| fɒg kəmˈpjuːtɪŋ|

# FOG COMPUTING

Fog computing is like  cloud computing
but closer to the “Things”

| fɒg kəmˈpjuːtɪŋ|

# FOG COMPUTING

Fog is about reactive cyber-physical applications

| fɒg kəmˈpjuːtɪŋ|

# FOG COMPUTING

Horizontal, system-level architecture that distributes computing, storage, control and networking functions closer to the users along a cloud-to-thing continuum

Cloud technologies are not always applicable on the edge because of performance and resource constraints

A new infrastructure has to be "invented" for Fog Computing, innovating where necessary and reusing when possible

# FOG COMPUTING TRAITS

Real-Time Performance and Reliability

Location- and Resource-Aware deployment

Resource and Device Virtualisation

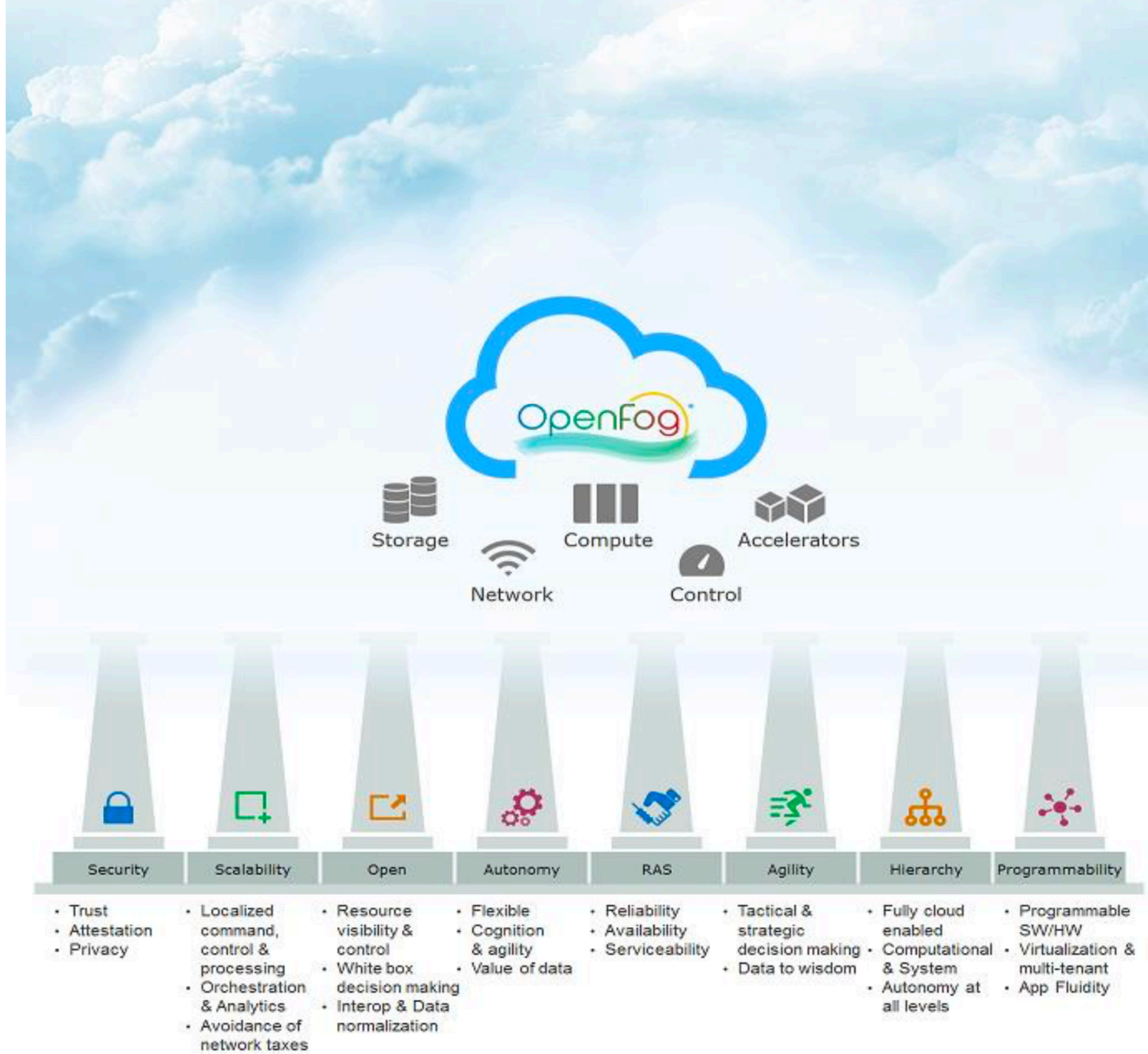
# FOG COMPUTING TRAITS

Resource aware provisioning of applications and tenants

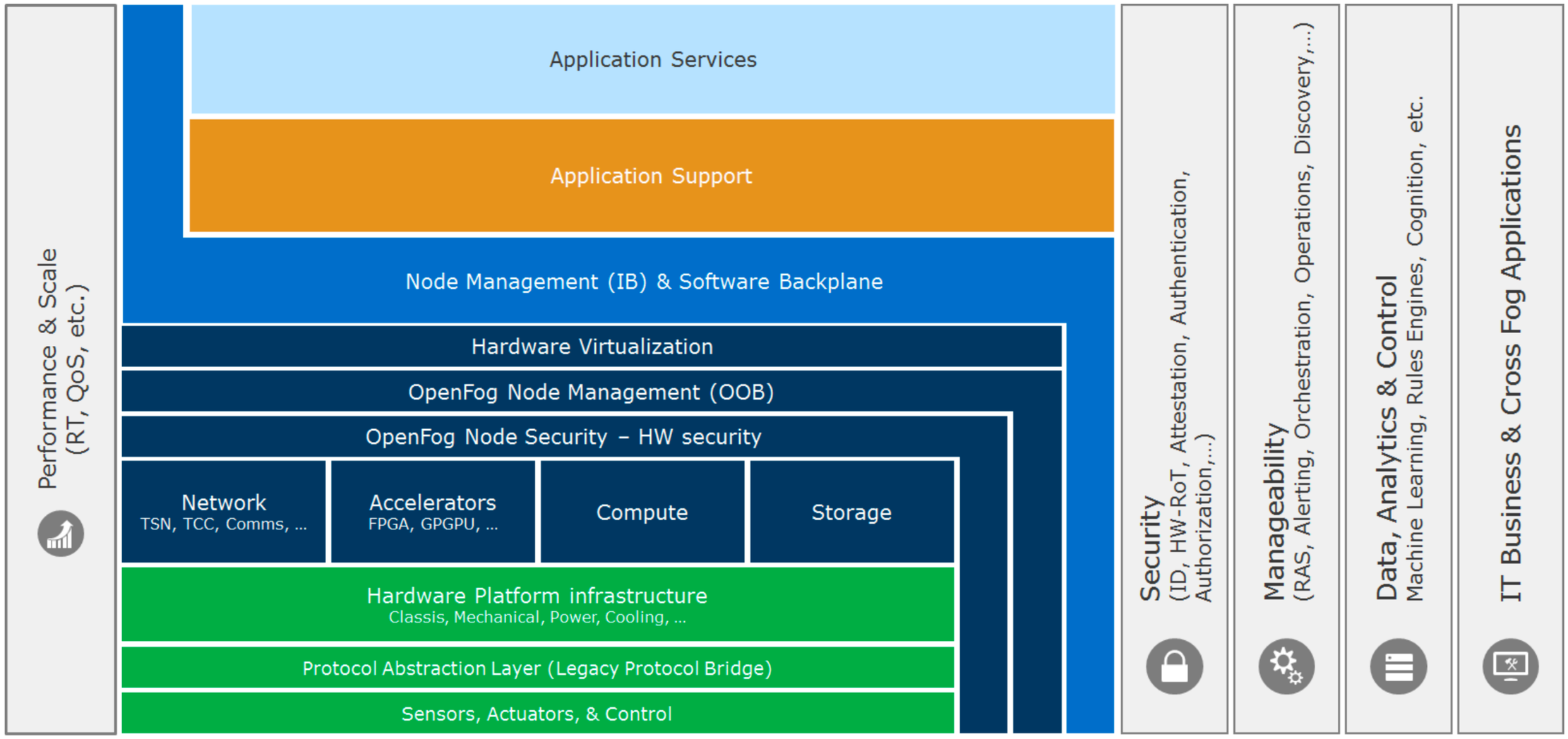
Tamper Proof Security (in some deployments it is easier to get physical access to the fog platform)

# OPEN FOG CONSORTIUM

The recently established OpenFog is accelerating and facilitating the expansion, convergence and interoperability of Fog computing stacks



# OPEN FOG REFERENCE ARCHITECTURE



# HAS IT BEEN PROVEN?

# BARCELONA
# SMART CITY PLATFORM

Fog Computing Platform

Dashboard

-- choose ready node --

Fog Computing Platform

admin

Dashboard

fognodes

system

dashboard

fognode5

Status | Metrics | Cabinet Energy Control | Services | Logs

Select Device:

P1 P2

Consumption 1 Consumption 2

2000

0

12:30 12:35 12:40

Wed 2 December

12:30 12:35 12:40

Wed 2 December

rt-01

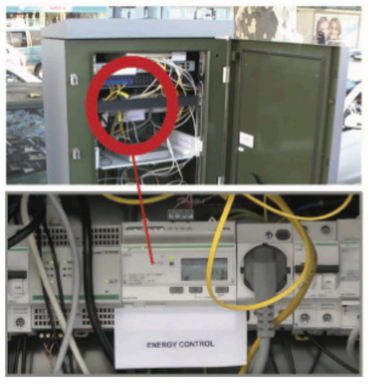
Temperature

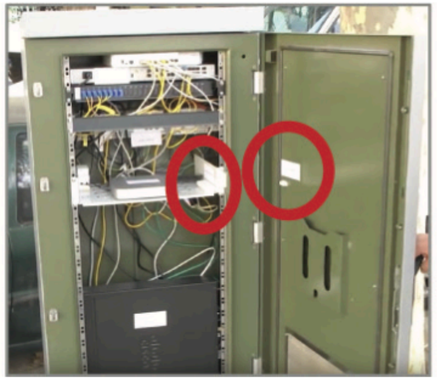
Humidity

Humidity

C/ Llacuna, 162, Barcelona, 08018

| Criticality | Policy/regulation | Connectivity limitations & bounded delay | Local processing |
|---|---|---|---|
| A | B | C | D |
| Autonomous operation at the edge | Data privacy policies and/or operational reasons | Physical constraints | Anomaly detection |
| A | A | B C D | A B | B |
| UC1<br>Power monitoring and control of elements in public spaces | UC2<br>Access control and telemetry of sensors through street cabinets | UC3<br>Event-based video | UC4<br>Traffic analysis and regulation | UC5<br>Connectivity on demand |



# FOG & MEC

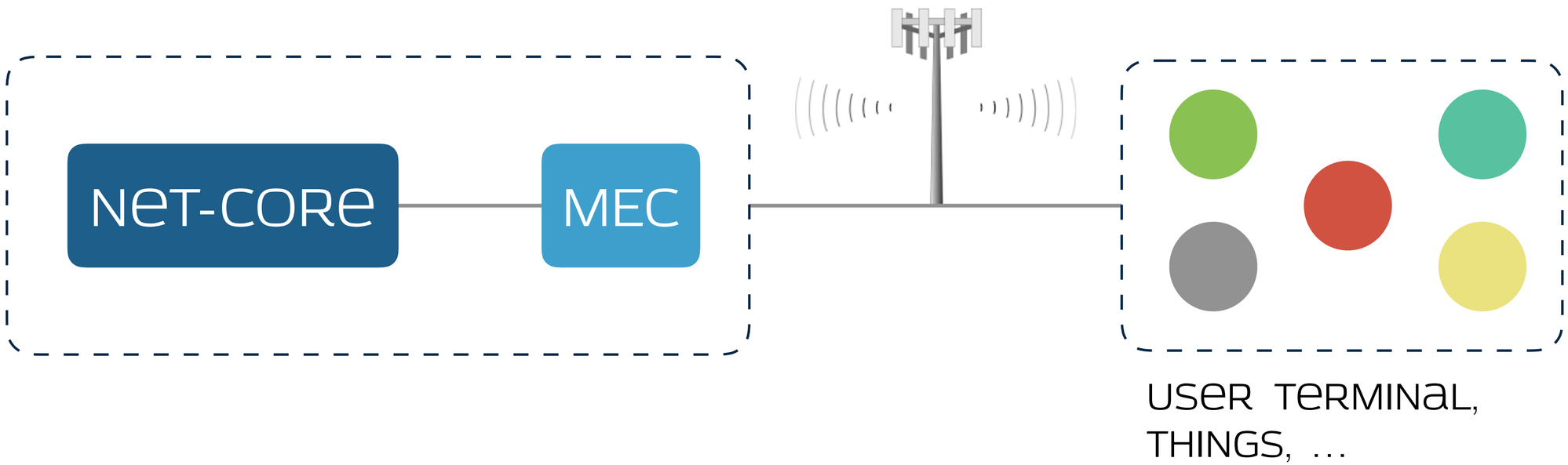
# MEC

A **network architecture concept** that enables **Integrated networking, computing and storage resources** into one **programmable and unified edge infrastructure**.

# MEC BOUNDARIES

The MEC infrastructure resides at the **edge of the operator infrastructure**.

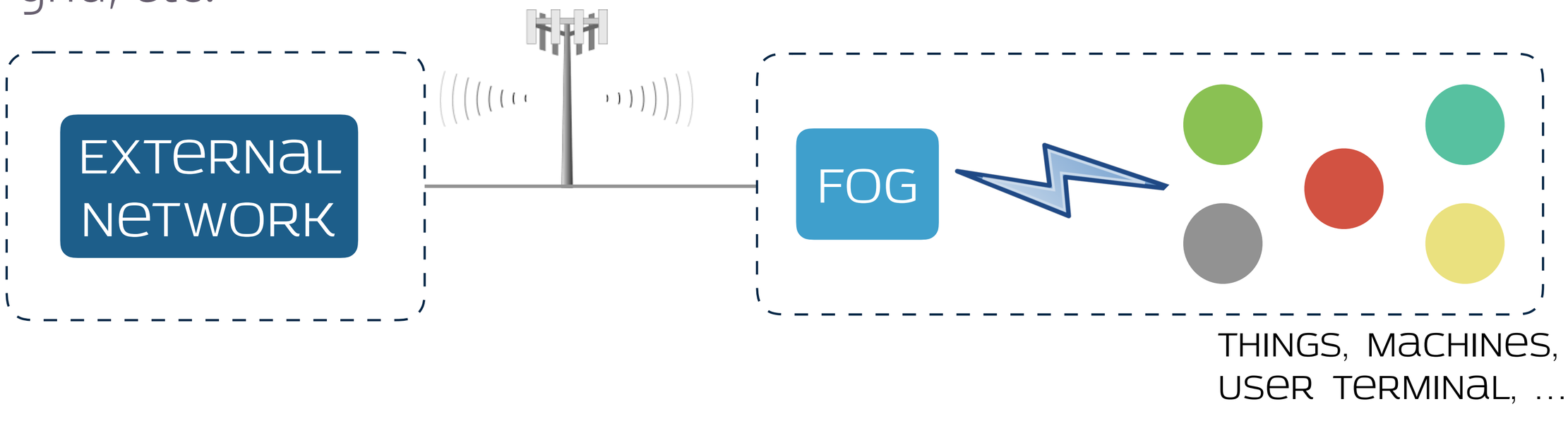
The operator own and manages the infrastructure but not the “things”



# FOG BOUNDARIES

The Fog infrastructure resides **on premises** and at the **edge of end-system infrastructure**.

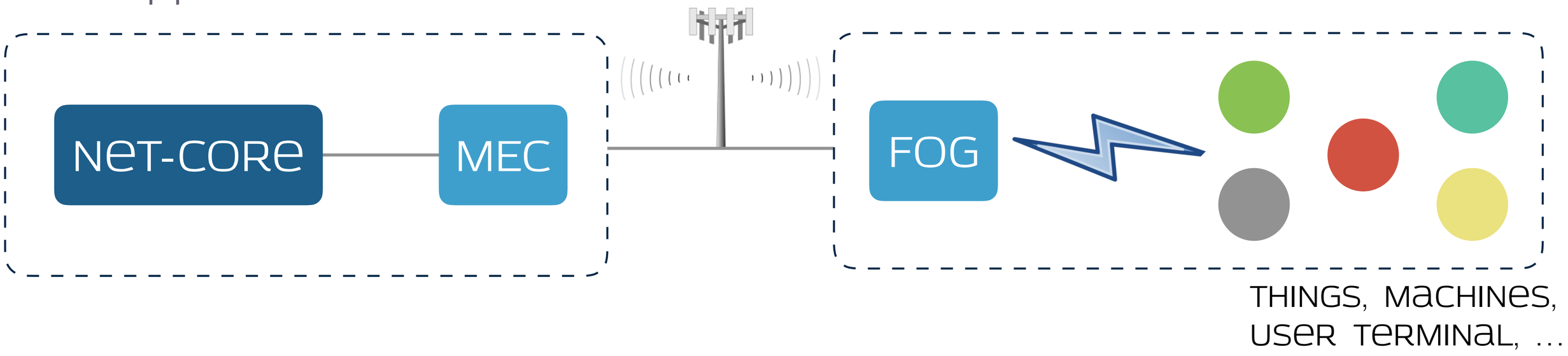
The fog infrastructure as well as the “things” are often owned and managed by the same authority, i.e. smart factory, smart grid, etc.



# FOG / MEC BOUNDARIES

The Fog and MEC infrastructure exist within different administrative boundaries

The ability of leveraging Fog, **on premises**, and MEC at the **edge of the network**, will be the ideal situation for demanding IIoT applications



# REAL-FAST VS. REAL-TIME

5G and MEC focus on **Real-Fast**

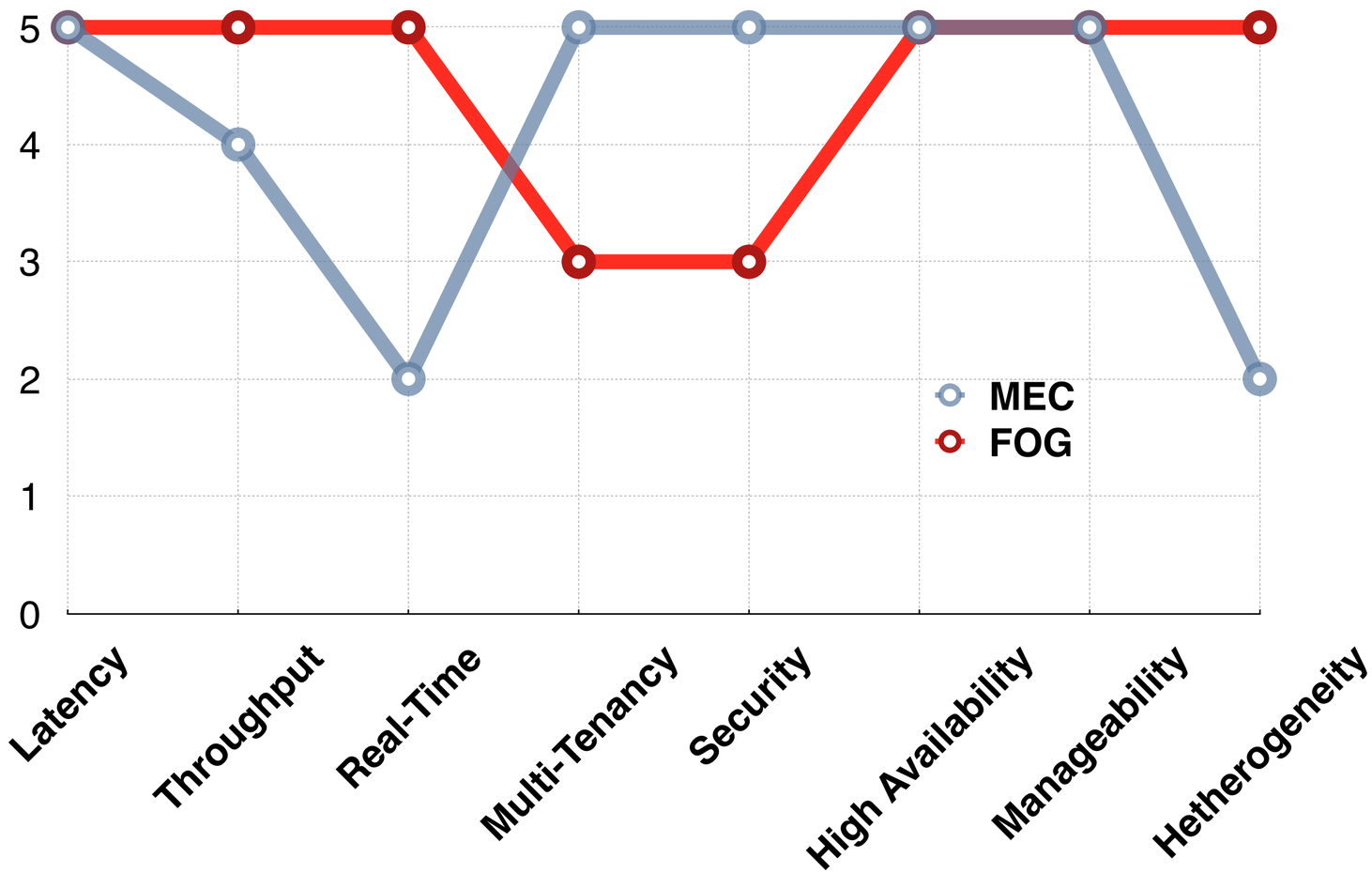
Beside the real-fast Fog has to support **Real-Time**

**Real-Time** and **Real-Fast are not the same!**

# MEC / FOG NEEDS

From an high level perspective MEC and Fog computing aim at virtualising compute, storage and networking at the edge

Yet, their requirements differ significantly in some areas as Fog computing deals with OT systems



# SUMMING UP

**Fog computing** is an architectural paradigm and technology framework **essential to make IoT happen**.

**Fog Computing complements Cloud computing** and can be used as an alternative or an addition

**MEC and Fog Computing aims at the same high level goal,** which is providing a virtualised compute, storage and communication fabric, but have different constraints.

# Reference Architectures

# CIOT AND IIOT

The Industrial Internet Consortium (IIC) and the Industrie 4.0 (I4.0) have  defined reference models and architectures for IIoT systems.

As IIoT requirements  are a superset of CIoT's we'll investigate the need of the former

# Industrie 4.0 / RAMI 4.0

# THE INTERNET OF THINGS AND SERVICES

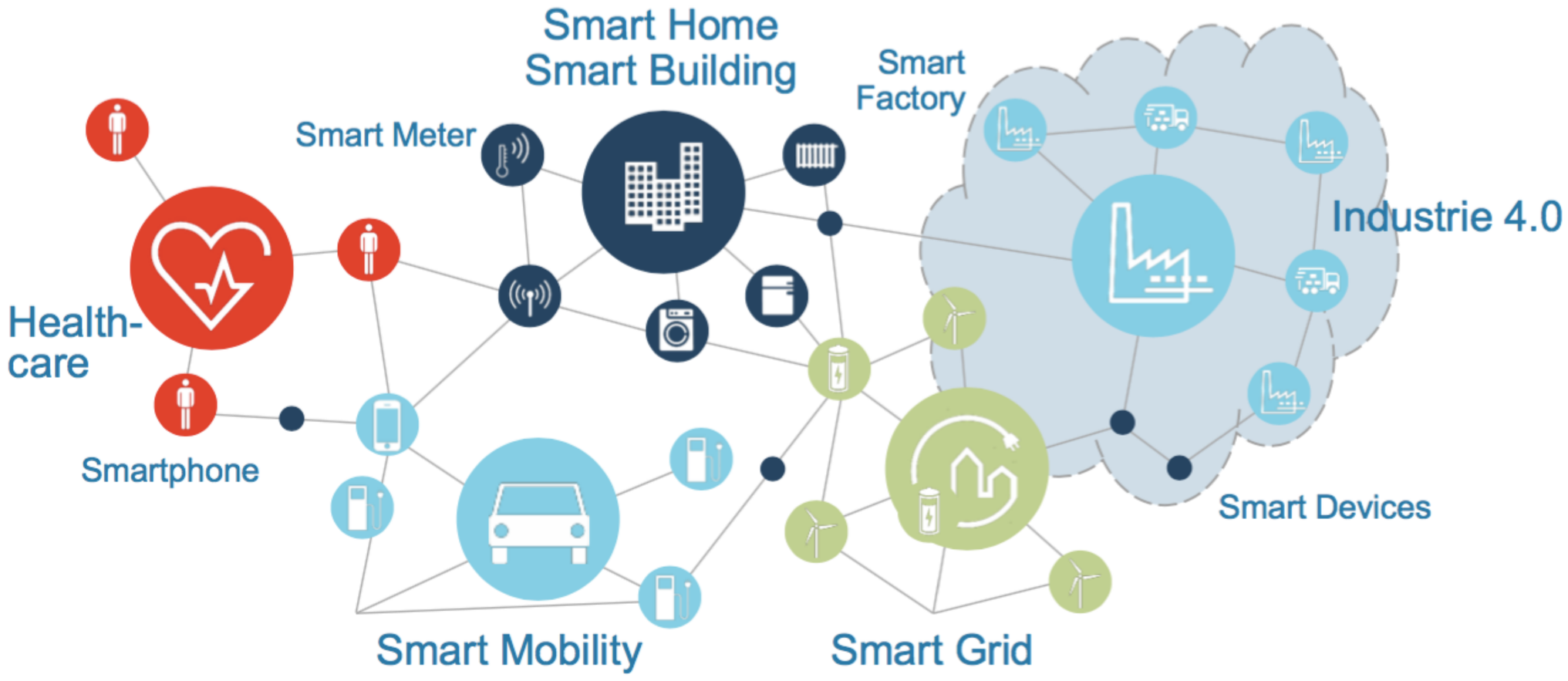



Image curtesy of Bosch Rexroth AG

# INDUSTRIE 4.0 GOALS

I4.0 links production systems with information and communication technology

Customer and machine data are networked.
Machines mutually communicate to control and achieve flexible, efficient, production.

# INDUSTRIE 4.0
# DESIGN PRINCIPLES

Plattform INDUSTRIE 4.0

**Interoperability.** Machines, devices, sensors, and people can freely communicate with each other

**Information Transparency.** A **virtual representation** of the **physical world** is made available by enriching digital plant models with sensor data

**Technical assistance.** Leverage information to make more informed decisions and solving urgent problems on short notice. Physically support humans by conducting a range of tasks that are unpleasant, too exhausting, or unsafe for humans.

**Decentralised Decisions.** Autonomous decisions are the norm. Higher level delegation happens only in presence of interferences or conflicting goals

# RAMI 4.0 GOALS

Group and coherently capture three extremely diverse perspective/aspects into a single model.

1. **Vertical Integration** (within the factory)

2. **End-to-End Engineering** (integrated administrative, commercial, and production processes)

3. **Horizontal Integration** (across factories)

# REFERENCE ARCHITECTURE

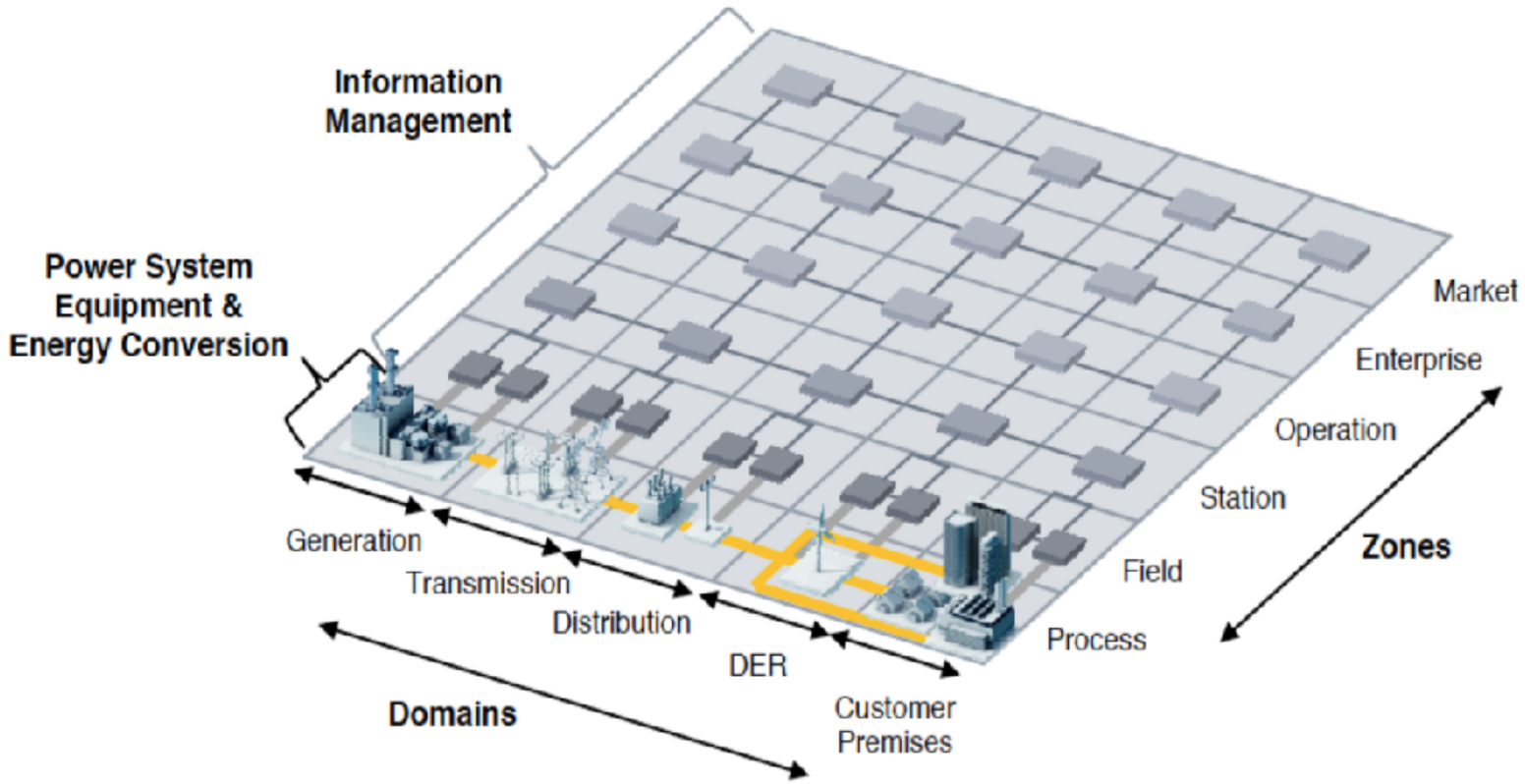
A Reference *Architecture* describes the *structure* of a system with its element types and their structures, as well as their *interaction* types, among each other and with their environment. Describing this, a Reference Architecture defines restrictions for an instantiation (concrete architecture). Through abstraction from individual details, a Reference Architecture is universally valid within a specific domain. Further architectures with the same functional requirements can be constructed based on the reference architecture. Along with *reference* architectures comes a *recommendation*, based on experiences from existing developments as well as from a wide acceptance and recognition by its users or per definition. [ISO/IEC42010]

In other terms, a Reference Architecture it is the specification of which language you should use to describe the system

# Intermezzo: Smart Grid Architecture Model (SGAM)

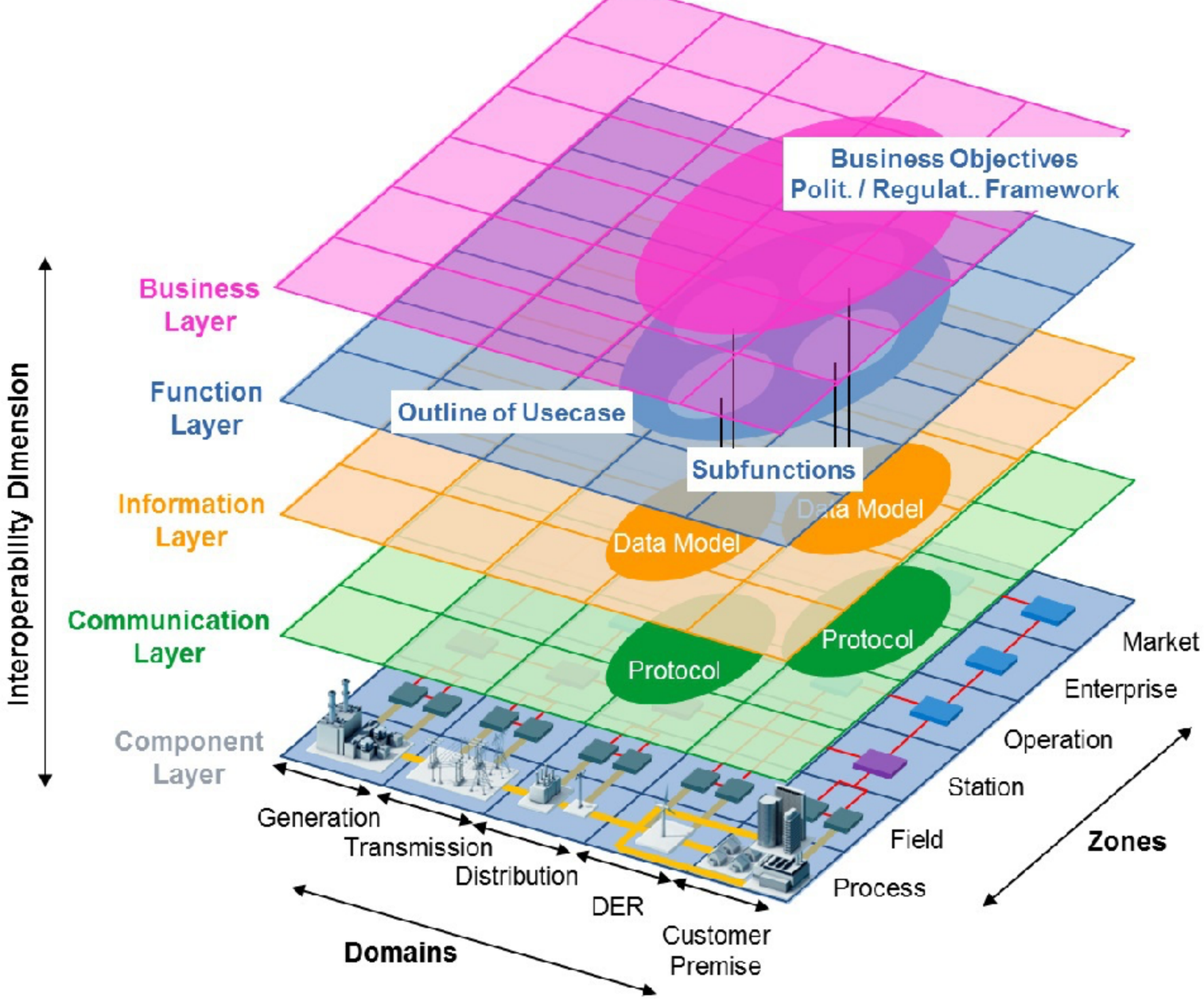
# SMART GRID PLANE

This smart grid plane allows to represent the levels at which interactions between power system management take place



# SGAM FRAMEWORK

SGAM consists of **five interoperability layers** that allow the **representation of entities and their relationships,** in the context of smart grid domains, and **information management hierarchies**



# Back to RAMI4.0

# RAMI 4.0

The Industrie 4.0 Reference Architecture (RAMI) is three dimensional and organises the **life-cycle/value streams** and the **manufacturing hierarchy levels** across the six layers of the IT representation of Industrie 4.0

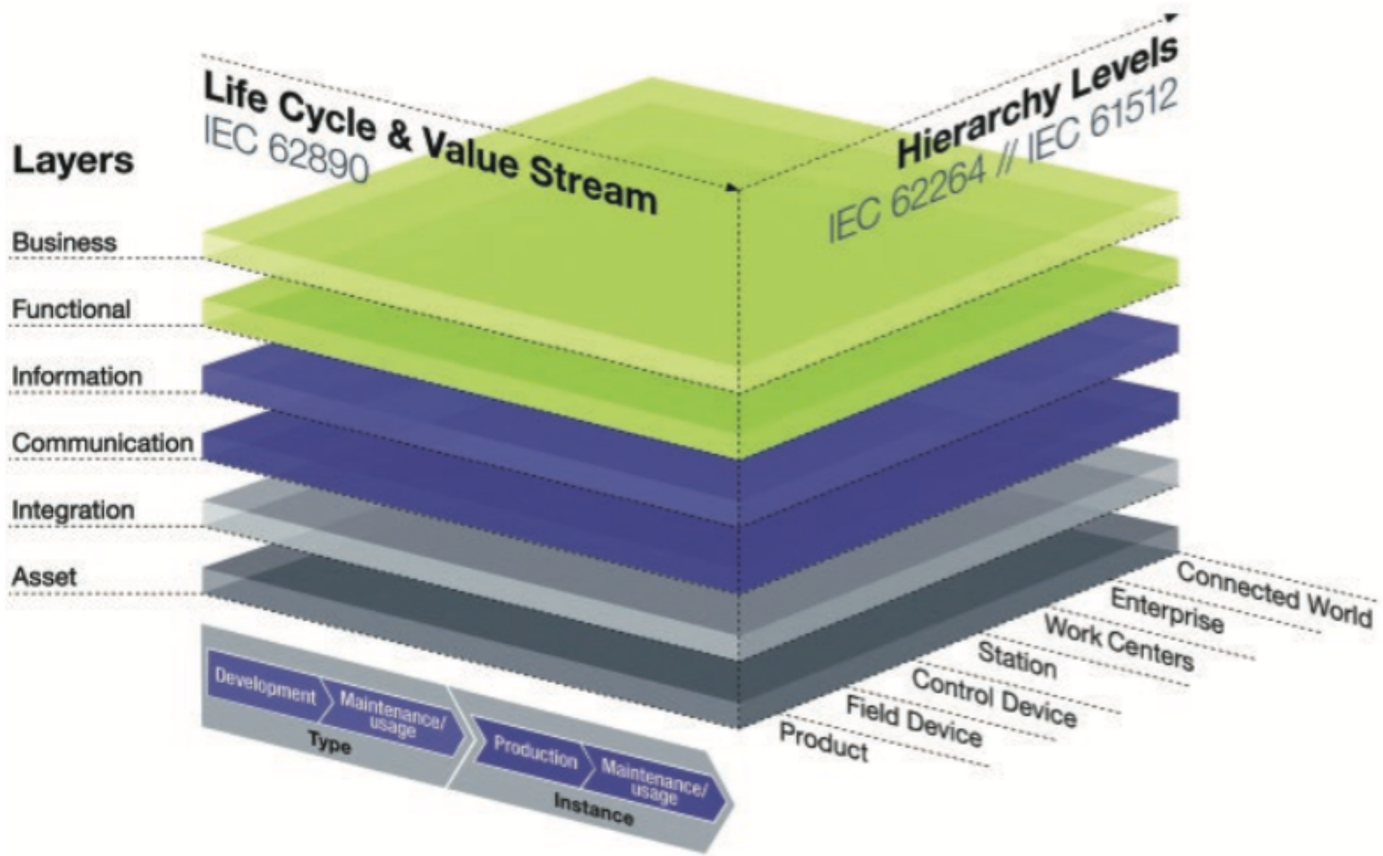
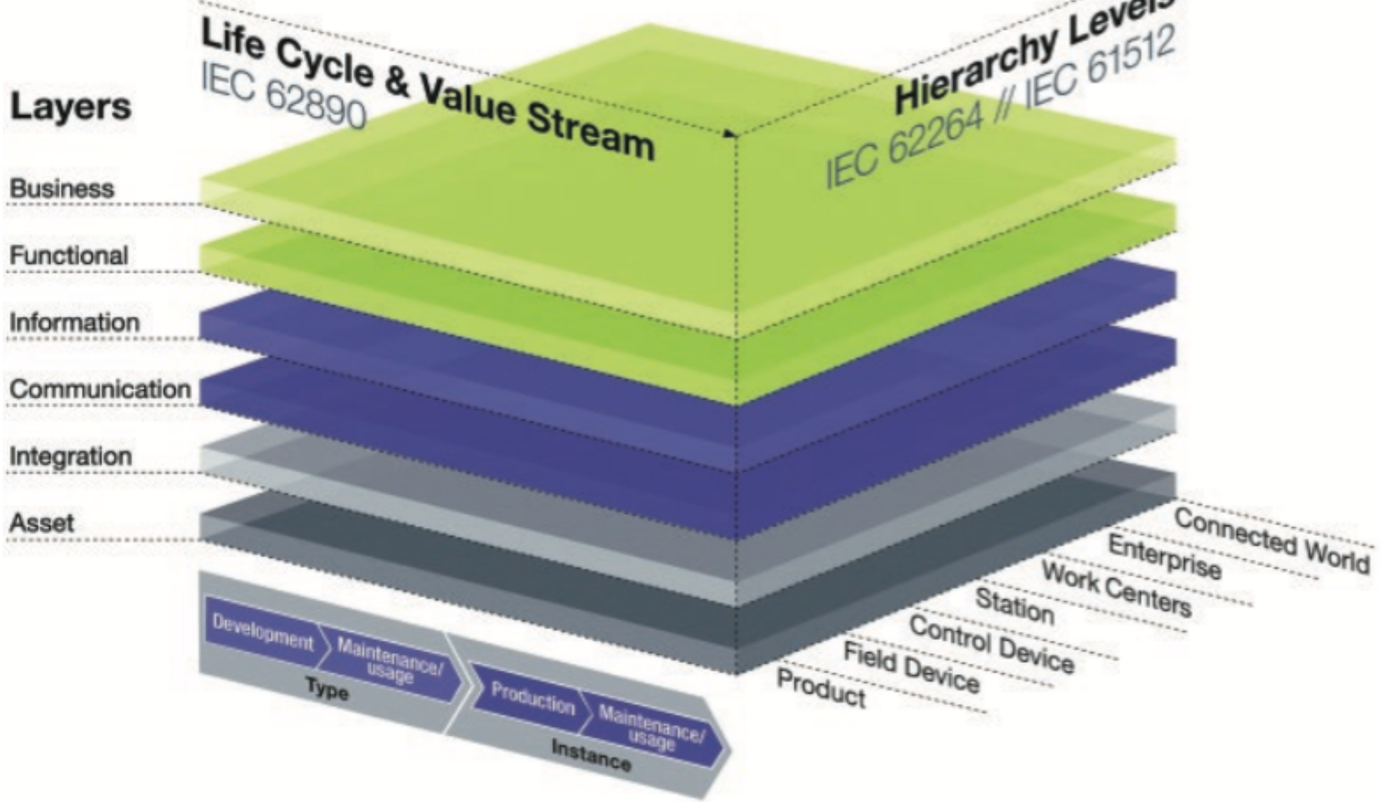
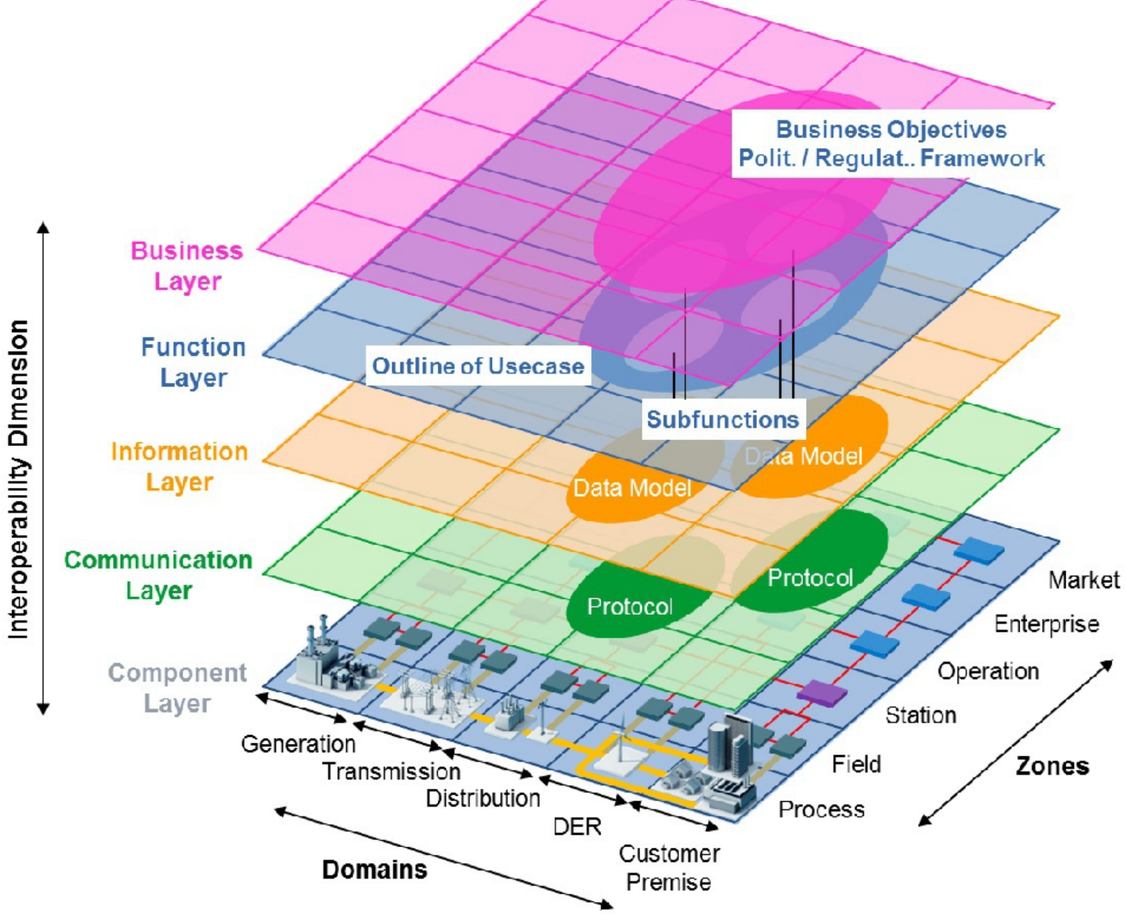



Image from: “Reference Architecture Model Industrie 4.0”

# RAMI VS. SGAM

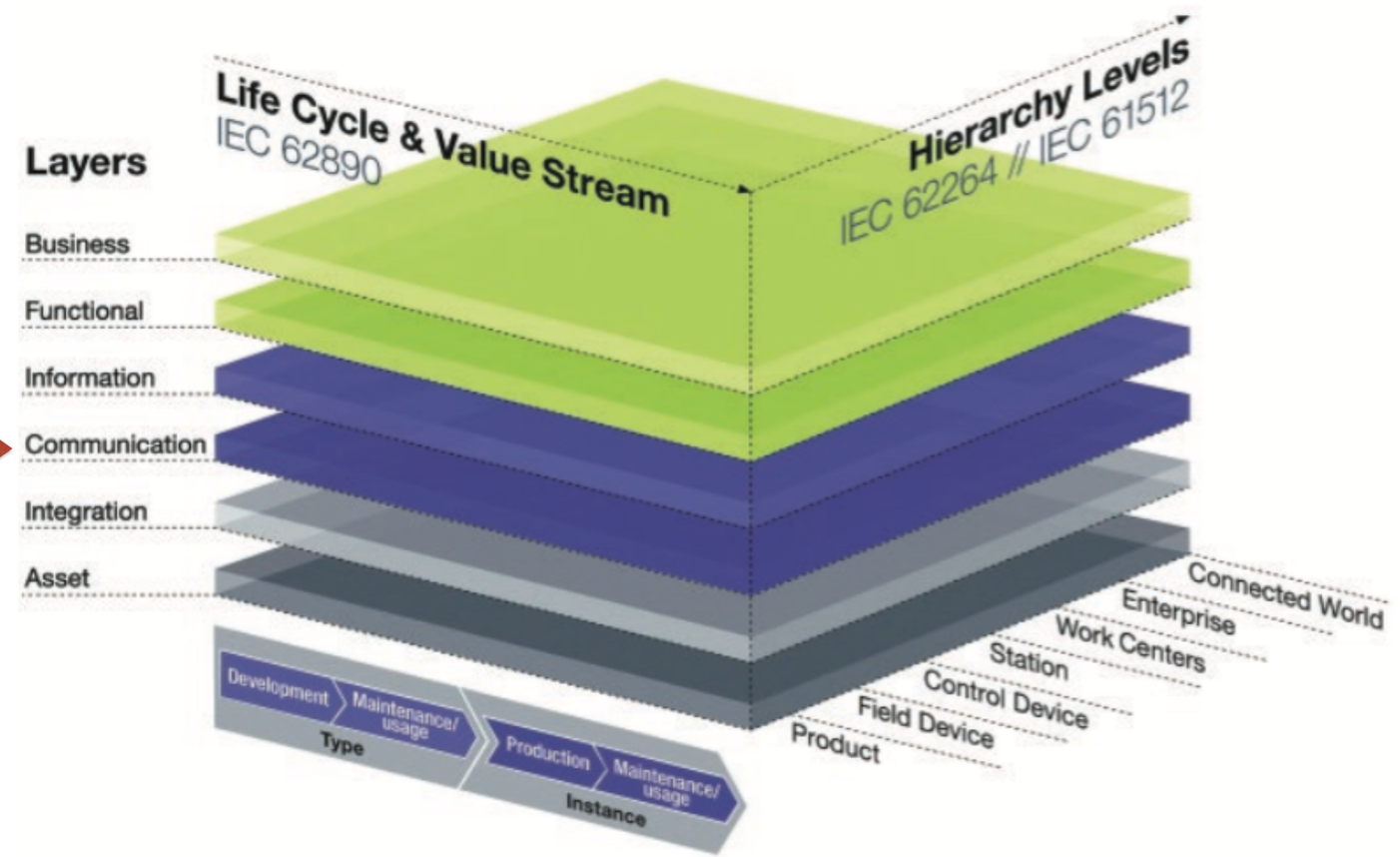

Layers
Life Cycle & Value Stream
IEC 62890
Hierarchy Levels
IEC 62264 // IEC 61512
Business
Functional
Information
Communication
Integration
Asset
Connected World
Enterprise
Work Centers
Station
Control Device
Field Device
Product
Development
Maintenance/ usage
Type
Production
Maintenance/ usage
Instance


Interoperability Dimension
Business Objectives
Polit. / Regulat.. Framework
Business Layer
Function Layer
Outline of Usecase
Subfunctions
Information Layer
Data Model
Data Model
Communication Layer
Protocol
Protocol
Component Layer
Market
Enterprise
Operation
Station
Field
Process
Zones
Generation
Transmission
Distribution
DER
Customer Premise
Domains

# COMMUNICATION LAYER

Standardisation of communication, using a uniform data format, in the direction of the Information Layer.

Provision of services for control of the Integration Layer.



# INFORMATION LAYER

Run time environment for processing of events.

Persistence of the data which represent the models.

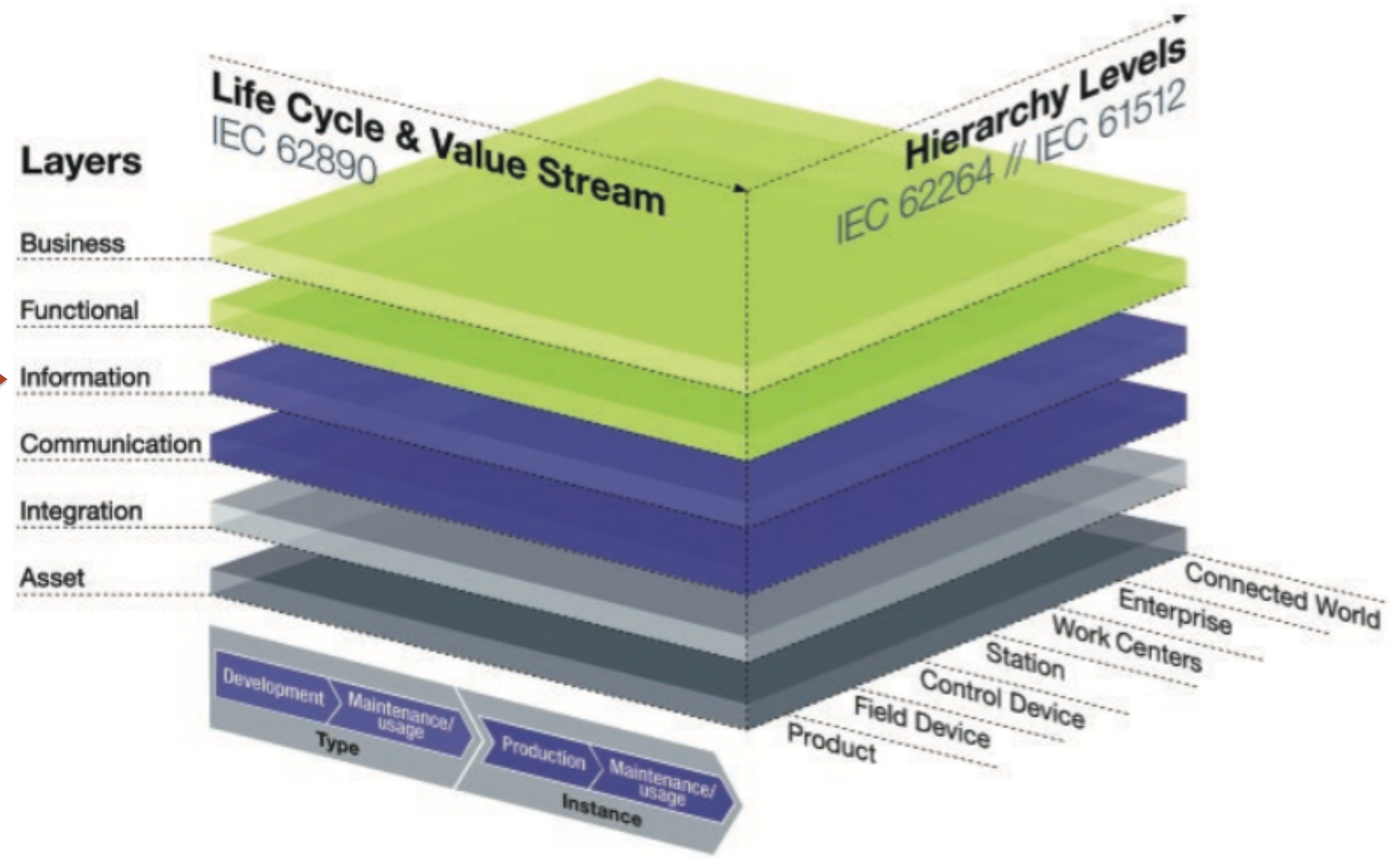
Ensuring data integrity.

Consistent integration of different data.

Obtaining new, higher quality data (data, information, knowledge).

Provision of structured data via service interfaces.

Receiving of events and their transformation to match the data which are available for the Functional Layer.

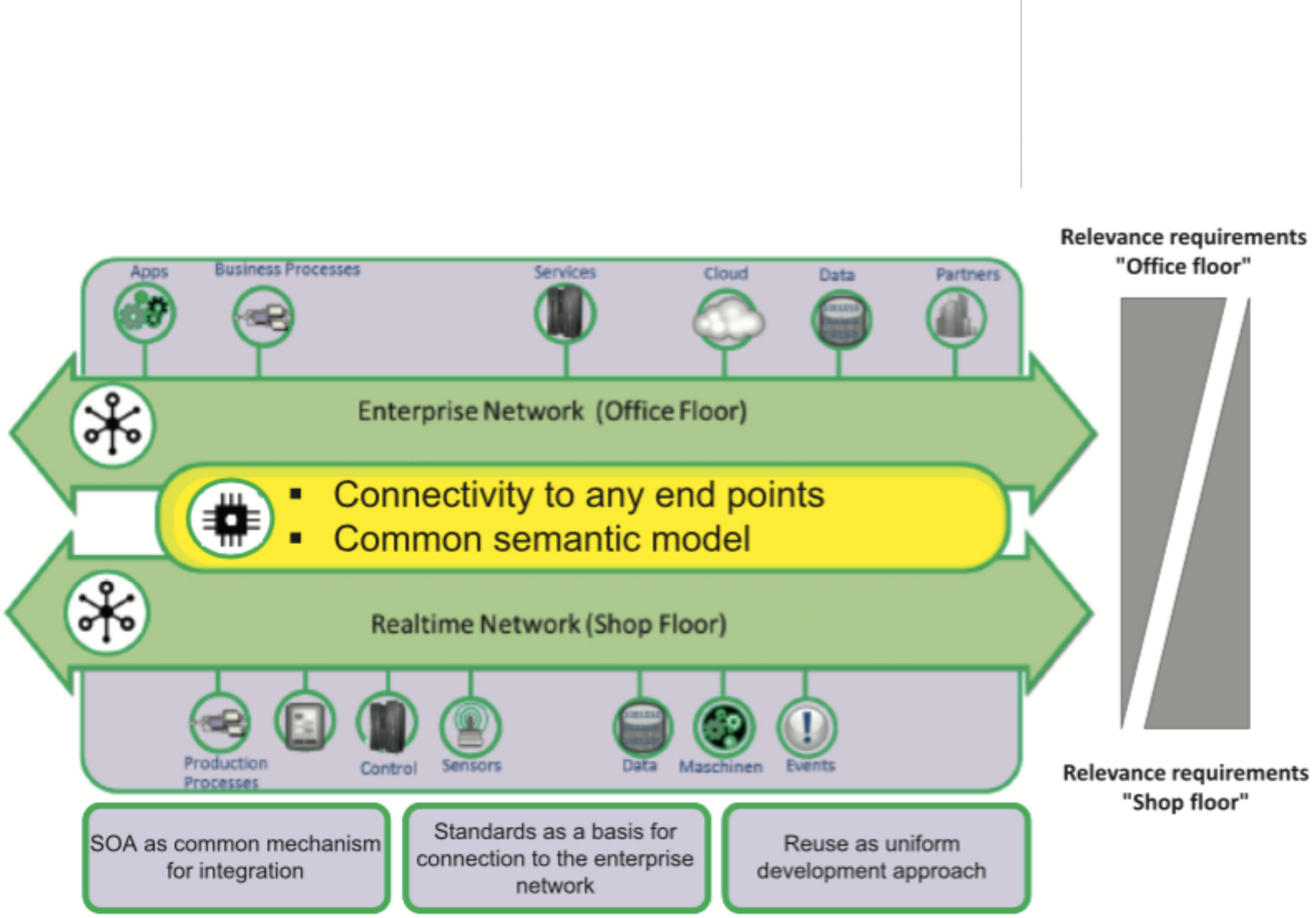


# I4.0 COMPONENTS

To allow for **seamless integration** of the “Office Floor” and the “Shop Floor” I4.0 requires connectivity to any end points and a common semantic model.

Components must have certain common properties independently of the levels.

They are specified in the form of the I4.0 components.



# I4.0 COMPONENTS REQUIREMENTS

A network of I4.0 components must be structured in such a way that connections between any end points (I4.0 components) are possible. The I4.0 components and their contents are to follow a common semantic model.

# I4.0 COMPONENTS REQUIREMENTS

It must be possible to define the concept of an I4.0 component in such a way that it can meet requirements with different focal areas, i. e. “office floor” or “shop floor”.

# I4.0 COMPONENTS REQUIREMENTS

The I4.0 compliant communication must be performed in such a way that the data of a virtual representation of an I4.0 component can be kept either in the object itself or in a (higher level) IT system.

# I4.0 COMPONENT

The ability to virtualise physical entities and make information available is key to RAMI4.0 and  captured as part of the I4.0 Component

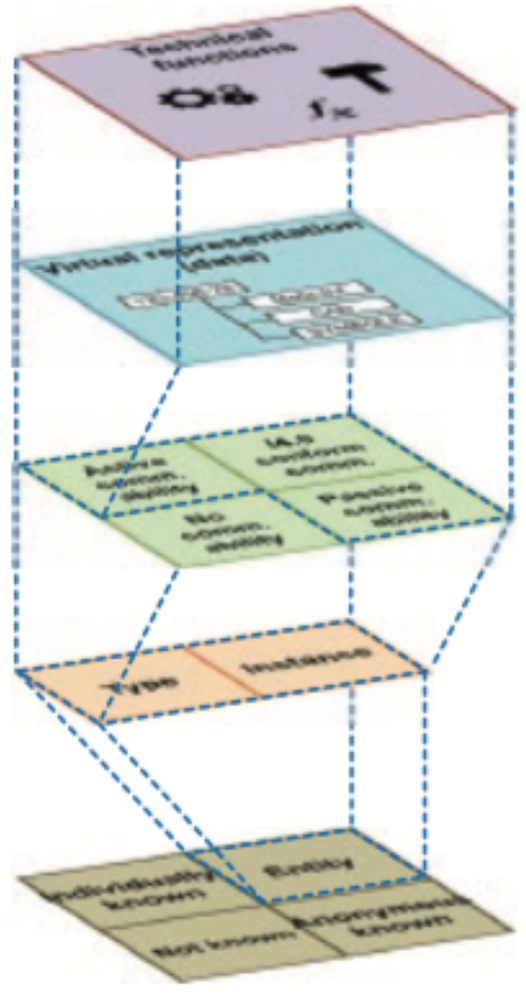


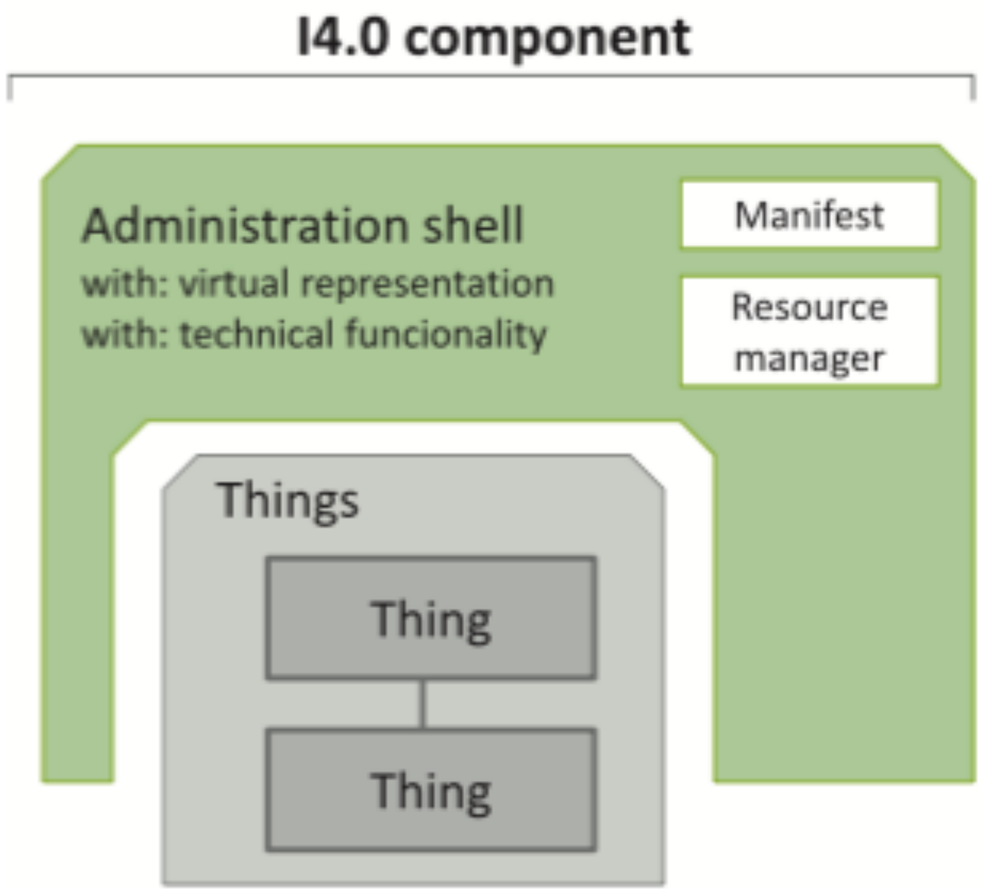

Image from: “Reference Architecture Model Industrie 4.0”

# ADMINISTRATION SHELL

From a logical point of view, an **I4.0 Component** is made by **one or more objects** and an **administration shell**

The **administration shell** contains the **data** for **virtual representation and the functions of the technical functionality**.

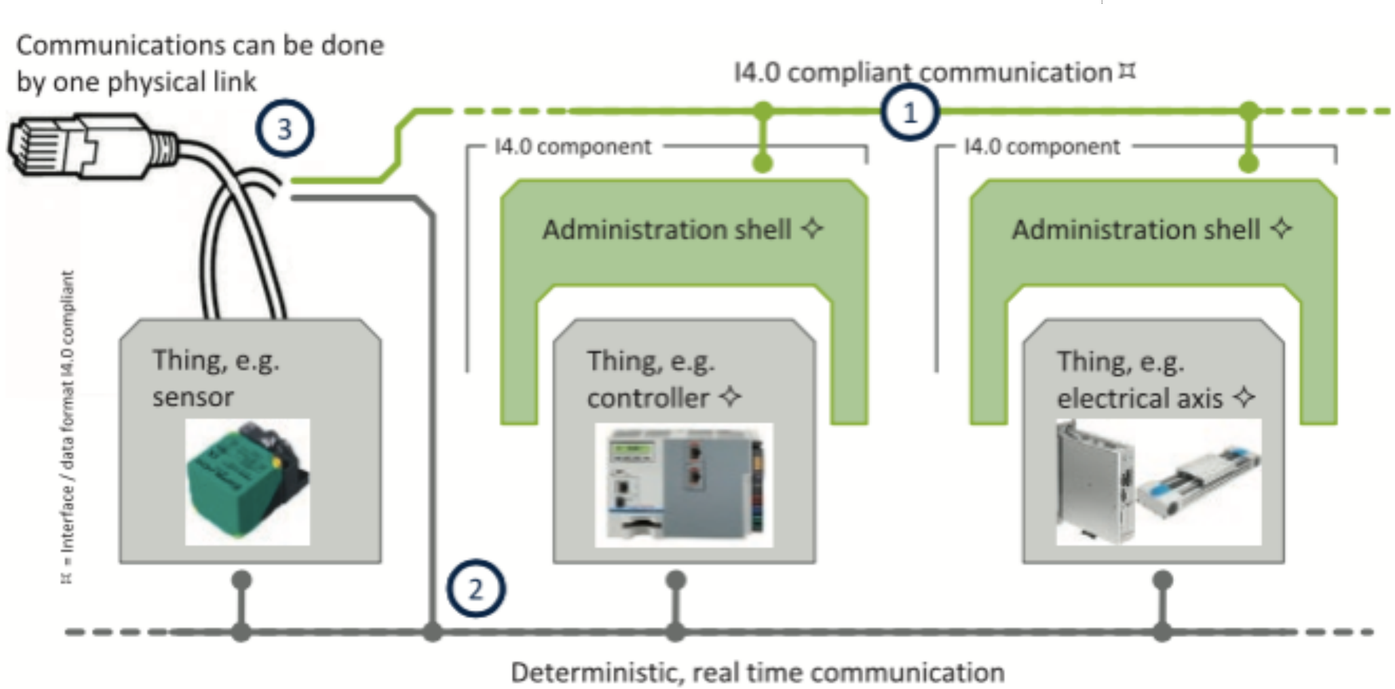
The mani fest, as part of the virtual representation, details the necessary administrative details on the I4.0 component.



# SEPARABILITY OF FLOWS

I4.0 compliant communication does not have to implement deterministic or realtime communication itself, it can delegate to existing technologies.

The Realtime Ethernet protocols which are standard today permit the expectation that it will be possible to effect both forms of communication via the same communications infrastructure.



# IIRA

# THE INTERNET OF THINGS AND SERVICES

IIRA

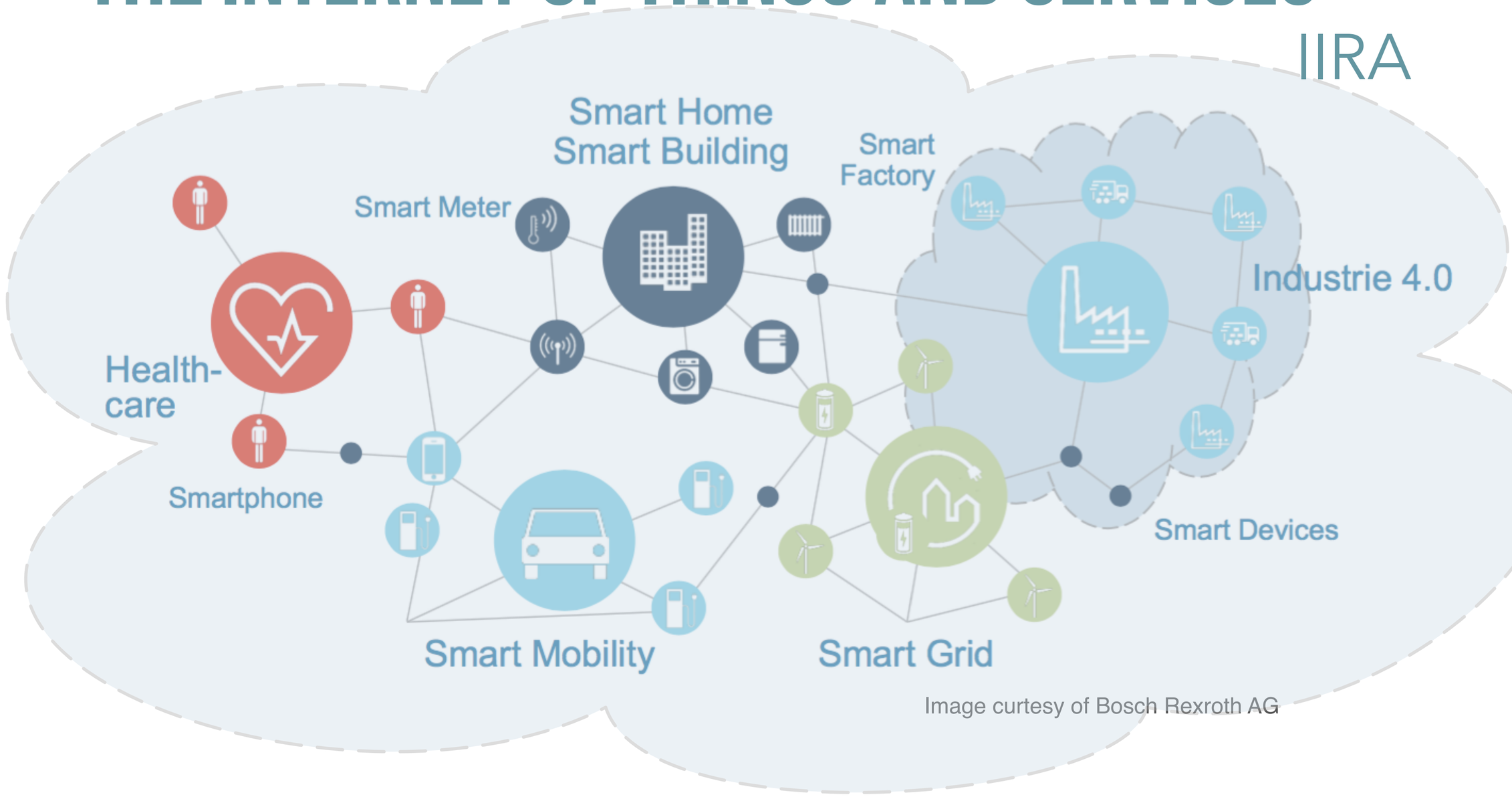
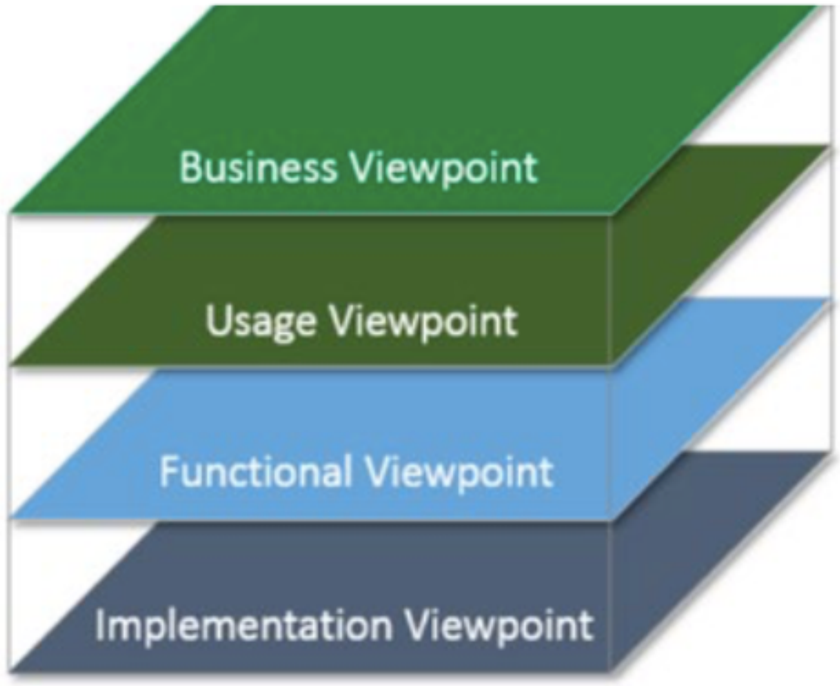



Image curtesy of Bosch Rexroth AG

# IIRA

The industrial internet architectural framework adopts general concepts from the ISO/IEC/IEEE 42010:2011 standard which includes concerns, framework and viewpoints.

IISs are characterised by four viewpoints: Business, Usage, Functional, and Implementation



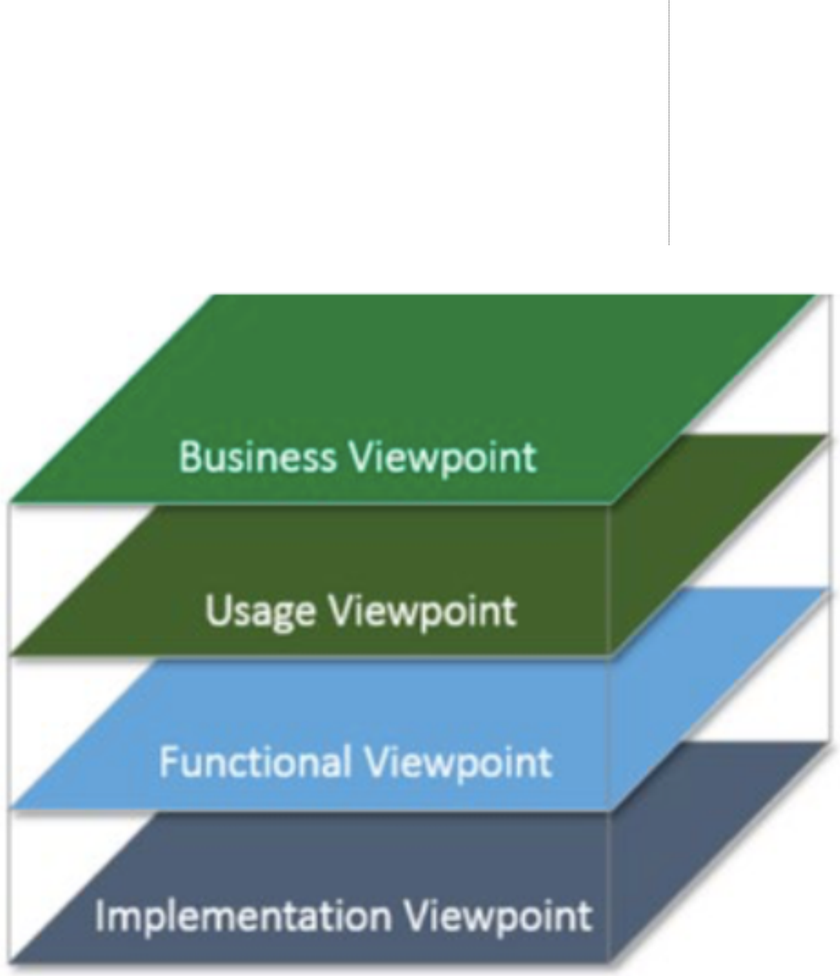
# IIRA

The **Business Viewpoint** Identifies the business stakeholders

The **Usage Viewpoint** looks at the expected system usage

The **Functional Viewpoint** concerns the functional components of an IIS, their interrelationships and external interactions,

The **Implementation Viewpoint** concerns the technologies required to implement functional components.



# IIRA FUNCTIONAL DOMAINS

The IIRA decomposes an Industrial Internet System (IIS) in five **functional domains**: **Control**, **Operation**, **Information**, **Application** and **Business**

**Data** flows and **control flows** take place in and **between** these **functional domains**.

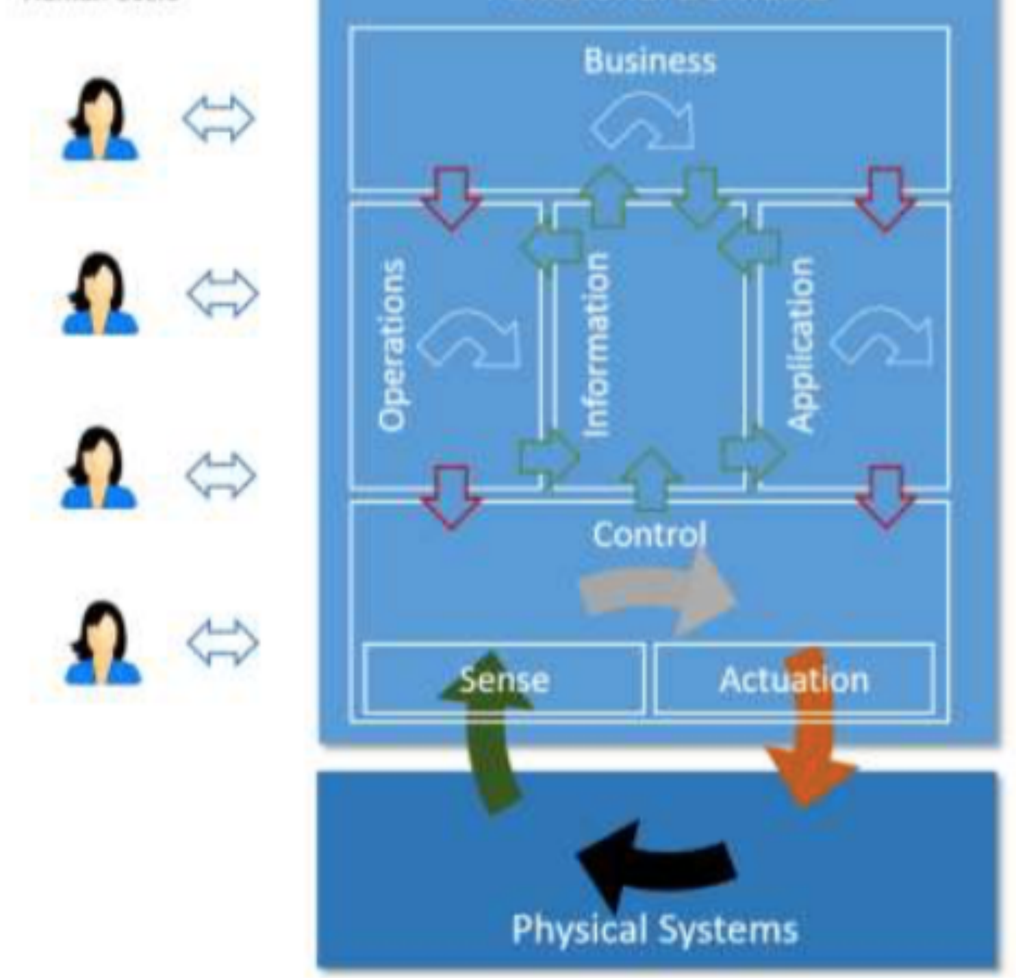
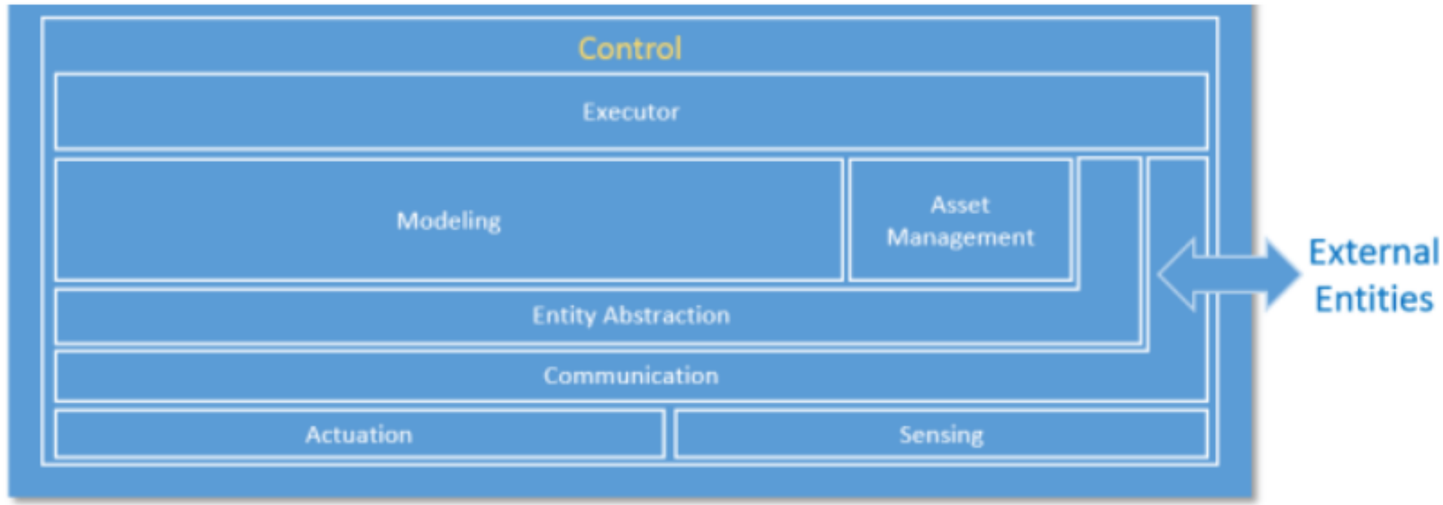



Image from: “Industrial Internet Consortium Reference Implementation v1.7”

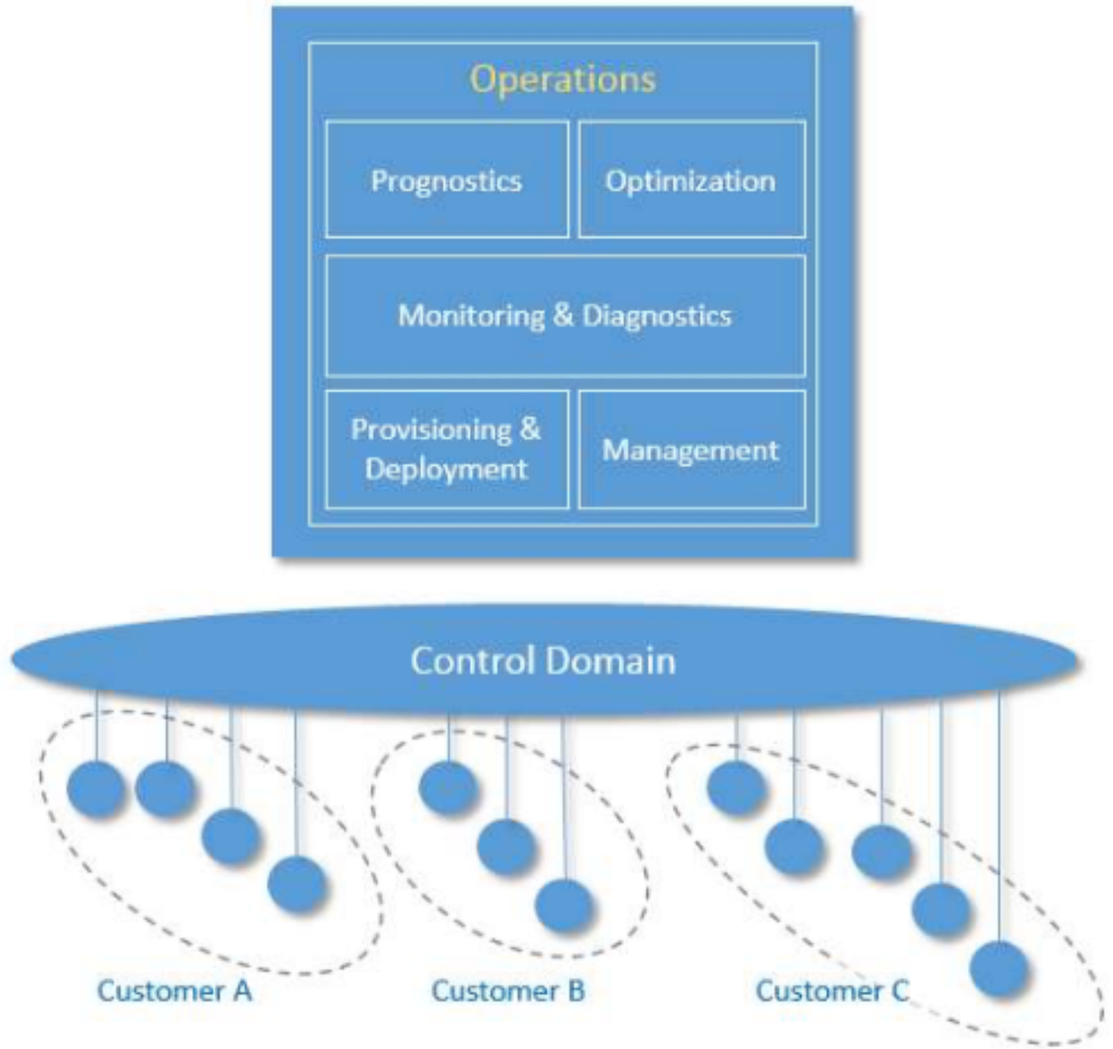
# CONTROL DOMAIN

The control domain represents the collection of functions that are performed by industrial control systems. The core of these functions comprises fine-grained closed-loops, reading data from sensors, applying rules and logic, and exercising control over the physical system through actuators



# OPERATION DOMAIN

The operations domain represents the collection of functions responsible for the provisioning, management, monitoring and optimisation of the systems in the control domain. Existing industrial control systems mostly focus on optimising the assets in a single physical plant. The control systems of the Industrial Internet must move up a level, and optimise operations across asset types, fleets and customers.

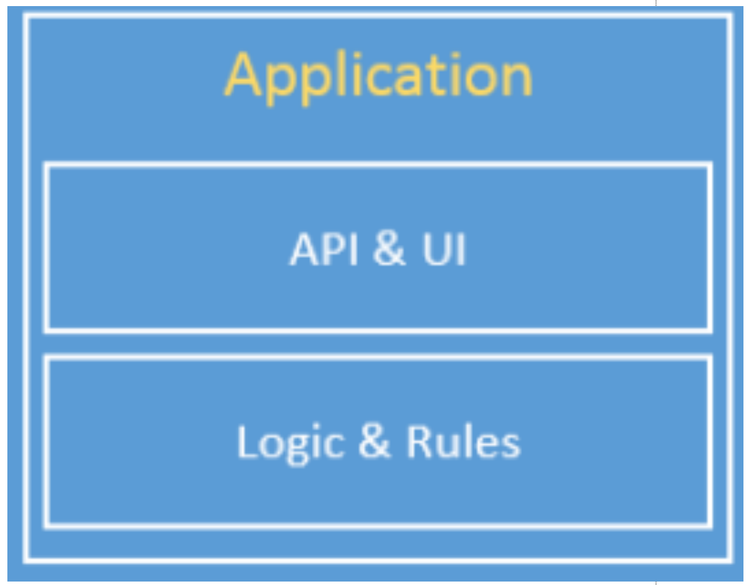


# INFORMATION DOMAIN

The Information Domain represents the collection of functions for gathering data from various domains, most significantly from the control domain, and transforming, persisting, and modelling or analysing those data to acquire high-level intelligence about the overall system.

# APPLICATION DOMAIN

The application domain represents the collection of functions implementing application logic that realises specific business functionalities. Functions in this domain apply application logic, rules and models at a coarse-grained, high level for optimisation in a global scope.



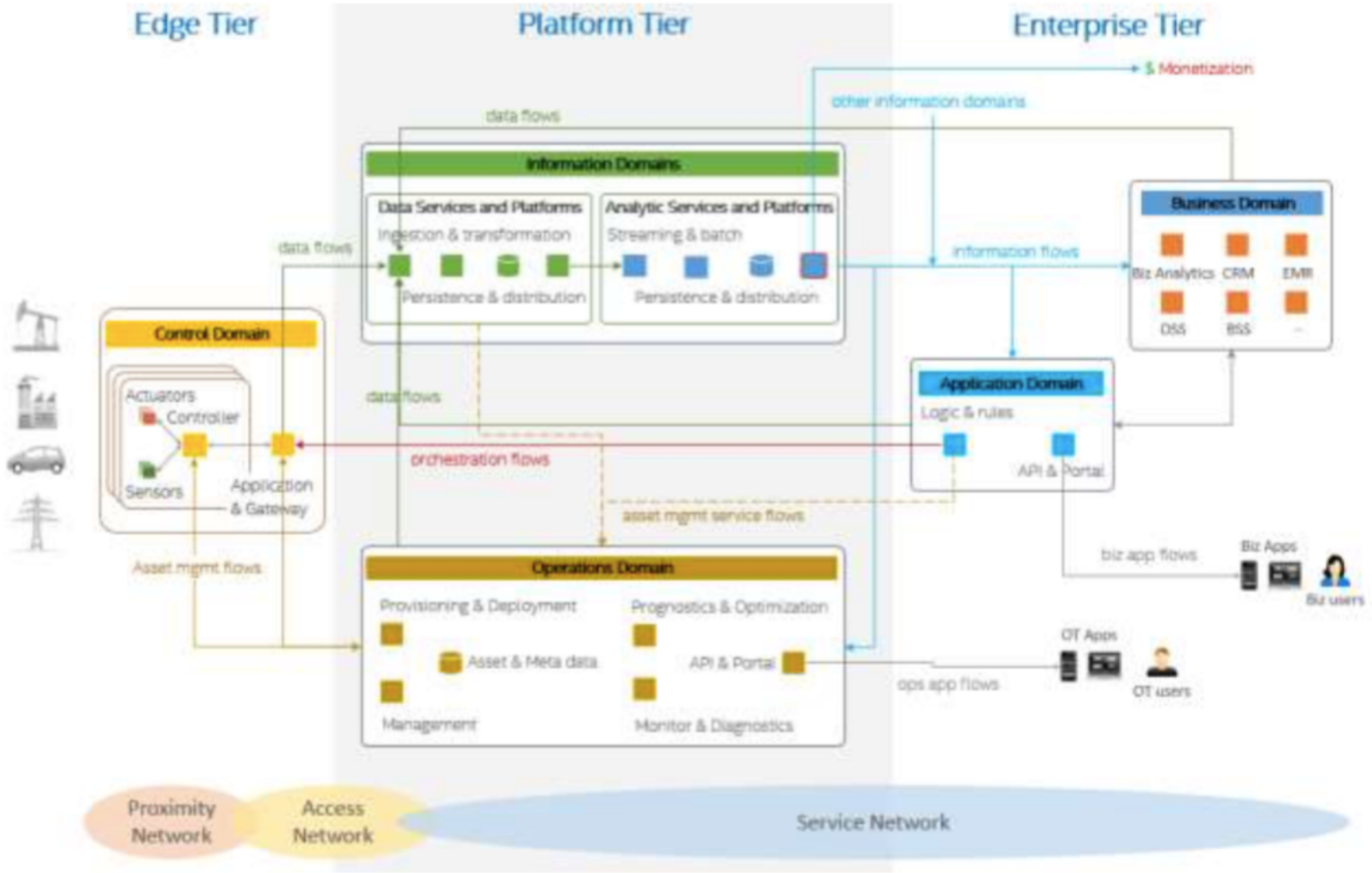
# BUSINESS DOMAIN

The application domain represents the collection of functions implementing application logic that realizes specific business functionalities. Functions in this domain apply application logic, rules and models at a coarse-grained, high level for optimization in a global scope.

# IMPLEMENTATION VIEWPOINT

The implementation viewpoint is concerned with the technical representation of an Industrial Internet System and the technologies and system components required to implement the activities and functions prescribed by the usage and functional viewpoints.

# FUNCTIONAL DOMAINS MAPPING



# IIRA CONNECTIVITY

IIRA connectivity foresees the use of a Connectivity Core Standard (such as DDS) and then Gateways to integrate other connectivity technologies

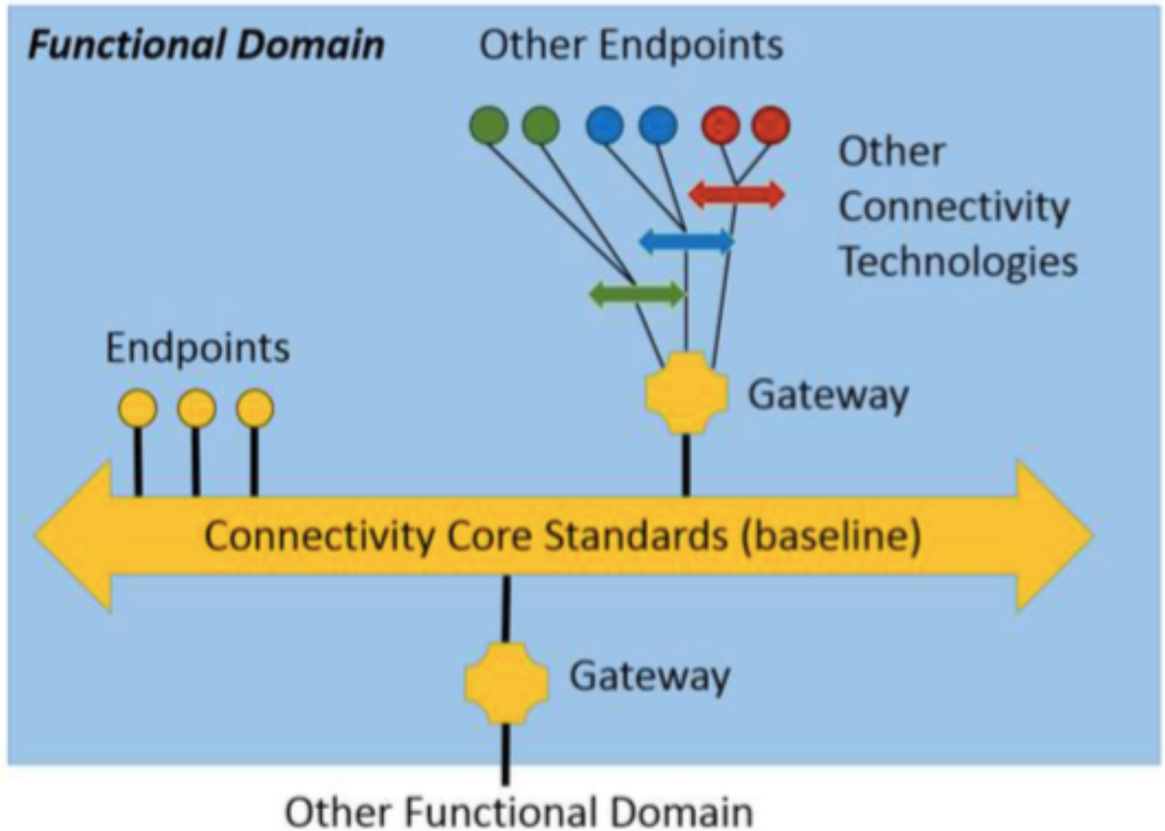



Image from: “Industrial Internet Reference Architecture v1.7”

# RAMI & IIRA

# IIRA/I4.0 RELATIONSHIP

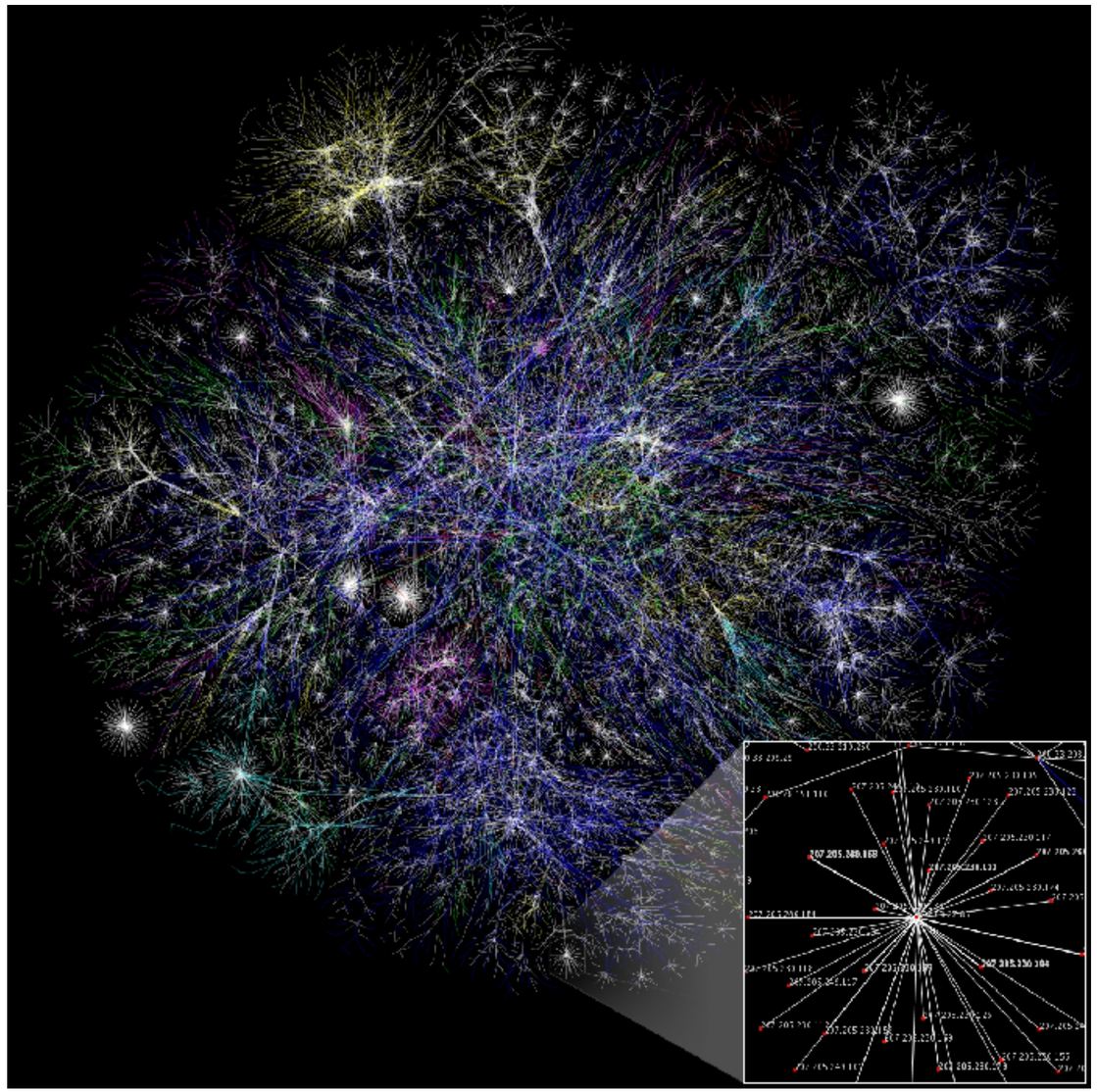
# Architectural Challenges

# SCALE

IoT systems tend to fall in the category of Ultra-Large Scale Systems.

These systems whose connectivity tend to follow a power-law, tend to be characterised by emergent behaviours

Proper care should be taken in the design of algorithm for these systems to ensure self-stabilisation properties



# HETHEROGENEITY

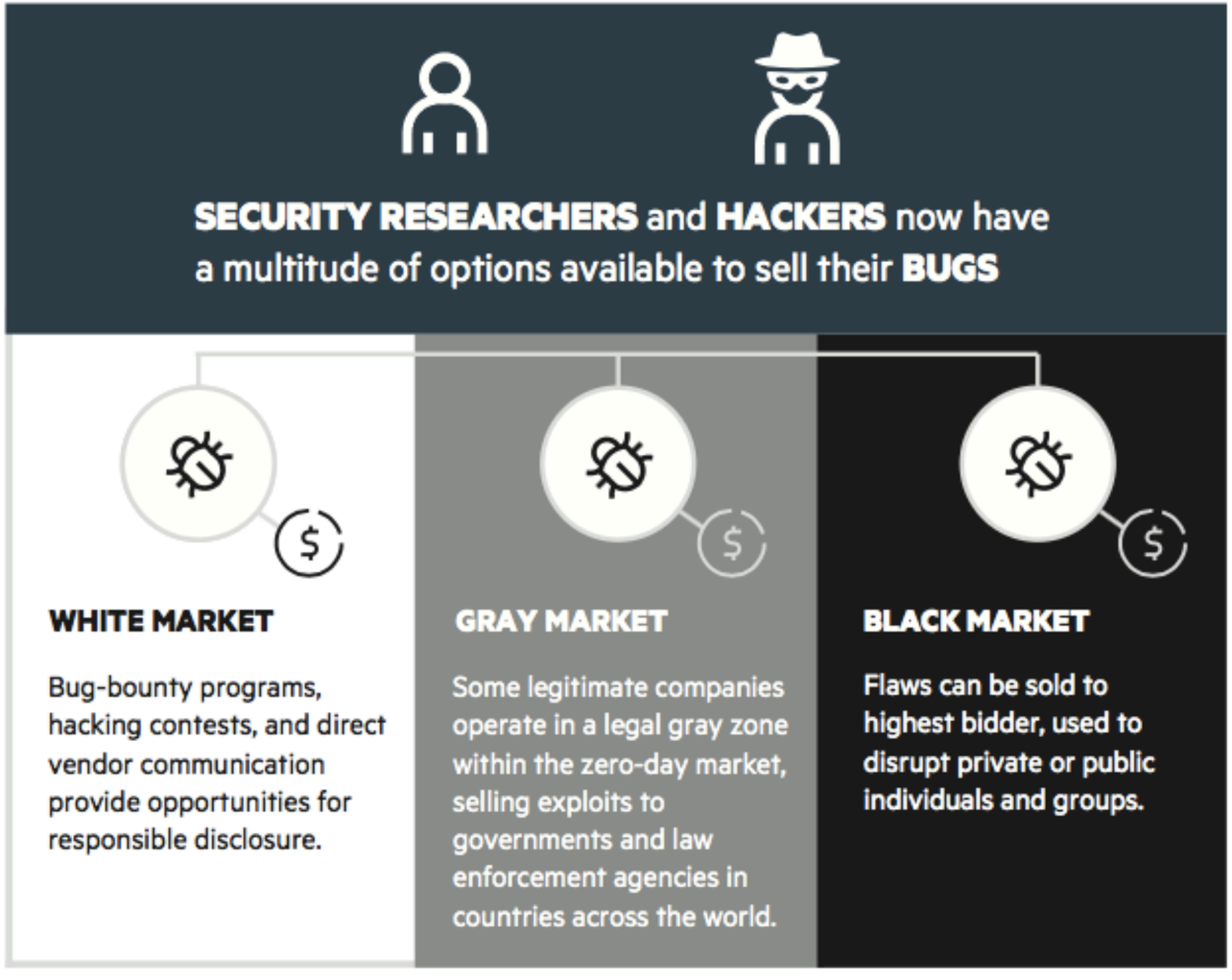
IoT systems are characterised by an extreme heterogeneity in computational power of their nodes as well as characteristics of the interconnect.

This poses major challenges in ensuring that system remain stable and don't diverge or oscillate due to asymmetry

# The Security Market

# SECURITY MARKET

Security Bugs are source of revenues through white, grey and black market




**Source**: HPE Cyber Risk Report 2016

# SECURITY STATUS

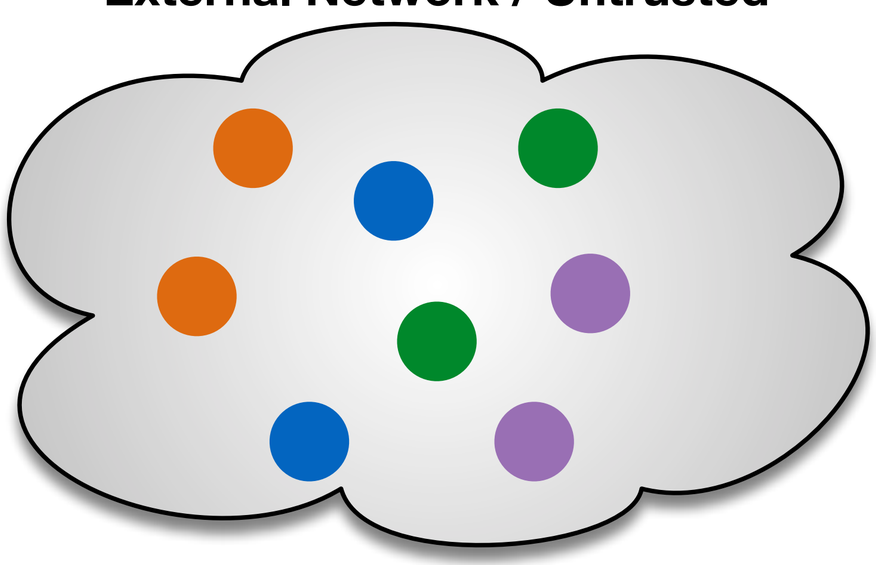
With sufficient time and funding, there are few things that today cannot be hacked.

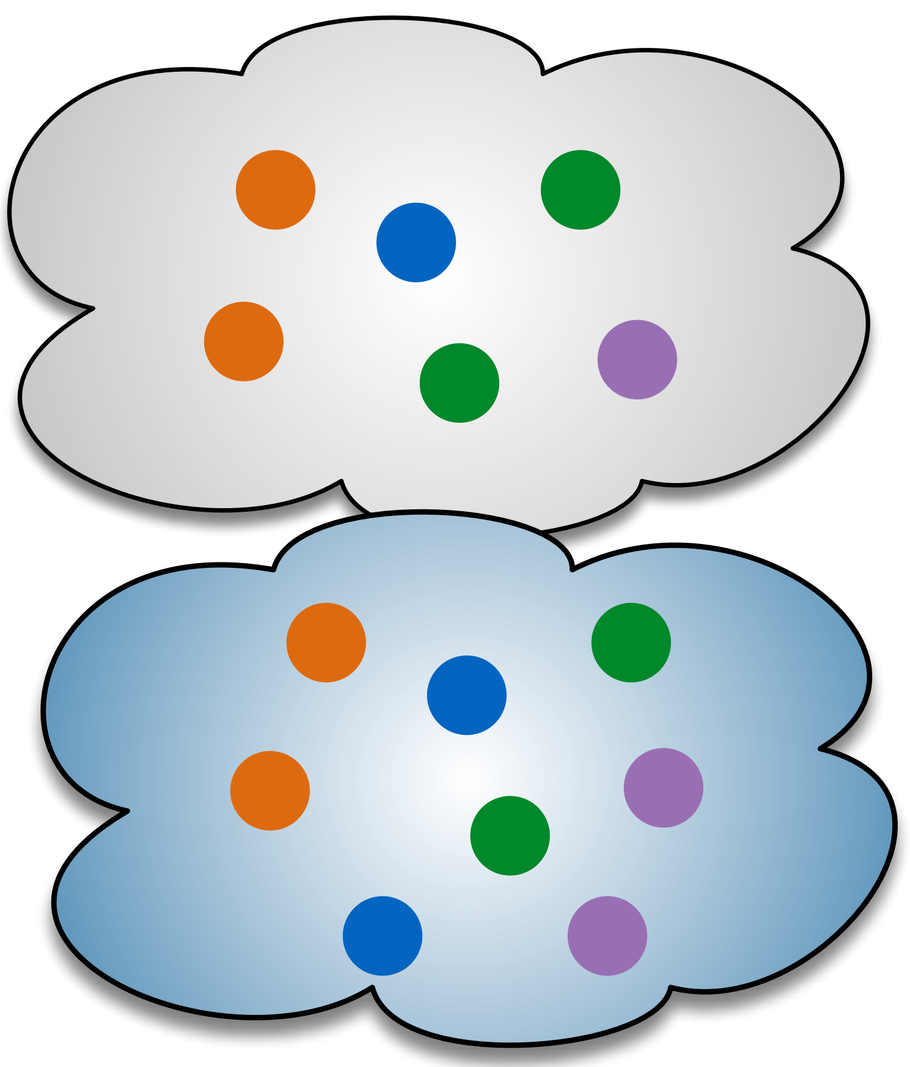
Latest example of remote hacking of high value “connected things”are **BMW Connected Drive**, **Tesla Model S** and **JEEP**

**Based on** security research from HP Fortify **80%** of lower value connected devices, such as home appliances, are  insufficiently secure or completely unsecured


# Security in IIoT

# DEVICE & SYSTEM SECURITY



# SECURITY IN IIOT

In many instances, Security in IIoT is a bit different than consumer IoT

Often it is easier to draw a boundary between what is trusted and was is not that can help making the security solution more manageable.

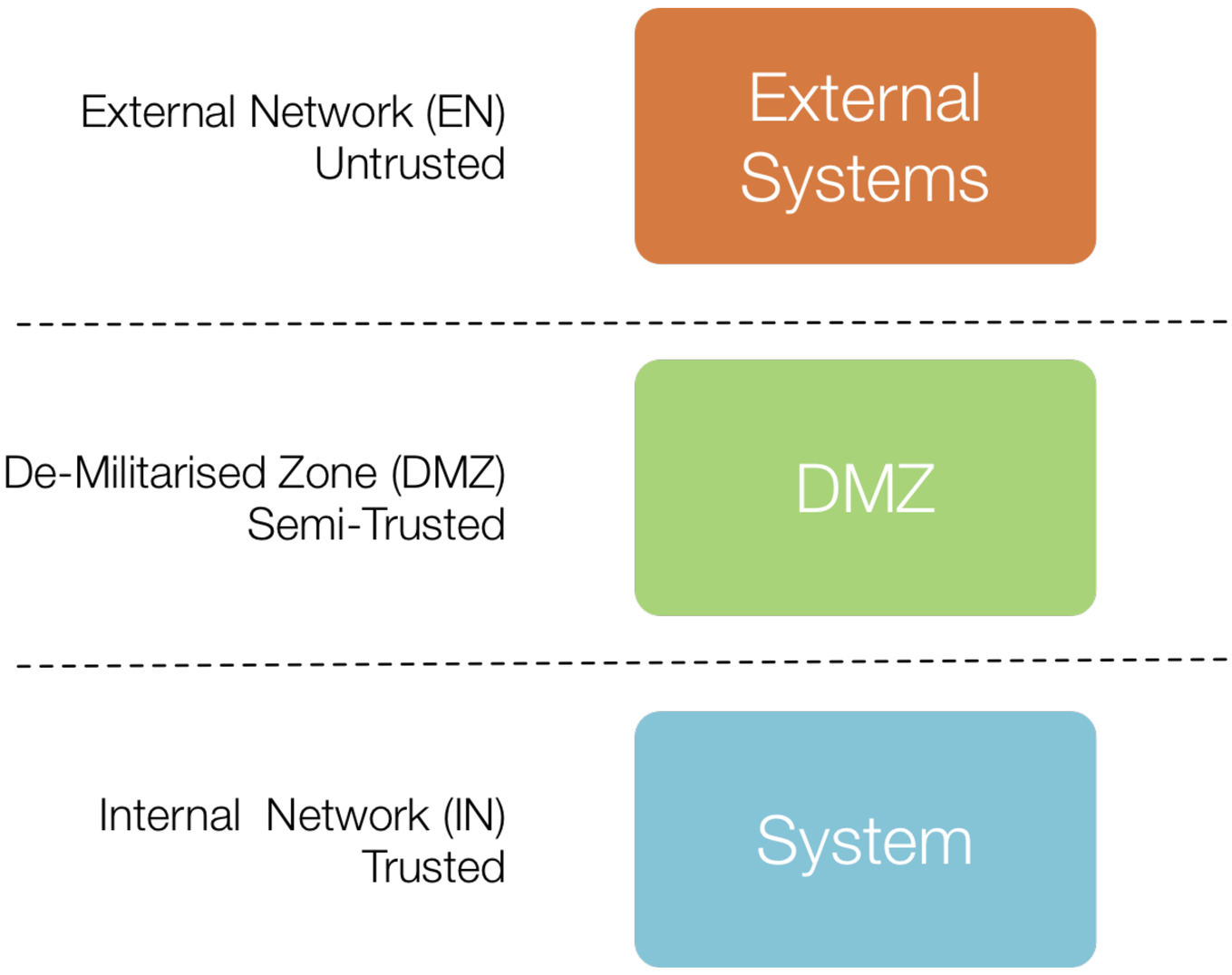
# System Security Architectures

# BOUNDARY SECURITY

Boundary security is concerned with securing the interconnection of a system with an untrusted network.

The system network, is considered  trusted. In any case security within the system is addressed using traditional LAN-level  security techniques

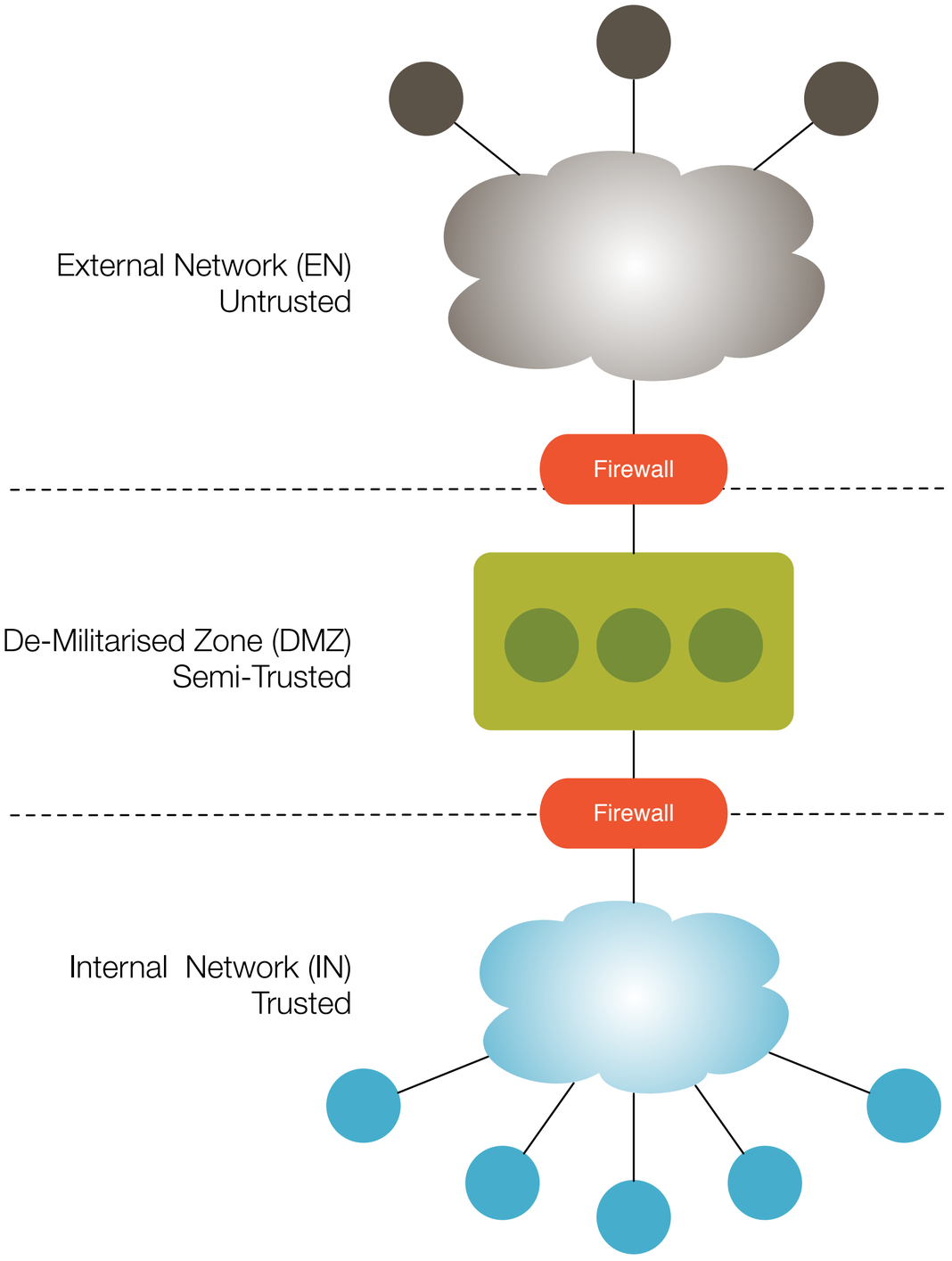
DMZ is a common way of implementing boundary security



# DMZ SECURITY

DMZ assumes that anything within the **Internal Network** (IN) is trusted — the IN defines  the boundary of trust.

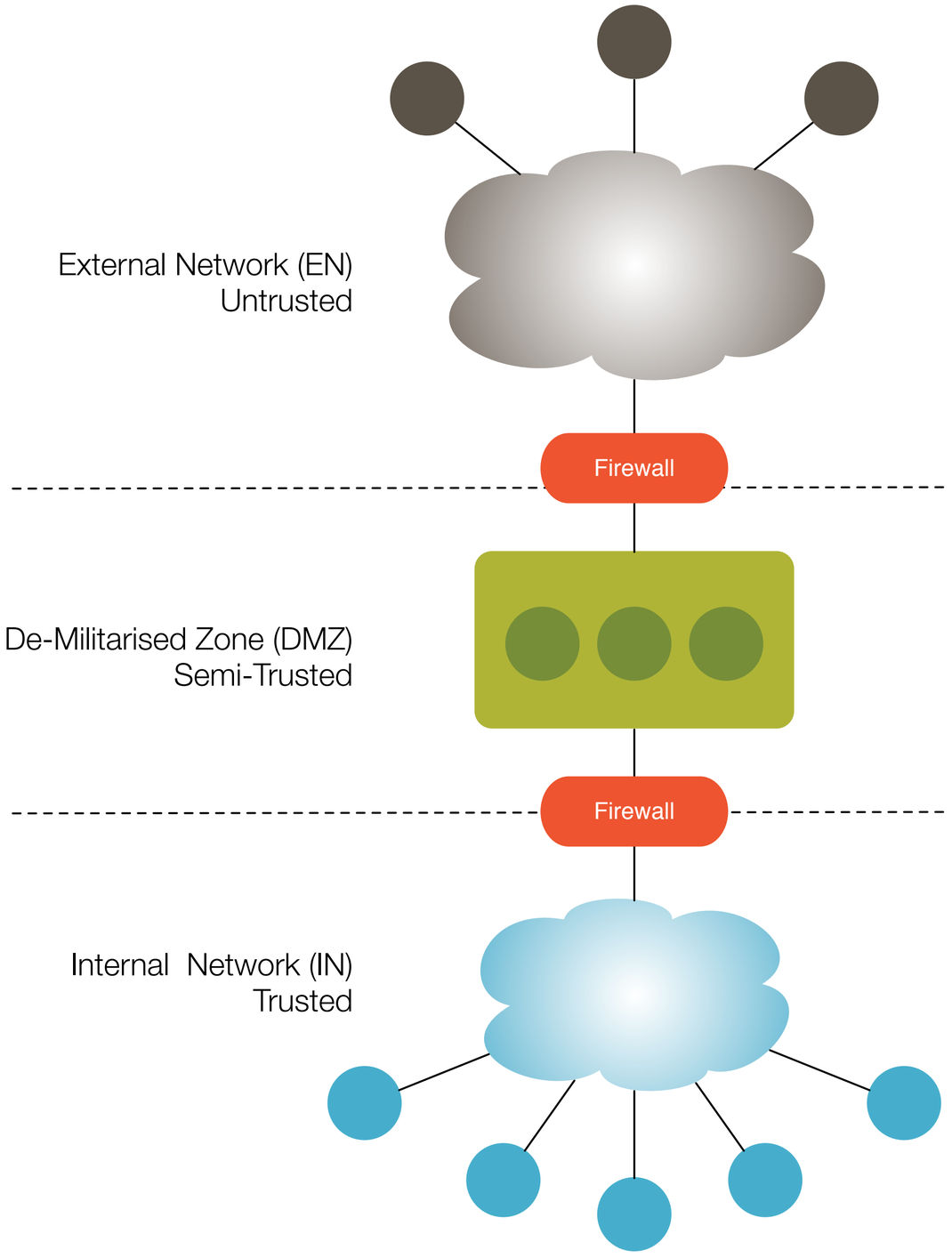
The DMZ is considered as a semi-trusted and the communication with the trusted zone is often restricted by allowing only (1) TCP/IP from IN to DMZ, (2)  Connections from the IN to DMZ but not vice-versa



# DMZ SECURITY

The nature of the **External Network** (EN) may be different across deployments and business domains.

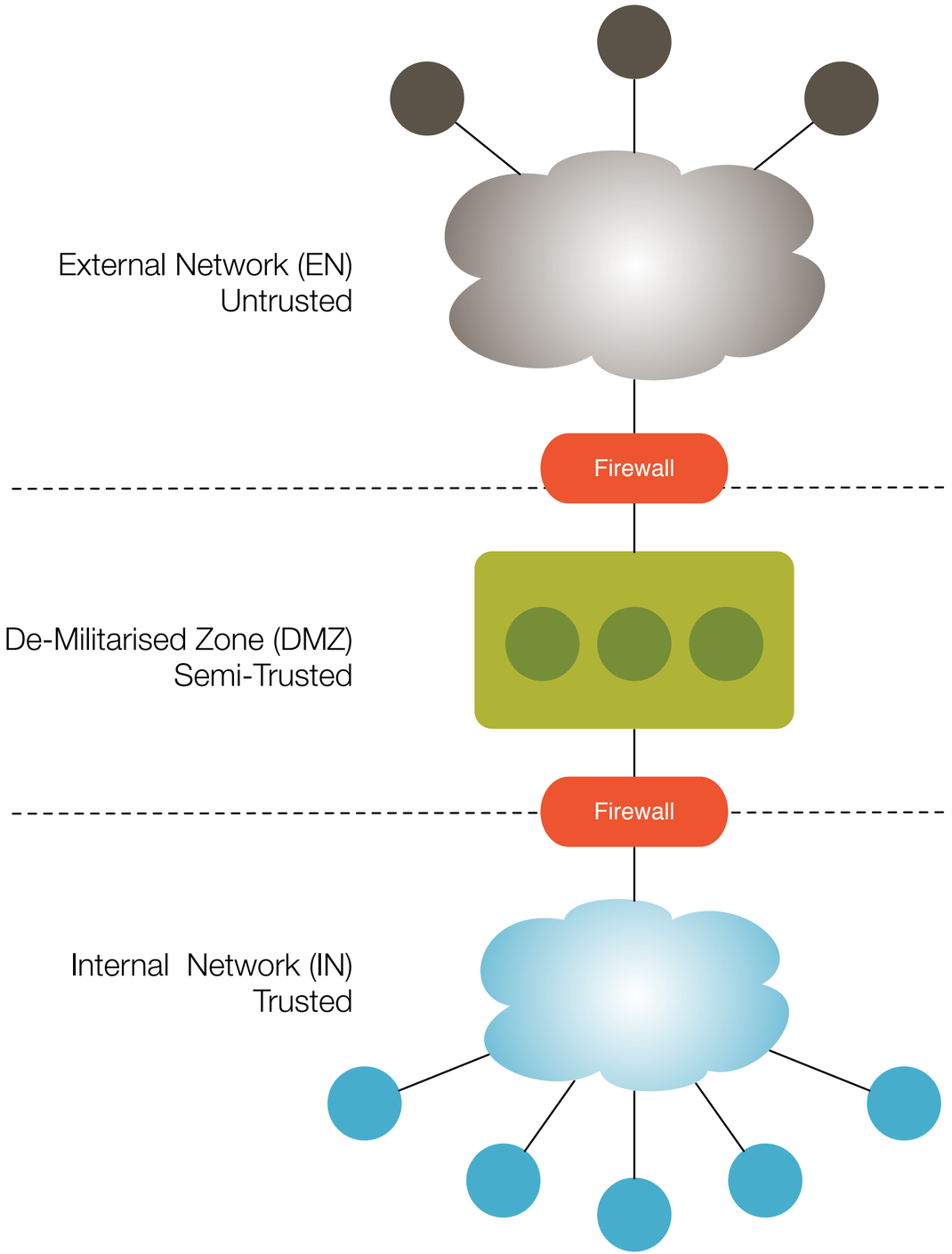
In some deployments the **EN** is not the Internet but a WAN with some level of trust.



# DMZ SECURITY

Please be aware that there are different ways of implementing boundary security with a  DMZ

To make the scope manageable we consider the relatively standard double-firewall architecture, but several variations on the theme exist.



# PRIVACY

Privacy will be major issue in IoT.

Today people are willing to easily give away their data… But eventually will realise that this is a key value.

Technologies like Homomorphic Encryption can help addressing this problem.

# SUMMARY

The IoT can be classified in CIoT and IIoT

IIoT is characterised by more stringent needs

Reference architectures have focused to a great extent on IIoT

RAMI4.0 and IIRA are two example of IIoT Reference Architectures

Data is the key asset that creates value in IoT