IoT Reference Framework

IoT Alliance Australia

Enabler Workstream #3 Cybersecurity & Network Resilience

Version 1.3
August 2022

eWS#3 Workstream Chair: Matt Tett
eWS#3 Workstream Author: Nam Nguyen

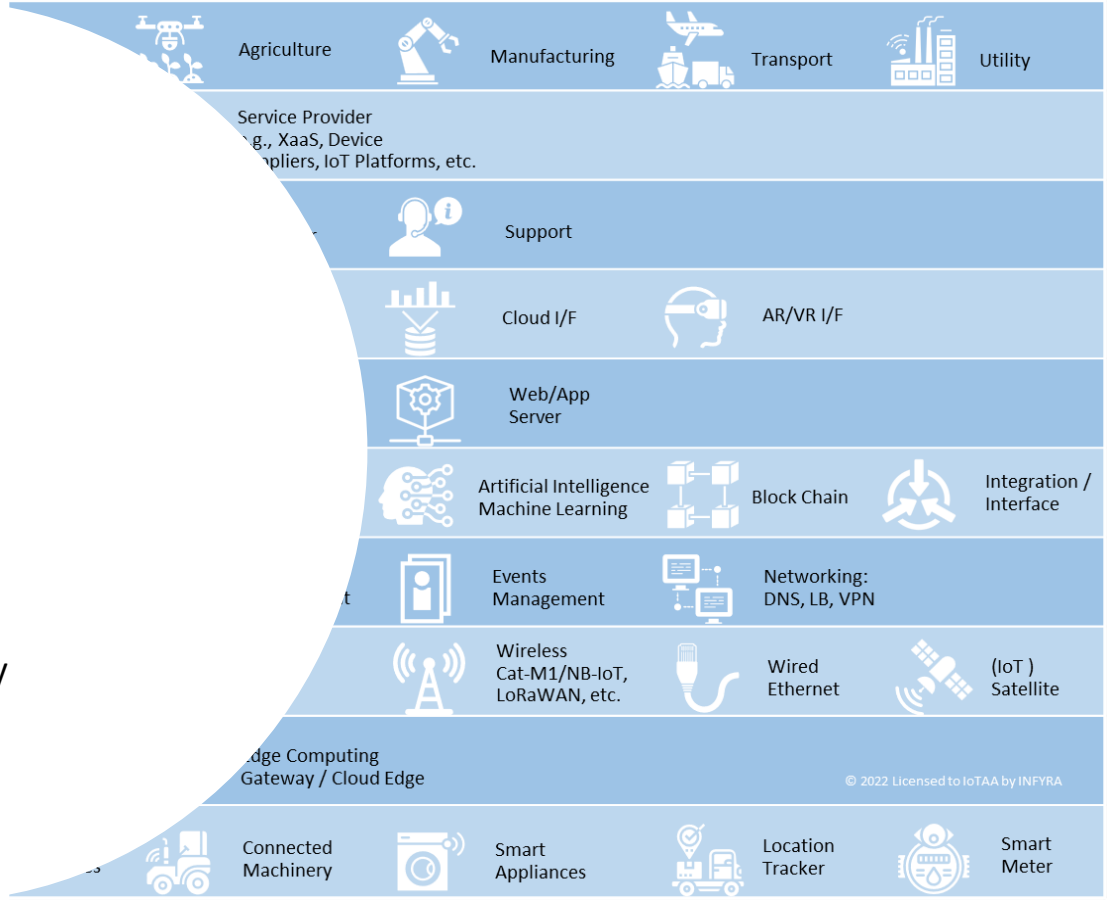
IoT Reference Framework

The IoT Reference Framework

- is a generic and vendor-neutral reference framework for all IoT solutions
- shows IoT building blocks
- brings in one place the relationship between technical architecture, IoT users, business stakeholders, and industry sectors
- Is a communications tool

It's Purpose

- serves as reference building blocks for all IoT applications across multiple industry sectors
- provides a 'Common Language' to avoid ambiguity amongst stakeholders
- Enables organisations to articulate IoT solution requirements clearly by looking through the various business lenses, e.g., business, data, cybersecurity, technology, etc.
- Helps demystify IoT



IoT Reference Framework – Overview

IoT Alliance Australia

10	Industry Sector & Solution		Smart City		Health Care		Agriculture		Manufacturing		Transport		Utility		
9	Solution / Service Provider		IoT Solution Owner		Connectivity Provider		Service Provider e.g., XaaS, Device Suppliers, IoT Platforms, etc.								
8	Users		Internal		Admin		End User		Support						
7	User Interface		Mobile I/F		Web / API Portals		B2B System I/F		Cloud I/F		AR/VR I/F				
6	Application Enablement		API Gateway		User I/F Security		Business Logic Engine		Web/App Server						
5	Intelligence Enablement		Data Enablement		Data Ingestion Rules Engine		Analytics		Artificial Intelligence Machine Learning		Block Chain		Integration / Interface		
4	Connection Management		Configuration / Identity Management		Device / Meta Data Management		Connectivity Management		Events Management		Networking: DNS, LB, VPN				
3	Connectivity		Bluetooth		Zigbee 6LoWPAN		Wi-Fi Mesh		Wireless Cat-M1/NB-IoT, LoRaWAN, etc.		Wired Ethernet		(IoT) Satellite		
2	Edge Gateway		Protocol Gateway		Field Gateway		Edge Computing Gateway / Cloud Edge								
1	IoT Endpoint		Smart Light		Sensor / Wearables		Connected Machinery		Smart Appliances		Location Tracker		Smart Meter		

IoT Reference Framework – editable icons

10	Industry Sector & Solution		Smart City		Health Care		Agriculture		Manufacturing		Transport		Utility	
9	Solution / Service Provider		IoT Solution Owner		Connectivity Provider		Service Provider e.g., XaaS, Device Suppliers, IoT Platforms, etc.							
8	Users		Internal		Admin		End User		Support					
7	User Interface		Mobile I/F		Web / API Portals		B2B System I/F		Cloud I/F		AR/VR I/F			
6	Application Enablement		API Gateway		User I/F Security		Business Logic Engine		Web/App Server					
5	Intelligence Enablement		Data Enablement		Data Ingestion Rules Engine		Analytics		Artificial Intelligence Machine Learning		Block Chain		Integration / Interface	
4	Connection Management		Configuration / Identity Management		Device / Meta Data Management		Connectivity Management		Events Management		Networking: DNS, LB, VPN			
3	Connectivity		Bluetooth		Zigbee 6LoWPAN		Wi-Fi Mesh		Wireless Cat-M1/NB-IoT, LoRaWAN, etc.		Wired Ethernet		(IoT) Satellite	
2	Edge Gateway		Protocol Gateway		Field Gateway		Edge Computing Gateway / Cloud Edge							
1	IoT Endpoint		Smart Light		Sensor / Wearables		Connected Machinery		Smart Appliances		Location Tracker		Smart Meter	

IoT Reference Framework – Overview

IoT Alliance Australia

10	IoT Industry & Solution		The **IoT industry & solution** layer aims to provide the context for an IoT solution such as the industry segment (industrial, consumer, enterprise) that the IoT solution belongs to, and the potential implications that IoT solution owners/practitioners might have to comply to in terms of regulatory compliance such as cybersecurity, data privacy, critical infrastructure, etc.
9	Solution / Service Provider		The **IoT Solution Owner / Service Provider** layer intends to bring in the business aspects of the IoT solution into consideration. Understanding the roles of stakeholders in a solution can enable clear understanding of roles, responsibilities as well as missing items such as strategies, processes, people and skills that need to be actioned. Examples of items can include (but not limited to) Governance, Cybersecurity compliance, Strategy, Risks, Data Sharing, etc.
8	IoT Users		The **IoT User** layer helps businesses identify who the end-users (and/or beneficiary of) the IoT solution. As a suggestion, IoT Users can be categorised as **Primary** or **Secondary**. **Primary** users are those who will act upon / make their (business) decisions based directly on the outcome/information that their IoT solution produced. **Secondary** users are those who might use the IoT data to derive further value, but not directly affecting the primary users.
7	IoT User Interface		The **IoT User Interfaces** layer shows the type of interfaces that need to be supported by the Application Enablement layer. Examples include interfaces that are widely used today such as from mobile apps, to the emerging type such as AR/VR devices. User Interface that enable access and or manage of the IoT system and devices. IoT Client devices 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 includes functions that are both business and technical in nature to be accessible to the 'users'. You might have come cross other sources of information refers to Application Enablement as IoT platform. This layer forms one part of what is commonly referred to as the **'IoT Platform'**. (*The functions in this layer could be a PaaS/SaaS solution.)*
5	Intelligence Enablement		The **Intelligence Enablement** layer refers to the use of smart technologies such as Analytics, Artificial Intelligence, Machine Learning, Deep Learning, Block Chain, etc. as part of the IoT solution, in order to generate insightful outcomes and to drive smart actions. The functions in this layer is what really make IoT solutions truly smart and value-adding. This layer forms another part of what is commonly referred to as the '**IoT Platform'**. (*The functions in this layer could be a PaaS/SaaS solution or Edge solution.)*
4	Connection Management		The **Connection Management** layer refers to a set of the **IoT Core functions**, commonly refers to as Connection Management, which includes, but not limited to 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'**. (*The functions in this layer could be a PaaS/SaaS solution.)*
3	Connectivity		The **Connectivity** layer represents the digital connectivity between end-point/gateway devices (layer 1, 2) and various platforms in layers 4, 5 or 6. Digital connectivity technologies in this layer can be any of the followings, wired or wireless: Bluetooth, WiFi, Ethernet, 6LoPAN, LoRaWAN, Sigfox, Weighless-D, 2G/3G/4G LTE, 5G (Cat-M1, NB-IoT and 5G NR), DECT (Wirepas) as well as any other proprietary radio technologies (e.g., Taggle); This layer can also represent **(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, or embedded devices, etc., or complex products that have multiple endpoints embedded in it, or an appliance (e.g., washing machines, vehicle, industrial machines, etc.) that has embedded sensors.

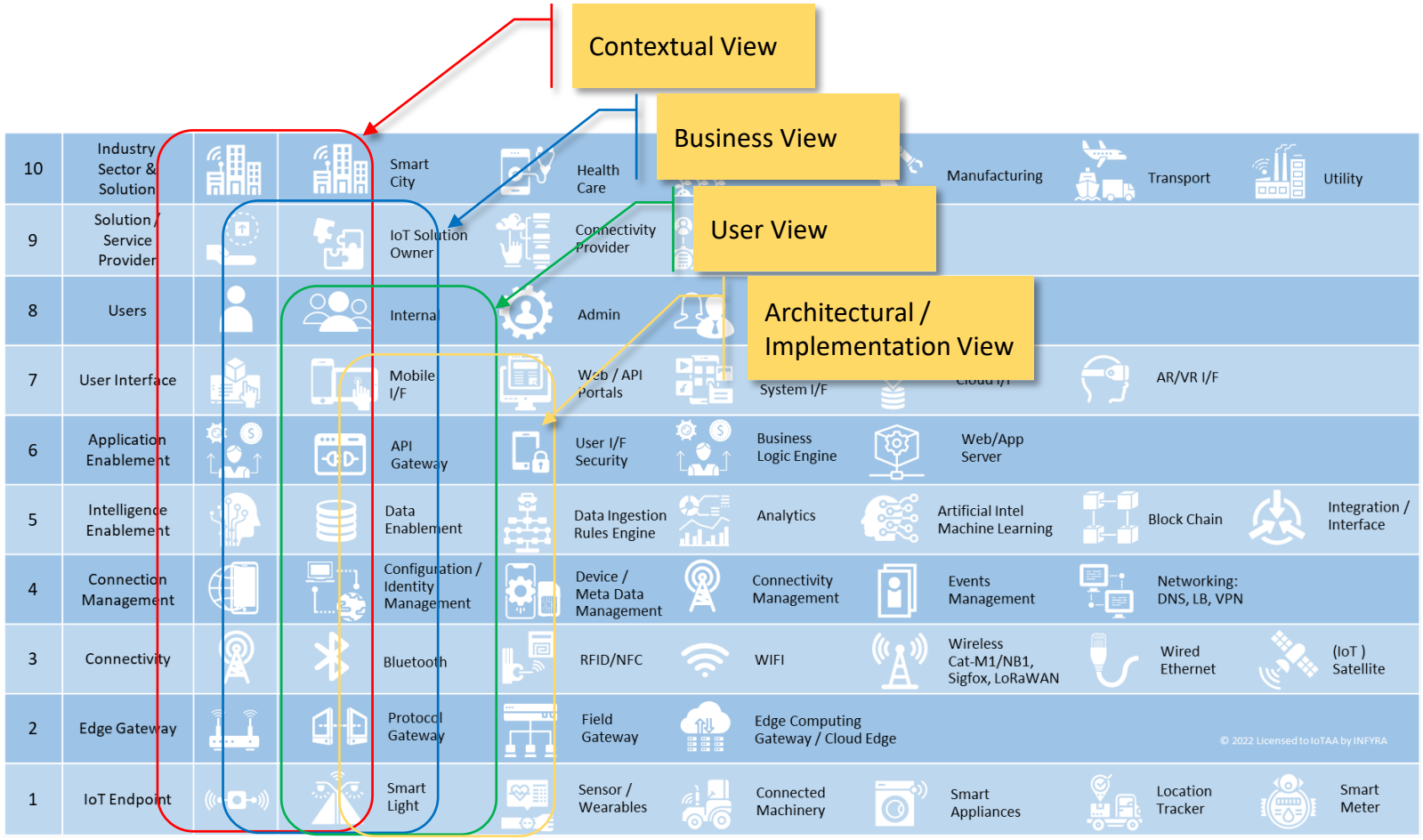
IoT Reference Framework – Template

10	Industry Sector & Solution		
9	Solution / Service Provider		
8	Users		
7	User Interface		
6	Application Enablement		
5	Intelligence Enablement		
4	Connection Management		
3	Connectivity		
2	Edge Gateway		
1	IoT Endpoint		

IoT Reference Framework – Views

The IoT Reference Framework shows

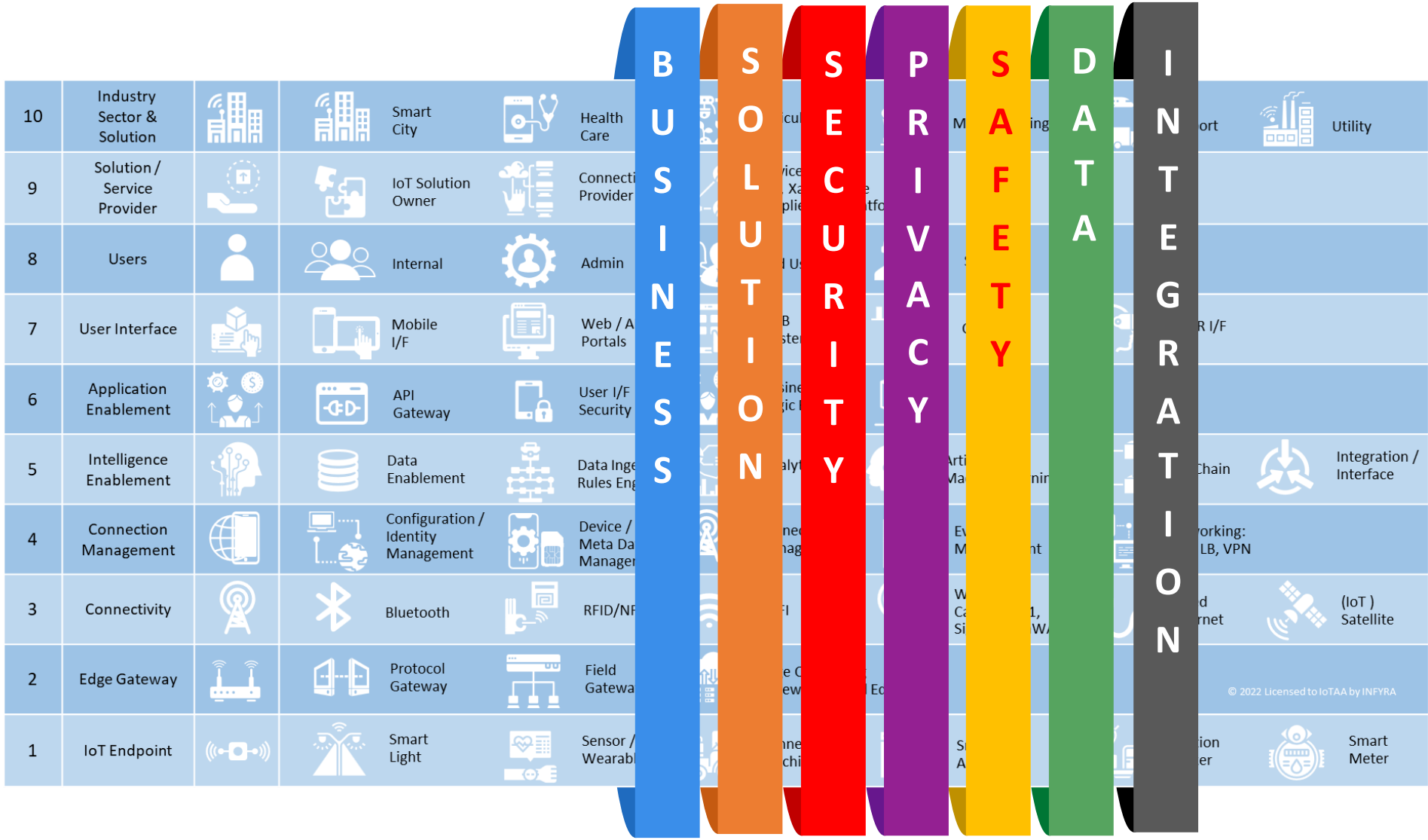
- Contextual View
  - Industries, markets, solution, revenue, value-chain
  - security, risks, regulations, etc.
- Business View
  - Stakeholders, processes, policies, industry and regulatory compliance
- User View
  - Organisations, consumers, governments, communities
- Architectural View
  - Solution, architecture, network, system, sub-system (each layer), component (detailed view)



IoT Reference Framework – Lenses

IoT solution requirements can be viewed through the lenses of:

- Business requirements
- Technical solution;
- Security;
- Privacy;
- Safety;
- Data;
- reliability;
- Integration;
- And more



Acknowledgements

This IoT Reference Framework was developed by

Nam Nguyen
Principal Consultant

INFYRA

www.infyra.net

nam@infyra.net

nam.nguyen@iot.org.au

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

Terms of Use

Revision History

REVISION	DATE	CHANGE HISTORY
V1.0	November 2018	First release
V1.1	October 2020	Updated with new icons, and licence agreement
V1.2	February 2022	Updated to Layers 4, 5, 6 and 7, to better explain the concept behind those icons
V1.3	August 2022	Updated explanations as well as general editing