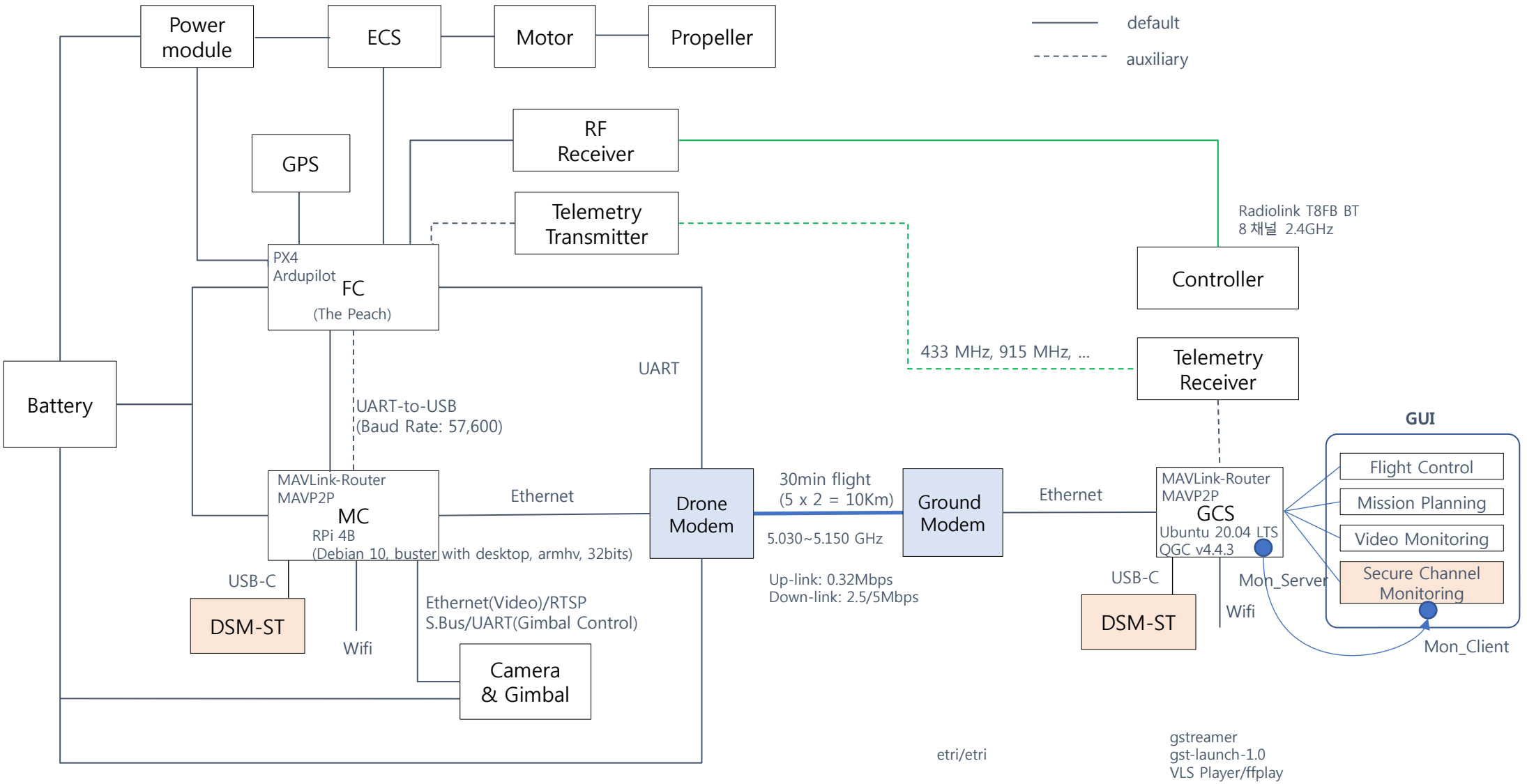
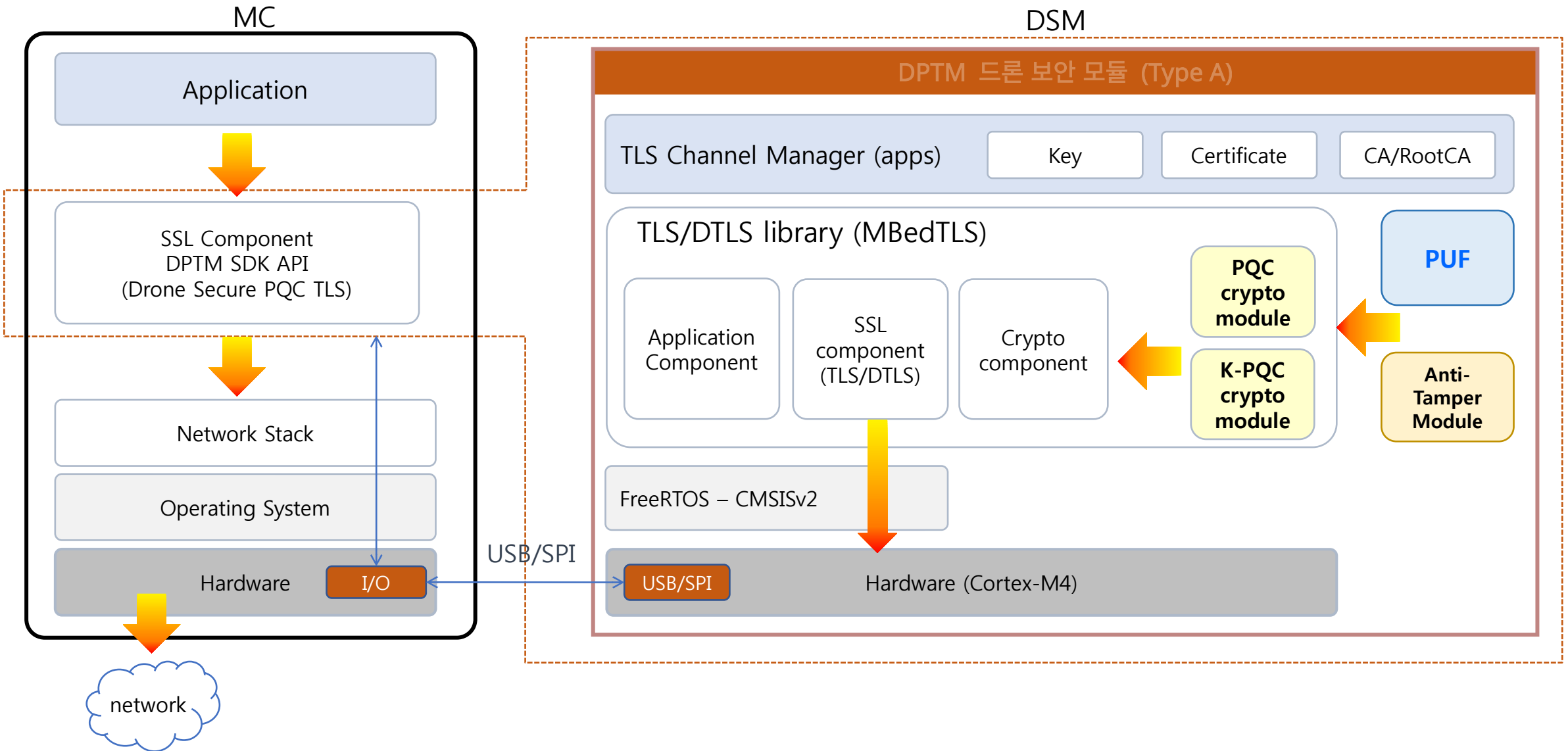
보안채널 모니터링 GUI 설계

(Secure Channel Monitoring)

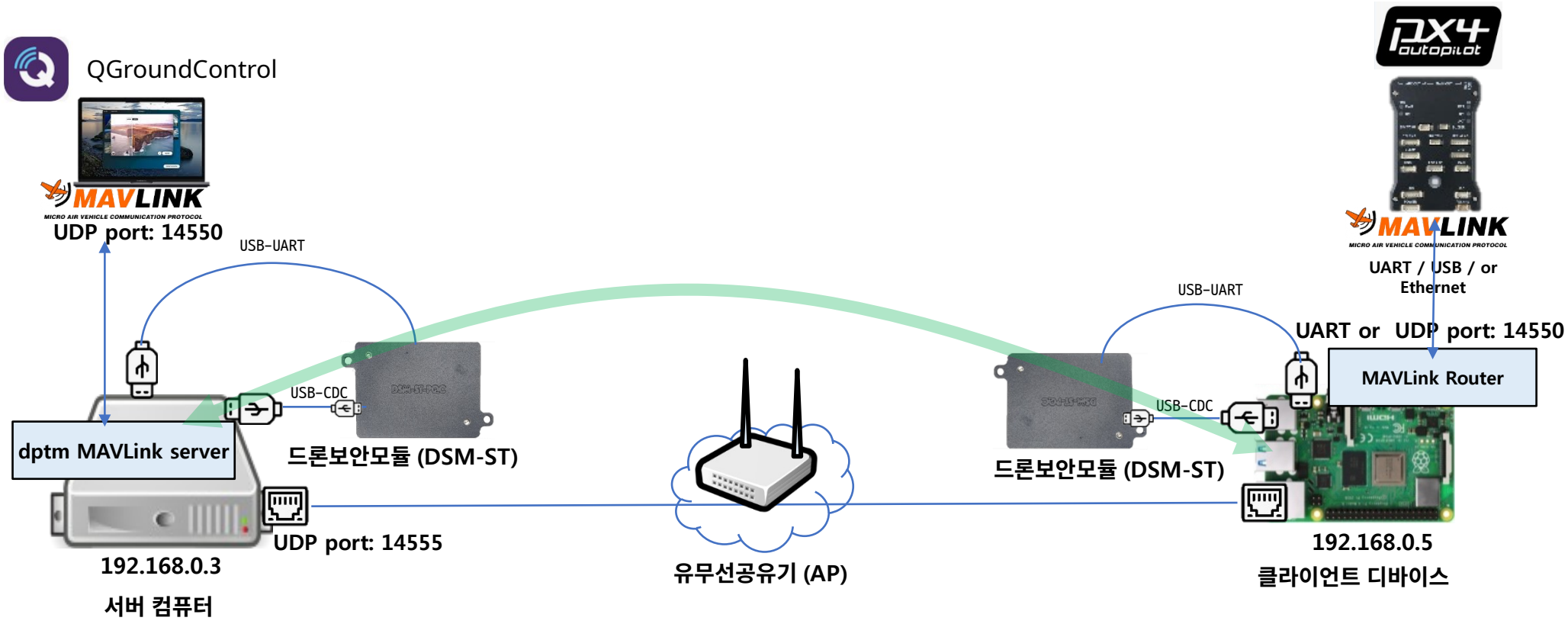
국방 드론 시스템 구조도 (DSM-ST 연동)



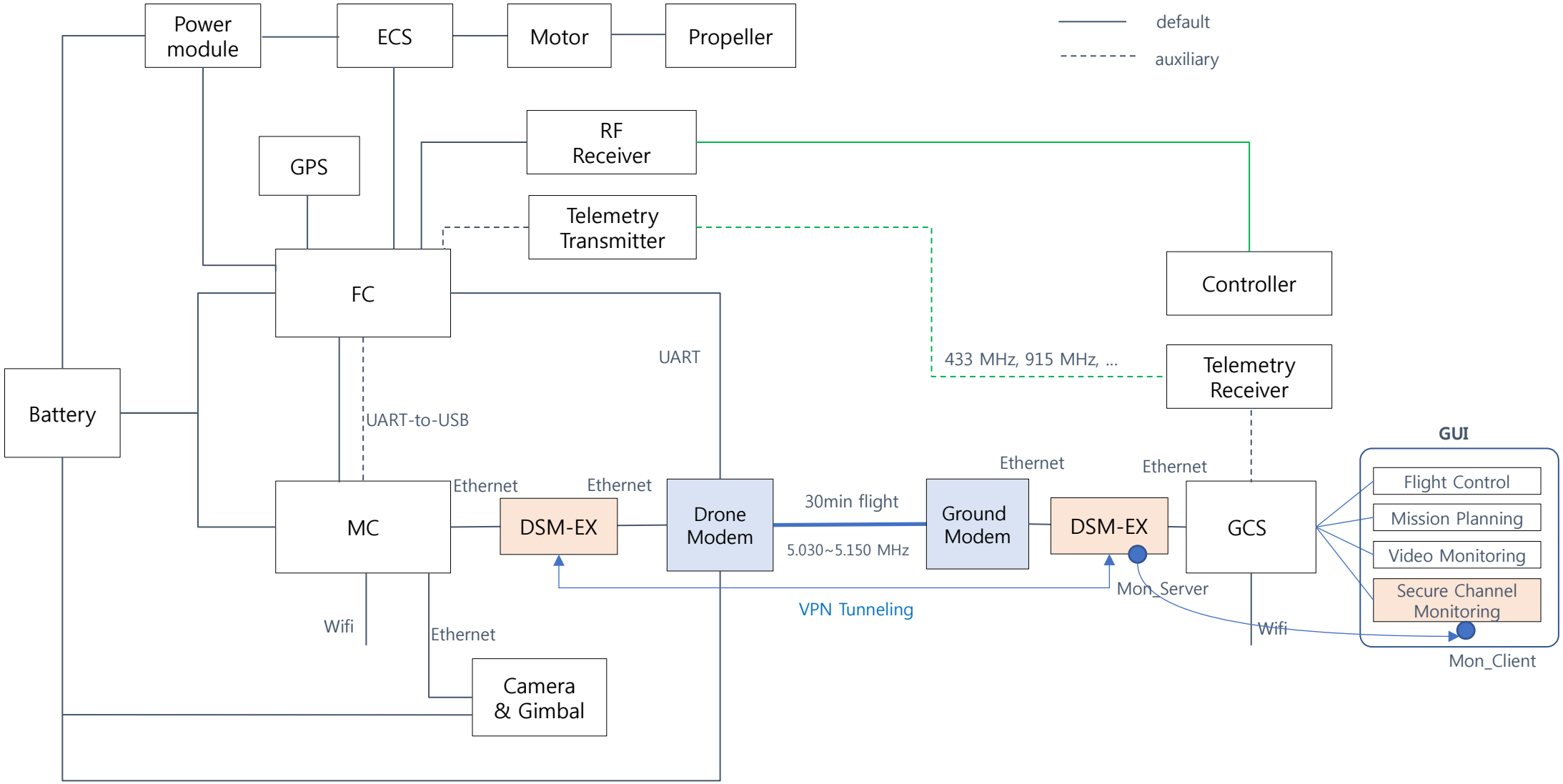
DSM-ST


MC
Application
SSL Component
DPTM SDK API
(Drone Secure PQC TLS)
Network Stack
Operating System
Hardware
I/O
network
USB/SPI
DSM
DPTM 드론 보안 모듈 (Type A)
TLS Channel Manager (apps)
Key
Certificate
CA/RootCA
TLS/DTLS library (MBedTLS)
Application Component
SSL component (TLS/DTLS)
Crypto component
PQC crypto module
K-PQC crypto module
PUF
Anti-Tamper Module
FreeRTOS – CMSISv2
USB/SPI
Hardware (Cortex-M4)

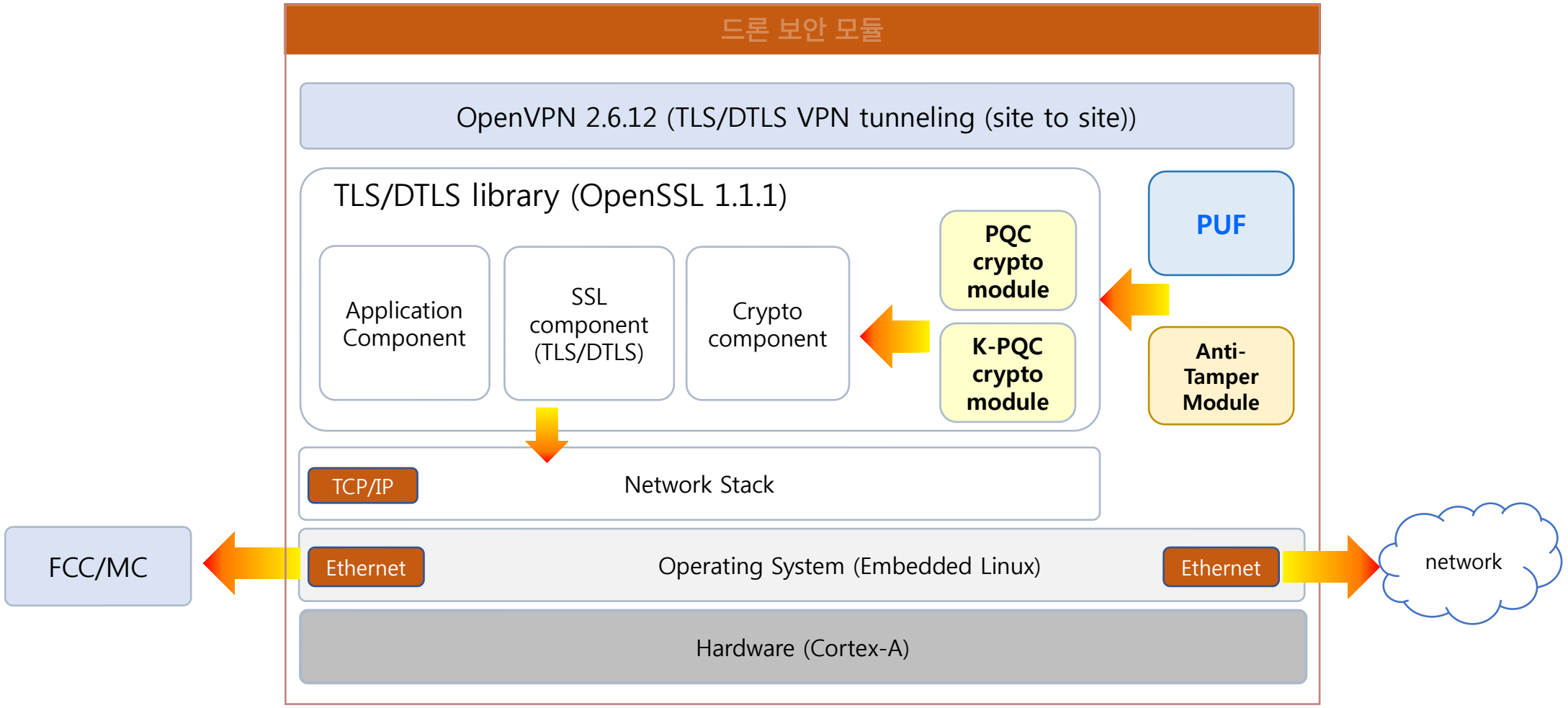
DSM-ST – 네트워크 구성도



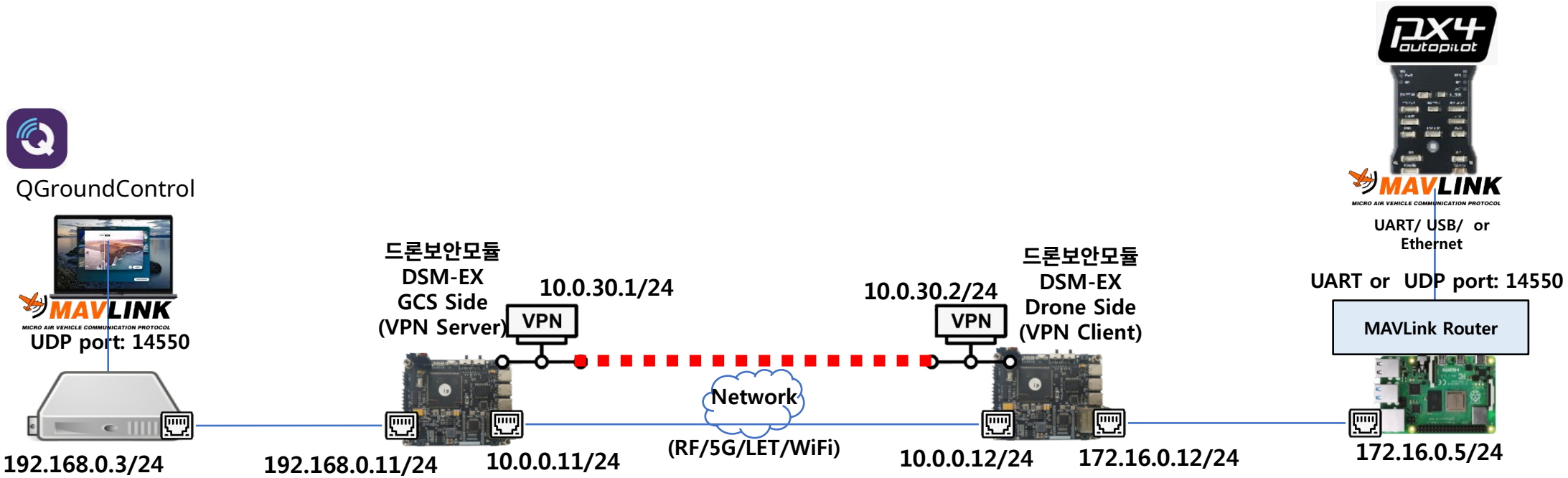
국방 드론 시스템 구조도 (DSM-EX 연동)



DSM-EX


드론 보안 모듈
OpenVPN 2.6.12 (TLS/DTLS VPN tunneling (site to site))
TLS/DTLS library (OpenSSL 1.1.1)
Application Component
SSL component (TLS/DTLS)
Crypto component
PQC crypto module
K-PQC crypto module
PUF
Anti-Tamper Module
TCP/IP
Network Stack
Ethernet
Operating System (Embedded Linux)
Ethernet
Hardware (Cortex-A)
FCC/MC
network

DSM-EX – 네트워크 구성도



Secure Channel Monitoring

State Information

cmd: 16

- State: Connected
- Protocol: TLSv1.2
- KEM: Kyber512
- DSA: Dilithium2
- Ciphersuite: AES_256_GCM_SHA384

- Tx Packets: 0
- Rx Packets: 0
- Tx Bytes: 0
- Rx Bytes: 0

Visualization: FCC → GCS

Visualization : GCS → FCC

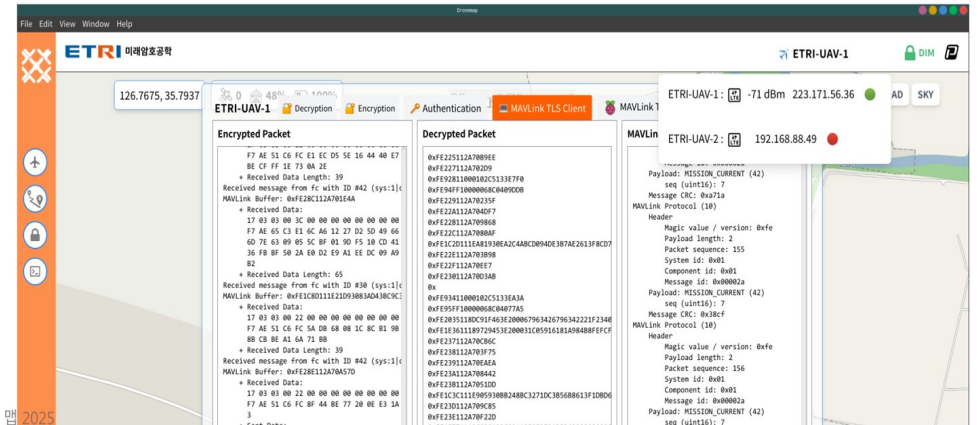
Data Monitoring: FCC → GCS

cmd(DSM-ST): 2 0

cmd(DSM-EX): 6 4

Ciphertext (Encrypted Data)	Plaintext (Decrypted Data)	MAVLink (Flight & Sensing)

- 암호화 데이터와, 복호화 데이터 터미널 출력을 GUI 텍스트 박스에 출력
- MAVLink 파싱은 네트워크 프로토콜 분석기 Wireshark 이용



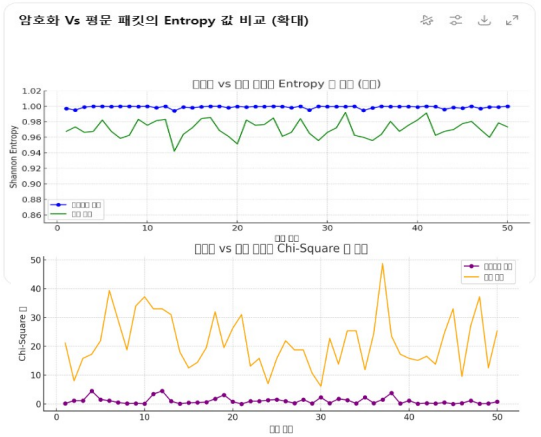
Data Monitoring: GCS → FCC

cmd: 1 3

cmd: 5 7

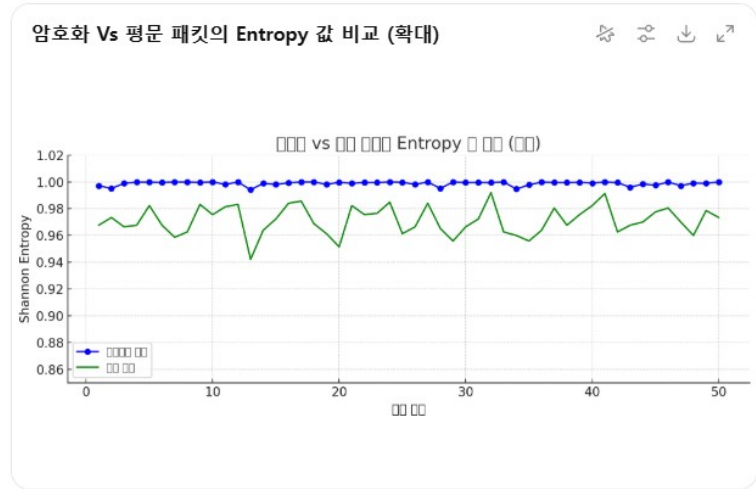
MAVLink (Command & Control)	Plaintext (Decrypted Data)	Ciphertext (Encrypted Data)

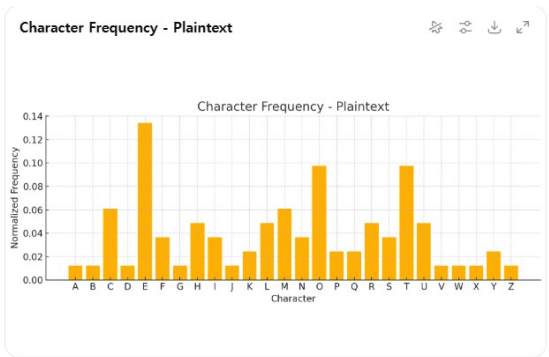
- 그래프를 이용한 시각화 (if possible)

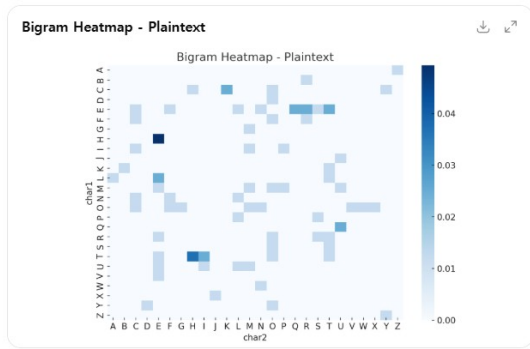


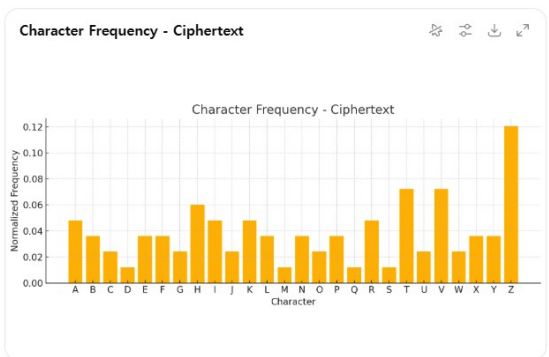
시각화 요약 그래프 구성 아이디어

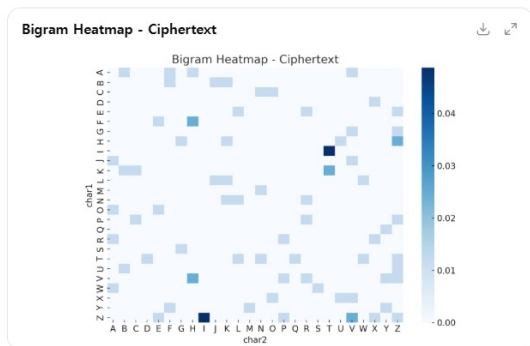
분석 종류	Plaintext 예시	Ciphertext 예시
문자 빈도 히스토그램	불균형한 분포	균등 분포
bigram 히트맵	특정 조합이 빈번	무작위
엔트로피 수치	낮음 (4~5)	높음 (7~8)
chi-square 값	작음	큼

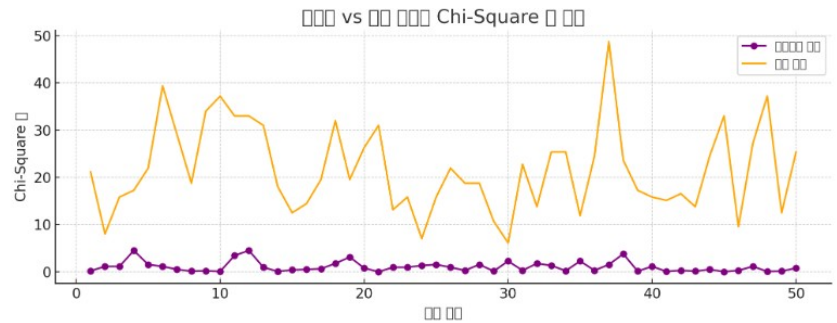


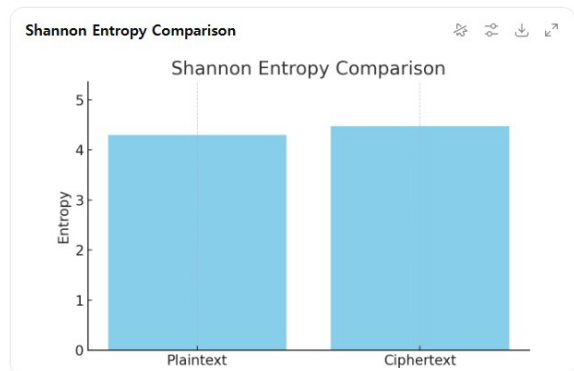


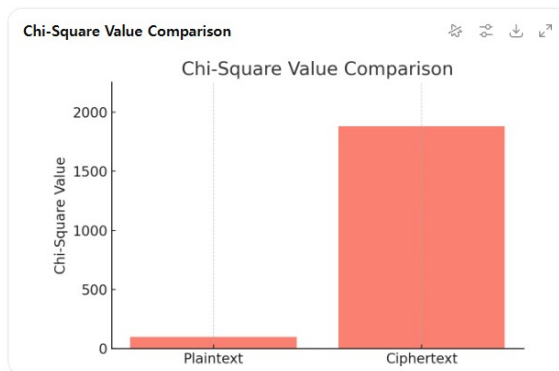












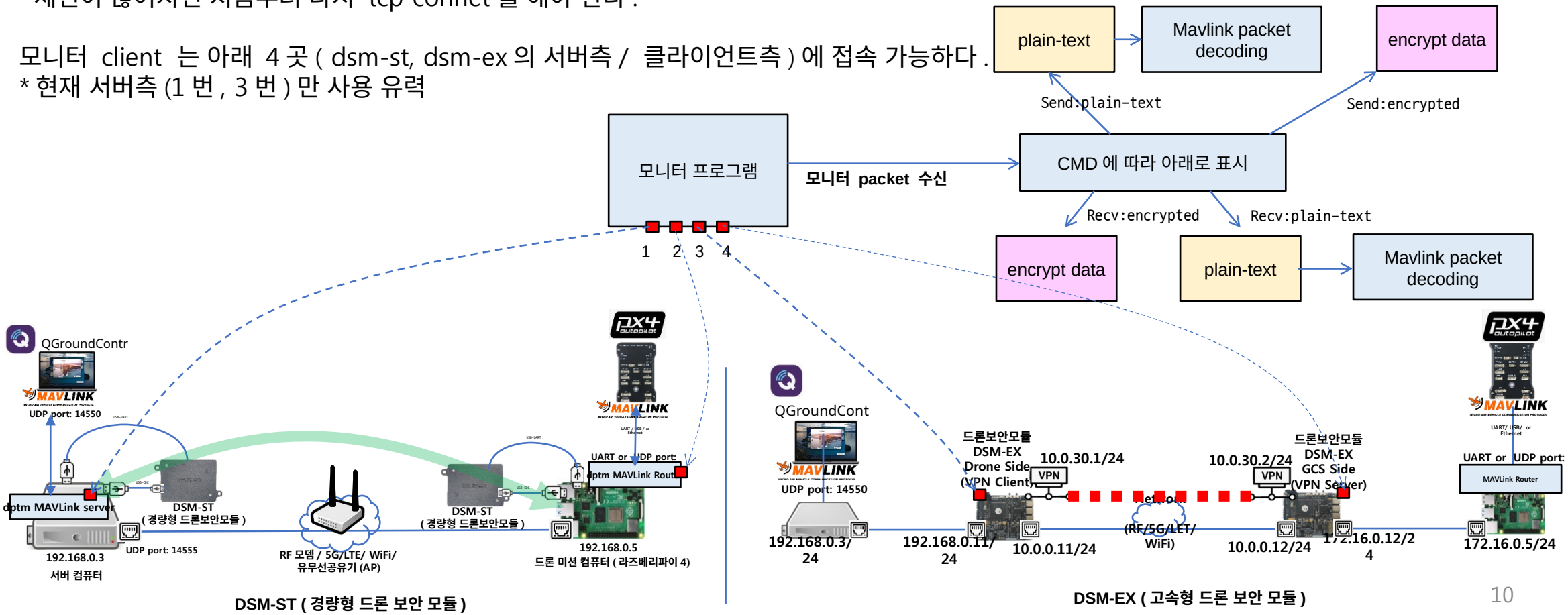
DSM-TLS 모니터링 프로토콜

- connection 실패 시 : 경량형 - 세션 없음 , 고속형 - 치명적 오류 (무조건 connection 은 가능해야함)
- TCP port : 14445

- 세션 상태 표시 : 모니터 서버에 연결 후 수초 마다 전송됨 .

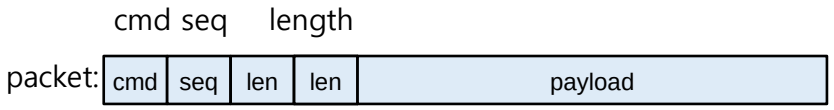
- 모니터 client 는 지속적으로 수신 해야 하며 , 수신을 일정 시간 하지 않으면 세션이 끊어진다 .
  세션이 끊어지면 처음부터 다시 tcp connet 를 해야 한다 .

- 모니터 client 는 아래 4 곳 (dsm-st, dsm-ex 의 서버측 / 클라이언트측) 에 접속 가능하다 .
  * 현재 서버측 (1 번 , 3 번) 만 사용 유력



TLS 모니터링 프로토콜

- 프로토콜은 아래와 같다 .(IP/TCP)
- 4byte head 를 먼저 수신 한다 .
- head 에서 length(16bit, big-endian) 를 얻어 , 길이가 0 이 아니면 , 해당 길이 만큼 무조건 수신 (읽어야) 한다 .

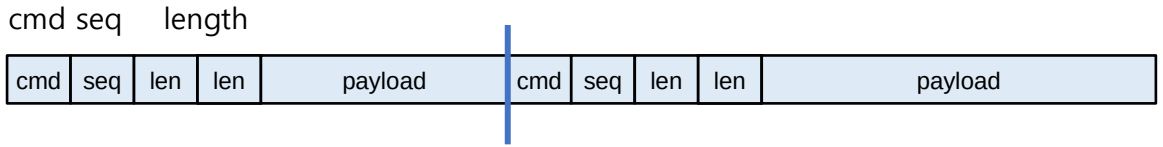



```
cmd bit: 7654 3210
         0000 0000:  recv
         0000 0001:  send

         0000 0010:  encrypted
         0000 0100:  packet mode(DSM-EX)
         0000 1000:  ping(no data)
         0001 0000:  status

0:  RECV
1:  SEND
2:  encrypt RECV
3:  encrypt SEND
4:  packet: RECV
5:  packet: SEND
6:  packet: encrypt RECV
7:  packet: encrypt SEND
8:  PING
16: status
```

데이터는 지속적으로 아래와 같이 전송된다 .

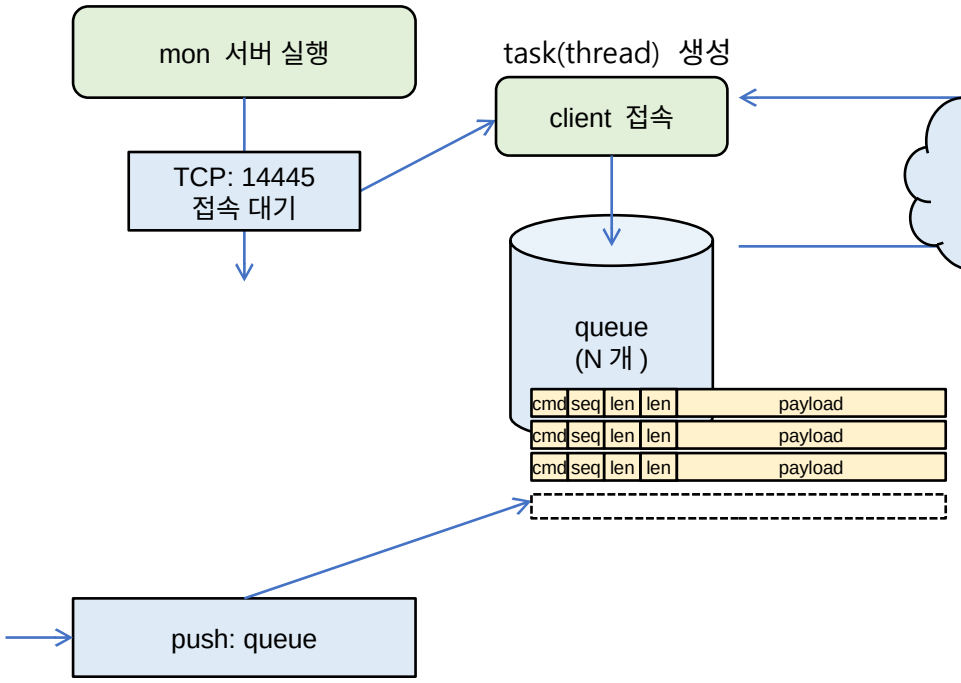


16: status – example(json 형태)

```
{
   "state": "connected",
   "tls_ver": "dtls1.2“,
   "kem": "MLKEM512",
   "sig": "MLDSA44",
   "ciphersuite":
“TLS_AES_128_GCM_SHA256",
   "tx_packets": 0,
   "rx_packets" 0,
   "tx_bytes": 0,
   "rx_bytes": 0
}
```

TLS 모니터링 서버 구조

- mon server (DSM-ST, DSM-EX)



event: packet 수신 시 접속된 queue 에 push

- mon client
  - mon_svc library