Vodafone Technology Resilience Programme overview

Ettore Genta – Vodafone Group

18th November 2024
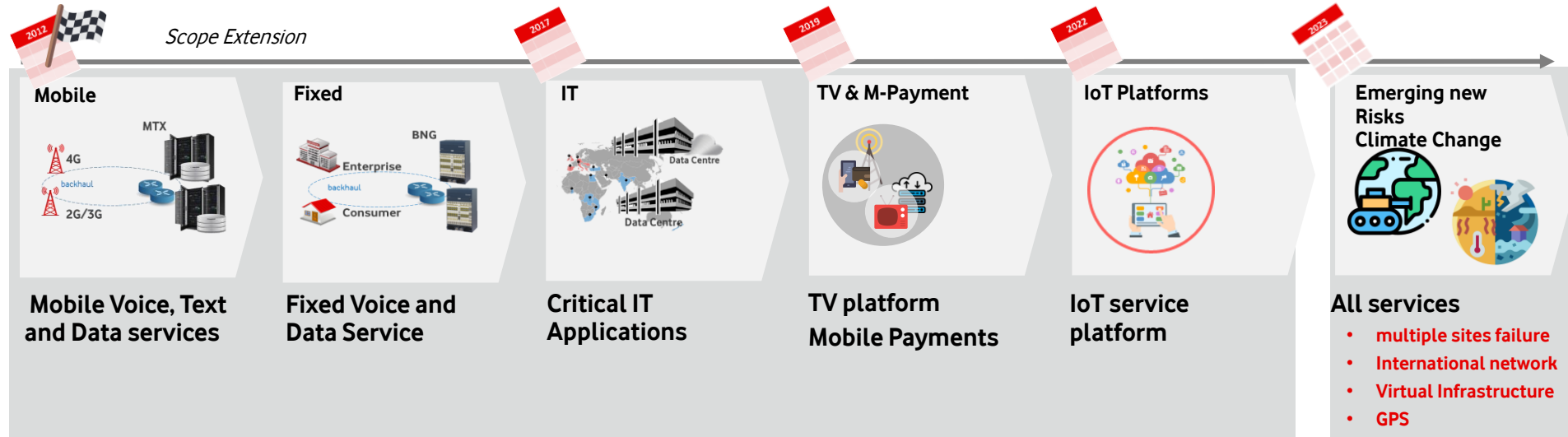
Agenda

- Technology Resilience Program and its evolution

- Protection and Disaster Recovery highlights

Technology Resilience | Scope evolution

We recognize that the risk of major disasters is growing and have been tackling this issue since 2012

Scope Extension

2012 **2017** **2019** **2022** **2023**

Mobile	Fixed	IT	TV & M-Payment	IoT Platforms	Emerging new Risks Climate Change
Mobile Voice, Text and Data services	**Fixed Voice and Data Service**	**Critical IT Applications**	**TV platform** **Mobile Payments**	**IoT service platform**	**All services** • **multiple sites failure** • **International network** • **Virtual Infrastructure** • **GPS**

Resilience is governed through a Technology Resilience Policy that defines:
Risk scenarios, Scope and Service Level Targets according to Vodafone Risk appetite

3

Technology Resilience | Defence methodologies

Defense against technology failure is based on three pillars: Prevention, Reaction, Governance
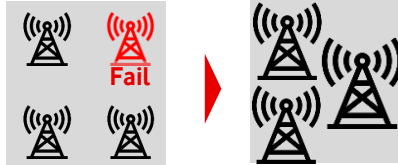
Preventive – Resilient Design	Reactive- Disaster Recovery Solution

Infrastructure and fibre enhancement

- Emergency Power
- Fibre redundancy

Distributed Network setup

Allows to redistribute traffic to other Core sites and Disaster Recovery nodes

Highly meshed backhaul network

Ring or Multiple fibre connection allow to re-address traffic to other sites

On Site Intervention

Truck-based Disaster Recovery solution is used to intervene where re-routing is not an option

Governance

TR01	TR02	TR03	TR04	TR05	TR06	TR07	TR08	TR09	TR10
Site Risk Assessment	Service Level Target Assessment	Resilience by design	Technology, service and site documentation	Recovery Plans	Resilience Testing	Programme Management	Third Party support during recovery	Near Miss and Policy Breach	Outsourced Activity Control

Agenda

- Technology Resilience Program and its evolution

- Protection and Disaster Recovery highlights

Resilient design helped in surviving from catastrophic event
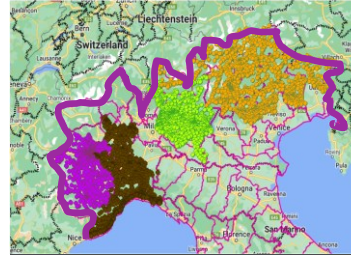## lesson learnt from Fire in Milan LTC
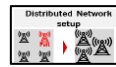
What Happened

- Fire started in air handling unit out of the Core room
- Fire brigade blocked site access for safety reasons
- All Aircon shutdown, temperature reached limit in 20m
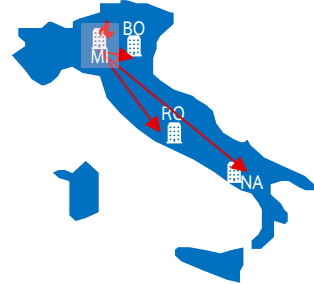- Core Network equipments started to suffer and were switched off

⚠ The incident impacted services in Northern Italy

- Potential impact: 3.3M customers
- Service impacted: Mobile voice and data, fixed and VoLTE

👍 The DR response worked well

- Traffic automatically rerouted to the other sites
- ~ 95% customers moved to the other region – no impact
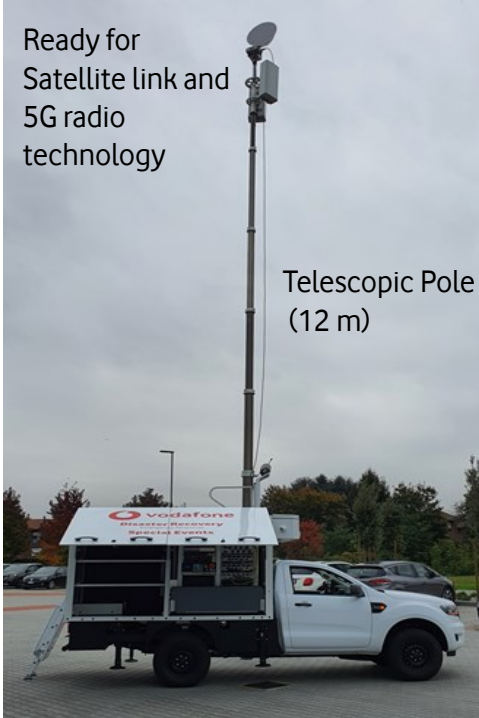
👎 What did not work as expected

5% of customers was not recovered immediately due to a DNS error, promptly solved with manual intervention

Disaster Recovery | Recovery solutions

Mobile Radio Access

Ready for Satellite link and 5G radio technology

Telescopic Pole (12 m)

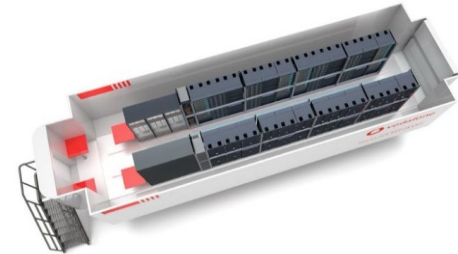
Fixed Access

INSIDE

- Fixed Access equipment
- Energy Power Unit
- Battery Backup

External panel

- Fast and safe Optical Fiber connections

Core Network
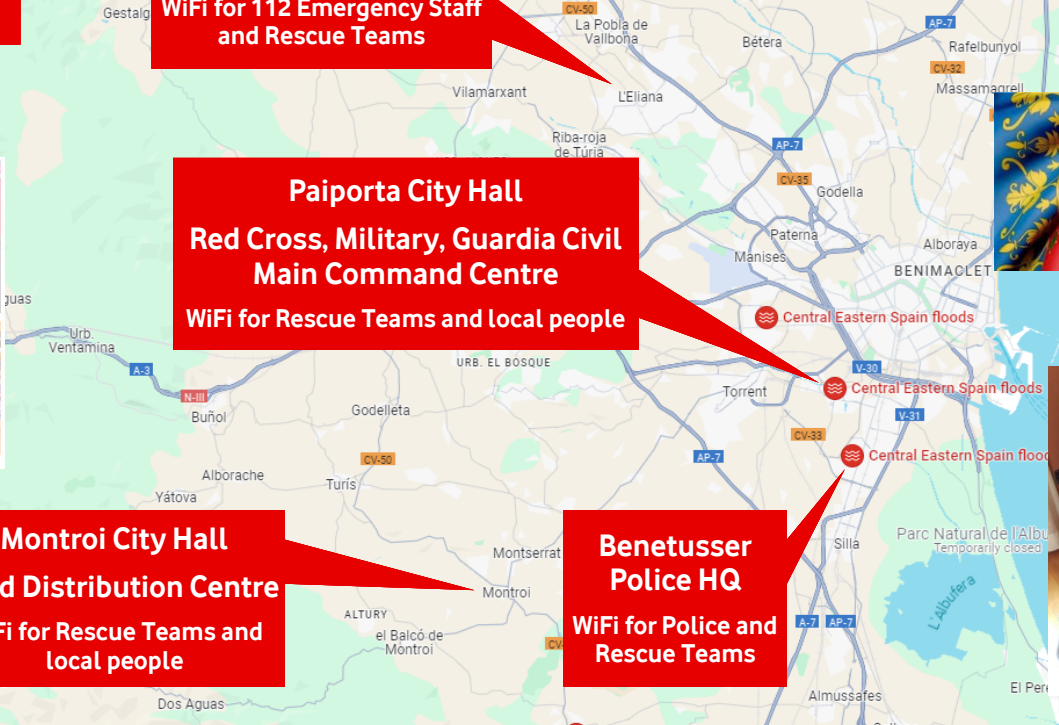
Instant Network – Valencia Flood Disaster (ES)

Utiel City Hall

Food & Clothing Distribution Centre

WiFi for Rescue Teams and local people

L'Eliana 112 Emergency Coordination Centre

WiFi for 112 Emergency Staff and Rescue Teams

Paiporta City Hall

Red Cross, Military, Guardia Civil Main Command Centre

WiFi for Rescue Teams and local people

Montroi City Hall

Food Distribution Centre

WiFi for Rescue Teams and local people

Benetusser Police HQ

WiFi for Police and Rescue Teams