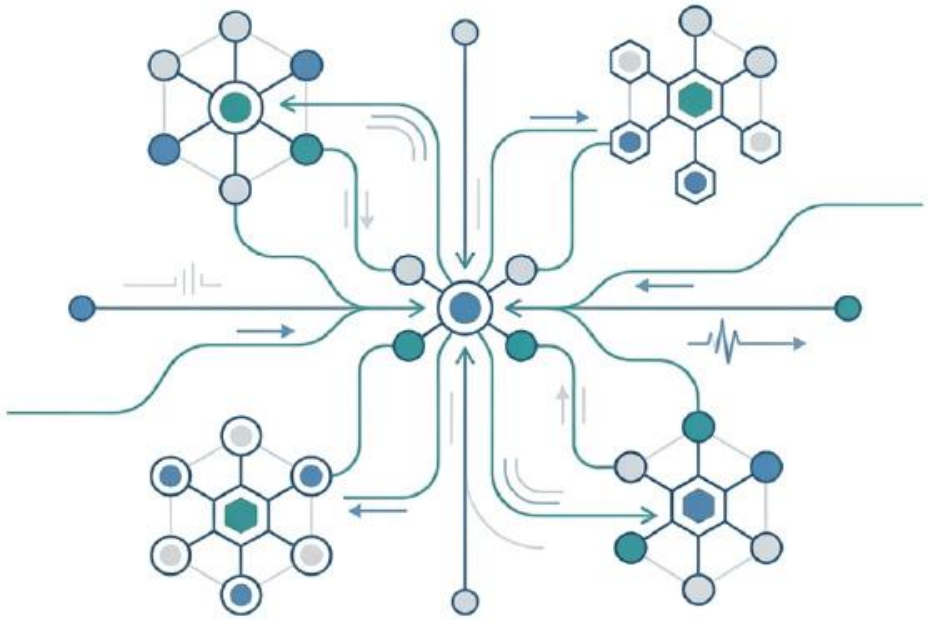
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ



Επιστημονική Ημερίδα της Αρχής:
2η Ημέρα Διαλόγου με την Ερευνητική Κοινότητα

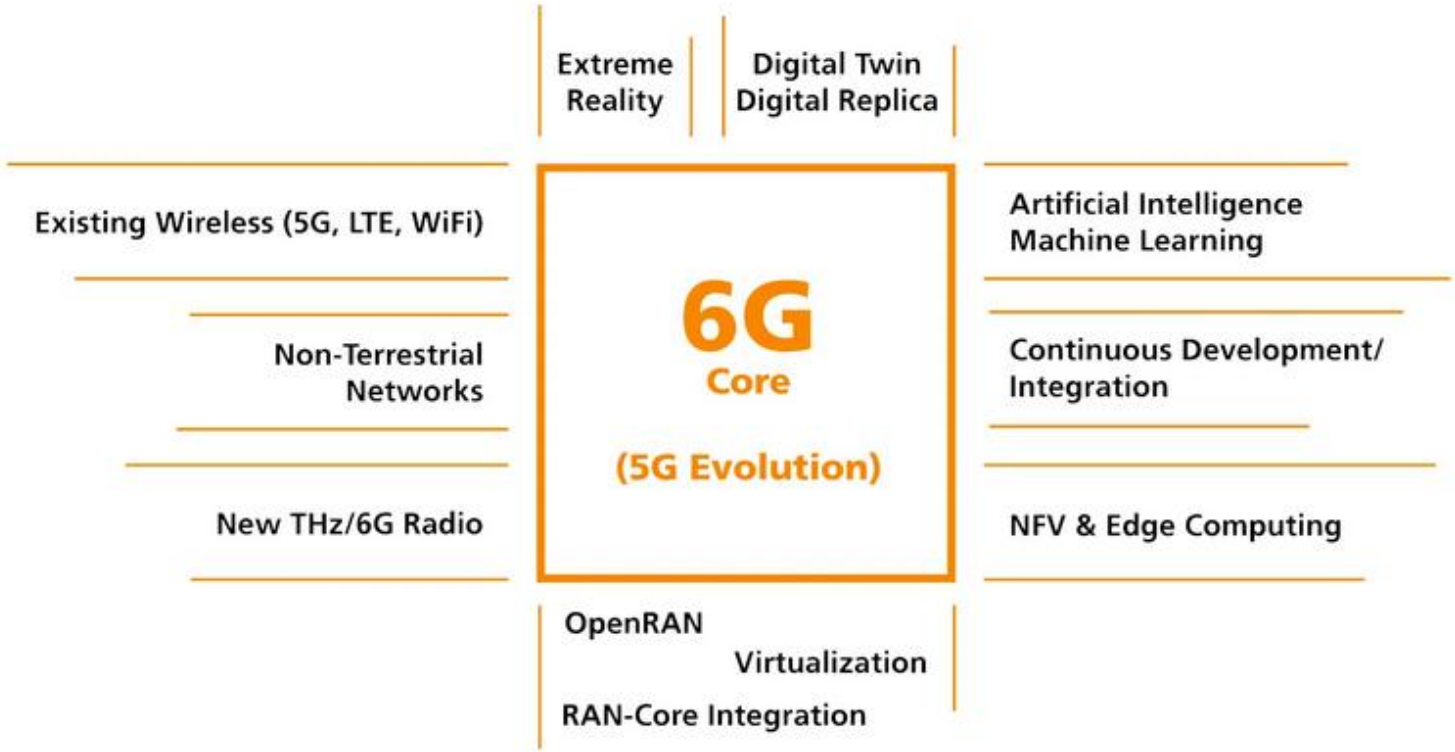
22 Οκτωβρίου 2026

Ασφάλεια και ιδιωτικότητα σε δίκτυα 6G με την ενσωμάτωση τεχνολογιών O-RAN για αυτοματοποιημένη διαχείριση

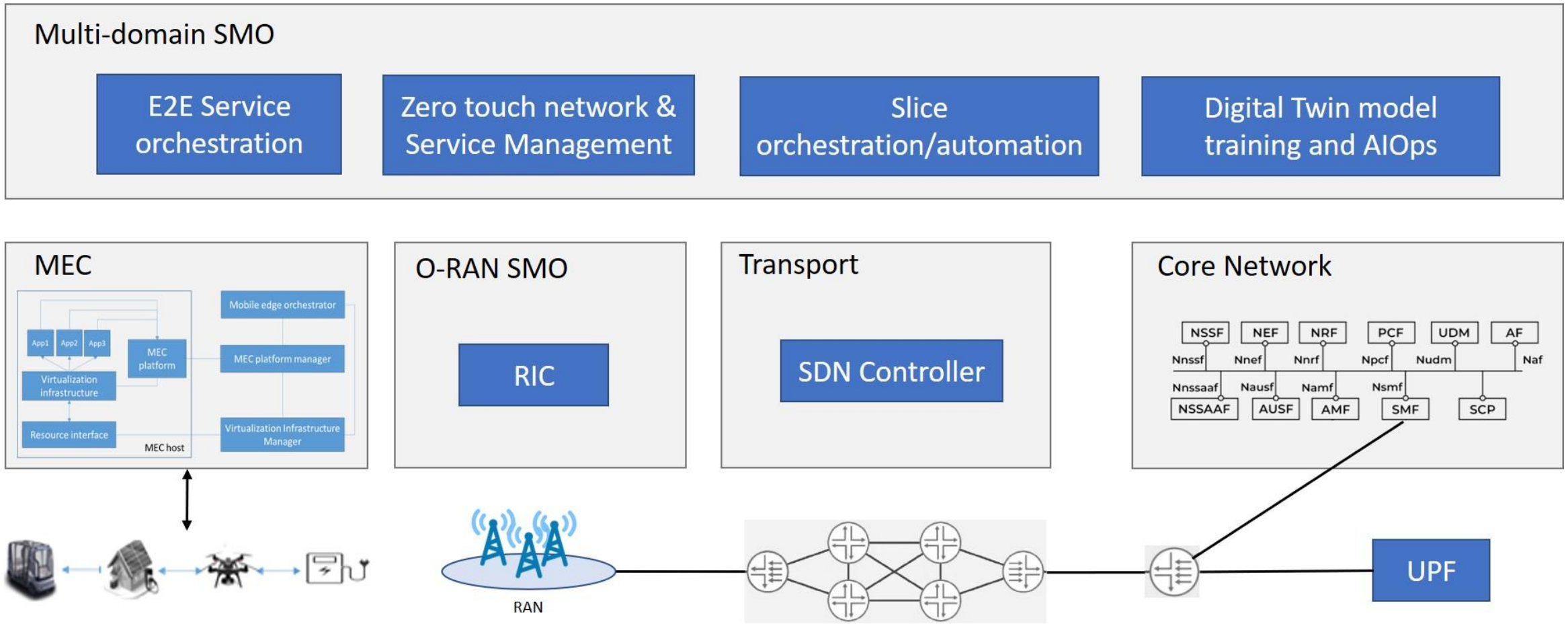
Αλέξιος Λεκίδης

Δίκτυα 6G και νέας γενιάς

- Διανεμημένη RAN υλοποίηση για πιο εκτεταμμένη υποστήριξη του δικτύου
- NG-RAN υποστήριξη απομόνωσης πόρων μεταξύ των τμημάτων δικτύου
- Αυτόνομη και αξιόπιστη λειτουργία για κρίσιμες υποδομές

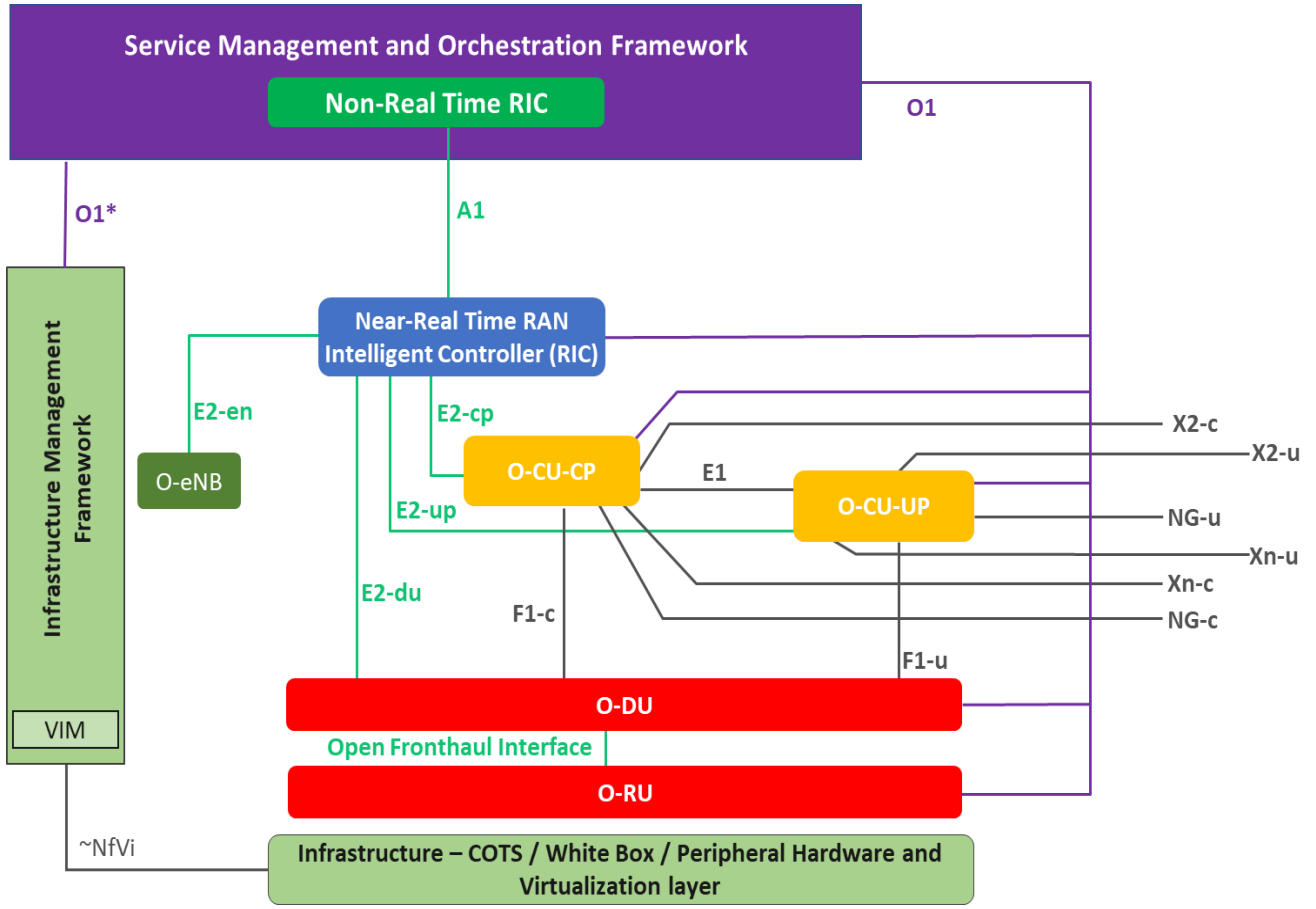


Δίκτυα 5G και νέας γενιάς

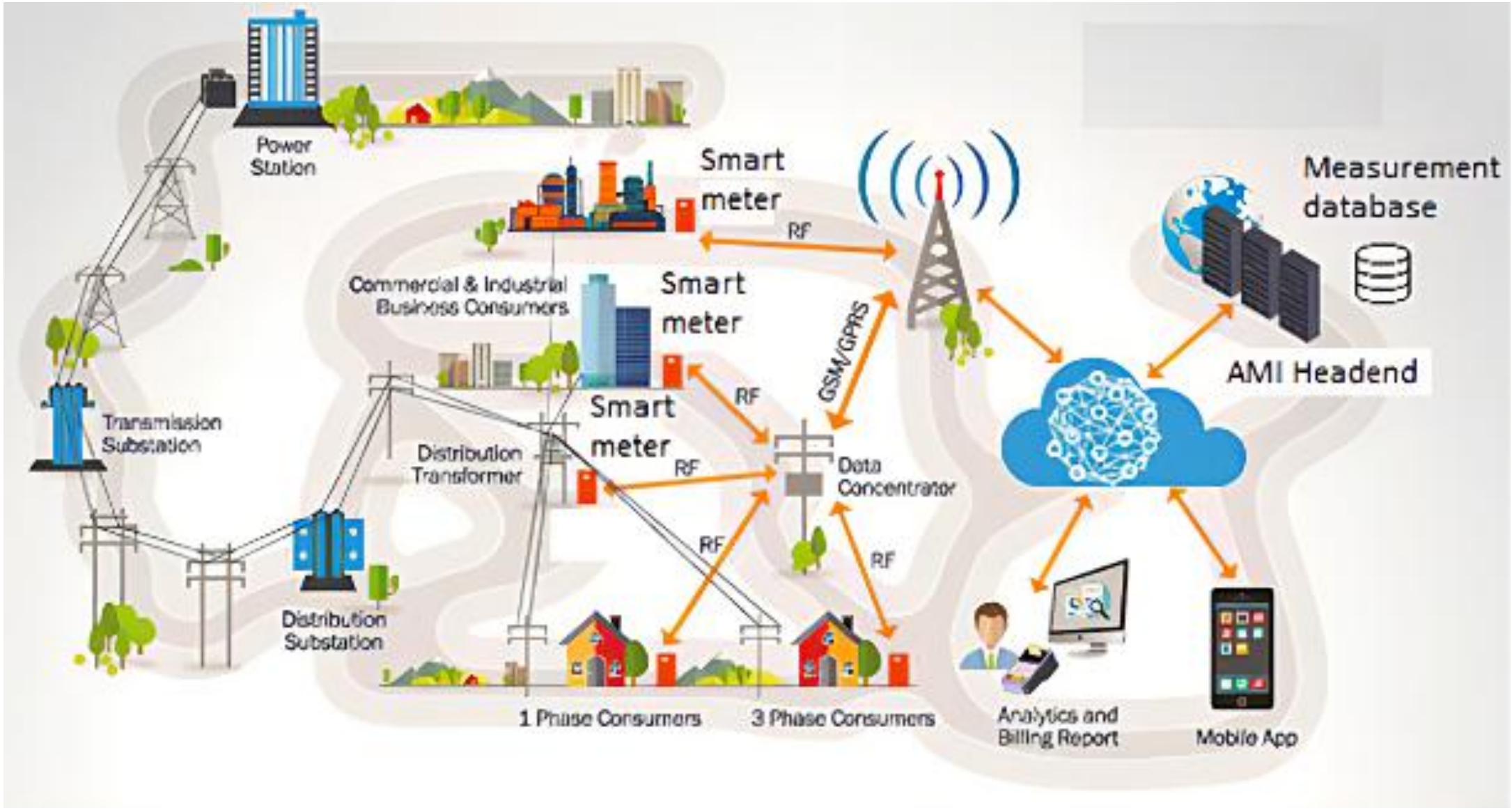


Αρχιτεκτονική O-RAN

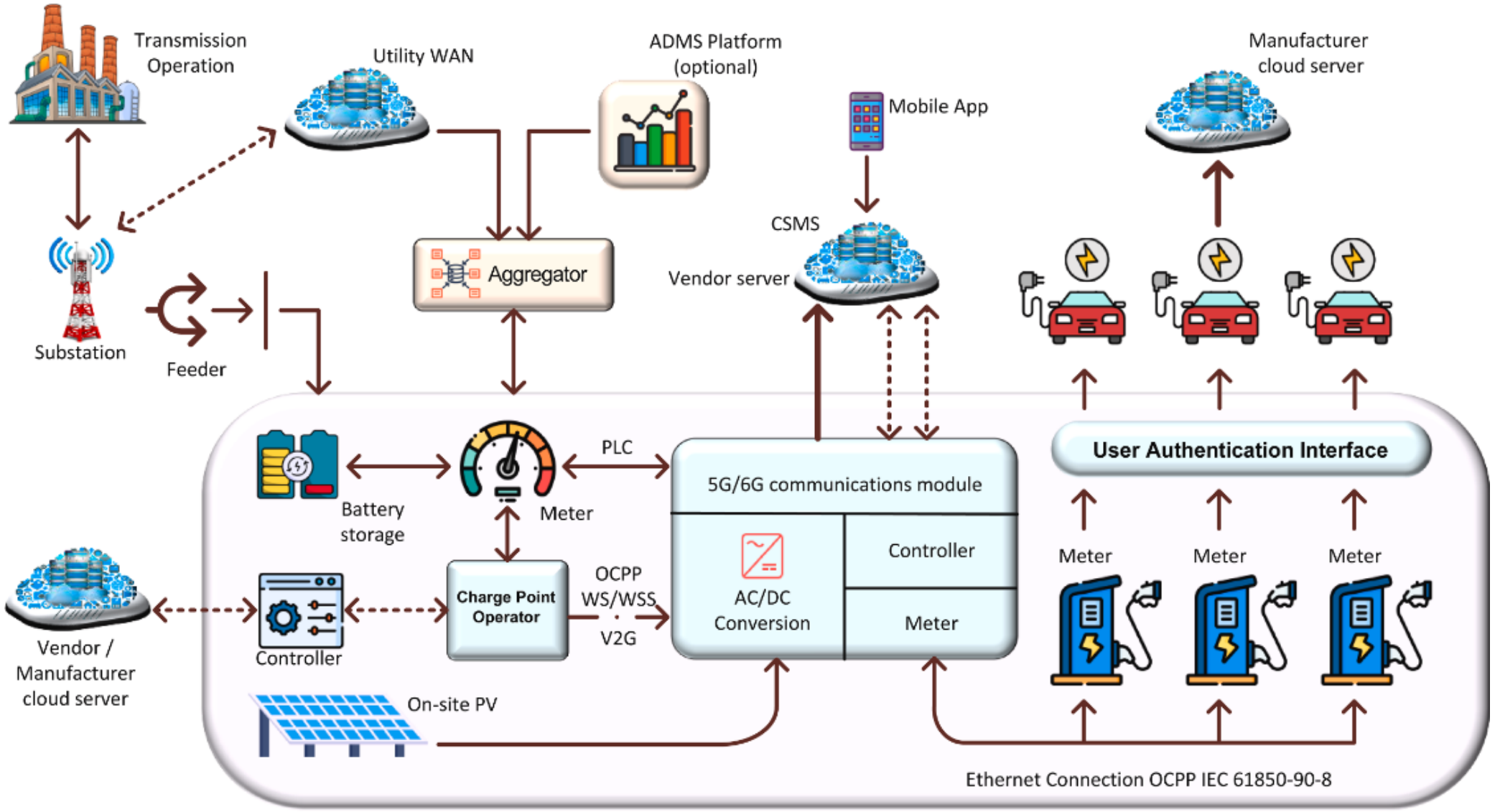
- Αρχιτεκτονική O-RAN:
  - O-RU / O-DU / O-CU: Διαχωρισμός του εξοπλισμού σε μονάδες Physical, Real-time και High-layer επεξεργασίας
- RAN Intelligent Controller (RIC):
  - Near-RT & Non-RT RIC: Βελτιστοποίηση πόρων μέσω xApps και rApps
- Δυναμικός προγραμματισμός πόρων (scheduling) και περιορισμός παρεμβολών
- Πλήρης συγχρονισμός εντολών ελέγχου και τηλεμετρίας μεταξύ 5G Core και O-RAN μέσω ανοιχτών API



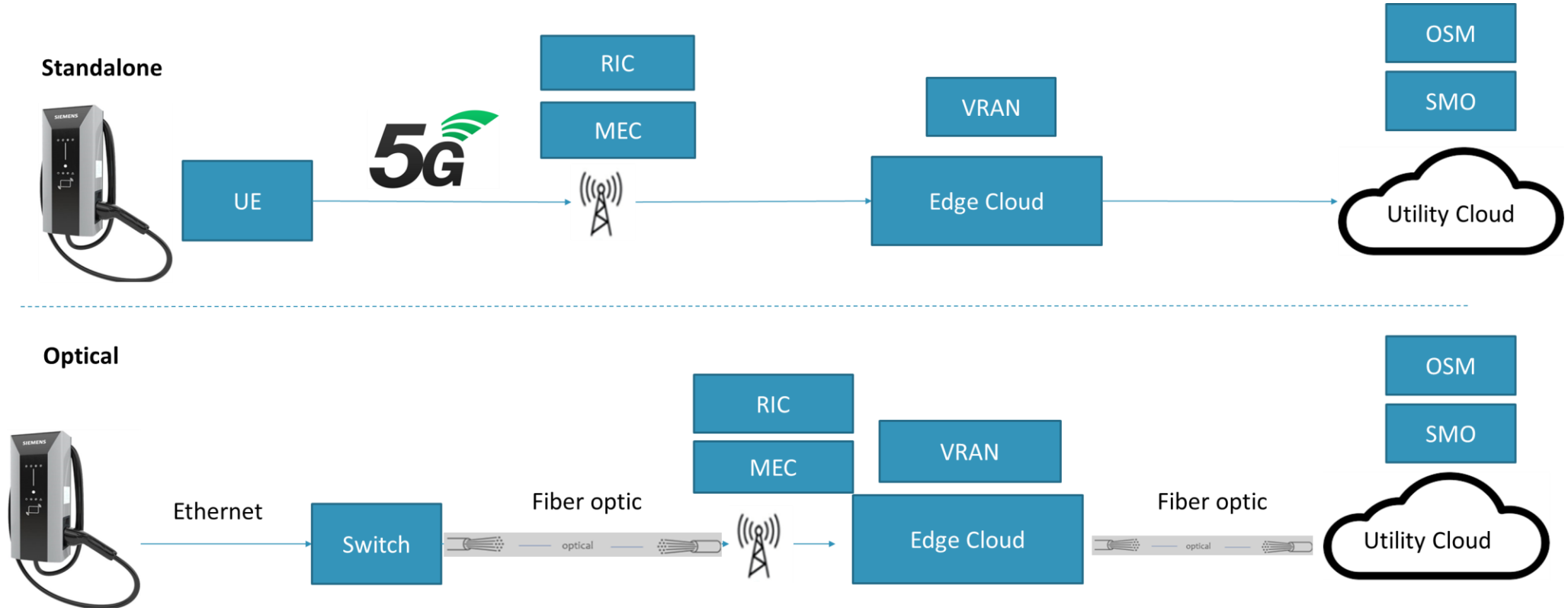
Δίκτυα έξυπνων μετρητών



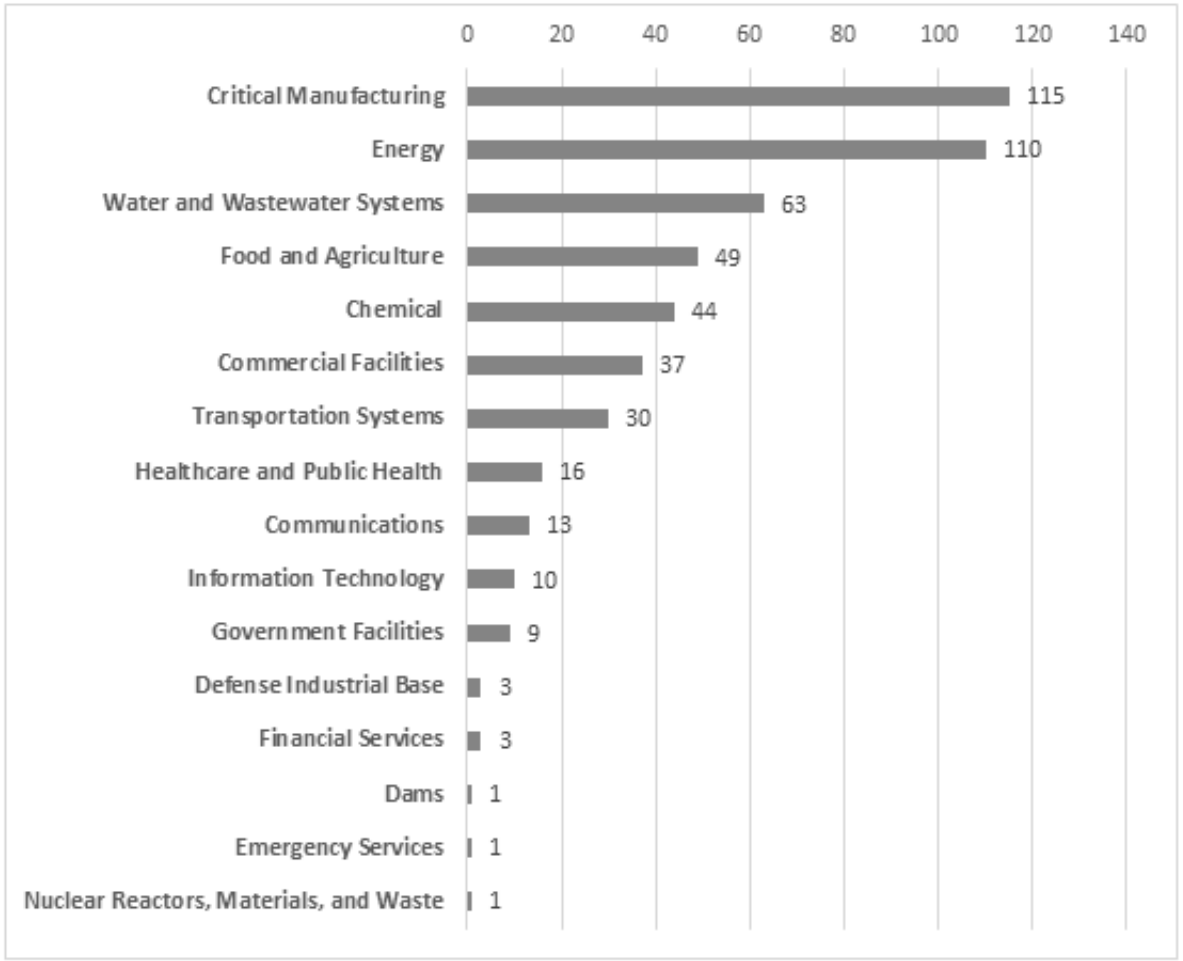
Δίκτυα Ηλεκτροκίνησης

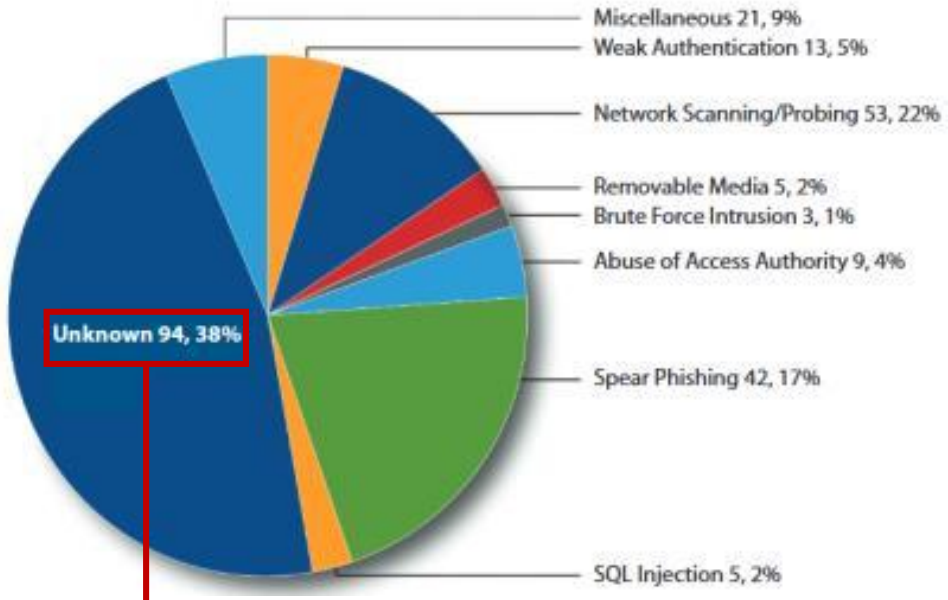


Σύνδεση 5G+/6G δικτύων με ενεργειακές εφαρμογές



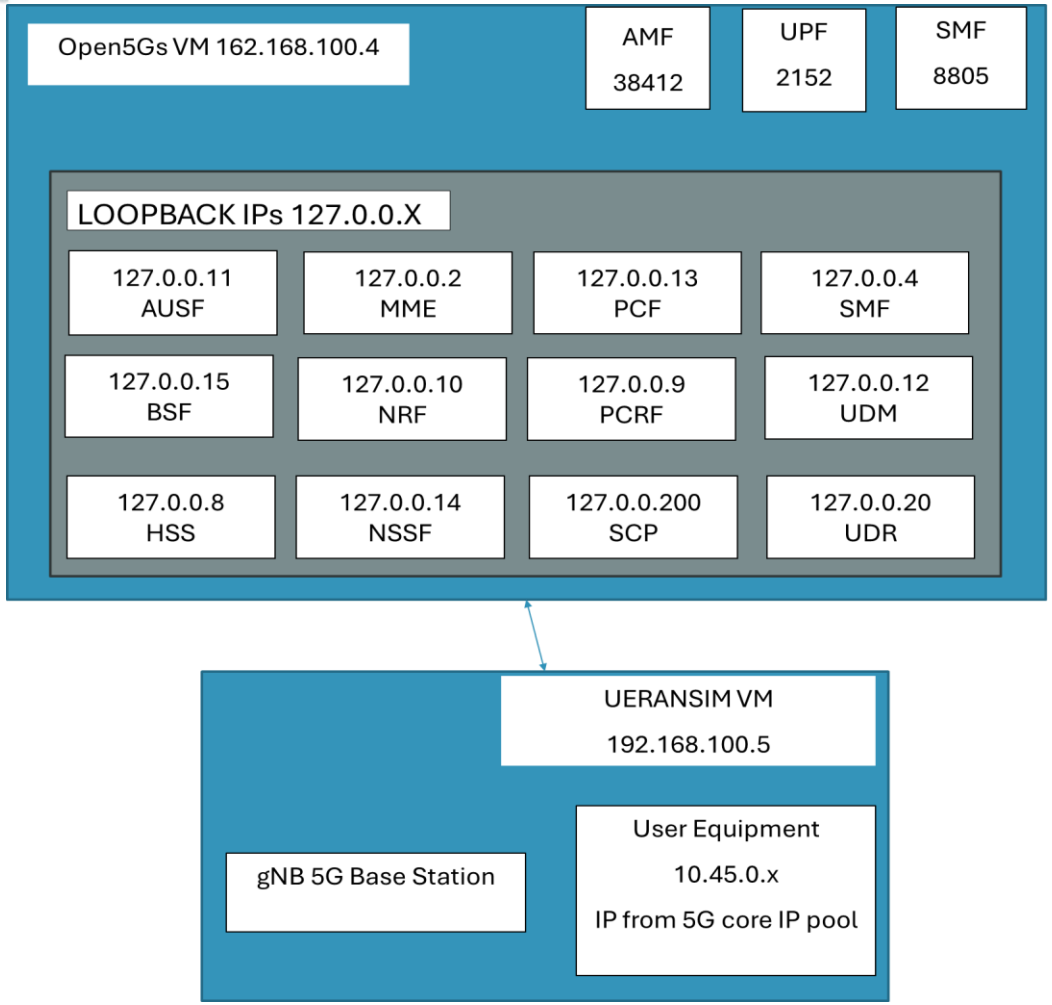
Πηγές κινδύνου και κυβερνοεπιθέσεων





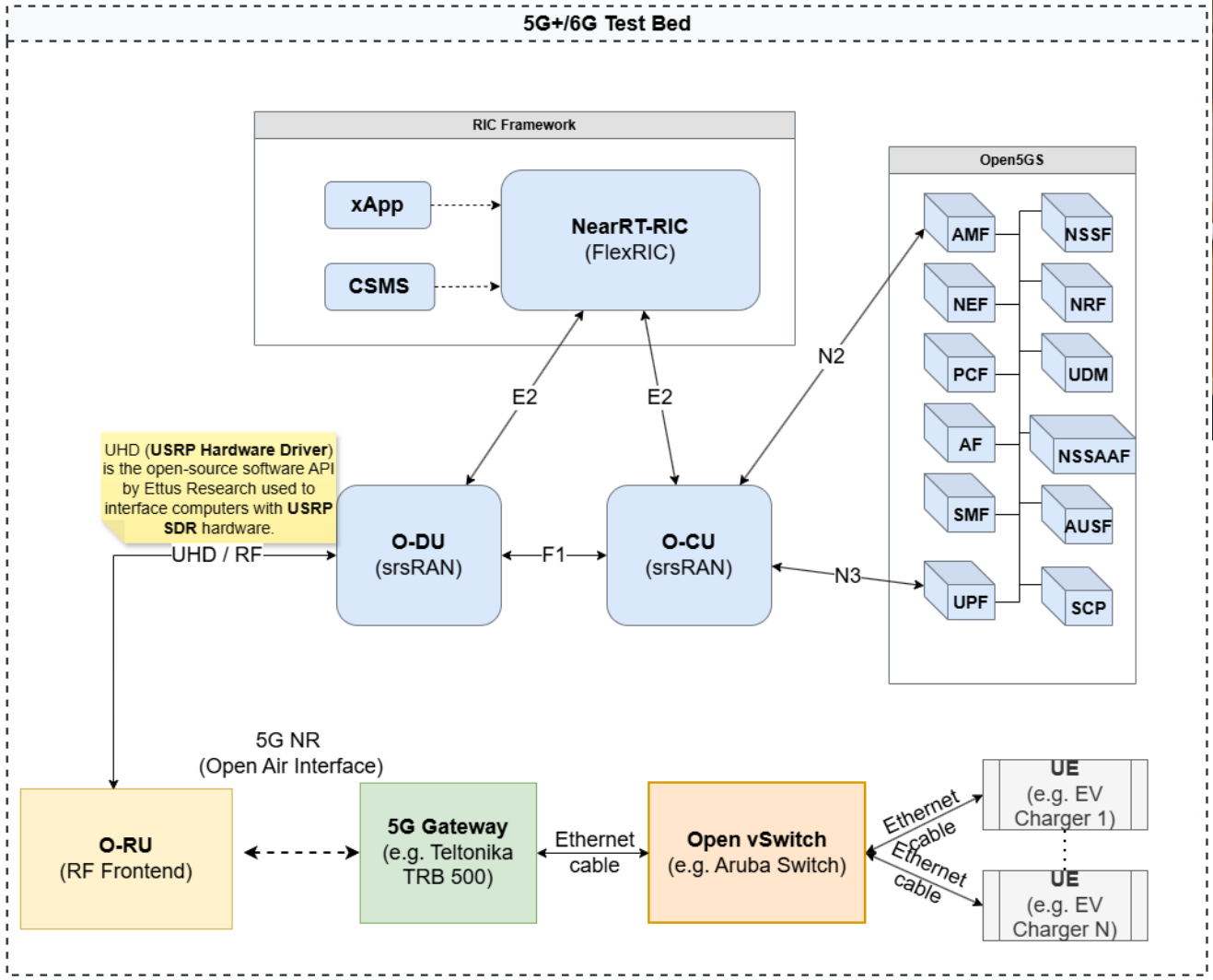
- Unauthorized exploitation of SCADA devices
- Exploitation of zero-day vulnerabilities in control system devices and software

Υλοποίηση 5G+/6G δικτύων



- Κύριες Λειτουργίες Ελέγχου (Control Plane):
  - AMF/SMF: Διαχείριση κινητικότητας, πρόσβασης και sessions.
  - NRF, PCF, UDM: Ανακάλυψη υπηρεσιών, έλεγχος πολιτικής και αυθεντικοποίηση χρηστών.
- User Plane Function (UPF): Προώθηση δεδομένων και κατεύθυνση κίνησης προς εξειδικευμένα network slices.
- Network Slicing: Πλήρης υποστήριξη end-to-end slice instantiation μέσω του NSMF.

Διασύνδεση 5G+/6G με ενεργειακά δίκτυα

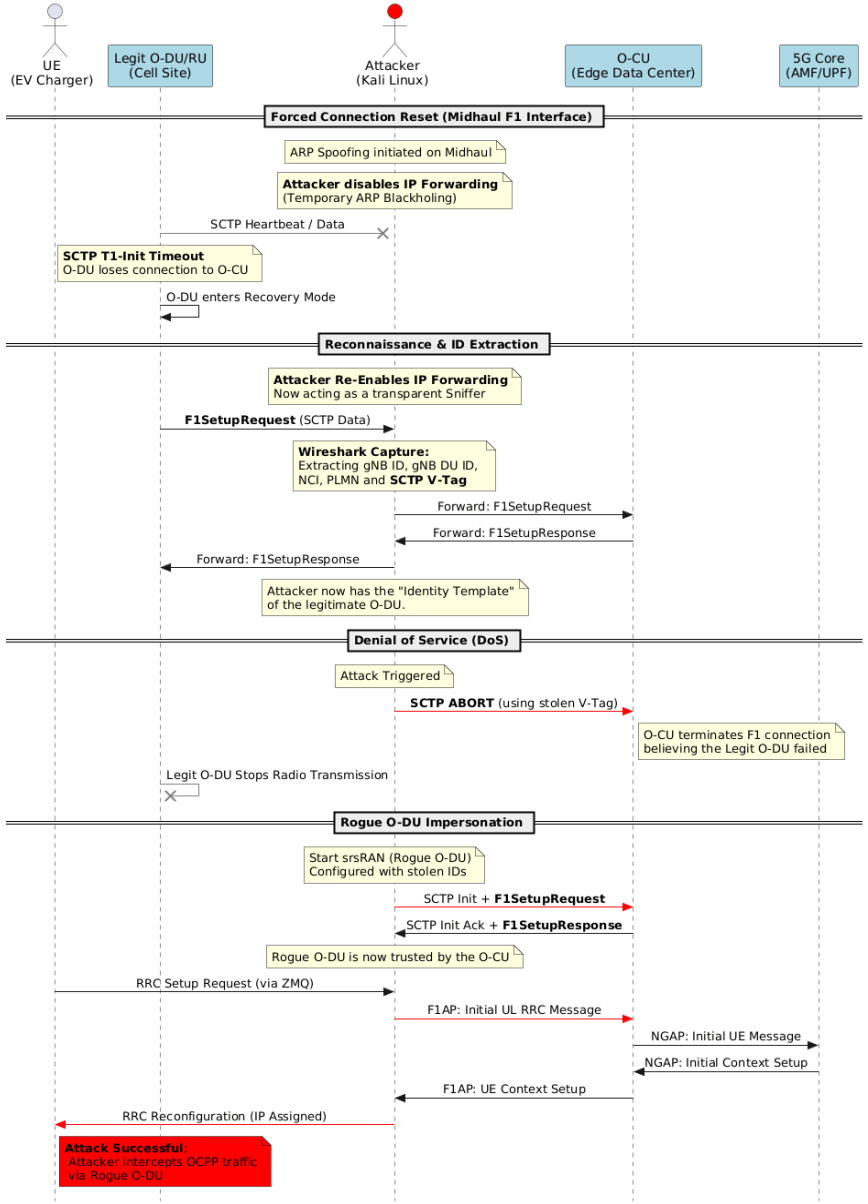






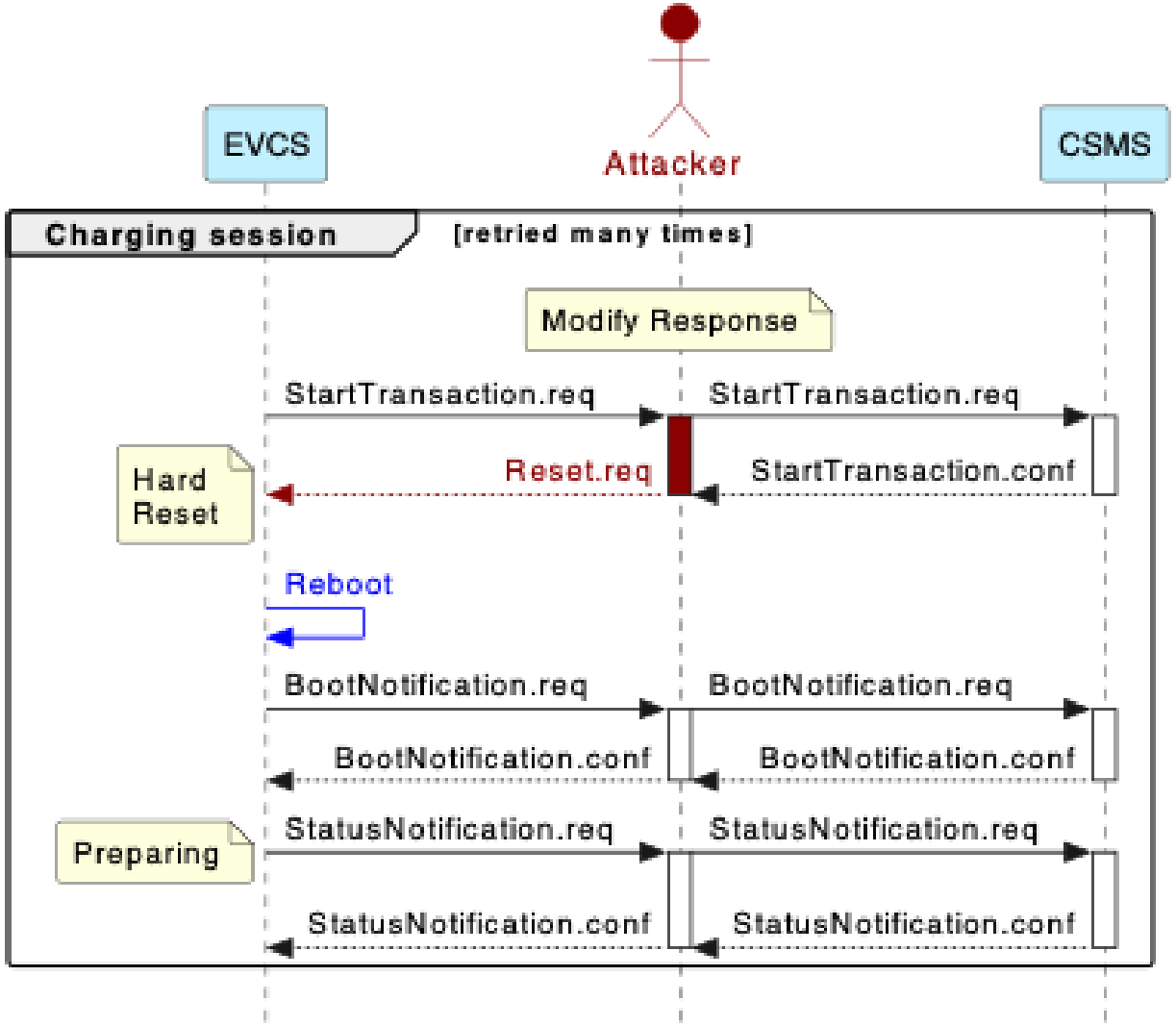
Κυβερνοεπίθεση σε 5G+/6G δίκτυα

- Δημιουργία ψευδούς σταθμού βάσης ώστε να στέλνονται σε εκείνον τα πακέτα επικοινωνίας του 5G και O-RAN δικτύου
  - Ο ψευδής σταθμός σετάρεται με όλες τις παραμέτρους του κανονικού σταθμού ώστε να μην μπορεί να ανιχνευθεί από παραδοσιακά εργαλεία παρακολούθησης δικτύου (Wireshark) ή εργαλεία τεχνητής νοημοσύνης για anomaly detection

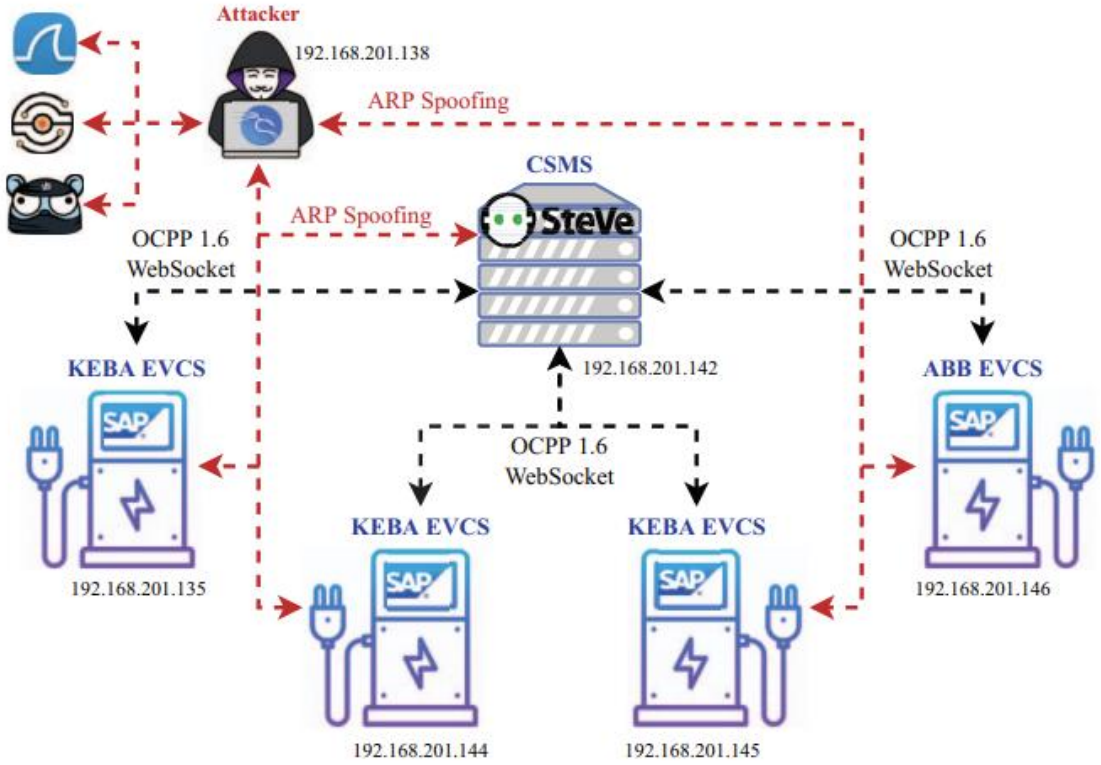


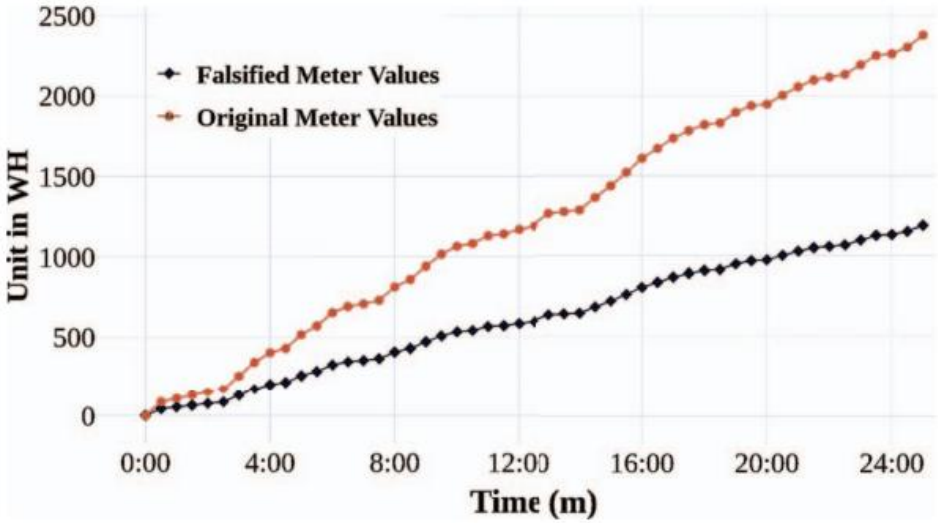
Πραγματοποίηση επιθέσεων σε δίκτυα φόρτισης

- Παραποίηση μηνυμάτων ελέγχου OCPP (StartTransaction, StopTransaction ή Reset)
- Πραγματοποιείται από θέση ενδιάμεσου (Man-in-the-Middle) στο επίπεδο 2 (Layer 2), συχνά μέσω πλαστογράφησης του ARP
- Οδηγεί τον σταθμό φόρτισης να επανεκκινηθεί και να στείλει ένα BootNotification ως απάντηση, με αποτέλεσμα να αποτυγχάνει η διαδικασία StartTransaction

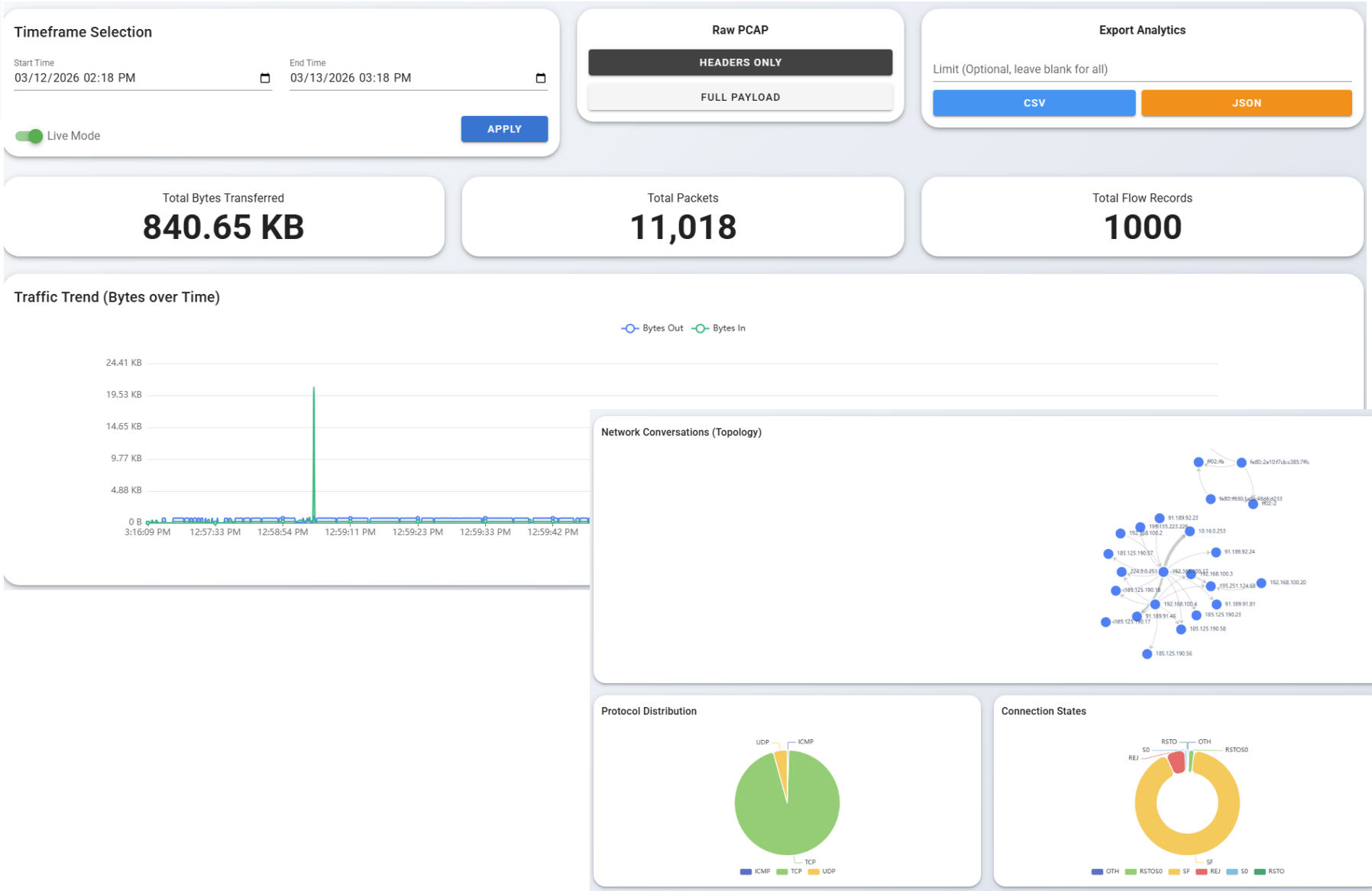


Αποτελέσματα επιθέσεων



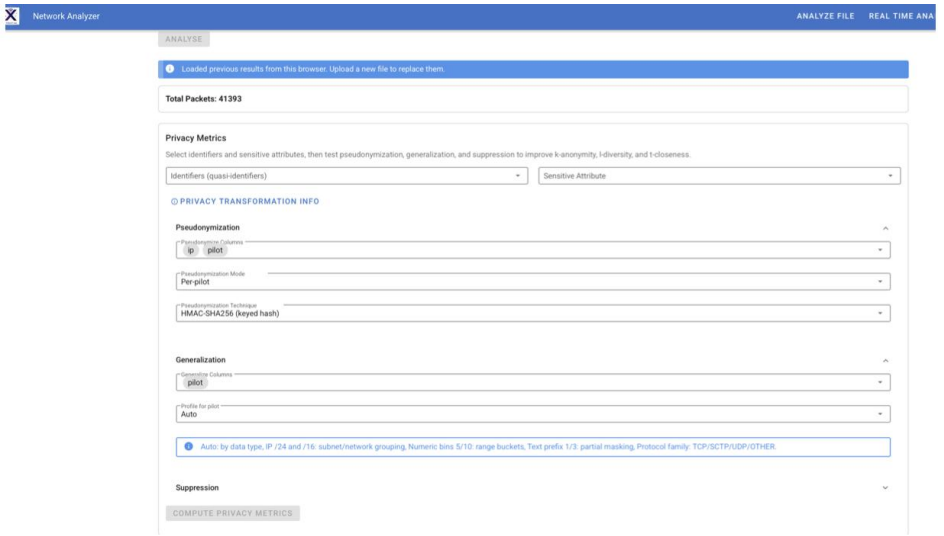


Ανίχνευση επιθέσεων



Μέτρηση ιδιωτικότητας

Session ID	Location	Time	Charger Type	Vehicle Model	Payment Type
1	Location A	09:00	DC	Tesla X	Card Number
2	Location A	09:00	DC	Nissan Leaf	Card Number
3	Location A	09:00	DC	BYD e6	Voucher
4	Location B	09:00	AC	Tesla Y	RFID
5	Location B	09:00	AC	Tesla Y	RFID
6	Location A	09:00	DC	Tesla X	Card Number
7	Location A	09:00	DC	Nissan Leaf	Card Number



Before Transformations

k-anonymity: 1
l-diversity: 1
t-closeness: 0.9831

After Transformations

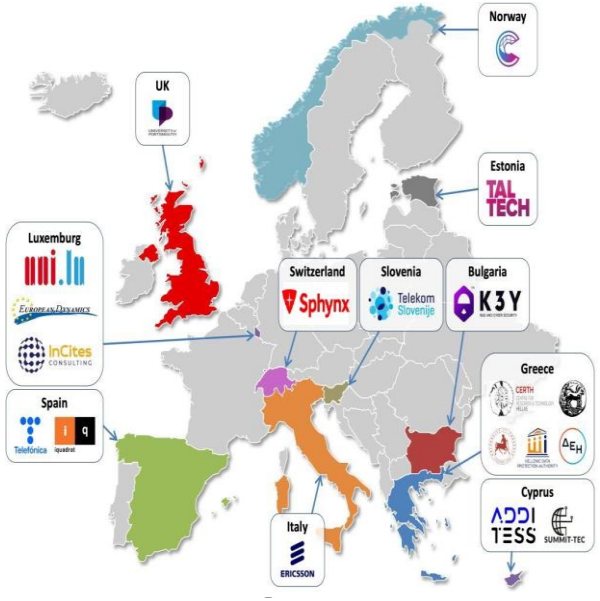
k-anonymity: 59
l-diversity: 9
t-closeness: 0

Transformed Records Preview

ip	role	protocol count	protocols	pilot
10.109.136.133	Unidentified	ps_*	*	PUC#1
10.109.136.133,10.244.0.92	Unidentified	ps_*	*	PUC#1
10.111.213.21	Unidentified	ps_*	*	PUC#1
10.244.0.1	E2_NODE	ps_*	*	PUC#1
10.244.0.68	Unidentified	ps_*	*	PUC#1
10.244.0.69	Unidentified	ps_*	*	PUC#1

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Ερευνητικό έργο XTRUST-6G



HORIZON-JU-SNS-2024-STREAM-B-01-04
"Reliable Services and Smart Security–Standardisation and Follow-up/PoCs"

Type:
HORIZON-RIA
HORIZON Research & Innovation Actions

19 Partners

10 Countries

36 Months

7,998,595 EU Contribution

Information Technologies Institute

European Dynamics | K3Y R&D and Cyber Security | Université du Luxembourg | ADDITESS | InCites Consulting | Hellenic Data Protection Authority | Sphynx | SUMMIT-TEC | ERICSSON | Telekom Slovenije | ΔΕΗ | TAL TECH | iquadrat | Telefónica



Αλέξιος Λεκίδης
Επίκουρος Καθηγητής
Πανεπιστήμιο Θεσσαλίας

alekidis@uth.gr