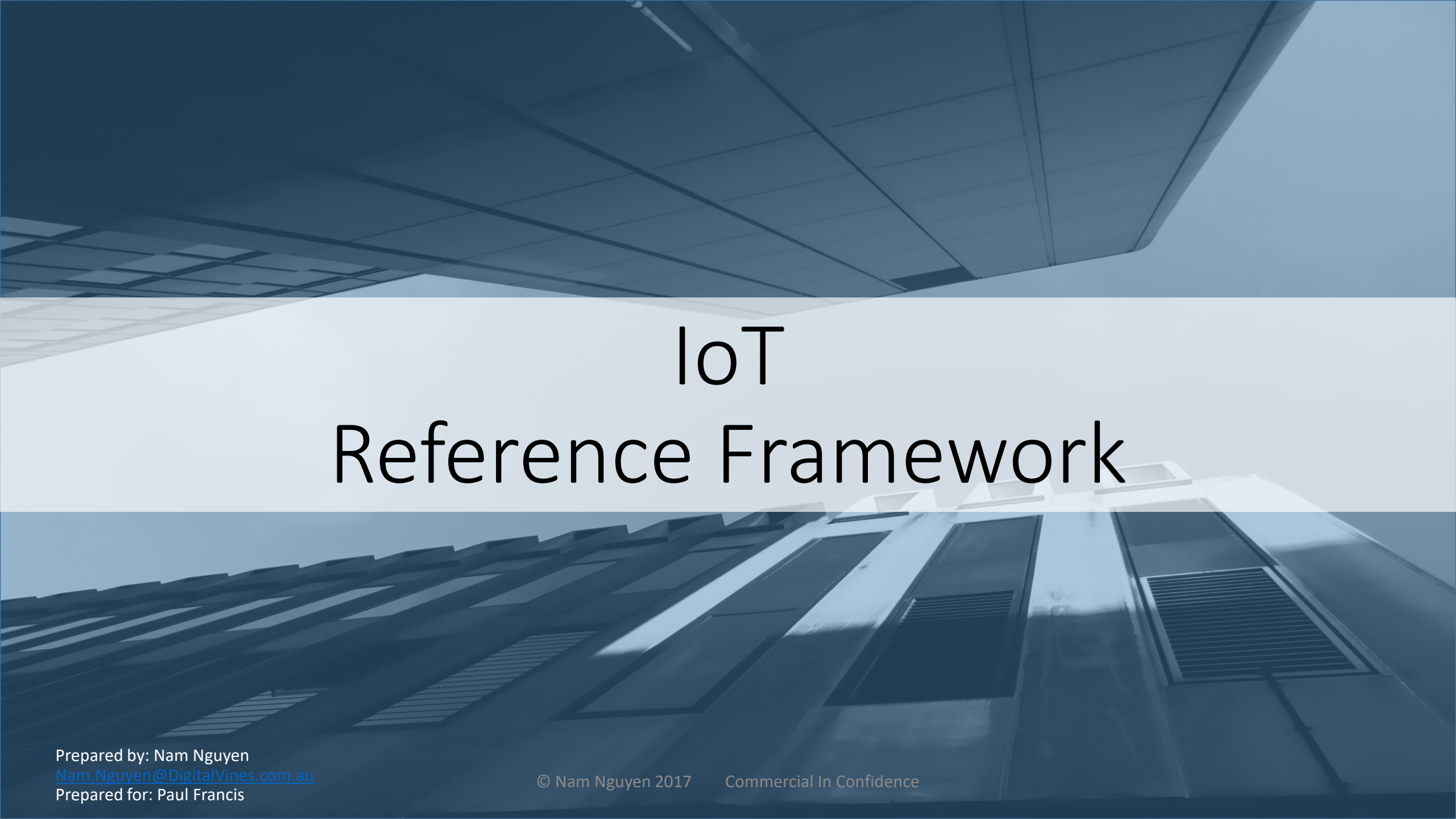


# IoT
# Reference Framework

Prepared by: Nam Nguyen
Nam.Nguyen@DigitalVines.com.au
Prepared for: Paul Francis

# General Use Restrictions



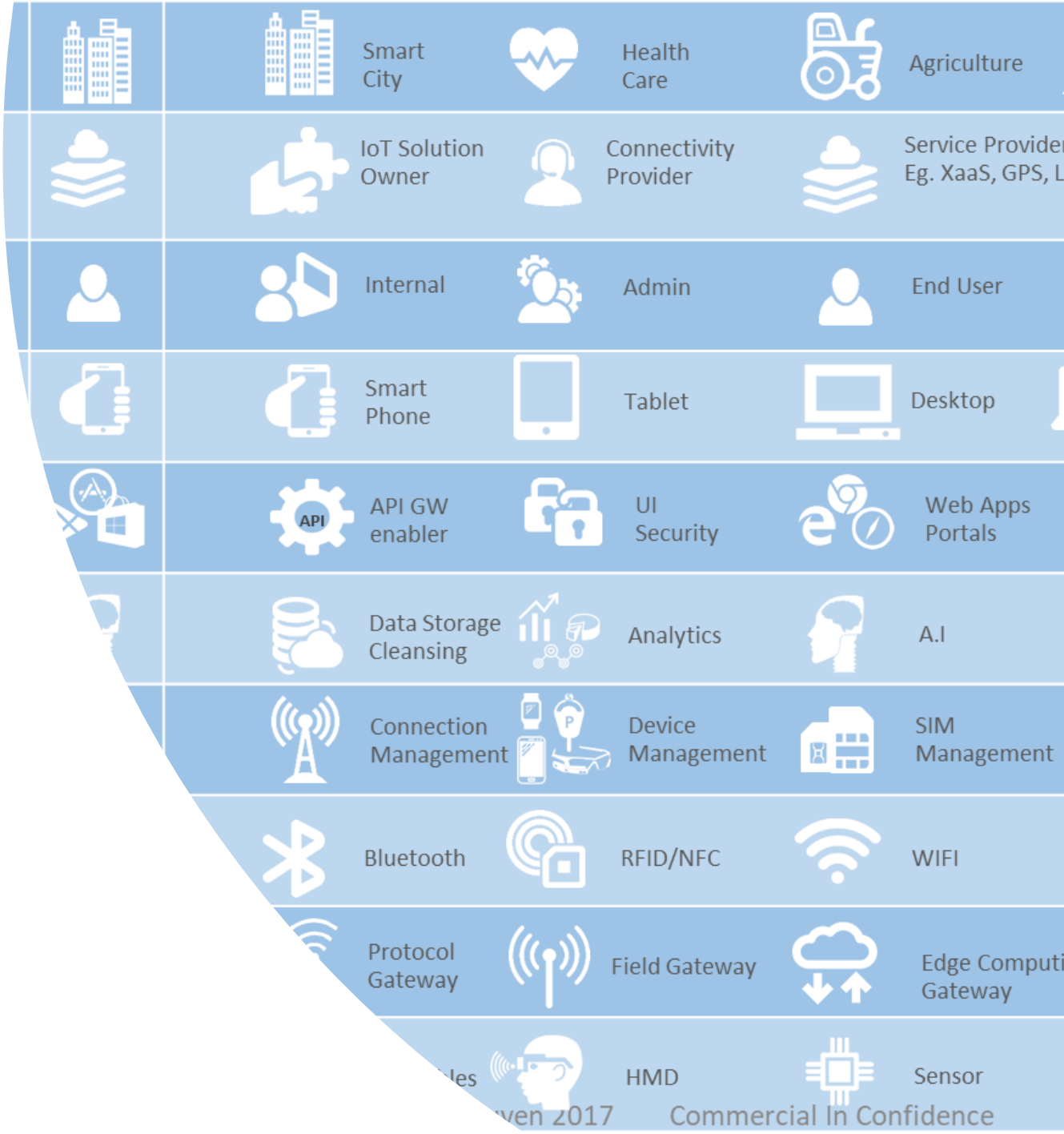
nam.nguyen@digitalvines.com.au

# IoT Reference Framework – Top Level

| | | | |
|---|---|---|---|
| 10 | IoT Industry Solution |  |  Smart City  Health Care  Agriculture  Manufacturing  Transport  Utility |
| 9 | Solution / Service Provider |  |  IoT Solution Owner  Connectivity Provider  Service Provider Eg. XaaS, GPS, Location, etc |
| 8 | IoT Users |  |  Internal  Admin  End User  Support |
| 7 | IoT User Interface |  |  Smart Phone  Tablet  Desktop  Laptop  HMD |
| 6 | Application Enablement |  |  API GW enabler  UI Security  Web Apps Portals  Mobile Apps |
| 5 | Intelligence Enablement |  |  Data Storage Cleansing  Analytics  A.I  ML  Block Chain |
| 4 | Connection Management |  |  Connection Management  Device Management  SIM Management  Identity Management  Networking: DNS, LB, VPN |
| 3 | Connectivity |  |  Bluetooth  RFID/NFC  WIFI  Wireless Cat-M1/NB1, Sigfox, LoRaWAN  Wired Ethernet  (Nano) Satellite |
| 2 | IoT Gateway |  |  Protocol Gateway  Field Gateway  Edge Computing Gateway |
| 1 | IoT EndPoint |  |  Wearables  HMD  Sensor  Connected Car  Smart Meter  Washing Machine |

# IoT Reference Framework – Top Level

- SIMPLE – 10 LAYERs
  - Applies to most, if not all, IoT solutions
  - A business and a solution build & deployment framework
- PRACTICAL
  - A self explanatory framework
  - IoT solution can be easily understood by using the framework
- PURPOSEFUL
  - Each layer can be expanded to include more / purposeful details to suit a wide range of users
- END-TO-END
  - Shows ecosystem, end-to-end
  - Identifies **value chain** players
- VALUE ADDING – provides a common language to
  - IoT solution users
  - Product and system vendors
  - Suppliers/Service providers
  - System Integrators



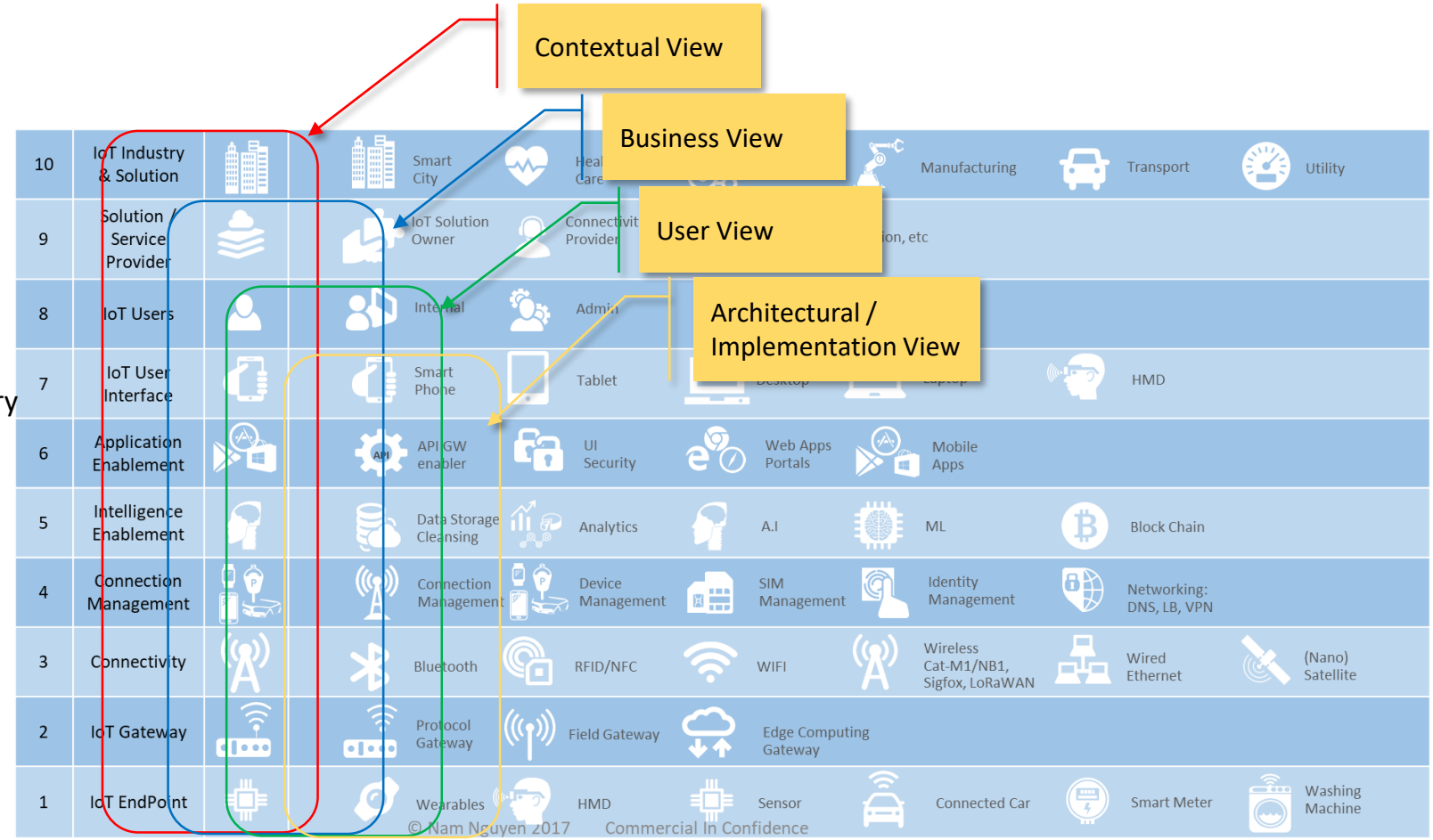


yen 2017 Commercial In Confidence

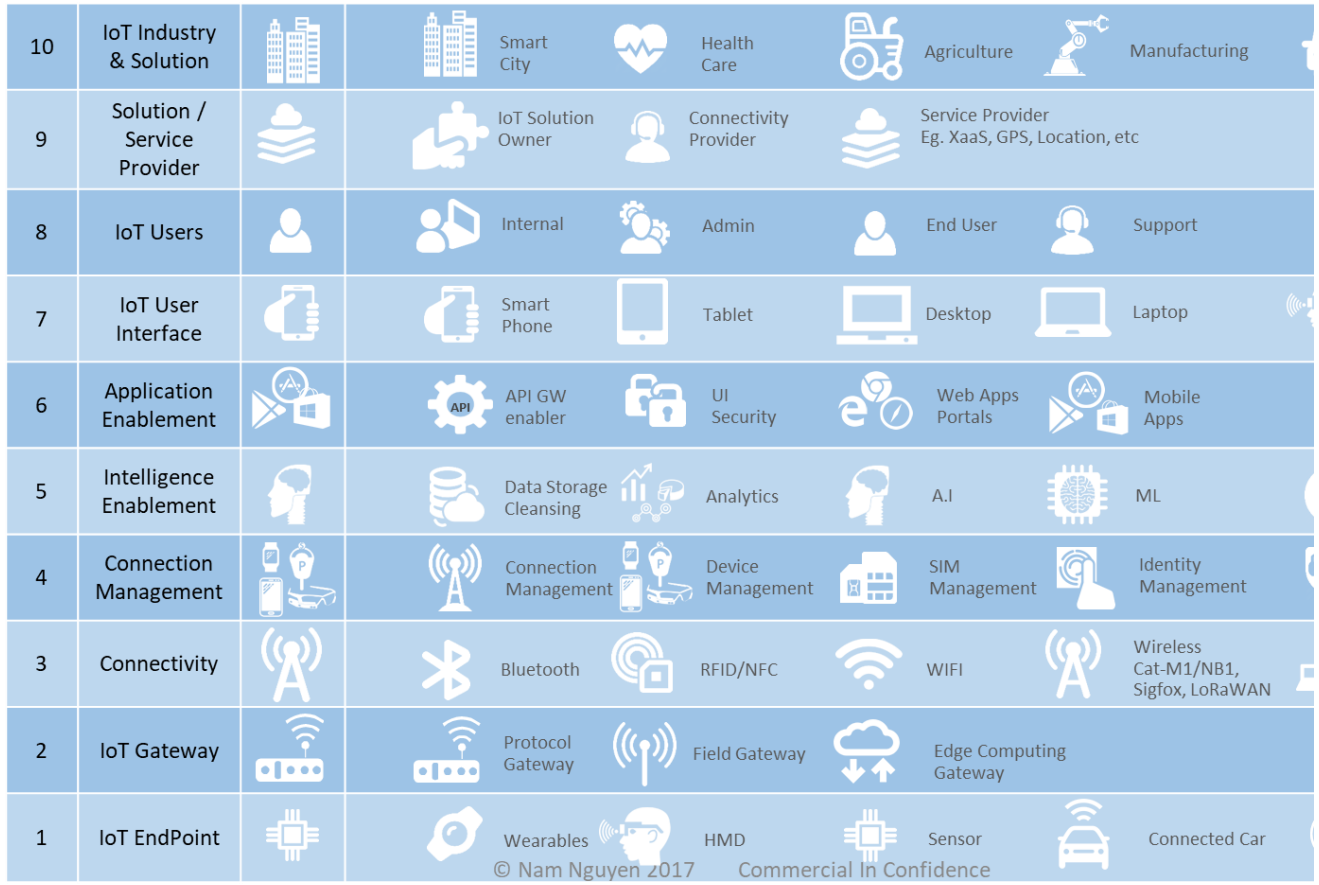
# IoT Reference Framework - Viewpoints

The IoT Reference Framework shows

- Contextual View
  - Industries, Markets, Solution, Revenue, Value Chain
  - Security, Risks, Regulations,
- Business View
  - Stakeholders, processes, policies, industry and regulatory compliance
- User View
  - Business, consumers, governments, communities
- Technical View
  - Solution
  - Architecture
  - Network
  - System
  - Sub-system (each layer)
  - Component (detailed view)



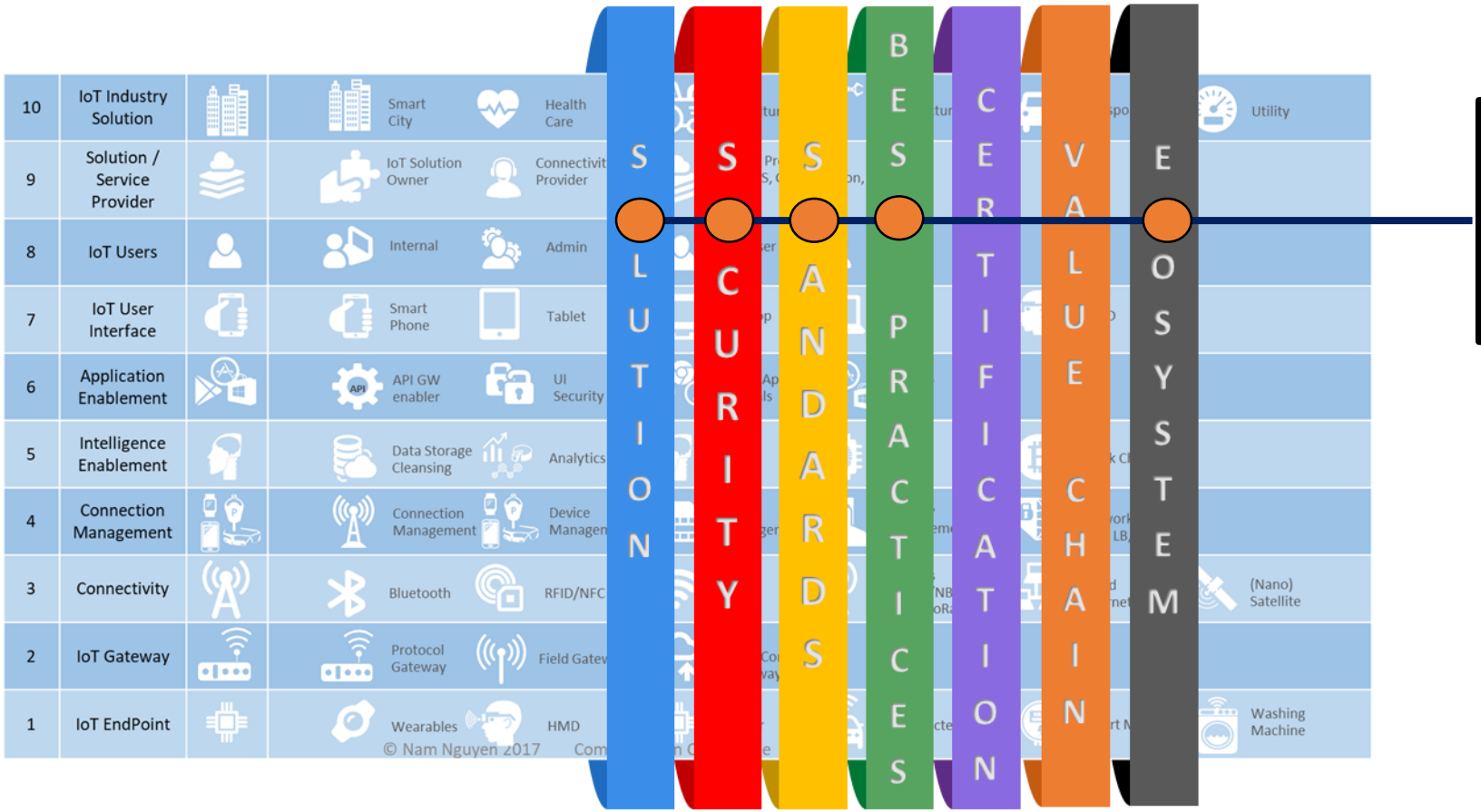
# IoT Reference Framework as a Collaboration Platform




Ideas for Collaboration

1. Definitions, References and Standards
2. Use Cases and Good Practices sharing
3. Security Guidelines
4. Industry Specific Information and Guidelines
5. Ecosystem of partners

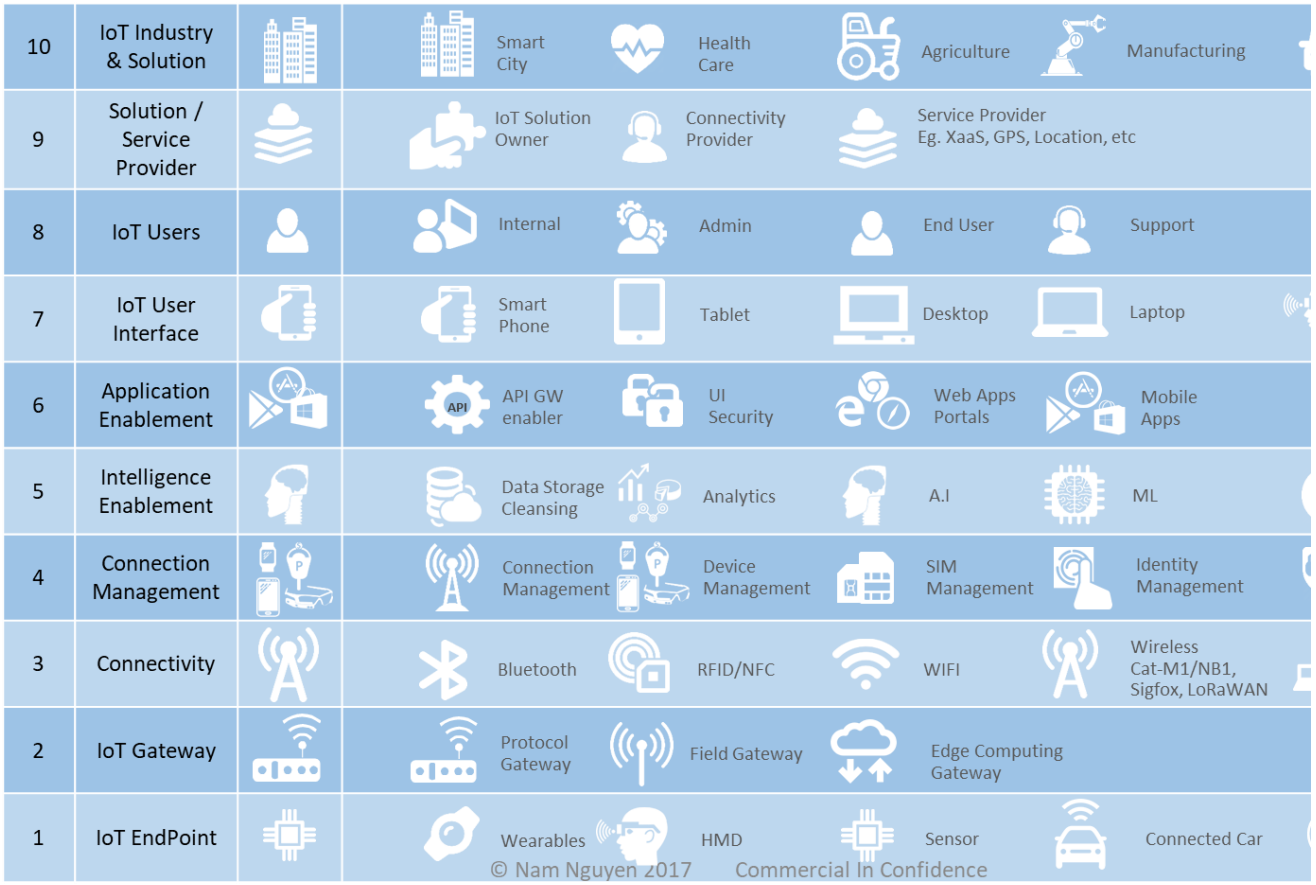
# IoT Reference Framework – Roadmap




The Roadmap includes collaboration functions discussed in the previous slide

# Collaboration Ideas

# IoT Reference Framework as a Collaboration Platform





1. Definitions, References and Standards
2. Use Cases and Good Practices sharing
3. Security Guidelines
4. Industry Specific Information and Guidelines
5. Ecosystem of partners

# Definitions, References & Standards

- Definitions
  - The IoT Reference Framework enables IoT users to contribute to the definitions of IoT terminologies, as one of the aims of the framework is to provide a common language to all.

- References and Standards – Body of Knowledge
  - Encourage users to add references relating to IoT standards, practices, and use cases, over time building up a body of knowledge that would benefit all

# IoT Definitions, References & Standards

- Allows IoT community to contribute to the definitions of terminologies, adding references and standards as appropriate.
- This can be done to each of the 10 layers in the framework
- Examples (see following slides) include:
  - Information on each of the IoT industries – to provides relevant inudstry information to solution owners, developers, etc
  - Connectivity technologies – to provide vendor-neutral, and correct information on available technologies, their benefits, pros and cons

# IoT Reference Framework – Industry & Solution

| | | |
|---|---|---|
| 10 | IoT Industry & Solution |  |
| 9 | Solution / Service Provider |  |
| 8 | IoT User |  |
| 7 | IoT User Interface |  |
| 6 | Application Management |  |
| 5 | Intelligence Enablement |  |
| 4 | Connection Management |  |
| 3 | Connectivity |  |
| 2 | IoT Gateway |  |
| 1 | IoT EndPoint |  |

| IoT Industry & Solution stack | |
|---|---|
| What | Stakeholder |
| **IoT Industry & Solution**<br>For each industry, provides context to the solution by considering the followings:<br>• Legals (regulation, policy, compliance)<br>• Security<br>• Market size estimate<br>• Growth and revenue projection<br>• Ecosystem players involved in said industry<br>• devices | IoT Solution owner<br>IoT device and end point manufacturer<br>IoT product owner<br>IoT software stack developer |

Provide industry description and context that would benefit the IoT community

# IoT Reference Architecture – Industry & Solution

| | | |
|---|---|---|
| 10 | IoT Industry & Solution |  |
| 9 | Solution / Service Provider |  |
| 8 | IoT User |  |
| 7 | IoT User Interface |  |
| 6 | Application Management |  |
| 5 | Intelligence Enablement |  |
| 4 | Connection Management |  |
| 3 | Connectivity |  |
| 2 | IoT Gateway |  |
| 1 | IoT EndPoint |  |

| IoT Industry & Solution stack | |
|---|---|
| **SMART CITIES** | Solutions include Connected Street Lighting, Smart Bin, Smart Parking, Smart Parks, Smart Building, etc. There's no one definition of what a Smart City includes, and it's really up to each city to define its own Smart City Framework, one that suits a city's best interests. |
| **AGRICULTURE** | Solutions in this category could include anything from farming, to livestock to aquaculture. Typical solutions today include temperature and humidity sensing, soil moisture sensing, and so on. |
| **HEALTHCARE** | Smart Healthcare solutions covers anything from family healthcare, community health, personal care to age care, and disability. Typical solutions includes in-home age care, tracking for disability and dementia clients. |
| **TRANSPORT** | Anything from traffic, road condition, vehicle to vehicle/X, drone, intelligent transport system, etc. |
| **UTILITY** | Definition of this industry includes Gas, Water, Electricity, alternative Energy, etc. Examples of Utility solutions Smart Water leakage detection and monitoring. |
| **MANUFACTURING** | Manufacturing has been pioneering M2M, or IoT for quite sometimes with automation in their manufacturing process, and this trend will continue, especially under the umbrella term Industry 4.0 |
| **EDUCATION** | Probably a ripe area for disruption, though solutions in this sector are more the result of enabling smarter digital solutions, rather than a direct implementation of IoT solution. |
| **ENTERTAINMENT** | Evidently seen more from the children sector with devices that can track a child |

# IoT Reference Framework – Connectivity

| | |
|---|---|
| 8 | IoT User |
| 7 | IoT User Interface |
| 6 | Application Management |
| 5 | Intelligence Enablement |
| 4 | Connection Management |
| 3 | Connectivity |
| 2 | IoT Gateway |
| 1 | IoT EndPoint |



## IoT Connectivity

| What | Stakeholder |
|---|---|
| The **Connectivity Network** stack provides the connection between end-point/gateway devices and IoT core platforms. Connectivity technologies includes Bluetooth, WiFi, NFC, RFID, Ethernet, 6LoPAN, LoRaWAN, Sigfox, 3G/4G LTE, LTE-M (Cat-M1), NB-IoT (Cat-NB1) and other proprietary radio technologies; This layer should also represent **Access Network** for IoT client devices which could be WiFi, Ethernet, and or 3G/4G LTE. | IoT Connectivity provider<br>IoT Solution owner<br>IoT Solution / Managed Service operator<br>IoT solution architect |

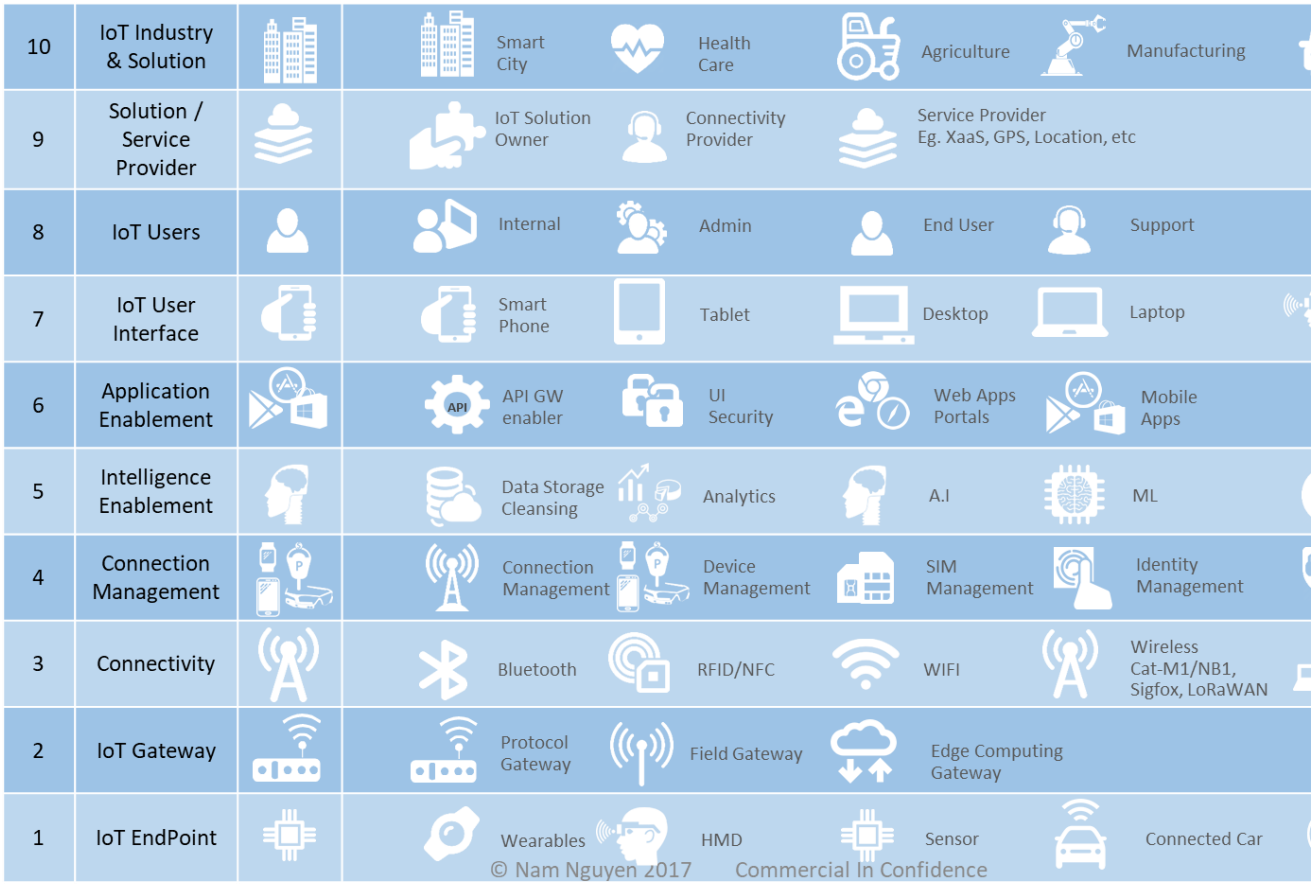
| | |
|---|---|
| 8 | IoT User |
| 7 | IoT User Interface |
| 6 | Management |
| 5 | Intelligence Enablement |
| 4 | Connection Management |
| 3 | Connectivity |
| 2 | IoT Gateway |
| 1 | IoT EndPoint |

# IoT Reference Framework – Connectivity

Example: Provides vendor-neutral explanations of IoT Connectivity Technologies by describing
The different types of connectivity technologies available, their pros and cons, and
Their suitability for certain applications

| IoT Connectivity | |
|---|---|
| **WIRELINE** | eg. Ethernet, Modbus, powerline, etc. |
| **WPAN** | Wireless Personal Area Network – Bluetooth, 6LoWPAN, RFID, NFC, Z-Wavw, ZigBee, wireless USB,etc |
| **WLAN** | Wireless Local Area Network – WiFI, DECT |
| **LPWAN** | Low Power Wide Area Network technologies such as Sigfox, LoRaWAN, Cat-M1, Cat-NB1, Weightless-P, etc. |
| **WWAN** | Wireless Wide Area Network – GPRS, 3G, 4G, LTE, CAT-1, 5G, etc. |

# IoT Reference Framework as a Collaboration Platform






1. Definitions, References and Standards
2. Use Cases and Good Practices sharing
3. Security Guidelines
4. Industry Specific Information and Guidelines
5. Ecosystem of partners

# Use Cases

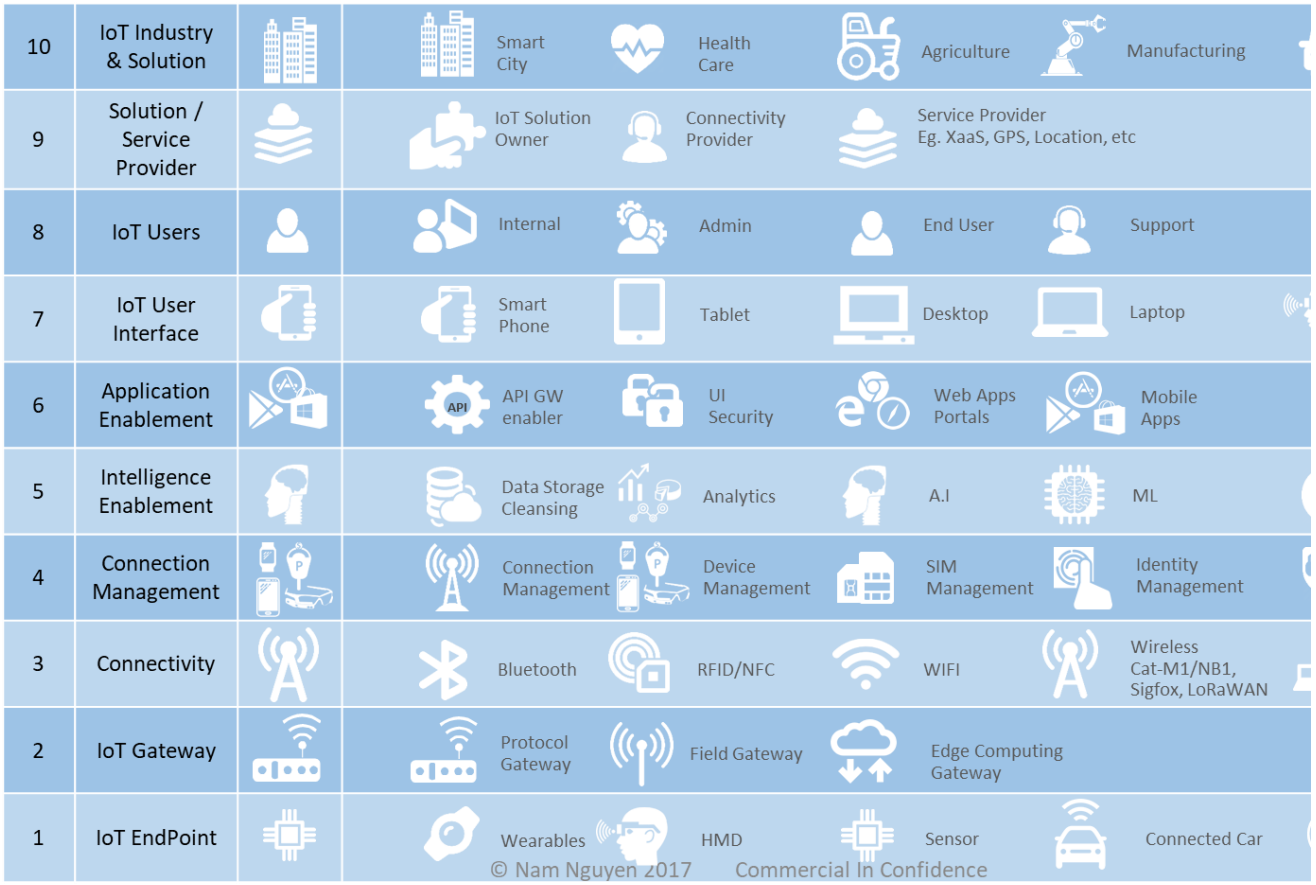
- Encourage IoT users to contribute their Use Cases. Over time, this will create a rich depository of valuable real life IoT use cases that will benefit everyone

- See example Use Case on the next slide

# IoT Use Case – Healthcare

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 10 | IoT Industry & Solution |  | HealthCare | Patient Monitoring | | | |
| 9 | Solution / Service Provider |  | Solution Provider | Private PaaS | ISP Provider | Hospital Solution Owner | |
| 8 | IoT Users |  | Physician | Nurse | Patient | Hospital | Smart Health Provider/Insurance |
| 7 | IoT User Interface |  | Personal smart device | | | | |
| 6 | Application Enablement |  | | Mobile Apps | UI Security | | |
| 5 | Intelligence Enablement |  | Data Storage Analytics | | | | |
| 4 | Connection Management |  | Connection Management | Device Management | Identity Management | | |
| 3 | Connectivity |  | Fixed Broadband ISP / NBN | | | | |
| 2 | IoT Gateway |  | Connection Gateway | | | | |
| 1 | IoT EndPoint |  | Body Temperature sensor | Vital signs | Blood pressure | | |

# IoT Reference Framework as a Collaboration Platform






1. Definitions, References and Standards
2. Use Cases and Good Practices sharing
3. Security Guidelines
4. Industry Specific Information and Guidelines
5. Ecosystem of partners

# IoT Security

- To provide a guideline to identify and assess security vulnerabilities based on the framework
- See following slides as examples

# IoT Security Architecture Framework

| | | | IoT Architecture Stack | Security (CIA) | Safety | Reliability | Resiliency | Privacy |
|---|---|---|---|---|---|---|---|---|
| | | | | | TRUST WORTHINESS FRAMEWORK | | | |
| 10 | IoT Industry & Solution |  | | | | | | |
| 9 | Solution / Service Provider |  | | | | | | |
| 8 | IoT User |  | | | | | | |
| 7 | IoT User Interface |  | | | | | | |
| 6 | Application Enablement |  | | | | | | |
| 5 | Intelligence Enablement |  | | | | | | |
| 4 | Connection Management |  | | | | | | |
| 3 | Connectivity |  | | | | | | |
| 2 | IoT Gateway |  | | | | | | |
| 1 | IoT EndPoint |  | | | | | | |

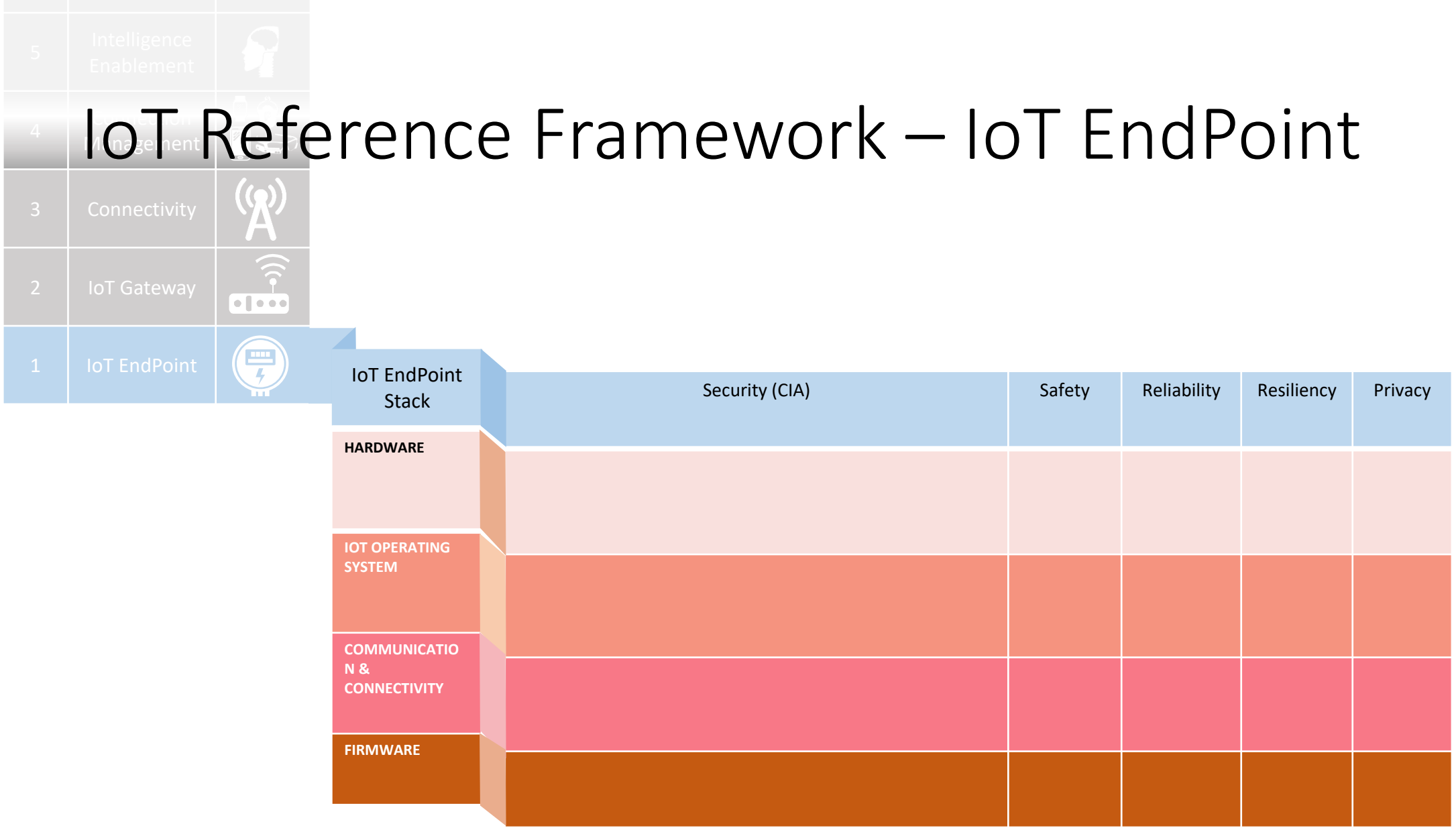
# IoT Reference Framework – IoT EndPoint

| | |
|---|---|
| 5 | Intelligence Enablement |
| 4 | Management |
| 3 | Connectivity |
| 2 | IoT Gateway |
| 1 | IoT EndPoint |



| IoT EndPoint Stack | |
|---|---|
| **HARDWARE** | MCU, Sensors, actuators, controllers, interfaces, SIM card, IoT module |
| **IOT OPERATING SYSTEM** | "many devices will run with 'bare metal', but some will have embedded or real-time operating systems that are particularly suited for small constrained devices, and that can provide IoT-specific capabilities" (from the Eclipse Foundation) |
| **EMBEDDED SOFTWARE (FIRMWARE)** | a software that is embedded in the hardware, and that enables a specific function(s) to be performed, such as remote management, security agent, at start up. |
| **COMMUNICATION & CONNECTIVITY** | Drivers and protocols required to support device connectivity (bluetooth, Z-Wave, RFID, Wifi, Ethernet, Sigfox, LoRaWAN, Cat-M1/NB1, etc.) and communication protocols such as MQTT, CoAP, HTTP, etc. |

# IoT Reference Framework – IoT EndPoint



# IoT Reference Framework – IoT EndPoint

| | |
|---|---|
| 5 | Intelligence Enablement |
| 4 | Management |
| 3 | Connectivity |
| 2 | IoT Gateway |
| 1 | IoT EndPoint |



| IoT EndPoint Stack | Security | Safety | Reliability | Resiliency | Privacy |
|---|---|---|---|---|---|
| HARDWARE | **1. Device Identity & Management** – How is device identity assigned? How do you know you are talking to the right device? (if the device or part of the device has been replaced by some other device?) | | | | |
| IOT OPERATING SYSTEM | **5. Device Identity & Authentication** – Will your device's unique ID be used for authentication? Can it be cloned? In the cellular world, each mobile phone has a IMEI, which is uniquely identifies the device type, model and firmware level. The device can be black listed if stolen. | | | | |
| COMMUNICATION & CONNECTIVITY | | | | | |
| FIRMWARE | | | | | |

Example questions only

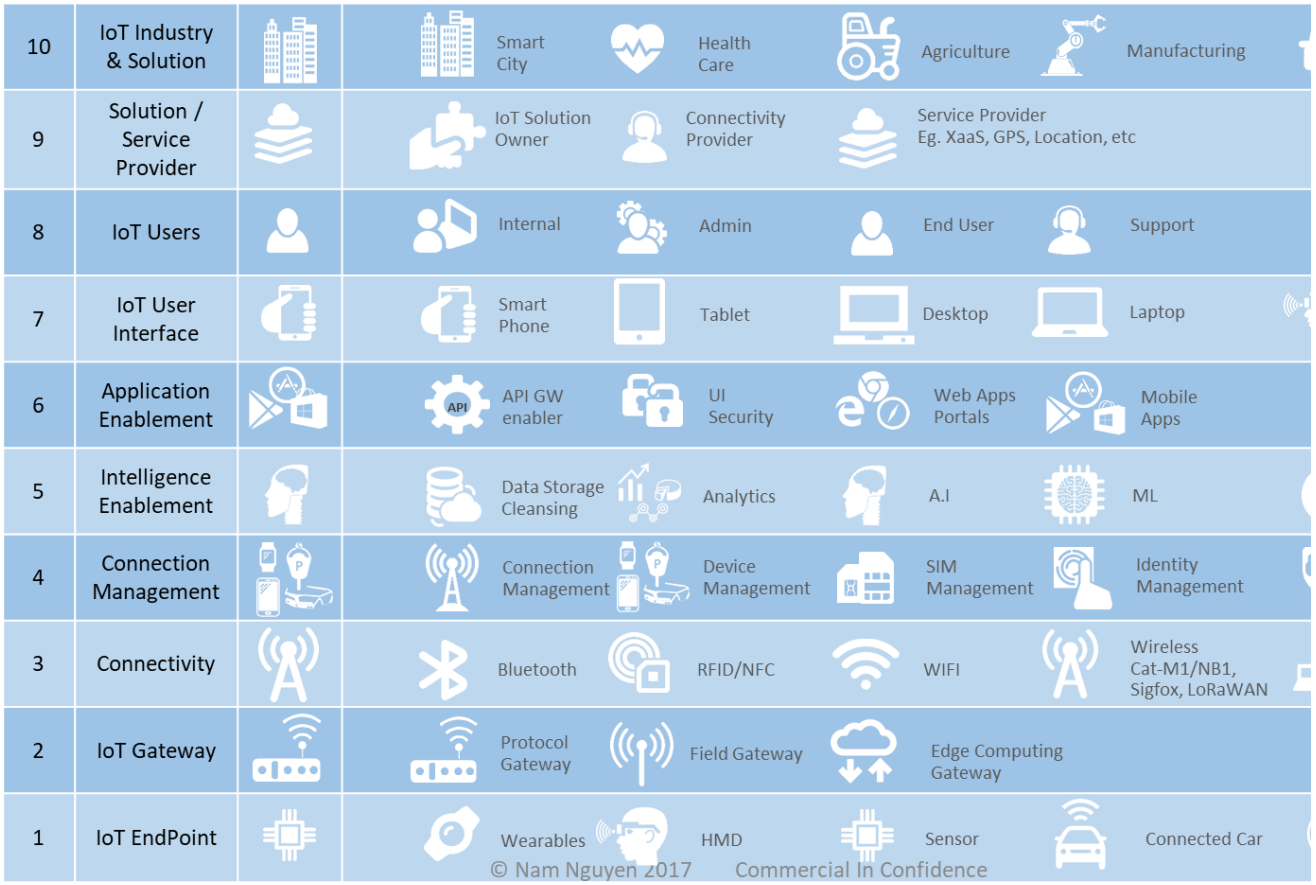
# IoT Reference Framework – IoT EndPoint

| | | |
|---|---|---|
| 5 | Intelligence Enablement |  |
| 4 | Management |  |
| 3 | Connectivity |  |
| 2 | IoT Gateway |  |
| 1 | IoT EndPoint |  |

| IoT EndPoint Stack | Security | Safety | Reliability | Resiliency | Privacy |
|---|---|---|---|---|---|
| HARDWARE | **1. Device Identity & Management** | **2. Tampering** | 8. **HW Lifecycle Management** – Is there a process for managing device HW/SW lifecycle? How would you ensure device is available when it comes to end of life? | | |
| IOT OPERATING SYSTEM | **5. Device Identity & Authentication** | **4. Data Storage** | | | |
| COMMUNICATION & CONNECTIVITY | | | | | |
| FIRMWARE | | | | | |

Example questions only

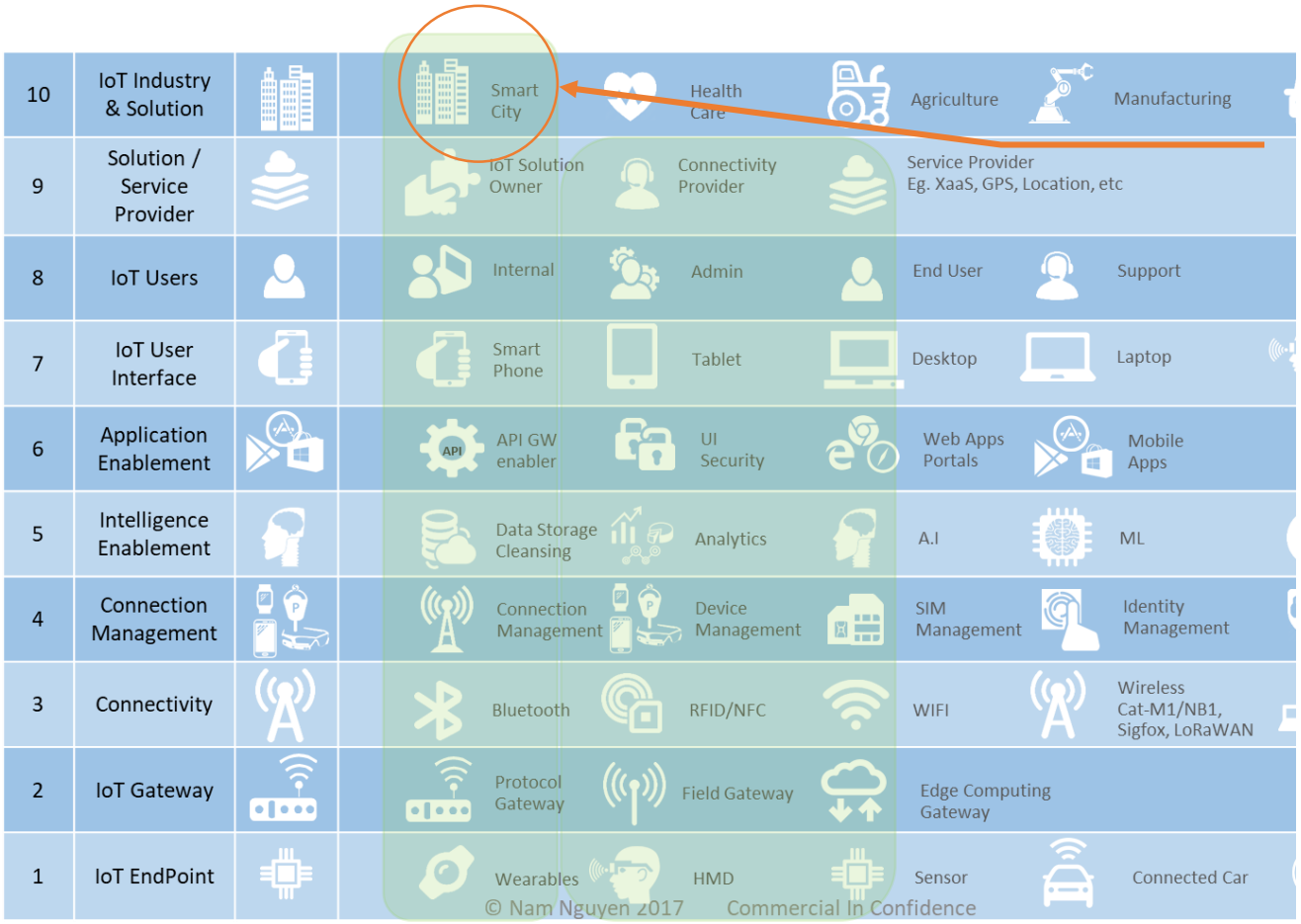
# IoT Reference Framework as a Collaboration Platform





1. Definitions, References and Standards
2. Use Cases and Good Practices sharing
3. Security Guidelines
4. Industry Specific Information and Guidelines
5. Ecosystem of partners

# Industry Specific Info & Guidelines




The framework could be used describe a specific IoT industry, eg.

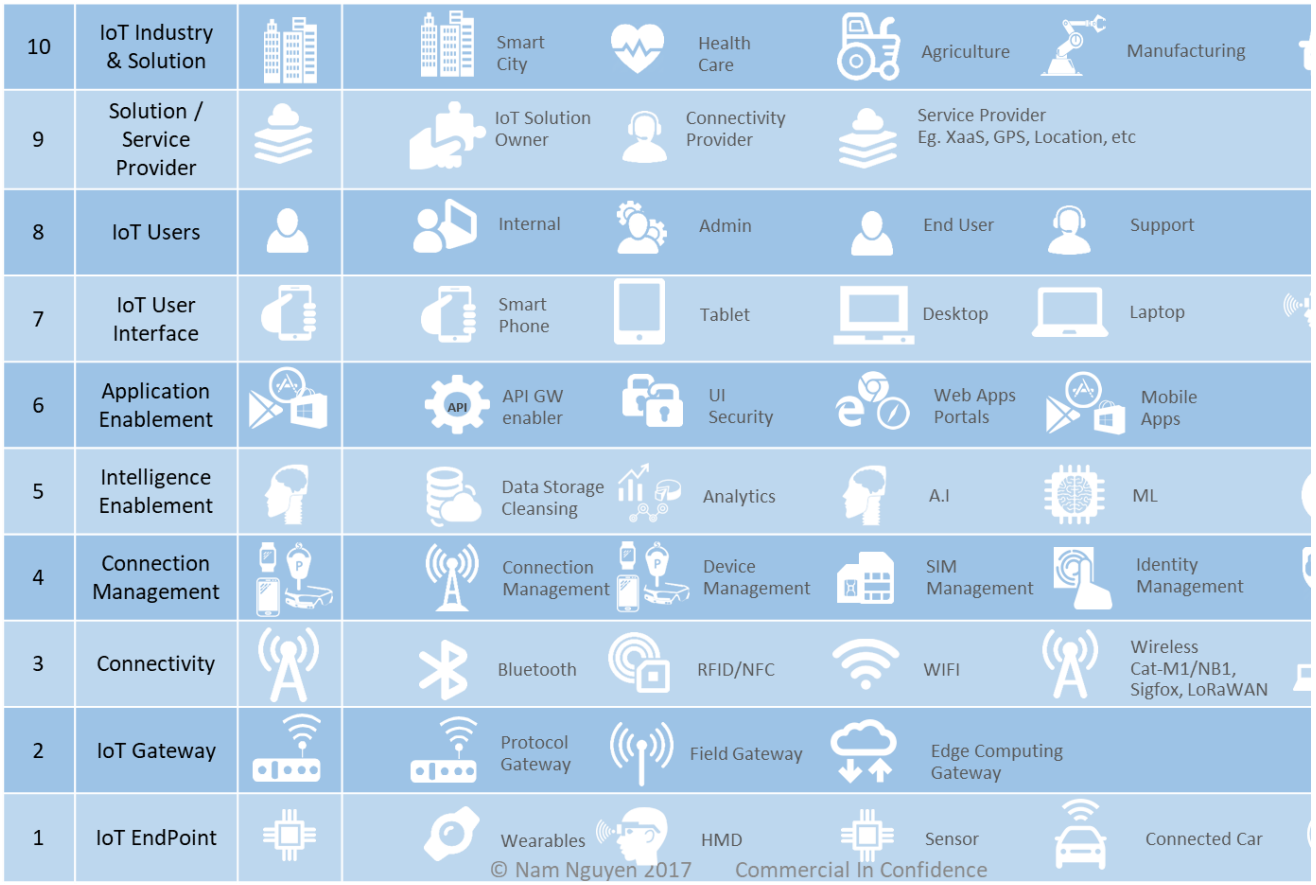
- Smart Cities

And would benefits those who practice, Or manage Smart Cities solutions only.



© Nam Nguyen 2017 Commercial In Confidence

# IoT Reference Framework as a Collaboration Platform






1. Definitions, References and Standards
2. Use Cases and Good Practices sharing
3. Security Guidelines
4. Industry Specific Information and Guidelines
5. Ecosystem of partners

# Ecosystem of Partners

- An ecosystem for a specific industry, or for all industries could be created based on this framework, one which could provide
  - Trusted ecosystem suppliers
  - A market place for sellers and buyers