IT/OT Integration
(Integrated Production Management System)

Marcel Kelder

Sales Manager Advanced Solutions

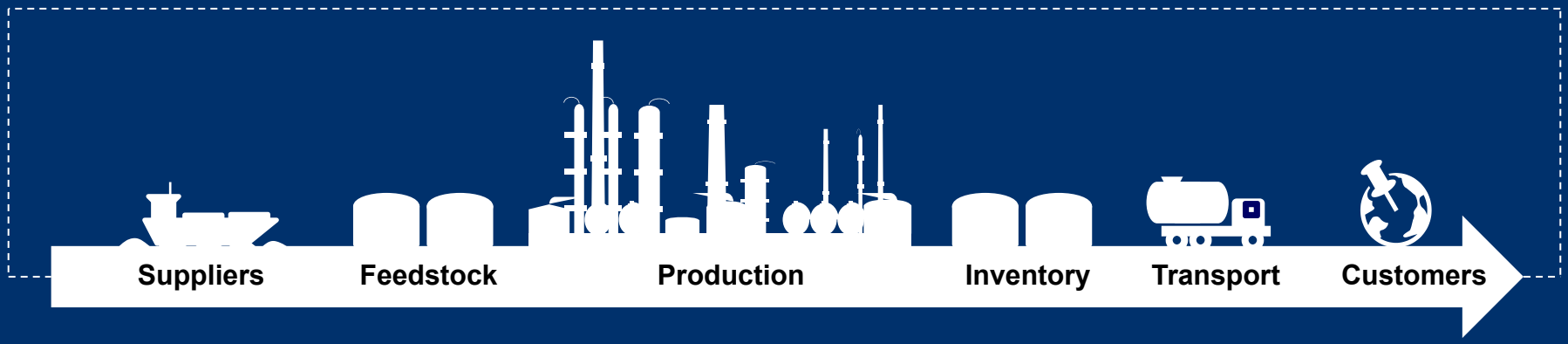
May 26, 2016

Topics

- What we observe
- Different worlds
- IT/OT integration
- Cyber Security
- Infrastructure
- Services
- Summary

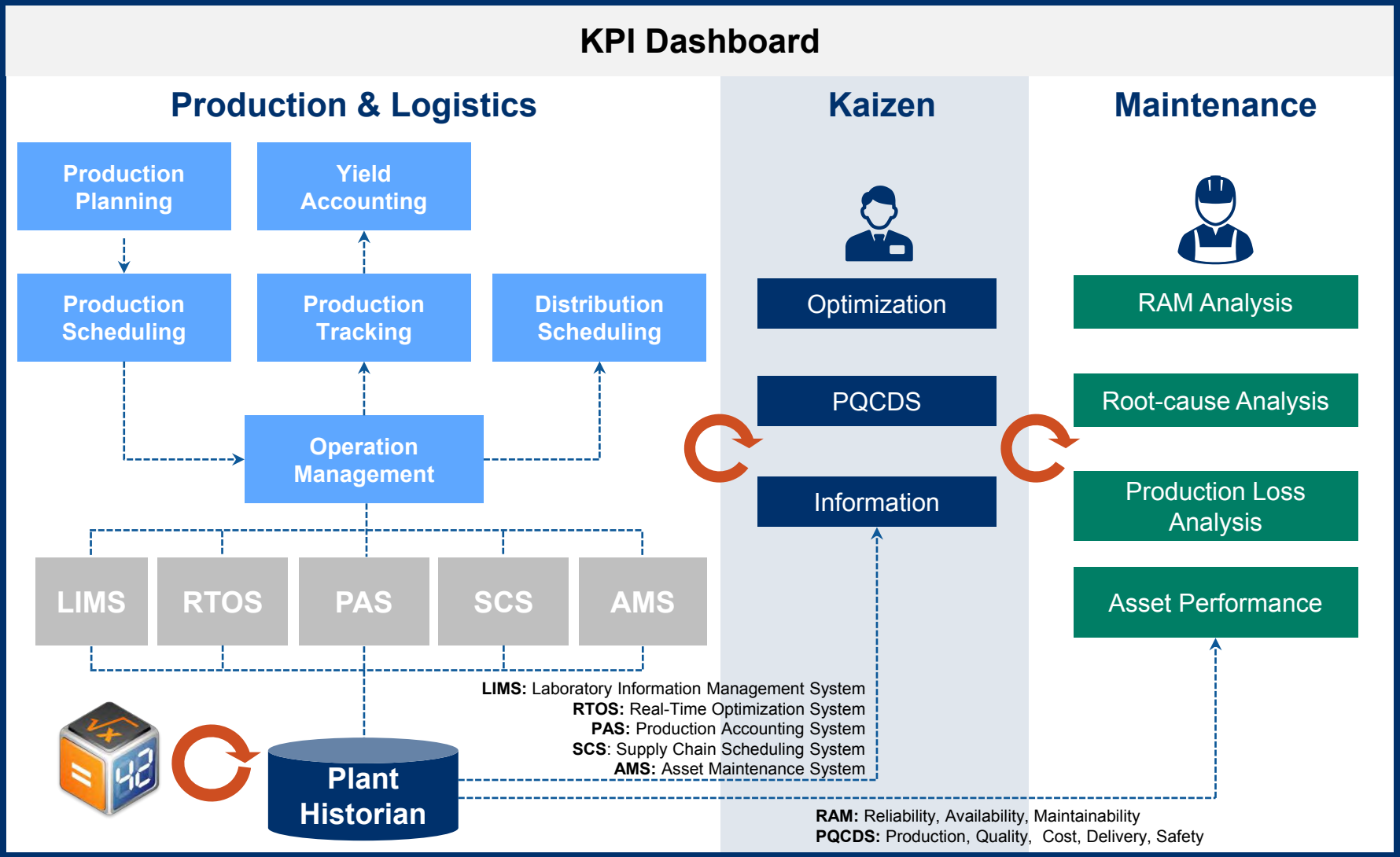
What we observe

Supply Chain Program



Supply Planning	**Annual Delivery Program**	**Sales and Operations Plan**
Tactical Planning	**90 Days Planning**	**Production and Distribution Plan**
Production Scheduling	**Weekly Schedule**	**Production and Logistic Schedule**

Information



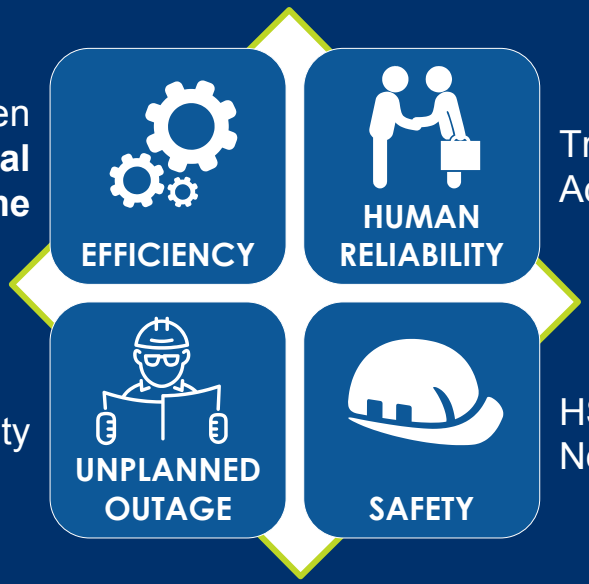
Our Observation - POOR INTEGRATION LEAD TO “SILORIZATION”

MANY HAVE INVESTED IN ADVANCED SOLUTIONS TO IMPROVE OPERATIONAL EFFICIENCY, BUT POOR INTEGRATION LEAD TO “SILORIZATION”

- Planning and Scheduling;
- Operational Management;
- Asset Management, Vibration Monitoring, AMADAS, etc.;
- Alarm Management, Operator Training Simulator

MANAGEMENT CONCERNS AND CONTINUOUS IMPROVEMENT

Close the “Gaps” between **Planned** and **Actual** in **Real-time**



Trained Competency versus Actual Competency

Asset Reliability

HSE, Asset, Personnel, Incidents, Near miss reporting

Different worlds

The different domains

Internet

Level 4	Enterprise Resource Planning system (Office domain)	IT
Level 3.5	Demilitarized Zone (DMZ)	
Level 3	Systems to integrate level 2 and 4 (MES)	OT
Level 2	Supervisory, control and safety systems (PCD)	OT
Level 1	Sensing and manipulating equipment (e.g. instrumentation and valves)	

PCD = Process Control Domain
MES = Manufacturing Execution System

So many stakeholders

Share holders

Senior Management

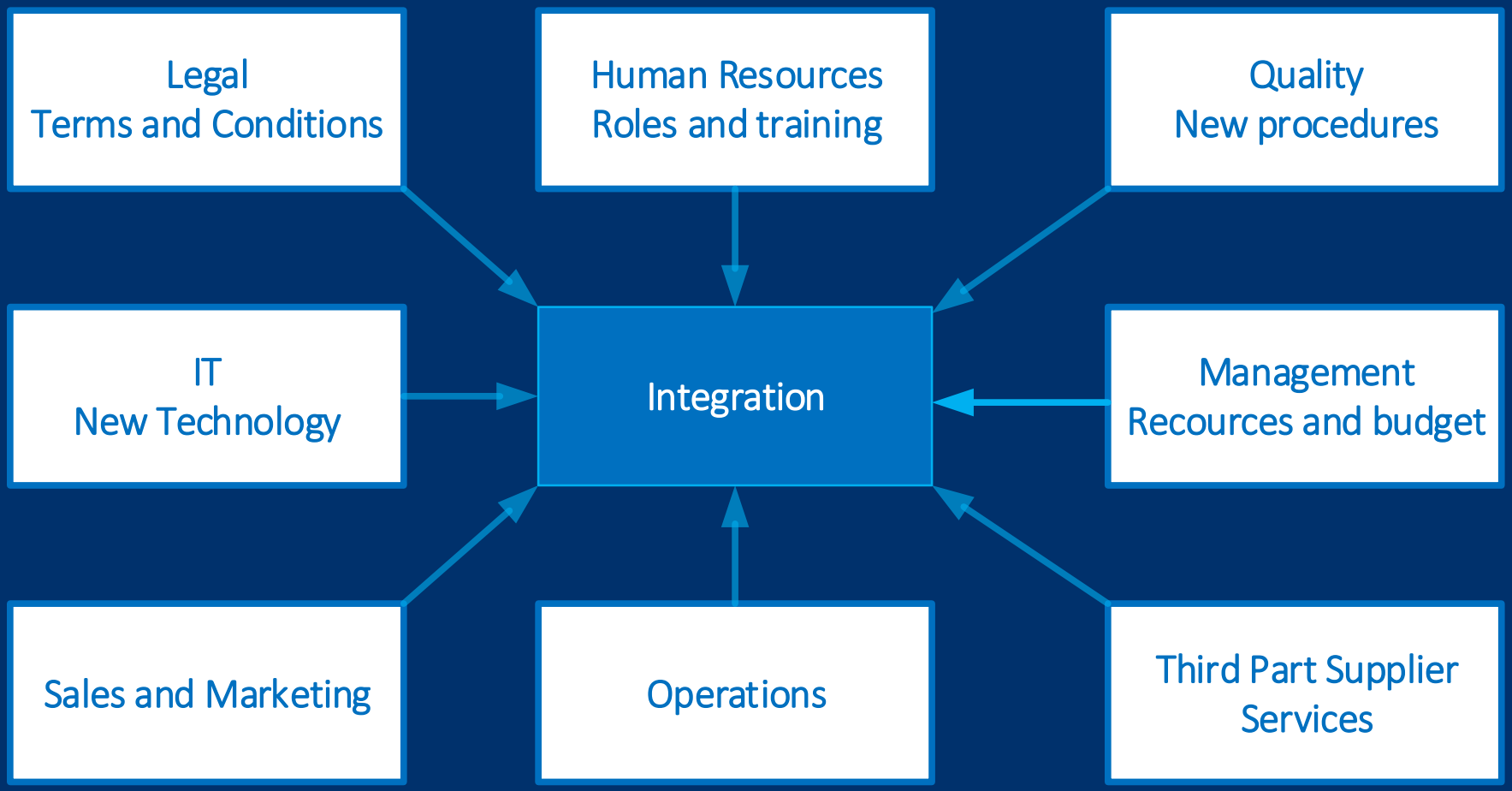
Trade | Planning | HSE | Finance | HR → Readiness → Business

Communication and integration

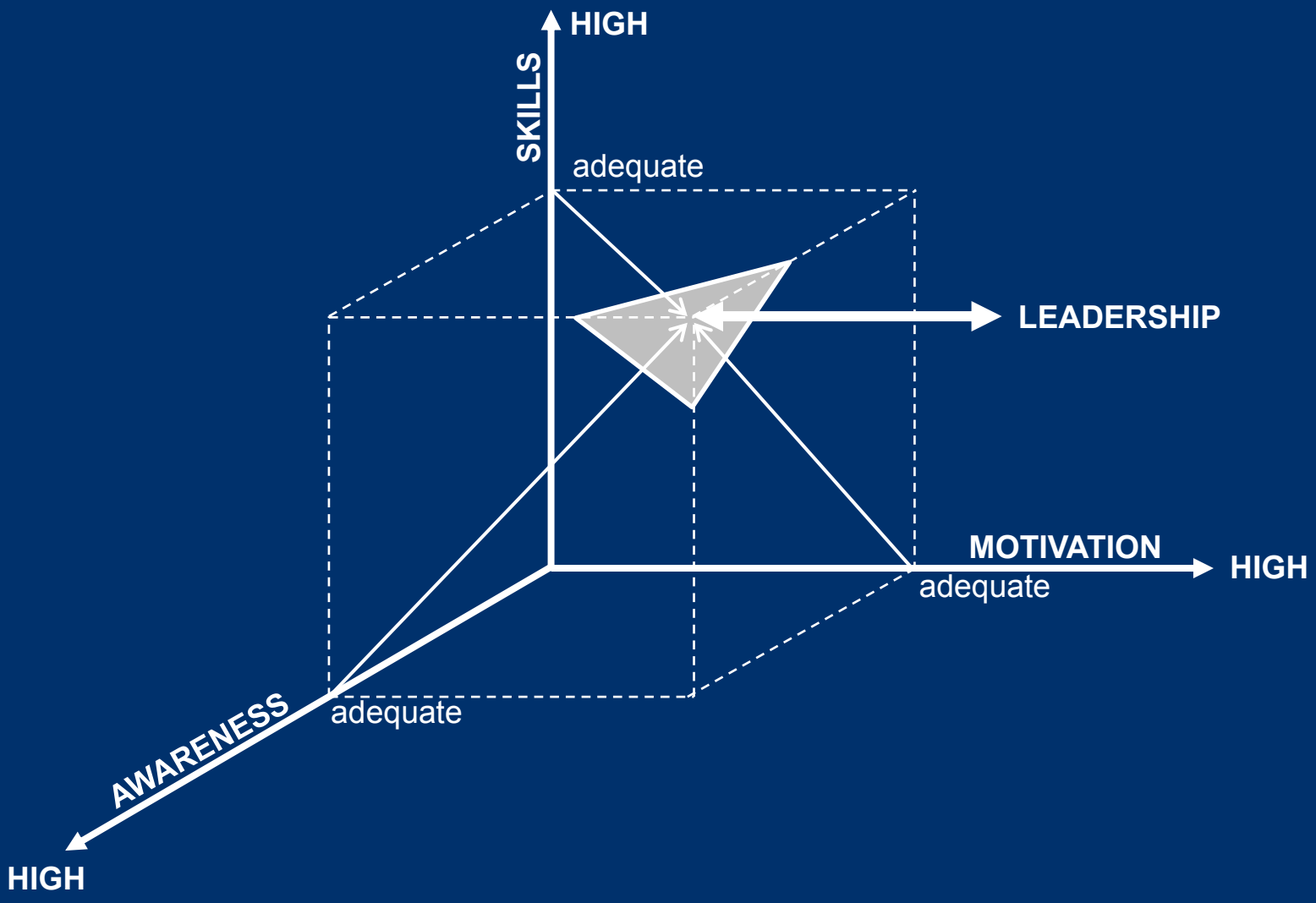
Operation | Maintenance | Training | Marine / Port | Engineering → Readiness → Operations

Contractor / Vendor

Change management



Prerequisites for Change



IT/OT Integration

Business Excellence

Operational performance

Business performance

Key Pillars for Operational & Business Performance

Business Performance

Supply Chain Management

Minimize disruption to supply chain and ensure committed delivery.

Operations Management

Ensure safe operation and regulatory compliance
- License to operate.

Asset Management

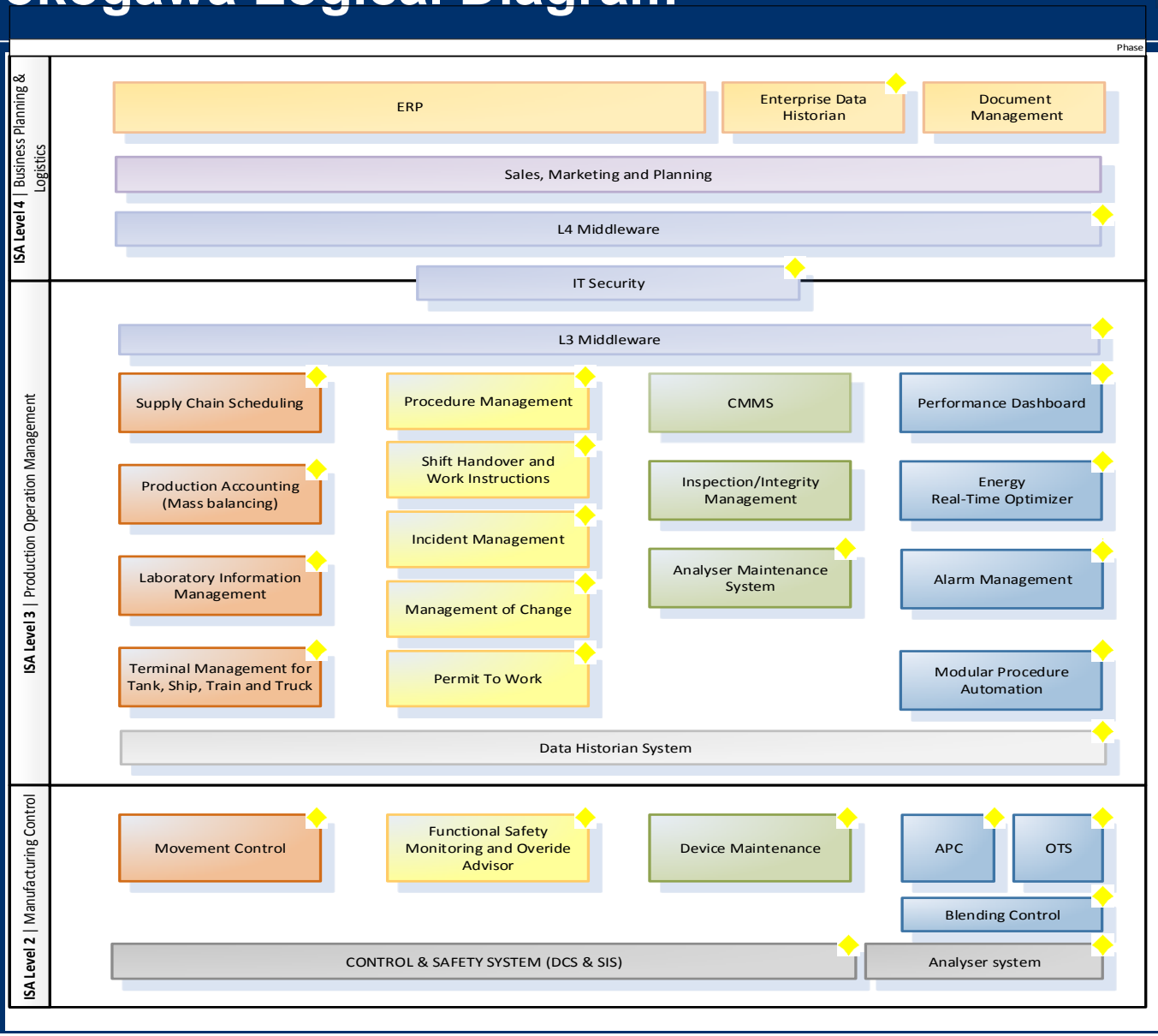
Maximize asset deployment and avoid unplanned downtime by ensuring equipment is healthy and operating in the optimum mode.

Production Management

Clear alignment of business and production objectives. Minimize operating cost and improve yield.

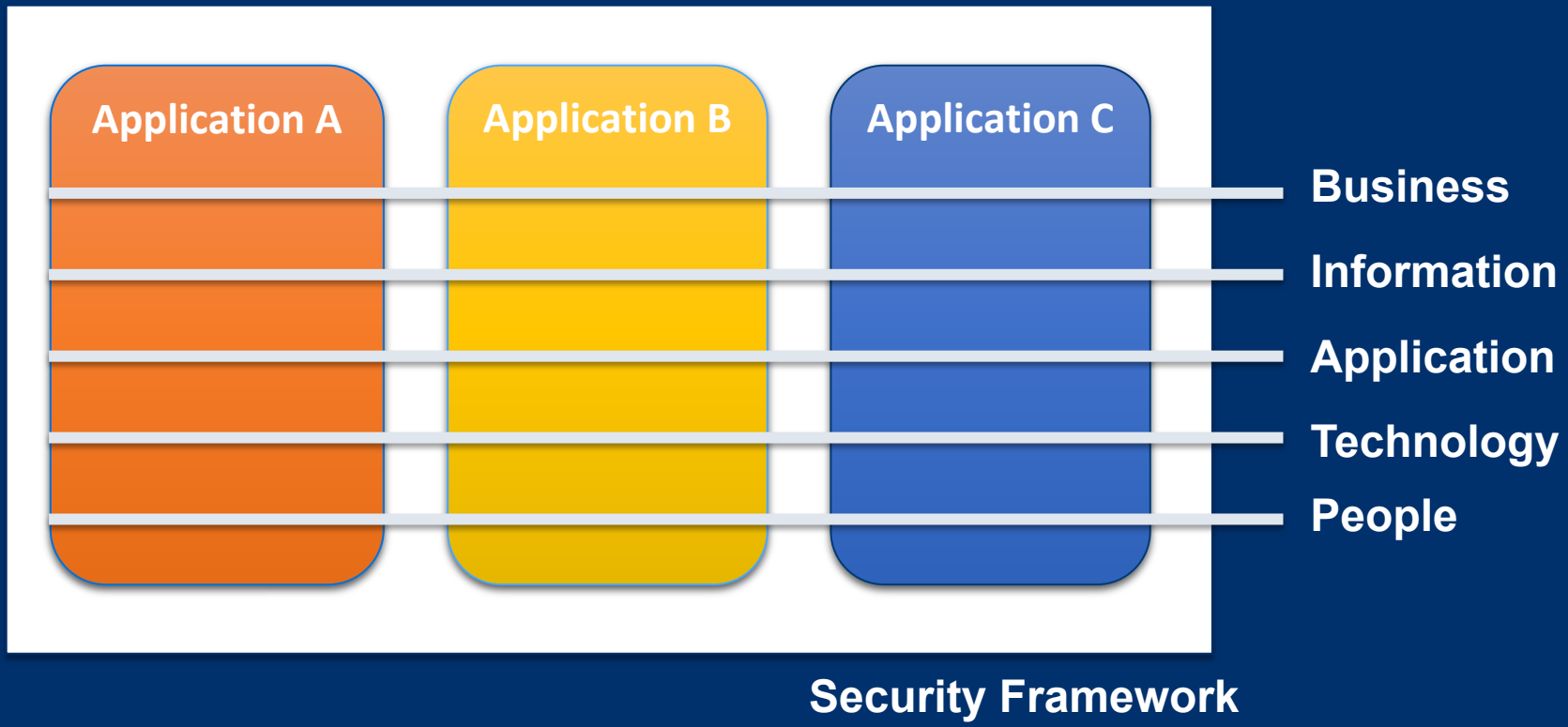
Operational Performance

Typical Yokogawa Logical Diagram

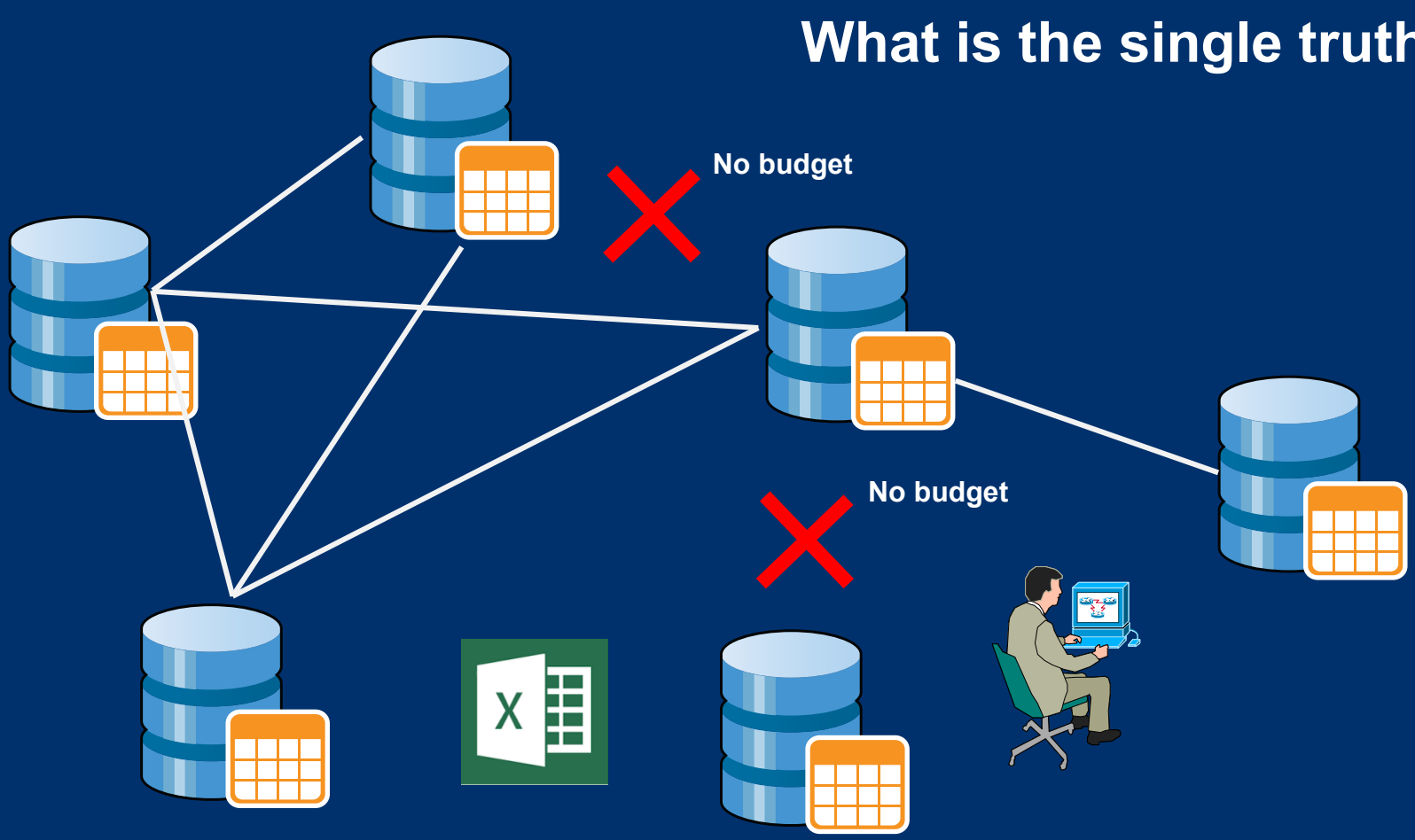


Integration levels

- Value added lies in integrating the various applications into one environment



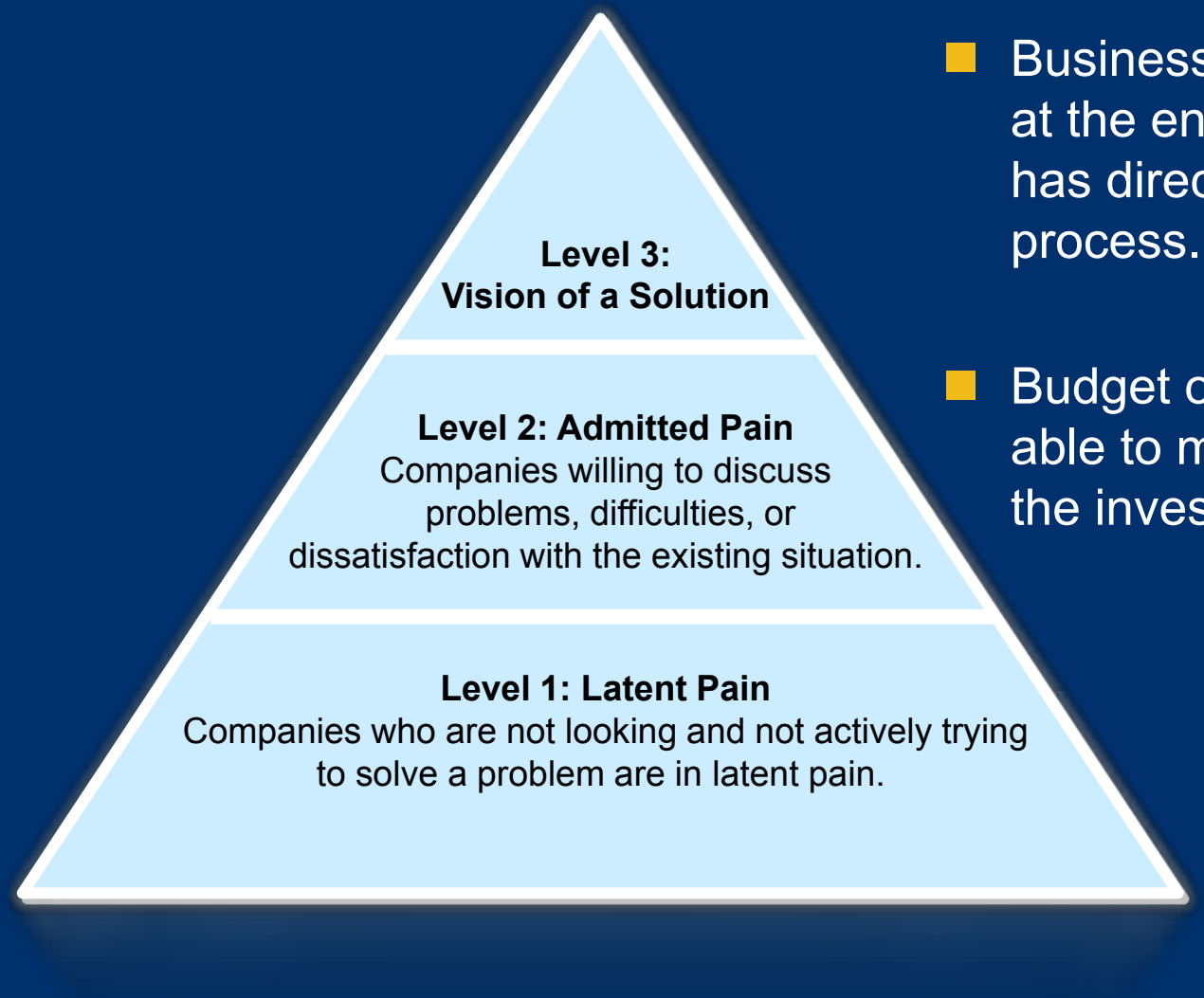
From zero to chaos



Focus integration

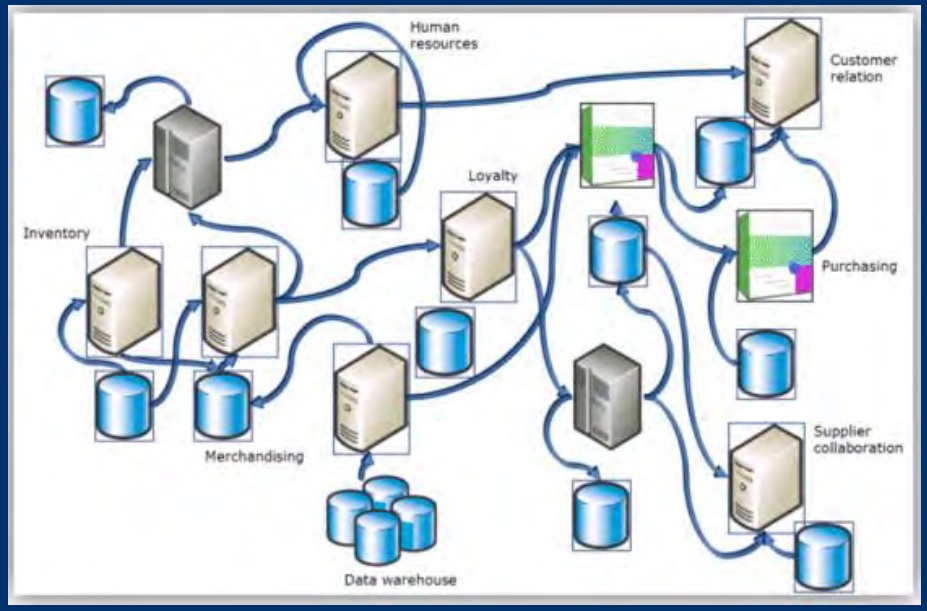
Implementation by	Contractor	IT department	Business consultant
Focus L3 Integration	Low	Medium	Medium
Scope uncertainly	Relatively low	High	Relatively high
Interdependency	Moderate	High	Very High

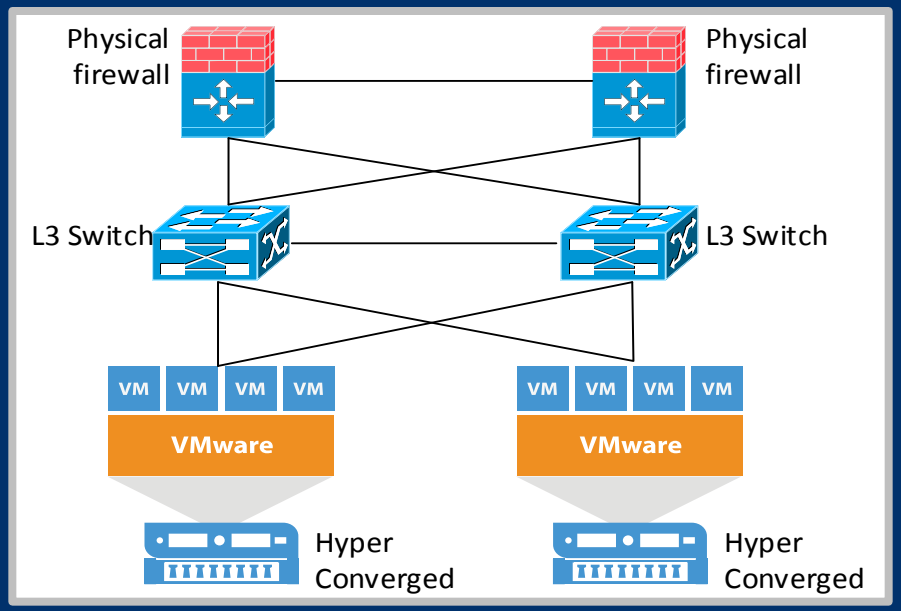
Pain and Owners



- Business owner: Often the person at the end of the pain chain and has direct influence on the process.
- Budget owner: The person who is able to make budget available for the investment

Chaos versus managed





- Many boxes many brands
- Multiple policies for infrastructure and security
- Many point to point interfaces

- Excel is our best friend
- Significant human intervention
- No single truth

- Brands and boxes managed
- One policy for infrastructure and security
- Few interfaces preferable via middleware

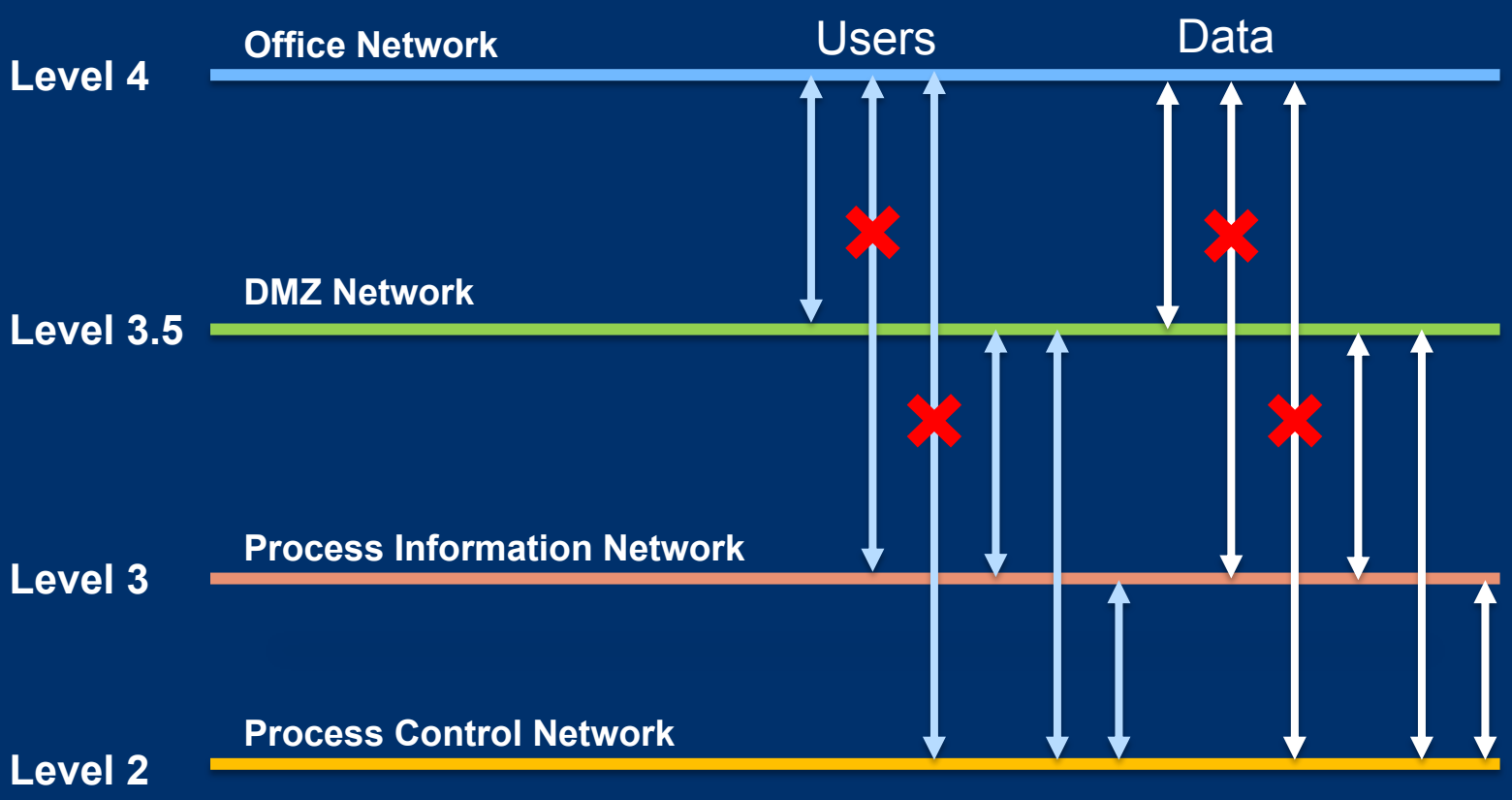
- Excel is not an solution
- Almost no human intervention
- One single truth

Cyber Security

Causes of intrusions

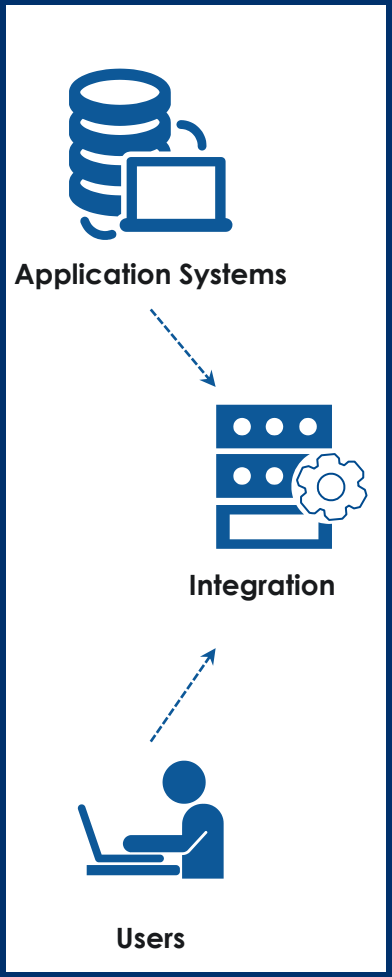
- No proper procedure in place for Cyber security in the Operational Technology (OT) Domain.
- No ownership for Cyber security in the OT Domain.
- Company information not well protected.
- User profiles not well defined.
- Hardware not proper hardened (e.g. switch of USB ports)
- Computers and servers don’t have to latest patches.
- No updated anti virus software.
- No proper monitoring of hardware, software and applications.

User and Information streams



The way information is exchanged between the different layers significantly determines the Cyber Security Infrastructure

Security Precausions

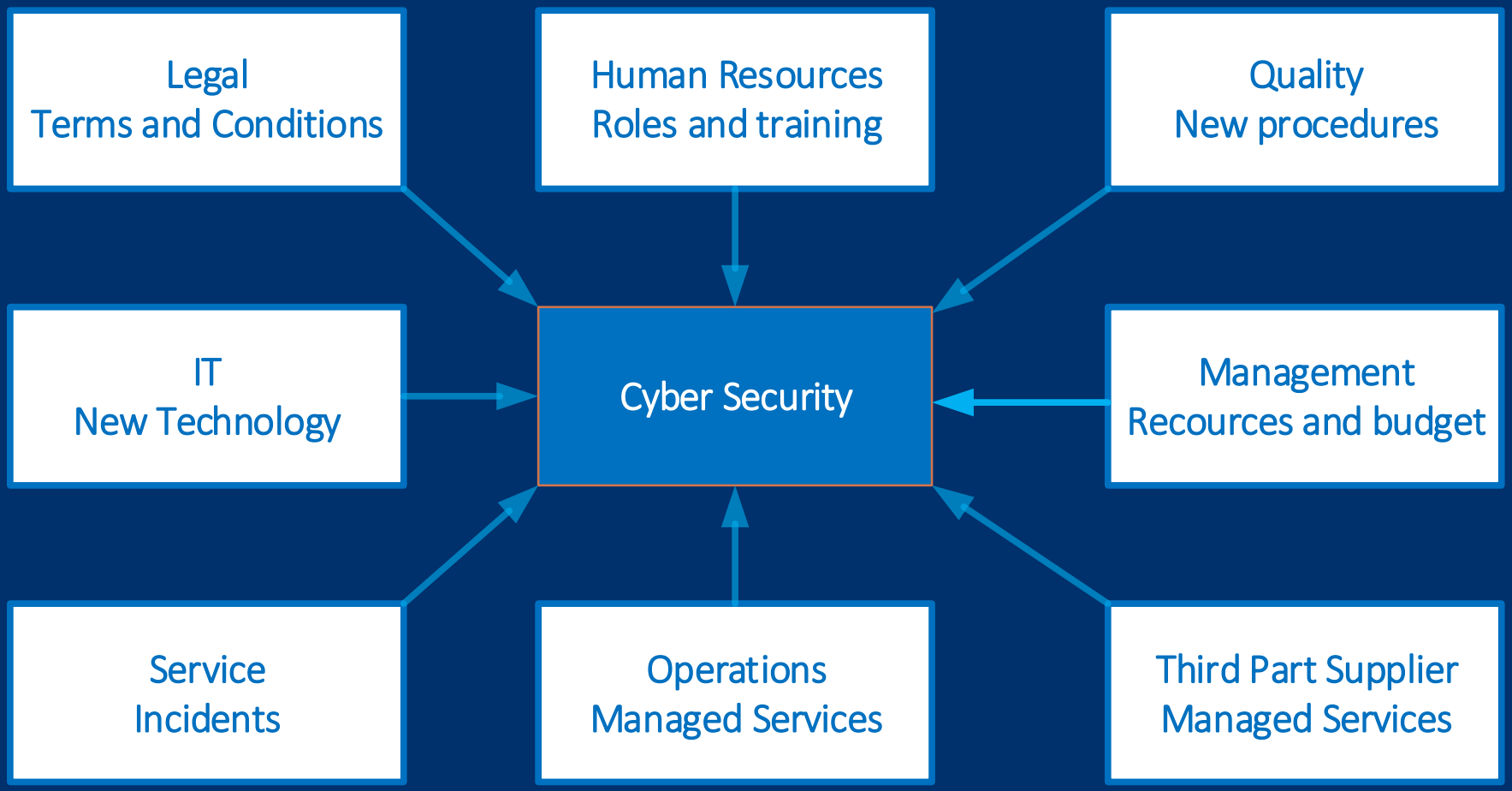


- Physical Security
- Network Security
- Host Based Security
- Application Based Security
- Disaster Recovery
- Services

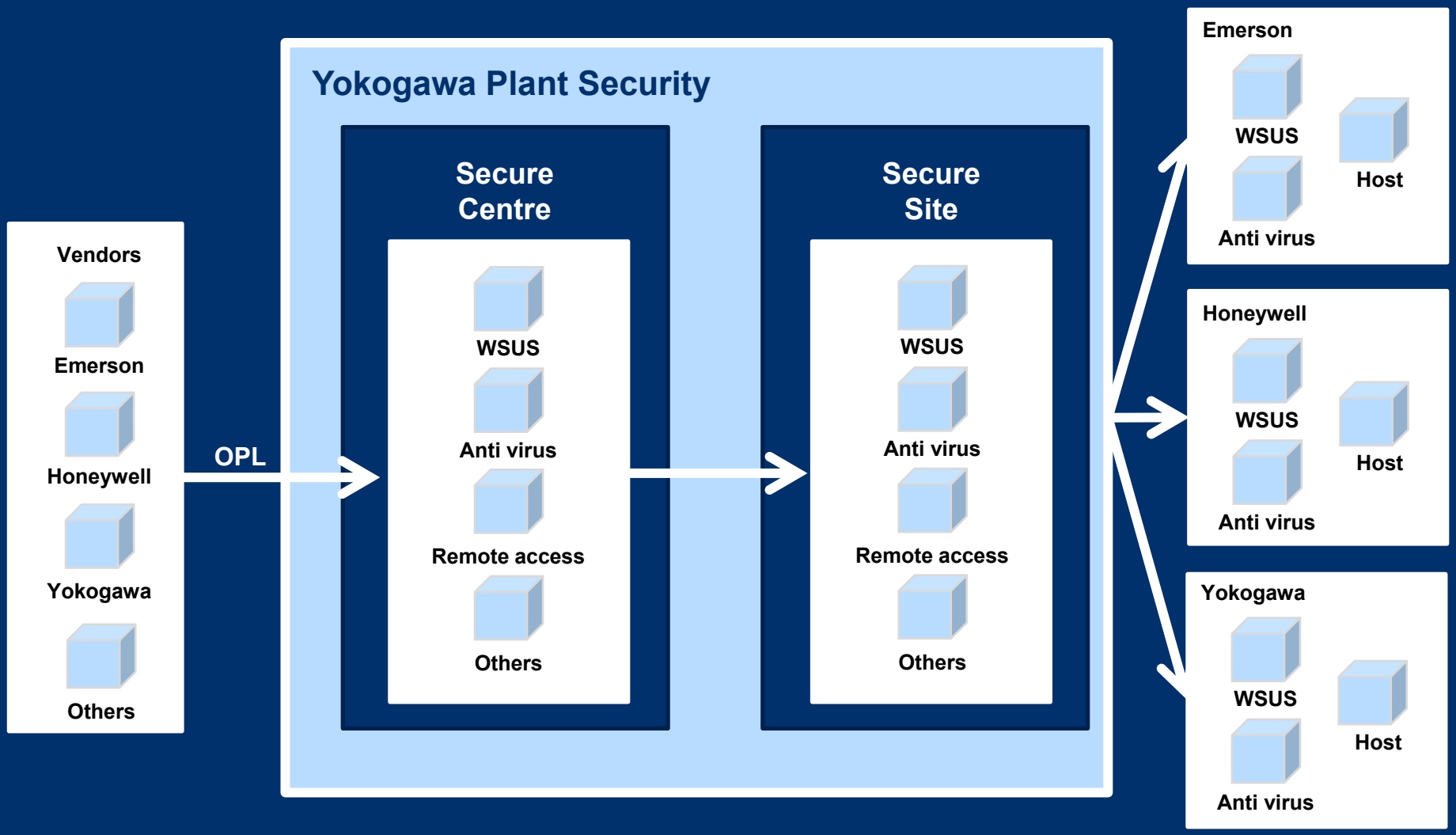
Plant Security Program

	Plant Security Program Level		
	Plant Alert	**Plant Remote**	**Plant Secure**
Plant Baseline Assessment	✓	✓	✓
Awareness Cyber Security Training	✓	✓	✓
Plant Security Master plan design	✓	✓	✓
Plant Security Policy and Procedures	✓	✓	✓
Plant Security Design Service		✓	✓
Plant Security Implementation Service		✓	✓
Plant Security Capability Training Package		✓	✓
Remote Monitoring			
- 24/7 Live Monitoring		✓	✓
- Patching and update service			✓
- Asset Management and logging			✓
- Third party remote access			✓
Incident Management			
- Incident Response		✓	✓
- Maturity Reporting			✓

Change management assessment



Infrastructure Yokogawa Plant Security



Secured Remote Solutions FY'14 Achievements

ARC Forum (9th – 12th Feb. 2015 in Orlando)

Press Release (Japanese/English)

Press Release YOKOGAWA

Tokyo, Japan - February 10, 2015

Yokogawa and Cisco Deliver Cybersecurity Solutions for Shell

Yokogawa Electric Corporation announces a collaboration with Cisco Systems, Inc. to deliver Shell's SecurePlant initiative at Shell. SecurePlant is a comprehensive security management solution for plant control systems that was jointly developed as an initiative between Cisco, a leader in the IT industry, Yokogawa, a leader in mission-critical plant automation systems, and Shell. The three companies have agreed to proceed over the next three years with the implementation of SecurePlant at around fifty Shell plants globally.

Industrial producers around the world face a wide range of operational challenges in areas such as cybersecurity that pose a pervasive threat to safety and availability. Most companies with global operations, however, still take a relatively simplistic plant-by-plant approach, such as implementing operating system security patches and anti-virus pattern file updates. As a result, security levels tend to vary at each plant.

In the general practice of control system security management, individual control system vendors extensively validate security patches and anti-virus pattern files to confirm that they do not interfere with system operation, and then report the results to their customers for implementation. Since plants tend to use a variety of control systems and equipment from different vendors, occasionally with multi-generation platforms from a single vendor, this process is often complicated. For this reason, plants increasingly have the need for plant-wide integrated services that take a more holistic and efficient approach to the management of system security.

With the aim of standardizing security practices at Shell plants around the world and minimizing control system vulnerability, Yokogawa and Cisco collaborated on the design of the SecurePlant service and will jointly provide deployment and operational services.

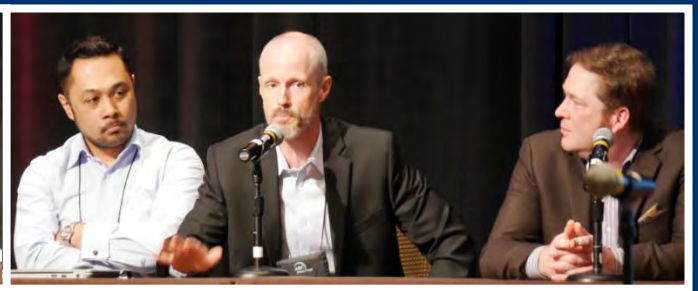
The SecurePlant solution is designed as a standard solution that consists of the delivery of OS patches and anti-virus pattern files for control systems and the provision of real time and proactive monitoring of solution delivery, as well as a help desk operation to manage this solution.

Supplier-certified Windows security patches and virus signature files are distributed from a SecureCenter to the SecureSite at each plant via Shell's existing global network. The real time and proactive monitoring capabilities enable the centralized management of plant security. A customer help desk operated jointly by Yokogawa and Cisco is available 24/7/365 to manage solution related incidents.

Moving forward, Yokogawa and Cisco will continue to offer comprehensive security solutions involving the deployment, operation, and monitoring of control system environments. These services are applicable to plants of all sizes in a wide variety of industries, including facilities spread out over a large geographic area. In addition, both companies will leverage their technologies and experience to develop deep industrial

1

User Presentation & Panel Discussions



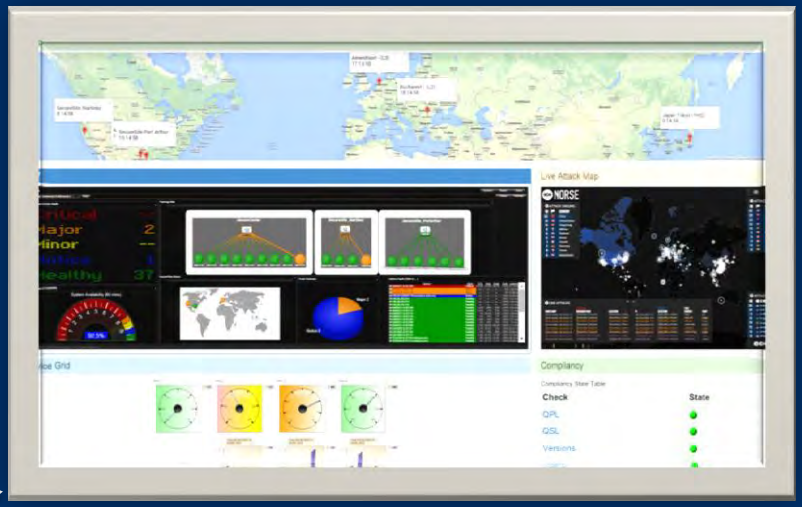
Managed Services delivered by Yokogawa

Requirement	Yokogawa Managed Service
Asset Inventory	Automated asset discovery and asset inventory
O.S. Security patching	Automated distribution of validated Microsoft updates
Anti-Virus Management & Updates	Automated distribution of validated signature updates
Remote Access	Unified secured remote access, with 2 factor authentication
Log file collection	Automated log file collection to central log server
Security majority reporting	Automated report of the status of the applied security measures
Proactive system monitoring	CPU, Memory load, Disk usage, system and software failures
24x7x365 supported	Helpdesk and managed services
Incident response	Global security incident response team

Incident response center

Glance overview to support Help Desk Operation & SLA with below information:

- **SecureCentre and SecureSite Locations**
- **SecureCentre/Sites Monitoring**
- **Call Handling Status**
- **Ticketing/Incident Monitoring**
- **Compliance Status/Report**



L2 Help Desk in Romania

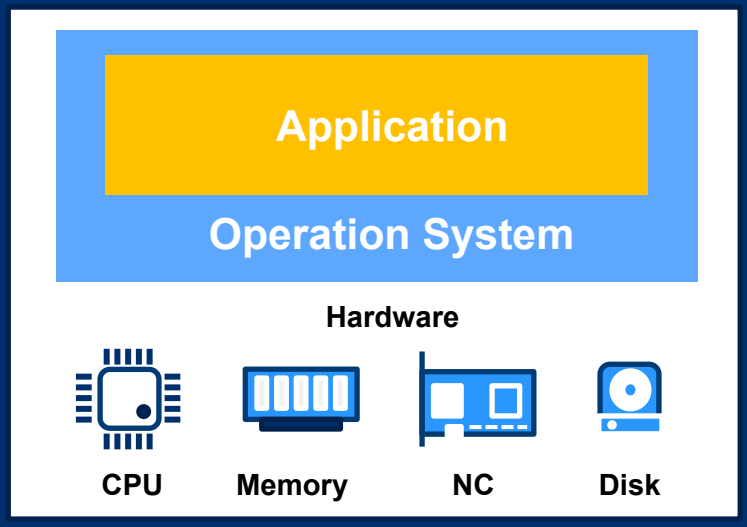
L3 Help Desk in Amersfoort

| V2016 | April 2016 |

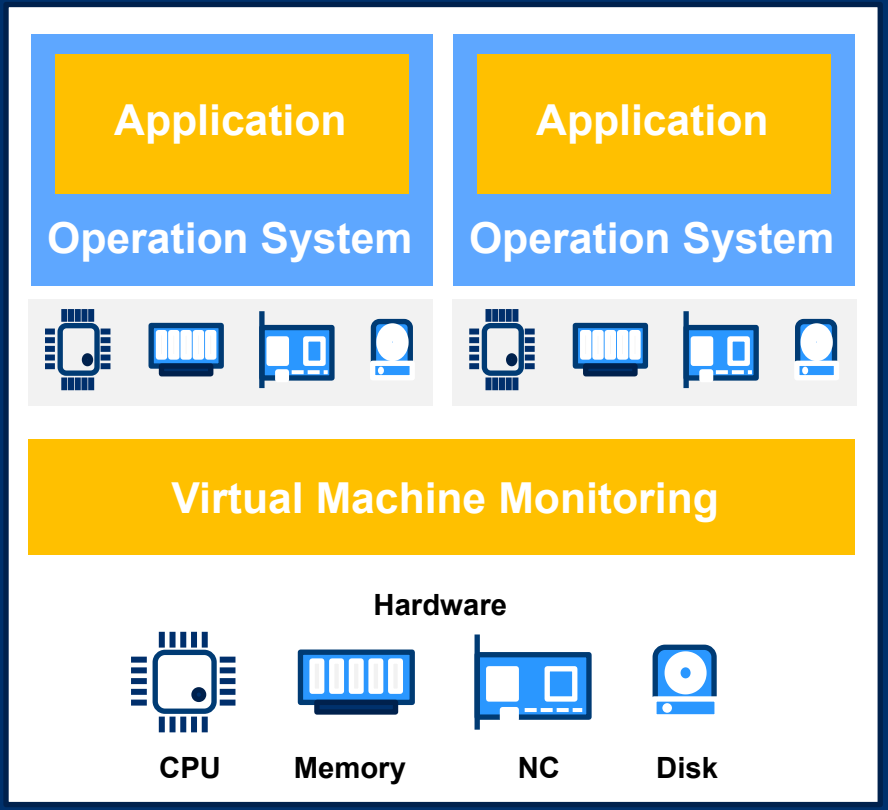
Infrastructure

Virtual Machines

Virtualization is a proven software technology that is rapidly transforming the IT landscape and fundamentally changing the way that people compute, such as an operating system, a server, a storage device or network resources.

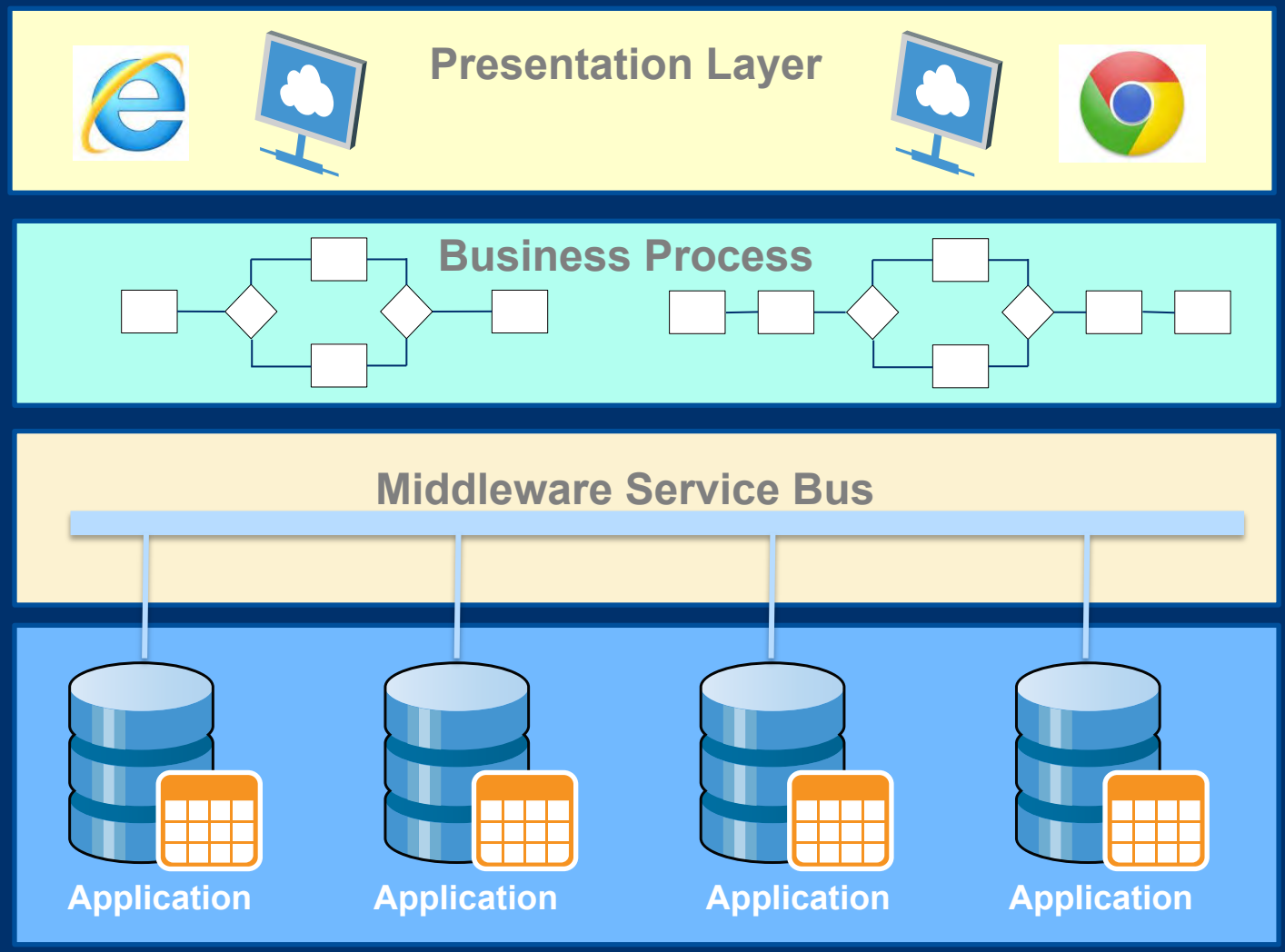


Traditional server with operating software



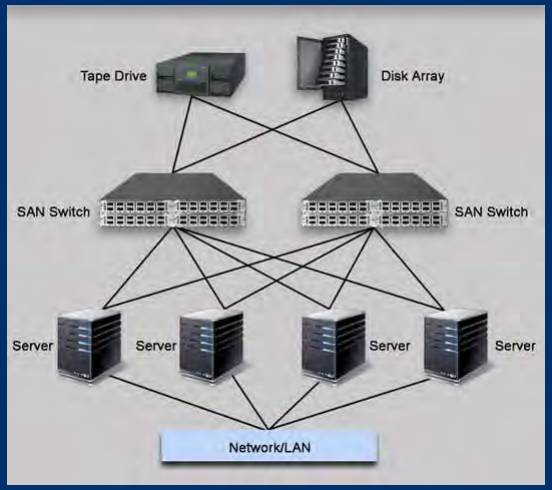
Server with two virtual machine operating software

Middleware setup



Storage

- **Storage Area Network (SAN)**
  - Block level data
  - Primary media: Optical fiber
  - Reliability
  - Performance
  - Access



- **Network Area Storage (NAS)**
  - File level data
  - Primary media: Ethernet
  - Remote Access
  - File Sharing
  - Scalable

Hyperconverged Systems

- Optimize performance and efficiency - simplify deployment of servers, storage, and networking for business applications
- Centralized management of compute, storage and virtual machines
- 10GbE networking for application and storage performance
- High availability

Summary Integrated Production Management System

- IPMS is critical for the operational and business performance of the plant
- Assign a business owner and budget owner for the IPMS
- Write a IPMS master plan at an early stage of the project
- IPMS budget is often forgotten with consequences
- Deployment of the IPMS afterwards happens rarely
- IPMS is the responsibility of the operator and not the EPC
- Delivery time IPMS is often under estimated (12 – 18 months)
- The IPMS provides the single truth which is a completive benefit

Co-innovating tomorrow™