Mindteck

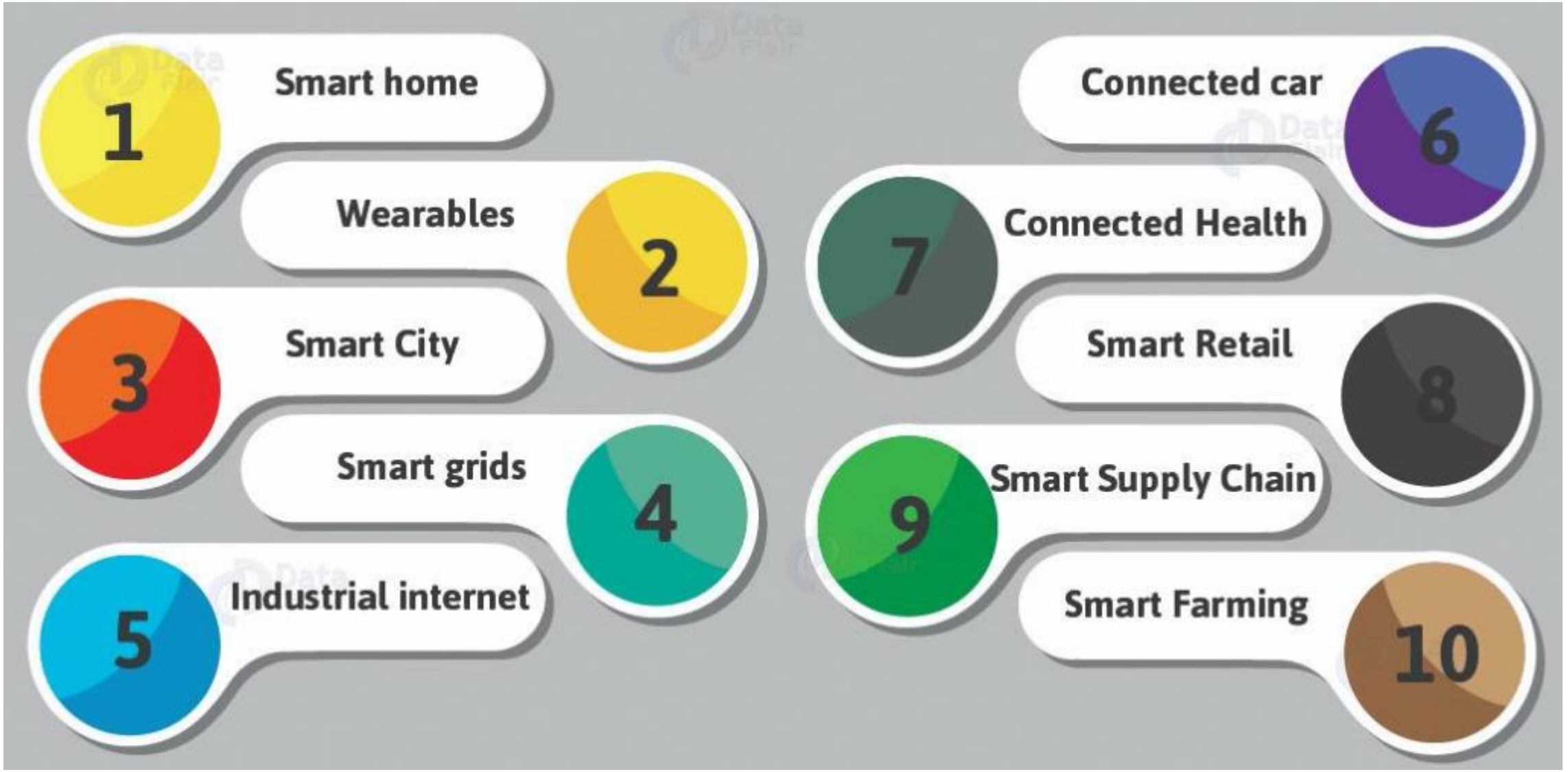
IOTSHOW.IN
PROFIT FROM IOT

RISC: Secured IoT and Cybersecurity

Secure IoT through Framework
Design and Deployment considerations

Ratnakar Gandhe

IOT Penetration



Secure IoT **Vulnerability of Connected Devices and Systems**

Secure IoT **Vulnerability of Connected Devices and Systems**

ST. JUDE MEDICAL

Mindteck

Secure IoT **Standards, Guidelines and Recommendations**

50+ Worldwide organisations
100 + documents

oneM2M **GSMA**

3GPP **ETSI** **OASIS**

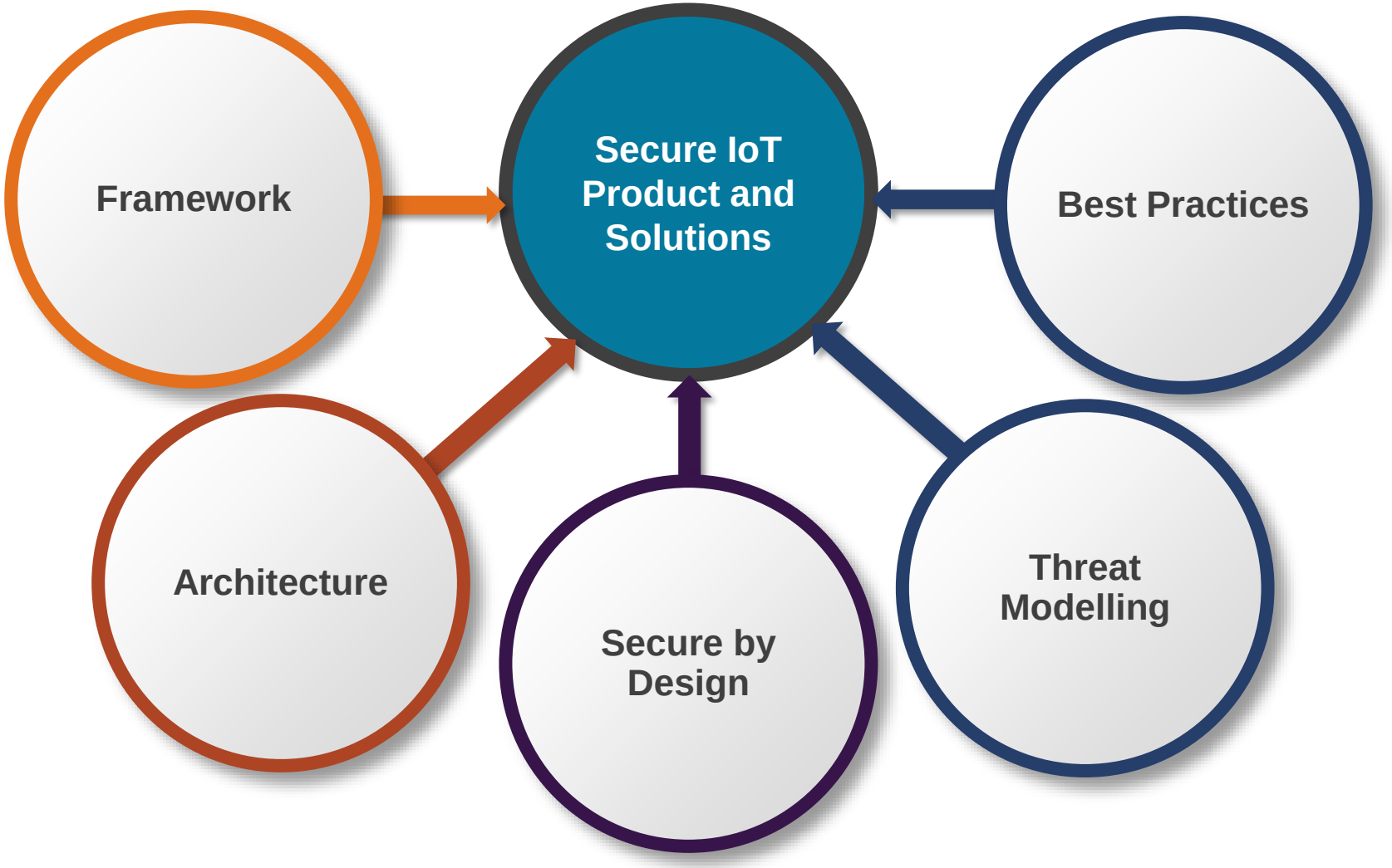
NIST **OWASP** **IOTSF**

ISO **IETF**

Disclaimers

Secure IoT **Product and Solutions**

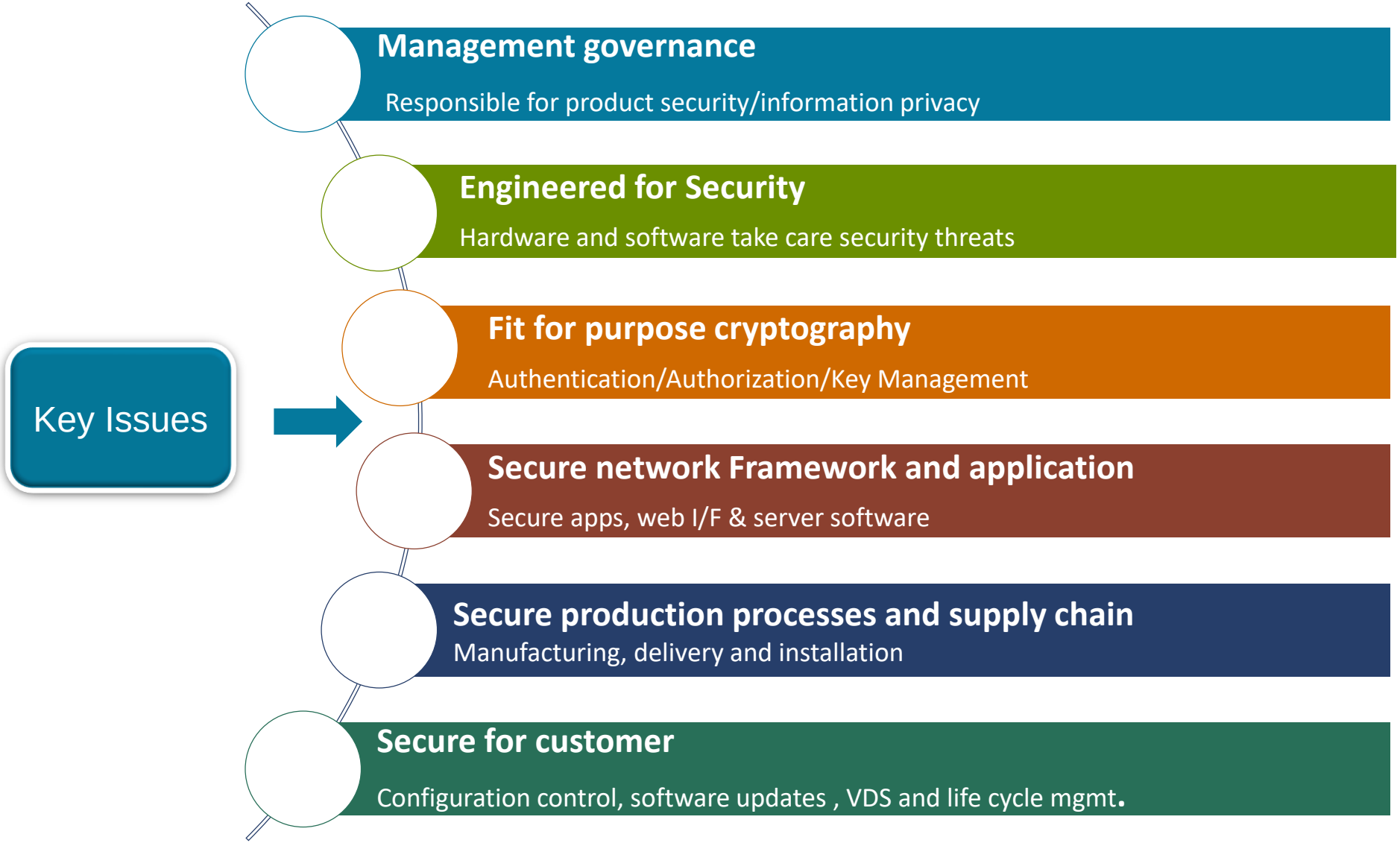
Contributing Factors



Stakeholders

- Manufacturers
- Service Providers
- System Integrators
- Developers
- Customers

Framework Security key issues and supply chain of trust



Key Issues

Supply of product/ solutions components from variety of sources need to be under consideration (Electronics/Mechanical/Web , mobile apps)

Framework **Risk based process**

Risk analysis of the product/Solution in target environment
(Risk register, CIA triad)

Determine compliance class
(Security objectives, Product environment)

Compliance requirement mapping for the class
(Mandatory, Advisory)

Context is important : Find risk appetite
Each application differs, driven by use case and operating environment

Little discernible impact to organisation, person

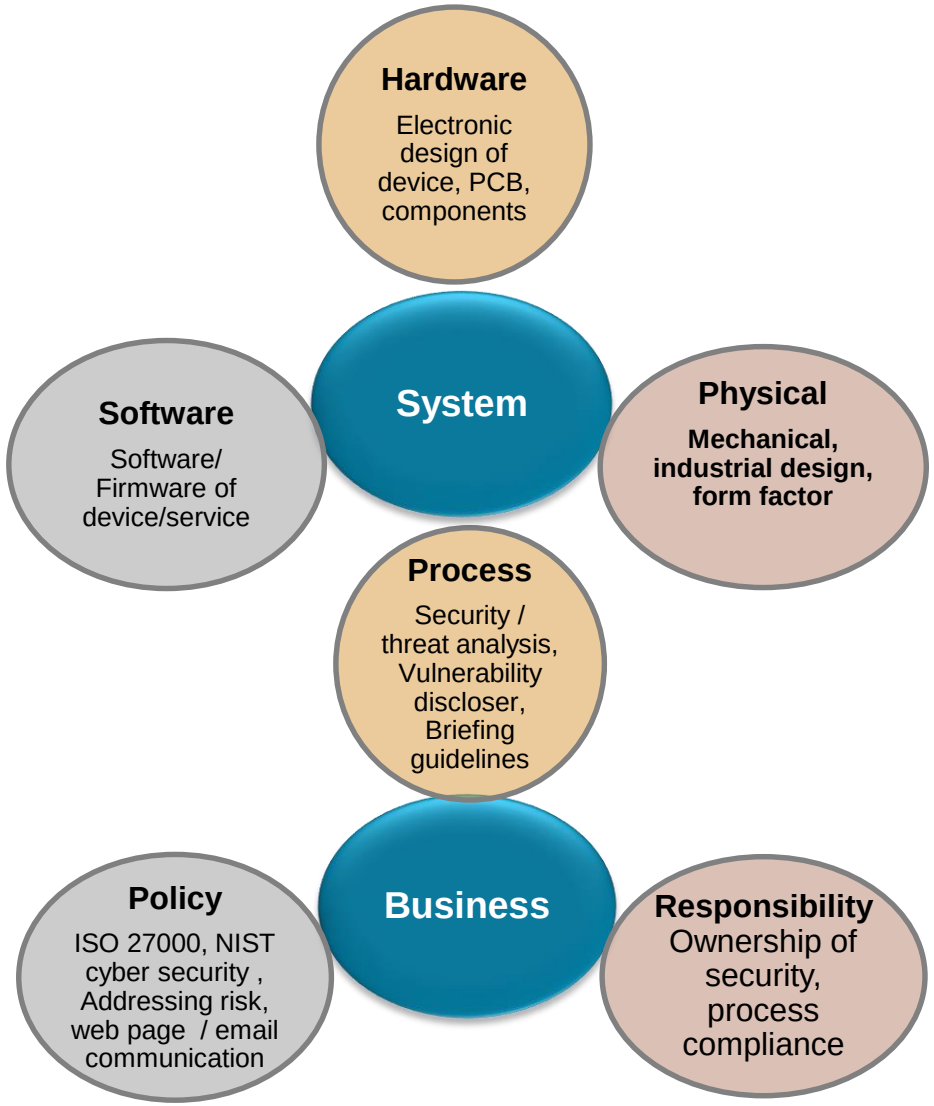
High impact, personal injury

Compliance Class	Security Objective(CIA triad)		
	Confidentiality	Integrity	Availability
Class 0	Basic	Basic	Basic
Class 1	Basic	Medium	Medium
Class 2	Medium	Medium	High
Class 3	High	Medium	High
Class 4	High	High	High

- Basic : Public info, Minor impact and disruption
- Medium: Personal sensitive info, limited impact
- High : Personal sensitive info, high impact

Source :IOTSF-IoT-Security compliance Framework release 2.0

Framework **Security Requirements compliance**



Compliance requirements from System and business point of view

- Business Security Processes, Policies and Responsibilities
- Device Hardware & Physical Security
- Device Software
- Device Operating System
- Device Wired and Wireless Interfaces
- Authentication and Authorization
- Encryption and Key Management for Hardware
- Web User Interface
- Mobile Application
- Privacy : Data protection, regulatory compliance
- Cloud and Network Elements
- Secure Supply Chain and Production
- Configuration
- Device Ownership Transfer

Framework **Requirements compliance samples**

Business Security Processes, Policies and Responsibilities

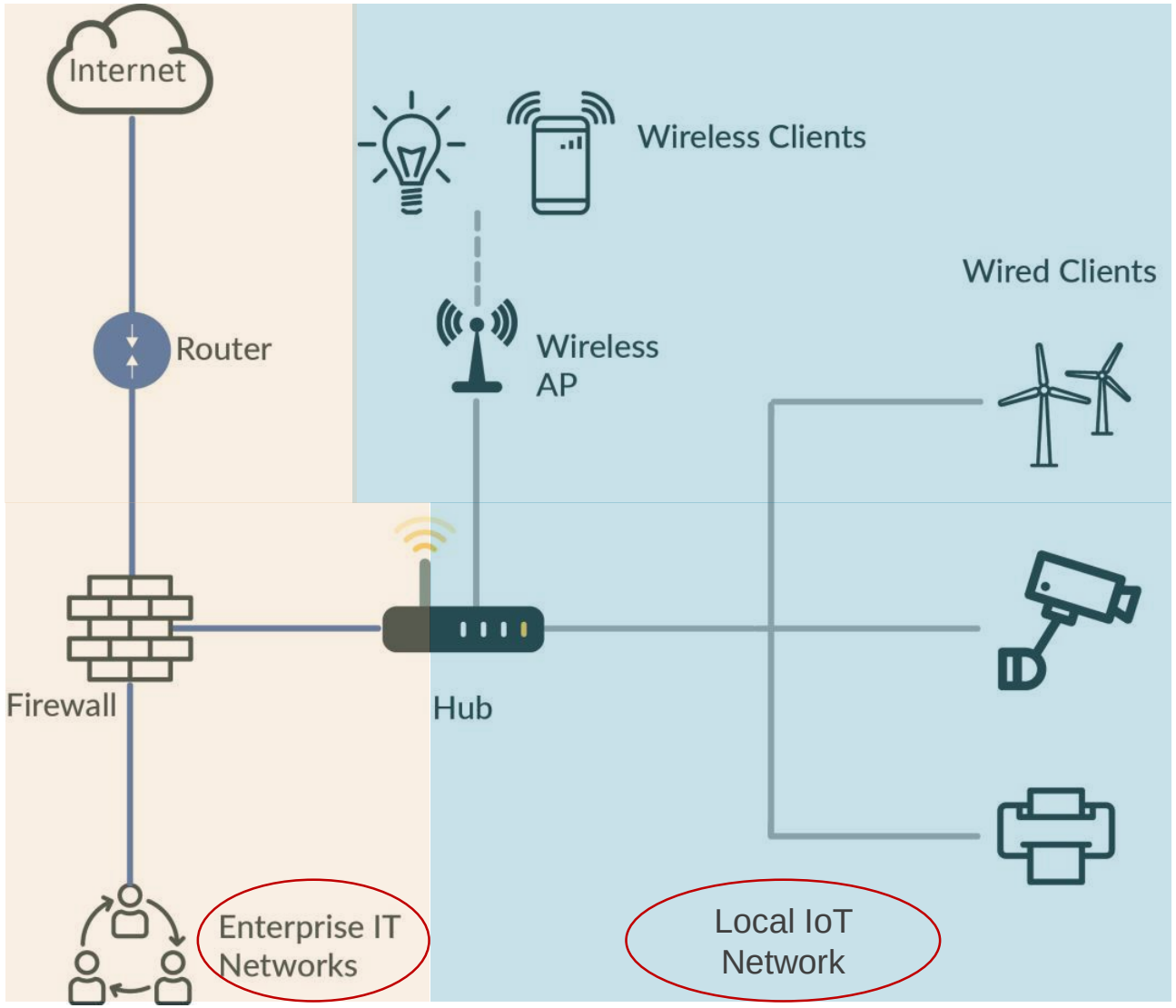
Requirement	Compliance Class and Applicability	Primary Keyword	Secondary Keyword
There is a person or role, typically a board level executive, who takes ownership of and is responsible for product, service and business level security.	M for All classes	Business	Responsibility
There is a person or role, who takes ownership for adherence to this compliance checklist process.	M for All Classes	Business	Responsibility
The company follows industry standard cyber security recommendations (e.g. UK Cyber Essentials, NIST Cyber Security Framework, ISO27000 etc.).	M for Class 2 and above	Business	Policy
A policy has been established for interacting with both internal and third party security researcher(s) on the products or services.	M for All Classes	Business	Policy

Device Hardware & Physical Security

Requirement	Compliance Class and Applicability	Primary Keyword	Secondary Keyword
The product's processor system has an irrevocable hardware Secure Boot process.	M for Class 1 and above	System	Hardware
The product's processor system has an irrevocable "Trusted Root Hardware Secure Boot".	M for Class 2 and above	System	Hardware
The product's processor system has a measured irrevocable hardware Secure Boot process.	M for Class 3 and above	System	Hardware
The Secure Boot process is enabled by default.	M for Class 1 and above	System	Hardware
Any debug interface (for example, I/O ports such as JTAG) only communicates with authorised and authenticated entities on the production devices.	M for Class 1 and above	System	Hardware Software

Source :IOTSF-IoT-Security compliance Framework release 2.0

Architecture **Hub based architecture**



Stakeholders

- CxO, IoT purchase
  - *Informed decision*
- IT department
  - *Security focused IoT device management*
- Developers, OEM
  - *IoT management and security needs*

Classes

1. *Fully controlled/connected*
2. *Partially controlled/connected*
3. *Information sharing*

Hub control

Hub's 3 main Features

1. ***Network Management and Security tools***
2. ***Connecting devices securely***
3. ***Lifecycle management***

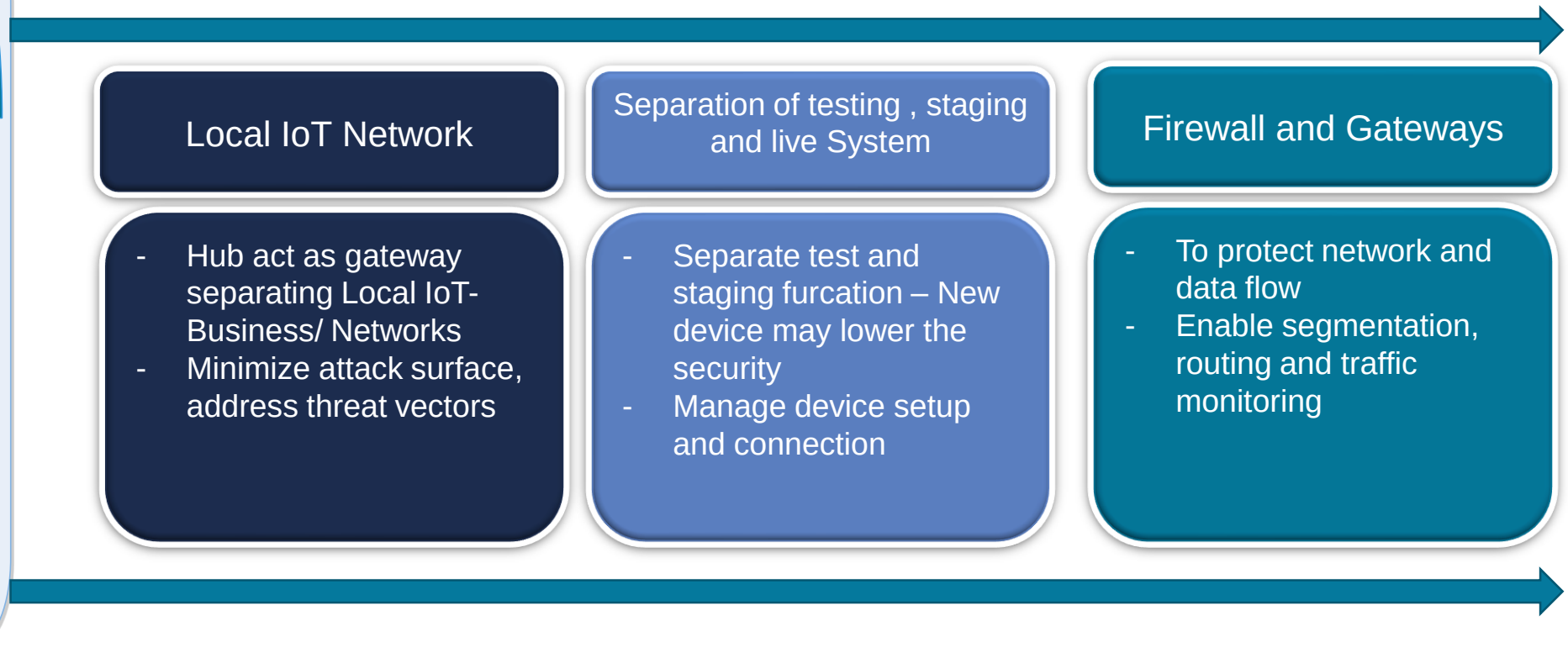
Source :IoTSF "IoT-Security-Architecture-and-Policy-for-the-Enterprise-a-Hub-Based-Approach.pdf

Mindteck

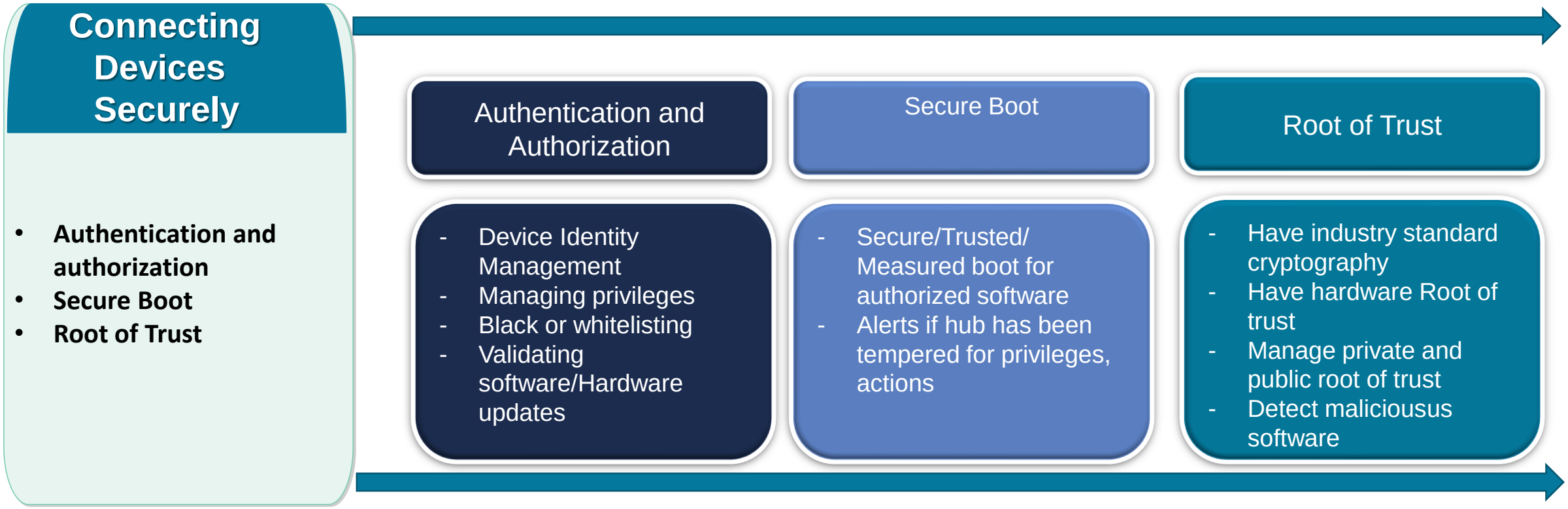
Architecture **Hub feature 1 : Network Management and security tools**

Network Management and security tools

- **Local IoT Network**
- **Separation of Testing, staging and Live system**
- **Firewall and Gateways**



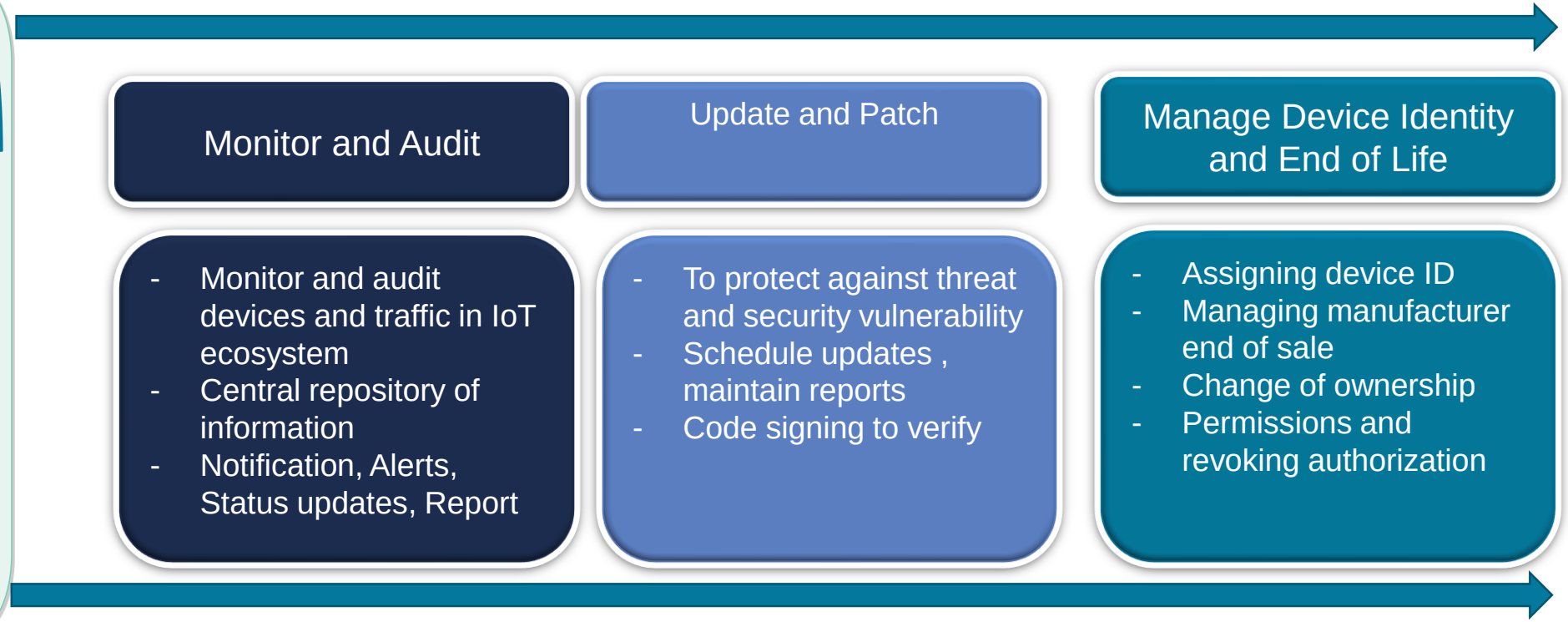
Architecture **Hub feature 2:** Connecting Devices Securely



Architecture **Hub feature 3:** Life Cycle Management

Life Cycle Management

- Monitor and Audit
- Update and Patch
- Manage Device Identity and End of Life



Architecture **Why hub based architecture**

Charateristics	Hub Architecture	Tree Network	Hub-and-Spoke / Star	Mesh	Ring
Centralized network management tool					
Hybrid network sub-architectures					
Direct communication with management tool (not through unneeded nodes or pathways)					
Information must be shared in a hierarchical manner					
Network management tool is resilient to device and network disruptions					
In the event of management point failure, networks and devices can continue functioning					
Central management and information aggregation point					
Management tool supports IoT device identity, access and authorization resources					
Management tool supports minimization of attack surface					
Dedicated device for network and IoT device management					

Source Enterprise_IoT-Security-Architecture-and-Policy-for-the-Enterprise-a-Hub-Based-Approach.pdf

Hub Architecture characteristics for IoT ecosystem

- **Centralized management**
  - *Focal point in a network, IoT lifecycle management, monitor traffic, RoT*
- **Software update and patch**
  - *Protect devices without update capabilities*
- **Security compliance**
  - *Act as firewall, log and reporting, status repository*
- **Troubleshooting**

Architecture **Support security principles and Threat modeling**

Hub architecture support to treat STRIDE* threat model

Threat	Threat example	Treatment	Architecture (Hub) to support
Spoofing	Address Resolution Protocol (ARP) used to redirect traffic	Update and patch device to prevent vulnerability	Authentication & Authorization, Update and Patch
Tempering	Tampering software to modify permissions, install spyware	Secure boot and upate by trusted resources	Secure boot, Monitor and audit
Repudiation	sensor data modified in transit to colud services	Secure identity of devices and users. PKI to manage and revoke certificates , RoT	Authentication & Autorisation, Roots of Trust (RoT)
Inforamation Disclosure (Data Breach)	Diagnostics information containing Enterprise information	Traffic monitoring and management, separte IoT/business network	Local IoT network, Gateway and firewalls
Deniel of Service	Using exploits in a device to execute DoS or DDoS attack on another IoT device	Traffic monitoring on IoT netowrk, Gateway and firewall to monior and block traffic	Local IoT network, Monitor and Audit , update and patch
Elevation of Privilege	Unautorized access of a cloud serive provider to get on the IT/IoT network	Separation of IoT and business ntework	Local IoT network, Authentication and authorization, Monitor and Audit

*Based on IoT deployment may use other models: PASTA, NIST, ISO 27000, OWASP

Security risk in IoT implementation and security principles

- **Three Key principles**
  1. *Confidentiality*
  2. *Integrity*
  3. *Availability*
- **Connecting device to IoT network****
  1. *Data need to be private, audited and trusted*
  2. *Timely arrival of data*
  3. *Access or control of device*
  4. *Updating*
  5. *Ownership management*
- **Who (hub) provides**
  - *Trust management*
  - *Layered security*
  - *Network access/revoke*
  - *Safe to make data transparent (M&C)*
  - *Enterprise data info, criticality and safety*

** *Source* :IoTSF "Make it safe to connect: Establishing principles for Internet of Things Security" IoTSF-Establishing-Principles-for-IoT-Security-Download.pdf

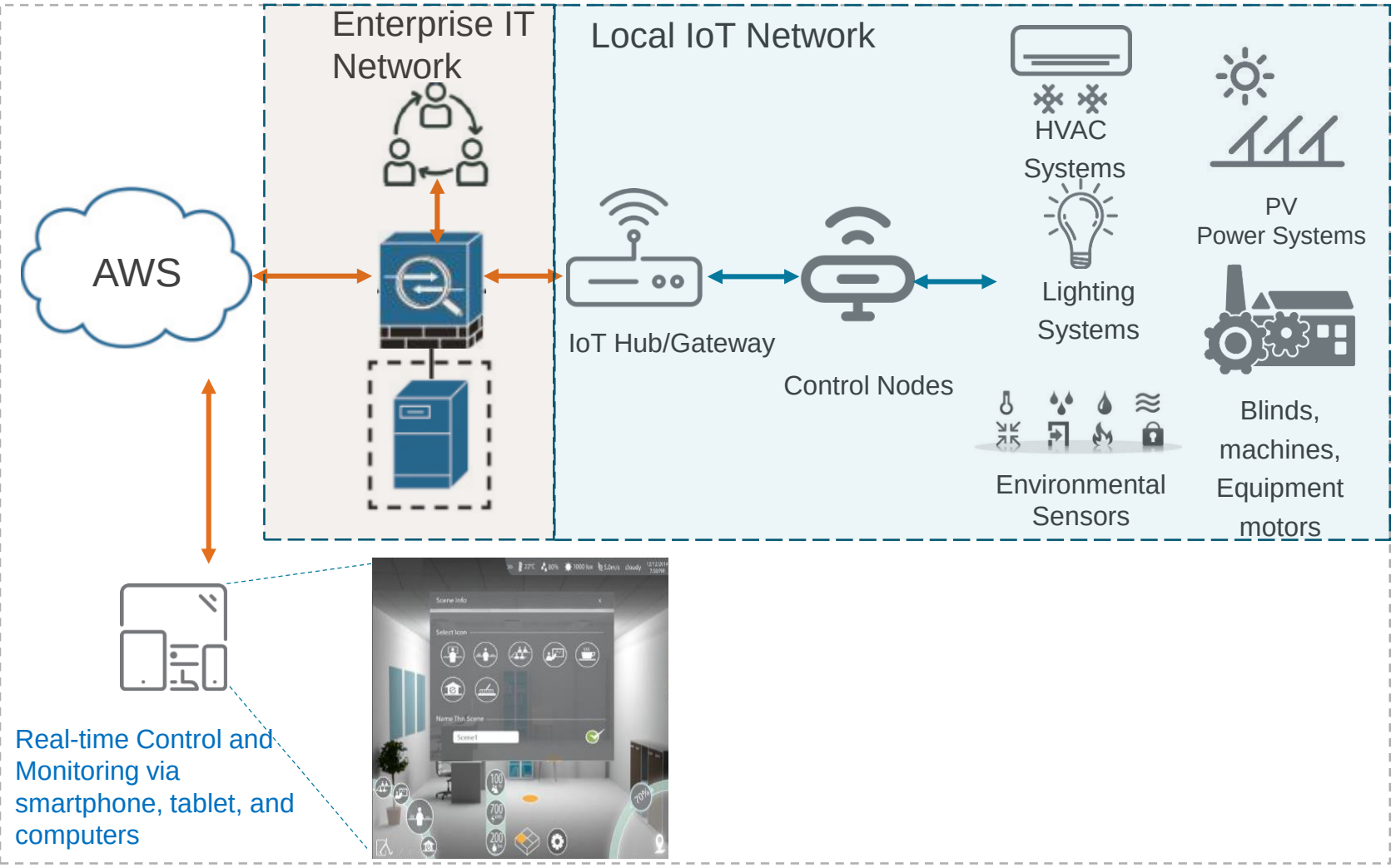
Secure by Design **Code of practice/Security mindset**

Stakeholders Responsible for implementation	
Device Manufacture	
IoT Service Providers	
Mobile Application Developers	
Retailers	

Guiding principles

1. To reduce burden : consumer/Supply chain
2. Transparency : what security mechanism
3. Measurability : Effectiveness
4. Facilitating Dialogue: Share best practices
5. Resilience: Business continuity, fall back mechanism

Case study **Smart Building Energy Management (Hub based)**



Building management with energy efficient operations, fault detection, operational scenario and schedules.

IoT Hub/ Gateway with following features

- Secure boot
- Device Identity Management
- Managing privileges
- Black or whitelisting
- Validating software/Hardware updates
- Routing and traffic monitoring
- Notification, Alerts, Status updates, Report

Case study **Smart Parking with Hub Features** (Distributed Hub)

Allows drivers to access parking quickly and efficiently

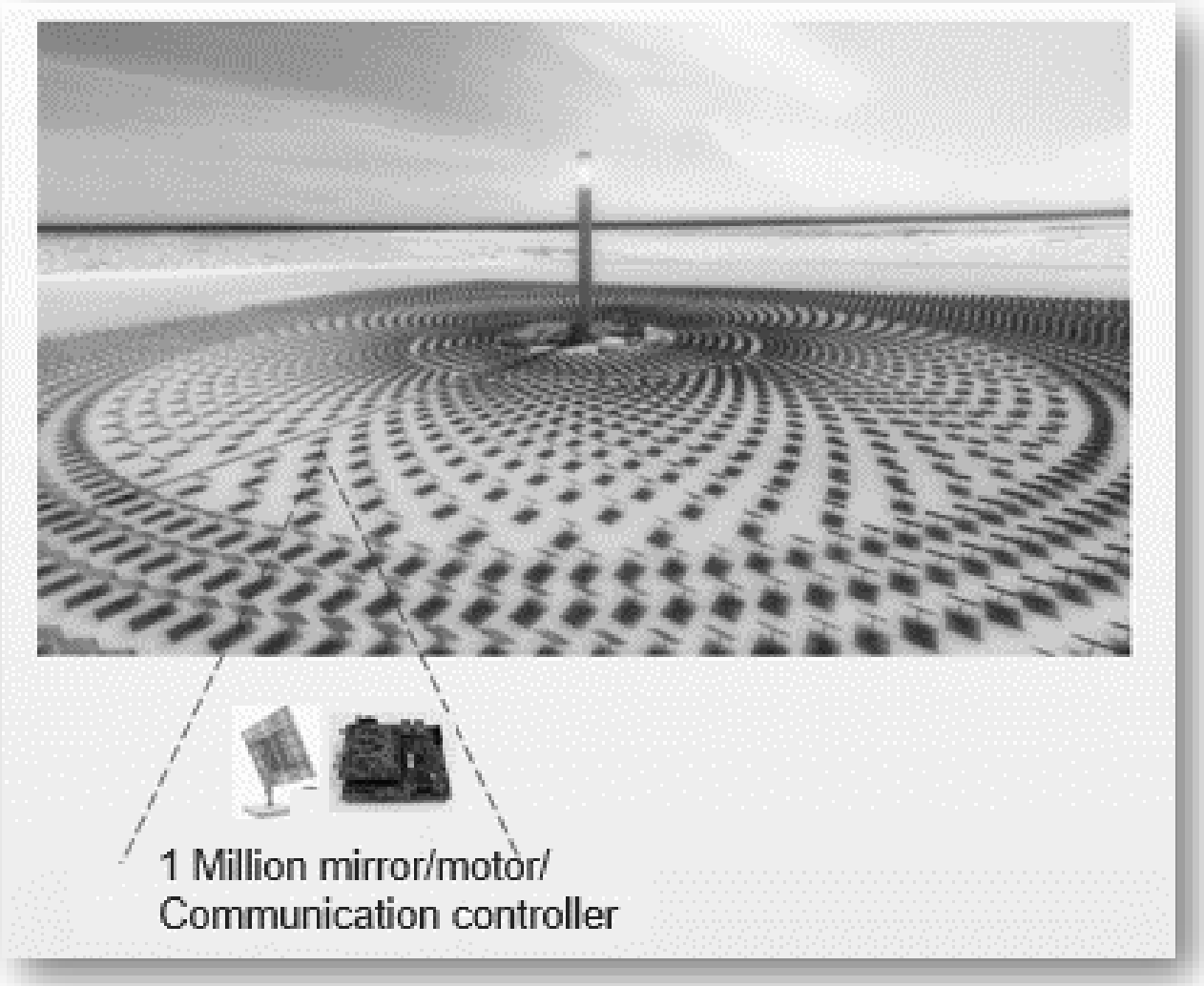
Enables real-time monitoring and management of available parking space, maximizing parking occupancy

.

IoT Hub/ Gateway

- *IoT Hub Gateway function distributed .*
- *Security Management is part of video analytics server*

Case study **Secure by design :** Hardware and system level



- *Concentrated solar power plant mirror controller with modified WiMax protocol*

Secure and reliable communication hardware with

- 802.16 phy
- Modified WiMax for security breach
- Protocol on FPGA to achive the high speed of 26 Mbps
- Frequency diversity : Software Defined Radio to operate single hardware in 800MHz to 6 GHz

References

- Jeep hacking prompts FCA software update to enhance security https://www.autonews.com/article/20150721/OEM06/150729970/jeep-hacking-prompts-fca-software-update-to-enhance-security
- Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm
- Code of Practice for consumer IoT security https://www.gov.uk/government/publications/secure-by-design/code-of-practice-for-consumer-iot-security
- Researchers Find Serious Flaws in WeMo Home Automation Devices https://threatpost.com/researchers-find-serious-flaws-in-wemo-home-automation-devices/104300/3/
- The CEO's Guide to Securing the Internet of Things https://www.business.att.com/content/dam/attbusiness/reports/exploringiotsecurity.pdf
- ENTERPRISE IoT Security Architecture and Policy *FOR SECURITY ARCHITECTS https://www.iotsecurityfoundation.org/wp-content/uploads/2018/11/IoT-Security-Architecture-and-Policy-for-the-Enterprise-a-Hub-Based-Approach.pdf
- IoTSF Compliance Framework, Compliance Checklist and Vulnerability Disclosure Guidelines can be found https://iotsecurityfoundation.org/best-practice-guidelines
- ESTABLISHING PRINCIPLES FOR INTERNET OF THINGS SECURITY https://www.iotsecurityfoundation.org/establishing-principles-for-internet-of-things-security/

Confidentiality and **Disclaimer Notice**

This document contains confidential information of Mindteck which is provided for the sole purpose of permitting the recipient to evaluate the capabilities submitted herewith. In consideration of receipt of this document, the recipient agrees to maintain such information in confidence and not to reproduce or otherwise disclose this information to any person outside the group directly responsible for evaluation of its contents, except that there is no obligation to maintain the confidentiality of any information: which was known to the recipient prior to receipt of such information from Mindteck, or becomes publicly known through no fault of recipient, or is received without obligation of confidentiality from a third party owing no obligation of confidentiality to Mindteck.

This publication is produced by Mindteck for private circulation among selected constituents. It is for informational purposes only. While every effort is made to ensure the information given is accurate, Mindteck will not accept any responsibility for loss or damage to any person resulting from reliance on information presented herein.

All trademarks, trade names, service marks, service names, and images mentioned herein belong to their respective owners, even if not clearly identified.

Mindteck

Thank You