수처리학회발표

IoT & Smart Water Management

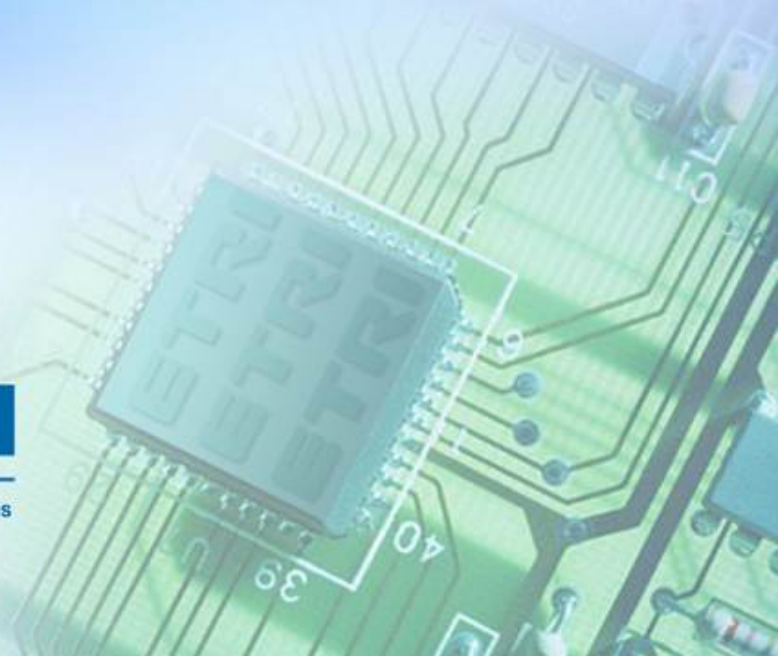
-Concerning IoT security issues in water management infra -

2015. 08. 25.

은재영

ETRI

Electronics and Telecommunications
Research Institute

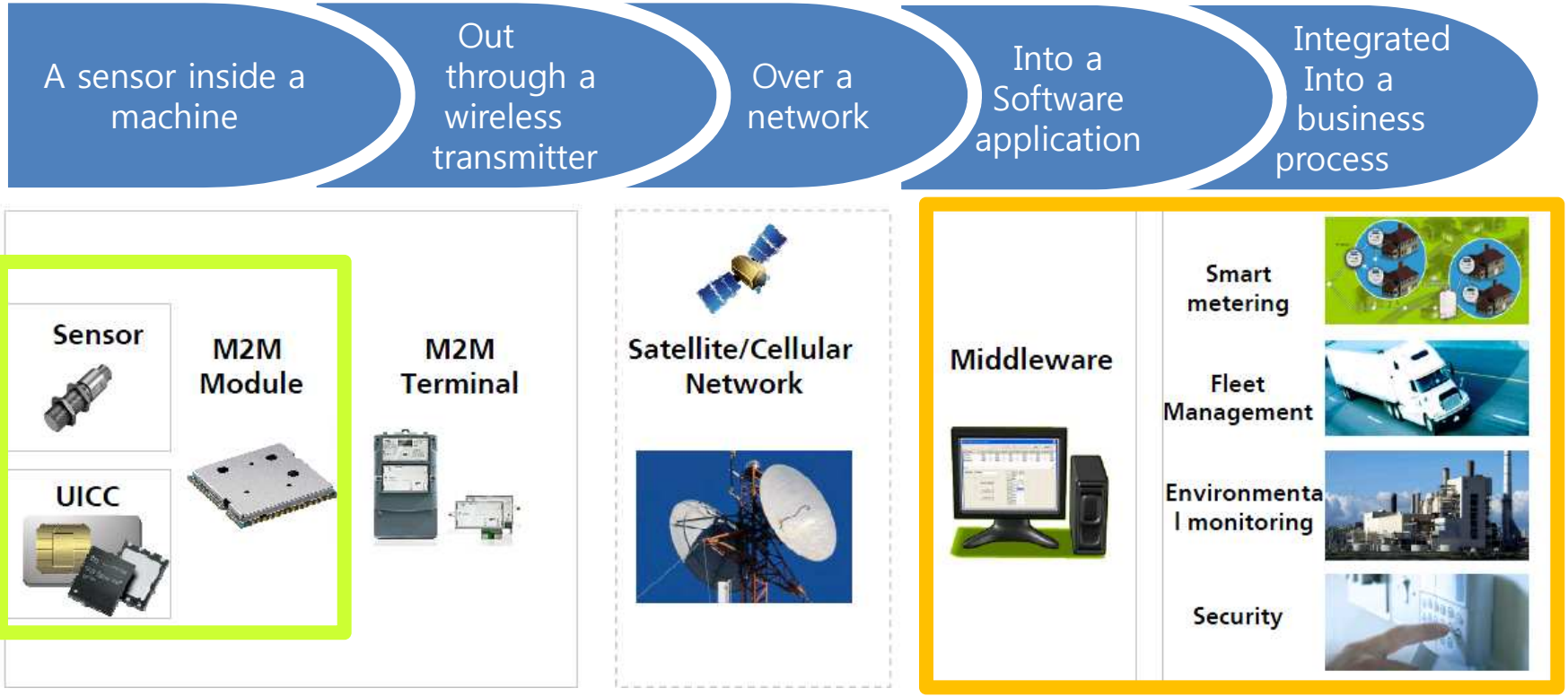


Contents

통신망 영역에서 정의하는 M2M/IoT 기본 구조

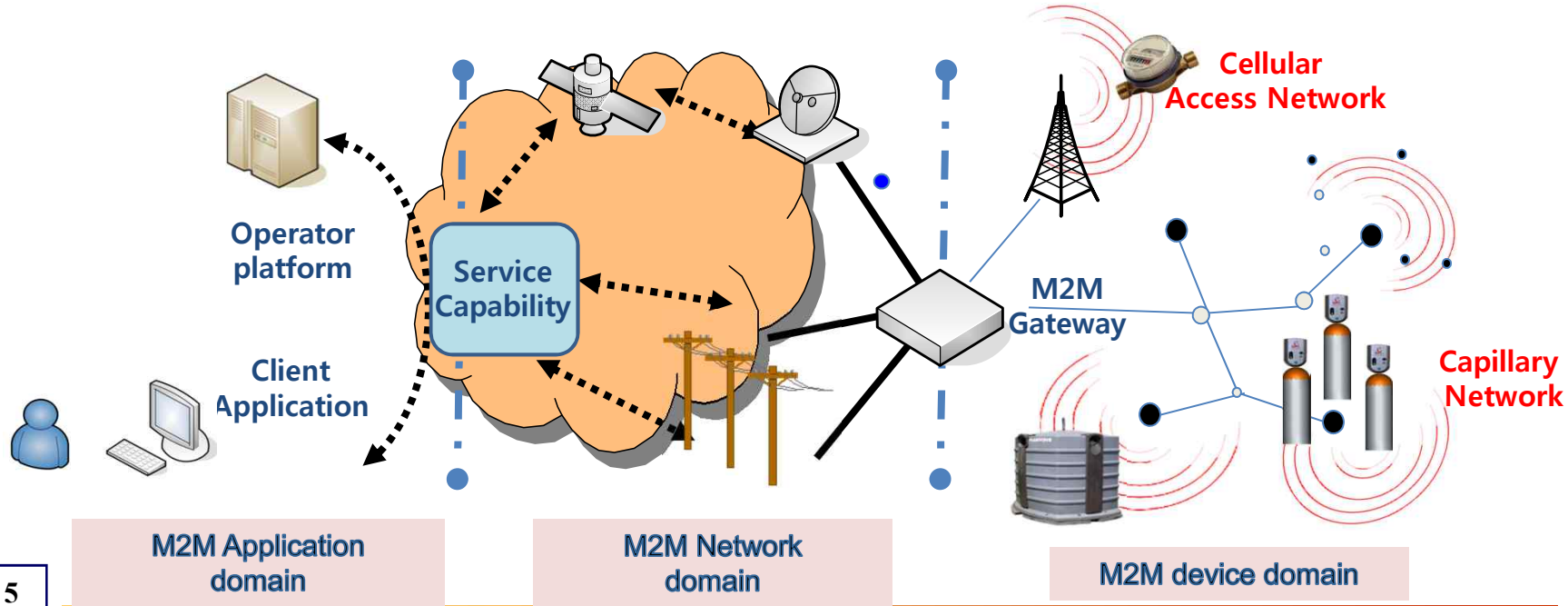
Practical M2M/IoT system overview

- M2M (machine to machine) involves communication without (or only limited) human intervention
  - M2M is essentially about combining electronics, telecommunications & information technologies in order to connect devices & remote systems



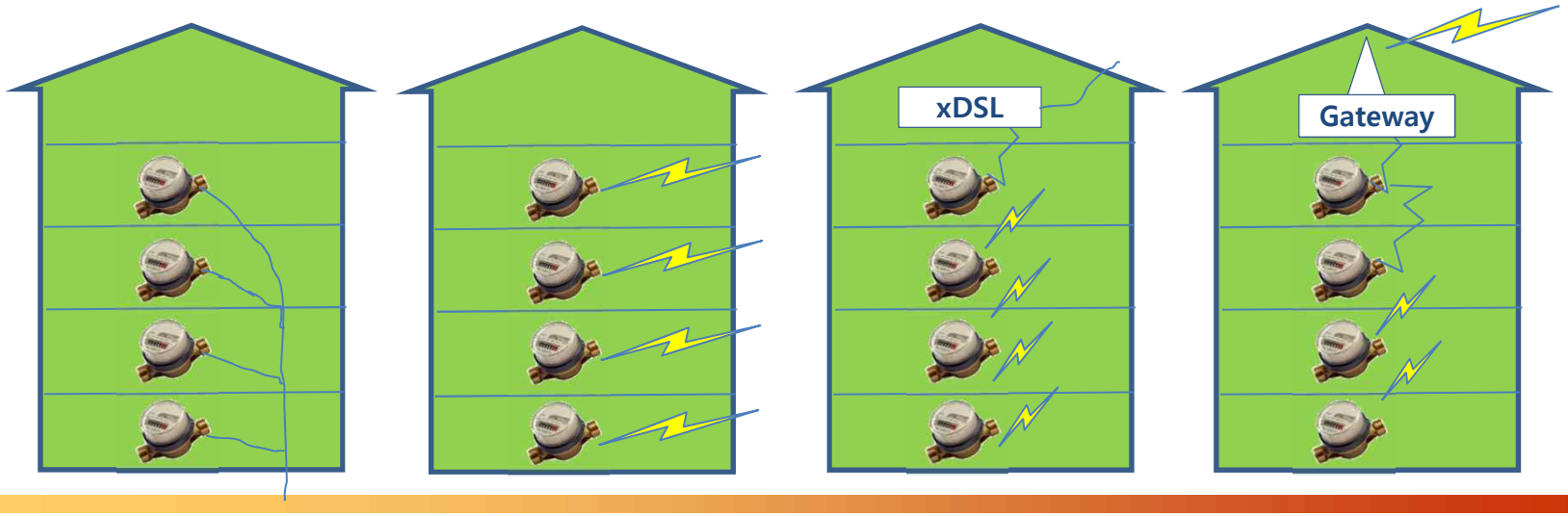
M2M E2E Network Architecture

- Access Network – connecting the sensor & actuators
  - Wired
  - Wireless – cellular
  - Wireless – capillary
- Gateway – connecting access and core network
  - Network address translation
  - Packet (de) fragmentation, etc
- Core/Backbone Network – connecting the computer system



M2M Access Networks

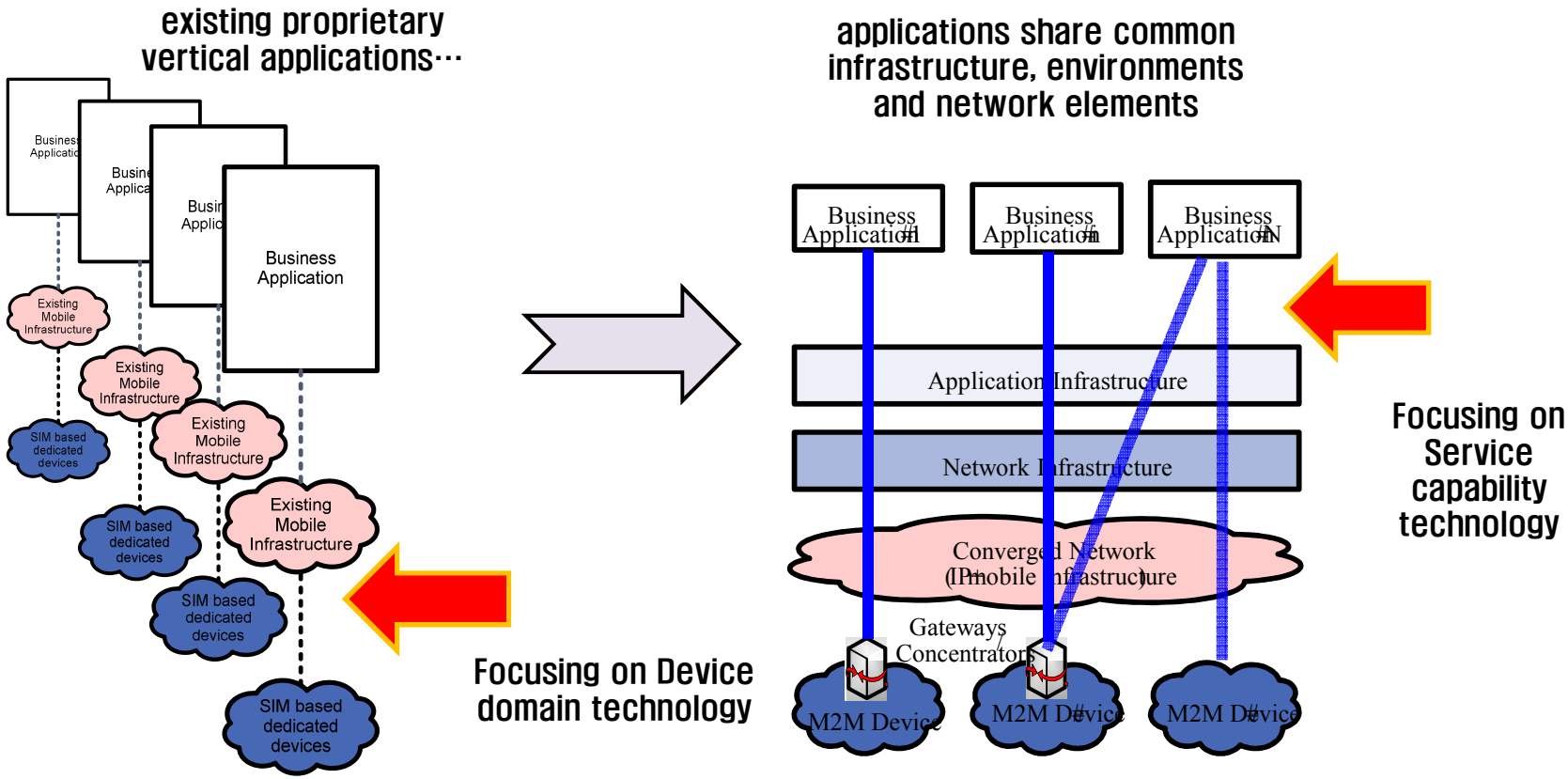
- Wired Solution – dedicated cabling between sensor – gateway:
  - pros: very, very reliable; very high rates, little delay, secure, cheap to maintain
  - cons: very expensive to roll out, not scalable
- Wireless Cellular Solution – dedicated cellular link:
  - pros: excellent coverage, mobility, roaming, generally secure
  - cons: expensive rollout, not cheap to maintain, not power efficient, delays
- Wireless Capillary Solution – shared short-range link/network:
  - pros: cheap to roll out, generally scalable, low power
  - cons: not cheap to maintain, poor range, low rates, weaker security, large delays
- (Wireless) Hybrid Solution – short-range until cellular aggregator:
  - pros: best tradeoff between price, range, rate, power, etc.
  - cons: not a homogenous and everything-fits-all solution



Standardization of M2M platform

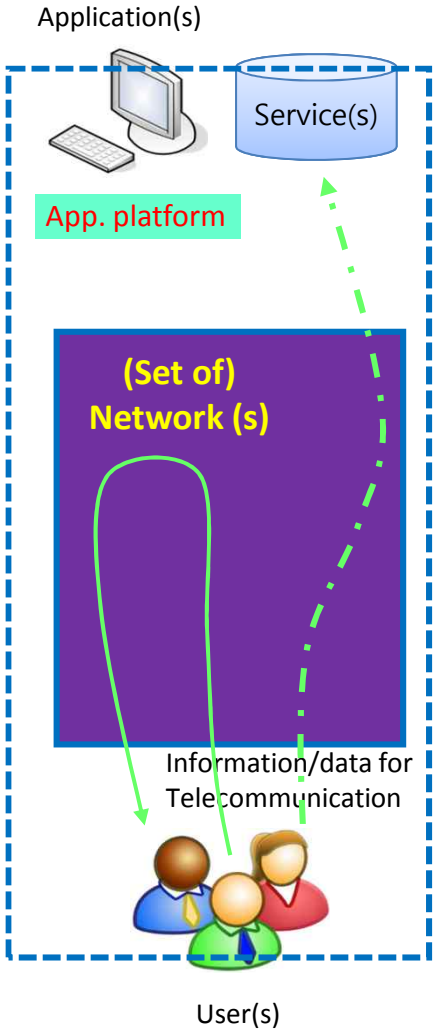
❑ TC M2M : use case, end-to-end architecture, service capabilities

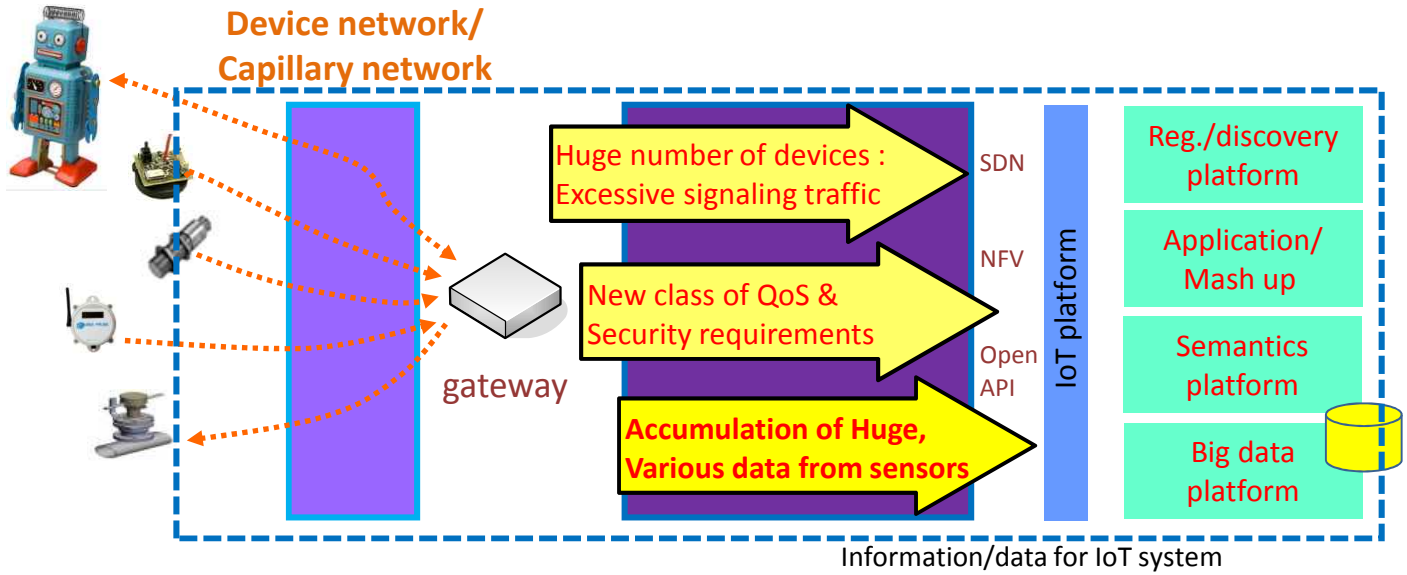
- Selecting a limited number of M2M use cases for operators, to avoid diverging visions and technical expansions
- Based on technology agnostic model for M2M communication, developed application scenarios and end-to-end architecture, focusing on horizontal integration of verticals



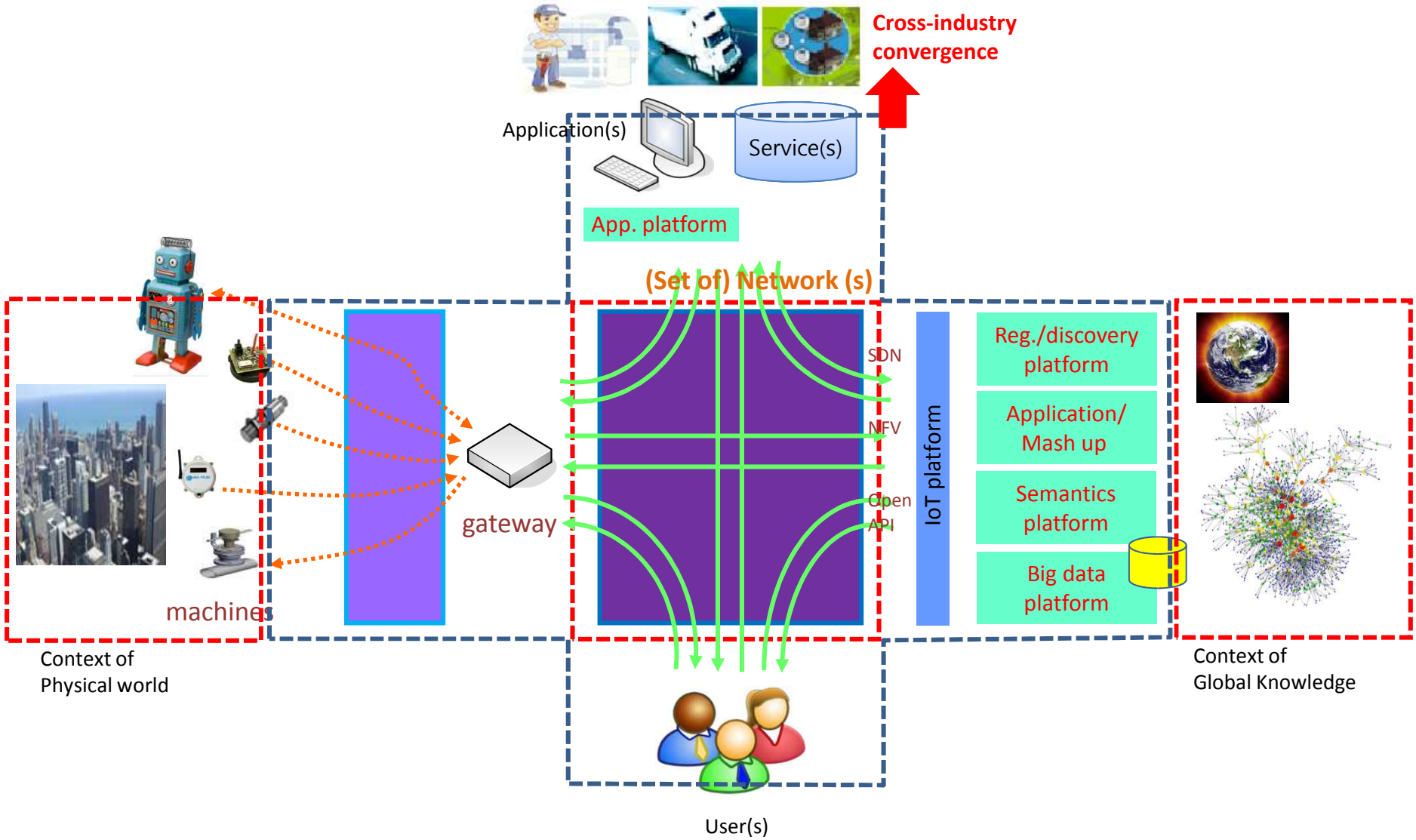
Implication of IoT Innovation

통신망…


Application(s)
Service(s)
App. platform
(Set of)
Network (s)
Information/data for
Telecommunication
User(s)


Device network/
Capillary network
gateway
Huge number of devices :
Excessive signaling traffic
New class of QoS &
Security requirements
Accumulation of Huge,
Various data from sensors
SDN
NFV
Open
API
IoT platform
Reg./discovery
platform
Application/
Mash up
Semantics
platform
Big data
platform
Information/data for IoT system

3 Ways of Openness

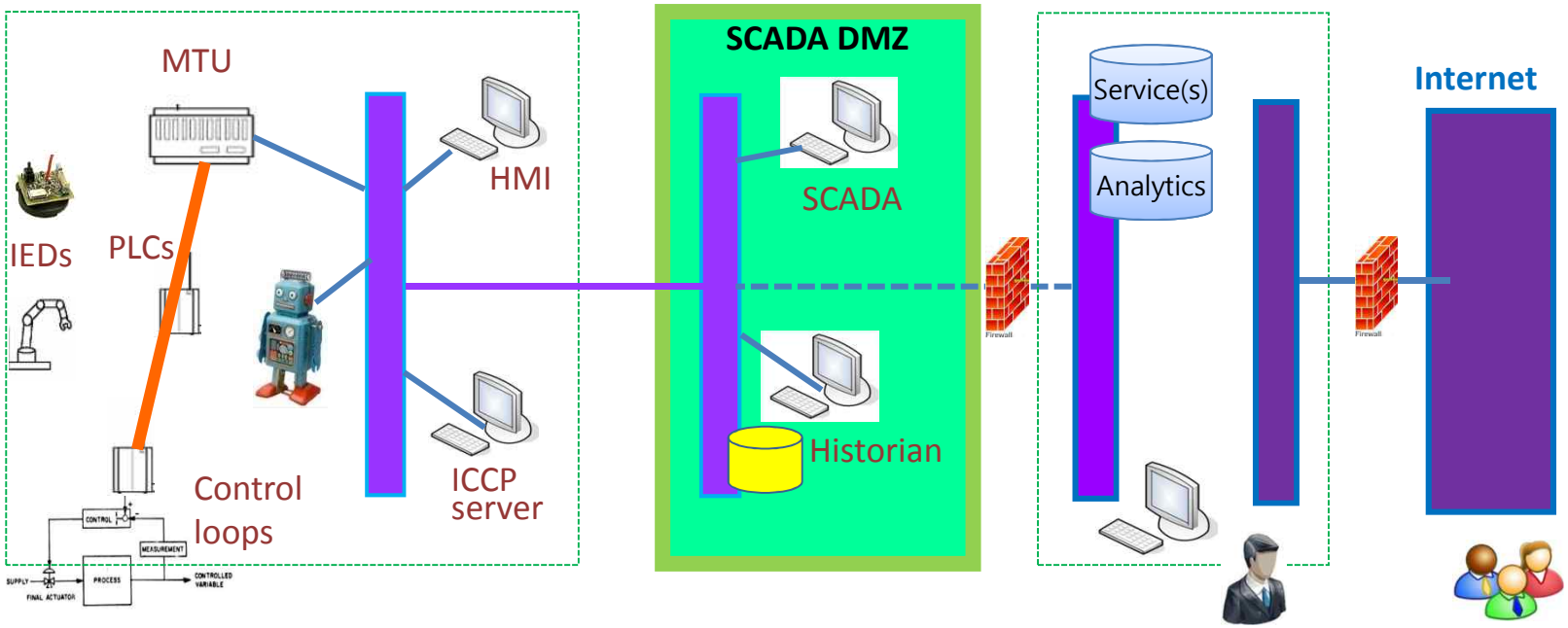


Innovative industry network for Water Management?

Architecture by Functions

Industrial automation & control system | SCADA/ supervisory system | Business & information system

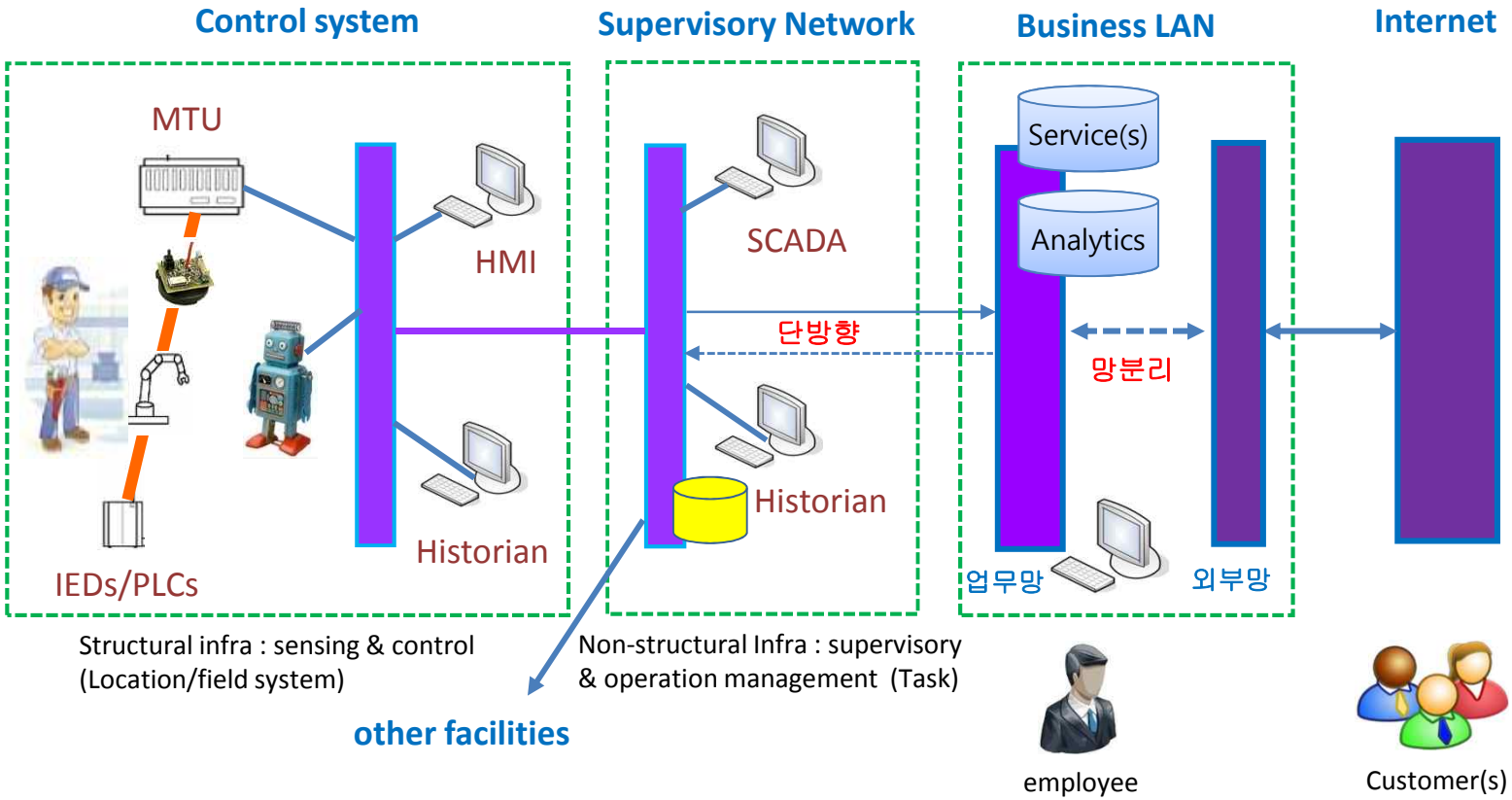
Functions	Control	SCADA	Enterprise
Real-time operation	Critical	High	Best effort
Reliability requirements	Critical	High	Best effort
Bandwidth requirements	Low	Low	High
Protocols used	Fieldbus	Fieldbus, TCP/IP	TCP/IP



Industrial Network

❑ Cross-industry Convergence

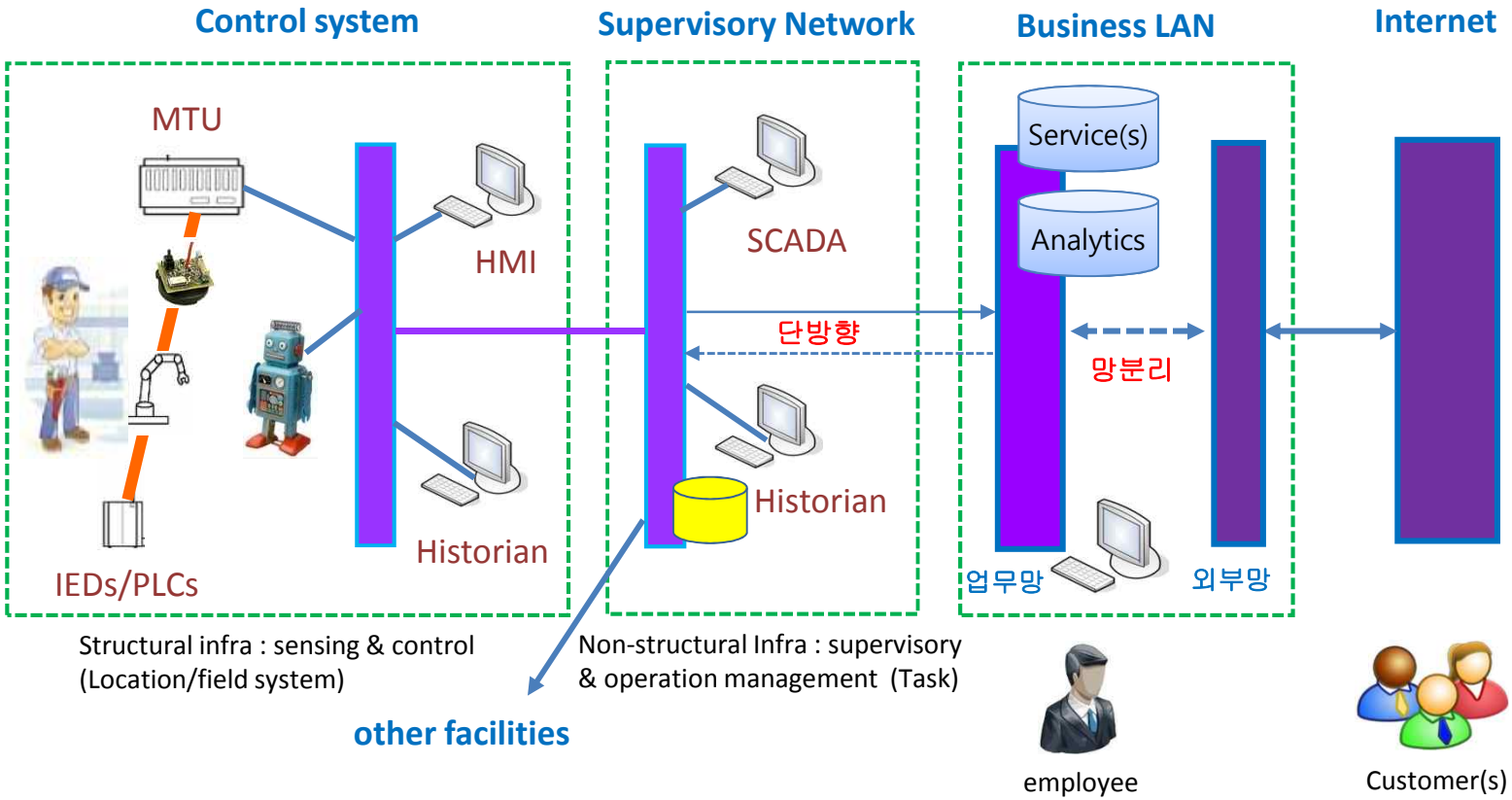
- 산업간 융합을 지원하는 IoT 시스템이 Industrial Network 까지 지원 가능 한지?
- Industrial Network => 제어망 (감시 및 운용) + 업무망 (정보응용)을 구현



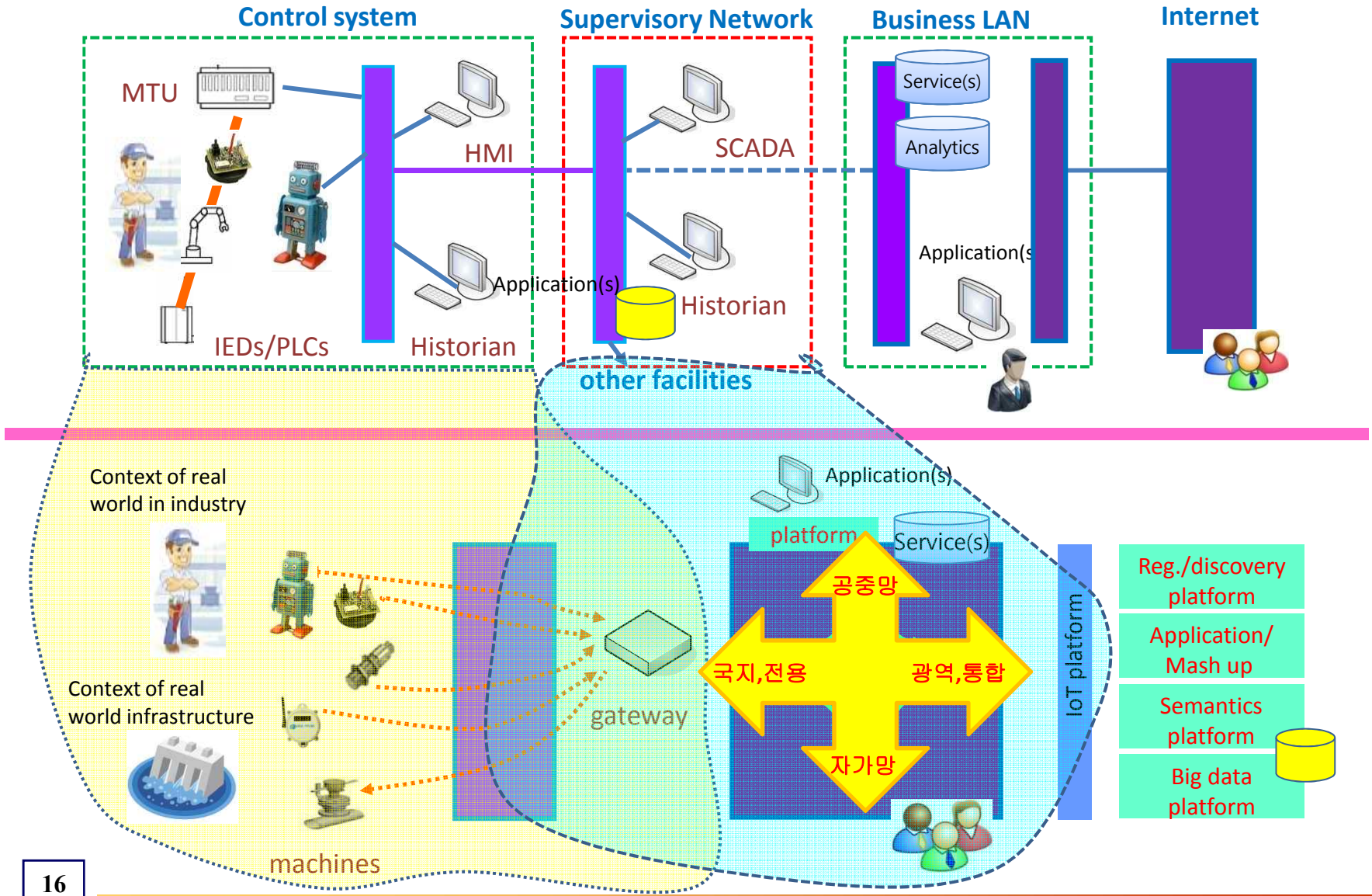
Industrial Network

❑ Cross-industry Convergence

- 산업간 융합을 지원하는 IoT 시스템이 Industrial Network 까지 지원 가능 한지?
- Industrial Network => 제어망 (감시 및 운용) + 업무망 (정보응용)을 구현



Mapping for Comparison



Critical Infrastructure Protection

❑ Critical Infrastructure (CI)

- " The assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health, or safety, or any combination thereof." (US Department of Homeland Security)

❑ Key Resources (KR)

- "Publicly or privately controlled resources essential to the minimal operations of the economy and government." (US Department of Homeland Security)

❑ CI/KR Sectors Identified (17 in USA)

- Homeland Security Presidential Directive (HSPD) -7
- Agriculture and Food , Banking and Finance, Chemical, Commercial Facilities, Communications, Dams, Defense Industrial Base, Emergency Services, Energy, Government Facilities, Information Technology, National Monuments and Icons, Nuclear Reactors, Materials, and Waste, Postal and Shipping, Public Health and Healthcare, Transportation Systems, Water

❑ Priority/immediate responder CI/KR needs (6 in USA)

- Agriculture and food (food)
- Communications
- Energy (particularly electric power and fuel)
- Information technology
- Transportation systems
- Water

Critical Infrastructure Network

❑ Industrial Network

- Automated control system (IDES, PLCs,)들의 네트워크, 분산 제어 및 SCADA 를 구현
- 시스템 신뢰도 (reliability, resiliency) 및 안전성 (security) 를 제공해야 함

❑ Industrial Network Security

- 산업용 네트워크에, 일반적인 security requirement 를 적용

1) Critical Asset 의 식별 : 어떤 시스템을 보호해야 하는지 판정
2) Network Segmentation/Isolation of Systems : 시스템들을 기능 그룹 단위로 논리적 분리
3) Defense in Depth : 각 시스템 주변을 보호하는 정책 구현
4) Access Control : 각 그룹들간의 액세스를 제어

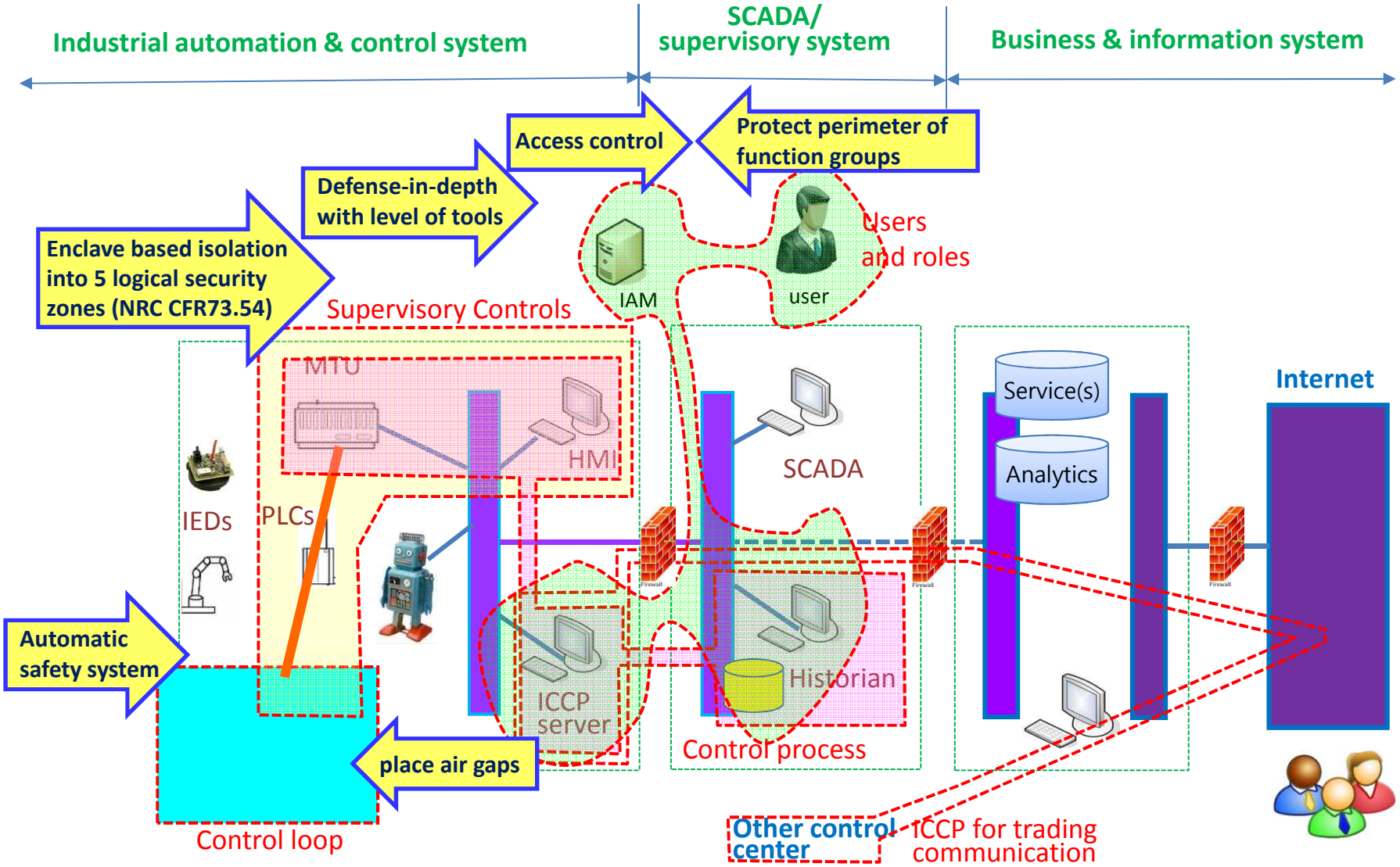
❑ Critical Industrial Network (?)

- 민감하고 중요한 산업용 네트워크
- attack 의 결과가 심대한 지장을 초래하는 산업용 네트워크
- Critical Infra Network 과 기술적 특징으로는 유사한 의미로 사용가능

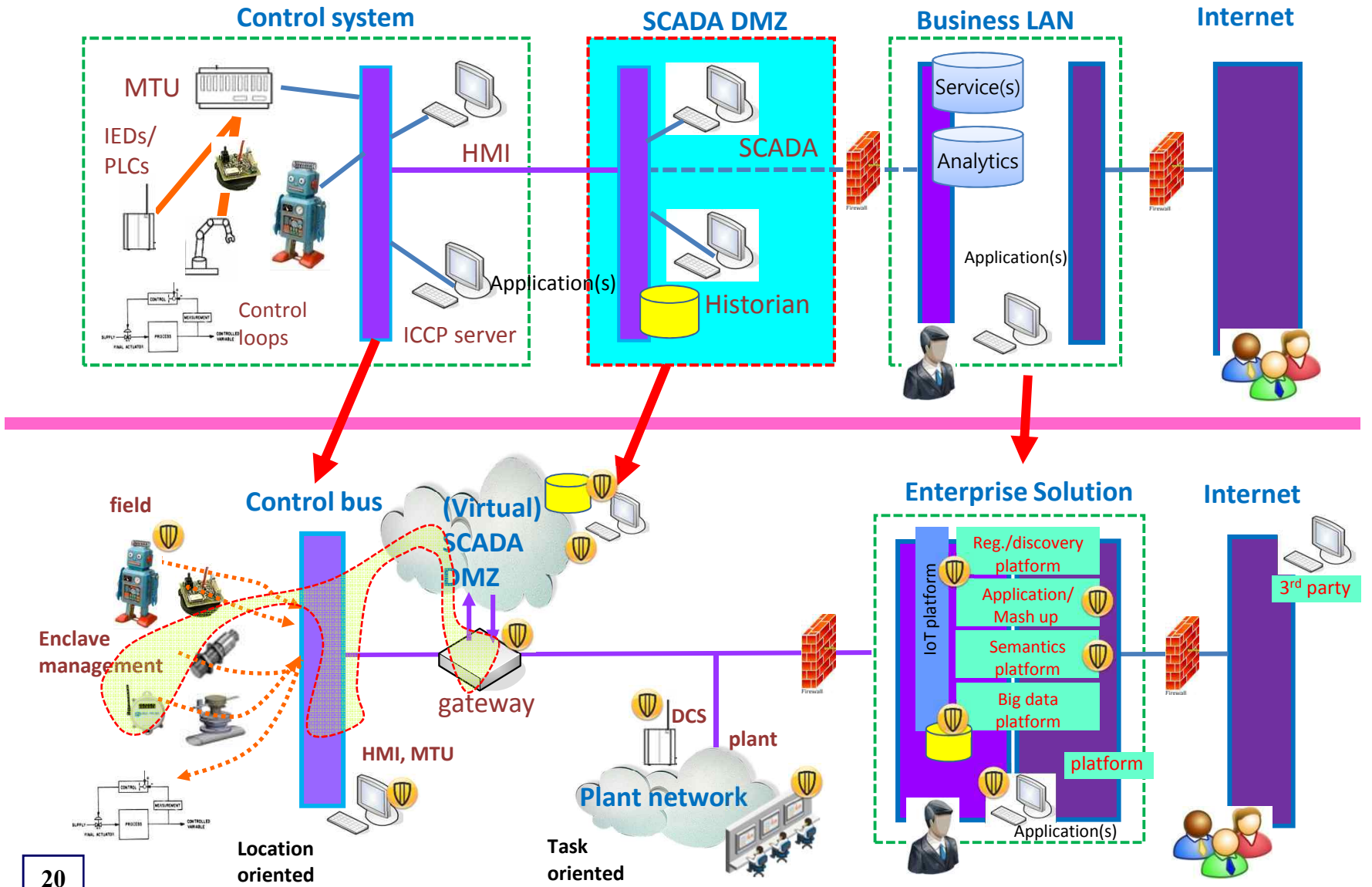
❑ [CIN : Critical Infrastructure 의 직접 운용을 위해 사용되는 Network]

- 민감한 중요 인프라용 네트워크. 자체적으로도 민감 자산을 보유
- Critical Infrastructure Protection Plan 을 구현해야 함

Security Concepts



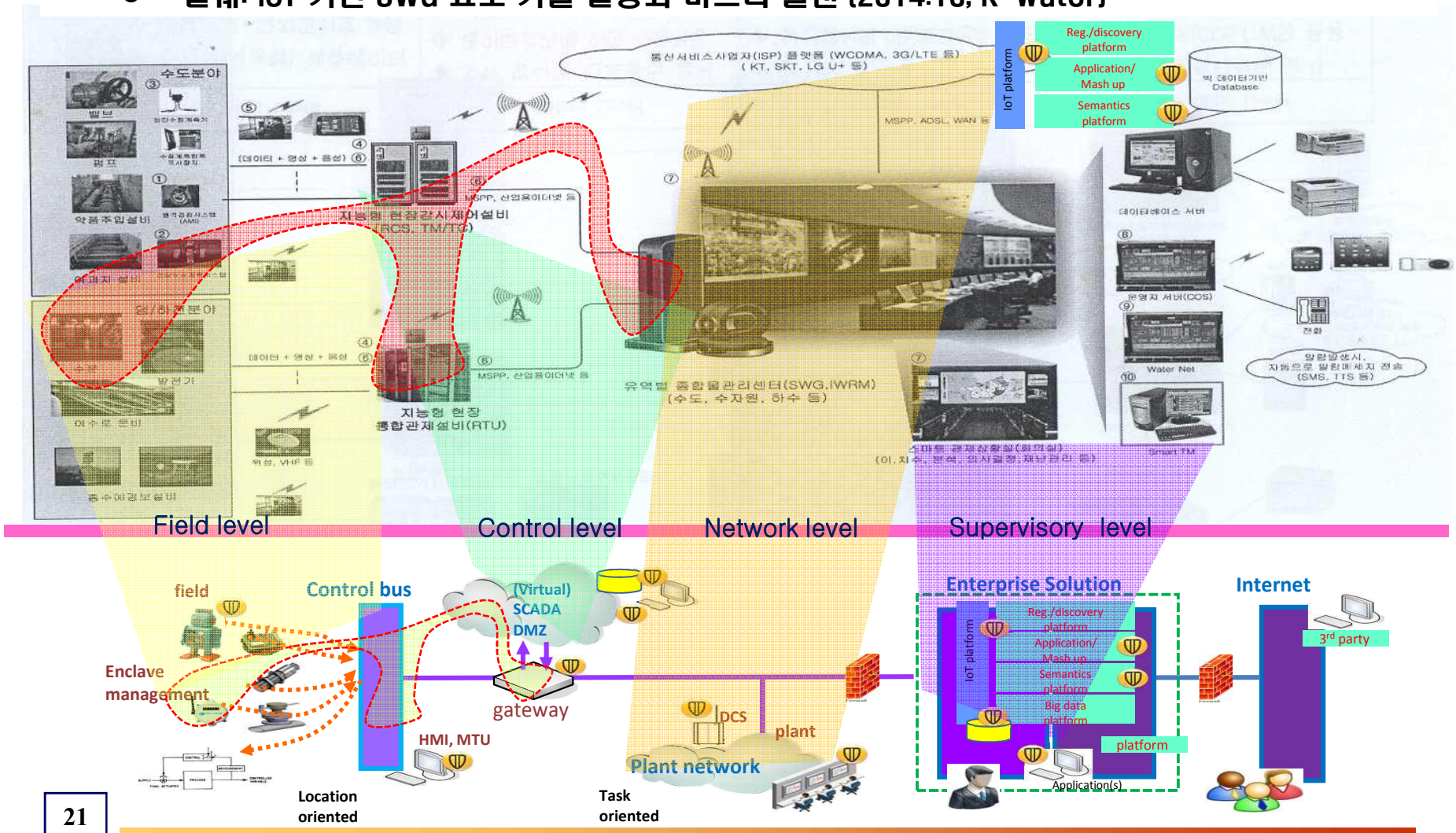
Mapping for IoT operator ?



Water Management System

❑ 원격감시제어시스템 구성 개념도 (2018 ~)

- 발췌: ICT 기반 SWG 요소 기술 실용화 마스터 플랜 (2014.10, K-water)



Conclusion

- ❑ IoT 기술의 Innovation impact 는 service 측면에서 확장
  - 서비스 플랫폼과 빅 데이터를 중심으로 한 응용에 집중
  - Networking 의 이슈가 간과되어 왔으나, 최근 일부 확장 중
  - 3ways of openness 모델에 따라, access network 부분에 큰 혁신 역량이 잠재
- ❑ 수자원관리 망에서 IoT 를 도입 할 경우 보안이슈가 관검
  - 데이터 연동, 글로벌 연동과 자율운영의 특성을 수용할 인프라가 필요
  - 현재 SWG 등 수자원 관리망은 IoT 기능 플랫폼의 안전한 수용방법에 대해 구체적 고려 미비
- ❑ 융합 Network infra 의 제공 => 융합 infra 를 위한 network 으로
  - IoT 시스템 전반의 기본 모델이 real world 를 다루는 industry / infra network 과 유사
  - 산업 인프라 네트워크, 특히 수자원관리 망등 국가적 critical infra 의 진화를 고려해야
- ❑ CIP/CIR을 도입하는 과정에서, 시대적으로 IoT security 를 포함 하는 것
  - 진보적인 IoT 의 도입은 서비스 효율과 인프라 탄력성을 강화
  - CIP 의 Security 설계 개념은 미래의 IoT 인프라 구축에 도움이 될 것
- ❑ 상호의존적, 복합적 인프라의 안전성/탄력성 이슈
  - 수자원관리망의 경우도 상호 의존성, 혹은 중복성이 있는 다수 인프라들 간의 통합 운영과 security 이슈를 고려 해야 함
- ❑ C^2IN을 확장, 초연결 시대의 네트워크 access 기반 구조 모델의 제공이 가능