Safeguarding IoT Devices in Digital Age – Building IoT Test Lab

Frank Chow
Head of Cyber Security and HKCERT
Hong Kong Productivity Council

Mr. Frank Chow

CISSP-ISSAP-ISSMP CSSLP CCSP CISA CISM CRISC CGEIT CDPSE CEH CHFI CBCP TOGAF PMP

Head of Cyber Security & HKCERT
Hong Kong Productivity Council
frankchow@hkpc.org
frankchow@hkcert.org

https://hk.linkedin.com/in/chowfrank

Expertise

# technology risk # cyber security # fintech

# business continuity # IT governance

Previous Experience and Awards

- Honoree of Asia Pacific Information Security Leadership Award from (ISC)2

- Received the Asia Business Continuity Award from BCI

- Received the Cyber Security Professional Award from HK Police Force

- Former Head of Cyber Security, Ping An OneConnect Bank

- Former Head of Information Security, Livi Bank

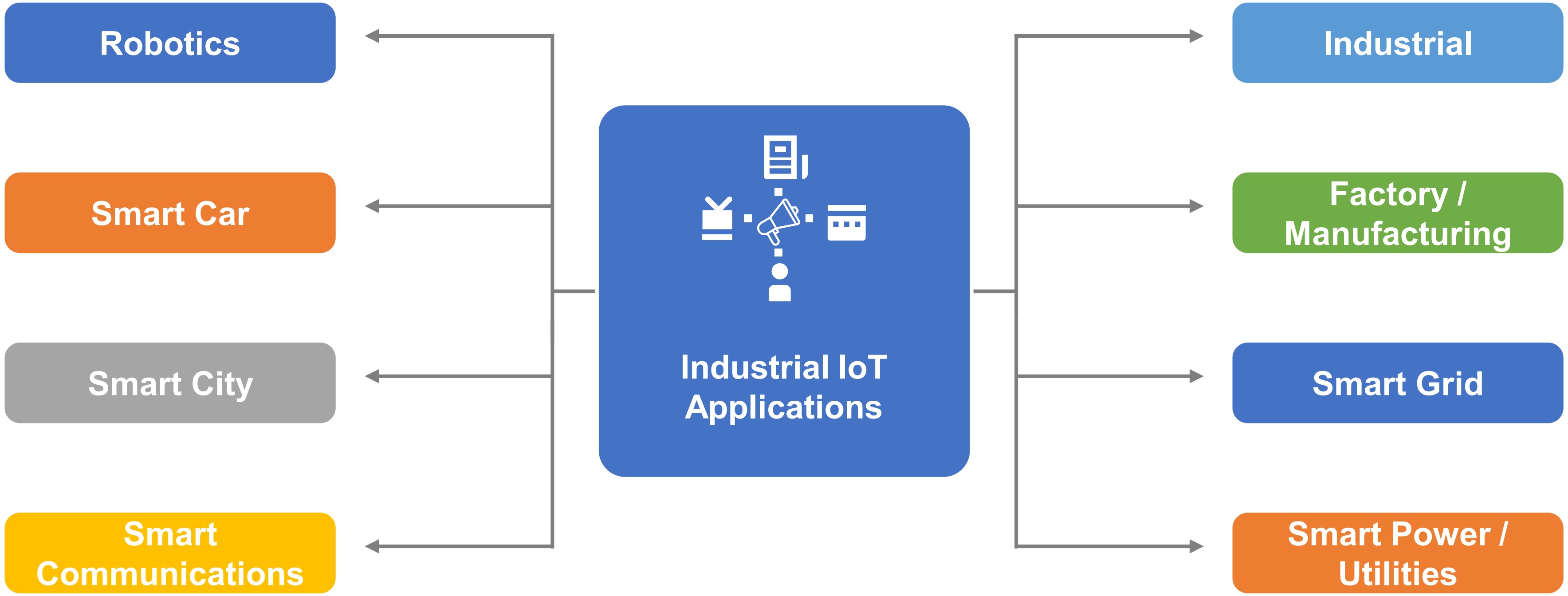
- Former Associate Director, Manulife Asia

- Former Head of Information Security and Risk Control, Fubon Bank

- Served on various advisory panels of local and global organizations, including (ISC)2, DotAsia, EDB, ERB, HKCAAVQ, HKCSS and HKIRC

Introduction

Industrial IoT Applications



Industrial IoT Applications

Robotics

Smart Car

Smart City

Smart Communications

Industrial

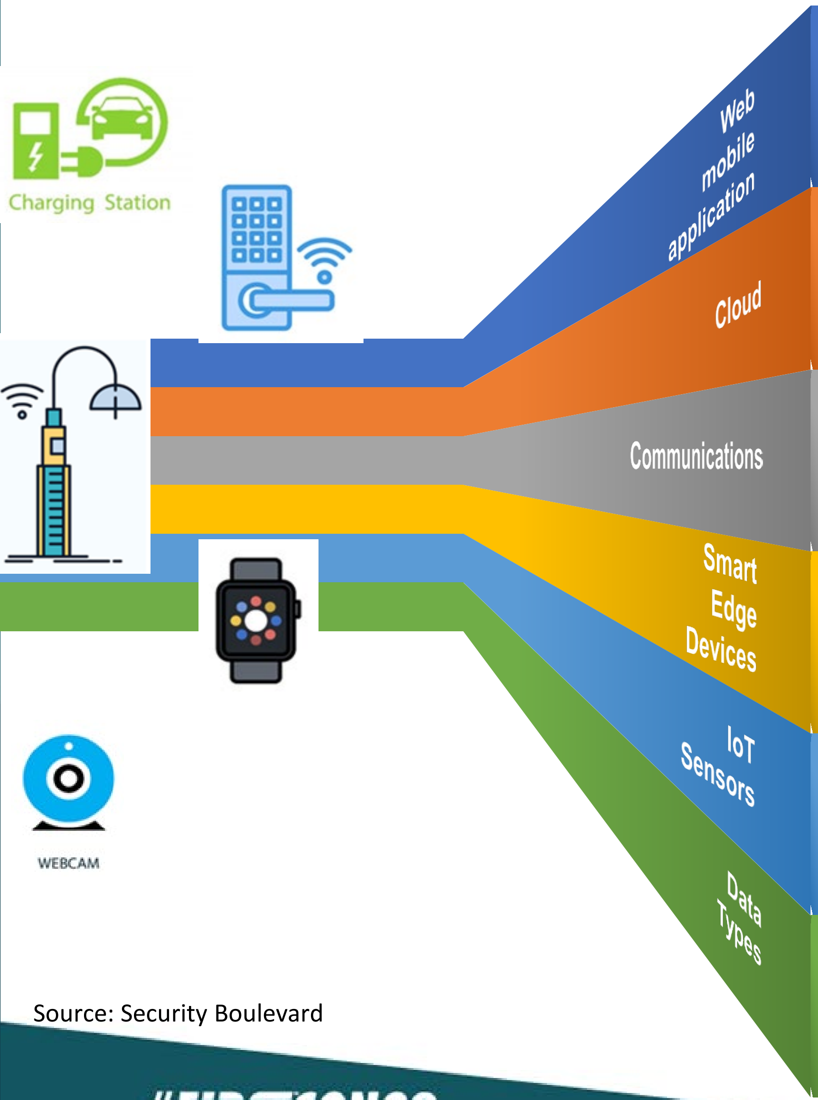
Factory / Manufacturing

Smart Grid

Smart Power / Utilities

Source: Tech Target

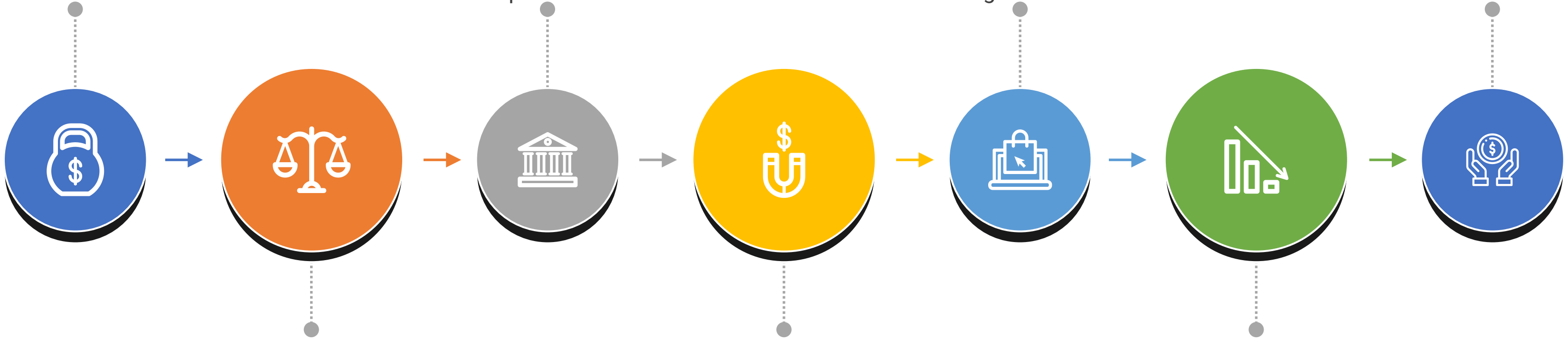
Are IoT Devices Safe?



	IoT Characteristics	Potential Security Weakness
Web mobile application	Closed / open platforms High data volume handling	Lack of penetration testing Weak User / Third Party Authentication
Cloud	Public / private / hybrid Cloud deployment	Code Policy management
Communications	DSL, Fibre, LPWAN 5G, Wi-Fi, Bluetooth, MQTT, ZigBee etc	Insecure communications
Smart Edge Devices	Variable communications protocols Time-sensitive data analysis	Denial-of-service No / insecure updates Poor hardware design
IoT Sensors	Limited power, Low bandwidth Constrained capabilities	Design faults Software implementation faults Inability to update
Data Types	Sensitive data: video, audio, location, personal information	Users Data storage

Source: Security Boulevard

Compromise Corporate Networks thru IoT



0 Sec
Intrusion
Attacker uses Shodan to scan open devices with default login credentials

30 sec
Scanning
Attacker gets access to a rogue web camera connected to the network, performs reconnaissance.

3 min
Exploitation
Attacker identifies a printer, attempts to get access via CVE exploitation.

9 min
Credential Stealing
Access to printer enables attacker to harvest credentials in the network.

12 min
Lateral movement
Credentials are used to move laterally to a sensitive DB containing customer data

50 min
Data theft
Attacker gets hold of 10GB of documents and leaks it out through the compromised web camera.

1 hr
Exfiltration
Data exfiltrated to Attacker and sold in Darkweb to higest bidder

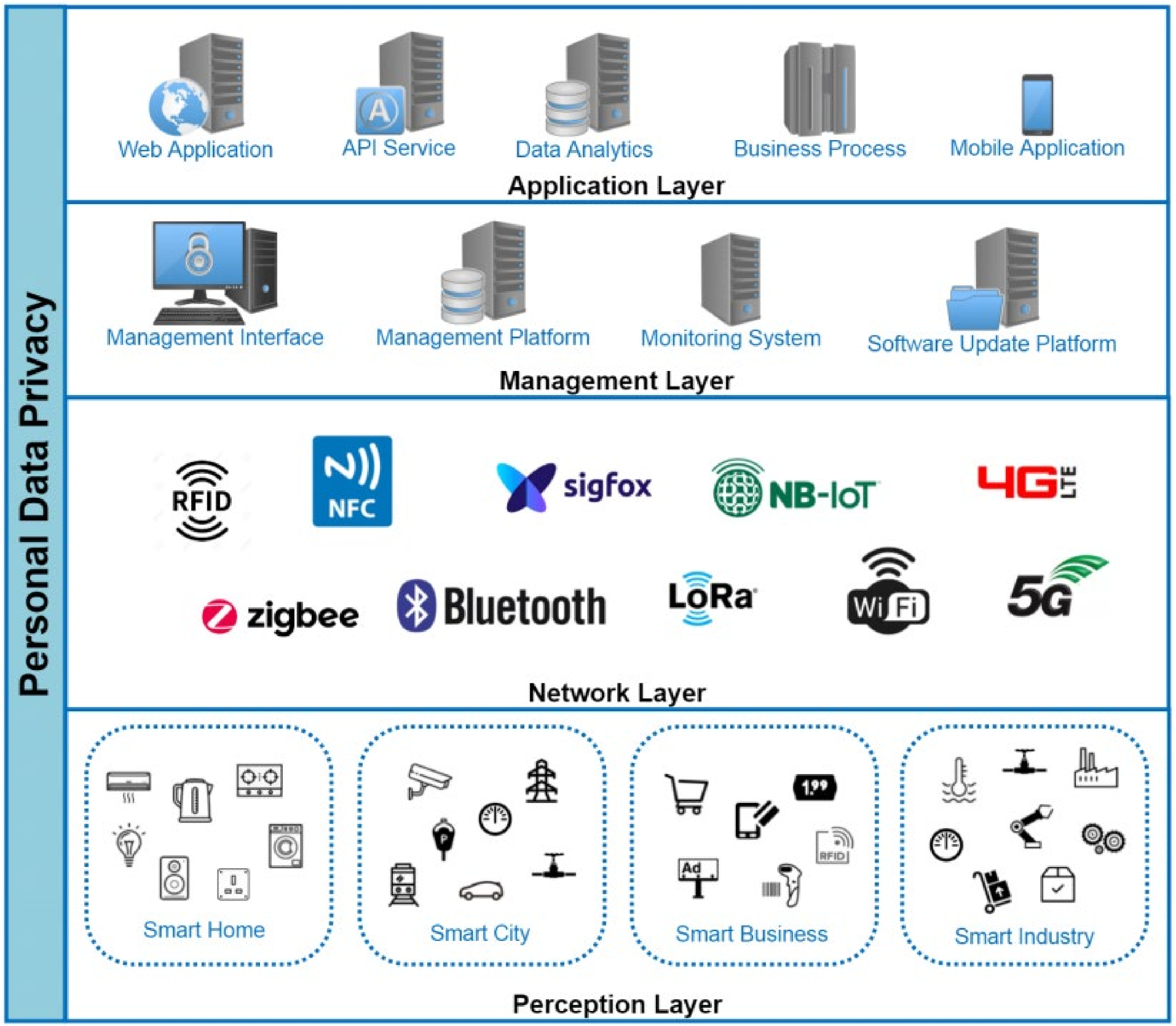
Source: Microsoft

IoT Test Lab Design and Implementation

Layers of the IoT Testing Framework

IoT Security Best Practice Guidelines

- Follow Personal Data (Privacy) Ordinance - Data processing lifecycle



- Web & API security
- OWASP Top 10

- Device registration with unique identifier
- Software Update Deployment

- Encryption
- Authentication (User side)
- Authenticity (Server backend)

- Device integrity
- Software Update Mechanism
- Mandatory change of default settings

Source: https://www.hkcert.org/security-guideline/implementing-iot-security-best-practice

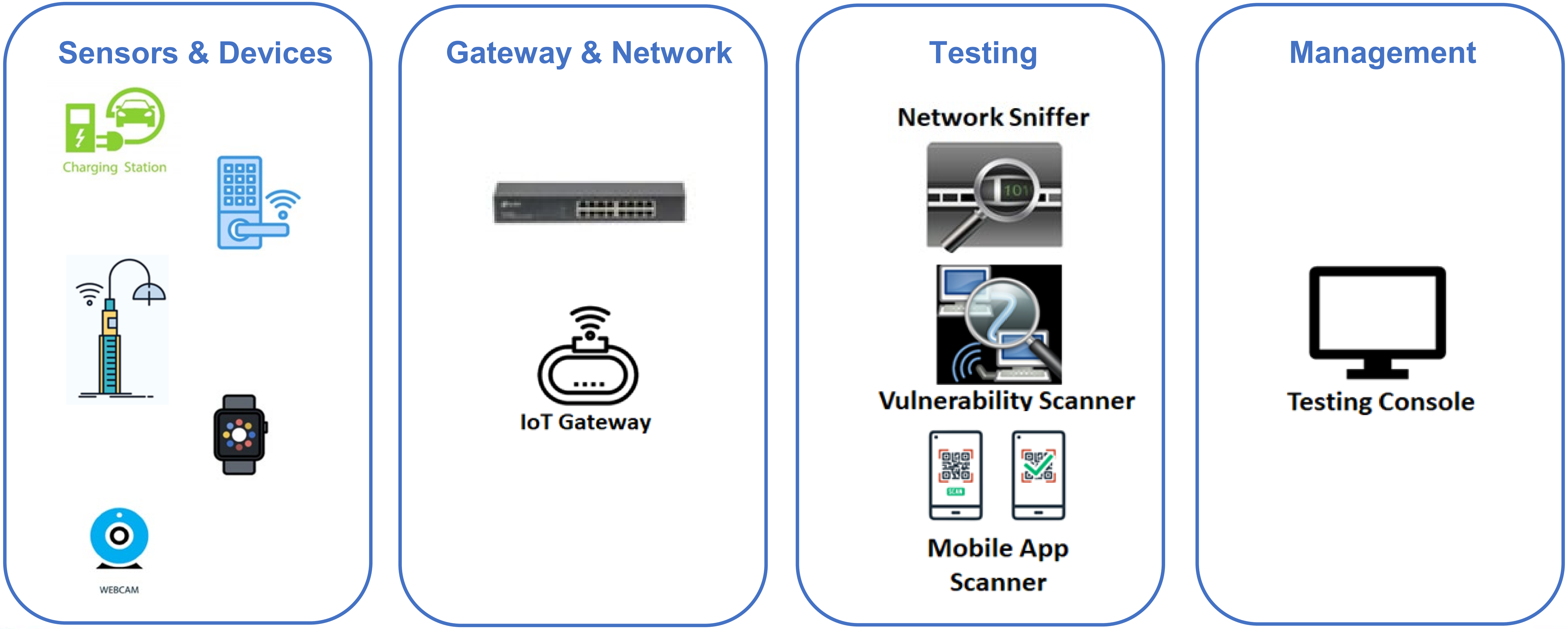
IoT Test Lab

- Compatibility Testing
- Device Interoperability Testing
- End-user application Testing
- Performance Testing
- Security Testing

IoT Security Focus Areas

- Device Security
- Network Security
- Data Security
- Physical Security

Basic IoT Test Lab (1)



Sensors & Devices

Gateway & Network

IoT Gateway

Testing

Network Sniffer

Vulnerability Scanner

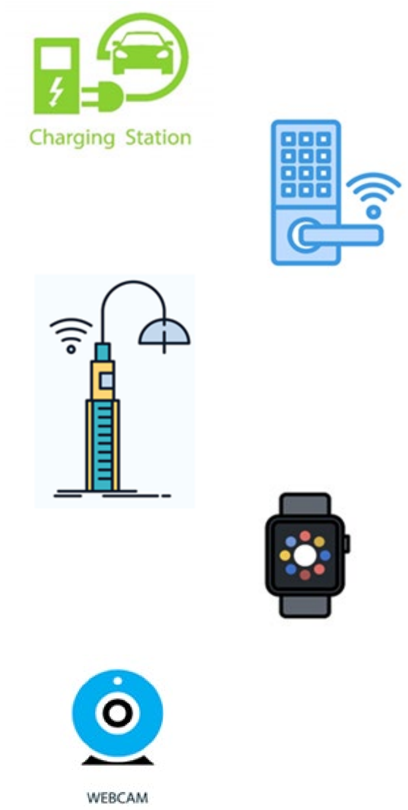
Mobile App Scanner

Management

Testing Console

Basic IoT Test Lab (2)

Sensors & Devices



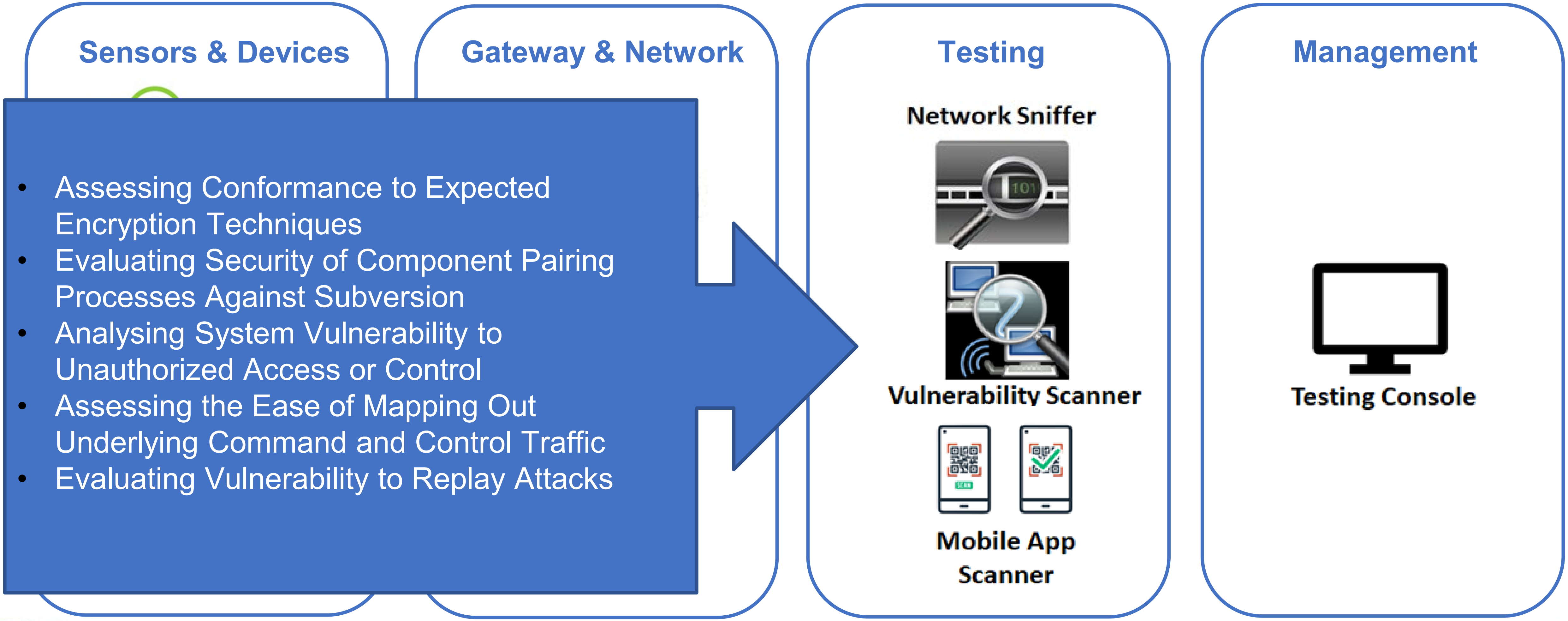
Gateway & Network

Testing

Management

- Assessing Security Risks of Exterior USB and Port Access
- Evaluating Location and Medium of Storage for Security Risks
- Analyzing the Availability of Serial and Debug Console Access for Security Risks
- Assessing Physical Security of the Device: Efforts Required for Disassembly
- Evaluating Risks of Compromise Based on Physical Access to the Device
- Analysing Security Risks Based on Allowed Connectivity Mediums (Wireless, Wired, Bluetooth, etc.)

Basic IoT Test Lab (3)



- Assessing Conformance to Expected Encryption Techniques
- Evaluating Security of Component Pairing Processes Against Subversion
- Analysing System Vulnerability to Unauthorized Access or Control
- Assessing the Ease of Mapping Out Underlying Command and Control Traffic
- Evaluating Vulnerability to Replay Attacks

IoT Test Lab Core SW & HW (1)

- Penetration testing tools:
  - Software tools allow you to simulate attacks on your devices and networks.
  - Some popular penetration testing tools include Kali Linux, Metasploit, and Nmap.
- Vulnerability scanners:
  - Software tools scan your devices and networks for known vulnerabilities.
  - Some popular vulnerability scanners include Nessus, OpenVAS, and Qualys.

IoT Test Lab Core SW & HW (2)

- Network sniffers:
  - Software tools allow you to capture and analyze network traffic.
  - Some popular network sniffers include Wireshark, tcpdump, and Fiddler.
- Firewalls:
  - Hardware or software devices allow you to control network traffic and block malicious traffic.
  - Some popular firewalls include pfSense, Fortinet, and Check Point.

IoT Test Lab Core SW & HW (3)

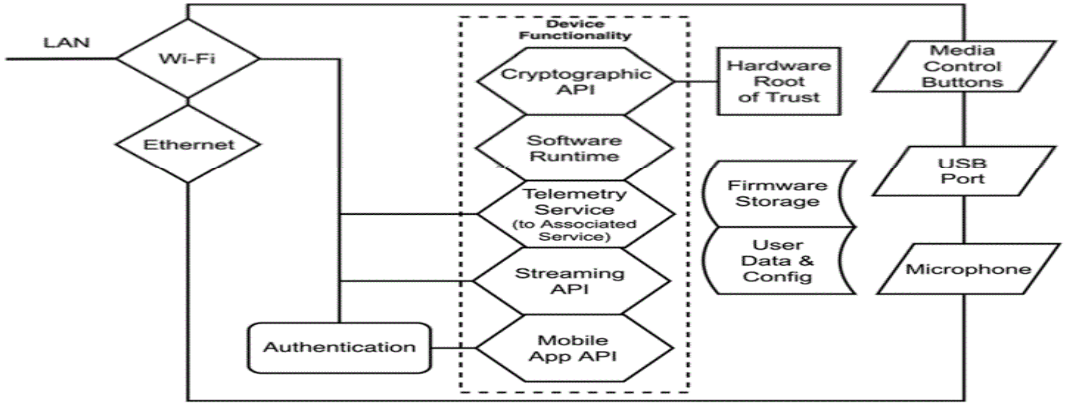
- Network switches and routers:
  - Hardware devices that allow you to create a network topology for testing purposes.
  - Some popular network switches and routers include Cisco, Juniper, and MikroTik.
- Virtualization software:
  - Create virtual machines for testing purposes, which can help you simulate attacks and vulnerabilities in a controlled environment.
  - Some popular virtualization software includes VirtualBox, VMware, and Hyper-V.

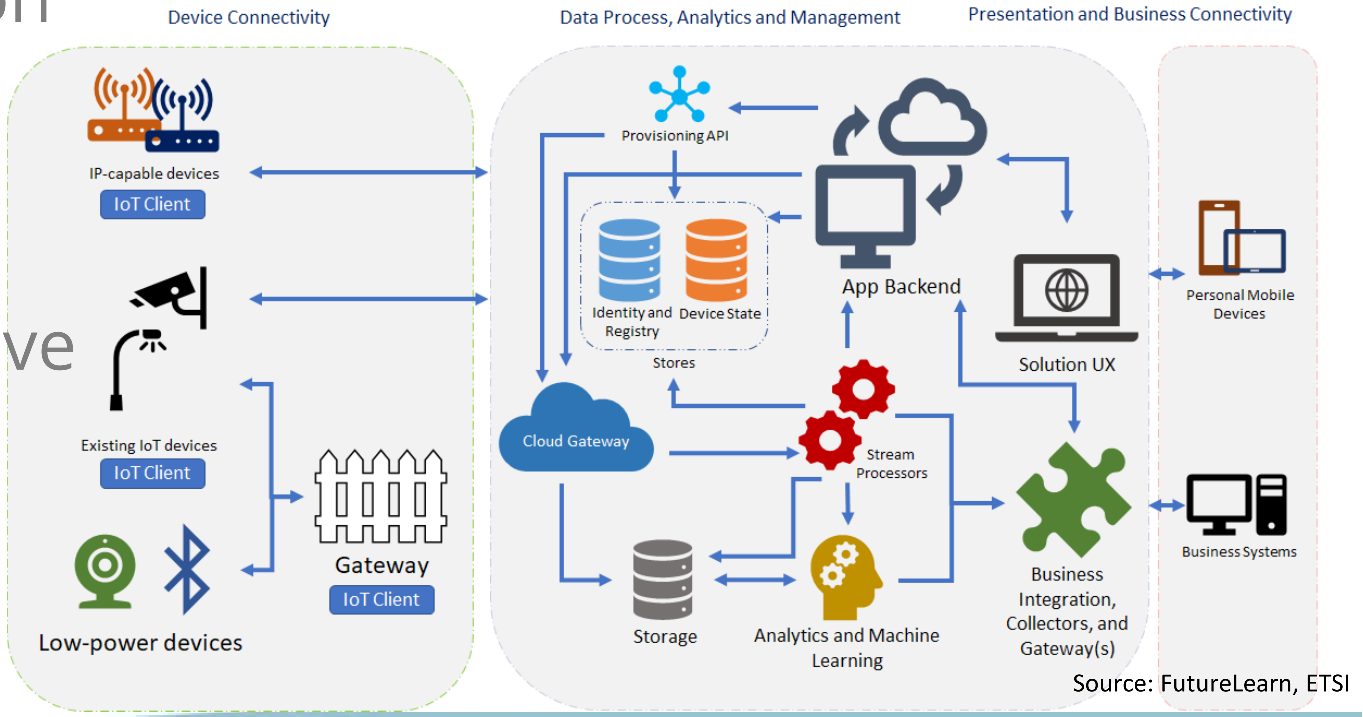
IoT Test Lab Core SW & HW (4)

- IoT devices:
  - To simulate attacks and vulnerabilities on IoT devices, you will need a range of devices to test.
  - This can include smart home devices, industrial IoT devices, and wearables, etc.
- Code Scanners:
  - Software tools used to analyze the security of code used in IoT devices. These scanners are designed to identify vulnerabilities and potential security weaknesses in the code, such as hardcoded passwords, buffer overflows, and other common security issues.

Techniques for Performing Tests on IoT (1)

- Building Threat Modelling
  - Defining security requirements
  - Creating an IoT application diagram
  - Identifying threats
  - Mitigating threats
  - Validating that threats have been mitigated





Source: FutureLearn, ETSI

Techniques for Performing Tests on IoT (2)

- Designing IoT Device Penetration Testing
  - Identify potential attack vectors
  - Vulnerability scanning
  - Exploit testing
  - Password cracking
  - Network traffic analysis

Configuration and Setup of the IoT Test Lab

- Setup a Dedicated Environment for Testing
- Configuring Security Settings for IoT Devices and Networks: Firewalls, Access Control, and Encryption.
- Regularly Maintaining the IoT Test Lab by Updating Devices, Software, and Security Settings

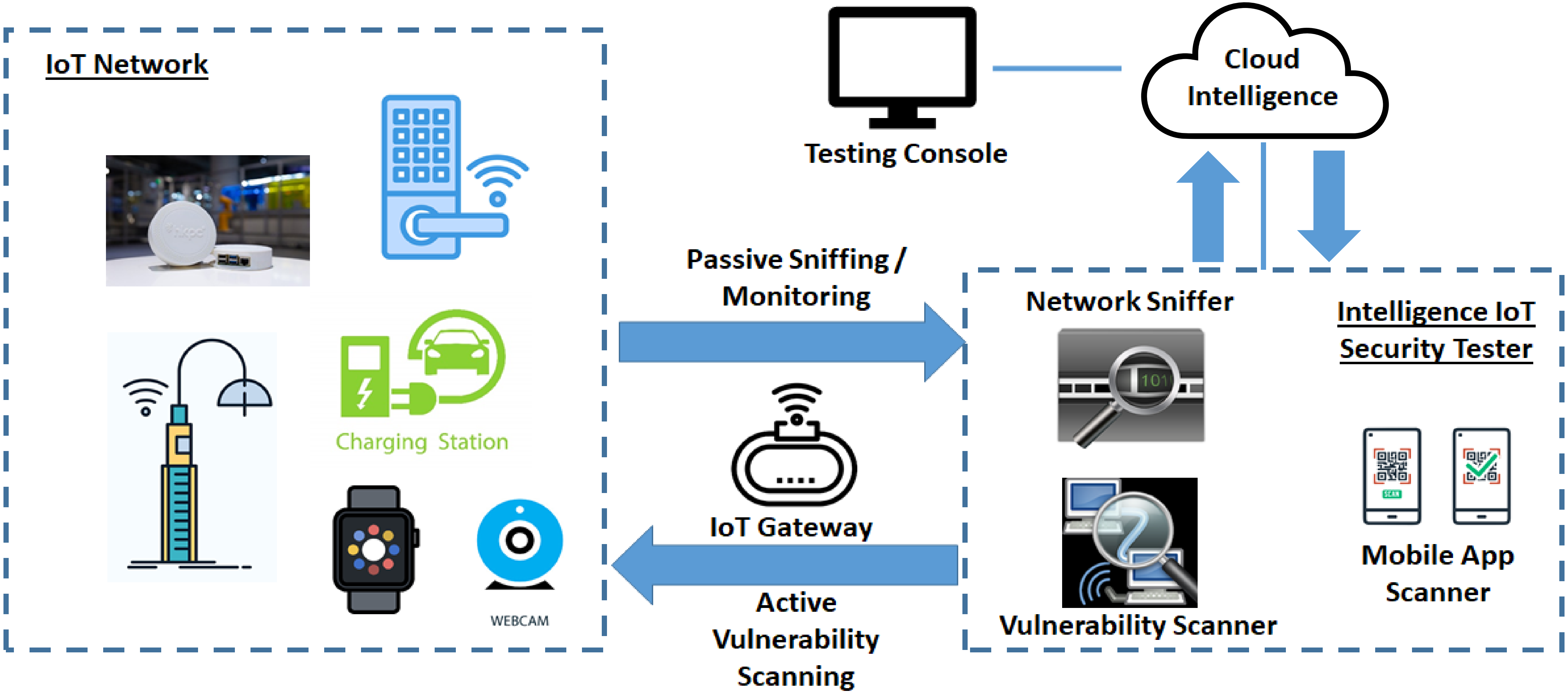
Sniffing IoT Communication & Scanning

- Sniffing IoT communication - Network sniffers like Wireshark or tcpdump are commonly used in IoT cybersecurity testing to capture and analyze network traffic
- Vulnerability scanning - Vulnerability scanners like Nessus, OpenVAS, or Qualys are commonly used in IoT cybersecurity testing to identify potential vulnerabilities in IoT devices and networks

Data Collection and Analysis

- Determine what data to collect
- Collect data
- Analyze data
- Prioritize vulnerabilities
- Recommend remediation steps
- Repeat the process

IoT Testing Architecture



Load Test + Security Test for IoT Devices

Source: HKPC

Source: HKPCI

Pen Test + Security Test for IoT Devices

Source: HKPC

DevOps + Security Test for IoT Devices

CODE
PLAN
DEPLOY
BUILD
DEV
RELEASE
OPS
OPERATE
TEST
MONITOR
1.6783

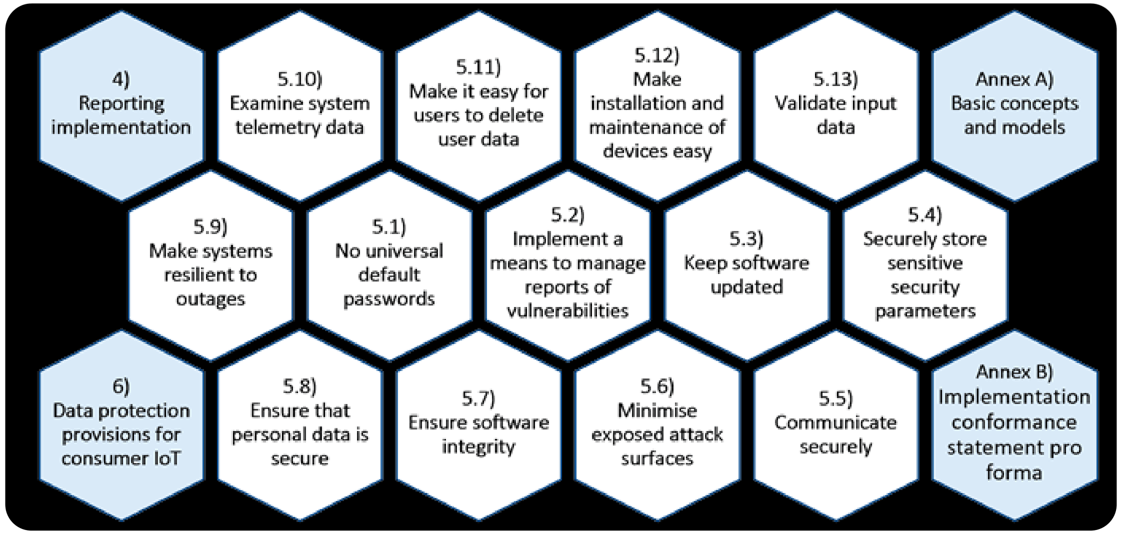
Source: HKPC

Source: HKPCI

Labelling Scheme & Standards

Cyber Security Labelling Scheme

- Countries are adopting Cyber Security **Labelling Scheme** for IoT devices



4) Reporting implementation

5.10) Examine system telemetry data

5.11) Make it easy for users to delete user data

5.12) Make installation and maintenance of devices easy

5.13) Validate input data

Annex A) Basic concepts and models

5.9) Make systems resilient to outages

5.1) No universal default passwords

5.2) Implement a means to manage reports of vulnerabilities

5.3) Keep software updated

5.4) Securely store sensitive security parameters

6) Data protection provisions for consumer IoT

5.8) Ensure that personal data is secure

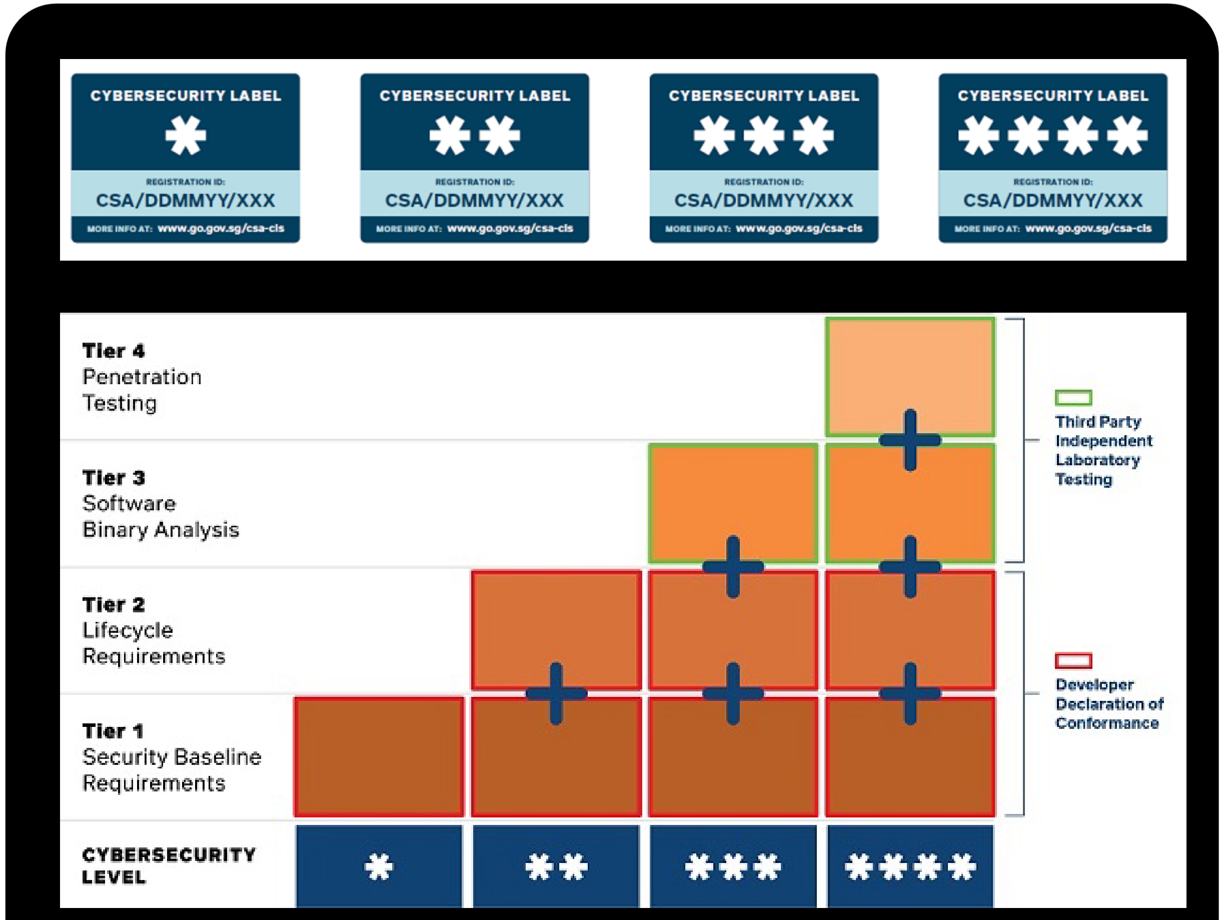
5.7) Ensure software integrity

5.6) Minimise exposed attack surfaces

5.5) Communicate securely

Annex B) Implementation conformance statement pro forma

EUROPEAN STANDARD ETSI EN 303 645
Cyber Security for Consumer Internet of Things: Baseline Requirements



CYBERSECURITY LABEL
✱
REGISTRATION ID:
CSA/DDMMYY/XXX
MORE INFO AT: www.go.gov.sg/csa-cls

CYBERSECURITY LABEL
✱✱
REGISTRATION ID:
CSA/DDMMYY/XXX
MORE INFO AT: www.go.gov.sg/csa-cls

CYBERSECURITY LABEL
✱✱✱
REGISTRATION ID:
CSA/DDMMYY/XXX
MORE INFO AT: www.go.gov.sg/csa-cls

CYBERSECURITY LABEL
✱✱✱✱
REGISTRATION ID:
CSA/DDMMYY/XXX
MORE INFO AT: www.go.gov.sg/csa-cls

Tier 4 Penetration Testing

Tier 3 Software Binary Analysis

Tier 2 Lifecycle Requirements

Tier 1 Security Baseline Requirements

CYBERSECURITY LEVEL ✱ ✱✱ ✱✱✱ ✱✱✱✱

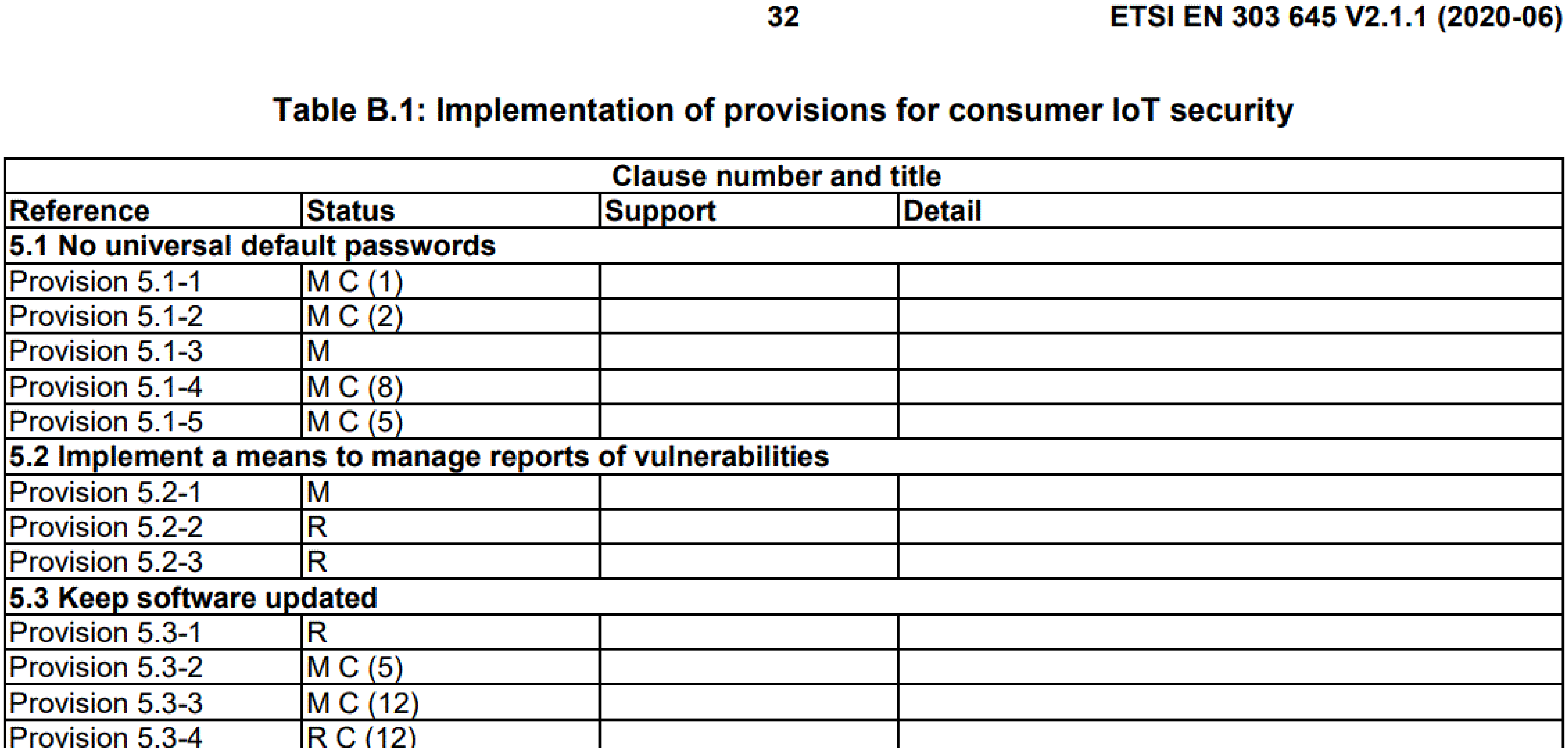
🟩 Third Party Independent Laboratory Testing

🟥 Developer Declaration of Conformance

CSA Singapore Cybersecurity Labelling Scheme

Source: https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/for-manufacturers
https://www.etsi.org/technologies/consumer-iot-security

ETSI EN 303 645



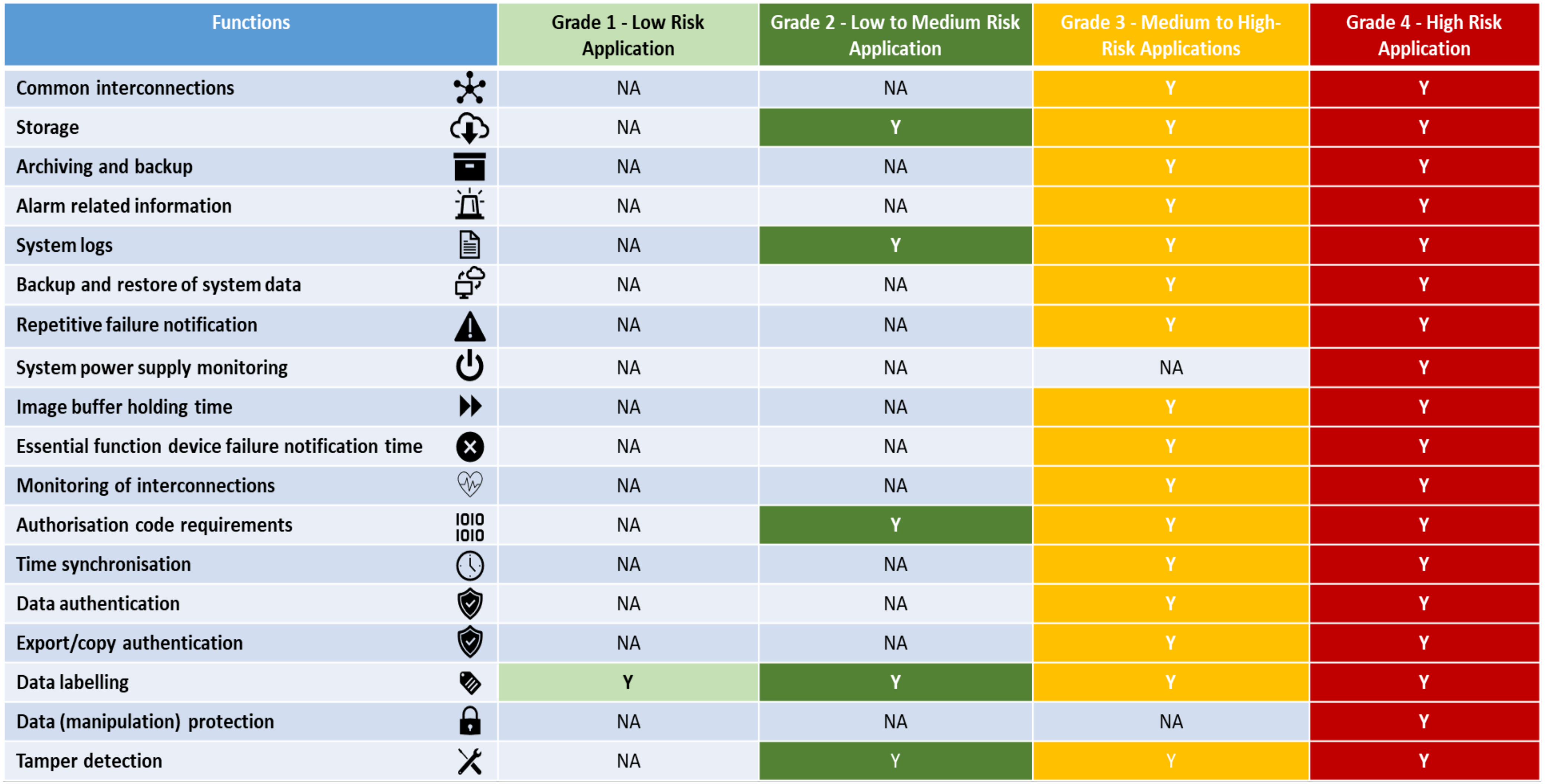
32 ETSI EN 303 645 V2.1.1 (2020-06)

Table B.1: Implementation of provisions for consumer IoT security

Clause number and title			
Reference	**Status**	**Support**	**Detail**
5.1 No universal default passwords			
Provision 5.1-1	M C (1)		
Provision 5.1-2	M C (2)		
Provision 5.1-3	M		
Provision 5.1-4	M C (8)		
Provision 5.1-5	M C (5)		
5.2 Implement a means to manage reports of vulnerabilities			
Provision 5.2-1	M		
Provision 5.2-2	R		
Provision 5.2-3	R		
5.3 Keep software updated			
Provision 5.3-1	R		
Provision 5.3-2	M C (5)		
Provision 5.3-3	M C (12)		
Provision 5.3-4	R C (12)		

Source: ETSI

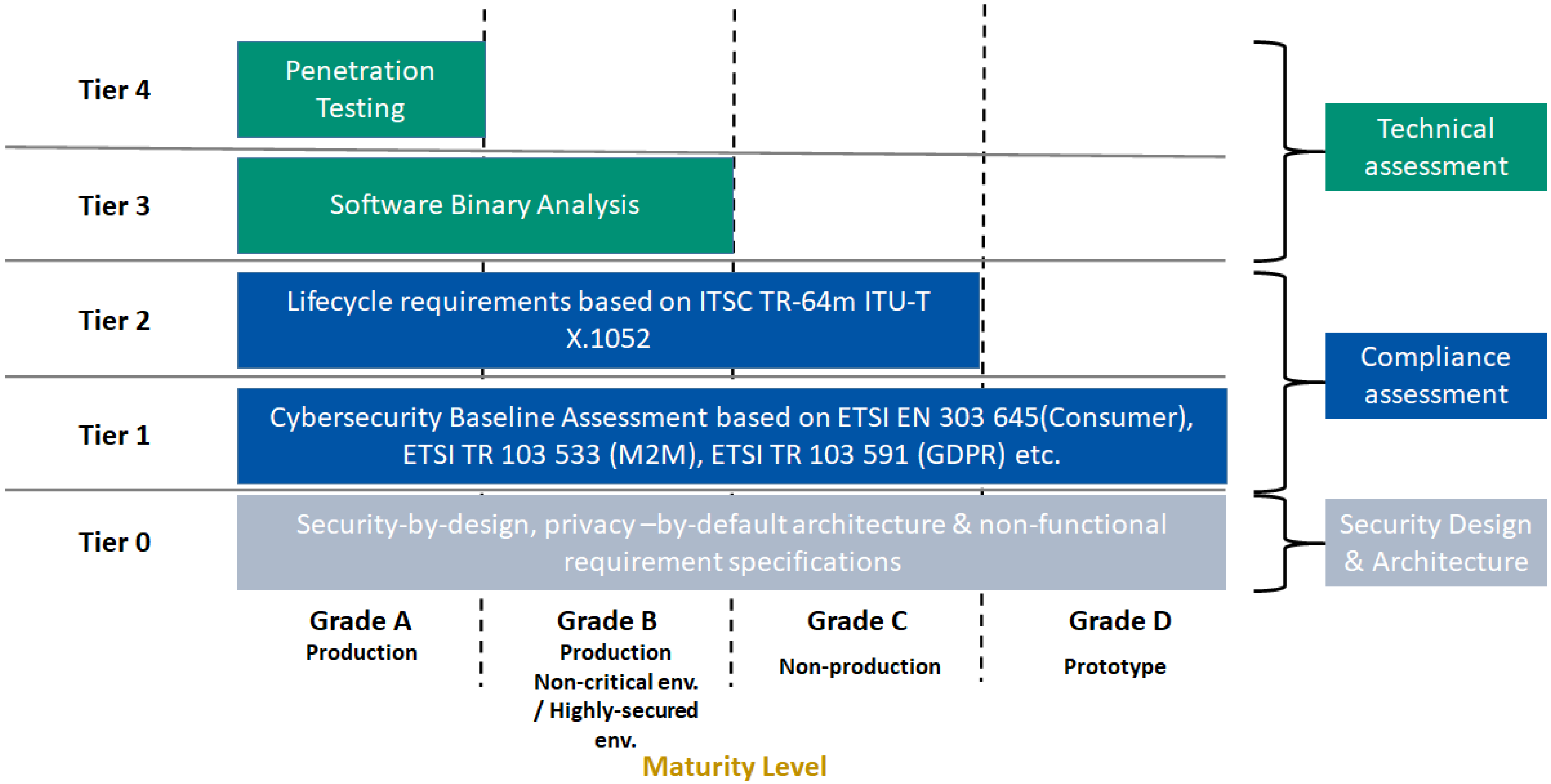
BS EN 62676-1



Functions	Grade 1 - Low Risk Application	Grade 2 - Low to Medium Risk Application	Grade 3 - Medium to High-Risk Applications	Grade 4 - High Risk Application
Common interconnections	NA	NA	Y	Y
Storage	NA	Y	Y	Y
Archiving and backup	NA	NA	Y	Y
Alarm related information	NA	NA	Y	Y
System logs	NA	Y	Y	Y
Backup and restore of system data	NA	NA	Y	Y
Repetitive failure notification	NA	NA	Y	Y
System power supply monitoring	NA	NA	NA	Y
Image buffer holding time	NA	NA	Y	Y
Essential function device failure notification time	NA	NA	Y	Y
Monitoring of interconnections	NA	NA	Y	Y
Authorisation code requirements	NA	Y	Y	Y
Time synchronisation	NA	NA	Y	Y
Data authentication	NA	NA	Y	Y
Export/copy authentication	NA	NA	Y	Y
Data labelling	Y	Y	Y	Y
Data (manipulation) protection	NA	NA	NA	Y
Tamper detection	NA	Y	Y	Y

Source: BSI

IoT Maturity Model



Tier 4: Penetration Testing

Tier 3: Software Binary Analysis

Tier 2: Lifecycle requirements based on ITSC TR-64m ITU-T X.1052

Tier 1: Cybersecurity Baseline Assessment based on ETSI EN 303 645(Consumer), ETSI TR 103 533 (M2M), ETSI TR 103 591 (GDPR) etc.

Tier 0: Security-by-design, privacy –by-default architecture & non-functional requirement specifications

Technical assessment

Compliance assessment

Security Design & Architecture

Grade A: Production

Grade B: Production Non-critical env. / Highly-secured env.

Grade C: Non-production

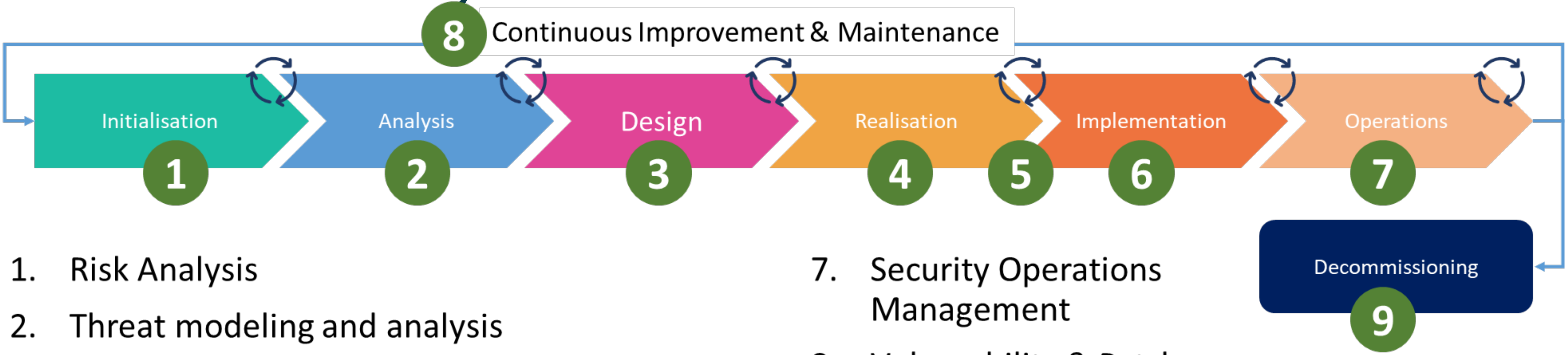
Grade D: Prototype

Maturity Level

Source: CSA Singapore

Advice & References

Security-by-design Compliance/Privacy-by-default lifecycle



1. Risk Analysis
2. Threat modeling and analysis
3. Secure design & architecture
4. Security testing, scanning & code/configuration review
5. Penetration testing
6. Hardening & Enforcement
7. Security Operations Management
8. Vulnerability & Patch Management
9. Secure Decommissioning

Free HKCERT IoT Security Best Practices

Response to Threats During Work from Home Arrangements

- **Cloud Storage Security** and **Data Protection** Guideline
- Assessing the Security of **Remote Access Services** Guideline
- Enterprise Guideline
- Six Secur e **Office**

IoT

Security Best Practice Guidelines

January 2020

IoT Security Best Practice Guideline

Emerging Technologies

- Security Study on IoT Wireless Technologies (**BLE, WiFi, ZigBee**) and IoT Security **Best Practice** Guidelines
- Introduce **Zero Trust** Architecture
- ity Re to S t
- e St g N ses
- uce g an ures
- duce cu ous Scan tec gies

IoT

Device (BLE) Security Study

February 2020

IoT BLE Security Study

IoT

Device (Wi-Fi) Security Study

March 2020

IoT Wi-Fi Security Study

IoT

Device (ZigBee) Security Study

April 2020

IoT Zigbee Security Study

https://www.hkcert.org/security-guideline

Source: HKCERTI

Guideline For Testing and Certification Requirement on 5G/IoT Devices

GUIDELINE FOR TESTING AND CERTIFICATION REQUIREMENT ON 5G/IOT DEVICES

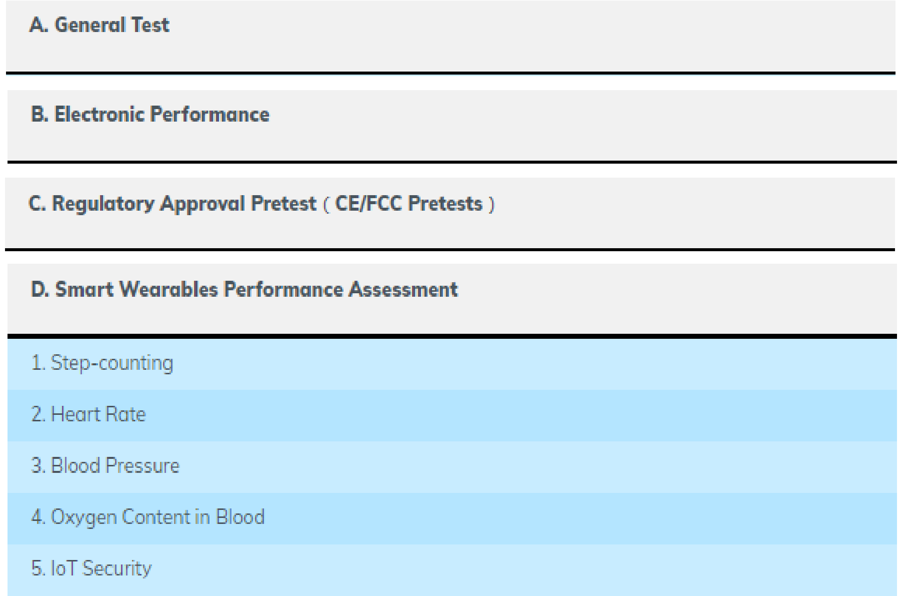
Organiser: hkpc

Funding Organisation:

Sponsor: ROHDE&SCHWARZ

SupportingO rganisations:

IOT AND 5G TESTS REQUIREMENT IN CYBERSECURITY



A. General Test

B. Electronic Performance

C. Regulatory Approval Pretest (CE/FCC Pretests)

D. Smart Wearables Performance Assessment

1. Step-counting
2. Heart Rate
3. Blood Pressure
4. Oxygen Content in Blood
5. IoT Security

- Released “**Guideline for Testing and Certification Requirements on 5G/IoT Device**” in 2021

Reference: https://www.hkpc.org/sites/default/files/2021-11/gsp-guidebook.pdf
https://www.hkpc.org/en/support-resource/support-centers/smart-wearables-watch-clock-technology-centre#introduction

Thank you!

Frank CHOW
Head of Cyber Security and HKCERT
Digital Transformation Division

frankchow@hkpc.org
frankchow@hkcert.org
+852 2788 5420
https://www.hkcert.org

Hong Kong Productivity Council
香港生產力促進局

HKPC Building, 78 Tat Chee Avenue, Kowloon, Hong Kong
香港九龍達之路78號生產力大樓
+852 2788 5678   www.hkpc.org