Industry 4.0 (I4.0)

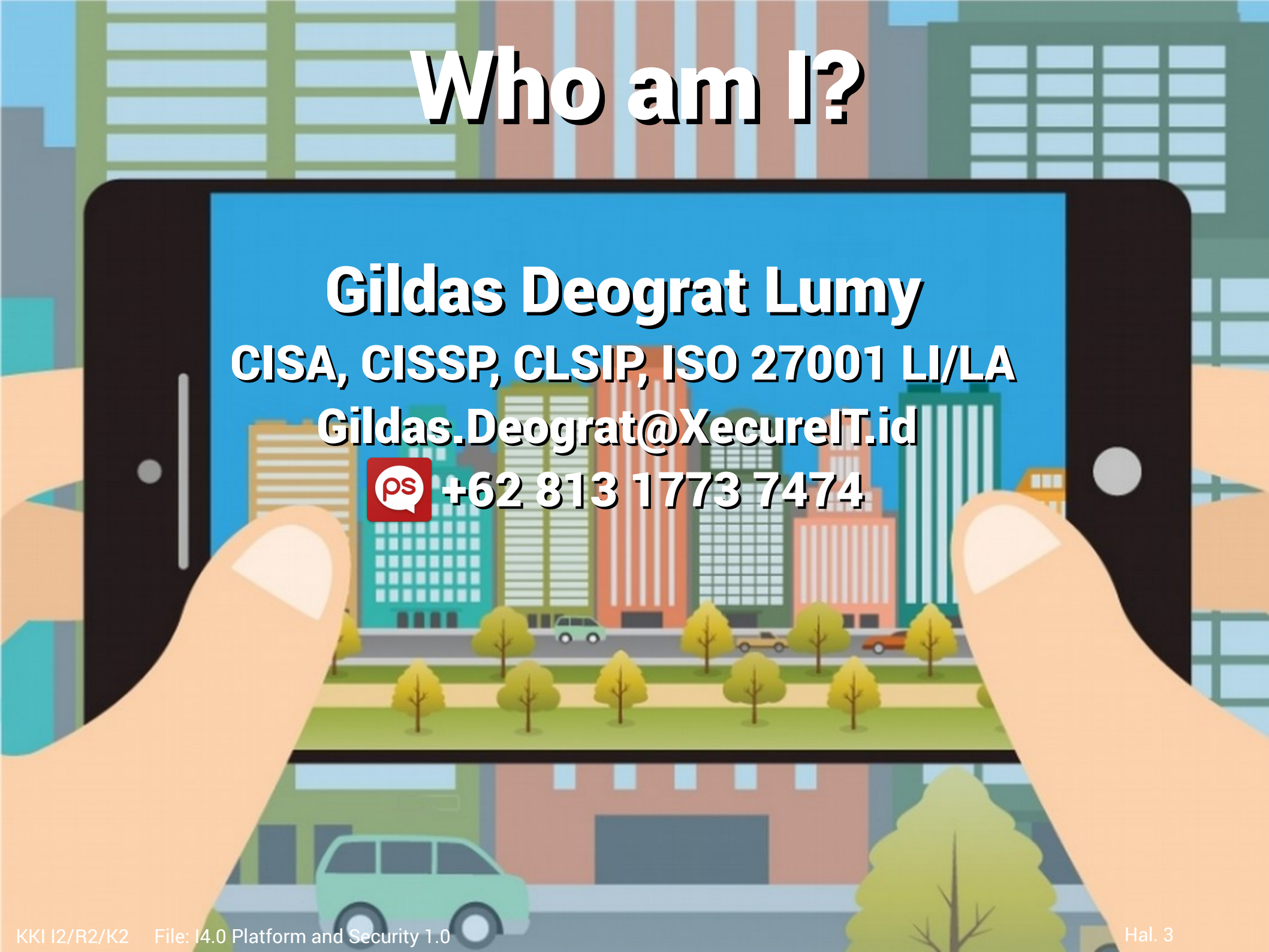
Internet of Things
Platform and Security

What is Internet of Things (IoT)?

Kevin Lonergan at Information Age, a business-technology magazine, has referred to the terms surrounding IoT as a “terminology zoo”. The lack of clear terminology is not “useful from a practical point of view” and a “source of confusion for the end user”.

https://en.wikipedia.org/wiki/Internet_of_things

Who am I?



Gildas Deograt Lumy

CISA, CISSP, CLSIP, ISO 27001 LI/LA

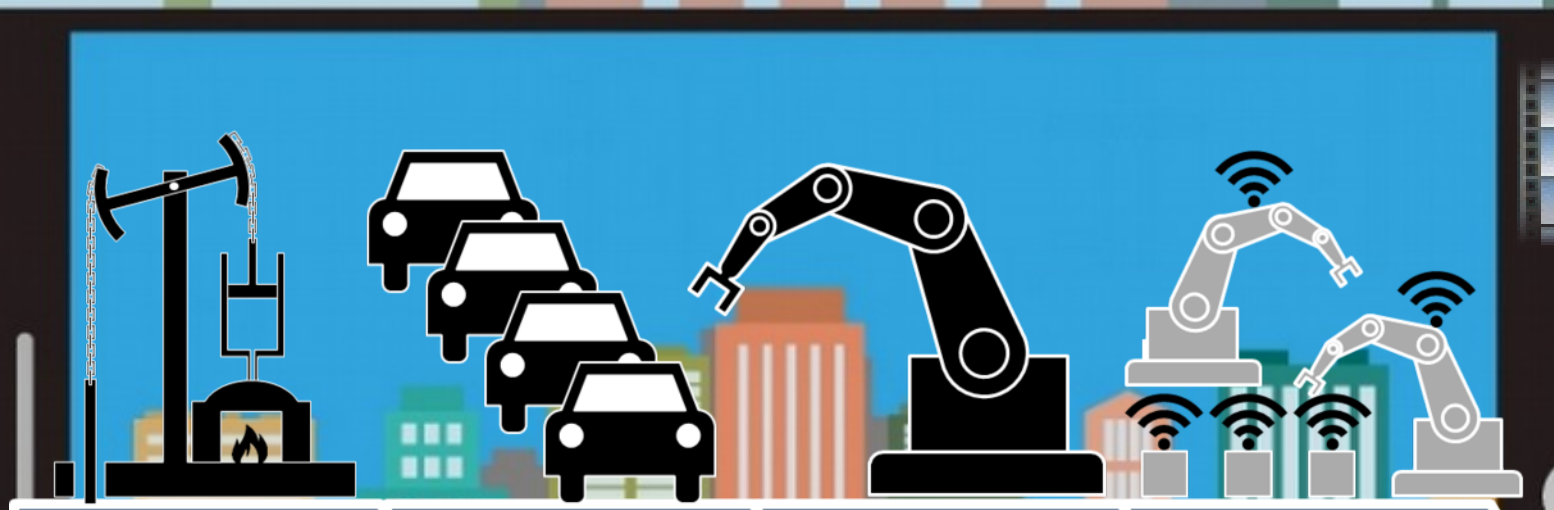
Gildas.Deograt@XecureIT.id

+62 813 1773 7474

Who am I?
Gildas Arvin Deograt Lumy

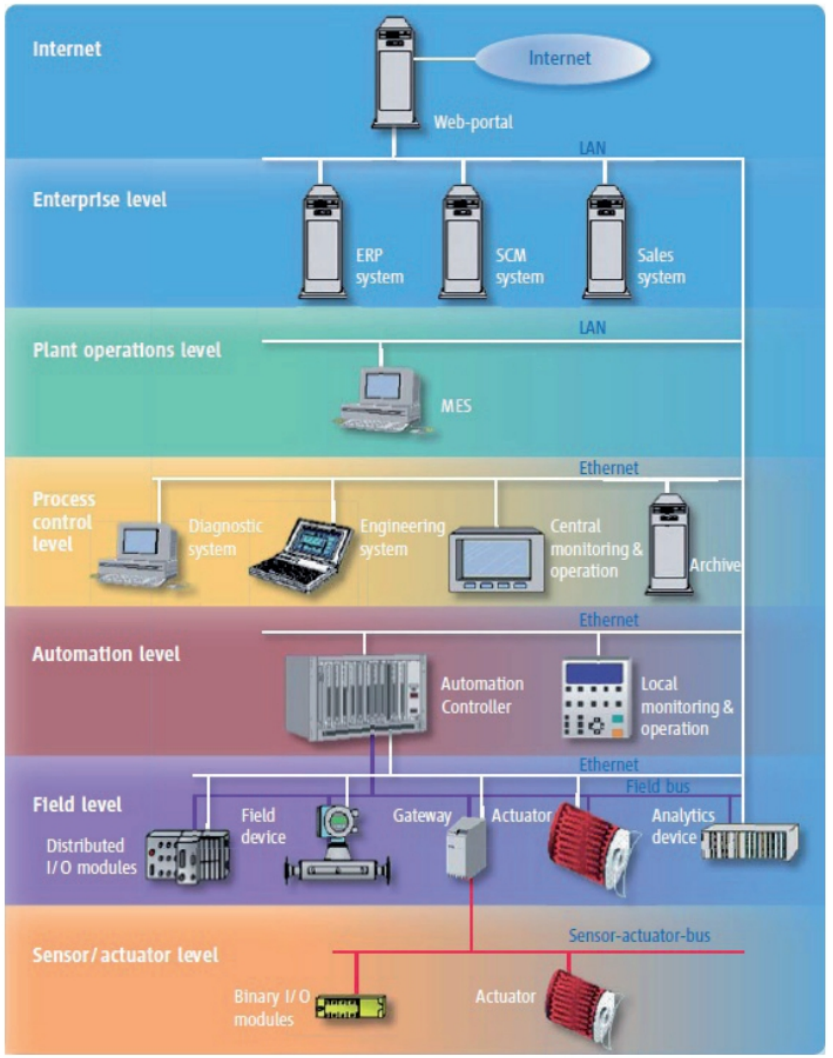
- 7 years supporting industrial automation system infrastructures in some big Indonesian companies.
- 8 years in Total Group, the 4th world largest oil gas company, with following Industry 3.0 responsibilities:
  - 3 years operation to manage secure connections in the fields of Total EP Indonesie.
  - 3 years reviewing and advising the DCS security in all subsidiaries of Total Exploration and Productions (EP).
  - 2 years creating Total EP Industrial Security Architecture Standard and its security organization structure.
  - 2 years creating and implementing Total Group high grade cyber security architecture.
- 10 years doing R&D of High grade security architecture Industry 4.0 and its solution.

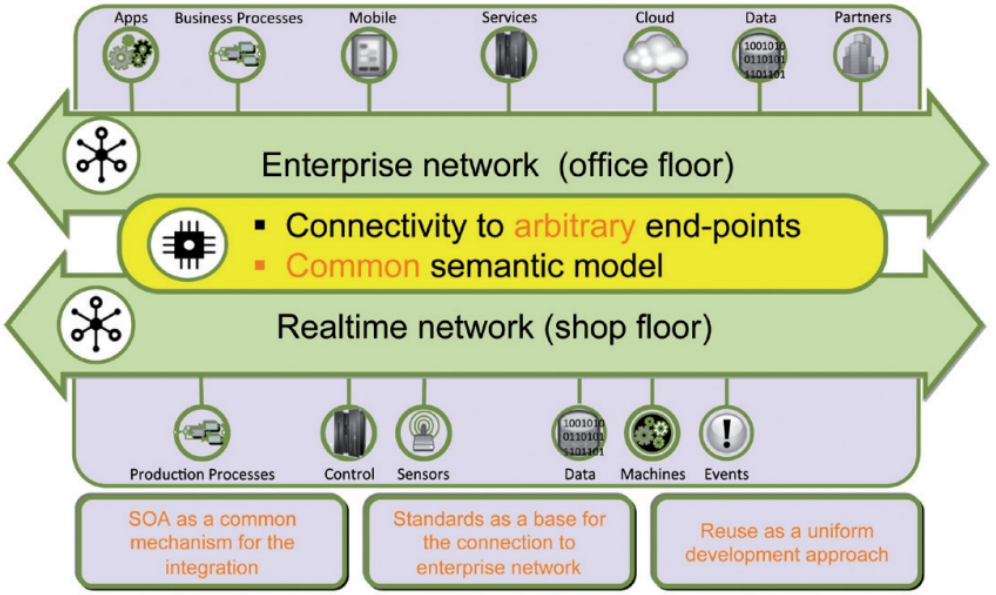
Industry Revolution



1st	2nd	3rd	4th
Mechanization, water power, steam power	Mass production, assembly line, electricity	Computer and automation	Cyber Physical Systems

Industry Revolution:
Industry 3.0 to Industry 4.0





Source: ZVEI-Führungskreis Industrie 4.0

Industry 3.0 Security Overview

SCADA (in)security

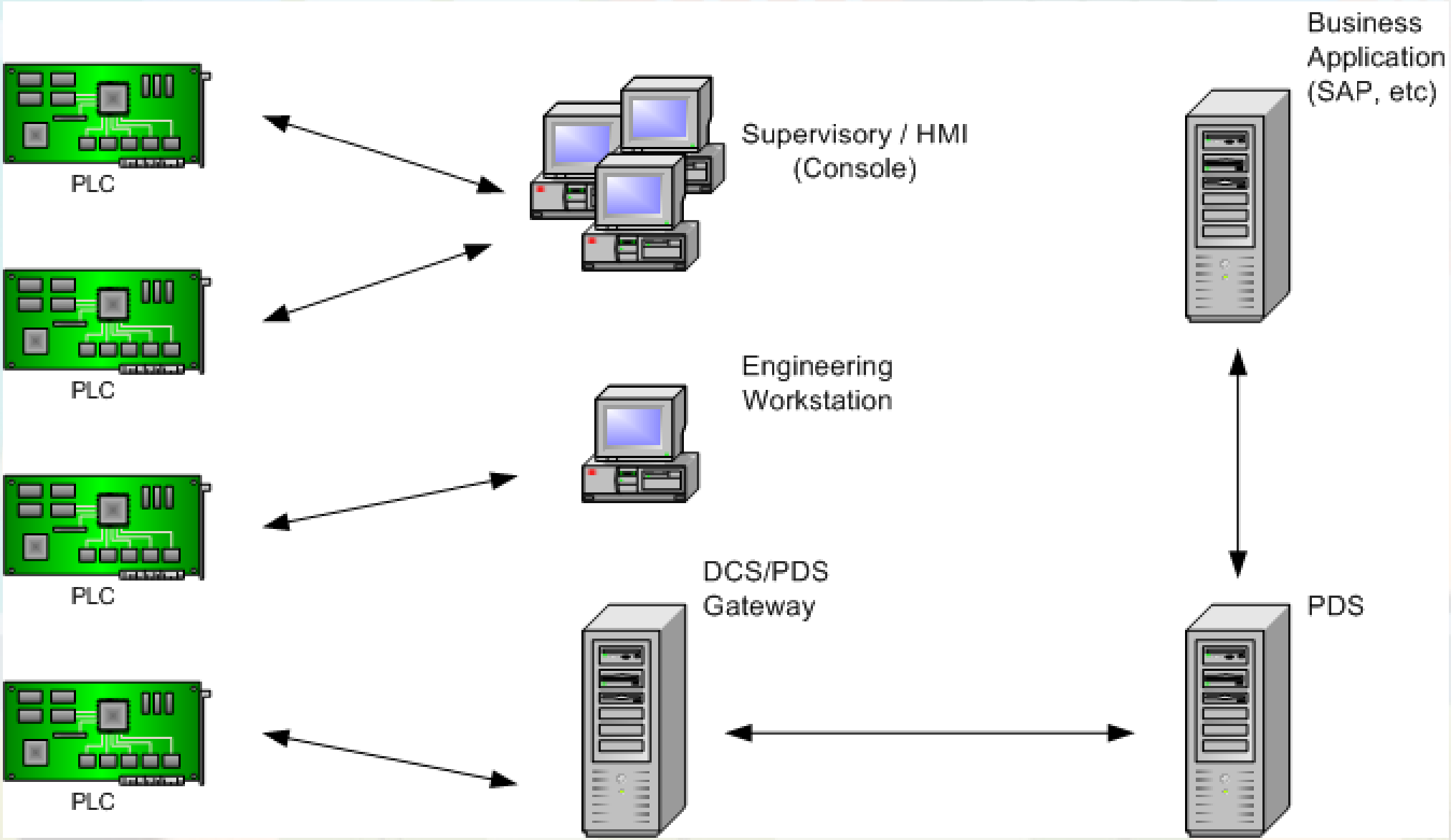
FORMASI (d/h KKI), 6th Security Night, 2006

- SCADA=Supervisory Control And Data Acquisition
  - Also called as Distributed Control System (DCS) or Human Machine Interface (HMI)
  - Components

    Supervisory (Console), Engineering Workstation, PLC alias RTU, Input/Output devices, Communication Infrastructure (network)
- Engineering Workstation:
  - To programme the PLCs = The “key” to configure the kingdom
- PLC (Programmable Logic Control) alias RTU (Remote Terminal Unit)
  - PLCs needs to be properly managed
  - PLCs are distributed across the plant. Oil and Gas pipeline can be thousands KM.
- Primary Constraint
  - It must very high availability and work well in extreme condition
  - Very sensitive in term of integrity and performance

SCADA (in)security

FORMASI (d/h KKI), 6th Security Night, 2006



SCADA (in)security

FORMASI (d/h KKI), 6th Security Night, 2006

- Real threat
  - Worldwide cases: various major disruption or incident due to attack on DCS by worm or disgruntled employees
  - Cyberwar is real. Possibility of terrorist threats is becoming higher
- It is critical infrastructure: Major Safety, Environmental, Economic, Legal and Organization Image Risks
- Vulnerable SCADA hosts (DCS Gateway and PDS)
  - Only certififed patch and security hardening are allowed
  - Anti virus could decrease the performance
  - Unknown vulnerability on un-common applications
- The industry trend is to use more and more common OS with known vulnerabilities

SCADA (in)security

FORMASI (d/h KKI), 6th Security Night, 2006

- Production monitoring and reporting from business network

  Users needs to access PDS system using PDS client or web interface from business network using business PC/ Laptop located in office building with weaker physical protection.

- Local and remote maintenance by SCADA engineer (outsourced)
- It's complex. Different systems combinations need different types of traffic
  - Control Systems product (such as Yokogawa, Honeywell, Foxboro, etc) combines with PDS product (such as PI, IP-21, SIM-21, etc)
  - Various types implementation for each combination, for example: 3 possibilities for Yokogawa with IP-21 implementation

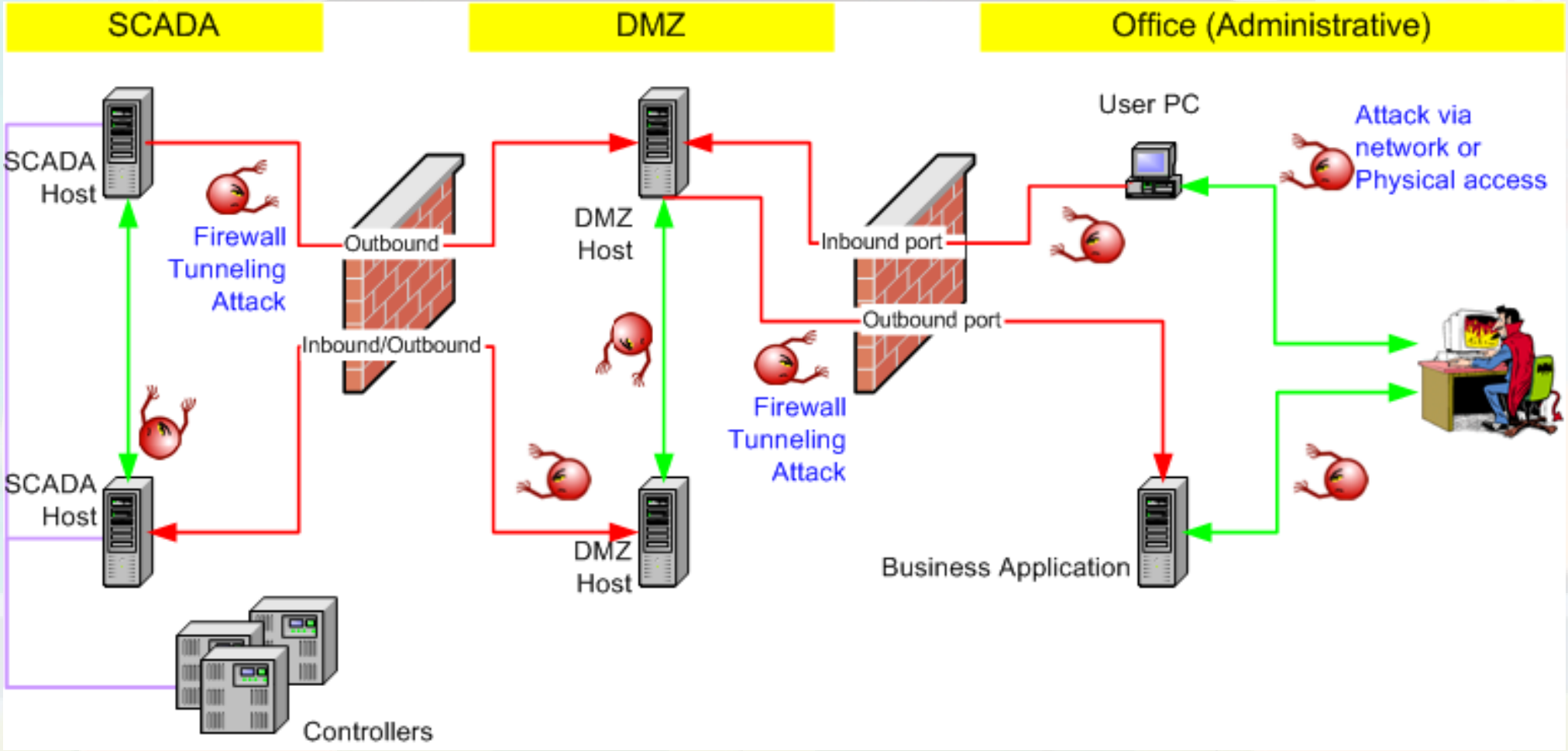
SCADA (in)security

FORMASI (d/h KKI), 6th Security Night, 2006

- Swiss Cheese Firewall
  - Does not analyze the packet content of non-standard traffics
  - More and more PDS products use RPC (Remote Procedure Call) and (sometimes) NetBIOS between PDS server and its client using dynamic ports
    ➔ Need to open inbound all ports above 1024/TCP
- Firewall Tunneling – old concept, but new issue and becoming more popular
  - Accessing internal host from external through authorized outbound traffic
  - Need to transfer file from PDS to office systems, i.e. outbound FTP to PDMS
- Security by obscurity simply does not work
  - Widespread availability of detail technical information about control systems
- Low level of awareness

SCADA (in)security

FORMASI (d/h KKI), 6th Security Night, 2006



Industry 3.0 to Industry 4.0
The Security Revolution: More Oups!

- 40 years evolution = More fragile digital ecosystem across industry sectors
  - More Open
  - More Unmanaged
  - More Unskill
  - More Physically insecure
  - More Security nigthmare

Qualitatif Risk Analysis Scoring

(1 less secure, 10 more secure)

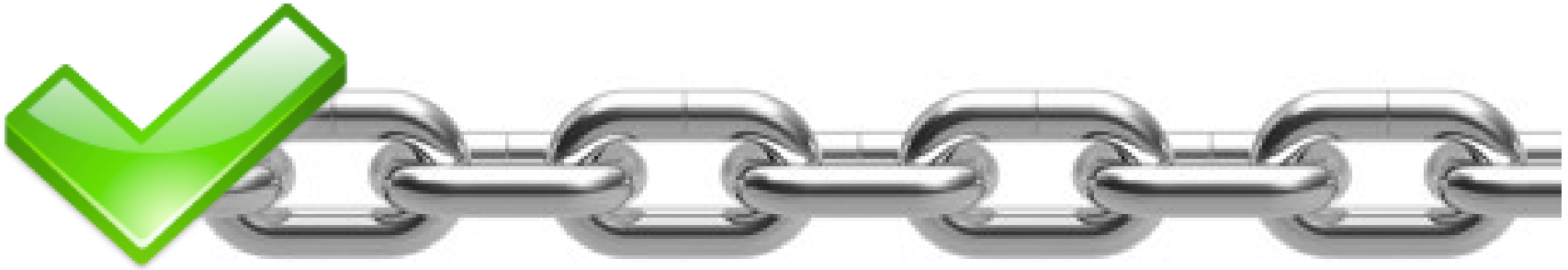
- 1980-2000, score 8-9
- 2000-2010, score 6-7
- 2010-now, score 4-5

Industry 3.0 to Industry 4.0
The Security Revolution: More Oups!

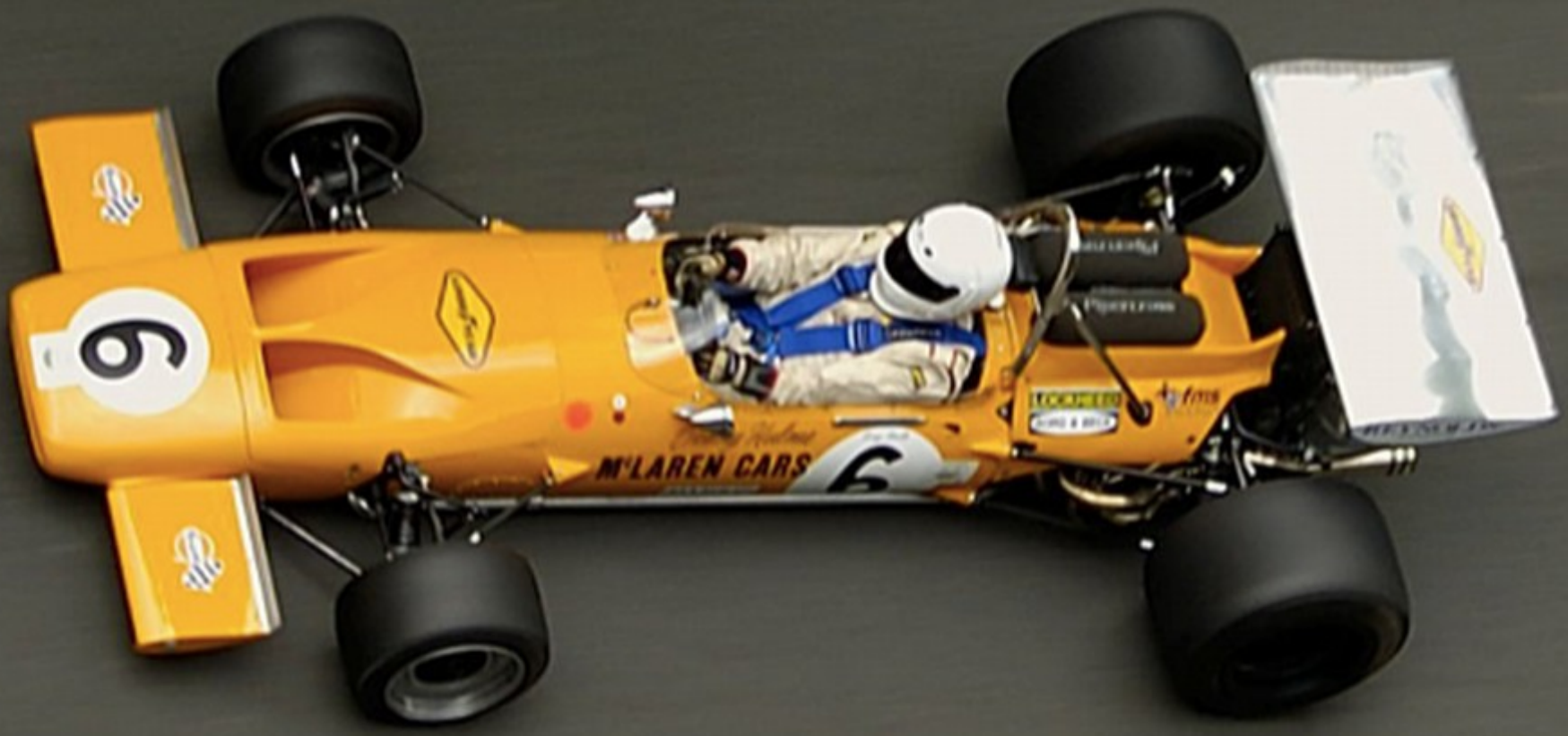
- More Open
  - More open connection
  - More open systems and protocols
  - More open knowledges and tools
- More Unmanaged
  - More Unmanaged Security Policies Implementation
  - More Unmanaged Access Control
  - More Unmanaged Vulnerability
- More Unskill
  - More Unskill Users
  - More Unskill Attackes
- More Physically insecure
  - More Mobile and Public Location
  - More Accessible to Configure
- More Security nigthmare
  - More incident quantity
  - More incident quality

Industry 4.0 (I4.0)

The I4.0 High Grade Security Objective



The I4.0 High Grade Security



The Biggest Challenge:
Cyber Security **Mindset Revolution**

The I4.0 High Grade Security : Components

- High security (and high privacy) business model
- High grade security strategy
  - Effective risk identification
  - Integrated information security concept
  - Integrated Cybersecurity strategy
- High grade security tactical
  - Effective attacks mitigation concepts
  - High grade security architecture and procedures
- High grade security operation
  - Effective implementation of the architecture and procedures
  - High grade security solution

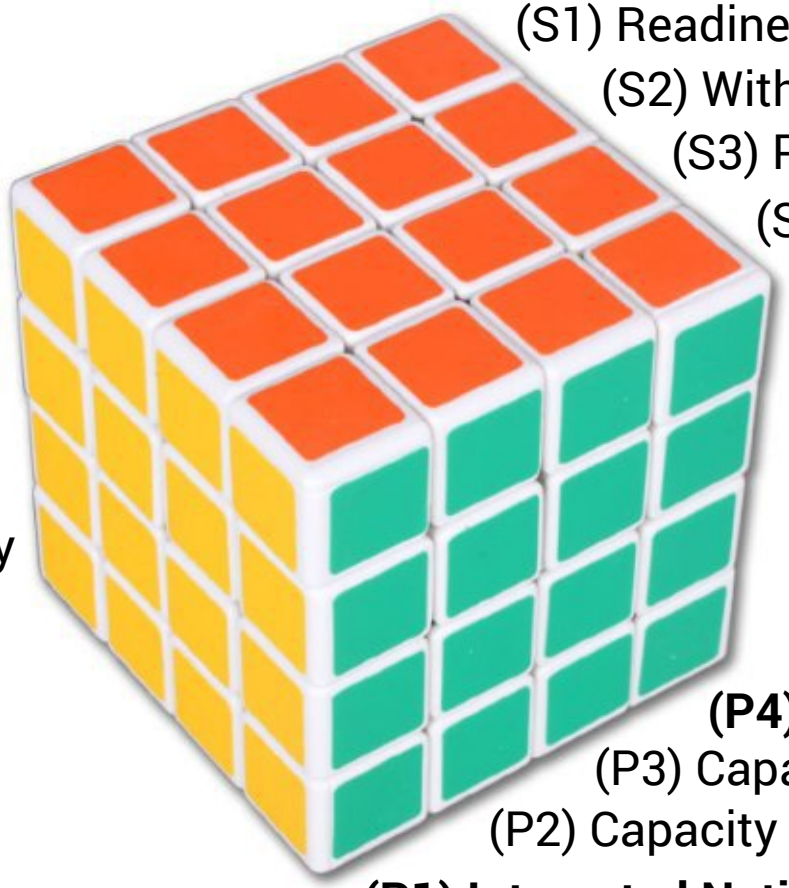
Integrated Cybersecurity Strategy

STAGE (T)

(S1) Readiness
(S2) Withstand
(S3) Pemulihan (Recover)
(S4) Berkembang (Evolve)

LAYER (L)

(L4) Information & Transaction
(L3) IT system
(L2) Cyber Infrastructure
(L1) Energy



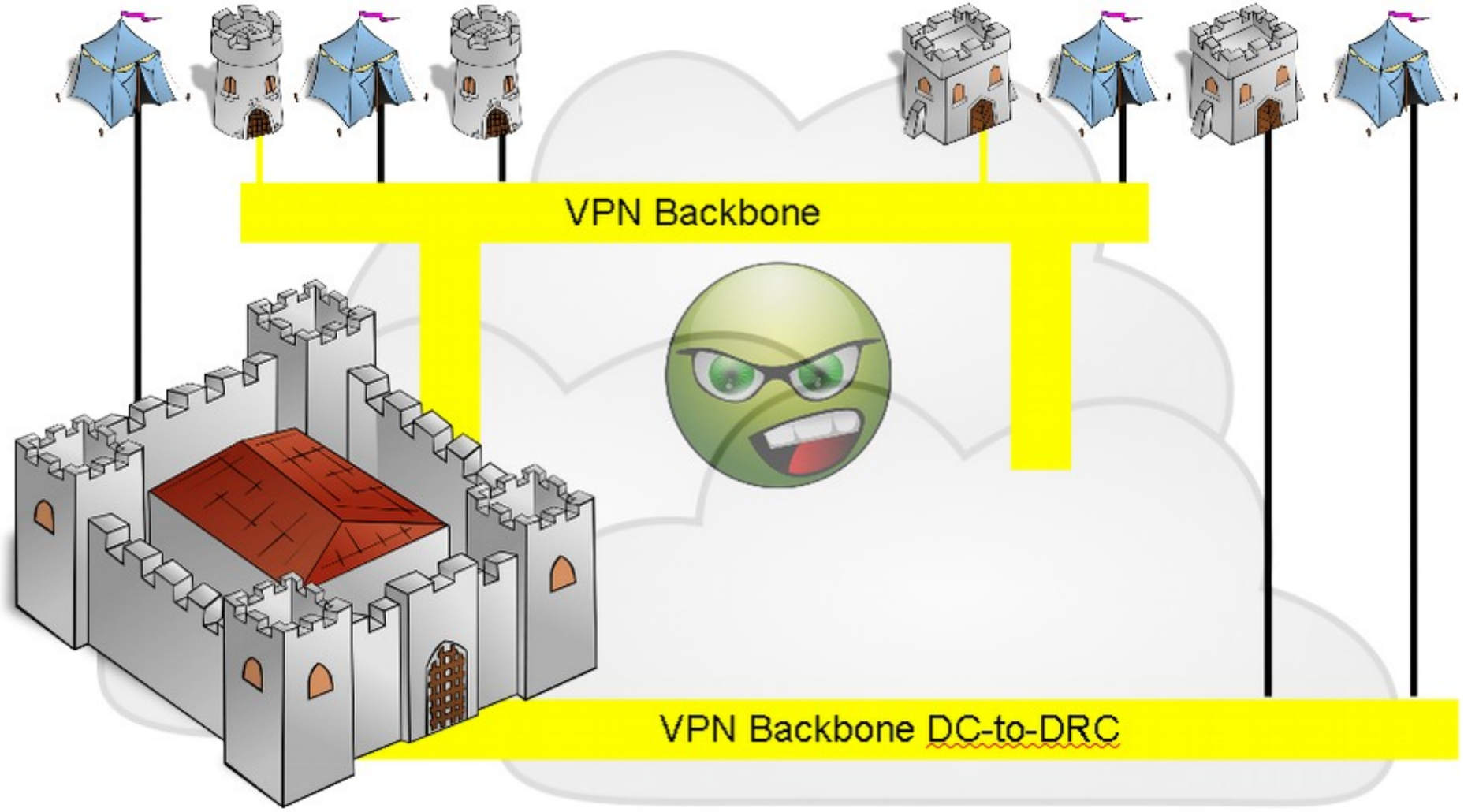
PILLAR (P)

(P4) Culture
(P3) Capacity & Capability
(P2) Capacity and Capability
(P1) Integrated National Strategy

VARIABEL (V)
(V1) Strategic Objectives and Policies
(V2) Tactical Steps
(V3) Operational Resources (Funds, People, Technology, Physical)

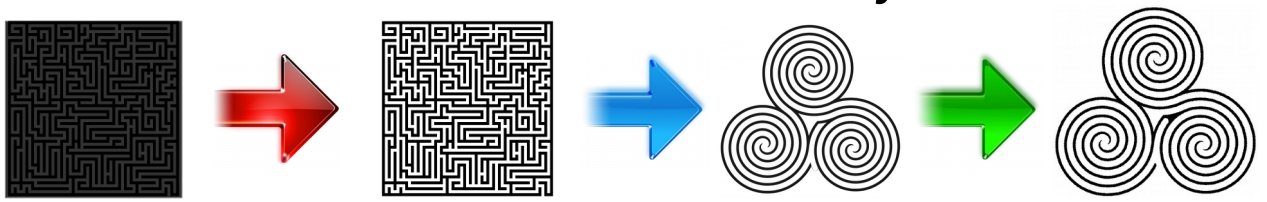
High Grade Security Architecture: Illustration

High Grade Security Architecture: Inconsistent Implementation

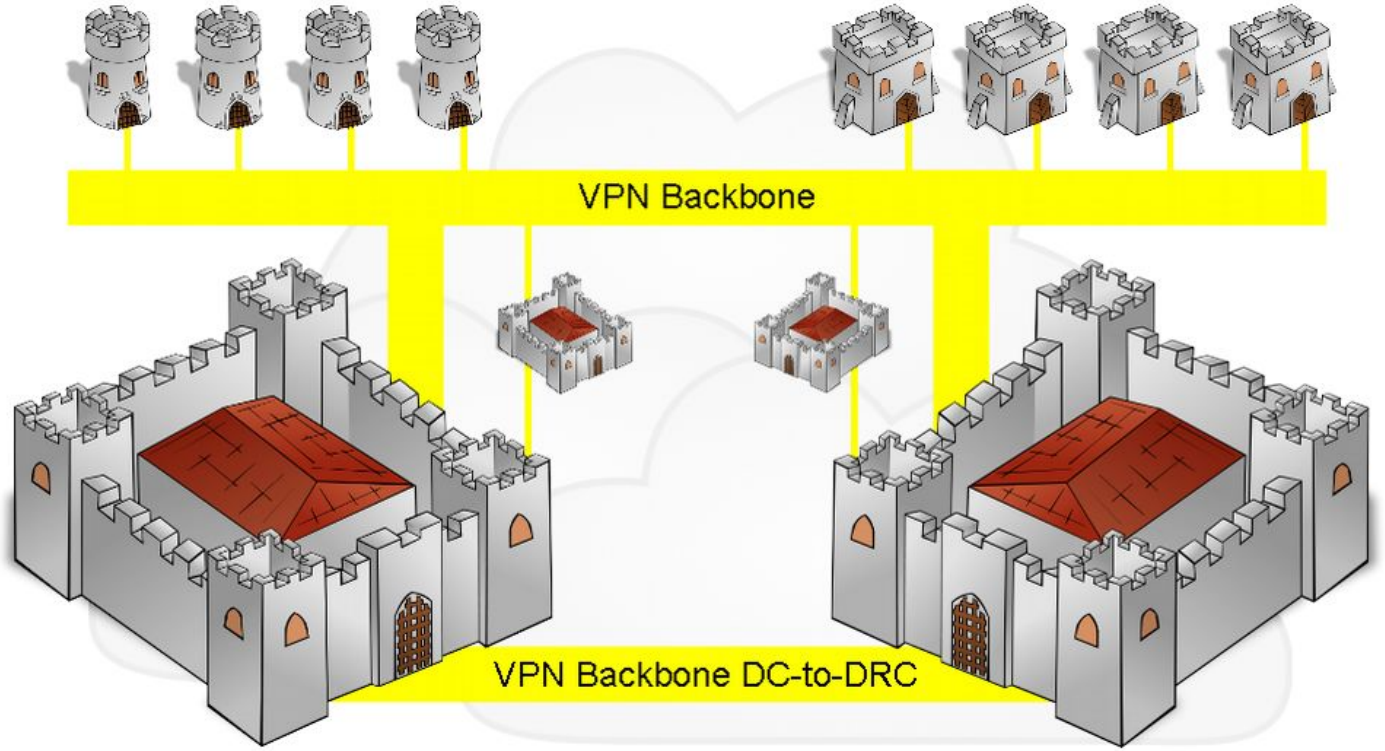


High Grade Security Architecture: Primary Objectives

1. Clear Visibility



2. Consistent Implementation



High Grade Security Architecture Example: SAKTTI

- Standar Arsitektur Keamanan Tingkat Tinggi Informasi (SAKTTI)
- An architecture to achieve high grade level of integrity, confidentiality, and availability **to build a highly secure interconnected digital fortresses system** through effective implementation of the **key principles** based on the **key factors**.

High Grade Security Architecture
Example: SAKTTI

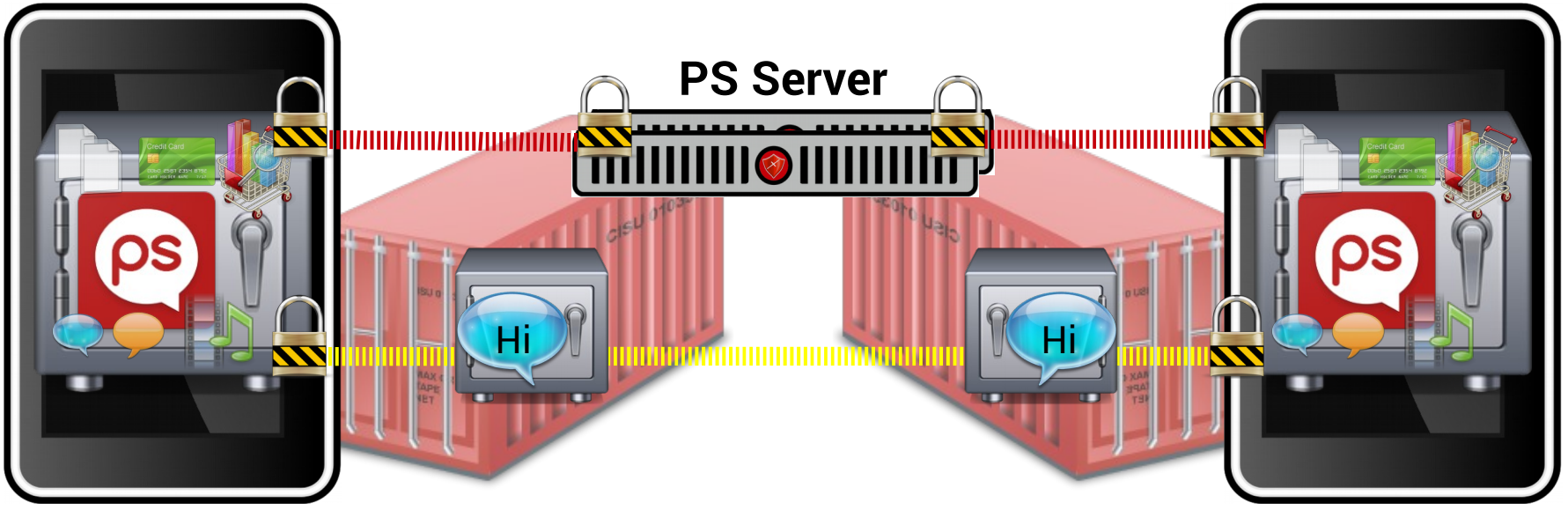
- Key Principles
  - Ensure holistic and balance information security control techniques (deterrent, preventive, detective, corrective, compensating and recovery).
  - Integrate information security control components (People, Administrative, Technology, Physical).
  - Cover all information life cycle: create, distribute, use, maintain, archive, destroy.

High Grade Security Architecture
Example: SAKTTI

- Key Factors
  - White list approach
  - Change management
  - Integrity assurance
  - Monitoring
  - Defense in depth
  - Least privilege
  - Separation of duties
  - Traffic flow control
  - Hardening
  - Comprehensive Encryption
  - Capacity
  - Performance
  - Redundancy
  - Backup

SAKTTI Implementation Example

- **Local database encryption**
- **Dedicated** End Point to End Point **Authentication Key**
- **End-to-End** encryption with **Dedicated Dynamic Key** between PS Client, **including within group discussion**
- **Anti SSL MITM attack traffic encryption** between PS Client and PS Server

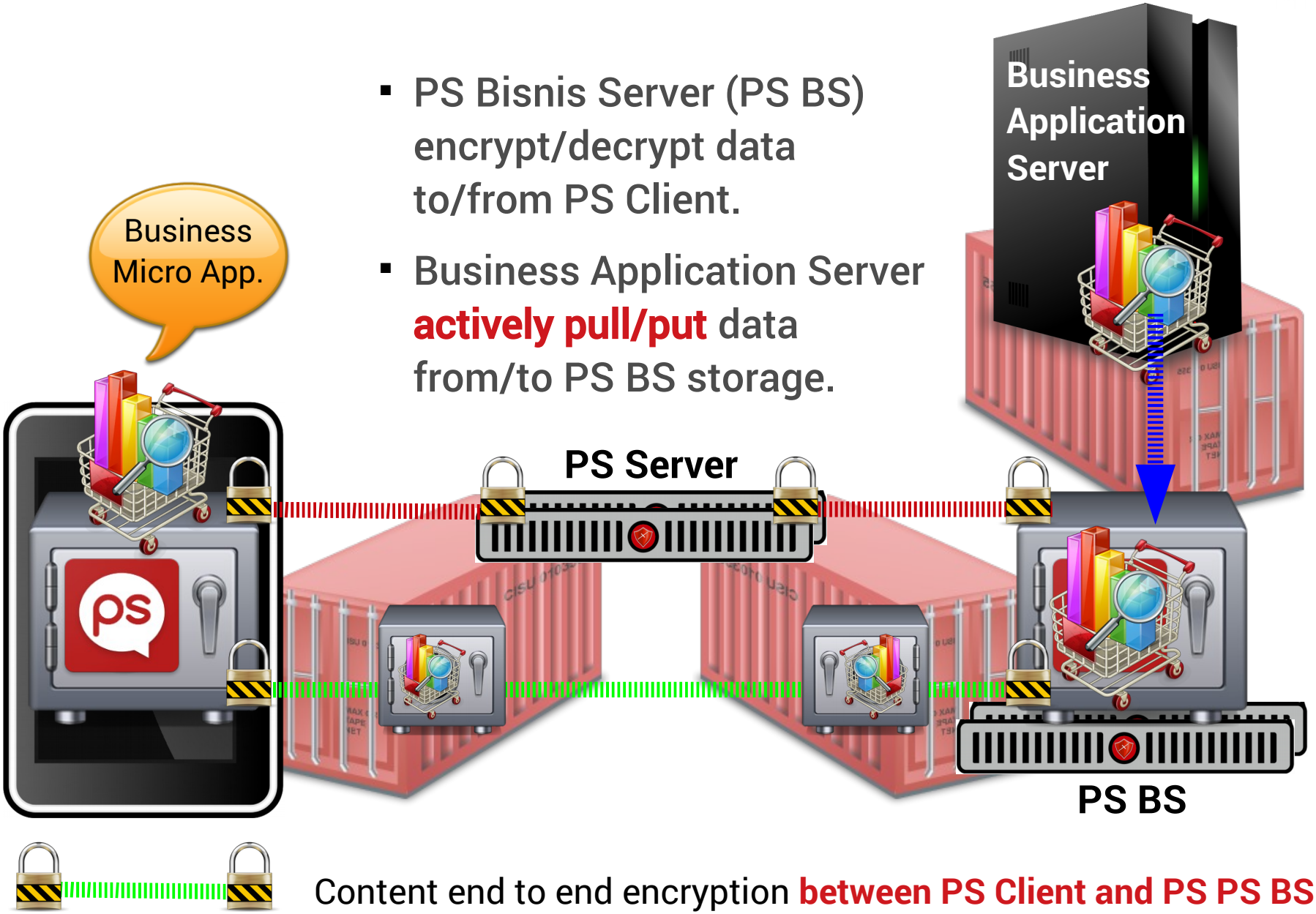


Traffic encryption **between PS Client and PS Server**.

Content end to end encryption **between PS Client**.

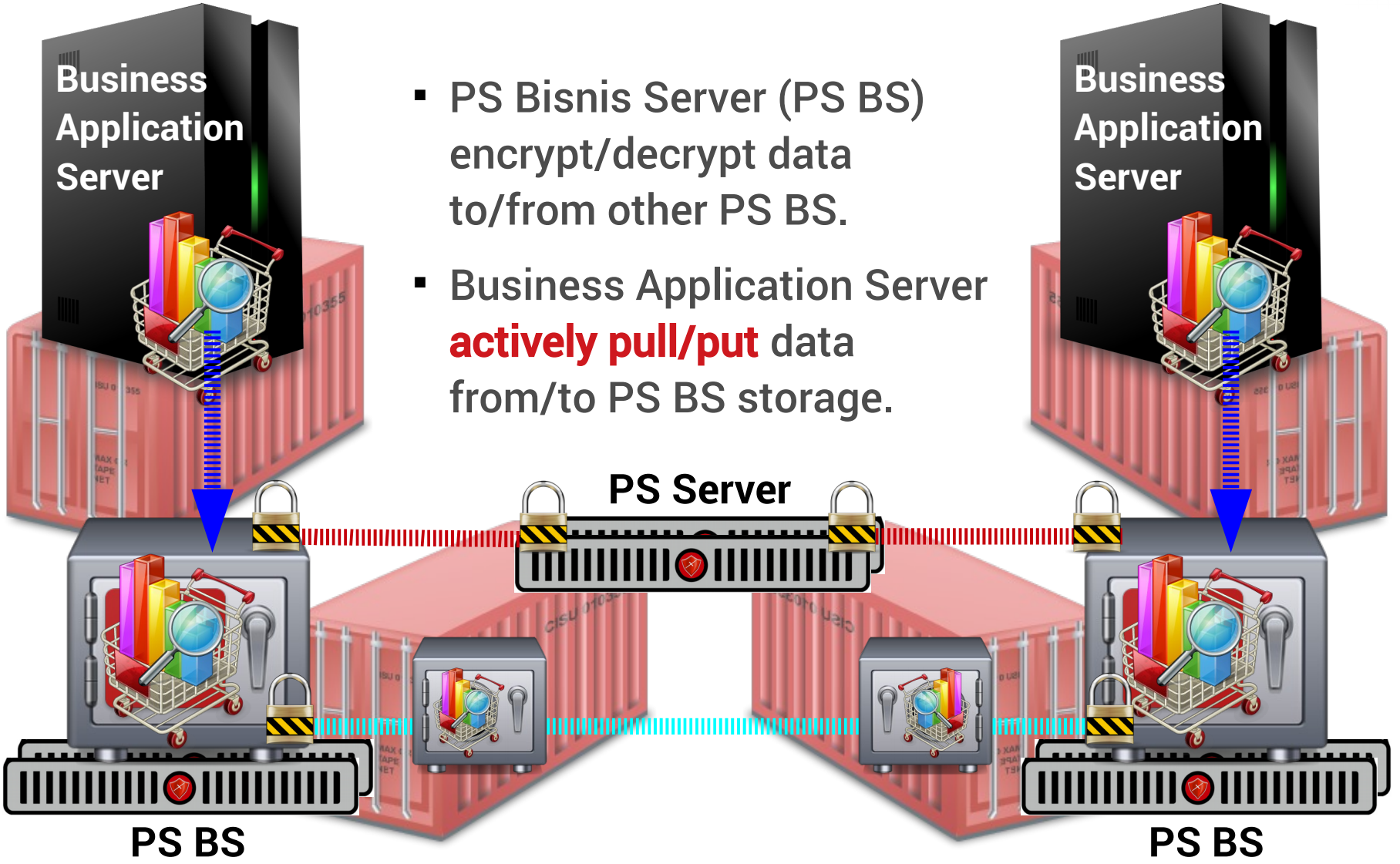
SAKTTI Implementation Example

- PS Bisnis Server (PS BS) encrypt/decrypt data to/from PS Client.
- Business Application Server **actively pull/put** data from/to PS BS storage.



Content end to end encryption **between PS Client and PS PS BS**.

SAKTTI Implementation Example

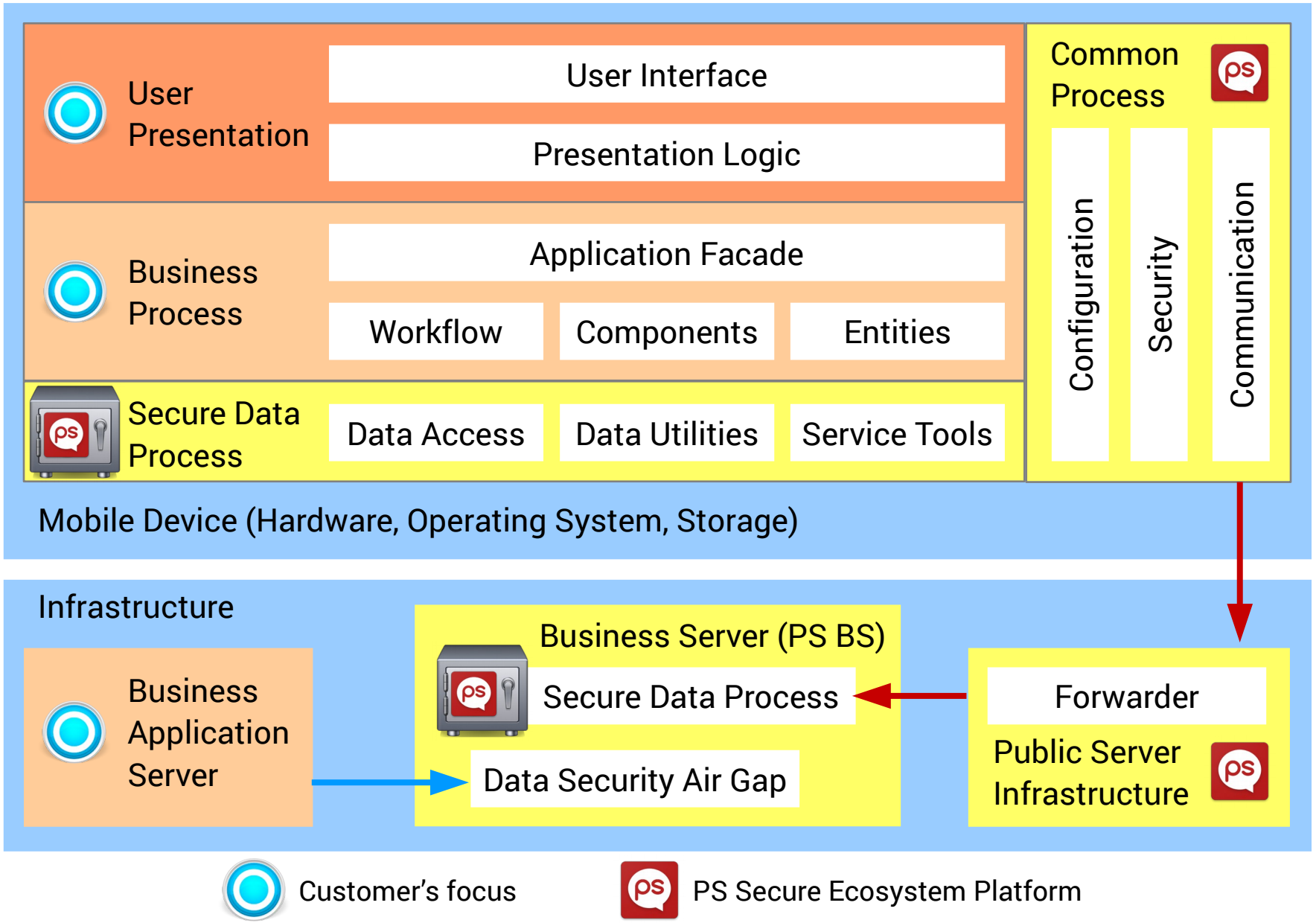


- PS Bisnis Server (PS BS) encrypt/decrypt data to/from other PS BS.
- Business Application Server **actively pull/put** data from/to PS BS storage.

Content end to end encryption **between PS PS BS**.

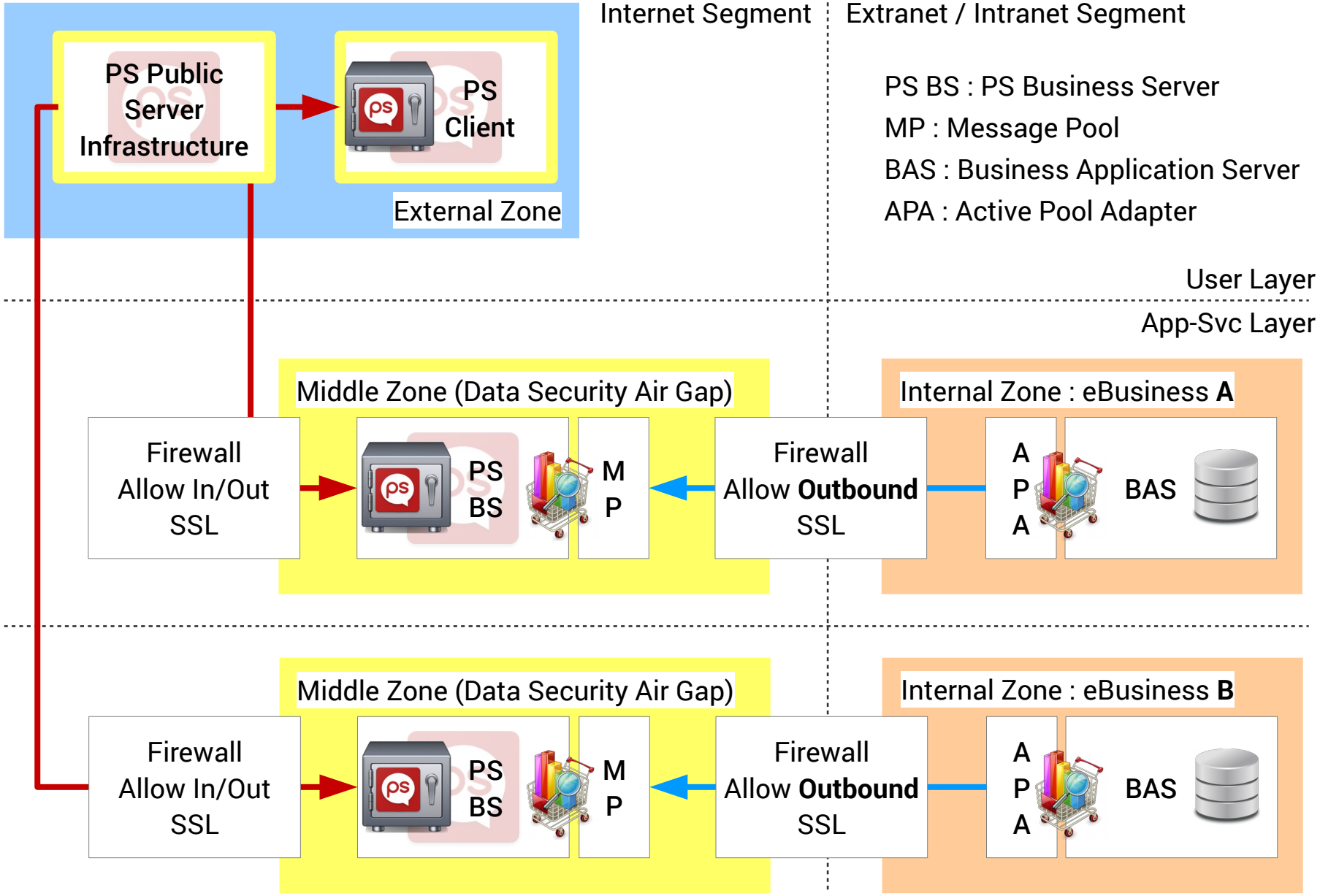
SAKTTI Implementation Example

PS Secure Mobile Application Architecture



SAKTTI Implementation Example

PS/SAKTTI Architecture Level 0



Industry 4.0 Platform

Secure.Optimum.Simple
Digital Life Ecosystem Platform