DNS Abuse and the IoT

Case Study on IoT innovated applications in Taiwan

ICANN75 Tech Day
2022.09.19

Chia-Ling Ho
Taiwan Telecom Technology Center

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

Contents

- Research Background/ Limitations
- Research Methodology
- Research Objectives
- Studied Cases
- Research Findings

Background

- Research **Scope**:
- ➢ 1**.** IoT industry: study cases of Critical Infrastructure in Taiwan (using 5G as IoT field primary communication protocol)
- ➢ 2. DNS abuse definition: primarily on internet integrity and cyber-resilience

- **ICANN SAC105** on IoT and DNS, and **5G** report overview

- **TTC's domain of expertise** on Cybersecurity, authentication, and certification labs (TAF, TAICS, UL and so on)

- **Taiwan Vulnerability Note** from TWCERT/CC(Taiwan Computer Emergency Response Team/Coordination Center) about the IoT devices and its scale.

Background

Taiwan Vulnerability Note about the IoT devices (2021/2022)

Device	Quantity	CNA *	Number
Webcam	5	TWCERT/CC	CVE*-2021-30165、CVE-2021-30166、CVE-2021-30167、CVE-2021-30168、CVE-2021-30169
Network Attached Storage Device	149	TWCERT/CC	CVE-2021-32506、CVE-2021-32507、CVE-2021-32508、CVE-2021-32509、CVE-2021-32510、CVE-2021-32511、CVE-2021-32512、CVE-2021-32513、CVE-2021-32514、CVE-2021-32515、CVE-2021-32516、CVE-2021-32517、CVE-2021-32518、CVE-2021-32519、CVE-2021-32520、CVE-2021-32521、CVE-2021-32522、CVE-2021-32523、CVE-2021-32524、CVE-2021-32525、CVE-2021-32526、CVE-2021-32527、CVE-2021-32528、CVE-2021-32529、CVE-2021-32530、CVE-2021-32531、CVE-2021-32532、CVE-2021-32533、CVE-2021-32534、CVE-2021-32535、CVE-2021-37216
		Z**el	CVE-2022-34747
		S*****gy	CVE-2022-27621、CVE-2022-27620、CVE-2022-27619、CVE-2022-27618、CVE-2022-27617、CVE-2022-27616、CVE-2022-27615、CVE-2022-27614、CVE-2022-27613、CVE-2022-27612、CVE-2022-27611、CVE-2022-27610、CVE-2022-22688、CVE-2022-22687、CVE-2022-22686、CVE-2022-22685、CVE-2022-22684、CVE-2022-22683、CVE-2022-22682、CVE-2022-22681、CVE-2022-22680、CVE-2022-22679、CVE-2021-43929、CVE-2021-43928、CVE-2021-43927、CVE-2021-43926、CVE-2021-43925、CVE-2021-34812、CVE-2021-34811、CVE-2021-34810、CVE-2021-34809、CVE-2021-34808、CVE-2021-33184、CVE-2021-33183、CVE-2021-33182、CVE-2021-33181、CVE-2021-33180、CVE-2021-31439、CVE-2021-29092、CVE-2021-29091、CVE-2021-29090、CVE-2021-29089、CVE-2021-29088、CVE-2021-29087、CVE-2021-29086、CVE-2021-29085、CVE-2021-29084、CVE-2021-29083、CVE-2021-27649、CVE-2021-27648、CVE-2021-27647、CVE-2021-27646、CVE-2021-26569、CVE-2021-26566、CVE-2021-26565、CVE-2021-26564、CVE-2021-26563、CVE-2021-26562、CVE-2021-26561、CVE-2021-26560
		Q**P	CVE-2021-44057、CVE-2021-44056、CVE-2021-44055、CVE-2021-44054、CVE-2021-44053、CVE-2021-44052、CVE-2021-44051、CVE-2021-38693、CVE-2021-38692、CVE-2021-38691、CVE-2021-38690、CVE-2021-38689、CVE-2021-38687、CVE-2021-38686、CVE-2021-38685、CVE-2021-38684、CVE-2021-38683、CVE-2021-38682、CVE-2021-38681、CVE-2021-38680、CVE-2021-38679、CVE-2021-38678、CVE-2021-38677、CVE-2021-38675、CVE-2021-34362、CVE-2021-34361、CVE-2021-34360、CVE-2021-34359、CVE-2021-34357、CVE-2021-34356、CVE-2021-34355、CVE-2021-34354、CVE-2021-34352、CVE-2021-34351、CVE-2021-34349、CVE-2021-34348、CVE-2021-34346、CVE-2021-34345、CVE-2021-34344、CVE-2021-34343、CVE-2021-28816、CVE-2021-28815、CVE-2021-28814、CVE-2021-28813、CVE-2021-28812、CVE-2021-28807、CVE-2021-28806、CVE-2021-28805、CVE-2021-28804、CVE-2021-28803、CVE-2021-28802、CVE-2021-28801、CVE-2021-28800、CVE-2021-28800、CVE-2021-28799、CVE-2021-28798、CVE-2021-28797、

*CNA: CVE Numbering Authorities

*CVE, Common Vulnerabilities and Exposures

Background

Taiwan Vulnerability Note about the IoT devices (2021/2022)

Device	Quantity	CNA	Number
MCU – Multipoint Control Unit	1	TWCERT/CC	CVE-2021-32536
Audio Driver	1	TWCERT/CC	CVE-2021-32537
Wireless projector	1	TWCERT/CC	CVE-2021-37911
BAS controller	13	TWCERT/CC	CVE-2021-41290、CVE-2021-41291、CVE-2021-41292、CVE-2021-41293、CVE-2021-41294、CVE-2021-41295、CVE-2021-41296、CVE-2021-41297、CVE-2021-41298、CVE-2021-41299、CVE-2021-41300、CVE-2021-41301、CVE-2021-41302
Wireless router	10	TWCERT/CC	CVE-2021-37910、CVE-2021-41289
		Z***l	CVE-2022-26414、CVE-2022-26413、CVE-2021-4030、CVE-2021-4029、CVE-2021-35035、CVE-2021-35034、CVE-2021-35033、CVE-2021-3297
Router	12	TWCERT/CC	CVE-2021-44158、CVE-2022-22054、CVE-2022-23970、CVE-2022-23971、CVE-2022-23972、CVE-2022-23973、CVE-2022-25595、CVE-2022-25596、CVE-2022-25597、CVE-2022-26670、CVE-2022-26673、CVE-2022-26674
Laptop	1	TWCERT/CC	CVE-2022-21933
USB Card Reader Drive	1	TWCERT/CC	CVE-2022-21742
Cyber security	10	Z***l	CVE-2022-30526、CVE-2022-30525、CVE-2022-26532、CVE-2022-26531、CVE-2022-2030、CVE-2022-0910、CVE-2022-0734、CVE-2022-0342、CVE-2021-46387、CVE-2021-35029
Switch	4	Z***l	CVE-2022-0823、CVE-2021-35032、CVE-2021-35031、CVE-2021-35030
Wireless Base Station	2	Z***l	CVE-2022-0556、CVE-2021-4039
VPN Gateway	2	Z***l	CVE-2021-35028、CVE-2021-35027
Chips	22	M******k	CVE-2021-41788、CVE-2021-37584、CVE-2021-37583、CVE-2021-37572、CVE-2021-37571、CVE-2021-37570、CVE-2021-37569、CVE-2021-37568、CVE-2021-37567、CVE-2021-37566、CVE-2021-37565、CVE-2021-37564、CVE-2021-37563、CVE-2021-37562、CVE-2021-37561、CVE-2021-37560、CVE-2021-35055、CVE-2021-32469、CVE-2021-32468、CVE-2021-32467、CVE-2021-30636、CVE-2021-25477

Objectives

- Our contribution on Taiwan’s cybersecurity standards for IoT security
- Establishing a basic understanding of the level of DNS Abuse awareness and decision-making policies amongst the multi-stakeholders of the IoT industry
- Through our empirical case studies to polish IoT security regulations and standards, and to generate recommendations for the IoT technology developers and end-users defend their systems and reducing DNS threats

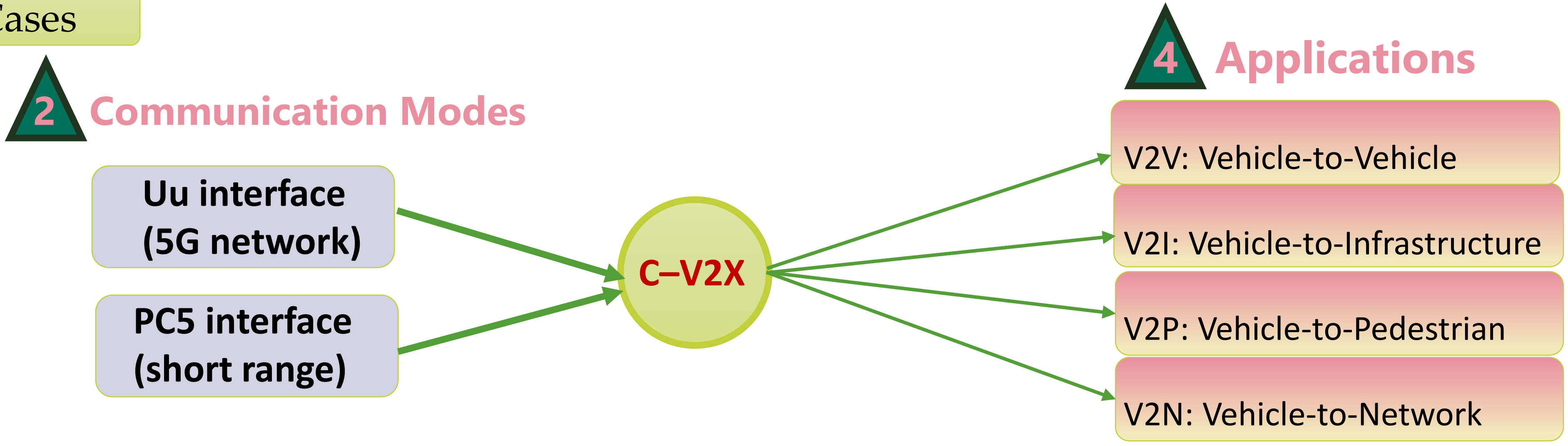
Methodology

- Data from Published studies, other publications, such as reports and academic journals, mainly from IEEE, ICANN and IETF.

- Evidence gathering from sources, such as relevant individual stakeholders, trade associations, experts, academics, public or government bodies which involved in our current examined IoT cases.
  - Questionnaires
  - Interviews

Presenting Case : C-V2X

Studied Cases



2 Communication Modes

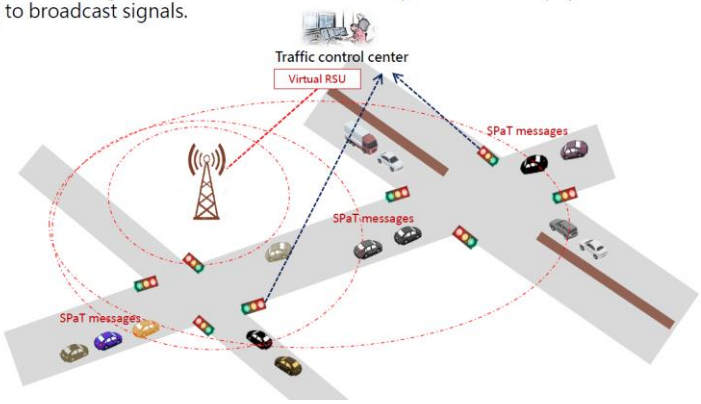
- Uu interface (5G network)
- PC5 interface (short range)

C–V2X

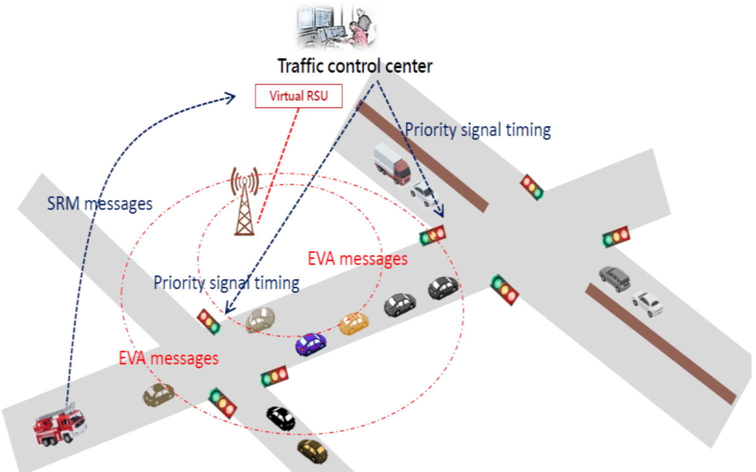
4 Applications

- V2V: Vehicle-to-Vehicle
- V2I: Vehicle-to-Infrastructure
- V2P: Vehicle-to-Pedestrian
- V2N: Vehicle-to-Network

Signal Phase and Timing (SPaT): One base station can replace dozens of physical roadside units (RSUs) to broadcast signals.



Signal Request Message (SRM), Emergency Vehicle Alert (EVA): The traffic control cente can use the base station to evacuate surrounding vehicles in advance.

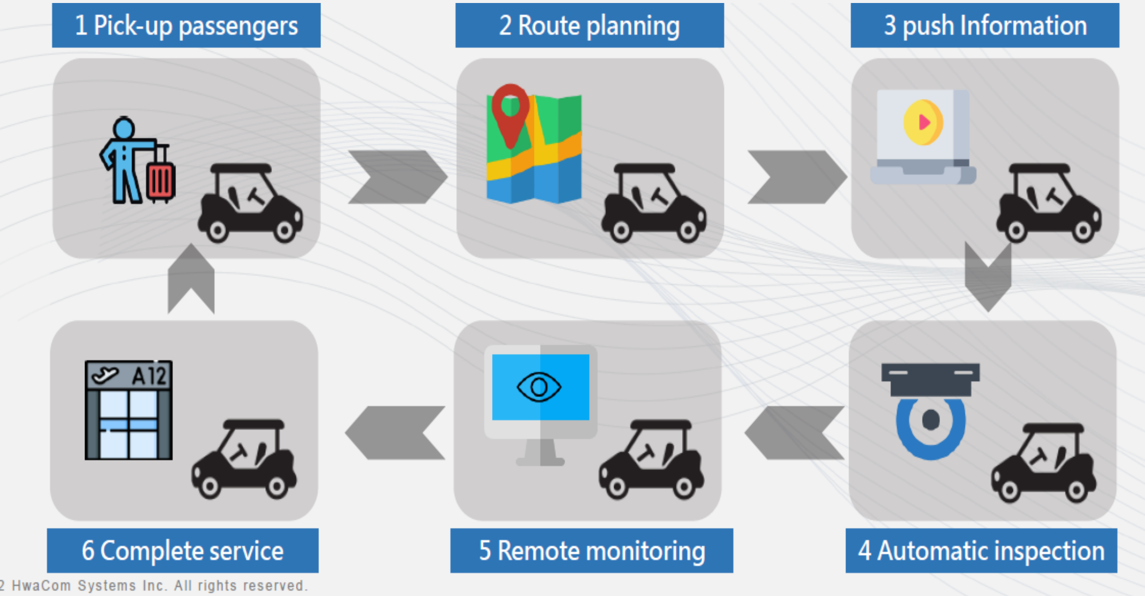


Time-critical applications still need to deploy roadside units (RSUs) to deliver warning messages quickly.
Something like **Vulnerable Road Users (VRUs) Protection.**

Source: Cht

Presenting Cases: Smart airport

Studied Cases



Intelligence travel carrier

Smart disinfection vehicle

Source: HwaCom Systems Inc.

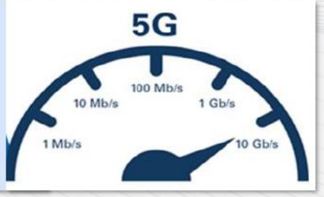
Back-end system functions and environments

Service field information displayed

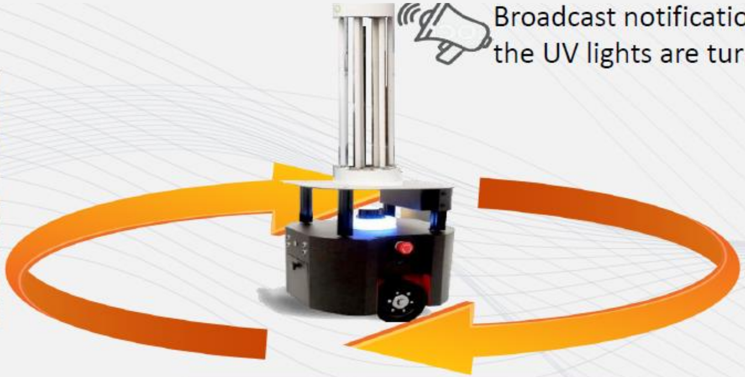
Remote control interface

Report of an incident

Bandwidth peaks(UL&DL)



Airport space tour,
Continuous disinfection of the environment

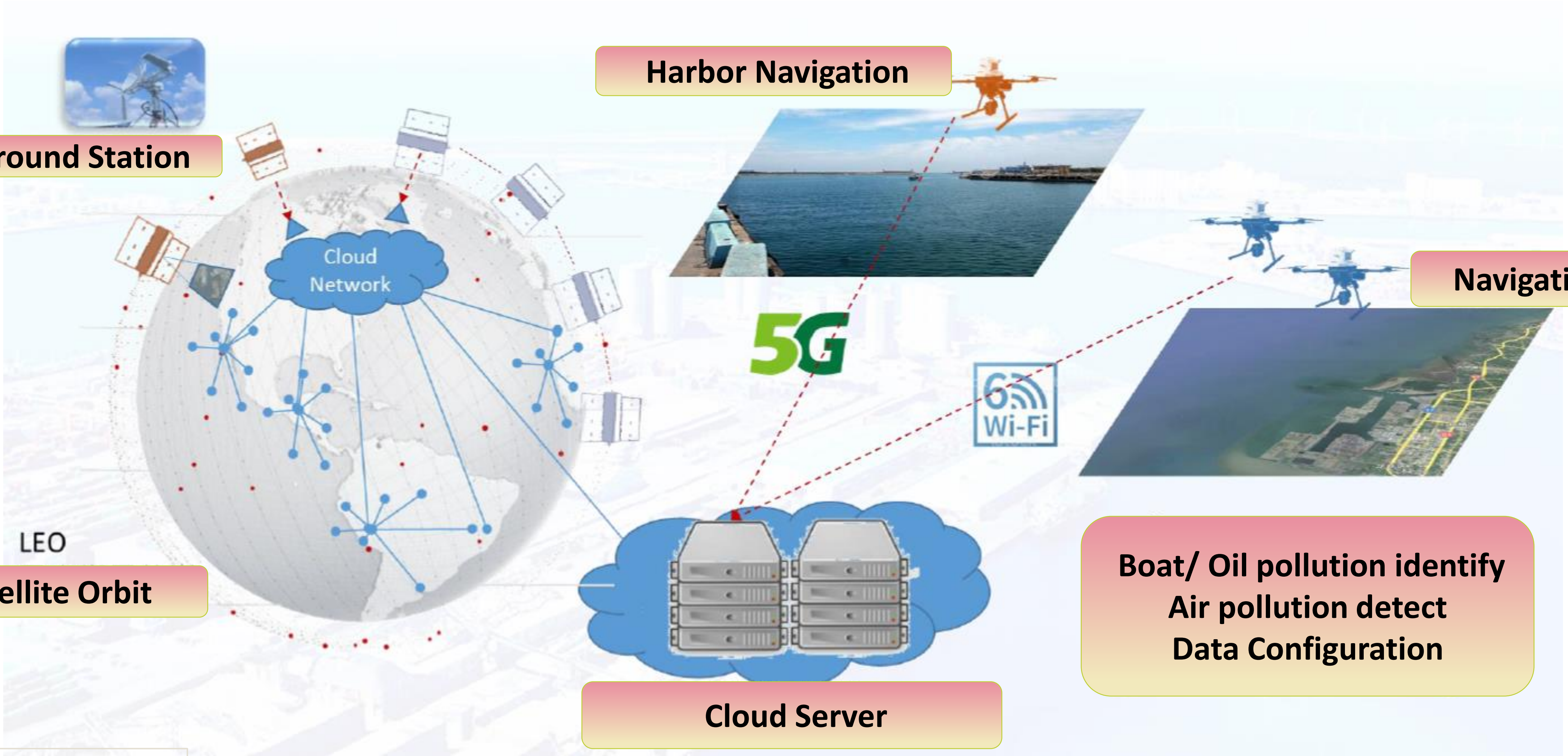


Broadcast notifications before the UV lights are turned on

1. Patrol disinfection
2. Task assignment disinfection

In accordance with the planned tasks,
Regular disinfection of the toilet environment

Presenting Cases: Smart Harbor

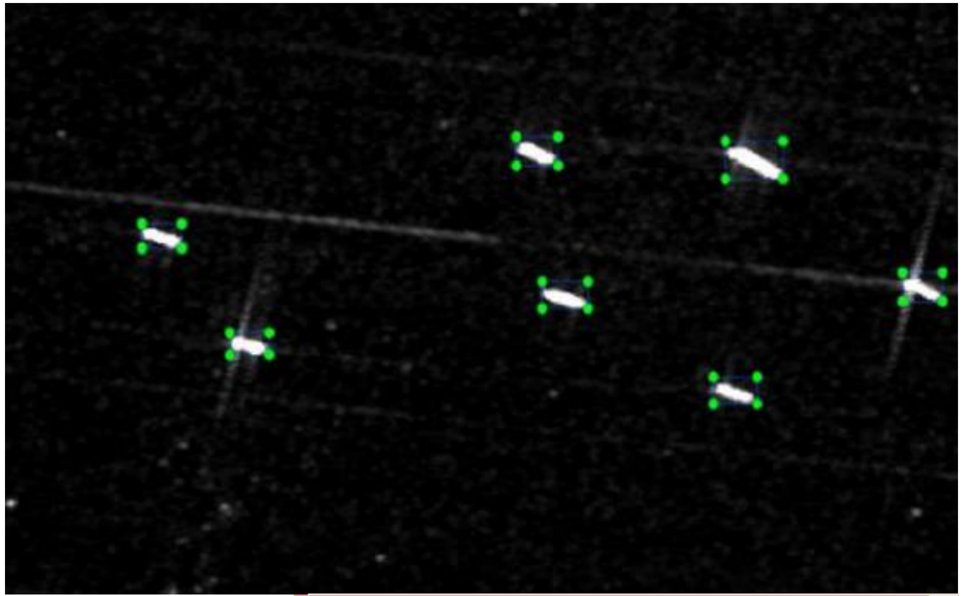


Source: Aptg

Presenting Cases: Smart Harbor

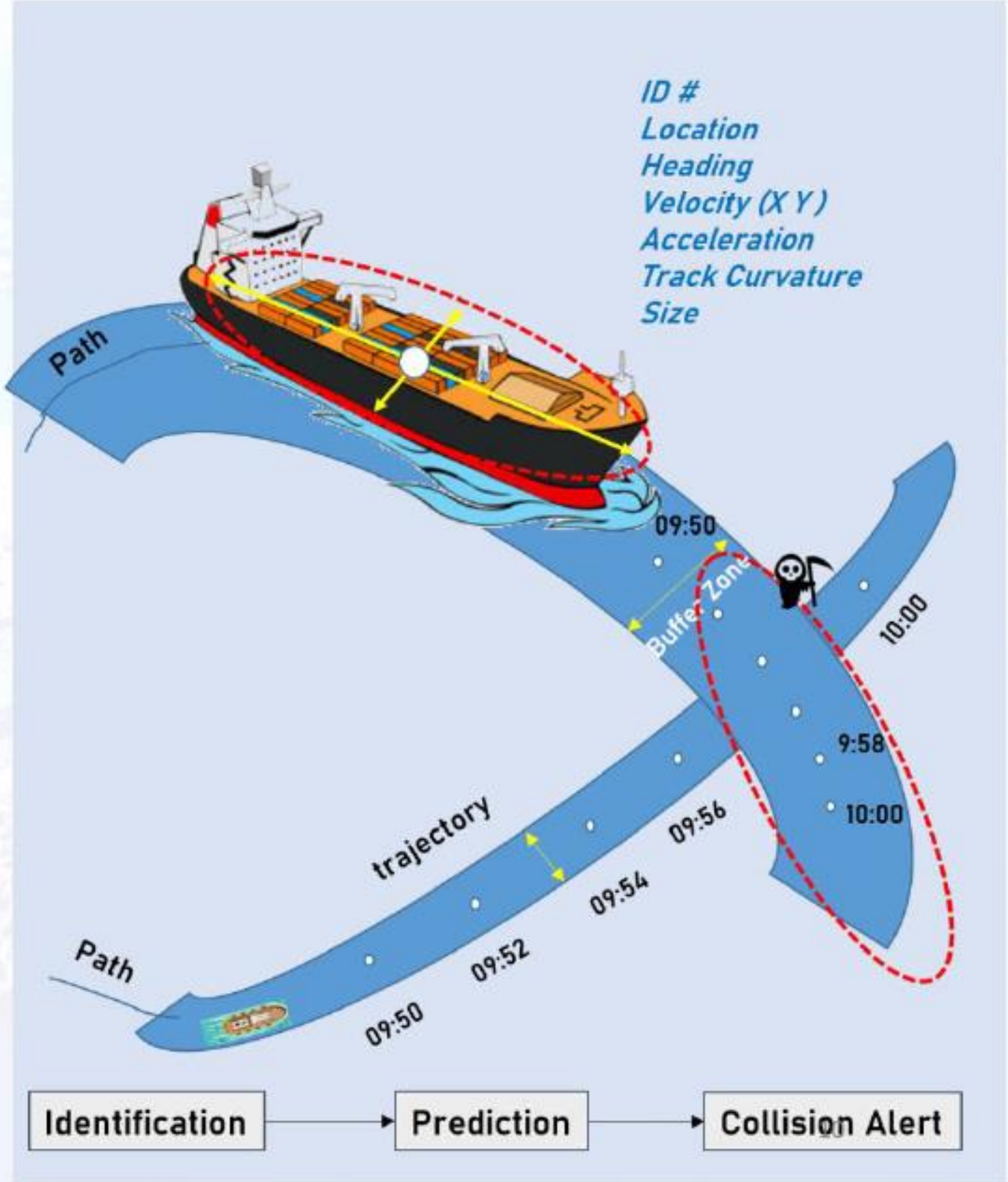
Studied Cases

- The ship has considerable inertia and cannot turn quickly, so collision often occurs. To avoid collision problems, the handling of "collision avoidance" is currently a goal of our government's security and safety plan.
- In the aerial photography operation of mobile UAVs, images recognized by the AI predict ship movement trajectory and send collision avoidance warnings.



Source: Aptg

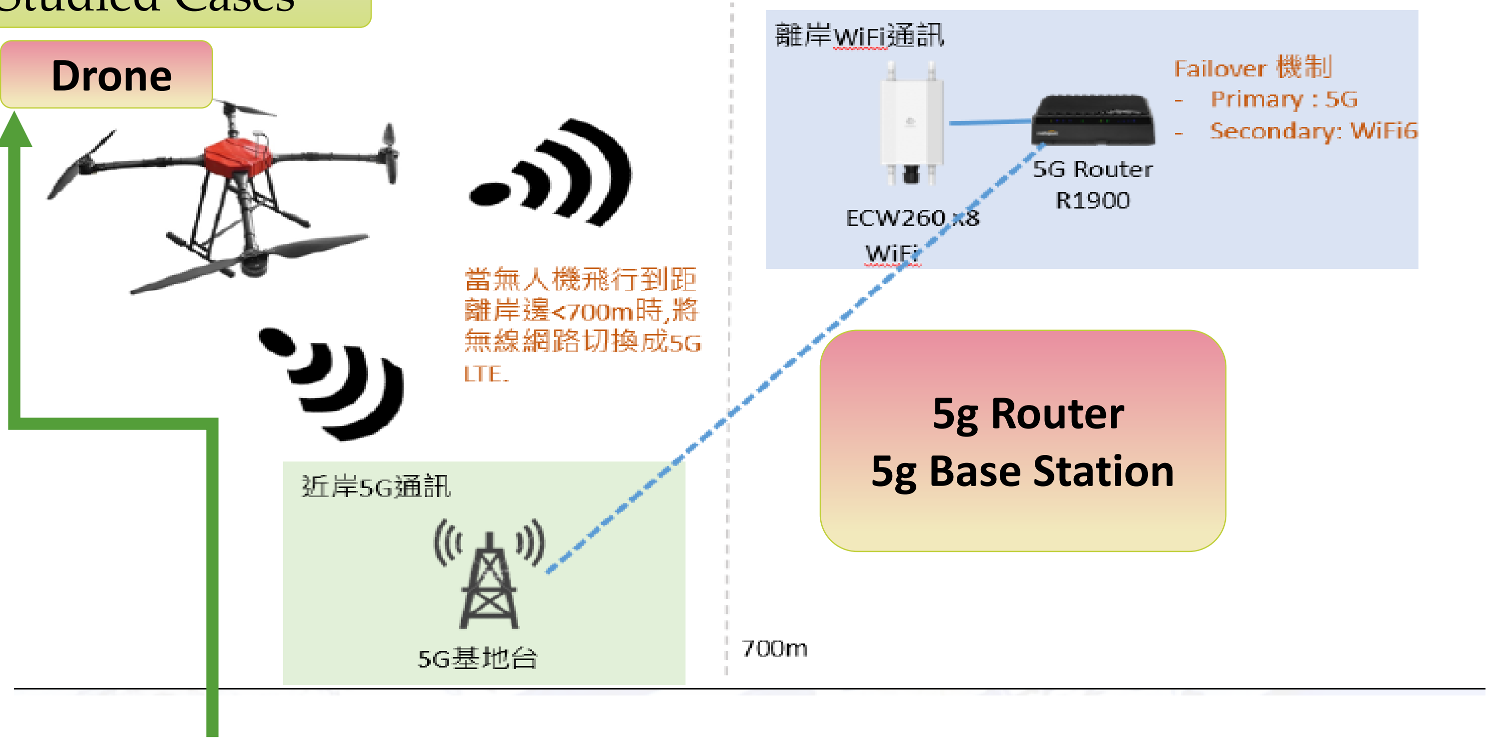
Labeling the image of boats



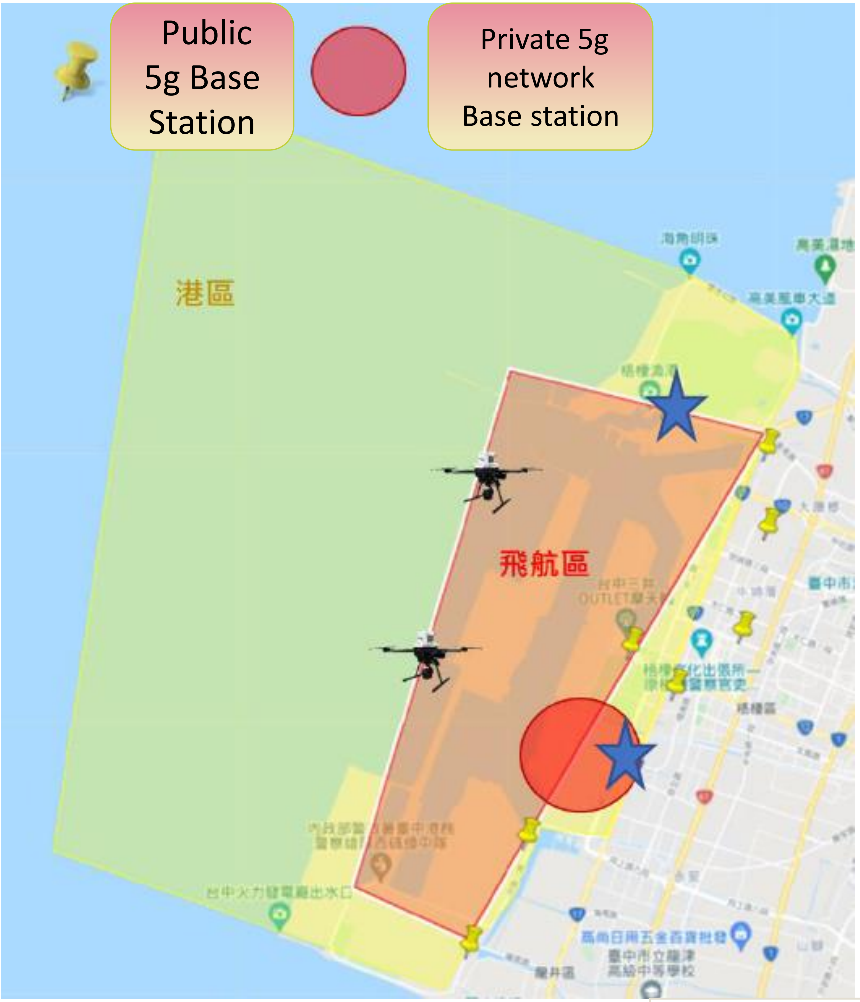
Presenting Cases: Smart Harbor

Studied Cases

Drone



5g Router
5g Base Station



Source: Aptg

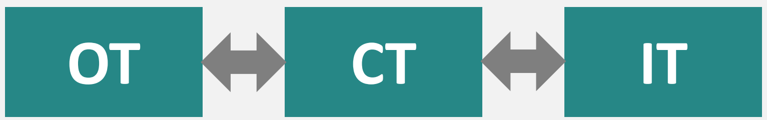
Web Cam

Optical Displacement Sensor

Infrared thermal sensor Camera (image)

4G and 5G IoT Systems’ Differences

Transform



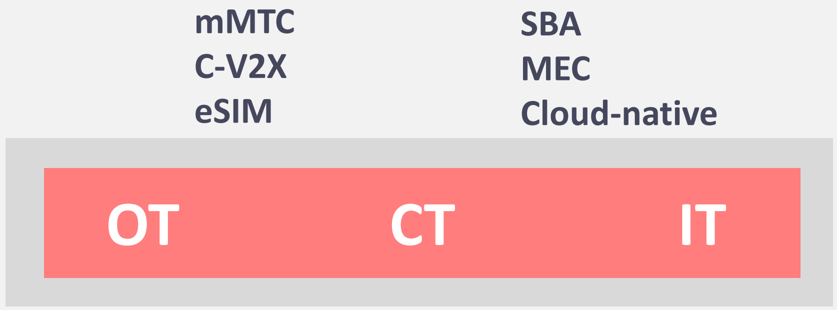
CT is an external device for verticals

OT: Operation Technology

CT: Communication Technology

IT: Information Technology

3G-4G

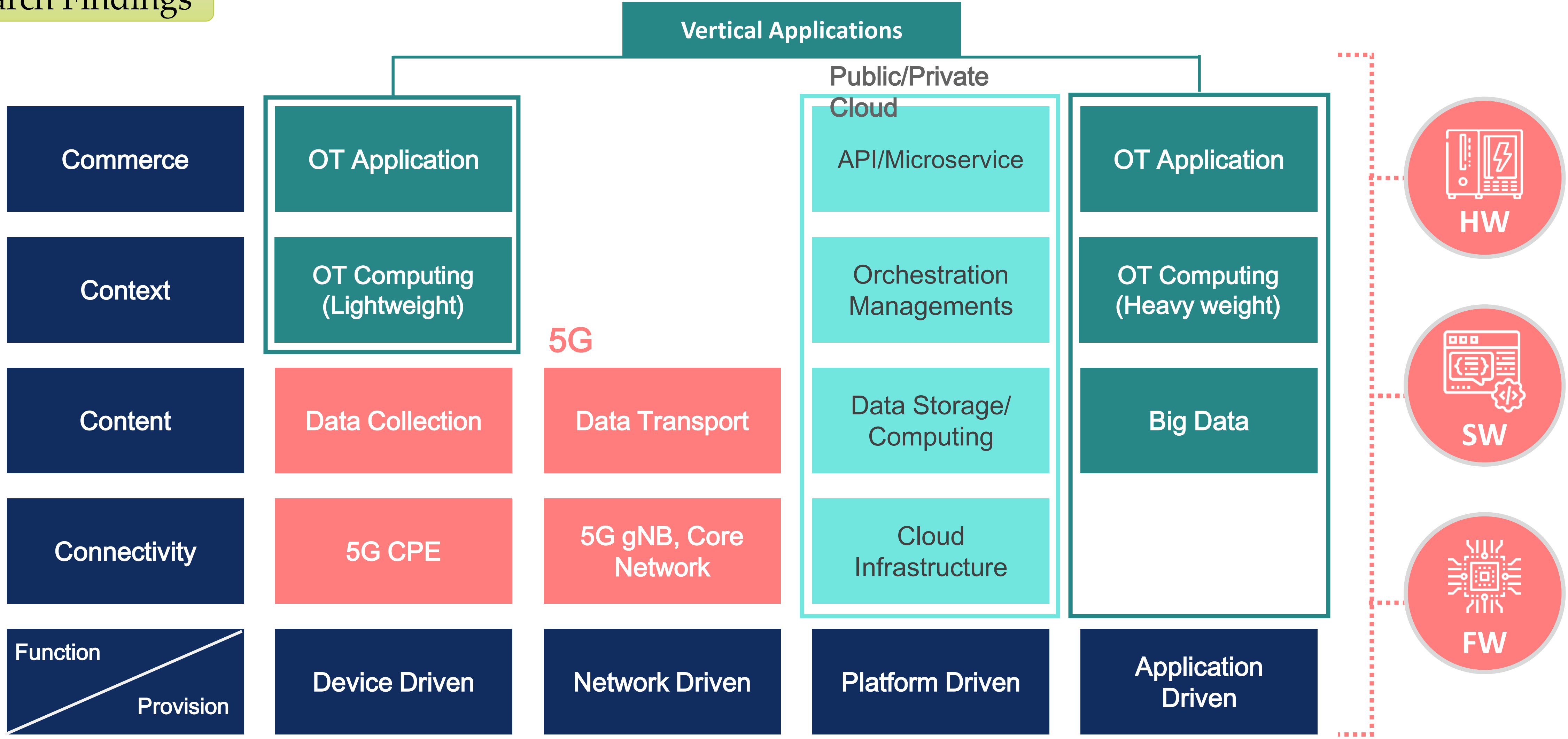


CT is natively designed to embed with the IoT systems and thus increases the security risks of vertical application systems

5G

Research Findings

High Complexity of 5G IoT Systems



Vertical Applications

Public/Private Cloud

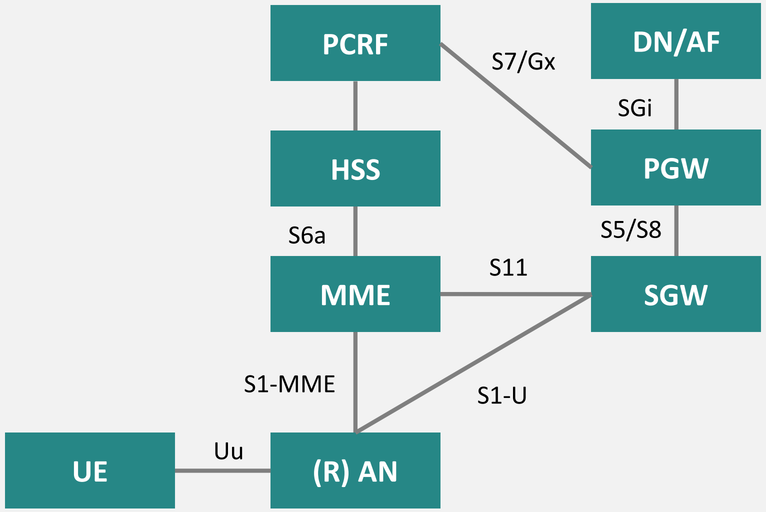
5G

Function / Provision	Device Driven	Network Driven	Platform Driven	Application Driven
Commerce	OT Application		API/Microservice	OT Application
Context	OT Computing (Lightweight)		Orchestration Managements	OT Computing (Heavy weight)
Content	Data Collection	Data Transport	Data Storage/ Computing	Big Data
Connectivity	5G CPE	5G gNB, Core Network	Cloud Infrastructure	

Source: TTC

Open and Service-Based Architecture(SBA)

Research Findings

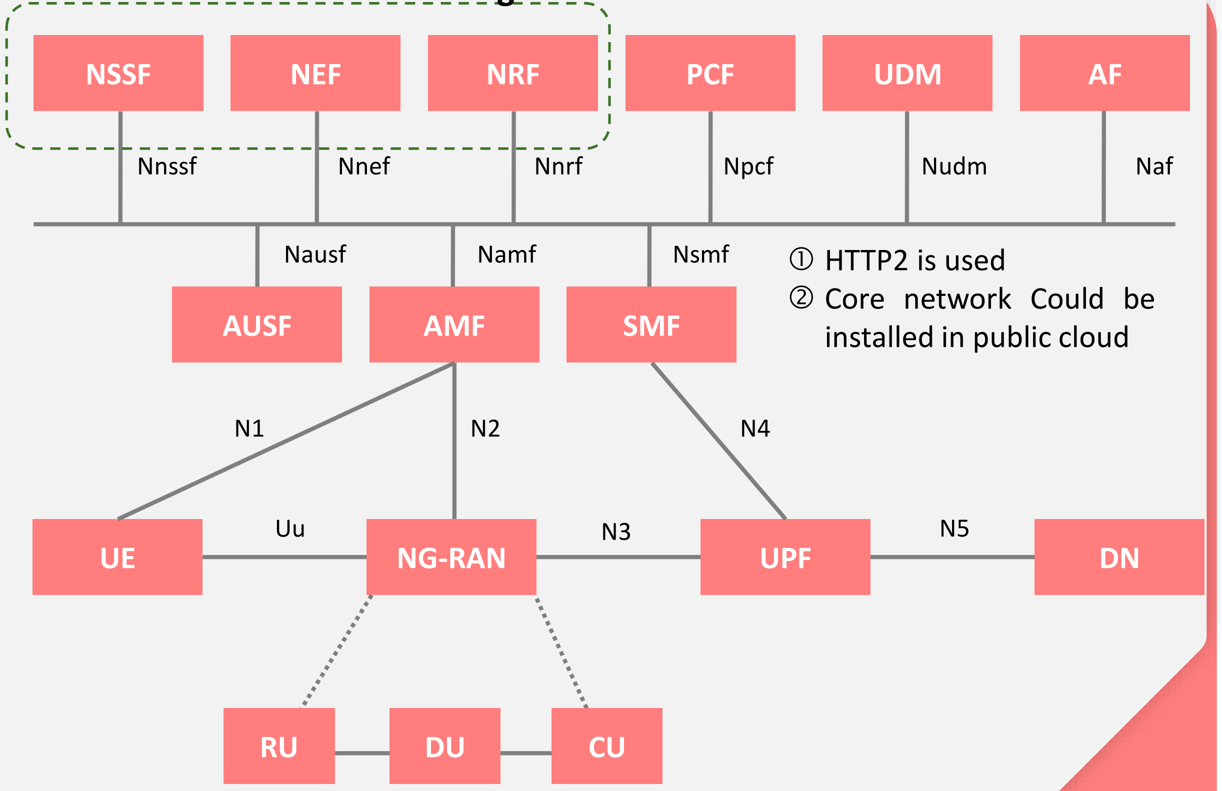


Although 4G is the all-IP network, it is a more closed network compared to 5G.

4G

Original :3GPP

New functions and SBA bring new risks



① HTTP2 is used
② Core network Could be installed in public cloud

Additional security risks from open RAN

5G

Research Findings

Security Practices of 5G IoT In Taiwan

5G Network Security

- The regulator clearly specifies the security requirements and obligations for the 5G operators in the telecom regulations.
- National Communications Commission (NCC) conducts periodic audit for each 5G operators.

IoT Device Security

- To promote the IoT certification and labeling programs
- Although the label is voluntary, more and more Government agencies regard it as an acceptance requirement of procurements.

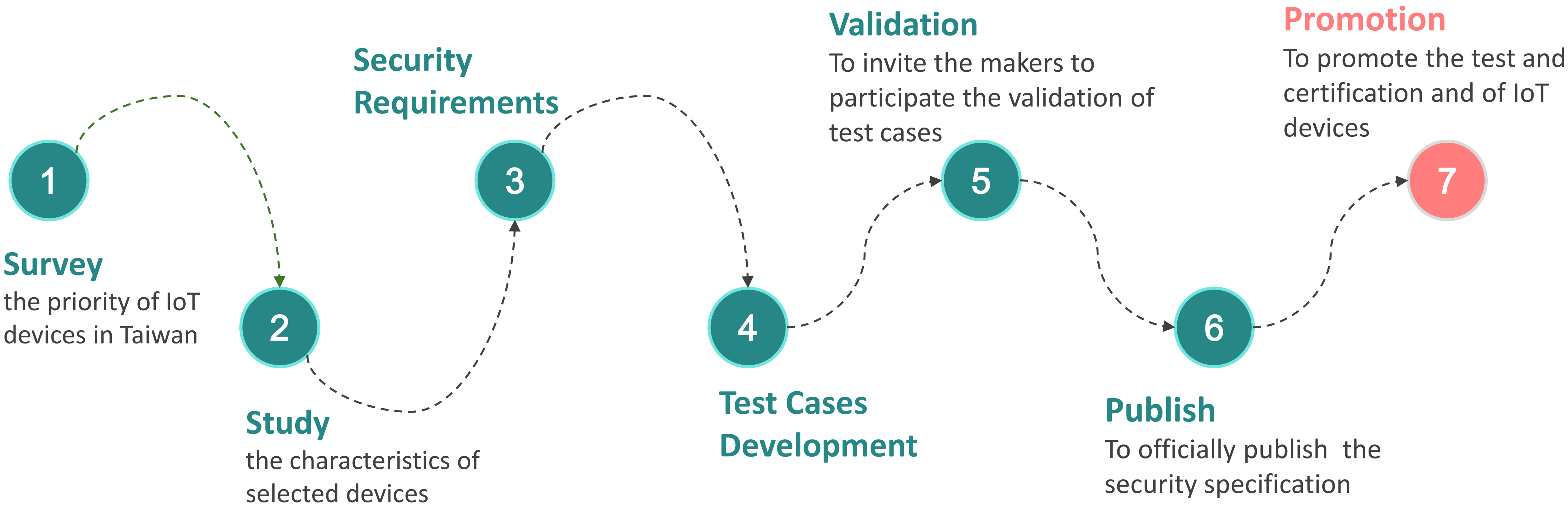
5G Verticals Security

- To publish the guideline of security evaluation for 5G IoT applications in the vertical Industries, where threat modeling, vulnerability testing, penetration testing, and impact analysis are included.
- To validate the security protection of the 5G IoT applications based on the aforementioned guideline.

Security Certification Programs of IoT Devices

Research Findings

To enact the cybersecurity testing specification of IoT devices, and promote the testing and labeling programs in Taiwan



1 **Survey**
the priority of IoT devices in Taiwan

2 **Study**
the characteristics of selected devices

3 **Security Requirements**

4 **Test Cases Development**

5 **Validation**
To invite the makers to participate the validation of test cases

6 **Publish**
To officially publish the security specification

7 **Promotion**
To promote the test and certification and of IoT devices

Cybersecurity Specifications for Selected IoT Devices

Research Findings

IoT Security Certification Marks in Taiwan

Level 3
Level 2
Level 1

2018

- IP cam
- Wi-Fi AP

2020

- Embedded software on smartphone systems
- Smart speakers
- Mobile Communication Repeater

2021

- Wireless broadband routers
- Wi-Fi AP /Wi-Fi Router
- Consumer IoT products
- Critical Telecom Security Products

2022

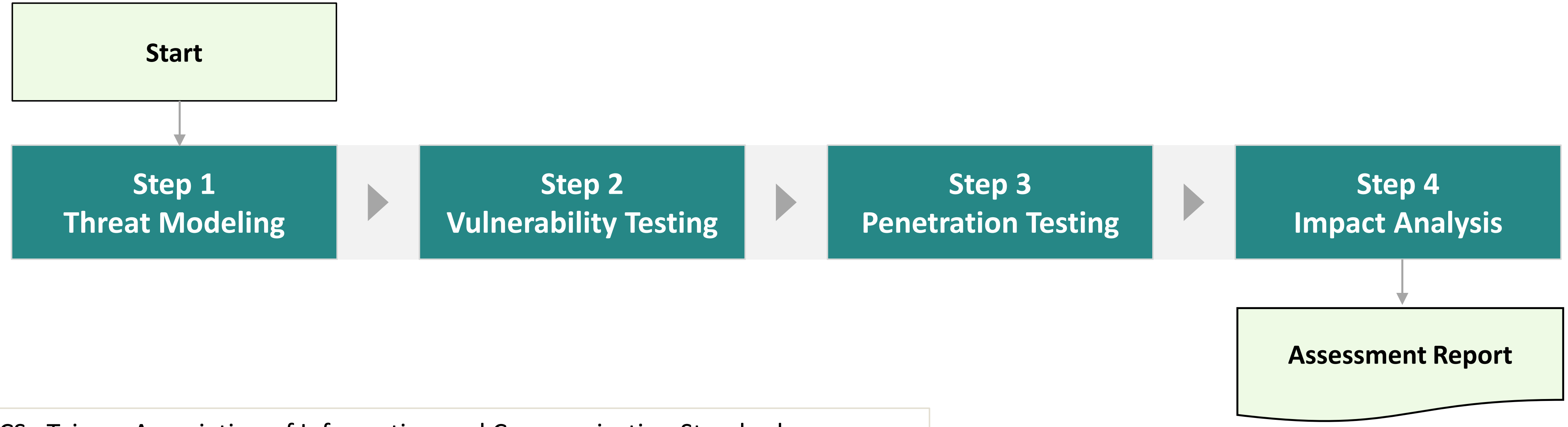
- Modem
- Digital Set Top Box

Guideline of Security Assessment for 5G IoT FIELD

Research Findings

The first End-to-End security assessment guideline for 5G IoT applications, which covers sensing layer, transport layer and application layer. (TAICS: TR 0022)

The evaluation process includes 4 phases listed as bellows.



*TAICS : Taiwan Association of Information and Communication Standards

The Contents Of The Security Guideline

Research Findings

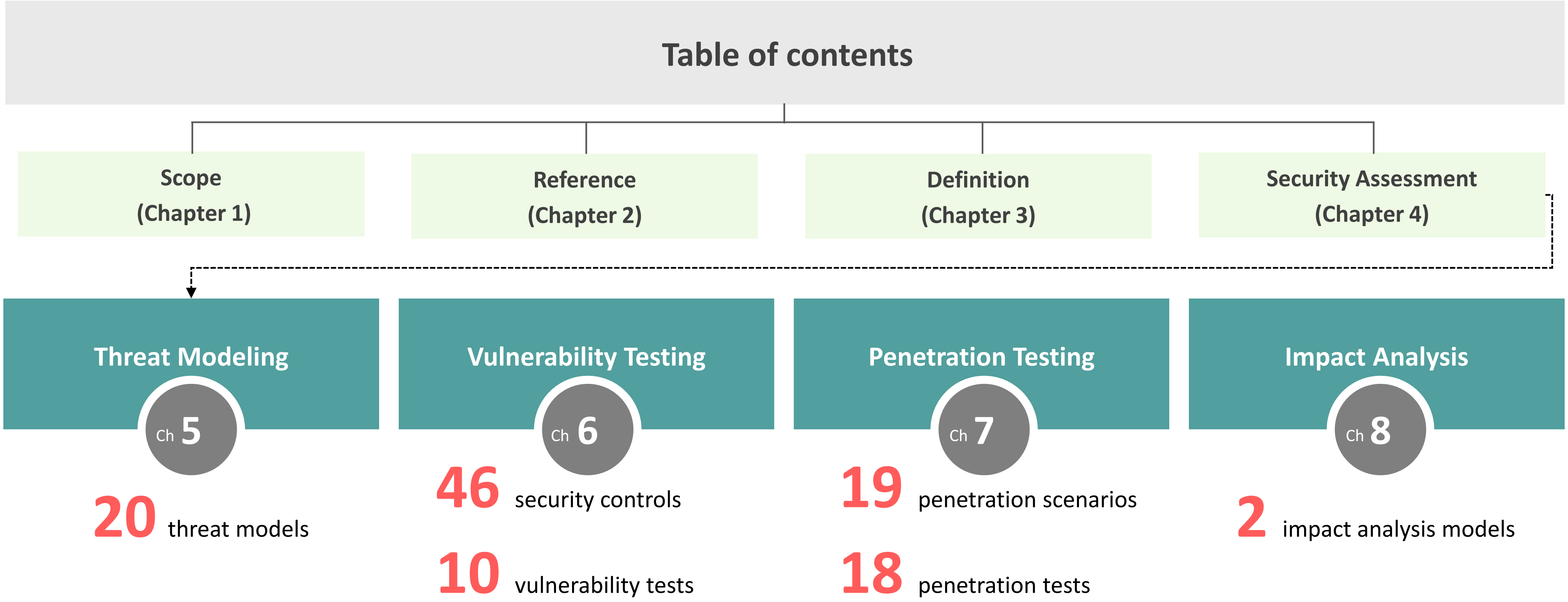


Table of contents

Scope (Chapter 1)

Reference (Chapter 2)

Definition (Chapter 3)

Security Assessment (Chapter 4)

Threat Modeling — Ch 5

20 threat models

Vulnerability Testing — Ch 6

46 security controls

10 vulnerability tests

Penetration Testing — Ch 7

19 penetration scenarios

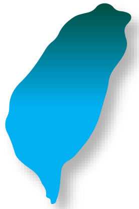
18 penetration tests

Impact Analysis — Ch 8

2 impact analysis models

Research Findings

IoT security Certifications Comparisons



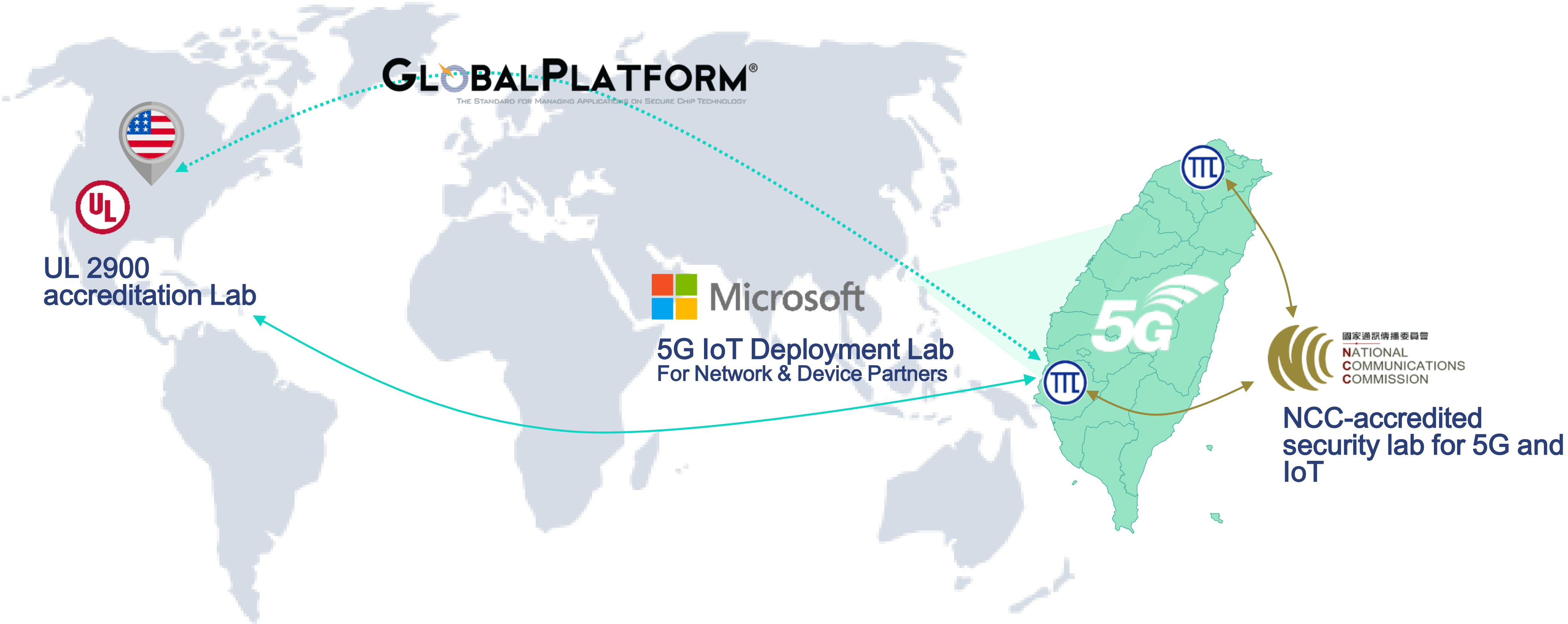
As of today, Taiwan's security guideline and certification for the **IoT field** is **an pioneer innovation relating to IoT security** .

Factors	Device certification	IoT Field certification(only Taiwan)
Time Consuming	Relatively short	Long
Scale (covered area)	Small and specific	Large and inclusive
Level of Security	Level 1,2 and 3	Level 1, 2 and 3
Certificate Usage	restricted	Practical and wildly accepted
ROI (Return on investment)	Medium	High(Funding by the government)

Connect With International Security Organizations

Research Findings

- Taiwan exports a large number of ICT products every year. With a worldwide increasing trend of security requirements, TTC's security Lab targets to be accredited by the international security standard organizations and assists Taiwanese manufacturers to comply with the security requirements.



GlobalPlatform®
The Standard for Managing Applications on Secure Chip Technology
UL
Microsoft
5G
國家通訊傳播委員會
National Communications Commission

UL 2900 accreditation Lab

5G IoT Deployment Lab
For Network & Device Partners

NCC-accredited security lab for 5G and IoT

Research findings

- Risks to the DNS from the IoT:
  - DDoS Attack, Botnets targeting the DNS…etc.

IoT hardware manufacturers	Enough market share
IoT software developers	Not enough market share
IoT firmware providers	Not enough market share

- Challenges for the DNS and IoT industries:

DNSSEC	not to be deployed due to lacking of consensus
Training IoT and DNS professionals	urgently needed
Shared system on botnets and DDoS attack	private company defense products preferred

Thank you for listening!