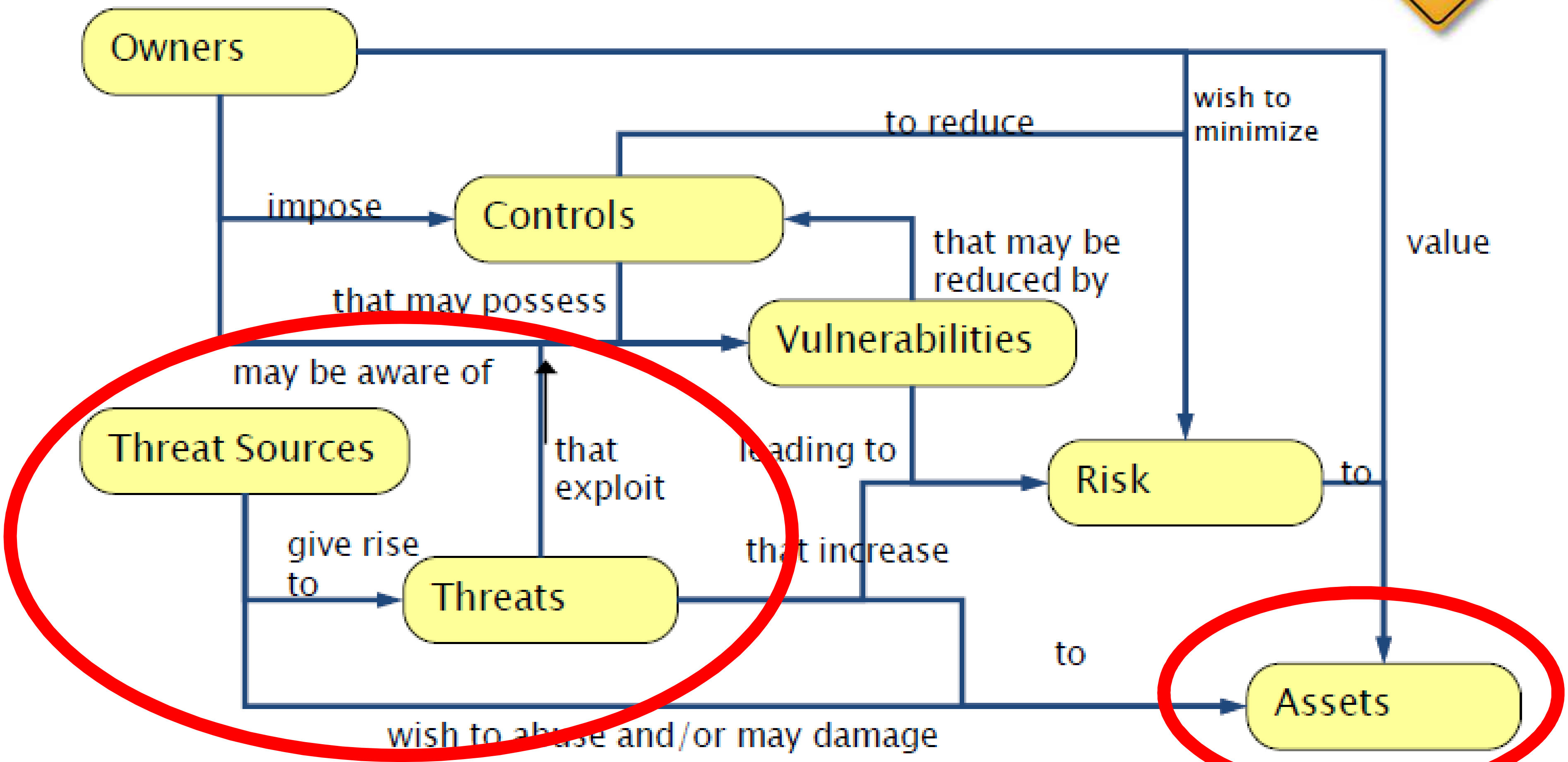
5G-ENSURE Risk Model: Threat Description, Assessment & Mitigation

Sophia Antipolis, 2017-6-16

Linas Maknavicius
NOKIA Bell Labs

Risk model & initial focus

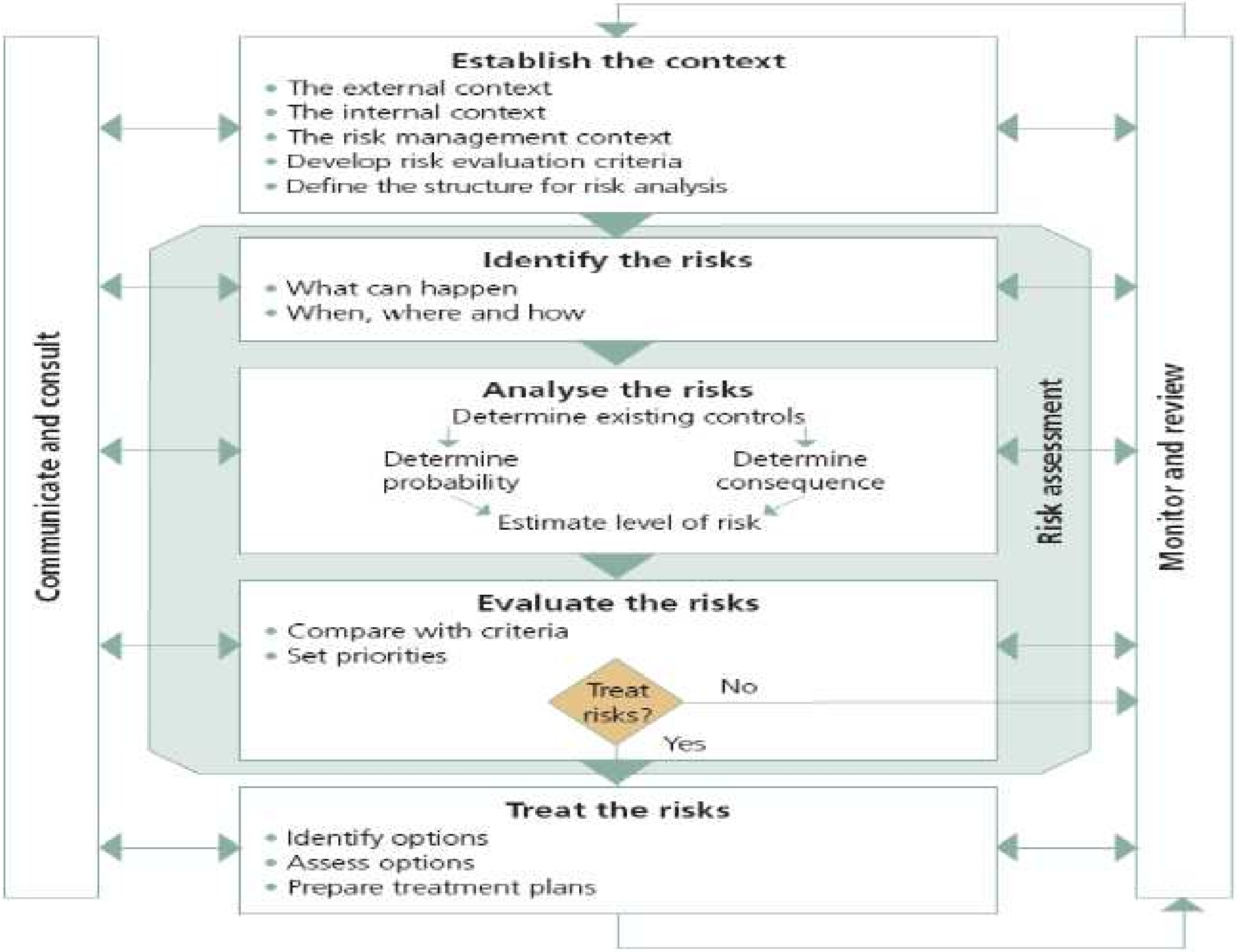


5G-ENSURE threat model

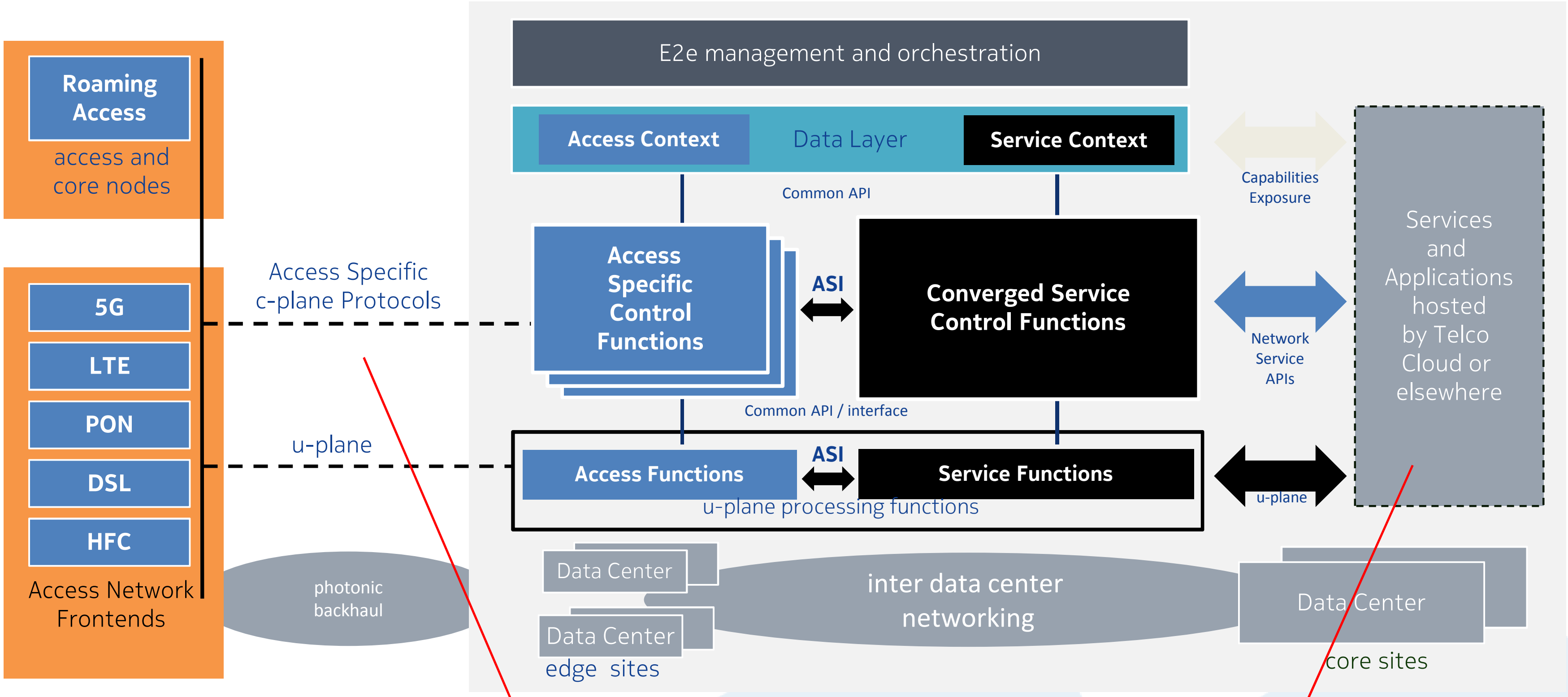
- derived from identified use cases
- 'external' threats (from NGMN, 3GPPP, 5G-NORMA, METIS archs)

5G asset description (extension of ENISA)

Risk Management Process (ISO 27005) & simplification of it: NIST SP-800-30



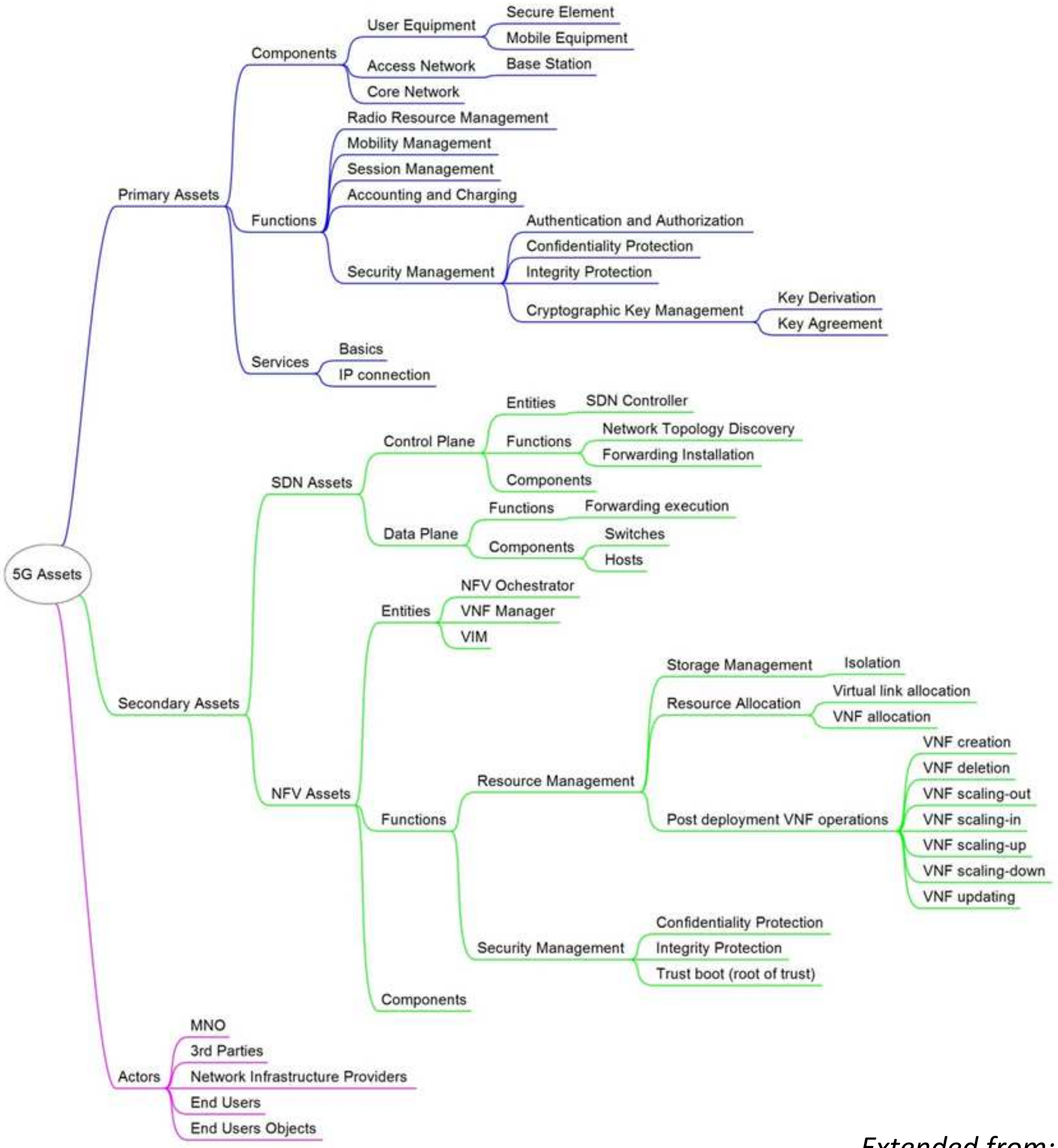
Holistic view on 5G ‘system of systems’ to derive ‘external’ threats: examples of prospective approach



E.g. Eavesdropping / man-in-the-middle type of threats

E.g. ‘Insider’ threats / Accidental misconfiguration

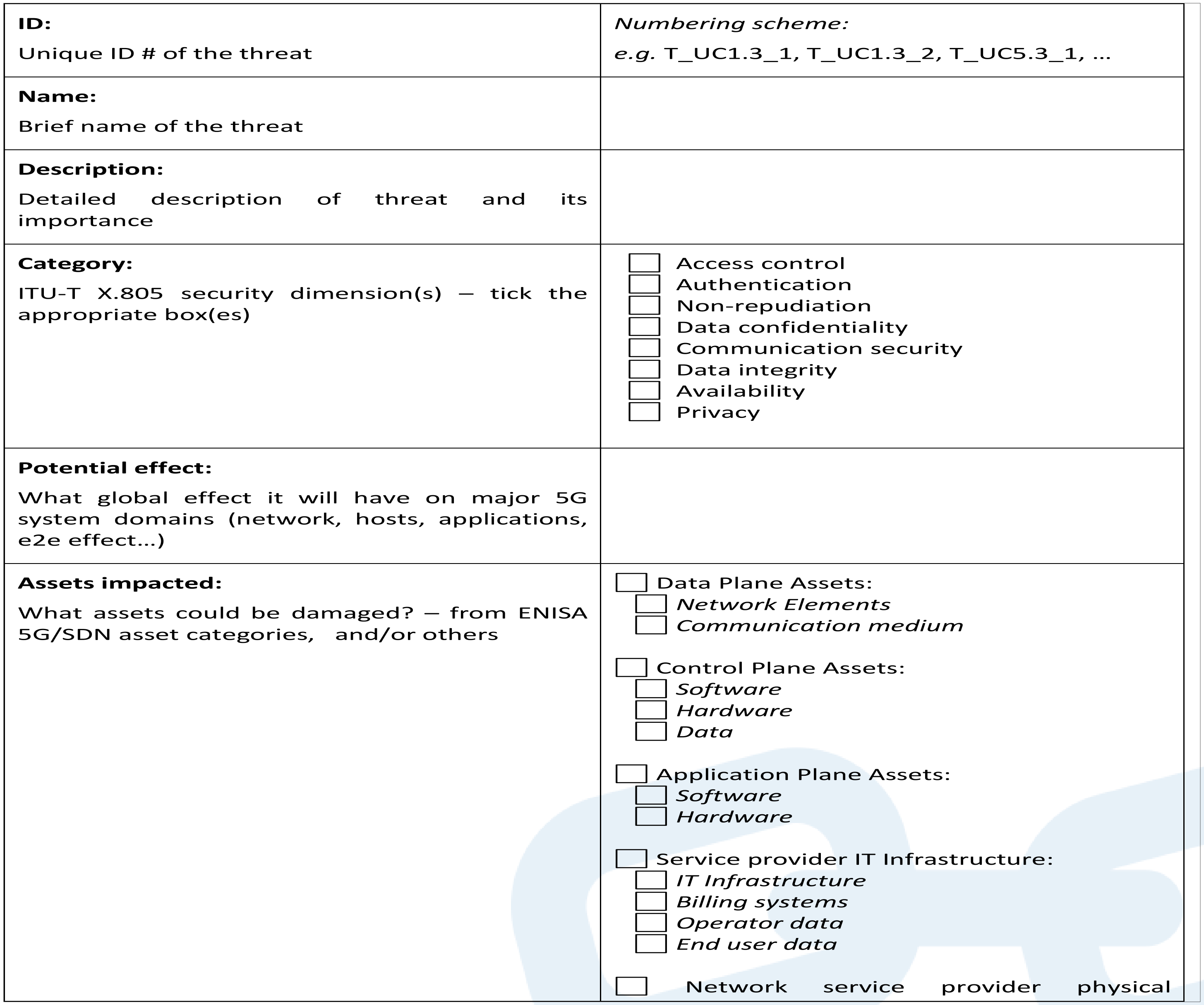
5G asset categories



- 5G Assets
  - Primary Assets
    - Components
      - User Equipment
        - Secure Element
        - Mobile Equipment
      - Access Network
        - Base Station
      - Core Network
    - Functions
      - Radio Resource Management
      - Mobility Management
      - Session Management
      - Accounting and Charging
      - Security Management
        - Authentication and Authorization
        - Confidentiality Protection
        - Integrity Protection
        - Cryptographic Key Management
          - Key Derivation
          - Key Agreement
    - Services
      - Basics
      - IP connection
  - Secondary Assets
    - SDN Assets
      - Control Plane
        - Entities
          - SDN Controller
        - Functions
          - Network Topology Discovery
          - Forwarding Installation
        - Components
      - Data Plane
        - Functions
          - Forwarding execution
        - Components
          - Switches
          - Hosts
    - NFV Assets
      - Entities
        - NFV Ochestrator
        - VNF Manager
        - VIM
      - Functions
        - Resource Management
          - Storage Management
            - Isolation
          - Resource Allocation
            - Virtual link allocation
            - VNF allocation
          - Post deployment VNF operations
            - VNF creation
            - VNF deletion
            - VNF scaling-out
            - VNF scaling-in
            - VNF scaling-up
            - VNF scaling-down
            - VNF updating
        - Security Management
          - Confidentiality Protection
          - Integrity Protection
          - Trust boot (root of trust)
      - Components
  - Actors
    - MNO
    - 3rd Parties
    - Network Infrastructure Providers
    - End Users
    - End Users Objects

Extended from: ENISA Threat Landscape for SDN/5G

5G-ENSURE threat description formalism (1/2)



ID: Unique ID # of the threat	*Numbering scheme:* *e.g.* T_UC1.3_1, T_UC1.3_2, T_UC5.3_1, …
Name: Brief name of the threat	
Description: Detailed description of threat and its importance	
Category: ITU-T X.805 security dimension(s) – tick the appropriate box(es)	□ Access control □ Authentication □ Non-repudiation □ Data confidentiality □ Communication security □ Data integrity □ Availability □ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	
Assets impacted: What assets could be damaged? – from ENISA 5G/SDN asset categories, and/or others	□ Data Plane Assets: □ *Network Elements* □ *Communication medium* □ Control Plane Assets: □ *Software* □ *Hardware* □ *Data* □ Application Plane Assets: □ *Software* □ *Hardware* □ Service provider IT Infrastructure: □ *IT Infrastructure* □ *Billing systems* □ *Operator data* □ *End user data* □ Network service provider physical

5G-ENSURE threat description formalism (2/2)

Assets impacted: What assets could be damaged? – from ENISA 5G/SDN asset categories, and/or others	□ Data Plane Assets: □ *Network Elements* □ *Communication medium* □ Control Plane Assets: □ *Software* □ *Hardware* □ *Data* □ Application Plane Assets: □ *Software* □ *Hardware* □ Service provider IT Infrastructure: □ *IT Infrastructure* □ *Billing systems* □ *Operator data* □ *End user data* □ Network service provider physical infrastructure: □ *Facilities* □ *Energy Power* □ SDN users: □ *End user data* □ *SLAs and regulations* □ Human agents: □ *SDN Administrators* □ *SDN Application Developers* □ *Network Service Operators* □ *End User Application Developers* □ *End User Application Administrators* □ *End User Service Providers* □ *End Users* □ Others (please specify): □ □
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	

Example threat analysis from 5G-ENSURE Use Case

General Principles: 'Sunny Day' vs 'Rainy Day'

- Describe the **'Sunny day' scenario**, i.e. what should happen if the threat does not arise
- Focus on locating the scenario **w.r.t. the 5G ENSURE architecture**
  - which processes or resources in which 5G domain?
  - used and managed by which stakeholders?
- Then **describe the threat ('Rainy day') with respect to the involved assets, processes and stakeholders**
  - what specifically goes wrong, not 'if someone could access this data or that service' but how

Example Analysis:

Device/ Subscriber Identity Privacy (UC 2.1/2.2)

These use cases cover the related issues of protecting device / subscriber identifiers from an attacker who wishes to track users

- 2 Threats described in deliverables D2.3 + D2.5 (available at http://www.5gensure.eu):
  - **T_UC2.1_1** Mobile user (e.g., IMSI/GUTI) interception and information interception
  - **T_UC2.1_2** Tracking of device/user location

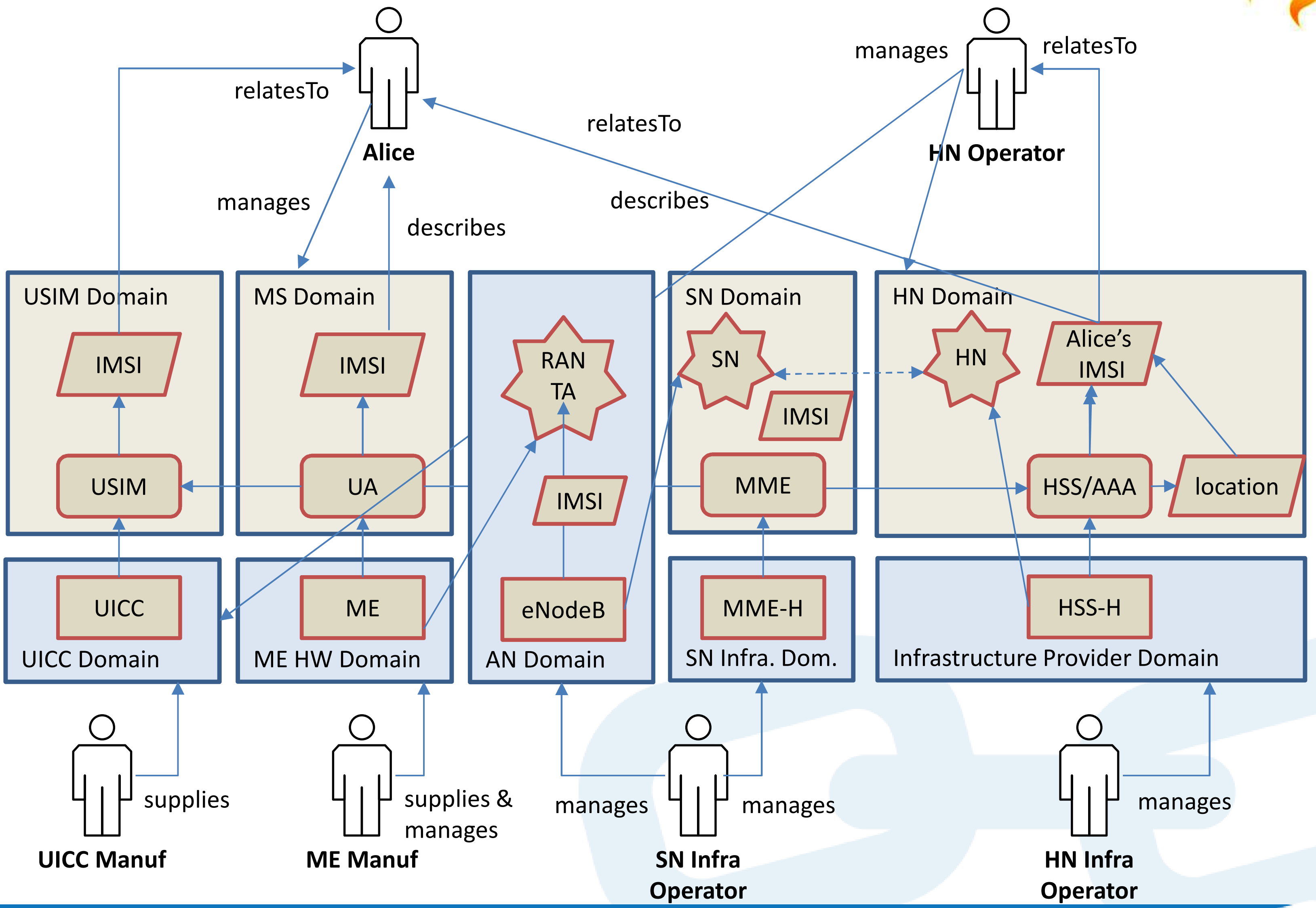
Example Analysis:

mobile user interception, location tracking

- **“Rainy day”**: Alice’s UE is switched on, **Mallory** (malicious user) **sets up a fake Base Station** (for passive/active listening of transmissions of legitimate eNodeB).
- **Basic flow of events:**
  - Alice’s UE connects to the 5G network, identified by her IMSI/GUTI
  - Mallory observes IMSI, and can track Alice’s UE
  - Mallory tracks Alice’s current location by triggering the mobile network into initiating the generation of paging messages to Alice’s UE (e.g. by using social media application to initiate unobtrusive communications, or monitoring radio spectrum from emergency calls)
  - Mallory observes the paging messages sent and can potentially correlate the contained GUTI with Alice’s social network identity

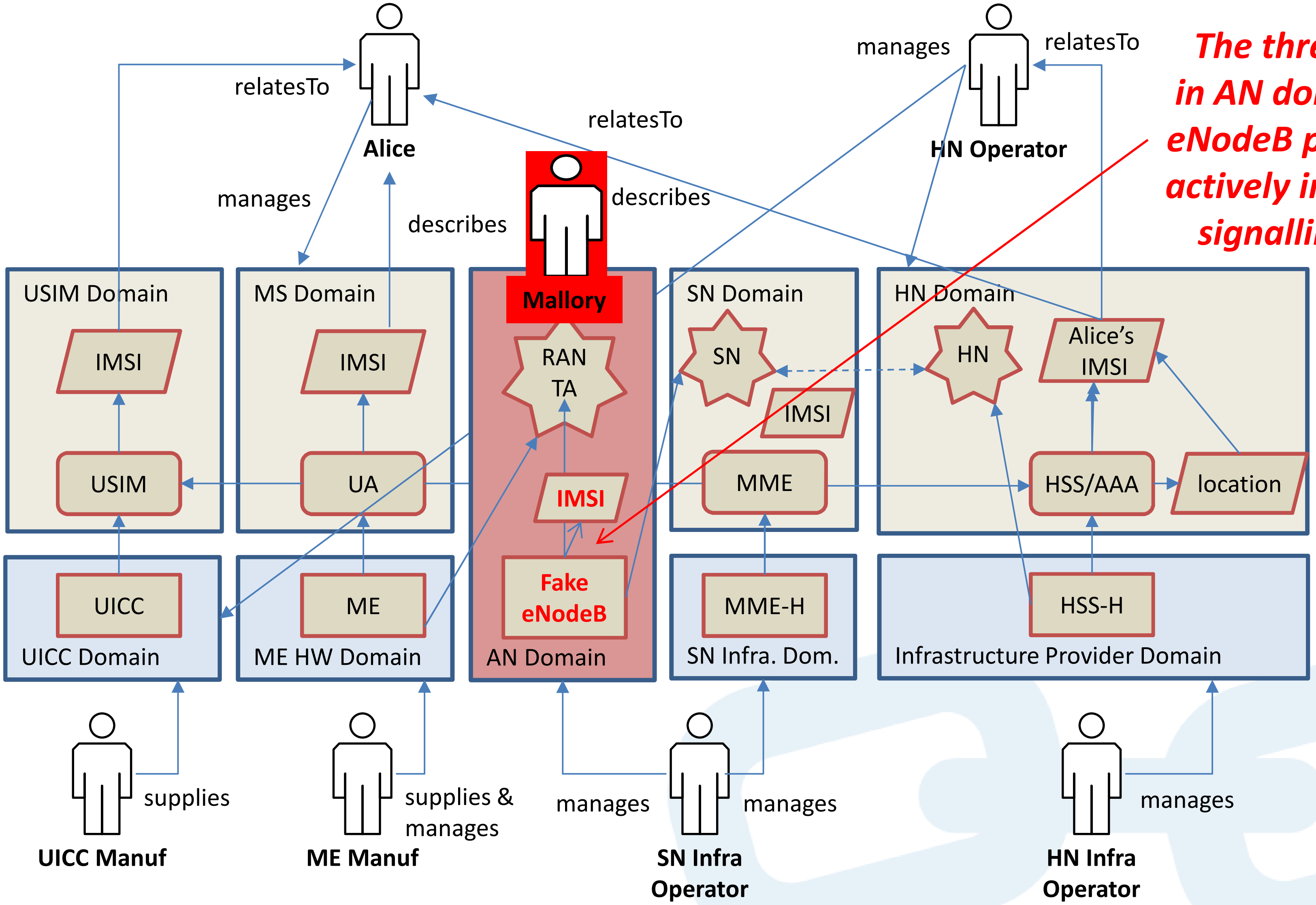
Example Analysis:

mobile user interception, location tracking



Example Analysis:

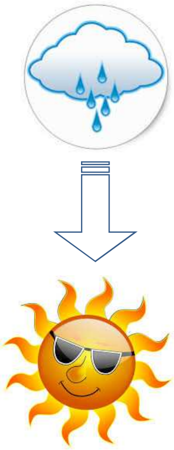
mobile user interception, location tracking



The threats arise in AN domain: fake eNodeB passively or actively intercepting signalling traffic

Example Analysis:

mobile user interception, location tracking



- **Threat mitigation strategies:**
  - **Mobile user interception and information interception**
    - Mitigation of this threat may be achieved through **protection of the device identifier during transport**. Such an approach might protect the transfer of the IMEI between the UE and AN using **transport layer encryption**. Another approach might be to **use a mobile Operator supplied key to just encrypt the IMEI** in transit. These solutions should ensure that the user's IMEI is not sent in clear text during network attachment. Whilst these approaches would make passive interception significantly harder, these solutions may not prevent the UE from attaching to a rogue eNodeB, but they would raise the bar in making it more difficult for an attacker to obtain the IMEI.
  - **Tracking of device's (user's) location**
    - The threats may be mitigated in this case through the deployment of **privacy enhanced functionality into the UE**. One approach to limit tracking is to provide for **randomisation of the device's MAC addresses**. Whilst a number of mobile Operating Systems do now provide for randomisation of the device's MAC addresses these are typically limited in their privacy protection as the randomisation only occurs in a limited set of protocol interactions.

Key take-aways

Industry Challenge

- Future 5G complexity raising **security challenges**:
  - 5G mobile VNFs protection, bigger attack surface, subscriber data protection, multi-tenancy, slicing…
  - Existing & new risks introduced by virtualization and wireless network topology (HetNets, multi-hop, D2D…)
  - Co-existence of new services (V2x, IoT, verticals, mission-critical): need for isolation & overall optimization

Game changing aspect

- Given the complexity of 5G architecture/deployment scenarios, distributed e2e security/risk model will be devised:
  - Comprising software-controlled **multiple stakeholder networks**
  - Multi-party trust model
  - **Secured sub-systems ≠ entire system is secure**
  - 5G system security needs to be built in from the start
  - Pave the road for **5G Security Reference Architecture**

5G Enablers for network and system security and resilience

🌐 5G-ENSURE: http://www.5gensure.eu

✉ contact@5gensure.eu

@5GEnsure

European Commission

5G ENSURE receives funding from the EU Framework Programme for Research and Innovation H2020 under grant agreement No 671562 | Duration November 2015 – October 2017

5G PPP

The 5G Infrastructure Public Private Partnership (SG PPP)