UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

Ingegneria Modena
Dipartimento di Ingegneria "Enzo Ferrari"

Software-Defined Network Orchestration for Mission-Critical Scenarios

Prof. Maurizio Casoni

Research Activities at UNIMORE

In FP7 projects:

ESPONDER

"A holistic approach towards the development of the first responder of the future"

Objective:

SEC-2009.4.2.1: First Responder of the future

Duration of the project:

54 months (started July 1st 2010, ended December 2014)

PPDR-TC:

"Building the Roadmap for future PPDR COMMUNICATION systems evolution"

Objective:

SEC-2012.5.2-1: Preparation of the next generation of PPDR communication network

Duration of the project:

30 months (started April 1st 2013, ends September 2015)

Workshop Organization

- IEEE Emergency Networks for Public Protection and Disaster Relief within IEEE WiMob 2014 in Larnaca (Cyprus), October 2014

- Next Generation Public Safety and Critical Infrastructure within EuCNC 2015 in Paris (co-organized with Thales CS and the FP7 Absolute project), June 29 2015.

- 2nd IEEE Emergency Networks for Public Protection and Disaster Relief within IEEE WiMob 2015, Abu Dhabi (UAE), October 2015

- 3rd IEEE Emergency Networks for Public Protection and Disaster Relief workshop proposal submitted to next IEEE WiMob 2016, New York City (U.S.A), October 17, 2016

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 in the last 25 years. On average, about 7 lethal earthquakes were occurring each year in the 20^{th} century.

- Terrorist attacks especially in high-rise buildings (e.g. 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

The ESPONDER project scope

- Enhance the effectiveness of FRs operations
  - Building an *independent* and *open*, *adaptable*, and *extensible* **platform** with components put together in a loosely coupled way
    - *Communications* (voice, video)
    - Data (information)
  - Logistics of FR operations
    - Real Time (on-line)
    - Simulations (off-line)
  - Pilot demonstrations (proof-of-concept)

- Ensure the safety
  - of any FR
  - during all stages of an operation

- Recognition of the *socio-economic context* & its *impact*
  - Emerging training needs
  - Standardization & regulation issues
    - Research of current standardisation framework in Europe

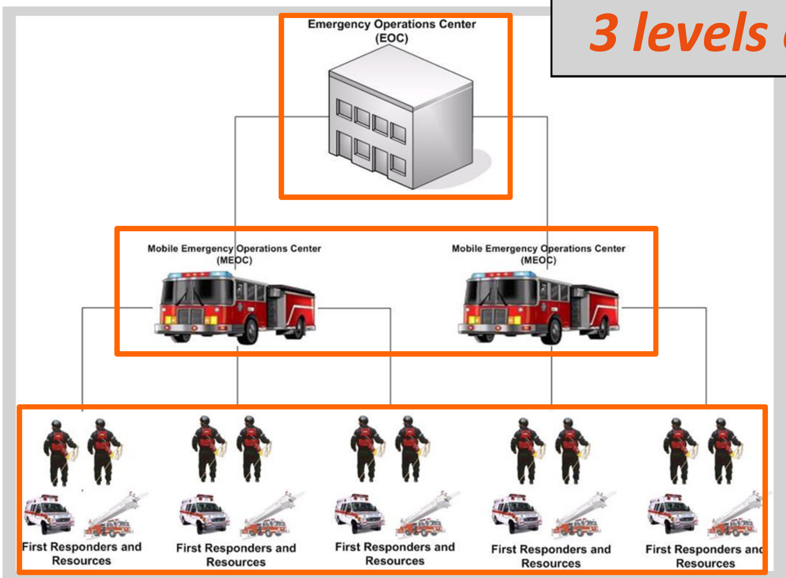
Holistic approach

- Technology integration & development
- Logistics
- Regulation
- Training

E-SPONDER at a glance

- Suite of real-time *data-centric* technologies forming a **Service Delivery Platform** for
  - Information & communications (monitoring of FRs during crisis)
  - Improvement of control and coordination between field units and command and control centers

3 levels of intervention



EOC: Emergency Operations Center

- Response planning, strategic view
- Communications
- Data fusion
- GIS
- Data bases
  - E-SPONDER portal

Strategic

MEOC: Mobile EOC

- Response coordination
- Communication interoperability
- Field base of operations
  - Data fusion (replica)
  - GIS (replica)

Tactical

FRU: First Responder Unit

- Smart jacket / Physio & Environmental sensors
- Communication systems & Mobile applications
- Positioning system

Operational

PPDR-TC: MAIN OBJECTIVES

- **To gather European PPDR facts and figures data.**
- **To define PPDR reference usage scenarios and identify service requirements and future needs in the European context.**
- **To implement a detailed study of the reference scenarios with a view to establishing service classification and identifying key technical issues.**
- **To identify candidate PPDR technologies and architectures.**
- **To develop validation tools for future PPDR.**
- **To derive technical recommendations on candidate technologies and architectures.**
- **To provide economical recommendations on candidate technologies and architectures.**
- **To provide a roadmap towards full satisfaction of future PPDR requirements and to develop recommendations for PPDR telecommunications standards for decisions-makers.**

Status

- *Defined PPDR user requirements and reference usage scenarios*
- *Established PPDR service classification*
- *Established a European PPDR facts and figures database for relevant PPDR authorities*
- *Analysed the radio spectrum currently utilized by PPDR agencies around the world and the projected future needs for radio spectrum*
- *Identified several business models (with sub-models) presenting different approaches to set a PPDR system up and developed a tool for Technical, financial, economical and organizational analysis*
- *Provided initial technical/economical recommendations for future PPDR systems*

Main outcomes - Key findings

- Distinct communication requirements identified:
  - Mission-critical Voice
  - Narrow Band Data (e.g. for messaging)
  - Broad Band Data (e.g. images or large files)
  - Video
  - Use of repeater stations to extend coverage or provide air-to-ground communication
- Video and Image transmission identified as important in various scenarios
  - Surveillance
  - Maintaining public order / safety at large events
  - Assisting treatment of casualties
  - Identification of suspects or vehicles
  - Situational awareness (e.g. during rioting or high speed pursuits)
- High level communication scenarios
  - A: Between a Central Control Station and Field Personnel at an Incident
  - B: Between PPDR Vehicles and an Incident Location or Control Station
  - C: Between Individuals at an Incident
  - D: Between Different PPDR Entities (e.g. Police, Fire, Ambulance, Volunteers)
  - E: Accessing External Data Sources (e.g. Internet)
  - F: Communication in Enclosed Spaces (e.g. Tunnels Or Basements)
  - G: Communication With Remote Locations (e.g. Mountains or at Sea)
  - H: Communication with or between Machines (e.g. Remotely Controlled Vehicles)

Main outcomes - *Key deficiencies*

- Coverage
  - Incomplete with significant black spots, especially indoors, underground or in remote areas.
  - Worse for data services
- Lack of Interoperability
  - At the technology and working protocol level
- **Resilience**:
  - At the network level (uninterruptable power supplies etc.) and terminals (e.g. need to be rugged and waterproof)
- Reliance on public networks:
  - Often unusable after major incidents due to congestion.

Main outcomes -*Future requirements*

- Video
  - Applications include automatic number plate recognition, body worn cameras, portable CCTV deployments, surveillance, suspect identification, telemedicine and thermal imaging
- Other data applications
  - Breathing apparatus telemetry, vital signs monitoring, access to on-line forms and databases
- Location services:
  - Tracking of personnel, vehicles and other assets. Also electronic mapping services are increasingly used
- **Resilience and Backup**:
  - Multiple networks preferred (e.g. voice and data) to provide fall back if one fails.
- Flexibility:
  - Rapid provision of extra coverage or capacity when needed
- Better interoperability between different agencies and ICT systems

Main outcomes -Technologies

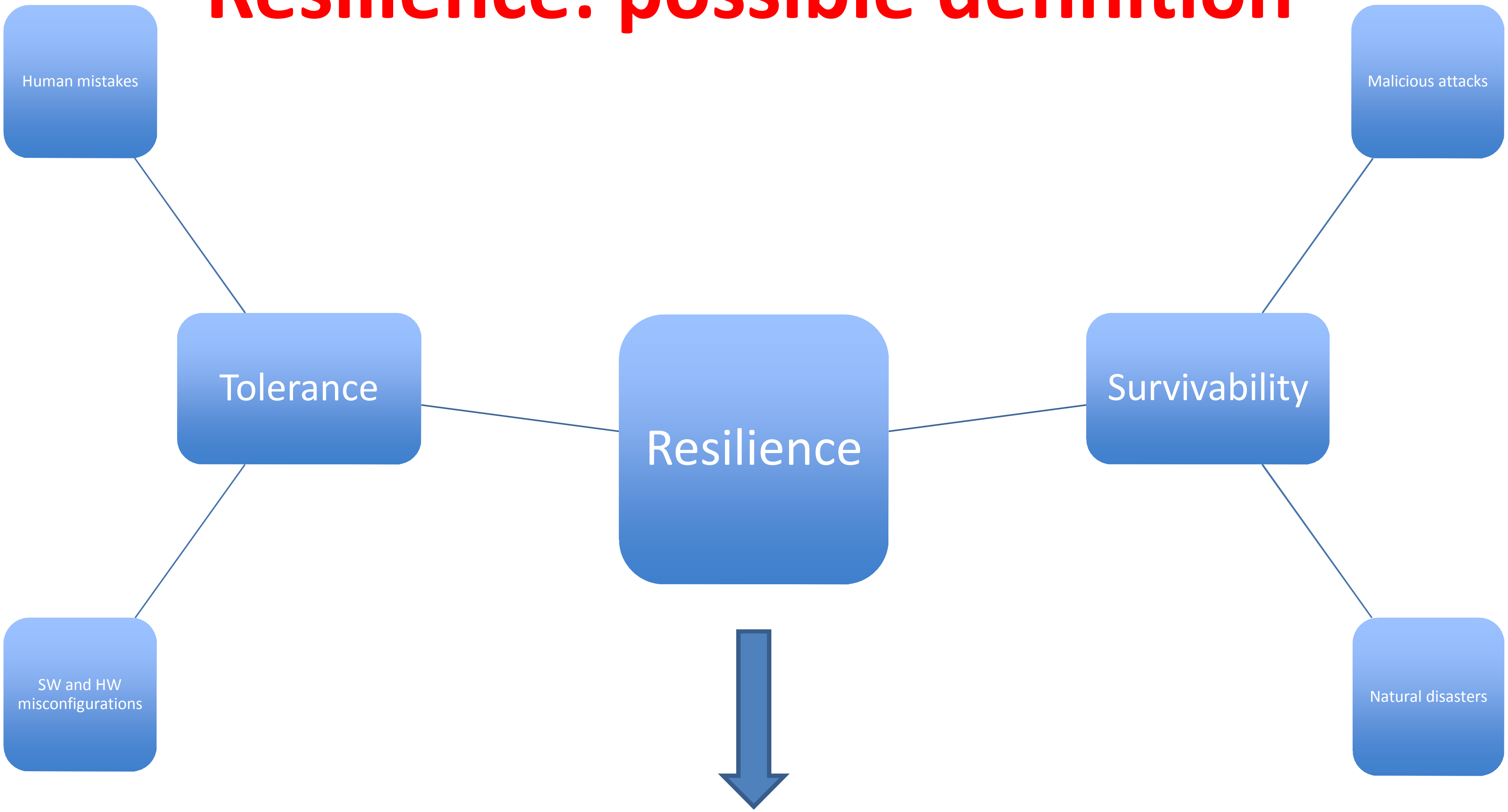
- **Several PPDR network solutions were analysed according to:**
  - Relevant players in the development and adoption
  - Standards development
  - Technical details
  - Requirements
  - Strengths and weaknesses for PPDR applications

Category	Network solution
Current PPDR technologies	TETRA Release 1
	TETRA Release 2
	TETRAPOL
	Analogue PMR
	Digital PMR
	DMR
	SATCOM
Public networks	CDMA2000
	GSM
	GPRS/EDGE
	UMTS
	HSPA/HSPA+
Candidate technologies for future PPDR applications	LTE (public/dedicated)
	Wi-Fi (public/dedicated)
	WiMAX
	MANETs
Transversal communication concepts	Software-Defined Radio
	Cognitive Radio

Main outcomes - Technology Gaps

PPDR-TC Network Requirements	TETRA Release 1	TETRA Release 2	TETRAPOL	Analog. PMR	Digital PMR	DMR	SATCOM	CDMA 2000	GSM	GPRS/EDGE	UMTS	HSPA/ HSPA+	LTE	Wi-Fi	WiMAX	MANETs
Users	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Partially Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Partially Compliant
Coverage area	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Partially Compliant	Partially Compliant	Partially Compliant
Required network topology	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Fully Compliant	Fully Compliant	Fully Compliant
Node connectivity models	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Fully Compliant	Fully Compliant	Fully Compliant
Capacity in terms of type of data and required bandwidth	Partially Compliant	Partially Compliant	Partially Compliant	Not Compliant	Not Compliant	Not Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant
Mobility requirements	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Partially Compliant	Fully Compliant	Fully Compliant
Interoperability requirements	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant
Service availability, reliability and resilience	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Partially Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Fully Compliant
Performance requirements	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Fully Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Fully Compliant	Fully Compliant	Partially Compliant	Partially Compliant	Partially Compliant
Security	Fully Compliant	Fully Compliant	Fully Compliant	Partially Compliant	Fully Compliant	Fully Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Fully Compliant	Partially Compliant	Fully Compliant	Fully Compliant
Specific voice communication requirements	Fully Compliant	Fully Compliant	Fully Compliant	Partially Compliant	Fully Compliant	Fully Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant
Specific data communication requirements	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Partially Compliant	Fully Compliant	Fully Compliant	Partially Compliant	Fully Compliant	Fully Compliant

Resilience: possible definition



PERSISTENCE OF SERVICE

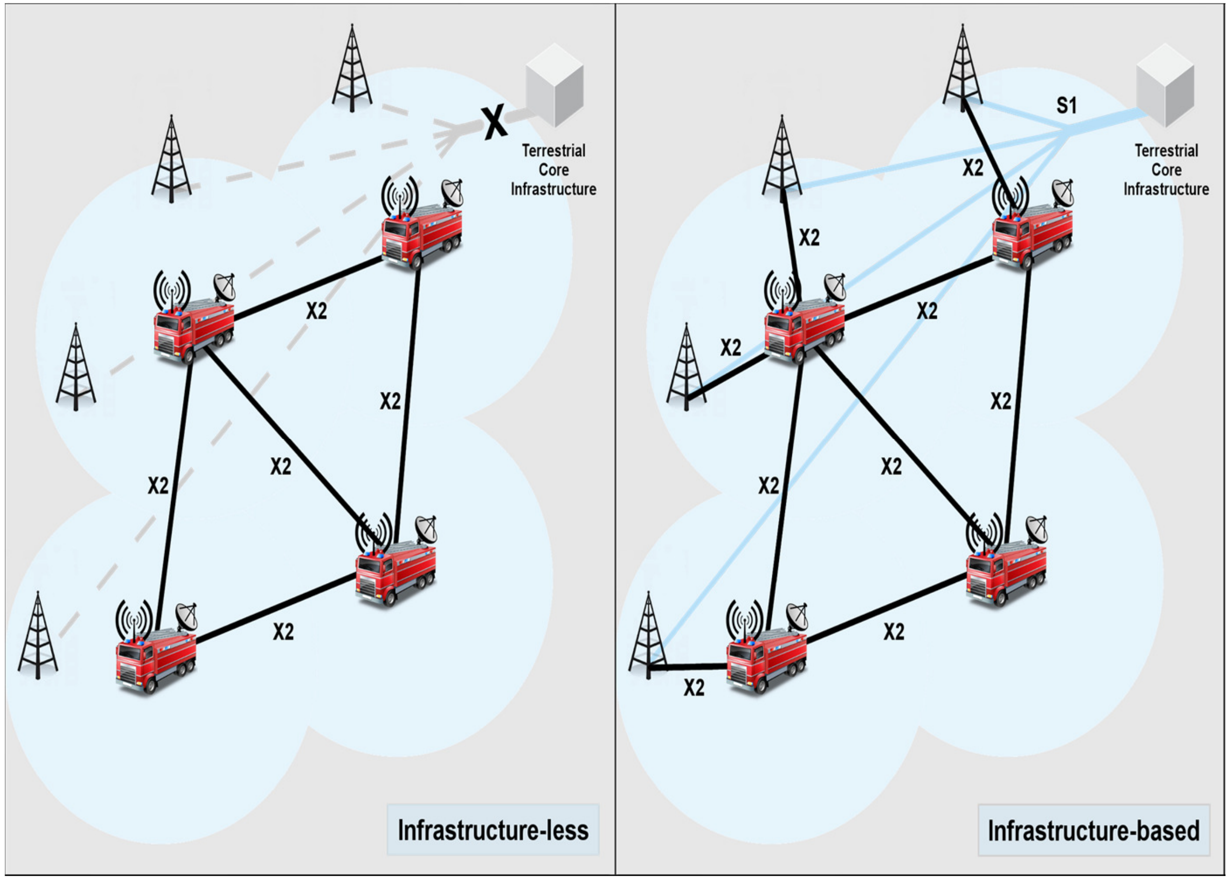
Possible Approaches to Resilience (some)

- **Survivable Network Design**
  - Plan in advance
  - Build the infrastructure by inserting **redundancy** wherever possible
  - Let the network react to localized failures through **Self-Organizing Network (SON) Features**
  - Keep ready some fast to deploy and easy to configure **ad-hoc mobile networks** with additional backhaul mechanisms for unrecoverable failures and mission-critical applications

Survivable Network Design

an example

Satellite-backhauled LTE vehicular ad-hoc network



Interoperability with terrestrial LTE infrastructure through SON capabilities

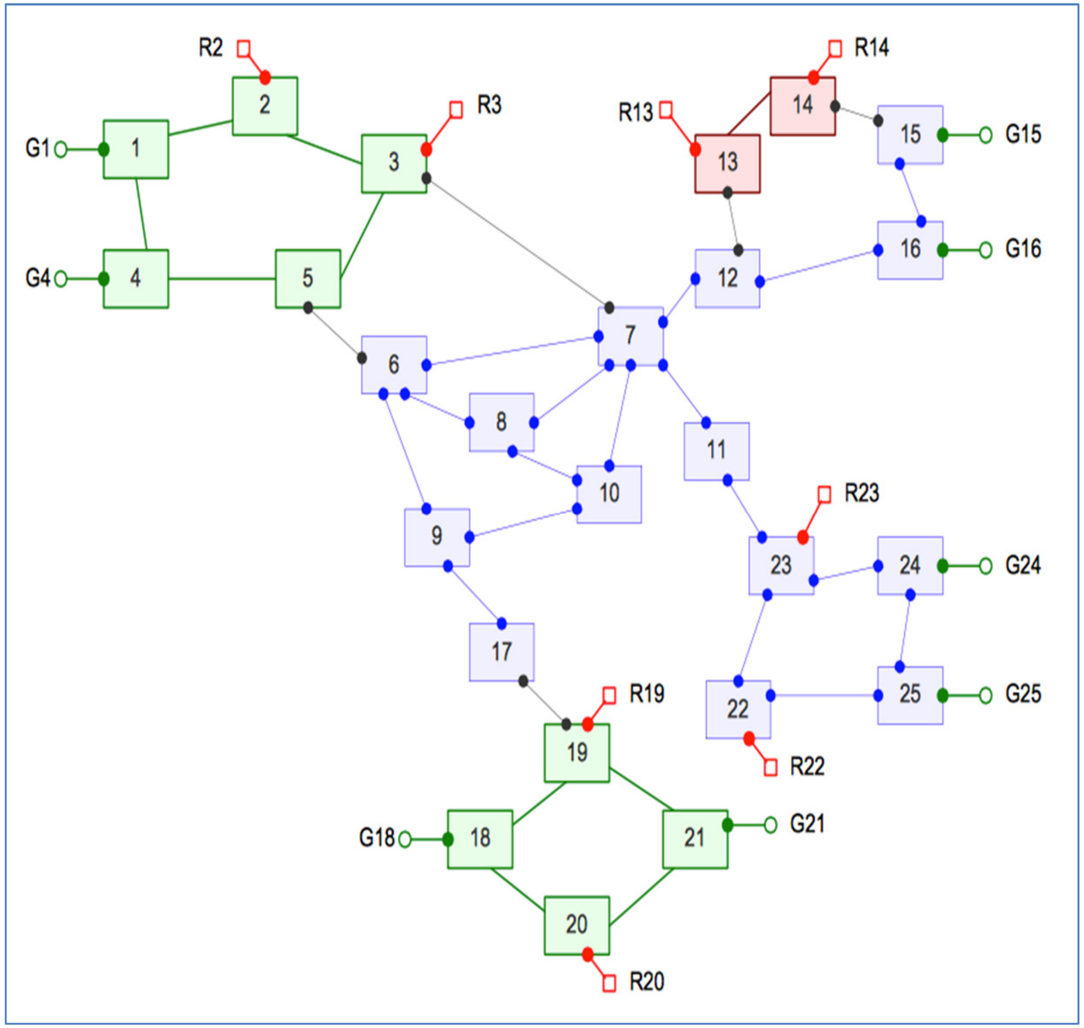
M. Casoni, Carlo A. Grazia, M. Klapez, N. Patriciello, A. Amditis and E. Sdongos, «Integration of Satellite and LTE for Disaster Recovery», IEEE Communications Magazine, pp. 47-53, March 2015

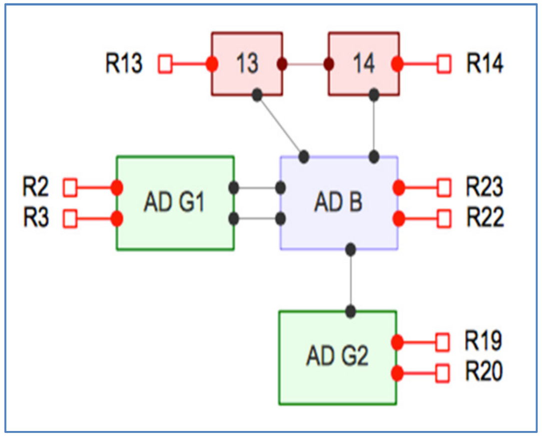
Possible Approaches to Resilience (some)

- Survivable Network Design
  - Plan in advance
  - Build the infrastructure by inserting **redundancy** wherever possible
  - Let the network react to localized failures through **Self-Organizing Network (SON) Features**
  - Keep ready some fast to deploy and easy to configure **ad-hoc mobile networks** with additional backhaul mechanisms for unrecoverable failures and mission-critical applications

- Interoperability
  - Share network infrastructure among multiple owners, through multiple administrative domains
  - Network Function Virtualization (**NFV**) for sandboxed and replaceable operations in core networks
  - Software-Defined Networking (**SDN**) for equipment interoperability and quick replacement

Interoperability among Network Providers, NFV and SDN





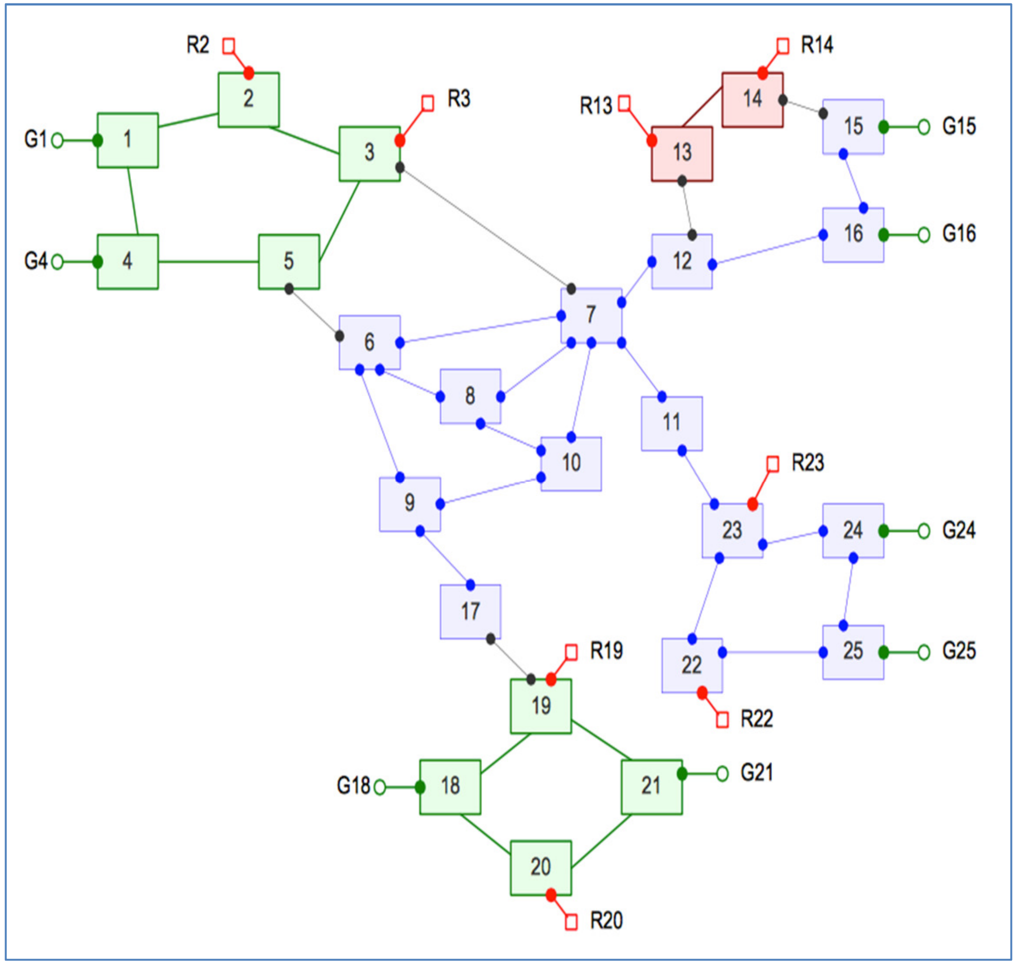
The network as seen by RED

RED sees full detail of its own network equipments and ports, but the BLUE and GREEN domains are virtualized

Network with multiple owners

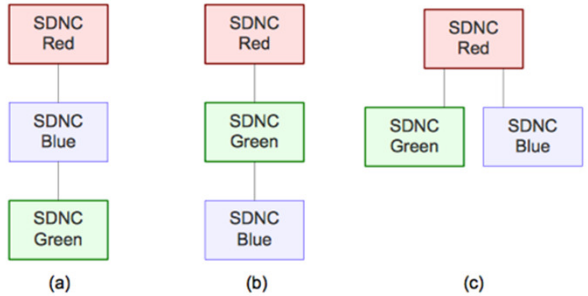
Open Networking Foundation, ”SDN architecture”, ONF TR-502, June, 2014

Interoperability among Network Providers, NFV and SDN



Network with multiple owners
Open Networking Foundation, ”SDN architecture”, ONF TR-502, June, 2014

Let us assume a Controller (SDNC) for each of the providers **RED**, **BLUE** and **GREEN**: 3 options exist for **RED**’s SDNC associations:



a) **GREEN** resources are leased by **BLUE** on behalf of **RED**, which interacts with **GREEN** resources only by way of virtualization provided by **BLUE**.

b) The inverse of (a)

c) **RED** has agreements with both **GREEN** and **BLUE**; **RED** has visibility of the three links between **GREEN** and **BLUE** domains, and it expects to have some control over them.

Possible Approaches to Resilience (some)

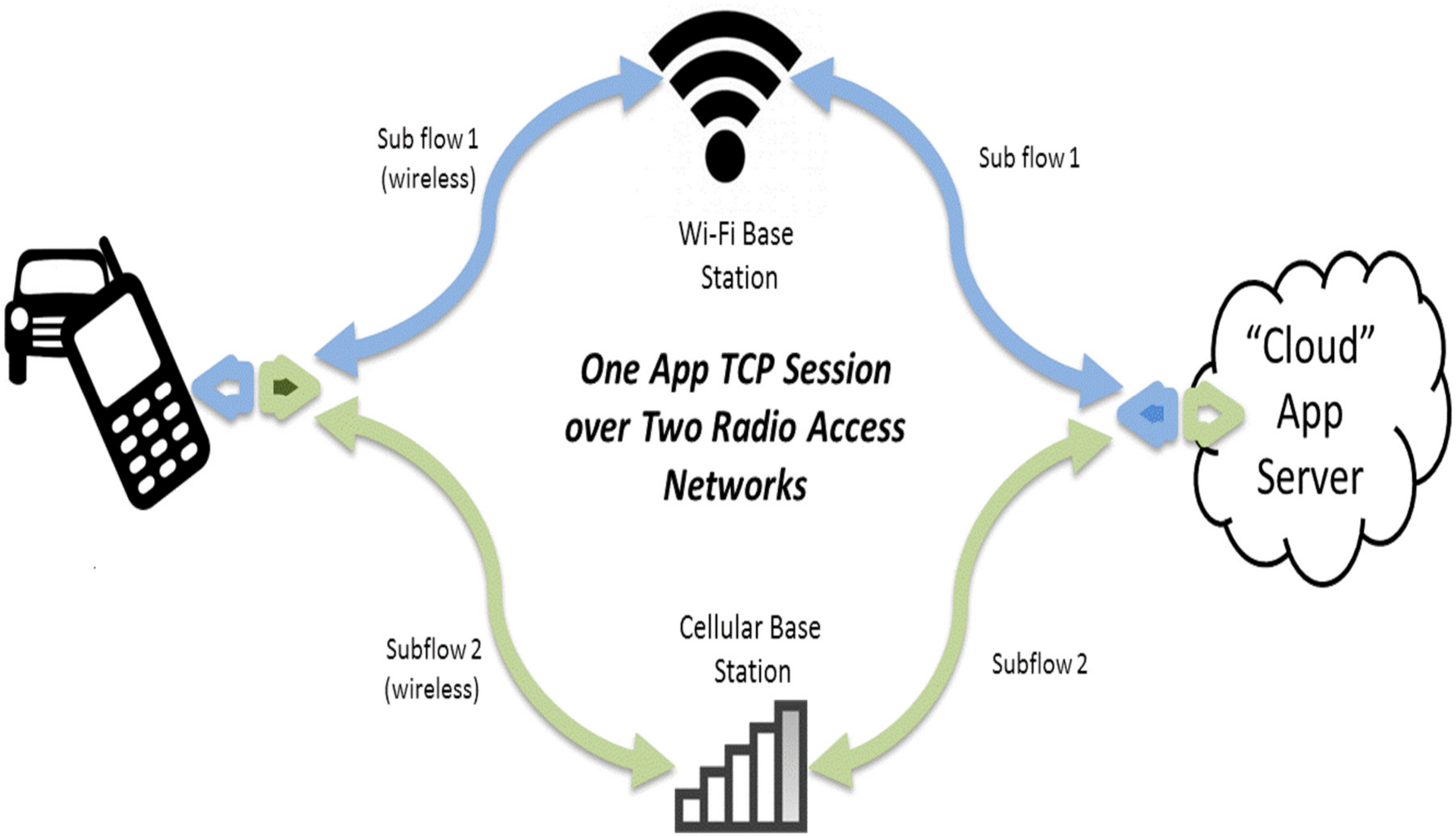
- Survivable Network Design
  - Plan in advance
  - Build the infrastructure by inserting **redundancy** wherever possible
  - Let the network react to localized failures through **Self-Organizing Network (SON) Features**
  - Keep ready some fast to deploy and easy to configure **ad-hoc mobile networks** with additional backhaul mechanisms for unrecoverable failures and mission-critical applications

- Interoperability
  - Share network infrastructure among multiple owners, through multiple administrative domains
  - Network Function Virtualization (**NFV**) for sandboxed and replaceable operations in core networks
  - Software-Defined Networking (**SDN**) for equipment interoperability and quick substitutability

- Resource Pooling
  - **Multihomed** devices with dedicated network protocols (e.g. **MultiPath-TCP**)
  - **Collaborative** frameworks through **SDN** and 5G or **SDN** and NFV in 4G

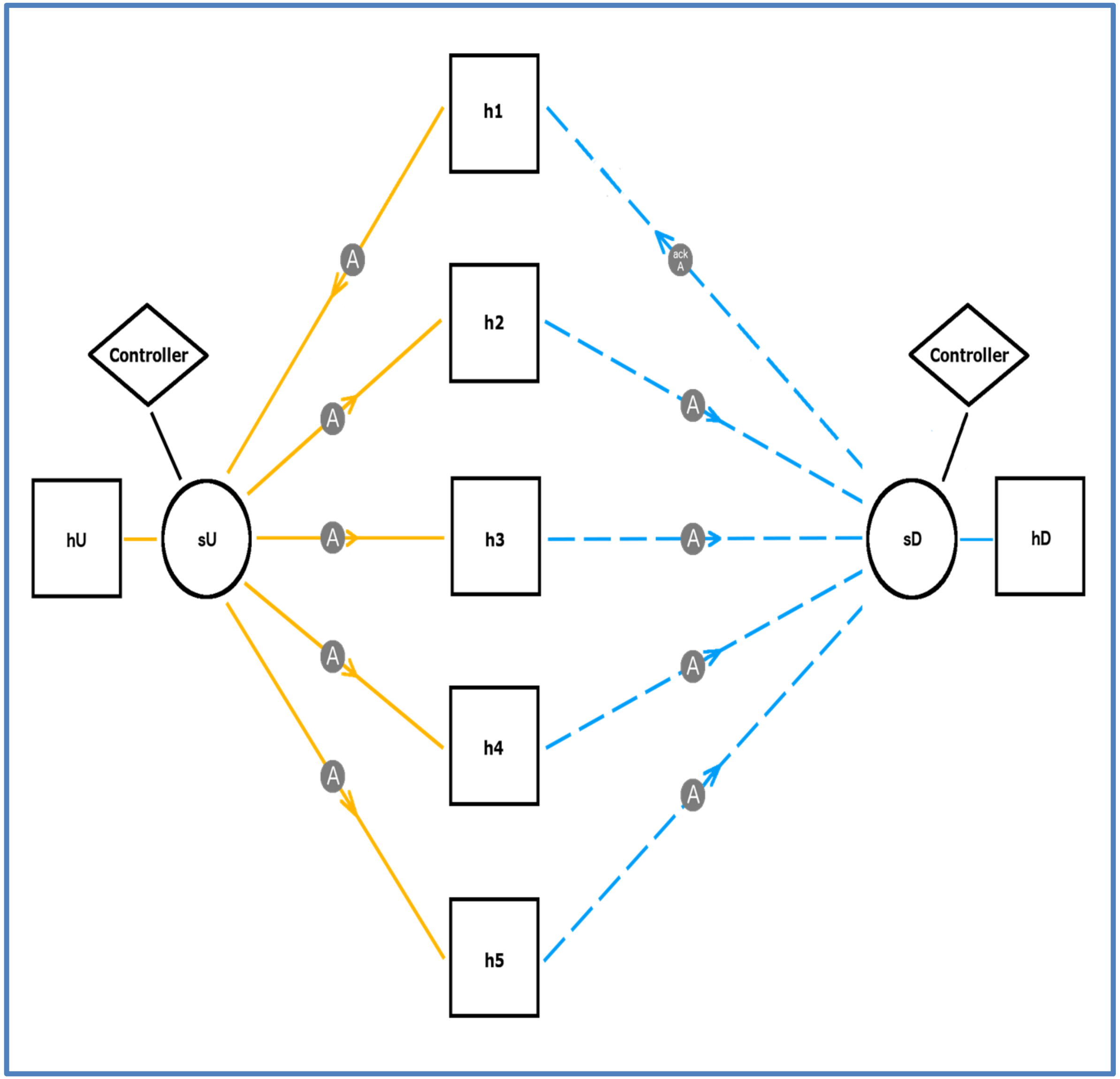
Resource Pooling

MultiPath TCP



Resource Pooling

SDN & NFV



Example of an upload **from host h1 to the remote host hD**.

BLUE, hatched lines represent low speed wireless links, while **ORANGE**, solid lines represent high-performance wireless links (e.g. IEEE 802.11n).

A is a packet;
host1, instead of sending data directly to hD, sends packets to a SDN-enabled gateway sU, which to its turn replicates these packets on a number of concurrent routes to hD.

SDN/NFV based PPDR Architecture

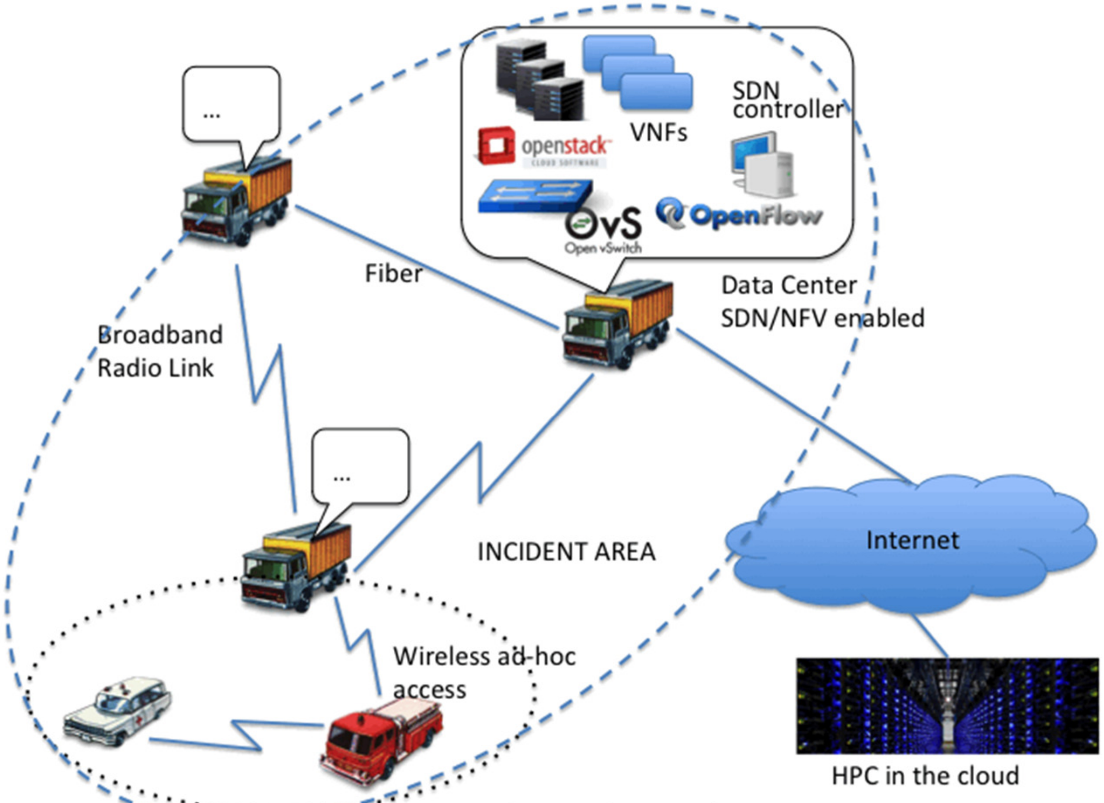


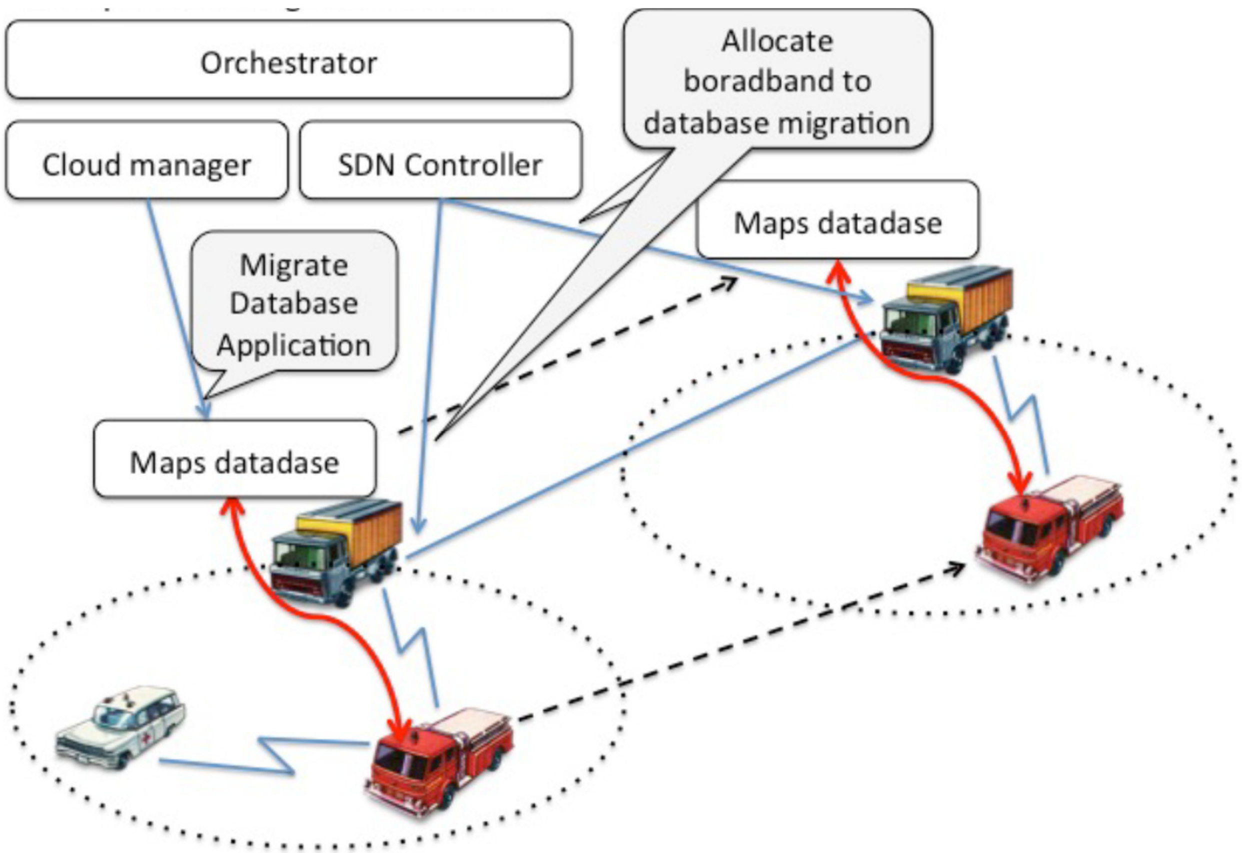
Fig. 1 : Softwarized PPDR achitecture

All resources are softwarized
Hosted and managed within
Mini-DataCentres, deployed
In properly equipped trucks

Mini-DCs host all the networking
Functions: wireless connectivity,
Authentication, firewalls, bandwidth
Shapers,…

IT services (i.e. software applications
hosted in the mDCs as close as possible to
the forces on the ground.
If the emergency scenarios will require
computational intensive applications
(e.g., access to GIS, meteo forecasting,
video analysis, risks mitigation) the cloud
computing approach integrated with SDN
allows to offload the tasks to remote
Data Centers (DCs) more suitable to
HPC applications.

Service migration following the user



Fire brigades require
High definition map data base
For quick consultation
And the vehicle moves to
Another coverage area

OPEN ISSUES (SOME)

- Coverage
  - Incomplete with significant black spots, especially indoors, underground or in remote areas.
  - Worse for data services
- Broadband data communications
- Harmonized frequency bands for PPDR use throughout Europe
- Lack of Interoperability : (from L1 upward), not just through gateways
  - Backward interoperability (Tetra/TEDS, Tetrapol)
  - Agencies interoperability
- Full IPv6 systems (some prototypes are on site)
- Effective and rapidly deployable infrastructure-less network (some hybrid LTE-SAT tests)
- Critical infrastructure resilience and security
- Location services (tracking of personnel, vehicles and other assets)

OPEN ISSUES and 5G vision for 2020

	OPEN ISSUE	5G VISION
1.	Coverage	1,000 times more network capacity and 10 to 100 more user-access capacity than today; ubiquitous 5G access including low density areas;
2.	Broadband data comms	Minimum guaranteed terminal data rate > 100Mb/s
3.	Effective and rapidly deployable infrastructure-less network	Reducing average service creation time from 90 days to 90 minutes;
4.	Interoperability + resilience	Increased resilience and continuity
5.	Resilience and security	Robust security and privacy
6.	Location services	Accuracy of terminal location < 5m

Thank you!

Maurizio Casoni

Department of Engineering “Enzo Ferrari”
University of Modena and Reggio Emilia - Italy
Email: maurizio.casoni@unimore.it