Network Architectural Issues in Emergency Networks

Maurizio Casoni

Department of Information Engineering
University of Modena and Reggio Emilia
Italy

Outline

- **Large Scale IP E-SPONDER: A holistic approach towards the development of the first responder of the future**
- **Introduction: Emergency Networks**
- **General Architecture for Emergency Networks**
- **Enabling Communication Technologies**
- **Network Architectures: possible options**
- **Focus on Open Platform for the Mobile Emergency Operation Centre**
- **Conclusions**

THEME

- **Objective:**

  SEC-2009.4.2.1: First Responder of the future

- **Duration of the project:**

  48 months (starting July 1st 2010)

- **Budget:**

  The total requested grant is € 8,790,044.00 while the overall foreseen budget of the ESPONDER project is €12,922,363.40

ESPONDER: list of participants

1. EXODUS S.A. (coordinator) (Greece)
2. University of Modena and Reggio Emilia (Italy)
3. CrisisPlan BV (NL)
4. PROSYST Software GmbH (D)
5. Immersion S.A. (F)
6. Rose Vision (SP)
7. Telcordia Poland Sp. z o.o. (POL)
8. Centre Suisse d'Electronique et de Microtechnique SA (CH)
9. SMARTEX (I)
10. Technische Univesität Dresden (D)
11. YellowMap (D)
12. PANOU S.A. (GR)
13. Telcordia Taiwan (TAIW)
14. Institute for Information Industry (TAIW)
15. Centre d'Essais et deRecherche de l'Entente (F)

Abstract

- The *ESPONDER* is a suite of real-time data-centric technologies which will provide actionable information and communication support to first responders that act during abnormal events (crises) occurring in critical infrastructures.
- This information will enable improved control and management, resulting in real time synchronization between forces on the ground (police, rescue, firefighters) and out-of-theater command and control centers (C&C).

- *The key concept behind all envisaged work of the ESPONDER project is the facilitation of effective first responder work through the employment of advanced and revolutionary ICT systems, applications, services and concepts*

Outline

- Large Scale IP E-SPONDER: A holistic approach towards the development of the first responder of the future
- **Introduction: Emergency Networks**
- General Architecture for Emergency Networks
- Enabling Communication Technologies
- Network Architectures: possible options
- Focus on Open Platform for the Mobile Emergency Operation Centre
- Conclusions

Introduction

- Natural disasters, CBRN (Chemical, Biological, Radiological, Nuclear) and terrorist attacks using explosives can cause massive destruction, high mortality and many casualties not only in urban areas but also in critical infrastructures, usually, without warning; this is particularly true for earthquakes.
- Earthquakes involve more than 30% of the total fatalities from natural disasters the last 20 years. On average, about 7 lethal earthquakes were occurring each year in the 20th century.
- Terrorist attacks especially in high-rise buildings (e.g. telecom hotels, airports) can be responsible for a large number of entrapped people. The 9/11 event was such a case.
- Entrapment is also the result of collapsed structures due to accidental or deliberate explosions (e.g. collapsed mines, technical failures, confined spaces).
- Disaster impacts are high in Critical Infrastructures for a number of reasons; CIs are positioned over large regions, are overpopulated, have very tall and extended building blocks with complicated street patterns

Emergency Networks: past experience

Lack of interoperability among systems of different organizations:

- Lack of specific standards;
- Proprietary solutions often not compatible;
- E.g.: World Trade Center, 9/11/01

Lack or limited data service and applications:

- Compared to recent wideband wireless networks;
- E.g.: important data such as maps, building plants, videostreaming systems

Excessive trust in fixed infrastructures:

- Communications towards hit by destructive events;
- E.g.: Katrina, New Orleans, 2005

Public Safety System Architecture

Incident Area Network

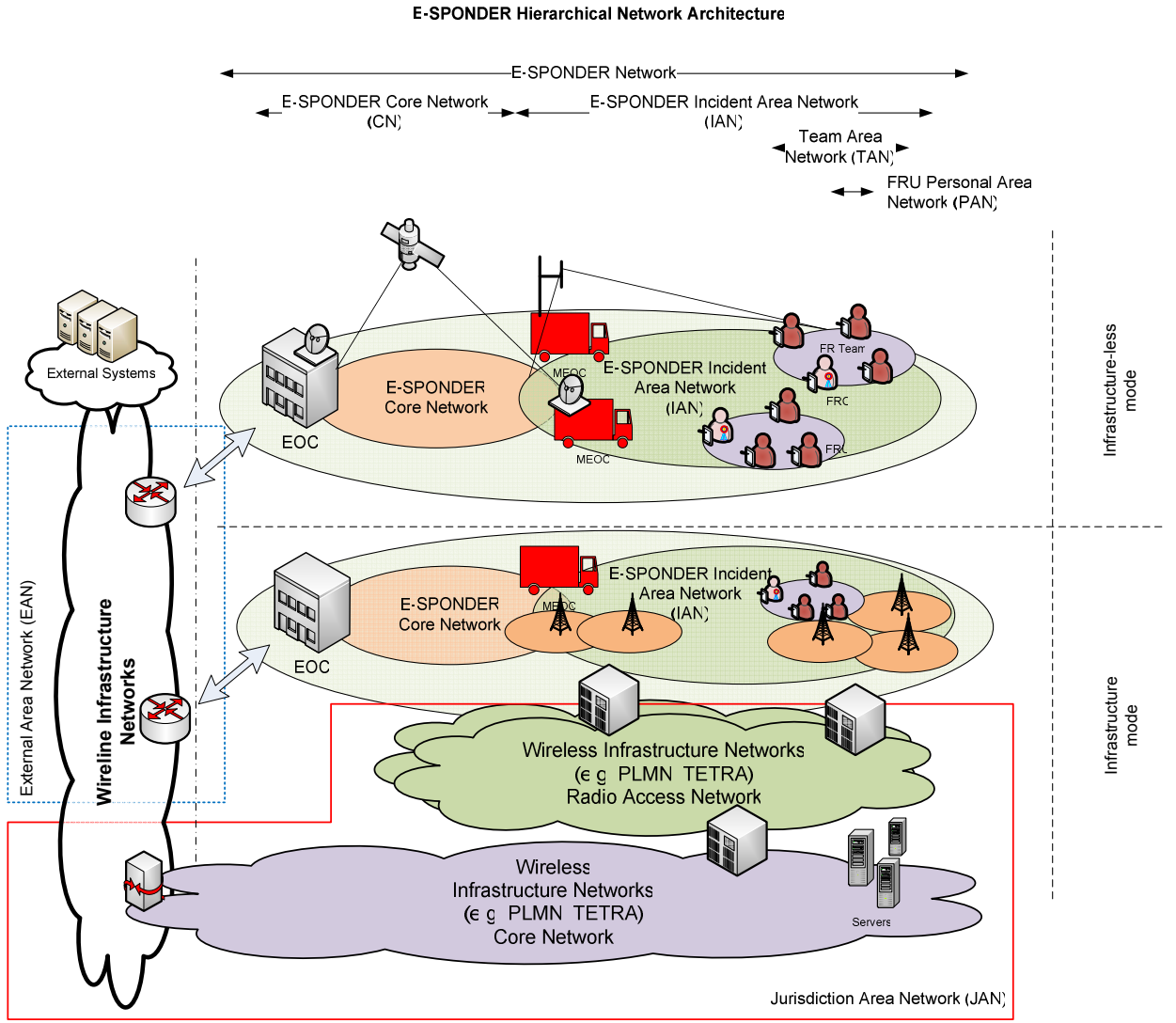
- Temporary network;
- Set up by MEOC;
- Data between users and MEOC;

Jurisdiction Area Network

- Main Emergency net;
- Fixed infrastructures;
- IAN traffic managmnt;

Extended Area Network

- Nation wide optical fibre network
- Backbone for First responders, IAN, JAN



Emergency Networks: basics (1/2)

- **Communication is a vital part of the First Responders' (FRs) operation, to connect them with the on-site (mobile) and remote (fixed) operations centres.**

- **Communications interoperability: major concern in emergency networks as there is the need to follow the "always-connected" approach.**

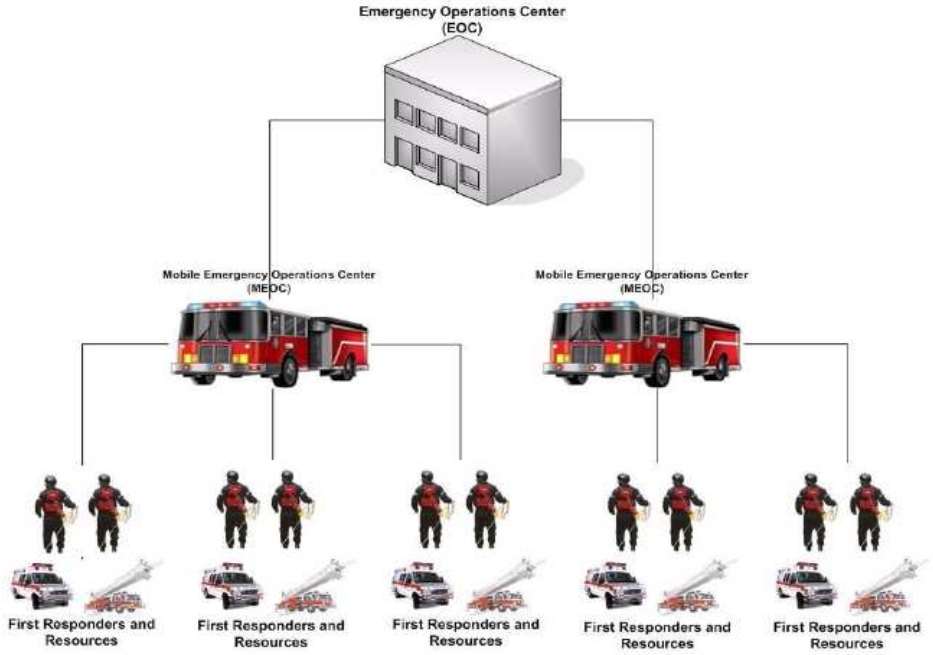
- **Therefore, a flexible, scalable and open emergency network should be based on standard radio access technologies, and provide the most reliable connectivity taking into account location, network availability and service characteristics.**

Emergency Networks: basics (2/2)

Integrated communications platform should be designed on the following criteria:

- **Channel rates for data and voice communications (bandwidth)**
- **Range of communication and radio coverage**
- **Size and weight of equipment**
- **Secure communications**
- **Power consumption**

Architecture (overview)



- **FRs normally act in remotely located areas with limited or disrupted communication infrastructures.**

- **They need to exchange information with the Mobile Emergency Operation Centre (MEOC) and with the remote Emergency Operation Centre (EOC), to enable cooperation at all levels with the target to minimize the uncertainty typical of crisis events.**

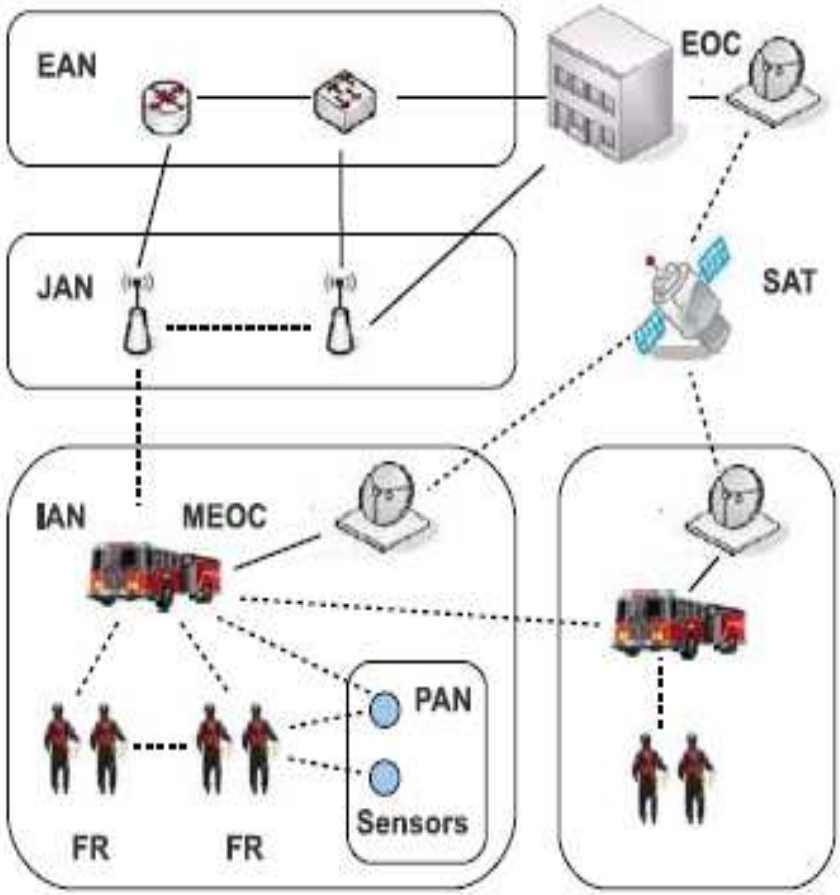
Main Architectural Components

- **EOC**, located at the headquarters, is the backbone for the operation of the emergency system. It is responsible for the collection of all data transmitted through the MEOC
- **MEOC**, the mobile local unit, acts as a bridge between the first responders in the incident field and the EOC located at the headquarters
- **FRs** (police, firefighters, etc.), operating on the field, should be provided with the best mobile hardware system according to the user needs and constraints (e.g. 3D visualization module, multi-radio module, etc.)

It is necessary to design an overall integrated system and to define the interactions and ways of communications among FRUs, MEOCs and EOC

General Network Architecture

- Main **backhaul link** via **satellite**
  - Fundamental role for an infrastructure-less emergency system
- Incident area network (IAN)
  - star/mesh network serving on-field FRs
- Personal area network (PAN)
  - wireless sensors collecting environmental information
- Jurisdiction area network (JAN)
  - fixed infrastructures, eventually used as backup backhaul links
- Extended Area Network (EAN),
  - backbone for JANs



Enabling Wireless Technologies

For instance:

- **MEOC-EOC (via Satellite):** DVB-RCS (and evolutions) to provide a full-duplex satellite link
- **IAN:** IEEE 802.11 “family” for access network and IEEE 802.16 for inter-IAN (MEOC-to-MEOC) communications
- **EAN/JAN:** (as backups) 3G/LTE, 2.5G, TETRA and/or other accessible wired infrastructures
- **PAN:** IEEE 802.15.1 (Bluetooth) and IEEE 802.15.4 (ZigBee), for wireless sensors data collection

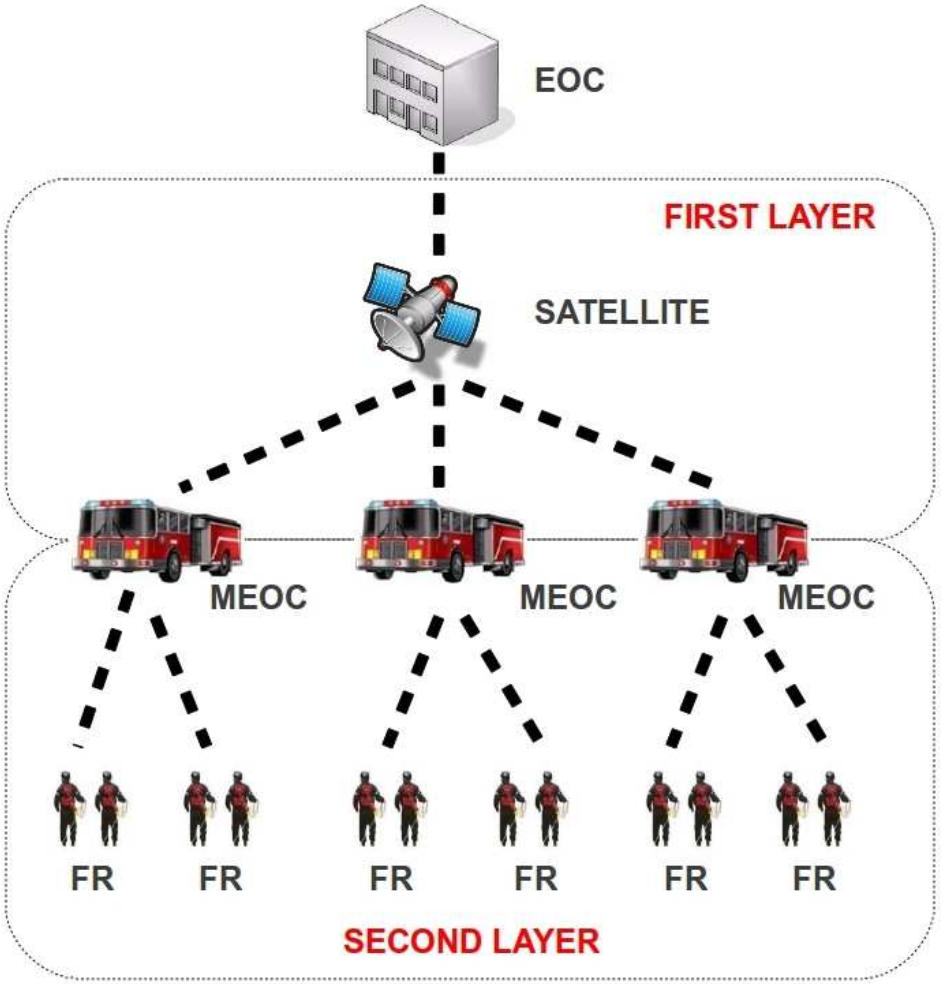
Outline

- Introduction: Emergency Networks
- General Architecture for Emergency Networks
- Enabling Communication Technologies
- **Network Architectures: possible options**
- Focus on Open Platform for the Mobile Emergency Operation Centre
- Conclusions

Architecture: Star

Option 1

- **Star-based** architecture
- Possible technologies:
  - DVB-RCS for the back-haul
  - IEEE 802.11 family



Architecture: Star

- **Pros**:
  - Centralized hub at both the first and the second layer
    - **Simple** QoS management
    - **Simple** access control and AAA procedures
    - **Simple** traffic filtering/shaping

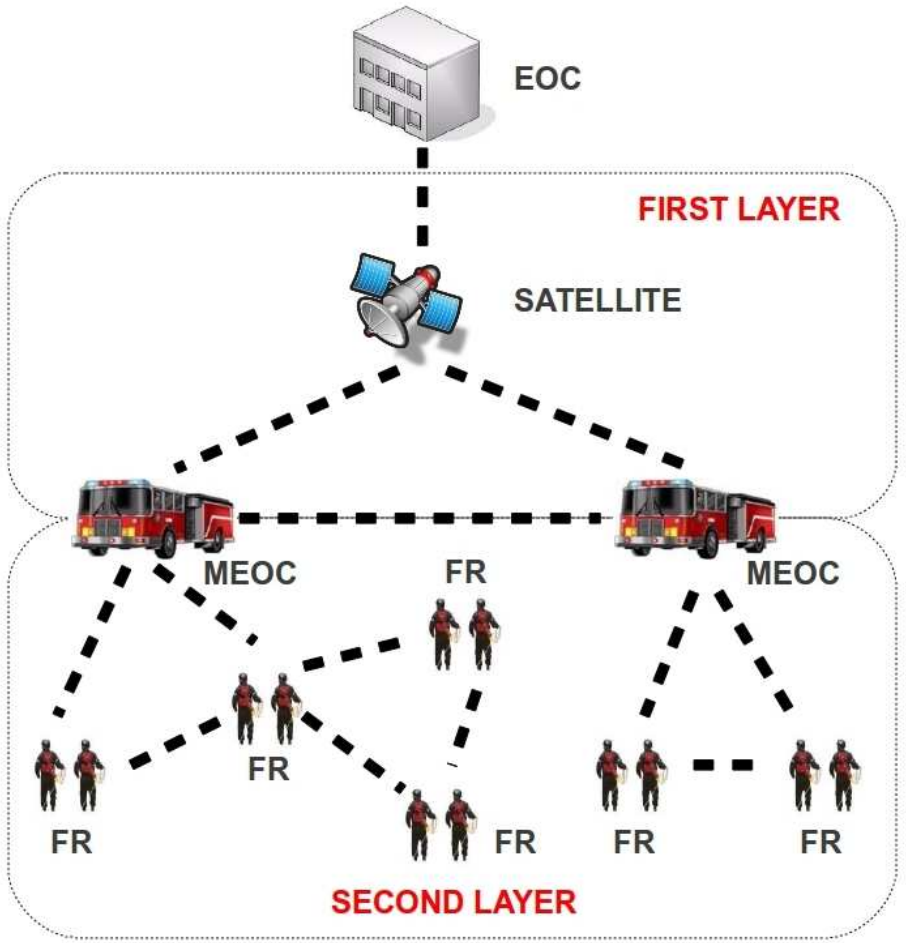
- **Cons**:
  - Centralized hub at both the first and the second layer
    - **Not** very resilient/robust
    - Presence of **single points of failure** (SPOFs)
  - For communications among FRs it is necessary to have a link to the MEOC

- **Comments**:
  - Very simple architecture
  - Simplicity + simple management vs. availability

Architecture: Mesh

Option 2

- **Mesh-based** architecture
- Possible technologies:
  - DVB-RCS for back-haul toward the MEOC
  - DVB-RCS NG for satellite mesh network among the MEOCs
  - IEEE 802.16 for terrestrial inter-MEOC links
  - IEEE 802.11s for communications among FRs



Architecture: Mesh

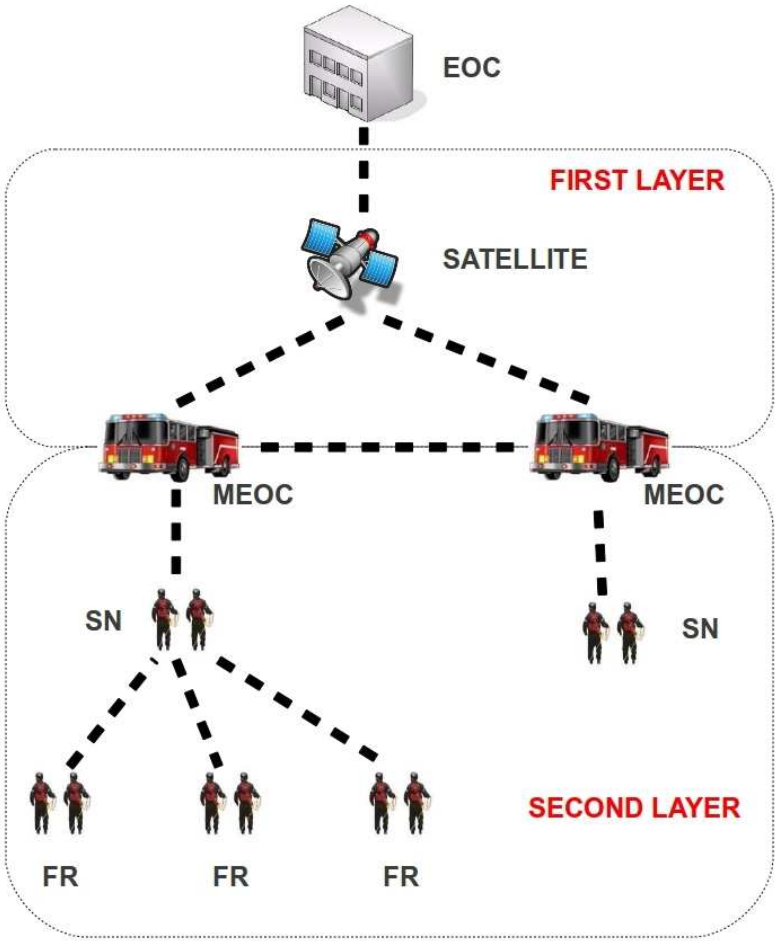
- **Pros**:
  - more resilient/robust than the star-based (no more SPOF)
  - direct p2p communications between FRs are possible

- **Cons**:
  - **More difficult** to implement access control at the second layer
  - Secure routing issues
  - **QoS issues** because of multi-hop communications

- **Comments**:
  - **More resilient** solution
  - Practical difficulties related to QoS, access control and secure routing
  - IEEE 802.11s still immature

Architecture: Hybrid

- **Trade-off** between the previous two architectures
- Closer to FRs team organization
- **Mesh-based** at the first layer
- "**Quasi star**" at the second layer
  - A **special node** (e.g. the FRs chief) acts as a hub, as in a star topology
    - It communicates with the MEOC via a back-haul link
- Possible technologies:
  - DVB-RCS and DVB-RCS NG for the main back-haul link at the first layer
  - IEEE 802.16 for terrestrial inter-MEOC links
  - IEEE 802.16/11 for the SN-MEOC link
  - IEEE 802.11 for inter-FR links



Architecture: Hybrid

- **Pros**:
  - Shares most of the benefits of the star-based architecture
  - FRs **local connectivity is possible** regardless of the SN-MEOC link
  - It **conforms** to the FRs' **group mobility** model

- **Cons**:
  - The **SN is a SPOF**

- **Comments**:
  - It is the natural extension of the star-based approach to the moving FRs group
  - It is **easier** to implement than the mesh-based
  - It is possible to introduce redundant links with the use of other technologies (e.g. 3G/LTE)
  - It is possible to **extend** this approach with the use of redundant and semi-fixed SNs (i.e. not human-equipped)
    - ✓ **No-more SPOF**
  - Our approach

General Design and Performance Evaluation

Main goals:

- Design a technical proposal which matches the operational needs in terms of flexibility, scalability, reliability and redundancy
- Determine performance limits in terms of throughput
- Study and employ end-to-end QoS schemes
- All communications must be secure (QoS vs Security)

and, in a realistic manner,

- with respect to the traffic pattern of the applications we want to support
- with respect to the uncertain nature of the wireless communication channels

Outline

- Introduction: Emergency Networks
- General Architecture for Emergency Networks
- Enabling Communication Technologies
- Network Architectures: possible options
- **Focus on Open Platform for the Mobile Emergency Operation Centre**
- Conclusions

The Mobile Emergency Operations Centre

An operational centre capable of enabling and supporting communications among FRs, other MEOCs and EOC through a variety of possible network technologies and infrastructures, such as:

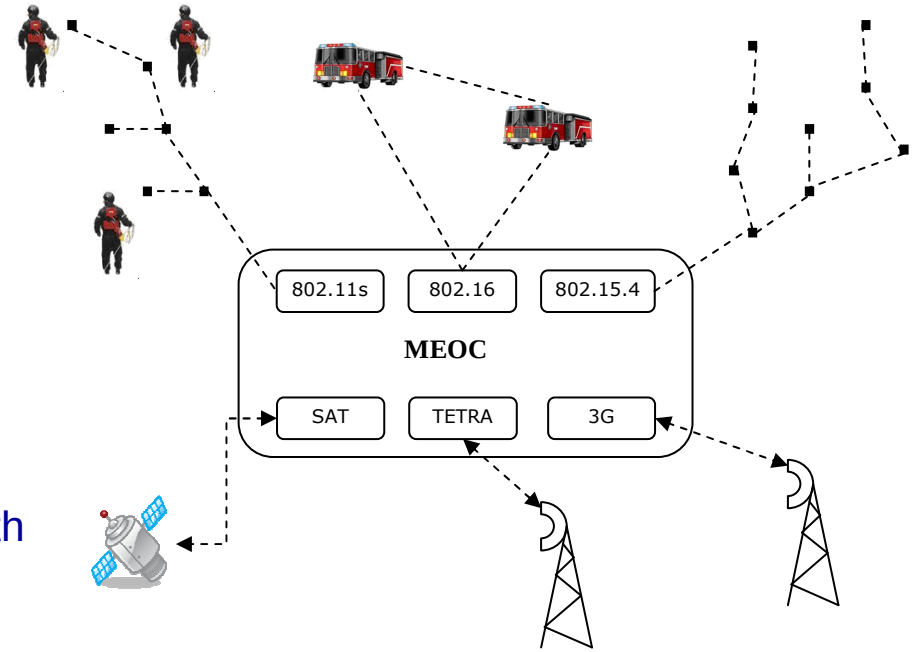
- DVB-RCS (main backhaul to the EOC)
- WiMAX (inter-MEOC mesh)
- WiFi (FRs mesh)
- 802.15.x (sensors)
- TETRA, 2.5, 3G/LTE

A Testing Framework for the MEOC

How to implement it ?

- **Physical** testbeds: realistic, but expensive, not reproducible testing, man-power expensive with no clear perspectives
- **Simulation** tools: cheap, adaptable, repeatable and scalable modeling of a network scenario, but not so accurate and not so useful for the implementation step

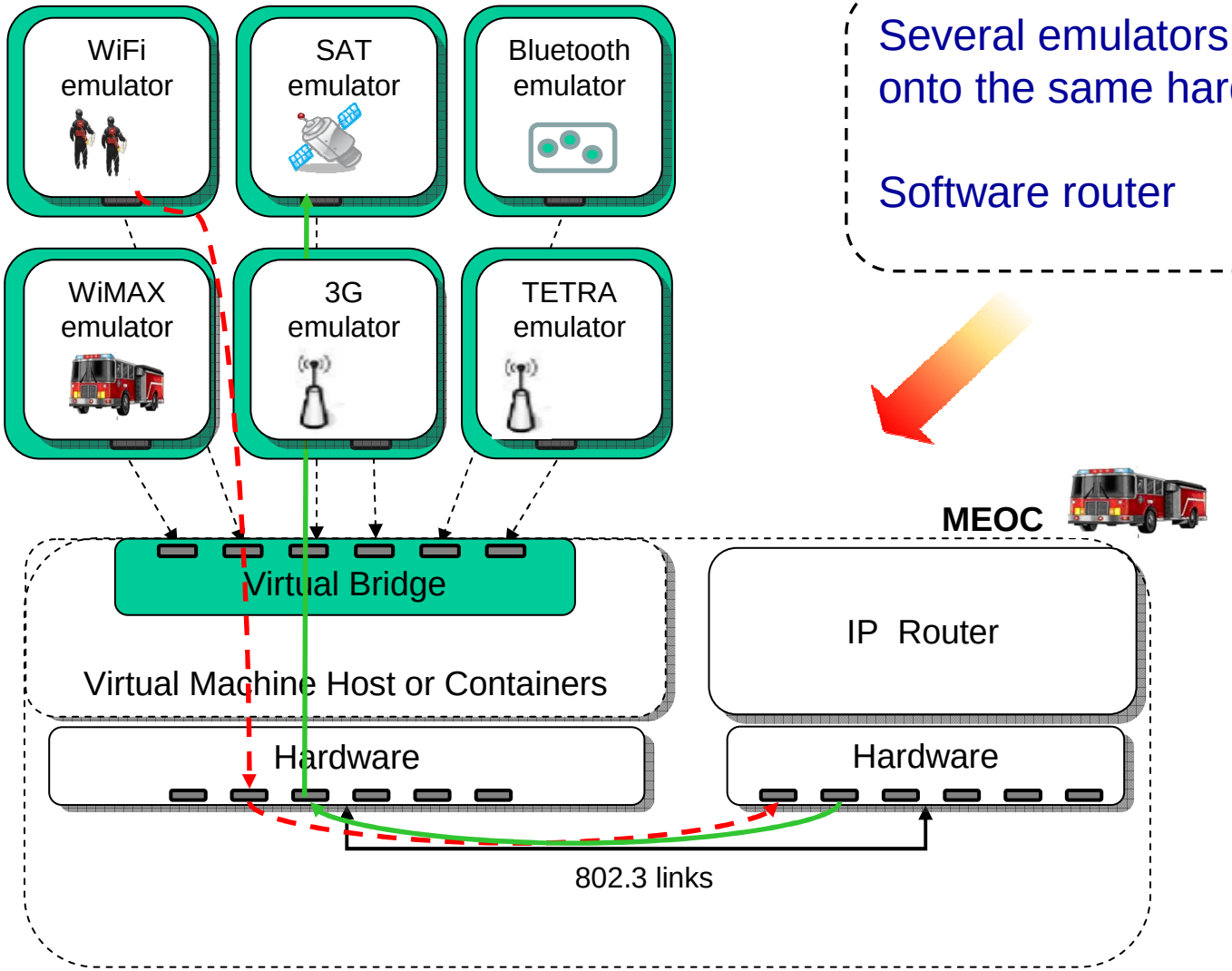
Hybrid approach: using emulative traffic generators and network simulators jointly with a real **software router**



Advantages:

- flexible, open to future integrations
- offers realistic forwarding performance and repeatable evaluations
- traffic differentiation and QoS policies capabilities
- technologically closer to the final equipment installed onboard the MEOC
- better yet, allows a step-by-step deployment

Emulation Test-bed for MEOC



Several emulators running in parallel onto the same hardware platform

Software router

Which software tools ?

- **The router**: Click, a Linux-based modular, open router; low cost, flexible, extensible, very good performance
- **The wireless networks simulation**: NS-3, one of the fastest simulators around, can also act as an emulator, allows real-world testbed integration
- **Virtual Machines**: traditional virtualization techniques allow to run several concurrent operating systems; e.g. VmWare, VirtualBox, etc. This technique usually requires lots of computing resources
- **Containers**: light virtualization technique, allow to virtualize a whole operating system as well as a single application – e.g. LXC
- **Why virtualization ?** Using Containers/VMs we can assign each NS3 instance a controlled amount of resources (CPU, memory, network interface, etc), as if NS3 was running on a different PC

G. Calarco, M. Casoni, "Virtual Networks and Software Router approach for Wireless Emergency Networks Design", Proc. of IEEE VTC 2011, 15-18 May 2011, Budapest (Hungary)

Conclusion

- Emergency networks require secure, interoperable and reliable ICT infrastructures to provide communication and decision support to the first responders operating in every possible crisis scenario, by adopting state of the art wireless technologies and advanced information systems.
- In such networks Satellites play a fundamental part, being the backbone for communications from the operation theatres to any given and remotely-located Emergency Operations Center.
- Possible solutions regarding system design, network architecture and Mobile Emergency Operations Center architecture have been presented
- Currently we are at the feasibility study step (simulation/emulation): next system design, development, prototyping, testing

THANK YOU FOR YOUR ATTENTION

casoni@ieee.org

… suggestions are very very welcome