SECRICOM

Seamless Communication for Crisis Management

Presentation to the

BAPCO National Conference

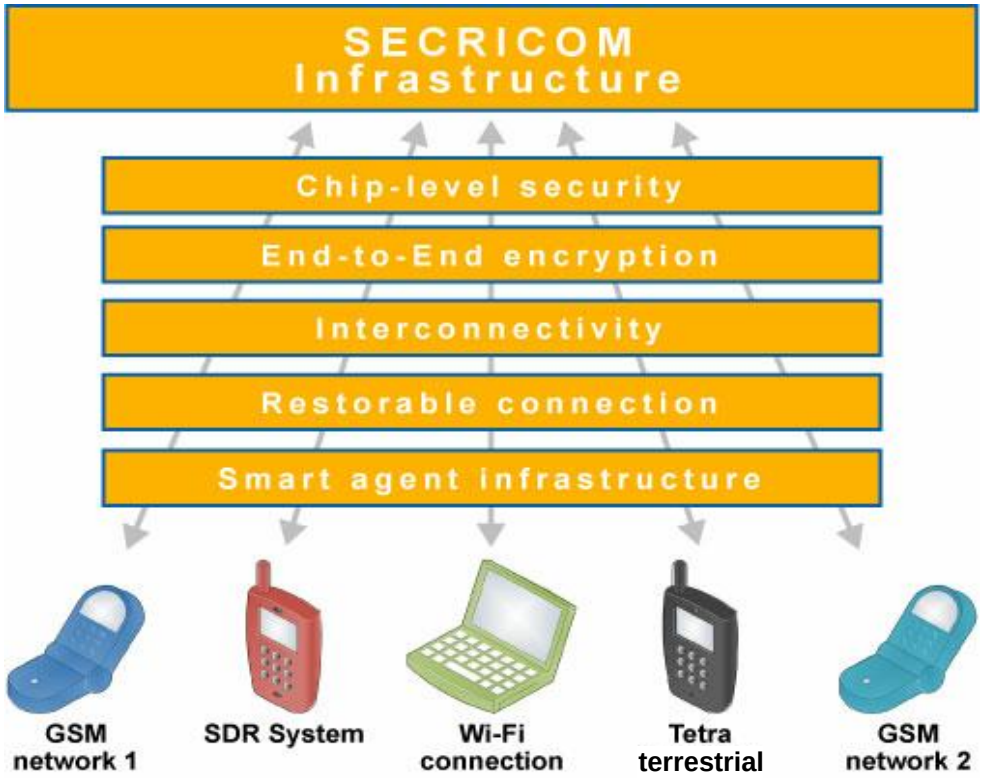
Mr Rich Edwards MIET, and
Dr Ahmed Aldabbagh CEng MIET

QinetiQ
www.QinetiQ.com

SEVENTH FRAMEWORK PROGRAMME

Presentation objectives

- Introduce the Project
- Approach Taken
- Aspects of User Requirements
- Architectures and Technology
- Wrap up



Key Project Facts

SECRICOM
Seamless Communication for Crisis Management

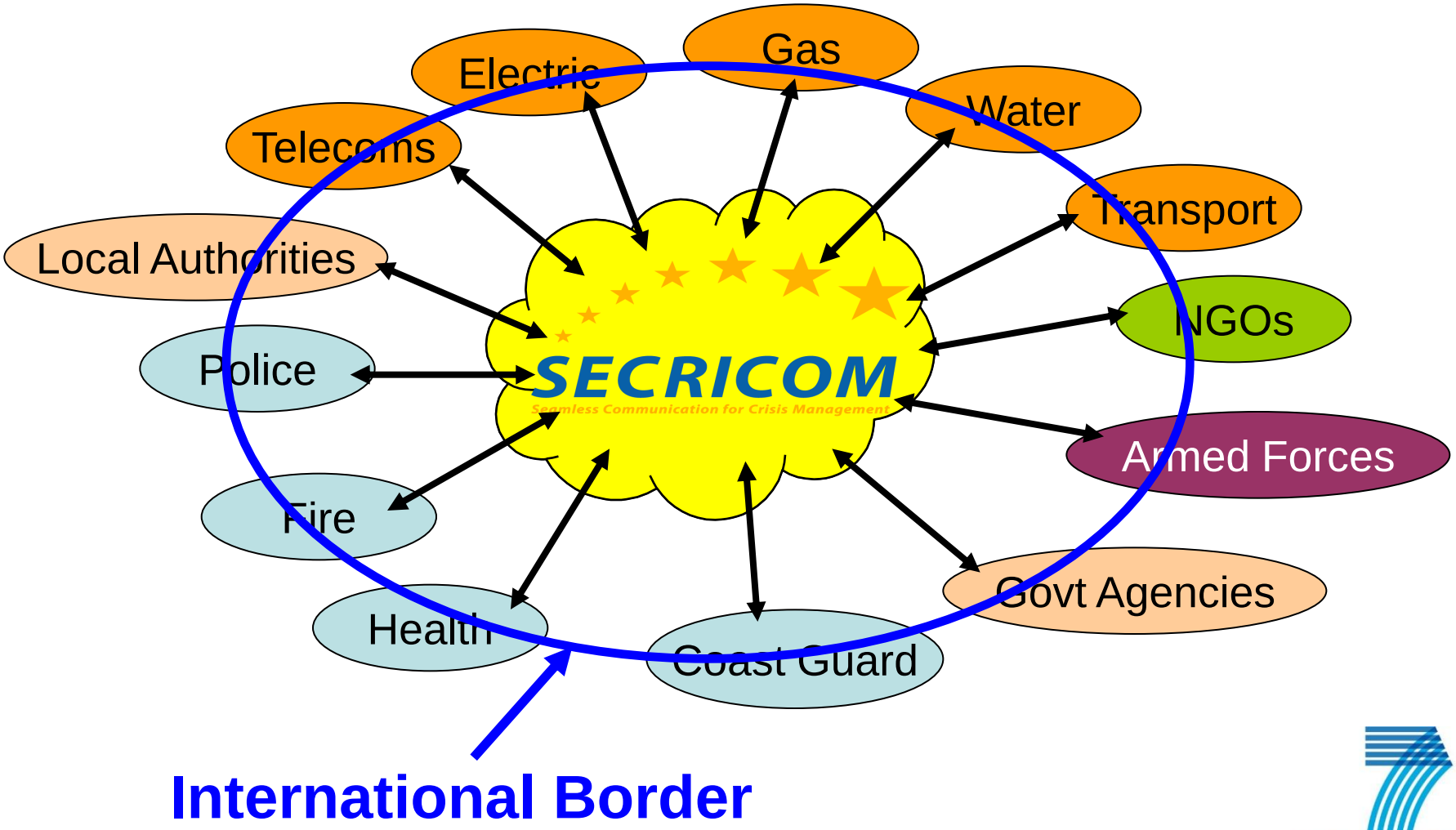
- Seventh Framework Programme – FP7
- Wireless Communication for Crisis Management
  - Multi-Agency/Multi-National

- 13 Partners
- Start date: 1 Sept 2008
- End date: 30 April 2012
- 44 months duration
- Total cost ~ €12.5M
- EU contribution ~ €8.6M

Aims

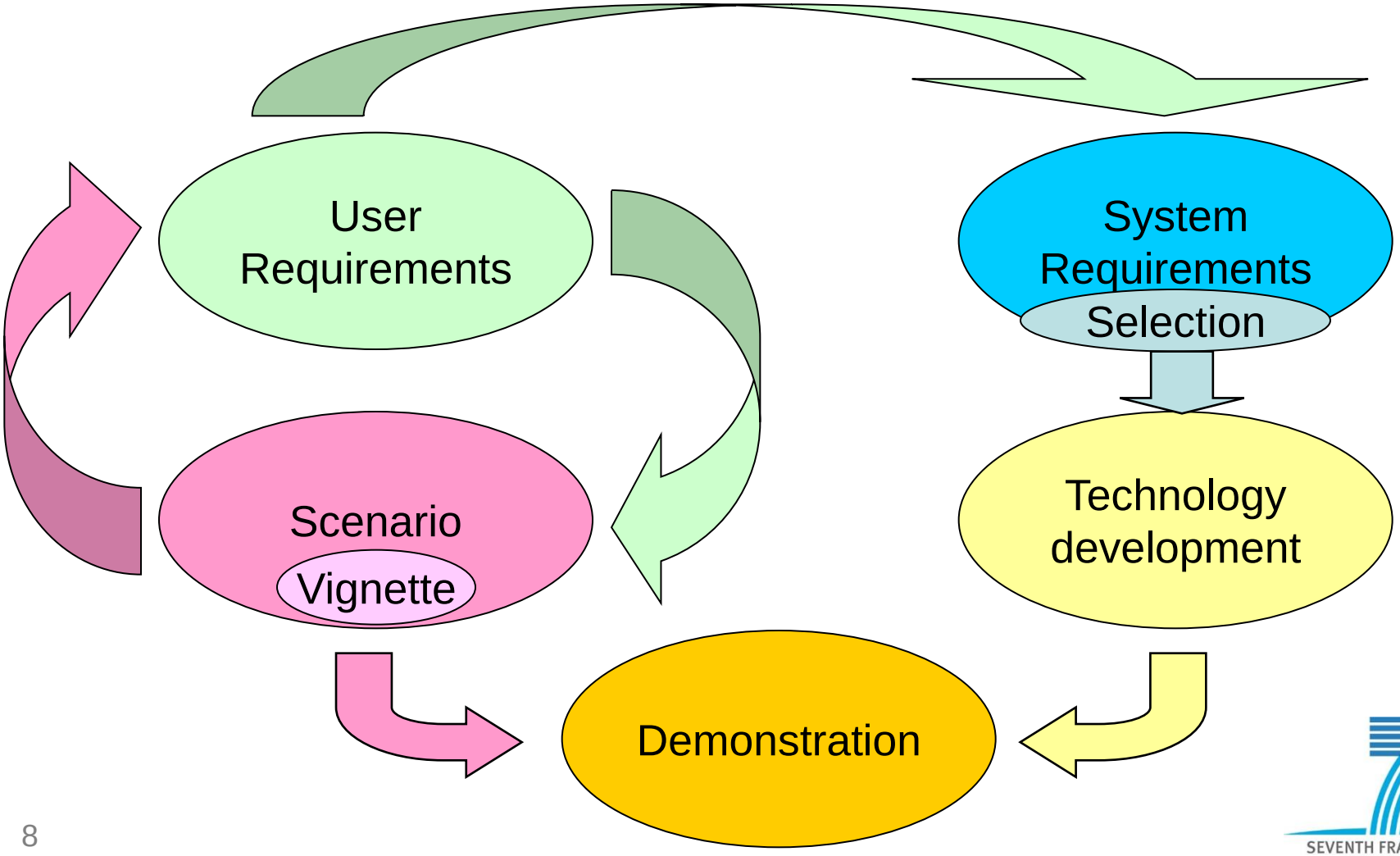
- Provision of secure seamless communications for emergency agencies at times of crisis
- Enhance interoperability among heterogeneous secure communication systems
- Enhance interconnectivity between different networks and User Access Devices
- Exploit existing communication systems
- Interface towards emerging SDR systems in a generic manner
- Mitigate the key capability gaps faced by users of existing systems

Business Stakeholders



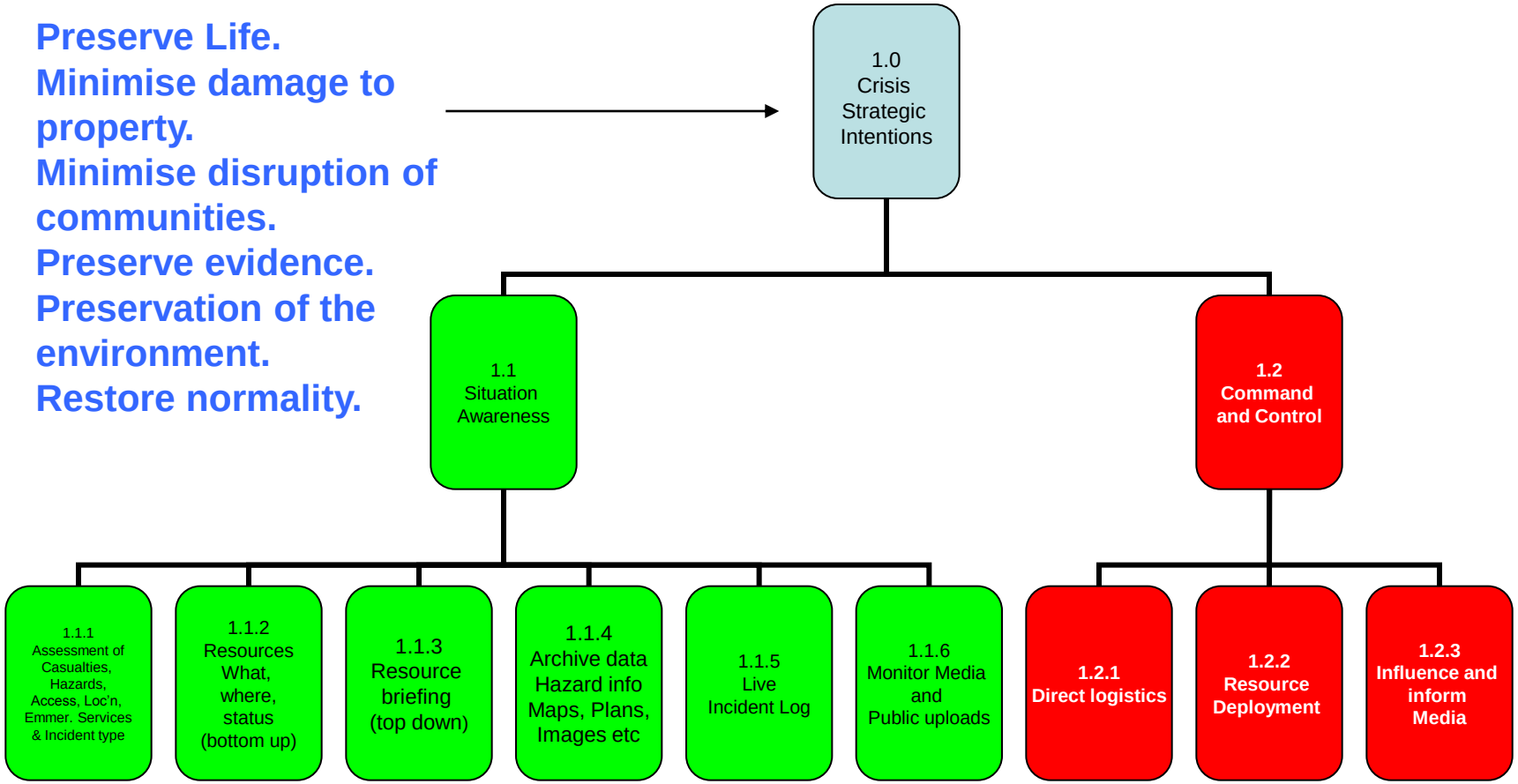
Principle of Crisis Management

Project Approach

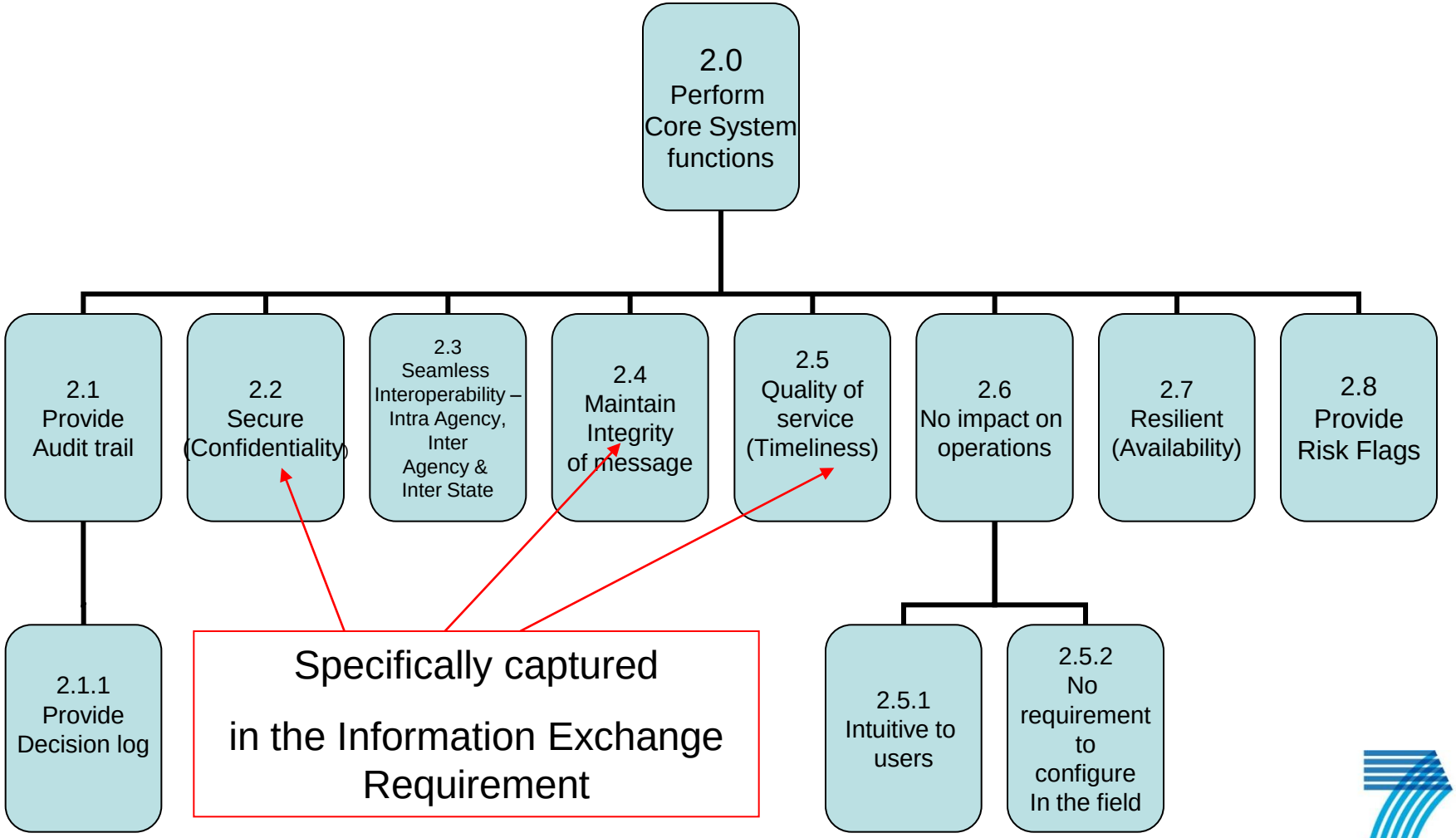


Top level User Requirements

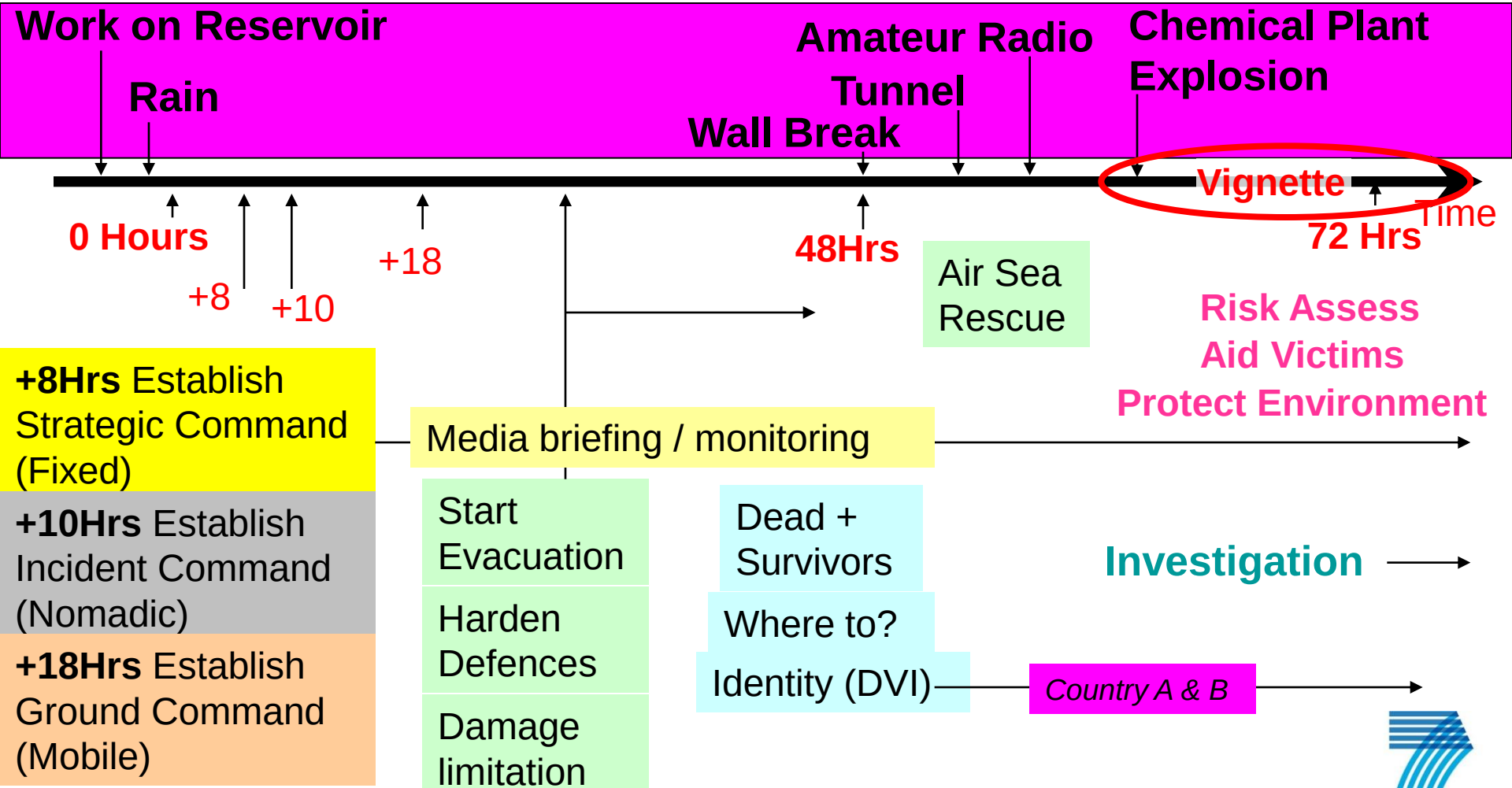
Preserve Life.
Minimise damage to property.
Minimise disruption of communities.
Preserve evidence.
Preservation of the environment.
Restore normality.



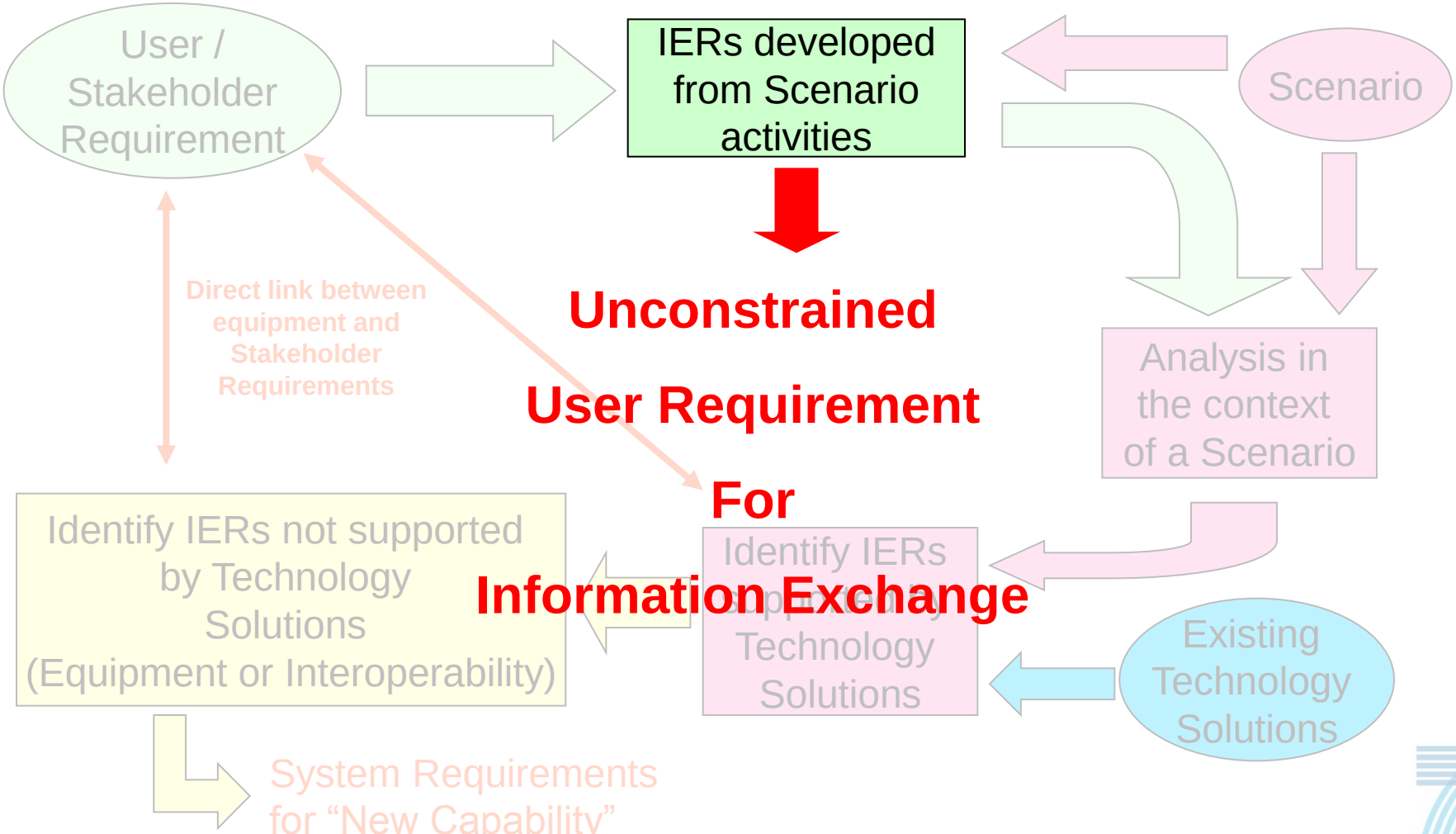
Core Functions



Scenario


Work on Reservoir
Rain
Amateur Radio
Tunnel
Wall Break
Chemical Plant Explosion
Vignette
Time
0 Hours
+8
+10
+18
48Hrs
72 Hrs
Air Sea Rescue
Risk Assess
Aid Victims
Protect Environment
+8Hrs Establish Strategic Command (Fixed)
+10Hrs Establish Incident Command (Nomadic)
+18Hrs Establish Ground Command (Mobile)
Media briefing / monitoring
Start Evacuation
Harden Defences
Damage limitation
Dead + Survivors
Where to?
Identity (DVI)
Country A & B
Investigation

Analysis of User Requirements

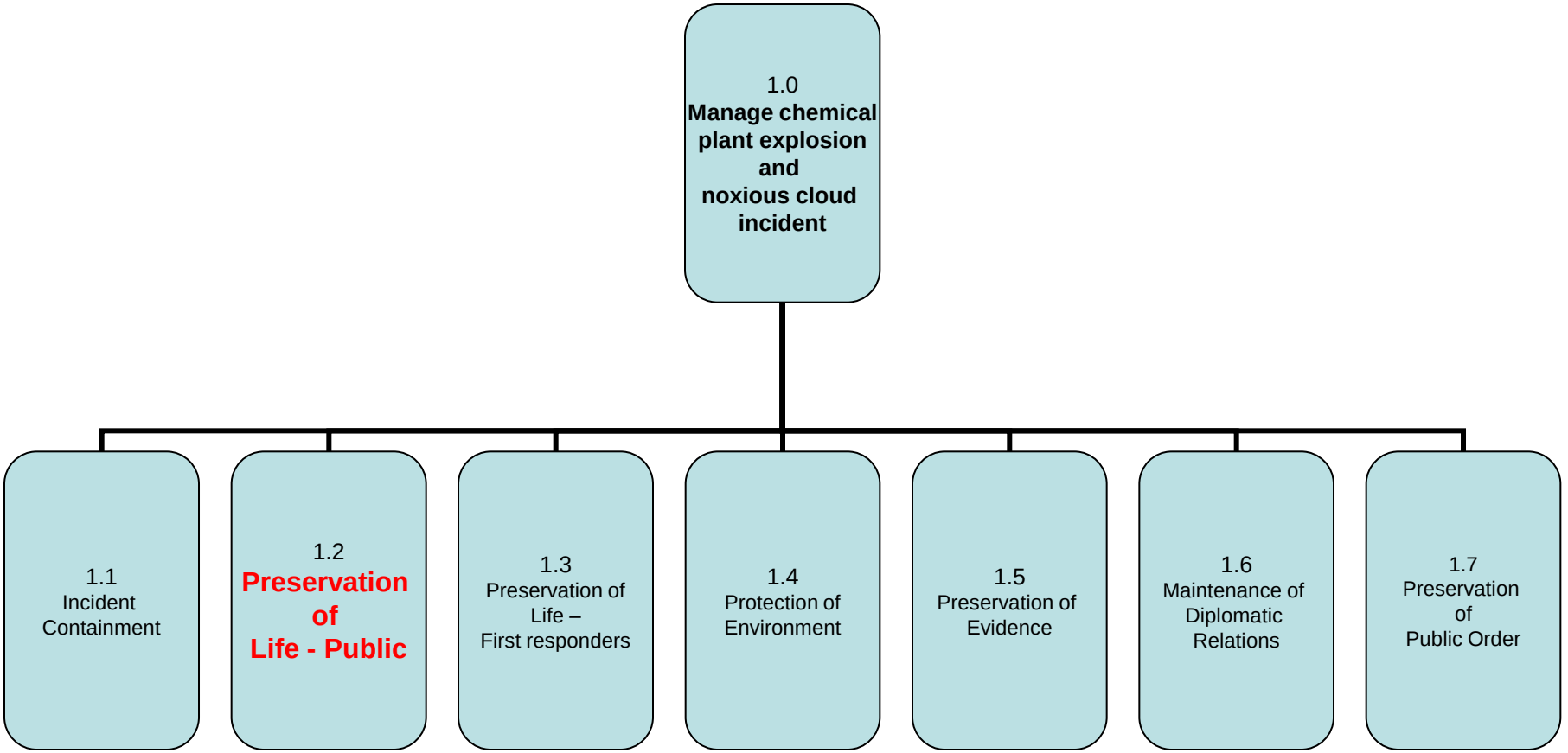


IER Capture

- User team exercise – September 2009
- Captured over 700 IERs linked to Activities
- IER Key Information criteria:
  - **Source** & **Destination**
  - **Information Type** (e.g. Voice, Messaging)
  - **Size** (linked to Information Type)
  - **Timeliness** (“worst case time to delivery”)
- Additional Information required:
  - **Criticality**
  - **Confidentiality**
  - Other analysis attributes (e.g. Business Function)

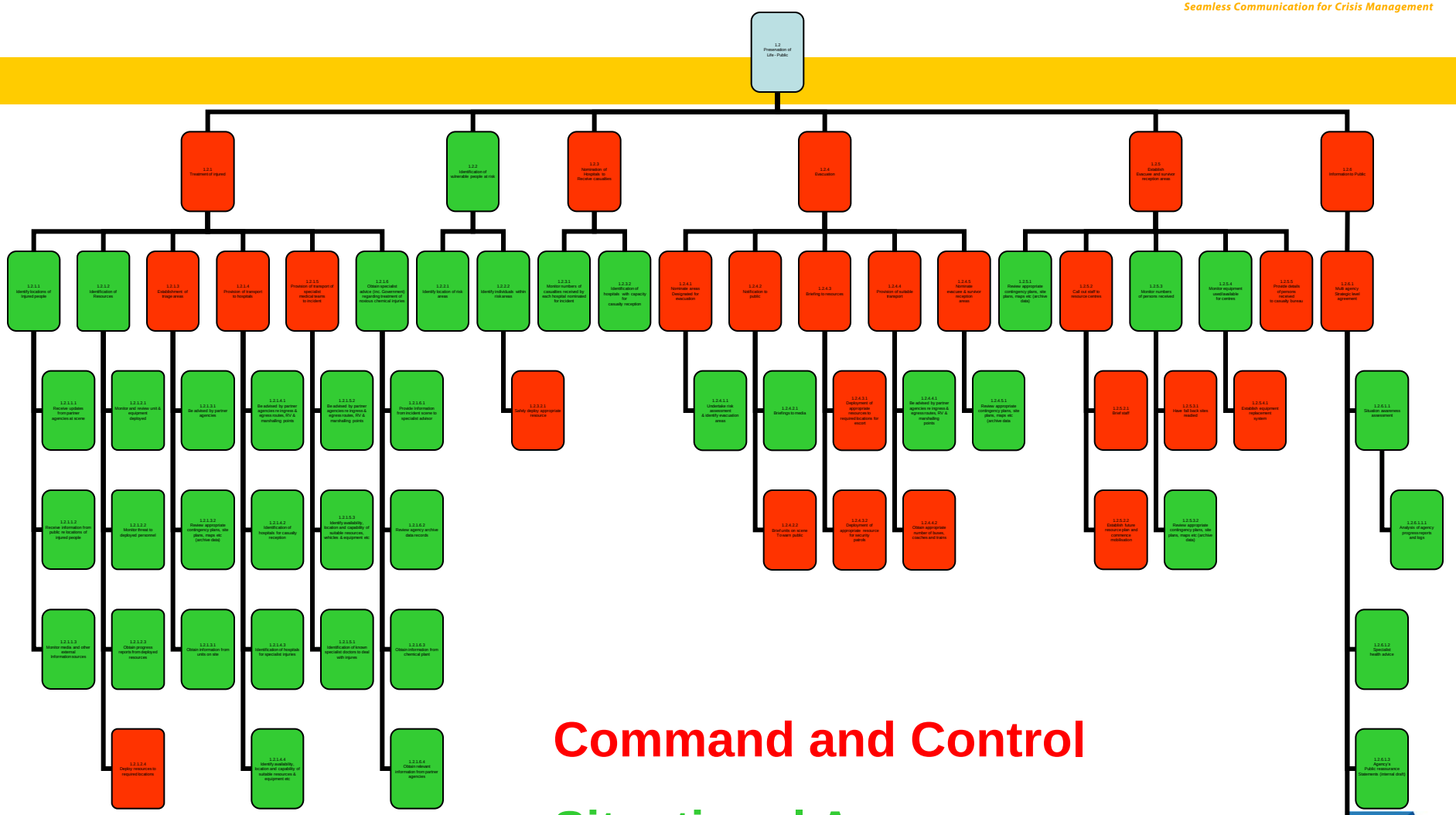
Use Case (Vignette Example)

Chemical Plant Explosion



Preservation of Life 1.2

SECRICOM
Seamless Communication for Crisis Management



Command and Control

Situational Awareness

SEVENTH FRAMEWORK PROGRAMME

Task Flow Diagrams

SECRICOM
Seamless Communication for Crisis Management

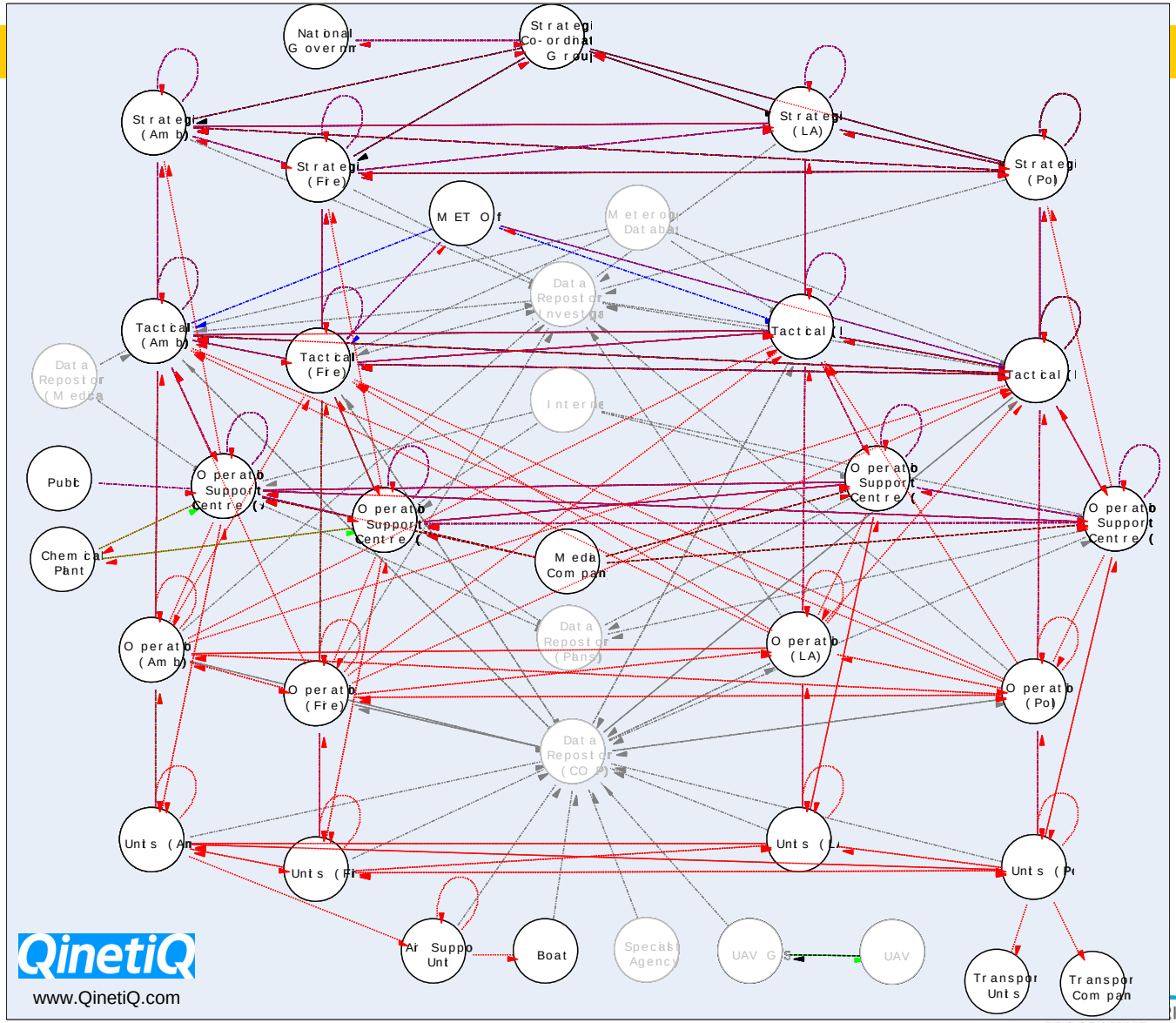
GREEN = Data (File / Imagery Transfer)
Blue = Messaging
GREY = Data Source / Web (Update / Retrieval)
BLACK = Video
RED = Voice

Crisis Management ("Standard Operating Procedures"):

Briefings / Liaison:-

- Inter-Agency
- Intra-Agency
- At all levels
- Inc. Cross Border

Dissemination of Information (Weather / News / Hazmat / Medical / Positional)

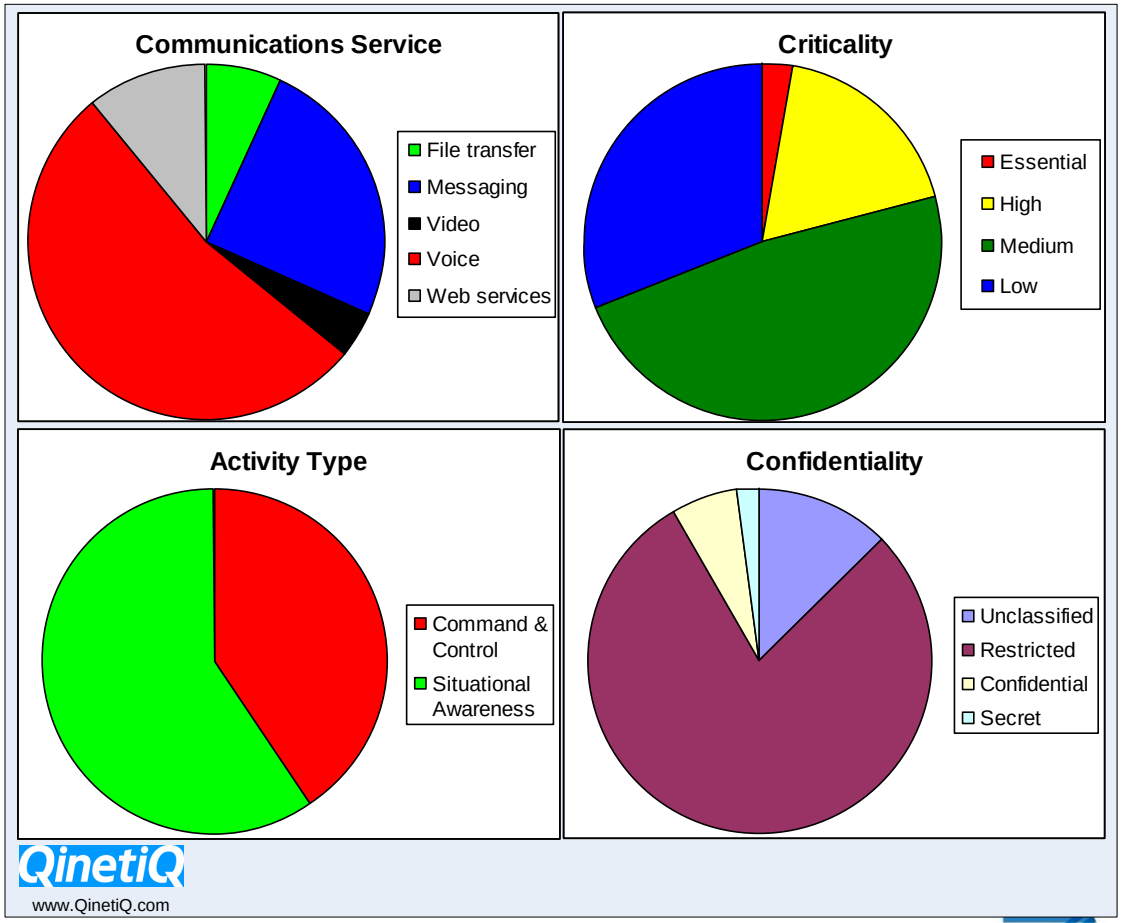


QinetiQ
www.QinetiQ.com

PROGRAMME

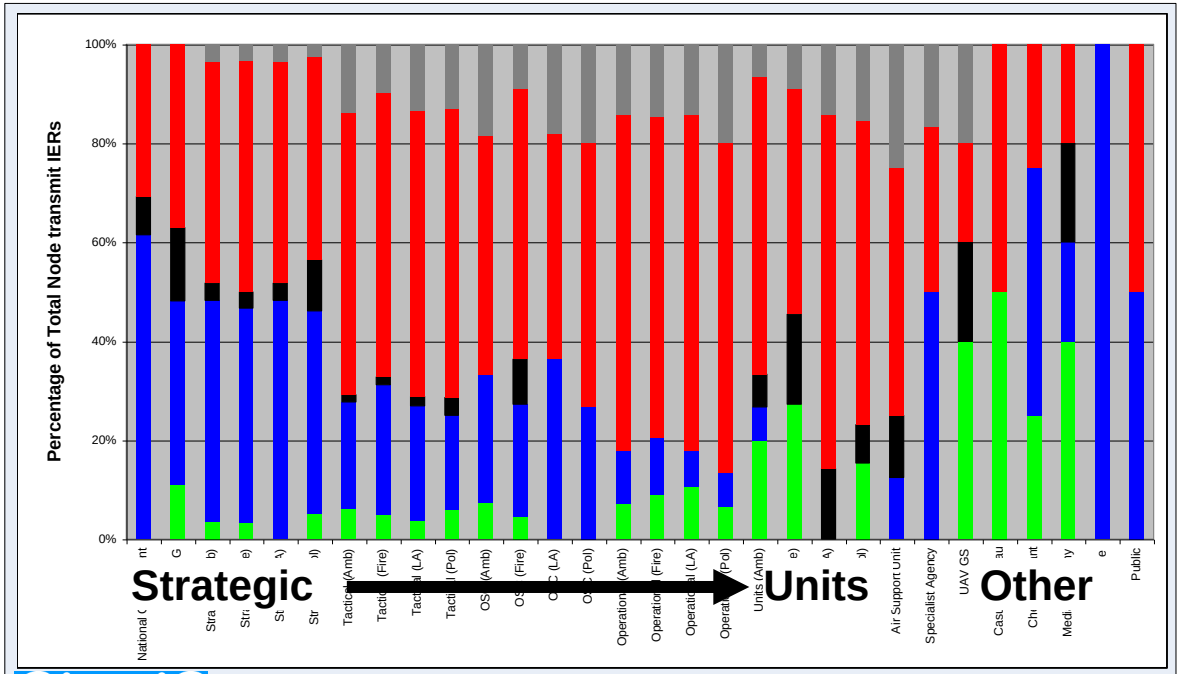
IER Summary

- 700+ IERs Captured during Main exercise and subsequent user engagement:
  - ~50% Voice, ~25% messaging (data)
  - Mostly medium criticality
  - ~75% are Restricted, ~8% are of a higher classification
  - ~60% relate to Situational Awareness activities



IER Summary

- Similar data type ratios across most nodes
  - Mostly Voice,
  - However data type of Information Exchanges account for significant proportion of IERs at lower level nodes



GREEN = Data (File / Imagery Transfer)
Blue = Messaging
GREY = Data Source / Web (Update / Retrieval)
BLACK = Video
RED = Voice

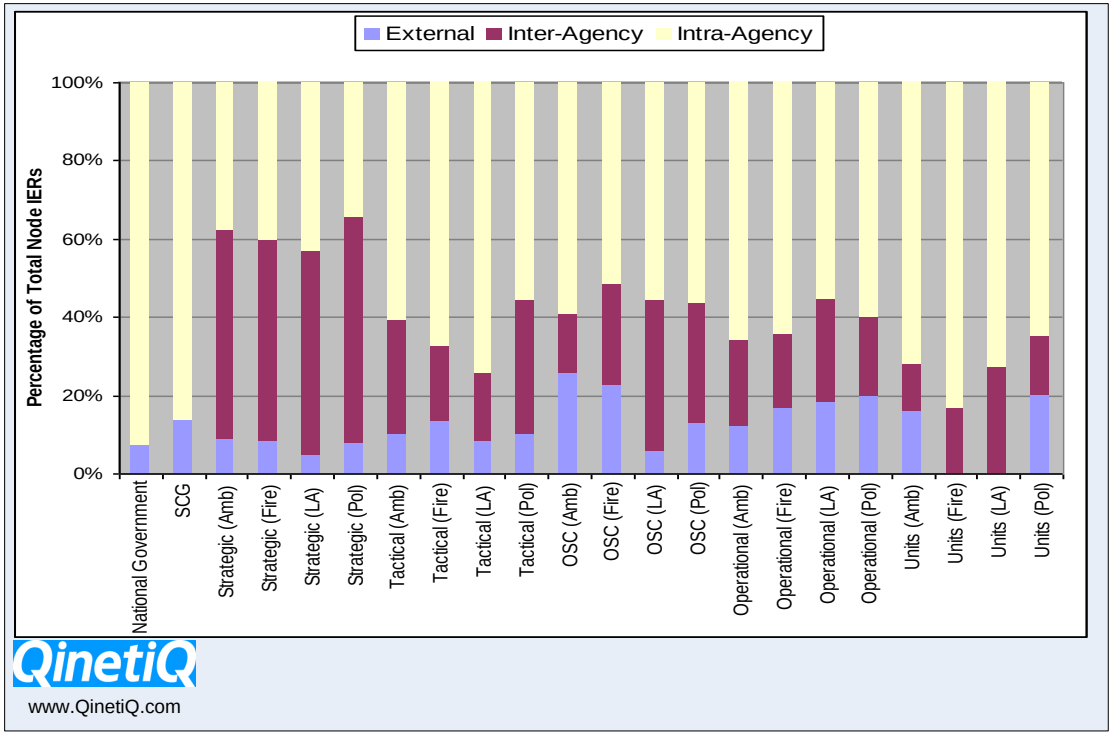
QinetiQ
www.QinetiQ.com

SECRICOM
Seamless Communication for Crisis Management

SEVENTH FRAMEWORK PROGRAMME

IER Summary

- Most communications within own agency (Intra-Agency) – **~60%** of IERs
- Inter-Agency account for **~25%** of IERs
- External account for **~10%** of IERs



Key Findings

- Voice remains (~50%) Messaging (~25%)
- Use of voice and data is inversely proportional between Strategic and Operational levels
- Intra-Agency communications is key at all levels of command
- Inter-Agency communications account for nearly a quarter of all IERs for any node
- Situation awareness is the greatest proportion of IERs (~59%)
  - Ratio of C2 to Situational Awareness is close to 3:2 due to voice & data versions of the same IER (i.e. voice command backed-up with data type IER).
- Voice remains most significant IER data type for both C2 and Situation Awareness however Situational Awareness demands a greater use of non-voice data types

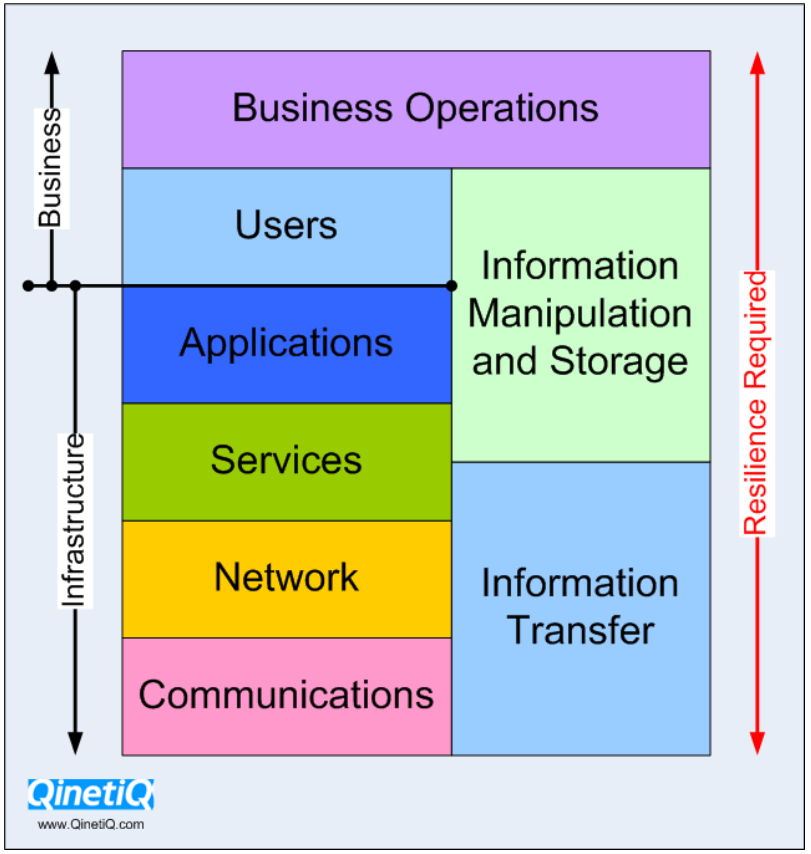
Applications: Current & Future

	Information Exchange Type				
Application	*File Transfer*	*Messaging*	*Video*	*Voice*	*Web Services*
Mobile Office	Yes	Yes	Yes	Yes	Yes
Images	Yes	Yes			Yes
Biometric Data	Yes				Yes
Number Plate Recognition	Yes				Yes
Mapping and Location Services	Yes	Yes			Yes
Remote Database Access	Yes				Yes
Personnel Monitoring		Yes			
Sensor Devices		Yes	Yes	Yes	
Remotely Controlled Vehicles		Yes	Yes	Yes	Yes
Non-Real Time Video	Yes				Yes
Non-Real Time Voice	Yes				Yes
Real Time Video			Yes	Yes	
Real Time Voice				Yes	
Collaborative Tools	Yes	Yes	Yes	Yes	Yes

Critical IT Infrastructure

- Critical IT infrastructures require *resilience* to support business continuity during critical/non-critical business operations:
  - Robustness during stressed times
  - Robustness against natural failures
  - Graceful degradation: by design and not luck

Behind Every Resilient IT-Reliant Business is Resilient Data Networks/Communications



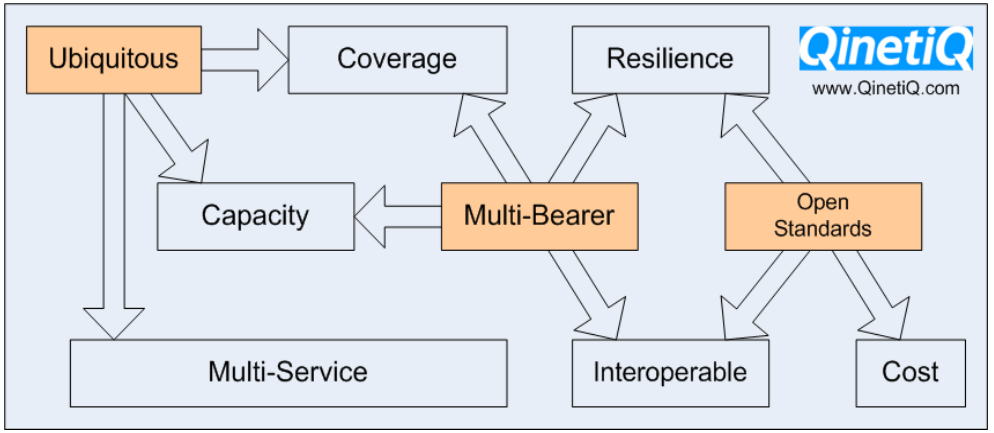
System Requirements for Networks and Communications

Requirements	***Implications***	***IP Support for Requirements/Implications***
Functionality	*Multi-Services*	Ability to Support Multi-Media and Data Services that Underpins the Applications mentioned previously
Connectivity	*Coverage*	Standard Technology with the Highest Penetration into Government IT combined with Wireless Technology
	Capacity	Scalability through a Vast Address Space
	Projection into Theatre	Nomadicity and Mobility is well Supported aided by Supporting Wireless/Mobile Communication Technology
Reliability	*Resilience*	Resilience is Achievable through Standard Techniques
	Security	Matured VPN Technology either End-to-End/Otherwise
Deployability	*Interoperability*	Highest Penetration into Government, UK and EU-Wide
	Cost	Cost Effectiveness through Diversity of Suppliers Leading to Vendor-Unlocking and Support for Multi-Services

Ubiquitous Services to Support of End User Applications

Avoidance of reliance on a single comms system/provider

- Make simultaneous use of TETRA, 3G, GSM, WiFi, WiMax, Satellite, SDR, etc

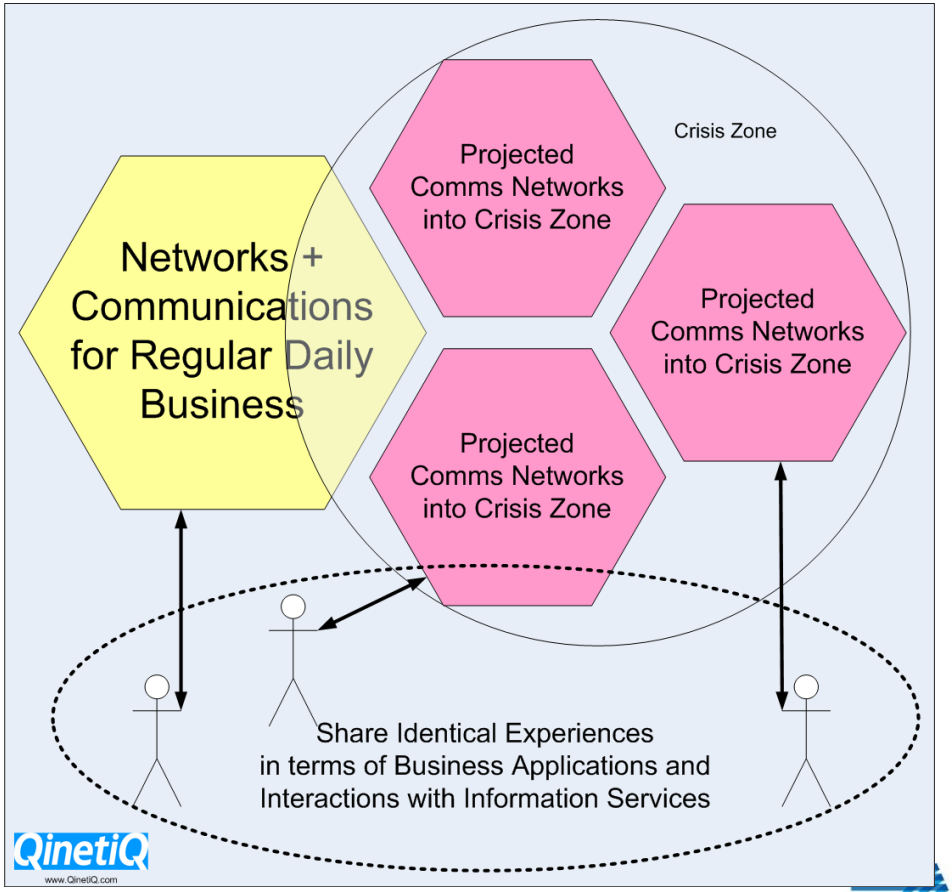


Usage of open/non-proprietary standards

- Network: IPv6 as the principle standard for networking
- Wireless: 3G, GSM, WiFi, WiMax, TETRA, Satellite, etc
- Fixed: Ethernet

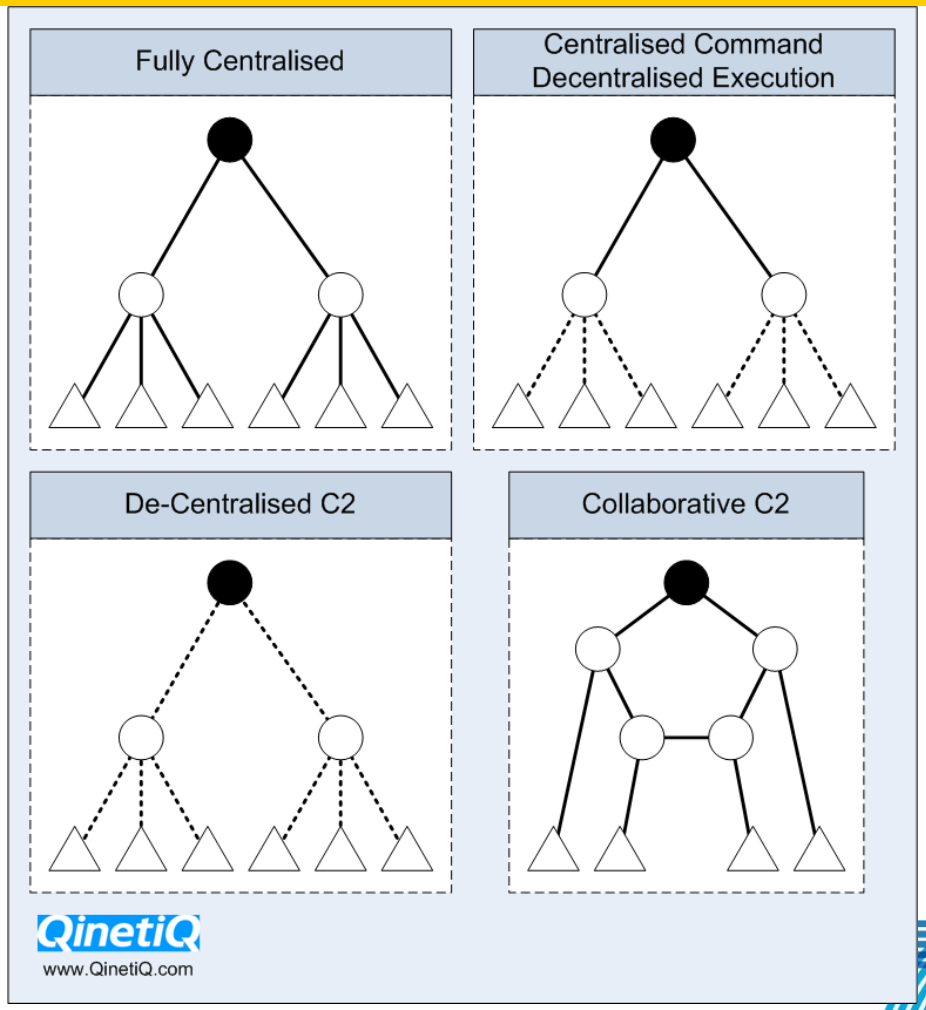
Projection of Networks and Communications into Crisis Zone

- Assumption: Networks and Comms don't Necessarily Survive in the Crisis Zone.
- Need the Ability for Networks and Comms Re-Establishment
  - Multi National, and
  - Multi Agency.
- User Experience.

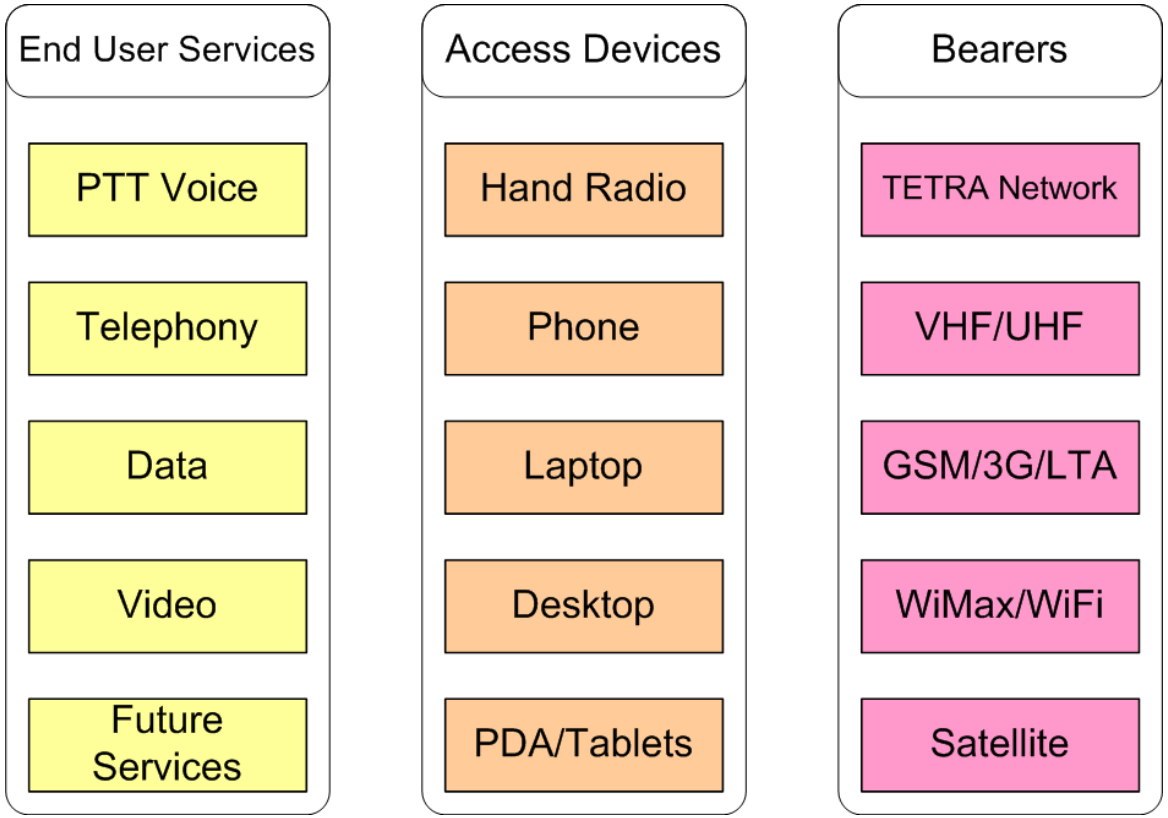


IP Support for C2

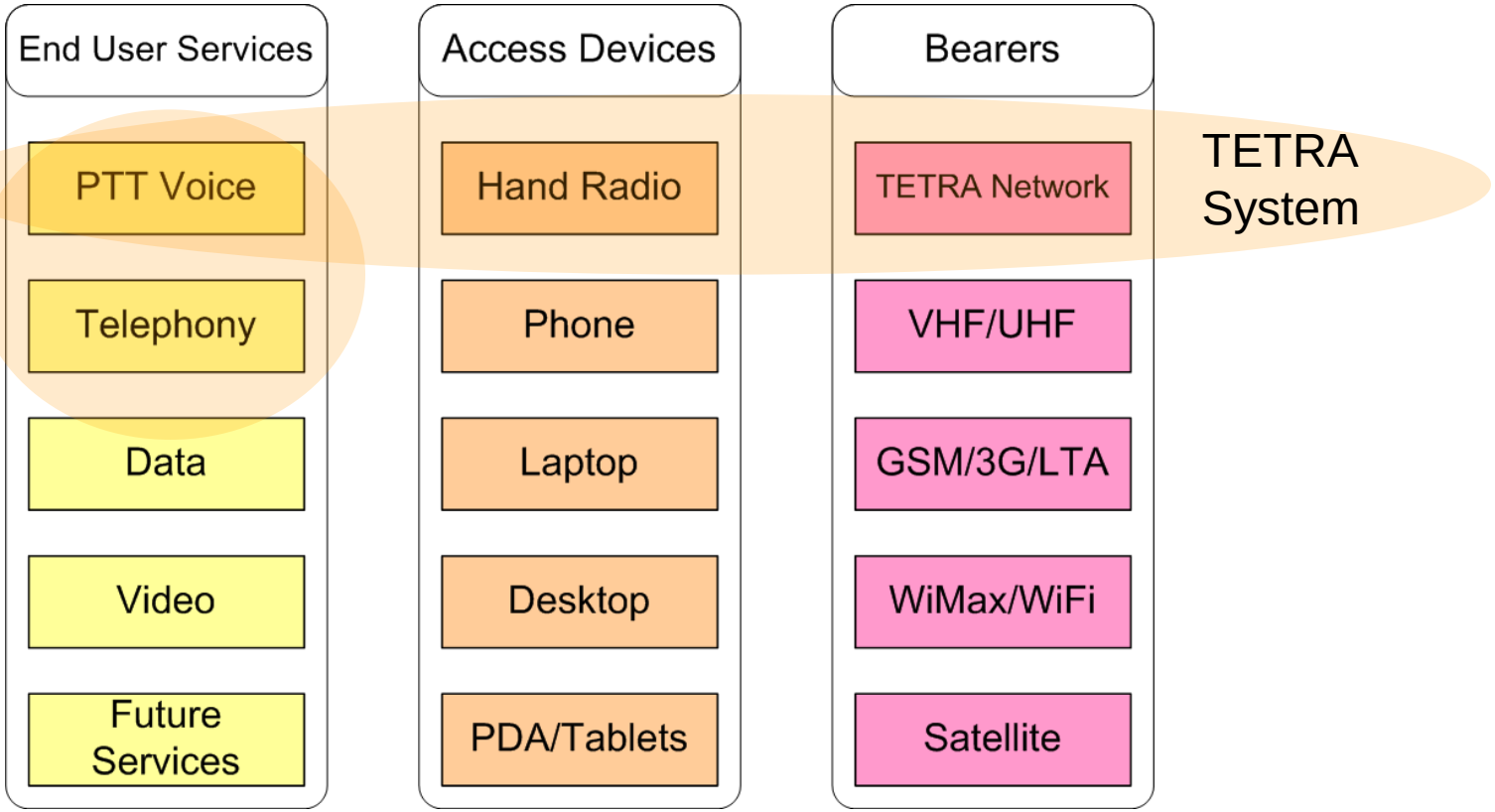
- Different C2 Structures for Different
  - Agencies
  - Operations
    e.g. multi-agency
- IP Supports all Types of C2 Structures with Soft Configuration



Services, Access Devices and Bearers



In-Service Systems

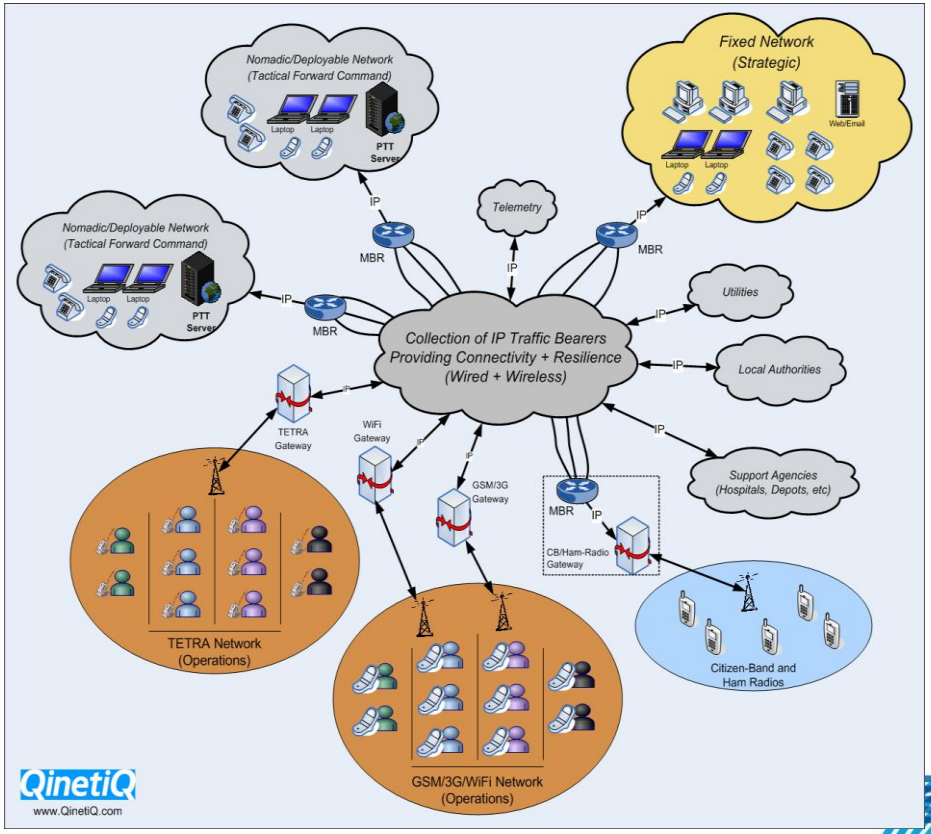


System Requirements for Networks and Communications: High Level View

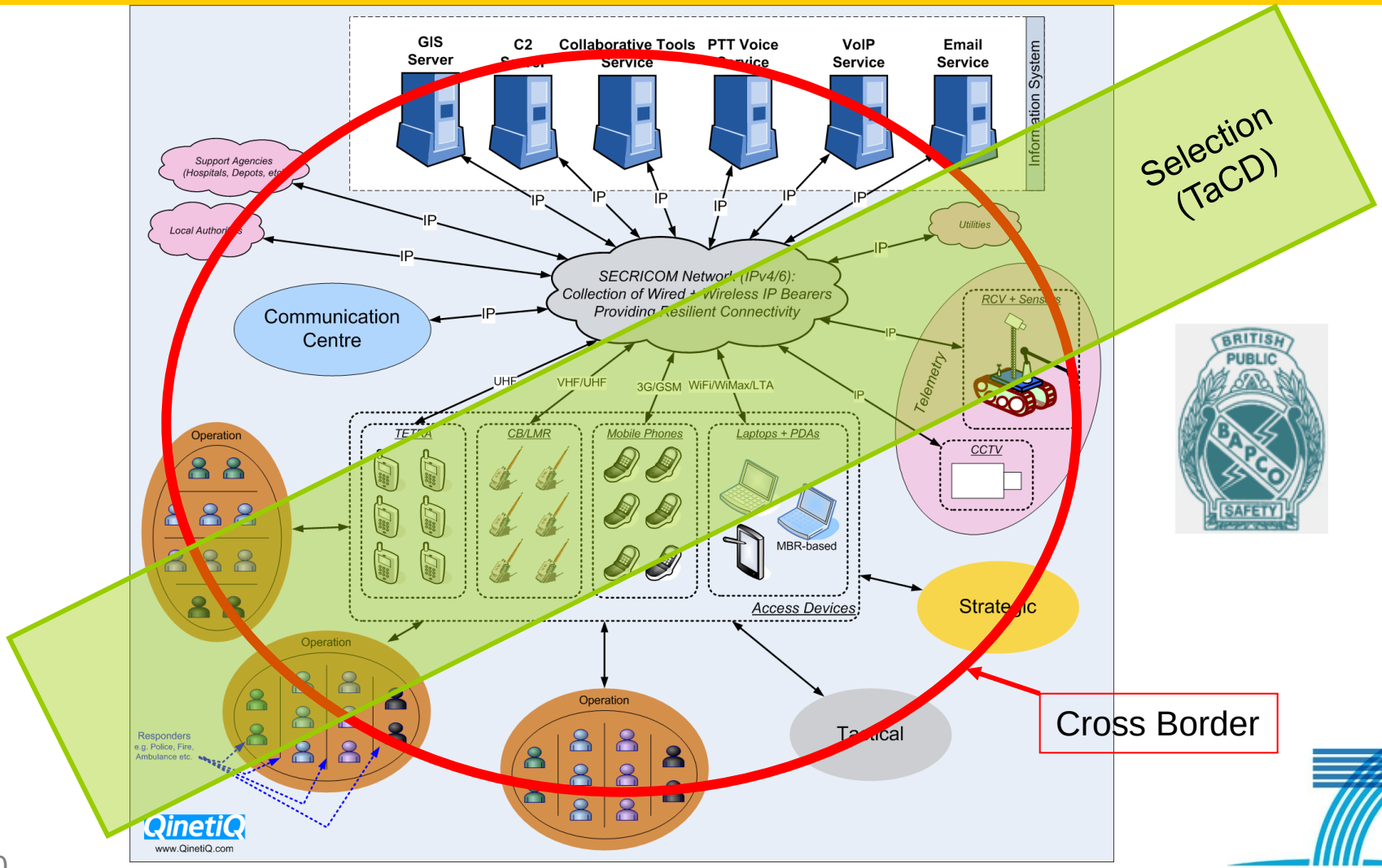
The Networks/Comms System Architecture Allows:

•<u>Technical Interoperability:</u>
Able to extend comms across different agencies and countries.

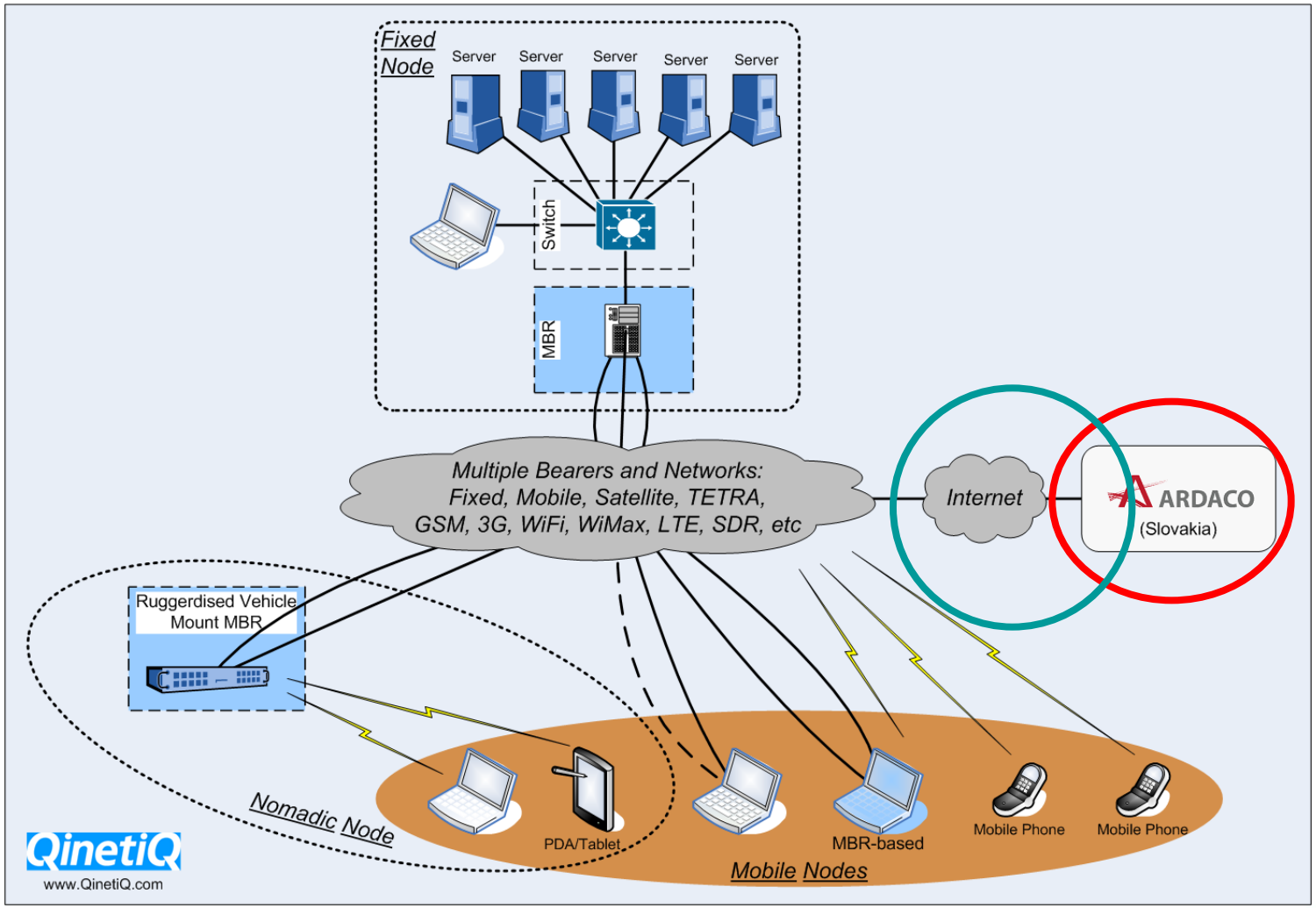
•<u>Service Extensibility:</u>
Able to extend comms into the crisis zone and/or areas of poor coverage.



SECRICOM Plan



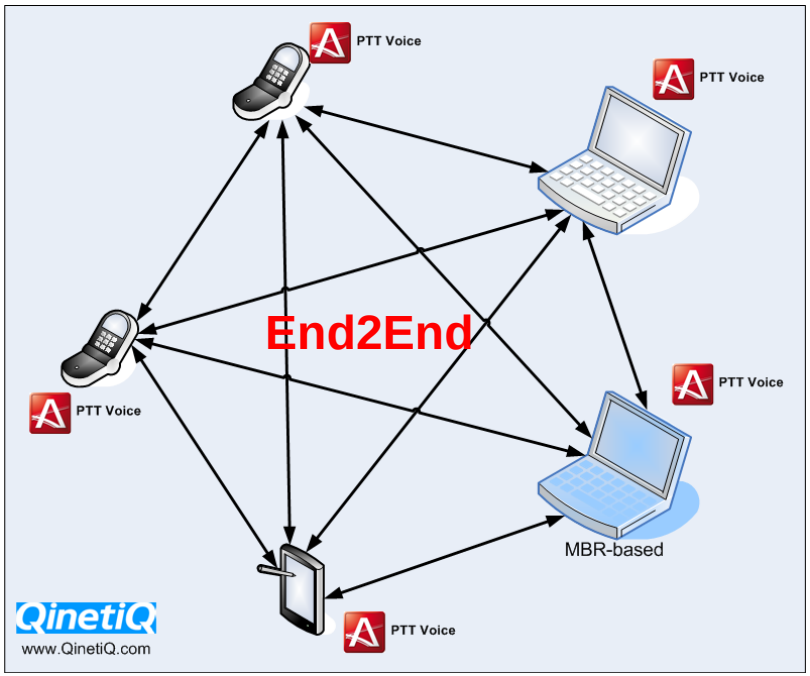
Technology and Capability Demonstrator (TaCD) – Selection

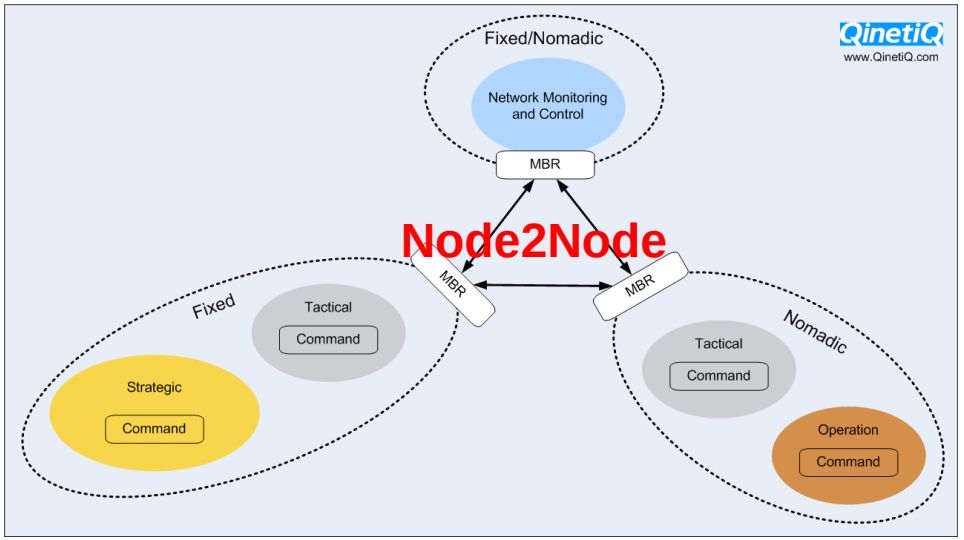


System Requirements: Security/ Confidentiality

This is being tackled in two ways:

- End-device to End-Device; and Node to Node





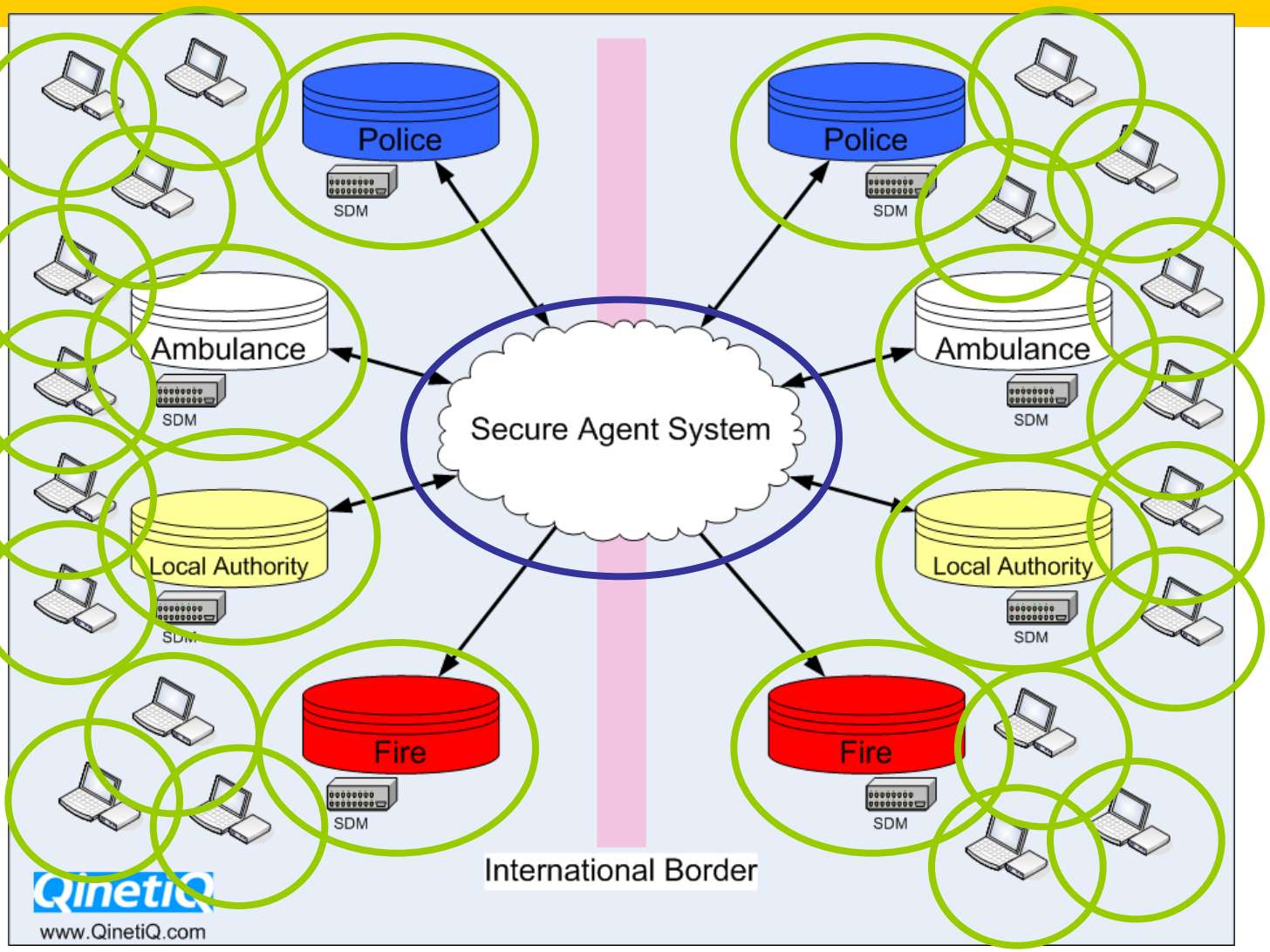
System Requirements: Security/ Integrity

- ***System Integrity:*** is the terminal/computer platform you are using being breached? Has the platform integrity been compromised?
  - Malware, Trojan horses, etc

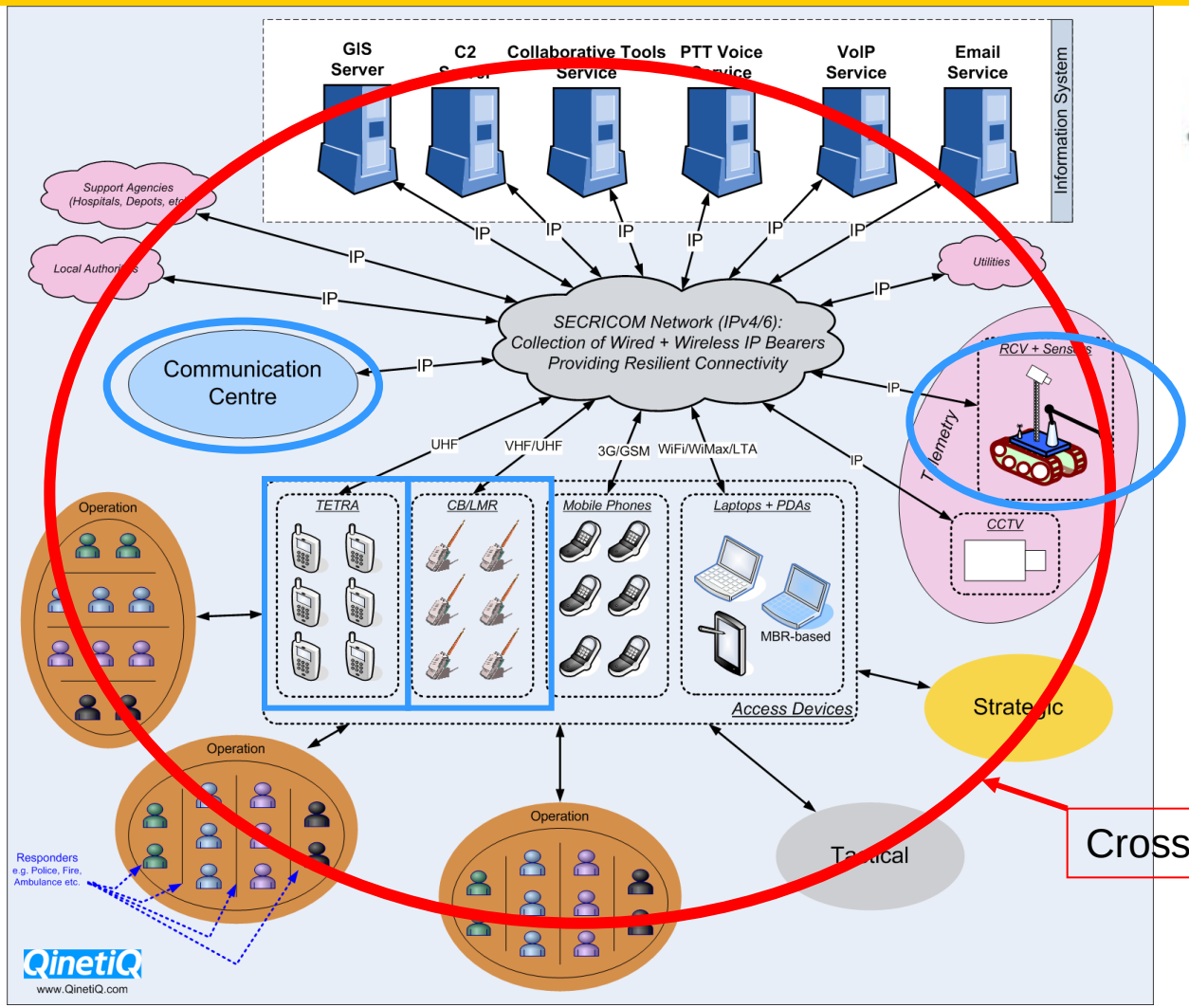
- ***Information Exchange Integrity:*** in a multi-agency/multi-national scenario, how is 'trust' established in an agency's database?
  - Issues:
    - Is the query made from a trusted entity?
    - Should the requesting entity be given access to this info?
    - Is the information in the response trusted?

Communications System Requirements: Integrity

Device Integrity



SECRICOM Future Plans



Cross Border

Concluding Remarks

- Ability for responders to operate across different European emergency services / responder agencies as one cohesive unit at the time of a crisis

- Secure communication system during a crisis with technical interoperability & resilience built into the design

Acknowledgements

- BAPCO
  - Mr Jim A'Court (London Fire Brigade)
  - Mr Aaron Goddard (Northamptonshire Local Authority)
  - Mr Peter Kendall (Department of Health)
  - Mr Simon Moase (Hampshire Constabulary)
- National Police Board (Sweden)
  - Mr Matt Persson
- Departmento De Interior (Bilbao)
  - Elena Moreno Zaldibar
  - Jose Ignacio Trancho Elorriaga

Thank you for your attention

Visit SECRICOM at Stand 217a

SEVENTH FRAMEWORK PROGRAMME