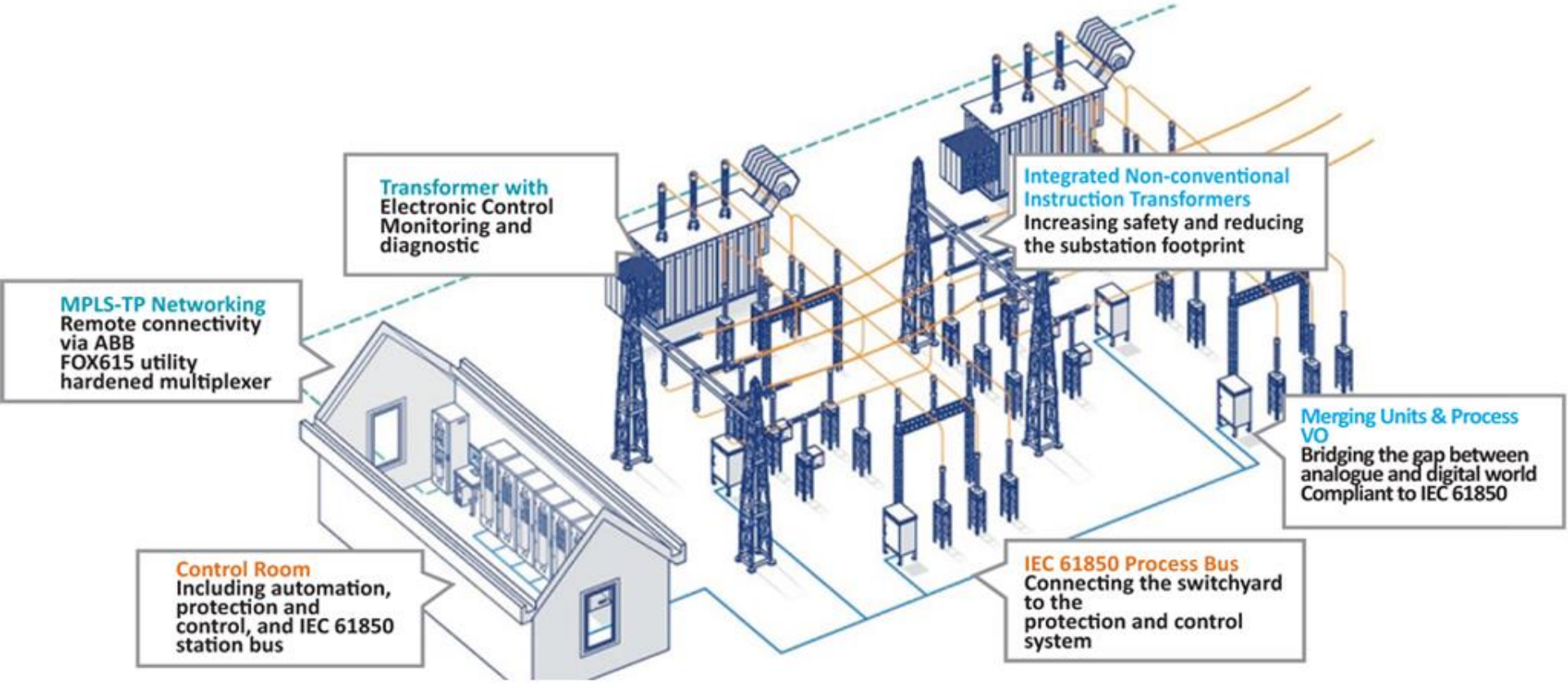
Cyber Security for the DIGITALISED GRID

A B SENGUPTA

Content

Understanding Power Sector OT System
Evolution of Threats against ICS
Analyzing threats on SCADA System
Future Road Map -Advanced Security Strategies

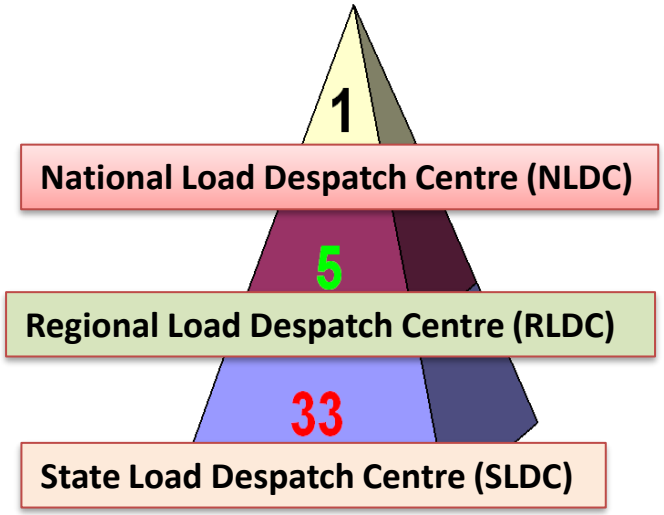
Understanding Power System Operations Technology (OT) (Indian Context)



Coordinated Multilateral Grid Operation

Mission of POSOCO

"Ensure Integrated Operation of Regional and National Power Systems to facilitate transfer of electric power within and across the regions and trans-national exchange of power with ***Reliability, Security and Economy"***



Functions of POSOCO

- Supervise and Control aspects concerning operations
- Apex organization for HR requirements
- Planning and implementation of infrastructure
- Co-ordinate the functioning of NLDC & RLDCs
- Advise and assist SLDCs including Specialized Training

Functional Autonomy
Independent Government Company
3rd Jan 2017

Financial Autonomy
CERC Fees and Charges Regulations
2009-14, 2014-19

MoP

POSOCO

Regulatory Framework
CERC

Grid Standards
CEA

NLDC, Delhi | **NRLDC, Delhi** | **ERLDC, Kolkata** | **WRLDC, Mumbai** | **SRLDC, Bengaluru** | **NERLDC, Shillong**

Overarching Regulatory Framework

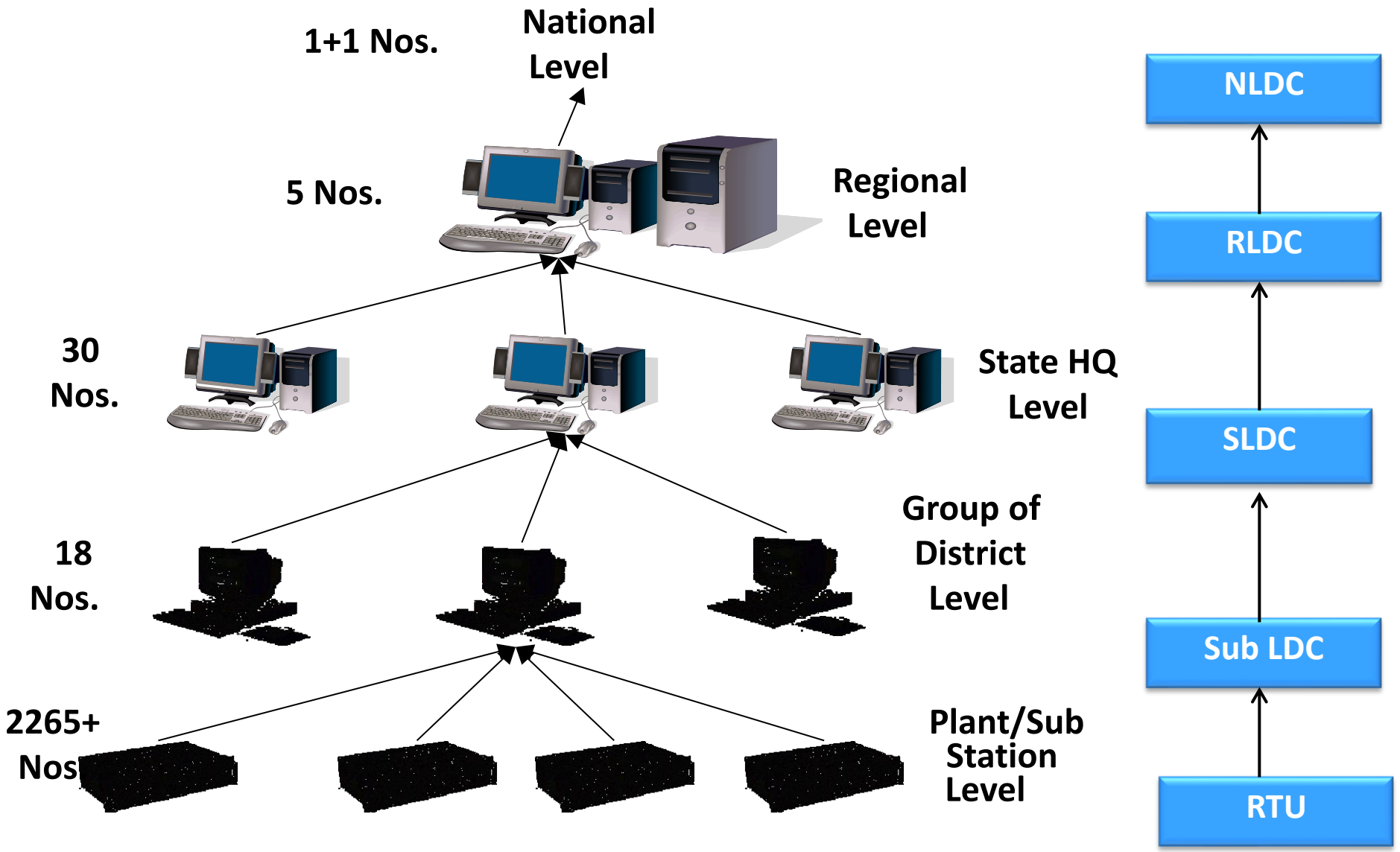
CERC

- **Regulations**
- Open Access in Inter-State Transmission
- Grant of Connectivity, LTA and MTOA
- Measures to relieve Congestion
- Grant of trading licence
- Power Market
- Renewable Energy Certificate
- Indian Electricity Grid Code
- Sharing of ISTS Charges & Losses
- Regulation of Power Supply
- Fixation of Trading Margin
- Intervening Transmission Facilities
- Standards of Performance
- Terms and Conditions of Tariff
- Power System Development Fund
- Deviation Settlement Mechanism
- Fees and Charges of RLDC
- Ancillary Services Operations
- Energy Savings Certificates
- Communication in Power Sector

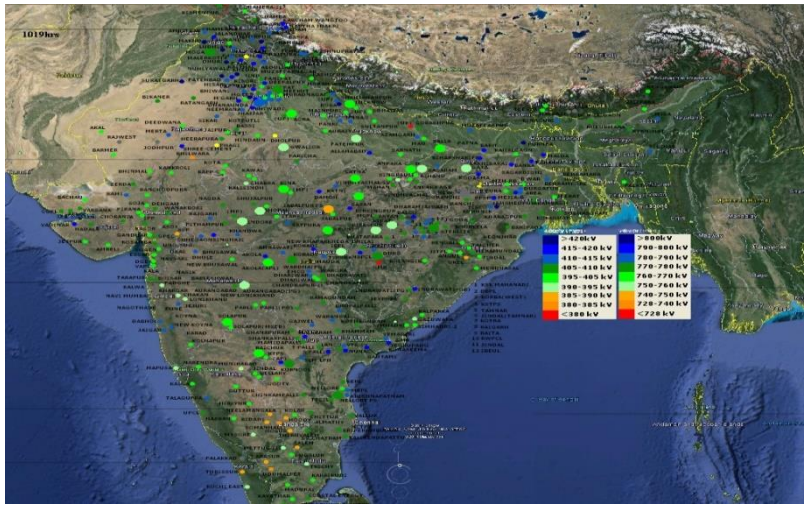
CEA

- **Standards**
- Grid Standards
- Connectivity to the Grid
- Installation and Operation of Meters
- Technical Standards for Connectivity of the Distributed Generation Resources
- Safety and Electricity Supply
- Technical Standards for Construction of Electrical Plants and Electric Lines

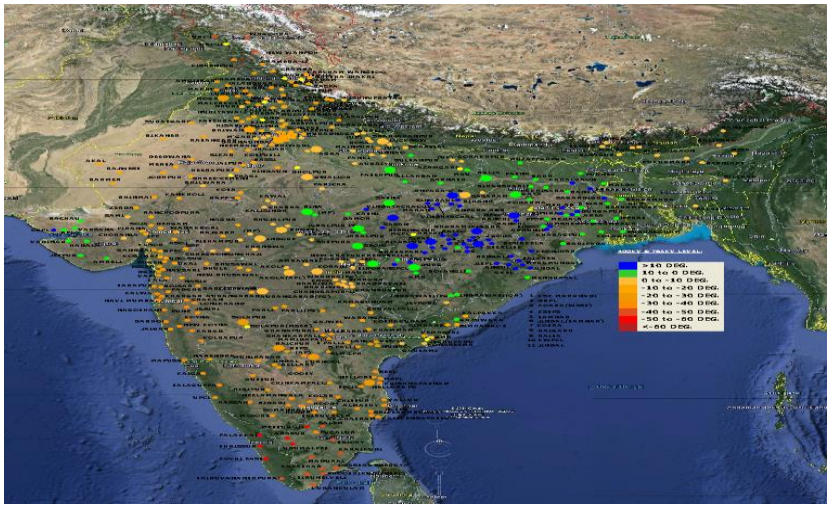
Control Centre Communications



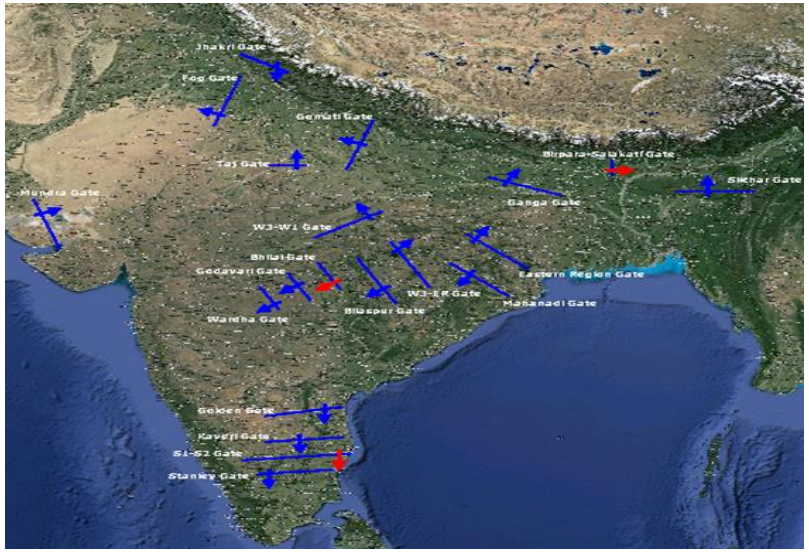
Visualisation Displays for System Operator



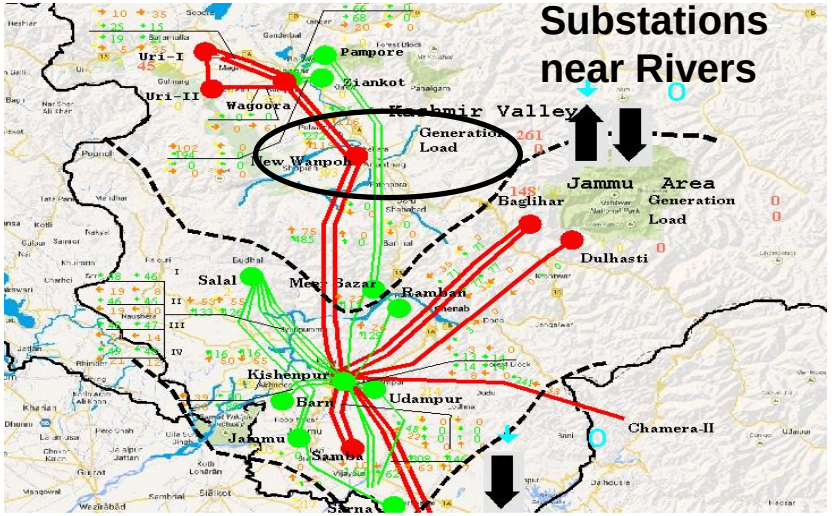
Contour Map - Voltage



Contour Map – Estimated Angle

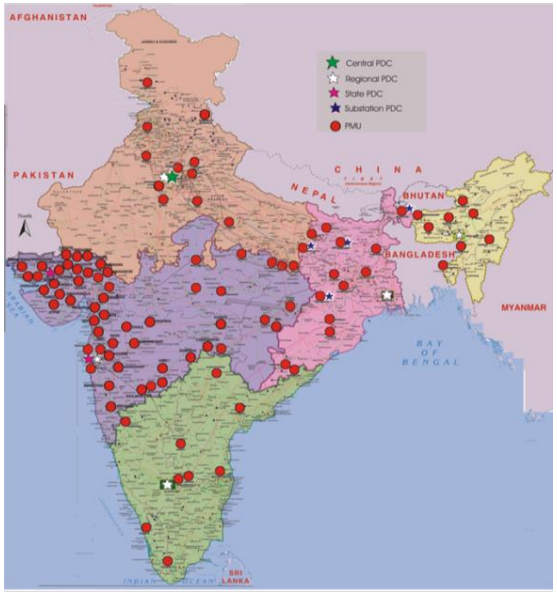


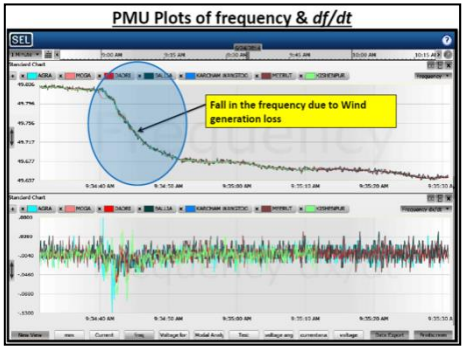
Flow Gate visualisation

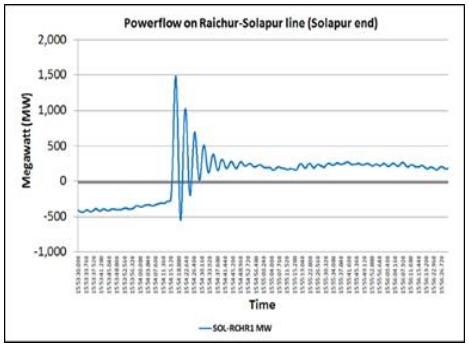


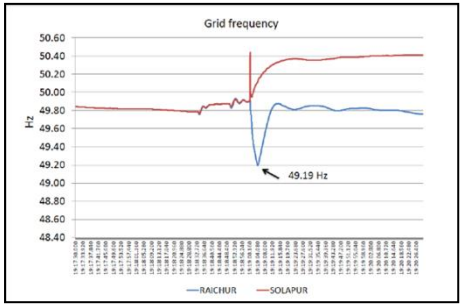
Display for disasters

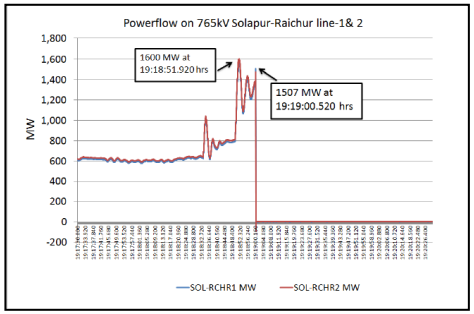
Technological Advancements - Phasor Measurement Units (PMU)











- Total number of installed PMUs: **1180 Nos. +**
  a. Pilot Project - 64 Nos.
  b. Gujarat - 75 Nos.
  c. Maharashtra - 15 Nos.
  d. URTDSM - >1000 Nos.
  (Unified Real Time Dynamic State Measurement System)

- Data from PMUs being used for improving grid performance

- URTDSM Scheme approved by CERC
  - Implementation by PGCIL with 1750 PMUs

- Three reports on WAMS by POSOCO:
  http://posoco.in/otherreports.aspx

Evolution of Threats Against Industrial Control System (ICS)

Why is ICS Security needed

Cyberattack becomes easier while ICS (OT System) becomes IT-like.

Convergence of IT and ICS(Industrial Control System)

- "Ethernet" becomes popular in the ICS network
- Dedicated OS to Versatile OS (Windows Embedded, Linux etc.)

Evolution of the targeted attack to ICS system

- 2010 Stuxnet Nuclear facilities in Iran were destroyed.
- 2014 Operation Dragonfly OPC information leakage in several European EPCOs
- 2015 Ukraine Attack(West) Blackout by the cyber attack(penetration to SCADA system)
- 2016 Ukraine Attack(Kiev) Blackout by the cyber attack(Time bomb, Modulization)
- 2017 TRISIS-TRITON-Hatman Safety system was attacked by the cyber attack

Formulate Security Guidelines for ICS/Critical Infrastructure

- ICS security Standard (International : IEC62443 Industry : NERC CIP, NIST IR 7628)
- National level efforts (US : NIST Cybersecurity Framework EU : NIS Directive)

Special & General

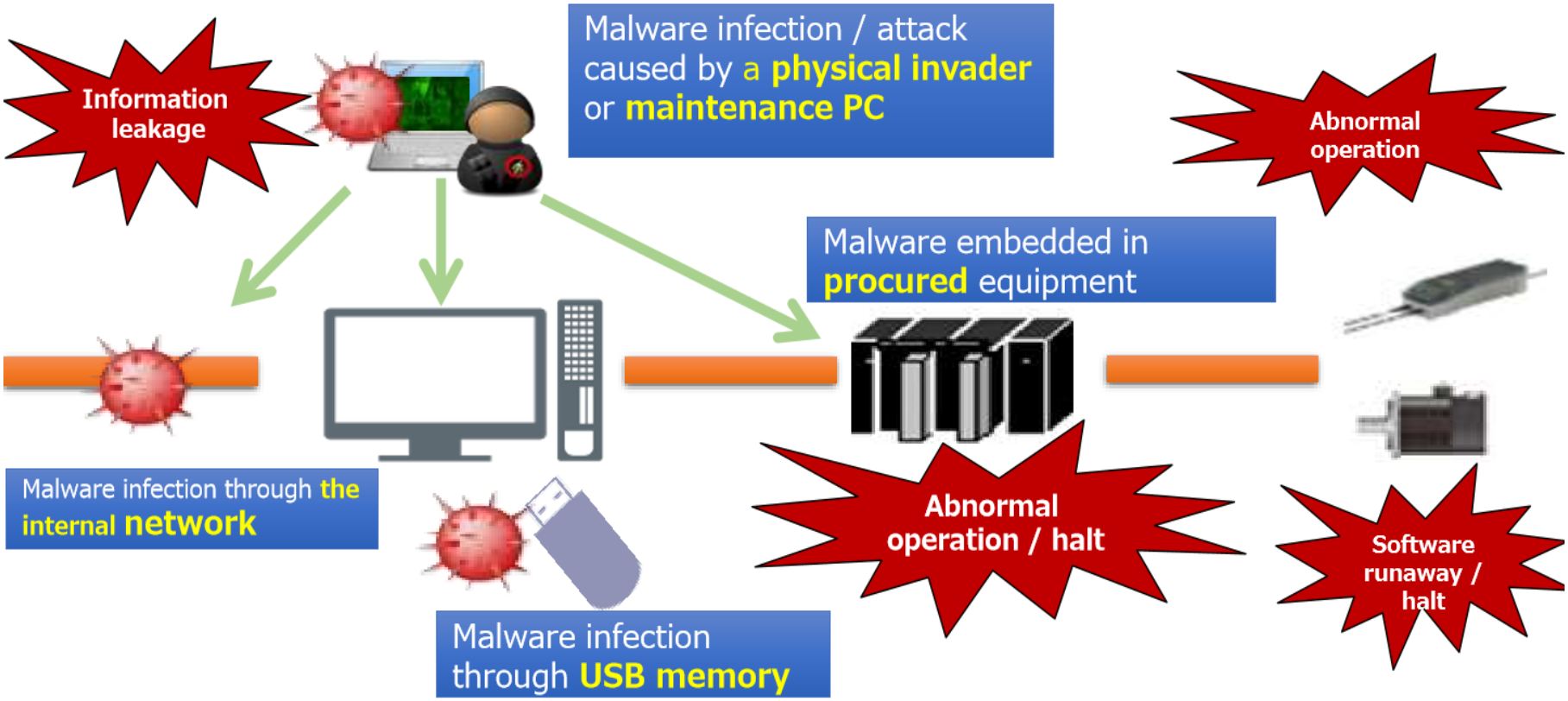
Stuxnet could realize much more easily now.
（Generalization enables cost-down of ICS malware development）

Attack	Feature
Stuxnet	- Crash purpose - Highly sophisticated & targeted attack - One single target
Operation Dragonfly	- Reconnaissance, Test purpose - General Target - General technology, understanding ICS operation
Ukraine 2015	- Crash, Outage purpose - Targeted attack and several targets - Direct Operation via Internet
Crashoverride /Industroyer 2016	- Crash, Outage purpose - Targeted attack and one single target - highly understanding ICS protocol - Modularization, Time bomb
TRISIS-TRITON-Hatman 2017	- Crash, Outage purpose - Targeted attack and one single target - highly understanding ICS safety

Analyzing Threat On SCADA System

ICS Threats

Security risks involved in a CLOSED SYSTEM (ICS)



Security Risk Scenario

Safety ←Addition

- Injury accident caused by malfunction of equipment
- Physical failures / breakage of equipment

And others

Availability

- Halt to production caused by system malfunction
- Decreased production caused by system malfunction

And others

Integrity

- Defective products caused by alteration
- Alteration of production data / daily report

And others

Confidentiality

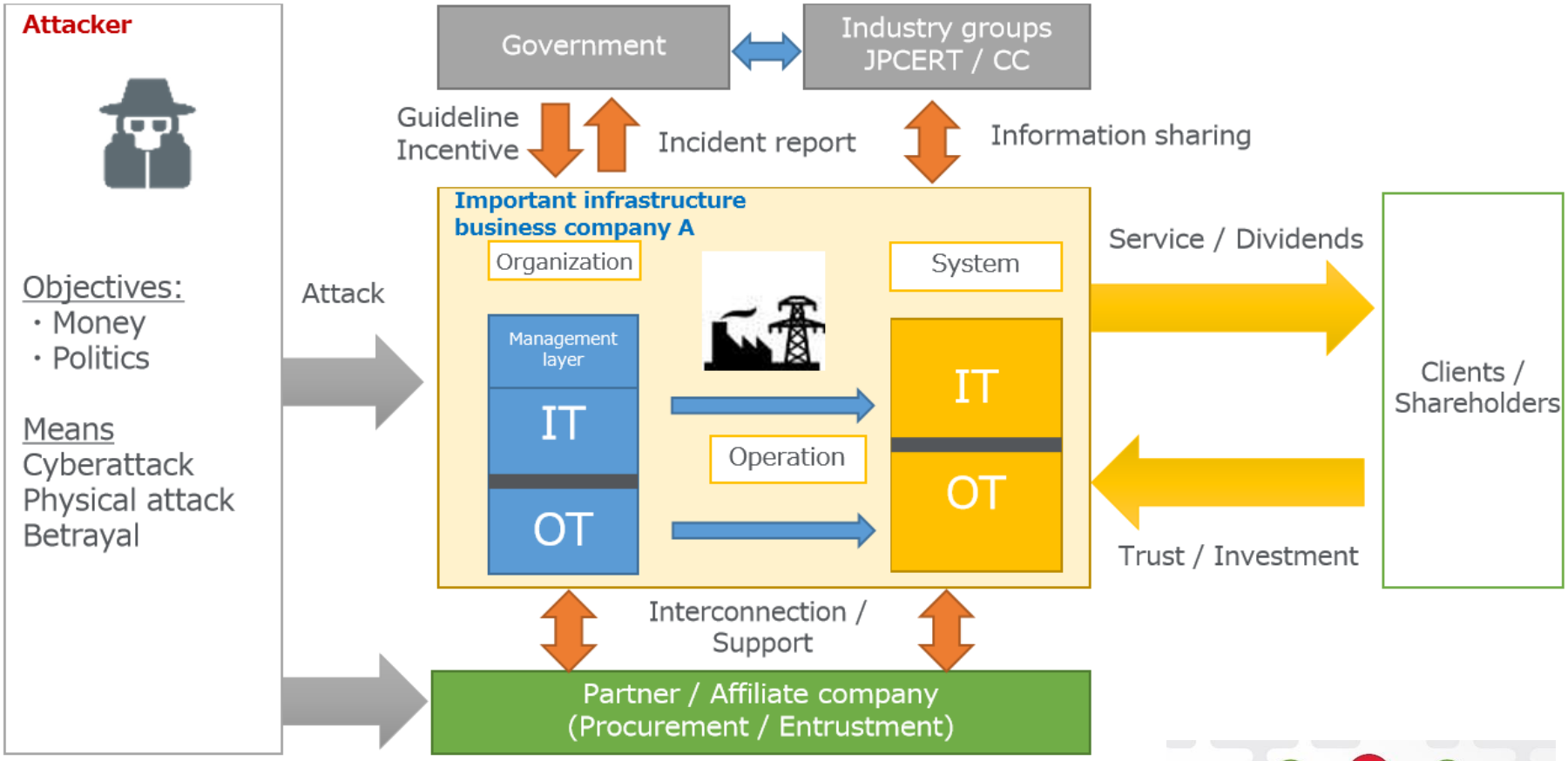
- Information leakage of design drawing / recipe
- Leakage of business secret / production data

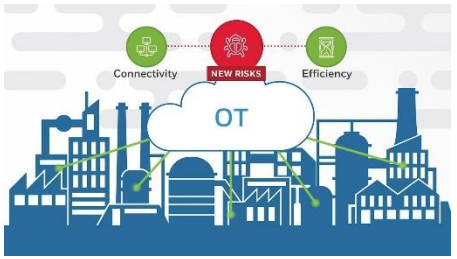
And others

Personal / physical / economic (sales / share price / compensation) / legal / social (confidence) can all be subject to attacks

Key influences

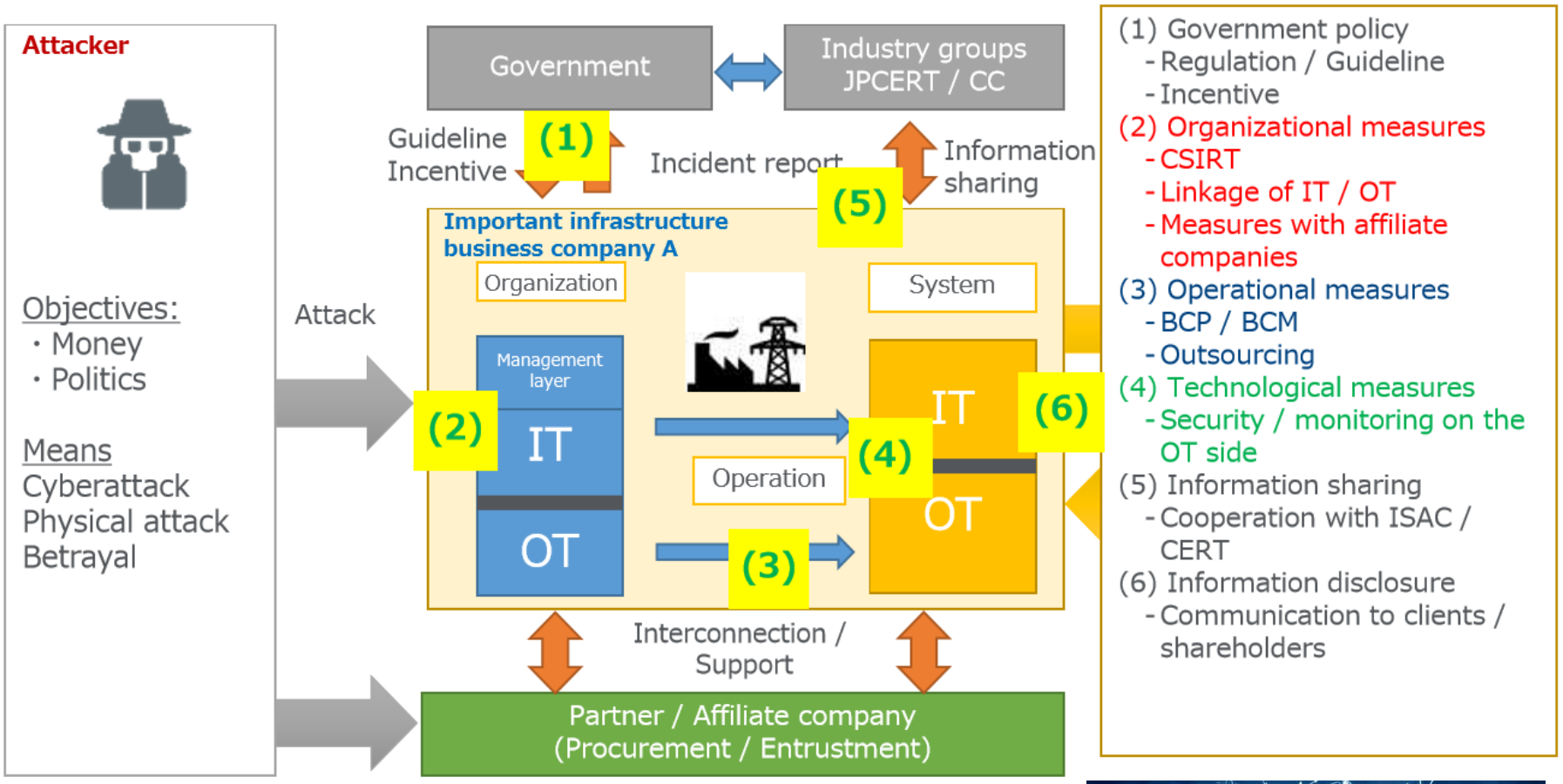
Surrounding environment of the critical infrastructure managing the closed system





Security Strategy

Need to develop a comprehensive strategy to Secure the ICS



Flow of Control System Security Measures

Basic procedure for control system security measures is the same as that of IT system. measures.

Understanding of actual conditions

- Desktop diagnostics
- Actual invasion testing
- Threat scenarios
- Risk evaluation

→

Drafting a plan

- Prioritization
- Goal setting
- Product evaluation
- Operation evaluation
- Organization design
- Education plan
- Integration with BCM*

→

Planning practice

- Product introduction
- Organizational changes
- Educational implementation
- Operational implementation
- BCM* implementation

→

Periodic diagnostic / review

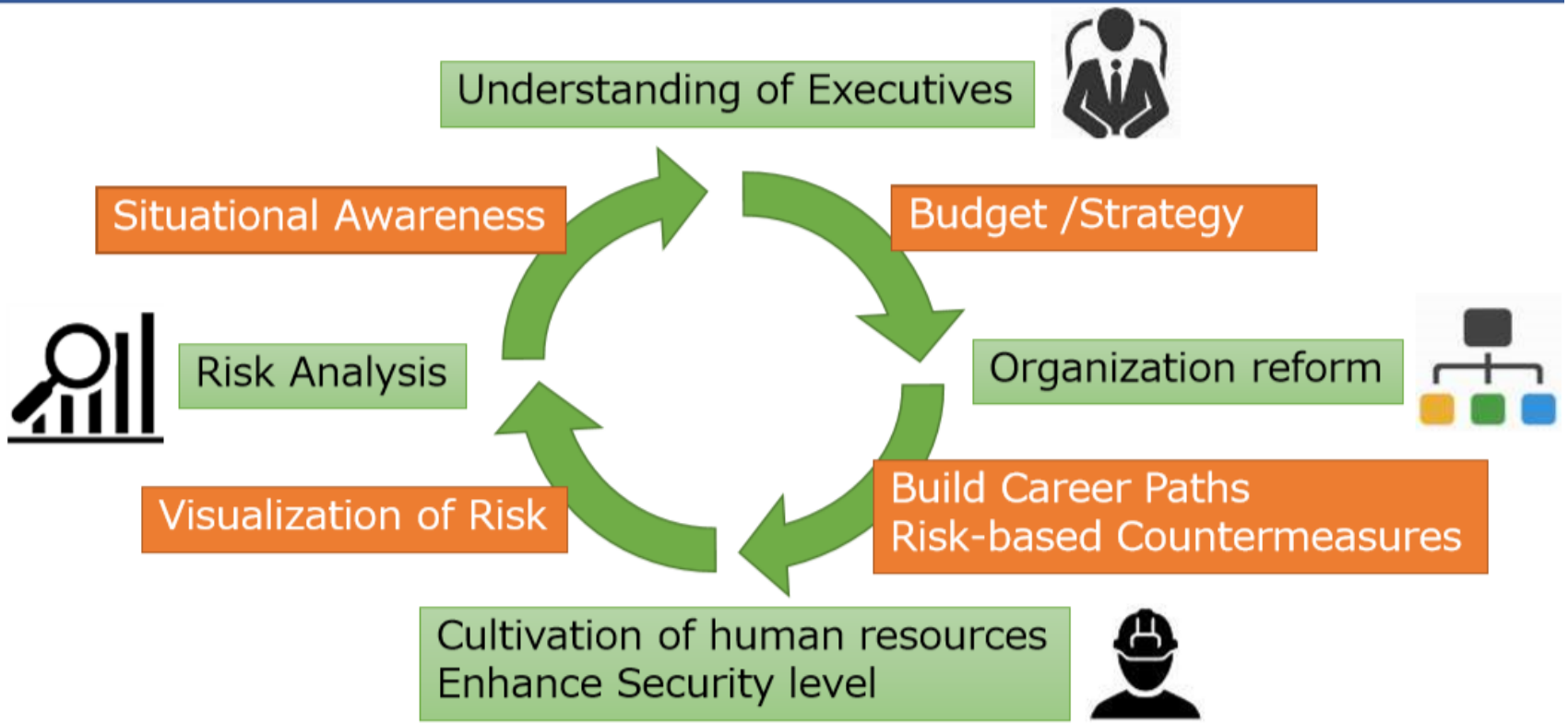
- Understanding of actual conditions
- Operational restructuring
- Educational restructuring
- BCP training

Understanding of actual conditions → Drafting a plan → Planning practice → Periodic verification / review
First, start understanding actual conditions

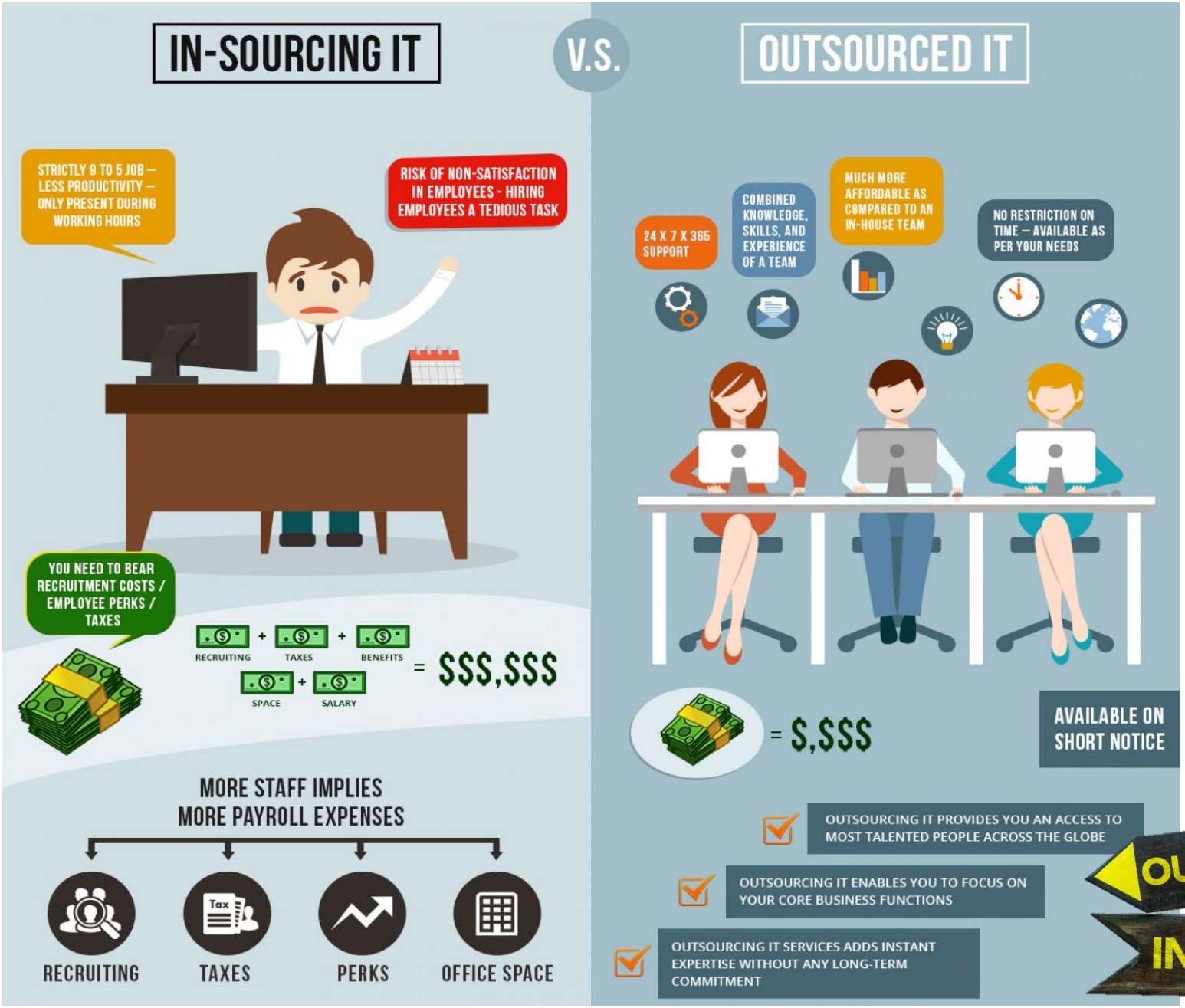
*BCM: Business Continuity Management

Basic Strategies for CI Companies

Strategy: Build Eco-system for improving CIP



The most important driver is the **understanding of Executives**.


IN-SOURCING IT
V.S.
OUTSOURCED IT
STRICTLY 9 TO 5 JOB – LESS PRODUCTIVITY – ONLY PRESENT DURING WORKING HOURS
RISK OF NON-SATISFACTION IN EMPLOYEES - HIRING EMPLOYEES A TEDIOUS TASK
YOU NEED TO BEAR RECRUITMENT COSTS / EMPLOYEE PERKS / TAXES
RECRUITING
TAXES
BENEFITS
SPACE
SALARY
= $$$,$$$
MORE STAFF IMPLIES MORE PAYROLL EXPENSES
RECRUITING
TAXES
PERKS
OFFICE SPACE
24 X 7 X 365 SUPPORT
COMBINED KNOWLEDGE, SKILLS, AND EXPERIENCE OF A TEAM
MUCH MORE AFFORDABLE AS COMPARED TO AN IN-HOUSE TEAM
NO RESTRICTION ON TIME – AVAILABLE AS PER YOUR NEEDS
= $,$$$
AVAILABLE ON SHORT NOTICE
OUTSOURCING IT PROVIDES YOU AN ACCESS TO MOST TALENTED PEOPLE ACROSS THE GLOBE
OUTSOURCING IT ENABLES YOU TO FOCUS ON YOUR CORE BUSINESS FUNCTIONS
OUTSOURCING IT SERVICES ADDS INSTANT EXPERTISE WITHOUT ANY LONG-TERM COMMITMENT
OUTSOURCE
IN-HOUSE

Advanced
Security Strategies
Tools & Techniques

Application Whitelist

Blacklist

A list of known bad elements to be detected

- Definition files must be updated. Maintenance is required.
- Scanning load is high.
- Unresponsive to unknown threats.

Whitelist

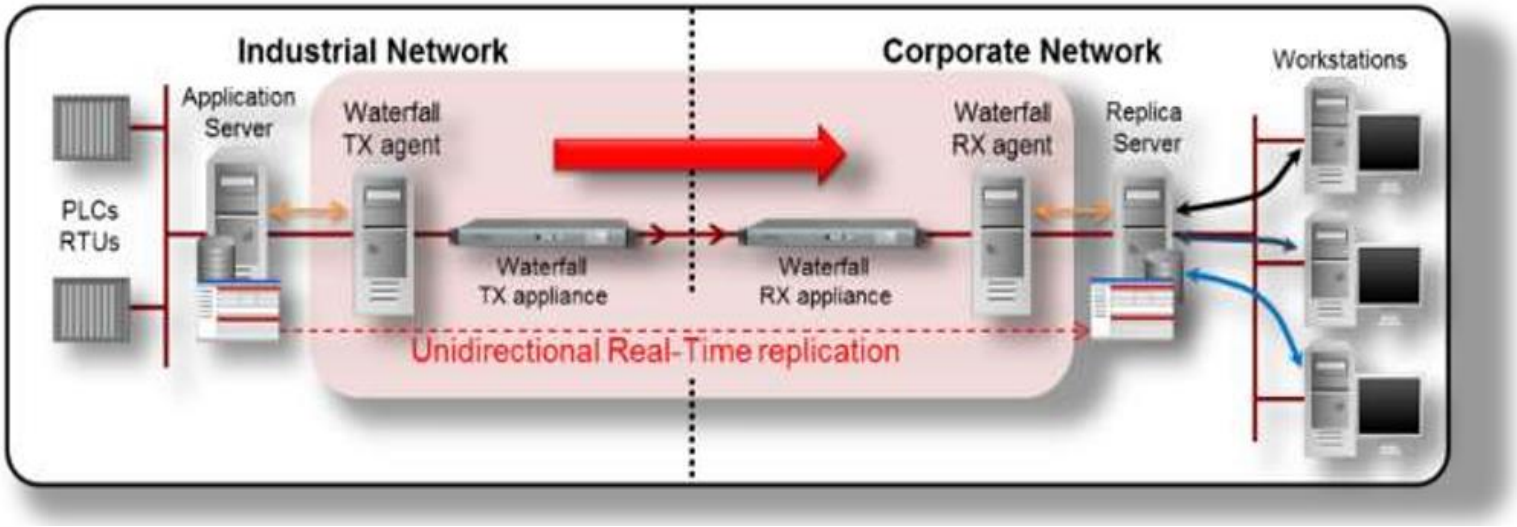
A list of known good elements to allow, blocking unknowns

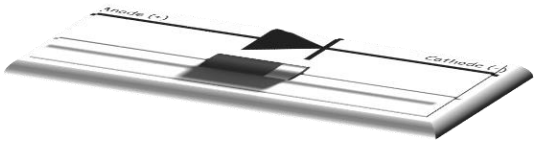
- If there are no changes, it can be left as is.
- As verification is performed during boot-up, there is almost no load.
- Able to respond to unknown threats.

Unidirectional Security Gateway – DATA DIODE

- Hardware-based security
- **Communication via laser from the TX (transmitter) to the RX (receiver) photocell, accomplished through optical fiber cable**

  ⇒ Data transmissions can be delivered, but nothing can be returned to the protected network
- With the use of an interactive protocol, TX collects data from protected and industrial networks
- With the use of an interactive protocol, RX publishes data to external networks
- Not protocol emulation, but server replication





Security Operations Centre (SOC)

SOC is a centralized function within an organization employing people, processes, and technology to continuously **monitor** and improve an organization's **security posture** while **preventing**, **detecting**, **analyzing**, and **responding** to cybersecurity incidents from various sources.

(1) Key functions (24/7)

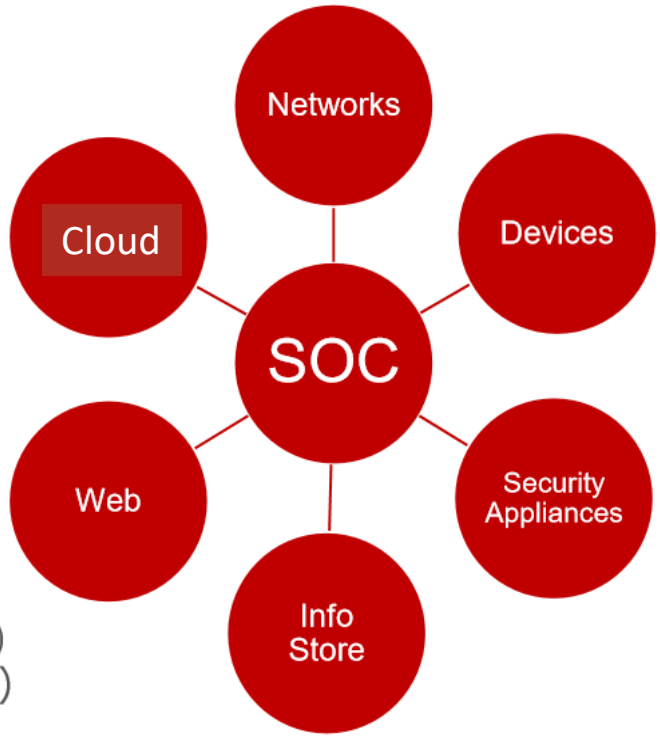
- Monitor
- Detect
- Investigate / analyze
- and respond to cyberthreats

(2) For what?

- Intellectual property
- Personnel data
- Business systems and ICS
- Brand integrity
- **Service supply, Safety, Health, Environment**

(3) People

- Security analyst (front line)
- Security Specialists (analysis and incident handing)
- Threat Investigators (Forensics and threat hunting)
- Manager or Director (Management)



Security Information Event Management

SIEM software and services combine **security information** management (SIM) and **security event** management (SEM). They provide **real-time analysis** of security alerts generated by applications and network hardware. SOCs have been typically built around a hub-and-spoke architecture, where a SIEM system aggregates and correlates data from security feeds.

(1) Key functions (24/7)

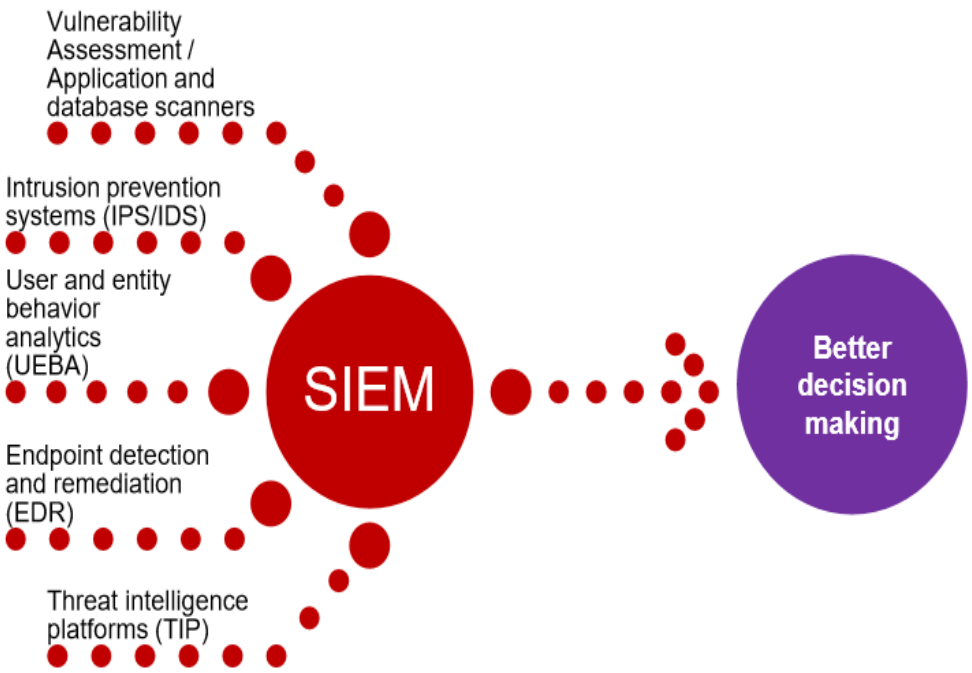
- Security information management
- security event management
- Real-time analysis of security alerts

(2) For what?

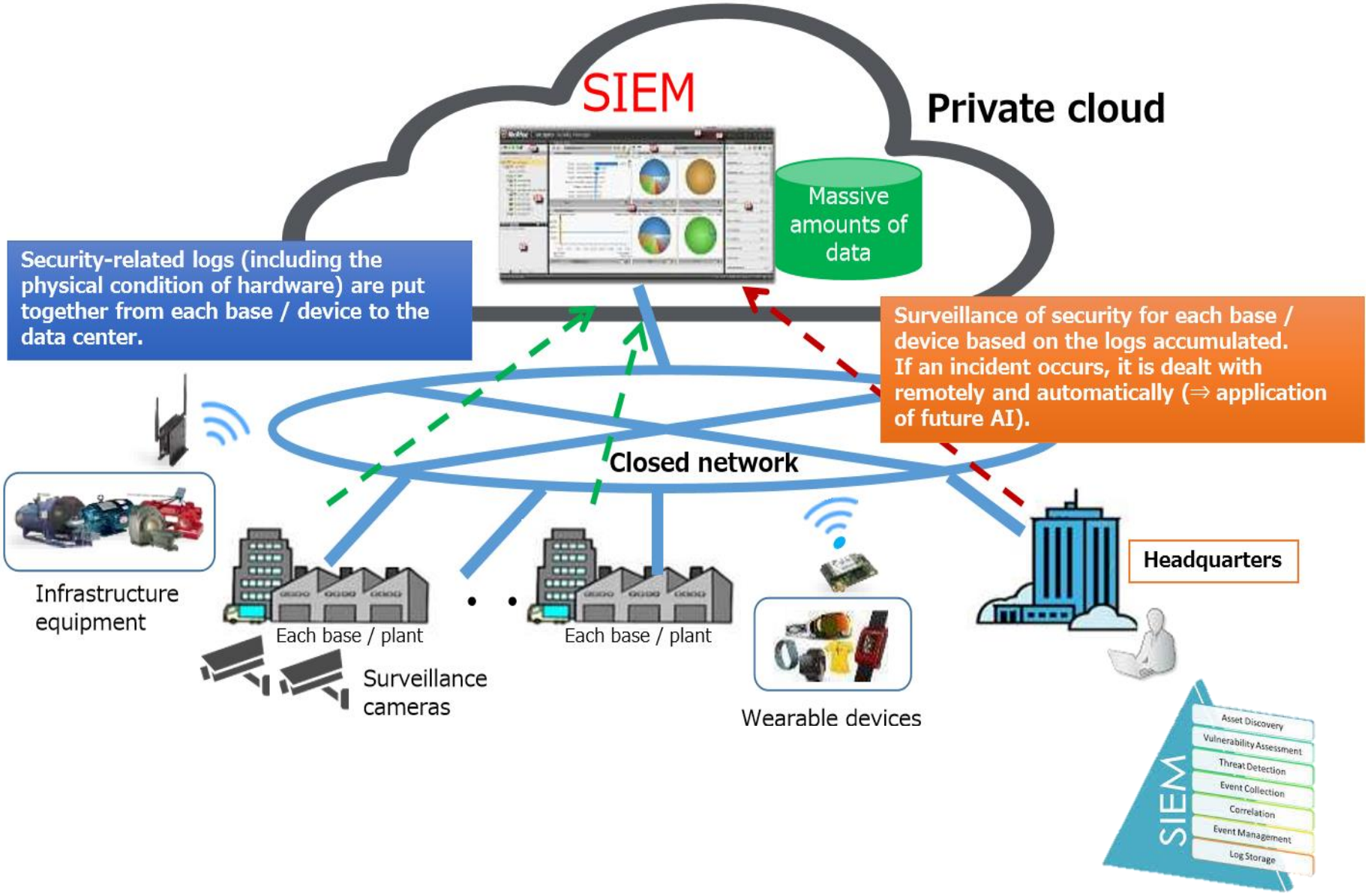
- Better analysis for SOC
- Information and event correlation
- Reduced the burden of manual Ops

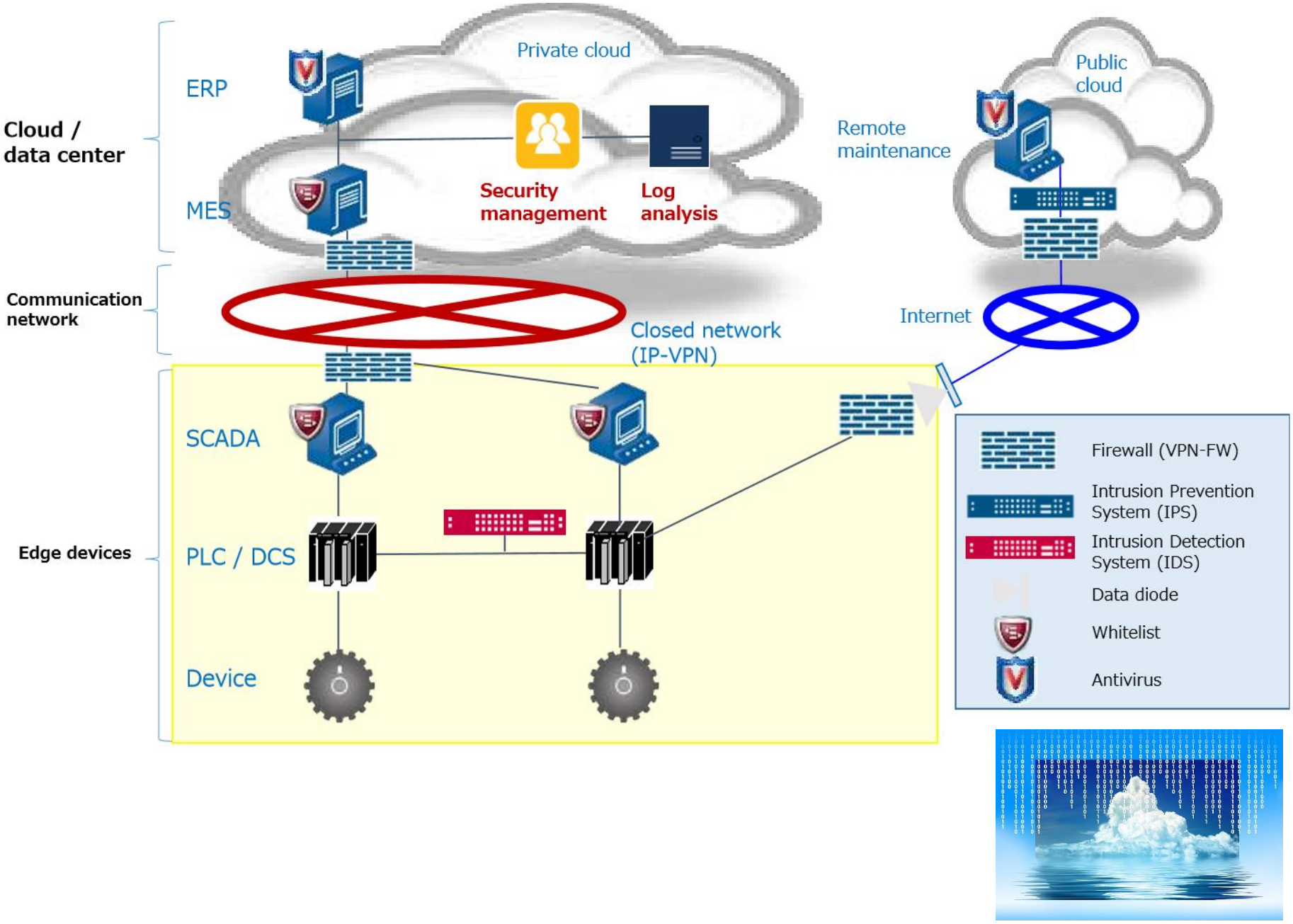
(3) Main components

- SIEM console
- Log manager
- Analysis/Correlation engine



Control system security model with the application of SIEM




Cloud / data center
Private cloud
ERP
MES
Security management
Log analysis
Public cloud
Remote maintenance
Communication network
Internet
Closed network (IP-VPN)
SCADA
PLC / DCS
Device
Edge devices
Firewall (VPN-FW)
Intrusion Prevention System (IPS)
Intrusion Detection System (IDS)
Data diode
Whitelist
Antivirus

WHO IS AT THE CENTRE OF

SECU  RITY

U-R

QUERIES

anwayasen@posoco.in
anwayasen@gmail.com