



IOT REFERENCE FRAMEWORK

Enabler WorkStream #3

CYBERSECURITY & NETWORK RESILIENCE

IOT ALLIANCE AUSTRALIA

V1.0

November 2018

Nam Nguyen & Matt Tett



- is applicable to any IoT solution architectures; and
- takes into consideration end-to-end solution aspects, including IoT endpoints, connectivity, network, user, platform, application, solution and ecosystem.



























































- It provides a ‘common language’ to facilitate discussions amongst the IoT community;
- It provides factual, vendor-neutral information on end-to-end IoT building blocks; and
- It assists organisations to clearly and simply document and articulate their IoT solution requirements

v1.0 11/2018





IoT Reference Framework – Overview

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	 Visualisation	
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

© Copyright 2018 – INFYRA www.infyra.net / IOT ALLIANCE AUSTRALIA www.iot.org.au



IoT Reference Framework – Overview

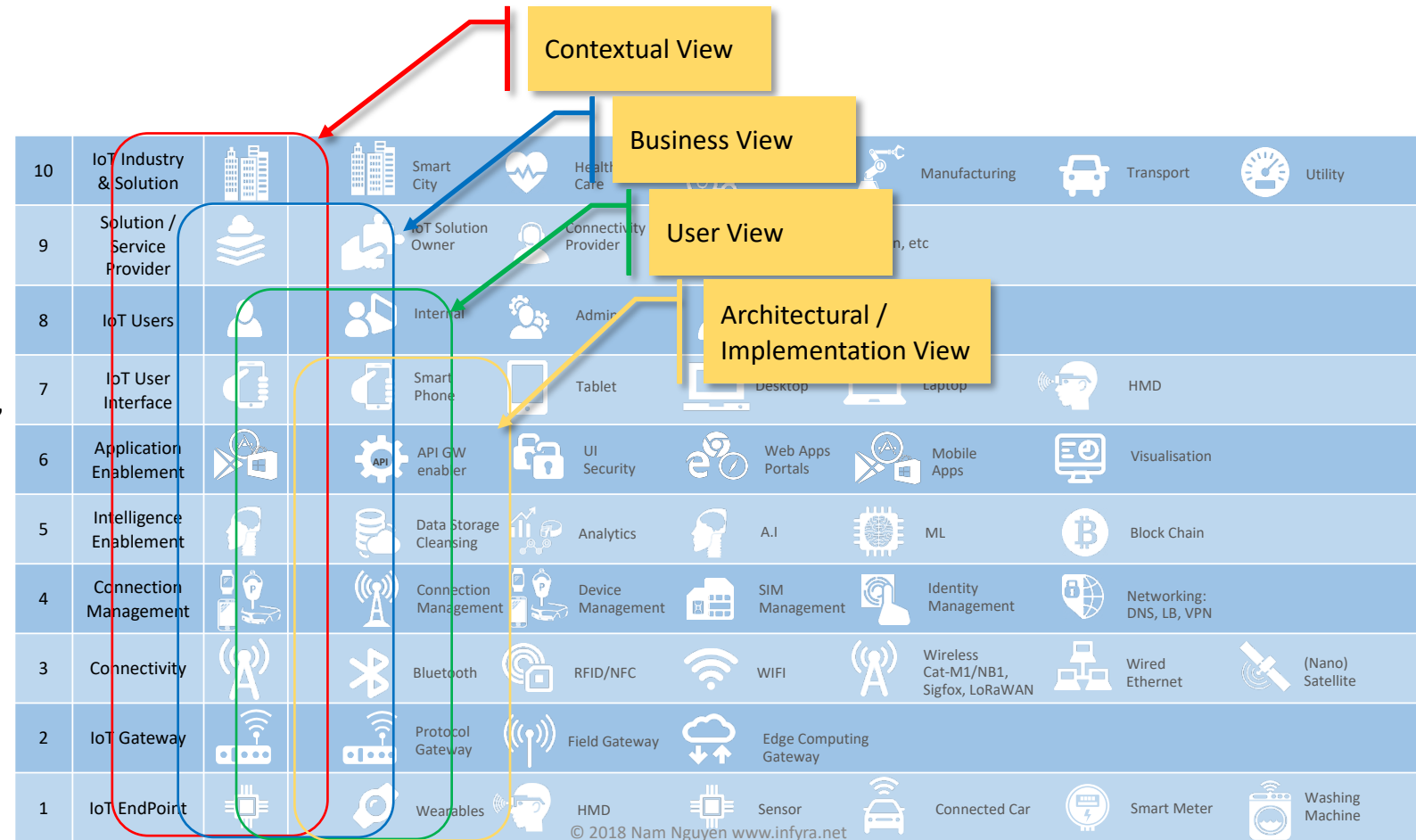


10	IoT Industry & Solution		IoT industry & solution layer provides the context for an IoT solution such as industry segment (industrial, consumer, enterprise) and its many implications such as security, regulations, supply chain, etc.
9	Solution / Service Provider		IoT Solution Owner / Service Provider – This layer provides the business perspective of an IoT solution. This layer should clearly indicate all IoT ecosystem stakeholders involved in the IoT solution, such as Solution Owner/Operator (business, enterprise, government) and Service Provider. Identifying all the stakeholders allows the underlying complexity in any IoT solution to be managed end-to-end, including: security, privacy, data integrity, solution resiliency, availability, processes, and resources.
8	IoT Users		IoT User – This layer identifies the type of IoT users who interact directly or indirectly with the IoT Solution. Users can be categorised as Primary or Secondary . Primary users are IoT solution owners which act upon the information produced by the solution. Secondary users are such as those who operate and manage the solution, or have a business interest in the solution. This layer helps the IoT solution owner identify who the real customers are.
7	IoT User Interface		IoT User Interfaces – shows standardised or specific types of devices / User Interface that enable access and or manage of the IoT system and devices. IoT Client Device can be a Desktop, Laptop, Tablet, Smart Phone, Wearables, or purpose-made devices .
6	Application Enablement		The Application Enablement layer, refers to a set of functions and foundational services such as the API enabler, Web Portal, Web & Mobile application building and enablement, User Interface Security, Developer services, etc. This layer enables both the business user and developer interfaces. This layer forms one part of what is commonly referred to as the ' IoT Platform '.
5	Intelligence Enablement		The Intelligence (Smart) Enablement layer refers to the use of smart technologies and/or techniques such as Analytics, Artificial Intelligence, Machine Learning, Deep Learning, Block Chain, etc. in order to produce insightful outcomes and to drive smart actions. The functions in this layer enable IoT solutions to be truly smart solutions. This layer forms another part of what is commonly referred to as the ' IoT Platform '.
4	Connection Management		The Connection Management layer specifies a set of the IoT Core functions , e.g., Connection Management, which refers to the management of networks, protocols, device/gateway management, ID management, User Authentication, etc. This layer forms the final part of what is commonly referred to as the ' IoT Platform '.
3	Connectivity		The Connectivity layer provides the network connection between end-point/gateway devices and IoT core platforms. This layer supports connectivity technologies Bluetooth, WiFi, NFC, RFID, Ethernet, 6LoPAN, LoRaWAN, Sigfox, Weighless-D, 3G/4G LTE, LTE-M (Cat-M1), NB-IoT (Cat-NB1) and other proprietary radio technologies; This layer also represents (Internet) Access Network for IoT client devices, which could be fixed or mobile broadband, as well as connectivity to ISP.
2	IoT Gateway		IoT Gateway layer represents 1) the Aggregation Point for a group of sensors and actuators to coordinate the connectivity of these devices to each other and to an external network such as a connectivity network; 2) a Protocol Gateway that performs protocol conversion between devices and the core platform; and/or 3) a Edge Computing Gateway that performs a subset of functions from layer 4, 5 and 6 above, such as data storage, analytics, ML, etc.
1	IoT EndPoint		IoT End Point (EP) layer represents end point devices that can be remotely managed. These endpoints can either be simple, stand-alone device such as wearables, sensors, etc, or a complex product that has a single or multiple endpoints embedded in it. The IoT End Point layer can be further expanded into an architectural functional stack comprising: hardware such as sensors and actuators, IO devices, MCU; Operating System, Hardware abstraction layer, Firmware; etc.

IoT Reference Framework – Views

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
 - Organisations, consumers, governments, communities
- Architectural View
 - Solution, architecture, network, system, sub-system (each layer), component (detailed view)

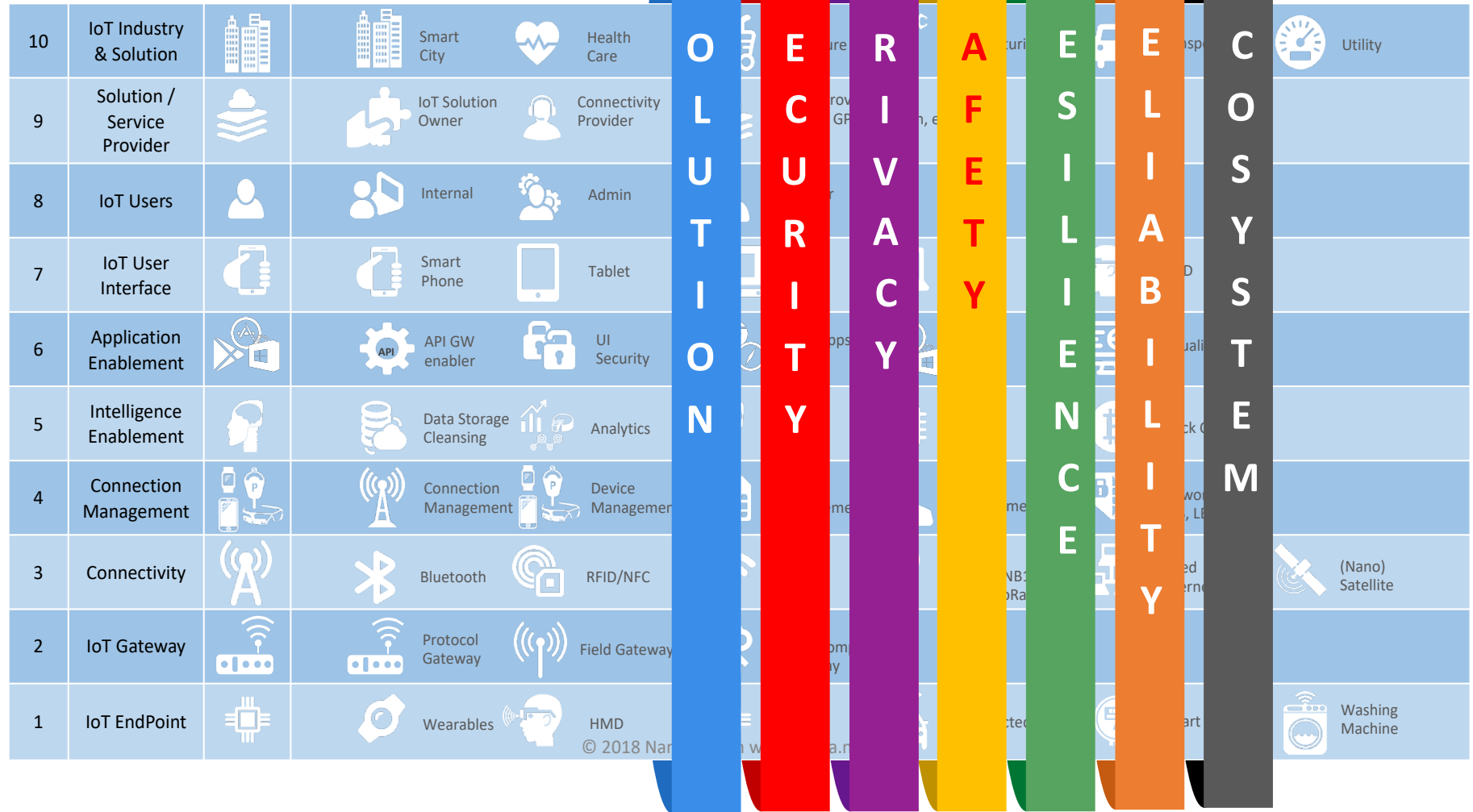


IoT Reference Framework – Applications

The IoT Reference Framework can be used to understand:

- the solution;
- security;
- privacy;
- safety;
- resilience;
- reliability;
- the ecosystem;
- and more

from and end-to-end perspective across the entire IoT solution.





Acknowledgements

This IoT Reference Framework was developed by

Nam Nguyen
Principal Consultant

INFYRA



www.infyra.net

nam@infyra.net

The IoT Reference Framework was further refined with contributors from

Members of Enabler Workstream 3
Cybersecurity & Network Resilience

IoT ALLIANCE AUSTRALIA



www.iot.org.au

The development of this IoT Reference Framework was influenced by foundational work by the organisations below. For a complete reference, refer to the document IoT Reference Framework – Application Guide

- The Industrial Internet of Things, Volume G1: Reference Architecture by the Industrial Internet Consortium, IIC. <https://www.iiconsortium.org/IIRA.html>
- NIST initiatives in IoT, <https://www.nist.gov/itl/applied-cybersecurity/nist-initiatives-iot>. In particular the following documents
 - Cybersecurity framework
 - Network of Things SP800-183
 - Low Power Wide Area IoT
- Digitising the Industry Internet of Things Connecting the Physical, Digital and Virtual Worlds
- Towards a definition of the Internet of Things (IoT), Revision 1, IEEE, <https://iot.ieee.org/definition.html>
- This IoT reference framework is inspired by the IT reference framework, created by Richard Diver www.rdiver365.com

Terms of Use

This work is licensed under a [Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-nc-sa/4.0/).



The IoT Reference Framework is available for non-commercial use by organisations and individuals, for purposes of communications, IoT architecture references, documentation, capability assessment, etc.

The use of this IoT Reference Framework for commercial purposes, such as marketing, advisory services, consulting tools, etc. for financial gains are not permitted, and subject to IP licensing.

Please contact [INFYRA](#) if you want to use this IoT Reference Framework for commercial purposes.

Copyright © 2018 Nam Nguyen Infyra