Internet of Things

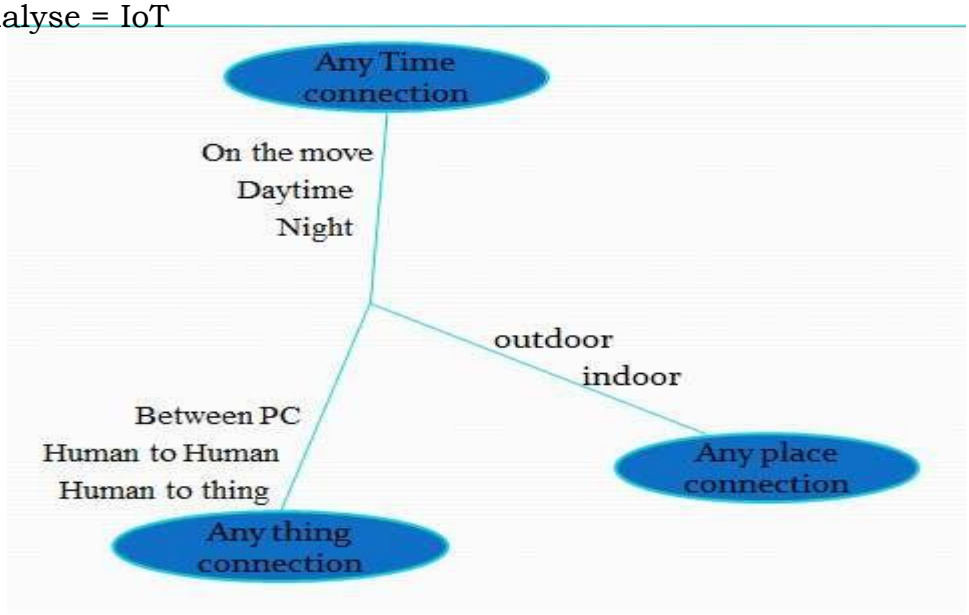
Unit 2: IoT Architecture and Communication Technologies (7)

Syllabus:

IoT Architecture by Oracle, Sources of IoT, M2M Communication, IoT/M2M systems, layers and design standards, Communication Technologies

2.1 IoT Architecture by Oracle:

- The **Internet of Things** is the network of physical objects—devices, vehicles, buildings and other items embedded with electronics, software, sensors, and network connectivity—that enables these objects to collect and exchange data.
- IoT is connecting every physical object in the world using wireless.
- **Internet of Things** are able to collect and exchange data using embedded sensors.
- Physical Object + Controller, Sensor and Actuators + Internet = IoT
- Gather + Enrich + Stream + Manage + Acquire + Organise and Analyse = IoT with connectivity to Data Centre, Enterprise or Cloud Server
- Gather + Consolidate + Connect + Collect + Assemble + Manage and Analyse = IoT



IoT: Characteristics, Features, Advantages, Disadvantages

Characteristics	Features	Advantages	Disadvantages
Intelligence	Device Virtualisation	Integration of Devices	Security
Connectivity	High Speed	Reliable, Secure Bi-Directional Communication	Privacy
Sensing	End Point Management	Enhanced Data Collection	Complexity
Expressing	Small Devices	Reduce Waste	Flexibility
Energy	Stream Processing	Real Time Analysis Improved Engagement	Compliance
Safety	Data Enrichment	Automation and Technology Optimization	Tier Management

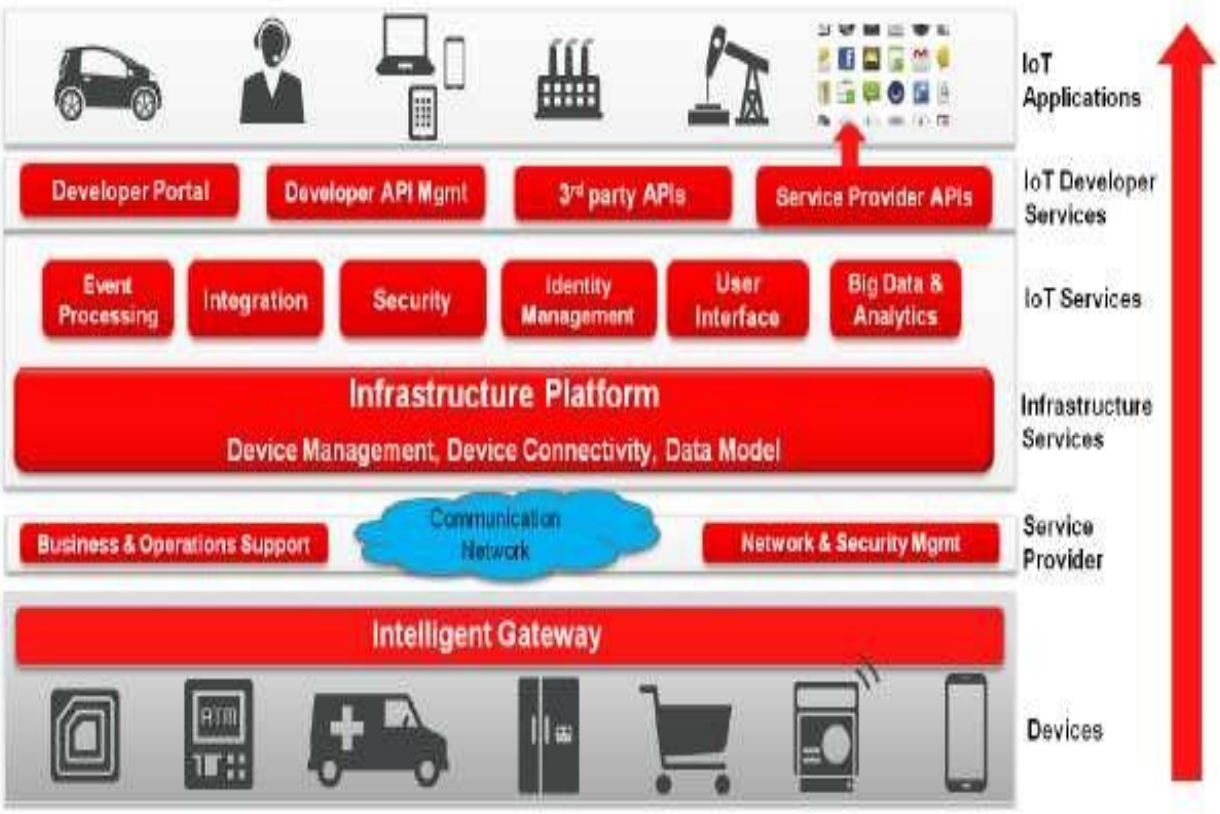
IoT Technologies:

- RFID
- WiFi
- Barcode
- QR Code
- ZigBee
- Sensors and Smartphones

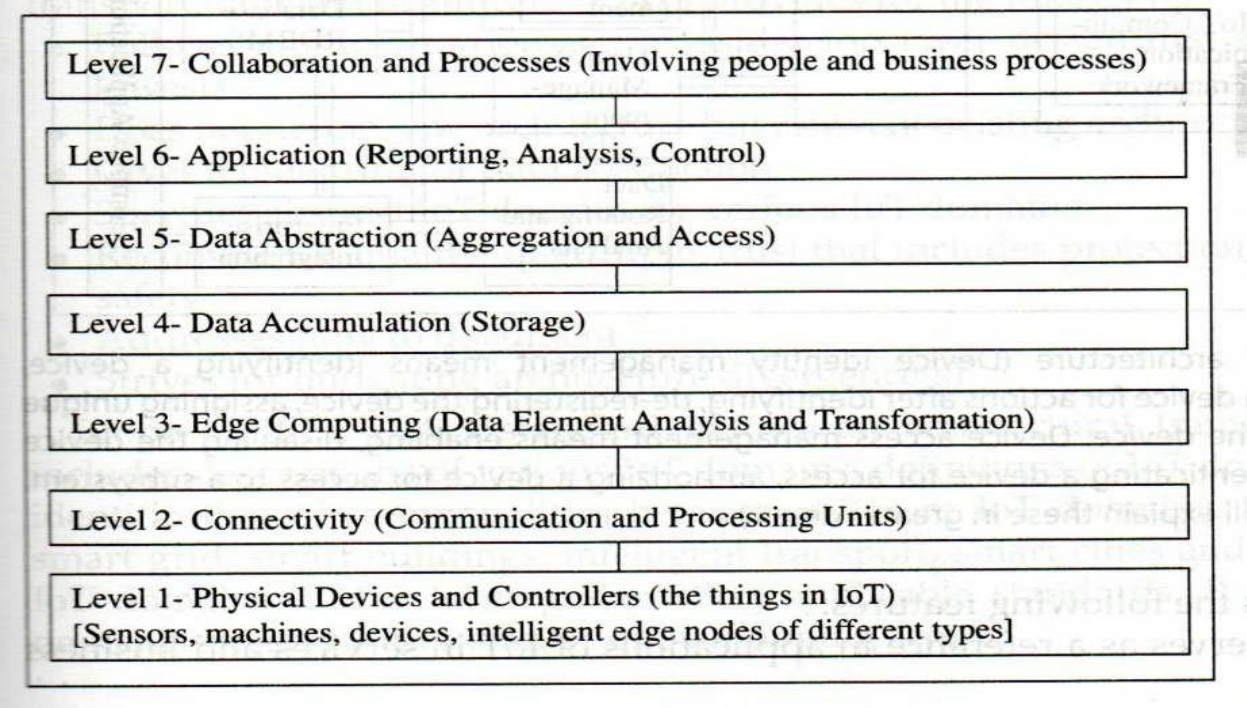
IoT: Hardware, Middleware and Software

Hardware	Middleware	Software
Arduino Nano Pro Mini	OpenIoT	Eclipse IoT
Raspberry-Pi	OpenRemote	Google Brillo
IBM Watson	OpenHUB	IBM IoT Foundation
Azure	Kaa	Azure IoT Suit
AWS	Oracle-Fusion	Cloud Sensor
INTEL JOULE		Ninja Sphere
Netduino		Control Any
Flutter		Arduino

Iot Architectural Framework:



IoT: Architectural View



IoT: Architectural View

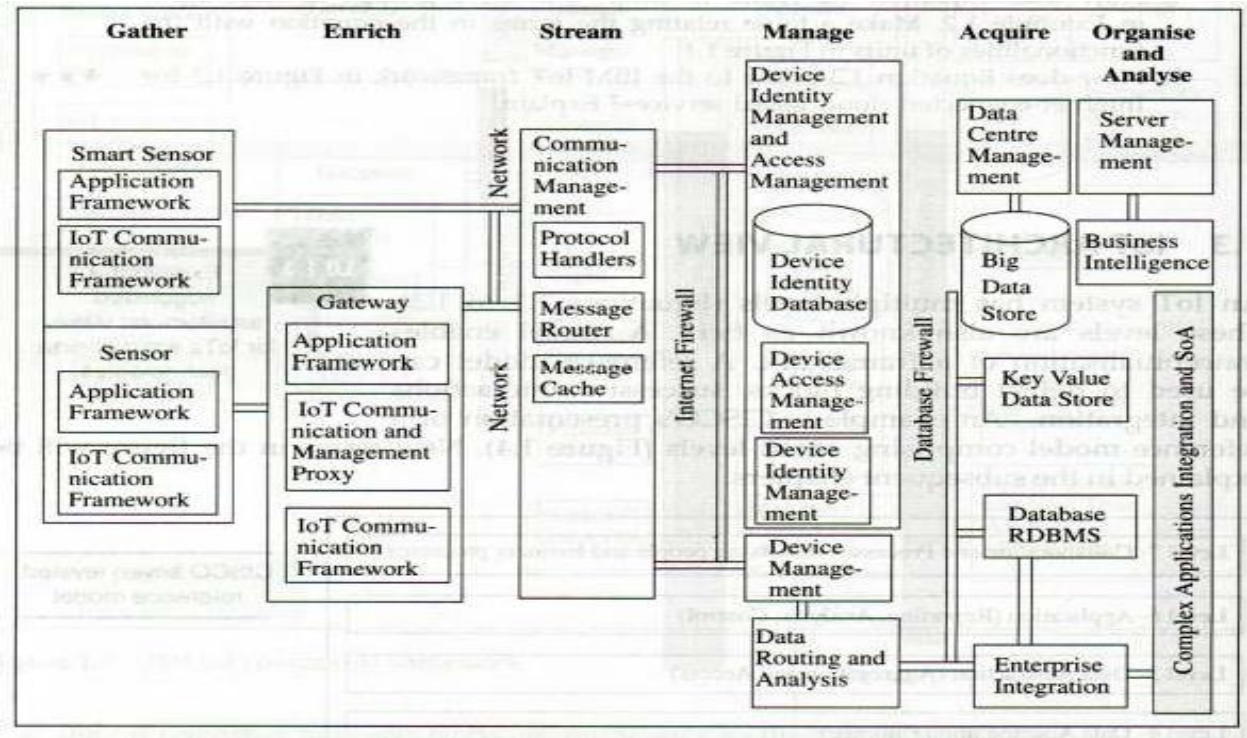


Fig: Oracle's IoT Architecture

Figure Oracle's IoT architecture (Device identity management means identifying a device, registering a device for actions after identifying, de-registering the

device, assigning unique identity to the device. Device access management means enabling, disabling the device access, authenticating a device for access, authorizing a device for access to a subsystem.

An architecture has the following features:

• The architecture serves as a reference in applications of IoT in services and business processes.

• A set of sensors which are smart, capture the data, perform necessary data element analysis and transformation as per device application framework and connect directly to a communication manager.

A set of sensor circuits is connected to a gateway possessing separate data capturing, gathering, computing and communication capabilities.

The gateway receives the data in one form at one end and sends it in another form to the other end. • The communication-management subsystem consists of protocol handlers, message routers and message cache.

• This management subsystem has functionalities for device identity database, device identity management and access management.

• Data routes from the gateway through the Internet and data centre to the application server or enterprise server which acquires that data.

• Organisation and analysis subsystems enable the services, business processes, enterprise integration and complex been proposed at SWG (Sub Working Group) Teleconference of December 2014. Standards for an architectural framework for the IoT have been developed under IEEE project P2413. IEEE working group is working on a set of guidelines for the standards. IEEE suggested P2413 3 standard for architecture.

2.2 Sources of IoT

Popular IoT Development Boards

Arduino Yún

Arduino Yún board uses microcontroller ATmega32u4 that supports Arduino and includes Wi-Fi, Ethernet, USB port, micro-SD card slot and three reset buttons. The board also combines with Atheros AR9331 that runs Linux.

Microduino

Microduino is a small board compatible with Arduino that can be stacked with the other boards. All the hardware designs are open source.

Intel Galileo

Intel Galileo is a line of Arduino-certified development boards. Galileo is based on Intel x86 architecture. It is open-source hardware that features the Intel SOC X1000 Quark based Soc.

Galileo is pin-compatible with Arduino. It has 20 digital I/O (12 GPIOs fully native), 12-bit PWM for more precise control, six analog inputs and supports power over Ethernet (PoE).

Intel Edison

Intel Edison[19] is a compute module. It enables creation of prototypes and fast development of prototyping projects and rapidly produces IoT and wearable computing devices. It enables seamless device internetworking and device-to-cloud communication. It includes foundational tools. The tools collect, store and process data in the cloud, and process rules on the data stream. It generates triggers and alerts based on advanced analytics.

Beagle Board

Beagle Bone based board has very low power requirement. It is a card-like computer which can run Android and Linux. Both the hardware designs and the software for the IoT devices are open source.

Raspberry Pi Wireless Inventors Kit (RasWIK)

RasWIK enables Raspberry Pi Wi-Fi connected devices. It includes documentation for 29 different projects or you can come up with one of your own. There is a fee for the devices but all of the included code is open source, and you can use it to build commercial products as well.

2.3 M2M COMMUNICATION

Machine-to-machine (M2M) refers to the process of communication of a physical object or device at machine with others of the same type, mostly for monitoring but also for control purposes. Each machine in an M2M system embeds a smart device. The device senses the data or status of the machine, and performs the computation and communication functions. A device

Communicates via wired or wireless systems. The communication protocols are 6LowPAN, LWM2M, MQTT, and XMPP. Each communication device is assigned 48-bits Ipv6 address.

2.3.1 M2M to IoT and IoT technology in industry

IoT technology in industry involves the integration of complex physical machinery M2M communication with the networks of sensors, and uses analytics, machine learning, and knowledge devices or machines located remotely. The close difference between M2M and IoT is that M2M must deploy device to device, and carry out the coordination, monitoring, controlling of the devices and communicate without the usage of Internet whereas IoT deploys the internet, server, internet protocols and server or cloud end applications, services or processes. M2M has many applications in fields such as industrial automation, logistics, smart grid, smart cities, health and defence. Initial applications of M2M were found in automation and instrumentation only, but now these include telemetric applications and Industrial Internet of Things (IIoT) as well.

2.3.2 M2M Architecture

M2M architecture consists of three domains (Figure below):

1. M2M device domain
2. M2M network domain
3. M2M application domain

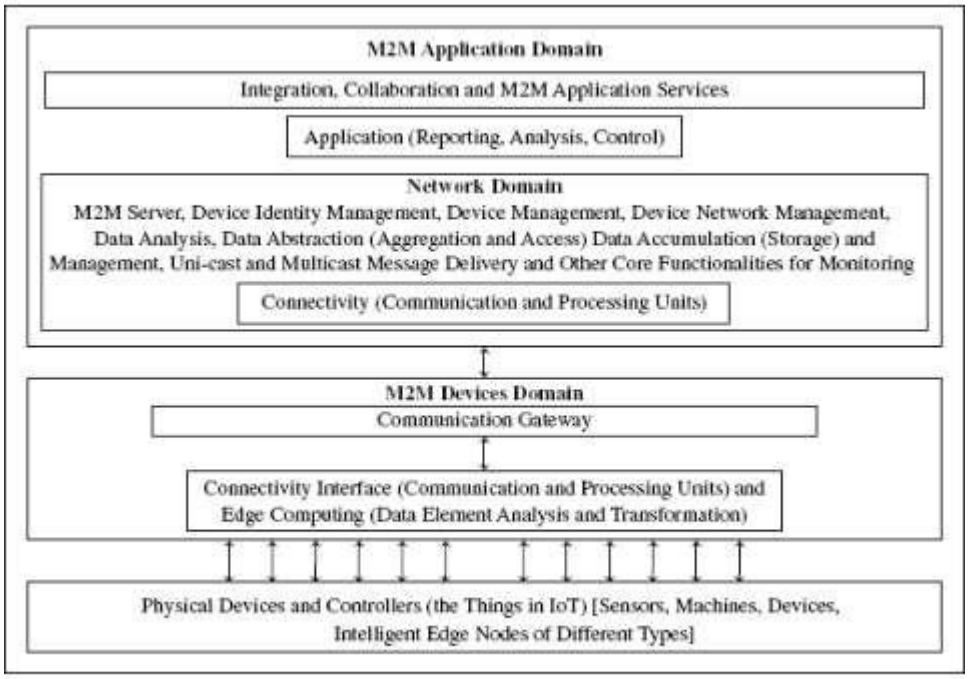


Figure Three domains of M2M architecture

Fig: 3 Domains of M2M Architecture

M2M device communication domain consists of three entities:

physical devices, communication interface and gateway. Communication interface is a port or a subsystem, which receives the input from one end and sends the data received to another. M2M network domain consists of M2M server, device identity management, data analytics and data and device management similar to IoT architecture (connect + collect + assemble + analyse) level. M2M application domain consists of application for services, monitoring, analysis and controlling of devices networks.

2.3.3 Software and Development Tools

Examples of M2M software and development tools are as follows:

• Mango is an open source M2M web-based software. It supports multiple platforms, multiple protocols, databases, meta points, user-defined events and import/export. 20

• Mainspring from M2MLabs is a development tool, and source framework for developing M2M applications. 21 It enables: configurations

• Communication between devices and applications

• Validation and normalisation of data
• Long-term data storage and data retrieval functions
• Programming in Java and Apache Cassandra
• Usages of no SQL database.
• DeviceHive is an M2M communication framework. It is an M2M platform and integration tool. It enables connecting devices to the IoT. It includes web-based management software that creates are the open protocols, tools and frameworks for M2M:
• XMPP, MQTT-OASIS standards group and OMA LWM2M-OMA standard group for protocol
• Various projects of Eclipse M2M industry working groups' are Koneki, Eclipse SCADA for open standards for communication protocols, tools and frameworks
• ITU-T Focus Group M2M global standardisation initiative for a common M2M service layer
• 3GPPP study group for security aspects of M2M equipment and automatic SIM activation covering remote provisioning and change of subscription.
• Weightless (wireless communications) group for standards and using wireless spaces for M2M Following is an example of M2M/IoT. security-rules-based e-networks and monitoring devices. The web software enables prototype projects built with DeviceHub and online tests to find out how it works.

Questions???

1. What does M2M mean?
2. How does M2M relate to IoT? What are the differences between the two?
3. Give examples of M2M applications.
4. What are the three architectural domain functionalities in M2M architecture?

2.4 IoT/M2M SYSTEMS, LAYERS AND DESIGNS STANDARDISATION:

A number of international organisations have taken action for IoT design standardisation. Following are the examples: Internet Engineering Task Force (IETF), an international body initiated actions for addressing and working on the recommendations for the engineering specifications for the Internet of Things. IETF suggests the specifications for the layers, and the engineering aspects for the IoT communication, networks and applications. International Telecommunication Union for Telecommunication (ITU-T) suggested a reference model for IoT domain, network and transport capabilities for the IoT services and the applications at the application and application-support layers. European Telecommunication Standards Institute (ETSI) initiated the development of a set of standards for the network, and devices and gateway domains for the communication between machines (M2M). ETSI proposed high-level architecture for applications and service capabilities. Open Geospatial Consortium (OGC), an International Industry Consortium, has also suggested open standards for sensors' discovery, capabilities, quality and other aspects with support to geographical information web support.
Following subsections describe these standardization efforts.

Modified OSI Model for the IoT/M2M Systems:

OSI protocols mean a family of information exchange standards developed jointly by the ISO and the ITU-T. The seven-layer OSI model is a standard model. It gives the basic outline for designing a communication network. Various models for data interchanges consider the layers specified by the OSI model, and modify it for simplicity according to the requirement. Similarly, IETF suggests modifications in the OSI model for the IoT/M2M. Figure 2.1 shows a classical seven-layer OSI model (on the left) and the modifications in that model proposed by IETF (in the middle). Data communicates from device end to application end. Each layer processes the received data and creates a new data stack which transfers it to the next layer. The processing takes place at the in-between layers, i.e. between the bottom functional-layer to the top layer. Device end also receives data from an application/service after processing at the in-between layers. Figure 2.1 also shows a similarity with the

conceptual framework in Equation 1.2: Gather + Enrich + Stream + (Manage + Acquire + Organise +Analyse) = IoT Applications and Services

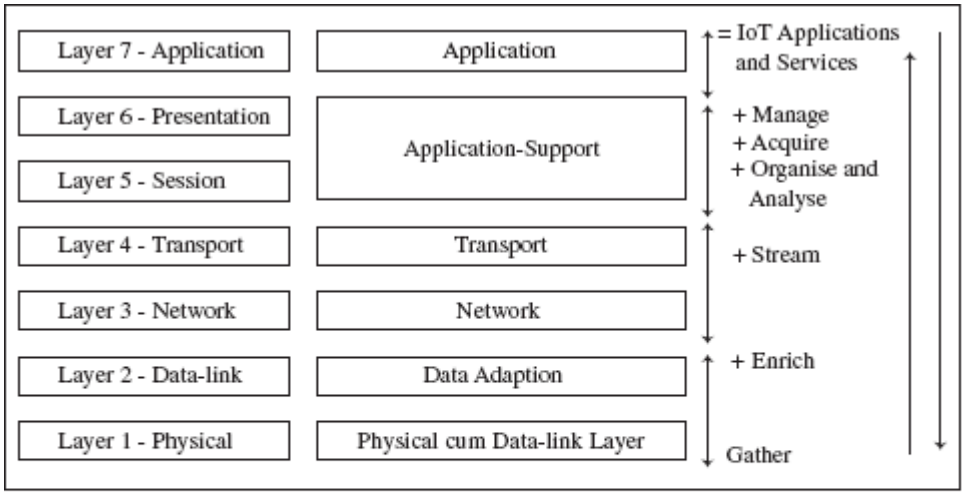


Figure Seven-layer generalised OSI model (on left) and IETF six layer modified OSI model for IoT/M2M (in the middle), and similarity with the conceptual framework Equation 1.2 (on right) for IoT applications and services

New applications and services are present at the application layer 6. A modification to this is that the application-support layer 5 uses may include processes for data managing, acquiring, organising and analysing which are mostly used by applications and services. Modifications are also at the data-link layer 2 (L2) and physical layer 1 (L1). The new layers are data-adaptation (new L2) and physical cum data-link (new L1). The data-adaptation layer includes a gateway. The gateway enables communication between the devices network and the web. A physical IoT/M2M device hardware may integrate a wireless transceiver using a communication protocol as well as a data-link protocol for linking the data stacks of L1 and L2. Example 2.1 explains the IETF six-layer OSI model for Internet of streetlights.

2 ITU-T Reference Model:

Figure 2.2 shows the ITU-T reference model RM1. It also shows correspondence of the model with the six-layers modified OSI model (Figure 2.1). The figure also shows a comparison with CISCO IoT reference model RM2 (Figure 1.4). RM1 considers four layers which are:

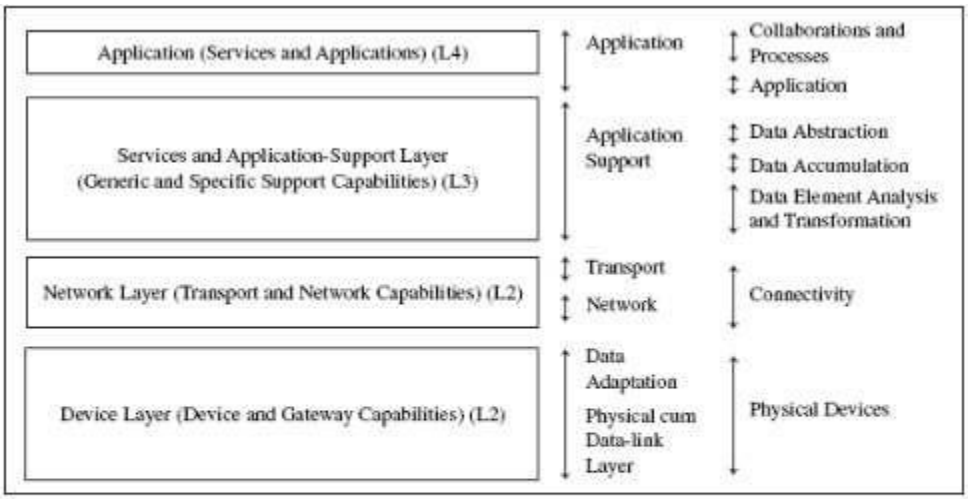


Figure ITU-T reference model RM1, its correspondence with six layers of modified OSI and a comparison with seven levels suggested in CISCO IoT reference model RM2

Lowest layer , L1, is the device layer and has device and gateway capabilities. The support layer has two types of capabilities—generic and specific service or application-support capabilities.

• Top layer , L4, is for applications and services. ITU-T recommends four layers, each with different capabilities. A comparison of ITU-T RM1 with the six-layer OSI model can be made as follows:

• RM1 device layer capabilities are similar to data-adaptation and physical cum data-link layers.

• RM1 network layer capabilities are similar to transport and network layers.

• RM1 upper two layer capabilities are similar to top two layers. A comparison with the CISCO IoT reference model (RM2) can be made as follows:

RM1 L4 capabilities are similar to RM2 collaborations and processes, and application top two levels.

• RM1 L3 capabilities are similar to RM2 three middle-level functions of data abstraction, accumulation, analysis and transformation.

• RM1 L2 layer capabilities are similar to RM2 functions at connectivity level.

• RM1 L1 device layer capabilities are similar to RM2 functions at physical devices level.

3 ETSI M2M Domains and High-level Capabilities:

A domain specifies the functional areas. High-level architecture means architecture for functional and structural views.

Figure below shows ETSI M2M domains and architecture, and the high-level capabilities of each domain. It also shows that the architecture correspondences with the six-layer modified OSI model as well as the four layers of the ITU-T reference model.

The ETSI network domain has six capabilities and functions:

1. M2M applications
2. M2M service capabilities
3. M2M management functions
4. Network management functions
5. CoRE network (for example, 3G and IP networks, network control functions, interconnections among networks)
6. Access network (for example, LPWAN (low power wide area network), WLAN (Wi-Fi) and WiMax networks)

The ETSI device and gateway domain has the following functional units:

• Gateway between M2M area network, and CoRE and access NFC, PAN, LAN)

• M2M devices modified OSI and four layers of ITU-T reference model.

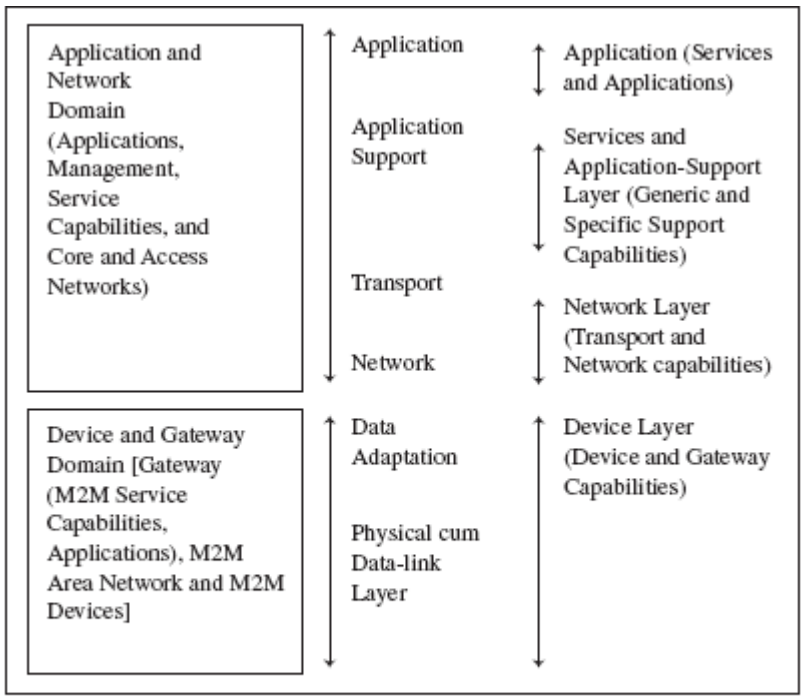


Figure . ETSI M2M domain architecture and its high-level capabilities, and its correspondences with six layers of

Questions:

1. Draw the IETF six-layer model for Internet of RFIDs applications for tracking and inventory control.
2. Draw the ITU-T reference model for Internet of streetlights.
3. Draw the proposed ETSI high-level architecture for the ATMs-bank server applications and services.
4. How can the functional units in CISCO seven levels be associated with four layers in the ITU-T reference model?
5. Why is a gateway necessary in a communication framework for IoT and M2M applications and services?

2.6 COMMUNICATION TECHNOLOGIES:

Physical cum data-link layer in the model consists of a local area network/personal area network. A local network of IoT or M2M device deploys one of the two types of technologies— wireless or wired communication technologies. Figure below shows connected devices (1 st to i th) connectivity using different technologies for communication of data from and to devices to the local network connectivity to a gateway.

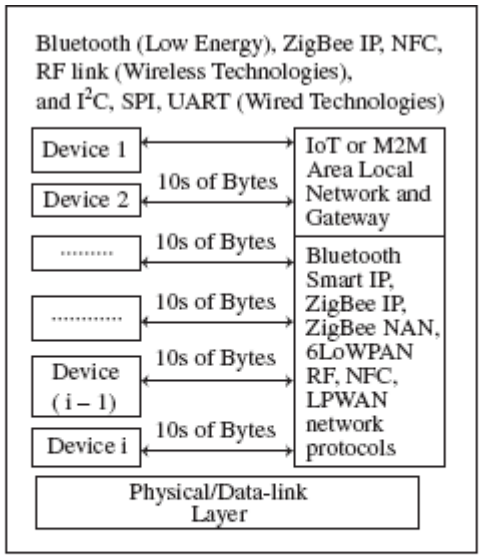


Figure Connected devices 1st to ith connected to the local network and gateway using the WPAN or LPWAN network protocols

Figure above shows number of devices present in an IoT or M2M devices network. The figure shows the local area network of devices. The connectivity between the devices (left-hand side) is by using RF, Bluetooth Smart Energy, ZigBee IP, ZigBee NAN (neighbourhood area network), NFC or 6LoWPAN or mobile. Tens of bytes communicate at an instance between the device and local devices network. Following subsections describe the technologies and standards recommended for the communication.

1 Wireless Communication Technology:

Physical cum data-link layer uses wired or wireless communication technologies. Examples of wireless communication technologies are NFC, RFID,

ZigBee, Bluetooth (BT), RF transceivers and RF modules. Following subsections describe these wireless communication technologies.

Near-Field Communication (NFC)

Near-Field communication (NFC) is an enhancement of ISO/IEC 2 14443 standard for contact-less proximity-card. NFC is a short distance (20 cm) wireless communication technology. It enables data exchange between cards in proximity and other devices. Examples of applications of NFC are proximity-card reader/RFID/IoT/M2M/mobile device, mobile payment wallet, electronic keys for car, house, office entry keys and biometric passport readers. NFC devices transmit and receive data at the same instance and the setup time (time taken to start the communication) is 0.1 s. The device or its reader can generate RF fields for the nearby passive devices such as passive RFID. An NFC device can check RF field and detect collision of transmitted signals. The device can check collision when the received signal bits do not match with the transmitted signal bits. Features of an NFC device are: Range of functioning is within 10 to 20 cm. The device can also communicate with Bluetooth and Wi-Fi devices in order to extend the distance from 10 cm to 30 m or higher. The device is able to receive and pass the data to a Bluetooth connection or standardised LAN or Wi-Fi using information handover functions. Device data transfer rates are 106 kbps, 212 kbps, 424 kbps and 848 kbps (bps stands for active devices in which RF fields alternately generate when communicating. 2. Card-emulation mode: Communication without interruption for the read and write as required in a smart card and smart card reader. FeliCa ™ and Mifare ™ standards are protocols for reading and writing data on the card device and reader, and then the reader can transfer information to Bluetooth or LAN. 3. Reader mode: Using NFC the device reads passive RFID device. The RF field is generated by an active NFC device. This enables the passive device to communicate.

RFID

RFID Radio Frequency Identification (RFID) is an automatic identification method. RFIDs use the Internet. RFID usage is, therefore, in remote storage and retrieval of data is done at the RFID tags. An RFID device functions as a tag or label, which may be placed on an object. The object can then be tracked for the movements. The object may be a parcel, person, bird or an animal. IoT applications of RFID are in business processes, such as parcels tracking and inventory control, sales log-ins and supply-chain management. Section 7.5.1 describes the details of the technology. Bluetooth BR/EDR and Bluetooth Low Energy Bluetooth devices follow IEEE 802.15.1 standard protocol for L1 (physical cum data-link layer). BT devices form a WPAN devices network. Two types of modes for the devices are Bluetooth BR/EDR (Basic Rate 1 Mbps/Enhanced Data Rate 2 Mbps and 3 Mbps) and Bluetooth low energy (BT LE 1Mbps). A latest version is Bluetooth v4.2. BT LE is also called Bluetooth Smart . Bluetooth v4.2 (December 2014) provides the LE data packet length extension, link layer privacy and secure connections, extended scanner and filter link layer policies and IPSP. BT LE range is 150 m at 10 mW power output, data transfer rate is 1 Mbps and setup time is less than 6 s. Bluetooth v5, released in June 2016, has increased the broadcast capacity by 800%, quadrupled the range and doubled the speed. Its features are: • Auto-synchronisation between mobile and other devices when both use BT. BT network uses features of self-discovery, self-configuration and self-healing. • Radio range depending on class of radio; Class 1 or 2 or radios: 100 m, 10 m or 1 m used in device BT implementation. • Support to NFC pairing for low latency in pairing the BT devices. • Two modes—dual or single mode devices are used for IoT/M2M devices local area network. • IPv6 connection option for BT Smart with IPSP (Internet Protocol Support Profile). • Smaller packets in LE mode. • Operation in secured as well as unsecured modes (devices can opt for both link-level as well as service-level security or just service level or unsecured level). • AES-CCM 128 authenticated encryption algorithm for confidentiality and authentication (Refer Example 2.4). • Connection of IoT/M2M/mobile

devices using BT EDR device to the Internet with 24 Mbps Wi-Fi 802.11 adaptation layer (AMP: Alternative MAC/PHY layer) or BT-enabled wire-bound connection ports or device. MAC stands for media access control sublayer at a data-link layer/sublayer.

ZigBee IP/ZigBee SE 2.0 ZigBee:

ZigBee IP/ZigBee SE 2.0 ZigBee devices follow the IEEE 802.15.4 standard protocol L1 (physical cum data-link layer). ZigBee devices form a WPAN devices network. ZigBee end-point devices form a WPAN of embedded sensors, actuators, appliances, controllers or medical data systems which connect to the Internet for IoT applications, services and business processes. ZigBee Neighbourhood Area Network (NAN) is a version for a smart grid. ZigBee smart energy version 2.0 has energy management and energy efficiency capabilities using an IP network. The features of ZigBee IP are:
L1 layer PDU = 127 B • Used for low-power, short-range WPAN • The device can function in six modes—end point, ZigBee-ZigBee devices router, ZigBee network coordinator, ZigBee-IP coordinator, ZigBee-IP router and IP host. • ZigBee IP enhancement provisions the IPv6 connectivity. A ZigBee IP device is a Reduced Function Device (RFD). RFD means one that functions for the 'sleepy'/ battery-operated device. Sleepy means one that wakes up infrequently, sends data and then goes back to sleep. ZigBee IP supports IPv6 network with 6LoWPAN header compression, connection for Internet communication and control of low power devices, TCP/UDP transport layer and TLSv1.2 public key (RSA and ECC) and PSK cipher suite for end-to-end security protocol, big-scale automation and remote controls. • A self-configuring and self-healing dynamic pairing mesh network, supports both multicast and unicast options. • Multicast forwarding to support multicast Domain Name System (mDNS) based service discovery (SD) • Support to development of discovery mechanism with full application confirmation • Support to pairing of coordinator with end-point devices and routers in star topology • Provides bigger network using multiple star topology and inter-PAN

communications • Support to sensor nodes and sensor (or appliances) network integration, sensor and appliances devices configured as router or end-devices • Low latency (< 10 ms) link layer connection • Range is 10–200 m, data transfer rate is 250 kbps, low power operation • ISM band frequencies direct sequence spread spectrum 16-channel radio, and provide link level security using AES-CCM-128 (Example 2.4) • Includes RFD in ZigBee SE 2.0 ZigBee NAN is for devices which are used for smart-metering, distribution automation devices and smart grid communication profile. NAN enables a utility's last-mile at HAN (Home Area Network), outdoor access network that connects smart meters to WAN (widearea network) gateways. Figure 2.5 shows ZigBee End Point, Coordinator, Router, ZigBee IP Router modes forming star, mesh and IP networks of ZigBee sensors, end devices and ZigBee router device which interconnect to to coordinator ZigBee devices forming a star network. • One end device, two routers and one coordinator forming a mesh network. • Mesh network router connects to an AP/gateway, which in turn connects to a cellular network. • Coordinator of mesh network connects to ZigBee IP border router, which enables local ZigBee networks' connectivity to the Internet.

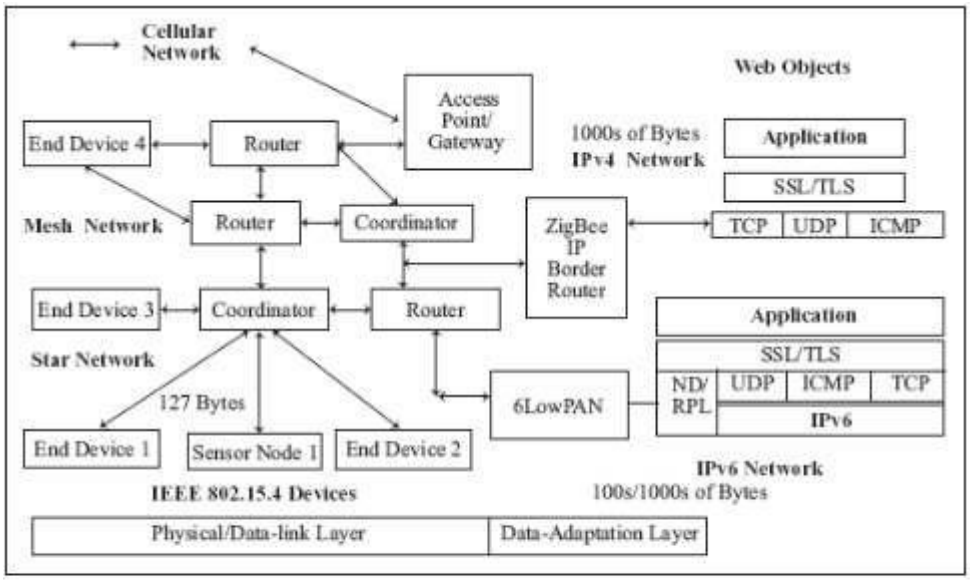


Figure ZigBee end point, coordinator, router, ZigBee IP router nodes forming the star, mesh and IP networks of ZigBee sensors, end devices, and ZigBee router devices which interconnect to

Features of a ZigBee network are:

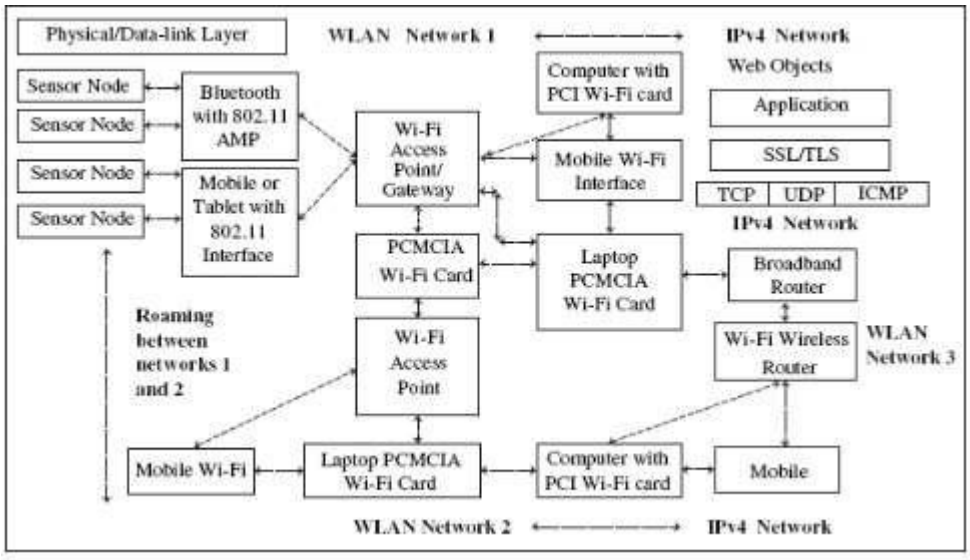
• A router in star network connects to 6LoWPAN, which connects an IEEE 802.15.4 devices network to IPv6 network. • 1000s of byte communicate between the network layer and IoT web objects. • 127 B communication between the adaptation layer IEEE 802.15.4 devices at single data transfer. • IETF ND (Neighbour Discovery), ROLL (Routing Over Low power Loss Network), RPL routing, IPv6/IPv4 network, TCP/UDP/ICMP transport, SSL/TLS security layer protocols for the communication between web object/application and ZigBee devices.

Wi-Fi

Wi-Fi Wi-Fi is an interface technology that uses IEEE 802.11 protocol and enables the Wireless Local Area Networks (WLANs). Wi-Fi devices connect enterprises, universities and offices through home AP/public hotspots. Wi-Fi connects distributed WLAN networks using the Internet. Automobiles, instruments, home networking, sensors, actuators, industrial device nodes, computers, tablets, mobiles, printers and many devices have Wi-Fi interface. They network using a Wi-Fi network. Wi-Fi is very popular. The issues of Wi-Fi interfaces, APs and routers are higher power consumption, interference and performance degradation. Wi-Fi interfaces connect within themselves or to an AP or wireless router using Wi-Fi PCMCIA or PCI card or built-in circuit cards and through the following: • Base station (BS) or AP • A WLAN transceiver or BS can connect one or many wireless devices simultaneously to the Internet. • Peer-to-peer nodes without access point: Client devices within Independent Basic Service Set (IBSS) network can easy setting of an 802.11 network. • Peer to multipoint nodes with Basic Service Sets (BSSs) using one in-between AP point or distributed BSSs connect through multiple APs. • Connectivity range of each BSS depends on the range of wireless bridges and antennae used and environmental conditions. • Each BSS is a Service Set Identifier (SSID).

Figure below shows three WLAN networks (BSSs) for sensor device nodes, mobiles, tablets, laptops, computers and Internet connectivity of WLAN networks with the IP4 networks (here dashed lines represent wireless

connectivity and solid lines represent wired connectivity). Figure 2.6 shows the following: • Sensor nodes connected to BT with Wi-Fi adaptation, 802.11 interfaces in a WLAN network 1 (WLAN1). • Tablets, Wi-Fi, computers also connect in WLAN 1 though an AP. • AP1 connects to a broadband router 1 and to the IP4 network 2. • WLAN1 and WLAN2 function as BSS. • WLAN 2 also consists of AP2, Wi-Fi router and other Wi-Fi enabled interfaces. • Wi-Fi router connects to multiple Wi-Fi nodes as well as to a broadband router 2. • Broadband routers 1 and 2 connect using wires, to IP4 networks and web objects for IoT apps, services and processes. The Wi-Fi interfaces, access points, routers features are as follows: • Generally used are the 2.4 GHz IEEE 802.11b adapters or 5 series protocols. • Interfaces use 2.4 GHz or 5 GHz antenna • Offers mobility and roaming



Three WLAN networks for sensor device nodes, mobiles, tablets, laptops, computers and Internet connectivity of WLAN networks with the IP4 networks (Dashed lines show wireless connectivity and solid lines show wired connectivity)

- Have easy installation simplicity and flexibility
- Coverage range is 30 m to 125 m
- Used in a room having the limited-coverage 802.11a which coexists with b, coexists with b and g

• Uses the 802.11b in wider coverage range because that is unaffected by walls and is meant for hotspots for public usage having range data rate 11 Mbps (802.11b) within 30 m

• Uses 802.11g for high data rates up to 54 Mbps, and 802.11n for very high 600 Mbps, using multiple antennas to increase infrastructure which ensures compatibility and enables easier access and hides complexity when enabling the wireless access to data, media and streams, and applications and services.

• Provides a dynamic environment of network expendability and scalability. Scalability means a system can have a large number of smaller interfaces, routers and APs

• Provides security, integrity and reliability • Uses Wireless Protected Access (WPA) and Wired Equivalent Privacy (WEP) security sublayers.

Comparisons /Difference

ZigBee, Bluetooth, NFC, vs., WiFi

	Low Energy Bluetooth	ZigBee	NFC	Low Power WiFi
Frequency (MHz)	2402 – 2482	868 - 868.8, 902 - 928, 2402 – 2482	13.56	2400 - 2500
Channels	3	16	1	3
Modulation	GFSK	BPSK & QPSK	ASK	64QAM
Max potential data rate	1 Mbps	250 Kbps	424 Kbps	54 Mbps
Range	10m	100+m	10cm	30m
Power Profile	Days	Months/Years	Months/Years	Hours
Complexity	Complex	Simple	Simple	Complex
Nodes/Master	7	65,000	1+1	
Extendibility	No	Yes	No	Yes

37

Short range radio links inside phones

RUTRONIK ELECTRONICS WORLDWIDE

	NFC	Bluetooth 2.1 (EDR)	Bluetooth Low Energy	ANT+	Wifi 802.11b/g	Wifi 802.11n
Standard by	ISO/IEC	Bluetooth SIG	Bluetooth SIG	Garmin	Wi-Fi Alliance	Wi-Fi Alliance
Network Standard	ISO 13157 etc.	IEEE 802.15.1	IEEE 802.15.1	proprietary	IEEE 802.11b/g	IEEE 802.11n
Network Type	Point to point	WPAN	WPAN	WPAN	WPAN	WPAN
Range free field	< 0.2 m	≈ 100 m (class 2) outdoor	≈ 100 m outdoor	≈ 100 m outdoor	≈ 38 m indoor / ≈ 140 m outdoor	≈ 70 m indoor / **≈ 250 m outdoor**
Frequency	13.56 MHz	2.4–2.5 GHz	2.4–2.5 GHz	2.4–2.5 GHz	2.4–2.5 GHz	2.4–2.5 GHz
Bit rate	424 kbit/s	2 to 3 Mbps	≈1.0 Mbps	≈1.0 Mbps	(Max/Typ/Min) 54Mbps / 36Mbps / 1Mbps	150 Mbps / 90 Mbps Multi stream max **600 Mbps**
Set-up time	< 0.1 s	< 6 s	**< 0.006 s**	?	?	?
Power consum-ption	< 15mA (read)	< 40 mA (class 2)	**< 15 mA RX and TX**	15 mA TX / 17 mA RX	(Max/Typ/Min) ? RX : 100 - 250mA TX: 250 - 350mA	

http://www.rutronik.com / Harald Naumann / harald_naumann@rutronik.com / +49 175 5774832 Page 4