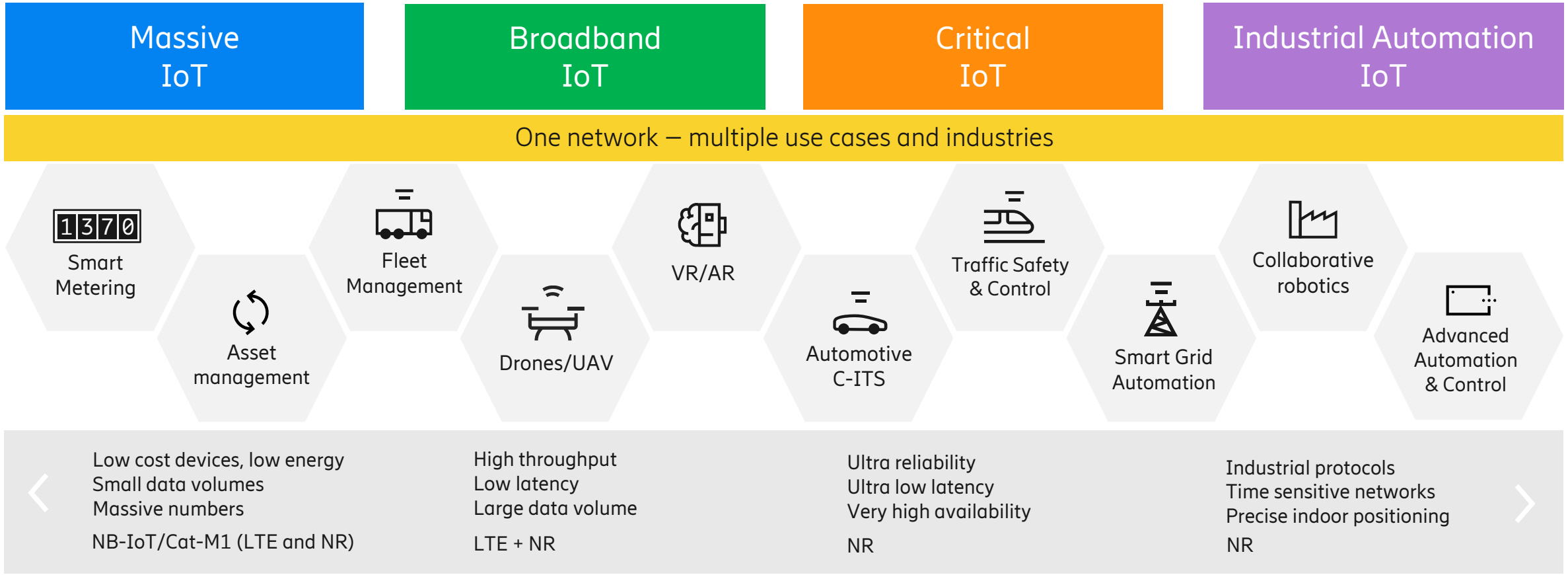
5G와 로봇 그리고 보안

October 2023

Dongjoo Park, Ph.D.
Professor, Dankook University
Chair, Ecosystem and Strategy Committee, 6G Forum
CEO, 5G Eco / MobilCon

Mobile system generations

Cellular IoT evolution and segments



Critical IoT – for ultra reliability, low latency

- 5G NR
- URLLC

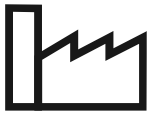
- 99.999% reliability
- 1ms one-way

- Local area/Wide area

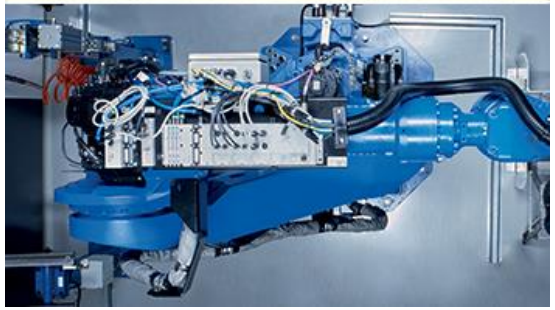
- Automotive
  Utilities,
  Smart Manufacturing
  in industry campus

- Autonomous vehicles
- Deeper integration with C-ITS systems
- Platooning

- Utilities – Smart Grids
- Renewables integrated into Grid
- Real time control

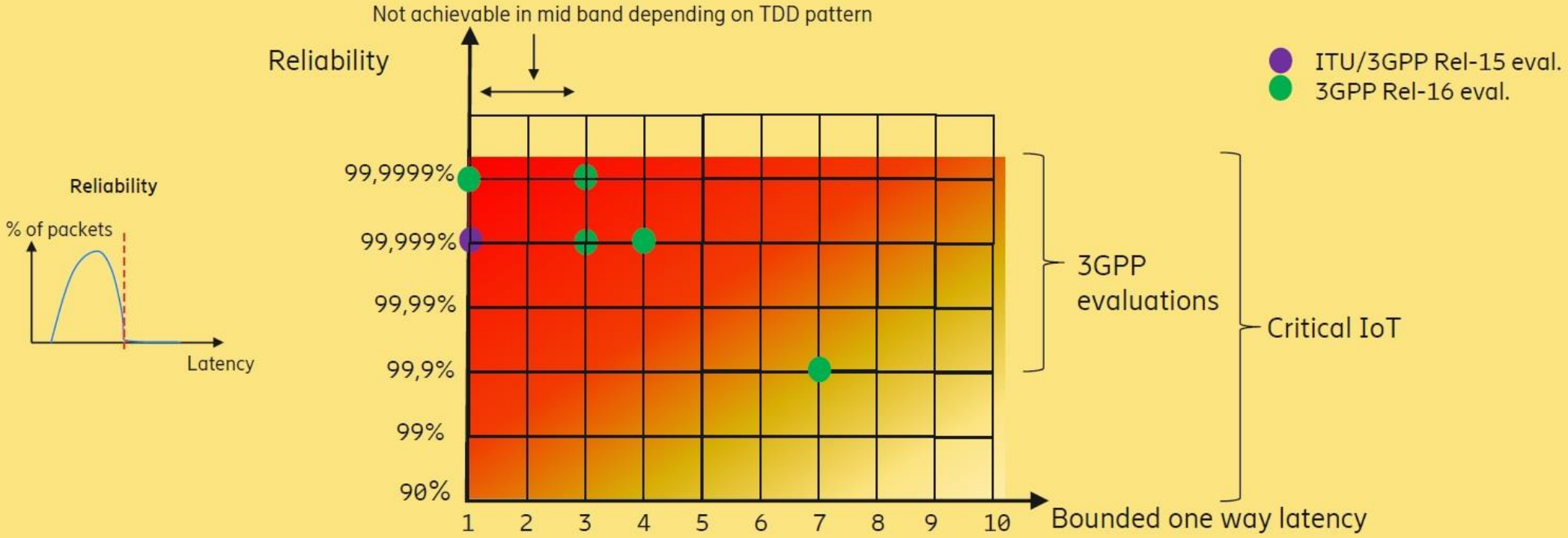


- Real time control of industrial systems
- Fully immersive AR/VR



Critical IoT evaluation in 3GPP

- ITU requires 99.999% reliability within 1ms UL/DL for a 32byte message
  - 3GPP concluded its feasibility in Rel-15
- In Rel-16, 3GPP is evaluating various combinations of reliability (99.9 – 99.9999%), latency (1-7ms), and throughput (up to Mbps)



Robot use case and communication requirements

Use case #	Characteristic parameter				Influence quantity							
	Communication service availability: target value [%]	Communication service reliability: mean time between failures	End-to-end latency: maximum	Service bitrate: user experienced data rate	Message size [byte]	Transfer interval: lower bound	Transfer interval: target value (note)	Transfer interval: upper bound	Survival time	UE speed	# of UEs	Service area
1	> 99.999 9	~ 10 years	< target transfer interval value	–	40 to 250	– < 25 % of target transfer interval value	1 ms to 50 ms	+ < 25 % of target transfer interval value	target transfer interval value	≤ 50 km/h	≤ 2,000	≤ 1 km²
2	> 99.999 9	~ 1 year	< target transfer interval value	–	15 k to 250 k	– < 25 % of target transfer interval value	10 ms to 100 ms	+ < 25 % of target transfer interval value	target transfer interval value	≤ 50 km/h	≤ 2,000	≤ 1 km²
3	> 99.999 9	~ 1 year	< target transfer interval value	–	40 to 250	– < 25 % of target transfer interval value	40 ms to 500 ms	+ < 25 % of target transfer interval value	target transfer interval value	≤ 50 km/h	≤ 2,000	≤ 1 km²
4	> 99.999 9	~ 1 week	10 ms	> 10 Mbit/s	–	–		–	–	≤ 50 km/h	≤ 2,000	≤ 1 km²

NOTE: The transfer interval is not so strictly periodic in these use cases. The transfer interval deviates around its target value within bounds. The mean of the transfer interval is close to the target value.

Use case #	Characteristic parameter				Influence quantity					
	Communication service availability: target value [%]	Communication service reliability: mean time between failures	End-to-end latency: maximum	Service bitrate: user experienced data rate	Message size [byte]	Transfer interval: target value (note 1)	Survival time (note 1)	UE speed	# of UEs	Service area (note 2)
1	99.999 9 to 99.999 999	~ 10 years	< 0.5 x transfer interval	2.5 Mbit/s	250; 500 with localisation information	> 5 ms > 2.5 ms > 1.7 ms	0 transfer interval 2 x transfer interval	≤ 6 km/h	2 to 8	10 m x 10 m x 5 m; 50 m x 5 m x 5 m
2	99.999 9 to 99.999 999	~ 10 years	< 0.5 x transfer interval	2.5 Mbit/s	250; 500 with localisation information	> 5 ms > 2.5 ms > 1.7 ms	0 transfer interval 2 x transfer interval	≤ 12 km/h	2 to 8	10 m x 10 m x 5 m; 50 m x 5 m x 5 m

NOTE 1: The first value is the application requirement, the other values are the requirement with multiple transmission of the same information (two or three times respectively).
NOTE 2: Service Area for direct communication between UEs (length x width x height). The group of UEs with direct communication might move throughout the whole factory site (up to several km²)

Cooperative motion control

Video-operated remote control

Standard robot operation and Traffic management

streaming data

Fragile work pieces

Elastic work pieces

Cooperative carrying

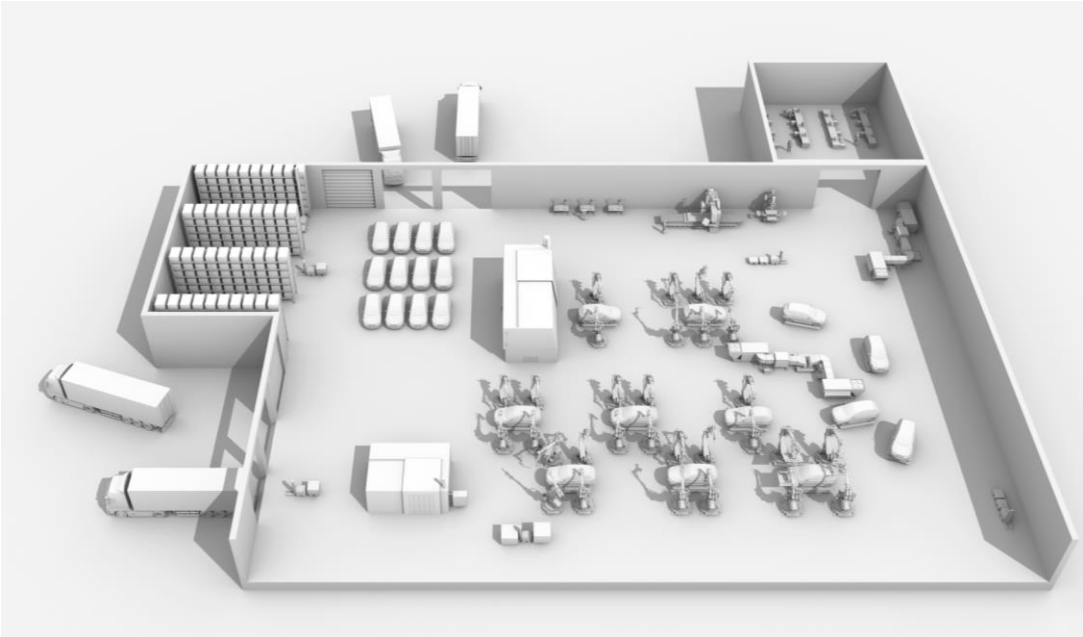
5G Use case in smart factory

The baseline factory

Automotive supplier

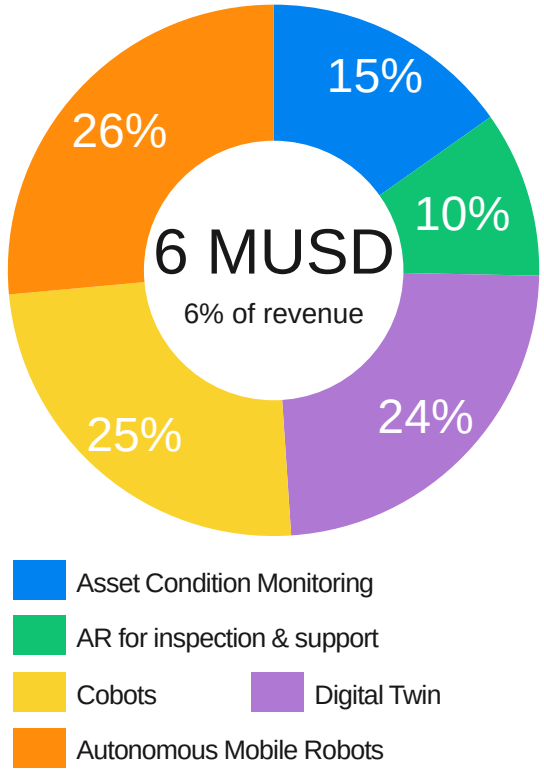
Mainly stamping & assembly operations

Revenue:100 MUSD
Gross profit:10 MUSD



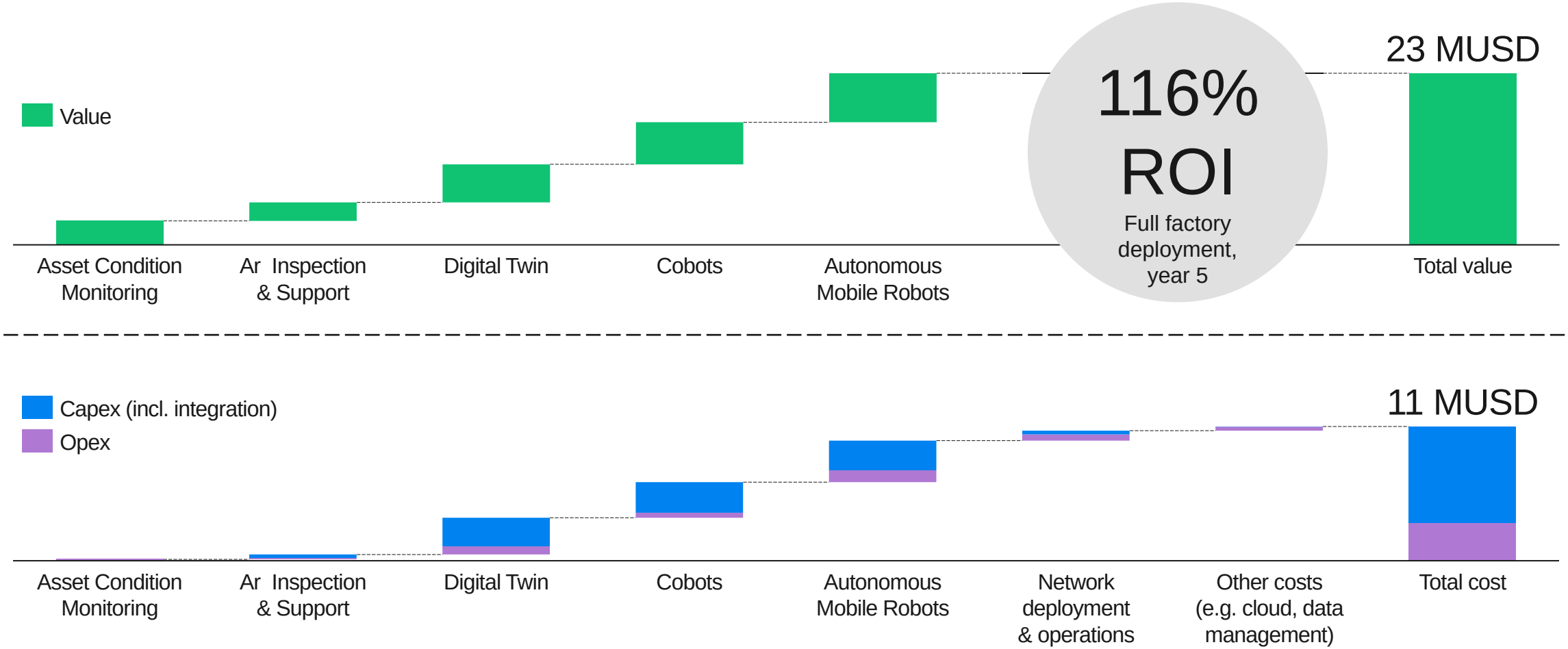
All 5 use cases implemented

Yearly steady state value



Source: Ericsson, Arthur D. Little

The full factory deployment has a ROI of 116% year 5, with total costs of 11 MUSD

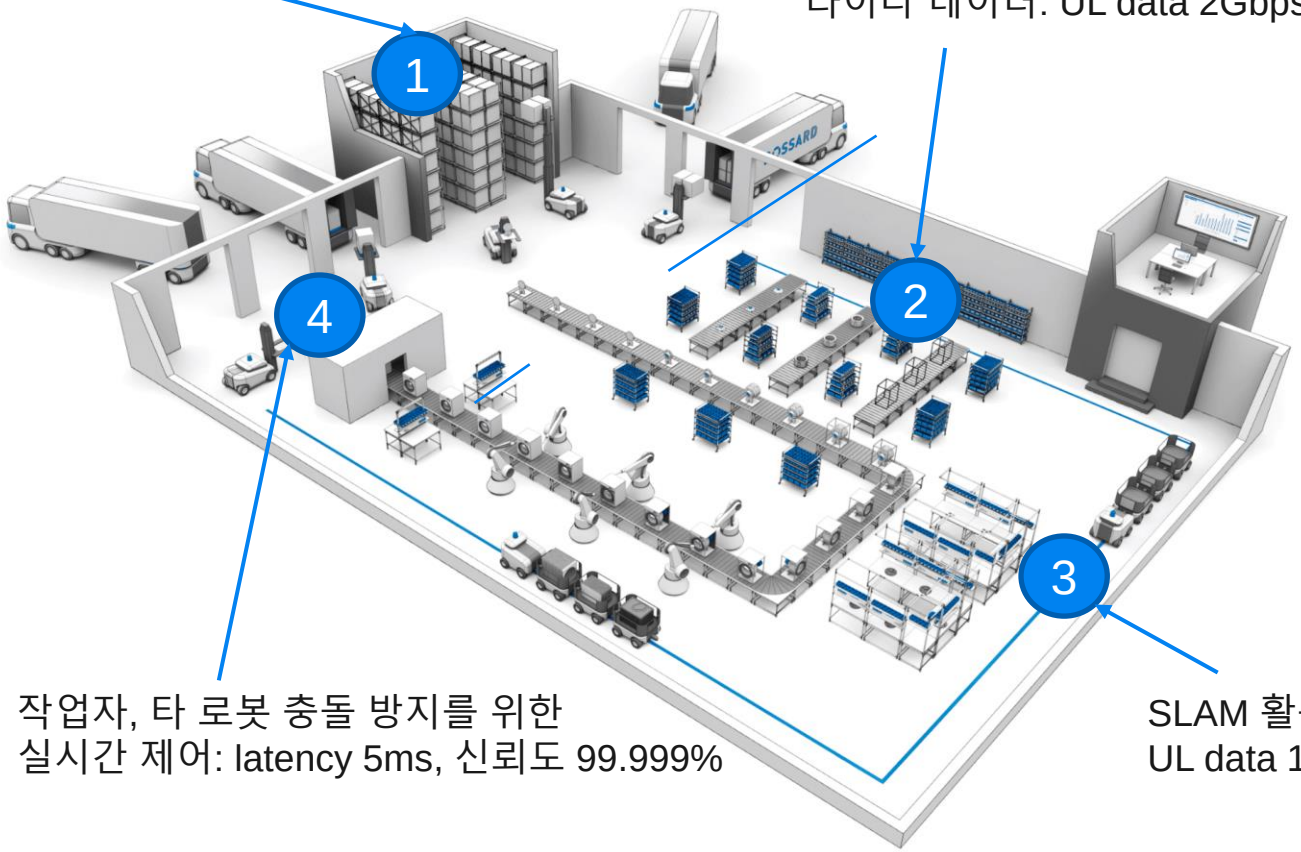


Source: Ericsson, Arthur D. Little

5G with robot at smart factory

물체인식: UL data 20Mbps

3D 모델 활용 위치 정확도를 위한
라이다 데이터: UL data 2Gbps



작업자, 타 로봇 충돌 방지를 위한
실시간 제어: latency 5ms, 신뢰도 99.999%

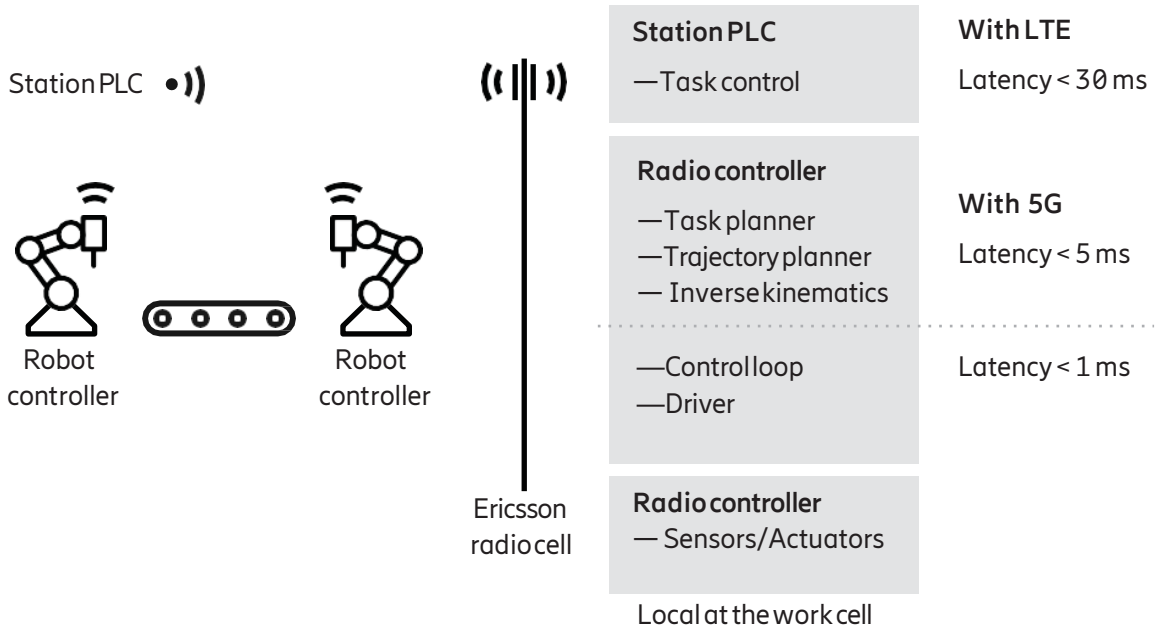
SLAM 활용 자율주행 모니터링:
UL data 1Mbps

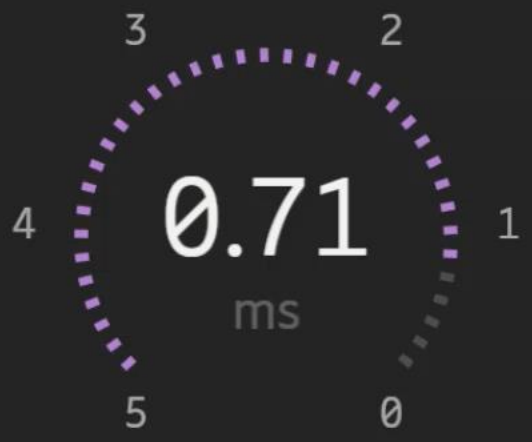
WiFi 기술의 단점

- 산업 현장에서 요구되는 전송속도 만족 못함
- 품질 보장이 안됨 (Best effort service)
- 이동 중 품질 저하
- 통신 품질 관리 불가

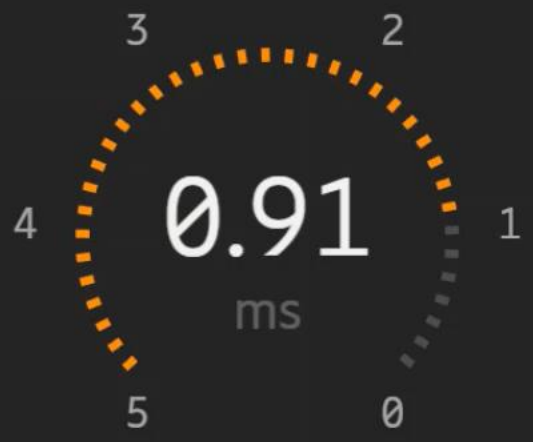
Flexible robotics with 5G Cloud

- Reduction of cabling in new plants or existing plants with help of cellular
- Remote monitoring of robots for preventive maintenance
- Move nodes computing to reduce installation costs (remote virtual PLC)

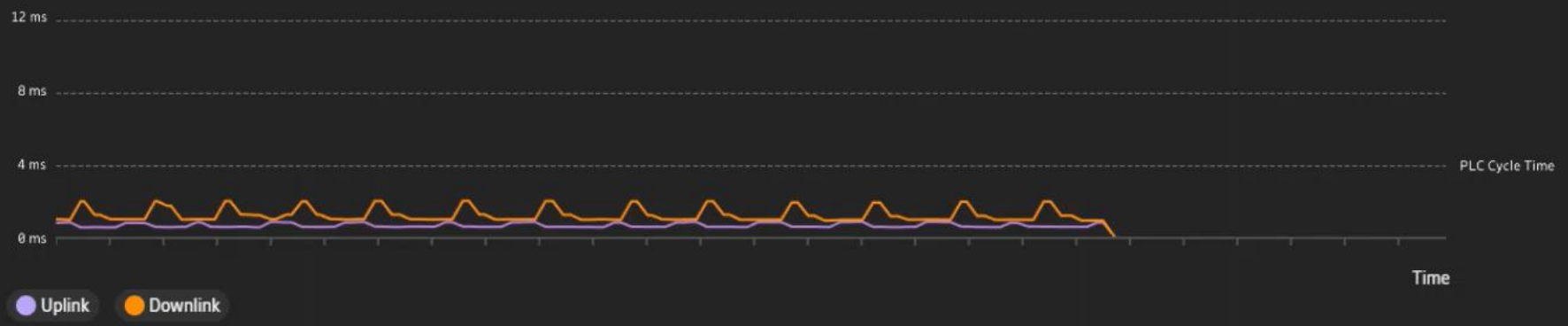




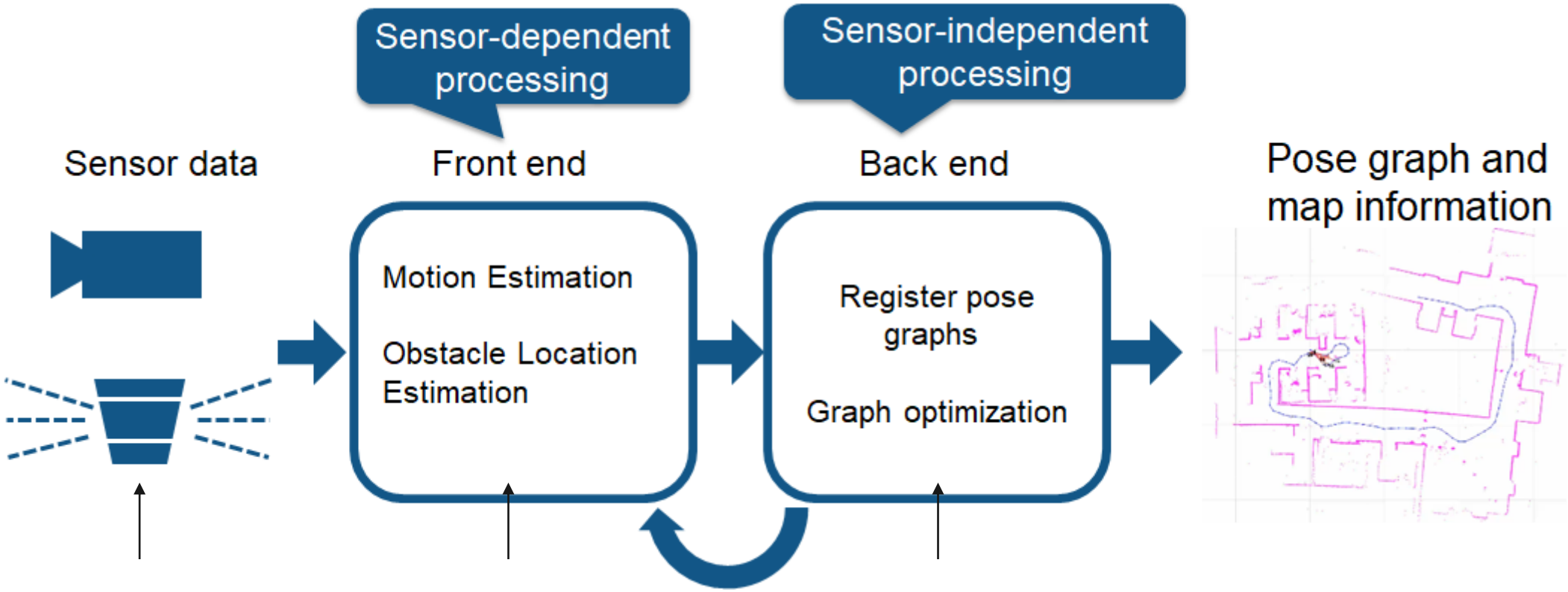
Uplink latency



Downlink latency



SLAM (simultaneous localization and mapping)
one of 5G robot use case



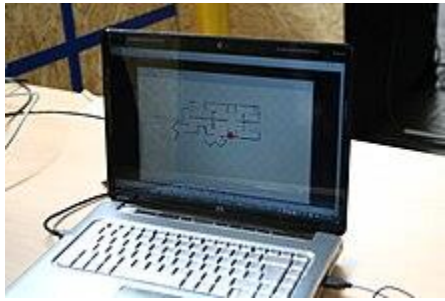
Sensor data
Visual/lidar/etc

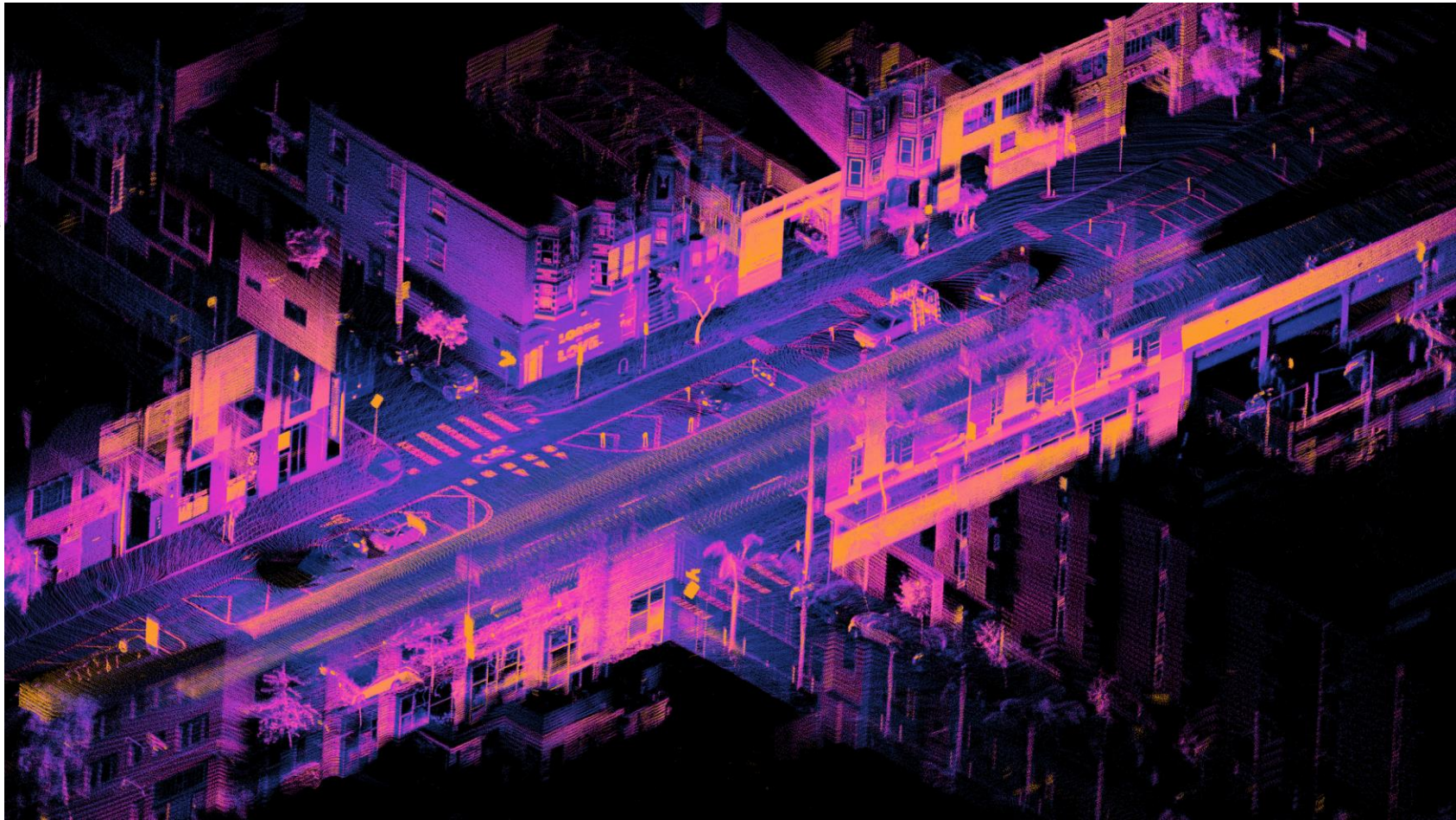
Mapping
Positioning
3D modeling
Motion estimation

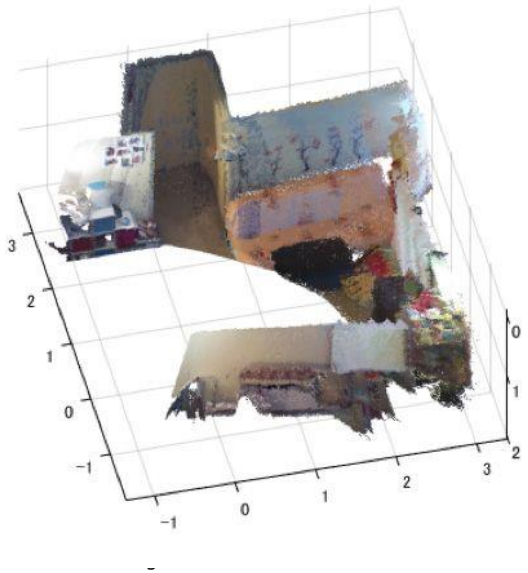
Loop closure
Exploration (navigation)
Moving objects

What is SLAM, MATLAB home page

SLAM sensing and 3D modeling





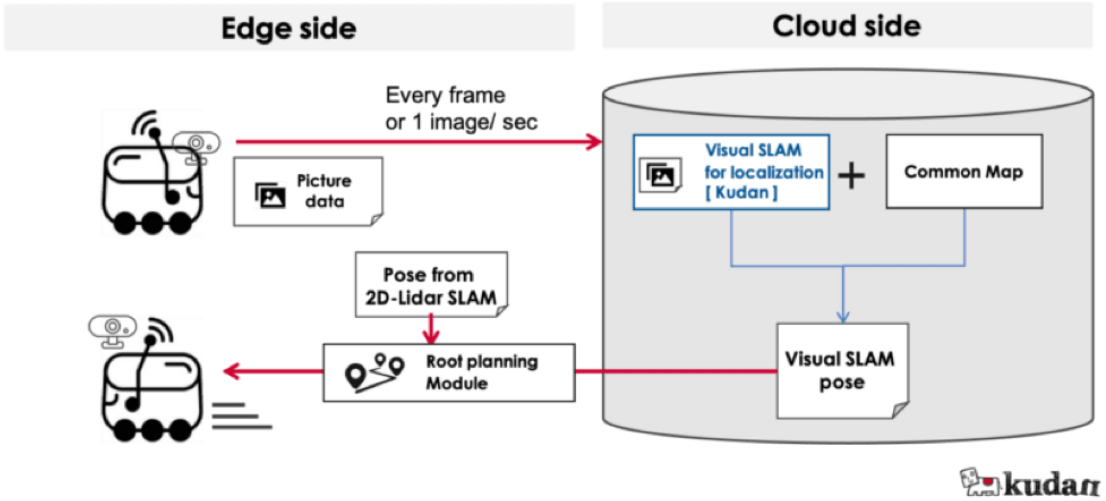


Common Challenges with SLAM

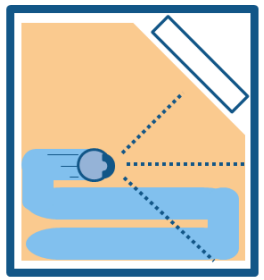
1. Localization errors accumulate, causing substantial deviation from actual values
2. Localization fails and the position on the map is lost
3. High computational cost for image processing, point cloud processing, and optimization

What is SLAM, MATLAB home page

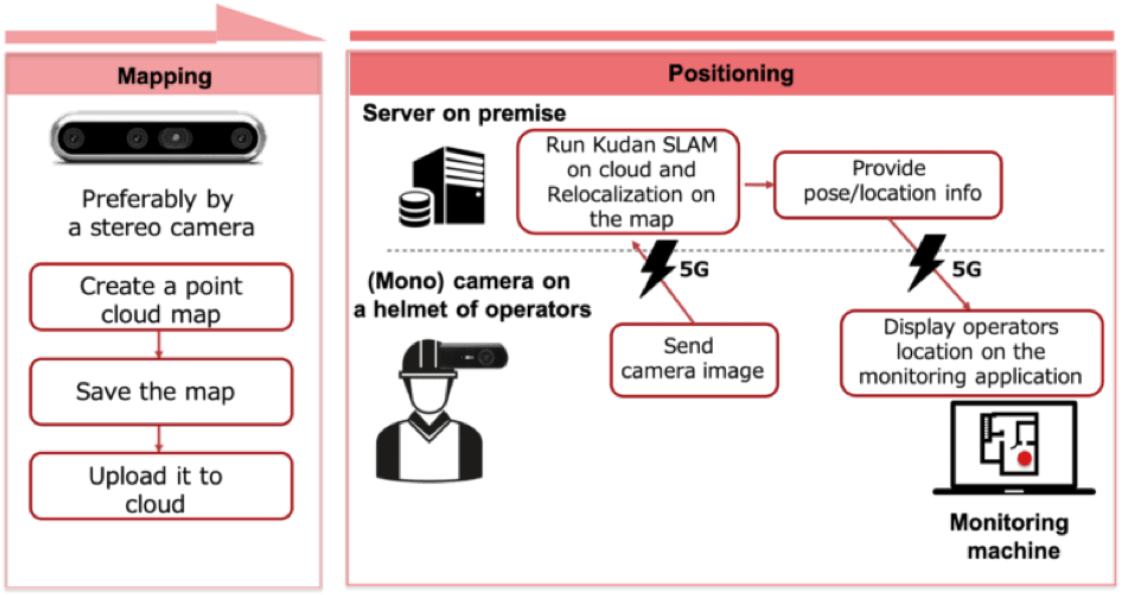
SLAM with Cloud edge (5G)

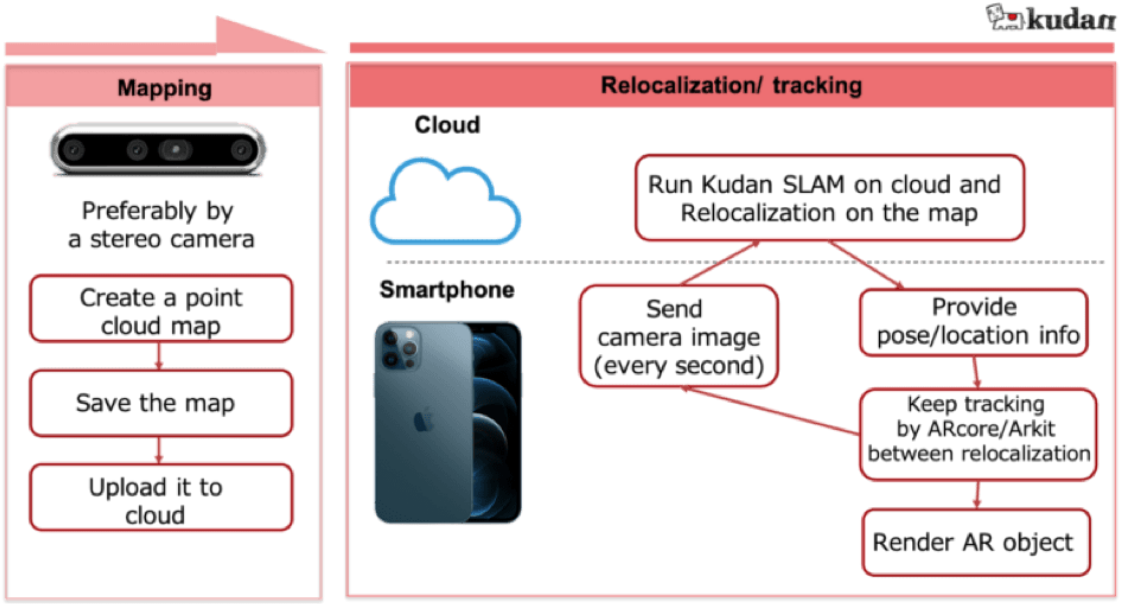


Without SLAM:
Cleaning a room randomly.



With SLAM:
Cleaning while understanding the room's layout.

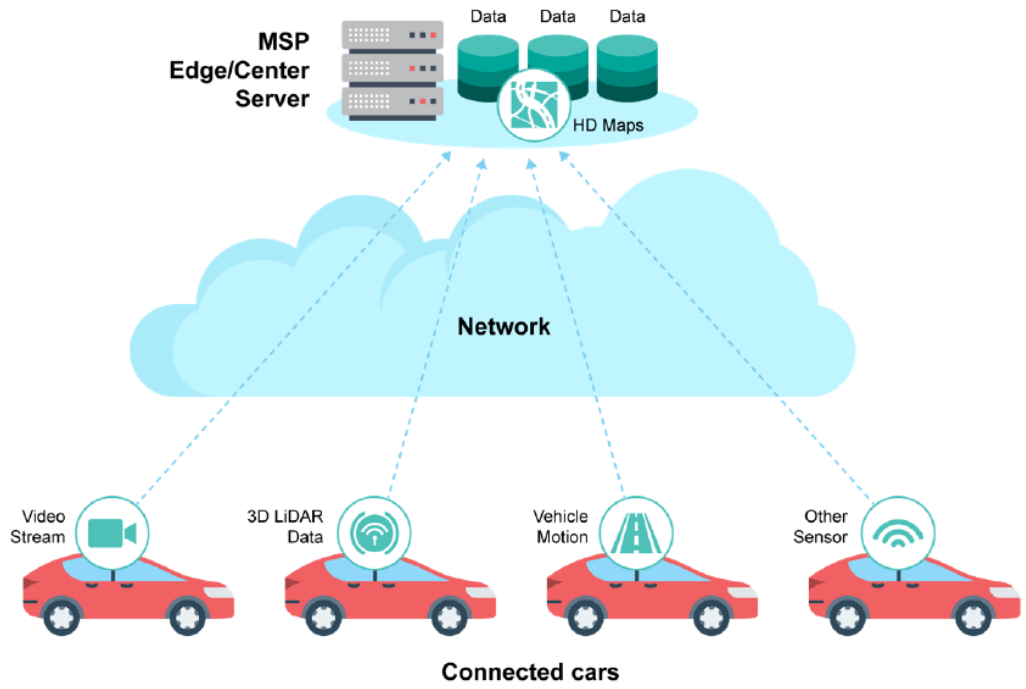




HD 3D Mapping

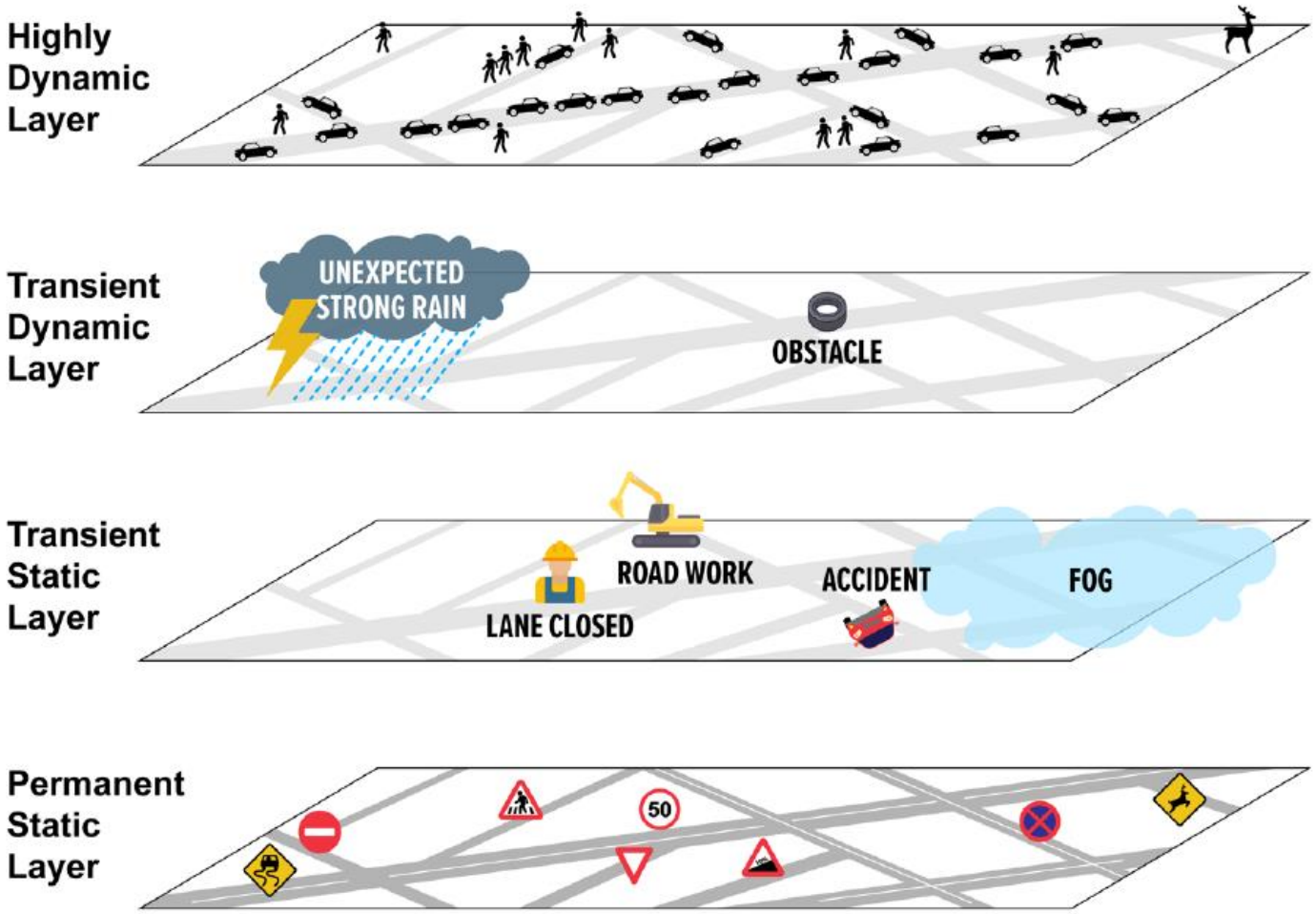
HD 3D map

What is an HD Map? The term generally means a map overlaid with various information such as traffic situations, access ways, street furniture within city streets and sub-surface ducts, with high precision at the centimeter level, which is updated frequently. In automotive use cases, the HD Map is a key to progress with Mobility as a Service, ADAS (Advanced Driver Assistance System) and autonomous driving



Operational behavior of a high-definition map application white paper, v.1.0.0 May 26, 2020

Layers of HD 3D map



Intervals of less than several seconds
Pedestrians, vehicles, bicycles, motorbikes, etc

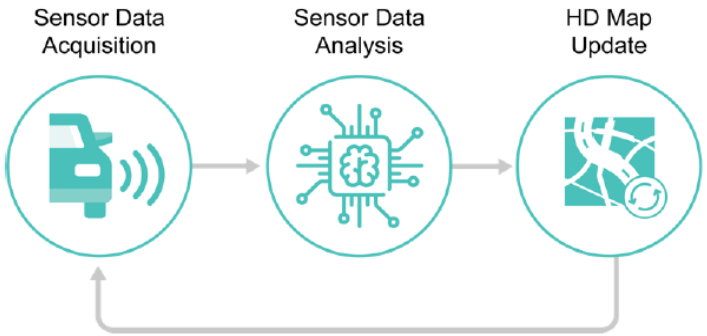
Intervals of less than several minutes
Fallen objects, illegally parked vehicle, trash, local weather, etc

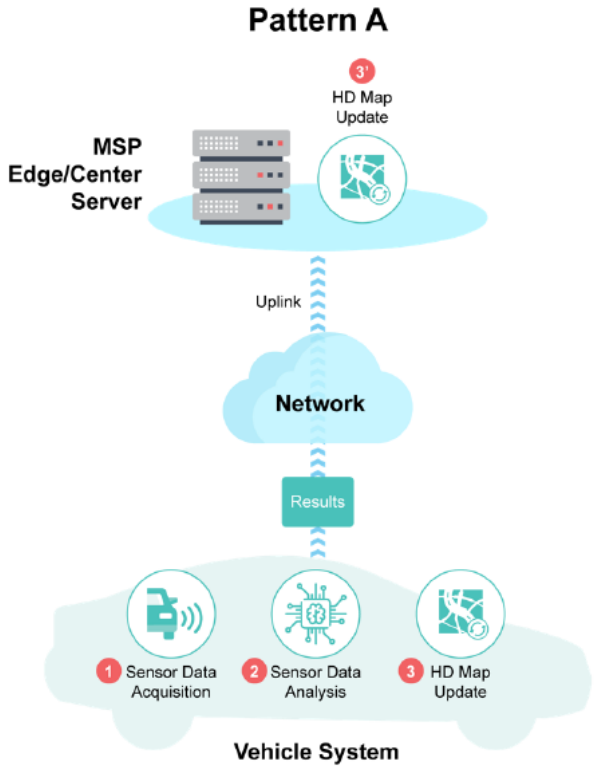
Intervals of less than several hours
Road works, lane closure, accidents, etc

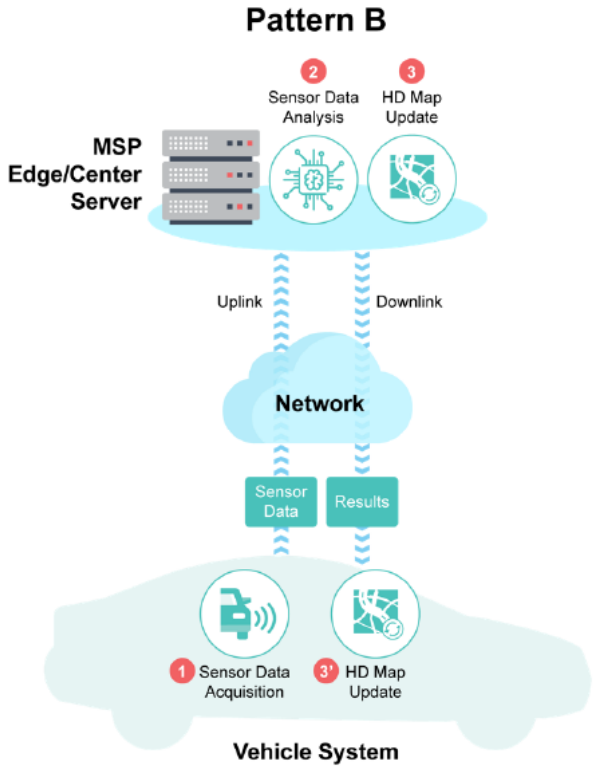
Intervals of one day or longer
Lanes, traffic signals, 3D structures, etc

Operational behavior of a high-definition map application white paper, v.1.0.0 May 26, 2020

Process flow and processing patterns



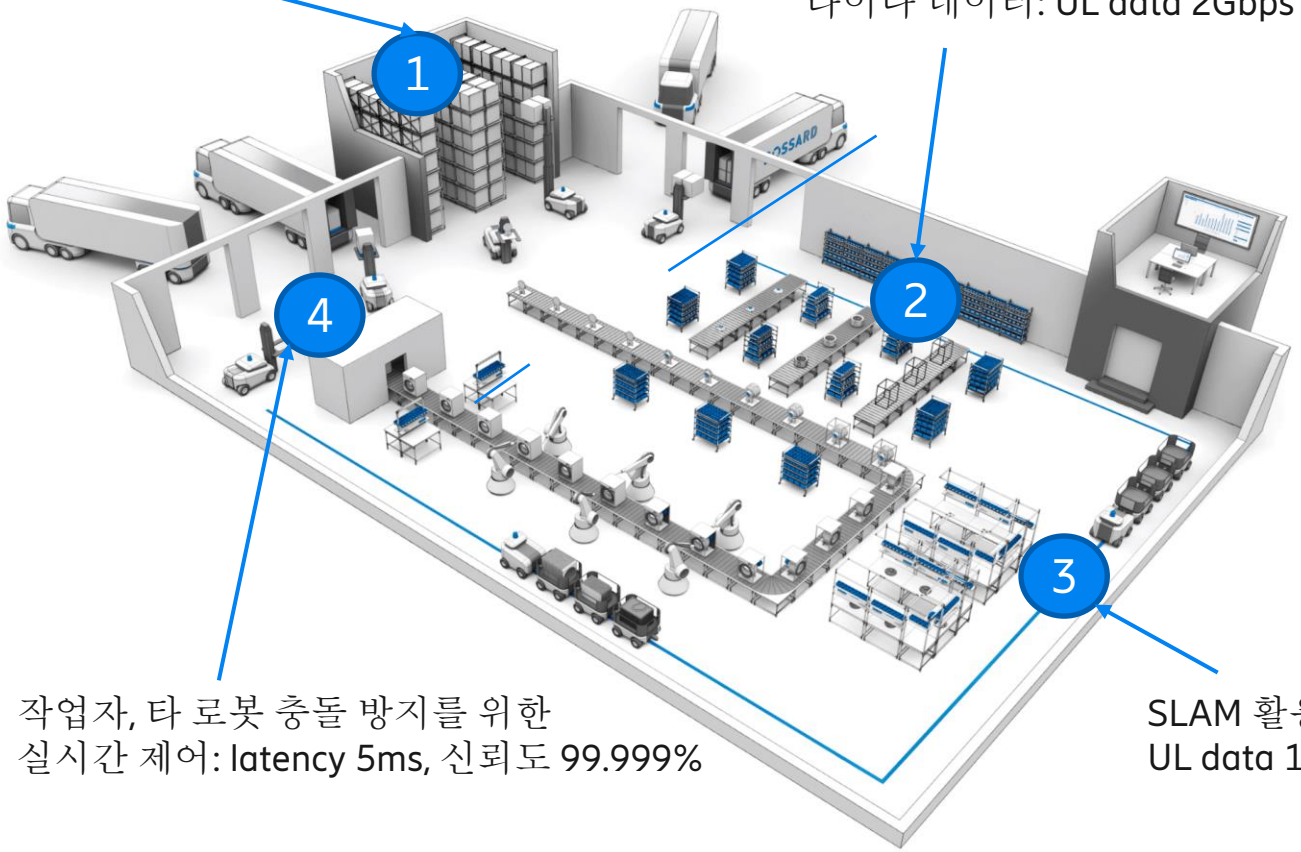




5G with robot at smart factory

물체인식: UL data 20Mbps

3D 모델 활용 위치 정확도를 위한
라이다 데이터: UL data 2Gbps



작업자, 타 로봇 충돌 방지를 위한
실시간 제어: latency 5ms, 신뢰도 99.999%

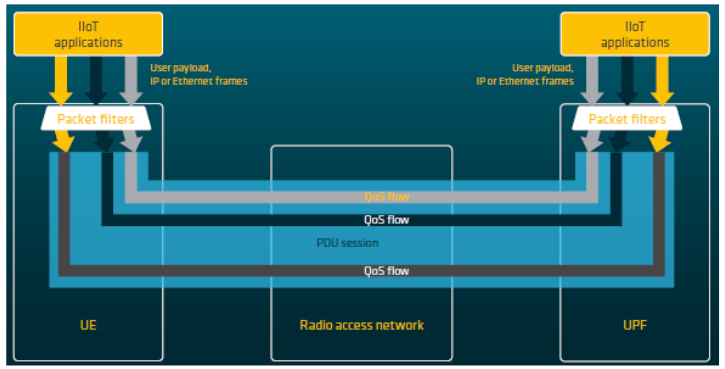
SLAM 활용 자율주행 모니터링:
UL data 1Mbps

WiFi 기술의 단점

- 산업 현장에서 요구되는 전송속도 만족 못함
- 품질 보장이 안됨 (Best effort service)
- 이동 중 품질 저하
- 통신 품질 관리 불가

Quality management in 5G

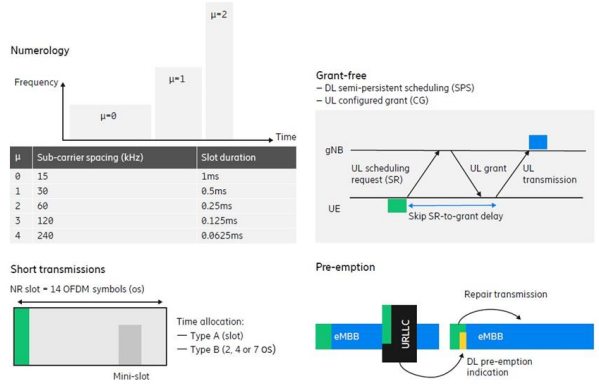
5G 품질 (QoS) 관리 모델



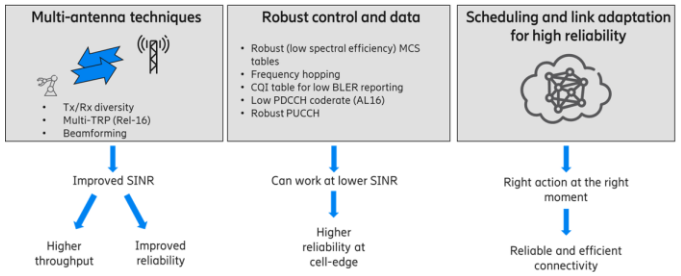
5G 품질관리를 위한 5QI 값과 QoS 간 매핑

5QI value	Resource type	Default priority level	Packet delay budget	Packet error ratio	Default maximum data burst volume	Default averaging window	Example services
2	GBR	40	150 ms	10^{-3}	N/A	2000 ms	Conversational video (live streaming)
6	Non-GBR	60	300 ms	10^{-6}	N/A	N/A	Video (buffered streaming) TCP-based
---	---	---	---	---	---	---	---
82	Delay-critical GBR	19	10 ms	10^{-4}	255 bytes	2000 ms	Discrete automation
83	Delay-critical GBR	22	10 ms	10^{-4}	1354 bytes	2000 ms	Delay-critical GBR

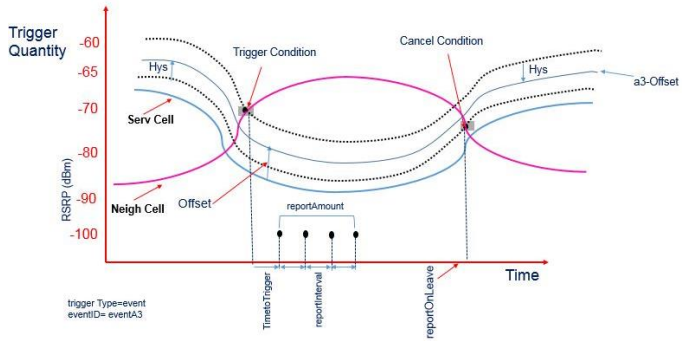
5G 통신 품질 보장 기술



Low latency (낮은 전송 지연)

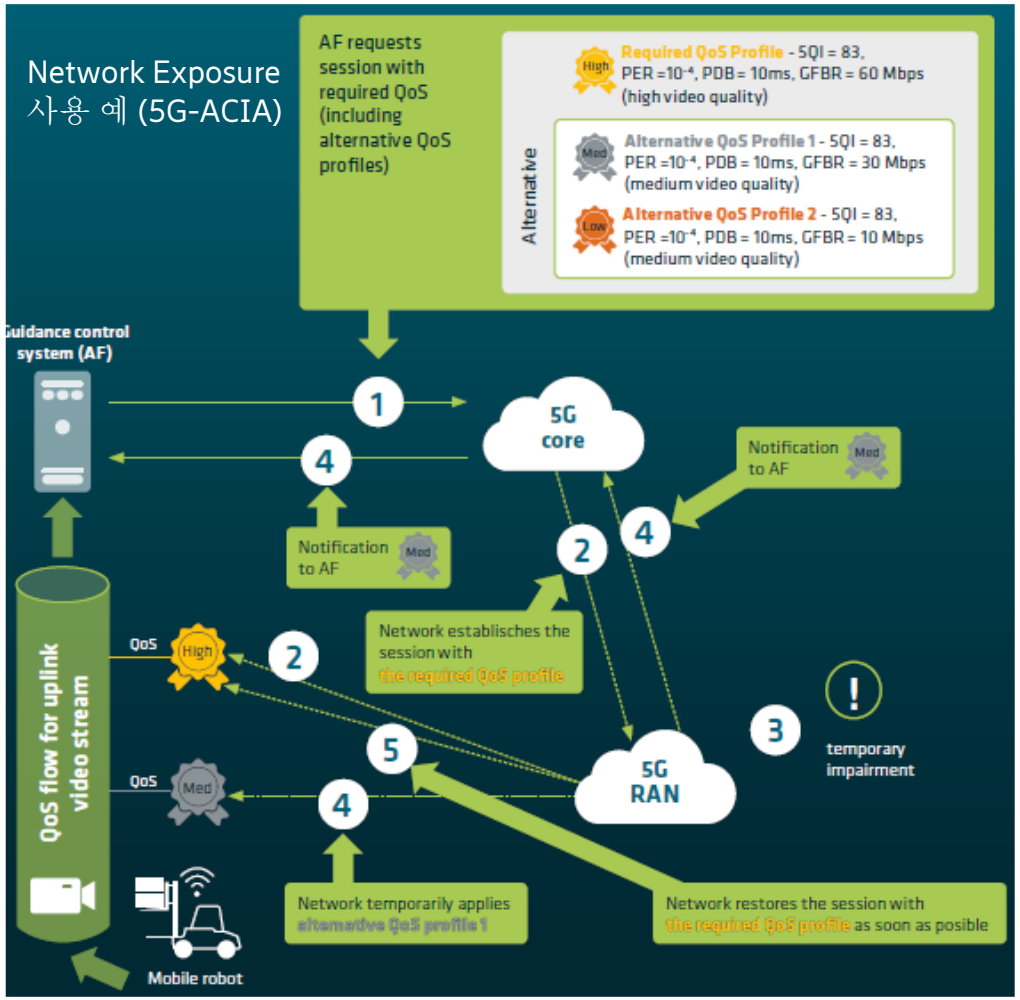


Reliability (신뢰성)

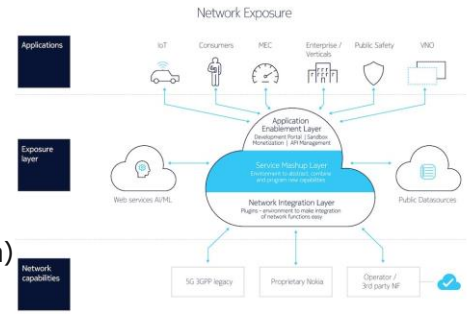


Handover (이동성)

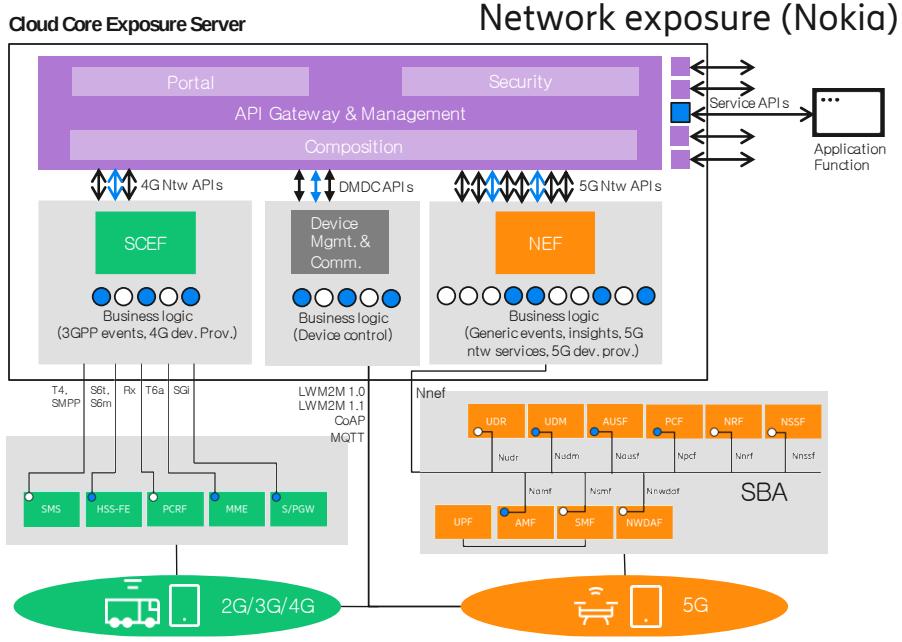
Quality management with API(NEF)



3GPP Network exposure 표준
NEF (Network Exposure Function)

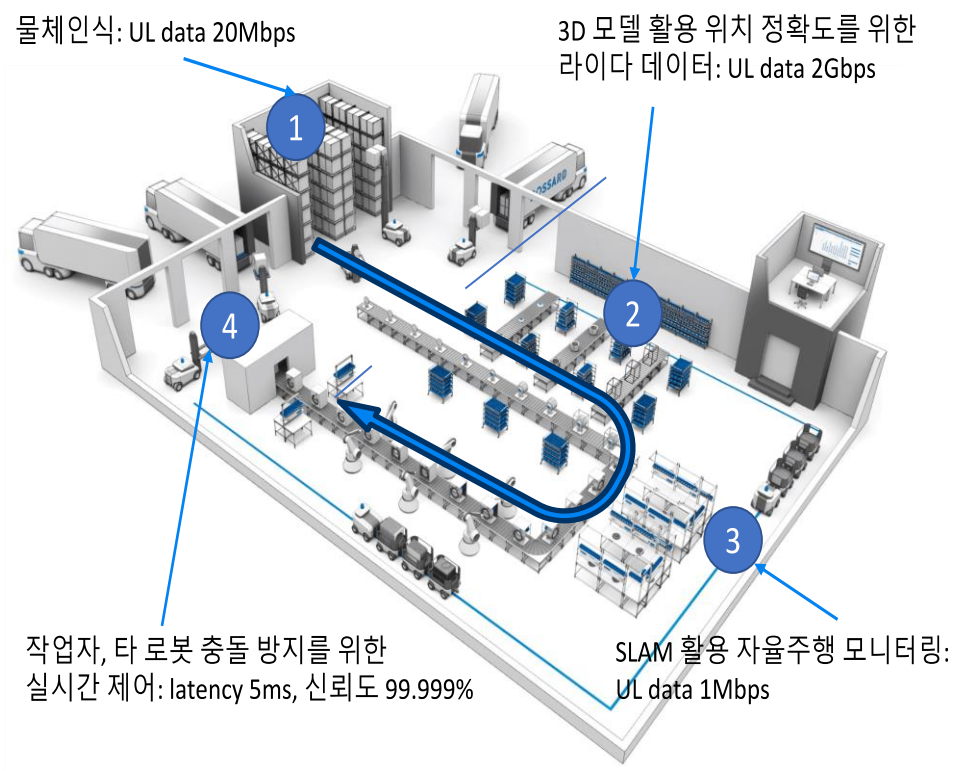


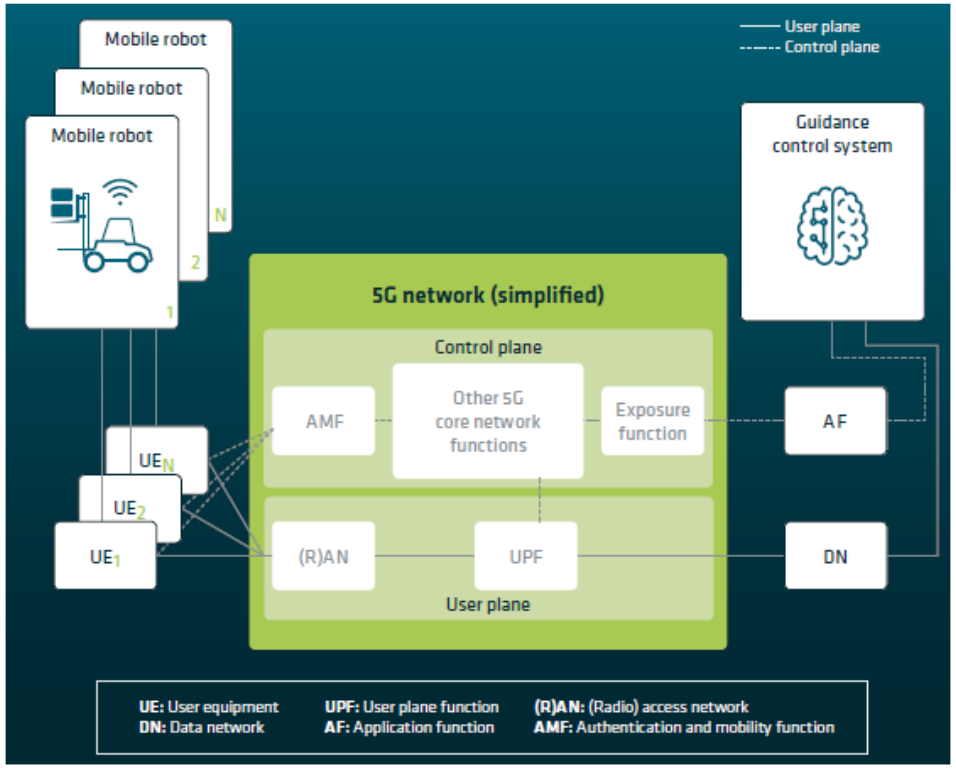
Network exposure (Nokia)



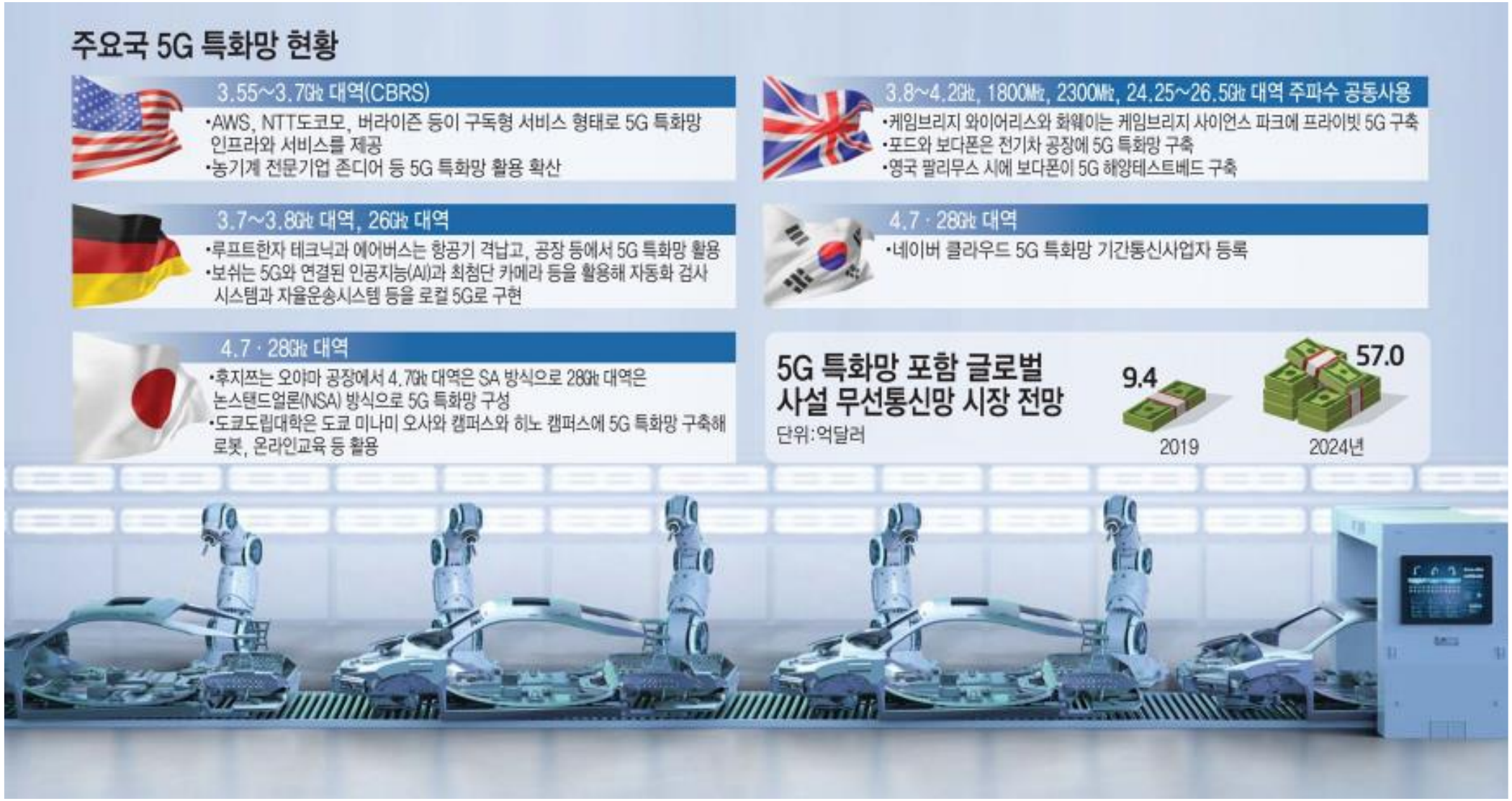
Network exposure (Ericsson)

Quality management in 5G with QoS model and API(NEF)



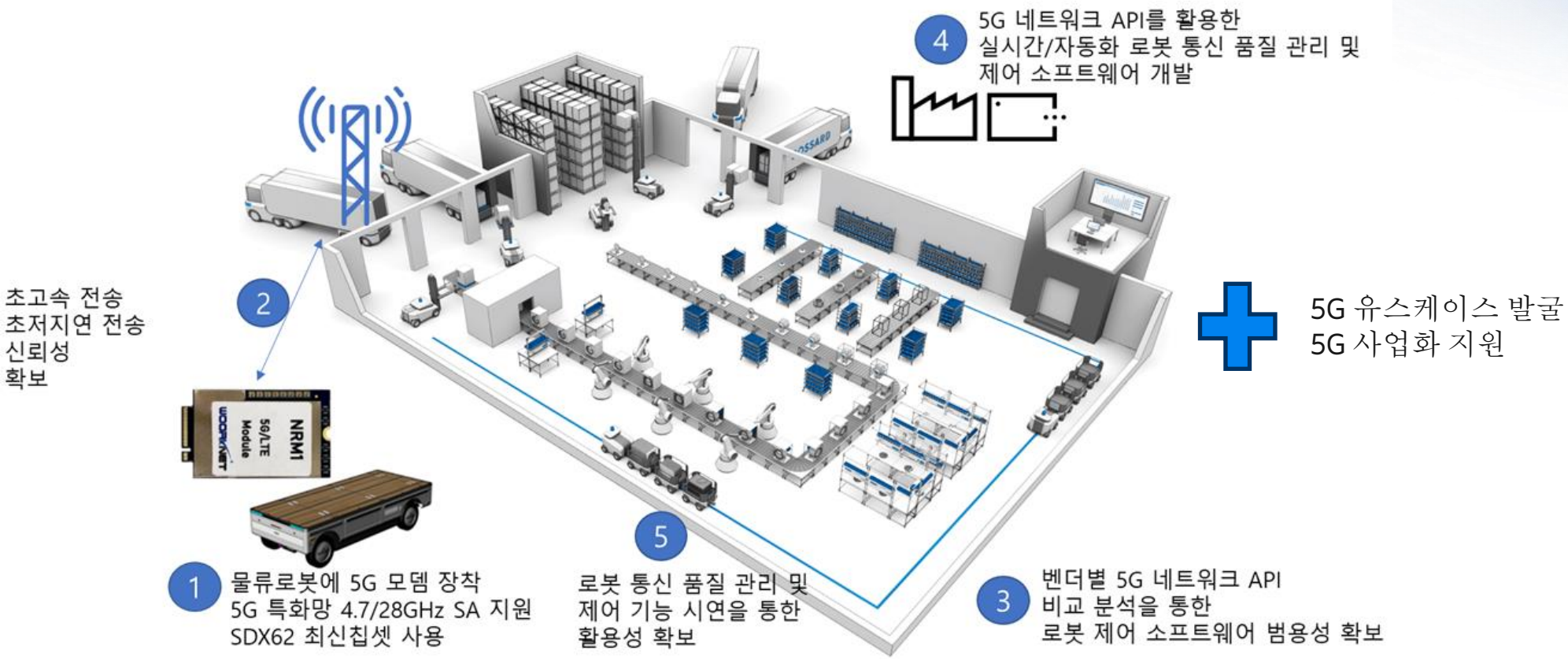


5G 특화망

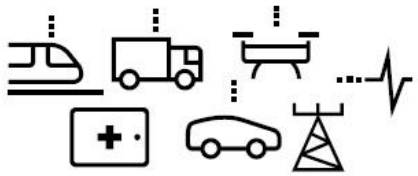
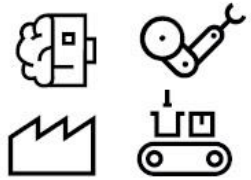

주요국 5G 특화망 현황
3.55~3.7㎓ 대역(CBRS)
•AWS, NTT도코모, 버라이즌 등이 구독형 서비스 형태로 5G 특화망 인프라와 서비스를 제공
•농기계 전문기업 존디어 등 5G 특화망 활용 확산
3.8~4.2㎓, 1800㎒, 2300㎒, 24.25~26.5㎓ 대역 주파수 공동사용
•케임브리지 와이어리스와 화웨이는 케임브리지 사이언스 파크에 프라이빗 5G 구축
•포드와 보다폰은 전기차 공장에 5G 특화망 구축
•영국 팰리무스 시에 보다폰이 5G 해양테스트베드 구축
3.7~3.8㎓ 대역, 26㎓ 대역
•루프트한자 테크닉과 에어버스는 항공기 격납고, 공장 등에서 5G 특화망 활용
•보쉬는 5G와 연결된 인공지능(AI)과 최첨단 카메라 등을 활용해 자동화 검사 시스템과 자율운송시스템 등을 로컬 5G로 구현
4.7 · 28㎓ 대역
•네이버 클라우드 5G 특화망 기간통신사업자 등록
4.7 · 28㎓ 대역
•후지쯔는 오야마 공장에서 4.7㎓ 대역은 SA 방식으로 28㎓ 대역은 논스탠드얼론(NSA) 방식으로 5G 특화망 구성
•도쿄도립대학은 도쿄 미나미 오사와 캠퍼스와 히노 캠퍼스에 5G 특화망 구축해 로봇, 온라인교육 등 활용
5G 특화망 포함 글로벌 사설 무선통신망 시장 전망
단위:억달러
9.4
2019
57.0
2024년

2023년 5G기반 첨단제조로봇분야 「기술사업화기업지원사업」

- 물류로봇에 5G 모뎀 장착. 초고속 전송, 초저지연, 신뢰성 제공.
- 벤더 독립형 API 기반의 5G 품질 관리 SW 개발 및 가상 환경에서의 활용성 확보
- 5G 유스케이스 발굴, 5G 사업화 지원, 통신 품질 확보/관리 방안 제공 등 컨설팅 수행



Critical IoT – use cases and spectrum bands

	Wide area use cases	Local area use cases	
			
High bands (24GHz– 40GHz)			- Extremely low latency - Ultra-high reliability - High capacity - Limited coverage
Mid bands (1GHz – 6GHz)			- Extremely low latency (with FDD/latency favorable TDD) - Ultra-high reliability - Decent coverage & capacity
Low bands (sub-1GHz)			- Extremely low latency - Ultra-high reliability - Wide area coverage - Limited capacity

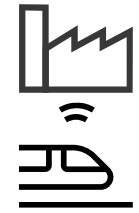
Industrial Automation IoT – for advanced smart manufacturing

- 5G NR
- eURLLC
- Deterministic networks

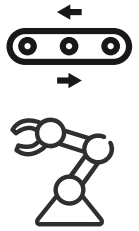
- Ethernet support
- Time sensitive networking

- Local Area / Non-public networks

- Smart industries



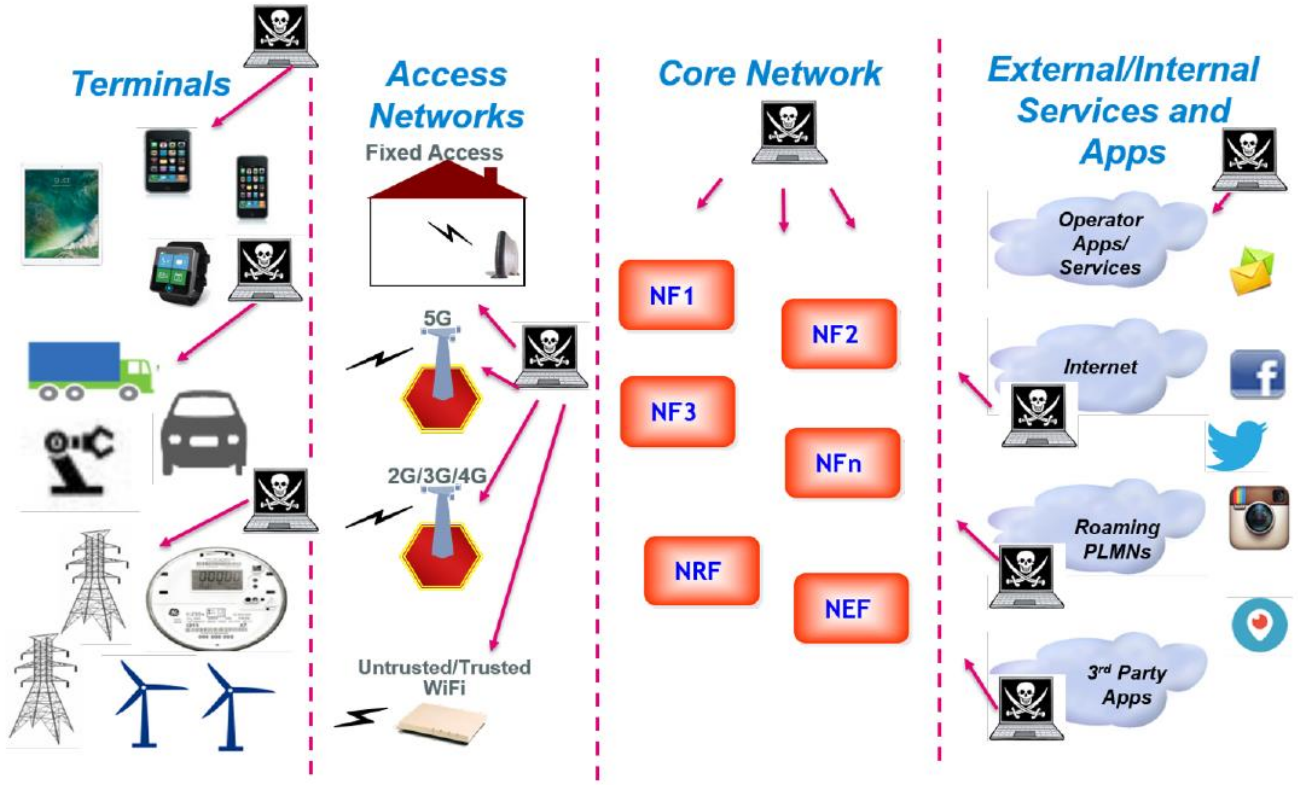
- Smart Manufacturing, Railways, Power generation and distribution
- Automation for Robotics, Control systems and Process optimization



- Native ‘Ethernet over NR’ to support industrial protocols
- TSN and QoS
- Precise positioning

- 5G enabling Industry 4.0
- 5G-ACIA and other industry body collaborations

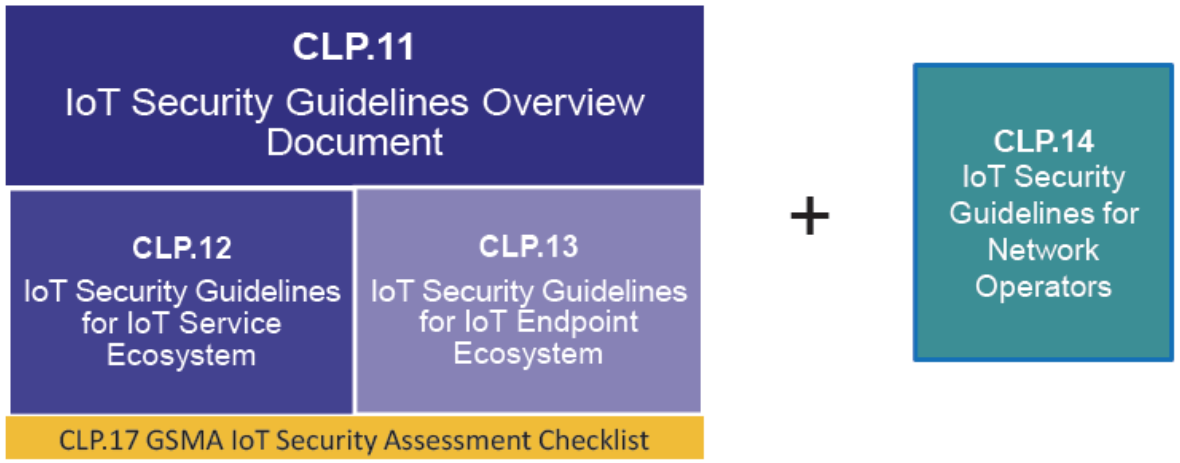
Mobile network security and 3GPP standards

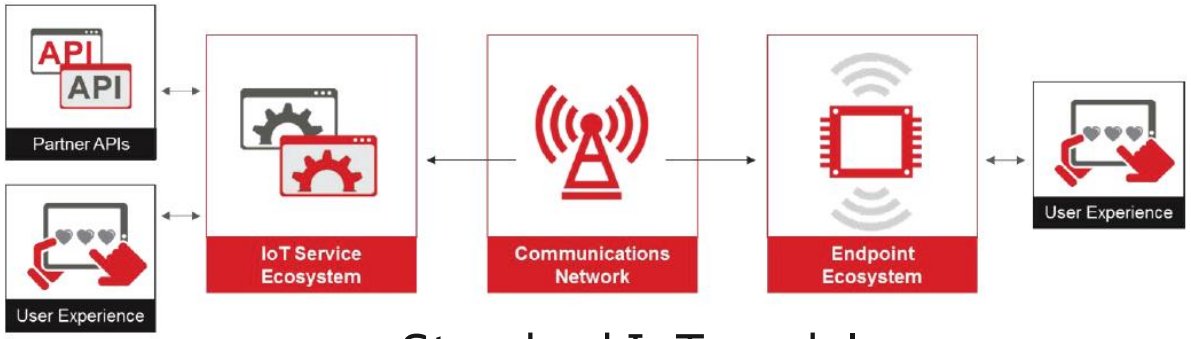


3GPP 5G Security Standards

- Increased Home Control
- Unified Authentication Framework
- Security Anchor Function (SEAF)
- Subscriber Identifier Privacy
- 3GPP 5G Security Architecture
- Requirements for e2e Core Network Interconnection Security
- Authentication Framework
- Granularity of Anchor Key Binding to Serving Network
- Mitigation of Bidding Down Attacks
- Service Requirements
- 5G Identifiers
- Subscription Permanent Identifier (SUPI)
- Subscription Concealed identifier (SUCI)
- Subscription Identification Security
- Permanent Equipment Identifier
- Subscription Identifier De-Concealing Function
- 5G Globally Unique Temporary Identifier
- Procedure for Using Subscription Temporary Identifier
- Subscriber Privacy
- Secure Steering of Roaming
- UE-Assisted Network-Based Detection of False Base Station

GSMA security architecture

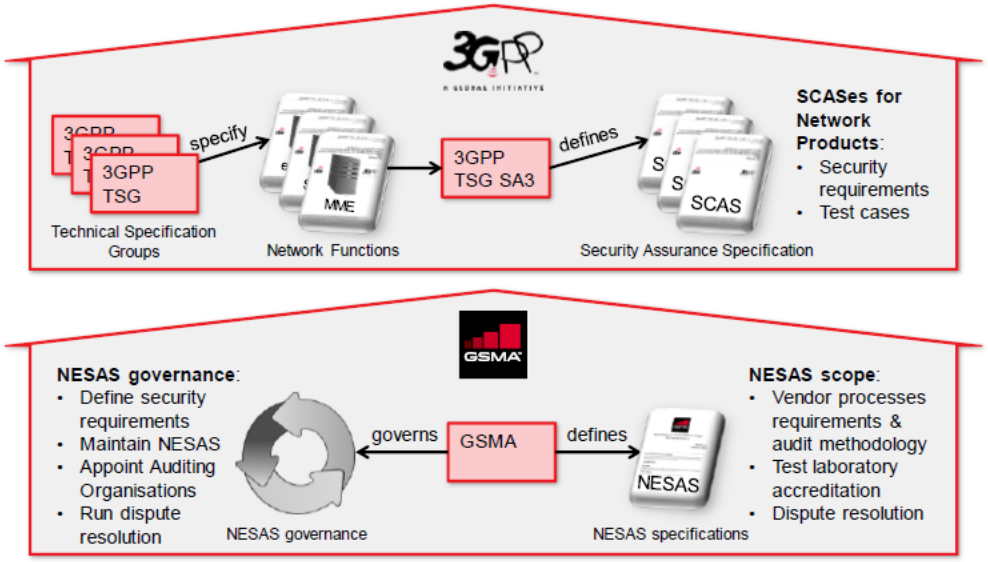




Standard IoT model

- 기술 모델 평가 (Evaluate the technical model)
- 제품 또는 서비스의 보안 모델 검토 (Review the current product or service's Security Model)
- 권장 사항 검토 및 평가 (Review and evaluate Recommendations)
- 구현 및 검토 (Implementation and Review)
- 지속적인 라이프사이클 (Ongoing Lifecycle)

GSMA NESAS



Document title:
GSMA PRD FS.13
Network Equipment Security Assurance Scheme – Overview

This document

Description: High level explanation of NESAS

Owner: GSMA

Document title:
GSMA PRD FS.14
Network Equipment Security Assurance Scheme – Security Test Laboratory Accreditation

Description:
Test laboratory accreditation process and requirements

Owner: GSMA

Document title:
GSMA PRD FS.15
Network Equipment Security Assurance Scheme – Development and Lifecycle Assessment Methodology

Description:
Methodology of vendor development and lifecycle processes assessment

Owner: GSMA

Document title:
GSMA PRD FS.16
Network Equipment Security Assurance Scheme – Development and Lifecycle Security Requirements

Description:
Requirements for vendor development and lifecycle processes assessment

Owner: GSMA

Document title: **informative**
GSMA PRD FS.46
Network Equipment Security Assurance Scheme – Audit Guidelines

Description:
Guidelines to Auditors and Equipment Vendors on how to conduct the vendor assessment

Owner: GSMA

Document title:
GSMA PRD FS.47
Network Equipment Security Assurance Scheme – Product and Evidence Evaluation Methodology

Description:
Methodology of product and evidence evaluation

Owner: GSMA

Document title: **informative**
3GPP TR 33.916
Assurance Methodology for 3GPP network products

Description:
Network Equipment Evaluation Process and Creation of SCAS

Owner: 3GPP

Document title:
3GPP TS 33.117
Catalogue of General Security Assurance Requirements

Description:
Generic SCAS for all Network Functions

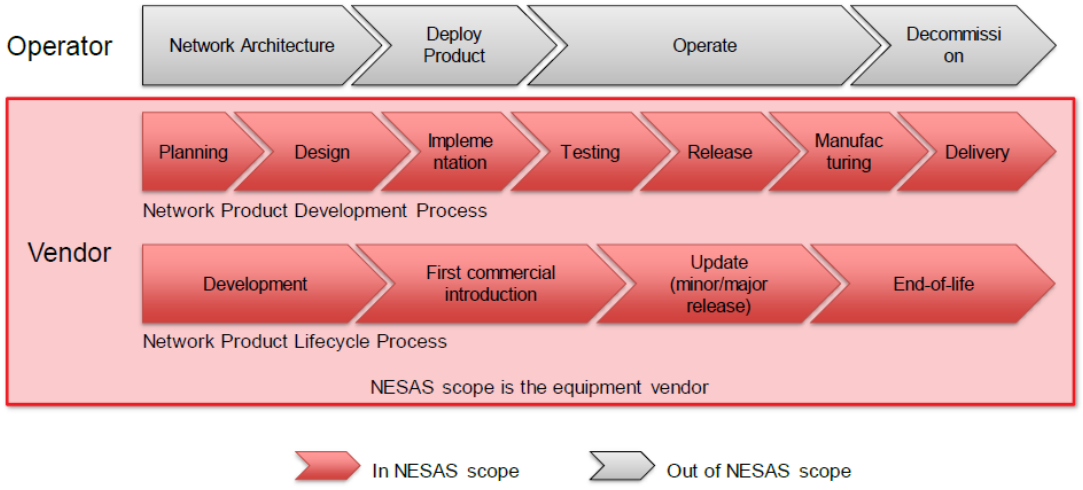
Owner: 3GPP

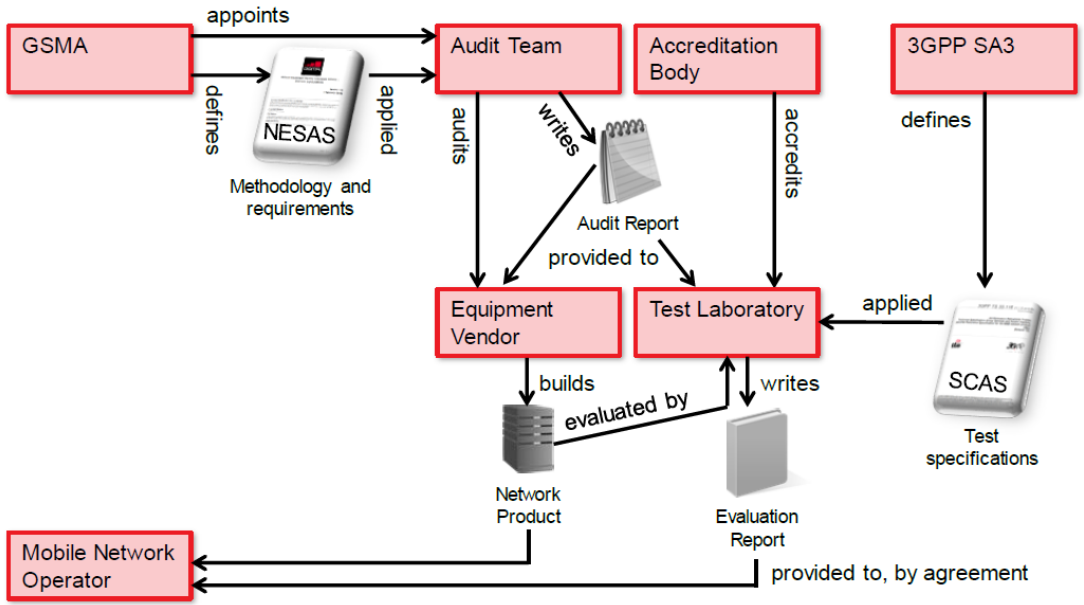
SCAS specific to 3GPP-defined Network Functions are published by 3GPP

Reference:
https://www.3gpp.org/DynaReport/33-series.htm

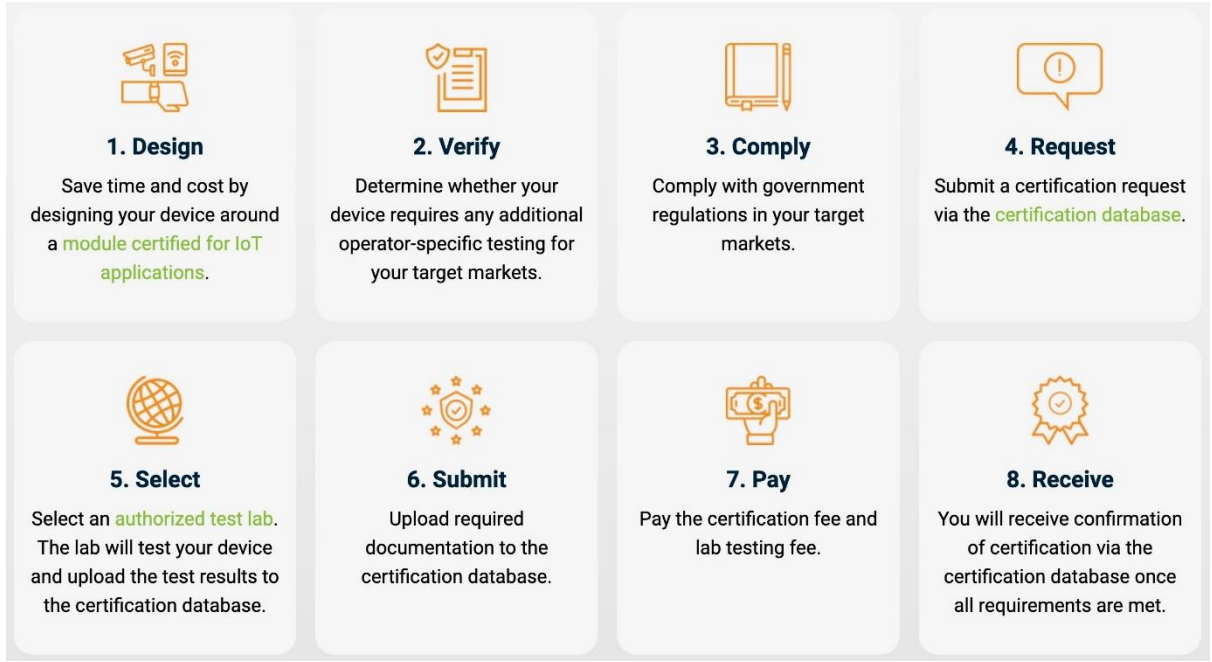
Owner: 3GPP

NESAS operations





CTIA Cybersecurity Certification Test Plan for IoT Devices




CTIA Certification

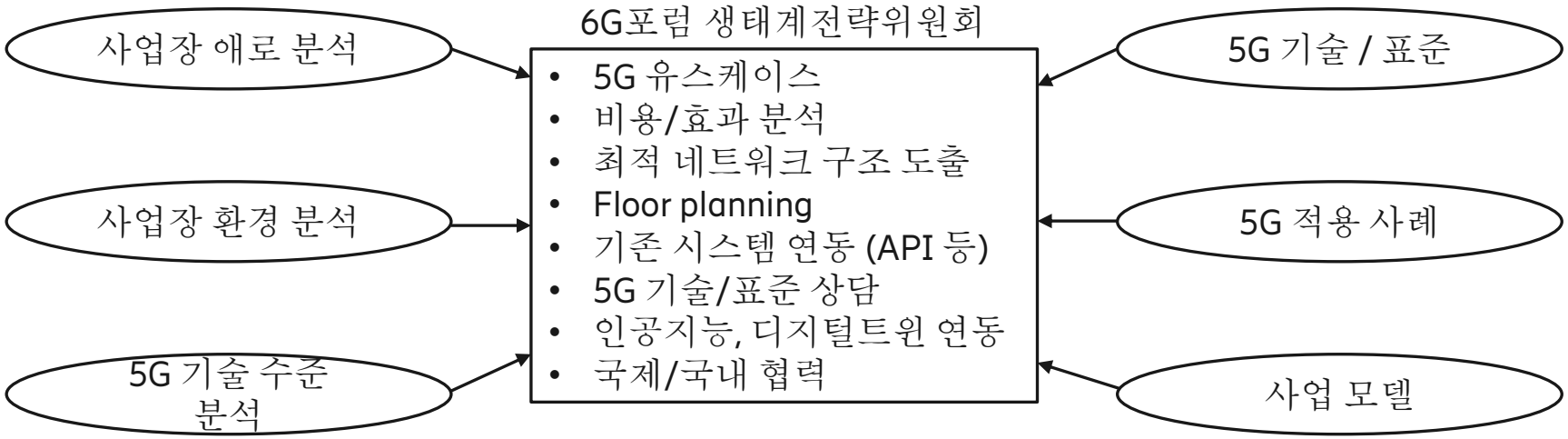
Cybersecurity Certification Test Plan for IoT Devices

Version 1.2.2

January 2021

BV CPS ADT Korea, CETECOM, Eurofins KCTL, Global CS Center of Samsung Electronics, HCT, KTL, MTCC, SEQAL, SGS Korea, TTA

특화망 활성화를 위한 생태계전략위원회 역할



with

5G Eco