Sharing Session

Industrial Control System (ICS) Cyber Security

System Management, Compliance and Challenges

fedco

fedco.co.id

Outline

- Industrial Control System Overview
- The Essential of Cyber Security in ICS
- ICS Cyber Security Management
- ICS Cyber Security Recommended Practices
- Sustainability, Stewardship and Compliance
- Standard and References

Industrial Control System Overview

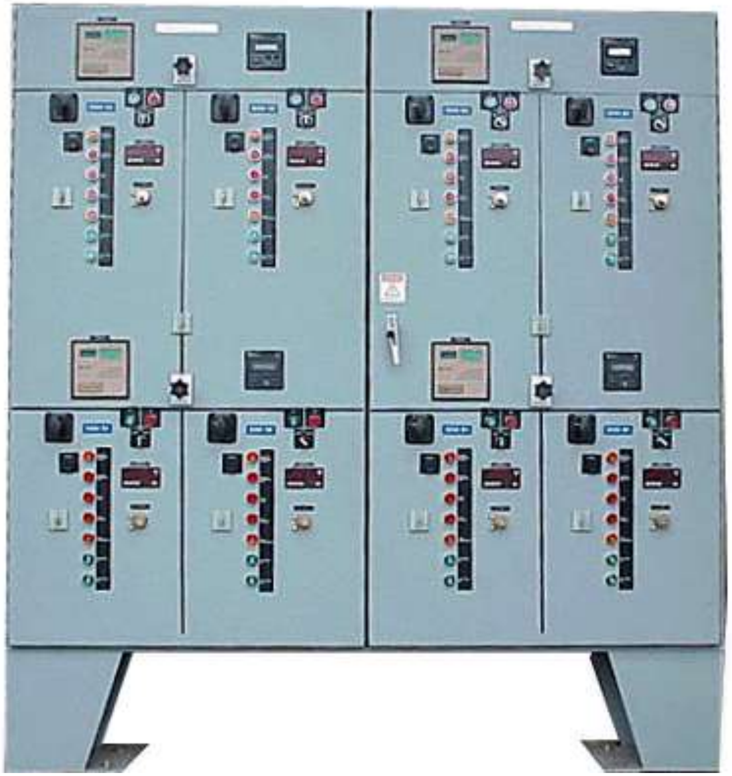
Industrial Control System Overview

- What is Industrial Control System (ICS)
  - Automation control system that cover varies of system which has the main function to:
    - ✓ Control the plant entities
    - ✓ Ensure the plant safety operations
    - ✓ Plant monitoring and surveillance
  - ICS typically used in some critical industries such as Oil and Gas, Petrochemical, Power Plant, Nuclear Plant, Discrete Manufacturing (automobile, aerospace), etc.

Industrial Control System Overview

Evolution of ICS

- Panel Based Controls
  - Push buttons
  - Single loop controls
  - Stand alone
  - No networks
  - No communication



From cyber threat perspective,
this system is "isolated"

fedco.co.id

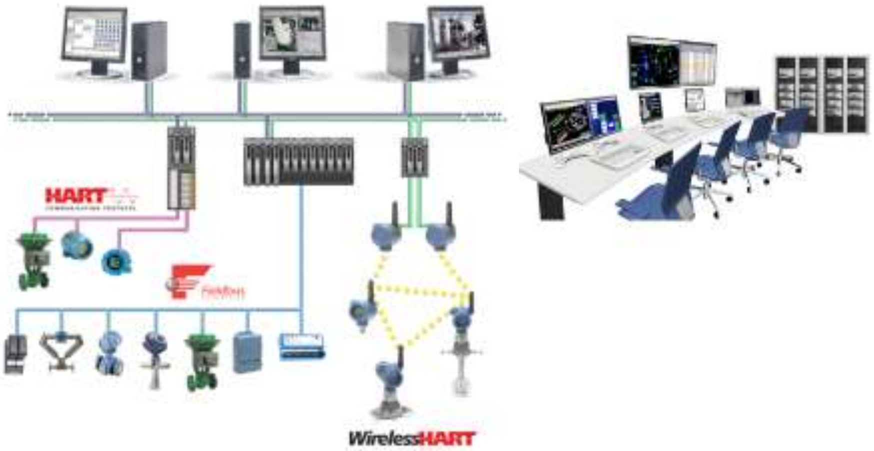
Industrial Control System Overview

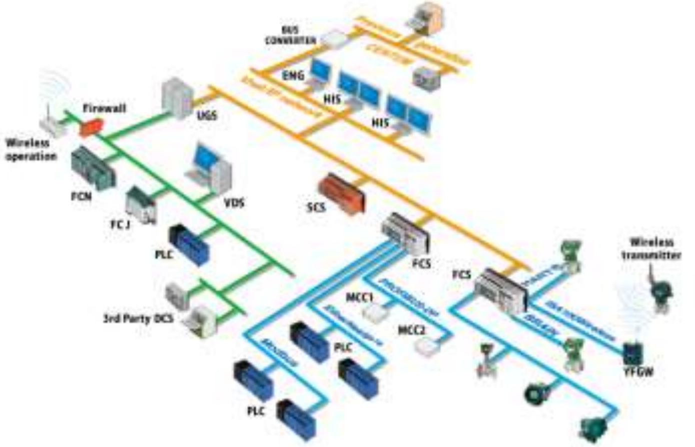
- Legacy Equipment
  - Proprietary network
  - Proprietary OS
  - No Ethernet
  - No Intranet connections

From cyber threat perspective, this system is “exploitable – but not a trivial task”

Industrial Control System Overview

- Modern Equipment
  - Open protocols
  - Ethernet everywhere
  - Remote configuration
  - Windows environment
  - Unix/Linux platform
  - Integrated system





From cyber threat perspective, this system is "a huge challenge – readily exploitable"

Industrial Control System Overview

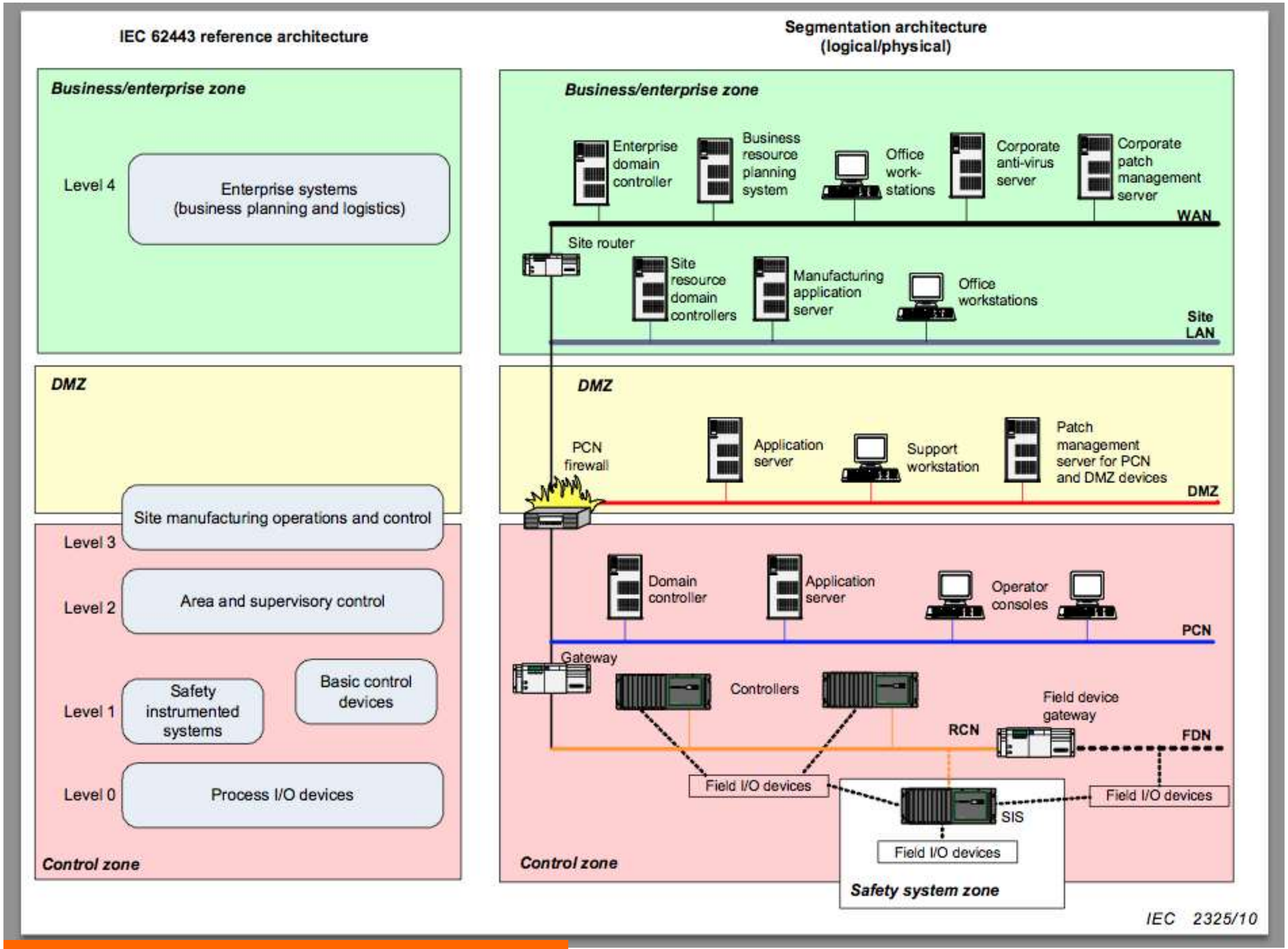
Refer to IEC 62443, segmented architecture is used to give better understanding and well managed entities in ICS environment

- Layer 4: Business Network
- Layer 3: Historian/PI/Apps Server/SCADA/DMC
- Layer 2: DCS/Control Server
- Layer 1: Basic Control Devices, DCS Controllers, PLC, RTU
- Layer 0: Process I/O Devices

ICS Environment

Layer 3 and 4 interface architecture & configuration is one of the critical concern in ICS-CS

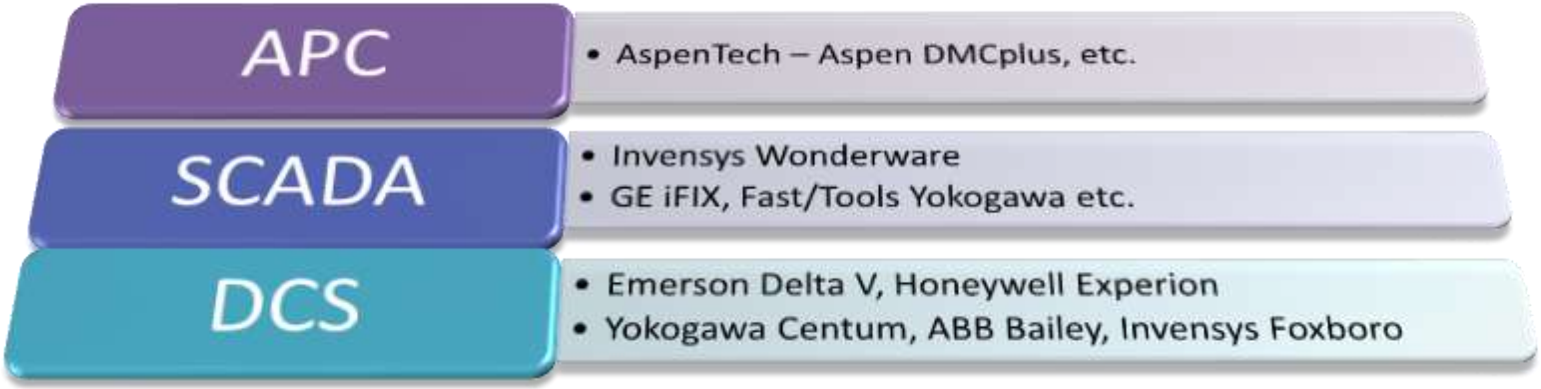
Industrial Control System Overview



IEC 62443 reference architecture
Business/enterprise zone
Level 4
Enterprise systems (business planning and logistics)
DMZ
Site manufacturing operations and control
Level 3
Level 2
Area and supervisory control
Level 1
Safety instrumented systems
Basic control devices
Level 0
Process I/O devices
Control zone
Segmentation architecture (logical/physical)
Business/enterprise zone
Enterprise domain controller
Business resource planning system
Office work-stations
Corporate anti-virus server
Corporate patch management server
WAN
Site router
Site resource domain controllers
Manufacturing application server
Office workstations
Site LAN
DMZ
PCN firewall
Application server
Support workstation
Patch management server for PCN and DMZ devices
DMZ
Domain controller
Application server
Operator consoles
PCN
Gateway
Controllers
Field device gateway
RCN
FDN
Field I/O devices
SIS
Field I/O devices
Field I/O devices
Safety system zone
Control zone
IEC 2325/10

L0-L4 Architecture Hierarchy

Industrial Control System Overview



APC

- AspenTech – Aspen DMCplus, etc.

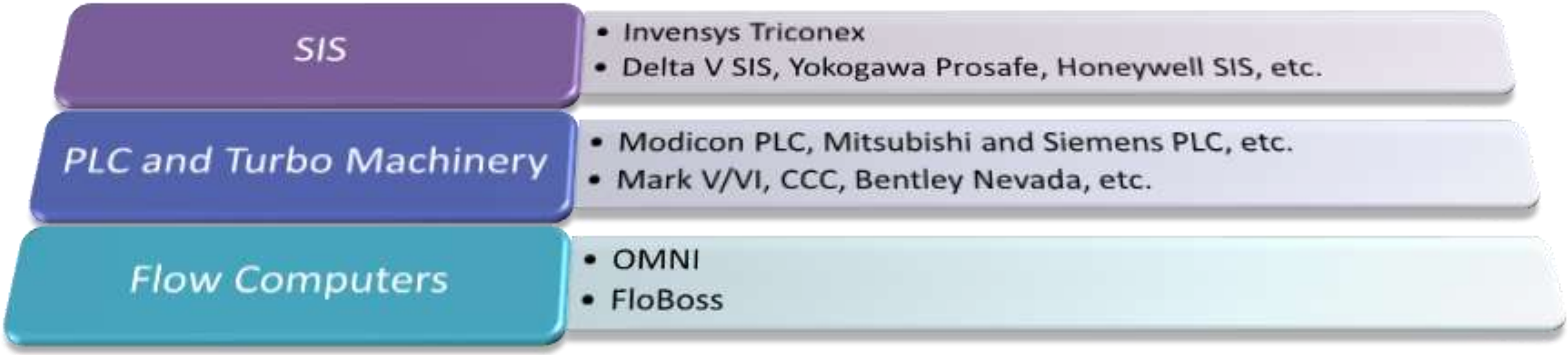
SCADA

- Invensys Wonderware
- GE iFIX, Fast/Tools Yokogawa etc.

DCS

- Emerson Delta V, Honeywell Experion
- Yokogawa Centum, ABB Bailey, Invensys Foxboro

ICS Environment



SIS

- Invensys Triconex
- Delta V SIS, Yokogawa Prosafe, Honeywell SIS, etc.

PLC and Turbo Machinery

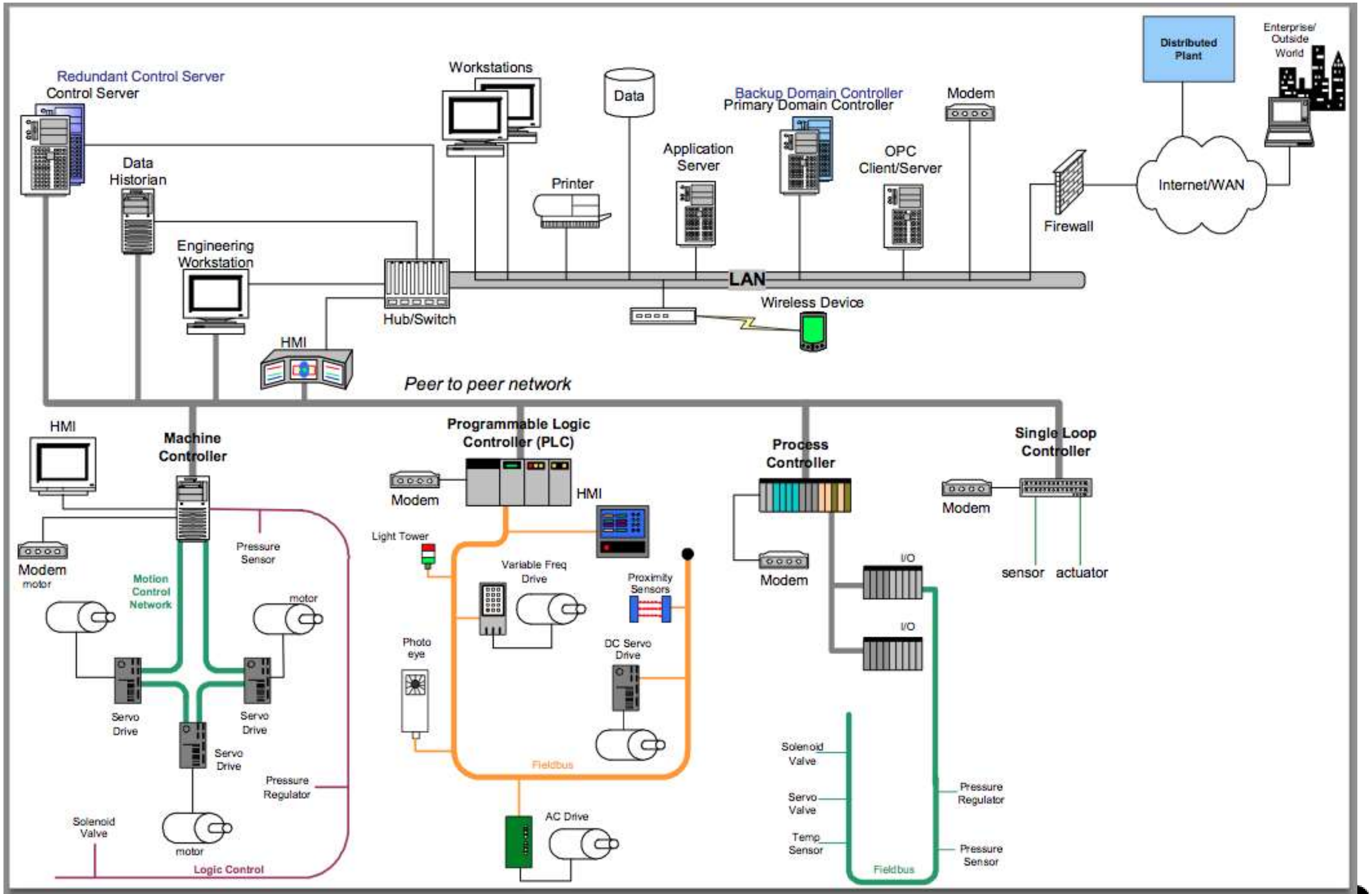
- Modicon PLC, Mitsubishi and Siemens PLC, etc.
- Mark V/VI, CCC, Bentley Nevada, etc.

Flow Computers

- OMNI
- FloBoss

Industrial Control System Overview

Typical sample of Industrial Control System (ICS)

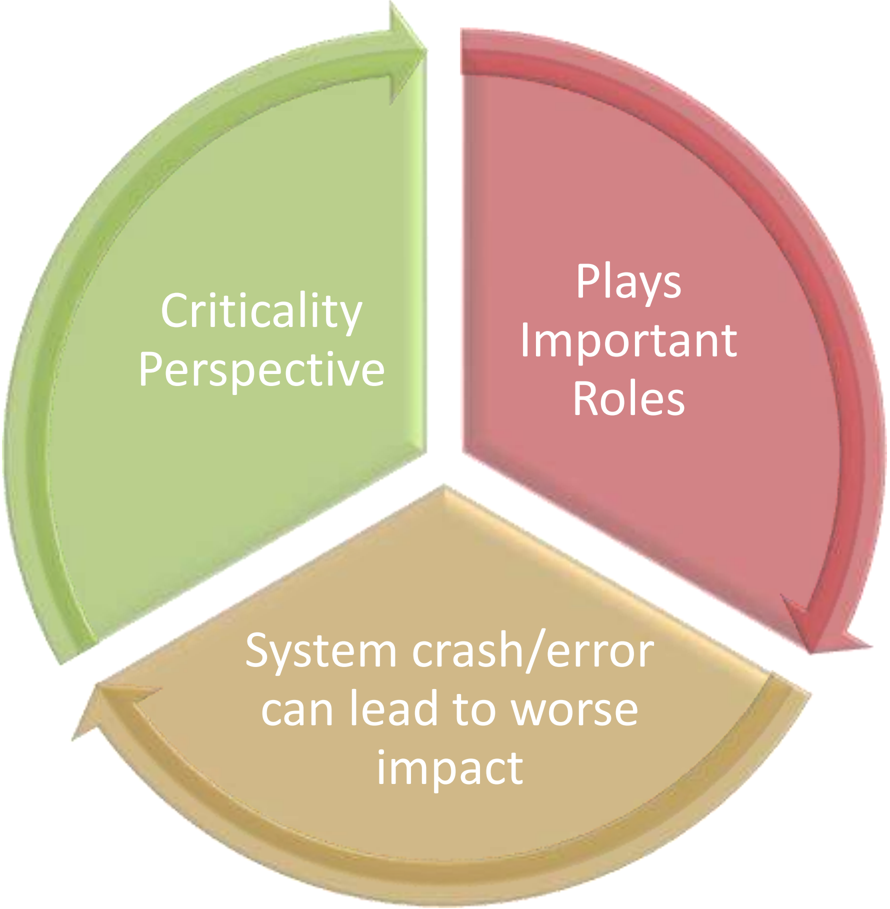


fedco.co.id

The Essential of Cyber Security in ICS

The Essential of Cyber Security in ICS

Why ICS is important


Criticality Perspective

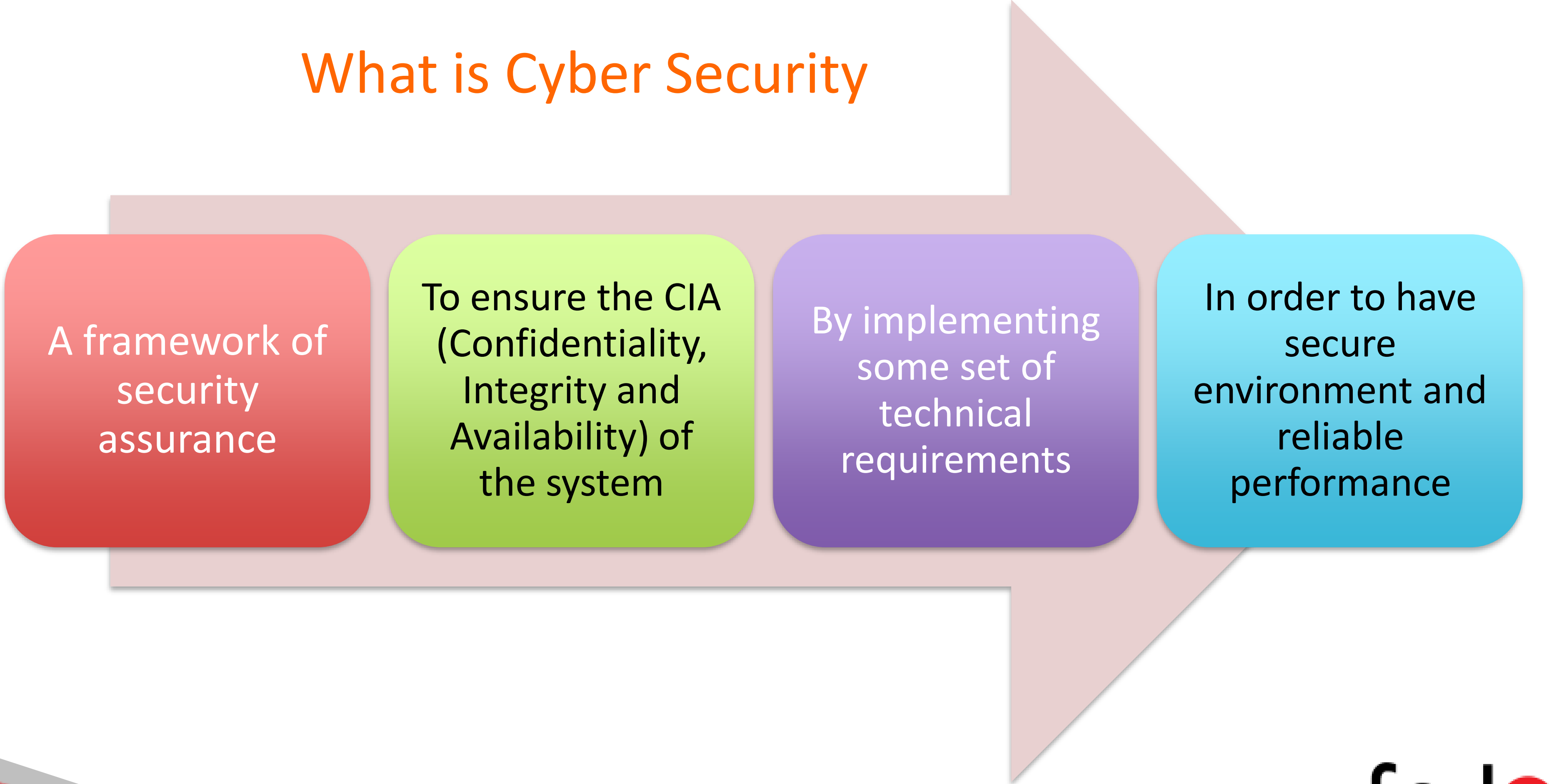
Plays Important Roles

System crash/error can lead to worse impact

“One of the crucial aspect that usually ignored in ICS is cyber security assurance”

The Essential of Cyber Security in ICS

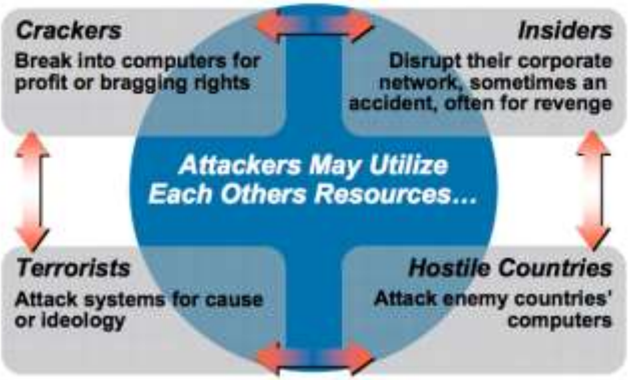
What is Cyber Security



A framework of security assurance
To ensure the CIA (Confidentiality, Integrity and Availability) of the system
By implementing some set of technical requirements
In order to have secure environment and reliable performance

The Essential of Cyber Security in ICS

Cyber Threat Facts



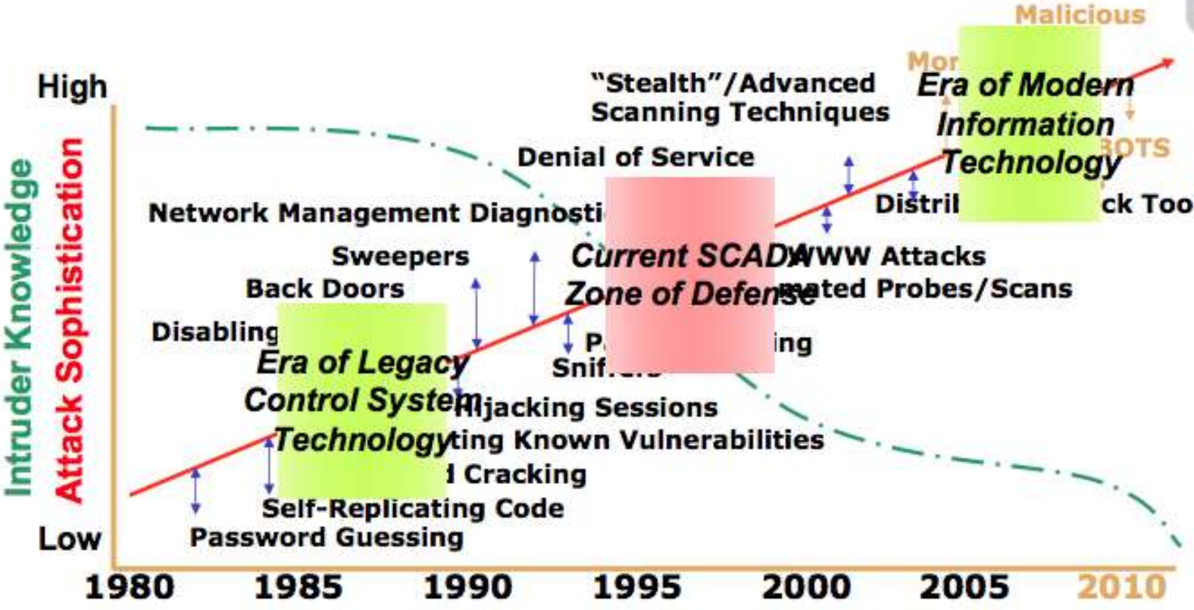
Crackers
Break into computers for profit or bragging rights

Insiders
Disrupt their corporate network, sometimes an accident, often for revenge

Attackers May Utilize Each Others Resources…

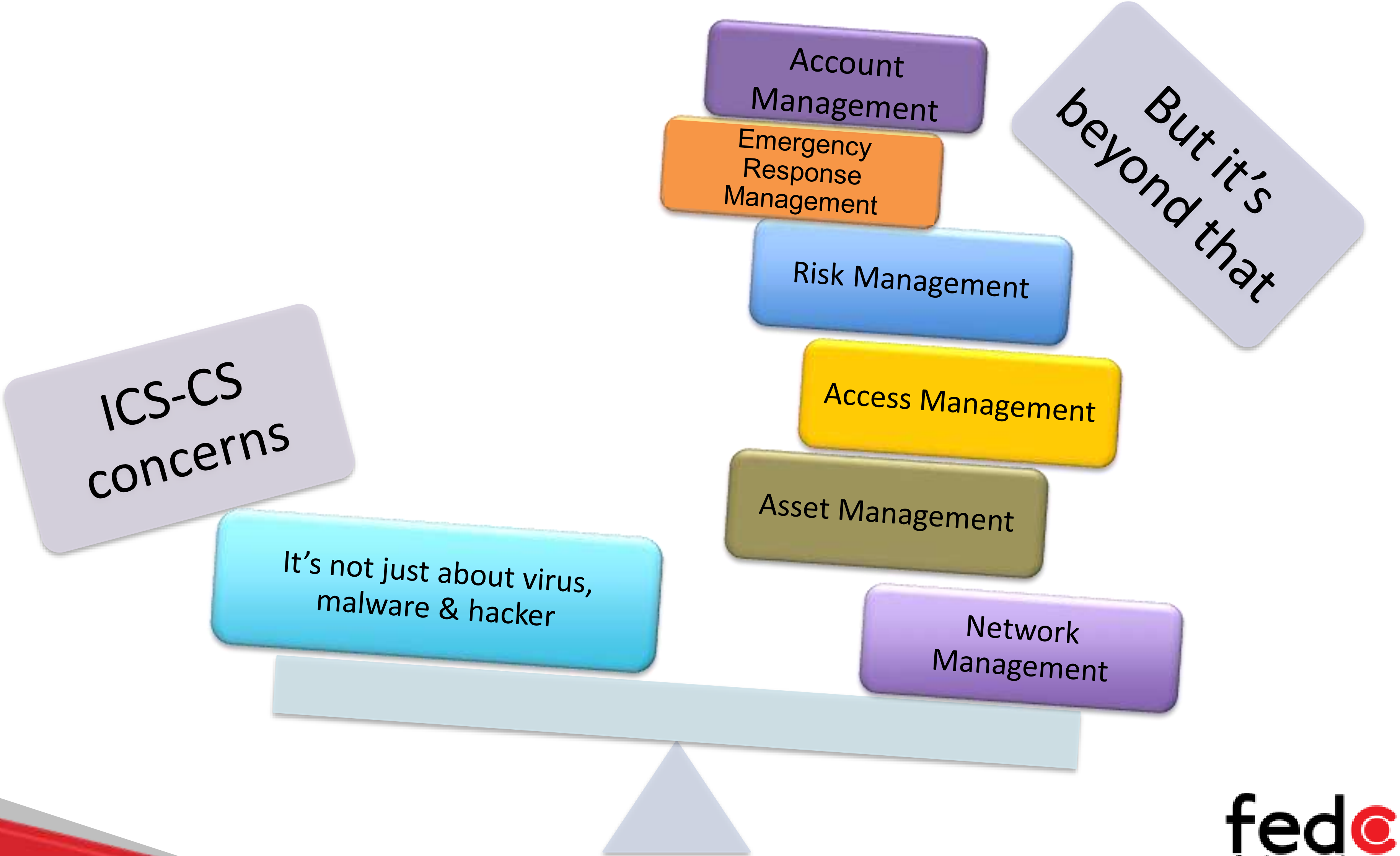
Terrorists
Attack systems for cause or ideology

Hostile Countries
Attack enemy countries' computers



Lipson, H. F., *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*, Special Report CMS/SEI-2002-SR-009, November 2002, page 10.

The Essential of Cyber Security in ICS



ICS-CS concerns

It's not just about virus, malware & hacker

But it's beyond that

Account Management

Emergency Response Management

Risk Management

Access Management

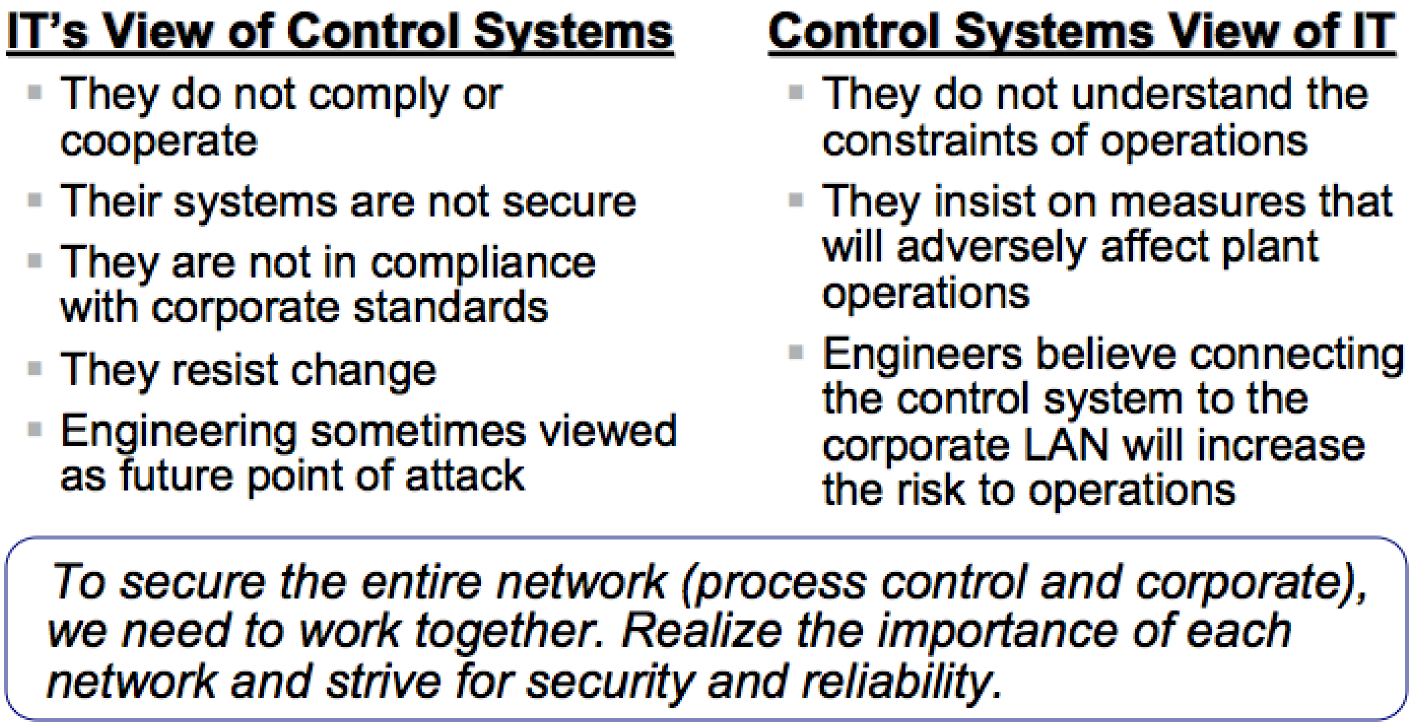
Asset Management

Network Management

No.	Threats	Vulnerabilities	Risks
1	Registry error in un-updated Windows environment	System error/crash with registry failed	Varies risk level, such as for DCS server, it will cause server error or down and will lead to plant shutdown (financial impact) For SIS system, failed in the communication interface with DCS system will lead to plant shutdown if no redundant line available
2	Internal/external intruder	No proper segregation between Business and Control Networks	System compromised with critical parameter changed, can lead to plant shutdown or disaster
3	Unauthorized access to critical system	Lack of access control management	System audit trail and critical system protection is compromised, can lead to sabotage, in-proper parameter setting, CIA aspects not guaranteed
4	System recovery failed	Lack of proper BCP/DRP and no proper backup and restore system management	In appropriate action plan if incident/disaster occur can lead to worse impact on safety/financial/environment

The Essential of Cyber Security in ICS

- Common Perceptions



IT's View of Control Systems

- They do not comply or cooperate
- Their systems are not secure
- They are not in compliance with corporate standards
- They resist change
- Engineering sometimes viewed as future point of attack

Control Systems View of IT

- They do not understand the constraints of operations
- They insist on measures that will adversely affect plant operations
- Engineers believe connecting the control system to the corporate LAN will increase the risk to operations

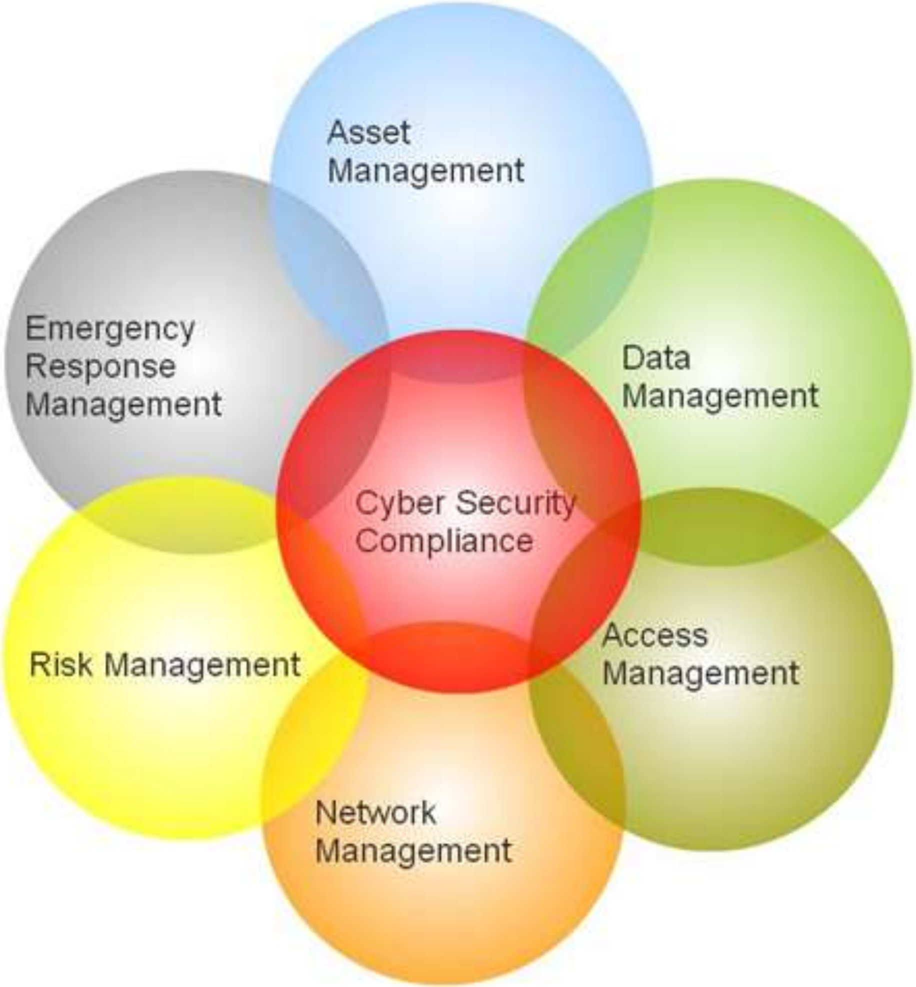
To secure the entire network (process control and corporate), we need to work together. Realize the importance of each network and strive for security and reliability.

The Essential of Cyber Security in ICS

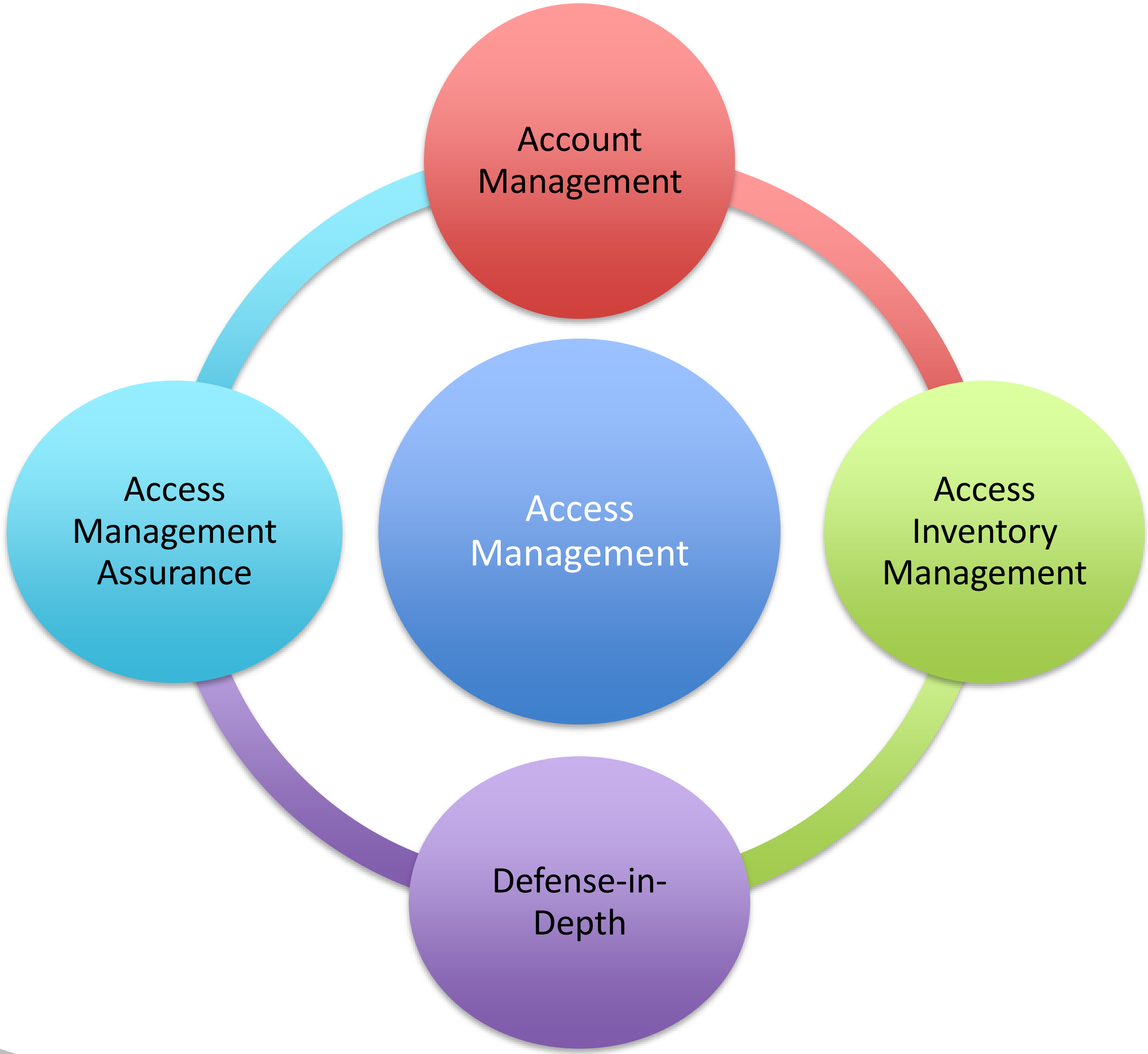
- Some challenges to deploy ICS-CS
  - Lack of awareness of the cyber security criticality in ICS environment
  - People thinking of ICS has no relation with ICT stuff, no need to deploy cyber security in ICS environment
  - Lack of capable professionals that has ability to cover Automation Control engineering and Information Communication Technology disciplines to deal with the Cyber Security Management and Compliance in ICS
  - Business driven is not seeing the critical requirement of having cyber security assurance for their ICS environment
  - Standards/policy/procedures/manuals not in place or inadequate
  - Culture and behaviour

ICS Cyber Security Management

ICS Cyber Security Management



ICS Cyber Security Management



Account Management

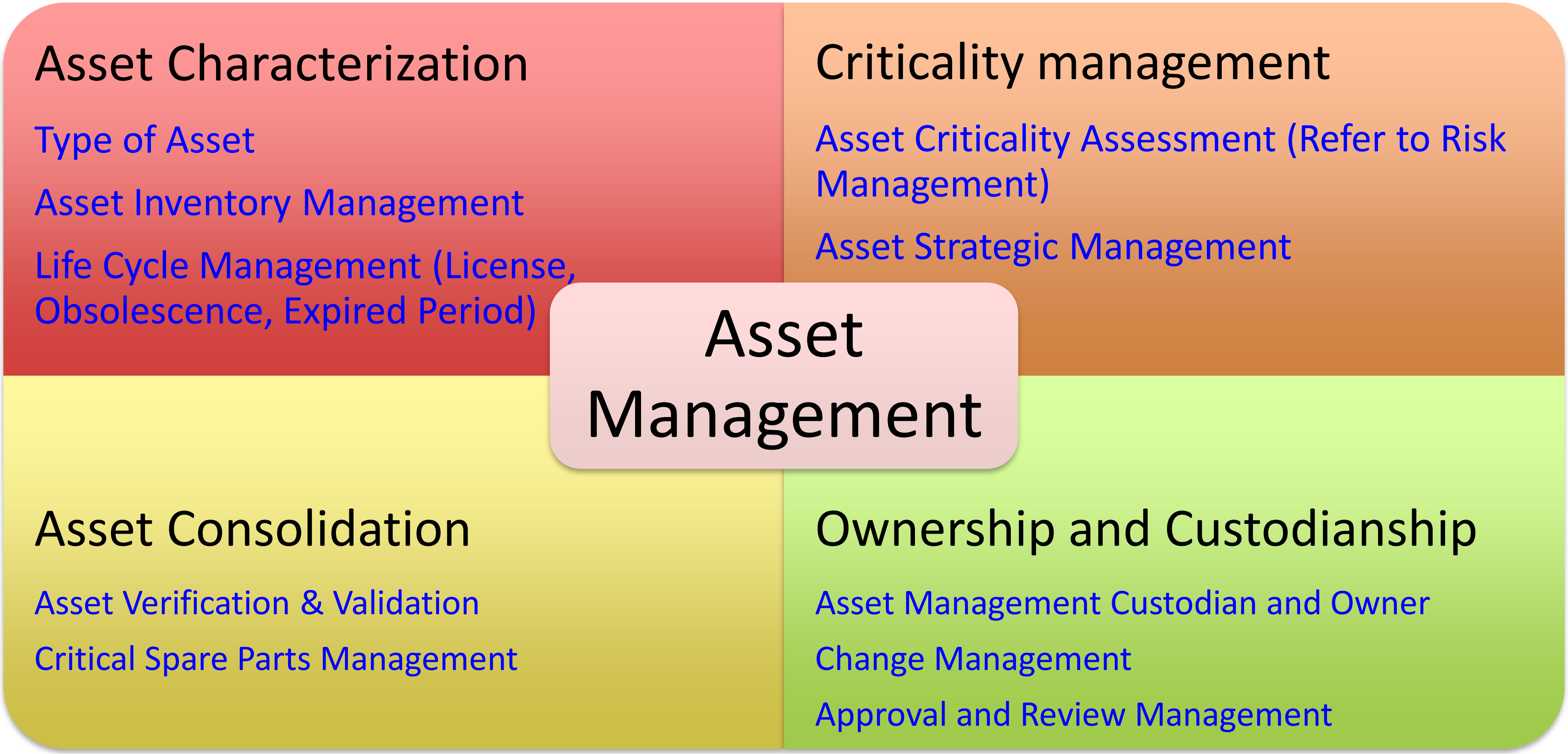
Access Management Assurance

Access Management

Access Inventory Management

Defense-in-Depth

ICS Cyber Security Management



Asset Management

Asset Characterization

- Type of Asset
- Asset Inventory Management
- Life Cycle Management (License, Obsolescence, Expired Period)

Criticality management

- Asset Criticality Assessment (Refer to Risk Management)
- Asset Strategic Management

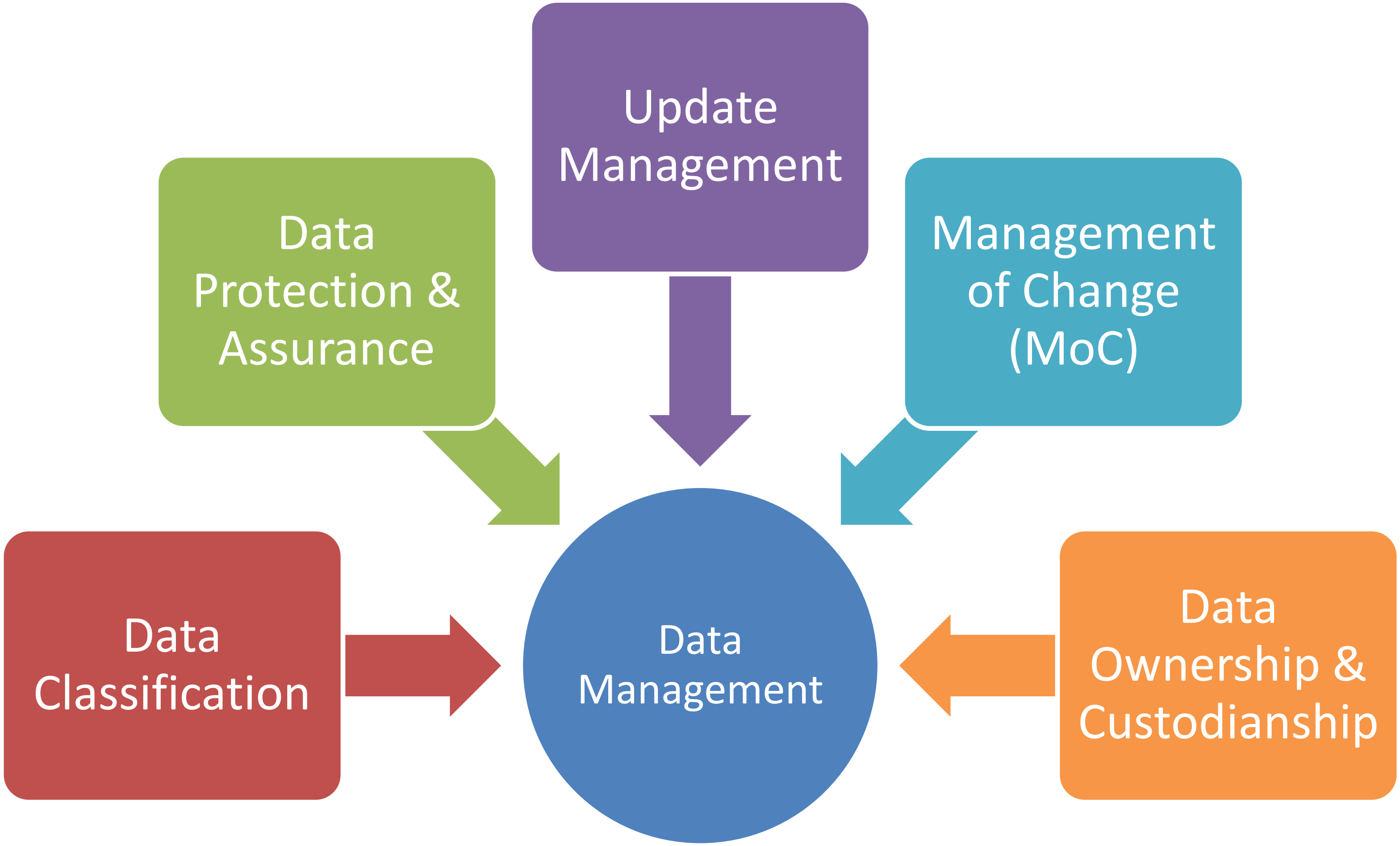
Asset Consolidation

- Asset Verification & Validation
- Critical Spare Parts Management

Ownership and Custodianship

- Asset Management Custodian and Owner
- Change Management
- Approval and Review Management

ICS Cyber Security Management



Update Management

Data Protection & Assurance

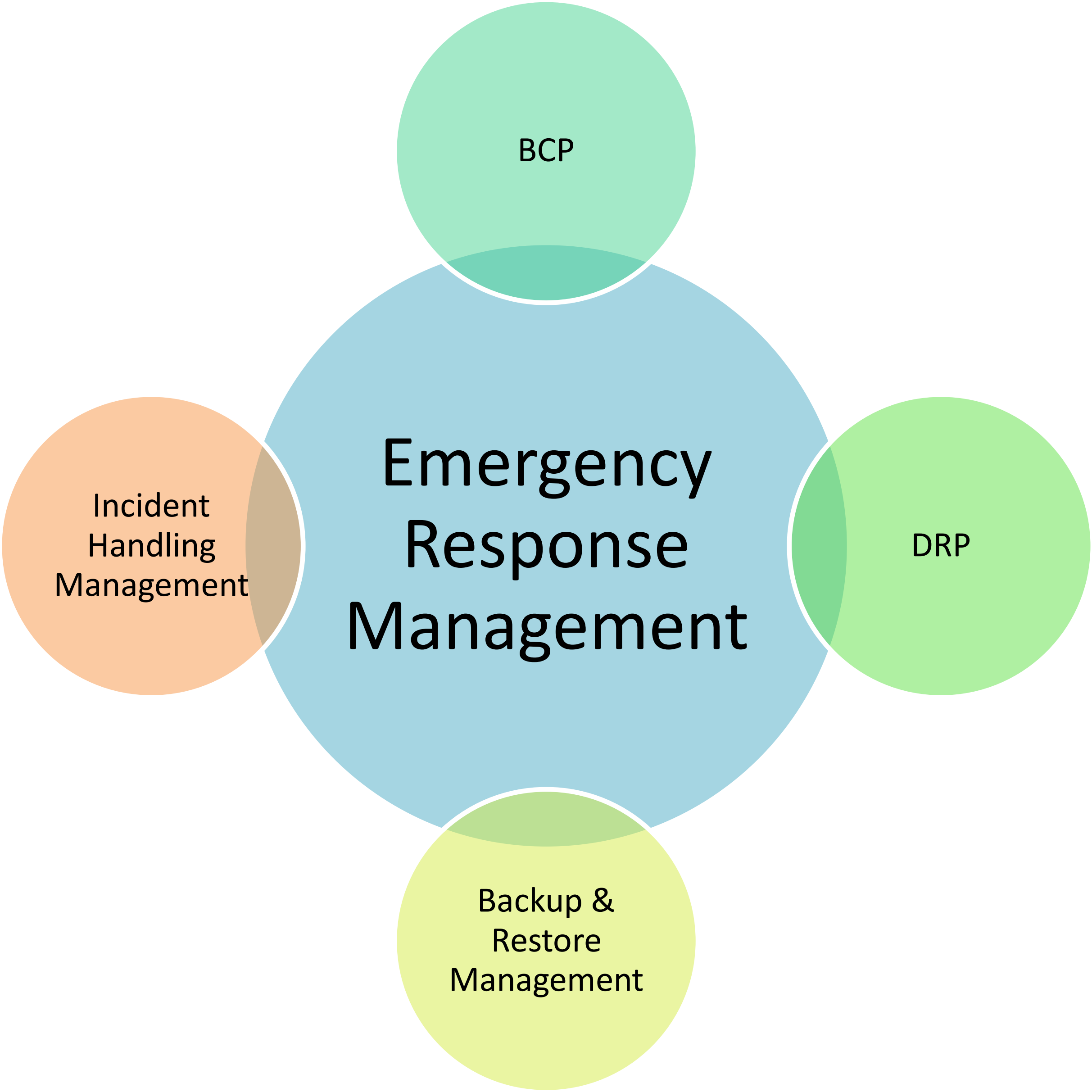
Management of Change (MoC)

Data Classification

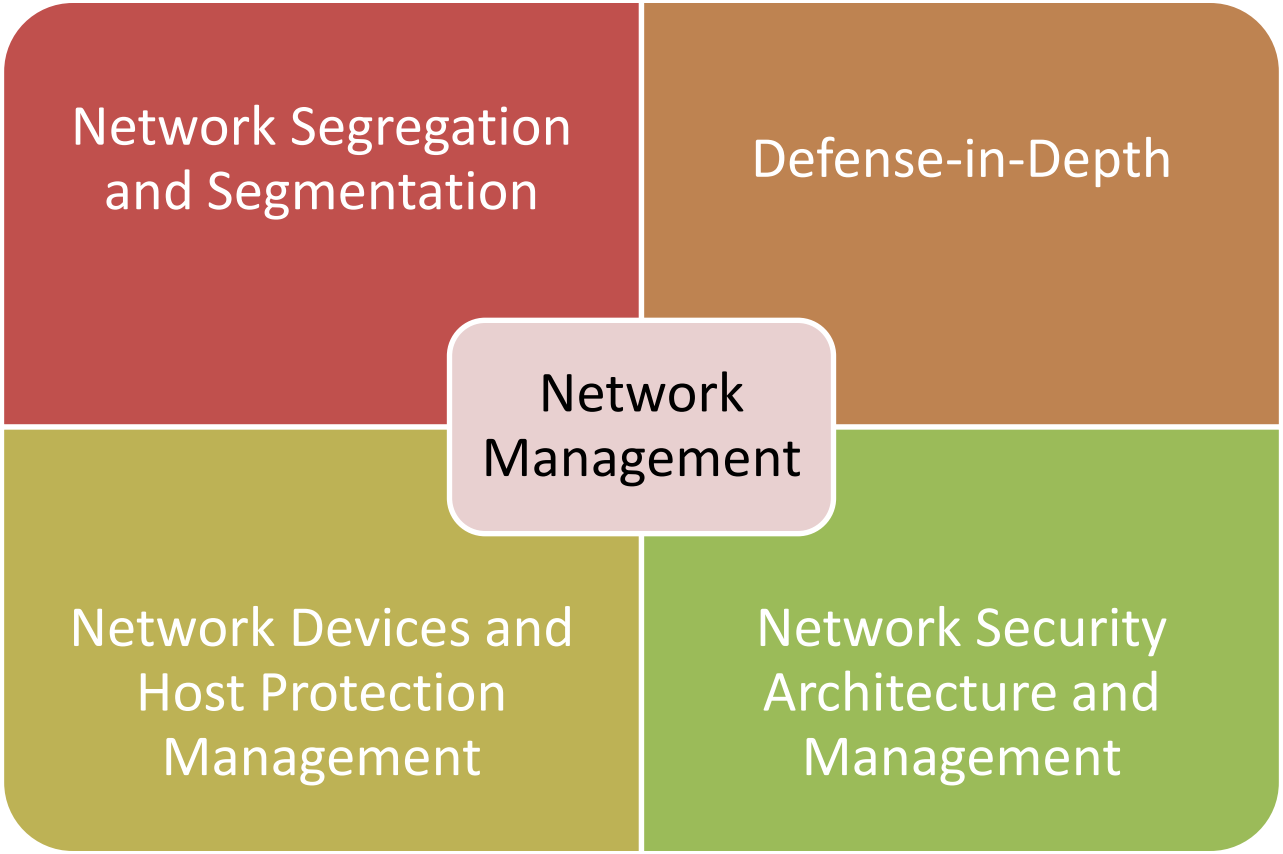
Data Management

Data Ownership & Custodianship

ICS Cyber Security Management


BCP
Incident Handling Management
Emergency Response Management
DRP
Backup & Restore Management

ICS Cyber Security Management


Network Segregation and Segmentation
Defense-in-Depth
Network Management
Network Devices and Host Protection Management
Network Security Architecture and Management

ICS Cyber Security Management

Risk Management Framework

Develop the team

Create Team charter

Specify the goals

Build the strategy

Risk Assessment Workshop

Define the Risk, Analyze the Risk, Past/Current/Future Situation Consideration, Scheme the Scenario, Define the Risk Level, Implement Controls Strategy, Assign Responsible Party, Put the Timeline, Controls Catalog Documentation

Controls Catalog Agreement

Actioner and Custodian Endorsement

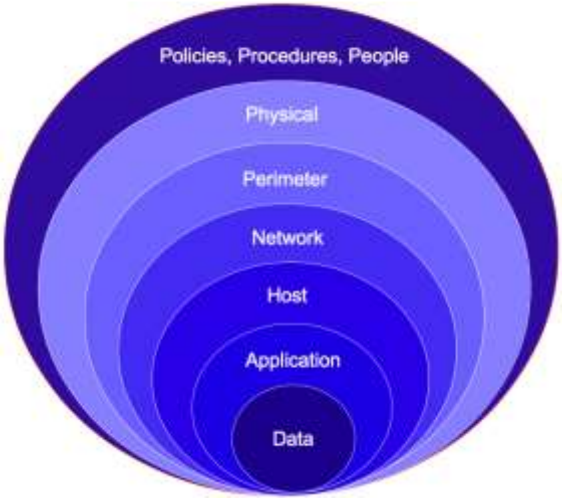
Owner and Management Approval

Action and Commitment

Sustainability and Periodic Review

(Some of) ICS Cyber Security Recommended Practices

ICS Cyber Security Recommended Practices



Defense-in-Depth in ICS-CS

Policies, Procedures, People

Framework of standard & guidelines, people competency and expertise regarding ICS-CS

Physical

Physical security control to protect and restrict access to control system environment and critical assets (such as secure locked door with smart card access, fence perimeter with 24/7 access control, etc.

Perimeter

More restricted access with strengthen and limited access control, such as DCS locked cabinet, controlled network infrastructure cabinet, highly restricted server room access, etc.

Network

Internal network architecture and configuration to ensure secure access in ICS environment. External network and business network interface should be highly concerned for secure access assurance

Host

HMI, workstation, Engineering station, operator station, maintenance laptop, vendor access laptop, should be managed and controlled appropriately with least privilege access as default

Application

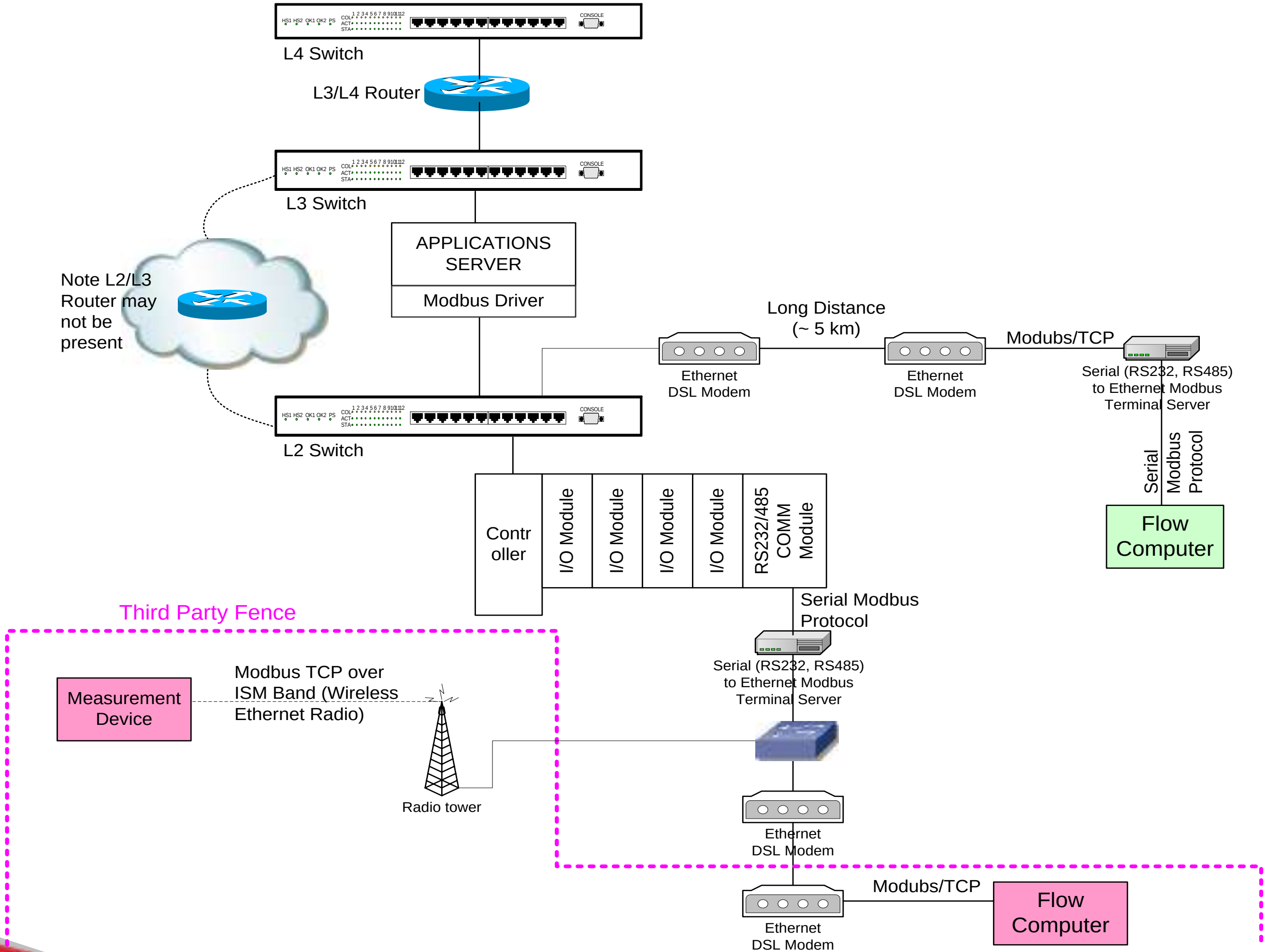
Open and proprietary application management for ICS environment

Data

Data CIA assurance and management

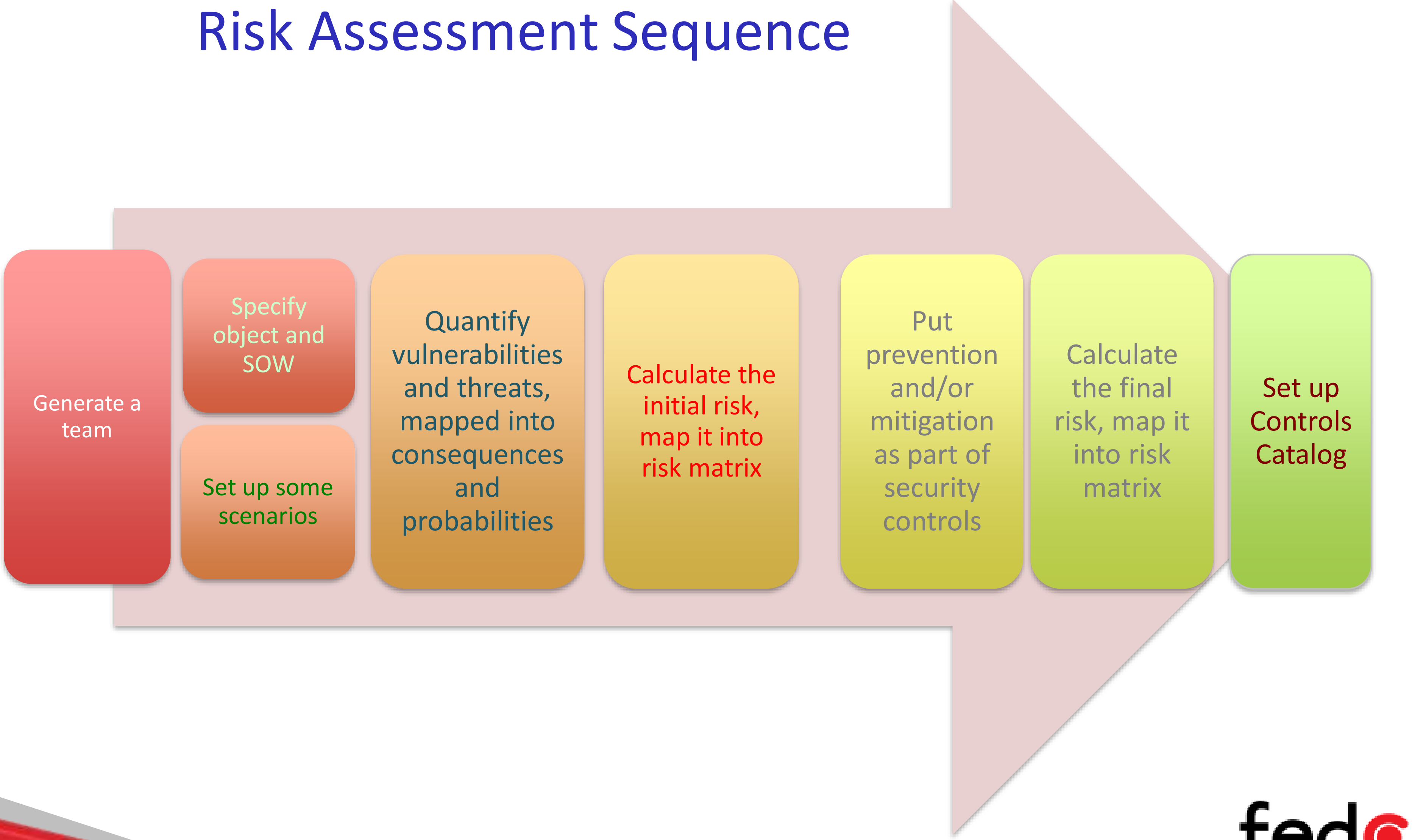
ICS Cyber Security Recommended Practices

- External Network Management
  - ✓ Risk assessed, controls strategy development, put controls in place, access control implementation, periodic review



ICS Cyber Security Recommended Practices

Risk Assessment Sequence



Generate a team

Specify object and SOW

Set up some scenarios

Quantify vulnerabilities and threats, mapped into consequences and probabilities

Calculate the initial risk, map it into risk matrix

Put prevention and/or mitigation as part of security controls

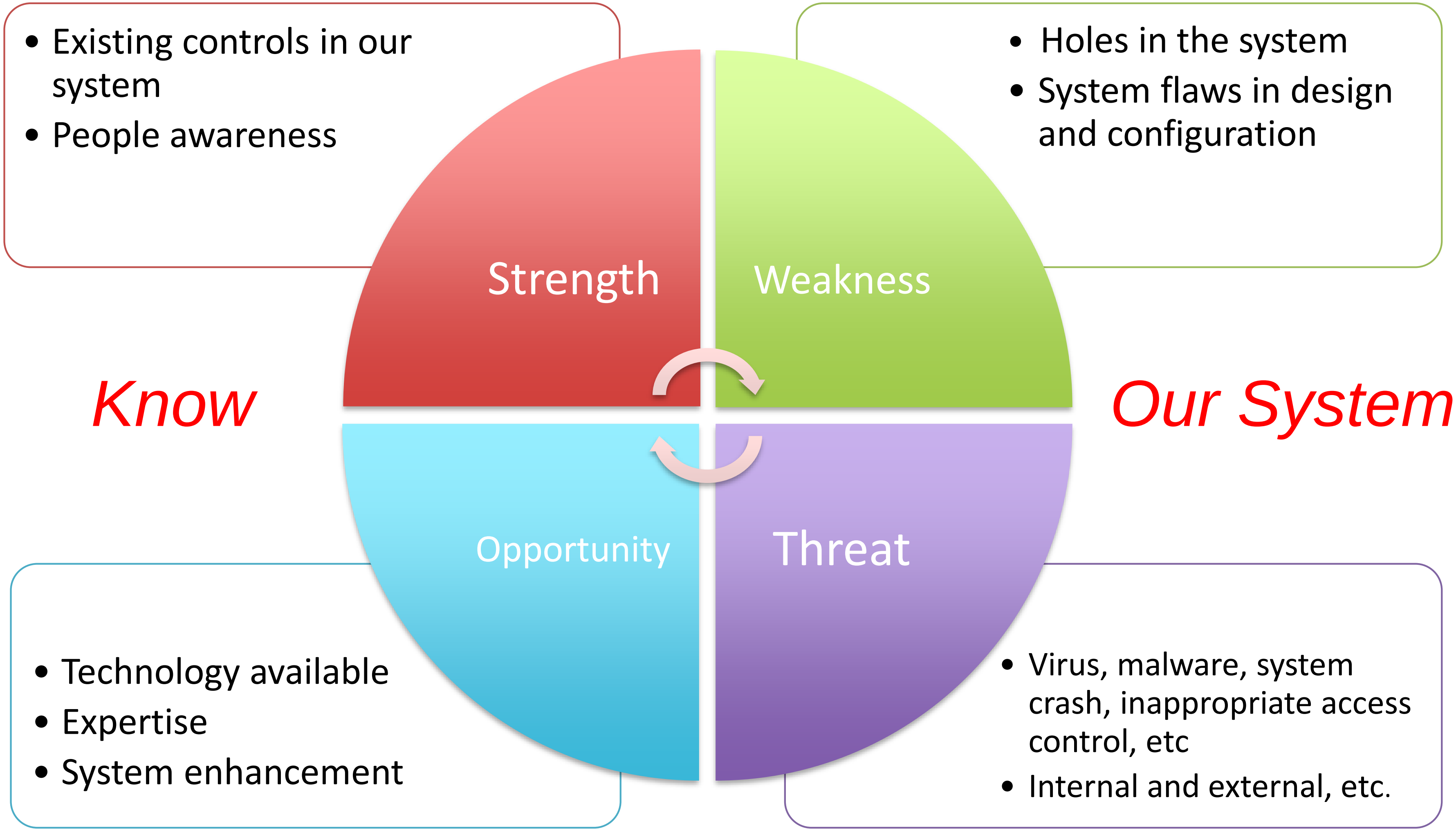
Calculate the final risk, map it into risk matrix

Set up Controls Catalog

ICS Cyber Security Recommended Practices

- Every System is Unique
  - Develop the policy based on local situation
  - Observe, assess, strategize and implement
- Special Strategy for Every System
  - Consider the special situation
  - Consider the system architecture and the environment
- Risk Prevention, Mitigation and Controls Strategy
  - Develop integrated and robust risk assessment
  - Formulate the scenario, assess the consequence, apply risk controls
  - One package, one summary and one agreed action

ICS Cyber Security Recommended Practices



- Existing controls in our system
- People awareness

- Holes in the system
- System flaws in design and configuration

Strength

Weakness

Know

Our System

Opportunity

Threat

- Technology available
- Expertise
- System enhancement

- Virus, malware, system crash, inappropriate access control, etc
- Internal and external, etc.

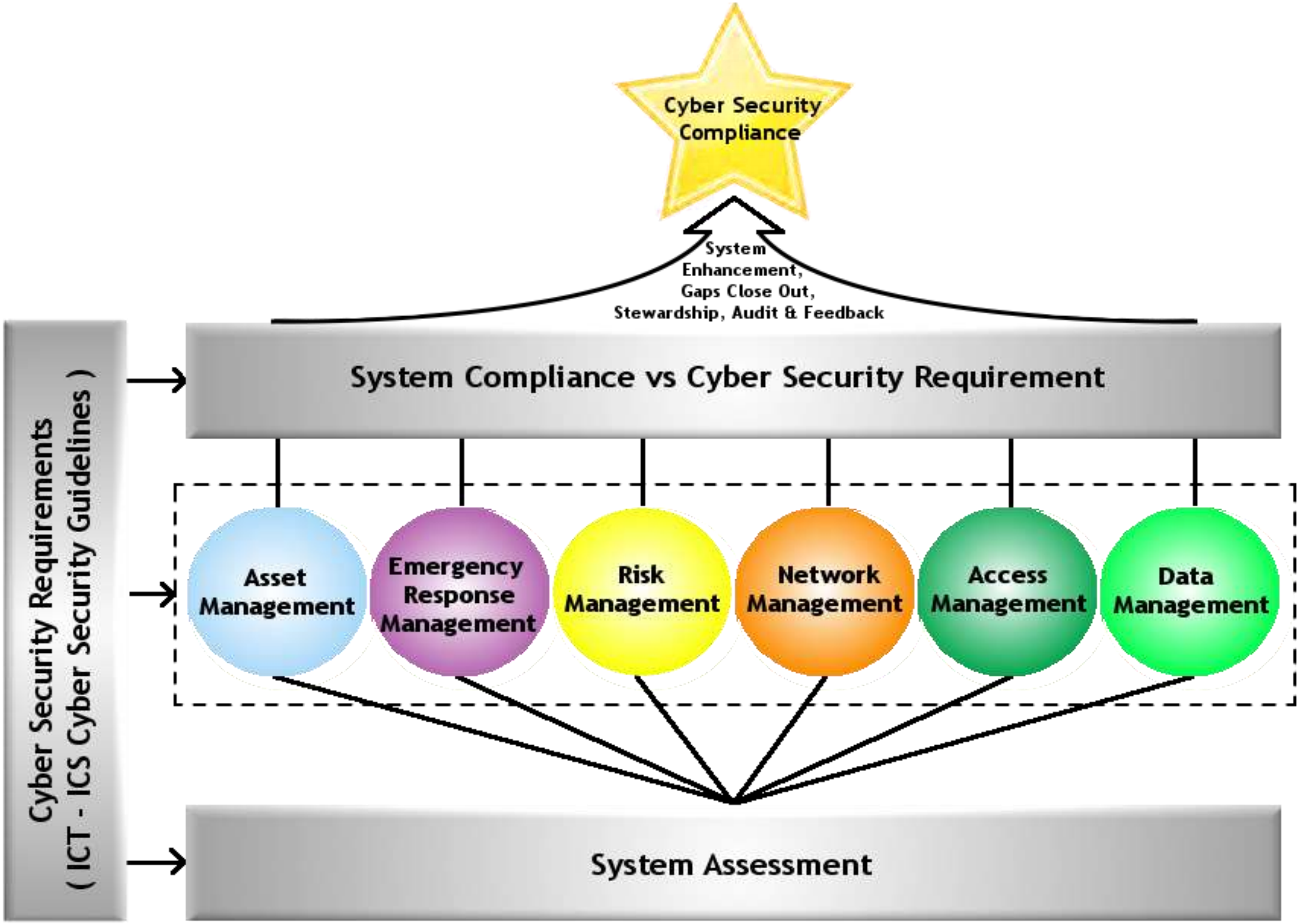
Sustainability, Stewardship and Compliance

Sustainability, Stewardship and Compliance

- Cyber Security Compliance
  - Assess, strategize and comply with the high and medium risk level requirement
  - System and people awareness are critical
  - Working as a team (ICS engineer, IT support, Operations & Maintenance, Third Party support, and Management)
  - Use ICS-CS assessment platform and controls catalogue as the references

Sustainability, Stewardship and Compliance

- Sustainability and Stewardship
  - Steering committee (team) or dedicated person for ensuring compliance sustainability
  - Periodic review including access review, asset inventory (H/W & S/W), risk assessment, emergency response testing, etc.
  - Periodic Audit and Feedback for robust system compliance and sustainability assurance (Team and Management)
  - Controls Calendar


Cyber Security Compliance
System Enhancement, Gaps Close Out, Stewardship, Audit & Feedback
System Compliance vs Cyber Security Requirement
Asset Management
Emergency Response Management
Risk Management
Network Management
Access Management
Data Management
System Assessment
Cyber Security Requirements (ICT - ICS Cyber Security Guidelines)

fedco.co.id

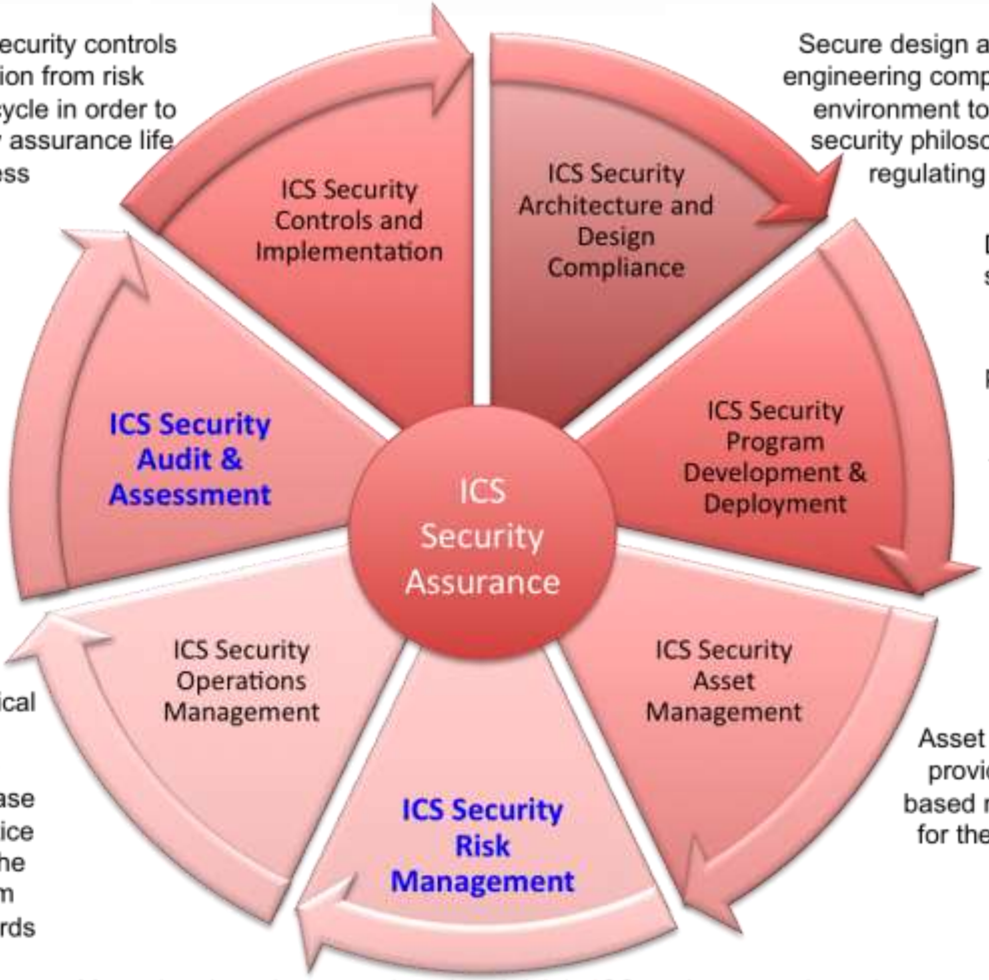
Standard and References

Standard and References

Some standards related to ICS-CS:

- NIST SP 800-82
  Guide to ICS Security
- API STD 1164
  Pipeline SCADA Security
- IEC 62443-3
  Network and System Security
- ISA 99
  Security for Industrial Automation and Control System
- ISO 27001
  Information Security Management System

SCADA ICS Security Assurance Services



ICS Security Assurance

ICS Security Controls and Implementation

ICS Security Architecture and Design Compliance

ICS Security Program Development & Deployment

ICS Security Asset Management

ICS Security Risk Management

ICS Security Operations Management

ICS Security Audit & Assessment

Implementing the ICS security controls as per recommendation from risk assessment and audit cycle in order to ensure the ICS security assurance life cycle process

Secure design architecture and engineering compliance of an ICS environment to meet the ICS security philosophy based on regulating standard

Develop and deploy* the short term and long term ICS security program to cover the Operations phase in order to ensure the continual improvement lifecycle

*the next steps will cover the actual ICS security program deployment in more detail content

Asset criticality assessment to provide the proper asset risk based management as the basis for the ICS security assurance level

Managing the cyber security related risk in ICS environment through risk assessment, strategic security planning and controls action

Assistance and technical consultancy in ICS security assurance during Operations phase to ensure actual practice compliance against the ICS security program and regulating standards

Auditing ICS environment against ICS security standard to have the detail ICS security posture and its compliance level

CONTACT US

fedco

www.fedco.co.id

fedco@fedco.co.id