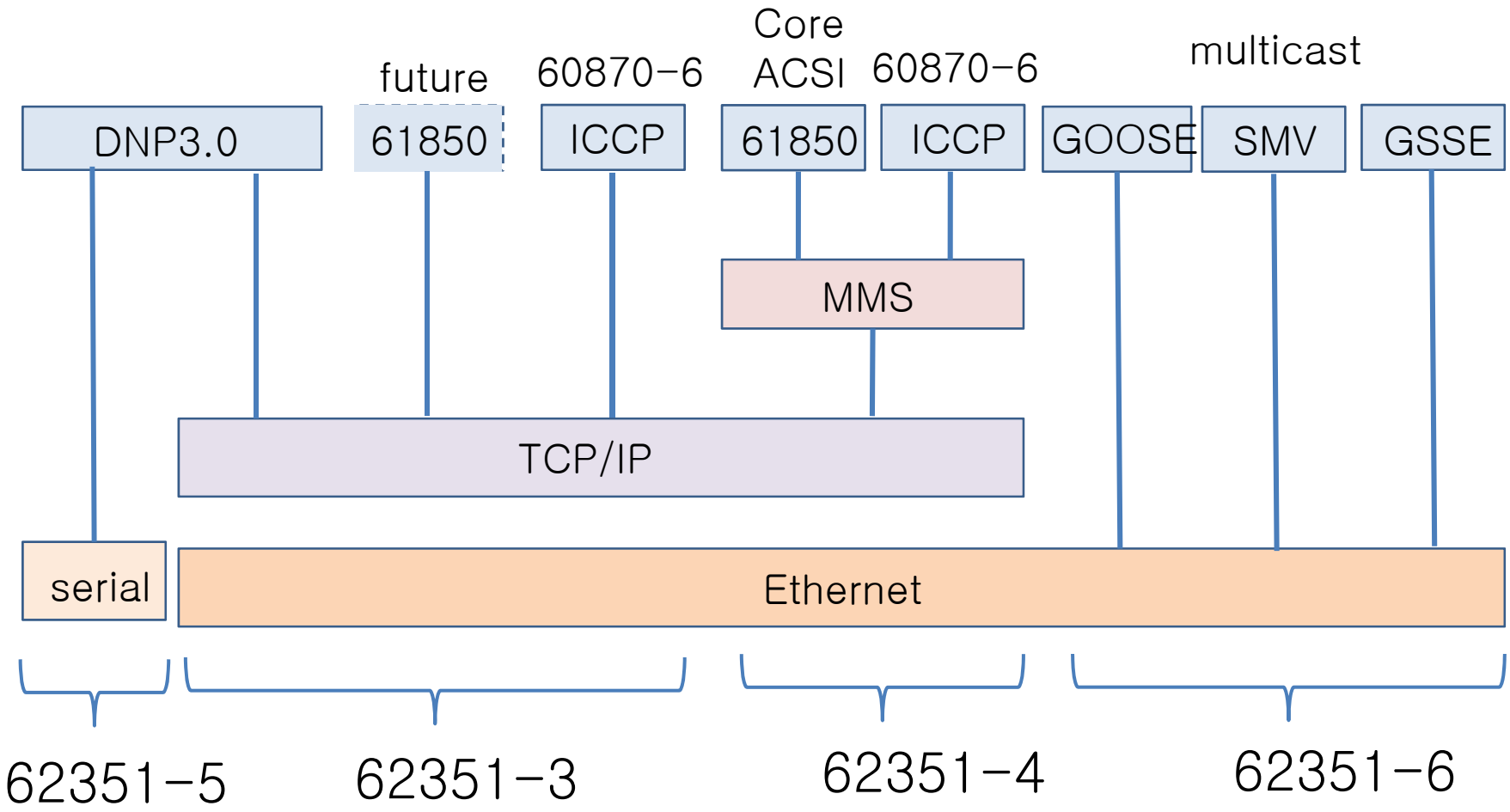
IEC 61850 system vulnerability



IEC 61850 comm services



IEC 62351 and 61850 services



Communication message security(3)

- Evaluation
  - IEC 62351 security measures are the typical crypto algorithms and security protocols which are commonly used in IT network security nowadays.
  - Challenges
    - Implementation
      - Considering most devices are computing-power-restrained embedded systems, we can meet requirements of real time constrained delay such as GOOSE message
    - Cost
    - migration

Monitoring(1)

- For detection and reaction(recovery) for any unanticipated event, we need to view a complete configuration of all elements, actions and status of the elements, and traffic flow between these elements in real-time.
- Deploy SCADA/ICS-appropriate security technologies to raise an alarm when critical equipment at risk of compromise

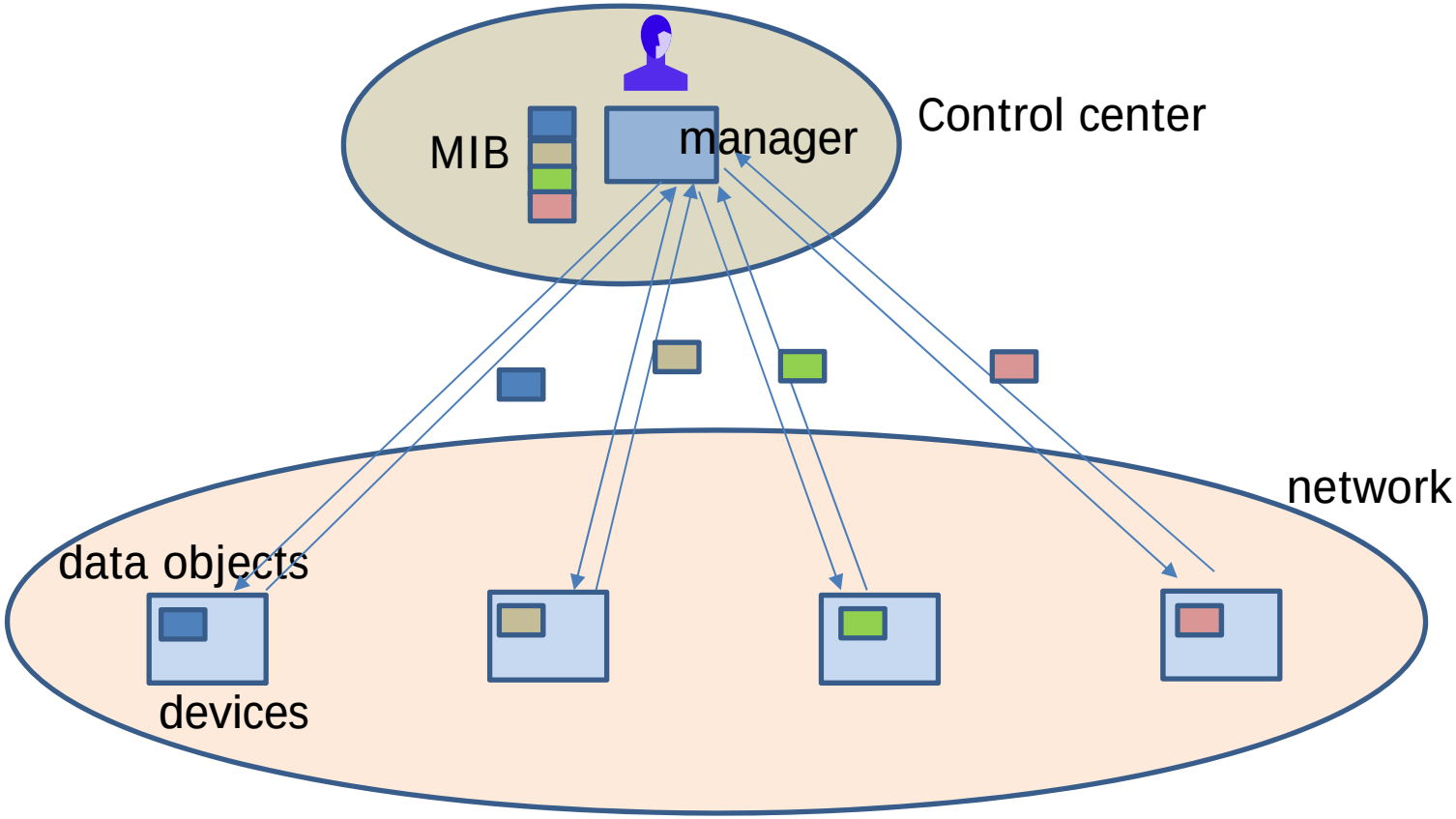
Monitoring(2)

- Monitor ALL data flows into the network.
- Monitor ALL data flows out of the network.
- Detect unusual behaviors in the network.
- Alarm any suspicious incidents to provoke proper reactions to the system.
- Problem is how the system can do it?
  - SCADA-appropriate IDS

Network management

- In IT networks, the Network Management provides a tool to view a entire network in a unified way.
  - Network devices collect pre-agreed data, and send the data to a manager on request.
  - A manager can monitor the whole network in real time, using all data sent from devices.

IT Network Management

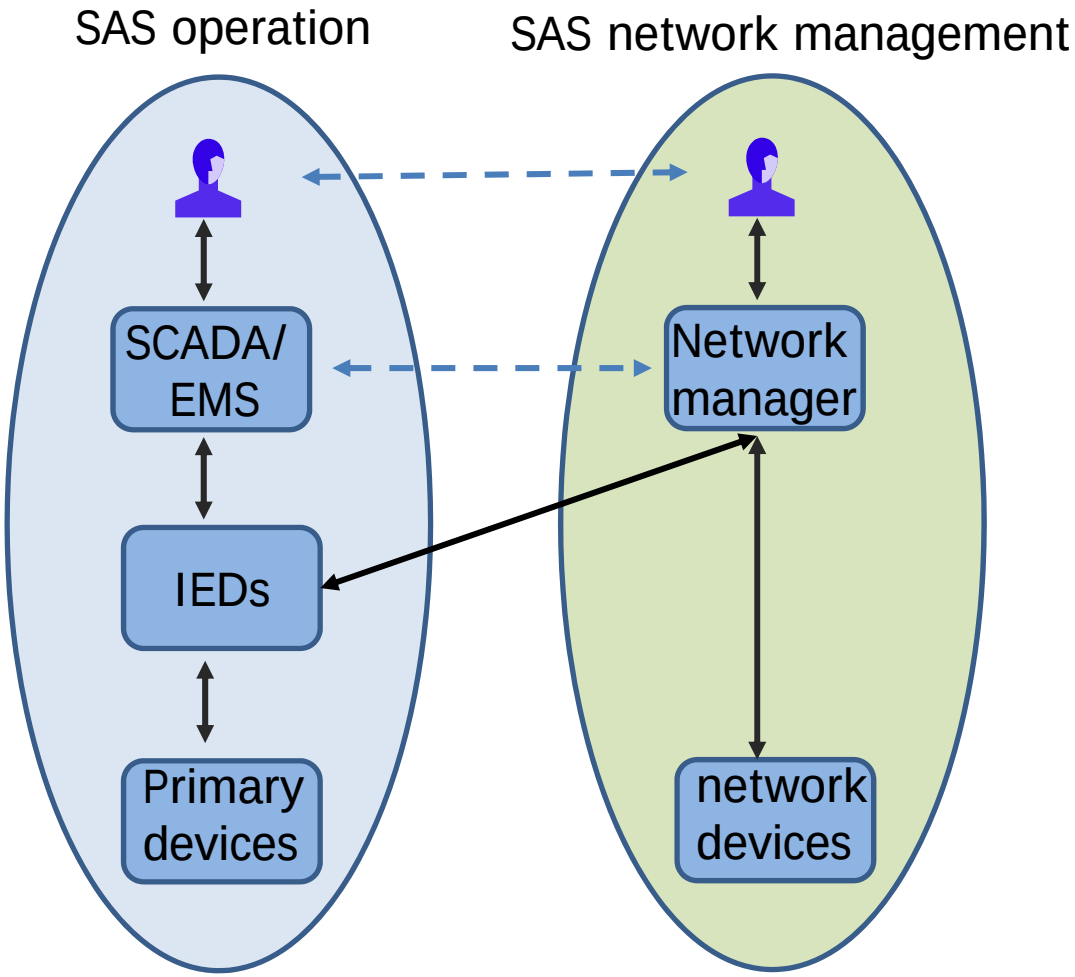


Monitoring(3)

- Problem: two separate operation domains
  - In the current SCADA, OT operators are responsible for operations and IT operators are responsible for communication networks.
  - So, the SCADA network manager is blind to communication information of devices such as IEDs.
- What is missing?
  - The SCADA network manager needs the data objects that are specific to SCADA operations.

Monitoring(4)

- SCADA network management



Monitoring(5)

- IEC TC 57 addresses this issue.
  - IEC 62351-7: Network and System Management (NSM) data object models
    - The goal of this standard is to define a set of abstract (data) objects that will allow the remote monitoring of the health and condition of IEDs, RTUs, DERs systems and other systems that are important to power system operations.

Monitoring(5)

- The data objects covers the wide range of information:
  - Physical access
  - Communication security: authentication and traffic
  - SAS communication related information
  - Clock information and CPU/memory utilization
  - Environmental information such as temperature and power supply
- So, these objects enable NSM to detect various cyber attacks as well as help maintenance.

Conclusion

- All security measures for the SCADA/ICS systems can fall into three strategies: network separation, communication message security, and monitoring.
- Understanding of these strategies will help us to approach to security issues in the systems.
- The current SCADA/ICS security entirely relies on network separation in the context of “security in depth.” But the communication message security can make us achieve the complete “security in depth.”
- The monitoring strategy will play a critical role in SAS security.

Conclusion

- The most important thing is understanding of the nature of security.
  - "Security is a process, not a product. Products provide some protection, but the only way to effectively do business is to put processes in place that recognize the inherent insecurity in the products."
  - Security is to provide as great a degree of prevention and detection and reaction as possible, so mitigates the impact of undesirable incidents to the least degree.
  - The whole point of security is the security management in a integrated way.