COURSE OUTCOMES (CO)

CO1: Understand the revolution of internet in field of cloud, wireless network, embedded system and mobile devices.
CO2: Apply IOT design concepts in various dimensions implementing software and hardware.
CO3: Analyze various M2M and IOT architectures.
CO4: Design and develop various applications in IOT.

Contents of the Lecture

Different between IOT & M2M SDN

Difference between IoT and M2M

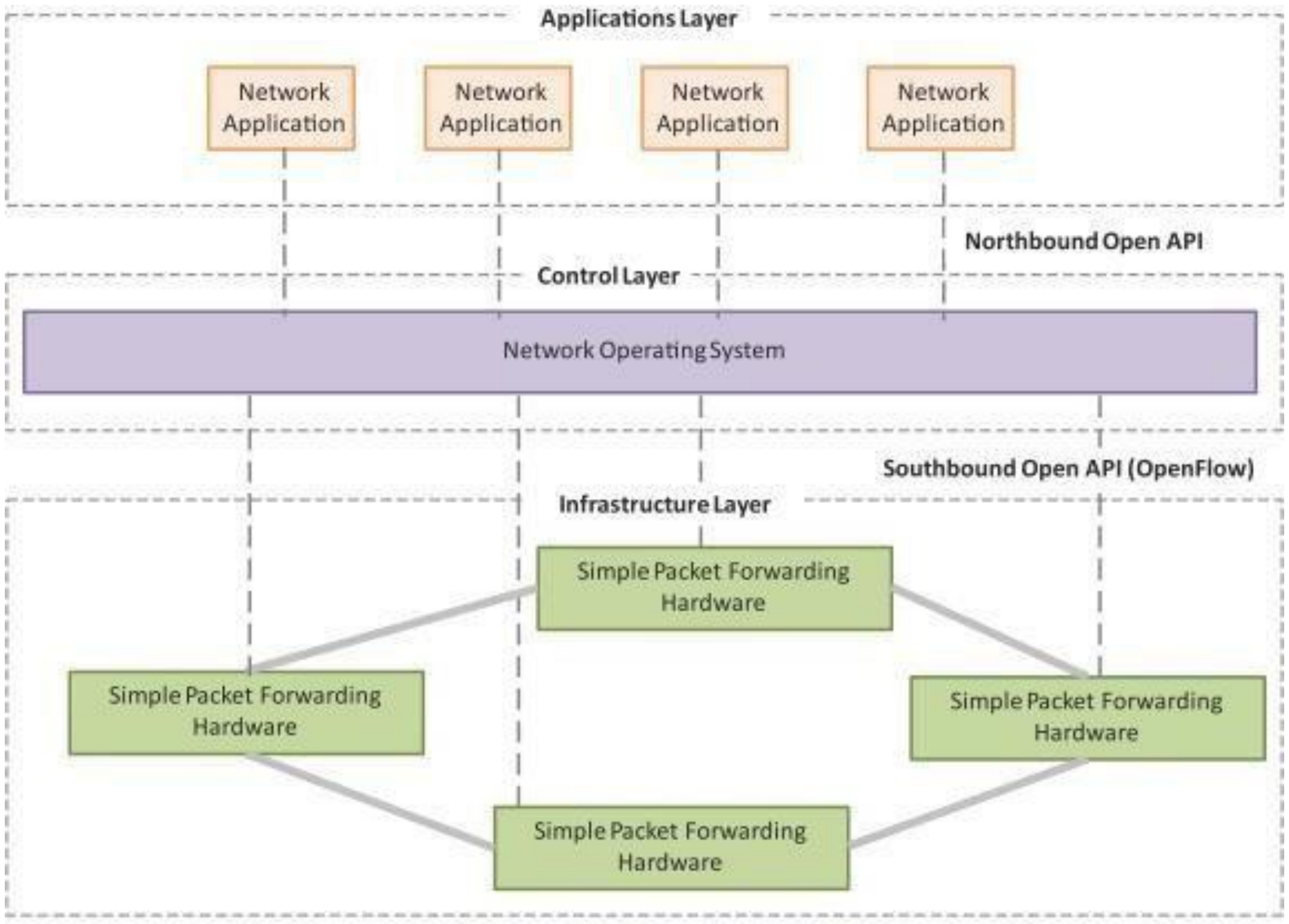
- Communication Protocols
  - M2M and IoT can differ in how the communication between the machines or devices happens.
  - M2M uses either proprietary or non-IP based communication protocols for communication within the M2M area networks.
- Machines in M2M vs Things in IoT
  - The "Things" in IoT refers to physical objects that have unique identifiers and can sense and communicate with their external environment (and user applications) or their internal physical states.
  - M2M systems, in contrast to IoT, typically have homogeneous machine types within an M2M area network.

Difference between IoT and M2M

- Hardware vs Software Emphasis
  - While the emphasis of M2M is more on hardware with embedded modules, the emphasis of IoT is more on software.
- Data Collection & Analysis
  - M2M data is collected in point solutions and often in on-premises storage infrastructure.
  - In contrast to M2M, the data in IoT is collected in the cloud (can be public, private or hybrid cloud).
- Applications
  - M2M data is collected in point solutions and can be accessed by on-premises applications such as diagnosis applications, service management applications, and on- premisis enterprise applications.
  - IoT data is collected in the cloud and can be accessed by cloud applications such as analytics applications, enterprise applications, remote diagnosis and management applications, etc.

SDN

- Software-Defined Networking (SDN) is a networking architecture that separates the control plane from the data plane and centralizes the network controller.
- Software-based SDN controllers maintain a unified view of the network and make configuration, management and provisioning simpler.
- The underlying infrastructure in SDN uses simple packet forwarding hardware as opposed to specialized hardware in conventional networks.

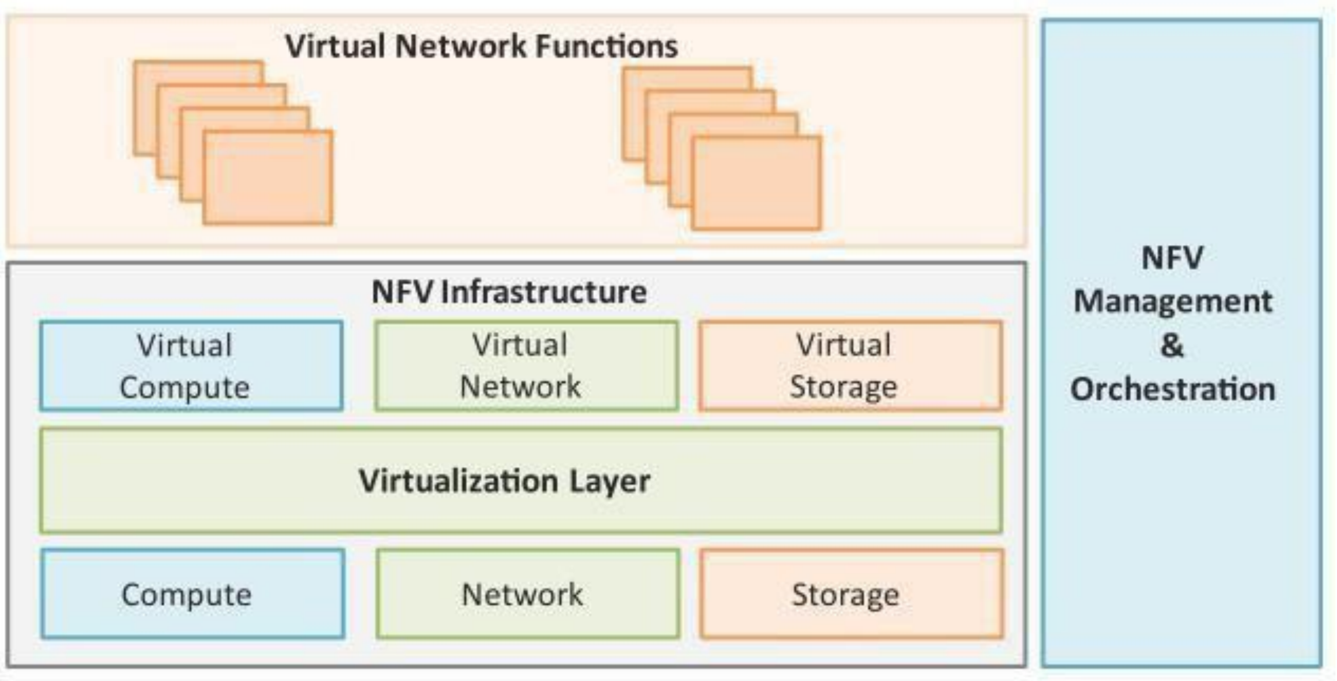


Key elements of SDN

- Centralized Network Controller
  - With decoupled control and data planes and centralized network controller, the network administrators can rapidly configure the network.
- Programmable Open APIs
  - SDN architecture supports programmable open APIs for interface between the SDN application and control layers (Northbound interface).
- Standard Communication Interface (OpenFlow)
  - SDN architecture uses a standard communication interface between the control and infrastructure layers (Southbound interface).
  - OpenFlow, which is defined by the Open Networking Foundation (ONF) is the broadly accepted SDN protocol for the Southbound interface.

NFV

- Network Function Virtualization (NFV) is a technology that leverages virtualization to consolidate the heterogeneous network devices onto industry standard high volume servers, switches and storage.
- NFV is complementary to SDN as NFV can provide the infrastructure on which SDN can run.

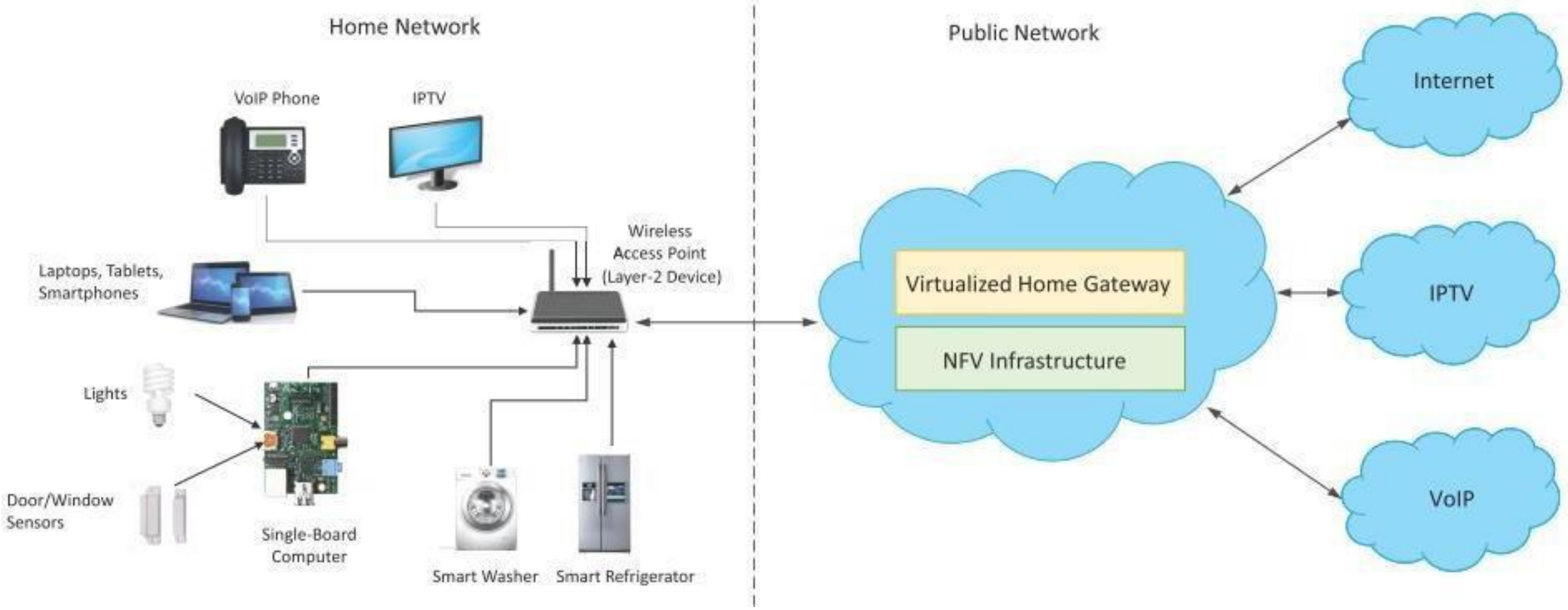


Key elements of NFV

- Virtualized Network Function (VNF):
  - VNF is a software implementation of a network function which is capable of running over the NFV Infrastructure (NFVI).
- NFV Infrastructure (NFVI):
  - NFVI includes compute, network and storage resources that are virtualized.
- NFV Management and Orchestration:
  - NFV Management and Orchestration focuses on all virtualization-specific management tasks and covers the orchestration and life-cycle management of physical and/or software resources that support the infrastructure virtualization, and the life-cycle management of VNFs.

NFV Use Case

- NFV can be used to virtualize the Home Gateway. The NFV infrastructure in the cloud hosts a virtualized Home Gateway. The virtualized gateway provides private IP addresses to the devices in the home. The virtualized gateway also connects to network services such as VoIP and IPTV.



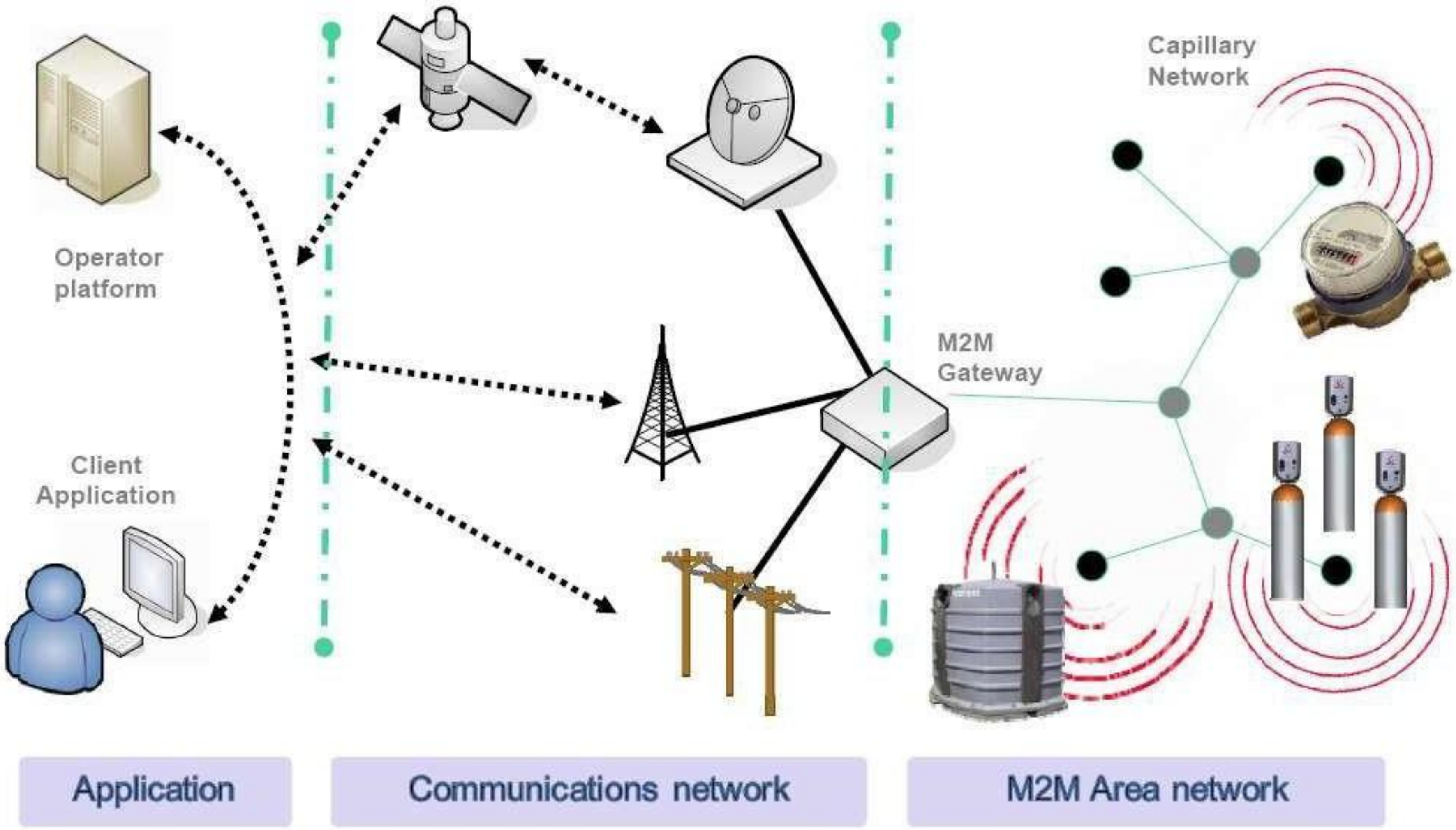
What is M2M?

-Machine-to-Machine (M2M) communications refers to communication between computers, embedded processors, smart sensors, actuators and mobile devices without, or with only human intervention.

-M2M is a new business concept originating from the telemetry technology.

-M2M is based on very common used technologies – wireless sensors, mobile networks and the Internet.

Architecture



Contd...

Explanation

4 basic stages that are common to most M2M based applications:

- Collection of data;
- Transmission of data througha communication network;
- Assessment of data;
- Response to the availableinformation;

Architecture

-M2M devices reply to requests for data contained within them or transmit the data automatically.

-M2M devices may constitute an M2M area network, which can be realised as, e.g. a Bluetooth based personal area network of body sensors. M2M gateway provides interconnection of M2M devices and forwards data collected from them to communications network.

-The communication network serves as infrastructure for realising communication between M2M gateway and M2M end-user application or server.

Contd...

For this purpose cellular network, telephone linesand communicationsatellites can be used.
There are several means of sending data over the cellular network, such as CDMA and GPRS. **(Advantage of cellular data services is the ability to send large amounts of data frequently)**.

Finally, when data reach an M2M application, they can be analysed.

M2MAccess Networks

Wired Solution – dedicated cabling between sensor gateway

PROS: very, very reliable; very high rates, little delay, secure

CONS: very expensive to roll out.

Wireless Capillary Solution – shared short-range link/network.

PROS: cheap to roll out, generally scalable, low power

CONS: short range, multi-hop not a solution, low rates, weaker security, lack of universal coverage

Wireless Cellular Solution – dedicated cellularlink PROS: excellent coverage, mobility, roaming, generally secure

Cons: expensive operate, not cheap to maintain, not power efficient

How does it Work ?

When machines “talk” they do so in a language known as “Telemetry”. The concept of telemetry – remote machines and sensors collecting and sending data to a central point for analysis, either by humans or computers.

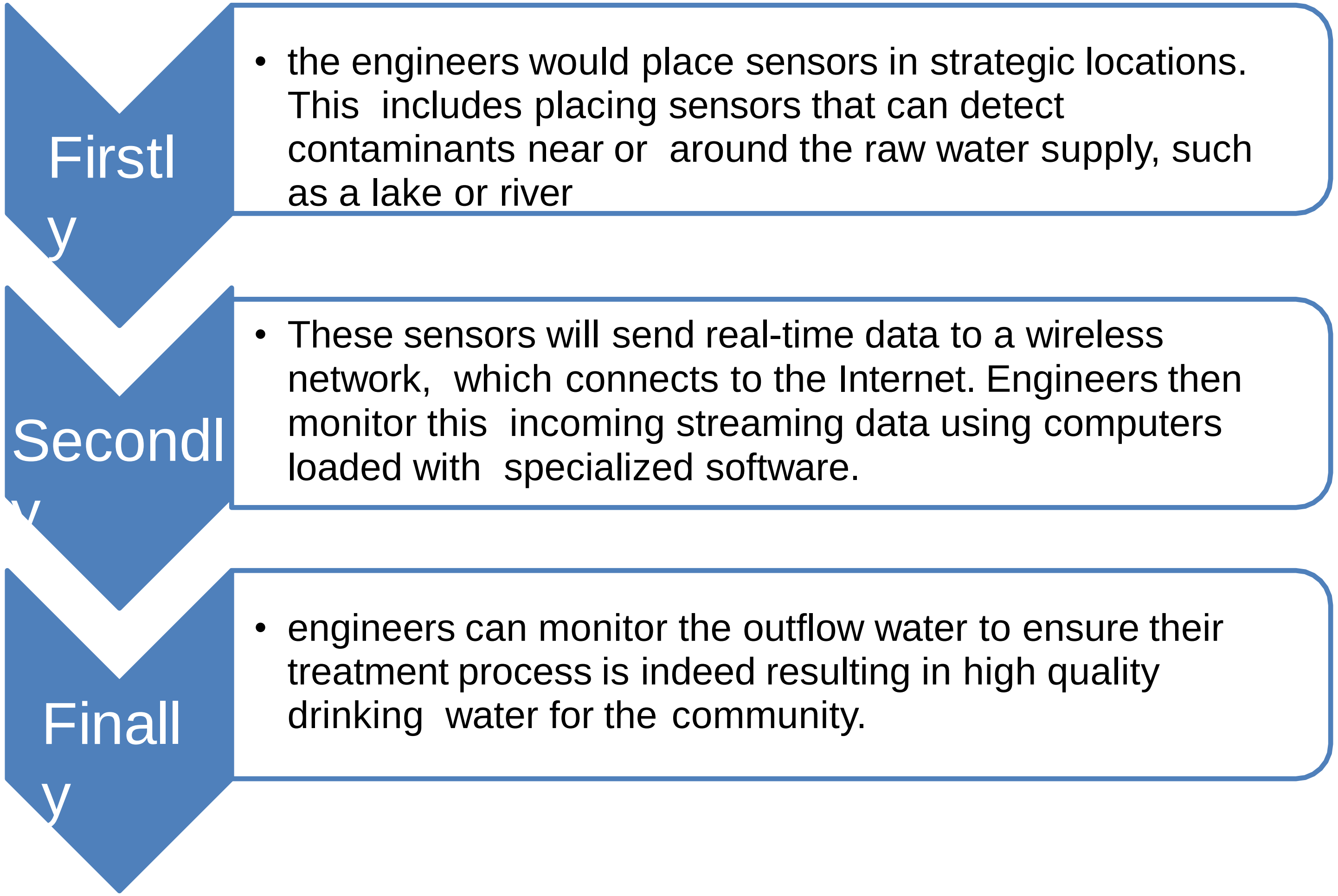
Making a machine-to-machine communications system work is a step-by-step process. The main elements involved are sensors (usually the kind that can send telemetry wirelessly), a wireless network and a computer connected to the Internet.

Contd...

Lets take the case of Water Treatment Faciltiy

City engineers are charged with supplying the community with fresh drinking water. They need to monitor the raw water supply, the treatment process and the end product, which is drinkable water.

WaterTreatment Facility



Firstl
y

- the engineers would place sensors in strategic locations. This includes placing sensors that can detect contaminants near or around the raw water supply, such as a lake or river

Secondl
y

- These sensors will send real-time data to a wireless network, which connects to the Internet. Engineers then monitor this incoming streaming data using computers loaded with specialized software.

Finall
y

- engineers can monitor the outflow water to ensure their treatment process is indeed resulting in high quality drinking water for the community.

Applications

Security

- surveillance applications Alarms

Transportation

- Toll payment, road safety,

E-Health

-remote patent monitoring

Manufacturing

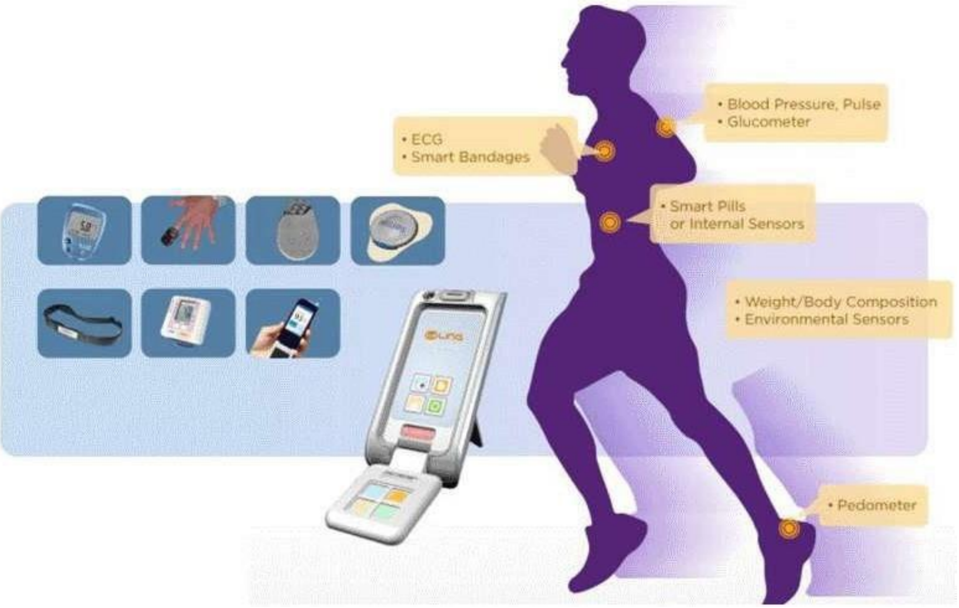
-production chain monitoing and automation

Applications - eHealth

Disease Management

Ageing independently

Personal Fitnes



Remote Monitoring

Health Chec

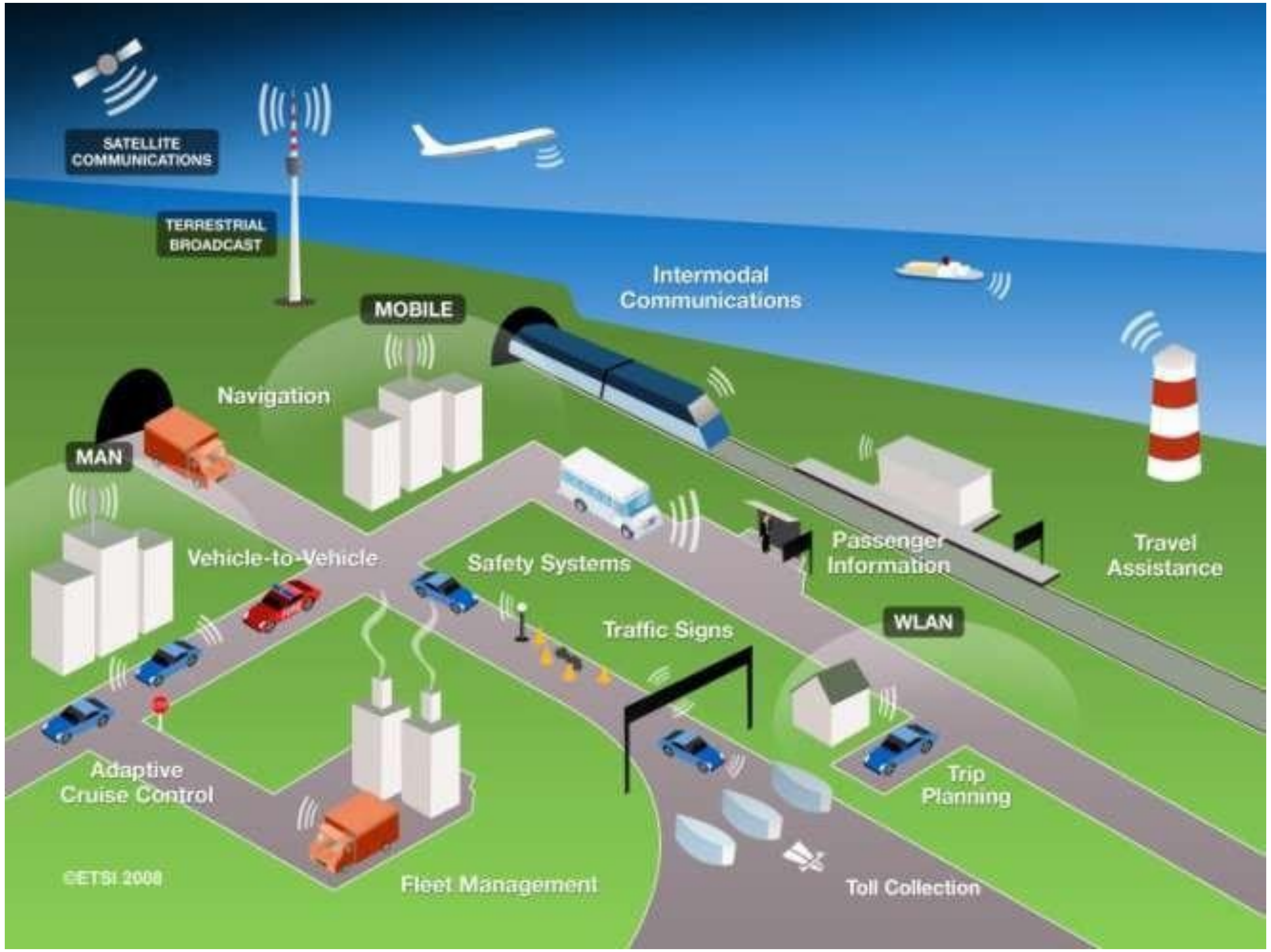
On-line health

Applications - Avoid Road Accidents

The possibilities for M2M communications seem virtually limitless. But one of the areas where M2M holds potential for the most transformative change is the automotive industry. The ability to share realtime information with a vehicle opens the door for a broad range of new and exciting applications that will make driving safer, more convenient, and more efficient.

An exciting area within M2M is the work going on within vehicular networks, including new work on vehicle-to-vehicle (V2V) communications.

Applications - Automotive



Use Cases for Automative application

Automative applications integration in M2M platform

V2V Communication

Wireless technology allows connected vehicles to communicate with one another, as well as the infrastructure around them and alert motorists of road conditions. Drivers can be alerted to dangerous road conditions, possible collisions, and hazardous curves using vehicle systems based on Dedicated Short Range Communications (DSRC). DSRC is a technology similar to Wi-Fi and connected vehicles could also "talk" or provide the driver with information regarding tolls, work zones, traffic signals, and school zones, giving relief to delays and other surprises that motorists face.

Benefits of V2V

Benefits of V2V communication technologies could be endless. A study by the NHTSA stated that connected vehicle technology could handle roughly 80% of crash scenarios involving non-impaired drivers.

Contd...

Source: U.S. DOT

Wireless Connectivity allows cars to be continuously aware of each other so when one car brakes suddenly cars several yards behind the vehicle get a safety warning before they get tooclose

Contd...

Connected vehicles can help to mitigate crashes on busy urban streets.